

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA,

v.

KEITH RANIERE,

Defendant.

-----X

Case No. 1:18-cr-00204-NGG-VMS

**EXHIBITS IN SUPPORT OF MOTION TO  
VACATE JUDGMENT AND GRANT A  
NEW TRIAL PURSUANT TO RULE 33**

**EXHIBITS IN SUPPORT OF  
DEFENDANT KEITH RANIERE'S MOTION FOR RULE 33 RELIEF**

Dated: May 3, 2022,  
Martinez, CA

Joseph M. Tully  
CA SBN 201187  
Tully & Weiss Attorneys at Law  
713 Main Street  
Martinez, CA 94553  
Phone: (925) 229-9700  
Fax: (925) 231-7754

*Attorneys for Defendant Keith Ranieri*

**TABLE OF CONTENTS**

EXHIBIT A ..... - 3 -  
(FBI's Field Evidence Management Guide) ..... - 3 -  
EXHIBIT B..... - 4 -  
(Trial Exhibit 961)..... - 4 -  
EXHIBIT C..... - 5 -  
(FBI's Digital Evidence Guide) ..... - 5 -  
EXHIBIT D ..... - 6 -  
(Report of Dr. James Richard Kiper, Ph.D)..... - 6 -  
EXHIBIT D1 ..... - 7 -  
(CV of Dr. James Richard Kiper, Ph. D)..... - 7 -  
EXHIBIT E ..... - 8 -  
(Report of Steven Abrams)..... - 8 -  
EXHIBIT E1 ..... - 9 -  
(CV of Steven Abrams) ..... - 9 -  
EXHIBIT F ..... - 10 -  
(Report of Wayne B. Norris) ..... - 10 -  
EXHIBIT F1 ..... - 11 -  
(CV Of Wayne B. Norris)..... - 11 -  
EXHIBIT G ..... - 12 -  
(SW- 8 Hale Drive)..... - 12 -  
EXHIBIT G1 ..... - 13 -  
(Return on SW - 8 Hale Drive)..... - 13 -  
EXHIBIT H ..... - 14 -  
(Defense Discovery Request – 3/16/2022) ..... - 14 -  
EXHIBIT H1 ..... - 15 -

(Correspondence From Defense Re Discovery Request) .....- 15 -  
EXHIBIT H2 .....- 16 -  
(Correspondence From Government Re Discovery Request) .....- 16 -  
EXHIBIT H3 .....- 17 -  
(Correspondence From Government Re Discovery Request) .....- 17 -  
EXHIBIT I.....- 18 -  
(Discovery Letter April 29, 2019) .....- 18 -

# **EXHIBIT A**

**(FBI's Field Evidence Management Guide)**

**Field Evidence Management and Operations  
Policy Implementation Guide (PG)**



**Federal Bureau of Investigation (FBI)**

**0120PG**

**October 27, 2009**

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

**UNCLASSIFIED  
FOR OFFICIAL USE ONLY**

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**GENERAL INFORMATION:**

Questions or comments pertaining to this handbook can be directed to:

**FBIHQ/Laboratory Division  
Forensic Analysis Branch  
Evidence Control Unit**

**Division Point of Contact:**

**Field Evidence Program Manager**

b6  
b7c

**(NOTE: This document supersedes all existing policy contained in MAOP Sections 2-4.4.1 through 2-4.4.15, 2-4.4.17, and 2-4.4.18)**

**PRIVILEGED INFORMATION:**

**Any use of this report, including direct quotes or identifiable paraphrasing, will be marked with the following statement:**

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

Table of Contents

- 1. (U//FOUO) Scope .....1
- 2. (U//FOUO) Roles and Functional Responsibilities .....2
  - 2.1. (U//FOUO) Assistant Directors in Charge (ADIC) and Special Agents in Charge (SAC)..... 2
  - 2.2. (U//FOUO) Field Evidence Program Manager (PM) ..... 2
  - 2.3. (U//FOUO) Evidence Control Technicians and Alternate Evidence Control Technicians ..... 3
- 3. (U//FOUO) Policies .....4
- 4. (U//FOUO) Procedures and Processes .....5
  - 4.1. (U//FOUO) Evidence ..... 5
    - 4.1.1. (U//FOUO) Form FD-597 (Receipt for Property Received/Returned/Released/Seized) ..... 5
    - 4.1.2. (U//FOUO) Chain-of-Custody (FD-1004)..... 5
  - 4.2. (U//FOUO) Evidence Control Room (ECR)..... 5
    - 4.2.1. (U//FOUO) Designated ECR ..... 5
    - 4.2.2. (U//FOUO) Personal Protective Supplies ..... 5
    - 4.2.3. (U//FOUO) Large Volume of Evidence ..... 5
    - 4.2.4. (U//FOUO) Form FD-455 (Access Log - Evidence Storage Facility)..... 6
    - 4.2.5. (U//FOUO) Access to the ECR..... 6
    - 4.2.6. (U//FOUO) Large Seizures After Hours..... 6
    - 4.2.7. (U//FOUO) Access to the Drug/Valuable Vault..... 6
    - 4.2.8. (U//FOUO) Emergency Access to the Drug/Valuable Vault..... 7
    - 4.2.9. (U//FOUO) Refrigerator/Freezer ..... 7
    - 4.2.10. (U//FOUO) Biohazard Warning Label ..... 7
  - 4.3. (U//FOUO) ECR Construction ..... 7
    - 4.3.1. (U//FOUO) General Evidence ECR..... 7
    - 4.3.2. (U//FOUO) Drug Evidence Room..... 8
    - 4.3.3. (U//FOUO) Valuable Evidence Room..... 9
    - 4.3.4. (U//FOUO) Federal Grand Jury Room ..... 9
    - 4.3.5. (U//FOUO) Computer Analysis Response Team (CART) Room ..... 9
    - 4.3.6. (U//FOUO) Off-Site Evidence Control Rooms ..... 10
  - 4.4. (U//FOUO) ECR Security..... 10
    - 4.4.1. (U//FOUO) Drug and Valuable Evidence Rooms ..... 10
    - 4.4.2. (U//FOUO) Personal Identification Numbers..... 11
    - 4.4.3. (U//FOUO) Combinations ..... 11
    - 4.4.4. (U//FOUO) Access Removal ..... 11
    - 4.4.5. (U//FOUO) Access Log Printed and Retained..... 11
    - 4.4.6. (U//FOUO) Changing Combinations..... 11
    - 4.4.7. (U//FOUO) Off-Site Alarms..... 11
  - 4.5. (U//FOUO) Responsibilities of the Evidence Control Technician ..... 11
    - 4.5.1. (U//FOUO) General Familiarity ..... 11

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

- 4.5.2. (U//FOUO) Access to the ECR..... 12
- 4.5.3. (U//FOUO) Protective Clothing/Equipment..... 12
- 4.5.4. (U//FOUO) Hazardous Materials (HAZMAT) Transportation Training..... 12
- 4.5.5. (U//FOUO) Collected Item Database..... 12
- 4.5.6. (U//FOUO) Recordkeeping, Storage, and Maintenance of Evidence..... 12
- 4.5.7. (U//FOUO) Ten Calendar-Day Rule for Submission ..... 12
- 4.5.8. (U//FOUO) Ten Calendar-Day Rule for Capture in the Collected Item Database 13
- 4.5.9. (U//FOUO) Location of Property..... 13
- 4.5.10. (U//FOUO) Chain-of-Custody Documentation ..... 14
- 4.5.11. (U//FOUO) Forwarding Evidence ..... 14
- 4.5.12. (U//FOUO) Retrieving Evidence from the ECR..... 14
- 4.5.13. (U//FOUO) Non-Evidentiary Property ..... 14
- 4.5.14. (U//FOUO) Closed Cases with Pending Evidence ..... 14
- 4.5.15. (U//FOUO) Disposing of Property..... 14
- 4.5.16. (U//FOUO) Testify in Court ..... 14
- 4.5.17. (U//FOUO) Evidence Response Team..... 15
- 4.5.18. (U//FOUO) Inspects Field Office Evidence Programs ..... 15
- 4.5.19. (U//FOUO) Conducts Training and Assessments..... 15
- 4.5.20. (U//FOUO) Top Secret Evidence..... 15
- 4.6. (U//FOUO) Administrative Handling and Storage of Evidentiary Property ..... 15
- 4.6.1. (U//FOUO) For Pre-automated Evidence Only: ..... 19
- 4.6.2. (U//FOUO) Assessment Evidentiary Property..... 20
- 4.7. (U//FOUO) General Evidence ..... 21
- 4.7.1. (U//FOUO) Items of Evidence..... 21
- 4.7.2. (U//FOUO) Documentary Items ..... 21
- 4.7.3. (U//FOUO) Electronic Surveillance (ELSUR) Evidence ..... 22
- 4.7.4. (U//FOUO) Blood/Liquid Stained Clothing Evidence ..... 22
- 4.7.5. (U//FOUO) Storing and/or Shipping Blood-Stained Garments..... 22
- 4.8. (U//FOUO) Firearms Evidence..... 22
- 4.8.1. (U//FOUO) By Statutes..... 23
- 4.8.2. (U//FOUO) By Other Means ..... 23
- 4.8.3. (U//FOUO) Abandoned ..... 23
- 4.8.4. (U//FOUO) Seized/Recovered ..... 24
- 4.8.5. (U//FOUO) Rendered Safe ..... 24
- 4.8.6. (U//FOUO) Stored ..... 24
- 4.8.7. (U//FOUO) Contraband Items ..... 24
- 4.8.8. (U//FOUO) Destruction ..... 25
- 4.8.9. (U//FOUO) Accepted Legal Documentation for Destruction..... 25
- 4.8.10. (U//FOUO) Package for Shipping ..... 25
- 4.9. (U//FOUO) Drug Evidence..... 25
- 4.9.1. (U//FOUO) Maximum Security ..... 25
- 4.9.2. (U//FOUO) Storage Facility ..... 25
- 4.9.3. (U//FOUO) High Quantity..... 25
- 4.9.4. (U//FOUO) Form FD-455 (Access Log - Evidence Storage Facility)..... 26
- 4.9.5. (U//FOUO) Vault Witness Official (VWO) ..... 26



UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

4.9.6.	(U//FOUO) Submitting Drug Evidence.....	26
4.9.7.	(U//FOUO) Emergency Access .....	26
4.9.8.	(U//FOUO) Controlled Environment.....	26
4.9.9.	(U//FOUO) Weighed/Counted and Verified.....	26
4.9.10.	(U//FOUO) Laboratory Analyses by DEA .....	28
4.9.11.	(U//FOUO) Federal-Wide Drug Seizure System (FDSS).....	30
4.9.12.	(U//FOUO) Avoid Package Transfers .....	32
4.9.13.	(U//FOUO) Avoid Opening Drug Evidence .....	32
4.9.14.	(U//FOUO) Approximate Modifications in Automated Case Support.....	32
4.10.	(U//FOUO) Valuable Evidence.....	33
4.10.1.	(U//FOUO) Currency with an Unspecified Amount/Value .....	33
4.10.2.	(U//FOUO) Seized Currency Subject to Criminal or Civil Forfeiture.....	33
4.10.3.	(U//FOUO) Evidence Independently Counted/Verified .....	34
4.10.4.	(U//FOUO) Evidence Afforded Maximum Security .....	35
4.10.5.	(U//FOUO) Handling Transactional Documents.....	36
4.10.6.	(U//FOUO) Describing Valuable Evidence.....	36
4.10.7.	(U//FOUO) Handling Foreign Currency.....	37
4.10.8.	(U//FOUO) Evidence Purchase Money .....	37
4.11.	(U//FOUO) CART .....	38
4.11.1.	(U//FOUO) Transferring Evidence to a Regional Computer Forensic Laboratory (RCFL).....	38
4.11.2.	(U//FOUO) Procedures for Transferring Evidence Between an FO and an RCFL.....	39
4.11.3.	(U//FOUO) Handling Derivative Evidence (DE) .....	39
4.12.	(U//FOUO) Temporary Storage/Night Deposit - Drug and Valuable Evidence.....	40
4.12.1.	(U//FOUO) Security-Type Safe.....	40
4.12.2.	(U//FOUO) Off-Duty Hour Evidence Seizure.....	40
4.12.3.	(U//FOUO) Paperwork and Packaging .....	40
4.12.4.	(U//FOUO) Drop Slot.....	40
4.12.5.	(U//FOUO) FD-455 .....	40
4.12.6.	(U//FOUO) Daily Removal.....	40
4.12.7.	(U//FOUO) Prohibited Safes.....	40
4.13.	(U//FOUO) Storage of Evidence in Resident Agencies (RA) .....	41
4.13.1.	(U//FOUO) Evidence not Relinquished to the ECT .....	41
4.13.2.	(U//FOUO) Establishing an ECR in an RA .....	41
4.14.	(U//FOUO) Requesting Evidence Examinations from the Laboratory Division.....	41
4.14.1.	(U//FOUO) Requests for Examinations.....	41
4.14.2.	(U//FOUO) Request Forwarded with Evidence.....	42
4.14.3.	(U//FOUO) Each Case Separately .....	42
4.14.4.	(U//FOUO) International Law Enforcement Requests .....	42
4.14.5.	(U//FOUO) Operational Technology Division (OTD) Requests.....	42
4.15.	(U//FOUO) Packaging and Shipping Evidence to the Laboratory .....	43
4.15.1.	(U//FOUO) Packaging and Shipping Procedures .....	43
4.15.2.	(U//FOUO) Hazardous Materials.....	43
4.15.3.	(U//FOUO) Shipping .....	44

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

4.16.	(U//FOUO) Special Instructions Regarding the Following Evidence: .....	44
4.16.1.	(U//FOUO) Abrasives .....	44
4.16.2.	(U//FOUO) Biological Evidence (Blood, Buccal/Oral Swabs, Body Fluid Stains) .....	44
4.16.3.	(U//FOUO) Bank Security Dye .....	45
4.16.4.	(U//FOUO) Building Materials/Glass/Seal-Insulation/Soil .....	45
4.16.5.	(U//FOUO) Cigarettes/Cigars/Chewing Gum .....	45
4.16.6.	(U//FOUO) Drugs/Controlled Substances .....	45
4.16.7.	(U//FOUO) Explosives/Explosive Residue .....	45
4.16.8.	(U//FOUO) Firearms .....	46
4.16.9.	(U//FOUO) Hazardous Material .....	46
4.16.10.	(U//FOUO) Knives .....	46
4.16.11.	(U//FOUO) Latent Print Evidence .....	46
4.16.12.	(U//FOUO) Lubricants .....	47
4.16.13.	(U//FOUO) National Missing Person DNA Database Program Requests .....	47
4.16.14.	(U//FOUO) Paint/Polymers .....	47
4.16.15.	(U//FOUO) Pepper-Spray or Foam .....	47
4.16.16.	(U//FOUO) Product-Tampering .....	47
4.16.17.	(U//FOUO) Questioned Documents .....	47
4.16.18.	(U//FOUO) Serial-Numbers .....	48
4.16.19.	(U//FOUO) Shoe Print and Tire Tread .....	48
4.16.20.	(U//FOUO) Tape .....	48
4.16.21.	(U//FOUO) Toolmarks/Tools .....	48
4.16.22.	(U//FOUO) Unknown Substance .....	48
4.16.23.	(U//FOUO) Weapons of Mass Destruction .....	49
4.16.24.	(U//FOUO) Volatile Memory Devices (VMD) .....	49
4.17.	(U//FOUO) Transmittal of Evidence to Field Offices and FBIHQ/DEA Laboratories .....	49
4.17.1.	(U//FOUO) Mailing/Shipping to the Field Office or RA ECR .....	49
4.17.2.	(U//FOUO) U.S. Postal Service Registered Mail or Federal Express .....	49
4.17.3.	(U//FOUO) Collected Item Database .....	50
4.17.4.	(U//FOUO) From a Field Office to FBIHQ or DEA .....	50
4.17.5.	(U//FOUO) Evidence Seized/Recovered by RA Personnel .....	51
4.17.6.	(U//FOUO) Marking Obscene and Indecent Material .....	51
4.18.	(U//FOUO) Charge-Out Procedures - Evidentiary Property .....	51
4.18.1.	(U//FOUO) Evidence Stored in the ECR .....	51
4.18.2.	(U//FOUO) Collected Item Database Charge-Out Reminders .....	51
4.18.3.	(U//FOUO) Recharged Evidence .....	52
4.18.4.	(U//FOUO) Charge-Out Report .....	52
4.18.5.	(U//FOUO) Return of Evidence .....	52
4.18.6.	(U//FOUO) Agent Access for Review .....	52
4.19.	(U//FOUO) Evidence Released to Custody of Outside Agencies .....	52
4.19.1.	(U//FOUO) Evidence Permanently Released to an Outside Agency .....	52
4.19.2.	(U//FOUO) ECT Responsibility .....	52
4.19.3.	(U//FOUO) Evidence Temporarily Released .....	53

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

4.20. (U//FOUO) Physical Audit/Inventory - Evidentiary Property..... 53  
4.20.1. (U//FOUO) Conducting an Audit/Inventory..... 53  
4.20.2. (U//FOUO) Designating an Agent(s) and/or Support Supervisor..... 54  
4.20.3. (U//FOUO) Designating an RA Agent and/or RA Support Supervisor..... 54  
4.20.4. (U//FOUO) ECT/AECT Does Not Conduct an Audit/Inventory ..... 54  
4.20.5. (U//FOUO) VWO Presence During an Audit/Inventory ..... 54  
4.20.6. (U//FOUO) FD-455 Sign In/Out..... 54  
4.20.7. (U//FOUO) Sealed Drug and Valuable Evidence..... 54  
4.20.8. (U//FOUO) Inventory ..... 54  
4.20.9. (U//FOUO) Audit..... 55  
4.20.10. (U//FOUO) EC to the SAC/AO ..... 55  
4.21. (U//FOUO) Annual Evidence Program Audit Checklist ..... 55  
4.22. (U//FOUO) Non-evidentiary Property..... 55  
4.22.1. (U//FOUO) IAs ..... 55  
4.22.2. (U//FOUO) Bulky Non-Evidentiary Material..... 56  
4.22.3. (U//FOUO) Non-Evidentiary Property ..... 57  
4.22.4. (U//FOUO) Federal Grand Jury (FGJ) Material ..... 57  
4.23. (U//FOUO) Disposition of Property ..... 57  
4.23.1. (U//FOUO) When an Investigative Case is Closed ..... 57  
4.23.2. (U//FOUO) Permanent Retention ..... 58  
4.23.3. (U//FOUO) Disposition of Drug Evidence..... 58  
4.23.4. (U//FOUO) Disposition of Firearms..... 58  
4.23.5. (U//FOUO) Disposition of Forfeited and Abandoned Property ..... 58  
4.23.6. (U//FOUO) Disposition of Valuable Evidence..... 58  
4.23.7. (U//FOUO) Disposition of General Evidence..... 59  
4.23.8. (U//FOUO) Recordkeeping Procedures..... 59  
4.23.9. (U//FOUO) Closing Communication..... 60  
4.23.10. (U//FOUO) Retention in Closed Cases..... 60  
4.24. (U//FOUO) Authorization for Evidence Handling Deviations - FD-990 ..... 60  
4.24.1. (U//FOUO) Purpose..... 61  
4.24.2. (U//FOUO) Scope ..... 61  
4.24.3. (U//FOUO) Procedures ..... 61  
4.24.4. (U//FOUO) Initiating a Deviation Request..... 61  
4.24.5. (U//FOUO) Authorization..... 61  
4.24.6. (U//FOUO) Duration..... 61  
4.24.7. (U//FOUO) Documentation ..... 61  
4.25. (U//FOUO) Forms Used in the Evidence Program..... 62  
5. (U//FOUO) Recordkeeping Requirements ..... 63  
5.1. (U//FOUO) Form FD-455 (Access Log - Evidence Storage Facility)..... 63  
5.2. (U//FOUO) Form FD-597 (Receipt for Property Received/Returned/Released/  
Seized)..... 63  
5.3. (U//FOUO) Evidence Submitted to ECT ..... 64  
5.4. (U//FOUO) Evidence Entered Into the Collected Item Database ..... 64  
5.5. (U//FOUO) FD-192 ..... 64

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

5.6. (U//FOUO) FD-1004 ..... 64

5.7. (U//FOUO) Non-evidentiary Property ..... 65

5.8. (U//FOUO) Original Interview Notes ..... 65

5.9. (U//FOUO) Evidence Permanently Released to Outside Agency ..... 65

5.10. (U//FOUO) Audit/Inventory EC ..... 66

5.11. (U//FOUO) Annual Evidence Program Audit ..... 66

6. (U//FOUO) Summary of Legal Authorities ..... 67

6.1. (U//FOUO) Subpart H of Title 49, Code of Federal Regulations, Part 172 ..... 67

6.2. (U//FOUO) Title 18 U.S.C. Section 3665 ..... 67

6.3. (U//FOUO) Title 18 U.S.C. Section 3600A and Department of Justice (DOJ) ..... 67

7. (U//FOUO) Security Requirements ..... 68

7.1. (U//FOUO) General Evidence ECR ..... 69

7.2. (U//FOUO) Drug Evidence Room ..... 70

7.3. (U//FOUO) Valuable Evidence Room ..... 70

7.4. (U//FOUO) Federal Grand Jury Room ..... 71

7.5. (U//FOUO) CART Room ..... 71

7.6. (U//FOUO) Off-Site ECRs ..... 72

7.7. (U//FOUO) After-Hours/Temporary Storage of Drugs and/or Valuables ..... 72

8. (U//FOUO) Justice For All Act of 2004 ..... 73

8.1. (U//FOUO) For information and guidance regarding the Justice for All Act of 2004, refer to 319X-HQ-A1487720 serial 445 and Office of the General Counsel Website. [<http://ogc.fbinet.fbi>] ..... 73

**List of Appendices**

Appendix A: Legal Authorities ..... A-1

Appendix B: Sources of Additional Information ..... B-1

Appendix C: Contact Information ..... C-1

Appendix D: Key Words ..... D-1

Appendix E: Acronyms ..... E-1

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**1. (U//FOUO) Scope**

---

**(U//FOUO) Purpose:** This Field Evidence Policy Implementation Guide establishes consolidated, Bureau-wide streamlined administrative and operational processes for the seizure, storage, processing, analysis, presentation, and disposition of evidence.

**(U//FOUO) Background:** This policy implementation guide is a living document. It will be amended as new legal authorities are issued and as evidence policies change. It will undergo a total review every five years. All consumers are invited to provide the Field Evidence Program with recommendations on improving this product. This PG addresses both old and new evidence policies and takes precedence over other policies in electronic communication (EC) form or otherwise.

**(U//FOUO) Intended Audience:** This policy implementation guide applies to FBI employees, contractors working in FBI facilities, detailees, and any other person(s) assigned or detailed to the FBI. It also applies, where appropriate, to members of state and local law enforcement personnel assigned to FBI Joint Task Forces and Joint Terrorism Task Forces, and any other persons assigned to work in an FBI-controlled facility.

UNCLASSIFIED//FOUO

## Field Evidence Policy Implementation Guide

### **2. (U//FOUO) Roles and Functional Responsibilities**

---

#### **2.1. (U//FOUO) Assistant Directors in Charge (ADIC) and Special Agents in Charge (SAC)**

(U//FOUO) All field office ADICs and SACs, or individuals designated by the division, are responsible for ensuring compliance with all matters identified by this policy.

#### **2.2. (U//FOUO) Field Evidence Program Manager (PM)**

(U//FOUO) The Field Evidence Program Manager (PM) is a full-time assignment responsible for the National Field Evidence Program. The Field Evidence Program Manager, or individuals designated by the Field Evidence Program Manager, is responsible for the following functions:

1. (U//FOUO) Serving as the technical expert and PM for the FBI's Evidence Program. Overseeing all evidence handling procedures, automated programs, facilities, personnel policies, and all legal and administrative requirements pertinent to evidence acquired and maintained by the field.
2. (U//FOUO) Developing, administering, operating, managing, and maintaining all aspects of the FBI Evidence Program. Establishing standards and operating procedures to ensure the highest degree of consistency and compliance to federal rules and regulations governing the handling of evidence.
3. (U//FOUO) Formulating evidence policy for the new Field Evidence Management and Operations Policy Implementation Guide, which has replaced sections of the MAOP that referred to evidence policy. Establishing written evidence policy for all FBI personnel concerning collecting, analysis, storing, wrapping, packaging, and shipping, destroying, and disposing of evidentiary property in FBI custody.
4. (U//FOUO) Identifying problems and specific issues regarding the FBI's evidence database including electronic and automated records, based on input from the evidence control technician (ECT) in the field and Federal Bureau of Investigation Headquarters (FBIHQ). Conducting extensive analysis of reported issues and systematic surveys to determine the nature of requirements, logical work, and resource management. Effectively resolving significant concerns by formulating policy and procedures to address the same.
5. (U//FOUO) Promulgating written FBI Evidence Policy throughout the FBI and ensuring that all evidence manuals/training guides are factual and current.
6. (U//FOUO) Issuing directives, determining manpower utilization and work measurement techniques to maintain current evidence operations. Making recommendations for enhancements to existing systems when necessary and setting forth alternate approaches based upon available resources.
7. (U//FOUO) Preparing and conducting training schools for certification of FBI ECTs and alternate evidence control technicians (AECTs). Conducting on-site and regional training of FBI personnel, to include field office upper management. Planning training curriculum and directly instructing law enforcement evidence personnel on the appropriate methods for establishing an evidence policy for their respective police departments. Assessing the

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

evidence programs of other federal, state, and local law enforcement. Representing the FBI and lecturing throughout the law enforcement community in specialized schools and seminars on evidence procedures.

8. (U//FOUO) Maintaining contact with federal, state, local, and international law enforcement agencies and participating in inter-agency meetings and working groups concerned with rules and regulations for the administrative handling of evidence and establishment of Evidence Control Centers. Providing expert advice and guidance to colleagues throughout the national and international law enforcement community.
  9. (U//FOUO) Conducting on-site assessments and quality assurance audits of individual field offices, examining administrative procedures, policies, physical space and storage facilities, and transportation processes in order to ensure compliance with applicable evidence policy.
  10. (U//FOUO) Performing evaluations of unsolicited proposals submitted by vendors and manufacturers for custom or stock equipment.
- 2.3. (U//FOUO) Evidence Control Technicians and Alternate Evidence Control Technicians

(U//FOUO) The field ECTs and AECTs are responsible for the following functions:

- (U//FOUO) Becoming familiar with policies and procedures.
- (U//FOUO) Training in hazardous materials (HAZMAT) transportation..
- (U//FOUO) Keeping records, storage, and maintenance of all evidence.
- (U//FOUO) Transmitting evidence to FBIHQ, other field offices, the Drug Enforcement Administration (DEA), or a contributor.
- (U//FOUO) Retrieving evidence from the evidence control room (ECR).
- (U//FOUO) Running closed cases with pending evidence.
- (U//FOUO) Disposing of property.
- (U//FOUO) Testifying in a court of law regarding evidentiary property.
- (U//FOUO) Participating on the Evidence Response Team (ERT) as approved.
- (U//FOUO) Inspecting field office evidence programs.
- (U//FOUO) Assisting the evidence program manager with conducting training and ECR assessments.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

**3. (U//FOUO) Policies**

---

(U//FOUO) It is the policy of the FBI that all FBI Divisions strictly adhere to all procedures listed in Section 4.

(U//FOUO) See Corporate Policy Directive 0120D.



UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**4. (U//FOUO) Procedures and Processes**

---

**4.1. (U//FOUO) Evidence**

**4.1.1. (U//FOUO) Form FD-597 (Receipt for Property Received/Returned/Released/Seized)**

(U//FOUO) Property may be acquired during investigations according to the law concerning searches and seizures, and by warrant, subpoena, or consent including voluntary delivery. Form FD-597 (Receipt for Property Received/Returned/Released/Seized) is to be used to document the receipt or return of property acquired during investigations. The FD-597 consists of an original and two copies with carbon inserts. The original is to be filed in the 1A section (FD-340a) of the investigative case file. One copy of the FD-597 is to be furnished to the contributor and one copy is to be returned with the search warrant.

**4.1.2. (U//FOUO) Chain-of-Custody (FD-1004)**

(U//FOUO) It is essential that seized/recovered/contributed property is properly identified and described by investigative personnel at the time possession is transferred to the investigator. The items are to be carefully packaged and the containers properly identified. If appropriate, chain-of-custody is to be established and a record maintained from the time possession transfers to the investigator to the time of trial/disposition. To minimize the number of FBI personnel required to establish chain-of-custody, it is recommended that one or two investigators be designated to identify and describe all evidence at any particular search or arrest site.

**4.2. (U//FOUO) Evidence Control Room (ECR)**

**4.2.1. (U//FOUO) Designated ECR**

(U//FOUO) The designated ECR should be a separate area, usually within the confines of field office space, used solely for the storage of seized/recovered/contributed property that can reasonably be expected to be introduced in court and/or subject to chain-of-custody, regardless of size. Access to the ECR is restricted to ensure evidentiary property is accounted for, retrievable, and can withstand defense challenges concerning chain-of-custody.

**4.2.2. (U//FOUO) Personal Protective Supplies**

(U//FOUO) Appropriate personal protective supplies (e.g., first aid and safety equipment) must be stored in the ECR for easy accessibility. This includes, but is not limited to: disposable gloves and gowns, disposable plastic aprons, eye and mouth protection, pails with disinfectant, biohazard bags for the disposal of biohazardous material (bag to be placed in a hard cardboard box), containers to hold needles, sink with hot and cold running water (with elbow or foot connection), flammable cabinets, acid cabinets, poison cabinets, and biohazard labels and containers. The ECR must be equipped with a fire extinguisher.

**4.2.3. (U//FOUO) Large Volume of Evidence**

(U//FOUO) In the event evidentiary property is of such volume that it is not practical to store it in the ECR or a similar facility within field office space, it may be stored in a secure off-site facility at the discretion of the SAC. The off-site facility should be established and afforded the same security measures as an ECR. Every effort should be made to store evidence in the ECR.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

However, if a similar facility within field office space or an off-site facility is used, this facility is considered a satellite of the ECR and is subject to the same administrative controls afforded the ECR

#### 4.2.4. (U//FOUO) Form FD-455 (Access Log - Evidence Storage Facility)

(U//FOUO) Form FD-455 is to be maintained for each ECR or satellite ECR, whether located within field office space or at an off-site. In addition, a separate FD-455 is to be maintained for each valuable, drug, and electronic surveillance (ELSUR) evidence repository, regardless of size or location. The FD-455 establishes a reliable record of persons gaining entry. The visitor signs his/her own name (one name per line), reason for entry, the case file number and 1B/1D number, if appropriate, and the date and time of entry/exit. This information is extremely useful in defense against attacks regarding chain-of-custody. In field offices where an "enclosed reception area" has been established at the entrance to the ECR, it is not required that the FD-455 be signed, as long as the visitor does not enter beyond the "enclosed reception area." Investigative personnel reviewing evidence in the reception area are not required to sign the FD-455; however, the chain-of-custody must be signed as a record of their review of the evidence.

(U//FOUO) The FD-455 log must be maintained indefinitely.

(U//FOUO) The ECT and AECT (when substituting for the ECT for one day or longer) are required to sign in and out on the FD-455 log maintained for the ECR only upon initial entry and final departure on a given day. Any other employee, including the AECT when the ECT is on duty, must sign in/out on the FD-455 log for each entry/exit on a given day. Only one signature per line is permitted.

(U//FOUO) In those field offices where more than one full-time ECT and/or more than one evidence storage facility is operated on a daily basis, access to the storage facility(s) is to be recorded on the FD-455 log as follows:

- (U//FOUO) The ECT must sign in/out on the FD-455 log for the primary ECR, when first entry/last exit of the day is made. Access to any satellite ECR must be recorded on the FD-455 log maintained for that satellite ECR for each entry/exit on a given day.

#### 4.2.5. (U//FOUO) Access to the ECR

(U//FOUO) Access to the ECR and/or other evidence storage facilities that store general evidence, located within or outside field office space, is strictly limited to the ECT and AECT. Access by other employees is prohibited unless accompanied by the ECT/AECT, or as outlined in (4.2.7) below, and documented on the FD-455 log maintained for the facility accessed.

#### 4.2.6. (U//FOUO) Large Seizures After Hours

(U//FOUO) In instances involving large seizures of evidentiary property that occur during off-duty hours (nights/weekends/holidays), the services of the ECT/AECT should be used to assist with analyzing, cataloging, inventory, and storage of the seized/recovered property.

#### 4.2.7. (U//FOUO) Access to the Drug/Valuable Vault

(U//FOUO) The ECT/AECT is not authorized to access the drug/valuable vault unless accompanied by the administrative officer (AO) or the person(s) designated to act on behalf of

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

the AO as the vault witness official (VWO). The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO cannot be an AECT. Each office should limit the number of designated VWOs, and must document the list of authorized vault witnessing personnel in the evidence control file. The VWO must also sign the FD-455 for each entry/exit.

4.2.8. (U//FOUO) Emergency Access to the Drug/Valuable Vault

(U//FOUO) The only people having emergency access to the drug/valuable vault [redacted] and the ECR are the SAC, the ASAC, and the (SSRA). The [redacted]  
[redacted]

b7E

4.2.9. (U//FOUO) Refrigerator/Freezer

(U//FOUO) A refrigerator/freezer must be in the ECR for the storage of body fluids and any perishable-type evidence. Food items for personal consumption are not to be stored in this refrigerator.

4.2.10. (U//FOUO) Biohazard Warning Label

(U//FOUO) A Biohazard Warning label must be placed on the entrance to the ECR (preferably the door) and on the refrigerator in the ECR.

4.3. (U//FOUO) ECR Construction

(U//FOUO) ECRs within a stand-alone FBI-controlled building or within contiguous FBI space, occupied 24 hours a day, 7 days a week, with a perimeter secured to specifications established by the Security Division, must be constructed according to the requirements set forth herein.

(U//FOUO) The externally accessible door to the ECR, as well as drug evidence room and valuable evidence room doors, must be secured with [redacted]  
[redacted]

b7E

4.3.1. (U//FOUO) General Evidence ECR

(U//FOUO) General evidence control rooms must be constructed and controlled as indicated below:

- (U//FOUO) [redacted]
- (U//FOUO) Only one externally accessible door to the ECR is permitted. Entrance to the ECR should be secured by [redacted]  
[redacted] II  
additional access doors are constructed [redacted]  
[redacted]

b7E

b7E

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

- (U//FOUO) The externally accessible door must be equipped with [redacted]

- (U//FOUO) [redacted]

b7E

- (U//FOUO) [redacted]

- (U//FOUO) [redacted] room designated for housing weapons and ammunition must be constructed of [redacted]. Access must be controlled by [redacted]

b7E

- (U//FOUO) [redacted] in the general evidence ECR. This [redacted]

b7E

- (U//FOUO) The ECR should be equipped with a fire extinguisher. Appropriate personal protective supplies and first aid safety equipment must be stored in the ECR for easy accessibility. This includes, but is not limited to: disposable gloves and gowns, disposable plastic aprons, eye and mouth protection, pails with disinfectant, biohazard bags for the disposal of biohazardous material (bag to be placed in a hard cardboard box), containers to hold needles, sink with hot and cold running water (with elbow or foot connection), flammable cabinets, acid cabinets, poison cabinets, and biohazard labels and containers.

4.3.2. (U//FOUO) Drug Evidence Room

(U//FOUO) The drug evidence room must be a separate room constructed and controlled as indicated below:

- (U//FOUO) [redacted] of the drug evidence room.

b7E

- (U//FOUO) There may be only one externally accessible door to the drug evidence room.

- (U//FOUO) The externally accessible door to the drug evidence room must be equipped with [redacted]

- (U//FOUO) [redacted]

b7E

- (U//FOUO) [redacted]

- (U//FOUO) [redacted] is required for the valuable evidence room. This [redacted]

b7E

- (U//FOUO) An exterior 24-hour ventilation system is required. The drug evidence room should be afforded outside ventilation for the storage of odoriferous substances. The floor should be made of a non-porous material so that it can be disinfected.

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

4.3.3. (U//FOUO) Valuable Evidence Room

(U//FOUO) The valuable evidence room must be a separate room constructed and controlled as indicated below:

- (U//FOUO) The entire perimeter of the valuable evidence room must be constructed of [redacted] of the valuable evidence room. b7E
- (U//FOUO) There may be only one externally accessible door to the valuable evidence room.
- (U//FOUO) The door to the valuable evidence room must be equipped with [redacted]
  - (U//FOUO) [redacted] b7E
  - (U//FOUO) [redacted]
- (U//FOUO) [redacted] for the valuable evidence room. This [redacted] b7E

4.3.4. (U//FOUO) Federal Grand Jury Room

(U//FOUO) The Federal Grand Jury Room (FGJR), designated for housing Federal Grand Jury (FGJ) material, must be constructed and controlled as indicated below:

- (U//FOUO) [redacted] of the Federal Grand Jury Room. b7E
- (U//FOUO) Only one externally accessible door to the Federal Grand Jury Room is permitted. Entrance to the room should be secured by [redacted] b7E
- (U//FOUO) The externally accessible door must be equipped with [redacted]
  - (U//FOUO) [redacted] b7E
  - (U//FOUO) [redacted]
- (U//FOUO) [redacted] is required for the Federal Grand Jury Room. This [redacted] b7E

4.3.5. (U//FOUO) Computer Analysis Response Team (CART) Room

(U//FOUO) The Computer Analysis Response Team (CART) Room, designated for housing computer evidence, to include various types of magnetic media excluding ELSUR evidence, must be constructed and controlled as indicated below:

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

- (U//FOUO) The entire perimeter of the CART Room must be constructed of [redacted] of the CART Room. b7E
- (U//FOUO) Only one externally accessible door to the CART Room is permitted. Entrance to the room should be secured by [redacted]. b7E
- (U//FOUO) The externally accessible door must be equipped with [redacted].
  - (U//FOUO) [redacted]. b7E
  - (U//FOUO) [redacted].
- (U//FOUO) [redacted] is required for the CART Room. This [redacted]. b7E

4.3.6. (U//FOUO) Off-Site Evidence Control Rooms

(U//FOUO) Off-site evidence control rooms must be constructed and controlled as indicated below:

- (U//FOUO) The entire perimeter of an off-site ECR must be constructed of [redacted]. b7E
- (U//FOUO) Only one externally accessible door is permitted to the ECR. If additional access doors are constructed [redacted]. b7E
- (U//FOUO) The externally accessible door must be equipped with [redacted].
  - (U//FOUO) [redacted]. b7E
  - (U//FOUO) [redacted].
- (U//FOUO) [redacted] for the off-site ECR. This [redacted]. b7E

4.4. (U//FOUO) ECR Security

4.4.1. (U//FOUO) Drug and Valuable Evidence Rooms

(U//FOUO) Drug and valuable evidence rooms require that [redacted] to gain authorized access. In order to ensure that the [redacted]. b7E

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

4.4.2. (U//FOUO) Personal Identification Numbers

(U//FOUO) [Redacted]  
[Redacted] It is acceptable and encouraged that [Redacted]  
[Redacted]

b7E

4.4.3. (U//FOUO) Combinations

(U//FOUO) [Redacted]  
[Redacted]

b7E

4.4.4. (U//FOUO) Access Removal

(U//FOUO) In the event an ECT, AECT, or VWO no longer has authorized access to a drug and/or valuable room [Redacted]  
[Redacted]

b7E

4.4.5. (U//FOUO) Access Log Printed and Retained

(U//FOUO) At the end of each month, the evidence program supervisor must ensure that the electronic access logs for each ECR and drug and valuable room are printed and retained. (The printed logs must be retained from inspection period to inspection period.)

4.4.6. (U//FOUO) Changing Combinations

(U//FOUO) [Redacted]  
[Redacted]

b7E

4.4.7. (U//FOUO) Off-Site Alarms

(U//FOUO) For field offices having off-site ECRs, the field office must create a documented response plan detailing how an activated alarm must be handled. The response plan must be permanently retained and readily accessible for review.

4.5. (U//FOUO) Responsibilities of the Evidence Control Technician

(U//FOUO) The ECT is the designated custodian of seized/recovered evidentiary property, which encompasses the following responsibilities:

4.5.1. (U//FOUO) General Familiarity

(U//FOUO) The ECT is familiar with the procedures set forth herein; the Forfeiture Manual concerning the disposition of property subject to forfeiture, and the Forfeiture and Abandoned Property Manual, Section 10, concerning Dangerous Goods Regulations, International Air Transport Association (IATA).

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.5.2. (U//FOUO) Access to the ECR**

(U//FOUO) The ECT ensures that access to the ECR and other evidence storage facilities is limited to persons having an official need, that all individuals entering the facilities are escorted, and that access is recorded on Form FD-455, maintained for each storage facility.

**4.5.3. (U//FOUO) Protective Clothing/Equipment**

(U//FOUO) The ECT ensures that the proper protective clothing/equipment is stored and is readily available in the ECR, and that it is used when handling hazardous or potentially hazardous evidentiary property.

**4.5.4. (U//FOUO) Hazardous Materials (HAZMAT) Transportation Training**

(U//FOUO) In conjunction with Subpart H of Title 49, Code of Federal Regulations, Part 172, it is required that training be provided to those individuals who, in the course of their employment, directly affect HAZMAT transportation safety, and that those individuals avail themselves of such training. ECTs are to receive specialized HAZMAT training for air transport shipments every two years by a certified Department of Transportation or IATA-approved school. Strict fines are imposed on individual employees by the Federal Aviation Administration for noncompliance.

**4.5.5. (U//FOUO) Collected Item Database**

(U//FOUO) The ECT ensures, by physical examination of property, that the descriptive data entered into the automated evidence system (aka, collected item database [CI]), as furnished by case agent/acquiring agent, adequately and properly reflects the property being retained. (When evidence is heat-sealed, the sealing/witnessing officials are responsible for the accurate description of the evidentiary items.)

**4.5.6. (U//FOUO) Recordkeeping, Storage, and Maintenance of Evidence**

(U//FOUO) The ECT is responsible for the recordkeeping, storage, and maintenance of all evidence. Responsibility for non-evidentiary property acquired during investigations may, at the discretion of the SAC, be assigned to the ECT if his/her workload permits. Otherwise, the SAC should assign responsibility for non-evidentiary property to an employee other than the ECT.

**4.5.7. (U//FOUO) Ten Calendar-Day Rule for Submission**

(U//FOUO) The case agent, acquiring agent, and/or agent supervisor, depending upon the circumstances, as individuals or collectively, share the responsibility for ensuring that seized/recovered/contributed evidence is properly documented on the FD-192. The evidence and/or documentation must be submitted to the ECT within ten calendar days from the date that the evidence was seized/recovered. The ten calendar days for the acquiring agent begin with the seizure of the property and end when the ECT receives the evidence and signs the chain-of-custody.

(U//FOUO) Should extenuating circumstances prevent submission of the evidence to the ECT within ten calendar days, the ECT advises the agent that a late submission EC (aka, late day memo) is to be submitted to the squad supervisor and thereafter placed in the investigative case file. (A copy of the EC is to be directed to the ECT, placed in a binder in the ECR, and maintained from inspection to inspection.)



UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) The ECT is authorized to reject evidence that is submitted late without an accompanying EC.

(U//FOUO) If the acquiring agent submits the FD-192 within ten days, but maintains the evidence, the ECT can issue the FD-192 reflecting that the evidence continues in the custody of the acquiring agent, has not been taken into custody by the ECT, and proper charge-out procedures are being followed.

- (U//FOUO) When a lead office (LO) forwards evidence to the office of origin (OO), the following documents (when necessary) should accompany the evidence:
  - (U//FOUO) FD-192 (package copy and file copy).
  - (U//FOUO) EC for late submission – special agent and/or ECT.
  - (U//FOUO) FD-597.

#### 4.5.8. (U//FOUO) Ten Calendar-Day Rule for Capture in the Collected Item Database

(U//FOUO) The ECT is responsible for ensuring that the seized/recovered/contributed evidence is properly captured in the collected item database (CI) within ten calendar days from the date the evidence and/or documentation was presented to him/her by the seizing agent. Should extenuating circumstances prevent the ECT from entering the information into the automated evidence system within ten calendar days, the AO is to be advised by EC, which is to be placed in the investigative case file. (A copy of the ECT's EC is placed in a binder in the ECR and maintained from inspection to inspection.) The ten calendar days for the ECT begin when:

- (U//FOUO) The ECT signs the chain-of-custody at the time he/she acquires the evidence, or
- (U//FOUO) The ECT acquires only the documentation, and ends when he/she enters the information into the collected item database.

(U//FOUO) Secondary evidence from the lab is to be entered as a new 1B. If the ECT receives the secondary evidence from the lab by FedEx, the ECT is responsible for getting the evidence entered into the collected item database within ten days. If the ECT is late, then the ECT is responsible for the late EC. If an agent picks up the evidence from the lab and waits more than ten days to submit it to the ECT, then the agent is responsible for writing the late EC.

#### 4.5.9. (U//FOUO) Location of Property

(U//FOUO) The ECT must make certain that the exact location of property is noted in the collected item database; that the 1B, 1C, or 1D number is recorded on the automated FD-192/FD-192a for file; that bar code labels are placed directly on the general evidence packaging and on the plastic pouches containing valuable or drug evidence; that an automated FD-192/FD-192a is filed in the case file; and that a second copy is attached to the property or placed in the binder/folder maintained in the valuable/drug evidence repository.

(U//FOUO) The ECT ensures that every container of evidence has its own, FD-192, FD-1004, and barcode. A barcode must be affixed to each container.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.5.10. (U//FOUO) Chain-of-Custody Documentation**

(U//FOUO) The ECT ensures that chain-of-custody documentation for evidence is recorded in the collected item database and on the automated FD-192 maintained with the evidence. (See Chain-of-Custody User Guide.)

**4.5.11. (U//FOUO) Forwarding Evidence**

(U//FOUO) The ECT ensures that evidence is properly packaged and labeled for forwarding to FBIHQ, other field offices, the Drug Enforcement Agency (DEA), or a contributor, and that transmittal/disposition information is recorded in the collected item database. The ECT properly prepares evidence for mailing/shipping to the appropriate field office ECR or RA ECR. The ECT must refer to the ECR Directory for shipping information prior to sending shipment.

**4.5.12. (U//FOUO) Retrieving Evidence from the ECR**

(U//FOUO) The ECT retrieves evidence from the ECR and any other evidence storage facility as requested by agent personnel. The evidence control technician then accurately records chain-of-custody on the form maintained with the package copy of the automated FD-192 and in the collected item database. The ECT produces a charge-out reminder report to ensure property held over 60 days is either recharged or returned to the ECR.

**4.5.13. (U//FOUO) Non-Evidentiary Property**

(U//FOUO) Upon request, the ECT retrieves non-evidentiary property from the facility and charges out the property by using an FD-5 (Serial Charge-Out Form) according to established charge-out procedures. The ECT maintains and monitors a record of property charged out to ensure property held over 60 days is either recharged or returned to the facility.

**4.5.14. (U//FOUO) Closed Cases with Pending Evidence**

(U//FOUO) The evidence control technician closely follows the automated property disposition tracking system to ensure every effort is being made to return property to the contributor and that property declared abandoned is processed on a timely basis. A Closed Cases with Pending Evidence Report is to be run and distributed to squad supervisor(s) for evidence disposition decisions every 60 days.

**4.5.15. (U//FOUO) Disposing of Property**

(U//FOUO) The ECT assists case agents in disposing of property (on instructions of FBIHQ, other field offices, or agent personnel) through actual destruction (drug evidence excluded), return to contributor, or other methods, as appropriate. Should property that has been declared abandoned become the property of the FBI, the ECT ensures action is taken by supply personnel to have the property placed on the field office inventory. (See Forfeiture and Abandonment Manual.)

**4.5.16. (U//FOUO) Testify in Court**

(U//FOUO) As necessary, ECTs may be required to testify in a court of law regarding evidentiary property (chain-of-custody) for which they are responsible.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.5.17. (U//FOUO) Evidence Response Team**

(U//FOUO) At the discretion of the SAC, an ECT may serve as a fully trained member of the Evidence Response Team.

**4.5.18. (U//FOUO) Inspects Field Office Evidence Programs**

(U//FOUO) Upon the advice of the Evidence Program Manager, FBIHQ, and at the request of the Inspection Division, FBIHQ, the ECT conducts inspections of field office evidence programs with SAC approval.

**4.5.19. (U//FOUO) Conducts Training and Assessments**

(U//FOUO) At the request of the Evidence Program Manager, FBIHQ, and with the consent of the SAC, ECTs may assist the Evidence Program Manager to conduct training and ECR assessments in various field offices.

**4.5.20. (U//FOUO) Top Secret Evidence**

(U//FOUO) The ECT is not authorized to accept, store, or enter Top Secret evidence into the ECR. The ECT should have the agent contact the field office security officer for guidance.

**4.6. (U//FOUO) Administrative Handling and Storage of Evidentiary Property**

(U//FOUO) To facilitate recordkeeping and storage procedures, evidentiary property is divided into five categories: general evidence, valuable evidence, drug evidence, firearms evidence, and CART evidence. All newly acquired evidence must be entered into the collected item database. Procedures for the administrative handling and storage of evidence are described below.

(U//FOUO) In field offices where special agent personnel do not directly enter their own evidence into the collected item database, the traditional green FD-192 is to be used as a "data loading form" (draft) to communicate to the ECT the information that is to be entered in the collected item database. The evidence, together with the "draft" FD-192, and a signed FD-1004 are then furnished to the ECT. Upon entering the information into the collected item database, the "draft" FD-192 is destroyed. It is not to be used as the file or package copy.

(U//FOUO) Evidence and/or documentation is to be submitted to the ECT within ten calendar days from the date the evidence was seized/recovered/contributed. Should extenuating circumstances prevent handling of the evidence within ten calendar days, the ECT must advise the SA that an EC is to be submitted to the squad supervisor and thereafter placed in the investigative case file. (A copy of the EC is to be directed to the ECT, placed in a binder in the ECR, and maintained from inspection to inspection.)

(U//FOUO) The ECT is authorized to reject evidence that is submitted late without the accompaniment of an EC. The ten calendar days for the acquiring agent begin with the seizure of the property and end when the ECT receives the evidence and signs the chain-of-custody. (If the acquiring agent submits only the FD-192, thereby maintaining the evidence, the ECT is to be cognizant of the ten-day time frame and should not accept the late FD-192 without an EC. In the event the evidence is retained by the acquiring agent, proper charge-out procedures are to be followed.)

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) When LOs forward evidence to the OO, the following documents (when necessary) should accompany the evidence:

- (U//FOUO) FD-192 (package copy and file copy).
- (U//FOUO) EC for late submission (SA and/or ECT).
- (U//FOUO) FD-597.

(U//FOUO) In field offices where agent personnel directly enter their own evidence into the collected item database, the agent sends the automated FD-192 to the ECT's printer and thereafter provides the evidence, together with a signed chain-of-custody (automated sheet), to the ECT. The ten calendar days for the acquiring agent begin with the seizure of the property and end when the ECT receives the entered information through the collected item database.

(U//FOUO) The ECT is responsible for ensuring that the seized/recovered/contributed evidence is properly captured in the collected item database within ten calendar days from the date the evidence and/or documentation was presented to him/her by the seizing agent. Should extenuating circumstances prevent the ECT from entering the information into the collected item database within ten calendar days, the AO is to be advised by an EC that is to be placed in the investigative case file. (A copy of the ECT's EC is placed in a binder in the ECR, and maintained from inspection to inspection.) The ten calendar days for the ECT begin when:

- (U//FOUO) The ECT signs the chain-of-custody at the time the ECT acquires the evidence.
- (U//FOUO) The ECT acquires only the documentation, and ends when he/she enters the information into the collected item database.

(U//FOUO) The ECT accepts the evidence and signs the chain-of-custody. The ECT then enters the required information (if not already done so by the agent), and affixes a bar code number and a 1B/1D number to each evidence container. (For detailed procedures on entering evidence into the collected item database, see the Advanced Automated Case Support [ACS] Users' Guide.) The chain-of-custody and a record thereof must be maintained on evidentiary items from the time of acquisition to the time of disposition.

(U//FOUO) Upon assigning the bar code to the evidence, the ECT is required to print three new copies of the FD-192 which show the bar code. One copy of the automated FD-192 (file copy) is submitted to the supervisory special agent (SSA), primary relief supervisor, ASAC, or SAC for initialing, and is then filed in the first section of the investigative case file immediately above the 1A section (FD-340a). If there is no 1A section, the file copy becomes the first item in the first section of the investigative case file. The file copy may be maintained in a subfile, in which case a blank automated FD-192 should be placed in the main file as a substitute for the original, indicating its location (e.g., "1B numbers maintained in Subfile E").

(U//FOUO) For general evidence, the second copy (package copy) of the automated FD-192 and the written chain-of-custody is affixed to and remains with the evidence until final disposition. For valuable and drug evidence, the package copy and the written chain-of-custody are filed in sequence by file number in a binder that is maintained in the ECR. The first chain-of-custody is established as a result of entering the group data on the first page of the automated FD-192 and indicates the identity of the person who collected the evidence. Subsequent chain-of-custody

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

signatures must be made by the ECT or other individuals who receive the property. Chain-of-custody entries should not disclose that the evidence is received by the ECR; instead, the entry should show the signature of the person to whom the custody of the evidence has been given. (The only exception to this policy is when evidence is forwarded to the DEA or FBI Laboratories.)

(U//FOUO) In task force investigations, it is permissible for a federal criminal investigative agent from a participating federal agency or a deputized officer from a participating police department, to record chain-of-custody on Form FD-192 (Control Form for General/Valuable/Drug Evidence) when that investigator/officer is involved in the acquisition of the property documented on the FD-192. This individual may also participate as the sealing/witnessing agent in the verification and sealing of drug/valuable evidence. Support employees may be witnessing officials for valuable evidence only.

(U//FOUO) In emergency situations where circumstances dictate the immediate transmittal of evidence to FBIHQ and/or the DEA Laboratory by agent personnel in an RA, prior to being furnished to the ECT for handling, the property must be documented within the ten-calendar-day time frame in the collected item database, and handled according to the procedures described below.

(U//FOUO) The case/seizing agent is to note transmittal information on the chain-of-custody page of the automated FD-192 (e.g., forwarded to FBI/DEA Lab, registered mail number or Federal Express [FedEx] number, date of transmittal letter) and furnish the chain-of-custody and an automated FD-192 (or a drafted green data-loading FD-192) to the ECT. The ECT does not sign the chain-of-custody page unless he/she is physically taking custody of the evidence. The appropriate information must, however, be recorded in the collected item database.

(U//FOUO) The ECT assigns a bar code number and a 1B number to the evidence documentation. The bar code label is held by the ECT until the evidence is returned by the DEA or FBI Laboratory.

(U//FOUO) The file copy of the automated FD-192 is initialed by an SSA and filed in the case file.

(U//FOUO) The package copies of the automated FD-192 and FD-1004 are retained in the ECR and filed in a binder labeled "Evidence sent to FBIHQ" or "Evidence sent to DEA Lab," according to the transmittal date.

(U//FOUO) When the evidence is returned to the field office, the ECT attaches the assigned bar code to the property and properly executes the chain-of-custody on the package copy of the automated FD-192. The package copy of the automated FD-192 is affixed to the general evidence or filed in the binder maintained in the valuable/drug vault. The chain-of-custody information is then entered into the collected item database.

(U//FOUO) If the evidence is to be returned to the RA, and not to the ECT in headquarters city (HQC), the RA is to request that copies of the FD-192 and chain-of-custody be furnished to the ECT when the evidence is returned to the RA.

(U//FOUO) The collected item database produces 60-day charge-out reminders.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) Property or items seized or recovered incidental to a search and seizure should generally be treated as evidence and maintained in the ECR. The below-listed material/items are currently considered hazardous materials:

- (U//FOUO) Flash paper.
- (U//FOUO) Live ammunition.
- (U//FOUO) Explosives.
- (U//FOUO) Radioactive materials.
- (U//FOUO) Flammable liquids and solids.
- (U//FOUO) Flammable and nonflammable gases.
- (U//FOUO) Spontaneously combustible substances.
- (U//FOUO) Oxidizing and corrosive materials.

(U//FOUO) All hazardous materials require special packaging, and the amount of each item that can be shipped is regulated. (See the Handbook of Forensic Science, IATA, and Code of Federal Regulations [CFR] for specific requirements and instructions for the handling/storing/shipping of hazardous materials.)

(U//FOUO) Property seized for forfeiture, which is also evidence, should be treated as evidence and maintained in the ECR during the forfeiture process. (See the Forfeiture Manual.)

(U//FOUO) Non-evidentiary property, if size permits, may be filed in the 1A section of the case file. Large non-evidentiary property (serialized as a 1C), seized, subpoenaed or contributed pursuant to investigative activity, is to be stored in a separate area within the field office. At the discretion of the SAC, space outside the field office, specifically designated for the storage of non-evidentiary items may be used.

(U//FOUO) Chain-of-custody on Federal Grand Jury Material (Rule 6e Material) is not required unless specified by the case agent. The case agent must consult with the Assistant United States Attorney (AUSA) to determine whether an FD-1004 should be maintained on specific grand jury material. If so required, an FD-192 is completed and the material is stored in the ECR. When an FD-1004 is not required, grand jury material is documented on Form FD-192a (Control Form for Non-Evidentiary Items), entered into the collected item database as a 1C, and segregated from the other non-evidentiary property. Access is given only to those individuals named on the grand jury list. When grand jury material is entered into the collected item database as a 1C, it is charged out by using Form FD-5.

(U//FOUO) Special agents' original interview notes are not intended to be used as evidence at a trial. Questions raised by the defense with respect to them generally attempt to focus on inconsistencies between the original notes and the resulting FD-302. Just as it is not necessary to maintain chain-of-custody on the FD-302, it is not necessary to maintain chain-of-custody on original interview notes. They should be filed in the 1A section (FD-340a) of the case file.

- (U//FOUO) Classified national security information should be handled in the same manner as other evidence, with the exception that it must be retained in a storage receptacle, appropriate to

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

its level of classification. Full consideration must be given to the necessary chain-of-custody accountability. Money, weapons, and other items of intrinsic value must not be stored in the same security container unless they are also classified. Material believed to be classified, but not so identified, must be protected as though it is classified. Within 30 days, a determination as to its classification must be made either by presentation of the material to an Original Classification Authority or comparison with an approved classification guide in accordance with MIOG, Part II, 26-2.3. Under no circumstances may classified material be released to any person unless it has been determined that the individual has the necessary clearance and/or access commensurate with the classification level of the material and a demonstrated need to know.

(U//FOUO) ELSUR evidence (serialized as a 1D) should be handled in the same manner as general evidence, with the exception of Title III material, which must be sealed within five (5) days by the court. However, ELSUR evidence is not to be stored in the ECR, but rather in a room specifically designated for such material. The physical requirements for this room are the same as for an ECR. (See Foreign Counterintelligence [FCI] Manual, Introduction, 1-2.6.3.)

(U//FOUO) Obscene material that must be retained as evidence must be clearly marked "Obscene" and stored as general evidence in the ECR.

**4.6.1. (U//FOUO) For Pre-automated Evidence Only:**

(U//FOUO) Every effort should be made to enter all evidence into the collected item database. However, if extenuating circumstances prevent the entry of pre-automated evidence into the collected item database, the following guidelines are to be followed:

1. (U//FOUO) Three copies of the non-automated green Form FD-192 should exist for pre-automated evidence.
  - a) (U//FOUO) The original copy must be signed by an SSA and filed in the first section of the case file immediately above the 1A section (FD-340a). If there is no 1A section, the file copy becomes the first item in the first section of the case file. The file copy may be maintained in a subfile, in which case a blank non-automated green FD-192 should be placed in the main file as a substitute for the original indicating their location (e.g., "1B numbers maintained in Subfile E").
  - b) (U//FOUO) The package copy of the non-automated green FD-192 records the chain-of-custody and must remain with general evidence. (If valuable/drug evidence, the package copy is not affixed to the property, but is filed in numerical sequence by file number in a binder that is maintained in the valuable/drug evidence repository. The package copy may be reproduced if more than one copy is required.) The signatures of persons, including the ECT, accepting custody must be recorded thereon as follows:
    - i) (U//FOUO) The first chain-of-custody entry is the employee who first acquired the property as identified on the front page of the non-automated green FD-192.
    - ii) (U//FOUO) The second chain-of-custody entry is the individual to whom the property was first released. The date, time, and reason for release are also required.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

- iii) (U//FOUO) The third chain-of-custody entry is the signature of the ECT or other individual who accepts possession from the individual releasing it (second chain-of-custody entry) along with the date, time, and reason for acceptance.
  - iv) (U//FOUO) Chain-of-custody information continues in this fashion as the property changes hands. Chain-of-custody entries should not disclose that the evidence is released to or accepted by the ECR; the entry must show the signature of the person accepting/releasing custody.
- c) (U//FOUO) It is the responsibility of the ECT to ensure that the chain-of-custody is accurately recorded on the package copy of the non-automated green FD-192.
  - d) (U//FOUO) The index copy of the non-automated green FD-192 serves as the index of property acquired as evidence. A consolidated record of all index copies is to be maintained in the ECR in a binder labeled "(Name of Field Office) – Index of Evidence." The index copies are to be filed by evidence category (general, valuable, drug) in numerical sequence by file number. If a satellite ECR is established in a resident agency, the index copies of the non-automated green FD-192s for evidence maintained in that RA are to be maintained in the field office headquarters city ECR in a separate binder labeled "(Name of Resident Agency) – Index of Evidence" and filed therein as noted above. To maintain an effective recordkeeping system and to facilitate the conduct of physical inventories, the HQC's and RA's indices must be kept up to date by noting any type of charge-out/transmittal/disposition of property on the appropriate index copy.
- 2. (U//FOUO) A 1B number should be assigned to the non-automated green FD-192 by the ECT. A notation should be made on the non-automated green FD-192 noting the exact location of the property stored in the ECR. When applicable, the 1B number should also be listed on the evidence label attached to the plastic pouch containing drug or valuable evidence. The ECT should ensure that the location of the property and the 1B number are legible on each copy of the non-automated green FD-192.
  - 3. (U//FOUO) When physical inventories are conducted, the inventories of pre-automated evidence must be reconciled with the index copies of the non-automated green FD-192s maintained by the ECT in the headquarters city ECR, and not those maintained in satellite ECRs in the RA. Therefore, the headquarters city ECT should be advised of any type chargeout/transmittal/disposition of property located in the RA to prevent discrepancies.
  - 4. (U//FOUO) If pre-automated evidence is required to be transmitted to FBIHQ and/or the DEA Laboratory, it is suggested that the evidence be immediately entered into the collected item database.

#### 4.6.2. (U//FOUO) Assessment Evidentiary Property

(U//FOUO) Upon submitting evidence to the ECT, the FBI employee must ensure that the evidence is being submitted to an investigative file, including zero sub-assessment files for Type 1 and 2 Assessments, substantive classification assessment files for Type 3-6 Assessments, or predicated investigation files. Evidence is not authorized for entry into control files or other non-assessment zero files. Items collected as potential evidence during assessments must be



UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

entered into the appropriate zero sub-assessment file, substantive classification assessment file, or predicated investigation file in the appropriate classification.

**4.6.2.1. (U//FOUO) Administrative Handling and Storage of Evidentiary Property**

(U//FOUO) Administrative handling and storage of assessment evidence is conducted in the same manner as all evidence in the FBI's possession.

**4.6.2.2. (U//FOUO) Collected Items Report on Closed Assessments**

(U//FOUO) Retention of evidence/non-evidence in pending and closed zero sub-assessment and substantive classification assessment files must be monitored through ACS to:

- (U//FOUO) Provide supervisory personnel the tools to enforce prompt property disposition through the case review process.
- (U//FOUO) Provide field office management with statistical reports to identify individuals/squads which are not in compliance with property disposition procedures.
- (U//FOUO) Highlight noncompliance trends to the Inspection Staff for evaluation.
- (U//FOUO) Print and distribute a Zero Sub-Assessment Collected Items Report and a Substantive Classification Assessment File Collected Items Report to the appropriate FBI employee assigned the case at 60-day intervals in closed assessments. This is done by the ECT to ensure that those items eligible for disposition in closed assessments are handled. This report should encompass all items closed from 12/16/2008, to present. (The top and bottom copies of this report must be maintained by the ECT from inspection to inspection.)
- (U//FOUO) Indicate on the report if evidence/non-evidence in closed assessments is to be retained for an extended period of time. The FBI employee should do so by recording an anticipated disposition date and his/her initials on the report. (An EC to the zero sub-assessment file or substantive classification assessment file is then required explaining the reason for retaining the evidence. A copy of the EC is maintained in the ECR until final disposition of the evidence.) The report is then initialed by the supervisor and returned to the ECT. (The returned reports showing retention are to be maintained in a binder in the ECR from inspection to inspection.)

**4.7. (U//FOUO) General Evidence**

**4.7.1. (U//FOUO) Items of Evidence**

(U//FOUO) Items of evidence to include, but not limited to; clothing, typewriters, computer equipment, latent fingerprints lifted from a crime scene, and documentary items (exclusive of ELSUR evidence) such as books of account, printed materials, video tapes, motion picture films, magnetically or electronically recorded cards, tapes, and discs are treated as general evidence and stored within the ECR.

**4.7.2. (U//FOUO) Documentary Items**

(U//FOUO) If documentary items have been admitted into evidence during court proceedings or serve a continuing law enforcement purpose, the items may be retained by the FBI with the

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

concurrence of the United States Attorney (USA). (See the Legal Handbook for Special Agents, 5-12.4.)

#### 4.7.3. (U//FOUO) Electronic Surveillance (ELSUR) Evidence

(U//FOUO) ELSUR evidence is treated as general evidence in the collected item database, and handled according to procedures set forth herein.

#### 4.7.4. (U//FOUO) Blood/Liquid Stained Clothing Evidence

(U//FOUO) Clothing that may contain blood and/or other liquids of known or unknown origin, should be completely dried before being stored or shipped. In field offices that are moving to newly acquired space, or are being renovated, a separate room (not inhabited by employees) should be used to air-dry these garments. This room is to be either in the ECR or adjacent to the ECR and have outside ventilation. If the drying room is outside of the ECR, it must be as secure as the ECR.

#### 4.7.5. (U//FOUO) Storing and/or Shipping Blood-Stained Garments

(U//FOUO) Prior to storing and/or shipping blood-stained garments, consult the Handbook of Forensic Science and the Dangerous Goods Regulations.

#### 4.8. (U//FOUO) Firearms Evidence

(U//FOUO) A firearm/weapon is defined as an assembly of a barrel and action from which a projectile(s) is propelled by the products of combustion, real or inoperable.

##### (U//FOUO) W - Weapon

- (U//FOUO) All firearms/weapons as defined above are to be classified and stored as firearms and categorized and entered into ACS/collected items as "Firearms/Weapons."
- (U//FOUO) Silencers must be treated as weapons and are required to receive their own IB numbers, regardless of whether or not they are attached to guns. Silencers are to be classified and stored as firearms and categorized and entered into ACS/collected items as "Firearms/Weapons."
- (U//FOUO) Any evidence item attached to, or packaged in, a primary container with a firearm, should be left in its original condition, stored with the firearm, categorized, and entered into ACS/collected items as "Firearms/Weapons."

##### (U//FOUO) O - Other

- (U//FOUO) A firearm/other is to include all accessories, parts, ammunition and associated items, including but not limited to: sites, holsters, bayonets, cases, scopes, flash suppressors, magazines, muzzle attachments, and flashlights/laser sighting devices that are designed or meant to be used in conjunction with a firearm, and are to be classified and stored as a firearm and categorized and entered into ACS/collected items as a "Firearms/Other."
- (U//FOUO) All BB guns, toy guns, water guns, pellet guns, starter pistols, items used as guns (that do not have an action from which a projectile(s) is propelled by the products of

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

combustion), and other firearm-like weapons, are classified and stored and as firearms and categorized and entered into ACS/collected items as "Firearms/Other."

- (U//FOUO) All items categorized as a firearms/other, to include ammunition, and accessories, parts and associated items, must also be stored as such, and entered into ACS/collected items as "Firearms/Other."
- (U//FOUO) All firearms/weapons and firearms/other, must be stored in the firearms section of the ECR, albeit separately, and entered into the ACS/collected item database under its own 1B number and barcode number.

**4.8.1. (U//FOUO) By Statutes**

- A. (U//FOUO) Title 18, U.S.C., Section 3665, provides as follows: Firearms possessed by convicted felons-

(U//FOUO) "A judgment of conviction for transporting a stolen motor vehicle in interstate or foreign commerce or for committing or attempting to commit a felony in violation of any law of the United States involving the use of threats, force, or violence or perpetrated in whole or in part by the use of firearms, may, in addition to the penalty provided by law for such offense, order the confiscation and disposal of firearms and ammunition found in the possession or under the immediate control of the defendant at the time of his arrest. The court may direct the delivery of such firearms or ammunition to the law enforcement agency which apprehended such person, for its use or for any other disposition in its discretion."

- B. (U//FOUO) In all cases in which firearms and ammunition are seized pursuant to the above statute, the USA must be notified of the seizure so that USA may bring it to the attention of the court at the time of sentencing.
- C. (U//FOUO) There is no objection to a court order directing disposal by the FBI Laboratory.
- D. (U//FOUO) Other federal statutes, indexed under "Firearms" in the U.S. Code Annotated, provide for forfeiture of firearms used in violation of various statutes including those involving liquor laws and those used in named national parks, and declares contraband any firearm with respect to which there has been committed a violation of any provision of the National Firearms Act (or any regulation issued pursuant thereto). The responsibility for selecting the applicable statutes, if any, is that of the USA.

**4.8.2. (U//FOUO) By Other Means**

(U//FOUO) If a firearm (or ammunition) is held for evidence and any person demands its immediate return, or if a firearm is otherwise held and two or more claimants dispute ownership, the weapon should be held and the legal problem referred to the USA.

**4.8.3. (U//FOUO) Abandoned**

(U//FOUO) For all firearms obtained by the FBI through a court order or the abandonment process, a waiver of ownership must be handled according to the following criteria:

1. (U//FOUO) All firearms must be submitted to the Firearms-Toolmarks Unit, FBI Laboratory, along with any requests for their return to the field offices and justification for such action.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

2. (U//FOUO) The Laboratory must have the option of retaining any such firearms for its Reference Firearms Collection (RFC) unless specifically instructed by court order to destroy a firearm.
3. (U//FOUO) The FBI Academy, Quantico, must be advised by the Laboratory of any firearms received that are not being included in the RFC and must decide whether they are needed for training purposes or for reissue.
4. (U//FOUO) If there is a request for the return of the firearm to the field office for issue or display and if it is not needed by the Laboratory or Training Division, the Training Division must evaluate the request and, if approved, perform the necessary refurbishing or deactivation of these firearms. It is to be noted that approval of such requests must not be routine and must be supported by ample justification.
5. (U//FOUO) If not needed by the Training Division or Laboratory Division, and there is no request to return the firearm to the field (or if the request is denied), the Laboratory must destroy the firearm. The field office is not authorized to destroy any confiscated firearms.

**4.8.4. (U//FOUO) Seized/Recovered**

(U//FOUO) Seized/recovered firearms that are to be retained by FBI field offices pending resolution of an investigative matter are to be stored in the evidence control room.

**4.8.5. (U//FOUO) Rendered Safe**

(U//FOUO) Firearms are not to be accepted by the ECT for storage until they have been examined by a field office firearms instructor (if a field office does not have a firearms instructor, a Special Weapons and Tactics [SWAT] member may be used) and rendered safe.

(U//FOUO) The firearms instructor is to certify the examination by:

- (U//FOUO) Signing his/her name.
- (U//FOUO) Placing the date that the weapon was examined and rendered safe in the lower portion of the chain-of-custody page of the package copy of the automated FD-192.
- (U//FOUO) Chain-of-custody information is not to be recorded if possession of the firearm does not change during the safety examination. Once rendered safe, firearms may be stored in a secured cabinet or on open shelving within the ECR.

**4.8.6. (U//FOUO) Stored**

(U//FOUO) Firearms and ammunition must be stored separately and entered into the collected item database under their own 1B numbers and barcode numbers.

**4.8.7. (U//FOUO) Contraband Items**

(U//FOUO) Muzzle attachments/silencers, fully-automatic firearms, firearms with no visible serial numbers, rifles with barrels under 16 inches (26 inches total length), and shotguns with barrels under 18 inches (26 inches total length) should be put through the abandonment process, as they may have been legally purchased and owned at one time.

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

**4.8.8. (U//FOUO) Destruction**

- (U//FOUO) The laboratory is responsible for the destruction of abandoned weapons. All firearms, including real guns, inoperable guns, replica guns, BB guns, toy guns and water guns, as well as all items used as guns, must be sent to the laboratory for destruction.
- (U//FOUO) Firearms and firearm-like weapons, ammunition, knives, holsters, gun cases, brass knuckles, and ammunition must be sent to the laboratory for destruction.
- (U//FOUO) The U.S. Marshal Service is responsible for the destruction of forfeiture weapons.
- (U//FOUO) The Defensive Systems Unit of the Training Division is responsible for the destruction of Bureau weapons and "Special Case Weapons."

**4.8.9. (U//FOUO) Accepted Legal Documentation for Destruction**

1. (U//FOUO) Court order for the destruction of the weapons.
2. (U//FOUO) Court order for the destruction of the weapons with a plea agreement.
3. (U//FOUO) Waiver of ownership with an indemnity agreement.
4. (U//FOUO) Abandonment paperwork.
5. (U//FOUO) Donation of weapon to the FBI (SF-597).
6. (U//FOUO) Transfer of property for Bureau purchased case weapons.

**4.8.10. (U//FOUO) Package for Shipping**

- (U//FOUO) Firearms and ammunition must be packaged separately.
- (U//FOUO) Firearms must be unloaded and must be strapped open or tied down to the box or wrapped in paper or bubble wrap.
- (U//FOUO) Ammunition must be packaged tightly to keep from moving about in the box. The box should be labeled "ORM-D AIR SMALL ARMS CARTRIDGES."
- (U//FOUO) Weapons from multiple cases must be shipped separately.

**4.9. (U//FOUO) Drug Evidence**

**4.9.1. (U//FOUO) Maximum Security**

(U//FOUO) Drug evidence, to include over-the-counter drugs, must be afforded maximum security while in the FBI's possession, and not co-mingled with any other drug or any other type of evidence.

**4.9.2. (U//FOUO) Storage Facility**

(U//FOUO) Storage should be in a [redacted] or within the ECR

b7E

**4.9.3. (U//FOUO) High Quantity**

(U//FOUO) If the quantity of drug evidence is of such volume that it cannot be stored in the ECR or another secure facility within the field office space as noted above, it may be stored in a

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

bonded warehouse provided that appropriate security and administrative controls are adhered to and chain-of-custody is preserved.

**4.9.4. (U//FOUO) Form FD-455 (Access Log - Evidence Storage Facility)**

(U//FOUO) A separate Form FD-455 (Access Log - Evidence Storage Facility) is to be maintained for each drug repository. If open shelving is used, then one FD-455 log for the room/vault is sufficient.

**4.9.5. (U//FOUO) Vault Witness Official (VWO)**

(U//FOUO) The ECT/AECT is not authorized to access the drug/valuable storage facility unless accompanied by the AO, or the person(s) designated to act on behalf of the AO as the VWO. The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO can not be an AECT. Each office should limit the number of designated VWOs and must document the list of authorized vault witnessing personnel in the evidence control file.

**4.9.6. (U//FOUO) Submitting Drug Evidence**

(U//FOUO) The agent submitting the drug evidence to the ECT must remain with the ECT while he/she processes the evidentiary property and until the VWO arrives to access the vault and witness the storage of the drugs.

**4.9.7. (U//FOUO) Emergency Access**

(U//FOUO) The only persons having emergency access to the drug/valuable storage facility [redacted] and the ECR are the SAC, the ASAC, and the SSRA. The [redacted]

b7E

**4.9.8. (U//FOUO) Controlled Environment**

(U//FOUO) Drug evidence should be stored in a reasonably controlled environment, as elevated temperatures or humidity may result in some drug decomposition. Marijuana and crude preparations of some other drugs, such as cocaine, PCP (phencyclidine), and methamphetamine, are highly odoriferous and require more than normal ventilation for odor control. Wet or freshly harvested marijuana mildews if not thoroughly dried before being sealed and stored. It is also advisable to fumigate marijuana to curb insect growth within the bundles. For health and safety reasons, proper outside ventilation of the drug vault/room is required.

**4.9.9. (U//FOUO) Weighed/Counted and Verified**

(U//FOUO) Two federal criminal investigative agents and/or deputized officers, one designated the sealing agent/officer and one the witnessing agent/officer (who are not support employees), are responsible for ensuring that drug evidence is weighed/counted and verified before the evidence is sealed. The evidence is then transmitted to the DEA Laboratory or placed in storage according to the following procedures:

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

1. (U//FOUO) Place the drug evidence, along with the original container, in a plastic evidence pouch (9 ½" x 16" or larger) and then weigh and/or count it. The weighing should be performed on a scale capable of weighing in gram increments, and the weight recorded on the FD-723 (Evidence Label). If the drug seizure involves tablets or capsules, determine the number of tablets or capsules by actual count if the quantity is small or, if too voluminous to count, by computation based on relative weights (e.g., count and weigh 100 units to determine a unit weight, and then divide this weight into the net weight of the entire exhibit to determine the total number of units). If liquids are involved, report the gross quantity by volume. Base estimates on the known or apparent size of the container.
2. (U//FOUO) Complete the FD-723 with the following information:
  - (U//FOUO) Name of field office.
  - (U//FOUO) File number.
  - (U//FOUO) Date of seizure or purchase.
  - (U//FOUO) Sealing official's printed name.
  - (U//FOUO) Sealing official's signature.
  - (U//FOUO) Witnessing official's printed name.
  - (U//FOUO) Witnessing official's signature.
  - (U//FOUO) Laboratory examiner's signature (if applicable).
  - (U//FOUO) Total package weight (for drugs).
  - (U//FOUO) DEA Exhibit Number (for drugs).
3. (U//FOUO) Ensure that the completed FD-723 is placed on the outside of the plastic evidence pouch (9½" x 16" or larger), at the top, and folded at the perforation over both sides of the pouch. Insert the evidence pouch into the heat sealer, ensuring that the heat seal is made across the FD-723 and within two inches from the top of the evidence pouch.
4. (U//FOUO) The use of plastic evidence envelopes is not always practical for bulk drug evidence seizures. Therefore, package the entire bulk shipment in boxes or cartons of uniform size. Each box should contain no more than 15-20 kilograms of substance and should be packed as full as possible. Packing material should be added, if required, to ensure that boxes are not crushed when stacked and transported.
5. (U//FOUO) Close each box or carton with fiber-reinforced plastic tape ensuring that the tape encircles the carton and that the tape ends meet or overlap on the top.
6. (U//FOUO) Complete an FD-723 to include the date of sealing and the printed names and signatures of the sealing agent/officer and witnessing agent/officer.
7. (U//FOUO) Affix the FD-723 to each box at the top to ensure that it covers both ends of the plastic fiber-reinforced tape.
8. (U//FOUO) Number each box consecutively (e.g., 1 of 10; 2 of 10; 3 of 10) in large print with a permanent marker.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

9. (U//FOUO) Mark each box with the number of packages it contains (for additional specifics on bulk drug seizures.)
10. (U//FOUO) Open and reseal drug evidence in the presence of at least two federal criminal investigative agents/deputized officers. The reasons and procedures must be fully documented in an FD-302. Two copies of the FD-302 are to be generated; one is designated for the investigative case file, and a second copy is to be presented to the ECT with the resealed evidence. (The ECT is to maintain the ECR copy of the FD-302 in a binder from inspection to inspection.)
11. (U//FOUO) Open a sealed plastic evidence pouch by cutting off the sealed upper edge with scissors or a paper cutter, ensuring that the FD-723 remains intact. If the evidence is to be resealed, both portions of the used pouch are to be retained, placed in a new evidence pouch with the evidence and sealed following the above-listed instructions. Opening and resealing drug evidence is to be continued in this fashion.
12. (U//FOUO) The "repackage" function in the collected item database must be used and the new packaging must be given a new barcode for the resealing process.
13. (U//FOUO) When bulk drug evidence must be opened, it is done so by first cutting the FD-723 from the top of the box. If the evidence is to be resealed, the previously used FD-723 is placed in a plastic envelope affixed to the outside, then the box is sealed following the above-listed instructions. (For detailed procedures on entering drug evidence into the collected item database, see the Advanced Automated Case Support [ACS ] User's Guide.)
14. (U//FOUO) The "repackage" function in the collected item database must be used, and the new packaging must be given a new barcode for the resealing process.

