

* FILED *

2022 JUN 21 PM 11:28

CLERK
U.S. DISTRICT COURT
E.D.N.Y.
AFTER HOURS DROP BOX

EXHIBIT A

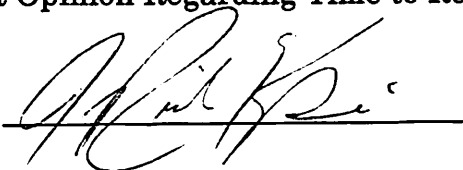
EXHIBIT A

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. # GG386579
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 number¹. 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_0180–0183 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.

¹ 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 01/01/2003². 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

² 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 dates³.

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	f7ac8c54897985961f729299756fc319	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	b5ea586450d43d25eda07fffb7f76f82	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>Carey Cleary</i>	9/19/2018 0902	Signature: <i>Michael Lever</i>	9/19/18 9:00am
Printed Name/Agency: <i>Carey Montgomery</i>		Printed Name/Agency: <i>Michael Lever / FBI</i>	
Reason: <i>CLC to SA</i>		Reason: <i>Evidence Review</i>	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: <i>Michael Lever</i>	9/26/18 1:15 PM	Signature: <i>Carey Montgomery</i>	9/26/18 1:15 PM
Printed Name/Agency: <i>Michael Lever / FBI</i>		Printed Name/Agency: <i>Carey Montgomery</i>	
Reason: <i>For Evidence Review</i>		Reason: <i>Camera to be returned</i>	

³ **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	97d26874707bf3f9e76fc22b57d86d0	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	884764bfbb7a72ed5f726af5d5eb11b5	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/
IMG_0094.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	4795f46d36fa9c33e20b90ca2eebdc63	WD External Device/
IMG_0095.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	3c89631e7576a554a13efca5fd3fb8d3	WD External Device/
IMG_0096.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	dd2adf19eb671d7cdad10fe43e1e977	WD External Device/
IMG_0097.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	f3cba2fe0cf8fca83eab33d0afcb522a	WD External Device/
IMG_0098.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:34	a28460e871c2127a4a6b652785a79c3d	WD External Device/

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	53834a379843cc754d6860b0c6525c9a	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	c16e661d4bc58afe43f24efd13d24e	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/

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”.

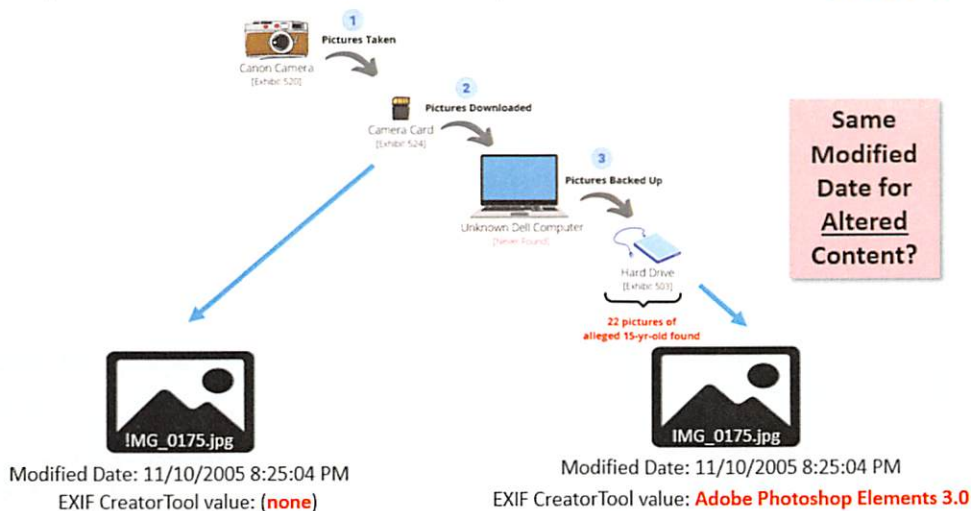
Name IMG_0175.JPG
Extension jpg
Item Number 1064
Path Lexar CF 2GB Card/Partition 1/LEXAR MEDIA [FAT16]/[root]/DCIM/101CANON/!
 MG_0175.JPG
Created Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
Accessed Date 11/10/2005
Modified Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
MD5 Hash
Deleted 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.”

