EXHIBIT 1

U.S. Department of Justice

Matthew M. Graves
United States Attorney

District of Columbia

Patrick Henry Building
601 D Street, N.W.
Washington, D.C. 20530

January 2, 2024

Mark E. Schamel
Ana L. Jara
Counsel for Shane Lamond
mescahmel@venable.com
aljara@venable.com

Re: ***United States v. Shane Lamond*** (Case No. 23-cr-177)

Dear Counsel:

The government hereby provides notice of intent to offer the testimony of Jennifer Kathryn Cain, Senior Digital Forensic Examiner for the Federal Bureau of Investigation ("FBI"). The government does not assert that the testimony of Examiner Cain constitutes expert witness testimony pursuant to Federal Rules of Evidence 702, 703, and 705. Out of an abundance of caution, however, and to the extent Examiner Cain's testimony may be construed by the Court as requiring expert testimony under those Rules, the government hereby gives notice of expert witness testimony pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G).[1]

Attached to this letter are descriptions of the qualifications and anticipated testimony of Examiner Cain. Specifically, Attachment A is a description of Examiner Cain's anticipated testimony. As noted, Examiner Cain's anticipated testimony will be about digital evidence collected from a cell phone belonging to Mr. Lamond and a cellphone belonging to Enrique

[1] If a law enforcement witness testifies to what files he or she found on a digital device or account, his or her testimony is not expert testimony. *See United States v. Berry*, 318 Fed. Appx. 569, 570 (9th Cir. 2009) (agent's testimony was not expert testimony because the agent "simply testified to what he found on the [defendant's] hard drive…, without expressing an opinion that required specialized knowledge or offering insight beyond common understanding") (citing Fed. R. Evid. 702). Thus, much of the anticipated testimony we lay out in Attachment A falls into this category, and does not require expert notice.

Tarrio. The evidence related to these devices has been provided to you through discovery, including discovery productions made on May 24, 2023, June 15, 2023, and June 23, 2023.

Attachment B is Examiner Cain's curriculum vitae. For your convenience, in Attachment C, the government is providing transcripts from Examiner Cain's prior expert testimony. The government reserves the right to: (1) supplement this notice with additional expert testimony; (2) provide you with any future expert reports prepared; and (3) provide you with any supplemental information.

Accordingly, this letter, and the incorporated attachments, constitute the government's expert notice disclosure, pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G), of witnesses who may be called as experts during trial in this matter to testify regarding the topics listed in the attached.

Pursuant to Rule 16(b)(1)(C) of the Federal Rules of Criminal Procedure, the government requests immediate reciprocal disclosure from the defense of any evidence that defendant intends to introduce at trial under Rules 702, 703, and/or 705 of the Federal Rules of Evidence

Sincerely,

MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar Number 481052

/s/ Rebecca G. Ross
Rebecca G. Ross
Joshua S. Rothstein
Assistant United States Attorneys
601 D Street, N.W.
Washington, D.C. 2053
Office: 202-252-7164 (JSR), 202-252-6937 (RR)
Rebecca.Ross2@usdoj.gov
Joshua.Rothstein@usdoj.gov

ATTACHMENT A

ATTACHMENT A

I. FBI Senior Digital Forensic Examiner Jennifer Kathryn Cain

Examiner Cain has been with the Federal Bureau of Investigation ("FBI") for over ten years and has served as a digital forensic examiner for approximately six years, earning the "senior examiner" certification in 2021. Her expert qualifications are further detailed in her curriculum vitae, which is attached as Attachment B.

The government seized a significant amount of evidence in the form of photographs, videos, and messages extracted from the digital devices of the defendants and co-conspirator, Enrique Tarrio ("Tarrio"). That electronic evidence seized from digital devices will be admissible through lay/fact witness testimony by FBI special agents or Examiner Cain who extracted, located, and/or reviewed this evidence. [1]

The government may qualify Examiner Cain as an expert in the field of digital forensic analysis and have Examiner Cain offer some background testimony about how data is extracted, processed, and analyzed from digital devices, and then to offer testimony about conclusions she drew about a limited subset of the electronic evidence in this case.