(U//FOUO) Investigative or operational requirements may necessitate the temporary storage of bulk drug evidence for later use by investigators. The original containers cannot be marked or otherwise altered without adversely affecting the investigation or operation. Storage of the drugs in the ECR is temporary, although the drugs may be permanently stored in the ECR at a later date. Under these circumstances, the drugs must remain in the original packaging (boxes, suitcases, individual kilograms, etc.) and then be placed in additional boxes, cartons, or other containers and sealed as described. The original packaging containing the drugs may not be marked or otherwise altered. In this manner, the original packaging containing the drugs remains unaltered, while the external packaging is sealed with appropriate documentation.

**4.9.10. (U//FOUO) Laboratory Analyses by DEA**

(U//FOUO) Laboratory analyses of seized drugs must be conducted by the DEA Laboratories. The transmittal to and return of drug evidence from the DEA Laboratories are to be recorded in the collected item database.

(U//FOUO) Usually, FBI requests DEA to forward the original packaging that contained the drugs to the FBI Laboratory for latent fingerprint analysis. When this occurs, the packaging must be returned, separate from the drugs, at a later date. To account for the evidentiary property that has now become two pieces, the "split" function is performed in the collected item database when the drugs are returned. This gives both pieces of evidence their own chain-of-custody and barcode. If the DEA chemist properly seals the drugs, the evidence pouch is not to be resealed by



UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

the FBI. The DEA chemist will testify to the contents and to his/her sealing procedures. (The DEA Laboratory may complete the lower portion of the FD-723 that states "For Lab Use Only." However, it is not required to do so, and DEA reseals the evidence pouch with its own seal.)

(U//FOUO) When drug packaging has been examined for latent fingerprints by the FBI Laboratory (therefore having been separated from its original contents), it is also treated as a drug, and therefore should be sealed by the FBI Laboratory in the same manner as any drug. The FBI Laboratory must heat seal the evidence pouch. The field office ECT is to properly package and heat seal the evidence, completing a new FD-723. The field office must process the sealed drug packaging in the collected item database (continuing the entry that was begun by using the "split" function), and place the evidence in storage in the drug vault with a new barcode. DEA Form 7 (Report of Drug Property Collected, Purchased or Seized) is a six-part form (original and five copies) and is to be used when transmitting drug evidence to the DEA Laboratory. DEA Form 7 is transmitted to the appropriate DEA Regional Laboratory by cover communication. Procedures for filling out the form are as follows:

- (U//FOUO) Type DEA Form 7. Each form is limited to three (3) exhibits inasmuch as there is not sufficient space for the results of analyses of more than three (3) exhibits. Place the submitting office case file number and exhibit number (see Item 9 below) on all drug evidence pouches so they can be matched with the accompanying correspondence. Complete the form as follows:
- (U//FOUO) Item 1: Self-explanatory. Check money flashed only where drugs were seized as a result of using a flash roll.
- (U//FOUO) Item 2: Enter field office file number (e.g., 245A-HN-1234). This number is essential for future case identification and retrieval.
- (U//FOUO) Item 3: Disregard.
- (U//FOUO) Item 4: Enter "FBI."
- (U//FOUO) Item 5: Self-explanatory.
- (U//FOUO) Item 6: Disregard.
- (U//FOUO) Item 7: Self-explanatory.
- (U//FOUO) Item 8: Disregard.
- (U//FOUO) Item 9: The submitting office or the DEA chemist must assign the exhibit number or sequence number. An exhibit is defined as any substance differing in form, color, or shape from any other submitted materials or acquired at a different time and place. When there are several submissions from one field office or separate submissions from several field offices, it is the responsibility of the office of origin to assign the sequential exhibit numbers. The DEA Laboratory may also be contacted to determine the next sequential exhibit number for that particular case.
- (U//FOUO) Item 10: The "alleged" drug is that drug which the evidence is purported to be, or is sold as, by the defendant.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

- (U//FOUO) Item 11: Describe fully the labels on the original containers and specify whether seals on these containers were intact. This entry may be continued under Item 15 ("Remarks"), as necessary.
- (U//FOUO) Item 12: Approximate the amount of substance in each exhibit by size or weight. The exact count and precise weight of submitted exhibits are determined by the DEA chemist.
- (U//FOUO) Item 13: Indicate whether all the materials seized are being submitted or only a portion thereof.
- (U//FOUO) Item 14: Complete only if the evidence was acquired through an undercover purchase.
- (U//FOUO) Item 15: Identify the OO and the OO file number under "Remarks." The OO file number becomes the DEA Laboratory case control number for all future submissions in that case. When drug evidence is submitted by lead offices the lead office must determine the OO file number and enter it under Item 15. It should be indicated under "Remarks," whether latent fingerprint examinations or other forensic laboratory examinations are to be performed by the FBI's Laboratory Division. The cover communication should also set forth these requests and include appropriate case background data.
- (U//FOUO) Item 16: Self-explanatory.
- (U//FOUO) Item 17: Supervisory special agent.

(U//FOUO) The copy distribution for DEA Form 7 is as follows:

- (U//FOUO) Forward copies one through five by cover communication, with the evidence, to the appropriate DEA Laboratory.
- (U//FOUO) Copy six is to be detached by the submitting office, attached to the field office file copy of the cover communication, and filed in the case file.

(U//FOUO) When the laboratory analyses are complete, copy three must be sent to the OO and copies one and two must be returned to the submitting field office. These copies contain results of the DEA analyses and are to be filed in the 1A section (FD-340a) of the case file of the respective field office. All evidence must be returned to the submitting field office for retention and eventual destruction. The DEA Laboratory may not accept responsibility for the storage of drug evidence.

**4.9.11. (U//FOUO) Federal-Wide Drug Seizure System (FDSS)**

(U//FOUO) The Federal-Wide Drug Seizure System is a computerized system that produces records of federal drug removals, without regard for individual agency involvement. Participating agencies are DEA, FBI, the Immigration and Naturalization Service (INS), the U.S. Coast Guard (USCG), and the U.S. Customs Service (USCS). The FBI's participation in the FDSS is required whenever the weight of drugs recovered by the FBI exceeds established weight thresholds. At that time, a Federal Drug Identification Number (FDIN) must be telephonically obtained from the El Paso Intelligence Center (EPIC) and recorded on the DEA Form 7. The FDIN must be used by DEA's Statistical Services Section to capture records from the participating federal agencies. DEA's System to Retrieve Information from Drug Evidence

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

(STRIDE) continues to capture statistical information on FBI drug removals and uses that information for quality control of the FDSS. The following procedures have been established for implementation of the FDSS:

- (U//FOUO) An FDIN is required for drugs recovered if the weight entered in Item #12 of DEA Form 7, "Approx. Gross Quantity Seized," or Item #13 of DEA Form 7, "Approx. Gross Quantity Submitted," exceeds the following thresholds:
  - (U//FOUO) Heroin, 100 grams or ¼ pound
  - (U//FOUO) Morphine, 100 grams or ¼ pound
  - (U//FOUO) Opium, 500 grams or 1 pound
  - (U//FOUO) Cocaine, 500 grams or 1 pound
  - (U//FOUO) Marijuana, 25 kilograms or 50 pounds or 50 plants
  - (U//FOUO) Khat, 5 kilograms or 10 pounds
  - (U//FOUO) Hashish, 1 kilogram or 2 pounds
  - (U//FOUO) LSD, 100 units
  - (U//FOUO) Other drugs, 5,000 units
- (U//FOUO) Separate FDINs are required for each drug that exceeds the above weight thresholds, regardless of whether they came from the same incident. Samples extracted from a bulk seizure do not require separate FDINs. Some examples of when an FDIN is needed are:
  - (U//FOUO) Exhibits 1, 2, and 3 of cocaine are seized during the execution of a warrant. Collectively, the evidence weighs 900 grams; individually, none weighs more than 500 grams. No FDIN is needed for any exhibit.
  - (U//FOUO) Exhibits 1, 2, and 3 of cocaine are seized during the execution of a warrant. Exhibit 1 weighs 600 grams and needs an FDIN. Exhibits 2 and 3 weigh less than 500 grams; neither requires an FDIN.
  - (U//FOUO) Exhibit 1 is 600 grams of cocaine. Exhibit 2 is 250 grams of heroin, and both were seized during the execution of a warrant. Each exhibit requires a separate FDIN.
  - (U//FOUO) Exhibit 1 is a bulk marijuana seizure and is reported on DEA Form 7 along with sub-exhibits 1A through 1K, which are samples extracted from the seizure. The total collected exceeds 25 kilograms. An FDIN is needed for exhibit 1, but not for sub-exhibits 1A through 1K. The FDIN must be obtained by the first federal agency to take custody of the drug evidence. On the rare occasions when the FBI assumes custody of drug evidence from another federal agency, the FDIN must be provided to the FBI as part of the custody transfer.
- (U//FOUO) The FDIN must be obtained by contacting EPIC at FTS (Federal Telecommunication System) [REDACTED] Be prepared to provide the following information that must be recorded in a log maintained by EPIC:
  1. (U//FOUO) Name and title of official requesting the FDIN.

b7E

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

2. (U//FOUO) Agency and telephone number of the official requesting the FDIN.
  3. (U//FOUO) Date and local time collected.
  4. (U//FOUO) Place collected (city and state).
  5. (U//FOUO) Conveyance type (e.g., vehicle, vessel, aircraft, or person).
  6. (U//FOUO) Conveyance identifier (e.g., name or number).
  7. (U//FOUO) Quantity of drug collected (including unit of measure).
  8. (U//FOUO) Type of drug collected (e.g., heroin, cocaine, or marijuana).
- (U//FOUO) EPIC must issue an FDIN, which is a ten-digit number beginning with the four digits of the fiscal year in which the drug evidence was collected (e.g., 1999000325). There are no dashes or periods in the number.
  - (U//FOUO) The FDIN is listed in the "Remarks" section of DEA Form 7.
  - (U//FOUO) The method of drug removal (seized, recovered, collected, or purchased) does not affect the need for an FDIN. The determining factor is the weight estimate which includes the minimum wrapping necessary for evidentiary or packaging purposes.

4.9.12. (U//FOUO) Avoid Package Transfers

(U//FOUO) To maintain the integrity of the drug evidence and to avoid unnecessary handling and possible exposure to toxic materials, agent personnel should not attempt to transfer drug contents from the original package, wrapper, or container into a substitute container. Those items that require both chemical analyses for drug contents and subsequent latent fingerprint, laboratory examinations of the packaging material itself for handwriting, or other type of forensic laboratory analyses, should be submitted to the DEA Laboratory with the appropriate information noted in the "Remarks" section of DEA Form 7. The DEA chemist must conduct the chemical analysis and then forward the items directly to FBIHQ, Attention: Laboratory Division, as appropriate.

4.9.13. (U//FOUO) Avoid Opening Drug Evidence

(U//FOUO) Drug evidence returned from the DEA Laboratory is not to be opened if properly sealed by the DEA chemist, but placed in storage as received. The DEA chemist occasionally removes the evidence from the original container(s) and returns the examined evidence to the submitting office in a substitute container(s), causing uncertainty as to whether the returned evidence is identical to the submitted evidence. In such instances, the ECT should note the change in containers on the package copy of the FD-192, stating the number of sealed containers returned from the DEA Laboratory and the DEA Laboratory numbers that appear on the containers. Appropriate modifications must be made in the collected item database to accurately describe the evidence in storage.

4.9.14. (U//FOUO) Approximate Modifications in Automated Case Support

(U//FOUO) When an agent recovers a piece of drug evidence, that evidence must be weighed with all wrappings and sealed in an evidence pouch. This must be recorded in the accompanying FD-302 as the "approximate gross weight" of the "total package." The drugs must then be tested

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

by the DEA, whereupon the DEA chemists must provide the actual "confirmed" weights used for statistical and trial purposes (net weight of drugs without packaging) and a new total package weight after they have resealed the evidence. The DEA has recorded the last "gross weight" or "total package weight" upon their resealing of the evidence; it is that weight that is used for comparison when weighing the drugs prior to destruction. If the drugs have not been tested, the original weight taken at time of seizure is used for comparison. If there has been any documented change (e.g., resealing event), then the last time the drugs were weighed and re-sealed is used for comparison purposes.

(U//FOUO) When drugs are returned from the DEA Laboratory, the ECT is responsible for making appropriate modifications in the collected item database. When drugs come back confirmed, "Drug Type" and "Drug Confirmed" fields must be modified as such in the collected item database. The "approximate gross weight" of the "total package" drug weight in the "Drug Weight" field must be changed to show the official DEA laboratory-determined "total package weight."

To document all weights, the "Description" field of the collected item database must then be modified as follows:

"Original approximate gross weight of the total package before analysis was \_\_\_\_."

"DEA confirmed weight after analysis is \_\_\_\_."

#### 4.10. (U//FOUO) Valuable Evidence

(U//FOUO) Valuable evidence is defined as money, regardless of amount and country of origin; jewelry, regardless of value or composition; rare coins; works of art; antiques; furs; and other items of intrinsic value. Additionally, items having transactional value, including but not limited to the following list (excluding drug evidence) are considered valuable evidence:

- (U//FOUO) ATM card, bond, calling card, bearer bond, credit card, stock certificate, debit card, transportation token, game token, money order, gambling chip, WIC (Special Supplemental Nutrition Program for Women, Infants, and Children) coupon, gambling card, coupon bond, airline ticket, certificate of deposit, cashier's check, food stamp, check, postal stamp (individual or book).

#### 4.10.1. (U//FOUO) Currency with an Unspecified Amount/Value

(U//FOUO) The ECTs are not to accept currency with an unspecified amount/value.

#### 4.10.2. (U//FOUO) Seized Currency Subject to Criminal or Civil Forfeiture

(U//FOUO) Seized currency subject to criminal or civil forfeiture is to be delivered to the U.S. Marshal Service for deposit in the Seized Asset Deposit Fund, and such transfer is to be recorded by the ECT in the collected item database. However, if the seized currency serves a significant independent, tangible, evidentiary purpose (e.g., presence of fingerprints, packaging in an incriminating fashion, or the existence of a traceable amount of drug residue on the bills), the currency is retained pending final disposition of the investigative matter. When seized currency subject to forfeiture is retained for evidence and not deposited into the Seized Asset Deposit Fund, the United States Attorney's Office must approve. If the cash retained is \$5,000.00 or

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

more, the Department of Justice's (DOJ) Asset Forfeiture and Money Laundering Section Chief must approve.

(U//FOUO) If the currency is subject to forfeiture, the case agent is responsible for ensuring that the forfeiture paralegal specialist, who may want to be present at the verifying count, has been advised of the seizure. After the count, the currency should be converted to a cashier's check made payable to the United States Marshal Service. In some field offices, the determined value of the currency must be transferred electronically to the Seized Asset Deposit Fund, eliminating the need for a cashier's check. The chain-of-custody documentation reflects that the currency was charged out and released for forfeiture.

#### 4.10.3. (U//FOUO) Evidence Independently Counted/Verified

(U//FOUO) Valuable evidence is to be independently counted/verified by two officials. The sealing official is to be a federal criminal investigative agent or deputized officer or support employee; the witnessing official may include the ECT, the paralegal specialist, or other support employee directly involved in the processes of seizing, packaging, and initial documentation of the evidence. They are to verify the accuracy of the count and/or detect any errors before the evidence is sealed and placed in storage.

(U//FOUO) The valuable evidence is placed in a 9½" x 16" (or larger) plastic evidence pouch. The FBI evidence label, FD-723, is to be completed with the following information:

1. (U//FOUO) Field office name.
2. (U//FOUO) File number.
3. (U//FOUO) Date of seizure or purchase.
4. (U//FOUO) Sealing official's printed name.
5. (U//FOUO) Sealing official's signature.
6. (U//FOUO) Witnessing official's printed name.
7. (U//FOUO) Witnessing official's signature.
8. (U//FOUO) Laboratory examiner's signature (where applicable).
9. (U//FOUO) Total estimated value.
10. (U//FOUO) Not applicable.

(U//FOUO) The completed FD-723 is placed on the outside of the plastic evidence pouch (9 ½" x 16" or larger) at the top, and folded at the perforation over both sides of the pouch. Insert the evidence pouch into the heat sealer ensuring that the heat seal is made across the FD-723 and within two inches from the top of the evidence pouch.

(U//FOUO) The agent submitting the valuable evidence to the ECT must remain with the ECT while he/she processes the evidentiary property and until the VWO arrives to access the vault and witness the storage of the valuable evidence.

(U//FOUO) Opening and resealing of valuable evidence must be conducted in the presence of:

1. (U//FOUO) Two federal criminal investigative agents/deputized officers; or

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

- 2. (U//FOUO) One federal criminal investigative agent/deputized officer and one witnessing official; or
- 3. (U//FOUO) Two paralegal specialists (one of whom serves as a sealing official and one as a witnessing official).

(U//FOUO) The sealing and witnessing officials must fully document the reasons and procedures in an FD-302. Two copies of the FD-302 are to be generated. One is designated for the investigative case file, and a second copy is to be presented to the ECT with the resealed evidence. (The ECT is to maintain the ECR copy of the FD-302 in a binder from inspection to inspection.)

(U//FOUO) A plastic evidence pouch is opened by cutting off the sealed upper edge with scissors or a paper cutter, ensuring that the FD-723 remains intact. If the evidence is to be resealed, both portions of the used pouch are to be retained, placed in a new evidence pouch with the evidence, and sealed following the above-mentioned instructions. Opening and resealing evidence is to be continued by this method.

(U//FOUO) The "repackage" function in the collected item database must be used, and the new packaging must be given a new barcode for the resealing process.

(U//FOUO) If valuable evidentiary items are of such size as to preclude the use of a plastic evidence pouch (e.g., paintings), the property should be boxed or wrapped in brown paper and secured with plastic fiber-reinforced tape ensuring that the tape encircles the package and that the tape ends meet or overlap. The FD-723 label is to be completed with all pertinent information and affixed to each box top or package front to ensure that it covers both ends of the plastic fiber-reinforced tape.

(U//FOUO) The "repackage" function in the collected item database must be used and the new packaging must be given a new barcode for the resealing process.

(U//FOUO) When it becomes necessary to open large valuable evidentiary items, the FD-723 is cut first from the front of the package or top of the box. If the evidence is to be resealed, the previously used FD-723 is placed in a plastic envelope and affixed to the outside of the new package or box, and the new package or box is then sealed following the above-detailed instructions.

4.10.4. (U//FOUO) Evidence Afforded Maximum Security

(U//FOUO) Valuable evidence must be afforded maximum security while in the FBI's possession, and not co-mingled with any other type of evidence. Storage should be:

- (U//FOUO) Within the ECR [redacted]
- (U//FOUO) [redacted]

b7E

(U//FOUO) If the quantity of valuable evidence is of such volume that it cannot be stored in the ECR or another secure facility within the field office space as noted above, it may be stored in a

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

[Redacted]

b7E

(U//FOUO) A separate Form FD-455 is to be maintained for each valuable repository.

(U//FOUO) The ECT/AECT is not authorized to access the drug/valuable storage facility unless accompanied by the AO, or the person(s) designated to act on behalf of the AO as the VWO. The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO should not be an AECT. Each office should limit the number of designated VWOs and must document the list of authorized vault witnessing personnel in the evidence control file.

(U//FOUO) The only persons having emergency access to the drug/valuable storage facility [Redacted] and the ECR are the SAC, the ASAC(s), and the SSRAs. The

[Redacted]

b7E

4.10.5. (U//FOUO) Handling Transactional Documents

(U//FOUO) If the account of a transactional document has been closed or the document itself indicates it has been negotiated, the item is no longer considered to be valuable evidence and must be housed in general evidence storage.

(U//FOUO) Fraudulent checks, counterfeit money, checks, or credit cards on closed accounts can be stored as general evidence if submitted as evidence with an FD-302, certifying that the item has no value.

(U//FOUO) The case agent is responsible for marking the container housing the item to indicate that the associated account is closed prior to submitting the item(s) for storage as general evidence.

(U//FOUO) If valuable items are housed in another container (e.g., a wallet or bank bag) upon seizure, the container and the valuable(s) may be stored in one container as valuable evidence.

(U//FOUO) Without a clear indication on the container, as well as an FD-302 certifying the account is closed, the ECT requires the item(s) to be deemed valuable evidence.

4.10.6. (U//FOUO) Describing Valuable Evidence

(U//FOUO) The agent completing the FBI Evidence Data-Loading Form (draft FD-192) must completely describe the evidence being submitted for storage. If the draft FD-192 contains the term "miscellaneous" to describe any of the items, the ECT is not authorized to accept custody of the evidence until such time as the evidence is completely described.

(U//FOUO) If valuable items are housed in another container, the container and its contents must be completely described on the draft FD-192.

4.10.6.1. (U//FOUO) Cash and Non-cash Valuable Evidence

(U//FOUO) Cash and non-cash evidence must be separate evidence records. They may have the same 1B number, but must have different barcodes.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) Cash seized with no value items, either through appraisal or with general evidence items, do not need a separate barcode.

(U//FOUO) Non-cash valuables are not assigned a "Cash Value" in collected item until appraised or the case agent provides a fair market value (FMV).

#### 4.10.7. (U//FOUO) Handling Foreign Currency

(U//FOUO) Foreign currency is to be handled the same way as United States (U.S.) currency. The case agent is responsible for ensuring that foreign currency is assigned a U.S. dollar value prior to submitting the currency to the evidence control technician for storage. The person who obtained the U.S. dollar value of the foreign currency generates an FD-302 including, at a minimum, the date and the source from which the value was obtained. A copy of the FD-302 must be presented to the evidence control technician with the sealed evidence container. The "Est. Dollar Value" entry on the FD-723 must contain the U.S. dollar amount, not the foreign currency value.

(U//FOUO) The evidence control technician is not authorized to accept custody of foreign currency without an accompanying FD-302 containing the U.S. dollar value.

(U//FOUO) Upon custody transfer to the evidence control technician, the following information must be entered into the collected item database:

- (U//FOUO) The "Description" field must contain the denomination of what is received, followed parenthetically by the U.S. dollar value and the date that value was obtained.
- (U//FOUO) The "Dollar Value" field must contain the U.S. dollar value of the foreign currency.
- (U//FOUO) The copy of the FD-302 must be attached to the package copy of the FD-192 and retained with the currency.

(U//FOUO) Note: U.S. dollar values may be found on the internet at [www.reuters.com](http://www.reuters.com). Click onto the "currencies" link and enter the amount and type of foreign currency at the "Currency Calculator." The U.S. dollar value is calculated for you. It is suggested that a copy be printed to supplement the FD-302. A bank will also have currency index information available.

#### 4.10.8. (U//FOUO) Evidence Purchase Money

(U//FOUO) Evidence purchase money is defined as any FBI money that leaves FBI possession and goes into the custody of a subject. Any of this money that is then seized as evidence from said subject, subsequent to the evidence purchase, is entered into evidence as evidence purchase money. At the conclusion of the case, this money is returned to the FBI Finance Division or to the general treasury fund.

- (U//FOUO) All evidence purchase money that is being classified as evidence must be stored and maintained as a valuable.
- (U//FOUO) All evidence purchase money will be marked on the FD-192 as such by the case agent.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

- (U//FOUO) All evidence purchase money will be classified and stored as a valuable and categorized and entered into ACS/collected items as a valuable, sub-category "E."

**4.11. (U//FOUO) CART**

(U//FOUO) (Refer to the Digital Evidence Laboratory [DEL] Quality Assurance Manual)

(U//FOUO) CART evidence includes a CPU (central processing unit), laptop, hard drive, thumb drive, PDA (personal digital assistant), memory stick/card, computer disk, portable game station, memory capable printer/scanner, and other types of data storing equipment. Monitors, keyboards, or non-memory storing printers can be stored as general evidence.

**4.11.1. (U//FOUO) Transferring Evidence to a Regional Computer Forensic Laboratory (RCFL)**

(U//FOUO) FBI-controlled evidence is sent to a Regional Computer Forensic Laboratory (RCFL). An RCFL is a joint venture between the FBI, other federal agencies, and state and local law enforcement established to meet the growing needs of investigators as the volume of computer-related crimes increases. While the FBI has assumed the lead role in establishing and managing these laboratories, they are to be viewed as non-FBI entities when evidence transfers occur between an FBI field office and an RCFL.

(U//FOUO) Computer-related evidence is to be sent directly from a field office to the RCFL of choice. When computer-related evidence is transferred to an RCFL, the following procedures must be followed by FBI personnel:

- (U//FOUO) Update the FD-192 chain-of-custody to reflect that evidence has been transferred to an RCFL. The transfer date and, if applicable, the tracking number under which it was sent are to be recorded on the FD-192.
- (U//FOUO) Update the "Add Chain-of-Custody" field in the collected item database by typing in "(location) RCFL" (e.g., CGRCFL) in the organization field and enter "analysis" in the "reason" field.
- (U//FOUO) Retain the FD-192 and place it into a binder for RCFL transfers until the evidence is returned to your office.
- (U//FOUO) Update both the FD-192 and the collected item database with the relevant information upon receipt of evidence from an RCFL, and return the evidence to its appropriate storage.

(U//FOUO) When a division Charge-out Report is generated, the RCFL location must be segregated.

(U//FOUO) According to the EC dated 11/22/2002, 66F-HQ-A1155003-QAQC, serial 17, evidence derived from the seized item(s) must be handled in the following manner:

- (U//FOUO) Digital media produced from a seized computer during the archive process and media containing data extracted from the original evidence in response to a request is defined as Derivative Evidence (DE). DE must be labeled as such and entered as a (new) 1B collected item. As needed, the case agent may charge out the DE from the collected item database for review and/or analysis.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

- (U//FOUO) It should be noted that copies of DE are to be handled and tracked by the CART examiner. Custody of the DE must be tracked using the FD-192. In the event a copy of the DE is made, it is not to be handled as evidence; it must be marked "1A Material." It is the responsibility of the case agent to ensure that the copy of DE is placed into the 1A section of the investigative file.

**4.11.2. (U//FOUO) Procedures for Transferring Evidence Between an FO and an RCFL**

(U//FOUO) Computer-related evidence charged out of an FO evidence control room must be released to the person taking custody of the evidence after that person signs the FD-192. The FD-192 remains with the ECT. The FD-192 must be placed into a binder for RCFL transfers until the evidence is returned.

(U//FOUO) The ECT must update the chain-of-custody record in the collected item database to reflect the name of the person who charged out the evidence.

(U//FOUO) Upon transfer of the computer-related evidence to the appropriate RCFL, a receipt must be given to the person relinquishing custody.

(U//FOUO) The person who relinquished custody of the computer-related evidence must return the receipt to the field office ECT. If the receipt is not returned to the ECT, the person who charged out the evidence is responsible for verifying every 60 days (when Charge-Out Reports are generated) that the evidence has remained in the custody of the RCFL. If the receipt is returned and the collected item database is updated, the Charge-Out Report must reflect that the RCFL has custody of the evidence.

(U//FOUO) The ECT must then update the chain-of-custody record in the collected item database to reflect that the evidence was transferred to an RCFL by entering the "(location of the RCFL) RCFL." For example, the Greater Houston RCFL would be entered as GHRCFL.

(U//FOUO) Upon return of the evidence from the RCFL, the ECT must execute the FD-192 and appropriately update the chain-of-custody record in the collected item database. The computer-related evidence must be placed into storage.

**4.11.3. (U//FOUO) Handling Derivative Evidence (DE)**

(U//FOUO) When evidence is returned from a forensic examiner, there must be DE returned as well. There must be copy of the evidence (typically on a hard drive or DVD [digital versatile disk]), which is referred to as DE and marked "Archived."

(U//FOUO) The "Archived" and "Results" copies must each be assigned new 1B numbers and new barcodes. In the "Description" field, include the 1B number from which it was derived. (See Chain-of-Custody User Guide.)

(U//FOUO) The "Archived" copy may only be charged out by a CART examiner or an RCFL examiner. The "Results" copy may be charged out to the case agent or any other party authorized by the case agent.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.12. (U//FOUO) Temporary Storage/Night Deposit - Drug and Valuable Evidence**

**4.12.1. (U//FOUO)** [REDACTED]

(U//FOUO) In the event drug and/or valuable evidence needs to be secured after hours, it may be secured in [REDACTED] until the next business day.

b7E

(U//FOUO) [REDACTED]

**4.12.2. (U//FOUO) Off-Duty Hour Evidence Seizure**

(U//FOUO) In the event the seizure occurs after normal business hours, the drug/valuable evidence is to immediately be brought to the field office and placed in overnight drug/valuable night depository/temporary storage. If the package is too large for the night depository, an ECT and a VWO are to be called into the office to store the item(s).

**4.12.3. (U//FOUO) Paperwork and Packaging**

(U//FOUO) When drugs and/or valuables are placed in the night depository/temporary storage, and the paperwork or the packaging is not executed properly, the ECT must not remove the container from the night depository. The ECT must then contact the agent who stored the item(s) and advise him/her what was incorrectly executed. The agent is responsible for immediately making the appropriate corrections and transferring the item(s) to the ECT for storage.

**4.12.4. (U//FOUO) Drop Slot**

(U//FOUO) The drug and/or valuable room may be outfitted with a "drop slot" for after-hours storage of drug and/or valuable evidence. The "drop slot" is to be installed into an external ECR wall that is accessible from an external hallway outside of the ECR and allows for the evidence to be dropped into the drug or valuable room. The "drop slot" is to be constructed in such a manner as to prevent a person from reaching inside to retrieve the drug and/or valuable evidence.

**4.12.5. (U//FOUO) FD-455**

(U//FOUO) An FD-455 must be completed when evidence is placed in and removed from the temporary storage/night deposit.

**4.12.6. (U//FOUO) Daily Removal**

(U//FOUO) The contents of the temporary storage/night depository safe must be removed at the beginning of each work day by the ECT (accompanied by the VWO), properly stored in the ECR pursuant to established policy, and entered into the collected item database. Evidence that is being temporarily stored within the container is to be properly heat-sealed and appropriate documentation is to be attached prior to its temporary storing.

**4.12.7. (U//FOUO) Prohibited Safes**

(U//FOUO) Neither the SAC's safe nor a squad supervisor's safe are to be used for the temporary storage of drug/valuable evidence. In those instances when seizures of drug/valuable evidence are anticipated during off-duty hours (i.e., nights, weekends, or holidays) the services of the ECT/AECT should be used to assist with the analyzing, cataloging, and labeling of the evidence.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

4.13. (U//FOUO) Storage of Evidence in Resident Agencies (RA)

4.13.1. (U//FOUO) Evidence not Relinquished to the ECT

(U//FOUO) Evidence that is needed at the RA for agent review, court proceedings, etc., must be charged out by the ECT to the appropriate agent, who is then responsible for storing it securely.

(U//FOUO) Evidence that is seized, subpoenaed, or voluntarily contributed, and is not relinquished to the ECT for processing into the collected item database, must be stored temporarily within RA space [redacted]

b7E

(U//FOUO) Access to the temporary storage facility is limited to the appropriate agent, and the SSRA or Senior Resident Agent (SRA).

(U//FOUO) An FD-455 is to be maintained for the facility and each instance of access must be recorded thereon to include the signature of the person(s) gaining entry, reason for entry, case file number and 1B number, and the date and time of entry/exit, in order to successfully defend any chain-of-custody challenges.

4.13.2. (U//FOUO) Establishing an ECR in an RA

(U//FOUO) At the discretion of the SAC, an ECR may be established in an RA according to the ECR guidelines, and all rules and regulations applicable to evidence storage and handling must apply. Drug and valuable evidence may be stored within the ECR [redacted]

b7E

[redacted] An employee in the RA is to be designated an ECT, and is directly responsible for the recordkeeping, storage, and maintenance of evidence in the RA. In the event [redacted] the ECT must be [redacted]

b7E

(U//FOUO) An FD-455 is to be maintained for the ECR and the drug and/or valuable repository, whether located within the ECR or [redacted]. Each instance of access must be recorded on the FD-455 to include the signature of the person(s) gaining entry, reason for entry, case file number and 1B, and the date and time of entry/exit, in order to successfully defend any chain-of-custody challenges.

b7E

(U//FOUO) Access to the RA evidence control room and/or [redacted] is strictly limited to the RA evidence control technician and the SSRA/SRA. Access by other employees is prohibited unless accompanied by the RA evidence control technician and SSRA/SRA. Access is to be documented on Form FD-455. For access to the drug/valuable evidence storage facility, whether located within the field office or in [redacted] the RA ECT is accompanied by the SSRA/SRA, who is the vwo. If the drug/valuable evidence is stored in a [redacted] the names of the RA's ECT and SSRA/SRA are to [redacted] and documented in the field office evidence control file by EC. These should be updated as necessary.

b7E

4.14. (U//FOUO) Requesting Evidence Examinations from the Laboratory Division

4.14.1. (U//FOUO) Requests for Examinations

(U//FOUO) All requests for evidence examinations should be addressed in an EC, attention to the FBI Laboratory Evidence Control Unit.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**4.14.2. (U//FOUO) Request Forwarded with Evidence**

(U//FOUO) A request for an examination should be forwarded with the evidence and contain the following:

- (U//FOUO) The nature of and the basic facts concerning the violation insofar as they pertain to the laboratory examination.
- (U//FOUO) The name(s) and sufficient descriptive data (FBI number, date of birth, and Social Security Number) of any subject, suspect, or victim.
- (U//FOUO) A request stating what types of examinations are desired should include, if applicable, comparisons with other cases, listing captions of these cases and Bureau file numbers, if available.
- (U//FOUO) Reference to any previous correspondence submitted to the Laboratory in the case.
- (U//FOUO) Information where the original evidence is to be returned as well as where the original Laboratory report is to be sent
- (U//FOUO) A statement, if applicable, as to whether:
- (U//FOUO) The evidence has been examined previously by another expert.
- (U//FOUO) Any local controversy is involved in the case.
- (U//FOUO) If non-Bureau law enforcement agencies have an interest in the case.
- (U//FOUO) Notification of the need and reason(s) for an expeditious examination.

(U//FOUO) It is only necessary to set one lead to the Laboratory to conduct appropriate examinations.

**4.14.3. (U//FOUO) Each Case Separately**

(U//FOUO) Do not submit multiple cases under a single EC. Each case should be submitted with a separate communication and shipped separately.

**4.14.4. (U//FOUO) International Law Enforcement Requests**

(U//FOUO) All international law enforcement agency/police requests should be coordinated through the appropriate FBI Legal Attaché (Legat). Legats should fax the request to the Evidence Control Unit, 703-632-8334, prior to submitting any evidence to the Laboratory. Questions concerning international submissions should be directed to 703-632-8360.

**4.14.5. (U//FOUO) Operational Technology Division (OTD) Requests**

(U//FOUO) Evidence for audio, computer, electronic device, image analysis, and video examinations should be submitted to the Operational Technology Division (OTD). Do not submit the evidence to the Laboratory Division unless examinations such as latent print, trace evidence, DNA (deoxyribonucleic acid), ballistics, or other Laboratory Division examinations are also needed.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**4.15. (U//FOUO) Packaging and Shipping Evidence to the Laboratory**

(U//FOUO) For any questions regarding packaging and shipping evidence, call the Evidence Control Unit, 703-632-8360.

**4.15.1. (U//FOUO) Packaging and Shipping Procedures**

- (U//FOUO) Take precautions to preserve the evidence. Package each item of evidence separately to avoid contamination.
- (U//FOUO) Ensure that primary evidence packaging is clearly labeled with the date, time, person's name, location, collector's name, case number, and evidence number whenever possible.
- (U//FOUO) Seal the inner container(s) with tamper-evident or filament tape.
- (U//FOUO) Affix Biohazard Warning labels, if appropriate, on the inner container(s).
- (U//FOUO) Place the sealed inner container(s) in a clean, dry, and previously unused shipping container with clean packing materials. Do not use loose styrofoam.
- (U//FOUO) Include the requesting EC between the inner and outer containers in a readily accessible location. If unable to include the EC between the inner and outer containers, contact the Evidence Control Unit, 703-632-8360, for alternate arrangements. Do not send a working copy of an EC.
- (U//FOUO) Seal the shipping container so that tampering with the container would be evident and to
- (U//FOUO) Affix a "Refrigerate Upon Arrival" label on the shipping container if the contents require refrigeration. Do not use ice or dry ice for shipment. Ice can cause damage to the shipping container and evidence as it melts. If necessary, include cold packs in shipment. If cold packs are used, protect invoice or other paperwork to prevent damage from any moisture released by the cold packs.

**4.15.2. (U//FOUO) Hazardous Materials**

(U//FOUO) All shipments of suspected or confirmed hazardous materials, including live ammunition, must comply with U.S. Department of Transportation and International Air Transport Association regulations. Title 49 of the Code of Federal Regulations (CFR) lists specific requirements that must be observed when preparing hazardous materials for shipment by air, land, or sea. In addition, the International Air Transport Association annually publishes Dangerous Goods Regulations detailing how to prepare and package shipments for air transportation. Title 49 CFR 172.101 provides a Hazardous Materials Table that identifies items considered hazardous for the purpose of transportation. Title 49 CFR 172.101 also addresses special provisions for certain materials, hazardous materials communications, emergency response information, and training requirements for shippers. A trained and qualified evidence technician must assist with the typing, labeling, packaging, and shipping of all hazardous materials.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.15.3. (U//FOUO) Shipping**

(U//FOUO) If the request has a deadline or other special circumstances requiring the Laboratory Division's immediate attention, please notify the Evidence Control Unit, 703-632-8360, prior to or upon shipment.

(U//FOUO) Address the outer container as follows:

Evidence Control Unit  
Laboratory Division  
Federal Bureau of Investigation  
2501 Investigation Parkway  
Quantico, VA 22135

(U//FOUO) Ship the evidence by FedEx, U.S. Postal Service Registered Mail, or other trackable method of shipment.

**4.16. (U//FOUO) Special Instructions Regarding the Following Evidence:**

**4.16.1. (U//FOUO) Abrasives**

- (U//FOUO) Submit abrasives in heat-sealed or resealable plastic bags or paint cans. Do not use paper or glass containers.

**4.16.2. (U//FOUO) Biological Evidence (Blood; Buccal/Oral Swabs, Body Fluid Stains)**

- (U//FOUO) Refrigerate, do not freeze, liquid blood samples (tubes may break if frozen). Use cold packs, not dry ice, during shipping.
- (U//FOUO) Pack liquid blood tubes individually in styrofoam or cylindrical tubes with absorbent material surrounding the tubes. Multiple tubes can be included in a single shipment.
- (U//FOUO) Air-dry swabs and place in clean paper or an envelope with sealed corners.
- (U//FOUO) Do not use plastic containers for any samples other than tissue samples.
- (U//FOUO) Place tissue samples in a clean, airtight plastic container (without formalin or formaldehyde) and store in a freezer. If a freezer is not available, refrigerate the sample. (Buccal samples do not need to be refrigerated.) Submit to the Laboratory as soon as possible.
- (U//FOUO) Protect skeletal remains stored in paper bags with protective material such as bubble wrap or paper to prevent damage to the bones during shipment.
- (U//FOUO) Pack evidence with potential stains very carefully in order to prevent stain removal by abrasive action during shipping.
- (U//FOUO) Handle immovable objects by cutting a suspected stain with a clean, sharp instrument and pack in clean paper or an envelope with sealed corners. If unable to cut stain from object, absorb suspected stain onto a clean cotton cloth or swab. Air-dry the cloth or swab and pack in clean paper or an envelope with sealed corners.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**4.16.3. (U//FOUO) Bank Security Dye**

- (U//FOUO) Do not submit large stained evidence (e.g., car seats). Cut a small sample of the stained area and submit in a heat-sealed or resealable plastic bag
- (U//FOUO) Submit an unstained control sample, packaged separately.
- (U//FOUO) Transfer questioned stains (if unable to collect cutting) by rubbing with a clean (dry or wet with alcohol) cotton swab. Air-dry the swab and pack in a heat-sealed or resealable plastic bag.
- (U//FOUO) Submit an unstained control swab, packaged separately.

**4.16.4. (U//FOUO) Building Materials/Glass/Seal-Insulation/Soil**

- (U//FOUO) Ship known and questioned debris separately to avoid contamination.
- (U//FOUO) Package debris in leakproof containers such as film canisters or plastic pill bottles. Keep lumps intact.
- (U//FOUO) Do not use paper or glass containers.
- (U//FOUO) Package all glass separately and securely to avoid shifting and breaking during shipping.
- (U//FOUO) Secure large pieces of glass between plywood or sturdy cardboard.
- (U//FOUO) Include a map identifying soil-sample locations.

**4.16.5. (U//FOUO) Cigarettes/Cigars/Chewing Gum**

- (U//FOUO) Do not submit ashes.
- (U//FOUO) Do not use plastic containers.

**4.16.6. (U//FOUO) Drugs/Controlled Substances**

- (U//FOUO) Do not submit quantities exceeding 100 grams of marijuana or 10 grams of all other drugs, including cocaine, methamphetamine, and heroin.
- (U//FOUO) Package drug evidence properly. Drug residue requests can be accepted only if evidence is properly packaged to avoid contamination.
- (U//FOUO) Submit evidence in separate heat-sealed bags.
- (U//FOUO) Do not submit used drug field-test kits with the evidence.

**4.16.7. (U//FOUO) Explosives/Explosive Residue**

(U//FOUO) Explosives are hazardous materials and must be handled only by qualified public safety personnel, military explosive ordnance disposal personnel, or certified bomb technicians.

- (U//FOUO) Notify the Evidence Control Unit, 703-632-8360, when shipping bomb components.
- (U//FOUO) Do not use Ziplock bags for shipping or storing explosive residue evidence.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

- (U//FOUO) Do not store or ship explosive residue evidence with bulk explosive material.
- (U//FOUO) Do not store or ship explosive residue evidence from a crime scene with evidence from a search site.

**4.16.8. (U//FOUO) Firearms**

- (U//FOUO) Unload all firearms.
- (U//FOUO) Package and ship to avoid shifting during shipment. For example, secure the firearm in gun box with zipties.
- (U//FOUO) Package and ship firearms separately from ammunition.

**4.16.9. (U//FOUO) Hazardous Material**

(U//FOUO) Over 3,000 items, including flash paper, live ammunition, explosives, radioactive materials, flammable liquids and solids, flammable and nonflammable gases, spontaneously combustible substances, and oxidizing and corrosive materials are currently considered hazardous materials. All items require special packaging, and the amount of each item which can be shipped is regulated. Therefore, the applicable action listed below is to be taken:

- (U//FOUO) Flash paper: Contact the Scientific Analysis Section for shipping instructions each and every time this item is to be submitted to the Laboratory.
- (U//FOUO) Other hazardous materials: Contact the Explosives Unit for shipping instructions each and every time any hazardous material, except flash paper or live ammunition, is to be submitted to the Laboratory.

**4.16.10. (U//FOUO) Knives**

- (U//FOUO) Package knives securely in a rigid container.
- (U//FOUO) Do not package knives in paper or plastic bags.

**4.16.11. (U//FOUO) Latent Print Evidence**

- (U//FOUO) Known prints must be shipped with other evidence. Do not submit known prints by Bureau mail. If known prints must be submitted separately from the evidence, submit with requesting EC by trackable method.
- (U//FOUO) Hands or fingers of an unknown, deceased individual should be shipped in the condition in which they were found (e.g., in water, frozen, dried) by overnight trackable method of shipment. Each hand or finger should be in a separate unbreakable, watertight, and airtight container.
- (U//FOUO) Legible, complete ten-print fingerprint cards that are not related to an ongoing Laboratory investigation should be sent to the Criminal Justice Information Services Division. Address the outer container as follows:

Criminal Justice Information Services Division  
Federal Bureau of Investigation  
1000 Custer Hollow Road  
Clarksburg, WV 26306

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**4.16.12. (U//FOUO) Lubricants**

- (U//FOUO) Package lubricants separately in leakproof containers.

**4.16.13. (U//FOUO) National Missing Person DNA Database Program Requests**

- (U//FOUO) Include a copy of the anthropology, odontology (dental), medical examiner and/or coroner, and law enforcement reports.
- (U//FOUO) Include a Consent and Information Form for the National Missing Person DNA Database (FD-935) with samples from biological relatives of missing persons.

**4.16.14. (U//FOUO) Paint/Polymers**

- (U//FOUO) Do not use plastic bags, cotton, or envelopes as primary packaging for paint specimens.
- (U//FOUO) Do not attach paint particles to adhesive tape.
- (U//FOUO) Package paint specimens in leakproof containers such as vials or pillboxes.
- (U//FOUO) Remove damaged suspect motor vehicle parts and package separately in resealable plastic bags or boxes.
- (U//FOUO) Submit entire item. If it is not possible to submit an entire item, cut section where the transfer is suspected with a clean, sharp instrument. Collect an unstained control sample. Pack to prevent stain removal by abrasive action during shipping. Pack in clean paper. Do not use plastic containers.

**4.16.15. (U//FOUO) Pepper-Spray or Foam**

- (U//FOUO) Submit spray canisters when possible.
- (U//FOUO) Refer to Hazardous Material Transportation Manual when submitting pepper-spray canisters.

**4.16.16. (U//FOUO) Product-Tampering**

- (U//FOUO) Package and ship control and suspect samples separately to avoid contamination.
- (U//FOUO) Submit samples in leakproof containers such as film canisters or plastic pill bottles.
- (U//FOUO) Do not use paper or glass containers.
- (U//FOUO) Use caution to prevent destroying latent prints.

**4.16.17. (U//FOUO) Questioned Documents**

- (U//FOUO) Do not fold, tear, mark, soil, stamp, write on, or excessively handle document evidence.
- (U//FOUO) Protect documents from inadvertent indented writing by packaging in a hard container such as a box or other rigid container.
- (U//FOUO) Package typewriters securely to prevent damage during shipment.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

- (U//FOUO) Do not store or ship photocopies in plastic envelopes.
  - (U//FOUO) Do not add indentations by writing on top of the evidence.
  - (U//FOUO) Ship burned or charred paper in the container in which it was burned, in polyester film encapsulation, or between layers of cotton in a rigid container.
  - (U//FOUO) Submit rubber stamps uncleaned.
- 4.16.18. (U//FOUO) Serial-Numbers
- (U//FOUO) If possible, remove the section containing the serial number on large objects, and submit it to the Laboratory.
  - (U//FOUO) If unable to remove the section containing the serial number, make a cast to submit to the Laboratory. Contact the Firearms-Toolmarks Unit at 703-632-8442 for casting instructions. Pack the cast to prevent breakage during shipment.
- 4.16.19. (U//FOUO) Shoe Print and Tire Tread
- (U//FOUO) Submit original evidence whenever possible (shoes, tires, photographic negatives, casts, lifts).
  - (U//FOUO) Package casts carefully to prevent breakage.
  - (U//FOUO) Do not clean casts.
  - (U//FOUO) Do not package casts or lifts in plastic.
  - (U//FOUO) Dry casts for at least 48 hours before shipment.
- 4.16.20. (U//FOUO) Tape
- (U//FOUO) Tape should not be removed from substrate if possible. If unable to submit entire object, tape should be placed adhesive side down on a clean, colorless piece of plastic sheeting (e.g., transparency film or Kapak tubular rollstock), not on cardboard, paper, or vinyl document protectors. Do not distort or tear the tape during removal.
  - (U//FOUO) If tape was cut during removal/collection, document and initial each cut prior to submitting to the Laboratory. If possible, use a method that produces a unique cutting pattern (e.g., pinking shears).
- 4.16.21. (U//FOUO) Toolmarks/Tools
- (U//FOUO) Submit samples of any material deposited on tools in leakproof containers such as film canisters or plastic pill bottles.
  - (U//FOUO) Do not place the tool against the toolmarked evidence for shipment unless tool and toolmarked evidence are packaged in rigid containers.
  - (U//FOUO) Mark ends of evidence to specify which end was cut during evidence collection.
- 4.16.22. (U//FOUO) Unknown Substance
- (U//FOUO) Submit powder and liquid samples in leakproof containers.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.16.23. (U//FOUO) Weapons of Mass Destruction**

(U//FOUO) Suspected or confirmed Weapon of Mass Destruction (WMD) crime scenes should be handled only by qualified personnel. Upon notification or suspicion of a possible WMD incident, contact the FBI's Strategic Information and Operations Center at 202-323-3300 and ask for the Weapons of Mass Destruction Operations Unit Duty Officer.

(U//FOUO) Suspected or confirmed WMD evidence must be properly field-screened by qualified personnel to determine the absence or presence of hazardous materials before it can be analyzed by the Laboratory or partner laboratories. Questions concerning WMD evidence examinations should be directed to the Chemical and Biological Sciences Unit at 703-632-7766.

**4.16.24. (U//FOUO) Volatile Memory Devices (VMD)**

(U//FOUO) Special requirements have been established for the handling, storing, and protecting of VMDs. VMDs need to be maintained in a charged state to prevent data loss, as well as wireless communications digital evidence, such as PDAs, cell phones, and computers that can be altered by wireless communication while in storage.

(U//FOUO) To obtain more information on these requirements, contact the CART Unit Chief or Forensic Electronic Device Analysis (FEDA) personnel.

**4.17. (U//FOUO) Transmittal of Evidence to Field Offices and FBIHQ/DEA Laboratories**

**4.17.1. (U//FOUO) Mailing/Shipping to the Field Office or RA ECR**

(U//FOUO) The ECT is responsible for properly preparing evidence for mailing/shipping to the appropriate field office ECR or RA ECR. The ECT must refer to the ECR Directory for shipping information prior to completing shipment.

(U//FOUO) The inner packaging must be appropriately wrapped to protect the integrity of the evidence. The shipping invoice and/or FD-192 must be placed between the inner and outer packing for easy retrieval.

(U//FOUO) The outer packaging must be appropriately marked to indicate the contents of shipment, (i.e., D-drugs, V-valuables, F-firearms, C-CART, and G-general). The shipping label must have clear transparent yellow tape affixed over the address portion of the label (not over the barcode).

(U//FOUO) For shipping of drug and valuable evidence, the case agent is to ensure that the evidence is properly heat-sealed prior to being packaged for shipment. Because drug/valuable evidence is not to be left solely in the custody of the ECT, the case agent/acquiring agent and/or the VWO is to witness the wrapping/packaging of such evidence by the ECT for shipment.

(U//FOUO) The transmitting office ECT should notify the receiving office ECT of the shipment.

**4.17.2. (U//FOUO) U.S. Postal Service Registered Mail or Federal Express**

(U//FOUO) Because of chain-of-custody requirements, all evidence transmitted between FBI offices in the U.S. and Puerto Rico, is to be sent by either U.S. Postal Service, using only registered mail, or by Federal Express.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) Bureau policy for the general instruction for mailing / shipping must be followed as stated in MAOP, Part 2, 2-2.2.

(U//FOUO) Regardless of the mode of shipping, clear yellow evidence tape must always be placed over the shipping address label.

(U//FOUO) Evidence that is shipped to other agencies is to be shipped by U.S. Registered Mail, return receipt requested (Postal Service Form [PS] 3811.) The receipt is then placed in the 1A section of the investigative case file.

(U//FOUO) Evidence that is being returned to the contributor/owner is to be shipped U.S. Registered Mail, return receipt requested. The receipt is then placed in the 1A section of the investigative case file. An FD-597 should be completed and enclosed with a self-addressed envelope with instructions to return it to the ECR.

#### 4.17.3. (U//FOUO) Collected Item Database

(U//FOUO) If evidence is being transmitted from one field office to another, the evidence must first be entered the collected item database.

(U//FOUO) The ECT in the transmitting office must print out two copies of the automated FD-192. The file copy is initialed by the squad supervisor and filed in the investigative case file. If the case file is in the office of origin and it is the lead office that is shipping the evidence to the OO, then the file copy of the FD-192 and all other appropriate documents required by the investigative case file are to be shipped to the OO with the evidence. (Drug and valuable evidence must be appropriately sealed before being transmitted.) The package copy of the automated FD-192 must accompany the evidence that is being shipped. When transmitting to the FBI or DEA Laboratories, the package copy of the automated FD-192 remains filed in a binder marked "(Name of Office) - Evidence Sent to FBI Lab" or "(Name of Office) - Evidence Sent to DEA Lab." The binder is maintained in the ECR.

(U//FOUO) The ECT in the transmitting office must record the manual chain-of-custody on the automated FD-192 maintained with the evidence. Refer to Chain-of-Custody User Guide [[http://lab.fbinet.fbi/ecu/field\\_evidence\\_program.htm](http://lab.fbinet.fbi/ecu/field_evidence_program.htm)].

(U//FOUO) The ECT in the receiving office performs the "check in" function in the collected item database. The original FD-1004 that accompanied the evidence is appropriately signed and remains with the evidence in the receiving office.

#### 4.17.4. (U//FOUO) From a Field Office to FBIHQ or DEA

(U//FOUO) If evidence is being transmitted from a field office to FBIHQ or a DEA Laboratory, it must first be charged out manually and documented in the collected item database. Drug and/or valuable evidence must be sealed prior to being shipped.

(U//FOUO) The ECT in the transmitting office must record the manual chain-of-custody on the automated FD-192 maintained with the evidence. (Refer to Chain-of-Custody User Guide.) [[http://lab.fbinet.fbi/ecu/field\\_evidence\\_program.htm](http://lab.fbinet.fbi/ecu/field_evidence_program.htm)]. The package copy of the automated FD-192 is retained in the ECR and filed in a binder/folder labeled "Evidence Sent to FBI (or DEA) Laboratory" according to the date of transmittal.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) When the evidence is returned, the ECT is to record chain-of-custody on the automated FD-192 maintained with the evidence and in the collected item database. If it is general evidence, affix the package copy of the automated FD-192 to the evidence. If it is drug or valuable evidence, place the package copy of the automated FD-192 in the binder maintained in the drug/valuable vault.

#### 4.17.5. (U//FOUO) Evidence Seized/Recovered by RA Personnel

(U//FOUO) As a general rule, evidence seized/recovered by RA personnel is stored in HQC and transmittal of such evidence to another field office/FBIHQ/DEA Laboratory is handled by the headquarters city ECT. However, if an ECR has been established in an RA, evidence must be administratively handled and entered into the collected item database prior to being wrapped/packaged/shipped by the RA ECT, according to the aforementioned guidelines. Otherwise, RAs may only transmit evidence directly to another field office/FBIHQ/DEA Laboratory in instances where 1) the urgency of a particular situation demands expedient handling, or 2) in instances when the bulk of the evidence is such that to ship through HQC for subsequent shipping elsewhere would be impractical. In such instances where FBIHQ/DEA Laboratory returns evidence directly to an RA, and the RA does not have an established ECR, a copy of the communication transmitting/returning the evidence and copy of the updated chain-of-custody must be furnished to the headquarters city ECT for appropriate administrative handling.

#### 4.17.6. (U//FOUO) Marking Obscene and Indecent Material

(U//FOUO) Before filing or forwarding obscene and indecent material which has come into the possession of an employee during the course of an investigation, the employee must place the material in a sealed container. The container must be marked for identification and the label must be marked "Obscene." Such evidence is considered general evidence and stored in the ECR.

#### 4.18. (U//FOUO) Charge-Out Procedures - Evidentiary Property

##### 4.18.1. (U//FOUO) Evidence Stored in the ECR

(U//FOUO) Evidence stored in the ECR, or other evidence storage facilities, may be charged out to any employee having an official need. Evidence may be charged out for up to 60 calendar days and recharged at the end of those 60 days. If necessary, the evidence may be charged out every 60 days thereafter as follows:

- (U//FOUO) The ECT is to record chain-of-custody on the automated FD-192 and in the collected item database.
- (U//FOUO) The package copy of the automated FD-192 must remain with the evidence. Care should be exercised by the employee accepting custody of the evidence to ensure that chain-of-custody information is recorded on the package copy of the automated FD-192.

##### 4.18.2. (U//FOUO) Collected Item Database Charge-Out Reminders

(U//FOUO) The ECT must run the collected item database charge-out reminders, and recharge evidence every week or every two weeks, depending on the size of the field office. This report should encompass all items charged-out from 01/01/1970, to present.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

#### 4.18.3. (U//FOUO) Recharged Evidence

(U//FOUO) If the evidence is to be recharged, the person to whom the evidence is currently charged out must initial next to that item on the Evidence Charge-Out Report and return the report to the ECT. If the evidence is no longer required to be charged out, the person to whom the evidence is currently charged out must immediately return the evidence to the ECR for storage.

#### 4.18.4. (U//FOUO) Charge-Out Report

(U//FOUO) Two copies of the Charge-Out Report should be printed by the ECT. One copy is forwarded to the appropriate squad supervisor for initialing by appropriate squad personnel. The second copy is maintained by the ECT to reconcile responses from each squad/RA. Charged-out evidence must appear on the Charge-Out Report at 60-day intervals until the evidence is returned to the ECR for storage.

(U//FOUO) The top and bottom copies of the Charge-Out Report must be maintained by the ECT from inspection to inspection.

#### 4.18.5. (U//FOUO) Return of Evidence

(U//FOUO) Upon return of the evidence, the ECT records chain-of-custody on the automated FD-192 and in the collected item database. Once all charged-out evidence has been accounted for, both copies of the Charge-Out Report are to be discarded.

#### 4.18.6. (U//FOUO) Agent Access for Review

(U//FOUO) When evidence is accessed by agent personnel for review/examination outside the ECR, or in the "reception area" of the ECR, chain-of-custody must be executed on the automated FD-192 maintained with the evidence and in the collected item database. If the review/examination takes place in the "reception area" of the ECR, the FD-455 need not be completed, as the visitor did not enter the actual ECR where the evidence is stored.

#### 4.19. (U//FOUO) Evidence Released to Custody of Outside Agencies

##### 4.19.1. (U//FOUO) Evidence Permanently Released to an Outside Agency

(U//FOUO) When evidence is permanently released to the custody of an outside agency, disposition and chain-of-custody documentation is to be recorded on the package copy of the automated FD-192 and in the collected item database. A receipt for the property (Form FD-597) must be signed by the person representing the receiving agency and then filed in the 1A section of the investigative case file. When money is involved, the receipt should clearly indicate that the receiving agency counted the money and that the amount corresponds to the amount listed on the original documentation.

##### 4.19.2. (U//FOUO) ECT Responsibility

(U//FOUO) The ECT is to:

- (U//FOUO) Place the package copy of the automated FD-192 and the chain-of-custody in the 1A section of the investigative case file. The chain-of-custody must show the disposition of evidence prior to being placed in the 1A. (See Chain-of-Custody User Guide.)



UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

- (U//FOUO) Modify the collected item database to reflect chain-of-custody and disposition. (See Chain-of-Custody User Guide.)
- (U//FOUO) Perform the "split" function in the collected item database if one or more items (as opposed to all items listed on the FD-192) are released. A new package copy of the automated FD-192 is generated and attached to the original chain-of-custody page for the remaining item(s), and is maintained with the remaining item(s) of property pending final disposition of all items. (See the Chain-of-Custody User's Guide for detailed instructions on the splitting of evidentiary items.)

#### 4.19.3. (U//FOUO) Evidence Temporarily Released

(U//FOUO) When property is temporarily released to an AUSA or non-task force officer, the agent charging out the evidence signs the chain-of-custody and retains the package copy of the FD-192 (with chain-of-custody attached) until the evidence is returned. The non-task force officer signs a receipt (FD-597) for the property. The receipt is attached to the FD-192 until the evidence is returned to storage, at which time the receipt is placed in the 1A section of the investigative case file. (AUSAs do not sign chains-of-custody, but may sign FD-597s as needed.)

#### 4.20. (U//FOUO) Physical Audit/Inventory - Evidentiary Property

##### 4.20.1. (U//FOUO) Conducting an Audit/Inventory

(U//FOUO) An audit (physical/telephonic/written verification of evidence charged out) coupled with an inventory (automated scanning of bar codes attached to evidence or primary evidence container housed in an evidence control center [ECC]), is to be conducted as follows:

- (U//FOUO) A 100 percent unannounced audit/inventory of general evidence (to include firearms, Federal Grand Jury and CART) and charged out evidence, at least once in a calendar year as determined by the SAC/AO.
- (U//FOUO) A 100 percent unannounced audit/inventory of drug and valuable evidence and charged out evidence at least once in a calendar year, as determined by the SAC/AO (not to coincide with the inventory of general evidence).
- (U//FOUO) A 100 percent audit/inventory of general (to include firearms, Federal Grand Jury and CART), drug and valuable evidence, and charged out evidence, prior to the departure of the AO.
- (U//FOUO) A 100 percent audit/inventory of general (to include firearms, Federal Grand Jury and CART), drug and valuable evidence, and charged out evidence, prior to the departure of an ECT/AECT in HQC (or in an RA that has a departing ECT/AECT).
- (U//FOUO) A 100 percent audit/inventory of all evidence before and after the relocation of a field office or RA ECR (within 30 days of the move).
- (U//FOUO) A 100 percent audit/inventory of all evidence at any time an SAC/AO deems an audit/inventory to be necessary.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**4.20.2. (U//FOUO) Designating an Agent(s) and/or Support Supervisor**

(U//FOUO) The SAC/AO is to designate a support supervisor who does not have a direct role in the Evidence Program and/or an FBI auditor to conduct the inventory/audit and write the accompanying EC. If a support supervisor or FBI auditor is not available, or if the SAC/AO chooses, an FBI agent may be used to conduct the inventory/audit. Additional personnel may be used to assist and conduct inventory/audit-related tasks with the designated support supervisor, FBI auditor, or agent.

**4.20.3. (U//FOUO) Designating an RA Agent and/or RA Support Supervisor**

(U//FOUO) The SAC/AO is to designate an RA support supervisor who does not have a direct role in the Evidence Program and/or an FBI auditor to conduct the inventory/audit of approved ECRs/ECCs in RAs and write the accompanying EC. If an RA support supervisor or FBI auditor is not available, or if the SAC/AO chooses, an FBI agent may be used to conduct the inventory/audit. Additional personnel may be used to assist and conduct inventory/audit-related tasks with the designated RA support supervisor, FBI auditor, or agent.

**4.20.4. (U//FOUO) ECT/AECT Does Not Conduct an Audit/Inventory**

(U//FOUO) The ECT/AECT is not to conduct an audit/inventory, nor write the accompanying EC. However, the ECT/AECT must be present in the designated ECR throughout the entire audit/inventory process to ensure the integrity of the evidence and to resolve any discrepancies that may develop.

**4.20.5. (U//FOUO) VWO Presence During an Audit/Inventory**

(U//FOUO) During an audit/inventory of the drug and valuable ECRs, the VWO must remain inside the designated ECRs throughout the entire audit/inventory process.

(U//FOUO) Note: VWOs have a role in the evidence program by their witnessing duties and, therefore, are exempt from conducting audit/inventories.

**4.20.6. (U//FOUO) FD-455 Sign In/Out**

(U//FOUO) The agent/support supervisor/auditor who is designated to conduct an audit/inventory must sign in/out on the FD-455 maintained for each ECR that they access in order to conduct the audit/inventory. The chain-of-custody is not to be signed by the employee(s) conducting the audit/inventory unless they take physical custody of the evidence.

**4.20.7. (U//FOUO) Sealed Drug and Valuable Evidence**

(U//FOUO) Sealed drug and valuable evidence pouches/boxes are not to be opened for an audit/inventory nor inspected. If a seal is found to be improperly applied, or has dried and has subsequently opened, the person conducting the audit/inventory is to immediately notify the case agent/sealing agent so that the evidence may be immediately resealed/repackaged and updated in the evidence database.

**4.20.8. (U//FOUO) Inventory**

(U//FOUO) An inventory is to include the automated scanning of all bar codes that are affixed to evidence (or the primary container) housed in the ECR that is being checked. Once scanned, the bar codes are uploaded, and an Exception Report is produced.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.20.9. (U//FOUO) Audit**

(U//FOUO) An audit is to be a physical, telephonic and/or written verification by the person conducting the audit/inventory to ensure that the evidence, said to be charged to a specific employee is, in fact, in the custody of that employee.

**4.20.10. (U//FOUO) EC to the SAC/AO**

(U//FOUO) An EC to the SAC/AO documenting that an audit/inventory of evidentiary property (name the type of evidence, general [including firearms, FGJ and CART], drugs, or valuables) was conducted must be prepared by the agent/support supervisor/auditor who conducted the audit/inventory. The approved/uploaded/serialized EC is then placed in the field office evidence control subfile designated for the audit/inventory of evidence. The EC should reveal the name(s) of the individual(s) who conducted the audit/inventory, the date(s) conducted, any deficiencies detected, and any steps taken to resolve those deficiencies. (The EC is to be maintained from field office inspection to inspection.) The final copy of the Exception Report is to be included as an enclosure to the EC. Separate ECs are to be done for each type of audit/inventory conducted.

(U//FOUO) The EC should contain a lead for the Laboratory Division, Attention: Evidence Program Manager, for information purposes. Copies of the Exception Report are NOT to be sent. If there are any unresolvable errors, the EC is to state this, as well as the steps being taken to resolve the problem. If the SAC recommends administrative action, this is to be so noted in the documentation to the FBI Evidence Program Manager.

**4.21. (U//FOUO) Annual Evidence Program Audit Checklist**

(U//FOUO) In conjunction with the Inspection Management Unit, Inspection Division, the Laboratory Division's Evidence Program (EVP), has issued a revised EVP audit documentation package, which includes interrogatories, guidelines, and checklists. A major component of the EVP audit is the Evidence Program Audit Checklist.

(U//FOUO) Assessments must be completed by August 31st. At the conclusion of the assessment, the signed original checklist is to be sent to the Field Evidence Program Manager no later than September 15<sup>th</sup>. It is suggested that the assessment be conducted by an evidence control technician and reviewed by the appropriate level of management.

(U//FOUO) The Evidence Program Audit Checklist can be located in electronic format on the Field Evidence Program Website, located on the home page of the Laboratory Division's Website,

[http://lab.fbinet.fbi/ecu/field\\_evidence\\_program.html](http://lab.fbinet.fbi/ecu/field_evidence_program.html).

**4.22. (U//FOUO) Non-evidentiary Property**

**4.22.1. (U//FOUO) 1As**

(U//FOUO) 1As are documents or items of property that are pertinent to an investigation. Generally the size, nomenclature, and/or value of the non-evidentiary items determine the place where they are to be filed; however, all physical evidence seized or contributed incidental to a search by search warrant, arrest, or crime-scene search that requires a chain-of-custody must be maintained in the ECR as 1B evidentiary property.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) If the evidence is not likely to come under attack regarding chain-of-custody, and is of such size that it can be filed in the investigative case file, it is to be placed in a 1A envelope (Form FD-340, FD-340b and/or FD-340c). The 1A must show the universal case file number and serial number of the item, the date received (by investigating employee), name and address of contributor, whether it may be returned, whether a receipt was given, and a description of the evidence. The serial number of the document in the investigative case file that originated and identifies the 1A may be recorded on the FD-340, FD-340b, and/or FD-340c at the discretion of the case agent. The FD-340, FD-340b and/or 340c is to be placed inside the 1A envelope, FD-340a, which is a letter-sized envelope known as the 1A serial in the investigative file. Because of the size of the FD-340c, it can be placed in front of the FD-340a inside an accordion-type folder. The FD-340a envelope is placed at the bottom of the file under serial number one. The FD-340a must be clearly marked as to contents and must bear the file number, serial number and date the FD-340, FD-340b and/or FD-340c was placed in the FD-340a. If the number of FD-340's, FD-340b's, and/or FD-340c's in the FD-340a envelope increases to the point where the file is unwieldy, a subfile must be opened and filed adjacent to the investigative case file.

(U//FOUO) In zero and control files, the FD-340a evidence envelope is to be filed adjacent to the EC, letter, or other communication to which it pertains.

(U//FOUO) When transmitting 1A evidence to another field office, leave the evidence in the white evidence envelope (FD-340, FD-340b, and/or FD-340c) and place a notation on the (FD-340a) 1A evidence envelope to show disposition and describe the method of transmittal. Transfer collected item to show the field office the 1A was sent to and the date it was transferred. Do not send FD-340s, FD-340b's, and/or FD-340c's to FBIHQ. If a portion of the evidence is being transmitted, prepare an FD-340, FD-340b, and/or FD-340c for the receiving office in the same fashion as above and place appropriate notations on the FD-340a. No outer enclosure envelope is required.

#### 4.22.2. (U//FOUO) Bulky Non-Evidentiary Material

(U//FOUO) If other non-evidentiary bulk property which may be pertinent to an investigation and must be retained is of such size that it cannot be filed in the 1A section (FD-340a) of the investigative case file, it is to be made a 1C, documented on Form FD-192a, and recorded in the investigative case file. The material is to be stored segregated from evidentiary property and access must be restricted to those persons with an official need.

(U//FOUO) The drafted FD-192a and the property are to be furnished to the ECT. (Form FD-340/  
FD-340b/FD-340c is to be furnished to the support services technician (SST).

(U//FOUO) The collected item database must computer-generate the 1A/1C number. The ECT must enter the exact storage location.

(U//FOUO) One copy of the automated FD-192a is to be filed in the 1C section of the investigative case file. (The FD-340/FD-340b/FD-340c is filed in the 1A section (FD-340a) of the investigative case file.)

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

(U//FOUO) A second copy of the automated FD-192a is to be affixed to and remain with the property until final disposition.

(U//FOUO) When non-evidentiary property is required to be charged out, Form FD-5 must be completed. Personnel having an official need may charge out non-evidentiary property for up to 60 calendar days, and if necessary, recharge every 60 days thereafter.

#### 4.22.3. (U//FOUO) Non-Evidentiary Property

(U//FOUO) Non-evidentiary property entered into the collected item database is handled the same way as evidentiary property. However, a chain-of-custody is not required, and an inventory is not conducted.

#### 4.22.4. (U//FOUO) Federal Grand Jury (FGJ) Material

(U//FOUO) Access to Federal Grand Jury Material must be limited to authorized persons appearing on the FGJ list. When not in use, FGJ materials must be placed in a secure location. The FGJ list may be the Rule 6(e) letter of the AUSA or (with the concurrence of the USA's office) an FBI internal certification list.

(U//FOUO) Absent chain-of-custody requirements, the material is to be placed in a subfile that is locked in a container (or room) with a combination lock. The combination should be known only by authorized persons appearing on the FGJ list. The material must be documented on Form FD-192a in a timely fashion. When the material is required to be charged out, Form FD-5 is used. Please note that when a secured room is used rather than separate secured containers, individuals with access to that room must be listed on the FGJ lists of all cases that are in that room.

(U//FOUO) When a chain-of-custody is required, the material is treated according to the rules and regulations pertaining to general evidentiary property (i.e., documented in the investigative case file within ten calendar days on Form FD-192). However, the material is stored segregated from all other types of general evidence in either a separate room with a combination lock (used exclusively for the storage of evidentiary FGJ material), or in a separate container or shelving within the ECR. When a separate room is used, a separate Form FD-455 (Access Log-Evidence Storage Facility) is to be maintained. The ECT, and in his/her absence, the AECT, accesses the material, as is the rule with all evidentiary property. When the need arises, appropriate charge-out procedures are used.

(U//FOUO) Evidentiary and non-evidentiary FGJ material must never be co-mingled during storage.

#### 4.23. (U//FOUO) Disposition of Property

##### 4.23.1. (U//FOUO) When an Investigative Case is Closed

(U//FOUO) When an investigative case is closed, it is the responsibility of the case agent to dispose of seized/recovered/contributed property when there is no further need for retention. Whenever there is any doubt regarding the need for retention, the AUSA should be consulted and the contact recorded in the investigative case file.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

#### 4.23.2. (U//FOUO) Permanent Retention

(U//FOUO) Certain case files must be marked for "Permanent Retention" and eventually be transferred to the National Archives and Records Administration (NARA). In such instances, only those evidentiary and non-evidentiary exhibits, regardless of size, that are documentary in nature, generated by and considered FBI records (e.g., agents' interview notes, photographs, work papers, ledgers, and journals), are to be preserved as part of the case file. Documentary materials (e.g., records of private enterprises, original or copies, contributed, seized or subpoenaed) should be returned to the rightful owner when the investigative or administrative purpose for which they were obtained has been satisfied. (See also Legal Handbook for Special Agents, 5-13.4.) Likewise, physical property (e.g., typewriters, radios, televisions, and firearms) is to be returned to its rightful owner.

#### 4.23.3. (U//FOUO) Disposition of Drug Evidence

(U//FOUO) Guidelines for the disposition of drug evidence are contained in the Manual of Investigative Operations and Guidelines (MIOG), Part I, Section 281-8.

#### 4.23.4. (U//FOUO) Disposition of Firearms

(U//FOUO) Guidelines for the disposition of firearms are contained Section 4.8 of this policy implementation guide.

#### 4.23.5. (U//FOUO) Disposition of Forfeited and Abandoned Property

(U//FOUO) Detailed procedures for disposition of forfeited and abandoned property are contained in the Forfeiture Manual.

#### 4.23.6. (U//FOUO) Disposition of Valuable Evidence

(U//FOUO) The following procedures must be followed for disposing/returning valuable evidence in a closed investigative case:

- (U//FOUO) The VWO must be present when the valuable evidence is removed from the valuable vault. The VWO or case agent must witness the relinquishment of the valuable evidence whether it is relinquished to the case agent; delivered or mailed to the owner/contributor, or someone accepting on his/her behalf; or turned over for forfeiture/abandonment. The relinquishment must be documented by an EC to the file, and both the ECT and VWO or case agent must sign the FD-597 as appropriate.
- (U//FOUO) The case agent and/or ECT (when advised in writing by an EC by the case agent) should make every effort to notify the owner/contributor of the property, telephonically or in writing, advising that the property may be reclaimed within 30 calendar days and will be released to him/her or his/her authorized agent. Record in the case file the fact that the contact was made.
- (U//FOUO) If property is personally returned to the owner/contributor, Form FD-597 is to be properly executed, with both the ECT and VWO or case agent signing the "Received From" section of the FD-597. The original of the FD-597 is to be placed in the 1A section of the investigative case file.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

- (U//FOUO) If the owner/contributor requests that the property be returned by mail, it is to be sent by U.S. Registered Mail, return receipt requested. When the return receipt (PS 3811) is returned to the field office, it is to be placed in the 1A section of the investigative case file. A transmittal letter is to accompany the property when the property is returned to the owner by mail. The letter should request that the owner sign the enclosed FD-597 and return it in the attached postage-paid, self-addressed envelope. The FD-597 should detail the exact property being returned, and must be signed by both the ECT and VWO or case agent in the "Received From" section. When the FD-597 is received by the field office (after being signed by the owner of the property), the original is to be placed in the 1A section of the investigative case file. The FD-192 (package copy) is to be placed in the 1A section of the investigative case file.

#### 4.23.7. (U//FOUO) Disposition of General Evidence

(U//FOUO) The following procedures should be followed for disposing/returning of general and valuable evidence in a closed investigative case:

- (U//FOUO) The case agent and/or ECT (when advised in writing by an EC by the case agent) should make every effort to notify the owner/contributor of the property, telephonically or in writing, advising that the property may be reclaimed within 30 calendar days and will be released to him/her or his/her authorized agent. Record in the case file the fact that the contact was made.
- (U//FOUO) If property is personally returned to the owner/contributor, Form FD-597 is to be properly executed. The original of the FD-597 is to be placed in the 1A section of the investigative case file.
- (U//FOUO) If the owner/contributor requests that the property be returned by mail, it is to be sent by U.S. Registered Mail, return receipt requested. When the return receipt (PS 3811) is returned to the field office, it is to be placed in the 1A section of the investigative case file. A transmittal letter is to accompany the property when the property is returned to the owner by mail. The letter should request that the owner sign the enclosed FD-597 and return it in the attached postage-paid, self-addressed envelope. The FD-597 should detail the exact property being returned. When the FD-597 is received by the field office (after being signed by the owner of the property), the original is to be placed in the 1A section of the investigative case file. The FD-192 (package copy) is to be placed in the 1A section of the investigative case file.

#### 4.23.8. (U//FOUO) Recordkeeping Procedures

(U//FOUO) The ECT is responsible for ensuring that the following recordkeeping procedures are followed when evidentiary and non-evidentiary property is disposed of:

- (U//FOUO) The package copy of Form FD-192 should have a completed chain-of-custody reflecting the disposition of the property. FD-192s are then placed in the 1A section of the investigative case file. The collected item database must be modified to reflect the date and method of disposition. Ensure that the disposition is reflected in the disposition field and on the automated chain-of-custody.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

- (U//FOUO) If one or more items, as opposed to all items listed on the FD-192 are disposed of, perform the "split" function in the collected item database. A new package copy of the automated FD-192 is generated and attached to the original chain-of-custody page for the remaining item(s), and is maintained with the remaining item(s) of property pending final disposition of all items.

#### 4.23.9. (U//FOUO) Closing Communication

(U//FOUO) A notation is to be placed on the closing communication indicating that property acquired during the investigation has been disposed of, disposal is being initiated through the forfeiture or abandonment process, or stating a valid reason for retention. Supervisors may not approve the closing of cases in which property has been seized/recovered/contributed without the appropriate notation.