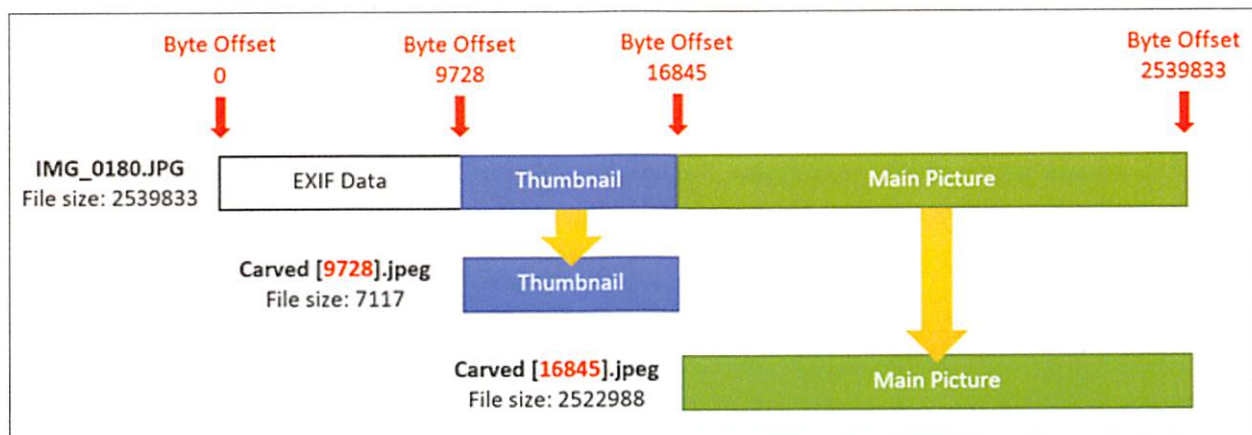


Figure 1. How a forensic tool creates and names files carved from digital photographs.

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	f6202d0b41e30c7c21aeae32c38baf9b	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 [XXXXX].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)¹.

Figure 1: Files Appearing on the First FBI Forensic Reports of the CF Card and WD HDD



04/11/2019 CF Card Report 	04/11/2019 WD HDD Report 
IMG_0021-41	
	IMG_0043-79
	IMG_0081-100
	IMG_0101-149
	IMG_0150-163
	IMG_0164,5,8,9
	IMG_0172-79 sans 173
IMG_0180-183	IMG_0180-183
	IMG_0184-191
	IMG_0194,7,8,9
	IMG_0203-223
IMG_0224-0243, sans 0226, 0232, and 0240	

Photo range of alleged contraband – not included in WD HDD report.




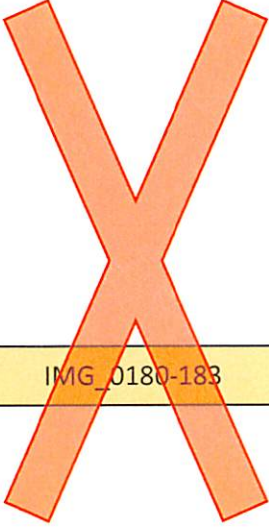
Photo range of alleged contraband – not included in WD HDD report.

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.

¹ 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_0172-179	IMG_0101-149
IMG_0180-183	IMG_0180-183	IMG_0150-163
	IMG_0193-200	IMG_0164,5,8,9
	IMG_0224-0243, sans 0226, 0232, and 0240	IMG_0184-191
IMG_0224-0243, sans 0226, 0232, and 0240	IMG_0224-0243, sans 0226, 0232, and 0240	IMG_0172-79 sans 173
		IMG_0180-183
		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.² 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* deleted³ 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.