Specifically, Examiner Cain's testimony will be about digital evidence collected from the following two devices:

Device Belonging to:	**Description**
Shane Lamond (Referred herein as "Lamond's Device")	One (1) iPhone XR [iPhone11,8 N841AP] running iOS 14.6 with S/N: DX3CJ7BMKXKN; IMEI: 356450107630375; MSISDN: 12024370434; and UUID: 00008020-000948AC3C0B002E.
Enrique Tarrio (Referred herein as "Tarrios's Device")	One (1) iPhone 11 Pro Max (iPhone 23,5 D431Ap) running iOS 14.2 with S/N: F2MZKPPGN70G; IMEI: 353891104722470; MSIDN: 1786916789, and UUID: 00008020-000948AC3C0B002E

[1] Law enforcement witness is not expert testimony if it is simply about what files he or she found on a digital device or account. See United States v. Berry, 318 Fed. Appx. 569, 570 (9th Cir. 2009) (agent's testimony was not expert testimony because the agent "simply testified to what he found on the [defendant's] hard drive…, without expressing an opinion that required specialized knowledge or offering insight beyond common understanding") (citing Fed. R. Evid. 702). Please let us know immediately if you disagree with this position so that we can raise this issue with the Court well in advance of trial.

II. General Topics

a. Examiner Cain will provide a basic overview of how data is extracted from cellular telephones and similar digital devices and then processed and examined, including certain specific steps that need to be taken to extract data from certain messaging platforms, including Telegram, from certain devices.

b. Examiner Cain will provide testimony about what the Telegram application is and how it works. Examiner Cain will testify that Telegram is an end-to-end encrypted communications application, available for use on mobile devices and computers. Examiner Cain will explain that end-to-end encryption is a method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. In end-to-end encryption, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it. As it travels to its destination, the message cannot be read or tampered with by an internet service provider ("ISP"), application service provider, hacker, or any other entity or service. Examiner Cain will explain that this technology makes it harder for providers to share user information from their services with law enforcement authorities.

c. Examiner Cain will testify about how group chats are set up and administered on the Telegram application and will walk the jury through what group chats look like and how to read them. Examiner Cain will explain that, if one joins a Telegram group chat after it was created, one will not see the prior chats and will only be able to see the chats from the point that person joined, going forward. Examiner Cain will explain how chats can be deleted on Telegram group chats and by whom. She will testify that the version of the Telegram app may affect how chats can be deleted on Telegram group chats and by whom.

d. Examiner Cain will also testify what the WhatsApp application is and how it works.

e. Examiner Cain will provide testimony about Google Voice and explain that Google Voice is a free telephone application that provides calling, text messaging, and voicemail. Examiner Cain will testify that Users must provide a valid phone number during registration. Once setup is complete, users are assigned a dedicated Google Voice number, which they can select from a variety of area codes.

f. Examiner Cain will explain that, by convention, many cellular telephone service providers, cellular telephone manufacturers, and social media and e-mail providers save their records and data using a twenty-four hour clock similar to "military" time and based on the 0° longitude meridian, also known as the "Greenwich meridian." Universal Coordinated Time ("UTC" or "UTC+0") refers to the time on that zero or Greenwich meridian. To convert UTC+0 time into local time here in the United States, one needs to subtract a certain number of hours from UTC depending on how many time zones away one is from Greenwich, England. Examiner Cain will explain that for the period of November 2020 through January 2021, Eastern Standard Time was five hours behind UTC+0 and referred to as UTC-5; Central Standard Time was six hours behind and referred to as UTC-6; Mountain Standard Time was seven hours behind and referred to as UTC-7; and Pacific Standard Time was eight hours behind and referred to as UTC-8.

g. Examiner Cain will offer some background testimony on how, generally, a forensic examiner can determine if and when data was deleted from a device or account.

III. Forensic Imaging/Data Extraction for the Relevant Devices and Online Accounts:

a. Examiner Cain will testify about, among other things, the forensic images and/or data extractions that he (or other law enforcement personnel) created of the electronic devices described above; methods used to confirm that the images were reliable copies of the original devices (for example by comparing hash values, where appropriate); the extractions of data from and searches of those images; and the tools and techniques used. For example, we anticipate she will testify that she and her colleagues used, among other tools, Cellebrite and Magnet. She will also testify about the difference between a logical versus a physical copy and the ability to recover and identify deleted files.

b. Examiner Cain will also explain the extraction reports that were generated for the cellphone extractions.