#### 4.23.10. (U//FOUO) Retention in Closed Cases

(U//FOUO) Retention of evidence/nonevidence in closed cases can be monitored through the ACS to:

- (U//FOUO) Provide supervisory personnel the tools to enforce prompt property disposition through the case review process.
- (U//FOUO) Provide field office management statistical reports to identify individuals/squads which are not in compliance with property disposition procedures.
- (U//FOUO) Highlight noncompliance trends to the Inspection Staff for evaluation.
- (U//FOUO) Print and distribute a Closed Cases with Pending Collected Items Report to the appropriate case agent(s) at 60-day intervals. This is done by the ECT to ensure that those items eligible for disposition are handled. This report should encompass all items closed from 01/01/1970, to present. (The top and bottom copies of this report must be maintained by the ECT from inspection to inspection.)
- (U//FOUO) Indicate on the report if evidence is to be retained for an extended period of time. The case agent should do so by recording an anticipated disposition date and his/her initials on the report. (An EC to the investigative case file is then required explaining the reason for retaining the evidence. A copy of the EC is maintained in the ECR until final disposition of the evidence.) The report is then initialed by the supervisor and returned to the ECT. (The returned reports showing retention are to be maintained in a binder in the ECR from inspection to inspection.)

#### 4.24. (U//FOUO) Authorization for Evidence Handling Deviations - FD-990

(U//FOUO) The Federal Bureau of Investigation Authorizing Evidence Handling Deviations sets forth procedures for deviating from established evidence handling procedures.

(U//FOUO) The Federal Bureau of Investigation Authorizing Evidence Handling Deviations offers the means by which interim change is proposed and authorized. Deviation requests are proposed using an FD-990, Evidence Handling Deviation Request, and are limited in scope to citations in the Field Evidence Management and Operations Policy Directive.



UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.24.1. (U//FOUO) Purpose**

(U//FOUO) This document specifies the actions required for authorizing FBI personnel to deviate from established documented evidence handling requirements.

**4.24.2. (U//FOUO) Scope**

(U//FOUO) This procedure is applicable when a deviation from an established evidence handling requirement is necessary.

**4.24.3. (U//FOUO) Procedures**

(U//FOUO) There are times when deviating from documented policies and procedures is necessary. Deviating from documented requirements is prohibited prior to receiving authorization from the appropriate parties.

**4.24.4. (U//FOUO) Initiating a Deviation Request**

(U//FOUO) When there is a need to deviate from a documented and authorized policy or procedure, the requestor initiates an FD-990, Evidence Handling Deviation Request, specifying the following:

- (U//FOUO) The citation from the Field Evidence Management and Operations Policy Directive for which deviation is sought.
- (U//FOUO) Description of the requested deviation.
- (U//FOUO) Duration of the deviation.
- (U//FOUO) Reason for the deviation.

**4.24.5. (U//FOUO) Authorization**

(U//FOUO) Two authorizations are required.

- (U//FOUO) If deviating from FBI evidence handling requirements is of importance to the United States Attorney's Office, the person requesting the deviation must contact the appropriate party within that office for concurrence with the deviation. The request and response must be documented in the investigative file.
- (U//FOUO) The person requesting the deviation must submit the request to the appropriate ASAC for the first authorization.
- (U//FOUO) The person requesting the deviation must submit the signed request to the Field Evidence Program Manager, who must then review and submit to the Evidence Control Unit Chief, Laboratory Division, for the second and final approval.

**4.24.6. (U//FOUO) Duration**

(U//FOUO) Authorized deviations must be valid only for a specified time period or circumstance.

**4.24.7. (U//FOUO) Documentation**

(U//FOUO) The deviation form provides documentation of the approved deviation. It is to be permanently retained in the field office evidence program control file.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**4.25. (U//FOUO) Forms Used in the Evidence Program**

- (U//FOUO) DEA-7 - Report of Drug Property Collected, Purchased or Seized
- (U//FOUO) FD-5 - Serial Charge-Out
- (U//FOUO) FD-192 - Control of General/Drug/Valuable/CART/Firearms Evidence
- (U//FOUO) FD-192A - Inventory of Non-Evidentiary Property
- (U//FOUO) FD-302 - Form for Reporting Information That May Become Testimony
- (U//FOUO) FD-340 - 1A Envelope (6 x 10 inches)
- (U//FOUO) FD-340a - 1A Envelope (9 x 11 ½ inches)
- (U//FOUO) FD-340b - 1A Envelope (4 ¼ x 10 ¼ inches)
- (U//FOUO) FD-340c - 1A Envelope (8 ½ x 11 inches)
- (U//FOUO) FD-455 - Access Log-Evidence Storage Facility
- (U//FOUO) FD-597 - Receipt for Property Received, Returned, Released, Seized
- (U//FOUO) FD-632 - Evidence Transmittal Envelope
- (U//FOUO) FD-723 - Evidence Label
- (U//FOUO) FD-737 - Indemnity Agreement
- (U//FOUO) FD-990 - Deviation Request
- (U//FOUO) FD-1004 - Chain-of-Custody
- (U//FOUO) PS-3811 - Domestic Return Receipt

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

## **5. (U//FOUO) Recordkeeping Requirements**

### **(U//FOUO) Forms Used in the Evidence Program:**

- (U//FOUO) DEA-7 - Report of Drug Property Collected, Purchased or Seized
- (U//FOUO) FD-5 - Serial Charge-Out
- (U//FOUO) FD-192 - Control of General/Drug/Valuable/CART/Firearms Evidence
- (U//FOUO) FD-192A - Inventory of Non-Evidentiary Property
- (U//FOUO) FD-302 - Form for Reporting Information That May Become Testimony
- (U//FOUO) FD-340 - 1A Envelope (6 x 10 inches)
- (U//FOUO) FD-340A - 1A Envelope (9 x 11 ½ inches)
- (U//FOUO) FD-340B - 1A Envelope (4 ¼ x 10 ¼ inches)
- (U//FOUO) FD-340C - 1A Envelope (8 ½ x 11 inches)
- (U//FOUO) FD-455 - Access Log-Evidence Storage Facility
- (U//FOUO) FD-597 - Receipt for Property Received, Returned, Released, Seized
- (U//FOUO) FD-632 - Evidence Transmittal Envelope
- (U//FOUO) FD-723 - Evidence Label
- (U//FOUO) FD-737 - Indemnity Agreement
- (U//FOUO) FD-990 - Deviation Request
- (U//FOUO) FD-1004 - Chain-of-Custody
- (U//FOUO) PS-3811 - Domestic Return Receipt

### **5.1. (U//FOUO) Form FD-455 (Access Log - Evidence Storage Facility)**

(U//FOUO) Form FD-455 is to be maintained for each ECR or satellite ECR, whether located within field office space or at an off-site. A separate FD-455 is to be maintained for each valuable, drug, and ELSUR evidence repository regardless of size or location. The FD-455 establishes a reliable record of persons gaining entry. The visitor signs his/her own name (one name per line), reason for entry, the case file number and 1B/ID numbers, if appropriate, and the date and time of entry/exit. The evidence control technician and alternate evidence control technician, (when substituting for the ECT for one day or longer) are required to sign in and out on the FD-455 log maintained for the ECR only upon initial entry and final departure on a given day. Any other employee, including the AECT, when the ECT is on duty, must sign in/out on the FD-455 log for each entry/exit on a given day. Only one signature per line is permitted. The Form FD-455 must be maintained indefinitely.

### **5.2. (U//FOUO) Form FD-597 (Receipt for Property Received/Returned/Released/Seized)**

(U//FOUO) Form FD-597 is to be used to document the receipt/return of property acquired during investigations. The FD-597 consists of an original and two copies with carbon inserts.

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

The original is to be filed in the 1A section (FD-340a) of the investigative case file. One copy of the FD-597 is to be furnished to the contributor, and one copy, when appropriate, returned with the search warrant.

#### 5.3. (U//FOUO) Evidence Submitted to ECT

(U//FOUO) Evidence and/or documentation are to be submitted to the ECT within ten calendar days from the date the evidence was seized/recovered/contributed. Should extenuating circumstances prevent handling of the evidence within ten calendar days, the ECT advises the FBI employee that an EC is to be submitted to the squad supervisor and thereafter placed in the investigative case file. (A copy of the EC is to be directed to the ECT, placed in a binder in the ECR, and maintained from inspection to inspection.) Upon submitting evidence to the ECT, the FBI employee must ensure that the evidence is being submitted to an investigative case file. Evidence is not authorized for entry into control files or zero files, except in zero sub-assessment or substantive classification assessment files.

#### 5.4. (U//FOUO) Evidence Entered Into the Collected Item Database

(U//FOUO) Seized/recovered/contributed evidence is properly captured in the collected item database within ten calendar days from the date the evidence and/or documentation was presented to him/her by the seizing agent.

#### 5.5. (U//FOUO) FD-192

(U//FOUO) Upon assigning the bar code to the evidence, the ECT is required to print three new copies of the FD-192 which show the bar code. One copy of the automated FD-192 (file copy) is submitted to the supervisory special agent, primary relief supervisor, ASAC, or SAC for initialing, and is then filed in the first section of the investigative case file immediately above the 1A section (FD-340a). If there is no 1A section, the file copy becomes the first item in the first section of the investigative case file. The file copy may be maintained in a subfile, in which case a blank automated FD-192 should be placed in the main file as a substitute for the original, indicating its location (e.g., "1B numbers maintained in Subfile E").

(U//FOUO) For general evidence, the second copy (package copy) of the automated FD-192 and the written chain-of-custody is affixed to, and remains with, the evidence until final disposition. For valuable and drug evidence, the package copy and the written chain-of-custody is filed in numerical sequence, by file number, in a binder which is maintained in the ECR.

(U//FOUO) A copy of the FD-192 or a report of all evidence entered must be furnished to the Forfeiture Unit. If not, ensure that the Forfeiture Unit generates a copy of this report for review.

#### 5.6. (U//FOUO) FD-1004

(U//FOUO) The written chain-of-custody documents the signatures of persons, including the ECT, who receive custody of the evidence while it is the property of the FBI. The first chain-of-custody is established as a result of entering the group data on the first page of the automated FD-192 and indicates the identity of the person who collected the evidence. Subsequent chain-of-custody signatures must be made by the ECT or other individuals who receive the property. Chain-of-custody entries should not disclose that the evidence is received by the ECR; instead the entry should show the signature of the person to whom the custody of the evidence has been

UNCLASSIFIED//FOUO

### Field Evidence Policy Implementation Guide

given. The only exception to this policy is when evidence is forwarded to the DEA or FBI Laboratories.

(U//FOUO) In task force investigations, it is permissible for a federal criminal investigative agent from a participating federal agency or a deputized officer from a participating police department, to record chain-of-custody on Form FD-192 when that investigator/officer is involved in the acquisition of the property documented on the FD-192. This individual may also participate as the sealing/witnessing agent in the verification and sealing of drug/valuable evidence. Support employees may be witnessing officials for valuable evidence only.

(U//FOUO) Chain-of-custody on Federal Grand Jury Material (Rule 6e Material) is not required unless specified by the case agent. The case agent must consult with the AUSA to determine whether a chain-of-custody should be maintained on specific grand jury material and document the consultation (date/name of AUSA and determination). If so required, an FD-192 must be completed and the material stored in the ECR. When a chain-of-custody is not required, grand jury material is documented on Form FD-192a (Control Form for Non-Evidentiary Items), entered into the collected item database as a 1C, and segregated from the other non-evidentiary property, with access given only to those individuals named on the grand jury list. When grand jury material is entered into the collected item database as a 1C, it is charged out by using Form FD-5.

#### 5.7. (U//FOUO) Non-evidentiary Property

(U//FOUO) Non-evidentiary property, if size permits, may be filed in the 1A section of the case file. Otherwise, large non-evidentiary property (serialized as a 1C), seized, subpoenaed, or contributed pursuant to investigative activity, is to be stored in a separate area within, or at the discretion of the SAC, outside the field office in space specifically designated for the storage of non-evidentiary items.

#### 5.8. (U//FOUO) Original Interview Notes

(U//FOUO) Special agents' original interview notes are not intended to be used as evidence at a trial, and questions raised by the defense with respect to them generally attempt to focus on inconsistencies between the original notes and the resulting FD-302s. Just as it is not necessary to maintain chain-of-custody on the FD-302, it is not necessary to maintain chain-of-custody on original interview notes. These should be filed in the 1A section (FD-340a) of the case file.

#### 5.9. (U//FOUO) Evidence Permanently Released to Outside Agency

(U//FOUO) When evidence is permanently released to the custody of an outside agency, disposition and chain-of-custody documentation is to be recorded on the package copy of the automated FD-192 and in the collected item database. A receipt for the property (Form FD-597) must be signed by the person representing the receiving agency and then filed in the 1A section of the investigative case file. When money is involved, the receipt should clearly indicate that the receiving agency counted the money and that the amount corresponds to the amount listed on the original documentation.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**5.10. (U//FOUO) Audit/Inventory EC**

(U//FOUO) An EC to the SAC/AO, documenting that an audit/inventory of evidentiary property (identify the type of evidence as general [to include firearms, FGI, and CART], drugs, or valuables) was conducted is to be prepared by the agent/support supervisor/auditor who conducted the audit/inventory. The approved/uploaded/serialized EC is then placed in the field office evidence control subfile designated for the audit/inventory of evidence. The EC should reveal the name(s) of individual(s) who conducted the audit/inventory, the date(s) conducted, any deficiencies detected, and any steps taken to resolve those deficiencies. (The EC is to be maintained from field office inspection to inspection.) The final copy of the Exception Report is to be included as an enclosure to the EC. Separate ECs are to be prepared for each type of audit/inventory conducted.

(U//FOUO) The EC should contain a lead for the Laboratory Division, Attention: Evidence Program Manager, for information purposes. (Copies of the Exception Report are not to be sent.) If there are any unresolvable errors, the EC is to state these errors, as well as the steps being taken to resolve the problem(s). If the SAC recommends administrative action, this is to be noted in the documentation to the FBI Evidence Program Manager.

**5.11. (U//FOUO) Annual Evidence Program Audit**

(U//FOUO) The Evidence Program has issued a revised EVP audit documentation package, which includes interrogatories, guidelines, and checklists. A major component of the EVP audit is the Evidence Program Audit Checklist. Assessments must be completed by August 31st. At the conclusion of the assessment, the signed original checklist is to be sent to the Evidence Program Coordinators no later than September 15<sup>th</sup>. It is suggested that the assessment be conducted by an evidence control technician and reviewed by the appropriate level of management.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**6. (U//FOUO) Summary of Legal Authorities**

---

**6.1. (U//FOUO) Subpart H of Title 49, Code of Federal Regulations, Part 172**

(U//FOUO) Subpart H of Title 49, Code of Federal Regulations, Part 172, requires that training be provided to those individuals who, in the course of their employment, directly affect hazardous materials transportation safety. The ECT is to avail himself/herself of such training. ECTs are to receive specialized HAZMAT training for air transport shipments every two years by a certified Department of Transportation or IATA-approved school. Strict fines are imposed on individual employees by the Federal Aviation Administration for noncompliance.

**6.2. (U//FOUO) Title 18 U.S.C. Section 3665**

(U//FOUO) Firearms possessed by convicted felons:

(U//FOUO) "A judgment of conviction for transporting a stolen motor vehicle in interstate or foreign commerce or for committing or attempting to commit a felony in violation of any law of the United States involving the use of threats, force, or violence or perpetrated in whole or in part by the use of firearms, may, in addition to the penalty provided by law for such offense, order the confiscation and disposal of firearms and ammunition found in the possession or under the immediate control of the defendant at the time of his arrest. The court may direct the delivery of such firearms or ammunition to the law-enforcement agency which apprehended such person, for its use or for any other disposition in its discretion."

**6.3. (U//FOUO) Title 18 U.S.C. Section 3600A and Department of Justice (DOJ)**

(U//FOUO) Justice For All Act (JFAA) Regulations regarding the preservation of biological evidence. The Act mandated the preservation of biological evidence secured in an investigation or prosecution of a federal offense, where a defendant was placed under a sentence of imprisonment for such offense.

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

7. (U//FOUO) Security Requirements

(U//FOUO) The drug and valuable evidence rooms require that an ECT or AECT be accompanied by a VWO to gain authorized access. In order to ensure that the appropriate two parties are gaining authorized access [redacted]

b7E

(U//FOUO) [redacted] it is acceptable, and encouraged, for [redacted]

b7E

(U//FOUO) [redacted]

b7E

(U//FOUO) In the event an ECT, AECT, or VWO no longer has authorized access to a drug and/or valuable room [redacted]

b7E

[redacted] The written request and documented confirmation of removal must be retained from inspection period to inspection period.)

(U//FOUO) At the end of each month, the evidence program supervisor must ensure that the electronic access logs for each ECR, drug, and valuable rooms are printed and retained. (The printed logs must be retained from inspection period to inspection period.)

(U//FOUO) [redacted] is required and must be retained in the evidence program control file.

b7E

(U//FOUO) For field offices having off-site ECRs, the field office must create a documented response plan detailing how an activated alarm must be handled. The response plan must be permanently retained and readily accessible for review.

(U//FOUO) In the event evidentiary property is of such volume that it is not practical to store it in the ECR or a similar facility within field office space, it may be stored in a secure off-site facility at the discretion of the SAC. The off-site facility should be established and afforded the same security measures as an ECR. Every effort should be made to store evidence in the ECR; however, if a similar facility within field office space or an off-site facility is used, these facilities are considered satellites of the ECR and are subject to the same administrative controls afforded the ECR.

(U//FOUO) The ECT/AECT is not authorized to access the drug/valuable vault unless accompanied by the AO or the person(s) designated to act on behalf of the AO as the VWO. The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO cannot be an AECT. Each office should limit the number of designated VWOs, and must document the list of

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

authorized vault witnessing personnel in the evidence control file. The VWO must also sign the FD-455 for each entry/exit.

(U//FOUO) The only persons having emergency access [redacted] to the drug/valuable vault and the ECR are the SAC, the ASACs, and the SSRA. The [redacted]

[redacted]

b7E

[redacted] SACs/ASACs/SSRAs who make an emergency entry/exit into the ECR must sign the FD-455, and document their access with an EC to the evidence control file. Access to the ECR [redacted]

(U//FOUO) A refrigerator/freezer is to be placed in the ECR for the storage of body fluids and any perishable-type evidence. Food items, for personal consumption, are not to be stored in this refrigerator.

(U//FOUO) A "Biohazard Warning" label is to be placed on the entrance to the ECR (preferably the door) and on the refrigerator in the ECR.

(U//FOUO) ECRs within a stand-alone FBI-controlled building or within contiguous FBI space, occupied 24 hours a day, 7 days a week, with a perimeter secured to specifications established by the Security Division, must be constructed in accordance with the requirements set forth below.

(U//FOUO) [redacted]

b7E

7.1. (U//FOUO) General Evidence ECR

(U//FOUO) The entire perimeter of the ECR must be constructed of [redacted] of the ECR.

b7E

(U//FOUO) There is to be only one externally accessible door to the ECR. Entrance to the ECR should be [redacted]

[redacted] If additional access doors are constructed [redacted]

b7E

(U//FOUO) The externally accessible door must be [redacted]

[redacted]

b7E

(U//FOUO) [redacted] designated for housing weapons and ammunition must be [redacted] Access must be controlled by [redacted]

b7E

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

(U//FOUO) [Redacted]

b7E

(U//FOUO) The ECR should be equipped with a fire extinguisher. Appropriate personal protective supplies and first aid safety equipment should be stored in the ECR for easy accessibility. This includes, but is not limited to: disposable gloves and gowns, disposable plastic aprons, eye and mouth protection, pails with disinfectant, biohazard bags for the disposing of biohazardous material (bag to be placed in a hard cardboard box), containers to hold needles, sink with hot and cold running water (with elbow or foot connection), flammable cabinets, acid cabinets, poison cabinets, and biohazard labels and containers.

7.2. (U//FOUO) Drug Evidence Room

(U//FOUO) The drug evidence room must be a separate room constructed and controlled as indicated below:

- (U//FOUO) The entire perimeter of the drug evidence room must be [Redacted]
- (U//FOUO) There may be only one externally accessible door to the drug evidence room.
- (U//FOUO) The externally accessible door to the drug room must be [Redacted] as indicated below:
- (U//FOUO) [Redacted]
- (U//FOUO) [Redacted]
- (U//FOUO) [Redacted]
- (U//FOUO) An exterior 24-hour ventilation system is required. The drug evidence room should be afforded outside ventilation for the storage of odoriferous substances. The floor should be made of a nonporous material so that it can be disinfected.

b7E

7.3. (U//FOUO) Valuable Evidence Room

(U//FOUO) The valuable evidence room must be a separate room constructed and controlled as indicated below:

- (U//FOUO) The entire perimeter of the valuable evidence room must be [Redacted] of the valuable evidence room.
- (U//FOUO) The door to the valuable evidence room must be [Redacted]
- (U//FOUO) [Redacted]

b7E

UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

- (U//FOUO) [redacted]  
[redacted]
- (U//FOUO) [redacted]  
[redacted]

b7E

7.4. (U//FOUO) Federal Grand Jury Room

(U//FOUO) The Federal Grand Jury Room, designated for housing Federal Grand Jury Material must be constructed and controlled as indicated below:

- (U//FOUO) The entire perimeter of the Federal Grand Jury Room must be [redacted]  
[redacted] of the Federal Grand Jury Room.
- (U//FOUO) There may be only one externally accessible door to the Federal Grand Jury Room. Entrance to the room should be [redacted]  
[redacted]
- (U//FOUO) The externally accessible door must be [redacted]  
[redacted] as indicated below:
- (U//FOUO) [redacted]  
[redacted]
- (U//FOUO) [redacted]  
[redacted]
- (U//FOUO) [redacted] the Federal Grand Jury Room.  
[redacted]

b7E

7.5. (U//FOUO) CART Room

(U//FOUO) The CART Room, designated for housing computer evidence, to include various types of magnetic media (excluding ELSUR evidence), must be constructed and controlled as indicated below:

- (U//FOUO) The entire perimeter of the CART Room must be [redacted]  
[redacted] of the  
CART Room.
- (U//FOUO) There may be only one externally accessible door to the CART Room. Entrance to the room should be [redacted]  
[redacted]
- (U//FOUO) The externally accessible door must be equipped with two security access control devices for single-person entry as indicated below:
  - (U//FOUO) [redacted]  
[redacted]

b7E

b7E

b7E

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

- o (U//FOUO) [redacted]
- o (U//FOUO) [redacted] the CART Room. This [redacted]

b7E

7.6. (U//FOUO) Off-Site ECRs

(U//FOUO) The off-site evidence control room must be a separate room constructed and controlled as indicated below:

(U//FOUO) The entire perimeter of an off-site ECR must be [redacted] of the ECR.

(U//FOUO) There may be only one externally accessible door to the ECR. If additional access doors are constructed, [redacted]

b7E

(U//FOUO) The externally accessible door must be [redacted] as indicated below:

- (U//FOUO) [redacted]
- (U//FOUO) [redacted]

(U//FOUO) [redacted] is required in the off-site ECR.

7.7. (U//FOUO) After-Hours/Temporary Storage of Drugs and/or Valuables

(U//FOUO) In the event drug and/or valuable evidence needs to be secured after hours, it may be secured in a [redacted] until the next business day.

b7E

(U//FOUO) [redacted]

(U//FOUO) The drug and/or valuable room(s) may be outfitted with a "drop slot" for after-hours storage of drug and/or valuable evidence. The "drop slot" is to be installed into an external ECR wall, which is accessible from an external hallway outside of the ECR and allows for the evidence to be dropped into the drug or valuable room. The "drop slot" is to be constructed in such a manner as to prevent a person from reaching inside to retrieve the drug and/or valuable evidence.

(U//FOUO) An FD-455 must be completed when evidence is placed in, and removed from, the temporary storage.

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**8. (U//FOUO) Justice For All Act of 2004**

---

- 8.1. (U//FOUO) For information and guidance regarding the Justice for All Act of 2004, refer to 319X-HQ-A1487720 serial 445 and Office of the General Counsel Website.  
[\[http://ogc.fbinet.fbi\]](http://ogc.fbinet.fbi)

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**(U//FOUO) Appendix A: Legal Authorities**

---

(U//FOUO) Subpart H of Title 49, Code of Federal Regulations, Part 172

(U//FOUO) Title 18, U.S.C., Section 3665

(U//FOUO) 18 U.S.C. Section, 3600A and DOJ

A-1

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

**(U//FOUO) Appendix B: Sources of Additional Information**

(U//FOUO) Please view the Laboratory Division, Forensic Analysis Branch, Evidence Control Unit, Field Evidence Program web site for additional information:  
[\[http://lab.fbinet.fbi/ecu/field\\_evidence\\_program.htm\]](http://lab.fbinet.fbi/ecu/field_evidence_program.htm)

**(U//FOUO) Additional Sources of Information:**

(U//FOUO) Evidence Chain-of-Custody (FD-1004) User Guide

(U//FOUO) Handbook of Forensic Sciences

(U//FOUO) Dangerous Goods Regulations

(U//FOUO) Digital Evidence Laboratory (DEL) Quality Assurance Manual

(U//FOUO) Office of the General Counsel Website

(U//FOUO) CID Drug Unit Website

B-1

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO  
**Field Evidence Policy Implementation Guide**

**(U//FOUO) Appendix C: Contact Information**

<b>Laboratory Division</b>	
<b>Assistant Director</b> D. Christian Hassell	
<b>Forensic Analysis Branch</b>	
<b>Deputy Assistant Director</b> Melissa Anne Smrz	
<b>Evidence Control Unit</b>	
<b>Unit Chief</b>	
<b>Field Evidence Program</b>	
<b>Program Manager</b>	Office
	Cell
<b>Management and Program Analyst</b>	
	Office
<b>Management and Program Analyst</b>	
	Office
<b>Address</b>	FBI Laboratory 2501 Investigation Parkway Quantico, Virginia 22135

b6  
b7c

C-1  
 UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO  
Field Evidence Policy Implementation Guide

**(U//FOUO) Appendix D: Key Words**

(U//FOUO) 1A - A Document or Item of Property That is Pertinent to an Investigation

(U//FOUO) 1B - Evidentiary Property

(U//FOUO) 1C - Large Non-Evidentiary Property

(U//FOUO) 1D - Serialized ELSUR Evidence

(U//FOUO) DEA Form 7 - Report of Drug Property Collected, Purchased, or Seized

(U//FOUO) FD-5 - Serial Charge-Out

(U//FOUO) FD-192 - Control Form for General/Valuable/Drug Evidence

(U//FOUO) FD-192a - Control Form for Nonevidentiary Items

(U//FOUO) FD-302 - Form for Reporting Information That May Become Testimony

(U//FOUO) FD-340 - 1A Envelope (6 x 10 inches)

(U//FOUO) FD-340a - 1A Section of the Investigative Case File

(U//FOUO) FD-340b - 1A Envelope (4 ¼ x 10 ¼ inches)

(U//FOUO) FD-340c - 1A Envelope (8 ½ x 11 inches)

(U//FOUO) FD-455 - Access Log - Evidence Storage Facility

(U//FOUO) FD-597 - Receipt for Property Received/Returned/Released/Seized

(U//FOUO) FD-632 - Evidence Transmittal Envelope

(U//FOUO) FD-723 - Evidence Label

(U//FOUO) FD-737 - Indemnity Agreement

(U//FOUO) FD-990 - Deviation Request

(U//FOUO) FD-1004 - Chain-of-Custody

(U//FOUO) [REDACTED]

b7E

(U//FOUO) PS-3811 - U.S. Postal Service Domestic Return Receipt

(U//FOUO) Rule 6e Material - Grand Jury Material

D-1

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Field Evidence Policy Implementation Guide

**(U//FOUO) Appendix E: Acronyms**

---

ACDC	Assistant Chief Division Counsel
ACS	Advanced Automated Case Support
ADIC	Assistant Director in Charge
AECT	Alternate Evidence Control Technician
AO	Administrative Officer
ASAC	Assistant Special Agent in Charge
AUSA	Assistant United States Attorney
CART	Computer Analysis Response Team
CFR	Code of Federal Regulations
CI	Collected Item Database
COMSEC	Communication Security
CPU	Central Processing Unit
DE	Derivative Evidence
DEA	Drug Enforcement Administration
DEL	Digital Evidence Laboratory
DNA	Deoxyribonucleic Acid
DOJ	Department of Justice
DVD	Digital Versatile Disc
EC	Electronic Communication
ECC	Evidence Control Center
ECR	Evidence Control Room
ECT	Evidence Control Technician
ELSUR	Electronic Surveillance
EPIC	El Paso Intelligence Center
EVP	Evidence Program
FBI	Federal Bureau of Investigation

E-1

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

FBIHQ	Federal Bureau of Investigation Headquarters
FDIN	Federal Drug Identification Number
FDSS	Federal-Wide Drug Seizure System
FEDA	Forensic Electronic Device Analysis
FEP	Field Evidence Program
FGJ	Federal Grand Jury
FGJR	Federal Grand Jury Room
GHRCFL	Greater Houston R
GSA	General Services Administration
HAZMAT	Hazardous Material
HQC	Headquarters City
IATA	International Air Transport Association
INS	Immigration and Naturalization Service
JFAA	Justice For All Act
LO	Lead Office
MAOP	Manual of Administrative Operations and Procedures
MIOG	Manual of Investigative Operations and Guidelines
NARA	National Archives and Records Administration
OO	Office of Origin
OTD	Operational Technology Division
PCP	Phencyclidine
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PM	Program Manager
PS	Postal Service
RA	Resident Agency
RCFL	Regional Computer Forensic Laboratory
RFC	Reference Firearms Collection

E-2

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

**Field Evidence Policy Implementation Guide**

SA	Special Agent
SAC	Special Agent in Charge
SRA	Senior Resident Agent
SSRA	Supervisory Special Resident Agent
SST	Support Services Technician
STRIDE	System to Retrieve Information from Drug Evidence
SWAT	Special Weapons and Tactics
U.S.	United States
USA	United States Attorney
USCG	U.S. Coast Guard
USCS	U.S. Customs Service
VMD	Volatile Memory Devices
VWO	Vault Witness Official
WMD	Weapon of Mass Destruction

E-3

UNCLASSIFIED//FOUO

# **EXHIBIT B**

**(Trial Exhibit 961)**

DRAFT

Blumberg No. 914  
 DEFENDANT'S  
 EXHIBIT  
 961



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

<b>Examiner:</b>	SA/FET Virginia Donnelly (VD) ITS/SFE Brian Booth (BB)	<b>UCFN:</b>	50A-NY-2233091
<b>Case Agent:</b>	SA Michael Lever, (Squad: C-2)	<b>Submission ID:</b>	196817
<b>Phone:</b>	(212) 384-3245	<b>Title/Sub:</b>	NXIVM; KEITH RANIERE (Subjects); ...
<b>Date Assigned:</b>	05/21/2018	<b>Legal Authority:</b>	Search and Seizure Warrant

Item #	Date	Init	Notes
	08/08/18	VD	<b>Legal Authority Reviewed:</b> Search and Seizure Warrant and Request Form reviewed.
			<b>BEGIN EXAM</b>
NYC023721 _1B16	08/08/18	VD	<b>Receipt of Evidence:</b> Evidence received directly from Case Agent.
NYC023722 _1B19			<b>E6261242 - 1B16</b> Western Digital external hard drive, dark gray, 500GB, model: WD5000P032, serial number (s/n): WCAS81365334, affixed barcode and designated as <b>NYC023721_1B16</b> . Evidence received in brown paper bag sealed with evidence tape.
NYC023723 _1B23			<b>E6261245 - 1B19</b> Amazon Kindle, white, model: D00611,s/n: B00418219322086, affixed barcode and designated as <b>NYC023722_1B19</b> . Evidence received in brown paper bag sealed with evidence tape. Item contained in black cover.
NYC023724 _1B26			<b>E6261247 - 1B23</b> Toshiba USB drive, silver, 4GB, model: U3 Smart, unique identifier: 6491J90506BM8K1, affixed barcode and designated as <b>NYC023723_1B23</b> . Evidence received in brown paper bag sealed with evidence tape. Key attached to USB drive.
NYC023725 _1B27			<b>E6261250 - 1B26</b> Western Digital external hard drive, white, 1TB, model: WD10000H1NC-00, s/n: WCAU47036371, affixed barcode and designated as <b>NYC023724_1B26</b> . Evidence received in brown paper bag sealed with evidence tape.
NYC023725 _1B27-1			<b>E6261251 - 1B27</b> Lenovo ThinkCentre M77 tower, black, model: ASU, s/n: MJREEDN, affixed barcode and designated as <b>NYC023725_1B27</b> . Containing: One (1) Western Digital hard drive, 500GB, model: WD5000AAKX, s/n: WMAYUX846984, designated as <b>NYC023725_1B27-1</b> . Containing: One (1) Seagate hard drive, 2TB, model: ST2000DM001, s/n: S1E0GFDN, designated as <b>NYC023725_1B27-2</b> . Tower was sealed with evidence tape.
NYC023725 _1B27-2			
NYC023726 _1B28			
NYC023727 _1B31			
NYC023728 _1B32			
NYC023729 _1B33			
NYC023730 _1B41			
NYC023731 _1B43			
NYC023732 _1B50			

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
---	------------------

DRAFT



FEDERAL BUREAU OF INVESTIGATION  
COMPUTER ANALYSIS RESPONSE TEAM  
NEW YORK DIVISION

EXAMINATION NOTES

		<p>Power cord was taped to tower.</p> <p><b>E6261252 - 1B28</b> Lacie external hard drive, silver, 500GB, model: 300964U, s/n: 164400534, affixed barcode and designated as <b>NYC023726_1B28</b>. Evidence received in a red accordion folder sealed with evidence tape.</p> <p><b>E6261239 - 1B31</b> ULTRA USB 2.0 Storage High Speed drive enclosure, black, no unique identifiers, affixed barcode and designated as <b>NYC023727_1B31</b>. Containing: Seagate hard drive, 120GB, model: ST9120821AS, s/n: 5PLOWPQC. Evidence received in a clear plastic bag sealed with evidence tape. Mini USB 2.0 cord provided. Item missing two (2) screws on each side, thus a total of four (4) screws.</p> <p><b>E6261238 - 1B32</b> Western Digital external hard drive, black, 1TB, product number (p/n): WDBAAH0010HCH-00, s/n: WCAV54873732, affixed barcode and designated as <b>NYC023728_1B32</b>. Evidence received in brown paper bag sealed with evidence tape. Digital screen reads "PICTURES 09."</p> <p><b>E6261237 - 1B33</b> Echo, black, 8GB, no unique identifiers, affixed barcode and designated as <b>NYC023729_1B33</b>. Evidence received in brown paper bag sealed with evidence tape. Item was in a black case with a micro USB 2.0 cord along with other accessories.</p> <p><b>E6280005 - 1B41</b> Lacie external hard drive, silver, 1TB, unique ID: 300798U, s/n: 154107441, affixed barcode and designated as <b>NYC023730_1B41</b>. Evidence received in a red accordion folder sealed with evidence tape. Item has a brown substance on the bottom.</p> <p><b>E6280007 - 1B43</b> Lexar Compact Flash Card, 256MB, p/n: 2250, Unique ID: 3884256AC2806A20A, affixed barcode and designated as <b>NYC023731_1B43</b>. Evidence received in a clear plastic bag sealed with evidence tape.</p> <p><b>E6280003 - 1B50</b> Apple iPod, black/silver, back has decorative skin, 100 GB, no visible unique identifiers, model: MA450LL, s/n: 8K7278QGV9R, affixed barcode and designated as <b>NYC023732_1B50</b>. Evidence received in brown paper bag sealed with evidence tape. Item was in a black case with accessories. Back of item has sticker</p>
--	--	--

<p>THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.</p>	<p>Affix Label Here</p>
--	-------------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			Forensic Exam Station F2552510 (s/n: H09381A020H) is a MAC Pro/2.26 Model A1289 running Windows 10 Enterprise 64-bit Operating System with 32GB RAM and 2 Intel Xeon E5520 processors.
	09/13/18	VD	<b>Performance Verification:</b> Forensic Exam Station F2630035 posted correctly. Forensic Exam Station F2673128 posted correctly.
Staging Drive 1	09/12/18	VD	<b>Staging Drive:</b> One forensically wiped Western Digital hard drive, 2TB, model: WD20EARX, s/n: WCAZAE561750, was formatted with New Technology File System (NTFS). This drive will be utilized for staging images.
Staging Drive 2	09/12/18	VD	<b>Staging Drive:</b> One forensically wiped Western Digital hard drive, 2TB, model: WD20EARX, s/n: WCAZAJ020571, was formatted with New Technology File System (NTFS). This drive will be utilized for staging images.
NYC023725 _1B27-1  Staging Drive 1  NYC023725 _1B27-1.E01	09/12/18	VD	<p><b>Preserve Evidence: Image</b>                  NYC023725_1B27-1 was imaged using a Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D3B0A6, to Staging Drive 1.</p> <p>-----Source Disk-----</p> <p>Interface: SATA                  Model: WDC WD5000AAKX-083CA1                  Firmware revision: 19.01H19                  Serial number: WD-WMAYUX846984                  Capacity in bytes: 500,107,862,016 (500.1 GB)                  Block Size: 512 bytes                  Block Count: 976,773,168                      Power-ON Block Count: 976,773,168                      HPA Block Count: 976,773,168                      DCO Block Count: 976,773,168</p> <p>-----Destination Disk-----</p> <p>Interface: SATA                  Model: WDC WD20EARX-00PASB0                  Firmware revision: 51.0AB51                  Serial number: WD-WCAZAE561750                  Capacity in bytes: 2,000,398,934,016 (2.0 TB)                  Block Size: 512 bytes                  Block Count: 3,907,029,168                      Power-ON Block Count: 3,907,029,168                      HPA Block Count: 3,907,029,168                      DCO Block Count: 3,907,029,168</p> <p>-----Disk Imaging Results-----                  Output file format: E01 - EnCase format</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here





FEDERAL BUREAU OF INVESTIGATION  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			<p>covering entire back.</p> <p>These additional items were included but will not be examined by CART at this time:</p> <p><b>E6261253 - 1B29</b> Apple AirPort Extreme Base Station, white, model: A1354, s/n: 6F1169XWACC.                      Evidence received in brown paper bag sealed with evidence tape. Power cord provided.</p> <p><b>E6261236 - 1B34</b> Ubee Cable Modem/Router, white/blue, model: DDW3611, s/n: B831U27000562.                      Evidence received in brown paper bag sealed with evidence tape. Power cord provided.</p> <p><b>E6261235 - 1B35</b> Netgear N600 Wireless Dual Band Router, black/silver, model: WNDR3400, s/n: 2BK3117S22DD3.                      Evidence received in brown paper bag sealed with evidence tape.</p>
	08/08/18	VD	<p><b>Administrative note:</b>                      Met Case Agent SA Michael Lever and SA Delise Jeffrey to discuss case while they dropped off the evidence. Agents asked CART to image items first and process later in order to provide copies of the images to AUSA. Agents then requested CART complete a standard exam process for the evidence provided. No specific additional analysis was requested.</p>
	09/10/18	VD	<p><b>Administrative Note:</b>                      Met with CA to discuss evidence items. CA was informed that routers would contain IP addresses and that Computer Scientists usually handle this type of item. CA stated to not image or process the routers.</p>
	09/13/18	VD	<p><b>Case Volume Creation:</b>                      A new case volume was created on NYCART-FS (\\NYCART-FS\cases02\NY-2233091_196817) using the Case Administration Tool v1.15.0.11. and mounted to Forensic exam station, hereinafter referred to as <b>CASE VOLUME</b>.</p>
	09/13/18	VD	<p><b>Equipment:</b>                      Forensic Exam Station F2630035 (s/n: H01290MGEUH) is a MAC Pro/2.4 Model A1289 running Windows 10 Enterprise 64-bit Operating System with 28GB RAM and 2 Intel Xeon E5620 processors.</p> <p>Forensic Exam Station F2673128 (s/n: CMVJ11M7F4MH) is a MAC Pro/2.4 Model A1289 running Windows 10 Enterprise 64-bit Operating System with 24GB RAM and 2 Intel Xeon E5645 processors.</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			Chunk size in bytes: 2,147,483,648 (2.1 GB) Chunks written: 54 Filename of first chunk: 2018-09-12_11-04-14/NYC023725_1B27-1.E01 Total errors: 0 Acquisition MD5: 5c4aead15ef34a54ddcd558dc2f7f947 -----Readback Verification Results----- Verification MD5: 5c4aead15ef34a54ddcd558dc2f7f947 Status: Verified
Staging Drive 1  NYC023725_1B27-1.E01	09/18/18	VD	Using Forensic Exam Station F2630035 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023725_1B27-1 from Staging Drive 1 to CASE VOLUME.
NYC023725_1B27-1.E01	09/19/18	VD	Copy was verified using <b>FTK® Imager 4.2.0.13</b> . Examiner created NYC023725_1B27-1.E01.txt to CASE VOLUME to retain logs.  Image Verification Results: Verification started: Wed Sep 19 08:15:52 2018 Verification finished: Wed Sep 19 09:53:23 2018 MD5 checksum: 5c4aead15ef34a54ddcd558dc2f7f947 : verified
NYC023725_1B27-2  Staging Drive 1	09/12/18	VD	<b>Preserve Evidence: Image</b> Attempted to image NYC023725_1B27-2 using a Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D3B0A6, to Staging Drive 1. Drive inoperable.
NYC023725_1B27-2	09/21/18	VD	Connected NYC023725_1B27-2 to Tableau TX1 Forensic Imager, version: 1.2.0, s/n: 000ecc5801109b. Drive inoperable. Cooled drive to a lower temperature. Connected NYC023725_1B27-2 to Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D3B0A6. Drive inoperable.
NYC023725_1B27-2	09/21/18	VD	<b>Administrative Note:</b> Notified CA that drive was Inoperable. CA not interested in sending drive to HQ at this time. No further processing to be conducted at this time.
NYC023727_1B31	09/11/18	VD	<b>Preserve Evidence: Image</b> NYC023727_1B31 was imaged using a Tableau TX1 Forensic Imager,

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

Staging Drive 2			version: 1.2.0, s/n: 000ecc5801109b, to Staging Drive 2. Errors encountered but image successful. First attempt to Image with TD3 was unsuccessful.
Image.E01			<p>-----Source Disk-----</p> Interface: SATA Model: ATA ST9120821AS Firmware revision: 7.01 Serial number: 5PL0WPQC Capacity in bytes: 120,034,123,776 (120.0 GB) Block Size: 512 bytes Block Count: 234,441,648 Power-ON Block Count: 234,441,648 HPA Block Count: 234,441,648 DCO Block Count: 234,441,648 Encrypted: No Error granularity: 32,768 bytes <p>-----Imaging-----</p> Output file format: E01 Chunk size in bytes: 2,000,000,000 (2.0 GB) <p>-----Image Destination-----</p> Interface: SATA Model: WDC WD20EARX-00PASB0 Firmware revision: 51.0AB51 Serial number: WD-WCAZAJ020571 Capacity in bytes: 2,000,398,934,016 (2.0 TB) Block Size: 512 bytes Block Count: 3,907,029,168 Power-ON Block Count: 3,907,029,168 HPA Block Count: 3,907,029,168 DCO Block Count: 3,907,029,168 Encrypted: No Folder: /tx1_images/ File name base: image Verification Status: Finished OK Verification Md5: bdcc 8a77 2491 4693 2587 181e 0e1a 2c0d <p>-----Duplication Results-----</p> LBA Range Duplicated: Entire Source Disk Total errors: 200 Acquisition Md5: bdcc 8a77 2491 4693 2587 181e 0e1a 2c0d
Staging Drive 2	09/20/18	VD	Using Forensic Exam Station F2630035 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023727_1B31 (Image.E01) from Staging Drive 2 to CASE VOLUME.  Copy was verified using <b>FTK® Imager 4.2.0.13</b> . Examiner created image.E01.txt to CASE VOLUME to retain logs.

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			Image Verification Results: Verification started: Thu Sep 20 08:53:11 2018 Verification finished: Thu Sep 20 09:44:37 2018 MD5 checksum: bdcc8a77249146932587181e0e1a2c0d : verified
NYC023723 _1B23  Staging Drive 1  NYC023723 _1B23.E01	09/13/18	VD	<b>Preserve Evidence: Image</b> NYC023723_1B23 was imaged using a Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D350ED, to Staging Drive 1.  -----Source Disk----- Interface: USB Model: TOSHIBA TransMemory Firmware revision: 6.51 Serial number: u USB Serial number: 0B901C6022B368A4 Capacity in bytes: 3,993,304,576 (3.9 GB) Block Size: 512 bytes Block Count: 7,799,423  -----Destination Disk----- Interface: SATA Model: WDC WD20EARX-00PASB0 Firmware revision: 51.0AB51 Serial number: WD-WCAZAE561750 Capacity in bytes: 2,000,398,934,016 (2.0 TB) Block Size: 512 bytes Block Count: 3,907,029,168 Power-ON Block Count: 3,907,029,168 HPA Block Count: 3,907,029,168 DCO Block Count: 3,907,029,168  -----Disk Imaging Results----- Output file format: E01 - EnCase format Chunk size in bytes: 2,147,483,648 (2.1 GB) Chunks written: 2 Filename of first chunk: 2018-09-13_08-44-54/NYC023723_1B23.E01 Total errors: 0 Acquisition MD5: dd5fcb5d670976ca749c35d14bba7f8e  -----Readback Verification Results----- Verification MD5: dd5fcb5d670976ca749c35d14bba7f8e Status: Verified
Staging Drive 1  NYC023723 _1B23.E01	09/19/18	VD	Using Forensic Exam Station F2630035 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023723_1B23 from Staging Drive 1 to CASE VOLUME.  Copy was verified using <b>FTK® Imager 4.2.0.13.</b>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			Examiner created NYC023723_1B23.E01.txt to CASE VOLUME to retain logs.  Image Verification Results: Verification started: Wed Sep 19 14:00:29 2018 Verification finished: Wed Sep 19 14:02:18 2018 MD5 checksum: dd5fcb5d670976ca749c35d14bba7f8e : verified
--	--	--	---

NYC023730_1B41  NYC023730_1B41.E01	09/13/18	VD	<p><b>Preserve Evidence: Image</b>                  NYC023730_1B41 was imaged with Forensic Exam Station F2630035 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 0208710F and a <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p>
--	----------	----	---

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

		<p>Properties</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Evidence Source Path</li> <li><input type="checkbox"/> Evidence Type</li> <li><input checked="" type="checkbox"/> Disk             <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Drive Geometry                 <ul style="list-style-type: none"> <li>Cylinders</li> <li>Tracks per Cylinder</li> <li>Sectors per Track</li> <li>Bytes per Sector</li> <li>Sector Count</li> </ul> </li> <li><input checked="" type="checkbox"/> Physical Drive Information                 <ul style="list-style-type: none"> <li>Drive Model</li> <li>Drive Serial Number</li> <li>Drive Interface Type</li> <li>Removable drive</li> </ul> </li> </ul> </li> </ul> <p>Program shutdown before completion.</p>
<p>NYC023730 _1B41</p> <p>NYC023730 _1B41.E01</p>	<p>09/14/18</p> <p>VD</p>	<p>Restart image process.  <b>NYC023730_1B41</b> was imaged with Forensic Exam Station F2630035 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 0208710F and a <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p> <p>Physical Evidentiary Item (Source) Information:          [Device Info]          Source Type: Physical          [Drive Geometry]          Cylinders: 121,605          Tracks per Cylinder: 255          Sectors per Track: 63          Bytes per Sector: 512          Sector Count: 1,953,588,224          [Physical Drive Information]          Drive Model: LaCie Bi ggerDisk USB Device          Drive Serial Number: A7E511243137          Drive Interface Type: USB          Removable drive: False          Source data size: 953900 MB          Sector count: 1953588224          [Computed Hashes]          MD5 checksum: 07df4939e1107220aa5dd1a39fb04767          Image Verification Results:          Verification started: Fri Sep 14 22:38:22 2018          Verification finished: Sat Sep 15 03:19:25 2018          MD5 checksum: 07df4939e1107220aa5dd1a39fb04767 : verified</p> <p>A <b>Directory/File Listing</b> was generated when evidence was imaged using</p>

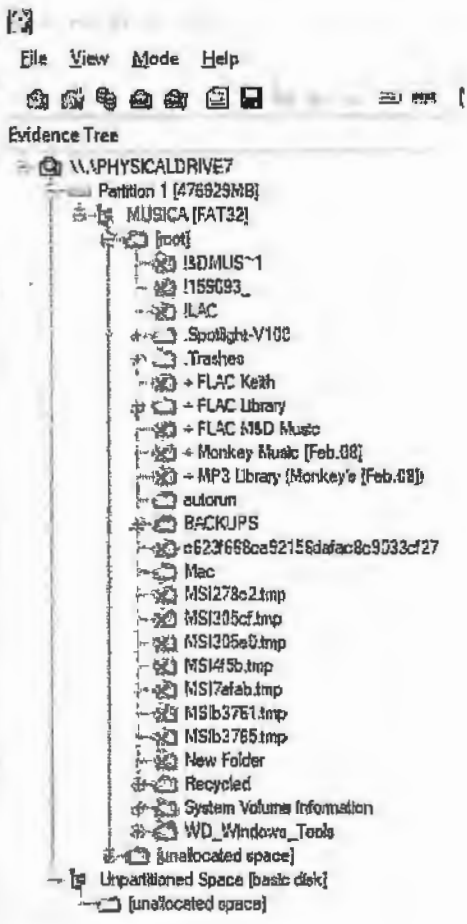
THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			<p><b>FTK® Imager 4.2.0.13.</b> Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.                  Directory listing created and saved as NYC023730_1B41.E01.csv within CASE VOLUME.</p>
<p>NYC023721_1B16                   NYC023721_1B16.E01</p>	<p>09/13/18</p>	<p>VD</p>	<p><b>Preserve Evidence: Image</b>                  NYC023721_1B16 was imaged with Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7, and <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p>  <p>The screenshot shows the Evidence Tree for a physical drive (\\.\PHYSICALDRIVE7). The tree structure is as follows:</p> <ul style="list-style-type: none"> <li>Partition 1 [476629MB]             <ul style="list-style-type: none"> <li>MUSICA [FAT32]                     <ul style="list-style-type: none"> <li>[root]                             <ul style="list-style-type: none"> <li>!SDMUS~1</li> <li>!155093_</li> <li>ILAC</li> <li>.Spotlight-V100</li> <li>.Trashes</li> <li>+ FLAC Keith</li> <li>+ FLAC Library</li> <li>+ FLAC MSD Music</li> <li>+ Monkey Music [Feb.08]</li> <li>+ MP3 Library (Monkey's [Feb.08])</li> <li>autorun</li> <li>BACKUPS</li> <li>e523f668ca92156dafac8c9033cf27</li> <li>Mac</li> <li>MSI278c2.tmp</li> <li>MSI205cf.tmp</li> <li>MSI205e0.tmp</li> <li>MSI45b.tmp</li> <li>MSI7efab.tmp</li> <li>MSIb3761.tmp</li> <li>MSIb3765.tmp</li> <li>New Folder</li> <li>Recycled</li> <li>System Volume Information</li> <li>WD_Windows_Tools</li> <li>[unallocated space]</li> </ul> </li> </ul> </li> </ul> </li> <li>Unpartitioned Space [basic disk]             <ul style="list-style-type: none"> <li>[unallocated space]</li> </ul> </li> </ul>

<p>THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.                  DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.</p>	<p>Affix Label Here</p>
---	-------------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			<p>Properties</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Evidence Source Path</li> <li><input type="checkbox"/> Evidence Type</li> <li><input checked="" type="checkbox"/> <b>Disk</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Drive Geometry</b> <ul style="list-style-type: none"> <li>Cylinders</li> <li>Tracks per Cylinder</li> <li>Sectors per Track</li> <li>Bytes per Sector</li> <li>Sector Count</li> </ul> </li> <li><input checked="" type="checkbox"/> <b>Physical Drive Information</b> <ul style="list-style-type: none"> <li>Drive Model</li> <li>Drive Serial Number</li> <li>Drive Interface Type</li> <li>Removable drive</li> </ul> </li> </ul> </li> </ul> <p>1<sup>st</sup> attempt never went past preparing for imaging.</p>
NYC023721 _1B16	09/14/18	VD	Restart Image process. Not reading the drive.
	09/19/18	VD	Open source search revealed Western Digital renamed the model number of NYC023721_1B16 from WD5000P032 to WDG1C5000N. Item name is "My Book Premium Edition."
NYC023721 _1B16  NYC023721 _1B16.E01	09/19/18	VD	<p><b>NYC023721_1B16</b> was imaged with Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7, and <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p> <p>Physical Evidentiary Item (Source) Information:                  [Device Info]                  Source Type: Physical                  [Drive Geometry]                  Cylinders: 60,801                  Tracks per Cylinder: 255                  Sectors per Track: 63                  Bytes per Sector: 512                  Sector Count: 976,773,168                  [Physical Drive Information]                  Drive Model: WD 5000A A External USB Device                  Drive Serial Number: 57442D57434153383133                  Drive Interface Type: USB                  Removable drive: False</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here





**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			<p>Source data size: 476940 MB                  Sector count: 976773168                  [Computed Hashes]                  MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e                  Image Verification Results:                  Verification started: Wed Sep 19 15:37:01 2018                  Verification finished: Wed Sep 19 20:09:15 2018                  MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e : verified</p> <p><b>A Directory/File Listing</b> was generated when evidence was imaged using <b>FTK® Imager 4.2.0.13</b>. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.                  Directory listing created and saved as NYC023721_1B16.E01.csv within CASE VOLUME.</p>
<p>NYC023731_1B43                   NYC023731_1B43.E01</p>	<p>09/14/18</p>	<p>VD</p>	<p><b>Preserve Evidence: Image</b>                  NYC023731_1B41 was imaged with Forensic Exam Station F2552510 using a Digital Intelligence USB 3.0 Forensic Card Reader, SKU# W2525, and <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p> 

<p>THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.                  DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.</p>	<p>Affix Label Here</p>
---	-------------------------



FEDERAL BUREAU OF INVESTIGATION  
COMPUTER ANALYSIS RESPONSE TEAM  
NEW YORK DIVISION

# EXAMINATION NOTES

		<p>Properties</p> <p>21</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Evidence Source Path</li> <li><input type="checkbox"/> Evidence Type</li> <li><input checked="" type="checkbox"/> Disk <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Drive Geometry <ul style="list-style-type: none"> <li>Cylinders</li> <li>Tracks per Cylinder</li> <li>Sectors per Track</li> <li>Bytes per Sector</li> <li>Sector Count</li> </ul> </li> <li><input checked="" type="checkbox"/> Physical Drive Information <ul style="list-style-type: none"> <li>Drive Model</li> <li>Drive Serial Number</li> <li>Drive Interface Type</li> <li>Removable drive</li> </ul> </li> </ul> </li> </ul> <p>Physical Evidentiary Item (Source) Information:</p> <p>[Device Info] Source Type: Physical</p> <p>[Drive Geometry] Cylinders: 31 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 503,808</p> <p>[Physical Drive Information] Drive Model: Generic- USB3.0 CRW-CF/MD USB Device Drive Serial Number: 2012062914345300 Drive Interface Type: USB Removable drive: True Source data size: 246 MB Sector count: 503808</p> <p>[Computed Hashes] MD5 checksum: a489bb0b99f598ba60e1ae3a1e591b38</p> <p>Image Verification Results: Verification started: Fri Sep 14 10:08:57 2018 Verification finished: Fri Sep 14 10:09:05 2018 MD5 checksum: a489bb0b99f598ba60e1ae3a1e591b38 : verified</p> <p>A <b>Directory/File Listing</b> was generated when evidence was imaged using <b>FTK® Imager 4.2.0.13</b>. Listing file is co-located along with the respective image files within the CASE VOLUME. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.</p>
--	--	--

<p>THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.</p>	<p>Affix Label Here</p>
--	-------------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

NYC023728 _1B32  NYC023728 _1B32.E01	09/14/18	VD	<p><b>Preserve Evidence: Image</b>                  NYC023728_1B32 was imaged with Forensic Exam Station Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7, and <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p> <hr/> <p>AccessData FTK Imager 4.2.0.13</p> <p>File View Mode Help</p> <p>Evidence Tree</p> <pre>                 \\PHYSICALDRIVE7                 - Partition 1 [953198MB]                 - My Book [HFSX]                 - [unallocated space]                 - 000168985                 - 034784603                 - My Book                 - HFS- Private Data                 - .seventd                 - .HFS- Private Directory Data                 - .Spotlight-V100                 - .Trashes                 - Backups.backupdb                 - Unpartitioned Space [basic disk]                 - [unallocated space]             </pre> <p>Properties</p> <p>Evidence Source Path</p> <p>Evidence Type</p> <p><input checked="" type="checkbox"/> Disk</p> <p><input checked="" type="checkbox"/> Drive Geometry</p> <ul style="list-style-type: none"> <li>Cylinders</li> <li>Tracks per Cylinder</li> <li>Sectors per Track</li> <li>Bytes per Sector</li> <li>Sector Count</li> </ul> <p><input checked="" type="checkbox"/> Physical Drive Information</p> <ul style="list-style-type: none"> <li>Drive Model</li> <li>Drive Serial Number</li> <li>Drive Interface Type</li> <li>Removable drive</li> </ul> <p>Physical Evidentiary Item (Source) Information:</p>
--	----------	----	---

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

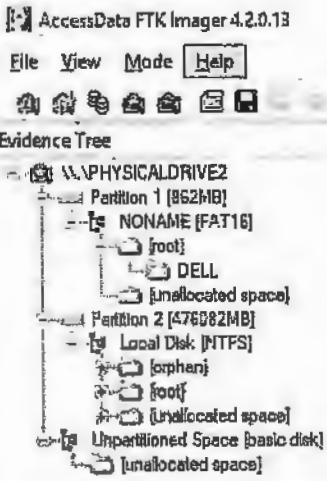
			<p>[Device Info]                  Source Type: Physical                  [Drive Geometry]                  Cylinders: 121,515                  Tracks per Cylinder: 255                  Sectors per Track: 63                  Bytes per Sector: 512                  Sector Count: 1,952,151,552                  [Physical Drive Information]                  Drive Model: WD My Bo ok 1111 USB Device                  Drive Serial Number: 57434156353438373337                  Drive Interface Type: USB                  Removable drive: False                  Source data size: 953199 MB                  Sector count: 1952151552                  [Computed Hashes]                  MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12</p> <p>Image Verification Results:                  Verification started: Sat Sep 15 00:31:12 2018                  Verification finished: Sat Sep 15 03:17:38 2018                  MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12 ; verified</p> <p><b>A Directory/File Listing</b> was generated when evidence was imaged using <b>FTK® Imager 4.2.0.13</b>. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.                  Directory listing created and saved as NYC023728_1B32.E01.csv within CASE VOLUME.</p>
NYC023732_1B50	09/14/18	VD JC	<p><b>Preserve Evidence: Extraction</b>                  Powered on device 09/14/2018 at approximately 12:00noon.                  No pin associated with device.                  Settings identifies the device as "Keith's iPod."                  Changed Backlight Timer from 10 seconds to Always On.</p> <p>Using Forensic Exam Station F2552510:  <b>UFED 4PC 7.8.0.942</b>                  Did not recognize device.</p> <p><b>UFED Physical Analyzer 7.1.0.106</b>                  Did not recognize device.</p> <p>Under the guidance of ITS/SFE John Chan, attempted IPEX 2.1.8 and IPHAT 1.13.0. Did not recognize device.</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

NYC023732 _1B50	09/21/18	BB	<p><b>Preserve Evidence: Extraction</b>                  Using Forensic Exam Station F5405659  <b>XRY 7.8</b>                  Physical- Successful</p> <p>Called CA to notify that XRY was working on device.</p>
NYC023726 _1B28  NYC023726 _1B28.E01	09/17/18	VD	<p><b>Preserve Evidence: Image</b>                  NYC023726_1B28 was imaged with Forensic Exam Station F2630035 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 0208710F, and <b>AccessData® FTK® Imager 4.2.0.13</b>, to the CASE VOLUME.</p> 

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION  
COMPUTER ANALYSIS RESPONSE TEAM  
NEW YORK DIVISION

# EXAMINATION NOTES


		<p>Properties</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Evidence Source Path</li> <li><input type="checkbox"/> Evidence Type</li> <li><input checked="" type="checkbox"/> Disk <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Drive Geometry <ul style="list-style-type: none"> <li>Cylinders</li> <li>Tracks per Cylinder</li> <li>Sectors per Track</li> <li>Bytes per Sector</li> <li>Sector Count</li> </ul> </li> <li><input checked="" type="checkbox"/> Physical Drive Information <ul style="list-style-type: none"> <li>Drive Model</li> <li>Drive Serial Number</li> <li>Drive Interface Type</li> <li>Removable drive</li> </ul> </li> </ul> </li> </ul> <p>Physical Evidentiary Item (Source) Information:</p> <p>[Device Info] Source Type: Physical</p> <p>[Drive Geometry] Cylinders: 60,802 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 976,794,336</p> <p>[Physical Drive Information] Drive Model: LaCie Bi gDisk USB Device Drive Serial Number: AAC3CC45261F Drive Interface Type: USB Removable drive: False Source data size: 476950 MB Sector count: 976794336</p> <p>[Computed Hashes] MD5 checksum: c3831223db43f2042a69f970bacb0b0a</p> <p>Image Verification Results: Verification started: Mon Sep 17 18:40:58 2018 Verification finished: Mon Sep 17 19:29:44 2018 MD5 checksum: c3831223db43f2042a69f970bacb0b0a : verified</p> <p>A <b>Directory/File Listing</b> was generated when evidence was imaged using <b>FTK® Imager 4.2.0.13</b>. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp. Directory listing created and saved as NYC023726_1B28.E01.csv within</p>
--	--	--

<p>THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.</p>	<p>Affix Label Here</p>
--	-------------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			CASE VOLUME.
NYC023724 _1B26	09/20/18	VD	<p><b>Preserve Evidence: Image</b>                      NYC023724_1B26 is a My Book World Edition network-attached storage system. Connected NYC023724_1B26 to internal network.</p> <ul style="list-style-type: none"> <li>▪ Installed and launched WD Link software.</li> <li>▪ Used default password to connect to the unit.</li> <li>▪ Connected to unit via web browser and continued through configuration settings to assign permanent password for administrative access (admin).</li> <li>▪ Noticed item was configured via DHCP (Dynamic Host Configuration Protocol).</li> <li>▪ Assigned static IP address of 192.168.1.2.</li> <li>▪ Enabled FTP (File Transfer Protocol) connection through anonymous authentication.</li> <li>▪ Removed device from internal network and connected the unit to a standalone network switch.</li> </ul> <p>The following images capture the findings:</p> 

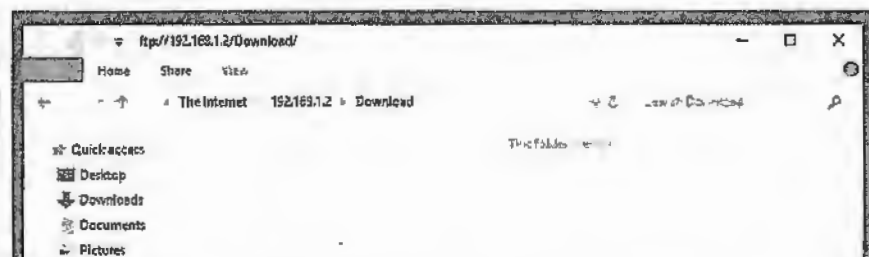
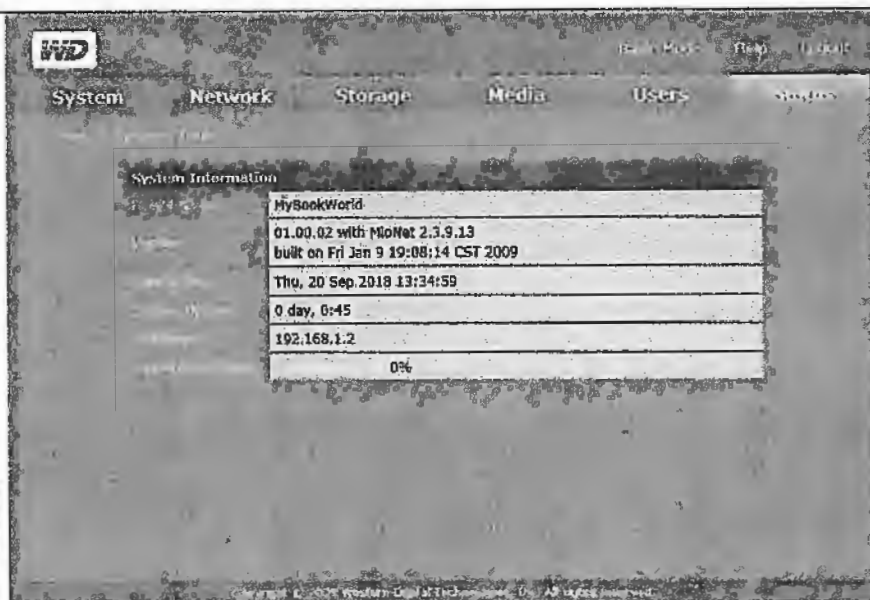
THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION  
COMPUTER ANALYSIS RESPONSE TEAM  
NEW YORK DIVISION

# EXAMINATION NOTES



THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

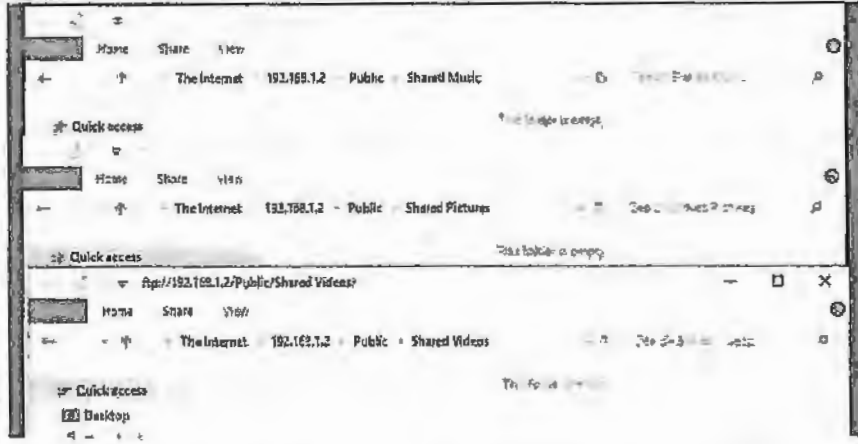
Affix Label Here





**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			 <p>System Log was screen grabbed and saved as WorldBook System Log.txt. See attached addendum for further information.</p>
NYC023724_1B26	09/20/18	VD	<p><b>Administrative Note:</b>                  Notified CA that examination of NYC023724_1B26 to date showed no data stored on the device; no further processing conducted at this time.</p>
NYC023729_1B26	09/20/18	VD	<p><b>Preserve Evidence: Image</b>                  NYC023729_1B26 was connected to Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7. Device would not turn on. Did not recognize device. Set aside device to charge.</p>
NYC023729_1B26	09/21/18	VD	<p>Device would not turn on.                  NYC023729_1B26 was connected to Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7. Did not recognize device.                  Connected device directly to Forensic Exam Station F2673128. Did not recognize device.</p>
	09/21/18	VD	<p><b>Administrative Note:</b>                  Notified CA that the device was not recognized by forensic machines. No further processing at this time.</p>
NYC023725_1B27-1,E01	09/14/18	VD	<p><b>Preserve Evidence: Discovery</b>                  Produce verified copies of images for discovery saved to Seagate Expansion Portable Drive, 1TB, model: SRD0NF1, p/n: 1TEAP5-500, s/n: NA8ZLFSQ, which was provided to CART by SA Lever.</p> <p>Using Forensic Exam Station F2552510 and Tableau eSATA Forensic Bridge</p>
Staging Drive 1			

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

Seagate HD			write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023725_1B27-1 from Staging Drive 1 to provided Seagate HD. Copy was verified using <b>FTK® Imager 4.2.0.13</b> .  Drive/Image Verify Results <span style="float: right;">- □ ×</span>  □ Name Sector count □ <b>MDS Hash</b> Computed hash Stored verification hash Verify result □ <b>SHA1 Hash</b> Computed hash □ <b>Bad Blocks List</b> Bad block(s) in image
NYC023723_1B23.E01  NYC023727_1B31.E01  NYC023731_1B43.E01  Staging Drive 1  Staging Drive 2  Seagate HD	09/17/18	VD	<b>Preserve Evidence: Discovery</b> Using Forensic Exam Station F2552510 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023723_1B23 from Staging Drive 1 to provided Seagate HD.  Drive/Image Verify Results <span style="float: right;">- □ ×</span>  □ Name Sector count □ <b>MDS Hash</b> Computed hash Stored verification hash Verify result □ <b>SHA1 Hash</b> Computed hash □ <b>Bad Blocks List</b> Bad block(s) in image  Using Forensic Exam Station F2552510 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC23727_1B31 from Staging Drive 2 to provided Seagate HD. Copy was verified using <b>FTK® Imager 4.2.0.13</b> .

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			<div data-bbox="519 340 1508 882"> <p>Drive/Image Verify Results</p> <ul style="list-style-type: none"> <li>[-]                     <ul style="list-style-type: none"> <li>Name</li> <li>Sector count</li> </ul> </li> <li>[-] <b>MDS Hash</b> <ul style="list-style-type: none"> <li>Computed hash</li> <li>Stored verification hash</li> <li>Verify result</li> </ul> </li> <li>[-] <b>SHA1 Hash</b> <ul style="list-style-type: none"> <li>Computed hash</li> <li>Stored verification hash</li> <li>Verify result</li> </ul> </li> <li>[-] <b>Bad Blocks List</b> <ul style="list-style-type: none"> <li>Bad block(s) in image</li> </ul> </li> </ul> </div> <p>Using Forensic Exam Station F2552510, copy images of NYC023731_1B43 from the CASE VOLUME to provided Seagate HD. Copy was verified using <b>FTK® Imager 4.2.0.13.</b></p> <div data-bbox="519 1008 1508 1638"> <p>Drive/Image Verify Results</p> <ul style="list-style-type: none"> <li>[-]                     <ul style="list-style-type: none"> <li>Name</li> <li>Sector count</li> </ul> </li> <li>[-] <b>MDS Hash</b> <ul style="list-style-type: none"> <li>Computed hash</li> <li>Stored verification hash</li> <li>Report Hash</li> <li>Verify result</li> </ul> </li> <li>[-] <b>SHA1 Hash</b> <ul style="list-style-type: none"> <li>Computed hash</li> <li>Stored verification hash</li> <li>Report Hash</li> <li>Verify result</li> </ul> </li> <li>[-] <b>Bad Blocks List</b> <ul style="list-style-type: none"> <li>Bad block(s) in image</li> </ul> </li> </ul> </div>
Seagate HD	09/17/18	VD	<p><b>Administrative Note:</b>                  Seagate HD provided to SA Lever. FD-597 completed and signed by SA Lever to accept.</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

NYC023730 _1B41.E01  Addonics HD	09/17/18	VD	<p><b>Preserve Evidence: Discovery</b>                  Produce verified copies of images for discovery saved to Addonics Diamond Cipher II ExDrive, 3TB, model: DCED6GEU3, s/n: 9797100411, which was provided to CART by SA Lever.</p> <p>Using Forensic Exam Station F2673128, copy images of NYC023730_1B41 from the CASE VOLUME to provided Addonics HD. Copy was verified using <b>FTK® Imager 4.2.0.13</b>.</p> <p>Original Computed Hashes:                  MD5 checksum: 07df4939e1107220aa5dd1a39fb04767                  Image Verification Results:                  Verification started: Mon Sep 17 16:39:58 2018                  Verification finished: Mon Sep 17 18:43:47 2018                  MD5 checksum: 07df4939e1107220aa5dd1a39fb04767 : verified</p>
NYC023728 _1B32.E01  NYC023726 _1B28.E01  Addonics HD	09/18/18	VD	<p><b>Preserve Evidence: Discovery</b>                  Produce verified copies of images for discovery saved to Addonics Diamond Cipher II ExDrive, 3TB, model: DCED6GEU3, s/n: 9797100411, which was provided to CART by SA Lever.</p> <p>Using Forensic Exam Station F2673128, copy images of NYC023728_1B32 from the CASE VOLUME to provided Addonics HD. Copy was verified using <b>FTK® Imager 4.2.0.13</b>.</p> <p>Original Computed Hashes                  MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12                  Image Verification Results:                  Verification started: Tue Sep 18 10:07:13 2018                  Verification finished: Tue Sep 18 11:55:47 2018                  MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12 : verified</p> <p>Using Forensic Exam Station F2673128, copy images of NYC023726_1B28 from the CASE VOLUME to provided Addonics HD. Copy was verified using <b>FTK® Imager 4.2.0.13</b>.</p> <p>Original Computed Hashes:                  MD5 checksum: c3831223db43f2042a69f970bacb0b0a                  Image Verification Results:                  Verification started: Tue Sep 18 12:47:22 2018                  Verification finished: Tue Sep 18 13:33:48 2018                  MD5 checksum: c3831223db43f2042a69f970bacb0b0a : verified</p>
Addonics HD	09/19/18	VD	<p><b>Administrative Note:</b>                  Addonics HD provided to SA Michael Lever. FD-597 completed and signed by SA Lever to accept.                  SA Lever and AUSA stated that the kindle, NYC023722_1B19, did not need</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			to be processed since the device powered on to the "thank you for purchasing" screen and seemed to only have the dictionary loaded.
NYC023732 _1B50  Addonics HD 2	09/26/18	VD	<b>Preserve Evidence: Discovery</b> Produce verified copies of images for discovery saved to Addonics Diamond Cipher II ExDrive, 3TB, model: DCED6GEU3, s/n: 9797100412, which was provided to CART by SA Lever.  Using Forensic Exam Station F2630035, copy images and reports of NYC023732_1B50 from the CASE VOLUME to provided Addonics HD using <b>VeriCopy v.3.18.</b>
NYC023721 _1B16.E01  Addonics HD 2	09/27/18	VD	Using Forensic Exam Station F2630035, copy images of NYC023721_1B16 from the CASE VOLUME to provided Addonics HD. Copy was verified using <b>FTK@ Imager 4.2.0.13.</b>  Original Computed Hashes: MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e Image Verification Results: Verification started: Thu Sep 27 11:12:28 2018 Verification finished: Thu Sep 27 12:58:24 2018 MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e : verified
Addonics HD 2	09/28/18	VD	<b>Administrative Note:</b> Addonics HD provided to SA Michael Lever. FD-597 completed and signed by SA Lever to accept.
NYC023721 _1B16.E01 NYC023723 _1B23.E01 NYC023725 _1B27- 1.E01 NYC023726 _1B28.E01 NYC023727 _1B31.E01 NYC023728 _1B32.E01 NYC023730 _1B41.E01 NYC023731 1B43.E01	09/24/18	VD	<b>Processing:</b> Images of NYC023721_1B16, NYC023723_1B23, NYC023725_1B27-1, NYC023726_1B28, NYC023727_1B31, NYC023728_1B32, NYC023730_1B41, and NYC023731_1B43 were added to <b>AD Lab v6.3.1.26</b> utilizing the Field Mode Processing Profile, default settings, on Forensic Exam Station F2673128. AD Lab will be used for examination in this case unless otherwise noted. Time zone setting: Eastern Time with Daylight Saving (US – New York)  <b>Additional Analysis:</b> First: <ul style="list-style-type: none"> <li>▪ Expand Compound Files (include deleted files)</li> <li>▪ Flag Bad Extensions</li> <li>▪ File Signature Analysis</li> </ul>
	09/25/18	VD	<b>AD Lab Additional Analysis:</b> Second:

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			<ul style="list-style-type: none"> <li>▪ Data Carve (all types selected)</li> <li>▪ Meta Carve</li> </ul> Errors encountered, failed.
	09/26/18	VD	<b>AD Lab Additional Analysis:</b> Third: <ul style="list-style-type: none"> <li>▪ Data Carve (all types selected)</li> </ul>
	09/27/18	VD	<b>AD Lab Additional Analysis:</b> Fourth: <ul style="list-style-type: none"> <li>▪ Meta Carve</li> </ul> Fifth: <ul style="list-style-type: none"> <li>▪ Create Thumbnails for Graphics</li> </ul>
	10/01/18	VD	<b>Administrative Note:</b> Spoke to SA Delise Jeffrey in person. Do not need thumbnails for videos.
	10/01/18	VD	<b>AD Lab Additional Analysis:</b> Sixth: <ul style="list-style-type: none"> <li>▪ MD5 Hash</li> <li>▪ Flag Duplicate Files</li> </ul> Seventh: <ul style="list-style-type: none"> <li>▪ Search Text Index (TR1)</li> <li>▪ Entropy Test (do not index compressed or encrypted items)</li> <li>▪ Include extended information</li> <li>▪ Merge case index when finished</li> </ul>
	10/03/18	VD	<b>Administrative Note:</b> E-mailed SA Lever and SA Jeffrey that the images and reports were available in CAIR.
	09/26/18	VD	<b>Evidence Disposition:</b> All evidence items were returned to SA Lever.
NYF00739 NYF01088	10/09/18 10/10/18	VD	<b>Preserve Evidence: Master Copy</b> Images were archived from the CASE VOLUME to two (2) TDK Tapes, both Model: Ultrium LTO 5, 1.5TB, previously affixed barcode and designated as NYF00739 and NYF01088, using Back This Up 3.1.17.5/Arcserve Backup. Logs retained.
NYF00739 NYF01088	10/12/18	VD	<b>Evidence Disposition:</b> CART created Master Copy was relinquished to Evidence Control. NYF00739 and NYF01088 were assigned 1B135 in captioned case file.
	11/16/18	VD	<b>Administrative Note:</b> SA Lever requested, via e-mail, a copy of the Directory File Listing for each individual device processed.