² 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.

³ 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.⁴ 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.

⁴ 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**¹.
- 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.

¹ 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.²
- 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

² *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.³

- 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.⁴ 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.⁵
- **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

³ 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.

⁴ 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.”

⁵ *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.⁶ I could not find a record of such an approval.

⁶ 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>.

* FILED *

2022 JUN 21

OPM 11:20

CLERK
U.S. DISTRICT COURT
E.D.N.Y.
AFTER HOURS MAIL BOX

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 Ranieri.

Background

In this case, the prosecution claimed that Ranieri 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).

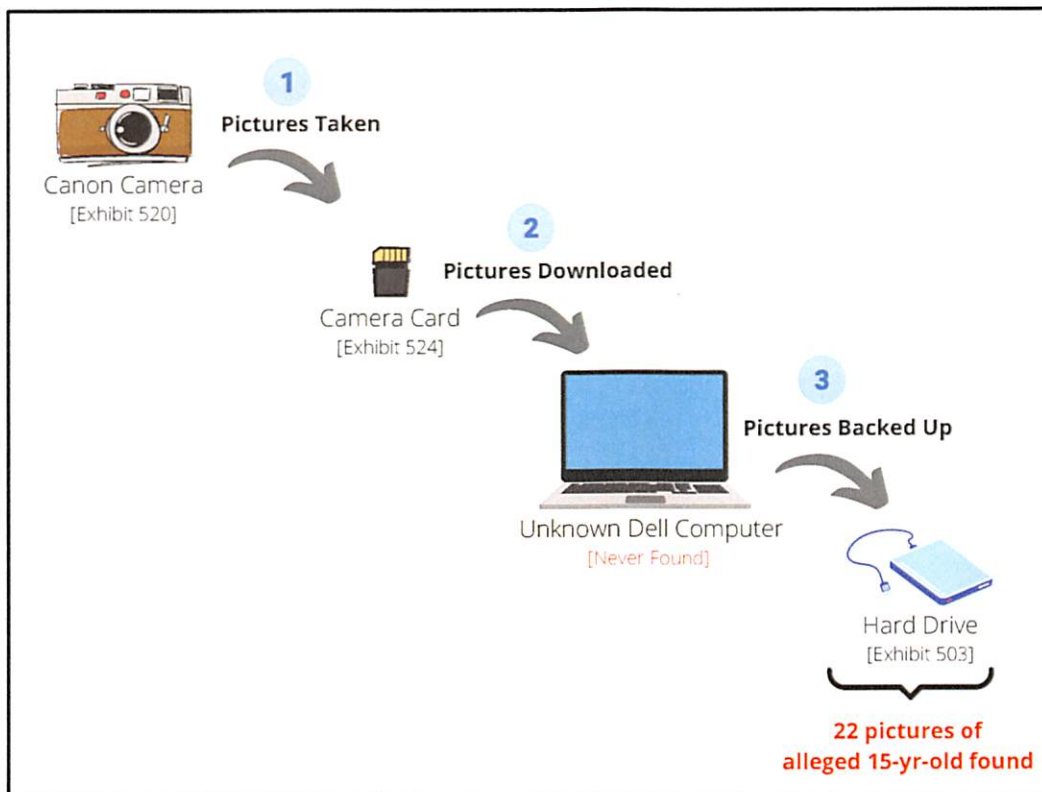


Figure 1: The Government’s narrative regarding alleged contraband found on a “backup” drive.

To demonstrate that the alleged user of the camera, Ranieri, 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.