IV. Analysis and Verification of Data From the Relevant Devices

a. Examiner Cain will also testify about how she analyzed or reviewed the data extractions that she (or others law enforcement personnel) created, and identified specific files that had been recovered from the various devices. This will include specific files he observed on these devices such as e-mail messages, e-mail and e-mail headers, text messages (to include iMessages, WhatsApp, and Telegram messages), voice messages, photographs, videos, and phone logs. She will also testify about the tools and techniques she used. For example, we anticipate that, for the cell phone extractions and analyses, she will testify that his colleagues and he used, among other tools, Cellebrite and Magnet hardware/software. These files have been produced to you in discovery, and copies of the data extractions and forensic images have also been produced to you in discovery.

V. Lamond's Device

a. Examiner Cain will testify that Lamond's device contains Telegram user account: 'BikNBil' (869476955). This account contains two Telegram contacts with the display name 'Enrique Tarrio': username 'bannern****' with phone number

17869616789 and Telegram ID 1150826464; and username 'NobleLead' with phone number 13057668213 and Telegram ID 581632416.

b. Examiner Cain will testify that 'BikNBil' is a member of the group chat 'Christian Nationalists' (formerly 'PROUD GOYS'), iOS group ID(s) 9928549958 and 1338615366. This chat contains thirty-three (32) messages from 'Enrique Tarrio' (581632416) and one (1) message from 'Enrique Tarrio' (1150826464) , all posted on 11/09/2020. There are two secret chats between BikNBil' and 'Enrique Tarrio' (581632416). The first chat begins on 12/18/2020 and contains remnants of deleted chat ID 14483375238. The contents of the nineteen (19) recovered messages are identical to the messages found in the secret chat on Tarrio's device. The attachment secret-file-5156987684941463853-1 is an audio file from Tarrio in this chat, however the corresponding message record could not be recovered. Examiner Cain will testify as to reasons why certain records could not be recovered.

c. Examiner Cain will testify that the second secret chat, ID 14667027830, contains messages from 01/07/2021 to 01/27/2021. The final messageID for 'Enrique Tarrio' is 28 and the final messageID for 'BikNBil'' is 36, indicating that the secret chat contains a minimum of sixty-four (64) messages. Of these messages, only fifty-eight (58) messages were fully recovered. The attachment secret-file-4902515399548993725-1 is an audio file from Tarrio in this chat, however the corresponding message record could not be recovered. Examiner Cain will testify as to reasons why certain records could not be recovered.

d. Examiner Cain will testify there is one incoming Telegram call on 01/09/2021 lasting approximately twenty five (25) minutes. Examiner Cain will testify as to why the call was likely initiated through the secret chat and why it was - by design - assigned a message ID in the private cloud chat.

VI. Tarrio's Device

a. Examiner Cain will testify that Tarrio's device contains two Telegram user account(s): 'DeathFromAbove' (1150826464) and 'NOBLE LEAD' (581632416). Both accounts contain Telegram contact 'Shane FBI Police' with phone number 2024370434 and Telegram ID 869476955.

b. Examiner Cain will testify that the 'DeathFromAbove' account shows that 'Shane FBI Police' joined group 'Christian Nationalists' (formerly 'PROUD GOVS'), iOS group ID 9928549958, on 11/9/2020 21:44:02 (EST/EDT).

c. Examiner Cain will testify the 'NOBLE LEAD' account contains two chat threads with 'Shane FBI Police'. The first chat is a private cloud chat containing seventy-nine (79) messages, ranging from 07/03/2020 through 12/17/2020. The second chat thread is a secret chat (E2E encryption) beginning 12/18/2020 and ending 01/04/2021. The final messageID for 'NOBLE LEAD' is 52 and the final messageID for 'Shane FBI Police' is 93, indicating that the secret chat contains a minimum of one hundred and forty-five (145) messages. Of these messages, only forty-four (44) messages were fully recovered. Examiner Cain will testify as to reasons why certain records could not be recovered.

d. Examiner Cain will further testify that there are two Telegram calls on 12/20/2020 and 12/30/2020 lasting approximately seven (7) minutes and fourteen (14) minutes, respectively. Examiner Cain will testify as to why the call was likely initiated through the secret chat and why it was - by design - assigned a message ID in the private cloud chat.

e. Examiner Cain will provide testimony that Tarrio's Device contains Google Voice phone number 3057668213 and shows activity from January 2020 to January 2021. All calls are configured to forward to 7869616789, which matches the phone number for Tarrio's Device. Forensic Examiner Cain will testify that between 02/10/2020 and 07/04/2020, there are fifty-six [56] messages and five [5] calls between 3057668213 and 2024370434.