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

NYC023723 _1B23.csv	12/17/18	VD	<b>Processing:</b> Using Forensic Exam Station F2673128: <b>FTK Imager, build 4.2.0.13</b> Process Directory File Listings for the following imaged evidence items: NYC023723_1B23 and NYC023725_1B27-1
NYC023725 _1B27-1.csv			
image.E01.csv	12/18/18	VD	Process Directory File Listings for the following imaged evidence items: NYC023727_1B31 (image.E01.csv)
	12/28/18	VD	<b>Administrative Note:</b> E-mailed SA Lever indicating that directory file listings were available for all evidence items with the exception of 1B50 and to inform the examiner if the directory file listing was necessary for 1B50.
	01/22/19	VD	<b>Administrative Note:</b> Met and spoke to SA lever. He no longer needed a copy of the Directory File Listings from the examiner.
	02/22/19	VD	<b>Administrative Note:</b> SA Lever e-mailed examiner to do an internet evidence review of AOL e-mail found on 1B28.
	02/25/19	VD	<b>Administrative Note:</b> SA Lever requested access via e-mail for SA Leslie Adamczyk to review evidence item 1B16. In a separate e-mail, SA Lever provided a copy of a new Search and Seizure Warrant pertaining to the search of evidence item 1B16 for evidence of child pornography.
NYC023726 _1B28	02/26/19	VD	<b>Processing:</b> Using <b>Internet Evidence Finder (IEF) v6.14.0.10770</b> , processed 1B28 for internet remnants SA Lever requested.
NYC023721 _1B16	02/26/19	VD	<b>Administrative Note:</b> SA Leslie Adamczyk granted access to entire case. E-mailed case agents of the same and indicated the scope of the new warrant only allows the search for child pornography on 1B16.
NYC023726 _1B28  NYC023744	03/05/19	VD	<b>Processing:</b> Created DVD-R of IEF report generated for item 1B28, affixed barcode and designated as NYC023744. Notified SA Jeffrey, in person, that the report was completed and ready for pick up.
	03/06/19	BB	<b>Administrative Note:</b>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			ITS/SFE Booth provided hand written notes on research of EXIF data pertaining to the CP images identified on 1B16.
1B16	03/13/19	BSB	<b>Administrative Note:</b> Provided access for separate review of 1B16 to defense council. Computer installed and 1B16 ran in AD Lab for full processing. SA Lever advised via Bureau cell phone that data was available for review in CART Review room on the 22 <sup>nd</sup> floor of 26 Federal Plaza.
NYC023744	03/15/19	VD	<b>Administrative Note:</b> Provided NYC023744 to SA Lever. Completed FD-597.
	03/15/19	VD	<b>Administrative Note:</b> SA Lever and AUSA, in person, requested a copy of evidence item 1B16 without CP for discovery.
1B16 My Passport	03/18/19	VD	<b>Processing:</b> SA Lever provided a My Passport Western Digital hard drive, 2TB, model: WDBS4B0020BBK-WESN, s/n: WXP1A38H88CX, for the copy of 1B16 sans possible CP. Logical export of 1B16 without files identified by case agent as contraband saved to the My Passport drive.
My Passport	03/20/19	VD	<b>Administrative Note:</b> Provided My Passport drive to SA Jeffrey. Completed FD-597. Agents were advised to review the drive for contraband prior to distribution.
	04/04/19	VD	<b>Administrative Note:</b> SA Lever and SA Jeffrey indicated other possible CP was identified on 1B16. Agents are retrieving the previously distributed drive for discovery and requested a new copy be made without CP once they review the newly identified images. Agents provided handwritten list of files they identified as contraband.
My Passport 2	04/04/19	VD	<b>Processing:</b> SA Lever and SA Jeffrey provided a My Passport Western Digital hard drive, 2TB, model: WDBS4B0020BBK-WESN, s/n: WX81A38D01U0, for the copy of 1B16 without possible CP. Logical export of 1B16 without files identified by case agents as contraband saved to the My Passport drive.
My Passport 2	04/05/19	VD	<b>Administrative Note:</b> Provided My Passport drive to SA Lever. Completed FD-597. Agents were advised to review the drive for contraband prior to any distribution.
	04/10/19	BSB	<b>Processing:</b> AD Lab not reporting EXIF data for item 1B16 as separate reportable html

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------





FEDERAL BUREAU OF INVESTIGATION  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			files. Re-ran "Expand Compound Files" in AD Lab on item 1B16 for only EXIF data expansion.
NYC023288 NYC023289	04/11/19	BSB	<p><b>Processing:</b>                  Created AD Lab Report containing bookmarks of the "Studies Folders" identified from item 1B16 as indicated by SA Lever. Report burned to Adams Evidence Grade DVD-R and affixed label and noted herein as NYC023288.</p> <p>Created AD Lab Report containing bookmarks of the "Suspected CP Images" identified from Item 1B16 as indicated by SA Lever. Report burned to Adams Evidence Grade DVD-R and affixed label and noted herein as NYC023289.</p> <p>Items signed over and entered into NY Evidence Control Unit (ECU).</p> <p>Generated AD1 image of two reports with FTK Imager 4.2.0.3 as 041119_Reports.ad1 directly to the CASE VOLUME / DE NYCART. Staging drive was forensically wiped.</p> <p>Case agent requested a copy of bookmarked CP Images to be redacted for facial identification. A list of requested image names were provided in an e-mail by SA Delise Jeffery. Using Microsoft Photos, a crop of each image was done to show only facial features. These images were then saved to the CASE FOLDER in addition to one CD-R that was burned and marked as a "Working Copy". Disc was provided to SA Lever at 2:30PM.</p>
NYC023290	04/23/19	BSB	<p><b>Processing:</b>                  Spoke to Agent Lever about received email from AUSA with a request from defense attorney for a copy of 1B16 image files in a redacted format. Request verbally denied to agent Lever as against DEPG and CART policy. Advised Agent Lever that images have been made available for full review by the defense team in the CART Review room located on the 22<sup>nd</sup> floor of 26 Federal Plaza. CART NY has made the review available to the defense team since it had been placed for review on</p> <p>As per agent Lever request, created AD Lab Report containing bookmarks of the "Suspected CP" identified from Item 1B16 sans the graphic images. Report burned to Adams Evidence Grade CD-R and affixed label and noted herein as NYC023290. Agent working copy generated on separate white label CD-R.</p> <p>Items signed over and entered into NY Evidence Control Unit (ECU).</p>
	04/30/19	VD	<p><b>Administrative Note:</b>                  SA Lever requested printed copies of 22 images which he identified as possible CP for judge and jury purposes. Examiner printed the images and</p>

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

			completed a Chain of Custody. SA Lever put the printed photos into evidence, 1Bxxxx.
	06/07/19	BSB	<b>Administrative Note:</b> Request was made by SA Lever of Item 1B15 to be processed in lieu of ITS/SFE Steven Flatleys availability as he would be overseas during trial. This exam would be utilized in trial. SSA Trenton Schmatz concurred and authorized to process the item.
1B15	06/10/19	BSB	<b>Receipt of Evidence:</b> Evidence received directly from Case Agent.  <b>E6261241 1B15</b> One (1) Cannon Ultrasonic Digital Camera, model:DS126061, s/n: 1420908348. In black Cannon camera bag stored in brown cardboard evidence box.  Containing: One (1) Lexar Professional 2GB WA compact flash card, model:2389, s/n:39132GBCI39052D97, in separate cellophane baggie affixed barcode <b>NYC024299</b> . Initialed by ITS/SFE Stephen Flatley on 02/22/2019
NYC024299	06/11/19	BSB	<b>Administrative Note:</b> Forensic Exam Station F5405659 (S/N: 3YSZDB2), identified as <b>BBOOTH-01</b> , successfully completed the Power On Self Test (POST) process and is being used to process evidence images.  F5405659 is a Dell T7910 running Windows 10 Enterprise Edition 64-bit Operating System with sixty-four (64) GB RAM and two (2) Intel Xeon X2650 processors at 2.30GHz.  F5405659 is running AccessData Lab 6.3.1.26 configured in a multi-node DPE cluster. AccessData Lab Lab 6.3.1.26 will be utilized in processing for this examination of NYC024299, unless otherwise noted.
NYC024299	06/11/19	BSB	<b>Preserve Evidence: NYC242299</b> NYC024299 was imaged using a Tableau Forensic Card Reader (s/n: CR000004832) and a <b>AccessData® FTK® Imager 4.2.0.13</b> , to the CASE VOLUME.  Drive Geometry as reported by FTK Imager:  [Drive Geometry] Cylinders: 249 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 4,008,816

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
 DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



**FEDERAL BUREAU OF INVESTIGATION**  
 COMPUTER ANALYSIS RESPONSE TEAM  
 NEW YORK DIVISION

**EXAMINATION NOTES**

		<p>[Physical Drive Information]                  Drive Model: Generic- USB3.0 CRW-CF/MD USB Device                  Drive Serial Number: 2012062914345300                  Drive Interface Type: USB                  Removable drive: True                  Source data size: 1957 MB                  Sector count: 4008816</p> <p>[Computed Hashes]                  MD5 checksum: 55729198b0cf6a3242d888287a3fe485</p> <p>Image Verification Results:                  Verification started: Tue Jun 11 11:06:26 2019                  Verification finished: Tue Jun 11 11:06:36 2019                  MD5 checksum: 55729198b0cf6a3242d888287a3fe485 : verified</p> <p>Drive/Image Verify Results</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Name</li> <li><input type="checkbox"/> Sector count</li> <li><input checked="" type="checkbox"/> MD5 Hash                         <ul style="list-style-type: none"> <li><input type="checkbox"/> Computed hash</li> <li><input type="checkbox"/> Stored verification hash</li> <li><input type="checkbox"/> Report Hash</li> <li><input type="checkbox"/> Verify result</li> </ul> </li> </ul> <p>The CASE VOLUME will be used for all further processing.</p>
NYC024299	06/11/19	BSB <b>Directory/File Listing:</b> Unless otherwise specified, a directory/file listing was originally generated for all imaged specimens using <b>FTK® Imager 4.2.0.13</b> Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.
<b>END EXAM</b>		

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION. DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.	Affix Label Here
--	------------------



**FEDERAL BUREAU OF INVESTIGATION**  
COMPUTER ANALYSIS RESPONSE TEAM  
NEW YORK DIVISION

## EXAMINATION NOTES

**Examiner:**

**SA/FET Virginia Donnelly  
ITS/SFE Brian Booth**

**Date of Report:**

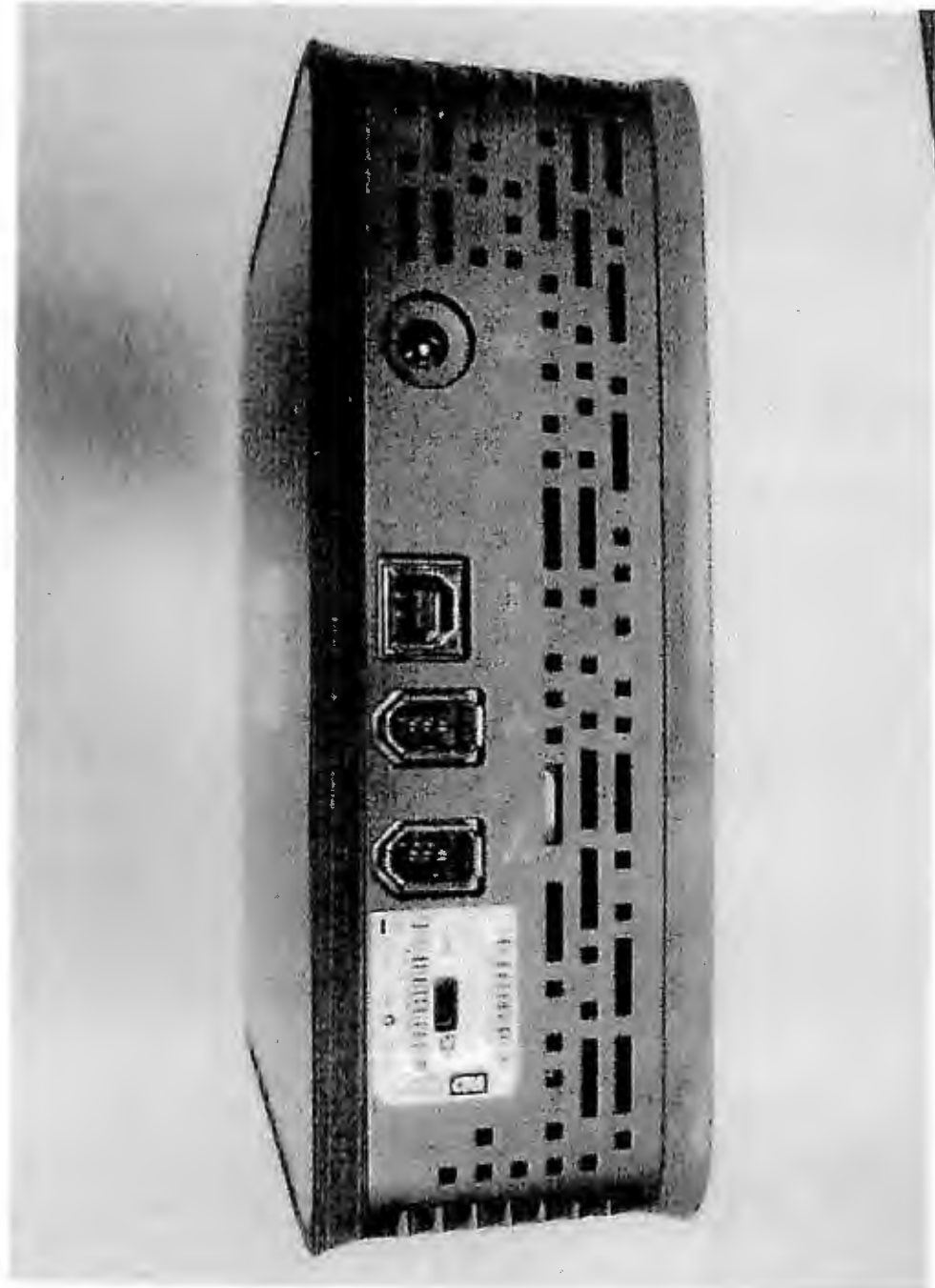
**Month XX, 20XX**

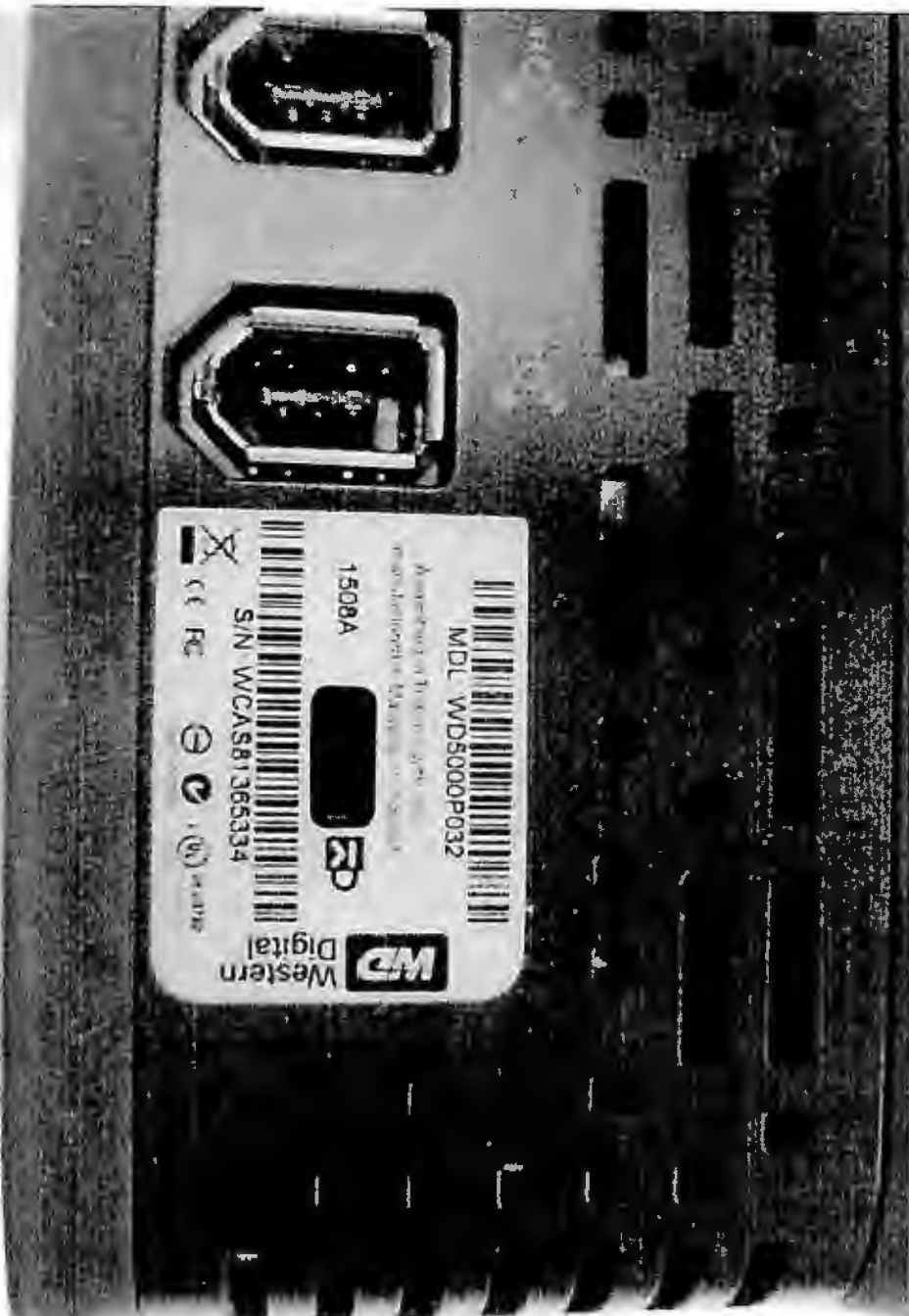
THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.  
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



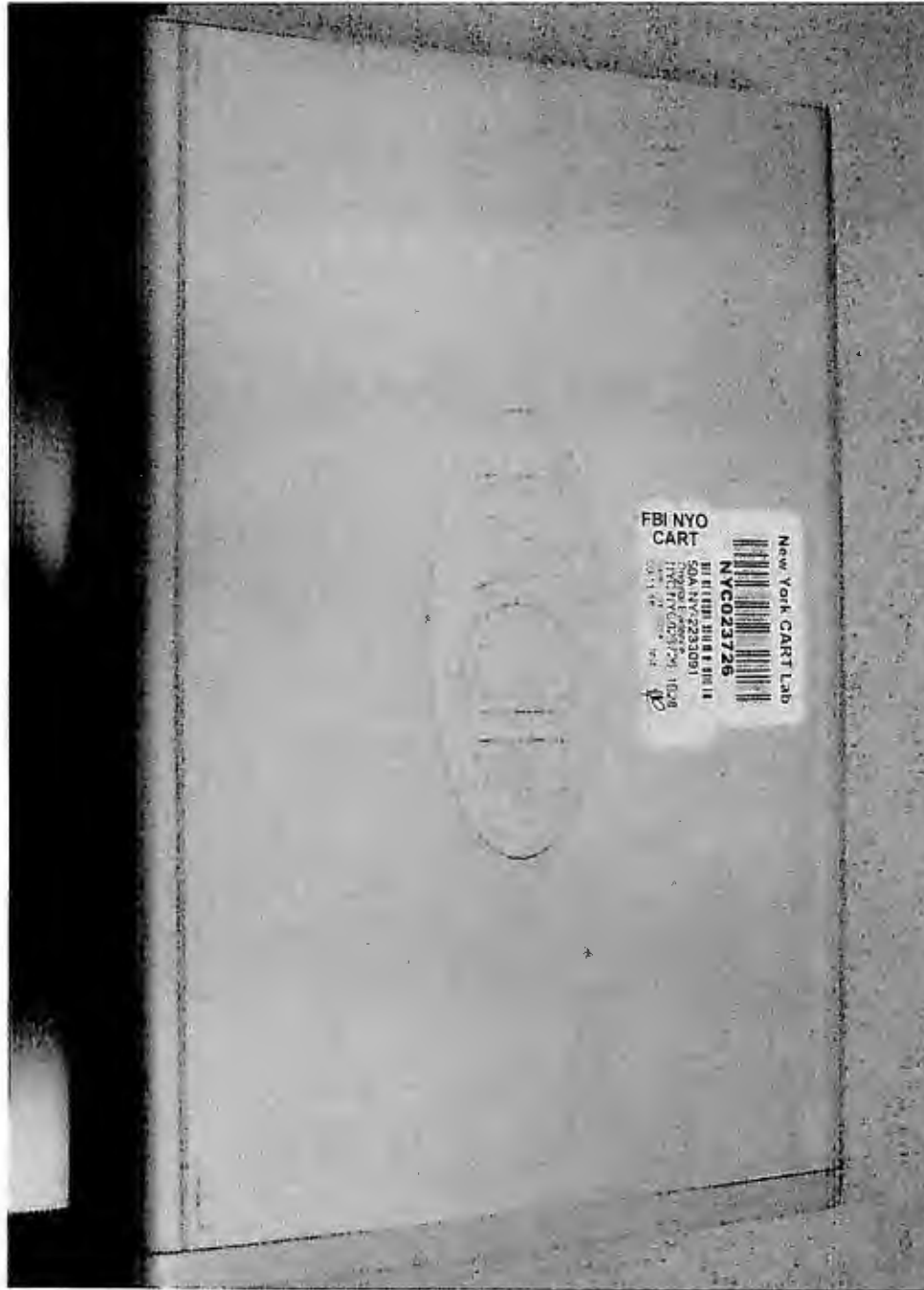














# **EXHIBIT C**

**(FBI's Digital Evidence Guide)**

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1256875-0

Total Deleted Page(s) = 1  
Page 24 ~ b3; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

~~UNCLASSIFIED//FOUO/LES~~

## **(U) Digital Evidence Corporate Policy Directive and Policy Implementation Guide**



**(U) Federal Bureau of Investigation  
(U) Operational Technology Division  
(U) 0639DPG**

**(U) Published Date: January 03, 2014  
(U) Review Date: January 03, 2017**

**(U) Note:** This document incorporates the Corporate Policy Directive and the Policy Implementation Guide.

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION  
CORPORATE POLICY DIRECTIVE



0639D

<b>1. Policy Directive Title.</b>	(U) Digital Evidence Policy Implementation Guide
<b>2. Publication Date.</b>	2014-01-03
<b>3. Effective Date.</b>	2014-01-03
<b>4. Review Date.</b>	2017-01-03

**5. Primary Strategic Objective.**

**6. Authorities:**

(U) Title 28 Code of Federal Regulations (C.F.R) Section (§) 0.85

**7. Purpose:**

(U) To promulgate the Digital Evidence Policy Implementation Guide.

**8. Policy Statement:**

8.1. (U) All Federal Bureau of Investigation (FBI) employees, task force members, contractors, and other persons assigned or detailed to the FBI must comply with the policies and procedures contained in the Digital Evidence Policy Implementation Guide (PG), which are consistent with the laws, rules, and regulations governing FBI investigations, operations, programs, and activities. (See the Digital Evidence Policy Implementation Guide for these policies and procedures.)

8.2. (U) Any revisions, amendments, or updates to this PG must be coordinated through the Corporate Policy Office (CPO), the Operational Technology Division (OTD) policy officer, and other relevant stakeholders (as determined by CPO and OTD). Resulting changes must then be approved by OTD's assistant director and the executive assistant director (EAD), Science and Technology Branch, as appropriate.

**9. Scope:**

(U) The guidance provided by the Digital Evidence Policy Implementation Guide is intended for all FBI employees, task force members, contractors, and other persons assigned or detailed to the FBI.

**10. Proponent:**

(U) Operational Technology Division

**11. Roles and Responsibilities:**

(U) See the Digital Evidence Policy Implementation Guide.

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

**12. Exemptions:**

(U) See the Digital Evidence Policy Implementation Guide.

**13. Supersession:**

(U) See the Appendix C of the Digital Evidence Policy Implementation Guide.

**14. References, Key Words, and Links:**

(U) 14.1. See the Digital Evidence Policy Implementation Guide.

(U) 14.2. See the [FBI Domestic Investigations and Operations Guide \(DIOG\)](#).

**15. Definitions:**

(U) See the Appendix E of the Digital Evidence Policy Implementation Guide, "Definitions and Acronyms."

**16. Appendices, Attachments, and Forms:**

(U) See the Digital Evidence Policy Implementation Guide.

**Sponsoring Executive Approval**

**Name:** Amy S. Hess

**Title:** Assistant Director, Operational Technology Division

**Stakeholder Executive Approval**

**Name:** Patrick W. Kelley

**Title:** The General Counsel (Acting)

**Final Approval**

**Name:** Steven M. Martinez

**Title:** Executive Assistant Director, Science and Technology Branch

~~UNCLASSIFIED~~

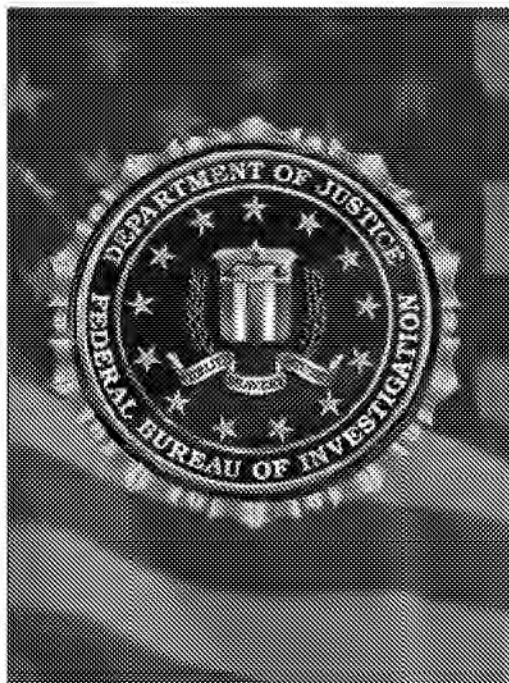
~~UNCLASSIFIED//FOUO/LES~~



~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

## (U) Digital Evidence Policy Implementation Guide



(U) Federal Bureau of Investigation

(U) Operational Technology Division

(U) 0639PG

(U) January 03, 2014

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

**(U) GENERAL INFORMATION**

(U) Questions or comments pertaining to this policy implementation guide can be directed to:

(U) Federal Bureau of Investigation Headquarters (FBIHQ) /Operational Technology Division

(U//~~FOUO~~) Division Point of Contact: Section Chief, Digital Evidence Section

b6  
b7C  
b7E

**(U) SUPERSESSION INFORMATION**

(U) Document supersedes (See Appendix C).

(U) Document is a new publication; no previous versions available.

**(U) CAVEAT**

(U) This policy implementation guide is solely for the purpose of internal Federal Bureau of Investigation (FBI) guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice (DOJ) and the FBI.

(U) ~~LAW ENFORCEMENT SENSITIVE~~: The information marked (U//~~LES~~) in this document is the property of the FBI and is for internal use within the FBI only. Distribution outside the FBI without Operational Technology Division authorization is prohibited. Precautions must be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the ~~LES~~ caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked ~~LES~~ on a Web site on an unclassified network.

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

## (U) Table of Contents

- 1. (U) Introduction ..... 1
  - 1.1. (U) Purpose ..... 1
  - 1.2. (U) Background ..... 1
  - 1.3. (U) Scope ..... 2
  - 1.4. (U) [Redacted] DE ..... 2
    - 1.4.1. (U) DE [Redacted] ..... 2
    - 1.4.2. (U) Reviews or Examinations of DE [Redacted] ..... 3
- 2. (U) Roles and Responsibilities..... 5
  - 2.1. (U) Digital Evidence Roles..... 5
  - 2.2. (U) Digital Evidence Responsibilities..... 8
    - 2.2.1. (U) All FBI Personnel Who Handle, Content Review, or Process DE..... 8
    - 2.2.2. (U//~~FOUO~~) Investigative Personnel and Analysts..... 8
    - 2.2.3. (U) FBI Headquarters (FBIHQ) ..... 10
    - 2.2.4. (U) FBI Field Offices ..... 12
- 3. (U) Policies and Procedures ..... 14
  - 3.1. (U) Digital Evidence Handling ..... 14
    - 3.1.1. (U) Personnel Authorized to Handle DE..... 14
    - 3.1.2. (U) Pre-Search Considerations ..... 14
  - 3.2. (U) Digital Evidence Processing..... 19
    - 3.2.1. (U) Imaging ..... 19
    - 3.2.2. (U) [Redacted] ..... 20
    - 3.2.3. (U) [Redacted] ..... 20
    - 3.2.4. (U) Content Review ..... 20
    - 3.2.5. (U) Documenting Review of DE ..... 22
    - 3.2.6. (U) Copies..... 28
    - 3.2.7. (U) Approved Tools..... 34
    - 3.2.8. (U) [Redacted] ..... 35
    - 3.2.9. (U) [Redacted] ..... 35

b3  
b7E

b7E

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- 3.2.10. (U) Service Requests in Support of Administrative or Civil Matters..... 36
- 3.2.11. (U) Re-examinations ..... 37
- 3.2.12. (U) Advanced Technical Analysis ..... 39
- 3.2.13. (U) Assigning Requests to Examiners and DE Backlog Definition..... 40
- 3.3. (U) Testifying Regarding DE Processing ..... 41
  - 3.3.1. (U) CART FEs, FAVIAU examiners, CS-FOs and OTD/DFAS Technical Experts..... 41
  - 3.3.2. (U) DExTs and CART Techs..... 41
- 3.4. (U) Seeking Legal Advice..... 41
- 4. (U) Summary of Legal Authorities..... 42
- 5. (U) Recordkeeping Requirements ..... 43
  - 5.1. (U/~~FOUO~~) FBI Central Recordkeeping System..... 43
  - 5.2. (U) Additional Guidance on Recordkeeping and Forms Use..... 43

b7E

**(U) List of Figures**

- Figure 1: (U/~~FOUO~~): [redacted] ..... 5
- Figure 2 : (U/~~FOUO~~) DE Copies ..... 28
- Figure 3: (U/~~FOUO~~) [redacted] ..... D-2

b7E

**(U) List of Appendices**

- Appendix A: (U) Sources of Additional Information ..... A-1
- Appendix B: (U) Contact Information ..... B-1
- Appendix C: (U) Superseded MIOG Sections and Documents ..... C-1
- Appendix D: (U) Definitions and Acronyms ..... D-1
- Appendix E: (U/~~FOUO~~) Examination Of FBI Evidence [redacted] ..... E-1

b7E

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

# 1. (U) Introduction

## 1.1. (U) Purpose

(U//~~FOUO~~) This policy implementation guide (PG) establishes and consolidates the policy and procedures for the proper handling, reviewing, and processing of digital evidence (DE) for the Federal Bureau of Investigation (FBI), whether it is seized, received, or otherwise legally obtained. Digital evidence is data that is obtained with the intent to assist in proving or disproving a matter at issue in a case or investigation and is stored or transmitted in binary form. Digital evidence includes binary data stored on magnetic, optical or mechanical storage devices including but not limited to integrated circuits, microcontrollers, chips, tapes, computers, cell phones, compact discs/digital video discs (CDs/DVDs), flash drives, random access memory (RAM), magneto optical cartridges, USB micro storage devices (commonly known as "thumb drives"), digital video recorders (DVRs) or other electronic devices that store or process data digitally. The Operational Technology Division (OTD)/Digital Forensics and Analysis Section (DFAS) is responsible for the FBI's DE Program and establishing DE policy.

b7E

(U//~~FOUO~~) Except as noted below, this PG applies to all DE obtained or acquired by the FBI in connection with an investigation.

(U//~~FOUO~~) This PG does not apply to digital evidence obtained through:

- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) Information originally obtained in a non-digital format that was later converted to digital form to facilitate storage, retrieval or search/query.
- (U//~~FOUO~~) Specialized evidentiary information or data collections regulated by another PG (e.g., digital fingerprints, digital DNA profile databases).
- (U//~~FOUO~~) Business, transactional, or other records obtained through a subpoena [Redacted] that were provided in digital form.

(U//~~FOUO~~) However, if exempted records are later submitted for a forensic examination, this PG would apply to the examination of said materials.

## 1.2. (U) Background

(U//~~FOUO~~) As computer technology has advanced over time, digital devices have become universally used to include individuals, groups, or organizations violating federal law [Redacted] DE is ever-present in FBI investigations and operations. All personnel that encounter DE must understand how to properly handle, review, and process DE to avoid damaging the integrity of the evidence or violating the Constitutional rights of a person during the course of an investigation.

b7E

(U//~~FOUO~~) The FBI requires that DE be seized, searched, stored, copied, processed, reviewed, examined, analyzed, presented, and disposed of in a scientifically proven and legally defensible manner to maximize its integrity, authenticity, probative value, and

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

evidentiary reliability, and to facilitate the DE's admissibility at trial or other adjudicative proceeding. DE is malleable and can be easily altered or destroyed (e.g., by viewing or copying files without following the proper procedures or by variance in temperature or exposure to heat or magnetic fields). Utilizing properly trained personnel, established procedures, approved tools, and an appropriate quality assurance (QA) program maximizes the reliability and integrity of DE for the purpose of authentication and presentation in court, as well as for investigative [redacted]

b7E

**I.3. (U) Scope**

(U//~~FOUO~~) This PG applies to all personnel working for or with the FBI, including FBI employees, contractors, detailees and task force personnel assigned to FBI field offices, FBI headquarters (FBIHQ) divisions, legal attaché (Legat) offices, regional computer forensics laboratories (RCFLs), and joint task forces (JTFs) who encounter, handle, review, or process DE.

(U//~~FOUO/LES~~) This PG addresses the handling, processing, and content review of DE. Handling includes procedures related to on-scene search and seizure, transportation and storage, evidence intake, and shipping. Processing of DE includes detailed procedures related to on-scene preview, imaging, memory capture, content review, search, extraction, report preparation, and advanced technical analysis [redacted]

b7E

[redacted]

[redacted] Content review is the viewing of the [redacted] digital evidence

container(s) in accordance with the scope of legal authority.

**I.4. (U) [redacted]**

(U//~~FOUO~~) Unless expressly stated otherwise, this PG applies equally to criminal [redacted] [redacted] FBI personnel should coordinate questions concerning legal authority required [redacted] with their chief division counsel (CDC) or assistant division counsel (ADC) or with the Office of the General Counsel, [redacted]

**I.4.1. (U) [redacted]**

(U//~~FOUO~~) [redacted]

b3  
b7E

(U//~~FOUO~~) [redacted]

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

~~(U//FOUO)~~ [Redacted]

b3  
b7E

**1.4.2. (U) Reviews or Examinations of DE** [Redacted]

~~(U//FOUO)~~ This section discusses some of the unique areas of concern raised when the FBI [Redacted]

**1.4.2.1. (U)** [Redacted]

b3  
b7E

~~(U//FOUO)~~ [Redacted]

~~(U//FOUO)~~ However, investigative personnel may review or analyze evidence seized under the authority of a criminal warrant or consent when the evidence at issue has been determined to be within the scope of the criminal warrant or consent pursuant to which it was seized. FBI personnel should not expand the search beyond the consent or criminal warrant's scope. FBI personnel should coordinate questions concerning their authority under this scenario with their servicing CDC/ADC and OGC [Redacted]

~~(U//FOUO)~~ In the event that the FBI [Redacted] need to conduct a search of criminally seized DE beyond the scope of the criminal warrant or consent, they should coordinate with their CDC/ADC and OGC [Redacted] to obtain additional legal authority,

[Redacted]

**1.4.2.1.1. (U) Use of Analytical Tools or Database Systems to Review or Examine DE**

~~(U//FOUO)~~ [Redacted]

b3  
b7E

The evidence must be tagged in some manner to permit its withdrawal from the holdings

[Redacted]

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

(U//~~FOUO~~) Before uploading DE seized [redacted]

[redacted]

b3  
b7E

1.4.2.2. (U [redacted])

(U//~~FOUO~~) Often during reviews or examinations of DE [redacted]

[redacted] (when providing technical assistance to the FBI) [redacted] may be employed in accordance with

the provisions of this PG. DOJ policy requires the approval of the deputy attorney general

[redacted] in the furtherance of a

criminal case. For more information please see [redacted]

[redacted]

1.4.2.2.1. (U//~~LES~~) [redacted]

[redacted]

b3  
b7E

(U//~~LES~~) During the course of [redacted]

[redacted]

(U//~~LES~~) [redacted]

[redacted]

(U//~~FOUO~~) When this circumstance applies, the case agent is responsible for notifying and coordinating with his CDC/ADC and OGC [redacted] To ensure appropriate disclosures are made, case agents must coordinate with the AUSA or DOJ Trial Attorney.

~~UNCLASSIFIED//FOUO/LES~~



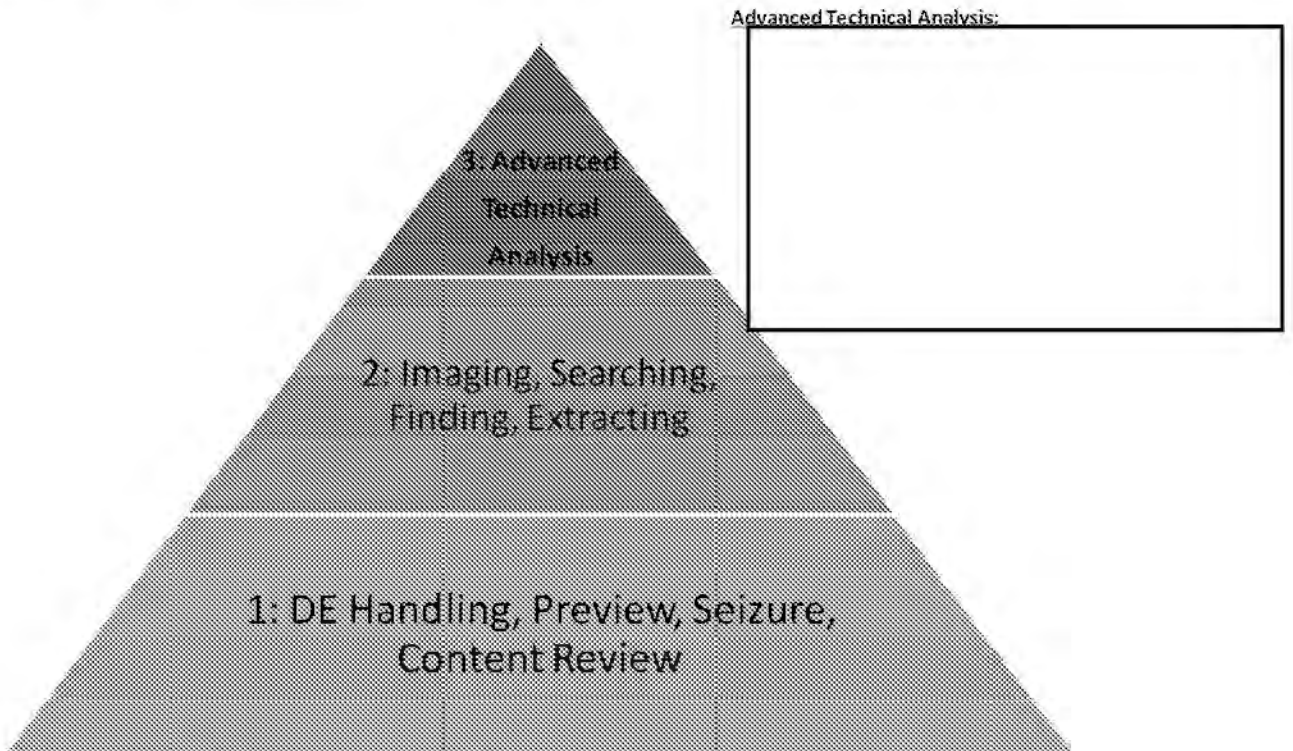
UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

## 2. (U) Roles and Responsibilities

### 2.1. (U) Digital Evidence Roles

(U//~~FOUO~~) The FBI's DE Program divides DE work functions into general categories or levels based upon the type and complexity of work performed at each level, and the training and experience required of FBI personnel to competently perform the duties at each level. Each category of work depicted in Figure 1, below, has its own set of training and procedural requirements. The first tiered category requires less training and fewer procedures, while the upper two categories require more training and expertise as well as more involved procedures.



b7E

Figure 1: (U//~~FOUO~~) [Redacted]

(U//~~FOUO~~) The first tiered category on the pyramid represents the broad population of FBI personnel who, with minimal training, are authorized to handle, preview, seize, and/or review DE content. The second tiered category represents a smaller population of FBI personnel who have been trained to the technician level, which allows them to image, search, find, and extract DE. The FBI considers the search and find function an investigative, as opposed to forensic, process, but the imaging and extraction remain forensic processes that require training to forensic standards. The third tiered category represents the smallest population of FBI personnel who have received extensive training and possess the requisite experience necessary to complete the most technically complex DE examinations and analysis.

(U//~~FOUO~~) As used throughout this PG, references to training and certification refer to training and certification provided, approved, or recognized by the OTD, Digital Forensics and Analysis Section (DFAS). Similarly, unless expressly stated to the

UNCLASSIFIED//~~FOUO~~/LES

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

contrary, personnel authorized in any tier must comply with the OTD/DFAS approved training, follow OTD/DFAS approved policies, procedures, and protocols, and only use tools and/or devices in accordance with this PG and OTD/DFAS policies.

(U//~~FOUO~~) Level 1: The handling of DE for seizure or evidence control purposes, and/or the preview or review of DE content for investigative  can be performed by personnel such as evidence control technicians (ECTs), special agents (SAs) and analysts with proper training and approved tools under procedures approved by OTD/DFAS.

b7E

(U//~~FOUO~~) Level 2: DE technician level work can be performed by the following personnel (who can also perform Level 1 work) under procedures approved by OTD/DFAS:

- (U//~~FOUO~~) Computer Analysis and Response Team (CART) technician (CART tech): Personnel trained and certified to forensically copy or image DE.
- (U//~~FOUO~~) Digital extraction technician (DEXT): Personnel trained and certified to copy or image DE and perform simple search/find/extract processes on copies of DE.
- (U//~~FOUO~~) Field Audio Video Program (FAVP) forensic analysts (FAs): Personnel trained and certified to perform basic forensic functions related to audio and video DE.

(U//~~FOUO~~) Level 3: Advanced technical analysis is conducted by the following personnel (who can also perform Level 2 and Level 1 work):

- (U//~~FOUO~~) CART forensic examiner (CART FE): Headquarters or field personnel, typically assigned full time to DE work, who are trained, equipped, and certified to copy or image DE, search/find DE, extract data from DE, and provide opinions related to DE, computer forensics, computer or electronic device operations, and other related fields, as their expertise and training permit.
- (U//~~FOUO~~) CART trainees: Prior to achieving CART FE certification, personnel seeking experience and proficiency in the CART Program are considered trainees. While in trainee status, these personnel are authorized to perform forensic tasks under the supervision of a certified CART FE:
  - (U//~~FOUO~~) CART on-the-job trainee (OJT): Personnel identified by field office management to participate in training with a commitment toward becoming certified CART FEs.
  - (U//~~FOUO~~) CART forensic examiner trainee (FET): Personnel assigned to work 100% of their time toward CART FE certification. Typically, these are trainees hired into information technology specialist – forensic examiner (ITS-FE) positions. These may also be CART OJTs who are near the end of their training and have committed 100% of their time to CART FE work.
- (U//~~FOUO~~) Regional Computer Forensics Laboratory (RCFL) associate examiner: Former certified CART FEs from an agency participating in the RCFL

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

program who have completed their commitment to the RCFL and returned to their home agency, and who continue a relationship with the RCFL to maintain certification and training. When serving in this role, RCFL associate examiners must continue to be impartial forensic scientists, and are prohibited from conducting investigative activities.

b7E

- (U//~~FOUO~~) Computer scientist-field operations (CS-FO): The CS-FOs are experienced computer scientists who work as integral members of an investigative team supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis [redacted]

[redacted]

The

CS-FO is not authorized to engage in [redacted]. Additionally, because CS-FOs are part of the investigative team, they are prohibited from performing forensic examinations of DE.

- (U//~~FOUO~~) OTD/DFAS engineer/analyst/forensic examiner: DFAS [redacted]

b7E

[redacted]

(U) Table 1 depicts the various DE personnel roles and the functions that they are authorized to perform with the proper training and certification.

Functions	Investigative Personnel	CART Tech	DEXT	Field CART FEs, CS-FOs, DFAS
(U) DE Handling				
Preview	✓	✓	✓	✓
Seizure				
Content Review				
(U) Imaging		✓	✓	✓

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//**FOUO**/LES~~  
 (U) Digital Evidence Policy Implementation Guide

(U) Search/ Find/ Extract			<del>UNCLASSIFIED//<b>FOUO</b>/LES</del>	<del>UNCLASSIFIED//<b>FOUO</b>/LES</del>
(U) Advanced Technical Analysis				<del>UNCLASSIFIED//<b>FOUO</b>/LES</del>
(U) Role-specific SOPs				

Table 1: (U) Roles and Responsibilities

**2.2. (U) Digital Evidence Responsibilities**

**2.2.1. (U) All FBI Personnel Who Handle, Content Review, or Process DE**

(U//~~FOUO~~) All FBI personnel who handle, content review, or process DE, in addition to the specific responsibilities delineated below due to their position, are responsible for:

- (U//~~FOUO~~) Understanding and complying with the legal authority as it relates to the DE processed, handled, or content reviewed.
- (U//~~FOUO~~) Handling, content reviewing, and processing DE and documenting those actions in accordance with this PG, other applicable OTD/DFAS policies and procedures, and applicable QA standards.
- (U//~~FOUO~~) Ensuring all DE is handled, content reviewed and marked in accordance with [redacted]

[redacted]

- (U//~~FOUO~~) Ensuring that all DE is handled, stored, content reviewed and marked in accordance with FBI dissemination marking policy (e.g., grand jury [GJ] material and tax information) and OTD/DFAS policy (e.g., child pornography materia [redacted])
- (U//~~FOUO~~) Maintaining the chain of custody of all DE.
- (U//~~FOUO~~) Disseminating DE only in accordance with this PG.
- (U//~~FOUO~~) Providing testimony, as required, in any legal proceedings in accordance with this PG.

**2.2.2. (U//~~FOUO~~) Investigative Personnel and Analysts**

(U//~~FOUO~~) Investigative personnel handling, processing, and performing content review of DE (typically special agents and analysts) are responsible for:

- (U//~~FOUO~~) Conducting and/or directing the preview and/or review of DE content.

b3  
b7E

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) Using approved DE tools for which approved training has been completed.

**2.2.2.1. (U//~~FOUO~~) CART Techs**

(U//~~FOUO~~) CART techs are responsible for imaging DE using only approved tools and techniques.

**2.2.2.2. (U//~~FOUO~~) DEXTs**

(U//~~FOUO~~) DEXTs are responsible for:

- (U//~~FOUO~~) Processing images of DE to search, find, and extract items of interest from the DE within the defined scope of legal authority.
- (U//~~FOUO~~) If certified, and upon request, performing the DE functions authorized for CART techs as described above. When performing these functions, the DEXT must follow the protocols and limitations prescribed for that role.

**2.2.2.3. (U//~~FOUO~~) CART FEs**

(U//~~FOUO~~) CART FEs are responsible for:

- (U//~~FOUO~~) Upon request, performing any DE functions authorized for a CART tech or DEXT. When performing those functions, the CART FE must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Conducting and/or directing the forensic examination of DE including:
  - (U//~~FOUO~~) [Redacted]
  - (U//~~FOUO~~) [Redacted]
  - (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted] in accordance with all provisions of this PG and relevant OTD/DFAS quality assurance (QA) requirements.
- (U//~~FOUO~~) Providing [Redacted] execution of search warrants and preview/examinations of complex computer systems or situations.
- (U//~~FOUO~~) Providing on-scene consultation with investigators and prosecutors in the development of strategies for the seizure or on-scene imaging of digital media and equipment.

b7E

**2.2.2.3.1. (U//~~FOUO~~) Field Audio Video Program (FAVP) Forensic Analysts (FA)**

(U//~~FOUO~~) FAVP FAs are responsible for:

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) Conducting and/or directing the content review of audio and video DE.

- (U//~~FOUO~~) [Redacted]

- (U//~~FOUO~~) [Redacted]

- (U//~~FOUO~~) [Redacted]

2.2.2.4. (U//~~FOUO~~) Computer Scientists-Field Operations (CS-FOs)

(U) CS-FOs are responsible for:

- (U//~~FOUO~~) Performing any function carried out by a CART tech or DEX T related to DE. When performing those functions, the CS-FO must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Supporting investigative [Redacted] personnel with computer science expertise in support of cases or investigations (e.g., assistance with interviews and searches), as authorized by this PG.
- (U//~~FOUO~~) Using [Redacted] for all activities.

b7E

2.2.2.5. (U) RCFL Personnel

(U//~~FOUO~~) RCFL personnel are responsible for performing duties as outlined in the MOU between their agency and the FBI.

2.2.3. (U) FBI Headquarters (FBIHQ)

2.2.3.1. (U) FBIHQ Operational Divisions

(U//~~FOUO~~) The executive management of FBIHQ operational divisions is responsible for:

- (U//~~FOUO~~) Communicating the DE policies, procedures, and guidance set forth in this PG to personnel within their mission area by posting a link to this PG on their respective division websites.
- (U//~~FOUO~~) Ensuring compliance with all matters identified in this PG.
- (U//~~FOUO~~) Monitoring compliance and reporting non-compliance in their respective mission areas in accordance with DIOG guidance on compliance and non-compliance.

2.2.3.1.I. (U) FBIHQ Operational Divisions Routinely Handling DE

2.2.3.1.1.1. (U//~~FOUO~~) [Redacted]

b7E

(U//~~FOUO~~) [Redacted] DEX T personnel who are responsible for:

- (U//~~FOUO~~) Serving as [Redacted]

UNCLASSIFIED//~~FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (~~U//FOUO~~) [Redacted]
- (~~U//FOUO~~) Following FBI DE protocols applicable to DEXTs, as specified in this PG.
- (~~U//FOUO~~) [Redacted]
- (~~U//FOUO~~) At the request of the case agent or headquarters program management unit and with the approval of OGD [Redacted]
- (~~U//FOUO~~) At the request of the case agent or headquarters program management unit and with the approval of [Redacted]
- (~~U//FOUO~~) [Redacted]

b3  
b7E

**2.2.3.1.1.2. (~~U//FOUO~~) CID/Violent Crimes Against Children (VCAC) Section**

(~~U//FOUO~~) Criminal Investigative Division/Violent Crimes Against Children (VCAC) Section provides [Redacted] abuse and exploitation to children which may be investigated under the jurisdiction and authority of the FBI. The OTD/DFAS/Digital Analysis and Research Center (DARC)

[Redacted]

(~~U//FOUO~~) VCAC manages several programs including the Innocent Images National Initiative (IINI).

(~~U//FOUO~~) VCAC is responsible for establishing guidance for the handling of child pornography contraband for the IINI program.

**2.2.3.1.1.3. (~~U//FOUO~~) OTD/Digital Forensics and Analysis Section**

(~~U//FOUO~~) The Operational Technology Division (OTD)/Digital Forensics and Analysis Section (DFAS), in coordination with other FBI divisions, is responsible for:

- (~~U//FOUO~~) Creating and maintaining policy and procedures for the FBI's DE Program, wherein such policy and procedures ensure compliance with governing legal authorities, with regard to the manner in which DE is searched, processed, stored, accessed, used, and disseminated, to maintain the integrity of the evidence and to ensure adherence to applicable privacy and civil liberties laws, policies, and regulations.

b7E

b7E

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) Overseeing the FBI DE field subprograms, which include:
  - (U//~~FOUO~~) Computer Analysis Response Team (CART) Forensic Examiner (FE) subprogram.
  - (U//~~FOUO~~) Digital Extraction Technician (DEXT) subprogram.
  - (U//~~FOUO~~) Computer Scientist - Field Operations (CS-FO) subprogram.
  - (U//~~FOUO~~) Field Audio Video Program (FAVP) subprogram.
  - (U//~~FOUO~~) FBI Digital Evidence Laboratory (DEL) and Quality Assurance Program for DE.
  - (U//~~FOUO~~) Regional Computer Forensics Laboratory (RCFL) subprogram.
- (U//~~FOUO~~) Providing the following capabilities and resources:
  - (U//~~FOUO~~) Trained examiners who provide DE acquisition, preservation, processing, review, examination, presentation, and testimony.
  - (U//~~FOUO~~) Trained personnel to provide advanced analysis capabilities for DE including:
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
    - (U//~~FOUO~~)
  - (U//~~FOUO~~) Training, certification, and proficiency testing for personnel who process DE.
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)
  - (U//~~FOUO~~)

b7E

b7E

**2.2.4. (U) FBI Field Offices**

**2.2.4.1. (U) FBI Field Office Management**

(U//~~FOUO~~) FBI field office management (i.e., Assistant Director in Charge (ADIC), Special Agent in Charge (SAC), Assistant Special Agent in Charge (ASAC), and Supervisory Special Agent (SSA)) is responsible for:

- (U//~~FOUO~~) Promoting and communicating DE policy.
- (U//~~FOUO~~) Ensuring compliance with this PG.

~~UNCLASSIFIED//FOUO/LES~~



~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- ~~(U//FOUO)~~ Monitoring compliance and reporting non-compliance in their respective mission area in accordance with the DIOG.

**2.2.4.2. ~~(U//FOUO)~~ Evidence Control Technicians**

~~(U//FOUO)~~ With regard to DE, evidence control technicians (ECTs) are responsible for:

- ~~(U//FOUO)~~ Properly storing, protecting, and tracking DE, as described below in section 3.
- ~~(U//FOUO)~~ Properly packaging and shipping DE, as necessary, as described below in Section 3.1.

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

### 3. (U) Policies and Procedures

#### 3.1. (U//~~FOUO~~) Forensic Program Compliance within the FBI

(U//~~FOUO~~) All DE forensic programs conducted in FBI space must fully comply with FBI forensic policies, procedures and requirements as set by OTD/DFAS, and must be under the direct and immediate control and supervision of the OTD/DFAS unless prior written concurrence of the AD, OTD or his/her designee is obtained.

#### 3.2. (U) Digital Evidence Handling

b7E

(U//~~FOUO~~) This section sets forth policy related to the handling of DE for all personnel working for or with the FBI, including investigative and technical personnel, ECTs, CART techs, DEXTs, CART FEs, CSs, DFAS technical experts, FAVP FAs, RCFL personnel, and other personnel who encounter DE.

##### 3.2.1. (U) Personnel Authorized to Handle DE

(U//~~FOUO~~) FBI personnel must handle DE for seizure, transportation, and storage, as with any evidence, pursuant to requirements specified in the [redacted]

[redacted] FBI personnel must also be trained and/or certified in accordance with OTD/DFAS policy and procedures and follow all applicable protocols before processing DE, including making copies or images of DE.

##### 3.2.2. (U) Pre-Search Considerations

###### 3.2.2.1. (U//~~FOUO~~) Legal Review

(U//~~FOUO~~) FBIHQ and field office personnel must ensure that the seizure and examination of DE strictly adheres to the procedures listed in this PG. Personnel handling DE may request chief division counsel (CDC) or Office of the General Counsel (OGC) legal review of DE-related search warrants and subpoenas as applicable [redacted]

[redacted] Field office CDCs or OGC are also available to provide assistance in drafting search warrants or subpoenas for seizing or searching DE.

b3  
b7E

###### 3.2.2.2. (U) Timeframe for Warrants Involving DE

(U//~~FOUO~~) Although Rule 41(e)(2)(A) does not place a specific time limit on off-site copying or review of electronic storage media, some judicial districts place specific limits on the amount of time permitted for off-site review. The case agent should consult with the CDC or OGC [redacted] if there are questions pertaining to time permitted for examination.

b7E

###### 3.2.2.3. (U) Consent Searches for DE

(U//~~FOUO~~) Whenever possible, written consent must be obtained from the consenting party and documented on a form FD-26, Consent to Search or FD-941, Consent to Search Computers. However, this does not mean that oral consent is not valid. The case agent must, when relying on oral consent, appropriately document the oral consent on an FD-302.

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

~~(U//FOUO)~~ In consent cases, case agents should ensure that [redacted]

b7E

[redacted]

~~(U//FOUO)~~ If consent is terminated, the case agent must immediately contact personnel processing the DE and notify them of the revocation of consent. Once consent is withdrawn, any imaging not completed must be terminated. The case agent should also promptly contact the CDC or OGC for advice on how to proceed with searching any completed or partial images made prior to revocation.

**3.2.2.4. (U) Requesting Local Field Office Assistance**

~~(U//FOUO)~~ DExT personnel may provide on-scene support for routine DE handling and processing in accordance with the procedures outlined in this PG. DExT support should be requested by coordinating with the appropriate squad supervisor(s).

~~(U//FOUO)~~ FBI case agents who require search and seizure assistance and/or examination of DE must contact their field office CART supervisor, CART coordinator, or other CART personnel.

~~(U//FOUO)~~ Case agents must submit service requests for DE assistance within field offices via electronic communication (EC) to CART personnel. All service requests must include:

- ~~(U//FOUO)~~ Case ID – the universal case file number (UCFN)
- ~~(U//FOUO)~~ Case title
- ~~(U//FOUO)~~ Specific request
- ~~(U//FOUO)~~ Description of legal authority
- ~~(U//FOUO)~~ "CART Operations" in the synopsis field of ECs

**3.2.2.5. (U) Requests Involving Multiple Locations**

~~(U//FOUO)~~ Case agents must coordinate in advance any DE service requests involving multiple field offices with the CART supervisor or coordinator in their division as well as with the other applicable divisions. If further assistance is required, the CART supervisor or coordinator should coordinate with the OTD/DFAS/Forensic Operations Unit (FOU).

b7E

**3.2.2.5.1. (U) Providing [redacted] Technical Assistance in DE Cases**

~~(U//FOUO)~~ The FBI provides DE forensic services through [redacted]

[redacted]

~~(U//FOUO)~~ Pursuant to 28 CFR § 0.85(g) and the DIOG, the FBI Digital Evidence Laboratory (DEL) and RCFLs are authorized to provide, without cost, technical and scientific assistance, including expert testimony in federal or local courts, to all duly constituted law enforcement agencies, other organizational units of the Department of Justice, and other federal agencies. Under this authority, the FBI DEL and RCFLs may

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

also provide technical and scientific assistance, including expert testimony [redacted]

b7E

(U//~~FOUO~~) The FBI DEL consists of the following units, all of which are components of the OTD/DFAS: Forensic Operations Unit (FOU), Forensic Analysis Unit (FAU), Forensic Support Unit (FSU), the RCFL National Program Office (RCFL NPO) and the Forensic Audio, Video and Image Analysis Unit (FAVIAU). The DFAS forensic examiners (see Section 2.1, Digital Evidence Roles) that comprise the DEL consist of CART-FEs, CART-FETs and FAVIAU examiners.

(U//~~FOUO~~) The following OTD/DFAS units are not components of the FBI DEL: the [redacted]

[redacted] Field office CART assets and laboratories are not part of the FBI DEL. Although the RCFLs follow the FBI DEL's quality program, each RCFL is an individually accredited lab independent from each other and the FBI DEL.

(U//~~FOUO~~) In accordance with the DIOG, the provision of routine forensic analysis and examination of submitted evidence is considered technical and scientific support. Routine forensic analysis and examination of evidence performed by the FBI DEL, RCFLs, or CART personnel in field offices is not considered expert investigative assistance (as defined in the DIOG), even if those components are providing expert witness testimony in connection with the support.

**3.2.2.5.2. (U) Expert Investigative Assistance in DE Cases**

(U//~~FOUO~~) FBI personnel, particularly approving officials, must be careful to review requests for assistance with DE [redacted]

[redacted] see the DIOG.

(U//~~FOUO~~) During the course of providing either [redacted]

b3  
b7E

**3.2.2.5.3. (U) Requests for [redacted] the DEL or RCFLs**

(U//~~FOUO~~) FBI components that are not part of the FBI DEL or RCFLs, may only provide technical assistance pursuant to Attorney General Order 2954-2008 and the DIOG.

(U//~~FOUO~~) Requests for [redacted] than the FBI DEL or RCFLs must be processed and handled in accordance with the DIOG [redacted] as applicable.

UNCLASSIFIED//~~FOUO~~/LES

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

(U//~~FOUO~~) Requests for RCFL DE support from [redacted] will be handled in accordance with the applicable MOU governing the RCFL concerned, provided the MOU is not inconsistent with this PG.

b7E

(U//~~FOUO~~) Because the authority to provide this support is under 28 CFR § 0.85(g), a federal nexus is not required, and such services must be provided at no cost to the requesting agency. RCFLs may not provide [redacted]

[redacted] All such requests must be referred to the FBI DEL.

(U//~~FOUO~~) [redacted]

[redacted]

b3  
b7E

(U//~~FOUO~~) The processing of the DE and dissemination of materials and information pertaining to the technical assistance by the RCFLs must be in accordance with this PG.

(U//~~FOUO~~) RCFLs will track all service requests, and disseminate information to

[redacted]

3.2.2.5.5. (U//~~FOUO~~) Requests for the Use of [redacted]

(U//~~FOUO~~) Requests for the use of FBI or other [redacted] in criminal cases require the review and recommendation of OGC [redacted] and the DOJ's Criminal Division, as well as approval by the Deputy Attorney General. See Deputy Attorney General Memorandum [redacted]

(U//~~FOUO~~) Requests for the use of [redacted]

[redacted]

b7E

(U//~~FOUO~~) The dissemination of [redacted]

[redacted]

(U//~~FOUO~~) Prior to approval of a request, assurances must be obtained from the requesting agency, as well as the chief prosecutor for the applicable jurisdiction, that representatives of the requesting agency will not disclose [redacted] in court, through pre-trial motions, discovery, or other means, or through any federal or state freedom of information legislation or similar law, or otherwise disclose to the media or public, without the prior written consent of the Director, FBI, or his designee. The requesting agency and the chief prosecutorial official will also acknowledge they are receiving the requested technical assistance expressly conditioned on the fact that they are subject to the nondisclosure provisions governing FBI information as set forth in 28 CFR § 16.22, 16.24, and 16.26, as well FBI policy on the protection, use, and

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide



b7E

**3.2.2.6. (U) DE and Evidence Control Facilities (ECFs)**

(U//~~FOUO~~) The original DE seized at a search site must be securely transported to the FBI field office or RCFL site and, after processing and examination, placed, as appropriate, in an FBI or RCFL evidence control facility (ECF). [redacted] provides additional guidance and requirements.

**3.2.2.7. (U) DE Storage**

(U//~~FOUO~~) DE must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious change (e.g., DE must be sealed and protected from heat and light for preservation).

**3.2.2.8. (U) Shipping DE**

(U//~~FOUO~~) Shipping of DE from field offices to FBIHQ or RCFLs must be handled through an FBI ECF.

**3.2.2.9. (U) Shipping DE to CART**

(U//~~FOUO~~) When it has been determined that DE needs to be shipped either to another field office CART FE or to the OTD/DFAS, the DE must be processed through the field office's ECT. The ECT must ensure that the DE is packaged securely and that proper chain-of-custody procedures are followed. For assistance in packing DE for shipping, the case agent should contact the ECT in his or her field office.

b7E

(U//~~FOUO~~) The DE must be accompanied by an EC requesting examination as described in the [redacted]

**3.2.2.10. (U) Transferring a Working Copy of FBI DE** [redacted]

(U//~~FOUO~~) Case agents may submit working copies [redacted] Submission may be accomplished by completing a transmission request EC in the FBI's Central Recordkeeping System, and providing a working copy of the DE [redacted]

b7E

**3.3. (U) Digital Evidence Processing**

**3.3.1. (U) Imaging**

(U//~~FOUO~~) Imaging is the act of making [redacted] copy of the original DE to serve as an accurate reproduction of the original DE. Imaging must only be performed by certified DE personnel. Certified DE personnel (i.e., CART FEs, CART techs, DEXTs, and FAVP FAs) must follow standard CART procedures and QA requirements when imaging DE.

b7E

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

Specific procedures for imaging digital media are detailed in the [redacted]

3.3.2. (U) [redacted]

(U//~~FOUO~~) [redacted]

b7E

3.3.3. (U) [redacted]

(U//~~FOUO~~) [redacted]

b7E

3.3.3.1. (U) [redacted]

(U//~~FOUO~~) [redacted]

b7E

3.3.4. (U) Content Review

(U//~~FOUO~~) Investigative personnel can review DE for content [redacted]

3.3.4.1. (U) Scope and the Content Review

(U//~~FOUO~~) When searching DE pursuant to legal authority, an agent is authorized to seize only items specified in and responsive to the authority, absent an independent legal basis under which materials can be seized or retained.<sup>1</sup>

<sup>1</sup> (U//~~FOUO~~) [redacted]

b7E

UNCLASSIFIED//~~FOUO~~/LES

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

(U//~~FOUO~~) When searching DE pursuant to a criminal warrant, the warrant permits only a search for evidence of a specific, enumerated crime or crimes. Therefore, agents may only seize items that are within the bounds of the warrant, commonly known as the “scope” of the warrant.

(U//~~FOUO~~) When searching DE [redacted]

b7E

government must not exceed the scope authorized in the order. Questions regarding the authorized scope of a search should be directed to the servicing legal counsel (CDC/ADC or OGC).

**3.3.4.2. (U//~~FOUO~~) Scope Issues in Consent Cases**

(U//~~FOUO~~) Where consent is the legal authority for a search of DE, the ability of FBI personnel to review the digital evidence is bound by the terms of the consent provided. Consenting individuals may impose binding limitations on the areas or items that may be searched (e.g., specific rooms of a house, specific files or folders on a computer), either orally or on the written consent form.

**3.3.4.3. (U//~~FOUO~~) Search Protocols for DE**

(U//~~FOUO~~) All FBI personnel should observe all restrictions written into warrants, including local protocols attached to any warrants, when examining or reviewing DE. Questions regarding such provisions should be directed to the servicing legal counsel (CDC/ADC or OGC).

**3.3.4.4. (U) Self-service Kiosks**

(U//~~FOUO~~) Self-service kiosks are provided in most field offices. In addition, portable kiosk kits are available in many FBI resident agencies (RAs). When reasonably available, investigative personnel must use the kiosks to automatically process supported DE types.

(U//~~FOUO~~) [redacted] self-paced or hands on training is required.

b7E

(U//~~FOUO~~) [redacted] self-paced or hands on training is required.

**3.3.4.5. (U) When Content Review Is Authorized**

(U//~~FOUO~~) Content review is authorized only after DE is processed by authorized personnel (i.e., CART FEs, CART techs, DExTs, FAVP FAs), with the following exceptions:

- (U//~~FOUO~~) [redacted] approved by OTD/DFAS are utilized.

UNCLASSIFIED//~~FOUO~~/LES



UNCLASSIFIED//~~FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) Preview [redacted] OTD/DFAS policy.
- (U//~~FOUO~~) Preview by RCFLs or CART field office facilities in accordance with OTD/DFAS policy.
- (U//~~FOUO~~) The use of self-service kiosks for [redacted]

b7E

(U//~~FOUO~~) Content review of original DE is prohibited by those not trained and authorized by OTD.

3.3.4.6. (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted]

within the scope of the legal authority. The information obtained through [redacted]

[redacted]

3.3.4.7. (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted]

[redacted]

b7E

3.3.4.8. (U) Content Review Tools

(U//~~FOUO~~) All DE content review tools used by personnel working for or with the FBI or RCFL in their investigations must be legally obtained and used in accordance with the limitations in the licensing agreement, unless a legal exception applies (e.g., fair use or specific guidance in the legal authority) and the reviewer has coordinated with his or her CDC or OGC. If proprietary software is seized with the data, it may be used to view the data from the investigation.

3.3.5. (U) Documenting Review of DE

(U//~~FOUO~~) FBI personnel must document in a report all reviews and searches of DE from the point of the receipt of DE through completion of the search, including any identification of evidence that falls within the scope of the warrant [redacted]

[redacted] The documentation must be serialized to the investigative case file. Such documentation should identify, at a minimum, the general nature and manner in which the search of the media was conducted, major steps taken during the search, and forensic tools employed during the search.

b3  
b7E

(U//~~FOUO~~) Undocumented, "off-the-record" searches or reviews of DE are not permitted. The above documentation requirement does not apply to searches of results copies (see Section 3.2.6 for definition of [redacted])

UNCLASSIFIED//~~FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

~~(U//FOUO)~~ The four categories of reports are:

1. ~~(U//FOUO)~~ **Content Review Report:** Reports factual information resulting from the review of DE.
2. ~~(U//FOUO)~~ **DEXT Report:** Reports factual information [redacted]
3. ~~(U//FOUO)~~ **Report of Examination:** Reports the results of an examination performed by a certified examiner or other technical expert, usually with information regarding advanced analysis or opinions.
4. ~~(U//FOUO)~~ [redacted]

b3  
b7E

**3.3.5.1. (U) Content Review Report**

~~(U//FOUO)~~ A content review report is a factual report of investigative findings resulting from the review of original, master [redacted] of the DE. [redacted]

[redacted] The report details who performed the review, when it was performed, what was reviewed and found, and where it was found. A content review report may be documented by completing an FD-302. Content review reports must be serialized into the investigative file. A content review report must contain, at a minimum, the following information:

- ~~(U//FOUO)~~ Name and contact information of the reviewer.
- ~~(U//FOUO)~~ Description of the working copy reviewed, including case number and original DE description.
- ~~(U//FOUO)~~ The physical location of where the review was completed (i.e., location of the reviewer).
- ~~(U//FOUO)~~ The date of the report.
- ~~(U//FOUO)~~ The methodology and basis for their conclusion [redacted]

b7E

- ~~(U//FOUO)~~ Report of the responsive content found [redacted]

~~(U//FOUO)~~ All FBI personnel must also fully and officially document in the content review report any other individuals who provide substantive assistance (as opposed to purely technical assistance) [redacted]

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

[Redacted]

(U//~~FOUO~~) A content review report must contain only factual information and must not contain expert opinions related to the DE, other than those expressly permitted in this section and considered to be advanced technical analysis (see Section 2.1, figure 1).

b7E

**3.3.5.2. (U) DExT Report**

(U//~~FOUO~~) A DExT report is a factual report [Redacted] details who performed the work, when it was performed, what was reviewed and found, and where it was found. A DExT report may be documented by completing an FD-302 in accordance with [Redacted] prescribed by OTD/DFAS. DExT reports must be serialized into the investigative case file and must contain a minimum of the following information:

- (U//~~FOUO~~) Name and contact information of the DExT.
- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what they requested.
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).
- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) What was searched for and items found of investigative importance.
- (U//~~FOUO~~) Where the DExT is a case agent or investigator, and is reviewing or conducting [Redacted] on his/her own case evidence, the methodology and basis for his/her conclusion [Redacted]

b7E

[Redacted]

- (U//~~FOUO~~) Report of the responsive content found, including [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) What was targeted during the search and, if applicable, the order in which items were targeted [redacted]

b7E

(U//~~FOUO~~) All DExTs must also fully and officially document in the DExT report any other individuals who provide substantive assistance [redacted]

[redacted]

(U//~~FOUO~~) A DExT report must contain only factual information and must not contain expert opinions related to the DE, other than those expressly permitted in this section and considered to be advanced technical analysis (see section 2.1, figure 1).

(U//~~FOUO~~) If the DExT is an FBI investigative asset (agent or IA) and is conducting a content review and DExT review simultaneously in his or her own case, only a DExT report is required.

**3.3.5.3. (U) Report of Examination**

(U//~~FOUO~~) A report of examination is used to report the results [redacted] must be serialized into the investigative file. For CART FEs and forensic audio, video, and image examiners, the report of examination is required to be documented by completing all fields in an FBI [redacted]

b7E

by OTD/DFAS. Reports of examination must be serialized into the investigative case file and must contain a minimum of the following information:

- (U//~~FOUO~~) Name and contact information of the examiner.
- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what they requested.
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) Items searched for and items found of investigative importance.
- (U//~~FOUO~~) Report of the content found and [redacted]

[redacted]

- (U//~~FOUO~~) [redacted]

b7E

- (U//~~FOUO~~) What was targeted during the search, and, if applicable, the order in which items were targeted [redacted]

(U//~~FOUO~~) All FBI personnel must also fully and officially document in the report of examination whenever they receive substantive assistance from another individual during the examination or review process (not including "help desk" type assistance) [redacted]

[redacted]

(U//~~FOUO~~) Frequently, in the course of the investigation or during trial preparation, an examiner is asked to perform additional analysis of the DE. If this occurs, the examiner must file a supplemental report of examination, in accordance with the requirements above, to fully document the additional analysis requested in accordance with the Federal Rules of Criminal Procedure Rule 16.

3.3.5.4. (U [redacted]) Report

(U//~~FOUO~~) [redacted]

b7E

[redacted] reports must be serialized into the investigative case file and must contain the following information, if applicable:

- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what they requested.

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

- (~~U//FOUO~~) Description of the working copy processed, including case number and original DE description.
- (~~U//FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).
- (~~U//FOUO~~) The date of the report.
- (~~U//FOUO~~) List of procedures performed.
- (~~U//FOUO~~) What was searched for and items found of investigative importance.
- (~~U//FOUO~~) Report of the responsive content found, including [redacted]
- (~~U//FOUO~~) [redacted]
- (~~U//FOUO~~) What was targeted during the search, and, if applicable, the order in which items were targeted [redacted]

b7E

(~~U//FOUO~~) [redacted] report any other individuals who provide substantive assistance with the search/find/extraction (not including "help desk" type assistance) [redacted]. They must, at a minimum, include who assisted them during the processing, and if applicable, [redacted].

[redacted]

(~~U//FOUO~~) [redacted] report must contain only factual information and must not contain expert opinions related to the DE that would fall within the description of advanced technical analysis (see Section 2.1, figure 1).

**3.3.5.5. (U) Testifying Regarding Review of DE**

(~~U//FOUO~~) All personnel who handle DE must be prepared to testify concerning their findings and actions when seizing, handling, previewing, processing or reviewing DE. To facilitate accurate and complete testimony, documentation should be as detailed and extensive as necessary to recall all key aspects of their activity.

**3.3.5.6. (U) Retaining Results of Review**

(~~U//FOUO~~) After the DE is reviewed and/or examined, the set of data that is determined to be within the scope of the legal authority, relevant, and probative or exculpatory [redacted]

(~~U//FOUO~~) The results of a content review or examination [redacted]

b7E

UNCLASSIFIED//~~FOUO~~/LES

UNCLASSIFIED//~~FOUO~~/LES  
(U) Digital Evidence Policy Implementation Guide

[Redacted]

b7E

(U//~~FOUO~~) [Redacted] may be charged out by the case agent or any other party authorized by the case agent or case agent's chain of command.

3.3.6. (U) Copies

3.3.6.1. (U) Original DE vs. Master Copy vs. Working Copy [Redacted]

(U//~~FOUO~~) Digital evidence is unique in that it can, in many cases, be duplicated, or imaged, [Redacted]

[Redacted]

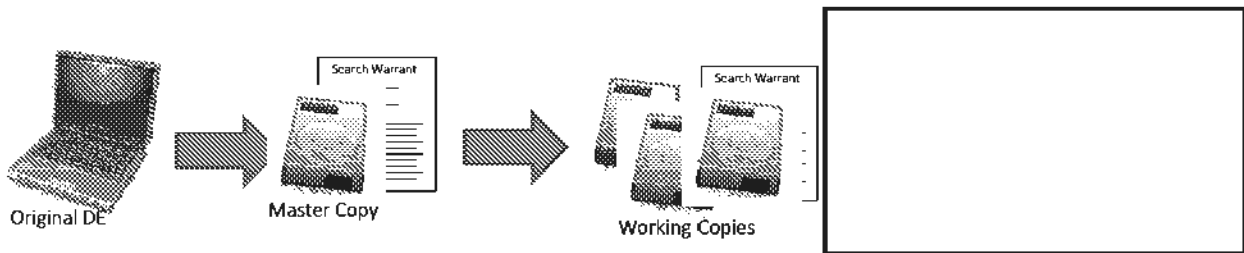


Table 2: (U//~~FOUO~~) DE Copies

(U//~~FOUO~~) **Original DE:** DE seized at a search scene or otherwise legally obtained and stored in an ECF. If another agency transmits image copies on digital media without the original device accompanying it, the original copy received is the original DE copy.

(U//~~FOUO~~) With the exception of contraband, items subject to statutory forfeiture, or instrumentalities of a crime, original DE may be returned to its rightful owners when all criminal proceedings have terminated and the CDC and AUSA/prosecutor have concurred. FBI personnel who are directed to return original DE prior to the conclusion of the trial should contact their CDC/ADC and OGC [Redacted] to ensure the proper stipulations are entered into to prevent challenges to authenticity after return of the media.

b7E

(U//~~FOUO~~) If the original DE contains contraband and the device was not forfeited, FBI personnel should not destroy the entire computer. Instead, the hard drive with the contraband should be removed and physically destroyed or contents removed in a manner that would preclude recovery.

(U//~~FOUO~~) **Master Copy:** The one required copy of DE that is stored on media to be retained and logged on a chain of custody [Redacted]

[Redacted]

(U//~~FOUO~~) **Working Copy:** [Redacted]

[Redacted]

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

b7E

[Redacted]

(U//~~FOUO~~)

[Redacted]

(U//~~FOUO~~) Restrictions on the tracking, dissemination and copying

[Redacted]

(U//~~FOUO~~) A copy of the original legal authority should be maintained with each working copy of the DE

[Redacted]

(U//~~FOUO~~)

[Redacted]

(U//~~FOUO~~) It is impossible to guarantee that

[Redacted]

**3.3.6.2. (U) Controlling Master Copies**

(U//~~FOUO~~) All master copies must be saved

[Redacted]

The original legal authority should be maintained with the master copy of the DE.

[Redacted]

(U//~~FOUO~~) Master Copies may be in two forms:

~~UNCLASSIFIED//FOUO/LES~~



~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

1. (U//~~FOUO~~) [Redacted]

b7E

2. (U//~~FOUO~~) [Redacted]

(U//~~FOUO~~) DE received in an ECF marked "master copy" must be assigned a new 1B number and given a new bar code (as applicable). In the description field, the ECT must include the original 1B number from which the DE was derived.

(U//~~FOUO~~) To ensure the integrity of the master copy and to prevent unauthorized copies from being disseminated, a master copy may only be charged out by DE personnel (i.e., CART FEs, CART techs, DExTs, and FAVP FAs).

**3.3.6.3. (U) Protecting Original Evidence or Master Copies**

(U//~~FOUO~~) Examinations or reviews of DE [Redacted]

**3.3.6.4. (U) Previews of Original Evidence**

(U//~~FOUO~~) In accordance with this PG, FBI personnel may conduct previews of original DE. In these cases, personnel may only conduct previews in accordance with procedures approved by OTD/DFAS [Redacted]

b7E

**3.3.6.5. (U) Disseminating [Redacted]**

(U//~~FOUO~~) [Redacted]

b3  
b7E

(U//~~FOUO~~) All FBI personnel receiving requests for [Redacted] must first look to the language of the relevant legal authority to determine whether dissemination of images or copies of DE is authorized by the court order for the stated purpose [Redacted]

[Redacted] FBI personnel may [Redacted] of that legal authority is included in the investigative case file and the provision of [Redacted] is documented as outlined in this section.

(U//~~FOUO~~) [Redacted] FBI personnel may, with OGC approval, disseminate [Redacted]

[Redacted] Such dissemination must be documented in the case file, as outlined in this section.

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

b7E

(U//~~FOUO~~) Only certified DE personnel (i.e., CART FEs, CART techs, DExTs, FAVP FAs, and OTD/DFAS Technical Experts) are allowed to make working copies. All copies made after (or from) the master copy [redacted] are required to be labeled as working copies.