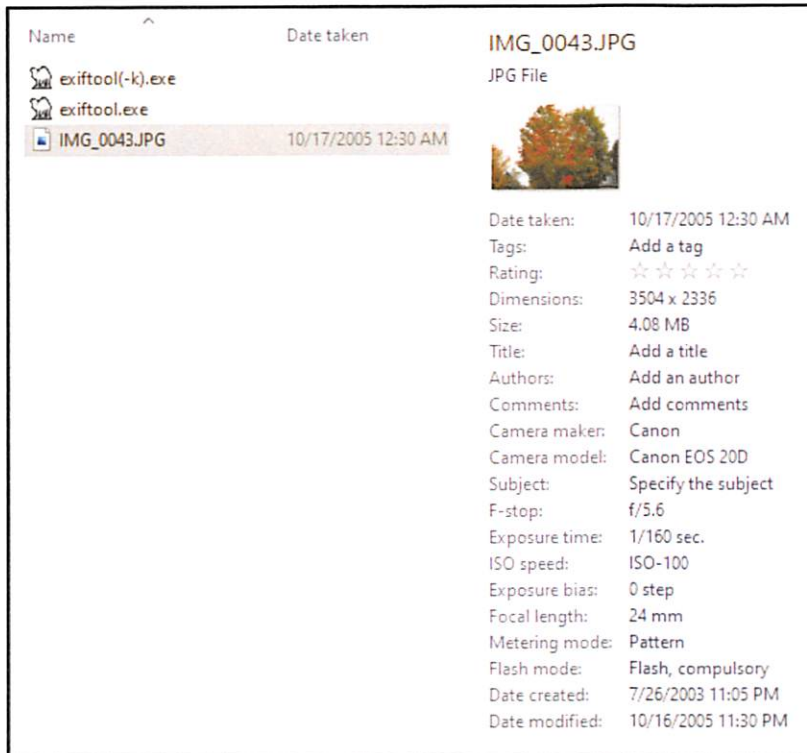


Figure 2. Windows display of EXIF data for IMG_0043.JPG.

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:

```

Make : Canon
Camera Model Name : Canon EOS 20D
Date/Time Original : 2005:10:17 00:30:04
Create Date : 2005:10:17 00:30:04

```

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.

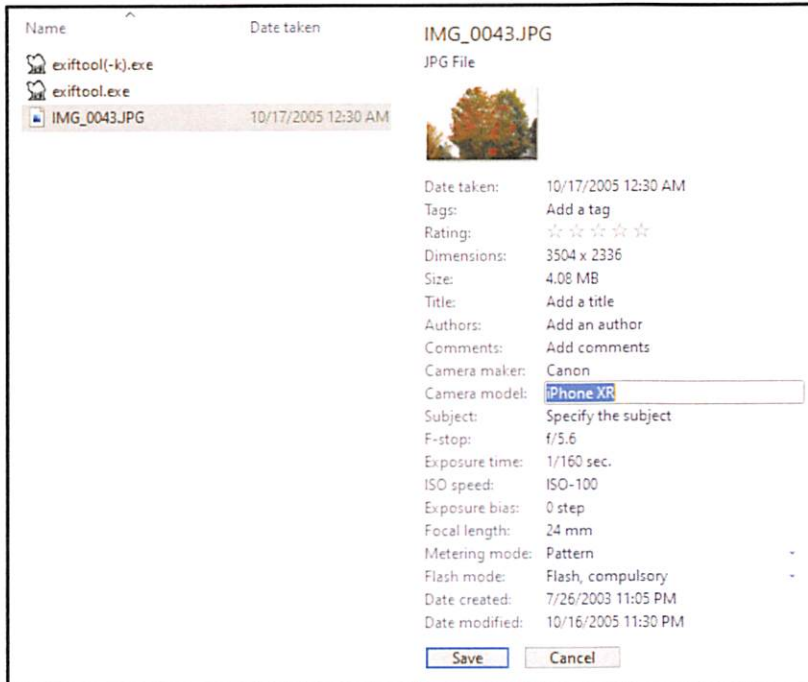


Figure 4. Changing the “Camera model” field in the EXIF data of a photo.

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.