VII. A list of cases in which, during the previous four years, the witness has testified as an expert at trial or by deposition:

a. *United States v. Ethan Nordean, et al.*
b. *United States v. Christopher Worrell*
c. *United States v. Elmer Stewart Rhodes III, et al.*

Transcripts of Examiner Cain's testimony have been provided for your convenience in Attachment C.

VIII. Bases and Reasons in Support of Testimony

a. The bases and reasons for Examiner Cain's anticipated testimony is her training and experience, education, and review of the facts and evidence provided in discovery in this case, including, but not limited to:

   i. Law enforcement reports produced in this case;
   ii. Cellebrite and similar forensic reports produced in this case;
   iii. Data extractions of electronic devices.

I had read and approve of the above statement:

Jennifer Kathryn Cain
Federal Bureau of Investigation, Senior Digital Forensic Examiner

ATTACHMENT B

JENNIFER KATHRYN CAIN

SENIOR DIGITAL FORENSIC EXAMINER, FEDERAL BUREAU OF INVESTIGATION
1501 DOWELL SPRINGS BLVD. KNOXVILLE, TN 37909 | 813.[redacted].[redacted] | [redacted]@FBI.GOV

EDUCATION

UNIVERSITY OF SOUTH FLORIDA

Tampa. FL | 2017
MS in Cybersecurity
Concentration in Digital Forensics

UNIVERSITY OF NORTH CAROLINA

Chapel Hill, NC | 2003
BS in Business Administration
Kenan-Flagler Business School

CERTIFICATIONS

GIAC Adv Smartphone Forensics (2023)
FBI Senior Forensic Examiner (2022)
GIAC Battlefield Forensics (2020)
FBI Forensic Examiner (2019)
CompTIA A+ (2019)
GIAC Forensic Examiner (2018)
AccessData Forensic Examiner (2018)
FBI Digital Extraction Technician (2017)
FBI CART Technician (2017)

VENDOR TRAINING

SANS Advanced Smartphone Forensics
Magnet Forensics: Advanced iOS Exams
Magnet Forensics: MacOS Exams
Magnet Advanced Computer Forensics
Magnet Axiom Forensic Fundamentals
Magnet Axiom Examinations
SANS Battlefield Forensics & Acquisition
SANS Mac & iOS Forensic Analysis & IR
SANS Windows Forensics Analysis
BlackBag Essential Forensic Techniques
AccessData Intermediate OS Artifacts
AccessData Web Artifacts
AccessData Windows Forensics & Tools

FBI TRAINING

CART Senior Moot Court
Analog Forensics
Enhancing Your Forensic Skills
CART Moot Court
Digital Forensic Examiner Capstone
Cyber BootCamp
Mobile Forensics
Linux Command Line Interface
File Systems Basics

FBI INSTRUCTOR

Incident Response, Acquisition, & Analysis
Digital Forensic Field Operations

PROFESSIONAL EXPERIENCE

SENIOR DIGITAL FORENSIC EXAMINER | FEDERAL BUREAU OF INVESTIGATION

Knoxville, TN | July 2017 – Present

Conduct forensic examinations of digital evidence for the Computer Analysis Response Team (CART). Participate in search and seizure operations, identifying, diagnosing, and correcting problem conditions to aid in the retrieval of data in complex situations. Perform technical analysis on digital evidence and prepare authoritative oral and written reports to investigative team. Complete routine application testing and validation on vendor software.

STAFF OPERATIONS SPECIALIST | FEDERAL BUREAU OF INVESTIGATION

Tampa, FL | Feb 2013 – July 2017

Performed tactical analysis for the Field Intelligence Group, specializing in violent crime and organized criminal activity threats. Conducted operational research and performed data exploitation and analysis to support analytic and investigative strategies. Collected, analyzed, and integrated raw data into comprehensive intelligence packages. Awarded 2017 Intelligence Professional of the Year.

SYSTEMS ANALYST | JOHNS HOPKINS MEDICINE ALL CHILDREN'S HOSPITAL

St. Petersburg, FL | Nov 2010 – Feb 2013

Served as a database administrator. Conducted system analysis projects including requirements definition, design, development, and implementation per the system life cycle methodologies and standards. Created and executed system test plans by defining test conditions, scenarios, and expected results. Participated in installation of software updates to ensure completion of expected results.