(U//~~FOUO~~) Case agents must document the dissemination of working copies for tracking purposes in the case file. The case agent is required to document the case agent name, the number of working copies provided, recipient [redacted] UCFN or file number, evidence number, who requested the working copy, date, time, and the purpose for the working copy.

(U//~~FOUO~~) At the discretion of the case agent or case agent's supervisor, working copies may be submitted to an ECF for chain of custody tracking. In addition, the creation of the copy must be documented by the certified DE personnel in the examination file or DExT report, as applicable.

(U//~~FOUO~~) The case agent or FBIHO program manager may disseminate working copies of DE [redacted]

(U//~~FOUO~~) Because DE may contain contraband, personally identifiable information (PII), privileged or other legally protected information [redacted]

[redacted] must be appropriately marked [redacted]  
[redacted]

**3.3.6.5.1. (U) Copies of DE for US Attorneys**

(U//~~FOUO~~) Only [redacted] DE shall be provided to USAOs, unless otherwise authorized by this section. To obtain a working copy of DE, the USAO must request the copy in writing and explain the purpose of obtaining an image or working copy of the media. The request must include whether the USAO intends to further disseminate the media and, if so, to whom and for what purpose (e.g., to facilitate an examination or review by non-FBI personnel). In this event, the request should be handled [redacted] request or re-examination request (as outlined below). When reviewing such a request, FBI personnel may only comply when the following requirements have been met:

- (U//~~FOUO~~) The court order clearly authorizes such a dissemination under the relevant circumstances.
- (U//~~FOUO~~) The affiant advised the court that such dissemination would occur under the relevant circumstances in the underlying application for the legal authority.
- (U//~~FOUO~~) The case agent, in consultation with his or her CDC and OGC [redacted] determines such a dissemination is otherwise authorized.

b7E

(U//~~FOUO~~) Statements in search warrant affidavits or other applications or orders ambiguously authorizing the search and seizure of media by "government personnel," or similar language, are insufficient to meet the above requirements. For purposes of this section, "government personnel" does not include assistant United States attorneys, paralegals, or other personnel in a United States Attorney's Office, or trial attorneys, paralegals or other personnel in the Department of Justice that do not meet the definition

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

of a "federal law enforcement officer" authorized to execute a search warrant in Rule 41(a)(2)(C), Federal Rules of Criminal Procedure.

~~(U//FOUO)~~ The above restriction applies in circumstances where the judicial order authorizes the ultimate seizure of only a subset of data that exists on the media initially seized



b7E

~~(U//FOUO)~~ If FBI personnel are requested to provide such copies or otherwise facilitate such a transfer, they should inform the unit chief, Forensic Operations Unit, their squad supervisor, and their CDC. When personnel comply with such a request pursuant to the procedures described above, they must clearly document the details of the request and compliance with the above requirements in the agent's investigative case file and, if applicable, any digital evidence examination file. FBI personnel also must comply with any other relevant policy or procedures, such as the need to obtain the approval of the assistant director of OTD for a second examination of digital evidence.

**3.3.6.5.2. (U) Discovery Requests**

~~(U//FOUO)~~ FBI personnel handling DE must comply with defense demands for discovery.

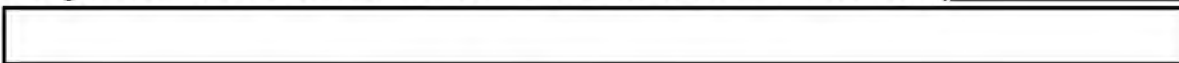
~~(U//FOUO)~~ The dissemination of working copies of DE to the defense to facilitate a discovery request is the case agent's responsibility. Prior to disseminating working copies for discovery, the case agent must protect PII, such as social security numbers, telephone numbers, bank account numbers, and medical records in accordance with federal law. The case agent must document the provision of discovery copies in the investigative case file.

**3.3.6.5.2.1. (U) Providing DE with No Contraband**

~~(U//FOUO)~~ The party requesting discovery must either supply suitable (size, quantity, and type) media for duplication of the data subject to disclosure or make arrangements for replacement of expended media.

~~(U//FOUO)~~ Copies prepared pursuant to a discovery request are typically [redacted] and must be verified as appropriate for disclosure by the case agent in consultation with the AUSA prior to release as discovery. In accordance with DOJ e-discovery guidance, the FBI is under no obligation to create [redacted]

[redacted] for discovery. The FBI does not provide this service due to the administrative burden and the inability [redacted]



b7E

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide



b7E

**3.3.6.5.2.2. (U) Requests for DE Containing Contraband**

(U//~~FOUO~~) When discovery is requested of material containing contraband (e.g., child pornography), the FBI must follow the procedures outlined in 18 U.S.C. § 3509(m) the "Adam Walsh Child Protection and Safety Act" (the Act). Pursuant to the Act, the FBI is required to make reasonable accommodations for the defense to have access to such material in an FBI facility specifically configured for these types of reviews, frequently called Adam Walsh rooms. Reasonable accommodations include access to the government-controlled facility during normal business hours, access to telephones, the Internet, and printers. Defense experts may make special, advanced arrangements to use the facility outside normal business hours. However, this must be based on a compelling need and will not be done as a matter of routine practice due to the fiscal and manpower expense to the FBI.

(U//~~FOUO~~) Defense experts may use their own computers and tools to conduct an analysis. However, they must be notified in advance that any digital media entering the government facility must be forensically wiped prior to departure in order to ensure FBI compliance with the requirements of the Adam Walsh Act. If the field office does not have a segregated Adam Walsh room, the chief security officer (CSO) must be notified in advance that defense experts may have laptops or other portable electronic devices to support the discovery. The case agent must coordinate with the CSO for appropriate access. If the defense expert requires more than one session to complete the exam, reasonable accommodation may also include that the FBI provide either a lockable, private space within the government-controlled facility or a locking safe, in which the defense expert may store his or her tools and equipment when away from the room. These measures ensure attorney-client privilege and work products are not accidentally exposed to the government.

(U//~~FOUO~~) If a defense expert requests to take any materials generated during the examination from the government-controlled facility, all materials must be reviewed to ensure that no contraband, law enforcement sensitive (LES), or classified materials are included. If the defense expert objects to this review, CART personnel should notify their supervisor(s) and CDC/ADC or OGC  for input and assistance in resolving the issue. If those parties are not able to negotiate a resolution, the prosecutor on the case must be notified to obtain his or her assistance in securing a protective order from the court handling the case. It is recommended that the order include, at a minimum, a direction to each member of the defense team to individually certify, under oath and in writing, that they have taken no materials which are considered contraband under federal law away from the government-controlled facility upon completion of the defense examination, and that they have not caused any contraband to be sent offsite.

b7E

(U//~~FOUO~~) If a defense expert represents to the court that it is not feasible to bring his or her tools and equipment to the government facility, the FBI may supply forensic tools and equipment, including appropriate forensic tool licenses, limited to the forensic tools and equipment currently used by the FBI at the time of the request.

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

**3.3.6.5.2.2.1. (U) Special Guidelines for RCFLs in State or Local Cases**

b7E

(U//~~FOUO~~) For purposes of handling DE reasonably believed to contain contraband in state and local cases, RCFLs should follow the guidelines listed above whenever possible to prevent the contraband from being redistributed and the victims re-victimized. However, with respect to purely state or local cases, RCFLs are obligated to follow state or local court orders governing discovery.

**3.3.6.6. (U) [Redacted]**

**3.3.6.6.1. (U) Disseminating [Redacted]**

(U//~~FOUO~~) Case agents may, with the supervisor's approval, provide copies of the [Redacted] to authorized law enforcement, prosecutors [Redacted] in furtherance of a lawful purpose and consistent with the terms of the search warrant or other legal authority.

(U//~~FOUO~~) All personnel who handle DE must document dissemination of [Redacted] copy in the case notes, case report, and CART database, if applicable [Redacted]

[Redacted]

(U//~~FOUO~~) Once submitted to the ECF, the case agent may copy and disseminate copies [Redacted] and associated reports. If the case agent makes copies [Redacted] he or she is required to label the media in the same manner as the original (e.g., classification markings, banners, file number, and handling caveats).

**3.3.7. (U) Approved Tools**

(U//~~FOUO~~) Approved tools must be used by all DE personnel during [Redacted]

b7E

[Redacted]

(U//~~FOUO~~) Approved tools for processing DE are listed [Redacted] of many approved tools requires successful completion of OTD/DFAS-approved training.

(U//~~FOUO~~) In addition to tools listed on the approved tool list [Redacted]

[Redacted]

(U//~~FOUO~~) For each approved version of each tool, the approved tool list provides information about the forensic processes for which the tool is approved, as well as the

UNCLASSIFIED//~~FOUO/LES~~

UNCLASSIFIED//~~FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

known limitations of the tool. DE personnel are responsible for understanding these limitations prior to the use of the tool on DE.

**3.3.7.1. (U) Adding Approved Tools**

(U//~~FOUO~~) OTD/DFAS must approve tools in accordance with OTD/DFAS test and validation protocol and based upon appropriate scientific and evidentiary criteria.

(U//~~FOUO~~) Recommendations to add tools to the approved tool list may be submitted to the OTD/DFAS/Forensic Support Unit (FSU). Tool testing, validation, and verification must be coordinated through OTD/DFAS/FSU, although actual testing may be performed by personnel from other divisions or agencies as approved by OTD/DFAS.

**3.3.8. (U)** [Redacted]

(U//~~FOUO~~) Case agents should coordinate with OTD [Redacted]

[Redacted] Case agents should be aware that the use of unapproved [Redacted] is discouraged [Redacted]

[Redacted]

(U//~~FOUO~~) When using [Redacted]

b7E

[Redacted]

**3.3.9. (U) Requests for** [Redacted]

**3.3.9.1. (U) Examinations of Digital Evidence in FBI Cases**

(U//~~FOUO~~) Except as authorized in this PG (see Appendix E, Examination of FBI Evidence [Redacted] all evidence generated by FBI criminal [Redacted] must be submitted for forensic examination or forensic analysis to an FBI laboratory or forensic program authorized by the FBI Science and Technology Branch (STB). "Forensic examination(s)" or "forensic analysis (es)" are either:

- (U//~~FOUO~~) Generated as part of a process applied by a recognized forensic discipline of the American Society of Crime Laboratory Directors (ASCLD) or the ASCLD-Laboratory Accreditation Board (ASCLD-LAB), or the International Standards Organization (ISO).
- (U//~~FOUO~~) Commonly described or recognized as "forensic" or otherwise relating to the analysis of evidence by scientific or technical means or manner of evidence by or through an expert witness, as defined by the Federal Rules of Evidence (or their applicable equivalent) or as pronounced by rule or ruling of any court or tribunal.

b7E

(U//~~FOUO~~) [Redacted]

[Redacted]

**3.3.9.1.1. (U) Transfer of Evidence**

UNCLASSIFIED//~~FOUO/LES~~

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

3.3.9.1.1.1. (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted]

[redacted]

b7E

(U//~~FOUO~~) [redacted]

[redacted]

3.3.9.1.1.2. (U) Chain of Custody

(U//~~FOUO~~) In criminal investigations, once FBI evidence has been [redacted]

[redacted]

[redacted] is responsible for maintaining any chain of custody on all original and derivative evidence [redacted] created through the examination process until the completion of all trials and appeals. FBI personnel may not retain duplicate evidence or samples of evidence [redacted] [redacted] without the prior written concurrence of the AD, OTD.

b7E

3.3.9.1.2. (U) Non-Circumvention of FBI Policy

(U) A referral authorized by this PG may not be used, in whole or in part, to purposefully effectuate or passively benefit from activity that would otherwise violate FBI policy, including:

- (U) [redacted]

[redacted]

- (U) [redacted]

[redacted]

b7E

3.3.10. (U) Service Requests in Support of Administrative or Civil Matters

(U//~~FOUO~~) FBI personnel and facilities [redacted] (s) may not accept service requests to provide DE services in administrative or civil matters. The AD, OTD, may grant exceptions after consultation with OGC [redacted] In considering requests for exceptions, the AD, OTD must consider:

- (U) Whether such support would constitute an acceptable use of appropriated funds.
- (U) The impact on the FBI of using available examiner and equipment resources in support [redacted]
- (U) The cost to the FBI in having to provide personnel to testify in a civil matter, as well as be deposed and complete other civil discovery.

UNCLASSIFIED//~~FOUO~~/LES

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U) Other relevant factors presented by particular situations.

(U//~~FOUO~~) These limitations do not preclude providing DE support for FBI internal investigation matters, or for RCFLs to provide DE support

[Redacted]

b7E

(U//~~FOUO~~) If the FBI receives civil or administrative legal process (e.g., a subpoena) in connection with DE services performed for a criminal [Redacted], the individual served must coordinate with his or her CDC/ADC or OGC counsel for guidance, as applicable.

b3  
b7E

**3.3.11. (U) Re-examinations**

**3.3.11.1. (U) Definition of Examination**

(U//~~FOUO~~) An examination is defined as a forensic process whereby a forensic examiner reviews digital evidence

[Redacted]

b7E

(U//~~FOUO~~) Examination of data previously reviewed by a DExT is not considered a re-examination.

**3.3.11.2. (U) Overview of Re-examinations**

(U//~~FOUO~~) Unless approved by the AD, OTD as outlined below, examinations are not conducted on any evidence that has been previously subjected to the same type of technical examination (hereafter referred to as a “re-examination.”)

(U//~~FOUO~~) A re-examination occurs when evidence, already subjected to a technical examination

[Redacted]

(U//~~FOUO~~) This requirement is intended to:

- (U//~~FOUO~~) Eliminate duplication of effort.
- (U//~~FOUO~~) Ensure that the integrity of the evidence is maintained.
- (U//~~FOUO~~) [Redacted]

b7E

[Redacted]

- (U//~~FOUO~~) [Redacted]

[Redacted]

~~UNCLASSIFIED//FOUO/LES~~



~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- o (U//~~FOUO~~) [Redacted]
- o (U//~~FOUO~~) [Redacted]

b7E

**3.3.11.3. Requesting a Re-examination**

(U//~~FOUO~~) Within the FBI, re-examinations may only be requested by an EC approved by the requesting field office's division head. ECs should be addressed to the AD, OTD, and be routed through the chief, CART-FOU and the appropriate CART Field Operations Program manager [Redacted]

[Redacted]

(U//~~FOUO~~) The request should include a letter from the United States Attorney (or District Attorney if a state or local case), containing:

- (U//~~FOUO~~) The extraordinary circumstances compelling the requested re-examination.
- (U//~~FOUO~~) A detailed explanation of the facts and circumstances surrounding the request.
- (U//~~FOUO~~) All existing service requests.
- (U//~~FOUO~~) All existing legal authorities.
- (U//~~FOUO~~) All prior examination results, notes, and reports pertaining to the previous examinations or reviews, or an explanation as to why this material is not available.

(U//~~FOUO~~) In the event of exigent circumstances [Redacted]

[Redacted]

b7E

**3.3.11.4. Approval of Re-examination Requests**

(U//~~FOUO~~) Upon receipt of a request for re-examination, the chief, CART-FOU will review the request and supporting materials to determine if a particular examination request is a re-examination for the purpose of seeking the AD, OTD's approval.

(U//~~FOUO~~) After the chief, CART-FOU determines that the requested examination is a re-examination, he or she prepares a recommendation of approval or denial for the AD, OTD that considers the following factors:

- (U//~~FOUO~~) Scope of the requested re-examination.
- (U//~~FOUO~~) Responsiveness of the prior examination to previous and current service requests or legal authorities.
- (U//~~FOUO~~) Type of tools used in the prior examination or review (e.g., generally accepted forensic tools).

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- (U//~~FOUO~~) Location of agency and type of facility that performed the prior examination or review [redacted]
- (U//~~FOUO~~) Nature of prior review or examination (including whether prior examination substantially followed or were analogous to FBI CART SOPs).
- (U//~~FOUO~~) Whether documentation of prior examination or review provides sufficient detail (including whether there are indicia of a completed examination, [redacted])
- (U//~~FOUO~~) Background and certification of previous examiner.
- (U//~~FOUO~~) Purpose of previous review or examination.

b7E

(U//~~FOUO~~) The AD, OTD will consider the request for re-examination and, after coordination with OGC [redacted] as needed, approve or disapprove the request. Notice of approval or disapproval of the re-examination request will be transmitted via EC (to FBI field offices or headquarters divisions [redacted] if approved and if required by the circumstances, the approval document may also outline any conditions or limitations placed on the re-examination. The approval documentation will be maintained in the examination file.

(U//~~FOUO~~) Questions regarding whether a service request constitutes a re-examination should be directed to the appropriate DFAS unit.

(U//~~FOUO~~) The case agent must make all necessary notifications to the prosecutor concerning potential [redacted] that is or may be created as a result of the re-examination.

**3.3.12. (U) Advanced Technical Analysis**

(U//~~FOUO~~) Advanced technical analysis of DE may only be performed by [redacted]

[redacted]

**3.3.12.1.1. (U)**

[redacted]

b7E

(U//~~FOUO~~) Requests for advanced analysis must be made via a service request. All service requests must be documented via EC or, where available, an automated request through the approved OTD [redacted], using an open FBI case file, or by a request for assistance from [redacted] to the field office or RCFL.

**3.3.12.2. (U//~~FOUO/LES~~)**

(U//~~FOUO/LES~~)

[redacted]

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

**3.3.12.3. (U) Forensic Audio Video Image Analysis** [redacted]

b7E

(U//~~FOUO~~) All requests for advanced forensic [redacted] must be submitted to OTD/FAVIAU via EC or other appropriate documentation identified by FAVIAU.

**3.3.12.3.1. (U//~~FOUO~~//LES)** [redacted]

[redacted]

(U//~~FOUO~~//LES) All requests for [redacted]

[redacted]

**3.3.12.3.2. (U//~~FOUO~~//LES)** [redacted]

[redacted]

(U//~~FOUO~~//LES) All requests for [redacted]

[redacted]

**3.3.13. (U) Assigning Requests to Examiners and DE Backlog Definition**

(U//~~FOUO~~) In order to more accurately assess backlog of DE requests, the backlog is defined as "any unassigned request that is over 30 days old." To ensure an effective and efficient workflow, supervisors should assign service requests as examiners become available to actively address the request. At no time should a service request be assigned to avoid being identified as backlog.

(U//~~FOUO~~) The goal is to more accurately track digital forensic backlog by identifying requests that the field office does not have the resources to address. To further facilitate an accurate accounting of backlog, service requests should be limited to no more than ten unique items. The case agent or requestor should list out the items in the service request and rank them in order of priority to their investigation. [redacted]

b7E

[redacted]

(U//~~FOUO~~) Service requests can be entered directly into the CART database by the case agent or by CART personnel on behalf of the case agent. Service requests entered by CART personnel into the CART database must be inputted within one business day of receipt, regardless of other proprietary software/databases used to manage service requests in individual field offices and RCFLs.

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

## 5. (U) Recordkeeping Requirements

### 5.1. (U//~~FOUO~~) FBI Central Recordkeeping System

(U//~~FOUO~~) DE must not be serialized into the FBI's central recordkeeping system or any other FBI administrative or records management system (e.g., [redacted]). The FBI's central recordkeeping system (current [redacted]) is the FBI's official recordkeeping system for all case file management. Non-record materials, per the legal definition of federal records, must not be placed in the case file or case file system. Non-record materials include any copies preserved for convenience or reference. Though the FBI's central recordkeeping system has the ability to accept many documents and file types as either a serial or an attachment to both electronic communications (ECs) and forms, current policies dictate the guidelines for what material is authorized to be placed in the FBI's central recordkeeping system. All original digital evidence (1B) and ELSUR evidence (1D) must be maintained and handled per evidence procedures and guidelines, and as such, original digital and ELSUR evidence must not be serialized, attached to any document, maintained, or stored in the FBI's central recordkeeping system [redacted]

b7E

b7E

[redacted] should be retained in the 1A or 1C section of the case file and thus may be serialized into the FBI's central recordkeeping system. Under no exception should contraband material be serialized into the FBI's central recordkeeping system [redacted]

[redacted]

### 5.2. (U) Additional Guidance on Recordkeeping and Forms Use

- (U) ~~FOU~~ Intranet web site:

[redacted]

b7E

- (U) DEL Quality Assurance Intranet web site:

[redacted]

- (U) DEL Training Intranet web site:

[redacted]

- (U) Domestic Investigations and Operations Guide (DIOG):

[redacted]

- (U)

[redacted]

UNCLASSIFIED//~~FOUO/LES~~

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

## Appendix A: (U) Sources of Additional Information

---

(U) Please review the following Intranet web sites for additional information:

(U//~~FOUO~~) All of the below are to be marked (U//~~FOUO~~),

b7E



They are not to be identified to the public.

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 



UNCLASSIFIED//~~FOUO~~/LES

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

## Appendix D (U): Definitions and Acronyms

### (U) Defined Concepts

#### **(U) Seizure vs. On-scene Imaging vs. Processing**

(U//~~FOUO~~) There is often a great deal of digital media at a search site. Because processing and reviewing this media consumes valuable FBI resources, it is important to

[Redacted]

(U//~~FOUO~~) On-scene, digital media may either be [Redacted]

[Redacted]

Otherwise, based on legal authority, there may be a decision as to whether to [Redacted]

[Redacted]

It is important to know that imaging is a time-consuming process that may take hours or days depending upon on the amount of data to be copied.

(U//~~FOUO~~) Once seized DE and images made on-scene are back at an FBI facility, they may be processed using kiosks or preview methods [Redacted]

[Redacted]

U//~~FOUO~~.

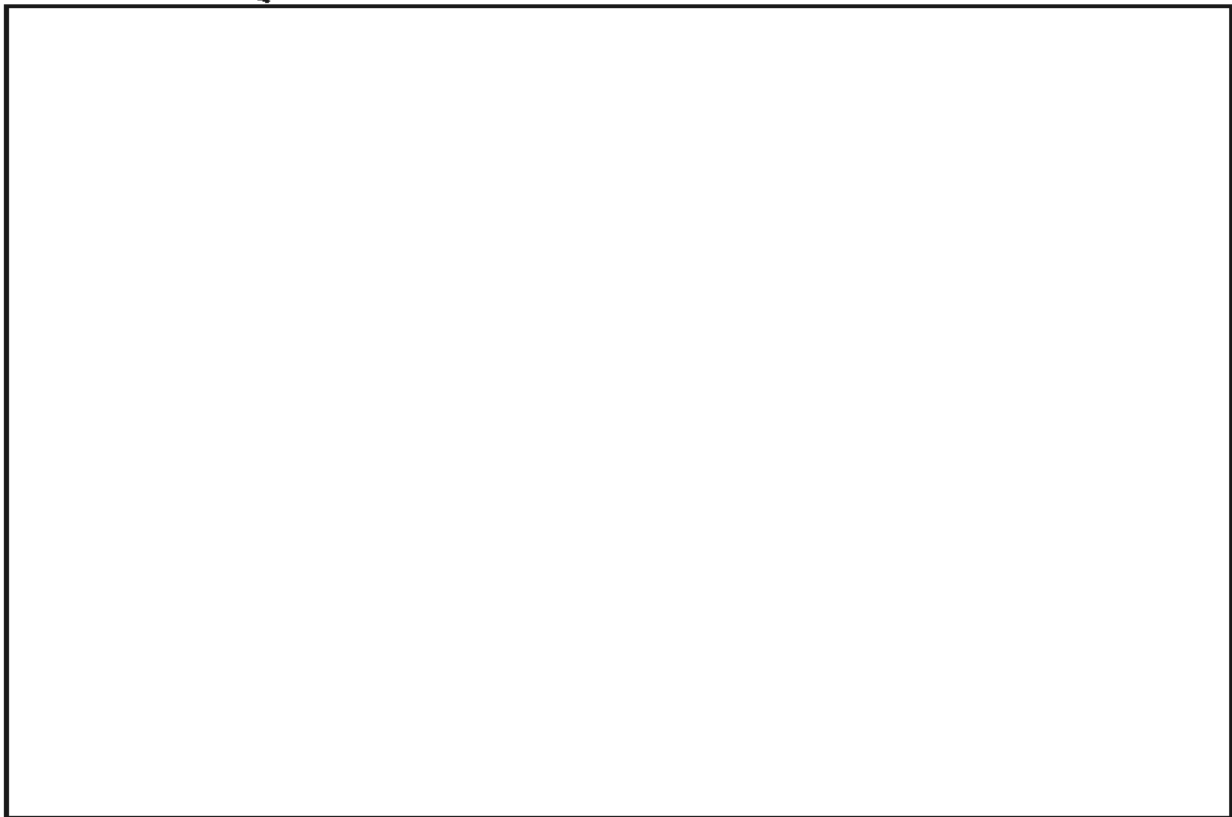


Figure 3: (U//~~FOUO~~) [Redacted]

b7E

b7E

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

**(U) Imaging (Copying) DE**

b7E

(U//~~FOUO~~) DE is an unusual kind of evidence in that, in most cases, it can be copied many times without degrading the original evidence. Most computer users are familiar with copying files [REDACTED]

(U//~~FOUO~~) In order to preserve and maintain the original evidence as it was found [REDACTED]

(U//~~FOUO~~) To prevent cross contamination [REDACTED]

(U//~~FOUO~~) The above processes related to [REDACTED] described in the CART standard operating procedures (SOPs).

**(U) Definitions**

(U//~~FOUO~~) **Approved Tools** – Tools that have been successfully tested and validated for processing DE or are native applications and utilities necessary for viewing files with proprietary formatting. Approved tools are listed on the OTD Intranet website.

(U//~~FOUO~~) **Computer Analysis Response Team –Technician (CART tech)** – Personnel trained and certified to forensically copy or image DE.

(U//~~FOUO~~) **Computer Analysis Response Team Forensic Examiner (CART FE)** – FBIHQ or field personnel, typically assigned full-time to DE work, who are trained, equipped, and certified to copy or image DE, search DE, extract data from DE, and who are authorized to provide opinions related to DE in court.

(U//~~FOUO~~) **CART On-the-Job Trainee (OJT)** – Personnel identified by field office management to participate in training with a commitment toward becoming certified CART FEs.

(U//~~FOUO~~) **CART Forensic Examiner Trainee (FET)** – Personnel assigned to work toward CART FE certification 100% of their time. Typically, these are trainees hired into ITS-FE positions. These may also be CART OJTs who are near the end of their training and have committed 100% of their time to CART FE work.

(U//~~FOUO~~) **Content Review Report** – Factual report of search/find/extract information that details who performed the work, when it was performed, what was reviewed and found, and where it was found.

(U//~~FOUO~~) **Computer Scientist - Field Operations (CS-FO)** – The CS-FO works as an integral member of an investigative team supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis, exploiting data

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

[Redacted]

b7E

(U//~~FOUO~~//LES) DFAS Technical Experts – DFAS

[Redacted]

(U//~~FOUO~~) **Digital Evidence** – Data stored digitally on integrated circuits, micro controllers, chips, tapes, magnetic media, optical media or other devices that assist in proving or disproving a matter at issue in a case or investigation.

(U//~~FOUO~~) **Digital Evidence Extraction Technician (DEXT)** – Personnel trained to copy or image DE and perform simple search/find/extract processes on copies of DE.

(U//~~FOUO~~) **Report of Examination** – The official report of examination used by CART FEs and Forensic Audio Video Image examiners and other DE technical experts to report the results of advanced technical analysis and/or document opinions formed as a result of that analysis (e.g., Digital Evidence Laboratory [Redacted])

[Redacted]

(U//~~FOUO~~) **Digital Evidence/Media Handling** – Physical treatment of digital media beginning with the initial identification, seizure, packaging, transport, shipment, storage, and control.

(U//~~FOUO~~) **Digital Evidence Personnel** – Personnel who are authorized upon completion of FBI approved training in the handling and processing of digital evidence/media (i.e., DEXT, CART personnel, and FAVP FA).

b7E

(U//~~FOUO~~//LES) **Digital Evidence Processing** – Processing of DE applies to personnel who are trained and tested to process DE and includes procedures related to on-scene preview, imaging, memory capture, content review, DE search, extraction, preparing reports, and advanced technical analysis [Redacted]

[Redacted]

(U//~~FOUO~~) **Examination** – Forensic process whereby a forensic examiner reviews digital evidence [Redacted]

[Redacted] Examinations have a specific scope as defined by the supporting legal authority and the service request pertaining to the evidence submitted for examination. The legal authority and service request may define the scope of the examination [Redacted]

[Redacted]

(U//~~FOUO~~) Examination of data previously reviewed by a DEXT is not considered a re-examination.

(U//~~FOUO~~) **Expert Opinion** – Judgment regarding certain facts or data either acquired by an expert’s own investigation, testing, or observations and based on his knowledge,

~~UNCLASSIFIED//FOUO/LES~~



~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

skill, experience, training, or education in a certain scientific, technical, or other specialized field.

(U//~~FOUO~~) **Expert Testimony** – Testimony of a witness qualified as an expert (scientific, technical or specialized field) by knowledge, skill, experience, training, or education, in the form of an opinion or otherwise. This testimony is based on sufficient facts or data, is the product of reliable principles and methods, and is grounded upon principles and methods that have been applied reliably to the facts.

(U//~~FOUO~~) **Extraction** – DE that has been [redacted] and provided for investigative purposes.

b7E

(U//~~FOUO~~) **Fact Witness** – A fact witness has personal knowledge of events pertaining to a case and can only testify to things he personally has observed. A fact witness cannot offer opinion.

(U//~~FOUO~~) **Field Audio Video Personnel (FAVP) Forensic Analyst (FA)** – Personnel trained to perform basic forensic functions related to audio and video DE.

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) **Master Copy** – The required copy of DE that is stored on media to be retained and logged on a chain of custody. This is [redacted] copy of the original DE or a logical copy that contains selected files and artifacts from the original DE, such as relevant files from a business server. It is important that the original legal authority be maintained with the master copy of the DE. If there is a question of whether a copy of the legal authority documents can be retained and/or forwarded, contact OGC or local CDC.

(U//~~FOUO~~) **Original DE** – DE seized at a search scene or otherwise legally obtained and stored in an ECF.

(U) **Random Access Memory (RAM)** – A computer system's memory which contains contents of recent applications and data so they can be accessed quickly when needed by the computer's processor.

(U//~~FOUO~~) **Regional Computer Forensics Laboratory (RCFL) Associate Examiner** – Former certified CART FE from an agency participating in the RCFL program who has completed their commitment to the RCFL, returns to their home agency, and continues a relationship with the RCFL to maintain certification and training.

(U//~~FOUO~~) **Re-examination** – A re-examination of DE occurs when data/evidence,

[redacted]

b7E

(U//~~FOUO~~) [redacted] – Less than a full copy of the original DE [redacted]

[redacted]

(U) **Volatile Memory** – Memory that is not retained when power is lost to a device.

(U//~~FOUO~~) **Working Copy** – Additional full copies of DE derived from the Master copy to allow review by personnel working for or with the FBI in its investigations [redacted]

[redacted]

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

## Appendix E (U//~~FOUO~~): Examination of FBI Evidence

b7E

(U//~~FOUO~~) As discussed above in section 3.2.9.1., all evidence generated by FBI criminal and [redacted] investigations (including joint investigations) must be submitted for forensic examination or forensic analysis to a laboratory or authorized forensic program of the FBI Science & Technology Branch (STB), unless an exception to policy is approved in accordance with this Appendix.

(U//~~FOUO~~) In rare instances, the unique demands of a particular case may prompt a USAO, DOJ entity, or other prosecutorial or investigative agency to have FBI evidence processed, examined or analyzed [redacted]

b7E

(U//~~FOUO~~) This procedure is separate and distinct from re-examination (as defined in section 3.2.11.2. above). A re-examination occurs when evidence, already subjected to a technical examination, is reviewed for the same probative data of its content, source, origin, and manner of creation, alteration, or destruction.

(U//~~FOUO~~) Further [redacted] FBI personnel shall follow the guidance in section 3.2.9.1.1 regarding the transfer of evidence.

(U//~~FOUO~~) Subject to the referral prohibitions described below (section entitled Mandatory Prerequisites and Discretionary Referral Factors), the SC, DFAS, after consultation as desired with an assistant general counsel (AGC [redacted]) (OGC [redacted]) may authorize [redacted] transfer of FBI evidence [redacted] certified forensic examiner or laboratory only under the following conditions:

b7E

- (U//~~FOUO~~) After a determination of the existence of the mandatory prerequisites and due consideration and evaluation of the discretionary referral factors described below.
- (U//~~FOUO~~) After consultation as may be deemed appropriate with the appropriate prosecutor and the applicable CDC or OGC supervisor.
- (U//~~FOUO~~) After compliance with the administrative requirements below (section entitled Administrative Requirements).

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Within the FBI [redacted] may only be requested via an EC approved by the requesting field office's division head. ECs should be addressed to the AD, OTD, and be routed through the chief, CART-FOU and the appropriate CART Field Operations Program manager.

b7E

UNCLASSIFIED//~~FOUO~~/LES

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

~~(U//FOUO)~~ The case agent must ensure that the request EC is serialized to the relevant investigative case file. This EC must include:

- (U) The FBI case ID or universal case file number (UCFN).
- (U) The FBI field office, telephone number and fax number.
- (U) The FBI case agent's name.
- (U) The applicable case prosecutor's name, if known.
- (U) A description of the original evidence to be released.
- (U) The full name, address and telephone number of [redacted]

b7E

- (U) A certification that a supervisory prosecutor and CDC have concurred in the request, and that the supervisory prosecutor has read and understands the FBI's policy [redacted]

- (U) The full name and position title of the case agent's Supervisory Special Agent (SSA).
- (U) An acknowledgement from the case agent that he/she understands it is the case agent's responsibility to make all required notifications to the prosecutor concerning [redacted]

~~(U//FOUO)~~ [redacted] request should include a letter from the United States Attorney, or District Attorney if a state or local case, [redacted]

b7E

~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ Approving [redacted]

~~(U//FOUO)~~ Mandatory Prerequisites and Discretionary [redacted]

~~(U//FOUO)~~ The SC, DFAS must not authorize [redacted] unless the SC affirmatively determines that either of the following prerequisites is met:

~~(U//FOUO)~~ [redacted]

b7E

~~UNCLASSIFIED//FOUO/LES~~

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

Directors -Laboratory Accreditation Board (ASCLD-LAB), or International Standards Organization (ISO). [redacted] forensic examiner must possess at the time of referral and, thereafter, maintain competency certifications(s) and meet proficiency requirements applicable to the recognized discipline or sub-discipline that has accredited [redacted]

b7E

(U//~~FOUO~~) [redacted]

• (U//~~FOUO~~) [redacted]

• (U//~~FOUO~~) In the judgment of the SC, DFAS, otherwise be objectively suitable after considering and weighing each [redacted]

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Assuming that the [redacted] prerequisites described in the section above are met, the SC, [redacted] at his or her discretion, may authorize an [redacted]

• (U//~~FOUO~~) Breadth of experience: the number and complexity of forensic examinations/analyses conducted [redacted]

• (U//~~FOUO~~) Testimonial experience: the experience [redacted]

• (U//~~FOUO~~) Report quality: the quantity and quality of written reports produced [redacted]

b7E

• (U//~~FOUO~~) Equipment acceptance: [redacted]

• (U//~~FOUO~~) Testing and evaluation documentation: whether there exists sufficient test and validation documentation on the equipment, tools or materials [redacted]

• (U//~~FOUO~~) Written protocols [redacted]

UNCLASSIFIED//~~FOUO~~/LES

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

documentation adequate to facilitate the repeatability of results by an equally qualified examiner.

- (U//~~FOUO~~) Applied quality assurance system [redacted]  
[redacted]
  - (U//~~FOUO~~) Annual, impartial, testing-based, proficiency examinations.
  - (U//~~FOUO~~) Peer review of examination results and reports.
  - (U//~~FOUO~~) Random and/or regular external compliance audits.
- (U//~~FOUO~~) Legal requirements [redacted]  
the examiner is employed or conducting forensic examinations has an affirmative procedure to evaluate, determine and monitor the ability of the examiner to testify in federal court relative to [redacted] or whether there exists a process for evaluating the existence of exculpatory information, which, as a matter of law, must be affirmatively disclosed, with or without request [redacted]  
[redacted]
- (U//~~FOUO~~) Law enforcement authority: whether there is a requirement that examinations are conducted by personnel employed by federal, state or local law enforcement agencies as may be required by law or under the direct supervision of a sworn law enforcement officer (see e.g., United States v Shrake, 515 F.3d U.S. 743 (7th Cir. 2008)) or whether the examination processes are conducted by an examiner who is a federal law enforcement officer or who is working at the direction of a federally sworn officer pursuant to 18 U.S.C. § 3105, if applicable.
- (U//~~FOUO~~) Space restrictions: whether the department, agency, or entity under which the examiner operates has an affirmative process in place requiring that examinations of contraband are conducted in law enforcement controlled space as required under the Adam Walsh Child Protection and Safety Act.
- (U//~~FOUO~~) Contraband: whether adequate controls exist to prevent unauthorized access or distribution of contraband pursuant to law (see e.g., child pornography at 28 U.S.C. § 2252, et seq. or controlled substances pursuant to 21 U.S.C. § 881, et seq.).
- (U//~~FOUO~~) Criminal history/indices check: [redacted]  
[redacted]
- (U//~~FOUO~~) Security requirements: the maintenance of an appropriate security level clearance relative to the FBI evidence being examined or analyzed in conformity with FBI security policy, as well as the facility and IT system in which the evidence will be stored and reviewed that is compliant with FBI security policy and [redacted]  
[redacted]

b7E

b7E

b3  
b7E

~~UNCLASSIFIED//FOUO/LES~~

UNCLASSIFIED//~~FOUO~~/LES

(U) Digital Evidence Policy Implementation Guide

- (~~U//FOUO~~) Occupational safeguard services: whether there is available [redacted]
- (~~U//FOUO~~) Depth/adequacy of examination: whether all necessary examinations, routines, and procedures will be conducted [redacted] (federal violations frequently require different elements of proof than do state or local violations of the same or similar nature).
- (~~U//FOUO~~) Preservation of original/best evidence: whether the examination process [redacted]
- (~~U//FOUO~~) Cost: [redacted]

b7E

**(U//~~FOUO~~) Administrative Requirements**

(U//~~FOUO~~) Prior to initiating a request [redacted]

- (~~U//FOUO~~) Conduct the examination(s) as well as testify as required at all proceedings associated with the case.
- (~~U//FOUO~~) Conduct all necessary examinations in light of the fact that violations of federal law often require different elements of proof than the same or similar state or local violations.
- (~~U//FOUO~~) Not destroy or impair the admissibility of the evidentiary material
- (~~U//FOUO~~) Consult either the FBI Laboratory or OTD DEL, as applicable, on scientific and technical aspects for the examination, if needed
- (~~U//FOUO~~) Notify either the FBI Laboratory or OTD DEL if examination will consume the evidentiary material.
- (~~U//FOUO~~) Promptly provide a copy of the examination report to either the FBI Laboratory or OTD DEL after the examination is completed.

(U//~~FOUO~~) The OTD DEL must notify the case agent of any prior knowledge regarding the proposed [redacted] concerning the examiner's ability to meet the basic standards of practice of the scientific discipline involved in the examination, or the use of practices that may call into question the ability to use the evidence and examination results at or administrative results at any judicial or administrative proceedings. This contact will be documented by the case agent via EC in the investigative case file.

b7E

**(U//~~FOUO~~) Referral Prohibitions**

UNCLASSIFIED//~~FOUO~~/LES

~~UNCLASSIFIED//FOUO/LES~~  
(U) Digital Evidence Policy Implementation Guide

(U//~~FOUO~~) Disqualified [redacted]

b7E

(U//~~FOUO~~) [redacted]

- (U//~~FOUO~~) [redacted]

- (U//~~FOUO~~) [redacted]

[redacted]

- (U//~~FOUO~~) The FBI has information to believe [redacted]

[redacted]

- (U//~~FOUO~~) [redacted]

[redacted]

**(U//~~FOUO~~) Second Opinion Examinations**

(U//~~FOUO~~) [redacted] may not be used, in whole or in part, to seek or obtain second opinions regarding or re-examinations of a forensic examination/analysis or variations of an examination/analysis already commenced or completed by an FBI STB laboratory without obtaining re-examination authority as described in section 3.2.11 of this PG. If authority is sought for a second opinion or re-examination, the case agent must notify the prosecutor that no testimony should be provided on the same technical subject or area, or regarding the initial examination (testimony will be provided for the defense if required by law). The case agent must make all required notifications to the prosecutor concerning [redacted] material that is created as a result of the second opinion or re-examination.

b7E

**(U//~~FOUO~~) "Curbstone" or Informal Evaluations or Advice**

(U//~~FOUO~~) [redacted] may not be used, in whole or in part, to seek or obtain "curbstone," ad hoc, or informal opinions or advice by or from non-FBI scientific or technical personnel to assess the potential value of FBI evidence prior to submitting it to FBI STB laboratories (e.g., FBI personnel may not provide FBI evidence to a non-FBI scientific or technical person to obtain an informal, undocumented or "off the record" opinion on whether it should be submitted to an FBI STB laboratory, or what type of examination should be requested).

(U//~~FOUO~~) [redacted]

**Investigations Prohibited.**

b3  
b7E

(U//~~FOUO~~) [redacted]

[redacted]

- (U//~~FOUO~~) [redacted]

[redacted]

~~UNCLASSIFIED//FOUO/LES~~

(U) Digital Evidence Policy Implementation Guide

- ~~(U//FOUO)~~ [redacted]
- ~~(U//FOUO)~~ [redacted]
- ~~(U//FOUO)~~ [redacted]
- ~~(U//FOUO)~~ [redacted]

b3  
b7E

~~(U//FOUO)~~ Documentation Requirements.

~~(U//FOUO)~~ The SC, DFAS must prepare an EC containing the approval or denial [redacted] request and the case agent must ensure that the EC is serialized to the relevant investigative case file. This EC must include:

b7E

- ~~(U//FOUO)~~ The date the request was either approved or denied.
- ~~(U//FOUO)~~ In the case of an approved [redacted] referral, a certification by the SC, DFAS that he/she has determined that the proposed [redacted]

[redacted]

~~UNCLASSIFIED//FOUO/LES~~



# **EXHIBIT D**

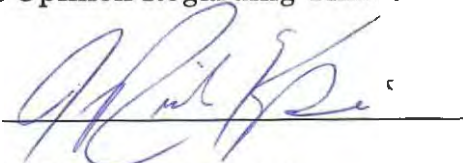
**(Report of Dr. James Richard Kiper, Ph.D)**

### Affidavit of Dr. James Richard Kiper, Ph.D.

State of Florida  
County of Leon

COMES NOW Dr. James Richard Kiper, Ph.D., being first duly sworn, under oath, and states that the contents of the following attached reports, including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Summary of Technical Findings
- Summary of Process Findings
- Analysis of the Testimony of Special Agent Christopher Mills
- Expert Opinion Regarding Time to Review Digital Evidence

Signature: 

Address: 818 Shannon Street  
Tallahassee, Florida 32305

SUBSCRIBED AND SWORN TO before me this 25 day of April, 2022, by  
James Kiper



**Michael Jordan**  
Comm. # GG366579  
Expires: October 1, 2023  
Bonded Thru Aaron Notary

  
NOTARY PUBLIC FOR FLORIDA

My Commission Expires: 10/1/23

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

## Summary of Technical Findings

### **Professional Background**

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have an in-depth knowledge of FBI digital evidence examination procedures and policies.

### **Review of Evidence**

On May 21, 2021, I signed the Protective Order Regarding Discovery in U.S. v. Raniere, et al., 18 CR 204 (NGG) and was subsequently provided access to certain evidence in this case. My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports **generated by members of the FBI's Computer Analysis Response Team (CART)**. Based on my review, I discovered specific actions that were taken to manually alter the evidence, in support of **the government's narrative that photos were taken by a Canon EOS 20D camera (GX 520), saved to a Lexar CF card (GX 524), copied to an unknown computer, and then backed up to a Western Digital hard disk drive (GX 503)**. In this report I will refer to the latter two items as the CF Card and the WD HDD.

In my 20 years serving as an FBI agent, I have never observed or claimed that an FBI employee tampered with evidence, digital or otherwise. But in this case, I strongly believe the multiple, intentional alterations to the digital information I have discovered constitute evidence manipulation. And when so many human-generated alterations happen to align with the **government's narrative, I believe any reasonable person would conclude that evidence tampering had taken place**. My analysis demonstrates that some of these alterations definitely took place while the devices were in the custody of the FBI. Therefore, in the absence of any other plausible explanation it is my expert opinion that the FBI must have been involved in this evidence tampering.

## Key Findings

1. Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.
2. Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.
3. An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.
4. Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.
5. The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.
6. The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.
7. The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

**Finding 1: Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.**

- As further explained in Finding #2, photos named IMG\_0093.JPG, IMG\_0094.JPG, IMG\_0096.JPG and IMG\_0097.JPG (hereinafter IMG\_0093-97) were among those that appeared on the FBI's WD HDD forensic report, but they did not initially appear on the CF Card forensic report generated on 04/11/2019. Subsequently, however, on 06/11/2019 the FBI created another version of the CF Card forensic report wherein these and other photo files were included. It is important to note that neither the IMG\_0093-97 files, nor any other of the newly-added files, were **viewable** as photo images in the 06/11/2019 forensic report of the CF Card.
- The government's narrative requires that the IMG\_0093-97 files on the second CF Card report be identical to the IMG\_0093-97 files found in the WD HDD report, because photos created

on the CF Card were supposedly backed up to the WD HDD unaltered. Indeed, they have identical file names, identical Modified dates, and (presumably) identical EXIF data, including the date taken, camera model, and serial number<sup>1</sup>. However, they cannot be identical photo files because their MD5 hashes (“**digital fingerprints**”) do not match (See **Appendix A**, Figure 3).

- Moreover, a content review of the files reveals the subjects of the photographs found on the two devices are actually two different people. Although the IMG\_0093-97 files were not viewable as photos in the 06/11/2019 CF Card report, their forensically recovered carved thumbnail photos were viewable, and they depicted a **blonde** woman. By contrast, the IMG\_0093-97 files on the WD HDD report were viewable photographs and they depicted a **brunette** woman. Again, the two sets of IMG\_0093-97 files share the same file names and the same last Modified dates and times – to the second. *This would mean the same camera, with the same serial number, took two different photographs of two different subjects at precisely the same time and assigned them the same file name.* This is impossible, of course, so the presence of these files indicates the manipulation of the content and metadata for these photos.
- In fact, a detailed analysis of the carved file listings for each device revealed that IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097 found on the CF Card are not only different from their namesakes on the WD HDD, but they also contain the same thumbnail images as those of IMG\_0180, IMG\_0181, IMG\_0182, and IMG\_183, *respectively*. This surprising observation points to someone creating copies of IMG\_0180–183 and then making changes to them on the CF card, including changing their file names to IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097. These intentional alterations likely resulted in the files being unviewable on the 06/11/2019 forensic report, but it did not destroy the thumbnail images left over from the IMG\_0180–183 photos. It is likely the custodians of the CF Card who added these files, the case agents or their associates, repurposed the IMG\_0180–183 files because at that time they did not have physical control of the WD HDD or its files. The FBI’s **Case Agent Investigative Review (CAIR)** system enabled the case agents to review the WD HDD evidence and bookmark items, but it prevented them from exporting any information from the evidence. Please refer to **Appendix C** for an in-depth analysis of the carved files found in the WD HDD and CF Card forensic (FTK) reports.
- The intentional modification of the IMG\_0093-97 files on the CF Card report cannot be explained by normal use of the camera or CF Card. In the context of this case, the alterations are best explained by the intentions of an unknown actor attempting to create a stronger relationship between the CF Card photo files and the WD HDD that supposedly contained their backups. These actions will be further explained in Finding 2.

---

<sup>1</sup> As noted in my Process Findings, neither the two forensic images of the CF card, nor the EXIF data from files in the associated FTK reports, were produced during discovery. However, I was able to determine that photographic data from IMG\_0180 to IMG\_0183, were actually found in the newly-added photos on the CF report with file names IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097 (See **Appendix C**). If I had full access to the CF card data, it is reasonable to assume I would find the same EXIF data in those files as well.

**Finding 2: Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.**

- On 4/11/19, FBI forensic examiner Stephen Flatley created a forensic copy of the CF card, processed the data, and generated a forensic report using AccessData Forensic Toolkit (FTK), also known as AD LAB. The report listed active files present on the CF card, as well as those that had been deleted.
- On 6/11/19, five weeks into the trial and one day before he took the stand, FBI Examiner Brian Booth created *another* forensic copy and *another* FTK report of the same CF card. In the FBI, this is considered a reexamination and is prohibited by policy (see my Process Findings report). However, in this second report there were **new files** present in the file listing that **were not on the previous report**: Namely, IMG\_0042, IMG\_0081–IMG\_0100, IMG\_0172–IMG\_0179, and IMG\_0193–IMG\_200.
- In the FBI, CART examiners generate FTK reports, which contain file listings, graphics, and exported files that were identified and bookmarked by the case agent or CART examiner. At times, new reports are generated from *existing forensic copies* of the same device, when the facts of the investigation change or when a new forensic tool becomes available. In this case, however, the difference between the two FTK reports cannot be attributed to the use of a different tool, because both examiners used the same tool and version number: AccessData Forensic Toolkit, Version 6.3.1.26.
- The appearance of new files on a subsequent forensic report does not, by itself, necessarily mean that files were added to the original device. However, I have generated hundreds of FTK reports for the FBI, and I can think of no legitimate reason for new files to appear on a subsequent FTK report generated by the same software and version number, working under the same set of facts, on the same piece of evidence, which is supposed to be preserved and immutable from the time of collection.
- In fact, there are several reasons to suspect that the new files appearing on the 06/11/2019 CF Card report did not legitimately originate on the CF Card itself:
  - None of the new files are viewable in the 06/11/2019 report, while all the files previously appearing on the 04/11/2019 report are viewable.
  - None of the new files are viewable on the CF Card report, so they cannot be visually compared with their namesakes on the WD HDD, which **are** viewable.
  - None of the **MD5 hashes** for the new files on the CF Card report match their namesakes on the WD HDD report. Mismatched MD5 hashes means they are not the same files.
  - Unlike the first 04/11 CF card report, the second 06/11 CF Card report **omitted the file sizes** for the photos, thereby preventing even a file size comparison of the new files with their namesakes on the WD HDD.
  - Aside from the manipulated IMG\_0093-97 files discussed in Finding #1, **the FBI's**

forensic tool (FTK) was **unable to carve a single viewable photo** from any of the new files appearing on the 06/11 CF Card report. In that same report, by contrast, FTK was able to carve out several dozen **viewable photos from the CF Card's** previous photos as well as from unallocated space (with no links to specific files).

- To summarize, there is nothing besides easily-modifiable file names and file system dates and times that connect the new files in the 06/11 CF Card report with their namesake photos on the WD HDD report.
- Moreover, the way the new files appear on the 06/11/2019 CF Card report is indicative of someone creating large swaths of **“new files” on the CF Card** based on file names, rather than on content. For example, as detailed in **Appendix D**, the appearance of 20 files (IMG\_0081-100) on the second CF Card report implies that the user had taken several pictures of three different subjects, saved them to the CF Card and eventually backed them up to the WD HDD. However, it also requires the user to return to the CF Card, delete only first two photos (by filename) of the first subject, delete no photos of the second subject, and then delete all BUT the first two photos of the third subject. Even more incredibly, the user would have had to delete them in such a way as to prevent the FBI's forensic tool (FTK) from recovering them (e.g. by writing over the sectors). As mentioned earlier, FTK had no problem recovering other deleted files, carving photos from those deleted files, or even recovering viewable photos from the CF Card's unallocated space.
- With the possible exception of IMG\_0093-97 files discussed in Finding #1, the new files **appearing on the FBI's CF Card** forensic report between the 04/11 and 06/11 versions **may not even be real digital photos**, since there is no data – no file sizes, no viewable images, no carved photos, no carved thumbnails – to indicate that they are. Nevertheless, these newly added CF card files and metadata match the filenames, dates, and times of files on the WD HDD, indicating that the likely reason for adding these files was to make it appear as though the corresponding files on the WD HDD at one time had originated on the CF card with the **dates indicated, consistent with the government's narrative. This is especially significant** because other than easily-modifiable EXIF data, there is no forensic evidence linking the hard drive's **alleged contraband to the CF card**. Again, for a detailed analysis of the new files appearing on the 06/11/2019 CF Card report, please see **Appendix D**.

**Finding 3: An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.**

- According to the CF card file listing (see **Appendix A**, Figure 1), the Accessed dates for *all the active files* were changed to 09/19/2018 (The rest of the files are recoverable deleted files). At a minimum, this finding demonstrates that file system dates on the CF card were altered on at least one occasion, 09/19/2018, six months after it was collected by the FBI on 03/27/2018.
- The presence of updated accessed dates also demonstrates the FBI did not use a write blocker to **preserve the evidence, which is a “critical procedure”** according to FBI CART SOP 4.3 (see my Process Findings).

- According to the FBI Chain of Custody for the Camera and CF card, Case Agent Michael Lever checked out these items from Evidence Control on 09/19/2018 and returned them on 09/26/2018 (see **Appendix A**, Figure 2). SA Lever recorded his purpose for accepting custody as “**Evidence Review.**” Therefore, SA Lever is most likely the person who accessed the CF card on 09/19/2018 without a write blocker. As I explain in my Process Findings report, this unauthorized access not only changed the evidence but it also violated FBI digital evidence handling policy.

**Finding 4: Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.**

- According to the file listing information in **Appendix B**, Table 1, there is an inconsistent relationship between two different dates presumably generated by the camera upon creation of the photographs. The EXIF date, generated by the camera, is embedded into the JPG file itself and does not change when the file is copied to another file system. However, the Modified date is saved to the CF card file system, and it may be interpreted differently by another computer, **depending on that computer’s time zone settings (The Created date is overwritten completely upon copy)**. I do not have access to the unknown computer into which the photographs were copied, so I have no information about its time zone settings. However, it appears a deliberate effort was made to alter Modified dates on the files so they might comport with the Daylight Saving Time, which ended 10/30/2005.
- From IMG\_0043 to IMG\_0126 the Modified dates were one hour behind those of the EXIF dates. On 10/30/2005 starting with IMG\_0127 the Modified dates of photos were adjusted to be **two hours** behind, and then on the same day starting with IMG\_0138 they were adjusted to be **exactly the same** as the EXIF dates. Notably, the photos IMG\_0127-137 belong to a single folder (Mnp102005\2005-10-29-2350-08) and were the only photos on the WD HDD with this two-hour difference between the Modified dates and the EXIF dates. Nothing outside of human intervention could account for these changes.
- In my experience, there is likewise no legitimate reason a normal user would be making these changes.

**Finding 5: The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.**

- The Modified date of **IMG\_0175** on the hard drive matches the Modified date of IMG\_0175 recovered on the CF card, which would normally indicate that IMG\_0175 was downloaded from the CF card onto an unknown computer and then copied to the hard drive without ever being modified.
- However, the EXIF CreatorTool value of IMG\_0175 is set to “Adobe Photoshop Elements



3.0,” which indicates that Adobe Photoshop was used to open and modify the file data. The Adobe Photoshop value could not have been set by the camera, and it was not observed in the EXIF data of any other photo. Since the EXIF data is part of the content portion of the file, its modification must result in an updated Modified date. The fact that the file’s Modified dates are exactly the same on both devices - in the face of obvious modification - indicates the dates have been manually altered to be the same (See **Appendix A**, Figure 6).

- Modified dates are normally unaltered when copying to a new file system. Therefore, the act of altering a Modified date when content modification occurred reveals an intent by the user to conceal the file modification by coordinating the Modified dates between the CF card and the hard drive.
- The uniqueness of the EXIF data in the IMG\_0175 file is also reflected in the thumbnail photo that was carved from it on the HDD. Every other carved thumbnail in this case is named “Carved [9728].jpeg,” meaning it was carved at the end of the fixed length EXIF portion of the file located at byte offset 9728 (See **Appendix C** for a more detailed explanation). However, the thumbnail carved from IMG\_0175 is named “Carved [9104].jpeg,” meaning the EXIF data in this file is different from all the others.
- The fact that only one file, IMG\_0175, still contains the EXIF CreatorTool value set at “Photoshop Adobe Elements 3.0” is likely due to an oversight on the part of the person altering the EXIF data. Like the other files in the WD HDD, it contains the EXIF model and serial number of the camera, but none of the other files contains a reference to Photoshop.

**Finding 6: The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.**

- At trial the government acknowledged that the upper level folders, such as Df101905, were created by a human when FE Booth testified, “Yes, it looks like someone put the date and time associated with two letters” (p. 4984).
- However, during court proceedings the government repeatedly asked FE Booth to confirm both the upper level and lower level folder names (such as 2005-11-02-0422-20) “roughly” correspond to the original date and time contained in the EXIF data of files in those folders (e.g., pp. 4852-56). The clear implication was that these folder names could be relied upon to corroborate the values in the EXIF data. In fact, during closing arguments the government stated, “Brian Booth testified that the most reliable metadata that the FBI could obtain from the images on the Western digital hard drive, said that they were taken exactly when the folders stated they were taken” (p. 5371).
- The folders could not have been generated by the Canon camera, since that camera creates folders named “CANON100” to store the first 100 photos, “CANON200” for the second 100 photos, and so on. This folder naming convention appears in the file paths of both of the

government's FTK reports of the CF card, dated 04/11/2019 and 06/11/2019.

- Testing has demonstrated that Adobe Photoshop Elements can indeed create folder names with the YYYY-MM-DD-HHMM-SS nomenclature, but the date and time is based upon the current system clock at the time the photos were imported into Adobe Photoshop, not on the created times of the photos themselves. This fact reveals how the folder names were subsequently manipulated.
- According to the date/time nomenclature, for example, **the folders “2005-10-19-0727-57” and “2005-10-19-0727-59” would have had to have been created two seconds apart** (7:27:57 AM and 7:27:59 AM, respectively). These folders reside under separate and uniquely named parent folders, **“Df101905” and “Msk101905,” respectively** (See **Appendix A**, Figure 5). The latter portion of these folder names could not possibly correspond to realistic folder creation times because two seconds is not enough time to manually select nine files, IMG\_0090-98, copy them into the Df101905 folder, and then manually select another eleven files, IMG\_0079-89, and manually navigate to the Msk101905 folder and save them there.
- In addition, I discovered a Thumbs.db file in each of the folders **“2005-10-19-0727-57” and “2005-10-19-0727-59.”** In earlier versions of Windows, a Thumbs.db was automatically generated in a folder to contain previews of each file in the folder. However, I discovered that the Thumbs.db file **in each of the “2005-10-19-0727-57” and “2005-10-19-0727-59” folders contain previews of the full range of photos IMG\_0079-98.** This means that all of those photos used to reside in a single folder in the past, and some time later they were divided and placed into their *current* locations, which are: IMG\_0090-98 into the / Df101905/2005-10-19-0727-57/ folder and IMG\_0079-89 into the /Msk101905/2005-10-19-0727-59/ folder. The fact that all photo previews were contained in both Thumbs.db files likely indicates that an earlier folder, containing all IMG\_0079-98 photos, was duplicated, the resulting folders were renamed and placed into the Df101905 and Msk101905 folders, and then unwanted photos from each folder were removed. No special skills are required to move files and rename folders in the way I just described, and people often do so to organize photos according to subject matter.
- It is certain that some of the timestamped folder names were manually manipulated, such as the ones described above. Given the ease with which one can alter folder names, it is possible the names of the folders containing alleged contraband (2005-11-02-0422-20 and 2005-11-24-0814-46) were **manually set in a way that aligns with the prosecution's narrative that the photos were taken in November 2005, and therefore the subject would have been fifteen years old, according to the trial record.** At the very least, the dates and times indicated in these folder names cannot be relied upon to determine or corroborate the creation dates of the photos contained in them.

**Finding 7: The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.**

- According to the file listing of a forensically imaged Western Digital hard drive (WD HDD), on 03/30/2009 a backup was made of a Dell Inspiron 700M and given the folder name “BKP.DellInspiron700M-20090330.” Also on 03/30/2009 a PowerMac was backed up to the folder “BKP.PowerMac8.2-2009-0330.” Unsurprisingly, all the Created dates in these folders were 03/30/2009 (or very early 03/31/2009), the backup date identified in the folder name (see Appendix A, Figure 4). By contrast, all the files in the unknown computer (“Dell Dimension”) backup folder (“BKP.DellDimension8300-20090330”) have a Created date of 07/26/2003, and the backup folder has a last Accessed date of 07/28/2003, despite the folder *name* indicating the same backup date as the others (03/30/2009).
- When files are copied from one file system to another, their Created dates are changed to the current clock time of the machine hosting the receiving file system. If all clocks are accurate, then the created time of these copied files will necessarily be AFTER the modified times.
- In this case, however, all the files in the unknown computer backup (“BKP.DellDimension8300-20090330”) have a Created date of 07/26/2003, while most of their Modified dates are from October 2005 and later. This observation indicates the system clock was rolled back to 2003 before copying these files manually onto the hard drive.
- **Sometimes the computer’s CMOS battery** – which enables the computer to retain information after shutdown such as system time – goes bad, resulting in the system clock being reset to a default date, such as 01/01/2003<sup>2</sup>. However, the computer will continue to reset the system clock to that date every time the computer powers up. Therefore, a bad CMOS battery cannot explain the system clock set to 07/26/2003 for the creation date of the files in the folder whose name, as mentioned previously, indicates a 03/30/2009 backup. It also fails to explain the creation dates of several hundred (mostly music) files copied to the WD HDD between 08/08/2003 and 08/18/2003 **that were NOT located in the “BACKUPS” folder.**
- The rolling back of the system clock is more likely the result of someone who was trying to backdate the folder content and make this folder appear to be a legitimate backup folder but may not have considered how and when file system dates are normally updated.

There are other significant anomalies in this backup folder that showcase the failed effort to create the appearance of an automated backup:

- The Dell Inspiron backup contains more than 15,000 files, while Dell Dimension backup was backed up in two separate copy operations, in total less than 500 files.
- The Dell Inspiron backup included several directories, such as Desktop, Favorites, and My

---

<sup>2</sup> Although the “factory default” date could theoretically be any date, I have never seen one that is NOT on the first day of the month, either in January or December of the year of manufacture.

Documents, while the Dell Dimension backup initially only included the Studies folder, containing the images in question. It is uncommon for a user to choose to primarily back up a particular folder (**in this case, the “Studies” folder**) from an entire desktop system, while ignoring more common file storage locations such as My Documents. To accept the legitimacy of this backup one would need to believe a highly improbable scenario where the user made a concerted effort to back up a folder containing his contraband, and specifically this folder, from an entire desktop system. In a likely attempt to create the appearance of a legitimate backup – more than an hour after **the “Studies” files were copied** – a Symantec folder with one file, and about 150 songs were added to the backup folder.

### **Conclusion**

In summary, the forensic evidence shows that folder names and dates (key facts upon which the **prosecution’s argument relied**) were **manually altered**, and the entire backup folder to which the alleged contraband belonged was manipulated. While it is impossible to determine exactly when the information on the WD HDD was altered, it is a scientific certainty that data on the CF card were added and/or modified while the device was in FBI custody.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP  
FBI Special Agent (Retired) and Forensic Examiner

### Appendix A: Figures

Figure 1. CF card file listing showing 9/19/2018 access dates<sup>3</sup>.

Name	Delete	Created	Accessed	Modified	Hash	Path
IMG_0224.JPG	N	3/9/2006 3:18	9/19/2018	3/9/2006 3:18	596a4251cf7782a440d9b6e8c5c18720	Lexar CF 2GB Card/
IMG_0225.JPG	N	3/9/2006 3:18	9/19/2018	3/9/2006 3:18	1b613027ddb1bafcfca88ffd20c6f1e	Lexar CF 2GB Card/
IMG_0227.JPG	N	3/9/2006 3:19	9/19/2018	3/9/2006 3:19	f7ac8c54897985961f729299756c319	Lexar CF 2GB Card/
IMG_0228.JPG	N	3/9/2006 3:19	9/19/2018	3/9/2006 3:19	341c44c7bd25375f6aeedf39a8db79cc	Lexar CF 2GB Card/
IMG_0229.JPG	N	3/9/2006 3:19	9/19/2018	3/9/2006 3:19	b5ea586450d43d25eda07fff7f76f82	Lexar CF 2GB Card/
IMG_0230.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	4836010357e1ba89baade965f3d89a0b	Lexar CF 2GB Card/
IMG_0231.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	8bdce71ed54222d649badfcc2d75d898	Lexar CF 2GB Card/
IMG_0233.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	83962b67a98f299f67e6262317c601d5	Lexar CF 2GB Card/
IMG_0234.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	760ac0e77c1d9455c28c07836c52c32b	Lexar CF 2GB Card/
IMG_0235.JPG	N	3/9/2006 3:21	9/19/2018	3/9/2006 3:21	d597dbff4c67fb186b55eff1862e330e	Lexar CF 2GB Card/
IMG_0236.JPG	N	3/9/2006 3:21	9/19/2018	3/9/2006 3:21	534518d5b7cb5e4ab864c04890642294	Lexar CF 2GB Card/
IMG_0237.JPG	N	3/9/2006 3:22	9/19/2018	3/9/2006 3:22	a280f9c541fa96731628987baec67095	Lexar CF 2GB Card/
IMG_0238.JPG	N	3/9/2006 3:22	9/19/2018	3/9/2006 3:22	30788af5673e78bf0365dfb39776d4a9	Lexar CF 2GB Card/
IMG_0239.JPG	N	3/9/2006 3:22	9/19/2018	3/9/2006 3:22	de746ef94d03b6c01797914747cb3601	Lexar CF 2GB Card/
IMG_0241.JPG	N	1/6/2007 7:03	9/19/2018	1/6/2007 7:03	e306c5177fc9cd747dde978233674043	Lexar CF 2GB Card/
IMG_0242.JPG	Y	1/6/2007 7:05	1/6/2007	1/6/2007 7:05	ba9411b3b34b626f73ee4649c757654	Lexar CF 2GB Card/
IMG_0243.JPG	N	1/6/2007 7:05	9/19/2018	1/6/2007 7:05	3b77bc0a1f64652b820d1804b88a8d80	Lexar CF 2GB Card/

Figure 2. Excerpt from DX 945, Chain of Custody for Camera and CF Card, showing SA Lever checking out evidence on 09/19/2018 and returning it on 09/26/2018.

Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: <i>Cory Cleus</i>	9/19/18 0900	Signature: <i>Michael Lee</i>	9/19/18 9:00am
Printed Name/Agency: <i>Cory Montgomery</i>		Printed Name/Agency: <i>Michael Lee - FBI</i>	
Reason: <i>CU to SA</i>		Reason: <i>Evidence Review</i>	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: <i>Michael Lee</i>	9/26/18 1:15pm	Signature: <i>[Signature]</i>	9/26/18 1:15pm
Printed Name/Agency: <i>Michael Lee - FBI</i>		Printed Name/Agency: <i>[Signature]</i>	
Reason: <i>Evidence Review</i>		Reason: <i>[Signature]</i>	

<sup>3</sup> Note: The HDD listing referenced in Figures 1, 3, 4, and 5 was generated by the defense using a computer set to Pacific Time while the government reports were generated by a computer set to Eastern Time.

Figure 3. Comparison of photograph metadata for files found on both the CF card and WD HDD.

Name	Created	Accessed	Modified	Hash	Path
IMG_0093.JPG	10/19/2005 19:33	10/19/2005 19:33	10/19/2005 19:33	04e96f3f0f48c3b117cbf4bcd516a857	Lexar CF 2GB Card/
IMG_0094.JPG	10/19/2005 19:33	10/19/2005 19:33	10/19/2005 19:33	97d26874707bf3f97e76fc22b57d86d0	Lexar CF 2GB Card/
IMG_0095.JPG	10/19/2005 19:33	10/19/2005 19:33	10/19/2005 19:33	81f59288eb1ca3ce02826f1ce46dc4d5	Lexar CF 2GB Card/
IMG_0096.JPG	10/19/2005 19:33	10/19/2005 19:33	10/19/2005 19:33	884764bfb7a72ed5f726af5d5eb11b5	Lexar CF 2GB Card/
IMG_0097.JPG	10/19/2005 19:33	10/19/2005 19:33	10/19/2005 19:33	5cb3245ec43bf2d9b0e373995336deee	Lexar CF 2GB Card/
IMG_0098.JPG	10/19/2005 19:34	10/19/2005 19:34	10/19/2005 19:34	452db09a0de54234504bb1211f6c30eb	Lexar CF 2GB Card/

Name	Created	Accessed	Modified	MD5	Path
IMG_0093.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	697cec1244dce21ecc4f82cd3a764644	WD External Device/i
IMG_0094.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	4795f46d36fa9c33e20b90ca2eebdc63	WD External Device/i
IMG_0095.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	3c89631e7576a554a13efca5fd3fb8d3	WD External Device/i
IMG_0096.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	dd2adf19eb671d7cdad10fe43e1e977	WD External Device/i
IMG_0097.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	f3cba2fe0cf8fca83eab33d0afcb522a	WD External Device/i
IMG_0098.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:34	a28460e871c2127a4a6b652785a79c3d	WD External Device/i

Figure 4. Records from the WD HDD File listing showing disparity in Created dates.

Created	Accessed	Modified	MD5	Path
3/30/2009 19:57	3/30/2009	3/30/2009 19:59	53834a379843cc754d686b0c6525c9a	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellInspiron700M-20090330.bkf
3/30/2009 22:03	2/12/2010	3/30/2009 22:03	016e661d4bc58afe43f24efd13d24e	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.PowerMac8,2-2009-0330/Desktop.dmg
7/26/2003 12:28	2/12/2010	6/26/2004 11:30	4cf9f92e6695c65aafabe532888b908a	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/i

Figure 5. The WD HDD file listing showing the disparity of parent folders and date/time stamps.

Created	Accessed	Modified	Path
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0079.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0080.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0081.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0082.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0083.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0084.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0085.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0086.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:56	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0087.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:56	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0088.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:56	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0089.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:32	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0090.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:32	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0091.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0092.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0093.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0094.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0095.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0096.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0097.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:34	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0098.JPG

Figure 6. A comparison of Modified Dates for IMG\_0175.JPG, which was modified.

Figure 6a. IMG\_0175 file system metadata from the recovered deleted file on the **CF Card** (GX 521 Replacement). This copy could NOT have contained an EXIF CreatorTool value set to “Photoshop Adobe Elements 3.0”.

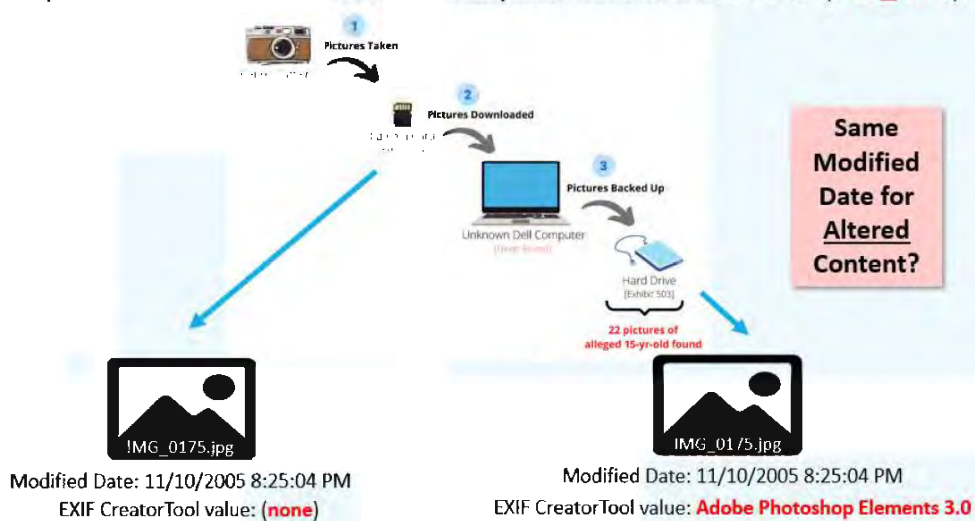
Name **IMG\_0175.JPG**  
Extension jpg  
Item Number 1064  
Path Lexar CF 2GB Card/Partition 1/LEXAR MEDIA [FAT16]/[root]/DCIM/101CANON/  
MG\_0175.JPG  
Created Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)  
Accessed Date 11/10/2005  
Modified Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)  
MD5 Hash  
Deleted True  
Carved False

Figure 6b. IMG\_0175 file system metadata from the **HDD** (GX 505A). This copy contained EXIF data with a CreatorTool value set to “Photoshop Adobe Elements 3.0”.

Name **IMG\_0175.JPG**  
Created Date 7/26/2003 2:06:31 PM (2003-07-26 18:06:31 UTC)  
Accessed Date 2/12/2010  
Modified Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)  
MD5 Hash 44725f873418dbf665de0198463f20c9  
Path 1B16 WD HD 500GB/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/  
BKP.DellDimension8300-20090330/Studies/A111005/2005-11-10-0718-42/IMG\_0175.JPG  
Exported as [Report Files/files/IMG\\_0175.JPG](#)

Figure 6c. File system metadata was altered to conceal EXIF data modification and support the government’s narrative.

File system metadata was altered to conceal photo content modification (IMG\_0175).