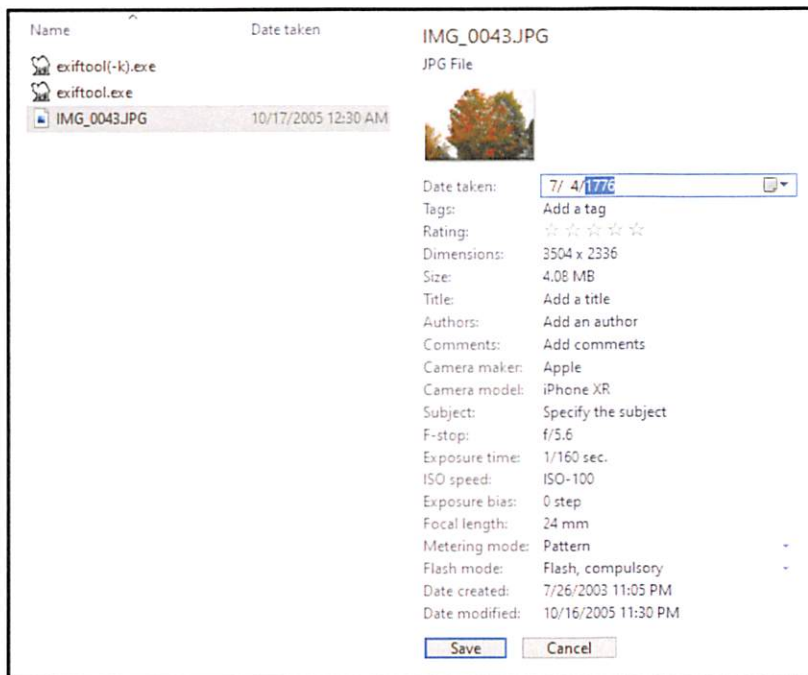


Figure 5. Changing the “Date taken” field in the EXIF data of a photo.

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.

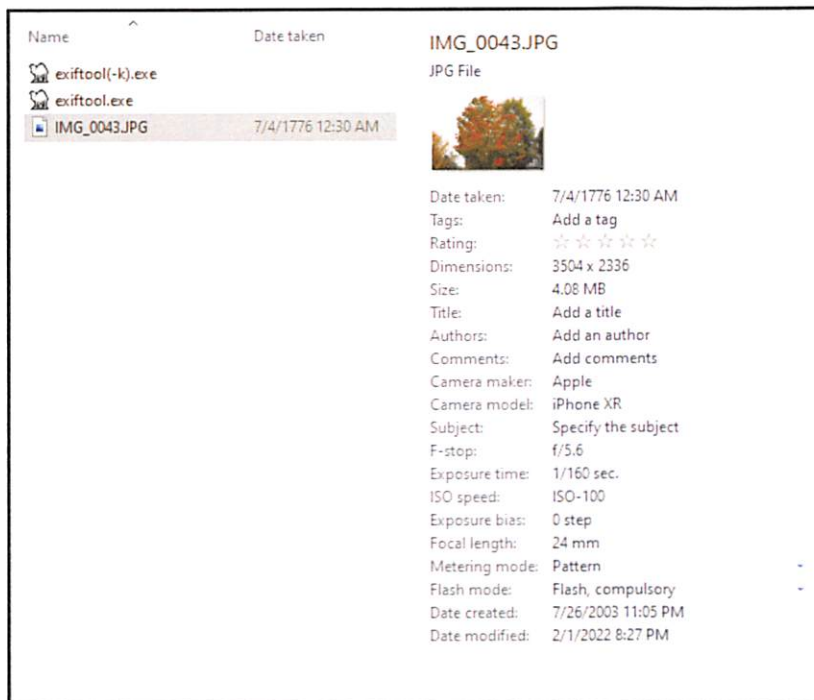


Figure 6. Windows display of saved changes in the EXIF data of photo IMG_0043.JPG.