SYSTEMS ADMINISTRATOR / BUSINESS ANALYST | PMSI

Tampa, FL | Jun 2009 – Nov 2010

Maintained, troubleshot and provided technical support for database applications. Performed User Acceptance Testing (UAT) and Quality Assurance (QA), and refined processes inside the system to automate process and functions. Designed database for the Centers for Medicare & Medicaid Services (CMS). Developed dashboards and reporting within the business intelligence portal.

OPERATIONS MANAGER | FOCUS INC

Tampa, FL | Feb 2007 – Jun 2009

Managed all product development activities for direct response marketing. Designed and managed database to track media planning and buying activities; and created automated reporting functions to show past purchase trends, detail historical performance behavior and predict future results.

JD POWER SYSTEMS ANALYST | LENNAR HOMES

Tampa, FL | Oct 2005 – Sep 2007

Designed and managed database to track all construction management activities including operational workflow, completion timelines, purchasing, and scheduling.

TRIAL EXPERIENCE

Expert Witness | District of Columbia

United States v. Christopher Worrell | Apr 2023
United States v. Ethan Nordean et al. | Feb 2023
United States v. Elmer Stewart Rhodes, III et al | Nov 2022

ATTACHMENT C

- - -

KATHRYN CAIN, WITNESS FOR THE DEFENDANT, SWORN

DIRECT EXAMINATION

- - -

BY MR. CRISP:

Q Good morning, ma'am.

A Good morning.

Q If you could please state your full name and city and state of residence?

A Jennifer Kathryn Cain and Knoxville, Tennessee.

Q And by whom are you employed?

A The Federal Bureau of Investigation.

Q And what do you do for them?

A I am a senior digital forensic examiner.

Q Is there a nickname for that?

A We go by FE for forensic examiner. And we work on the Computer Analysis Response team, which is commonly referred to as CART.

Q And, ma'am, I'm going to anticipate, if you can adjust the mic a little bit or slide up a little bit, I'm having a little hard time hearing you. I don't know if the rest of them are. And I apologize.

So, thank you.

What do you do? I understand the title, but what exactly do you do so we understand specifically how you operate?

A Sure.

I handle all aspects of digital evidence, including the identification and collection of it, the acquisition and extraction of digital evidence, processing those extractions into meaningful formats, and then analyzing the data and preparing reports.

Q And what type of training, education did you receive in order to obtain the position you hold?

A To become a forensic examiner, it takes roughly two years and about 400 hours of formal training.

We go through all type of technical and computer examination and mobile forensic work to include file systems and learning how to extract and process data.

From there, we roughly complete about 100 hours of advanced formal training each year after that.

Q And do you have a bachelor's degree?

A I do.

Q In what?

A Business administration.

Q Any advanced degrees?

A I have a master's in cybersecurity with a concentration in digital forensics.

Q Have you testified in court before?

A I have not.

Q All right.

And you would label your area of expertise in digital forensic extractions?

A In digital forensic extractions and processing and analysis.

MR. CRISP: Okay.

Your Honor, I don't believe the government has an objection, but I will move to admit her as an expert in this area.

MS. RAKOCZY: No objection to qualifying her in the area of forensic cell phone examination and digital evidence examination.

THE COURT: Okay.

So Ms. Cain will be so qualified as an expert in those areas.

BY MR. CRISP:

Q So, ma'am, I want to direct your attention to this case.

You conducted certain extractions from phones in this case?

A Some extractions and some I processed.

Q Okay.

And, again, so the jury understands, the distinction between an extraction and a processing, what comes first?

A First we extract the phone, which means to make a copy of the data that is contained on that device.

The second component is processing that data into a meaningful and useable format for our investigative teams to review.

Q What are the various programs that you would use to do that?

A For extracting, the most popular programs and the ones used in the case today were Grayshift's GrayKey and Cellebrite.

Q Is there also another one that was used in a few of them such as Axiom?

A That was used to process the devices. The second component to turn those extractions into meaningful data, yes.

Q So the extraction, if I can make an analogy, and if I am inaccurate please correct me, is pulling the data out of the phone in a way that you can view it in a readable format?

A That is correct.

Q Okay.

And then the processing of it would be putting it in a format that is actually readable to someone such as me?

A Yes, you could, similar to drawing blood -- someone's blood and then using that blood sample to read the certain indicators inside of it.

Q The first extraction program that you referenced GrayKey, is that used more specifically for a different -- for certain types of operating systems?