## Appendix B: File Listing Tables

**Table 1: Pictures on hard drive under “Studies” on the hard drive (GX 503)**

File Name	WD HDD FAT Modified Date	WD HDD EXIF DateTimeOriginal	Time Shift Between FAT Modified and EXIF DateTimeOriginal (within a few seconds)
IMG_0043.JPG	10/16/05 11:30:04 PM	10/17/05 12:30:04 AM	1
IMG_0044.JPG	10/17/05 3:53:24 PM	10/17/05 4:53:22 PM	1
IMG_0045.JPG	10/17/05 3:53:40 PM	10/17/05 4:53:40 PM	1
IMG_0046.JPG	10/17/05 3:54:08 PM	10/17/05 4:54:09 PM	1
IMG_0047.JPG	10/17/05 3:54:24 PM	10/17/05 4:54:24 PM	1
IMG_0048.JPG	10/17/05 3:54:38 PM	10/17/05 4:54:38 PM	1
IMG_0049.JPG	10/17/05 3:54:54 PM	10/17/05 4:54:54 PM	1
IMG_0050.JPG	10/17/05 3:55:04 PM	10/17/05 4:55:05 PM	1
IMG_0051.JPG	10/17/05 3:55:28 PM	10/17/05 4:55:28 PM	1
IMG_0052.JPG	10/17/05 3:55:42 PM	10/17/05 4:55:41 PM	1
IMG_0053.JPG	10/17/05 3:55:54 PM	10/17/05 4:55:52 PM	1
IMG_0054.JPG	10/17/05 3:55:58 PM	10/17/05 4:55:59 PM	1
IMG_0055.JPG	10/17/05 3:56:24 PM	10/17/05 4:56:25 PM	1
IMG_0056.JPG	10/17/05 3:56:36 PM	10/17/05 4:56:36 PM	1
IMG_0057.JPG	10/17/05 3:56:48 PM	10/17/05 4:56:48 PM	1
IMG_0058.JPG	10/17/05 3:56:58 PM	10/17/05 4:56:58 PM	1
IMG_0059-1.JPG	10/17/05 9:00:58 PM	10/17/05 10:00:57 PM	1
IMG_0060-1.JPG	10/17/05 9:01:06 PM	10/17/05 10:01:07 PM	1
IMG_0061-1.JPG	10/17/05 9:01:12 PM	10/17/05 10:01:13 PM	1
IMG_0062-1.JPG	10/17/05 9:01:24 PM	10/17/05 10:01:24 PM	1
IMG_0063-1.JPG	10/17/05 9:01:32 PM	10/17/05 10:01:32 PM	1
IMG_0064-1.JPG	10/17/05 9:02:00 PM	10/17/05 10:02:00 PM	1



IMG_0065-1.JPG	10/17/05 9:02:08 PM	10/17/05 10:02:07 PM	1
IMG_0066-1.JPG	10/17/05 9:02:14 PM	10/17/05 10:02:13 PM	1
IMG_0067-1.JPG	10/17/05 9:02:34 PM	10/17/05 10:02:34 PM	1
IMG_0068-1.JPG	10/17/05 9:03:02 PM	10/17/05 10:03:01 PM	1
IMG_0069-1.JPG	10/17/05 9:03:10 PM	10/17/05 10:03:10 PM	1
IMG_0070-1.JPG	10/17/05 9:03:24 PM	10/17/05 10:03:24 PM	1
IMG_0071.JPG	10/18/05 7:32:06 PM	10/18/05 8:32:06 PM	1
IMG_0072.JPG	10/18/05 7:32:26 PM	10/18/05 8:32:26 PM	1
IMG_0073.JPG	10/18/05 7:32:36 PM	10/18/05 8:32:36 PM	1
IMG_0074.JPG	10/18/05 7:32:44 PM	10/18/05 8:32:44 PM	1
IMG_0075.JPG	10/18/05 7:33:08 PM	10/18/05 8:33:09 PM	1
IMG_0076.JPG	10/18/05 7:33:14 PM	10/18/05 8:33:15 PM	1
IMG_0077.JPG	10/18/05 7:33:22 PM	10/18/05 8:33:22 PM	1
IMG_0078.JPG	10/18/05 7:33:30 PM	10/18/05 8:33:30 PM	1
IMG_0079.JPG	10/19/05 5:54:08 PM	10/19/05 6:54:09 PM	1
IMG_0080.JPG	10/19/05 5:54:22 PM	10/19/05 6:54:23 PM	1
IMG_0081.JPG	10/19/05 5:54:32 PM	10/19/05 6:54:33 PM	1
IMG_0082.JPG	10/19/05 5:54:56 PM	10/19/05 6:54:57 PM	1
IMG_0083.JPG	10/19/05 5:55:10 PM	10/19/05 6:55:10 PM	1
IMG_0084.JPG	10/19/05 5:55:36 PM	10/19/05 6:55:37 PM	1
IMG_0085.JPG	10/19/05 5:55:48 PM	10/19/05 6:55:49 PM	1
IMG_0086.JPG	10/19/05 5:55:56 PM	10/19/05 6:55:57 PM	1
IMG_0087.JPG	10/19/05 5:56:08 PM	10/19/05 6:56:09 PM	1
IMG_0088.JPG	10/19/05 5:56:24 PM	10/19/05 6:56:24 PM	1
IMG_0089.JPG	10/19/05 5:56:34 PM	10/19/05 6:56:34 PM	1
IMG_0090.JPG	10/19/05 6:32:52 PM	10/19/05 7:32:51 PM	1
IMG_0091.JPG	10/19/05 6:32:58 PM	10/19/05 7:32:57 PM	1

IMG_0092.JPG	10/19/05 6:33:08 PM	10/19/05 7:33:09 PM	1
IMG_0093.JPG	10/19/05 6:33:18 PM	10/19/05 7:33:18 PM	1
IMG_0094.JPG	10/19/05 6:33:26 PM	10/19/05 7:33:25 PM	1
IMG_0095.JPG	10/19/05 6:33:30 PM	10/19/05 7:33:29 PM	1
IMG_0096.JPG	10/19/05 6:33:52 PM	10/19/05 7:33:51 PM	1
IMG_0097.JPG	10/19/05 6:33:58 PM	10/19/05 7:33:57 PM	1
IMG_0098.JPG	10/19/05 6:34:08 PM	10/19/05 7:34:08 PM	1
IMG_0099.JPG	10/20/05 3:20:12 PM	10/20/05 4:20:13 PM	1
IMG_0100.JPG	10/20/05 3:20:30 PM	10/20/05 4:20:31 PM	1
IMG_0101.JPG	10/20/05 3:20:44 PM	10/20/05 4:20:44 PM	1
IMG_0102.JPG	10/20/05 3:21:02 PM	10/20/05 4:21:02 PM	1
IMG_0103.JPG	10/20/05 3:21:28 PM	10/20/05 4:21:28 PM	1
IMG_0104.JPG	10/20/05 3:25:14 PM	10/20/05 4:25:14 PM	1
IMG_0105.JPG	10/20/05 3:26:56 PM	10/20/05 4:26:56 PM	1
IMG_0106.JPG	10/20/05 3:27:04 PM	10/20/05 4:27:03 PM	1
IMG_0107.JPG	10/20/05 3:49:24 PM	10/20/05 4:49:23 PM	1
IMG_0108.JPG	10/20/05 3:49:26 PM	10/20/05 4:49:26 PM	1
IMG_0109.JPG	10/20/05 3:49:30 PM	10/20/05 4:49:29 PM	1
IMG_0110.JPG	10/29/05 4:11:16 AM	10/29/05 5:11:16 AM	1
IMG_0111.JPG	10/29/05 4:11:42 AM	10/29/05 5:11:43 AM	1
IMG_0112.JPG	10/29/05 4:43:36 AM	10/29/05 5:43:36 AM	1
IMG_0113.JPG	10/29/05 4:43:54 AM	10/29/05 5:43:54 AM	1
IMG_0115.JPG	10/29/05 4:44:52 AM	10/29/05 5:44:52 AM	1
IMG_0116.JPG	10/29/05 4:44:56 AM	10/29/05 5:44:55 AM	1
IMG_0117.JPG	10/29/05 4:45:06 AM	10/29/05 5:45:06 AM	1
IMG_0118.JPG	10/29/05 4:45:20 AM	10/29/05 5:45:20 AM	1
IMG_0119.JPG	10/29/05 4:45:26 AM	10/29/05 5:45:25 AM	1

IMG_0120.JPG	10/29/05 4:45:40 AM	10/29/05 5:45:40 AM	1
IMG_0121.JPG	10/29/05 4:45:50 AM	10/29/05 5:45:50 AM	1
IMG_0122.JPG	10/29/05 4:46:00 AM	10/29/05 5:46:00 AM	1
IMG_0123.JPG	10/29/05 4:47:00 AM	10/29/05 5:46:59 AM	1
IMG_0124.JPG	10/29/05 4:47:06 AM	10/29/05 5:47:05 AM	1
IMG_0125.JPG	10/29/05 4:47:10 AM	10/29/05 5:47:11 AM	1
IMG_0126.JPG	10/29/05 4:47:24 AM	10/29/05 5:47:24 AM	1
IMG_0127.JPG	10/30/05 2:34:20 AM	10/30/05 4:34:20 AM	2
IMG_0128.JPG	10/30/05 2:35:14 AM	10/30/05 4:35:14 AM	2
IMG_0129.JPG	10/30/05 2:36:06 AM	10/30/05 4:36:05 AM	2
IMG_0130.JPG	10/30/05 2:36:42 AM	10/30/05 4:36:42 AM	2
IMG_0131.JPG	10/30/05 2:36:54 AM	10/30/05 4:36:55 AM	2
IMG_0132.JPG	10/30/05 2:37:12 AM	10/30/05 4:37:12 AM	2
IMG_0133.JPG	10/30/05 2:37:44 AM	10/30/05 4:37:45 AM	2
IMG_0134.JPG	10/30/05 2:37:58 AM	10/30/05 4:37:58 AM	2
IMG_0135.JPG	10/30/05 2:38:00 AM	10/30/05 4:38:00 AM	2
IMG_0136.JPG	10/30/05 3:39:00 AM	10/30/05 5:39:00 AM	2
IMG_0137.JPG	10/30/05 3:39:06 AM	10/30/05 5:39:06 AM	2
IMG_0138.JPG	10/30/05 4:55:42 PM	10/30/05 4:55:41 PM	0
IMG_0139.JPG	10/30/05 4:55:52 PM	10/30/05 4:55:51 PM	0
IMG_0140.JPG	10/30/05 4:56:20 PM	10/30/05 4:56:21 PM	0
IMG_0141.JPG	10/30/05 4:56:46 PM	10/30/05 4:56:46 PM	0
IMG_0142.JPG	10/30/05 4:57:12 PM	10/30/05 4:57:12 PM	0
IMG_0143.JPG	10/30/05 6:01:08 PM	10/30/05 6:01:08 PM	0
IMG_0144.JPG	10/30/05 6:01:14 PM	10/30/05 6:01:14 PM	0
IMG_0145.JPG	10/30/05 6:01:20 PM	10/30/05 6:01:19 PM	0
IMG_0146.JPG	10/30/05 6:01:28 PM	10/30/05 6:01:28 PM	0

IMG_0147.JPG	10/30/05 6:02:08 PM	10/30/05 6:02:08 PM	0
IMG_0148.JPG	10/30/05 6:02:14 PM	10/30/05 6:02:15 PM	0
IMG_0149.JPG	10/30/05 6:02:22 PM	10/30/05 6:02:22 PM	0
IMG_0150.JPG	11/2/05 5:59:16 PM	11/02/05 5:59:16 PM	0
IMG_0151.JPG	11/2/05 5:59:26 PM	11/02/05 5:59:25 PM	0
IMG_0152.JPG	11/2/05 5:59:30 PM	11/02/05 5:59:30 PM	0
IMG_0153.JPG	11/2/05 5:59:34 PM	11/02/05 5:59:34 PM	0
IMG_0154.JPG	11/2/05 5:59:48 PM	11/02/05 5:59:47 PM	0
IMG_0155.JPG	11/2/05 6:00:22 PM	11/02/05 6:00:22 PM	0
IMG_0156.JPG	11/2/05 6:00:30 PM	11/02/05 6:00:29 PM	0
IMG_0157.JPG	11/2/05 6:00:38 PM	11/02/05 6:00:38 PM	0
IMG_0158.JPG	11/2/05 6:00:48 PM	11/02/05 6:00:49 PM	0
IMG_0159.JPG	11/2/05 6:01:10 PM	11/02/05 6:01:10 PM	0
IMG_0160.JPG	11/2/05 6:01:18 PM	11/02/05 6:01:18 PM	0
IMG_0161.JPG	11/2/05 6:09:00 PM	11/02/05 6:08:59 PM	0
IMG_0162.JPG	11/2/05 6:09:02 PM	11/02/05 6:09:02 PM	0
IMG_0163.JPG	11/2/05 6:09:10 PM	11/02/05 6:09:11 PM	0
IMG_0164.JPG	11/10/05 8:22:18 PM	11/10/05 8:22:18 PM	0
IMG_0165.JPG	11/10/05 8:22:30 PM	11/10/05 8:22:30 PM	0
IMG_0168.JPG	11/10/05 8:23:12 PM	11/10/05 8:23:12 PM	0
IMG_0169.JPG	11/10/05 8:23:26 PM	11/10/05 8:23:26 PM	0
IMG_0172.JPG	11/10/05 8:24:20 PM	11/10/05 8:24:19 PM	0
IMG_0174.JPG	11/10/05 8:24:48 PM	11/10/05 8:24:47 PM	0
IMG_0175.JPG	11/10/05 8:25:04 PM	11/10/05 8:25:04 PM	0
IMG_0176.JPG	11/10/05 8:25:10 PM	11/10/05 8:25:11 PM	0
IMG_0177.JPG	11/10/05 8:25:36 PM	11/10/05 8:25:35 PM	0
IMG_0178.JPG	11/10/05 8:25:54 PM	11/10/05 8:25:54 PM	0

IMG_0179.JPG	11/10/05 8:26:04 PM	11/10/05 8:26:04 PM	0
IMG_0180.JPG	11/10/05 8:26:22 PM	11/10/05 8:26:22 PM	0
IMG_0181.JPG	11/10/05 8:26:26 PM	11/10/05 8:26:25 PM	0
IMG_0182.JPG	11/10/05 8:26:30 PM	11/10/05 8:26:29 PM	0
IMG_0183.JPG	11/10/05 8:27:34 PM	11/10/05 8:27:33 PM	0
IMG_0184.JPG	11/24/05 9:07:50 PM	11/24/05 9:07:50 PM	0
IMG_0185.JPG	11/24/05 9:07:56 PM	11/24/05 9:07:55 PM	0
IMG_0186.JPG	11/24/05 9:08:08 PM	11/24/05 9:08:07 PM	0
IMG_0187.JPG	11/24/05 9:09:52 PM	11/24/05 9:09:52 PM	0
IMG_0188.JPG	11/24/05 9:10:08 PM	11/24/05 9:10:08 PM	0
IMG_0189.JPG	11/24/05 9:10:22 PM	11/24/05 9:10:23 PM	0
IMG_0190.JPG	11/24/05 9:10:28 PM	11/24/05 9:10:28 PM	0
IMG_0191.JPG	11/24/05 9:10:38 PM	11/24/05 9:10:37 PM	0
IMG_0194.JPG	12/18/05 12:37:58 AM	12/18/05 12:37:58 AM	0
IMG_0197.JPG	12/18/05 12:38:20 AM	12/18/05 12:38:20 AM	0
IMG_0198.JPG	12/18/05 12:38:28 AM	12/18/05 12:38:28 AM	0
IMG_0199.JPG	12/18/05 12:38:56 AM	12/18/05 12:38:55 AM	0
IMG_0203.JPG	12/25/05 2:59:44 AM	12/25/05 2:59:44 AM	0
IMG_0204.JPG	12/25/05 2:59:50 AM	12/25/05 2:59:50 AM	0
IMG_0205.JPG	12/25/05 3:00:42 AM	12/25/05 3:00:42 AM	0
IMG_0206.JPG	12/25/05 3:00:50 AM	12/25/05 3:00:49 AM	0
IMG_0207.JPG	12/25/05 3:01:40 AM	12/25/05 3:01:40 AM	0
IMG_0208.JPG	12/25/05 3:01:46 AM	12/25/05 3:01:46 AM	0
IMG_0209.JPG	12/30/05 5:56:06 PM	12/30/05 5:56:05 PM	0
IMG_0210.JPG	12/30/05 5:56:12 PM	12/30/05 5:56:11 PM	0
IMG_0211.JPG	12/30/05 5:56:16 PM	12/30/05 5:56:15 PM	0
IMG_0212.JPG	12/30/05 5:56:20 PM	12/30/05 5:56:20 PM	0

IMG_0213.JPG	12/30/05 5:56:46 PM	12/30/05 5:56:46 PM	0
IMG_0214.JPG	12/30/05 5:56:54 PM	12/30/05 5:56:53 PM	0
IMG_0215.JPG	12/30/05 5:56:56 PM	12/30/05 5:56:56 PM	0
IMG_0216.JPG	12/30/05 5:57:00 PM	12/30/05 5:56:59 PM	0
IMG_0217.JPG	12/30/05 5:58:50 PM	12/30/05 5:58:50 PM	0
IMG_0218.JPG	12/30/05 5:59:00 PM	12/30/05 5:58:59 PM	0
IMG_0219.JPG	12/30/05 5:59:08 PM	12/30/05 5:59:07 PM	0
IMG_0220.JPG	12/30/05 5:59:18 PM	12/30/05 5:59:18 PM	0
IMG_0221.JPG	12/30/05 5:59:56 PM	12/30/05 5:59:56 PM	0
IMG_0222.JPG	12/30/05 6:00:08 PM	12/30/05 6:00:08 PM	0
IMG_0223.JPG	12/30/05 6:00:24 PM	12/30/05 6:00:24 PM	0

## Appendix C: Analysis of Files Carved from HDD and CF Card

The content of four digital photos, IMG\_0180 through IMG\_0183, are the only ones that are exactly the same across both the CF card (GX 521A) and the external hard drive (GX 503), meaning they are the only photos whose file names and MD5 hashes match. Initially, this was **discovered by comparing the file hashes from two file listings, “CF card listing.csv” and “File Listing of Backup Folder (BKP.DellDimension8300-20090330).csv,” derived from the FBI’s FTK reports.**

In addition, I inspected two additional **file listings, “GX 521A Replacement (carved files)\_2019\_06\_11.csv” and “Full File Listing of Hard Drive Contents (GX 503).csv,”** which provided items *carved* from the CF card and external hard drive, respectively. In these listings I discovered a suspicious relationship between photos IMG\_0180 through IMG\_0183 and four other photos on the CF card, IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097, respectively.

Before I describe those relationships, however, it would be helpful for the reader to understand how carved files are generated. Figure 1 represents a digital photograph named **IMG\_0180.JPG**, which has a file size of 2,539,833 bytes (about 2.5 MB). The logical portion of the file consists of three primary components.

- **EXIF data**, which typically contains camera-generated metadata, is fixed length and occupies the first portion of the file from byte offset 0 to offset 9728.
- The second portion of the file is the picture **thumbnail**, a variable-length component that occupies the space between the end of the EXIF data (offset 9728) and the beginning of the main picture (offset 16845). Subtracting these two numbers provides the file size of the thumbnail, 7,117 bytes. When a forensic tool carves it from the parent file it is given the **file name “Carved [9728].jpeg,” indicating its starting location in the file.**
- The third portion of the file is the **main picture**, occupying the largest portion of the file at 2,522,988 bytes. Since the main picture begins at byte offset 16845, the carving forensic tool will give it a **file name of “Carved [16845].jpeg.”**

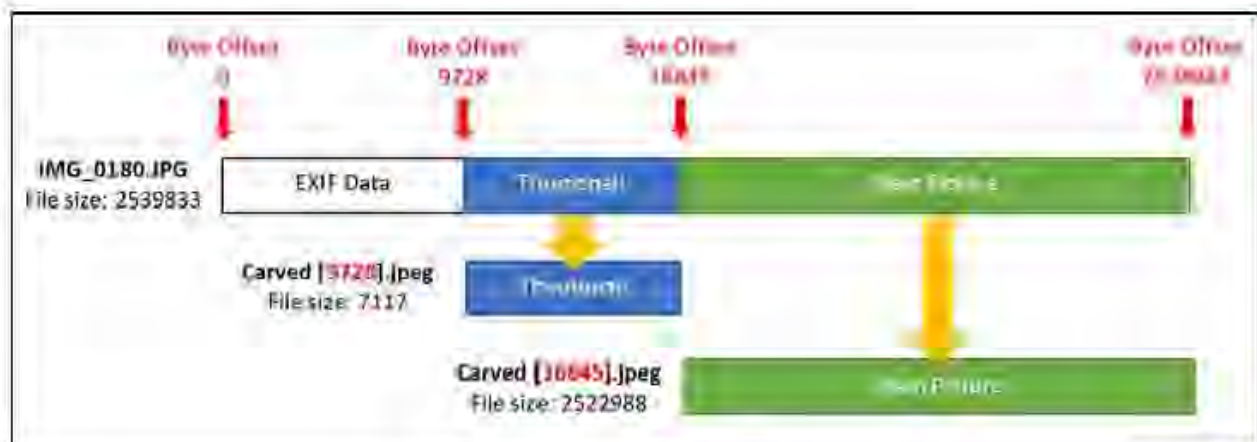


Figure 1. How a forensic tool creates and names files carved from digital photographs.

For brevity I will limit the discussion of the suspicious files (IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097) to the relationship between IMG\_0093 and IMG\_0180. The corresponding relationships between IMG\_0094, IMG\_0096, IMG\_0097 and IMG\_181, IMG\_182, IMG\_183, respectively, are identical.

Table 1 below was excerpted from “Full File Listing of Hard Drive Contents (GX 503).csv” and displays information about IMG\_0093 and IMG\_0180. As discussed elsewhere, the Created dates do not make sense. That anomaly aside, however, the file size information is consistent. For example, for each file the logical size (L-Size) added to the size of its corresponding FileSlack is equal to the physical size (P-size), as it should. Also, each of these files have corresponding carved files, including “Carved [9728].jpeg,” which is a thumbnail picture carved starting at byte offset 9728. With a single exception - as explained previously - the thumbnail files for each digital photograph in this case can be identified by the name “Carved [9728].jpeg.” A second carved file, “Carved [XXXXX].jpeg,” which is the main picture carved starting at byte offset XXXXX, will vary with each photo because thumbnail sizes are different. The table below demonstrates that subtracting the two starting byte offsets for the carved files (in red) predictably results in the logical size for the thumbnail (in blue).

Row	Name	Category	Created	Accessed	Modified	P-Size (bytes)	L-Size (bytes)	MD5
1	IMG_0093.JPG	JPEG EXIF	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	2523136	2500404	697cec1244dce 21ecc4f82cd3a7 64644
2	IMG_0093.JPG.File Slack	Slack Space	n/a	n/a	n/a	22732	22732	
3	Carved [14844].jpeg	JPEG	n/a	n/a	n/a	n/a	2485560	ae6cbe511c9f3b dec52917e3dca 05129
4	Carved [9728].jpeg	JPEG	n/a	n/a	n/a	n/a	5116	51202a6c4b8e6 084f153456561 56481c
5	IMG_0180.JPG	JPEG EXIF	7/26/2003 11:06	2/12/2010	11/10/2005 17:26	2555904	2539833	f6202d0b41e30 c7c21aeae32c38 baf9b
6	IMG_0180.JPG.File Slack	Slack Space	n/a	n/a	n/a	16071	16071	
7	Carved [16845].jpeg	JPEG	n/a	n/a	n/a	n/a	2522988	b991eaa84b4d9 1dfa2d0eece1e9 02430
8	Carved [9728].jpeg	JPEG	n/a	n/a	n/a	n/a	7117	6babe3f7c2bd2c 6c73d15e3d2db 42a95

**Table 1. Excerpt from “Full File Listing of Hard Drive Contents (GX 503).csv.”**



Next we turn our attention to an excerpt from “GX 521A Replacement (carved files)\_2019\_06\_11.csv,” which also displays information about IMG\_0093 and IMG\_0180 - but on the CF card. There are several inconsistencies with this data (See Table 2).

- The file named “Carved [2129920].jpeg” indicates the file was carved from IMG\_0093 starting at byte offset 2129920. This would mean the file would have been carved starting near the *end* of the digital photo file, which has a logical size of 2500404 bytes according to the previous table. There was no file size data present in this file listing (which is suspicious in itself). However, subtracting 2129920 from 2500404 yields a maximum file size of 370484 bytes for this carved file, which is too large to be a thumbnail and too small to be the main picture data for the photo.
- In row 2 a file named “Carved [16845].jpeg” indicates the file was carved from “Carved [2129920].jpeg” (which was itself carved from IMG\_0093) starting at byte offset 16845. Surprisingly, this is **precisely the same byte offset** that began the main picture carving in IMG\_0180 as shown in this table (row 5) and verified in the previous table by a matching MD5 hash (See Table 1, row 7).
- As discussed earlier, files in this case named “Carved [9728].jpeg” are thumbnails that are carved from their parent photo files starting at byte offset 9728. However, the **same thumbnail** (with matching hashes) was **carved from two different files, IMG\_0093 and IMG\_0180**. (See Table 2, rows 3-4 and compare at Table 1, row 8).

Row	Path	Hash	Name	Deleted?
1	/DCIM/100CANON/! MG_0093.JPG»Carved [2129920].jpeg	8514c14257901fca23dab82db71f6c0c	! MG_0093.JPG»Carved [2129920].jpeg	Y
2	/DCIM/100CANON/! MG_0093.JPG»Carved [2129920].jpeg»Carved [16845].jpeg	d4831cccb7f5ac74632cc09a32d28515	! MG_0093.JPG»Carved [2129920].jpeg»Carved [16845].jpeg	Y
3	/DCIM/100CANON/! MG_0093.JPG»Carved [2129920].jpeg»Carved [9728].jpeg	6babe3f7c2bd2c6c73d15e3d2db42a95	! MG_0093.JPG»Carved [2129920].jpeg»Carved [9728].jpeg	Y
4	/DCIM/101CANON/! MG_0180.JPG»Carved [9728].jpeg	6babe3f7c2bd2c6c73d15e3d2db42a95	! MG_0180.JPG»Carved [9728].jpeg	Y
5	/DCIM/101CANON/! MG_0180.JPG»Carved [16845].jpeg	b991eaa84b4d91dfa2d0eece1e902430	! MG_0180.JPG»Carved [16845].jpeg	Y

**Table 2. Excerpt from “GX 521A Replacement (carved files)\_2019\_06\_11.csv” (second listing for the CF card, with no file sizes present).**

As mentioned previously, the same pattern appears in the file listings for relationships between IMG\_0094 and IMG\_0181, IMG\_0096 and IMG\_0182, and IMG\_0097 and IMG\_0183. Two additional observations point to IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097 being counterfeit files on the CF card:

- With the exception of unallocated space, the files IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097 are the only files in the CF card file listing with apparent nested carving (carving from carved files).
- Unlike the consistency of files IMG\_0180 to IMG\_0183, the byte offset data and MD5 hashes of files IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097 are NOT consistent between Tables 1 and 2 (i.e., between the hard drive and CF card).

### **Other anomalous behavior**

Additional analyses of the CF card and WD HDD file listings reveal bizarre patterns that support the finding that files were altered and transferred between devices:

- A group of files located on the WD HDD were given **nonstandard file names**, from IMG\_0059-1 to IMG\_0070-1. Neither the 04/11/2019 nor the 06/11/2019 CF card file listings contain any record of these photos existing on the CF card, despite their camera-related EXIF data being identical to all the others. Notably, these names were not assigned automatically by the camera, but were rather created by a user action, thus proving at least one aspect of metadata editing.
- The CF card file listing shows large swaths of missing file name sequences, and sequences with no content, punctuated by groups of 5-6 files with recoverable content (see Table 3). This is not consistent with normal use of a camera, where the user might review and choose to occasionally delete unwanted photographs as desired. Rarely would this deletion activity follow such a distinctive pattern as what appears in the file listing. However, the pattern would be consistent with someone copying photos between the CF card and an unknown computer.

Name	Delete	Created	Accessed	Modified	Hash	Path
IMG_0089.JPG	Y	10/19/2005 18:56	10/19/2005	10/19/2005 18:56	NO HASH	Lexar CF 2GB Card/
IMG_0090.JPG	Y	10/19/2005 19:32	10/19/2005	10/19/2005 19:32	NO HASH	Lexar CF 2GB Card/
IMG_0091.JPG	Y	10/19/2005 19:32	10/19/2005	10/19/2005 19:32	NO HASH	Lexar CF 2GB Card/
IMG_0092.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	NO HASH	Lexar CF 2GB Card/
IMG_0093.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	04e96f3f0f48c3b117cbf4bcd516a857	Lexar CF 2GB Card/
IMG_0094.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	97d26874707bf3f97e76fc22b57d86d0	Lexar CF 2GB Card/
IMG_0095.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	81f59288eb1ca3ce02826f1ce46dc4d5	Lexar CF 2GB Card/
IMG_0096.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	884764bfbb7a72ed5f726af5d5eb11b5	Lexar CF 2GB Card/
IMG_0097.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	5cb3245ec43bf2d9b0e373995336deee	Lexar CF 2GB Card/
IMG_0098.JPG	Y	10/19/2005 19:34	10/19/2005	10/19/2005 19:34	452db09a0de54234504bb1211f6c30eb	Lexar CF 2GB Card/
IMG_0099.JPG	Y	10/20/2005 16:20	10/20/2005	10/20/2005 16:20	NO HASH	Lexar CF 2GB Card/
IMG_0100.JPG	Y	10/20/2005 16:20	10/20/2005	10/20/2005 16:20	NO HASH	Lexar CF 2GB Card/
GAP - Alleged contraband images 0150-0163 do not appear here at all						
IMG_0172.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24	NO HASH	Lexar CF 2GB Card/
IMG_0173.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24	NO HASH	Lexar CF 2GB Card/
IMG_0174.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24	NO HASH	Lexar CF 2GB Card/
IMG_0175.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0176.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0177.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0178.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0179.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	ab069f934603db10d2b579a5323a117c	Lexar CF 2GB Card/
IMG_0180.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	f6202d0b41e30c7c21aee32c38baf9b	Lexar CF 2GB Card/
IMG_0181.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	c22d37f14011b042388917706a89c4a9	Lexar CF 2GB Card/
IMG_0182.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	550df2c454f2c70cc0911f6ceaad4549	Lexar CF 2GB Card/
IMG_0183.JPG	Y	11/10/2005 20:27	11/10/2005	11/10/2005 20:27	b0d057b32850bfc7c20674f7dfa1ae3a	Lexar CF 2GB Card/
GAP - Alleged contraband images 0184-0191 do not appear here at all						
IMG_0193.JPG	Y	12/19/2005 0:37	12/19/2005	12/19/2005 0:37	NO HASH	Lexar CF 2GB Card/

Table 3. Analysis showing conspicuous gaps in data appearing in the CF card file listing.

### Summary

According to the file paths and hash values I observed, the carving byte offset data and thumbnails are exactly the same in two sets of files purported to be different. To be clear, two different digital photographs would *never* share exactly the same thumbnail picture. It is impossible without manual intervention. Moreover, the photographs IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097, produced multiple, duplicate carved files, which on flash media is indicative of file modification. By contrast, all the other files on the CF card file listing contain exactly two carved files: a thumbnail named “Carved [9728].jpeg” and a carved main picture named “Carved [XXXXXX].jpeg.”

Given the above facts, I believe the following actions describe the most plausible explanation for what I observed with regard to the eight files in question.

These four files (IMG\_0180 through IMG\_0183) were either manually copied from an unknown computer to the CF card or else were copied from the CF card to the unknown computer, where **they were “backed up” to the external hard drive. This action would explain** the fact that these four files (the only four of about 200) actually matched hashes between devices. Also, it is likely that someone copied another version of these *same four files* to the CF card, altered their content, and renamed them to IMG\_0093, IMG\_0094, IMG\_0096, and IMG\_0097. These actions would

explain 1) why these files bear no resemblance to those on the hard drive with the same file names, 2) why they contain the identical thumbnail pictures and common starting byte offsets as those contained in the IMG\_0180 to IMG\_0183 files, 3) why there are multiple, carved instances of these files on the flash media, and 4) why none of these files appeared on the 04/11/2019 CF card file listing while appearing on the subsequent 06/11/2019 file listing. There are no plausible natural or automated causes to explain such phenomena.

In summary, the forensic evidence demonstrates that alterations were intentionally made to files on the CF card, and the differences between the 04/11/2019 and 06/11/2019 file listings suggest those alterations took place while the CF card was in the custody of the FBI, as the devices were collected on March 27, 2018.

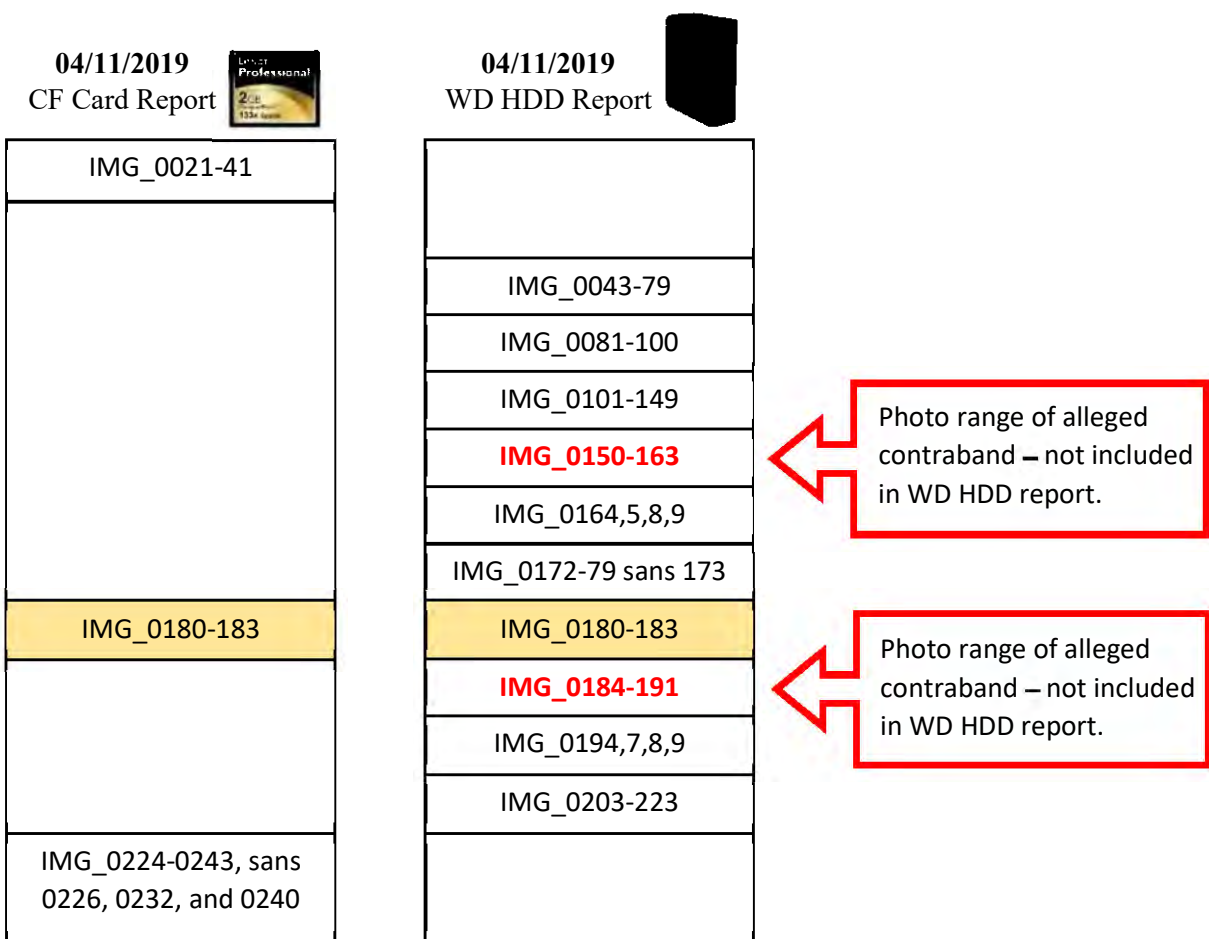
## Appendix D: Description of New Files Appearing on the FBI’s Forensic Report Between 04/11/2019 and 06/11/2019

By J. Richard Kiper, PhD, PMP  
FBI Special Agent (Retired) and Forensic Examiner

**Introduction:**

In the present case, U.S. vs KEITH RANIERE, the FBI completed two forensic examinations and generated two different reports on the same piece of evidence: A compact flash (CF) card found in a digital camera case. The Government claimed that digital photographs from this CF Card were eventually backed up to a Western Digital hard disk drive (WD HDD), which also contained alleged child pornography. **The government’s narrative depended on** creating a strong connection between the CF Card, allegedly belonging to the defendant, and the WD HDD that supposedly backed up photos from the CF Card. This brief analysis offers a plausible explanation for why a second examination, and a second report of the CF Card, were generated by an FBI forensic examiner (FE)<sup>1</sup>.

**Figure 1: Files Appearing on the First FBI Forensic Reports of the CF Card and WD HDD**




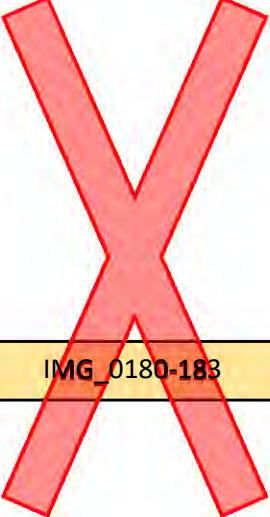


**Observations:**

- Both forensic reports were generated on the same day, **April 11, 2019**.
- The **CF Card report** was created by **FE Stephen Flatley**, who kept the CF Card until 06/07/2022.
- The **WD HDD report** was created by **FE Brian Booth**, using a forensic copy made by his trainee.
- Only **four photos**, named IMG\_0180-183, are common to both forensic reports (highlighted yellow).
- At this time **no other files** on the CF Card report could be shown to be **“backed up” to the WD HDD**.

<sup>1</sup> For more information about the background of the case and the Government’s narrative presented at trial, please see my full reports detailing Technical and Process Findings.

**Figure 2: Generating the Second FBI Forensic Report on the CF Card (June 11, 2019)**

04/11/2019 CF Card Report 	06/11/2019 CF Card Report 	04/11/2019 WD HDD Report 
IMG_0021-41	IMG_0021-41	
	IMG_0042	
	IMG_0081-100	IMG_0043-80
		IMG_0081-100
		IMG_0101-149
		<b>IMG_0150-163</b>
IMG_0180-183	IMG_0172-179	IMG_0164,5,8,9
	IMG_0180-183	IMG_0172-79 sans 173
	IMG_0193-200	IMG_0180-183
		<b>IMG_0184-191</b>
IMG_0224-0243, sans 0226, 0232, and 0240	IMG_0224-0243, sans 0226, 0232, and 0240	IMG_0194,7,8,9
		IMG_0203-223

**Observations:**

- As documented in the Chain of Custody, SA Mills delivered the CF Card, in an **unsealed bag**, to FE Booth on 06/10/2019, during the last week of trial and more than **14 months** after the search team had collected it.
- SA Lever requested that FE Booth complete a **new examination** and a **new “replacement” report** (dated 06/11/2019 in the above figure).
- **None** of the new files appearing on the 06/11/2019 report (shaded green) was viewable in the report.
- No explanation was provided for the appearance of the new files or why they were **unviewable**.
- **All** the previous CF Card files (in white) are viewable in both CF Card reports.
- It is extremely unlikely that **eight of the new files** on the 6/11 CF Card report (IMG\_0172-179) just happen to occupy the filename space before the small group of “common” photos (IMG\_0180-183) and then **another eight new files** (IMG\_0193-200) just happen to appear right after the alleged contraband photo range (IMG\_0184-191), which themselves just happen to appear immediately after the common photos.
- The **alleged contraband** photos, **IMG\_0150-163** and **IMG\_0184-191**, appear in neither of the CF Card reports. **If the government’s narrative was correct**, then one would reasonably expect some remnants of these photos **to have been included on the FBI’s reports**.
- IMG\_0042 appears **only** on the 6/11 CF Card report – so it seems to fill a filename **“gap.”**
  - IMG\_0021-0041 appear on the 4/11 CF Card report but not on the WD HDD report.
  - IMG\_0043-0179 appear on the WD HDD report but not on the 4/11 CF Card report.
- The new file ranges on the 6/11 report are **uninterrupted**. Unlike the WD HDD report, there are no missing file names or gaps within each group of new files.

**Figure 3: Evidence Supporting the Addition of New Files to the CF Card**

IMG_0079.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0079.JPG
IMG_0080.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0080.JPG
IMG_0081.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0081.JPG
IMG_0082.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0082.JPG
IMG_0083.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0083.JPG
IMG_0084.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0084.JPG
IMG_0085.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0085.JPG
IMG_0086.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0086.JPG
IMG_0087.JPG	10/19/05 2:56 PM	/Msk101905/2005-10-19-0727-59/IMG_0087.JPG
IMG_0088.JPG	10/19/05 2:56 PM	/Msk101905/2005-10-19-0727-59/IMG_0088.JPG
IMG_0089.JPG	10/19/05 2:56 PM	/Msk101905/2005-10-19-0727-59/IMG_0089.JPG
IMG_0090.JPG	10/19/05 3:32 PM	/Df101905/2005-10-19-0727-57/IMG_0090.JPG
IMG_0091.JPG	10/19/05 3:32 PM	/Df101905/2005-10-19-0727-57/IMG_0091.JPG
IMG_0092.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0092.JPG
IMG_0093.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0093.JPG
IMG_0094.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0094.JPG
IMG_0095.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0095.JPG
IMG_0096.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0096.JPG
IMG_0097.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0097.JPG
IMG_0098.JPG	10/19/05 3:34 PM	/Df101905/2005-10-19-0727-57/IMG_0098.JPG
IMG_0099.JPG	10/20/05 12:20 PM	/Mnp102005/2005-10-20-0640-31/IMG_0099.JPG
IMG_0100.JPG	10/20/05 12:20 PM	/Mnp102005/2005-10-20-0640-31/IMG_0100.JPG
IMG_0101.JPG	10/20/05 12:20 PM	/Mnp102005/2005-10-20-0640-31/IMG_0101.JPG
IMG_0102.JPG	10/20/05 12:21 PM	/Mnp102005/2005-10-20-0640-31/IMG_0102.JPG
IMG_0103.JPG	10/20/05 12:21 PM	/Mnp102005/2005-10-20-0640-31/IMG_0103.JPG
IMG_0104.JPG	10/20/05 12:25 PM	/Mnp102005/2005-10-20-0640-31/IMG_0104.JPG
IMG_0105.JPG	10/20/05 12:26 PM	/Mnp102005/2005-10-20-0640-31/IMG_0105.JPG
IMG_0106.JPG	10/20/05 12:27 PM	/Mnp102005/2005-10-20-0640-31/IMG_0106.JPG
IMG_0107.JPG	10/20/05 12:49 PM	/Mnp102005/2005-10-20-0640-31/IMG_0107.JPG
IMG_0108.JPG	10/20/05 12:49 PM	/Mnp102005/2005-10-20-0640-31/IMG_0108.JPG

Why were **only the last nine photos** (not the first two) from **Msk101905** added to the new 6/11 CF Card Report?

Photo files shaded in green were added to the **06/11** CF Card report and did not appear on the **4/11** report.

Why were **only the first two photos** (not the last eight) from **Mnp102005** added to the new 6/11 CF Card Report?

**Observations:**

- The above file listing was adapted from the WD HDD report, so **all** these files appear in the “**backup**” drive.
- **None** of these files appear on the 4/11 CF Card report.
- Files shaded in **green** appear on the 6/11 CF Card report, but none of them are viewable on that report.
- Files with a **red** boundary were located in the WD HDD’s Msk101905 folder.
- Files with a **blue** boundary were located in the WD HDD’s Mnp102005 folder.
- It is **extremely unlikely** that photos would have been saved to and deleted from the CF Card in this manner as a result of normal user behavior (See Implications discussion below).

## Implications

As explained elsewhere, the Government claimed that digital photos, including **alleged contraband**, had been created with a Canon camera, saved to **the camera's CF card, transferred to an unknown computer, and then backed up to the WD HDD**. **Figure 1** illustrates the initially weak relationship between files on the CF card and the alleged **"backup"** of those files contained in the WD HDD. In fact, **according to the FBI's report on 04/11/2019, only four photographs** were reported as being common to both devices.

In **Figure 2**, however, the introduction of **new files to the FBI's 06/11/2019 "replacement"** forensic report creates an obviously stronger relationship between the devices. In all, 37 photos with filenames matching those on the WD HDD were added to the 06/11/2019 report in small, contiguous groups of files. Unfortunately – or perhaps, *conveniently* – **none of the new files were viewable** as photographs in the second report. As a result, none of the new files could be verified visually or forensically against their namesakes on the WD HDD report.<sup>2</sup> The FBI never provided an explanation for the appearance of new photos on the 06/11/2019 report or why they were the only photos on the CF card that were not viewable in the report.

**Figure 3** requires a more robust explanation. In the case of the new files **IMG\_0081-100** (highlighted in green), it seems that someone decided to **add the appearance of those 20 files** using round start and end **file numbers** – but without regard for the three separate **folders** into which their namesakes would eventually be discovered on the WD HDD **"backup."** To accept the integrity and completeness of the 6/11 CF Card report, one must believe that the user:

- Took photos IMG\_0079-89 on the CF Card,
- Saved the eleven photos to the Msk101905/2005-10-19-0727-59 folder on the unknown computer,
- Returned to the CF Card and *securely deleted*<sup>3</sup> the only the first two photos in that series (IMG\_0079-80),
- Took photos IMG\_0099-108 on the CF Card,
- Saved the ten photos to the /Mnp102005/2005-10-20-0640-31 folder on the unknown computer, and
- Returned to the CF Card and *securely deleted* all BUT the first two photos in the series (IMG\_0099-100).

Such a creating, saving and deleting behavior is extremely unlikely (securely deleting from the camera only the first two photos in one series and all BUT the first two photos in a subsequent series). That the user would just happen to selectively curate and delete photos with consecutive filenames like this – based on content – is not a reasonably credible scenario.

A more plausible explanation is that someone with physical control of the CF Card:

- Recognized the **weak relationship** between the photos reported on the 04/11/2019 CF Card report and those reported as **"backup" files on the WD HDD**, including alleged contraband,
- Examined the file listing of the WD HDD and chose a convenient range based on **filenames** (IMG\_0081-100) rather than their saved **folders**,
- **Created the appearance** (through file and metadata manipulation) that those files had been discovered on the CF Card as reported on the 06/11/2019 report, and
- Botched the file creation and deletion of the new files, rendering them **unviewable** in the 06/11/2019 report.

---

<sup>2</sup> The Modified date/time stamps between the new files in the 06/11/2019 report and their namesakes on the WD HDD did match. However, as explained in my report of Technical Findings, such metadata is easily changed and in this case it was obviously manipulated, enhancing the CF Card – WD HDD relationship required by the Government's narrative.

<sup>3</sup> By *securely deleted* I refer to the process of selectively overwriting physical sectors on the media so that the files cannot be recovered by forensic tools. Selectively eradicating photos in this way is not something a normal user would be able to accomplish. If the deleted photos were recoverable, then the FBI would have included them in the second CF card report.



**Conclusion:**

The defense team was **provided the FBI's forensic report of the CF Card generated on 04/11/2019 and then the second "replacement" report**, which was generated on 06/11/2019 and contained 37 additional files.

Along with the appearance of new files on a second CF Card forensic report, it is also undisputed that the **contents of the CF card were modified** on 09/19/2018, while in FBI custody, and that the CF card was delivered to FE Brian Booth in an **unsealed** cellophane bag just two days before FE Booth took the stand.<sup>4</sup> Therefore, in my expert opinion all indications of means, motive, and opportunity point to FBI employees **creating the appearance of additional files** on the CF Card in order to substantiate a relationship between the CF Card and the WD HDD containing the alleged contraband.

---

<sup>4</sup> These two facts were verified by FE Brian Booth in his sworn testimony.

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

## Summary of Process Findings

### Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

### Review of Evidence

My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports generated by members of the FBI's **Computer Analysis Response Team (CART)**. Based on my review, I have observed several technical, administrative, and evidence handling irregularities that raise serious concerns about the integrity of the evidence. Specifically, in this paper I describe violations of processes and procedures which occurred in this case and that likely affected the outcome at trial.

### Key Findings

#### **Finding 1: Receiving unsealed evidence created a broken Chain of Custody.**

- Neither the camera (Court transcript, p. 4886) nor the CF card (p.4889) was sealed when delivered to CART Forensic Examiner (FE) Brian Booth on 06/10/2019, two days before he took the stand. The FBI Chain of Custody for the CF card (DX 945) indicates that at least three FBI employees – FE Stephen Flatley, SA Elliot McGinnis, and SA Christopher Mills – had physical control of the evidence from the date a reexamination was requested (06/07/2019) to the date it was delivered to FE Booth in an unsealed package (06/10/2019).
- **FE Booth's exam notes (DX 961)** make no mention of the chain of custody, or of the fact that he received the evidence in unsealed packaging, although in court he admitted it was unsealed when he received it (p.4886 and p.4905). As I will discuss later, FBI policy requires the securing and sealing of evidence, and employees may be disciplined if they fail to do so. In my experience with the FBI, I never received unsealed evidence other than in exigent (emergency) situations.

**Finding 2: FBI employees engaged in unusual evidence handling procedures.**

- **What normal looks like:** Large FBI offices like the New York Division, where the evidence was processed, have a centralized evidence control and storage facility sometimes referred to as the Evidence Control Unit (ECU). Normally, evidence is collected at a search site by the case agent or a designated seizing agent, and a description of the collected items is entered into Sentinel, the FBI's case management system. Then the agent has up to ten days to physically turn over the evidence to Evidence Control with the chains of custody. After the case agent submits a written request to have the evidence examined, the assigned CART examiner would check out the relevant evidence items from Evidence Control and sign the chains of custody. In her notes (DX 961), Forensic Examiner Trainee (FET) Virginia Donnelly recorded multiple instances where she created derivative evidence items (forensic copies, extractions, and backups of the originals) and turned them into Evidence Control. This is also normal.
- **Abnormalities in this case:** The digital evidence seized on 03/27/2018 seemed to be in and out of the physical control of the case agents, rather than primarily managed through the ECU as described above. Although the evidence was first turned into ECU by the ten-day deadline, it was subsequently checked out by individuals who were not authorized to review digital evidence. The chain of custody for the Camera and CF Card, for example, indicate that the evidence was checked out by SA Maegan Rees on 07/10/2018 for 17 days and by SA Michael Lever 09/19/2018 for seven days – before it was first examined by a CART examiner on 02/22/2019. Both SA Rees and SA Lever indicated “Review” as the reason they were checking the evidence out of the ECU, but **neither of these individuals were authorized to review the contents of unexamined digital evidence**<sup>1</sup>.
- Based on my own experience, a case agent would leave digital evidence in the ECU until a CART examiner is requested to check out and examine the evidence. For digital evidence, there is no good reason to check it out of Evidence Control, because the case agent cannot possibly gain any investigative benefit from retaining evidence that he or she cannot examine.
- According to the Chain of Custody for the WD HDD (DX 960), the last person to accept custody of the device was SA Michael Lever, who checked it out from ECU on 02/22/2019. The reason SA Lever provided was “SW,” presumably meaning “search warrant,” but it is unknown what actions SA Lever took on the WD HDD, or who took custody of the device when he was finished with it. Although the WD HDD had been forensically imaged (copied) by FET Donnelly on 09/19/2018 and processed on 09/24/2018, FE Booth did not generate a report of its contents until 04/11/2019.

---

<sup>1</sup> In their report regarding the Lawrence Nassar case, the DOJ/OIG made public certain information regarding the FBI's evidence handling procedures: “According to the FBI's Field Evidence Management Policy Guide, evidence must be documented into the FBI Central Recordkeeping System no later than 10 calendar days after receipt. Similarly, the Digital Evidence Policy Guide states that, ‘Undocumented, “off the record” searches or reviews of [digital evidence] are not permitted” (p. 13). (<https://oig.justice.gov/sites/default/files/reports/21-093.pdf>)

- Finally, FE Booth’s examination notes (DX 961) end abruptly after he created a forensic copy of the CF card. Strangely absent from his notes are the options he chose while processing the data with AD Lab, the generation of the “replacement FTK report” presented at trial or the final disposition of the original or derivative evidence. Such details would complete a normal CART forensic report.

**Finding 3: The CF Card was accessed by an unauthorized FBI employee.**

- According to the FTK reports, the last Accessed dates for active files on the CF card was 09/19/2018 – six months after the CF was collected by investigators and five months before it was first delivered to an authorized CART examiner.
- According to FBI Chain of Custody for the Camera and CF Card (DX 945), the FBI employee who had physical control over the CF card between 09/19/2018 and 09/26/2018 was SA Michael Lever, who recorded “Evidence Review” as his reason for accepting custody (see my Technical Findings report). SA Lever was the primary case agent and not a CART examiner, meaning he was not authorized to review the unexamined digital evidence.
- The FBI’s Digital Evidence Policy Guide expressly prohibits any “Undocumented, ‘off the record’ searches or reviews of digital evidence” and permits investigators to review digital evidence only after it has been processed by an authorized method.<sup>2</sup>
- According to the same Chain of Custody, SA Maegan Rees had previously checked out the Camera and CF card for “Review” on 07/10/2018 and kept them for 17 days. She is also not a CART examiner and also would be prohibited from reviewing unexamined digital evidence. However, if she did access the CF card without a write blocker, then the last Accessed dates would have been overwritten two months later by the actions of SA Lever, who did access the CF card without a write blocker.
- Therefore, there is no doubt the CF card was accessed by at least one unauthorized FBI employee using an unauthorized process.

**Finding 4: The CF Card was altered at least once, and likely twice, while in FBI Custody.**

- **On 9/19/2018:** File system dates were overwritten on the CF card on at least one occasion, on 09/19/2018, while in FBI custody. This means, at a minimum, that the CF card was accessed without the use of a write blocking device. Failing to preserve digital evidence against alteration is an automatic fail in many of the FBI forensics classes I have taught because write blocking is a critical procedure that, if skipped, becomes an admissibility issue in court.
- **Between 4/11/2019 and 6/11/2019:** According to an FTK forensic report of the CF card completed on 4/11/2019 by “srflatley” (FE Stephen Flatley) and another report completed

---

<sup>2</sup> *Ibid*, p.13. See also p. 83: “according to the FBI’s Removable Electronic Storage Policy Directive, employees may not connect non-FBI removable electronic storage, such as a thumb drive, to FBI equipment without authorization.”

on 6/11/2019 by “bsbooth” (FE Brian Booth), several files appeared on the second report that were not included on the first report. For reasons I described in my Technical Findings report (see Technical Findings #1 and #2), there is a high likelihood the new files were added to the CF card and altered between these dates. In Appendix D of my Technical Findings report, I explained why adding new files to the CF card could have been used to support the government’s narrative regarding the origin of photos on the WD HDD device.<sup>3</sup>

- The difference between the FTK reports cannot be attributed to the use of a different tool, because both examiners used the same tool and version number: AccessData Forensic Toolkit, Version 6.3.1.26.

**Finding 5: The FBI Expert Witness knowingly gave false testimony.**

- **FE Booth testified that receiving unsealed evidence is not extraordinary (p. 4887).** This characterization by Booth is false, as all CART examiners are trained to receive evidence that has been sealed and initialed.<sup>4</sup> According to FBI evidence handling protocols, anytime a seal is broken on evidence, it must be resealed with a date and initials before relinquishing it to the next person in the chain of custody.<sup>5</sup>
- **FE Booth testified he did not know who had the evidence prior to his examination – two days prior to his testimony.** When he was asked, “And who was it that had access to the camera or the box prior to the time of your examination of it?” FE Booth answered, “I don’t have that evidence sheet in front of me to be able to refer” (p. 4889). As mentioned previously, according to FE Booth’s examination notes (DX 961), it was the “Case Agent” (but in fact SA Mills) who gave Booth the unsealed camera and CF card on 06/10/2019. It is not credible that FE Booth after two days could have forgotten the person who gave him the one piece of evidence he processed alone during the case.
- **FE Booth repeatedly testified to the reliability of EXIF data, and that it is “very hard to remove,” (p. 4819) and “it’s not easily modifiable” (p. 4830).** In fact, there are several readily available tools that can easily modify EXIF data. This is a fact that would be well-known to any forensic examiner (see **Appendix A** for a white paper I wrote demonstrating – with screen shots – how easy it is to modify EXIF data). Also, prosecutor Mark Lesko used Booth’s false testimony about EXIF data as the basis for his argument that the alleged contraband photos were taken in 2005: “[EXIF] data is

---

<sup>3</sup> I base this finding on 1) the fact that CF card files were altered, 2) the motive for adding new files (to support the relationship between the CF card and WD HDD), and 3) the opportunity for alteration (the CF card was outside of Evidence Control for several months). This finding could be significantly strengthened (or disputed) if I were to be given access to both forensic copies of the CF card created on 04/11/2019 and 06/11/2019.

<sup>4</sup> The aforementioned DOJ/OIG report (<https://oig.justice.gov/sites/default/files/reports/21-093.pdf>), p.13 states digital evidence “must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious change.”

<sup>5</sup> *Ibid*, p.83 “Moreover, the FBI Offense Code subjects FBI employees to discipline if they fail to “properly seize, identify, package, inventory, verify, record, document, control, store, secure, or safeguard documents or property under the care, custody, or control of the government.”

extremely reliable. It's embedded in the jpeg, in the image itself. And the [EXIF] data shows that the data was created on the camera, in this instance, this particular instance, the 150 jpeg on November 2, 2005 which is consistent with the title of the folder." (p. 5571).

- **FE Booth minimized his knowledge about the previous CF card examination.** On page 4987 of the court transcript FE Booth acknowledged that the government had asked him to create "another report," meaning *in addition to the one created by FE Steven Flatley*. Therefore FE Booth knew, at a minimum, that FE Flatley had conducted an inventory of the camera and CF card, created a forensic copy the CF card, examined it with FTK (AD LAB), and then used FTK to create a report. However, when asked about his knowledge of what FE Flatley had done with the camera and CF card, FE Booth responded, "All I know is that he received it on that date. I have no idea exactly what he's done on the camera" (p. 4988).
- **FE Booth failed to disclose that his actions constituted a prohibited re-examination of digital evidence.** According to FE Booth's notes (DX 961), on 06/07/2019 SA Lever requested that FE Booth "process" item 1B15 (the Camera and the CF card) because FE Flatley "would be overseas during trial."
  - However, according to the Chain of Custody (DX 945) FE Flatley relinquished custody of the CF card to SA McGinnis on this same day (06/07/2019), so he was not yet "overseas."
  - FE Flatley was available to testify to his examination of the CF card, to include the forensic report he generated on 04/11/2019, *at any time during the preceding four weeks of trial*, which began on 05/07/2019. There was no legitimate need to re-examine the CF card and create a second report.
  - If FE Flatley was available to relinquish custody of the physical CF card on 06/07/2019, then he was also available to provide FE Booth with the forensic copy of the CF card he created (and named **NYC024299.001**). FE Booth should have used the *existing* forensic copy to generate a new report, if needed, rather than creating his own forensic copy.
  - By creating a new forensic copy of the CF card (named **NYC024299\_1B15a.E01**), FE conducted a "re-examination" – a duplication of all the technical steps that FE Flatley had already completed. CART policy strictly prohibits such re-examinations, unless approved by the executive management of the FBI Operational Technology Division.<sup>6</sup> I could not find a record of such an approval.

---

<sup>6</sup> The FBI Digital Evidence Policy Guide, Section 3.3.11.2 states, "Unless approved by the AD, OTD as outlined below, examinations are not conducted on any evidence that has been previously subjected to the same type of technical examination (hereinafter referred to as a 're-examination.')" One of the reasons for this policy is to "[e]nsure that the integrity of the evidence is maintained" (p. 37). A publicly released version of this document, which includes many other requirements for a re-examination, may be found at <https://vault.fbi.gov/digital-evidence-policy-guide/digital-evidence-policy-guide-part-01-of-01/view>.

- Instead, according to his notes FE Booth only obtained approval from his acting supervisor Trenton Schmatz to proceed with the re-examination. Given the above facts, therefore, it is not credible that FE Booth had no knowledge of the fact that FE Flatley had already inventoried the camera and CF card, imaged and processed the CF card, and created an FTK report (GX 521A), especially when the government asked FE Booth to create “another report” (GX 521A “replacement”). Also it is not credible that FE Booth did not know his actions violated FBI policy on re-examinations.
- **FE Booth’s testimony is especially troubling considering his status as a Senior Forensic Examiner.** In the FBI CART Program, an examiner may apply to be a senior examiner, which requires additional training, additional testing, a research project, and a special moot court exercise. As a Senior Forensic Examiner, Brian Booth should have known his actions were inconsistent with FBI CART policy and his testimony was false and misleading.

**Finding 6: The timeline of examination is suspicious.**

- 11 months passed between the seizure of the CF card (03/27/2018) and the date it was first delivered to a CART examiner (2/22/2019). As stated previously, several FBI employees – who were not authorized to view unexamined digital evidence – gained physical control of the CF card during that time. FE Flatley was the first CART examiner to receive the CF card and he imaged, then created an FTK report and file listing of the CF card on 04/11/2019. FE Booth first examined the CF card, from which the alleged contraband purportedly came, the day before he took the stand on 6/12/2019 - which was already more than four weeks after the trial began on 5/7/2019.
- It is highly unusual that digital evidence in such a case would be examined for the first time, by the testifying examiner, on the eve of his testimony. In my 20 years of FBI experience I have never seen such a delay – followed by a last-minute examination – in a case with no exigent (emergency) circumstances.

**Finding 7: Critical evidence was withheld from the defense team.**

- Examination photographs, including those documenting the initial condition of the evidence, were initially withheld (p. 4894). These photographs would include those taken of the evidence by FET Donnelly, FE Flatley, and FE Booth when they received them (on 08/08/2018, 02/22/2019, and 06/10/2019, respectively). In the examination notes of FET Donnelly and FE Booth, the examiners only included photographs of the WD HDD (1B16) and a Lacie HDD (1B28). Conspicuously missing were any photographs of the Camera (1B15) and CF Card (1B15a), as such photographs would document whether or not the evidence packaging was sealed when received by the examiner. Although FE Booth omitted the sealed status of the evidence in his notes, he admitted under oath that

the packaging for neither the camera nor the CF card was sealed when he received them (p. 4886-9).

- When a discovery order is issued by a court, it usually includes documents such as examination notes, reports, file listings, photographs, chains of custody, forensic images, and imaging logs. I have not seen a record of the government providing the CF card forensic image file (or forensic copy) created by FE Flatley (NYC024299.001), the CF card forensic image file created by FE Booth (NYC024299\_1B15a.E01), or any of the logs and .CSV file listings that normally accompany the images. To my knowledge, no one has represented that alleged contraband exists on these forensic images and administrative documents, so there is no reason to withhold them from defense counsel. In **Appendix B** I have listed several of these evidentiary and administrative items that would be crucial to supporting my analysis but were not produced by the government before trial.

## **Conclusion**

Never in my 20 years with the FBI have I seen a case brought to trial with such careless evidence handling, scant documentation, and obvious signs of evidence manipulation (see my Technical Findings report). The points above combined with technical findings of evidence alterations point strongly to the government, at a minimum, being aware that the evidence was unreliable and had been altered.

The government not only withheld this information from the jury but attempted to convey the opposite – that the evidence was reliable and authentic – by eliciting false testimony from FE Booth and making false and misleading statements in their closing arguments.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP  
FBI Special Agent (Retired) and Forensic Examiner



## Appendix A

### A White Paper: EXIF Data and the Case “U.S. vs KEITH RANIERE”

By J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

#### Introduction

The purpose of this article is to expose the government’s mischaracterization of EXIF data used as evidence against the defendant Keith Raniere.

#### Background

In this case, the prosecution claimed that Raniere used a Canon digital camera to take explicit photographs of a female while she was still a minor, saved them to a compact flash (CF) camera card, transferred them to an unknown computer, and then backed up those photographs to an external hard drive (See Figure 1).

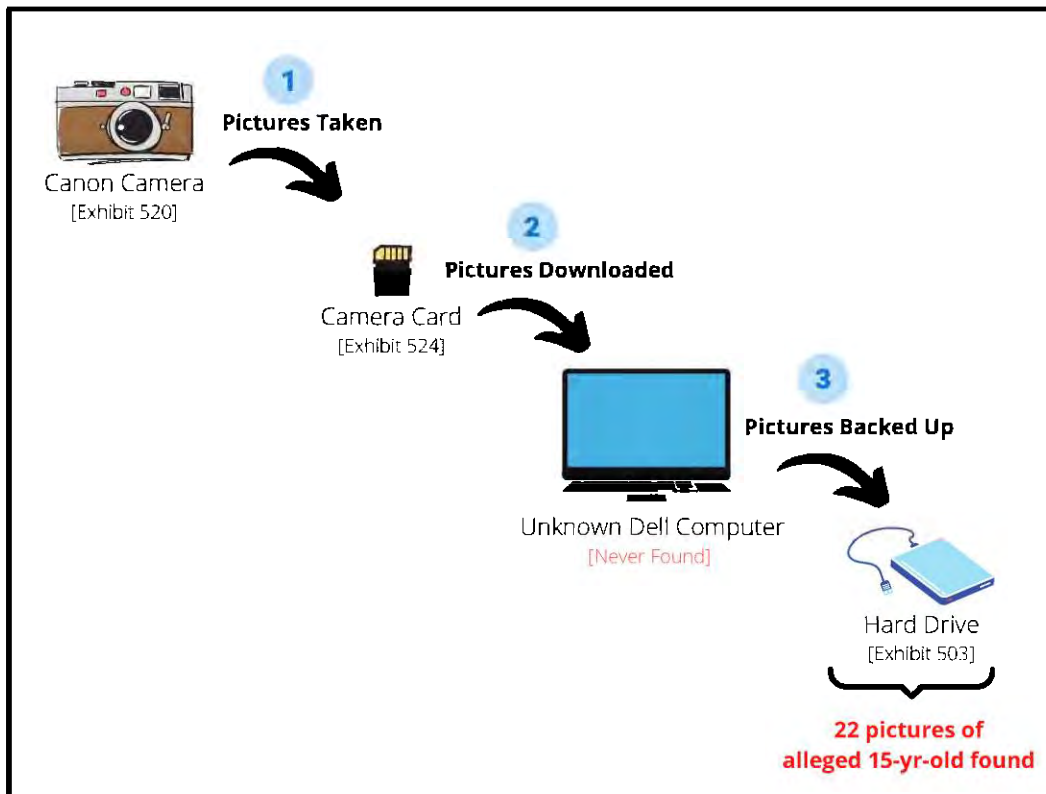


Figure 1: The Government’s narrative regarding alleged contraband found on a “backup” drive.

To demonstrate that the alleged user of the camera, Raniere, created the alleged contraband, the prosecution needed to prove two things:

1. The alleged contraband photographs were taken in 2005, and
2. The alleged contraband photographs were taken with the camera allegedly used by Raniere.

The prosecution relied upon information embedded inside the digital photographs, called **Exchangeable Image Format (EXIF) data**, which records how the photo was taken, on what date, and with which camera settings. Since EXIF data is saved into to the *content* portion of the digital photograph file, it does not change when the photograph is transferred to another device.

The prosecution used the photo's EXIF data, specifically their creation date, to argue the subject was underage in the pictures. They also pointed to the fact that the EXIF data of the photos showed the same make and model of the camera allegedly used by Raniere. At first glance, this is a seemingly logical line of argumentation.

But one important question needs to be asked.

### **How reliable is EXIF data?**

According to the FBI's expert witness, Senior Forensic Examiner William Booth, the photo EXIF data – the information that's embedded into the photograph file itself – is extremely reliable because it is "very hard" to change. Consider just a few of his statements from his court testimony (emphasis added):

Question: Is there a particular reason why **EXIF** data is **more difficult** to alter?

Booth: They purposely designed it that way.

Question: Do you know --

Booth: It's mainly to be able to store information. And they don't want data to be moved around and changed, **especially time and date information**. Those things are **very hard for the consumer to be able to modify**, unless you wind up getting **software** that's just developed to do that (p.4820).

Booth: Well, the best reference is the **EXIF** data because that gets put into the JPEG file and it's **not easily modifiable** and it moves with the file the same way from device to device, no matter where you place it. It has nothing to do with the bearing of a file system at all or the dates and times associated with it. So it's on its own, but are created at the same time that you take the picture (p.4830).

Booth: ...But when it comes to photos, they still keep you from changing **dates** and **times**. **It's not easy to change those**. You have to go through **special processes** to change those things. (p.4977)

These are just a few of Booth's statements about the reliability of EXIF data and how hard it is to modify. Prosecutor Mark Lesko emphasized Booth's testimony in his closing argument to the jury:

LESKO: ...I'm no expert, don't get me wrong, **but I heard Examiner Booth, just like you did. Exif data is extremely reliable**. It's embedded in the jpeg, in the image itself. And the exif data shows that the data was created on the camera, in this instance, this particular instance, the 150 jpeg on November 2, 2005... (p.5572).

So both the FBI's expert witness and the DOJ prosecutor told the jury they could rely on the photo EXIF data to determine that Raniere had created the alleged contraband with the Canon camera in 2005 because the EXIF data is "extremely reliable" and "very hard" to modify.

However, is it true that digital photograph EXIF data is "very hard" to change? A simple demonstration will help answer this question.

### **Modifying Photograph EXIF Data**

A quick Google search will enable anyone to find many of the freely-available, simple-to-use tools for editing EXIF data. One of my favorites is called **ExifTool**, which was recently featured in an online article titled, "7 Free Tools to Change Photo's Exif Data, Remove Metadata and Hide Dates" (<https://www.geckoandfly.com/7987/how-to-change-exif-data-date-and-camera-properties-with-free-editor/>). However – as I will demonstrate in a moment – a person doesn't even need to download a free tool to modify EXIF data.

For purposes of the following demonstration, I will use a real digital photograph from the U.S. vs KEITH RANIERE case. Although the photograph with the file name "IMG\_0043.JPG" is simply a picture of a tree, it was found on the evidence "backup" hard drive along with the alleged contraband and it was allegedly taken with the same camera at around the same time. In Figure 2 below, the Microsoft Windows details pane (invoked by selecting the "View" tab of any Windows folder) is interpreting some of the EXIF data of IMG\_0043.JPG.



Figure 2. Windows display of EXIF data for IMG\_0043.JPG.

According to the Windows display of EXIF data, this photo was taken on **10/17/2005** with a **Canon EOS 20D** digital camera. I verified this information by using the industry standard ExifTool I mentioned earlier. Here is how ExifTool interprets the EXIF data:



Figure 3. ExifTool display of EXIF data for IMG\_0043.JPG.

How hard is it to change the camera model? In the Windows folder with the Details Pane enabled, **I simply click the "Camera model" field and type whatever I want. Here I changed the camera model to an iPhone XR.**

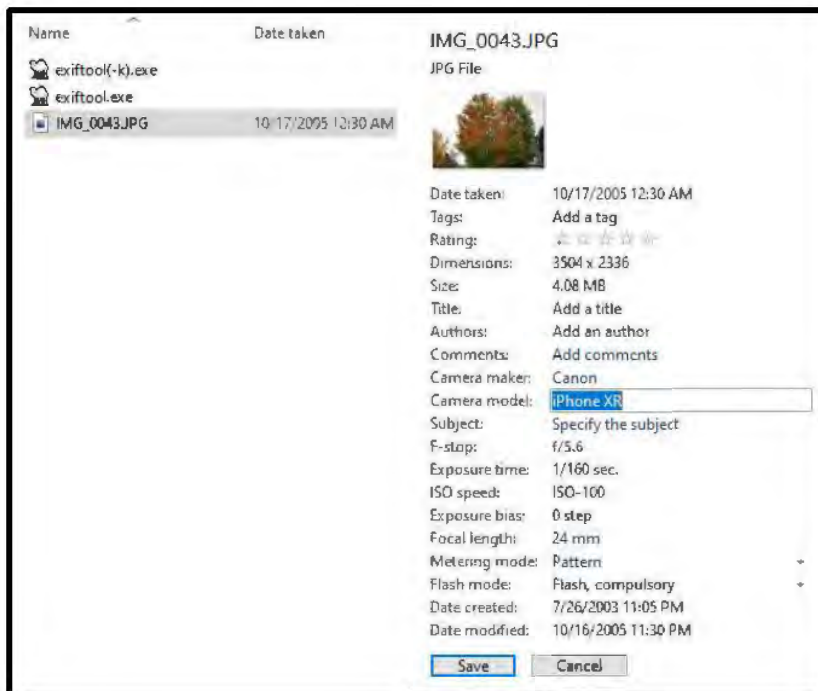


Figure 4. Changing the “Camera model” field in the EXIF data of a photo.

In the same way, I changed the Camera maker to Apple, and then I clicked on the “Date taken” field and set it to the United States Independence Day.

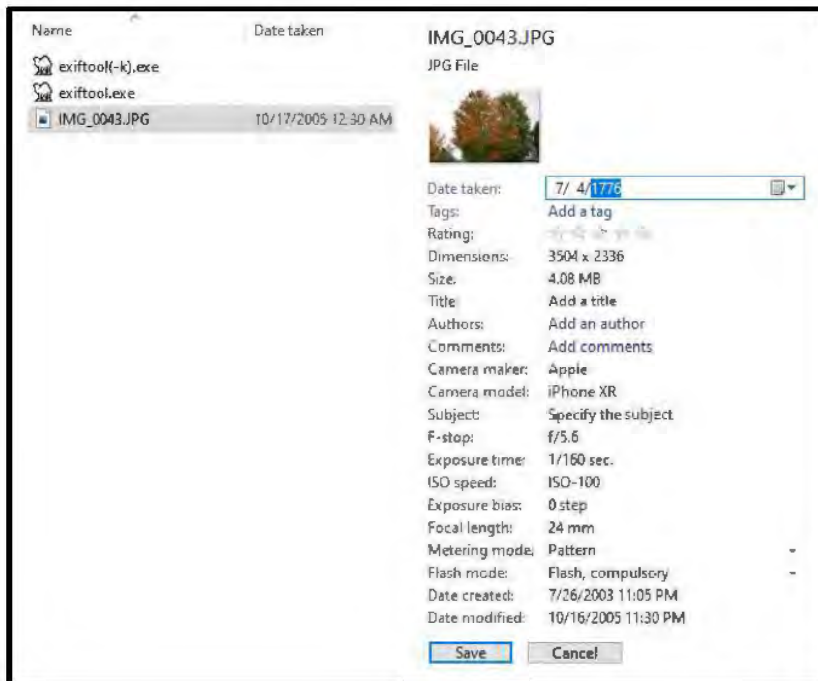


Figure 5. Changing the “Date taken” field in the EXIF data of a photo.

Therefore, a person viewing the file in Windows would now see a photo that was taken by an Apple iPhone XR, in the year 1776.

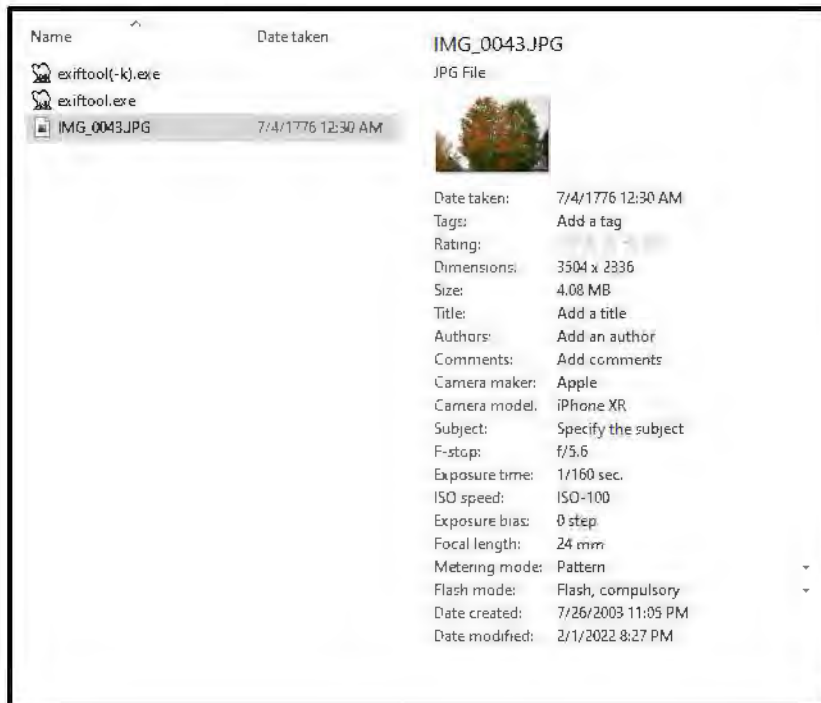


Figure 6. Windows display of saved changes in the EXIF data of photo IMG\_0043.JPG.

Despite the government’s contention in court, the EXIF data was very easy to change.

At this point a person might be thinking, “That’s fine for the Windows interpretation, but was the EXIF data really **modified?**” To verify that the changes I made in the Windows folder in fact changed the EXIF data in the file, I opened the file again in ExifTool:



Figure 7. ExifTool display of saved changes in the EXIF data of photo IMG\_0043.JPG.

The next question one might ask is: “What about a forensic tool? Would a digital forensic tool verify these changes in the EXIF portion of the file?”

One could argue that ExifTool is indeed a forensic tool, although it is in the public domain. But to put to rest any doubts about what happened, I viewed the photo in one of the most common (and FBI-approved) digital forensic tools available: AccessData’s FTK Imager. In Figure 8

below, I imported IMG\_0043.JPG and used the Hex viewer to read the raw EXIF data. All the EXIF changes I made were readily visible, and there were no traces to indicate that I or anyone else had ever made those changes.

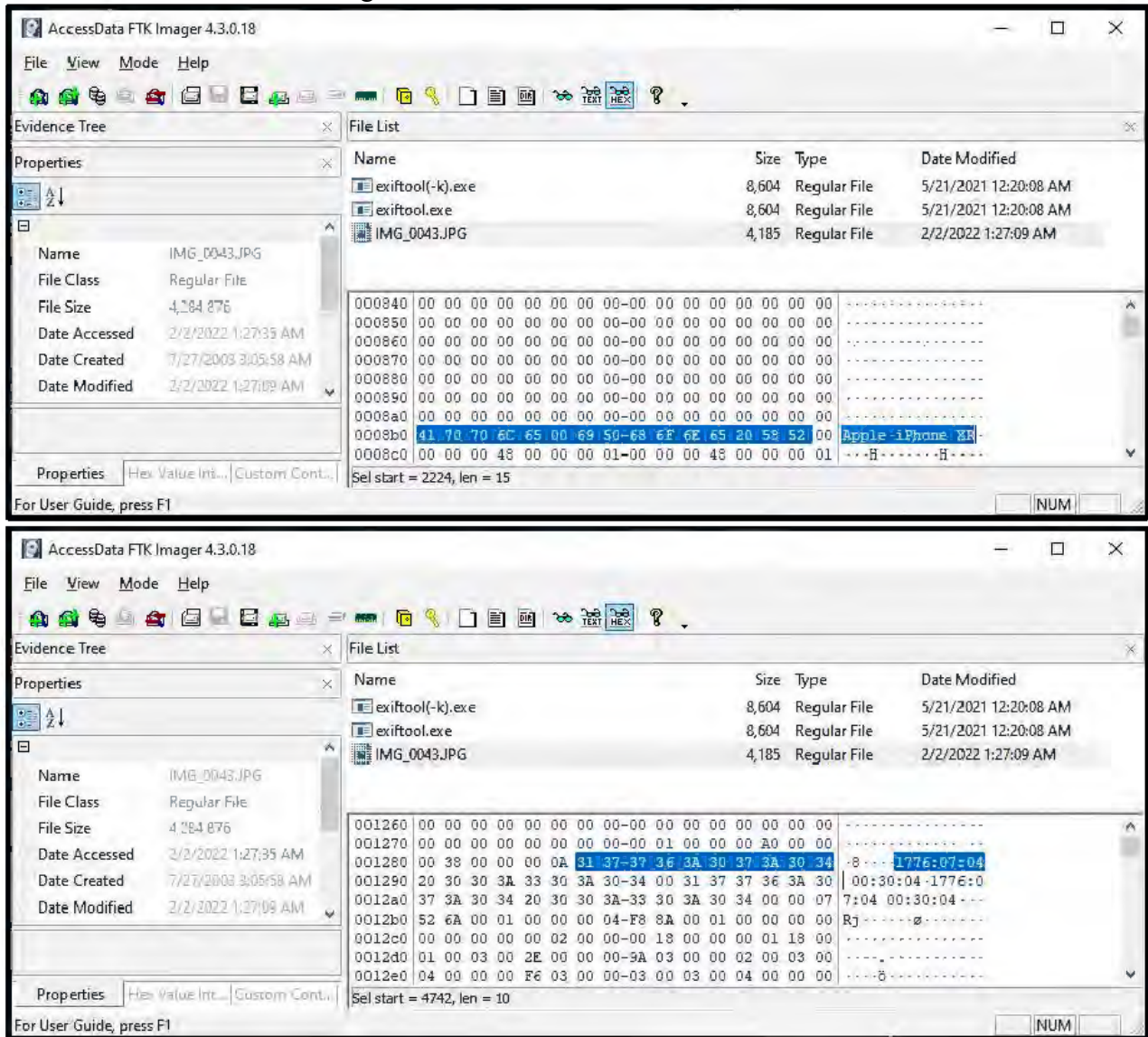


Figure 8. FTK Imager display of saved changes in the EXIF data of photo IMG\_0043.JPG.

## Conclusion

What does all this mean? It means the government misled the jury about the nature of EXIF data used to convict Keith Raniere.

I could have used one of the many freely available tools to modify the EXIF data that the **government claimed was “extremely reliable” and “very hard” to modify. Instead, I simply used the built-in features of Windows to modify the EXIF data of one of the actual digital**

photographs produced by the government at trial, and then I verified those changes in three different ways. In reality, anyone can reproduce what I just demonstrated in this article, using any digital photograph. Modifying EXIF data requires **none of the “software” or “special processes” claimed by FBI examiner Booth, nor is it “very hard” to modify, as he claimed in sworn testimony.** It is not clear to me why a Senior Forensic Examiner of his caliber would have made those false statements under oath.

## **Implications**

**Why would the FBI’s star witness, the digital forensic examiner, swear under oath that EXIF data cannot be easily modified? And why would he make such statements multiple times during his testimony? I just demonstrated how easy it is.**

The prosecution needed the jury to believe that EXIF data could not be easily modified because it was the only piece of digital information that supported the narrative that the photos on the drive allegedly belonging to Raniere were of an underage subject. If the prosecution had told the truth – that EXIF data can be easily modified with no special skills or tools – then the jury may have reasonably doubted its reliability as evidence of a crime.

The bottom line: It is a miscarriage of justice for the prosecution (and the jury) to have relied upon the authenticity of EXIF data to prove creation dates and the origin of digital photographs. If the government could blatantly mislead a jury about something so easy to disprove, it leaves me to ponder: What else were they lying about?

Respectfully submitted,

J. Richard Kiper, PhD  
FBI Special Agent (Retired) and Forensic Examiner.



## Appendix B

### Items Requested for Discovery

The following list represents critical evidence and administrative documentation that was not provided to me during my analysis of information pertaining to the case U.S. vs KEITH RANIERE, et al. After serving 20 years as an FBI Special Agent and Digital Forensic Examiner, I know these items should be readily available for the FBI to locate and produce in a timely manner, because most of these items are retrievable from the FBI Sentinel case management system or from the Evidence Control Unit (ECU), which is required to retain evidence for a criminal case until all appeals are exhausted. These items are critical to supporting my analysis of both the digital evidence and FBI procedures in this case, and to my knowledge none of these items were produced by the government before trial.