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:

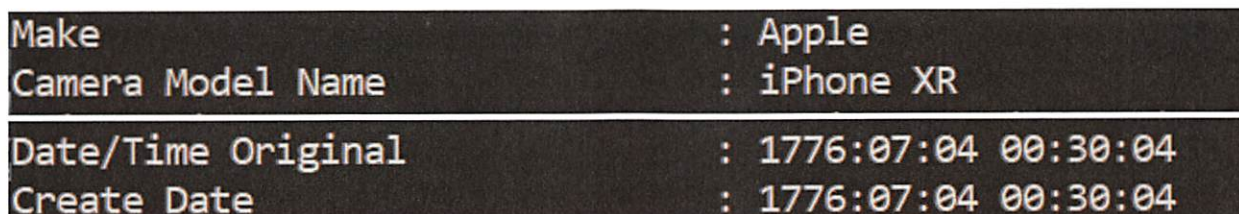


Figure 7. ExifTool display of saved changes in the EXIF data of photo IMG_0043.JPG.

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.

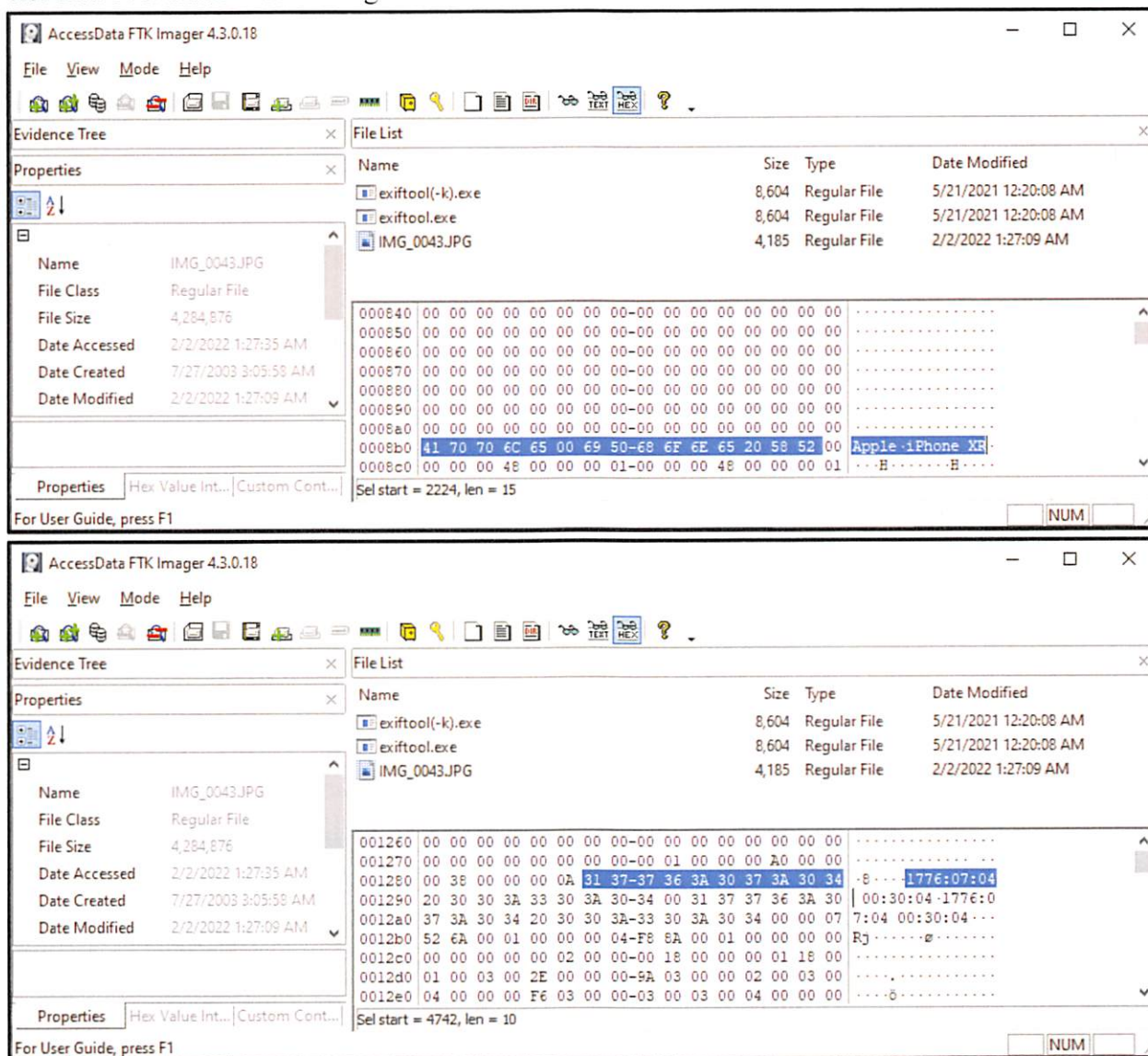


Figure 8. FTK Imager display of saved changes in the EXIF data of photo IMG_0043.JPG.

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 Ranieri 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 27th, 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 search¹, 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.

¹ 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 Raniere of child exploitation.

In describing one of the search photographs he took, SA Mills said, “*So 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 Raniere 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 Raniere – 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 Raniere.

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 receipt² 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?

² 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 03/13/2019¹, 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.

¹ 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 card² 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).

² See my Technical Findings and Process Findings reports, where I describe this anomaly in detail.

Conclusion

The government placed the Raniere 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 A1



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

Tariq A. Alsheddi, Ph.D. – Director of Naif Academy for National Security, Saudi Arabia

+966-1-2686308, t-alshedd@moisp.gov.sa

G. Clayton Grigg, PMP – FBI Chief Knowledge Officer

571-350-4217, gibtoo2003@gmail.com

Steven Krueger – FBI Section Chief, FBI Academy

337-233-2164, SKrueger314@gmail.com

Chris McCranie – FBI Special Agent, Washington Field Office

202-278-2000, cmccranie@hotmail.com

Micheal Neubauer, Ph.D. – Program Manager, FBI Laboratory

202-324-3000, mjneubauer@outlook.com

EXHIBIT B

**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

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

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

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

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