A Typically, we use it for iPhone extractions.

Q And why is that?

A It does an excellent job of obtaining an image of that device.

Q And is it also usable for android devices?

A It is in certain cases, yes.

Q Okay.

And I believe you said you have done digital extractions. Does that also include computer hard drives?

A It does.

Q All right. And there's a difference in extracting information from a computer hard drive from a cell phone; is that fair to say?

A That is fair.

Q And what are those differences?

A Well, when you look at a computer, we can actually remove the hard drive from those and keep everything powered off and make an actual bit-for-bit copy of that hard drive.

When we interact with mobile devices, the device has to be on and connected to one of our machines so that the data -- so that the tool used to extract the device is actually interacting with that phone in order to get the extraction of the phone.

Q So specifically as to some of the phones you've looking at, did you -- and I'll list a number of defendants here, individuals here, I should say, in this case. Did you look at Mr. Harrelson's phone, Ms. Watkins' phone, Mr. Caldwell's, Mr. Rhodes', Mr. Greene's, Ms. SoRelle's?

A Yes, all of those.

Q Okay.

And for clarity's sake, you either processed and extracted or -- I'm sorry, extracted and then processed -- or simply processed someone else's extraction?

A Yes, that is correct.

Q Okay.

Is it normal to rely in your line of work upon the extraction of another individual and then process that?

A Yes, it is.

Q Okay.

And you all use the same standards and systems?

A Yes, we do, we have the same standard operating procedure.

Q Now, I want to talk would you -- and if we can pull up what's been admitted into evidence as Government Exhibit 6740.

Ma'am, do you need some water while testifying?

A I'm good. Thank you.

Q Okay.

While we're waiting for that, I'll jump around here a little bit.

During the course of your work on this case, did you compile what's called an amalgamated report?

A I did.

Q Okay.

And an amalgamated report is what?

A I took -- for a specific requested chat, I took that chat and found it across several different devices and put that in one report so that it was all easily accessible in one location.

Q All right. Ma'am, what are we looking at here on what's been marked as Government Exhibit 6740.

MR. CRISP: And if we can -- do you know if this has been entered so we don't have issues with publishing it?

MS. RAKOCZY: I don't have an objection to publishing, Your Honor, but could we just briefly chat on the phone.

(Bench conference)

MS. RAKOCZY: Your Honor, my apologies. I am not certain that this witness has an ability to opine about call detail records, which the exhibit that we're looking at right now is about, so I'm just -- I'm not sure that a proper foundation has been laid for her to opine about call detail records which come from cell phone companies and are normally interpreted by an expert from the FBI CAST department or their cell site cell phone record experts.

MR. CRISP: Judge, I'll lay the foundation. I discussed this with her, so I can certainly lay a foundation as to how and why she's able to do that.

THE COURT: Okay.

(Open court)

BY MR. CRISP:

Q So, ma'am, I want to talk about something called CDRs. Are you familiar with them?

A Yes, I am.

Q Okay. And what does CDR stand for?

A Call detail record.

Q And what is it?

A They are essentially exactly what they sound like, call detail records provided by any given cell phone provider.

Q Okay.

And during the course of your work when you'd conduct an extraction and then process it, are you -- what do you pull from there? And if I may lead a little bit just to try and speed this along.

Do you pull things like voice detail records, text records, things -- or text messages, things like that?

A We do pull call logs and text messages from the extractions, yes.

Q All right.

So when you get call logs and you -- let's say, for example, you were to compare a call log from an individual A's phone versus individual B's phone and one shows a communication between one phone and the other, that doesn't -- it doesn't show up on the second phone. Do you use things like CDRs to reconcile those differences?

A Potentially as requested by the investigative team.

Q Okay.

So are CDRs things upon which you have relied on at times in the course of your work in conducting your extractions and processing?

A I have seen them.

Q And are you familiar with them and have you looked at CDRs in this particular case?

A I have looked at some of them.

Q Okay.

And have you looked at the CDRs for both Ms. -- I'm sorry, Ms. Watkins and Mr. Caldwell?

A I have.

MR. CRISP: Okay.

And, Your Honor, at that point I believe that based on that, I've laid a sufficient foundation and would submit that she can speak to this document.

MS. RAKOCZY: No objection to talking about this document, but I'm not -- I may have an objection when we go further.

THE COURT: Okay. See where it goes.

MR. CRISP: Thank you, Your Honor.