1. **The forensic image of the CF card (1B15a) created by FE Flatley (NYC024299.001)**, together with its imaging log and file listing (.CSV) file. This is a bit-for-bit duplication of the CF card, and I need to analyze it independently rather than rely on the FBI's submitted forensic reports. If the FBI did not delete it, this forensic image is located on the FBI shared server at: \\nycart-fs\cases05\NY-2233091\_208206\Evidence\NYC024299\NYC024299.001. An archive copy should also be stored in the ECU.
2. **The forensic image of the CF card (1B15a) created by FE Booth (NYC024299\_1B15a.E01)**, together with its imaging log and file listing (.CSV) file. Again, I need to analyze this data independently from the FBI's forensic report, which shows new files were added to the 06/11/2019 report that did not appear on the 04/11/2019 report. My analysis of these two forensic images would determine to a scientific certainty which contents of the CF card were altered while in the custody of the FBI. If the FBI did not delete it, this forensic image is located on the FBI shared server at: \\nycart-fs\CASES02\NY-2233091\_196817\Evidence\NYC024299\_1B15a\NYC024299\_1B15a.E01. An archive copy should also be stored in the ECU.
3. **FE Steven Flatley's complete Examination Notes.** These documents should include the steps taken by FE Flatley during his inventory, imaging, and analysis of the CF card, including software generated log files.
4. **Photographs of the CF card, documenting its condition and packaging, when received by FE Flatley on 02/22/2019 and by FE Booth on 06/10/2019.** FE Booth already testified he received the CF card in an unsealed plastic bag from the case agent. We have no information regarding the condition of the CF card when FE Flatley accepted custody of it.

5. **The original file listing of the WD HDD (1B16) created by FET Donnelly (NYC023721\_1B16.E01.csv)** and the imaging log for that item. I need to compare the original file listing to that which was provided to me.
6. **The FTK log (generated by AD LAB) of the processing, browsing, searching, and bookmarking of digital evidence.** I need the FTK logs for the examination of the WD HDD (1B16) and both instances of processing for the CF card (1B15a). Among other important data, the FTK log would capture the date and time SA Lever allegedly “discovered” contraband on the WD HDD.
7. **The CART Requests corresponding to SubID 196817 and SubID 208206.** These documents are normally part of an examiner’s “administrative notes,” and could help explain the rationale for originally assigning the CF card to FE Flatley while assigning all the digital evidence items (including a reexamination of the CF card) to FE Booth.
8. **All EXIF data for ALL photographs listed on both of the CF card reports (GX 521A, dated 04/11/2019, and GX 521A Replacement, dated 06/11/2019).** I need to compare EXIF data contained in files contained in the forensic images of the CF card with those contained in the WD HDD files. However, if I am provided both forensic images of the CF card (Items 1 and 2) then I do not require this item.
9. **A detailed description (Examination notes) of how GX 504B was generated,** including the tool, options selected, and steps taken. Detailed examination notes are required to be able to replicate the results of the FBI’s examinations.
10. **All communications,** including but not limited to texts, e-mail messages, notes, and voicemail messages, of FET Donnelly, FE Booth, FE Flatley, SA Lever, SA Jeffrey, SA Mills, SA Rees, SA McGinnis, AUSA Hajjar, and AUSA Penza, regarding this case. Among the above requested items, this is the only request for information that may not be readily retrieved from the electronic case file or from ECU. However, the communications between these DOJ employees would provide critical context to the actions taken regarding the collection, transportation, storage, and analysis of the digital evidence in this case.

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

## Analysis of the Testimony of Special Agent Christopher Mills

### **Professional Background**

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally sworn out affidavits for dozens of search warrants and collected, preserved, and analyzed hundreds of pieces of digital evidence. Therefore, I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

### **Introduction**

On March 27<sup>th</sup>, 2018, the FBI executed a federal search warrant at a two-story town home located at 8 Hale Drive, Halfmoon, New York. To my knowledge, the residence had been used as an executive library by Keith Raniere, defendant in the case U.S. vs KEITH RANIERE, et al. As part of my analysis of the digital evidence in this case, as well as the actions taken by the FBI to identify, collect, preserve, and analyze that evidence, I reviewed the testimony of FBI Special Agent Christopher Mills as he answered questions from prosecutor Tanya Hajjar regarding the search.

Among the many curiosities in this testimony, I was particularly struck by the fact that the first two pieces of evidence collected at the residence happened to be the **ONLY** two pieces of digital evidence used to convict Raniere of child exploitation. It was as if the FBI agents knew what **would eventually be “found” on those devices** and used at trial.

Moreover, in my opinion the questions by prosecutor Hajjar and the answers by SA Mills seemed specifically choreographed to give the jury the impression that the FBI followed robust procedures during the search, thereby distracting from the subsequent and obvious mishandling of the collected evidence.

## Testimonial Analysis

What follows are referenced excerpts from SA Mills' sworn testimony, followed by my analysis regarding their significance to the case.

### **1. Disproportionate attention to detail regarding search procedures rather than establishing an unbroken chain of custody.**

Prosecutor Tanya Hajjar asked, "*Agent Mills, can you just generally describe to the jury what the process is for conducting the search of a residence?*" (p. 4290).

What follows this quote was an unusually long and detailed description of FBI *search procedures*, complete with a discussion of the "knock-and-announce," **forced entry**, safety sweep, furniture present, search sketch, assignment of letters to each area, movement of agents through the residence, photograph procedures, etc. These 14 pages of detail stand in stark contrast to the vague, one-paragraph description of the *evidence collection and transportation* procedures recorded on page 4307 (discussed in #6, below). For example, the prosecutor introduced the search sketch, the photo log, and all the photos into evidence, but never introduced or even asked about the chains of custody or storage requirements for the evidence that was collected. From a reading of the transcript, it seems the over-emphasis on FBI search procedures was meant to distract from the under-emphasis on evidence handling procedures, which Hajjar must have known was problematic.

### **2. A new agent, rather than the on-scene case agent, was the sole witness to testify about the execution of the search warrant.**

When asked about the search team, Mills answered: "*There was a team, mostly comprised of agents from the New York office, as well as the Albany office*" (p. 4291).

Despite the involvement of a sizeable search team from two different field offices, SA Mills (with only three years on the job) was the *only witness* asked to testify about how the evidence was identified and collected that day. His role was to "assist with evidence collection and documentation" and to take photographs. By contrast, SA Michael Lever, who was the lead FBI investigator in the case (the "case agent"), the affiant on the search warrant, and was probably responsible for the mishandling of the digital evidence for many months after the search<sup>1</sup>, did NOT testify during the entire trial. A reasonable person may conclude that the prosecutor intentionally limited the risk of exposing the FBI's evidence mishandling by declining to put the case agent on the stand.

---

<sup>1</sup> See my Technical Findings and Process Findings reports.

**3. The search team ignored several other areas of the residence before starting to search the office.**

Hajjir asked, “*And where did you go from there, in terms of initiating the search?*” (p. 4294).

During the unusually long description of the movements of the search team, Mills indicated they moved past the kitchen, living room, bathroom, and open areas of the first floor. Then they took a spiral staircase to the second floor, where they moved through several more areas, including a bathroom, and a seating room area, **before finally arriving at the “office space.”** Although the office was the last of many areas discovered in the residence, it became the first area to be searched. In my experience, the case agent normally assigns groups of FBI personnel to search different areas of the building simultaneously to save time. Working this way in multiple simultaneous locations, search teams would be able to collect evidence, but no one would be able to assign consecutive evidence numbers. In this case, however, someone decided the office would be the first location to start finding AND numbering evidence.

**4. The very first item to be identified in the entire residence was a camera with a camera card, located under a desk, and which happened to be one of two key pieces of digital evidence used to convict Ranieri of child exploitation.**

In describing one of the search photographs he took, SA Mills said, “*So the there's a note there with the number one. So number one represents evidence item number one. So, in this case, this photo was taken underneath the desk or table and was assigned number one based on being the first evidence item that was found*” (p. 4304).

If SA Mills’ account is correct, then the FBI search team traversed several areas of the residence, went upstairs and straight to the office area, and then crawled under a desk to find the first piece of evidence – a camera bag containing a camera and camera card. At this point, the case agent, SA Lever, had not yet “discovered” alleged child pornography taken with this camera, so it seems more than a strange coincidence that it was the first evidence item identified.

Another anomaly is the fact that an item number was assigned to the camera immediately upon discovery. All the items documented in the photo log (GX 502) and represented in the photographs (GX 502A) have item numbers, written on sticky notes photographed next to the items. Generally, FBI search personnel do not assign item numbers to evidence at the moment of discovery/photography/collection, because there are multiple people working in different rooms and it would be impossible to coordinate the numbering among them. If any items are assigned item numbers, then it is done near the *end* of the search when the seizing agent collects all the evidence together and fills out the FD-597 receipt for items seized. Therefore, in practice the item numbers rarely correspond to the order in which they were collected.

**5. The very next item to be identified in the entire residence was an external hard drive, located away from the desk on a shelf, and which happened to be the second of two key pieces of digital evidence used to convict Ranieri of child exploitation.**

When asked about another photograph he took, SA Mills answered, *“So this is the still of the same office space as seen before and item number two, which is on top of the bookshelf here, is a gray or silver hard drive”* (p. 4308).

Once again, it is extremely convenient that from all the potential evidence in the residence, it was the Western Digital hard drive – where the alleged child pornography was stored – that was the *second* piece of evidence identified by the FBI on scene. It is also important to note that the camera card (Item #1) and the hard drive (Item #2), comprised the entirety of the child exploitation digital evidence against Ranieri – which supposedly was not “**discovered**” by the FBI for nearly a year later.

**6. Prosecutor Hajjar did not even attempt to establish an unbroken chain of custody for the digital evidence used against Ranieri.**

Hajjar: *What happens when you recover a piece of digital evidence like Government Exhibit 520 and 524?*

Mills: *So, when we receive -- when we recover digital evidence, we have a process in which we bring the digital evidence back to our office and if we want the evidence to be reviewed, we would submit a request to our CART team. And the CART is the Computer Analysis Response Team and they have specialists who are computer evidence examiners who would review that evidence for us or assisted us in reviewing the evidence with us.*

Hajjar: *And is that what happened in this case with Government Exhibit 520?*

Mills: *Yes.* (p. 4307).

After spending several minutes eliciting the details of search activities, the prosecutor was strangely disinterested in establishing an unbroken chain of custody for the two pieces of digital evidence presented at trial. Conspicuously missing were the following questions, for example:

- Who decided which pieces of evidence were relevant and within the scope of the search warrant?
- Why did you bypass documents and other potential evidence in other rooms in order to start with items in the office?

- While in the office, why did you start identifying and collecting evidence beneath the desk?
- The photo log shows that you went back and forth from room to room, photographing various evidence items there. Why didn't you stay in one room to photograph all the evidence there, before moving on to the next room?
- Who decided the order in which the items were to be photographed and assigned item numbers?
- After you photographed each piece of evidence, what specifically did you do with it?
- Who sealed the evidence?
- Who packaged the evidence?
- Who started the chains of custody for the evidence?
- Who transported the evidence back to your office?
- Who took custody of the evidence at the office, and how was it stored?
- You said you found the camera card (CF card) inside the camera (p. 4305). You must have removed it on scene to identify it here in court. Who removed it permanently and put it inside a cellophane bag?
- Why didn't you photograph the CF card after you discovered it inside the camera?
- Why wasn't the CF card noted on the photo log, chain of custody, electronic evidence entry, or any other documentation related to the seizure of the camera?
- When was this evidence relinquished to case agent Michael Lever?
- How long did he have custody of the evidence?
- Did you realize that the camera and the CF card were in unsealed containers when you regained custody and relinquished them to FE Booth on 06/10/2019?
- Who unsealed them and why were they not re-sealed?

In the above trial excerpt, it seems the prosecutor specifically crafted her sentence to avoid discussing *who* in the FBI had taken actions on the digital evidence after it was identified at the search site. As I detail in my Process Findings report, the chains of custody demonstrate that SA Lever and other FBI individuals not authorized to review unexamined digital evidence gained physical control over the digital evidence for several months before turning it over to CART forensic examiners. In fact, the CF card was checked in and out of the Evidence Control Unit (ECU) for eleven months before it was finally released to the first CART examiner, Stephen Flatley, on 02/22/2019. During that time, as the government has acknowledged, an FBI employee accessed that camera card on 09/19/2018. The Chain of Custody indicates that the case agent, SA Michael Lever, had custody of the CF card from 09/19/2018 to 09/26/2018. In my Technical Findings report, I describe several anomalies that demonstrate manual manipulation of data on that card.

The Chain of Custody also shows that other FBI employees, SA Elliot McGinnis and SA Christopher Mills, regained custody of the camera and CF card from the first CART examiner

before turning it over to a second CART examiner, Brian Booth, in *unsealed packaging* on 06/10/2019 – *the very day Mills testified about collecting it*. As explained in my Process Findings report, a second examination of digital evidence is strictly prohibited by policy, and for the second examiner to receive the original evidence from a case agent (rather than using the work of the previous examiner) is very abnormal.

Regarding SA Lever’s **handling** of the digital evidence in this case, there are several questions that must be answered, for example:

- Why did SA Lever and other FBI employees check out the evidence from the ECU multiple times, when they were not authorized to even look at it?
- Why did SA Lever access the CF card without a write blocker on 09/19/2018?
- Why does the Chain of Custody for the WD HDD (DX 960) end with SA Lever checking it out of Evidence Control on 02/22/2019?
- What did SA Lever do with the WD HDD after he checked it out?

It is very telling that the prosecutor completely avoided the topic of chain of custody with respect to the digital evidence in this case.

**7. Sometime after collecting the first and only two pieces of digital evidence eventually used at trial, the searching agents returned to the space beneath the desk and collected another external hard drive.**

After being asked to describe another photograph he took, SA Mills said, “*So this is, once again, underneath the desk or the table in the office space. And you see item number 14, so that's evidence item number 14, the gray or silver hard drive*” (p. 4310).

SA Mills later identified this second external hard drive as a LaCie external hard drive (Item #14). If (according to SA Mills) the item numbers correspond to the order in which they were collected, then this item was *discovered in the same place as the camera bag* (Item #1) – yet it was not discovered and collected until much later. In fact, according to the seized property receipt<sup>2</sup> and the search photos (GX 502A), the FBI collected a book, 30 cassettes, an Amazon Kindle, two CD discs, a thumb drive, and miscellaneous documents before returning to the space beneath the office desk to collect the LaCie hard drive and other computer equipment.

This strange behavior begs the following question: Why did the FBI agents first go straight to the camera bag (Item #1), located under the desk, then search a shelf, where they retrieved an external hard drive (Item #2), then collect dozens of other items (some found in other rooms) before returning under the desk, where they found the LaCie external hard drive?

---

<sup>2</sup> See FD-597, Receipt for Property Seized.



## Conclusion

The prioritized collection of the only two pieces of digital evidence used to support the child exploitation charges at trial (Items #1 and #2) strongly points to foreknowledge on the part of the FBI agents. In fact, a reasonable person would suspect the evidence collection process itself was influenced **by someone with an interest in the FBI “finding”** digital evidence against Ranieri.

Moreover, the question-and-answer interactions between prosecutor Hajjar and SA Mills seemed intent on convincing the jury of the reliability of the digital evidence through a robust discussion of FBI *search* procedures, while deliberately obfuscating the FBI's *aberrant evidence handling* activities that occurred thereafter. In short, the testimonial evidence recorded in this court transcript is consistent with the evidence manipulation opinions and conclusions expressed in my Technical Findings and Process Findings reports.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP  
FBI Special Agent (Retired) and Forensic Examiner

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

## Expert Opinion Regarding Time to Review Digital Evidence

### Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally sworn out affidavits for dozens of search warrants and collected, preserved, and analyzed hundreds of pieces of digital evidence. Therefore, I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

### Review of Events

In my experience serving in the FBI's Computer Analysis Response Team (CART), forensic examiners are typically given several months to examine digital evidence and prepare analyses for legal proceedings. Similarly, a court's discovery order usually requires that evidence against the accused be provided to the defense team with enough time to prepare a reasonable defense. In the case of U.S. vs KEITH RANIERE, neither of these norms were followed.

Two digital devices – a camera card (CF card) and an external hard drive (WD HDD) – were the only pieces of digital evidence **used to support the government's charge of child** exploitation in this case. However, despite having possession of these items for a year, the FBI did not provide defense counsel any access until 03/13/2019<sup>1</sup>, a mere twenty-six days before jury selection was scheduled. At that time, the FBI gave the defense access to the forensic image of the *external hard drive only*, and due to the allegation of child pornography, the defense expert could not remove any data from the premises beyond screen shots of file listings and handwritten notes.

Further impeding the ability of the defense to conduct a thorough review of the evidence with its own forensic tools, the FBI did not provide a **“clean”** (non-forensic) copy of the contents of the hard drive until 04/06/2019, less than a week prior to the scheduled jury selection.

---

<sup>1</sup> This was also the date of the government's Second Superseding Indictment alleging sexual exploitation of a child. According to the FBI examiner's notes, 03/13/2019 was the date the hard drive image was prepared for review. I do not know when the defense expert was provided access to review it.

Finally, the FBI significantly delayed the creation and delivery of the forensic reports used at trial. According to the sworn declaration of defense counsel Marc Agnifilo filed on 04/22/2019, “...when asked recently when we were going to get these reports, the prosecution stated that the reports were not completed but that the government would make the reports available when the FBI completed them.” In fact, the **“not completed” forensic reports already had been completed** on 04/11/2011 but *were still being withheld from the defense team two weeks prior to opening statements*.

The **government’s** delay of the second forensic report of the CF card was even more egregious. The FBI first examined the CF card and created a forensic report on 04/11/2019. Then, more than four weeks AFTER trial had begun – and against FBI digital evidence policy – the FBI conducted a *second examination* of the CF card<sup>2</sup> resulting in a *second forensic image* and **generated a “replacement” report of the CF card on 06/11/2019**. The defense team literally had no time to prepare a technical rebuttal before this report was introduced at trial.

### **Required Analysis**

A defendant is entitled to the opportunity to review, analyze, and rebut the evidence used against him. At a minimum, the analysis of digital evidence in this case should have included the following tasks:

- A review of the legal authority to conduct the examination.
- A review of the evidence collection, packaging, transportation, and storage procedures.
- A review of the chain(s) of custody.
- A review of the examination notes and administrative paperwork.
- Verification of evidence integrity (e.g., via MD5 hashing).
- Reproduction of the forensic steps used to produce the alleged results.
- New analysis of evidence, including but not limited to:
  - File system metadata,
  - EXIF data,
  - File content,
  - Application artifacts,
  - Operating system artifacts, and
  - Timeline analysis
- **Creation of new trial exhibits to rebut the government’s narrative.**

In my expert opinion, it would be impossible for a defense expert to have completed the above listed activities within a mere twenty-six days (in the case of the hard drive) much less instantaneously (in the case of the CF card).

---

<sup>2</sup> See my Technical Findings and Process Findings reports, where I describe this anomaly in detail.

## **Conclusion**

The government placed the Ranieri defense team at a significant and unjust disadvantage by intentionally withholding key evidence they intended to use at trial. At best, the defense team was given only twenty-six days to conduct a technical review of *some* of the digital evidence (a non-forensic and partial copy of the hard drive contents) and at worst, it was given *no opportunity* to review the second FTK forensic report related to the CF card.

It is my expert opinion that it was unreasonable to expect the defense team to have conducted a forensic analysis of the digital evidence in this case within the given time frames.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP  
FBI Special Agent (Retired) and Forensic Examiner

# **EXHIBIT D1**

**(CV of Dr. James Richard Kiper, Ph. D)**



CURRICULUM VITAE

**James Richard Kiper, PhD, PMP**

Special Agent (Retired) Forensic Examiner, Trainer, and Expert Witness  
2800 South Adams Street #6971, Tallahassee, FL 32314  
Office: 954-595-0805 / Cell: 954-995-3811 / E-mail: info@kipertekusa.com



**EDUCATION**

---

- Ph.D. 2013 Computing Technology in Education  
Nova Southeastern University, Fort Lauderdale, Florida, GPA: 3.88
- Ed.S. 2009 Computing Technology in Education  
Nova Southeastern University, Fort Lauderdale, Florida, GPA: 3.89
- M.S. 2007 Computing Technology in Education  
Nova Southeastern University, Fort Lauderdale, Florida, GPA: 3.96
- M.S. 2020 Information Security Engineering  
SANS Technology Institute, Bethesda, Maryland
- B.S. 1992 Science Education/Physics  
Florida Institute of Technology, Melbourne, Florida  
Honors: *Cum Laude*

**PROFESSIONAL EXPERIENCE**

---

- 2020-Present **Raytheon Technologies**  
*Troy, Michigan*  
Cyber Subject Matter Expert (SME): Develops a variety of cybersecurity training products using best practices in instructional systems design.
- 2020-Present **Nova Southeastern University**  
*Fort Lauderdale, Florida*  
Adjunct Professor: Develops and delivers engaging digital forensics instruction using a combination of live demonstrations, online discussions, and hands-on labs.
- 2019-Present **Kipertek, LLC**  
*Tallahassee, Florida*  
Vice-President and Co-founder: Provides contracted services in the areas of cybersecurity assessment, digital forensics, teacher training, and curriculum development. Develops instructors and designs **curriculum using Kipertek's** exclusive *Education is Salesmanship™* approach to instructional systems design. International conference speaker.
- 1999-2019 **Federal Bureau of Investigation**  
*FBI Academy, Quantico, Virginia*  
Unit Chief, Investigative Training Unit: Supervised curriculum and instructors for the FBI New Agent Training Program and National Academy in the areas of Financial

Investigations, Investigative Processes, Cybercrime, Counterterrorism, and Counterintelligence. Ensured all lesson plans, curriculum maps, and instructional methods were in compliance with Federal Law Enforcement Training Accreditation (FLETA) requirements. Served as Leadership Coordinator for the FBI Academy and advanced instructor in the FBI Instructor Development Program. Developed and delivered Cybercrime Investigations training to law enforcement partners in Albania, Bosnia, Singapore, Moldova, Georgia, Bulgaria, Colombia, Serbia, Azerbaijan, Saudi Arabia, and the Philippines on behalf of the FBI and the Department of Defense International Counterproliferation Program. Spearheaded instructor training and curriculum development assessments for the Kingdom of Saudi Arabia, Ministry of the Interior, King Fahd Security College and Prince Naif Academy, on behalf of the FBI International Law Enforcement Training Program. Co-authored the FBI Training Division Strategic Plan and led the job task analysis for the FBI Director's Initiative High Technology Environment Training (HiTET). Coordinated a team of 12 experts in the development of software requirements to develop a knowledge management system to coordinate FBI training programs with its business processes and policies.

*Miami and Washington Field Offices*

- Computer Forensic Examiner: Certified as an FBI Computer Analysis Response Team (CART) forensic examiner and qualified multiple times as an expert witness. Proficient in the collection, write-blocking, preservation, examination, extraction, analysis, and presentation of digital evidence for court proceedings. Mentor and Coach to four CART forensic examiner trainees (FETs). Consulted with case agents and prosecutors on technical, legal, and investigative aspects of criminal and national security investigations. Designed and delivered digital forensics and cyber investigations training for the FBI Operational Technology Division and Cyber Division. FBI Cyber Liaison to the Philippines, providing customized trainings, consulting, and conference presentations. Contributing author of the CSEC2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Curriculum designer and instructor for the FBI Cyber STEM Initiative in South Florida High Schools.
- Confidential Human Source (CHS) Coordinator: Coordinated the safe and legal operation of more than 600 FBI informants in the Southern District of Florida. Responsible for teaching and enforcing compliance with U.S. Attorney General Guidelines and FBI CHS Policy. Created relational database to manage CHS attributes, investigative/intelligence accomplishments, and compliance documentation.
- Investigator: Served as primary case agent on investigations of white collar crime, organized crime, and computer crime. Employed a variety of investigative techniques, including grand jury subpoenas, pen register/trap and trace orders, interviews, CHS development, physical surveillance, Title III wiretaps, search warrants, and undercover operations. On a single case, coordinated with more than a dozen federal, state, and local agencies to complete 16 search warrants, 24 seizure warrants, and recorded more than 100 statistical accomplishments. Coordinated the largest telemarketing fraud victim restitution in the history of the Department of Justice.

*U.S. Embassy, San Salvador, El Salvador*

Assistant Legal Attaché: Developed effective liaison relationships with law enforcement partners in El Salvador, Guatemala, Honduras, and Belize, to complete investigative leads and information requests in all FBI investigative programs, and especially transnational street gangs. Investigated six American citizen kidnappings, while coordinating with FBI Crisis Negotiation personnel and Victim Witness Specialists. Worked closely with the U.S. Country Team to coordinate and deconflict investigative and diplomatic activities in Central America. Created a Gang Problem Inventory to document how all U.S. Government agencies were applying resources to address the gang problem in Central America. Provided FBI training to the Salvadoran National Police, including tactical and investigative training. Spearheaded the first-ever U.S.-led witness security training for El Salvador, which culminated in a Witness Security Conference that was televised nationally.

*FBI Headquarters, Washington, DC*

Program Coordinator: Supervised a team of 15 FBI employees and contractors on the FBI Virtual Case File Project (now Sentinel Program). Served as training lead and developed a plan for workforce training, reporting, and document management. Lobbied for a \$1.1 million training budget, established clear criteria for contractor success, and coordinated software requirements with the most senior executives of the FBI, including Director Robert Mueller. Created briefings and presentations delivered to congressional committees, White House Chief of Staff Andrew Card, and Vice President Dick Cheney.

1996-1999 **KiperteK Internet Services, Melbourne, Florida**

Owner and Consultant: Created and operated an Internet services consulting company, specializing in web development, server maintenance, and inservice training. Created domains and web sites for more than twenty organizations, including Trinity College, Life Story Foundation, Spaceline, Inc., and Congressman Dave Weldon.

1992-1996 **Satellite High School, Satellite Beach, Florida**

Classroom instructor: **Taught Physics Honors, AP Physics "C,"** Astronomy (dual enrollment), and Science Research. Head coach for varsity cross country and track & field. Sponsor and coordinator for science competitions including JETS, Clash of the Titans, Physics Olympics, and Regional/State Science Fair. Served on the Brevard County Science Advisory Council. Created the first web site in the Brevard County school system. Subject matter expert, graphic designer, and editor for the Brevard County Integrated Science Curriculum (the standards of which were later adopted as the Sunshine State Standards for Science Education in Florida).

**CERTIFICATIONS, AWARDS AND CLEARANCES**

---

Project Management Professional (PMP) Global Credential  
CompTIA A+ Certification



CompTIA Net+ Certification  
Certified FBI Computer Analysis Response Team (CART) Forensic Examiner  
Essential Forensic Techniques I, Blackbag Technologies (MacOS)  
Certified Vehicle System Forensic Technician (VSFT) and Examiner (VSFE), Berla/iVE  
GIAC Security Essentials (GSEC) Certification  
GIAC Certified Incident Handler (GCIH) Certification  
GIAC Certified Intrusion Analyst (GCIA) Certification  
GIAC Certified Forensic Examiner (GCFE) Certification  
GIAC Certified Forensic Analyst (GCFA) Certification  
GIAC Certified Advanced Smartphone Forensics (GASF) Certification  
GIAC Certified Project Manager (GCPM) Certification  
GIAC Critical Controls (GCCC) Certification  
Certified FBI Police Instructor  
Certified FBI Advanced Instructor  
FBI National Behavioral Science Research Certification  
Outstanding Law Enforcement Officer of the Year, U.S. Department of Justice  
**Assistant Director's Award for Distinguished Service to the Law Enforcement Community**  
SANS Institute Lethal Forensic Award (for both FOR408 and FOR508)  
SANS Institute Capture-the-Flag Award for SEC504  
Distinguished Service Award, Church of the Nazarene  
FBI Quality Step Increase Award  
Three FBI Foreign Language Awards  
Four FBI Special Achievement Awards  
Seven FBI Cash Awards  
Four FBI Time Off Awards  
Top Secret/Sensitive Compartmented Information (TS/SCI) Clearance

#### **ADDITIONAL TRAINING**

---

SANS SEC401 – Security Essentials Bootcamp Style  
SANS FOR408 – Windows Forensic Analysis  
SANS FOR508 – Advanced Computer Forensic Analysis and Incident Response  
SANS SEC503 – Intrusion Detection In-Depth  
SANS SEC504 – Hacker Techniques, Exploits, and Incident Handling  
SANS MGT514 – IT Security Strategic Planning, Policy, and Leadership  
SANS MGT433 – How to Build, Maintain, and Measure a High-Impact Awareness Program  
SANS FOR518 – Mac Forensic Analysis  
SANS MGT525 – IT Project Management and Effective Communication  
SANS FOR585 – Advanced Smartphone Forensics  
SANS SEC566 – Implementing and Auditing the Critical Security Controls  
Blackbag Technologies Essential Forensic Techniques I (MacOS)  
FBI Computer Analysis Response Team (CART) – Forensic Toolkit Bootcamp  
CART – Basic Tools

CART – Digital Extraction Technician (DEXT) Practicals  
CART – AccessData Internet Forensics  
CART – AccessData Windows Forensics  
CART – Moot Court  
CART – Unix command line certification  
CART – Cell phone certification  
Kellogg Institute – Navigating Strategic Change (NSC)  
FBI Leadership Development Program - Strategic Decision-Making in the FBI  
FBI Leadership Development Program – Leadership Seminar for Senior Managers  
FBI Quarterly Legal Training  
FBI Quarterly Firearms Training  
FBI Annual Information Security Awareness Training

### **SCHOLARSHIP AND SERVICE**

(2014-Present). Proceedings of the Hawaii International Conference on System Sciences (HICSS). Paper reviewer for Advances in Teaching and Learning Technologies mini-track.

(2020). Working from Home: Cybersecurity in the Age of Telework. Conference keynote speaker and panelist. Contact Center Association of the Philippines (CCAP), Manila, Philippines, June 16 and 25, 2020.

(2020). Cybersecurity Education Program. Instructional Designer and Subject Matter Expert. *Raytheon Professional Services*, Troy, Michigan, January-April 2020.

(2019). FBI Digital Forensics Examiner Curriculum Development Event. Instructional Designer and Subject Matter Expert. *FBI Operational Technology Division*, Quantico, Virginia, May 20-24, 2019.

(2019). GIAC GCIA Standard Setting Workshop. Subject Matter Expert and contributor to GIAC Certified Intrusion Analyst (GCIA) certification definition and cut score. May 14, 2019.

(2019). Cyber Crime Investigation & Electronic Evidence. Lead instructor and curriculum designer – 40 hour course. *Naif College for National Security*, Saudi Arabia, April 21-May 2, 2019.

(2019). Advanced Cybercrime Course. Lead instructor and curriculum designer – 40 hour course. *International Criminal Investigative Training Assistance Program (ICITAP)*, Banja Luka, Bosnia and Herzegovina, April 15-19, 2019.

(2019). Basic Cybercrime Course. Lead instructor and curriculum designer – 40 hour course. *International Criminal Investigative Training Assistance Program (ICITAP)*, Mostar, Bosnia and Herzegovina, April 8-12, 2019.

(2019). FBI Instructional Strategies Course for Cybersecurity Instructors. Primary instructor – 40 hour course. *FBI Cyber Division and Operational Technology Division*. Quantico, Virginia, March 25-29, 2019.

(2018). FBI Instructional Strategies Course. Primary instructor – 40 hour course. *FBI Tampa Division*. Tampa, Florida, November 5-9, 2018.

(2018). FBI Presentation Skills Course. Primary instructor – 24 hour course. *FBI Miami Division*. Miramar, Florida, June 25-27, 2018.

(2018). FBI Instructional Strategies Course. Primary instructor – 40 hour course. *FBI Miami Division*. Miramar, Florida, April 23 – 27, 2018.

(2018). Cyber Threatscape: Business E-mail Compromise. *Chevron Holdings*. Manila, Philippines, April 18, 2018. Also delivered to the *American Chamber of Commerce (AMCHAM)*, Clark, Philippines, April 19, 2018.

(2018). Cyber Investigation and Digital Forensics Orientation. Lead instructor and course designer – 16 hour course. *Quezon City Police Department Anti-Cybercrime Team*. Quezon City, Philippines, April 11-12, 2018.

(2018). Patching the Human Vulnerability: An Introduction to Cybersecurity Awareness. *Alorica Asia Headquarters*. Quezon City, Philippines, April 2, 2018. Also delivered to the *Philippine Department of Environment and Natural Resources*. Quezon City, Philippines, April 13, 2018.

(2018). Kiper, J.R. Pick a Tool, the Right Tool: Developing a Practical Typology for Selecting Digital Forensics Tools. *The SANS Institute Reading Room*. March 16, 2018.

(2018). Joint Cybersecurity Working Group Intermediate Training. Lead instructor and course designer – 40 hour course. *Philippine Judicial Academy*. Tagaytay, Philippines, March 5-14, 2018.

(2018). Cybersecurity Investigative Techniques and Resources Course. Prince Naif Academy. Lead instructor and curriculum designer – 40 hour course. *Saudi Arabia Bilateral Law Enforcement (SABLE) Project*. Naif College for Security Studies, Riyadh, Saudi Arabia, February 5-16, 2018.

(2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Contributing author. *Joint Task Force on Cybersecurity Education*. Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), and the Association for Information Systems Special Interest Group on Security (AIS SIGSEC).

(2017) Wilkerson, W. S., Levy, Y., Kiper, J. R., & Snyder, M. (2017). Towards a development of a Social Engineering eXposure Index (SEXI) using publicly available personal information. *KSU Proceedings on Cybersecurity Education, Research and Practice*. 5.

(2017). Kiper, J.R. The OPTIC Approach: Objectives, Policies, and Tasks for Instructional Content. *Government Learning Technology Symposium*, Washington, DC, November 29-30, 2017.

(2017). FBI Instructional Strategies Course. Primary instructor – 40 hour course. *FBI Training Division*. Quantico, Virginia, November 13 – 17, 2017.

(2017). FBI CART Tech and Digital Extraction Technician (DEXT) Course. Primary instructor – 80 hour course. *FBI Operational Technology Division*. Stafford, Virginia, August 14-25, 2017.

(2017). FBI Instructional Strategies Course. Primary instructor – 40 hour course. *FBI Tampa Division*. Tampa, Florida, July 31 – August 4, 2017.

(2017). FBI Mobile Forensics Training Working Group. Instructional designer for FBI Computer Analysis Response Team (CART) curriculum. *FBI Operational Technologies Division*. Quantico, Virginia, June 19-23, 2017.

(2017). Kiper, J.R. “Forensication” Education: Towards a Digital Forensics Instructional Framework. *The Colloquium for Information Systems Security Education (CISSE)*. Las Vegas, Nevada. June 12-14, 2017.

(2017). Proceedings of the International Conference on Information Systems (ICIS). Paper reviewer for “Security, Privacy and Ethics of IS” track.

(2017). Digital Forensic Examiner Capstone Course. Instructor – 40 hour course. *FBI Operational Technologies Division*. Quantico, Virginia, May 15-19, 2017.

(2017). Joint Cybersecurity Working Group Intermediate Training. Lead instructor and course designer – 40 hour course. *Philippine Judicial Academy*. Tagaytay, Philippines, May 8-12, 2017.

(2017). FBI Instructional Strategies Course. Primary instructor – 40 hour course. *FBI Miami Division*. Miramar, Florida, April 24-28, 2017.

(2017). FBI Presentation Skills Course. Primary instructor – 24 hour course. *FBI Miami Division*. Miramar, Florida, March 21-23, 2017.

(2017). Cyber Field Instructor Program Refresher Course. Lead instructor and curriculum author – 24 hour course. *FBI Cyber Division*. Linthicum, Maryland, February 28 – March 2, 2017.

(2017). FBI Instructional Strategies Course. Primary instructor – 40 hour course. *FBI Operational Technologies Division*. Quantico, Virginia, February 13-17, 2017.

(2016). FBI Presentation Skills Course. Primary instructor – 24 hour course. *FBI Miami Division*. Miramar, Florida, October 17-19, 2016.

(2016). Cyber Investigative Methods for Law Enforcement. Lead Instructor and course designer – 40 hour course. *Dirección de Investigación Criminal e INTERPOL*. Bogotá, Colombia, August 8-12, 2016.

(2016). FBI Presentation Skills Course. Primary instructor – 24 hour course. *FBI Miami Division*. Miramar, Florida, June 7-9, 2016.

(2016). FBI CART Tech and Digital Extraction Technician (DExT) Course. Primary instructor – 80 hour course. *FBI Operational Technology Division*. Quantico, Virginia, April 25 – May 6, 2016.

(2016). FBI Instructional Strategies Course. Primary instructor and co-author – 40 hour course. *FBI Operational Technology Division*. Quantico, Virginia, February 29 – March 4, 2016.

(2016). Introduction to E-mail Header Analysis. Primary instructor and author – 3 hour course. *Miami Gardens Police Department*. Miami Gardens, Florida, January 27, 2016.

(2016). Kiper, J.R. Needs to Know: Validating User Needs for a Proposed FBI Academy Knowledge Management System. *Hawaii International Conference on System Sciences (HICSS)*, January 5-8, 2016.

(2015). FBI Presentation Skills Course. Primary instructor – 24 hour course. *FBI Miami Division*. Miramar, Florida, November 4-6, 2015.

(2015). Train the Trainer for Cyber Instructors. Primary instructor – 40 hour course. *FBI Cyber Division*. FBI Academy, Quantico, Virginia, September 14-18, 2015.

(2015). Whistleblower Retaliation at the FBI: Improving Protections and Oversight. Sworn Witness Testimony. *U.S. Senate Committee on the Judiciary*, Washington, DC, March 4, 2015.

(2015). WMD Cyber Crime Investigations. Primary instructor – 40 hour course. *Defense Threat Reduction Agency International Counterproliferation Program*. Sofia, Bulgaria, February 2-6, 2015.

(2015). Kiper, J.R. Eliciting User Needs for a Knowledge Management System to Align Training Programs with Business Processes in Large Organizations. *Hawaii International Conference on System Sciences (HICSS)*, January 5-9, 2015.

(2014). WMD Cyber Crime Investigations. Primary instructor – 40 hour course. *Defense Threat Reduction Agency International Counterproliferation Program*. Tbilisi, Georgia, September 15-19, 2014.

(2014). Education is Salesmanship. Primary speaker. *Interactive Learning Technologies Conference*. Reston, Virginia, August 15, 2014.

(2013). Curriculum Review and Instructor Development Course Update, King Fahad Security College and Prince Naif Academy. Workshop leader and Co-author of Specified Deliverables for the *Project Specific Agreement between the United States of America and the Kingdom of Saudi Arabia*. Riyadh, Saudi Arabia, November 7-22, 2013.

(2013). WMD Cyber Crime Investigations. Primary instructor – 40 hour course. *Defense Threat Reduction Agency International Counterproliferation Program*. Baku, Azerbaijan, September 16-20, 2013.

(2013). Theoretical framework for coordinating training programs with business processes and policies in large organizations. Primary speaker. *Interactive Learning Technologies Conference*. Reston, Virginia, August 16, 2013.

(2012). WMD Cyber Crime Investigations. Primary instructor – 40 hour course. *Defense Threat Reduction Agency International Counterproliferation Program*. Pristina, Moldova, November 12-16, 2012.

(2012). WMD Cyber Crime Investigations. Primary instructor – 40 hour course. *Defense Threat Reduction Agency International Counterproliferation Program*. Singapore, August 27-31, 2012.

(2012). Program Review for National Security Diploma for Higher Institute of Security Studies, King Fahad Security College. Author and Task Analysis Facilitator. *Summary of the FBI Visit to the King Fahad Security College and Prince Naif Academy*. Riyadh, Saudi Arabia, April 19 – May 5, 2012.

(2012). Program Review for Cyber Crime and Computer IT Security, Prince Naif Academy. Author and Workshop Facilitator. *Summary of the FBI Visit to the King Fahad Security College and Prince Naif Academy*. Riyadh, Saudi Arabia, April 19 – May 5, 2012.

(2012). ADDIE: Introduction to Instructional Systems Design. Speaker and Curriculum Assessor. *FBI Assessment of Police Training in the Kingdom of Saudi Arabia*. Riyadh, Saudi Arabia, April 19 – May 5, 2012.

(2012). WMD Cyber Crime Investigations. Primary instructor – 40 hour course. *Defense Threat Reduction Agency International Counterproliferation Program*. Tirana, Albania, February 27 – March 2, 2012.

(2011). Click and Talk: Tips for PowerPoint Presentations. *FBI Knowledge Week*. FBI Headquarters, Washington, DC, November 18, 2011.

(2011). Social Media: Introduction and Trends. Lead speaker. *FBI National Academy Alumni Association Conference*. Fort Lauderdale, Florida, July 18, 2011.

(2011-2012). Instructional Systems Design for Overseas Instructors. Instructor and Panelist. *FBI Weapons of Mass Destruction Directorate*. FBI Headquarters, Washington, DC.

(2008-2015). Instructor Development Course. Primary instructor – 40 hour course. *FBI Instructor Development Program*. Delivered a 40 hour course to FBI employees and local law enforcement officers in Miami, Florida, Oklahoma City, Oklahoma, Minneapolis, Minnesota, Wheeling, West Virginia, Fredericksburg, Virginia, and Quantico, Virginia.

(2008). Kiper, J.R. Online strategies for teaching business processes in large organizations. *Journal of Instruction Delivery Systems*, 22, 2. 14-18.

(2008). Adding value to e-learning with blogs, wikis and podcasts. Presenter and panel member with Trudy Abramson, Avril Best, Jennifer Bigus, Sandra Lebron-Lozada, Marilyn Olander, Brenda Stutsky and Yvette Dulohery. *Interactive Technologies Conference*. Arlington, Virginia, August 20, 2008.

(2007). Human intelligence (HUMINT) compliance matters. Presenter as Confidential Human Source Coordinator. *FBI HUMINT Conference*. Dallas, Texas, November, 2007.

(2007). Teamwork in investigation: Prosecutor and police – the U.S. experience. Primary speaker and panel member with Sam Nazzaro and Steve Salmieri. *ABA CEELI Judicial Training Conference*. Novi Sad, Serbia, September 13, 2007.

(2007). The elements of a protection program: Witness protection, victim/witness assistance, and witness security. Conference coordinator, primary speaker, and panelist. *El Salvador Witness Security Conference*. San Salvador, El Salvador, July 14-20, 2007.

(2004). **Preparing for the FBI's New Case Management System**. Training Team Lead, Conference Speaker, and Workshop Facilitator. *FBI VCF Transition Team Conference*. New Orleans, Louisiana. March 13 – April 15, 2004.

## **MEMBERSHIPS**

---

Global Information Assurance Certification (GIAC) Advisory Board  
FBI American Indian and Alaskan Native Advisory Committee (AIANAC)  
Project Management Institute (PMI)  
Upsilon Pi Epsilon (UPE) Honor Society  
FBI Agents Association (FBIAA)  
Federal Government Distance Learning Association (FGDLA)  
United States Distance Learning Association (USDLA)  
Society for Applied Learning Technologies (SALT)  
Association for Supervision and Curriculum Development (ASCD)  
Federal Law Enforcement Officers Association (FLEOA)  
Federal Law Enforcement Training Accreditation (FLETA)  
Society of Former Special Agents of the FBI  
Discovery Society Center for Science and Culture  
Church of the Nazarene

## **LANGUAGES**

---

English – Native language

Spanish – Speak fluently and read/write with high proficiency

Mandarin Chinese – Speak, read, and write with basic competency

## **RESEARCH INTERESTS**

---

Business Process Management

Instructional Systems Design

Knowledge Management

Online Learning

Law Enforcement Training

Investigative Techniques

Cybercrime and technology-enabled deviancy

## **OTHER SKILLS**

---

Business Process Modeling

Online Learning Environment design with Canvas

Proficiency with Adobe Illustrator, Photoshop, and all Office Suite applications

Graphic art – Ink, pencil, pastel, and digital art

Music performance – keyboard, percussion, bass guitar

## **REFERENCES**

---

Scott Janezic – FBI Supervisory Special Agent, Miami Field Office

754-703-2000, [scott.janezic@gmail.com](mailto:scott.janezic@gmail.com)

Tariq A. Alsheddi, Ph.D. – Director of Naif Academy for National Security, Saudi Arabia

+966-1-2686308, [t-alsheidd@moisp.gov.sa](mailto:t-alsheidd@moisp.gov.sa)

G. Clayton Grigg, PMP – FBI Chief Knowledge Officer

571-350-4217, [gibtoo2003@gmail.com](mailto:gibtoo2003@gmail.com)

Steven Krueger – FBI Section Chief, FBI Academy

337-233-2164, [SKrueger314@gmail.com](mailto:SKrueger314@gmail.com)

Chris McCranie – FBI Special Agent, Washington Field Office

202-278-2000, [cmccranie@hotmail.com](mailto:cmccranie@hotmail.com)

Micheal Neubauer, Ph.D. – Program Manager, FBI Laboratory

202-324-3000, [mjneubauer@outlook.com](mailto:mjneubauer@outlook.com)



# **EXHIBIT E**

**(Report of Steven Abrams)**

United States of America

v.  
Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF

Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

**PERSONALLY APPEARED BEFORE ME, the undersigned, who, being duly sworn,  
deposes and states the following:**

1. My Name is Steven Marc Abrams. I am a licensed Attorney and Counselor at Law, in good standing, in South Carolina, Washington, DC, and New York. I am a retired State Constable in South Carolina. My field of concentration is digital forensics. I have assisted municipal, county, state, and federal law enforcement agencies and the US Department of Defense and the Department of State with digital forensics investigations for over three decades. For 11 years, from 2008 until 2019, until my retirement I held a law enforcement commission from the Governor of South Carolina at the request of the United States Secret Service. My office address is 1154 Holly Bend Drive, Mount Pleasant, South Carolina 29466. My office phone number is (843) 216-1100. My full credentials are included in my CV which is appended to this affidavit.
2. From 2002 until 2014, I taught digital forensics classes to police and military organizations around the world using Accessdata FTK. I am familiar with the tool, first being certified in its use at the North Carolina Justice Academy (NC state police academy) in 2002. I have used FTK regularly for nearly 20 years.
3. In my career as a digital forensics' examiner working closely with law enforcement I have never observed, or examined creditable evidence of, a purposeful mishandling of digital evidence by any law enforcement agency, nor made any report of the same. I have never previously observed or reported evidence tampering by law enforcement.
4. I was retained by counsel and signed onto the Protective Order on 05/21/21 to review certain digital forensics evidence used in the trial of Keith Raniere *et al*. In the process of fulfilling that mission I reviewed (1) relevant portions of trial transcript,(2) the written statements of other experts for the defense, (3) the government's digital forensic evidence

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF

Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

provided to me by Mr. Raniere's defense counsel pursuant to the protective order, and (4) have conducted my own experiments using a Canon EOS 20D camera similar to the one that was used to create certain digital photographic material and related filesystem artifacts that are relevant to the government's case against Mr. Raniere. I have also used various digital forensics tools from AccessData, BlackBag Technologies, and CelleBrite to review portions of the Government's evidence that were provided to me.

5. This affidavit concerns my review of the April 25, 2022, "Summary of Technical Findings" by J. Richard Kiper, Ph.D., PMP. Dr. Kiper, is a retired FBI Special Agent and Forensic Examiner. Dr. Kiper reviewed forensic evidence and trial testimony related to certain digital photographs, some of which the government alleged were contraband. Crucial to this claim by the government was an accurate fixing of the date the photographs were taken, and as with all evidence, proof that the photographic evidence in question was reliable and authentic. The way the photographic material was handled by the FBI, who performed the forensic examination of the evidence for use at trial, is a crucial "gatekeeper" threshold question for any forensic evidence that is destined for use in a criminal trial. Dr. Kiper further addressed the FBI's evidence handling in this matter in his April 25, 2022, "Summary of Process Findings." While I have worked parallel investigations with the FBI, I have never worked for the Bureau, so I don't have direct knowledge of FBI policies and procedures and have therefore taken this document at face value and used it to provide further understanding of Dr. Kiper's Summary of Technical Findings.
6. In his Summary of Technical Findings Dr. Kiper noted seven key findings that lead him to conclude the evidence was manually altered while in the custody of the FBI, and these manual alterations taken together lead him to conclude the FBI tampered with key evidence during the months prior to Mr. Raniere's trial. After a careful review of the

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF

Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

evidence and the work done by Dr. Kiper, I agree that the data and forensic artifacts cited by Dr. Kiper are genuine. Further, it saddens me to concur that the only logical conclusion to be drawn by any reasonable person for the set of forensic artifacts demonstrated by Dr. Kiper is that a manual alteration of the digital photographic and filesystem evidence, and an unsuccessful attempt to cover that manual alteration, occurred while the evidence was in the custody of the FBI.

**Finding 1.**

7. Dr. Kiper's first finding deals with certain photos found both on a CF card from a Canon 20D camera and on a Western Digital Hard drive ("WD HDD") that were two key sources of evidence relied on by the Government. The Government needed to show that the photos in question were created and possessed by Defendant. However, the origin of the photos on the WD hard drive was uncertain. Throughout the case the government alleged that the Canon 20D camera belonged to Defendant and thus they could argue that any photos taken by that camera and found on a CF media card that was associated with that camera, were likely taken and possessed by Defendant.
8. the government made two different forensic images of the CF card associated with the 20D camera. This second image of the CF card is crucial to Dr. Kiper's first and second finding. On the second image of the CF card, and only on the second image, there appeared a set of files whose filenames and modified dates were identical to the digital photos found on the WD hard drive (WD HDD) that were in the same range as the alleged contraband, all purportedly taken by the same camera. Because the filenames and dates matched between the backup located on the WD HDD and CF card, it appeared that the contraband photos also came from the CF card that was in the camera that was alleged to be used by Defendant, even though none of the contraband, or remnants, were found

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
 DISTRICT COURT  
 EASTERN DISTRICT OF NEW YORK  
 CRIMINAL DOCKET FOR  
 CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF

Steven M. Abrams, J.D., M.S.  
 In Support of the Summary of  
 Technical Findings by  
 J. Richard Kiper, PhD, PMP

on the CF card. However, forensic analysis of the files from both the CF card and the WD hard drive revealed that although containing the same filenames and modified dates, they contained different MD5 hashes, and thus different contents. MD5 hash codes are large prime numbers that are computed from every byte of data in a file, and thus uniquely identify files by every bit of data contained within them. Any alterations to a file will change the MD5 hash code value for the file. Thus, hash codes, such as MD5, are used to quickly determine to near 100% accuracy if the data contained within two digital files is the same or different. In this case two sets of files that appeared outwardly to be the same, one set on the WD HDD backup and the other on the CF card from the camera, are in fact completely different. Dr. Kiper concluded in his first finding that it was not possible for these two unrelated sets of files to have the same filenames and dates, down to the exact second, unless someone intentionally set it up to look that way to create the appearance of a stronger connection between the contents of the CF card and a backup contained on the WD hard drive. I agree.

### Finding #2.

9. Dr. Kiper's second finding deals with the manual addition of digital photos onto the Compact Flash (CF) card used as digital media in a Canon 20D camera which held the photos that became the Government's key evidence in this case. These are the same suspicious digital photos that were discussed above in Finding 1. The trial record indicates that the FBI made two different forensic images of the CF card associated with the Canon 20D camera. The initial forensic image was made in April 2019 and a second forensic image was made in June 2019. The forensic image made in June contained additional files which the filenames indicate are digital photos (discussed in Finding 1) not contained

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
 DISTRICT COURT  
 EASTERN DISTRICT OF NEW YORK  
 CRIMINAL DOCKET FOR  
 CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF  
 Steven M. Abrams, J.D., M.S.  
 In Support of the Summary of  
 Technical Findings by  
 J. Richard Kiper, PhD, PMP

in the forensic image made in April 2019. That the contents of the two forensic images were not identical is significant and troubling. Forensic imaging is based on the foundational principle that no matter how many different examiners make an image of a given device that the forensic image produced by any competent examiner using any valid imaging tool will contain exactly the same data (e.g., set of contents) as the image produced by any other competent examiner from that common device. Any differences in the data between the forensic images, no matter how minor, is de facto proof that the contents of the device being imaged changed from the time the image was first made to when the subsequent image was made. In this case, alarmingly, the second image made in June 2019 contained additional files not contained in the original forensic image made in April 2019.

Upon determining that the two forensic images of the CF card contain different evidence a neutral investigator must ask if there could be any innocent explanation for how these two images of the same device contained different contents? In the past I have seen AccessData FTK under carefully controlled laboratory conditions produce different numbers of files from the same e01 forensic image file when running under different version of Microsoft Windows. That anomaly does not seem to apply here, the two forensic images contain different evidence. Dr. Kiper has identified specifically the files that were added to the second forensic image. Dr. Kiper explored the origins of these new files that appeared in the June 2019 forensic image of the CF card in his finding #1. He also determined that not a single viewable photo was able to be carved out of these new files despite filenames and system dates that made them appear to be specific digital photos that also appeared on the Western Digital hard disk drive ("WD HDD") that was another source of evidence used by the FBI in its investigation. Dr. Kiper noted that despite

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
 DISTRICT COURT  
 EASTERN DISTRICT OF NEW YORK  
 CRIMINAL DOCKET FOR  
 CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF  
 Steven M. Abrams, J.D., M.S.  
 In Support of the Summary of  
 Technical Findings by  
 J. Richard Kiper, PhD, PMP

the file names and system dates of the new files on the CF card being identical to photos appearing on the WD HDD, none of the MD5 hashes of the new files appearing on the CF card matched the MD5 hashes for similarly named files on the WD HDD. Thus, they were not the same files, only the names and dates were identical, not the contents. He surmises that someone created the new evidence on the CF card with similar names and dates to files on the WD HDD to make the link appear stronger between the evidence on the WD HDD (from an uncertain providence) and the evidence from the CF card that the government contended was linked to Keith Raniere. I have reviewed Dr. Kiper's analysis, and his work is conclusive to a scientific certainty. **Based on Dr. Kiper's thorough analysis, I sadly concur that the only reasonable explanation of the additional files appearing in the FTK listing of files on the CF card from the June 2019 forensic image is that additional evidence was manually added to the CF card between April 2019 and June 2019 while the CF card was in FBI custody and that was likely done to make evidence found on the WD HDD appear to be linked to the CF card, which the government contended was linked to Mr. Raniere.**

**Finding #3.**

10. Dr. Kiper's third finding is that the filesystem access date metadata was overwritten on 9/19/2018. I agree. This sort of mishandling of digital evidence is common among lay people, I regularly observe attorneys mishandle their client's evidence produced in discovery in this manner, but this sort of mishandling of evidence is unexpected from the FBI. This alteration of the access date metadata proves to a scientific certainty that the CF card was inspected without using a write protect device or write blocking software on the computer used to review the data on the CF card. This is either a rookie mistake, or

United States of America  
v.  
Keith Ranieri, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF  
Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

a purposeful act of digital sabotage. Either way **this crucial filesystem metadata was spoliated while the CF card was in FBI custody.**

**Finding #4.**

11. Dr. Kiper's fourth finding is "Dates of photos on the hard drive were altered through manual intervention." This finding is based on a comparison of the modified date metadata of certain jpeg files on the CF storage card from the Canon camera and the metadata on the same files in a backup copy on a computer hard drive. Every jpeg photo contains two types of metadata, filesystem metadata, common to all computer files, and EXIF metadata that is embedded within the JPEG photo itself. Both types of metadata preserve timestamp information associated with the photo. In a perfect world one would expect there to be a logical relationship between the EXIF timestamps from images on the camera CF card and the modified filesystem timestamp from the image files on the hard drive. In this case, the timestamps start out being 1 hour apart, with the hard drive copy being one hour behind the camera media. Then on 10/30/2005 when daylight saving time ends it appears the computer falls back and is two (2) hours behind the camera, which is not programmed to handle daylight savings time. This might be what one would expect to see happen at the end of daylight savings time. However, unexpectedly by the afternoon of 10/30/2005 when the next photo, IMG\_138.jpg, is taken the clocks in the computer and camera are in synchrony and there is no difference between the timestamps in the computer and camera. We do not know when the photos were copied to the hard drive, but the timestamp differences would not have happened in real time, as the data on the CF card was not written to the camera until some later time. Given that the camera was not programmed to make changes to its time settings as a result of Daylight Savings Time,



United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.AFFIDAVIT OF  
Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

and used a FAT 16 filesystem on the CF card two things are known to be true: First, the camera was incapable in making any automatic changes to its time settings and requires a manual setting of the time by the camera user for any time settings observed in the data produced by the camera. Second, given the FAT 16 file system one would expect the filesystem modified timestamp on the CF card to be copied exactly, without any adjustments for time zone or Daylight Savings Time, on any copies of the files copied to a computer or external media. There is a possibility that Windows may have been set to automatically adjust for Daylight Savings Time, and that might account for some of the one hour shifts of the clock in this data. This would not account for a two-hour shift seen in one day, as for example on 10/30/2005. Thus, it would appear that these odd shifts in timestamps could not be accounted for by any software mediated process, and at least some of these time shifts resulting in a two hour difference were more likely the result of manual intervention. **I agree with Dr. Kiper's Fourth finding. The filesystem modified timestamps on this evidence are highly suspect and unreliable. The most plausible explanation for the pattern of time differences observed in this data, especially those that are two hours different, is manual manipulation of the timestamps.**

#### **Finding 5.**

12. Dr. Kiper's fifth finding deals with IMG\_0175.jpg, and the curious metadata on and embedded within that photo. The first red flag in this photo is in the EXIF data which indicates that the image was modified using "Photoshop Adobe Elements 3.0." From this information alone we know that someone modified this photo. It is not in its original state as captured by the camera. Next, the filesystem modified timestamp on the CF card copy of the image matches the filesystem modified timestamp on the copy of this image on the hard drive. This is another red flag, as one would

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
 DISTRICT COURT  
 EASTERN DISTRICT OF NEW YORK  
 CRIMINAL DOCKET FOR  
 CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF  
 Steven M. Abrams, J.D., M.S.  
 In Support of the Summary of  
 Technical Findings by  
 J. Richard Kiper, PhD, PMP

expect that if one edited the photo and resaved it using Photoshop that the modified timestamp should reflect the time of the editing, not the time the photo was taken and written to the CF card by the camera. Thus, one must conclude there was an attempt to conceal the fact that the photo was altered on the hard drive by manipulating the filesystem modified timestamp on the computer hard drive to match the filesystem modified timestamp on the CF card. I therefore agree with Dr. Kiper that this digital photograph, IMG\_0175.jpg, was manually modified ("Photoshopped") using Photoshop Adobe Elements 3.0, and the fact that the filesystem modified timestamp was not changed to reflect the editing with Photoshop is evidence for Dr, Kiper and me, that someone likely manually modified the filesystem timestamp to conceal the fact the image was edited with Photoshop. The only reason we know that this file (IMG\_0175.jpg) was edited with photoshop is that this is the only photo that still has the CreatorTool field intact in the EXIF header. As Dr. Kiper points out this probably was an oversight by whomever did the editing. I think that Dr. Kiper is likely correct.

#### **Finding #6.**

13. Dr. Kiper's sixth finding concerns the folder names of the folders that contain the alleged contraband photos. The folder names appear to contain an embedded computer-generated time and date "timestamp". This embedded timestamp was crucial evidence for the Government at trial as it was the only basis the Government had to "independently" determine the date when the alleged contraband photos were taken, apart from easily editable EXIF dates. A careful review of this embedded timestamp data by several experts for the defense all conclude that this data is not reliable and at least some of this data was likely assembled manually in an attempt to appear to have been generated automatically

by a computer program to add an appearance of credibility to the timestamps. In finding #4 it was determined that Adobe Photoshop Elements 3.0 was used to edit at least one of the photos. This program can also be used to import photos from a camera. When the Adobe Photoshop Elements software is used to import photos from a camera it can create a timestamped folder with an embedded timestamp. It is important to note that that the timestamp which is embedded in the filename corresponds to the date the images are imported, not when they were taken. So even if this was the means of creating the timestamped folder names, the timestamps would not accurately reflect when the photos were created, as was claimed by the Government.

- 14. Upon careful review of the folder names and the files copied into each folder it appears impossible that a program imported the files and created the folder names with the embedded timestamps as the Government claimed had happened, and therefore had to have been manually manipulated. For example, the folders "2005-10-19-0727-57" and "2005-10-19-0727-59" would have been created only two seconds apart, yet the earlier folder ending -57 contains nine photos, and the later folder ending -59 contains 11 photos. It seems unlikely, given how slow the Canon D20 with its CF media was to upload photos, that these nine photos could be copied in only two seconds. Also, the sequence of photos in these folders doesn't make any sense if one assumes a program created the folders and copied the photos into them. The earlier folder (ending -57) contains images numbered 0090 to 0098, while the later folder (ending -59) contains images numbered 0079 to 0089. It seems very unlikely that a program would copy the photos off the CF media out of order. This is outside my experience as an avid amateur photographer familiar with all the leading photo software packages.

United States of America

v.  
Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF

Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

15. The only plausible explanation I can think of for this evidence is that someone manually created these folder names as part of a scheme to have a legitimate appearing means of proving when the alleged contraband images within the folders were taken. This was necessary as there was no reliable means of dating the alleged contraband photos from the computer filesystem metadata which had been corrupted prior to the FBI's examination of the computer, or the camera date which was also unreliable. During the trial the FBI examiner and the prosecutor both used the likely fictitious timestamp embedded in the folder names as a means of establishing a date for the alleged contraband photos contained within the folders and told the jury they knew when the photos were taken based on the dates in the folder names. This is totally unscientific and misleading at best. **Based on the totality of the evidence, the way in which the government relied on these embedded timestamps at trial, to establish a date certain that the alleged contraband photos were taken, was knowingly and purposely misleading to both the Court and the Jury. I agree with Dr. Kiper's conclusion regarding his finding #6.**

**Finding #7.**

16. Dr. Kiper's seventh finding deals with an apparent attempt to plant incriminating evidence in a backup on the hard drive. This planted evidence consists of a selective (manual) backup containing the alleged contraband images. The planted backup appears to be part of a series of backups performed on 03/30/2009. Each of the backups in the series contains the name of the computer model and the backup date embedded within the filename for the backup. It appears the filenames for each backup in the series was automatically generated from the computer name and the date the backup was made. The

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
 DISTRICT COURT  
 EASTERN DISTRICT OF NEW YORK  
 CRIMINAL DOCKET FOR  
 CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF

Steven M. Abrams, J.D., M.S.  
 In Support of the Summary of  
 Technical Findings by  
 J. Richard Kiper, PhD, PMP

files in the first two backups have filesystem metadata indicating they were copied into the backup on 3/30/2009, the date embedded in the filenames for the backups. However, this is not true for the files contained in the third (suspect) backup. Based on the filesystem metadata for the files within the third backup, it appears that someone manually generated the filename from the computer model and a misleading timestamp to make the backup appear to be part of the series of backups from 03/30/2009. This leads us to conclude there was an attempt to create this selective backup and make it appear to be part of a series of automatic backups that were made to the hard drive on 3/30/2009. This misleading filename and the fact that the alleged contraband images were cherry picked to be included in the backup strongly suggests that someone created this backup and placed it on the hard drive to plant incriminating evidence while attempting to conceal the fact the evidence was being planted in this manner. I agree with Dr. Kiper's interpretation of this evidence.

17. In addition to concurring with Dr. Kiper's observations and conclusions, I have a few additional observations that I made in my review of this evidence that I would like to include in this affidavit. In my reading of the trial transcript of FBI examiner Booth, I was struck by two points that he made and that were then echoed by the prosecution that he knew or should have known after his many years as an FBI Digital Forensics examiner to be false or likely false. To wit:
  18. First, Booth's insistence that the dates embedded in the EXIF headers of the evidence photos were known to be reliable, even in the absence of any extrinsic evidence, because EXIF data was so hard to alter is misleading at best. A cursory search of the Internet would inform Mr. Booth and the Prosecution that there are many readily available inexpensive

United States of America

v.

Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF  
Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

(or free) software products that facilitate changing EXIF data of the kind that Booth insisted was not easy to change. Additionally, the Adobe Photoshop Elements 3.0 software that was used to alter at least one evidence photo (see Finding 4 above.) and to possibly import some of the images discussed in Finding #5 above, has a built-in feature that allows one to alter the EXIF timestamps. Since we already know that someone was manipulating the photographic evidence in this case with Photoshop Elements software, we know that same person had a tool that was designed to easily change the EXIF timestamps at will. Thus, Booth was either negligent or perjurious in his insistence that the EXIF timestamp data embedded in the photographic evidence used at trial was hard to change because it "was designed that way."

- 19. Second, Booth's testimony that it was not unusual to receive evidence in an unsealed evidence bag is similarly misleading and similarly seems to be his position at trial because it helped bolster the crucial evidence that the Government needed to rely on despite its dubious nature. While I have never worked for the FBI, I was sworn law enforcement for over 11 years at the request of the US Secret Service field offices in South Carolina. In all I worked digital forensics cases for over two decades with Municipal, State and Federal law enforcement agencies (including the FBI and US Secret Service) and with military units of the United States and friendly foreign countries. During all that time it was always my experience that evidence was placed into a sealed evidence bag and a chain of custody started by the agent / officer who initially collected the evidence. In hundreds of cases I was the initial officer who collected the evidence and began the chain of custody. I always placed the evidence into an evidence bag and affixed a tamper evident seal before passing the evidence on in the chain of custody as I and every other classmate of mine at the North Carolina Criminal Justice Academy was trained to do. I was taught that

United States of America

v.  
Keith Raniere, et al

IN THE UNITED STATES  
DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
CRIMINAL DOCKET FOR  
CASE #: 1:18-cr-00204-NGG-VMS.

AFFIDAVIT OF  
Steven M. Abrams, J.D., M.S.  
In Support of the Summary of  
Technical Findings by  
J. Richard Kiper, PhD, PMP

any evidence that arrived from further down the chain of custody in an unsealed state should be considered to be outside a proper chain of custody and not usable in a criminal matter. This is not just my experience in all the agencies for whom I worked, but also what Dr. Kiper reported from his knowledge of how things worked at the FBI. Not only would Examiner Booth have known that unsealed evidence was unusual and suspect, the prosecutor also would have been well aware of this issue, and wary that it could form the basis of a successful motion by the defense for exclusion of the evidence. Booth's insistence that the unsealed evidence in this case was not unusual was nothing other than a gratuitous false statement meant to preserve evidence that rightly should have been found to be inadmissible.

**FURTHER THE AFFIANT SAYETH NOT!**



\_\_\_\_\_  
Steven Marc Abrams, J.D., M.S.

SWORN TO AND SUBSCRIBED BEFORE ME THIS  
16 DAY OF April, 2022.



NOTARY PUBLIC FOR SOUTH CAROLINA  
MY COMMISSION EXPIRES: March 18, 2024

# **EXHIBIT E1**

**(CV of Steven Abrams)**



**APPENDIX A.**

**Steven M. Abrams, J.D., M.S.  
Curriculum Vitae**

**Steven M. Abrams, J.D., M.S.**  
**Attorney, Digital Forensics Examiner and Instructor**  
**1154 Holly Bend Drive**  
**Mount Pleasant, SC 29466**  
**843-216-1100**  
**Steve@AbramsForensics.com**

**Curriculum Vitae**

My key practice areas are Computer Forensics, e-Discovery, and Computer Law.

**Education**

- 2016 -Techno Security 2016, Computer Forensics Training Seminar, Myrtle Beach, SC, June 5-8, 2016
- 2014 -Georgia Bureau of Investigations, Internet Evidence Finder Forensics Training, Decatur, Georgia, February 2014
- 2013 -Techno Security 2013, Computer Forensics Training Seminar, Myrtle Beach, SC, June 2-5, 2013
- 2012 -Techno Security 2012, Computer Forensics Training Seminar, Myrtle Beach, SC, June 3-6, 2012
- 2011 -November 9-12: EnCase 7 Training, Salt Lake City, UT  
-November 6 – 9: Paraben Forensics Innovations Conference, Park City, UT  
- South Carolina Assoc. of Legal Investigators (SCALI) Annual Training Seminar, May 2011  
- April 7, 2011: SC Electronic Crime Task Force Quarterly Meeting and Training
- 2010 -Techno Security 2010, Computer Forensics Training Seminar, Myrtle Beach, SC, June  
- SCALI Annual Training Seminar, May 2010
- 2009 - Cellebrite Mobile Device Forensics Certification (CCMDE), SEMAR, Mexico City, Mexico  
-SCALI Annual Training Seminar, May 2009
- 2008 - South Carolina Basic Constable Training, Tri-County Technical College / SC Criminal Justice Academy, October – November 2008  
- Commissioned as a South Carolina State Constable (LEO) on November 20, 2008.  
- Techno Security 2008, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- 2007 - Charleston School of Law, Charleston, SC, Juris Doctor (J.D. - Magna Cum Laude)  
- GMU2007 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2007 (40 CEU HTCIA)  
- Techno Security 2007, Computer Forensics Training Seminar, Myrtle Beach, SC, June

- 2006 - University of Aberdeen, School of Law, Kings College, Old Aberdeen, Scotland  
in collaboration with the University of Baltimore Law School  
Summer Law Program in Comparative Criminal Procedure and UK Business Entities &  
Taxation
- Techno Security 2006, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2006
  
- 2005 - SCALI Annual Training Seminar, May 2005
- SCALI Fall Training Seminar, October 2005
  
- 2004 - Access Data Advanced Windows Forensics, June 23-25, 2004, New York City. (24  
Credit Hours)
- SCALI Annual Training Seminar, May 2004 (10 CEU)
  
- 2003 - GMU2003 Computer Forensics Symposium, Regional Computer Forensic Group  
of the High Technology Crime Investigation Association, George Mason University,  
Fairfax, VA. Aug.2003, (40 CEU HTCIA)
- Techno Security 2003, Computer Forensics and Security Conference (24 CEU)
- SCALI Annual Training Seminar & PI Training Seminar (16 CEU SLED)
  
- 2002 - SCALI Annual & Fall Training Seminars (16 CEU SLED)
- GMU2002 Computer Forensics Symposium, Regional Computer Forensic Group  
of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2002,  
(40 CEU HTCIA)
- Access Data Computer Forensic Boot Camp, North Carolina Justice Academy,  
Edneyville, NC (24 CEU)
  
- 1992-1994 Microsoft Internet Developer Workshops NY, NY
  
- 1992-1993 Novell NetWare CNE Training, IBM Skills Discovery, Jericho NY
  
- 1984-1985 Microcomputer and Electronics Engineering, Hofstra University, Hempstead NY
  
- 1982-1983 Ph.D. Studies, Faculty Fellowship, Columbia University, Graduate School of Arts &  
Sciences
  
- 1981-1982 Columbia University, College of Physicians & Surgeons, Master of Science (M.S.)
  
- 1977-1981 Allegheny College, Meadville PA, Bachelor of Arts (B.A.) (Psychology - Computer  
Science)

### **Professional Licenses**

#### ***Current***

Licensed Attorney in South Carolina  
Licensed Attorney in District of Columbia  
Licensed Attorney and Counselor at Law in New York

#### ***Previous***

Licensed as a Private Investigator in South Carolina and New York (2002-2008), South Carolina  
State Constable (Sworn, 2008-2019).

**Experience (Selected)**

2016 – Present, Senior Attorney, Abrams Cyber Law & Forensics, LLC. Mount Pleasant, SC 29466. Concentration on Electronic Privacy and Defamation Cases, Electronic Discovery, and Digital Forensics.

2018 - Continuing Legal Education Instructor, ***Electronic Privacy Violations during Divorce: Legal and Ethical Guidelines for Family Law Practitioners***, SC Bar, Columbia SC (February 21, 2018).

2016 – Continuing Legal Education Instructor, ***Smartphones as evidence for Personal Injury Cases***, NBI, Charleston SC (December 8, 2016).

2011 – 2016 Sole Practitioner Abrams Law Firm, PC. Mount Pleasant, SC 29466

2011 - Digital Forensics Instructor / Investigator, H-11 Digital Forensics / United States Embassy, Tirane, Albania.

2010 – Facilitator, Instructor, Annual In-Service Legals and CDV Training (SLED), Lowcountry Constable Association.

2009 – Speaker, South Carolina Association for Justice, Hilton Head, SC (August 6, 2009) Topic: Civil Discovery of E-mails after *O’Grady*

2009 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Faculty, SC Bar Convention – Family Law Section CLE

2008 – 2011 Shareholder, Abrams Millonzi Law Firm, P.C., Mount Pleasant, SC 29464

2007 - Presenter, “E-Discovery: Definition, FRCP Changes and Application CLE”, NBI, Charlotte, NC, December 19, 2007

2007 - Digital Forensics Instructor/Investigator, H-11 Digital Forensics, United States Embassy, Mexico City, Mexico

2007 - **Presenter**, “Civil to Criminal: Collaborative Computer Forensics Investigations between PIs and Law Enforcement”, GMU2007, August 9th & 10th, 2007

2007 - Presenter – “A South Carolina Lawyer’s Roadmap to Navigating the New Federal E-Discovery Rules,” The South Carolina Bar (CLE Division), April 13, 2007.

2006 - Presenter – “Typical Internet Sexual Activity and its Detection”, Family Law CLE, The South Carolina Bar (CLE Division), November 2006.

2006 - Instructor, "3-day Hands-on Computer Forensics Workshop", Trident Technical College, N. Charleston, SC, CLE accredited by The South Carolina Bar, January 2006.

2005 - Lecturer, "Computer Forensic Introduction", Trident Technical College, CLE accredited by South Carolina Bar and CEU / In-Service hours for PIs / LE by SLED.

2001 - Present Steve Abrams & Company, Ltd. (dba Abrams Computer Forensics)  
Licensed Private Investigator, Computer Forensics Examiner

1998 - 2001 Steve Abrams & Company, Ltd. Mt. Pleasant, SC, President

1996 - Democratic National Committee, Instructor - Southeast and Northeast Regional Schools for Congressional Campaign Managers.

1995 – 1999 Direct Marketers of Charleston Mt Pleasant, SC, Partner  
Co-owner of Political Database Marketing Company and full service political print shop.

1994 - 1995 The Software Studio Mt Pleasant, SC, Owner  
Owner of software development company that developed database applications for the Newspaper publishing industry.

1992-1993 Town of North Hempstead, Manhasset, NY, Deputy Commissioner of Finance

1986 - 1992 Digitron Telecommunications, Inc., Huntington, NY, Director of R&D

1984 - 1986 Computer Associates International., Islandia, NY, Senior Systems Programmer

1983 Contel Information Systems Division. Great Neck NY, Software Engineer  
(Developed the first Network Forensics Applications for the DoD

### **Recent Publications**

Steven M. Abrams, Knowledge of Computer Forensics Is Becoming Essential for Attorneys in the Information Age, 75 N.Y. St. B. Assn. J. 8, 15 (Feb. 2003).

Steven M. Abrams, Knowledge of Computer Forensics, Essential for 21st Century Private Investigators, 16 PI Mag. 46, 59 (October 2003).

### **Professional Awards & Honors**

2008 – Member, SLED Ad Hoc Committee on Computer Forensics

2007 – CALI Excellence for the Future Award, Aviation Law, Charleston School of Law, Fall 2006

– CALI Excellence for the Future Award, Interviewing, Counseling & Negotiation, Charleston School of Law, Fall 2006

– CALI Excellence for the Future Award, Insurance Law, Charleston School of Law, Fall 2006

\_ Dean's List, Charleston School of Law, Fall 2006, Spring 2007.

2004 - "2004 SCALI Investigator of the Year"

2003 - Member, SLED Private Investigations Business Advisory Committee

### **Professional Associations**

Member, Institute of Electrical and Electronics Engineers - IEEE

Member, Lowcountry Constables Association - LCA

### **Bar Association Memberships**

Admitted to practice in **South Carolina, District of Columbia, and New York.**

### **Compensation**

I receive \$350 per hour, plus mileage, travel and lodging expenses, for all Computer Forensics services and for depositions and trial testimony.

### **Previous Expert Testimony**

I have completed over 1200 computer forensics investigations, the overwhelming majority of cases were settled and did not require me to testify.

South Carolina cases in which I was qualified in court as an expert are:

*Hillburn v. Hillburn*, (2001-DR-08-2354);  
*Smith v. Smith*, (2001-DR-22-212);  
*Natale v. Natale*, (2003-DR-10-775)  
*Berda v. Berda*, (2003-DR-10-1899);  
*Murphy v. Murphy* (2004-DR-10-1510) and  
*Overstolz v. Fountain of Youth Wellness Centers LLC* (2003-CP-10-000761).  
*Gitter v. Gitter* (2008-DR-10-2865)  
*Ricigliano v. Ricigliano*, (2009-DR-18-0102)  
*Edwards v Junevicus*, (2010-DR-10-4736)  
*BTM Machinery Inc. v. Michael J. Finley* (2013-CP-10-4366)  
*Cherry v Cherry* (2014-DR-10-95)  
*Whitfield v. Schimpf and Sweetgrass Plastic Surgery,*  
*LLC (Case No. 2017-CP-10-2758)*

I was qualified as a testifying expert on digital forensics in federal court in

*UHLIG, LLC, V JOHN ADAM SHIRLEY, (CIVIL ACTION No.. 6:08-1208-HFF)*

I have also prepared expert's reports under Federal Rule 26(a)(2)(B) for the following federal civil suits filed in the United States District Court for the District of South Carolina:

*Lumpkin v. Bennani*, (Civil Action No. 2:03-2904-23), and  
*Miller v. American LaFrance Corp.* (Civil Action No. 2:04-1668-23)  
*Microsoft v. BWC Products Inc.* (Civil Action No. 2:06-CV-2023-CWH)  
*Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al.* (Civil Action No. 2:07-CV-00673-PMD)  
*Mainfreight v. John Marco, et al.*, (Civil Action No. 9:cv00563 JFA)

I was appointed the Court's Expert in US District Court, District of South Carolina, Rock Hill Division:

*The Travelers Home and Marine Ins. Co. v. Pope*, C/A No.: 0:10-cv-1688-JFA

I was qualified as a computer forensics expert in North Carolina courts in:  
*Hollins v. Lightfoot.*

In addition, I have been deposed in the following matters over the past ten years:

*Thomas & Assoc. v. Christopher Humphreys* (Case No. 2018-CP-10-0455)  
*Catherine Cope v. Wells Fargo Bank N.A., Century 21 Properties Plus, and Jim Bailey, individually;* (Case No.: 2018-CP-18-00112)  
*Rick Gray v. Church Mutual* (2017)  
*Calandra v. Calandra* (2004-DR-10-2675)  
*McLernon v. McLernon* (2003-DR-10-3090)  
*White v. Cassidy* (2004-DR-08-256)  
*Khoury v. Noce* (2006-CP-10-001830)  
*Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al.* (Civil Action No. 2:07-CV-00673-PMD)  
*Mainfreight v. John Marco, et al.*, (Civil Action No. 9:cv00563 JFA)  
*Beard v. Dunn & Dixon-Hughes et al*, (Case No. 2010-CP-08-0776)  
*UHLIG, LLC, V JOHN ADAM SHIRLEY*, (CIVIL ACTION No.6:08-1208-HFF)  
*ALTMAN, ET AL. V. FIRST CITIZENS BANK AND TRUST COMPANY* (2012-CP-34-0124)

(Revised: Sept 11, 2019)

# **EXHIBIT F**

**(Report of Wayne B. Norris)**



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**



**Because Accuracy Matters**

2534 Murrell Road, Santa Barbara, CA 93109-1859

VOICE PHONE: +1-805-962-7703 FAX +1-805-456-2169

EMAIL [Wayne@Norris-Associates.com](mailto:Wayne@Norris-Associates.com) URL <https://Norris-Associates.com>

**LinkedIn** <https://www.linkedin.com/in/wayne-norris-193b88>

27 April 2022

**USA VS RANIERE**

**THIRD-PARTY REVIEW OF DR. JAMES RICHARD KIPER**

**FORENSIC COMPUTER ANALYSES**

**BY**

**WAYNE B. NORRIS**

By: \_\_\_\_\_

Wayne B. Norris, REVIEWER



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**EXECUTIVE SUMMARY**

My name is Wayne B. Norris. I have had a long career in information technology, software development, computer forensics, nuclear research, and aerospace engineering, with service in the legal, commercial, military, aerospace, and national security communities, and have been a software developer since 1959. I have served as an expert witness in more than 100 technology related cases in federal, state, and municipal courts since 1986.