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

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,

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

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.

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

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.

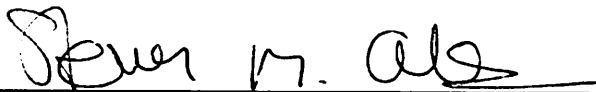
17. In addition to concurring with Dr. Kiper's observations and conclusions, I have a few additional observations that I made in my review of this evidence that I would like to include in this affidavit. In my reading of the trial transcript of FBI examiner Booth, I was struck by two points that he made 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

(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

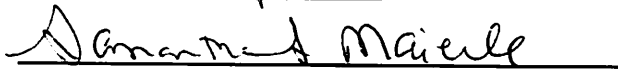
any evidence that arrived from further down the chain of custody in an unsealed state should be considered to be outside a proper chain of custody and not usable in a criminal matter. This is not just my experience in all the agencies for whom I worked, but also what Dr. Kiper reported from his knowledge 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
26 DAY OF April, 2022.



NOTARY PUBLIC FOR SOUTH CAROLINA

MY COMMISSION EXPIRES: March 18, 2024

* FILED *

2022 JUN 21 PM 11:28

CLERK
U.S. DISTRICT COURT
E.D.N.Y.
AFTER HOURS (DROP BOX)

EXHIBIT B1

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 ADAMSHIRLEY, (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 C

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 URL <https://Norris-Associates.com>

Linked in <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 nondisclosure 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.

A handwritten signature in blue ink, appearing to read 'Wayne B. Norris', written over a horizontal line.

WAYNE B. NORRIS

EXHIBIT C1

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 URL <https://Norris-Associates.com>

Linked  <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 12th 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/UYK-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 pixelated 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

A handwritten signature in blue ink, appearing to read 'Wayne B. Norris'. The signature is fluid and cursive.

WAYNE B. NORRIS