In my practice, I perform expert witness work in the areas of digital forensics, software intellectual property, engineering, and physics, and I make use of multiple forensic tools including FTK and FTK Imager from AccessData and Autopsy from The Sleuth Kit. I have served in approximately five cases involving alleged digital evidence tampering by civilians since 2003, all of them in civil. I have never been involved in, and indeed, have never previously heard of, any credible allegations of evidence tampering by any law enforcement agency under United States jurisdiction.

I was asked by individuals working for the Defense in the appeal of the case of USA vs Keith Raniere, *et al* to perform two related reviews of data relating to that case.

- The first review is referred to in this document as the **TECHNICAL REVIEW**. It consists of my review of the evidence analysis in the Raniere case that was prepared by the principal expert witness for the Defense, Dr. James Richard Kiper, and to comment on his analysis and his findings. Specifically, I was asked to state whether I agreed or disagreed with his analysis and findings.
- The second review is referred to in this document as the **MANAGEMENT REVIEW**. It consists of an estimate the scope of work required to produce the data alterations initially discovered in the Government's evidence by Dr. Kiper and listed in his report, as mentioned above.

For both reviews, I relied on the following resources:

- [Affidavit\\_with\\_Reports\\_04-25-2022.pdf](#) [59 pages].
- [DX 945.pdf](#)



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

- [DX 960.pdf](#)
- A forensic image in E01 format of files relevant to the case. This image did not contain any images suspected to be contraband;
- Data tables from the document [GX 521A.pdf](#) [36 pages]. This is a report by the Government dated 4/11/2019 that contains summaries of files from an evidence file image in dd form with the DISPLAY NAME NYC024299.001; and
- Data tables from the document [GX 521A-Replacement.pdf](#) [231 pages]. This is a report by the Government dated 6/11/2019 that contains summaries of files from the LEXAR CF 2 GB CARD. The ID NUMBER of the data image file is NYC024299\_1B15a.E01.

NOTE 1: The E01 image and the documents beginning with the letters GX are subject to nondisclosure of their contents. No part of those documents that was subject to non-disclosure was disclosed by me to any party as a result of this work.

NOTE 2: I did NOT personally receive a copy of the CF card image. Those files are analyzed in [GX 521A-Replacement.pdf](#).

I was NOT asked to duplicate Dr. Kiper's findings. Rather, I was asked to verify the underlying data, review his findings, and comment on it.

DISCLAIMER: In his [Affidavit\\_with\\_Reports\\_04-25-2022.pdf](#) report, Dr. Kiper discussed what, in his opinion as a retired FBI digital forensic examiner, were significant shortcomings in the internal handling of digital evidence from multiple storage media by agents and technicians assigned to this case. While I have worked in digital forensics for several decades and have always personally followed evolving industry best practices in this regard, I have never served as a law enforcement officer, and thus, I am not qualified to comment on Dr. Kiper's observations in this matter concerning internal FBI practices.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**TECHNICAL REVIEW**

In his [Affidavit\\_with\\_Reports\\_04-25-2022.pdf](#) report, Dr. Kiper identified in his “Summary of Technical Findings,” what he referred to as seven **Key Findings**. He concluded that these findings were the result of evidence tampering, at least some of which occurred while the media were in the custody of the FBI.

I compared the data he used in his report with the data I obtained independently from the E01 image provided to me, after performing an FTK ingestion of those files. Where I had data to compare, I agree that his description of this data matches the data I viewed.

This is difficult for me to discuss, since my own family proudly includes multiple law enforcement officers dating back approximately a century.

Below, I discuss Dr. Kiper’s findings and its relation to the data I obtained from FTK.

**GENERAL NOTES:**

- The files in question are all \*.JPG files, where “\*” represents “any text sequence” and is referred to as a “wild card character” after that term’s use in card games. Files of interest are restricted to those with names of the form “IMG\_0XXX”, where “X” may be a digit from 0 to 9.
- The mechanism of file recovery dictates that some files may bear names of the form “!IMG” rather than “IMG”, but this may be ignored.
- \*.JPG files exist with names containing the term “carved”. These are file fragments created and analyzed by FTK from the original \*.JPG files and are not material to the present analysis.
- Other file types exist, including \*.EXIF.HTML files with the same principal name as the \*.JPG files, but which contain metadata for the JPG files, in human-readable form.

**KIPER FINDING 1**

- Dr. Kiper’s first and second of five bullet points in FINDING 1 are that four photos, named IMG\_0093.JPG, IMG\_0094.JPG, IMG\_0096.JPG, and IMG\_0097.JPG were



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

listed in the FBI's WD HDD forensic report, but NOT on the CF Card report generated on 4/11/2019, despite the HDD allegedly having been a backup of the CF card. Surprisingly, those files were present in a second image of the CF card, made 6/11/2019, apparently having been added to the card in the interim.

- Dr. Kiper's third of five bullet points in FINDING 1 is that the subjects of the photos represent a different individual between the two versions of the CF card reports, based on comparisons between the thumbnails and the photos [available only on the 6/11 version]. Since these were both images of the same Evidence Item, they should not have differed in any way.
- Dr. Kiper's fourth of five bullet points discloses that the thumbnail images on the files mentioned above are actually identical to four DIFFERENT files, IMG\_0180.JPG thru IMG\_0183, respectively.
- Dr. Kiper's fifth and final bullet point points out that these discrepancies cannot be the result of any process other than intentional alteration, and that this alteration left behind a mistake in the thumbnail files, which allowed the alteration itself to be detected. I agree with him.

**KIPER FINDING 2**

- Dr. Kiper's Finding 2 contains 7 bullet points.
- His bullet points 1 thru 4 describe that a pair of FTK examinations of the same data, with the same version of FTK, would not report different file contents. I agree with this statement. I've never seen it in my own experience.
- His bullet point 5 lists six discrepancies between the files on the two CF card reports and those that should match, on the HDD, with the observation that those discrepancies could only be the result of evidence tampering. I agree with those bullet points.
- Dr. Kiper's bullet points 6 and 7 discuss the lack of consistency of the files on the 6/11/19 CF card image and the implications of that inconsistency. I examined his



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

logic in great detail and concur with his conclusions that there exists no innocent explanation I can think of for the inconsistency.

**KIPER FINDING 3**

- This Finding contains three bullet points, all addressing the fact that the Accessed Dates for all the active files were 9/19/2018, indicating the device was accessed without a Write Blocker. I agree that this is what that finding indicates.

**KIPER FINDING 4**

- This Finding contains three bullet points, all inconsistencies in the EXIF file metadata dates of the files. Dr. Kiper's observation is that these inconsistencies cannot reasonably be accounted for by any process other than human intervention, and, moreover, that the apparent purpose of the intervention was to make the file dates conform to Daylight Savings Time. However, that intervention contained a mistake that allowed it to be detected. As with his FINDING 2 above, I examined his logic in great detail and concur with his conclusions that there exists no plausible innocent explanation for these inconsistencies other than mistakes made during deliberate alteration of dates to support the government's narrative.

**KIPER FINDING 5**

- This Finding contains five bullet points, all addressing inconsistencies in the EXIF file metadata of the file IMG\_0175.JPG along with its MODIFIED DATE and the name assigned to its CARVED file counterpart. Specific mention is made of the EXIF CreatorTool metadata entry, "Photoshop Adobe Elements 3.0." Again, as with his FINDING 2 and FINDING 4 above, I examined his logic in great detail and concur with his conclusions that the data, frankly, was manipulated, and not in a casual or innocent fashion, but in such a way as to coincide with the Government narrative regarding the files in question.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**KIPER FINDING 6**

- This Finding contains seven Bullet Points, all addressing inconsistencies in the names given to folders containing the files. The apparent intention was to create folder names that appeared to be machine generated and thus lend credence to the manipulated file dates mentioned earlier.
- In Bullet Points 1 and 2, the Government's narrative was that the upper-level folders were human-generated and approximate but implied the lower-level folders were computer-generated and exact and corroborated the timestamps on the photos on the WD HDD.
- In Bullet Points 3 and 4, Dr. Kiper points out that the names could not have been created automatically, since the times are inconsistent with the way they were created in experiments he performed.
- In Bullet Point 5, Dr. Kiper points out that the timing between supposed auto-generated time stamps could not possibly be correct, since a 2-second difference between timestamps is impossibly small for this scenario.
- In Bullet Point 6, he discussed inconsistencies between the contents of **Thumbs . db** files and the actual contents of directories, indicating tampering.
- In Bullet Point 7, Dr. Kiper summarizes the lack of ability to rely on metadata to determine the creation dates of the photos in question.

I examined his logic in the above seven bullet points in great detail and concur completely with his conclusions in the case of these bullet points. Specifically, while the upper layer folder structure is credible, the anomalies relating to regarding the lower-level name structures and time stamps do not match any natural or automated behavior I have ever seen in my own experience. The anomalies noted in the Thumbs.db files are also very clear indications of data tampering [not with contents of files themselves, but with the file contents of folders]. And Dr. Kiper's bullet point regarding the reliability of



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

metadata to determine creation dates of photos is also completely consistent with my own experience.

**KIPER FINDING 7**

- This Finding also contains seven Bullet Points, all of them discussing the extreme anomalies of the dates and contents of the subject files in the presence of an intermediary computer, including improbable and contradictory file system dates and the absence of common expected files during backups. As before, with his FINDING 2, FINDING 4, FINDING 5, and FINDING 6 above, I examined his logic in great detail and concur with his conclusions that the likelihood for an innocent explanation is nil.

**CONCLUSIONS**

I believe based on what I have reviewed that Dr. Kiper is correct in his assessments that no plausible explanation exists for the anomalies in the Government's exhibits other than intentional tampering on the part of the Government.

I have served as an Expert Witness in more than 100 cases over 35 years, and I have worked in positions of great trust, supporting both civilian and also military segments of the United States Government. I have never personally witnessed tampering of digital evidence by any law enforcement agency, and I am personally disturbed by what I have learned in this case.





**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**MANAGEMENT REVIEW**

I was asked by Defendant's counsel to estimate the scope of work required to produce the data alterations initially discovered in the Government's evidence by Dr. Kiper.

I divided this analysis into two parts, described as "PROJECTS" so as to use the terminology of the Project Management community.

- In the first Project, I analyzed a possible scenario for the creation of altered data on the CF Card [1B15a].
- In the second Project, I analyzed a possible scenario for the creation of altered data on the WD HDD [1B16].

It should be noted that these two Projects actually occurred in the reverse time order of my presentation here. Dr. Kiper used this time order in order to make the most logical sense of the actual forensic results. I analyzed them in this same order so as to match the order used by Dr. Kiper in his analysis.

As with any such report, this one is based on assumptions driven by:

- Examination of artifacts;
- Analysis of schedules;
- Analysis of testimony; and
- Considerations of technologies.

The assumptions upon which this analysis and estimate are based are classified by artifact, as listed below.

**MY ANALYSIS SHOWS A TOTAL ESTIMATED POTENTIAL EFFORT OF 128 HOURS BY INDIVIDUALS WITH FOUR DIFFERENT SPECIALTIES.**

**PROJECT 1. Lexar CF ["Compact Flash"] Card 1B15a also cataloged as GX 524 [alternatively referred to in Dr. Kiper's reports as an "SD" or "Secure Digital" Card]**



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

This is an evidence item, cataloged as 1B15a or GX 524, consisting of an SD card that had been removed from a Canon camera, with abbreviated name SD Card. Below is a brief timeline of events pertinent to this analysis:

On 3/27/18, the CF card was seized, along with the camera and other devices, including the WD HDD.

From 7/10/18 to 7/27/18, Case Agent Rees had custody of the device, outside of Evidence Control. From 9/19/18 to 9/26/18, Case Agent Lever had custody of the device, during which time the CF card was altered (see Technical Finding #3 in Dr. Kiper's Technical Report). Thus, during 24 calendar days when the CF card was checked out of Evidence Control, and in the custody of Case Agents, it was modified. This was several months before the SD card was checked into CART, on 2/22/19, and imaged and analyzed by FE Flatley. (see Dr. Kiper's Process Findings.)

From 2/22/19 to 6/7/19, Flatley held the CF card. For the subsequent three days up until Booth received and then re-cloned the SD card, which arrived to him in an unsealed cellophane bag (see Dr. Kiper's Process Findings), three FBI personnel had custody of the CF card: SA McGinnis, SA Mills, and FE Booth. Based on the technical findings, it is likely that additional alterations took place by this time.

**Question Posed to Me:** I was asked to examine the hypothetical work needed to convincingly yield the artifacts described above. I identified only a single subtask.

**Assumptions:**

I made working assumptions that anyone doing this work was trained on standard computer subjects and on evidence handling, and that they had an expectation of "medium level" scrutiny for the evidence, a level below that of a highly skilled forensic investigator.

I also made a working assumption that anyone doing this work would attempt to minimize the amount of data alteration performed, since each alteration added risk of detection during an intensive search.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

Based on the evidence, I further assumed that the Government had deleted the errors made in the fabrication of the WD HDD, which occurred chronologically earlier, and thereby a decision was made to manipulate data on the CF card so as to make the data on the WD HDD appear more credible. Given that the purpose was to essentially “clean up” what could be cleaned up on the HDD, and that the schedule available for it was very limited, this work was likely undertaken under time pressure. I attribute the errors made during the alteration that allowed Dr. Kiper to discover the alteration to time pressure and lack of access to the HD.

**Discussion**

This process subsumes KEY FINDINGS 1, 2, and 3 by Dr. Kiper. His findings 4, 5, 6, and 7 are the subject of the second analysis in this report, below.

**PROJECT 1 ESTIMATED TOTAL HOURS:**

**32 HOURS by a SENIOR FORENSIC INVESTIGATOR**

---

**PROJECT 2. WD HDD 1B16 also cataloged as GX503 [ORIGINAL]**

At the outset there existed an evidence item, cataloged as 1B16 and also as GX 503, consisting of a Western Digital hard drive, with abbreviated name WD HDD.

**Question Posed to Me:** I was asked to examine the hypothetical work needed to convincingly add CP files to a version of WDD HDD 1B16 / GX 503 during the 134 days between the date it was taken into custody until it was transferred to FET VD.

**Assumptions:**

I made the same working assumptions for this Project as for the one above, including time pressure as a significant constraint.

As a consequence of these working assumptions, I analyzed a scenario in which:



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

- A. The drive was first analyzed, as a precaution, to determine the presence of deleted files, hidden files, file fragments, or other items whose content should be known prior to alteration of evidence. This could be done with either FTK, the tool used by the FBI itself, the freeware tool AUTOPSY, or other forensic tool such as ENCASE.
- B. CP files were acquired, or non-CP files were altered to make them CP [for example, by altering dates.]
- C. The files mentioned above were added to the WD HDD 1B16 drive

**TASK 1: ANALYZE THE DRIVE PRIOR TO ALTERATION OF EVIDENCE**

This would consist of a study of the existing drive for feasibility and content.

**ESTIMATED EFFORT:**

- 16 Hours by a **STAKEHOLDER**
- 16 Hours by a **TECHNICAL SUPERVISOR**

**TASK 2: ACQUIRE AND PREPARE THE CP FILE CANDIDATES**

Selection of CP file candidates would include choosing ones of the appropriate size, other metadata, and conformity with adjoining files.

**ESTIMATED EFFORT:**

- 24 HOURS by a **DATA ENGINEER.**

**TASK 3: PERFORM THE ACTUAL CREATION OF THE ALTERED DRIVE**

This task consists of actual alteration of their EXIF metadata as needed, deletion of the files they would replace, copying them into the working drive, and then imaging the resulting drive back to the original unit. File date alteration apparently included files outside the 22-file range of the added files, for the appearance of continuity.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**ESTIMATED EFFORT:**

- **40 HOURS BY A DATA ENGINEER**

**PROJECT 2 ESTIMATED TOTAL HOURS:**

**96 HOURS BY 3 DIFFERENT PARTIES**

---

**Discussion**

This process subsumes KEY FINDINGS 4, 5, 6, and 7 by Dr. Kiper. His findings 1, 2, and 3 were the subject of the first analysis in this report, above.

- A. In KEY FINDING 4, Dr. Kiper reported irregularities of file dates that could not have been the result of any innocent process
- B. In KEY FINDING 5, Dr. Kiper reported that irregularities in the EXIF headers of several files exist that could not be the result of any innocent process.
- C. In KEY FINDING 6, Dr. Kiper reported that the names of folders were apparently arbitrary, belying their state origins as computer-generated.
- D. In KEY FINDING 7, Dr. Kiper reported that the alleged CP were possibly planted and had dates altered to give the appearance they had been sourced from a 2009 backup.

The inclusion of detectable data manipulation errors that were detected by Dr. Kiper and confirmed by myself and by Mr. Abrams raises an obvious question of how such errors were not detected by the person or persons doing the data manipulation prior to their introduction into the FBI's system. Possibilities include lack of quality control, incorrect assumptions that the evidence would never be inspected as thoroughly as it has been by Dr. Kiper, myself, and Mr. Abrams, inadequate calendar time to complete the work efficiently, lack of skill by the full team, or some combination of those items. It seems likely that all four may have played a role.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**NOTES ON ESTIMATION**

As is well known in Project Management, creating overall estimates for project cost and schedule is extremely challenging:

- Once a task has been identified, that task may be estimated by comparing it with similar tasks from a Body of Knowledge of prior tasks, a process known as Parametric Estimation. Often, of course, the challenge is identifying the specific task.
- Further challenges arise because a task that is new to the individual performing it may take longer than it would for someone who's done it before.
- Still further challenges arise from task-to-task dependencies, the need to stop and start during task completion, and the likelihood that tasks may arise that were not foreseen at the start of the effort.
- The estimates I provided represent my best judgment based on my experience and the information provided to me, subject to the factors described above.

**COMMENTARY**

It causes me great disappointment to be aware of this situation, as I have the highest regard for law enforcement. I am well aware of the potential significance and ramifications of the analysis I present here, and for obvious reasons, do not make any such statements without significant study. Regrettably, based on the information available to me, and upon significant review, I cannot envision a plausible explanation for the discrepancies noted by Dr. Kiper and reviewed by myself and Mr. Abrams, aside from intentional alteration. This is not a conclusion I am pleased to make.

**RESERVATION OF RIGHTS**

I reserve the right to amend or augment my opinions and discussions in the above report based on any new information that may come to light, including but not limited to information brought by participants in this case, subsequent research of my own, or information from other reliable and legally proper sources. I further reserve the right to modify the scope of this or other communications I may have in conjunction with this matter, based on information then available.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**DISCLAIMER**

I am not familiar with the non-technical details of this case, other than having been minimally aware that a case of this nature was in process at the time it was taking place. I have no knowledge of or relationship to any of the participants.

I have provided my credentials in other documents in this case, and I incorporate them into this document by reference.

I am not an attorney, and thus, I have not, and will not, offer opinions of law.

I declare under penalty of perjury, under the laws of California, that the foregoing is true and correct.

Dated: April 27, 2022, at Santa Barbara, California.

---

**WAYNE B. NORRIS**

# **EXHIBIT F1**

**(CV Of Wayne B. Norris)**



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**

**Because Accuracy Matters**



2534 Murrell Road, Santa Barbara, CA 93109-1859

VOICE PHONE: +1-805-962-7703 FAX +1-805-456-2169

EMAIL [Wayne@Norris-Associates.com](mailto:Wayne@Norris-Associates.com) URL <https://Norris-Associates.com>

LinkedIn <https://www.linkedin.com/in/wayne-norris-193b88>

**16 April 2022**

**USA VS RANIERE**

**WAYNE B. NORRIS CURRICULUM VITAE**



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**QUALIFICATIONS Per FRCP 26(a)(2)(B)**

I have fifty-three years of professional experience in management, business, finance, accounting, engineering, software development, and scientific research.

1. I hold a Bachelor of Arts degree in Physics from the University of California, Santa Barbara, and have taken graduate courses in advanced physics and CPA accounting.
2. I formerly served as the Vice President of an international software development firm for 5½ years, as the President and Chief Financial Officer of an international software development firm with 130 employees and 3 offices on 2 continents I took public, for 2 years, as the Interim President and Chief Financial Officer of an Internet domain name registrar for 6 months, as the Chief Scientist of a military research and development company for 5½ years, and as the CEO of an expert witness company during the first half of 2017.
3. I have been awarded 6 patents in detection of conventional and nuclear explosives using neutron and gamma ray sensing, one patent in smart small caliber ammunition design, and have 6 provisional patents in securities options trading technology and one provisional patent in mobile device geolocation technology.
4. Currently I am an independent management and technology consultant and an expert witness in fields in which I am qualified to serve.
5. I have served as an expert witness in technology matters, including the valuation of technology, in more than 100 cases before federal, state, and local courts.
6. I served as the President and Chief Financial Officer of a publicly traded software firm with 130 employees and 3 offices on 2 continents.
7. I began costing, valuing, and managing software projects in 1986, and in the subsequent years, have performed technical and financial management of more than 100 software development projects and programs for civilian, government, and military customers.
8. I have been writing software for 62 years, with some breaks.
  - 8.1. I wrote my first computer program in April of 1959, just one month after my 12<sup>th</sup> birthday, on a Librascope LGP-30 computer at Cerritos Junior College in California, courtesy of my friend's older brother who was a student there. The computer had no RAM and no disk, only a magnetic drum. I wrote a numerical solution for the equation of motion of a yo-yo.
  - 8.2. I began writing software professionally in 1969 while working as a physicist at Rockwell Science Center in Thousand Oaks, CA, in support of an analysis of moon rocks returned by Apollos 11 and 12 and of microwave analysis of earth's



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

ocean temperatures and the atmospheric composition of Jupiter and Saturn. I wrote software in FORTRAN and assembly language on the CDC 6600 and RECOMP III computers.

- 8.3. Over the years, I wrote software on approximately 35 different operating systems and hardware platforms in numerous languages, many now legacy, including FORTRAN, ALGOL, COBOL, PL/1, APL, Pascal, LISP, PLM, c, c++, Visual Basic, Access, SQL, JavaScript, HTML / CSS, Java, Macromind Lingo, and assembly languages for the CDC 6600 / 6400 CPU and PPU units, CDC RECOMP III, AN/UYSK-6, IBM 7044, IBM 7094, IBM 360, SDS 910/920/930 series, the SIGMA series, the Burroughs B-3500, the VAX 11/70 series under VMS, the PDP-11 series under RSX-11m, the Intel 8080, 8088, and 8086 chipsets, the Motorola 6502 chipset, Xerox printer chipsets, and early versions of the Intel BIOS. In addition to machine-specific operating systems, I've worked under Linux, SCO Unix, most versions of Windows, and earlier "numbered" Macintosh operating systems.
- 8.4. I have written approximately 150,000 lines of code personally, on media including 8-bit ASCII punched paper tape, 7-bit Baudot partially punched paper tape, plugboards, IBM cards, 1/2" magnetic reels, multiple formats of floppy disks, modern hard drives, PROM chips, and optical media. I have written software in the areas of accounting, nuclear weapons simulations, stress analysis, bookkeeping, finance, video games, animations, 3D modeling, accounting, device drivers, robotic applications, vibration engineering, computerized test vector generation, oil spill simulation, compilers, parsers, inertial navigation systems, armored vehicle simulations, air quality simulations, Monte Carlo codes, electromagnetic scattering, finite element codes, cryptographic codes, and intelligence community applications.
- 8.5. I began managing software projects in 1986, and in the subsequent years, have managed more than 100 software development projects and programs for civilian, government, and military customers. I hold the designations of Microsoft Certified Professional [MCP], Project Management Professional [PMP], and Certified Scrum Master [CSM].
9. I have held the office of CEO, President, Vice President, Chief Financial Officer, Chief Scientist, and Board Member for multiple firms.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

16 April 2022

**Career Highlights**

- Expert Witness in more than 100 cases in the areas of digital forensics, software code review for compliance with best practices, GPS, software copyright infringement and valuation, technology and technology business valuation, aircraft crash investigation, and related cases.
  - Lead software development expert witness for the Internal Revenue Service in the \$1.7 billion *Microsoft et al v Commissioner of Internal Revenue*.
- Manager of more than 100 projects and programs since 1978, with budgets to \$7.5 million and headcounts to 38. PMP and CSM certified. Projects included software development, cybersecurity, manufacturing, research and development, environmental planning, and civil aviation. Environments included commercial, military, aerospace, and national security communities. Instructor in Project Management for the US Navy. Santa Barbara Chapter President, Project Management Institute.
- Project Manager, US Navy, Port Hueneme, Cybersecurity, DEVOPS, and Support.
- CEO, Precision Simulations, Incorporated [Grass Valley, CA] – Expert witness firm specializing in video and audio evidence analysis and forensic animation.
- Independent consultant:
  - 3d Flash LiDAR / super resolution in mining and aerial surveys
  - Secure military CANBUS encryption and hardening
  - Mobile device geolocation technology; Co-Inventor of a Provisional Patent
  - Sublethal handgun ammunition; Sole Inventor of a Pending Patent
  - Development of short-term securities options trading instrument. Sole Inventor of 6 FINTECH Provisional Patents
- Chief Financial Officer of an Internet Domain Name Registrar firm
- Chief Scientist / Co-Founder, SEDS, LLC [Redwood City, CA / Troy, MI / Santa Barbara, CA / Washington, DC / Oak Ridge, TN], a neutron physics counterterrorism research laboratory focusing on remote detection of improvised conventional and nuclear explosive devices and medical applications of thermal neutron technologies.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

Principal inventor of 6 Granted Patents. Chief engineer for millimeter microwave weapons detection systems installation at Cheyenne Mountain Complex.

- President and Chief Financial Officer, Offshore Creations, Inc. [Colorado Springs, CO / Santa Barbara, CA / Kiev, Ukraine / Simferopol, Crimea] – 160-person International software development firm. Took the company public before the SEC.
- Research and Development Manager, Biopac Systems, Inc. [Goleta, CA] Manufacturers of biomedical equipment
- Product Manager, 3DStockCharts.com, Inc. [Santa Barbara, CA] – a real-time stock data reporting and software development firm
- Vice President, Emulation Systems, Inc. [Santa Maria, CA] – makers of FAA approved simulators for light aircraft, helicopters and the F-18 Hornet.
- Director of Government Services, ExperTelligence, Inc. [Goleta, CA] – an Artificial Intelligence software firm supplying the US intelligence community,
- Chief Scientist, Morton Associates [Santa Barbara, CA] – An environment firm that created federally mandated Oil Spill Contingency and Emergency Plans [OSCEPs] and personnel training curricula for offshore and onshore oil drilling platforms, pipelines, production facilities, and storage facilities. Developer of air pollution management software for Unocal.
- Contract software developer, Anacapa Associates [Santa Barbara, CA] – Developer of a Human Terrain Modeling system used for tracking domestic terrorist groups and organized crime groups.
- Physicist, Member of Technical Staff, General Research Corporation [Santa Barbara, CA / Washington, DC] – Researcher and software developer in electromagnetic scattering, nuclear weapons effects, computerized polygraphy, military operations, and other classified topics. Project Manager for robotic software development.
- Contract Software Developer, multiple firms including Control Data Corporation, Raytheon Electromagnetic Systems, Edwards AFB, McDonnell Douglas, Vandenberg AFB, and GM Delco Electronics. Subjects included the AN/SLQ-32 shipboard fire control system, missile test autodestruct systems, AGM-86 / AGM-109 cruise missile test flyoffs, M1-Abams tank simulations.
- President and Chief Pilot, Norris Airways [Santa Barbara, CA] – A charter airline under FAR Part 135, fixed base operator flight school under FAR Part 61, and Cessna



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

dealership. 1,000 hours of flight instruction given. Personally graduated 35 pilots from Private Pilot to Airline Transport. Personally hold FAA Airline Transport Pilot [ATP], Senior Parachute Rigger, and Advanced / Instrument Ground Instructor certificates; formerly Certificated Flight Instructor, Airplane Single and Multi-Engine, Instruments [CFII/ASMEL].

- President and Founder, Gasohol, Inc., the first retail and wholesale automotive alcohol fuel firm west of the Mississippi River in modern times, with retail sales and bulk sales to the US Navy.
- Staff Associate Physicist, Rockwell Science Center [Thousand Oaks, CA] – Researcher / software developer for studies of moon rocks from Apollos 11 and 12 using Mössbauer Spectroscopy. Researcher in planetary atmospheres and liquid water analysis of terrestrial clouds.
- Laboratory Technician, Rockwell Space Center [Downey, CA] – Worked building the Apollo Command Module
- Laboratory Technician, Advanced Kinetics Corporation [Seal Beach, CA] – Laboratory simulation the earth's solar winds and the Van Allen Radiation Belts soon after they were discovered.
- Student software developer [La Mirada, CA] – Wrote simulation software for rotational dynamics on a Librascope LGP-30 in April 1959.
- Have written approximately 100,000 lines of software in approximately 38 computer languages.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**APPENDIX A – WAYNE B. NORRIS CURRICULUM VITAE**

Wayne B. Norris has acted as an expert witness in more than 100 cases in federal, state, and local venues over the last several decades, including:

- Software Copyright infringement, Abstraction / Filtration / Comparison [code analysis and damages / appraisal computations]
- Computer Security and Forensics / Industry Best Practices, Defects / Failure Analysis
- Software Contract Performance, Paternity and Valuation
- Software Outsourcing, with emphasis on Russia and Ukraine
- Engineering Best Practices
- Management Best Practices
- Software Taxation Issues
- Software Industry Appropriate Compensation
- Patents, Patent validity, Patent Infringement
- Copyright issues
- Trade Secrets
- General Engineering and Physics
- General aviation aircraft operations and skydiving operations
- Fiduciary duties of corporate officers
- Hazardous materials, oil spills, and industrial safety, including radiological safety
- Aviation safety, best practices, and pilot error

Mr. Norris personally holds 6 granted patents in nuclear instrumentation. He has 6 pending patents in online securities trading, 1 filed patent in cell phone geolocation, 1 pending patent covering novel ballistic projectiles, and has authored a 14th patent in real estate escrow processes.

He has been the CEO of an expert witness firm, the Vice President of a Russian-American software company and the President and Chief Financial Officer of a Ukrainian-American software company he took public on US markets.

He has testified on approximately 27 occasions, spanning both court testimony and depositions, and has authored approximately 80 expert reports.

Mr. Norris specializes in explaining extremely complex concepts to general audiences in accessible and understandable ways. He has 49 years of professional service and 59 years writing and managing the development of computer software, beginning in 1959.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**List of Testimonies, 2013 - 2022, per FRE 26**

- Pilton v Novell, Los Angeles County Civil Court, Case in Progress – For Plaintiff's Counsel – Email analysis
- People v Daniel Garcia, et al, Riverside County, California, Case in Progress – For Defendant's Counsel – Corruption of computer data
- Blogspiration v Mobile Computing, LLC, Los Angeles County Civil Court – For Plaintiff's Counsel – Software development contract performance
- Muzeit v Bytedance, US Trademark Court – For Defendant's Counsel – Technology analysis of Trademark claims
- Christian Cardoso v ASAP Drain Guys and Plumbing, San Diego, California County Superior Court – For Plaintiff's Counsel – Validation of video surveillance data
- People of the State of California vs Nikolov, Los Angeles County Superior Court – For Defendant's Counsel – Valuation of stolen credit card numbers obtained by hacking
- Live Face on Web vs Integrity -- US Federal District Court, Denver, Colorado -- For Defendant's Counsel – Valuation of allegedly misappropriated copyrighted software code
- Doe vs Corona Norco Unified School District, Riverside County, CA Superior Court – For Plaintiff's Counsel – Adequacy of school district software security
- Live Face on Web vs Moreno -- US District Court, Western District of Texas, San Antonio Division -- For Defendant's Counsel – Valuation of allegedly misappropriated copyrighted software code
- Felix v Ramirez -- Superior Court of Los Angeles County, CA -- for Defendant's counsel -- defendant prevailed on all counts, won counter-suit – Valuation of Internet URLs
- Paccione vs Albert -- Los Angeles County Superior Court – for Defendant's Counsel -- Analysis of text message records in a criminal contempt of court hearing as part of a divorce proceeding
- People of the State of California vs Keith Johnson -- Shasta County, CA Superior Court – for Defendant's Counsel – Analysis of potentially available forensic records from multiple sensors in a child molestation case
- Marriage of Jensen – Los Angeles County Superior Court – Analysis of email records for evidence of tempering.





**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

- Naroditskiy vs Eon Reality – Orange County Superior Court – for Defendant’s Counsel – Valuation of Russian-American software representation contracts
- People of the State of California vs Creech – Los Angeles County Superior Court – For Defendant’s Counsel – Analysis of prosecution’s use of animations in a high profile death penalty case



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**MOST RECENT CASES INCLUDE:**

- Analysis of tampered digital evidence in a high profile murder case, involving legacy mobile devices and storage appliances.
- Appraisals, valuations, and damages in very difficult cases that no other experts will touch, based on multiple valuation approaches and consolidation of results, including stolen credit card numbers offered for sale on the Dark Web
- “Should-Cost” valuations of software in piracy cases and engineering contract performance
- Unjust enrichment in trade secret theft cases
- Forensic analysis of JavaScript code in a copyright infringement / copyright validation case, including Abstraction / Filtration / Comparison [AFC] tests
- Forensic analysis of metadata in a case of alleged international fraud
- Forensic analysis of email trails in a case of alleged forgery
- Forensic analysis of text message records in a criminal case
- Investigation of damage mechanisms to a computer system
- Forensic analysis of alleged Dark Web disclosures of Personally Identifiable Information [PII]
- Forensic analysis of alleged online slander
- Forensic analysis of cell phone photos in an alleged child pornography case
- Procedure analysis of sheriff’s investigators in an alleged case of lewd photography of under aged minors
- Appropriate compensation in the software industry
- Valuation of software in a copyright infringement case
- Appropriate commission structure in a US-Russian software business
- Physics analysis in patent infringement cases

**PROFESSIONAL SUMMARY:**

Chief Executive Officer of Precision Simulations Inc., the leading provider of forensic / scientific documentation, analysis, and visualization services, including 3D laser scanning, animation, forensic video, photogrammetry, and testifying expert witness services for legal proceedings.

President and Chief Financial Officer of Offshore Creations, Inc. [OFSC.PK], a 130-person publicly traded international software company.

Chief Scientist of SEDS, LLC, a government contracting R&D firm working in counterterrorism; holder of 6 patents in nuclear technology, gamma ray sensing, and conventional and nuclear explosives detection using thermal neutron beams and pixilated gamma ray spectrometers. Specialist in millimeter microwave based weapons detection systems, profiling, ballistics, Munroe Effect penetrators, and explosives effects. Installed first millimeter microwave detection system at Cheyenne Mountain Complex. Analysis of Human Terrain Modeling with focus on bomb making.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**PROFESSIONAL SUMMARY (continued):**

Principal, Norris Associates, Environmental Consultants, an environmental and engineering consulting firm. Projects included residential developments, the MX missile rail garrison plan, a proposed nuclear plant in Omaha, a sewage system in Los Angeles, oil drilling offshore Orange County, CA, and fuzzy set simulation of governmental decision making.

Consulting Physicist and Computer Systems Analyst, Jet Propulsion Laboratories, Vandenberg AFB, Edwards AFB, Kirtland AFB, GM Delco Division, McDonnell Douglas, Raytheon, Hughes Aircraft, AlliedSignal Corporation, ExperTelligence Corporation: Technology development for aerospace, domestic police, organized crime gang and terrorism human terrain modeling, national defense, intelligence community, and commercial projects.

Chief Scientist, Morton Associates, Santa Barbara, CA, corporate author of federally mandated Oil Spill Contingency and Emergency Plans [OSCEPs] for the Chevron platforms in the Santa Barbara Channel, the KLMR pipeline from Bakersfield to Los Medanos, the Estero Bay Marine Terminal, Estero Spur, Gosford Production Facility, Chevron Cavern Point Unit, and Phillips Marine Terminal. Lead author of the Commercial Fisheries Handbook for Proposed Exploratory Drilling Operations, Cavern Point Unit. Software developer, fugitive emissions reporting system, Unocal refineries. Financial analyst and appraiser, Unocal Huntington Beach onshore oil drilling, pipeline, and production facilities.

Founder, CEO, and Chief Pilot Norris Airways, Santa Barbara, CA Municipal Airport, an aircraft fixed base operation ("FBO"), FAR 135 Air Taxi, and Cessna dealership with 14 employees, including 9 pilots, 3 departments, and 11 aircraft.

Co-Founder and CEO, Gasohol, Incorporated, Santa Barbara, CA, the first modern wholesale/retail gasohol company west of the Mississippi River. Wholesale customers included the U.S. Navy.

Physicist, General Research Corporation, investigator in electromagnetic scattering, neutron transport, nuclear weapons effects, counterterrorism, computer assisted polygraphy / electrophysiology and facial gesture recognition, and the Strategic Defense Initiative.

Physicist, Rockwell Science Center, investigator on lunar samples from Apollos 11 and 12, planetary atmospheres, cosmic background temperature, and terrestrial atmospheric liquid water content for environmental analysis and environmental impact statements and reports.

Financial Analyst / Business Plan Author, Consultant – Holder of 6 Provisional Patents in financial options trading.

Patent advisor, Consultant



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

Advisor to Multiple Initial Coin Offerings [ICOs]

Expert witness for issues in Technology, Intellectual Property, Valuation, and Conduct of Corporate Officers in Federal and State courts.

**EDUCATION AND CERTIFICATIONS:**

- University of California, Santa Barbara: B.A. Physics
- University of California, Santa Barbara: Post-graduate work in Advanced Mathematics and Physics, Human Factors, and Ergonomics, and CPA accounting
- Microsoft Certified Professional + Internet [MCP+I] designation
- Project Management Professional [PMP] designation
- Certified SCRUM Master [CSM] [Agile project management] designation
- University of Texas, Austin: Professional Certificate, Oil Field HAZOPS and Risk Management
- Security Management Certificate, Defense Industrial Security Clearance Office. Honolulu, HI
- Classified Warheads and Ballistics Seminars, US Naval Postgraduate School, Monterey, CA
- Former California State General Building Contractor, B-1 licensee
- FAA Airline Transport Pilot, Senior Parachute Rigger, Former CFII/ASMEI, Ground Instructor

**AFFILIATIONS:**

- Institute of Electrical and Electronics Engineers [IEEE] – Life Member
- International Right of Way Association [IRWA]
- Association of Old Crows [AOC] [Electronic and cyber warfare professional organization]
- Project Management Institute [PMI] – Santa Barbara Chapter Director
- SCRUM Alliance [Agile project management]
- Santa Barbara Science and Engineering Counsel
- Association of the United States Army [AUSA] Life Member
- American Association for the Advancement of Science [AAAS]



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**SELECTED COMMUNITY EXPERIENCE:**

- President, Board Chair, Mothers Against Drunk Driving Santa Barbara: Created a pioneer vehicle donation program and created 34 radio and TV commercials and bilingual sober driving literature.
- Santa Barbara County Deputy Sheriff for Search & Rescue
- Member, Santa Barbara County Grand Jury, Sheriff's/Seniors Committees

**PUBLICATIONS:**

*"Time-Resolved Emission Spectroscopy in Acetylene/Oxygen Explosions"*, Combustion and Flame Journal, February 1970 (with R.J. Oldman and H.P. Broida)

*"The Brightness Temperature of the Terrestrial Sky at 2.69 GHz"*, Journal of the Atmospheric Sciences, 29:1210 (with W.W. Ho, G.M. Hidy, M.J. Van Melle, W. Hall, H. Wang)

*Chevron Fisheries Handbook for the Cavern Point Unit* (with Prof. Milton, Love, Ph.D.)

**PATENTS:**

Mr. Norris currently hold 7 granted patents and 7 provisional patents, and has acted as an expert in numerous patent cases, including against Microsoft, Logitech, Pelican Research, and Analog Devices, Inc.

US 7,573,044 B2 *Remote Detection Of Explosive Substances* GRANTED 8/11/09 - Priority 7/18/06

US 8,080,808 *Remote Detection Of Explosive Substances* (CIP 7,573,044) GRANTED 12/20/2011

US 8,288,734 *Remote Detection Of Explosive Substances* CIP GRANTED 10/16/2012

US 8,357,910 *Background Signal Reduction In Neutron Fluorescence Applications Using Agile Neutron Beam Flux* GRANTED 1/22/2013

US 8,410,451 *Neutron Fluorescence with Synchronized Gamma Detector* GRANTED 4/2/2013

US 8,785,864 *Low-Cost, Organic-Scintillator Compton Gamma Ray Telescope* GRANTED 6/22/2014 [with K.N. Ricci, B. Paden]

US 11,226,185 *Multipurpose Projectile Having Preformed Pieces and a Variable Impact Deployment System* GRANTED 1/18/2022

US 62305645 *Method and System for Trading Low Priced Short Term Securities Option Contracts That Exhibit Specified Behaviors*, PENDING 3/9/2016

US 62307986 *Securities Trading Exchanges To Support the Sale and Exercise of Low Priced Short Term Securities Option Contracts That Exhibit Specified Behaviors*, PENDING 3/14/2016



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

US 62307999 *Method and Process To Support the Sale and Exercise of a Series of Low Price Securities Option Contracts To Achieve Specified Premium Price Values*, PENDING 3/14/2016

US 62378833 *Method and Process To Support the Interactive Sharing of Securities Trading Activities*, PENDING 8/24/2016

US 62378846 *Method and Process To Support the Positioning of Advertisements in a Securities Trading Platform*, PENDING 8/24/2016

US 62378858 *Method and Process for Combining Trades of Securities into a Lottery-Like Environment*, PENDING 8/24/2016

US 62/353,466 *US Method for Verifying Player Location in Online Lottery System*, PENDING 9/22/2016.

**EXPERT WITNESS EXPERIENCE DETAILED DISCUSSION:**

Mr. Norris has testified on approximately 27 occasions, spanning both court testimony and depositions, and has authored approximately 80 expert reports.

Mr. Norris specializes in explaining extremely complex concepts to general audiences in accessible and understandable ways. He has 49 years of professional service and 60 years writing and managing the development of computer software, beginning in 1959.

Mr. Norris was the US Government's expert witness for software development issues in the multi-year case of Microsoft Corporation versus Commissioner of Internal Revenue [US Tax Court Docket Number 16878-96], the largest tax case ever litigated by any jurisdiction in history. He authored four expert witness reports that were admitted into the record, and testified for approximately 7 hours, including *voire dire*, direct, cross, redirect, and recross.

Mr. Norris was the principal architect of the Government's technical approach toward interpretation of IRC 927(c) in the case of software. The Government won the case at trial, and his arguments were incorporated into the Court's opinion. He advised IRS attorneys on strategies for the examination of Microsoft expert witnesses.

Mr. Norris specializes in explaining very complex issues to the Court and Jury in accessible language.

He has recently developed a knowledge area with the trademarked name the Internet of Evidence™, [<http://InternetOfEvidence.com/>] a term he uses to refer to the vast and ever growing array of sensors and data recorders that can be used by the legal community to determine time lines, identities and intentions of actors, accuracy of alibis, external and environmental conditions, and who knew what and when they knew it. He delivered a Webinar for CLE credit on this topic on April 24 of 2014 under the auspices of Technical Advisory Services for Attorneys [TASA]. The webinar was attended by 132 attorneys nationwide.



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

The following year, 2015, Mr. Norris presented a similar webinar for CLE credits titled *The Internet of Things Thieves - What Data Security Lawsuits In the Very Near Future Will Look Like!*

Mr. Norris has worked as an expert witness in several modes, including depositions, testimony in court, and preparation of expert witness reports and strategy documents.

Due to confidentiality rules and stipulations, many are not able to be shared. Sharable information is shown below.

## **EXPERT WITNESS CASES**

SOME CASES ARE LISTED UNDER MULTIPLE HEADINGS FOR EASE OF ACCESS:

### **Animations and Simulations**

- People of the State of California vs Creech, Los Angeles County Superior Court - Analysis of prosecution's use of animations

### **Appraisals and Valuations**

- People of the State of California vs Nikolov, Los Angeles County Superior Court
- Live Face on Web vs Integrity -- US District Court, Denver, Colorado -- For Defendant's Counsel
- Live Face On Web vs Moreno et al, ongoing - for Defendant's Counsel
- Live Face on Web vs Integrity Systems, ongoing, for Defendant's Counsel
- Live Face on Web vs Puerto del Sol Condominiums, for Defendant's Counsel
- Naroditskiy vs Eon Reality, ongoing - for Defendant's Counsel
- People of the State of California vs Georgi Nikolov, for Defendant's Counsel
- Mitchell and Manhattan Software vs Jean Kasem, Little Miss Liberty, et al, - Superior Court of Los Angeles County, CA -- case settled - for Plaintiff's Counsel
- Felix v Ramirez -- Superior Court of Los Angeles County, CA -- defendant prevailed on all counts, won counter-suit - for Defendant's Counsel
- Clark-Martin vs Yahoo US District Court -- negotiated settlement - for Defendant's Counsel
- Microsoft vs Richter, OptInRealBig, et al -- US District Court, Seattle, damages -- defendant plead guilty to reduced charges - for Defendant's Counsel
- Young vs GFOS, Inc., San Diego Superior Court, case settled - for Plaintiff's Counsel
- Feltman v Otalvaro, et al - for Plaintiff's counsel -- case settled -- US Bankruptcy Court, Southern Florida
- Multiple others, cases sealed



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

### **Forensic Analyses of Electronic Media**

- People vs Garcia, Riverside County, California, for *in pro per* homicide defendant
- People vs Frazier, Los Angeles County Court, for Defense Counsel
- Live Face On Web vs Five Boro Mold et al - Superior Court of the State of New York - Case settled - for Plaintiff's Counsel
- Microsoft Corporation vs Commissioner of Internal Revenue - Victory by Defendant [IRS], US Tax Court, Seattle, WA and Washington, DC. [Court testimony; 7 hours; direct, cross, redirect, recross] - for Defendant's Counsel
- Weininger vs Weininger – online slander and reputation management - case settled
- Multiple cases in progress involving metadata, email authentication, spoofing, and damage to electronic media
- Riffle vs Hyde & Hyde, Northern California – case settled - for Plaintiff's Counsel
- People of the State of Wyoming vs Robinson – POS system tampering - guilty verdict - for Defendant's Counsel
- People of the State of California vs Threlkeld – Riverside County Superior Court forensic recovery from cell phones and hard drives – Defendant convicted and sentenced
- People of the State of California vs Keith Johnson – analysis of potentially available forensic records from multiple sensors in a child molestation case – Not Guilty Verdict – Shasta County, CA Superior Court [Court testimony; 2 hours; direct, cross, redirect] - for Defendant's Counsel
- Paccione vs Albert – Analysis of text message records in a criminal contempt of court hearing as part of a divorce proceeding – charges dropped – Los Angeles county Superior Court [Court testimony; 1 hour; direct, cross, redirect] - for Defendant's Counsel
- Offshore Supply Systems, LLC vs CS Industries, Inc. - Superior Court of Orange County, CA - case settled - for Defendant's Counsel
- Marriage of Jensen – Los Angeles County Superior Court - analysis of email records for evidence of tampering.

### **Software Intellectual Property**

- Microsoft Corporation vs Commissioner of Internal Revenue - Victory by Defendant [IRS], US Tax Court, Seattle, WA and Washington, DC. [Court testimony; 7 hours; direct, cross, redirect, recross] - for Defendant's Counsel

### **Patentability of Software**

- In re Mitchell, Los Angeles US District Court – advisory to Court





**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**Technology Infringement**

- Dolby Digital v General Satellite Research & Development, Ltd., San Francisco Federal District Court, for Defendant's Counsel
- Interlam vs Modular Arts, US District Court, Western District, Washington State, Seattle, WA, case settled [Deposition] - for Plaintiff's Counsel
- Young vs GFOS, Inc., San Diego Superior Court, settled - Plaintiff's Counsel

**Patent Infringement Cases**

- Jordan Spencer Jacobs v. Microsoft Corporation, Logitech, Inc., Pelican Accessories, and Analog Devices, Inc. - case settled, US District Court, Central Florida [Deposition] - for Plaintiff's Counsel
- Sequent Technologies vs Insight Video Net - US District Court, Los Angeles, CA - case settled - for Plaintiff's Counsel
- VOS Systems, Inc. vs Voice Signal Technology, Inc. – US District Court, San Diego, CA – case settled - for Plaintiff's Counsel
- Microsoft vs Comptek Plus, US District Court, Los Angeles, CA – case settled – for Defendant's Counsel
- Other cases settled under seal

**Software and Hardware Quality and Performance Cases**

- Allen & Schack vs Worldwide Environmental Products - settled, Superior Court of Ventura County, CA [Deposition] - for Plaintiff's Counsel

**Software Copyright Infringement Cases**

- Mitchell and Manhattan Software vs Jean Kasem, Little Miss Liberty, et al, – Superior Court of Los Angeles County, CA – case settled prior to trial - for Plaintiff's Counsel
- Other cases settled under seal, US District Court, Honolulu, Hawaii
- Live Face on Web, Inc. vs Moreno et al, ongoing, for Defendant's Counsel

**Software Piracy**

- People vs Joan Huang, US District Court, Los Angeles, CA – defendant plead guilty to a reduced charge - for Defendant's Counsel

**Software System Operational Integrity**

- People vs Mraz, Superior Court of Sheridan, WY – defendant convicted - for Defendant's Counsel

**Software Licensing**

- qad vs Ingersoll Rand – Los Angeles US District Court – case settled - for Plaintiff's Counsel



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**Misappropriation of Trade Secrets**

- Entertainment Printing Enterprises, Inc. vs CreativeMob, TicktBox, et al – Superior Court of Los Angeles County, CA – case settled prior to trial - for Plaintiff's Counsel
- Mitchell and Manhattan Software vs Jean Kasem, Little Miss Liberty, et al, – Superior Court of Los Angeles County, CA – case settled prior to trial - for Plaintiff's Counsel
- Lynch Communications, Inc. v Irish Communications, Inc, David O'Keefe, et al. – Superior Court of Riverside, CA - case dropped - for Plaintiff's Counsel

**Software Industry Appropriate Compensation**

- Feltman vs Otalvaro, et al – case settled – US Bankruptcy Court, Southern Florida – for Plaintiff's Counsel
- Smith, Dodson, Steele, Port, et al vs Kaiser Permanente [class action], US District Court, Northern California, case settled - for Plaintiff's Counsel
- Tan vs CSAA [class action], US District Court, Northern California, case settled - for Plaintiff's Counsel
- Langille vs EMC [class action], US District Court, Northern California, case settled – for Plaintiff's Counsel
- Delmare vs Sungard [class action], US District Court, Northern California, case settled - for Plaintiff's Counsel
- Apple vs Walsh [class action], US District Court, Northern California, case settled - for Plaintiff's Counsel
- Williams et al vs Lockheed Martin, US District Court, Southern California, case settled [Deposition] - for Plaintiff's Counsel

**Software Security Industry Best Practices**

- Doe vs Corona Norco Unified School District, Riverside County, CA Superior Court – For Plaintiff's Counsel

**Fiduciary Duties of Corporate Officers**

Lynch Communications, Inc. v Irish Communications, Inc, David O'Keefe, et al. – Superior Court of Riverside, CA - case dropped - for Plaintiff's Counsel

Other cases settled under seal

**Illegal Use of Business Name in HTML Metatags for SEO**

- Life Alert Emergency Response, Inc. vs ConsumerAffairs.com, Inc. – Los Angeles County
- Superior Court - case settled - for Plaintiff's Counsel



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

**Software Contract Performance**

- Alliance Manufacturing Software, Inc. vs Typhoon Software, Inc. – Santa Barbara Superior Court – [Deposition] - Judgement for Plaintiff - for Defendant's Counsel
- Wilmar Group vs Mastech Systems Corp. – Court of Common Pleas – Allegheny County, PA – case settled - for Plaintiff's Counsel

**Genealogy of Software Source Code to Determine Branching**

- Norton vs Norton, Los Angeles Family Court – case settled - for Defendant's Counsel

**Professional Conduct Among Scientists – Defamation**

- Watts vs Synolakis – US District Court - Juneau, Alaska - case settled - for Defendant's Counsel

**Evaluation of Private Pilot Dangerous Conduct**

- Lima vs Foster, Los Angeles Family Court – case settled

**Airline Liability**

- Case sealed

**Building Lighting Liability**

- Gordon vs Pacific Properties – Santa Barbara, CA – case settled - for Plaintiff's Counsel

**Aerial Law Enforcement**

- People of the State of California vs Stevenson, Santa Barbara County Superior Court – reduced misdemeanor sentence [Court testimony; 1 hour; direct, cross] - for Defendant's Counsel

**SUMMARY OF EXPERT WITNESS AREAS**

- Computer software development issues, practices, responsibilities, financing, responsibility, defects, failure analysis, and valuation
- Patent, Copyright, and Trade Secret issues, including infringement and misappropriation, including audits of computer source code
- Outsourcing, including domestic and international
- General physics, dynamics, engineering, technology, and mechanics
- Software industry appropriate compensation
- Engineering and software industry standards and contract performance, including industry best practices Management practices in engineering, science, research & development, and technology
- General aviation aircraft operations [FAA rated Airline Transport Pilot, former Flight Instructor, Ground Instructor, and Parachute Rigger]



**Wayne B. Norris, Chief Scientist, Norris Associates Technologies**  
**Because Accuracy Matters**

- Fiduciary duties of corporate officers
- Hazardous materials, oil spills, radiological and industrial safety

**WAYNE B. NORRIS**

# **EXHIBIT G**

**(SW- 8 Hale Drive)**

UNITED STATES DISTRICT COURT  
for the  
Northern District of New York

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )  
THE PREMISES KNOWN AND )  
DESCRIBED AS 8 HALE DRIVE, )  
HALFMOON, NY 12065, INCLUDING )  
ANY LOCKED AND CLOSED )  
CONTAINERS AND CLOSED ITEMS )  
CONTAINED THEREIN )

Case No. 18-MJ-164-(DJS)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer  
An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of New York  
(Identify the person or describe the property to be searched and its given location):  
Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (Identify the person or describe the property to be seized):  
Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before April 9, 2018  
(not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m.  at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Hon. Daniel J. Stewart.

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for \_\_\_\_\_ days (not to exceed 30).

until, the facts justifying, the later specific date of [Click here to enter a date..](#)

Date issued: March 26, 2018  
Time issued: ~~3:50 p.m.~~ 3:53 pm  
City and State: Albany, NY

  
\_\_\_\_\_  
*Judge's signature*  
Hon. Daniel J. Stewart, U.S. Magistrate Judge  
\_\_\_\_\_  
*Printed name and title*

<i>Return</i>		
<i>Case No.:</i> 18-MJ- (DJS)	<i>Date &amp; time warrant executed:</i>	<i>Copy of warrant &amp; inventory left with:</i>

*Inventory made in the presence of :*

*Inventory of the property taken and name of any person(s) seized:*

***Certification***

*I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.*

*Date:* \_\_\_\_\_

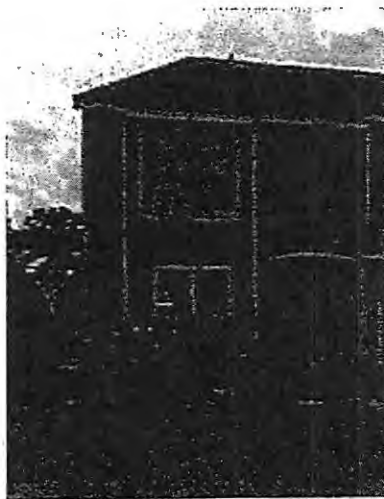
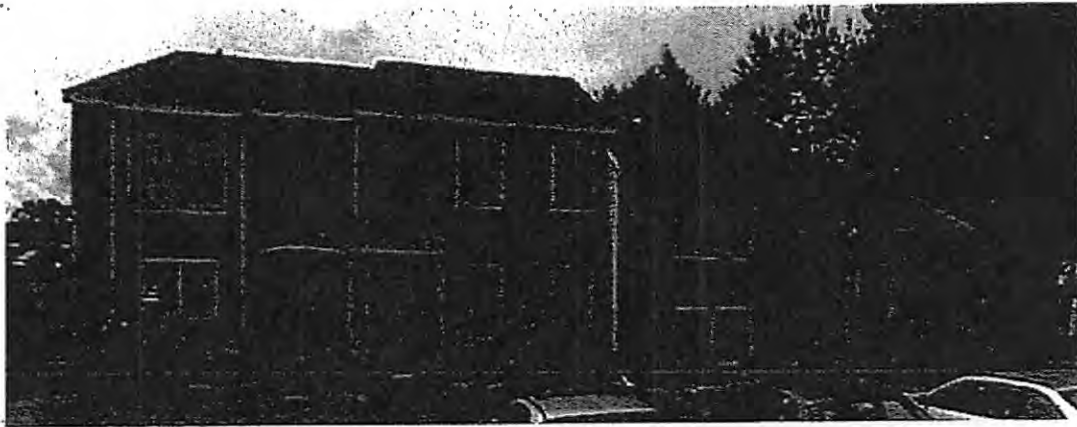
\_\_\_\_\_  
*Executing officer's signature*

\_\_\_\_\_  
*Printed name and title*



**ATTACHMENT A**  
**Property to Be Searched**

The premises to be searched is known and described as 8 HALE DRIVE, HALFMOON, NEW YORK 12065 (the "SUBJECT PREMISES") INCLUDING ANY LOCKED AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN, is a two story townhouse with beige siding. The townhouse is set back from Hale Drive and is accessible by a walkway that runs from a parking area directly to the front door. There is a "port" style window immediately next to the front door. A photograph of the SUBJECT PREMISES is below.



**ATTACHMENT B**  
**Particular Things to be Seized**

Things to be seized from the SUBJECT PREMISES, all of which constitute evidence, fruits and instrumentalities of violations of 18 U.S.C. § 1591 (sex trafficking by force, fraud or coercion and interference in an investigation into sex trafficking by force, fraud or coercion), 18 U.S.C. § 1589 (forced labor), [REDACTED]

(collectively, the “Subject Offenses”) involving KEITH RANIERE occurring in or after January 1, 2015, include:

- a. Records, things and other information that constitute evidence, fruits and instrumentalities of the Subject Offenses, including but not limited to, “collateral,” as described in the affidavit; sex trafficking paraphernalia; evidence regarding the formation and structure of DOS; notes or writings related to DOS; communications between RANIERE and any DOS masters/slaves; evidence showing an attempt to dissociate RANIERE and/or Nxivm from DOS; and evidence of RANIERE’s flight from prosecution;
- b. Records and information relating to Yahoo! account keithraniere@yahoo.com or other emails accounts or messaging services used by RANIERE or DOS slaves or masters;
- c. Computers or storage media used as a means to commit or facilitate the commission of the Subject Offenses (including to store “collateral,” as described in the affidavit); and
- d. Bundles of United States currency evidencing the existence of schemes to commit the Subject Offenses or proceeds of the Subject Offenses.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;

- d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. Evidence indicating the computer user's state of mind as it relates to the Subject Offenses;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about Internet Protocol addresses used by the COMPUTER;
- l. Records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. Contextual information necessary to understand the evidence described in this attachment; and
- n. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

**The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.**

# **EXHIBIT G1**

**(Return on SW - 8 Hale Drive)**

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/Seized

File # 50A-NY-2233091

On (date) March 27, 2018

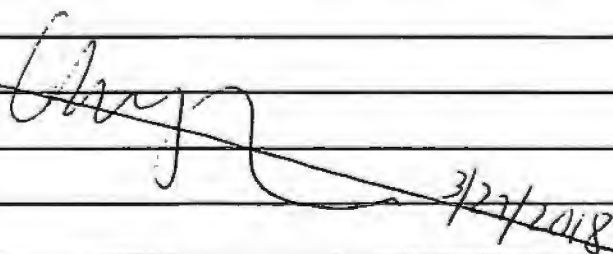
item(s) listed below were:  
 Received From  
 Returned To  
 Released To  
 Seized

(Name) EXECUTIVE HOUSING + PROP

(Street Address) E Hale Drive

(City) HALFMOON, NY

Description of Item(s): 1) Cannon Ultrastill (MILWA with accessories) SN:142090B348; 2) Nikon Digital SN: NCA551365334; 3) one book "History of Torture"; 4) 29 Mini DV cassettes; 5) 1 Sony DVI Cam cassette; 6) one Amazon Kindle SN B00418219322096; 7) one memory CDR disc; 8) one 4GB Toshiba thumb drive; 9) one CD titled "Heaven in Exile"; 10) misc documents; 11) one white storage device SN: NCAV47036371; 12) Lenovo computer tower SN: 1150A65310ZVJ6J324H020 13) Apple tower model A1047ENC2061; 14) Lacie storage device SN: 164400534; 15) airport extreme base station SN: 6F1169WACC with charger; 16) Marantz audio recorder and accessories; 17) 5 digital videotapes; 18) 1 ultra USB2 storage; 19) black storage device SN NCAV54873732 20) Echo voice recorder with case; 21) UBEE router with charger SN: B831U27000562; 22) Netgear router SN: 2BK3117S22DD3; 23) Panasonic 5.8 digital telephone; 24) 6 misc VHS tapes; 25) 1 book; 26) 2 DVDs; 27) 24 ~~DVR~~<sup>CDR</sup> CDRs; 28) 2 binders (black); 29) Times Union letter addressed to Keith Barriere; 30) \$265 in cash; 31) 1 DVD titled "Bought and Sold"; 32) box of white pills; 33) 1 micro cassette; 34) 16 DVC cassettes; 35) 1 Apple ipod with case and headphones; 36) 1 Sony DVD drive SN: 5042648; 37) Lacie hard drive SN: 154107441

  
3/27/2018

Received By: \_\_\_\_\_  
(Signature)

Received From: \_\_\_\_\_  
(Signature)

# **EXHIBIT H**

**(Defense Discovery Request – 3/16/2022)**



**TULLY & WEISS**  
ATTORNEYS AT LAW

March 16, 2022

**VIA EMAIL**

Assistant United States Attorney Tanya Hajjar  
U.S. Attorney's Office  
Eastern District of New York  
271 Cadman Plaza East  
Brooklyn, NY 11201  
Tanya.hajjar@usdoj.gov

**Re: *United States v. Keith Raniere*, 18-CR-204 (NGG)**

Dear AUSA Hajjar:

This letter is submitted on behalf of defendant Keith Raniere in the above-entitled case and pursuant to Rule 16 of the Federal Rules of Criminal Procedure, *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and *Kyles v. Whitley*, 514 U.S. 419 (1995). Mr. Raniere demands the following information, documents, and other materials based on newly discovered evidence that was uncovered following trial, sentencing, and appellate briefing in this case. Each below demand is supported by a specific finding made after the trial and sentencing of Mr. Raniere, which in turn, led to the discovery that the government either possesses additional information or materials related to these findings or should have been aware of same.

Firstly, we request information pertaining to photographic images that were purportedly taken in 2005 depicting underage nudity on a camera's CF card and hard drive that were seized from 8 Hale Drive on March 27, 2018. As the government is aware, the dates of these photographs were crucial to establishing the age of the individuals at the time the photographs were taken during jury trial. Mr. Raniere concludes that the above-mentioned evidence was manipulated and materially altered while in FBI custody.

Secondly, we request information pertaining to witness collusion and tampering between key witnesses, namely, Nicole and Daniela. Considering the newly discovered evidence on this issue, we also seek information concerning other witnesses and potential government tampering.

Thirdly, we request information concerning dates, times, and other documentary proof of Nicole's travels.

Lastly, we request information pertaining to the arrest of Mr. Raniere in Mexico.

Even if the government were unaware of the below issues, they constitute newly discovered evidence pursuant to Rule 33 of the Federal Rules of Criminal Procedure. Therefore, we request production of the following:

**Camera Images and Data**

**FRESNO**

1340 VAN NESS  
(559) 321-0907

**LOS ANGELES**

220 S. PCH, STE 106  
(424) 383-9700

**MARTINEZ**

713 MAIN ST.  
(925) 229-9700

**REDDING**

1388 COURT ST., STE G  
(530) 999-9700

**SAN FRANCISCO**

333 WEST PORTAL, STE A  
(415) 360 9007

**SELMA**

1916 E. FRONT ST.  
(559) 860-0970



**TULLY & WEISS ATTORNEYS AT LAW**

FIAT JUSTITIA RUAT CAELUM

PAGE 2 OF 4

1. The entire chain of custody of the seized camera, **camera's CF card**, and hard drive since its seizure on March 27, 2018, including every individual that had possession or control of these items along with specific dates as to when the evidence was in possession and when the chain of custody was broken as well as for any derivative evidence copies that were made.<sup>1</sup>
2. CART evidence receipts for all devices seized from 8 Hale Drive on March 27, 2018.
3. Documentation establishing exactly when, and the circumstance as to why, photographs were manually added to the **camera's CF card** between April 11, 2019 and June 11, 2019, while in FBI custody. Specifically, this request relates to the disparity between the two Forensic Toolkit reports produced on these dates and why new files appeared on the latter report.
4. The identity of the individual(s) who accessed the **camera's CF card** on September 19, 2018 and altered the file system dates while in the custody of the FBI. According to the **camera's CF card's file listing, the accessed dates for all active files were** changed to September 19, 2018, indicating that the dates were altered on at least this one occasion during the six months they were in the custody of the FBI. We further request the true and original dates that were indicated prior to alteration.
5. The identity of the individual(s) who altered the dates of the photographs through manual intervention and the dates on which the alterations occurred. Specifically, this request refers to the differences in dates between the EXIF dates and Modified dates.
6. The identity of the individuals(s) who manually altered the modified date on the photograph identified as IMG\_0175. Alteration is evidenced by the fact that the EXIF **CreatorTool value of said image is set to "Adobe Photoshop Elements 3.0,"** indicating Photoshop was used to open and modify the file data.
7. The individual(s) who altered the names of the folders containing the alleged contraband photographs so that it appeared the dates provided in the file names corresponded to the EXIF data of files in those folders. We further request the true and original folder dates.
8. The individuals(s) who backdated the folder content and rolled back the system time to 2003 before manually copying these files onto the seized hard drive. This request is in relation to the fact that all the files in the Dell Dimension backup folder have a created date of July 26, 2003, despite the folder name indicating the backup date as March 30, 2009, **the same date that appears on all the files' created dates.**
9. All examination notes of the forensic examiners.
10. Photographs of the **camera's CF card**, documenting its condition and packaging, when received by FE Flatley on 02/22/2019 and by FE Booth on 06/10/2019.
11. All communications, including but not limited to texts, e-mail messages, notes, and voicemail messages, of FET Donnelly, FE Booth, FE Flatley, SA Lever, and SA Jeffrey, SA Mills, SA Weniger, AUSA Hajjar, AUSA Penza, AUSA Lesko, regarding this case.
12. The original forensic image (NYC023721\_1B16.E01) and file listing of the WD HDD (1B16) created by FET Donnelly (NYC023721\_1B16.E01.csv) and the imaging log for that item.

---

<sup>1</sup> Accordingly, any evidence related to manipulation, alteration, or chain of custody breaks with said evidence should have been disclosed by the government in advance of trial.

**TULLY & WEISS ATTORNEYS AT LAW**

FIAT JUSTITIA RUAT CAELUM

PAGE 3 OF 4

---

13. The FTK log of the processing, browsing, searching, and bookmarking of evidence for the WD HDD (1B16) and both instances of processing for the **camera's CF card** (1B15a).
14. The forensic image of the **camera's CF card** created by FE Flatley (NYC024299.001), together with its imaging log and file listing (.CSV) file.
15. The forensic image of the **camera's CF card** (1B15a) created by FE Booth (NYC024299\_1B15a.E01), together with its imaging log and file listing (.CSV) file.
16. The CART Requests corresponding to SubID 196817 and SubID 208206.
17. All EXIF data for ALL photographs listed on both of the **camera's CF card** reports (GX 521A, dated 04/11/2019, and GX 521A Replacement, dated 06/11/2019).
18. The logical file layout of the **camera's CF card**

**Witness Collusion and Tampering**

1. All 3500 materials, including 302 notes, and all internal memoranda, including FBI messages, emails, and other communications regarding witnesses and witness meetings not previously provided;
2. All aforementioned materials specifically as they pertain to:
  - a. India
  - b. Siobahn Hotaling
  - c. Michele Hatchette
  - d. Danielle Roberts
  - e. Samantha LeBaron
3. All aforementioned materials specifically as they pertain to:
  - a. Mark Vicente
  - b. Souki
  - c. Audrey
  - d. Crystal
  - e. Sarah Edmondson
  - f. Nicole
  - g. Daniela
  - h. Catherine Oxenberg
  - i. **Jessica Joan ("Jaye")**
4. All text messages and email communications between the individuals reference in 3) between May 2017 and May 2019;
5. All documentation or communications between FBI agents and/or AUSAs concerning FBI conduct that could be perceived as direct or indirect witness intimidation;
6. All emails, text messages, letters, or other forms of written communication between Neil Glazer **and the government, including the United States Attorney's Office and FBI**;
7. Any audio recordings of Neil Glazer;
8. Any audio recordings, text messages, or other forms of communication between witnesses prior to any testimony.

**Nicole Travels**

1. Any Amtrak, Greyhound, or other commercial train or bus receipts, with corresponding dates and times, provided to the FBI and/or Justice Department **concerning Nicole's** train or bus travels to Albany where the purported sex acts occurred.

**TULLY & WEISS ATTORNEYS AT LAW**

FIAT JUSTITIA RUAT CAELUM

PAGE 4 OF 4

2. **Any payment information concerning Nicole's method of payment of the abovementioned travel.**
3. Any other documentation concerning the dates, times, **and modes of Nicole's travels.**

**Mr. Raniere's Arrest**

1. Any text messages, phone calls, emails between individuals from the United States Justice Department, including but not limited to the FBI, DEA, and **U.S. Attorney's Office**, any private citizens, and/or diplomats to further the detention, arrest, or capture of Mr. Raniere.
2. Any information concerning the arrest of Mr. Raniere upon his arrival in the US, including the identification of the arresting agents, any information concerning the purchase of the commercial airplane ticket for Mr. Raniere from Mexico to Texas, after his capture in Mexico, and the passenger manifest for that flight.
3. Any information concerning the capture of Mr. Raniere in Mexico on March 25, 2018, including the identification of the individuals involved in the capture.
4. Any official records of deportation, extradition, or expulsion of Mr. Raniere from Mexico.

We expect that the requested materials be produced as soon as possible given their already untimely production. If the government needs clarification of any of the above requests, please do not hesitate to contact me.

Very truly yours,



Joseph Tully

# **EXHIBIT H1**

**(Correspondence From Defense Re Discovery Request)**

**From:** [Joseph Tully](mailto:Joseph.Tully)  
**To:** [Tanya.hajjar@usdoj.gov](mailto:Tanya.hajjar@usdoj.gov)  
**Subject:** Informal Discovery Request (2022-03-16).pdf  
**Date:** Wednesday, March 16, 2022 1:21:00 PM  
**Attachments:** [Informal Discovery Request \(2022-03-16\).pdf](#)

---

Dear Ms. Hajjar,

Attached, please find an informal discovery request dated today's date sent pursuant to Rule 16 of the Federal Rules of Criminal Procedure, *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and *Kyles v. Whitley*, 514 U.S. 419 (1995). If you have any questions or need any clarification, please do not hesitate to reach out to me.

Very truly yours,

*Joseph M. Tully*

Joseph M. Tully  
Tully & Weiss Attorneys at Law  
Certified Specialist, Criminal Law



Certified Specialist in Criminal  
Law by the State Bar of California  
Board of Legal Specialization

**Bay Area:**

713 Main St., Martinez, CA 94553, [\(925\) 229-9700](tel:(925)229-9700)  
333 West Portal, Ste. A, San Francisco, CA 94127, [\(415\) 360-9007](tel:(415)360-9007)

**Central Valley:**

1340 Van Ness, Fresno, CA 93721, [\(559\) 321-0907](tel:(559)321-0907)  
1916 E. Front St., Selma, CA 93662, [\(559\) 860-0970](tel:(559)860-0970)

**Northern California:**

1388 Court St., Ste. G, Redding, CA 96001, [\(530\) 999-9700](tel:(530)999-9700)

**Southern California:**

220 S. Pacific Coast Hwy, Ste. 106, Redondo Beach, CA 90277 [\(424\) 383-9700](tel:(424)383-9700)

**Toll Free:** (844) 788-9700 (All Branches)

**Text msg:** (844) 788-9700 (All Branches)

**Fax:** (925) 231-7754 (All Branches)

# **EXHIBIT H2**

**(Correspondence From Government Re Discovery Request)**

**From:** [Hajjar, Tanya \(USANYE\)](#)  
**To:** [Joseph Tully](#)  
**Subject:** RE: Informal Discovery Request (2022-03-16).pdf  
**Date:** Friday, March 18, 2022 1:13:48 PM  
**Attachments:** [2022-03-18 Letter \(Raniero\).pdf](#)

---

Joseph,

Please see attached.

Thanks,  
Tanya

---

**From:** Joseph Tully <joseph@tully-weiss.com>  
**Sent:** Wednesday, March 16, 2022 4:21 PM  
**To:** Hajjar, Tanya (USANYE) <THajjar@usa.doj.gov>  
**Subject:** [EXTERNAL] Informal Discovery Request (2022-03-16).pdf

Dear Ms. Hajjar,

Attached, please find an informal discovery request dated today's date sent pursuant to Rule 16 of the Federal Rules of Criminal Procedure, *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and *Kyles v. Whitley*, 514 U.S. 419 (1995). If you have any questions or need any clarification, please do not hesitate to reach out to me.

Very truly yours,

*Joseph M. Tully*

Joseph M. Tully  
Tully & Weiss Attorneys at Law  
Certified Specialist, Criminal Law



**Bay Area:**

713 Main St., Martinez, CA 94553, [\(925\) 229-9700](tel:(925)229-9700)  
333 West Portal, Ste. A, San Francisco, CA 94127, [\(415\) 360-9007](tel:(415)360-9007)

**Central Valley:**

1340 Van Ness, Fresno, CA 93721, [\(559\) 321-0907](tel:(559)321-0907)

1916 E. Front St., Selma, CA 93662, [\(559\) 860-0970](tel:(559)860-0970)

**Northern California:**

1388 Court St., Ste. G, Redding, CA 96001, [\(530\) 999-9700](tel:(530)999-9700)

**Southern California:**

220 S. Pacific Coast Hwy, Ste. 106, Redondo Beach, CA 90277 [\(424\) 383-9700](tel:(424)383-9700)

**Toll Free:** (844) 788-9700 (All Branches)

**Text msg:** (844) 788-9700 (All Branches)

**Fax:** (925) 231-7754 (All Branches)



# **EXHIBIT H3**

**(Correspondence From Government Re Discovery Request)**



**U.S. Department of Justice**

*United States Attorney  
Eastern District of New York*

TH  
F. #2017R01840

*271 Cadman Plaza East  
Brooklyn, New York 11201*

March 18, 2022

By Email

Joseph M. Tully, Esq.  
Tully & Weiss  
joseph@tully-weiss.com

Re: United States v. Keith Ranieri  
Criminal Docket No. 18-204 (S-2) (NGG)

Dear Counsel:

The government is in receipt of your letter dated March 16, 2022.

The government fully complied with its obligations pursuant to Rule 16 of the Federal Rules of Criminal Procedure, 18 U.S.C. § 3500, and Brady v. Maryland, 373 U.S. 83 (1963) and its progeny prior to the jury trial in this case.

Very truly yours,

BREON PEACE  
United States Attorney

By: /s/  
Tanya Hajjar  
Assistant U.S. Attorney  
(718) 254-7000

# **EXHIBIT I**

**(Discovery Letter April 29, 2019)**



U.S. Department of Justice

*United States Attorney  
Eastern District of New York*

MKP/TH  
F. #2017R01840

*271 Cadman Plaza East  
Brooklyn, New York 11201*

April 24, 2019

By Hand

Marc Agnifilo, Esq.  
Brafman & Associates  
767 Third Avenue  
New York, NY 10017

Re: United States v. Keith Raniere  
Criminal Docket No. 18-204 (S-2) (NGG)

Dear Counsel:

Pursuant to Rule 16 of the Federal Rules of Criminal Procedure, the government is providing a disk with additional discovery in the above-captioned case, which is Bates-numbered NXIVM00930272-NXIVM00930321 and VDM\_NXIVM000265046 - VDM\_NXIVM000265047.

This discovery is being provided to you pursuant to the protective order entered by the Court on August 1, 2018. Where practical, documents have been watermarked "SUBJECT TO PROTECTIVE ORDER," but all materials being produced are subject to the protective order, regardless of the watermark. Certain materials, as set forth in the chart below, are designated as "Victim Discovery Material," and where applicable, "Highly Sensitive Material." Some categories of documents have been designated as "Victim Discovery Material" ("VDM") or "Highly Sensitive Material" ("HS") because the process of individually designating the items would have led to a significant delay in production. Consistent with the protective order, the government is open to discussing the designations with defense counsel.

The government will continue to provide discovery on a rolling basis and continues to request reciprocal discovery from the defendant.

<b>BATES RANGE</b>	<b>DESCRIPTION</b>	<b>DESIGNATION</b>
NXIVM00930272- NXIVM00930321	Property Records	SUBJECT TO PROTECTIVE ORDER
VDM_NXIVM000265046	Report - IB15	SUBJECT TO PROTECTIVE ORDER
VDM_NXIVM000265047	Report - 1B16	SUBJECT TO PROTECTIVE ORDER

Very truly yours,

RICHARD P. DONOGHUE  
United States Attorney

By: /s/ \_\_\_\_\_  
Moira Kim Penza  
Tanya Hajjar  
Assistant U.S. Attorneys  
(718) 254-7000

cc: Counsel of Record