BY MR. CRISP:

Q So, ma'am, do you see what's on the screen marked as 6740?

A I do.

Q Okay.

And what are we looking at, to your understanding?

A It looks like a summary of call detail records.

Q Is this something that you have seen before?

A I have.

Q All right. Fair to say you and I have gone over this?

A We did.

Q All right.

And I want to direct your attention to the discussions on the bottom block which lists Caldwell, Watkins, Donovan Crowl, Paul Stamey, specifically if we can -- starting at the second column -- I'm sorry, second row, sorry, I'm not terribly accurate here.

At 1/6 at 5:04, there's a call between Caldwell and Watkins. Do you see that?

A I do.

Q All right. And then I'll have you go down to the row here at 2:08, I want to focus on those series of phone calls.

Now, did you find evidence of those phone records in the extraction from Ms. Watkins' phones?

A I did.

Q Okay. Which ones?

A The call at 5:04, the call at 5:43, 6:49, and 2:08.

Q Okay.

So I'm clear, you did not find any evidence of a call at 10:04, 10:44, and 10:54 correct?

A Correct. In Eastern Standard Time.

Q Right.

And just so we're clear, when you conduct an extraction, you always perform that extraction in UTC?

A I do, yes.

Q Why?

A It is a -- it is the universal standard and almost are data is stored in UTC, so it's simply easier to keep that standard, especially when you're comparing multiple devices going across multiple time zones.

Q Okay.

Now, in Mr. Caldwell's CDR -- did you review his CDR?

A I did.

Q Did you find evidence of the calls listed at 10:04, 10:44, and 10:54 in his CDR?

MS. RAKOCZY: Objection.

THE COURT: Basis?

MS. RAKOCZY: Foundation.

(Bench conference)

MS. RAKOCZY: Your Honor, my only concern with this is that I know that she says she sometimes looks at CDRs but she is not an expert in CDRs. She does not have the familiarity with how the different cell phone providers keep their records, et cetera.

So I think it's a little bit unfair to show this witness some records without having her be an expert or having her had done the actual work that a CAST analyst would do, to ask her what call detail records show to try to seek her -- you know, put the imprimatur of an expert witness on examining call detail records when she's not been qualified as an expert as such.

MR. CRISP: It sounds like weight versus admissibility to me, Judge. I think I could ask her that.

She's looked at it. She can speak quite intelligently to a lot of these CDRs and has with me. I think the government can explore that on cross-examination.

THE COURT: If it's something she uses in her work and has used in her work, I don't know whether -- did she compile this report or no?

MS. RAKOCZY: No, Your Honor.

THE COURT: Okay.

In any event, she's testified she's looked at them as part of her work, and so I think she can testify.
Ms. Rakoczy, if on cross-examination you want to make clear she's not an expert and doesn't have specific knowledge, that's fine, and obviously, Mr. Crisp, you can do that in direct examination if you want to as well.

MR. CRISP: Thank you, Judge.

(Open court)

THE COURT: The objection will be overruled.

BY MR. CRISP:

Q So, ma'am, I believe I asked you did you find evidence of those calls in Mr. Caldwell's CDR?

A I can't recall in his CDR. I know I found records of them in his phone extraction.

Q Okay.

In his phone extraction or her phone extraction?

A Both.

Q Okay.

So when you say -- you're talking about the 10:04 or the 5:04?

A Well, since this has been standardized to Eastern Standard Time, in Eastern Standard Time records of 10:04 -- sorry, 5:04 Eastern Standard Time.

Q All right.

And would seeing Mr. Watkins -- I'm sorry, Mr. Caldwell's CDR help refresh your memory as to that, or are you clear that there were no records in Eastern Standard Time of a 10:04 call from Caldwell to Watkins?

A I believe his CDR matched exactly what was in his phone extraction.

Q Okay.

And that was what, the four calls we referred?

A The four calls we've referenced.

Q Okay.

A None in the 10:00 a.m. Eastern Standard Time.

Q All right.

And then I want to talk a little bit about --

Again, his CDR only had four calls between the two of them, is that fair to say?

A It included at least those four calls, yes.

Q On the date, time in question, so between the hours of 5:00 a.m. and 2:08 p.m., Eastern Standard Time, fair to say there were only four calls that you saw records of in the extraction?

A Yes, there was actually one more that is not listed on this exhibit.

Q Okay.

And what was that?

A I believe it was also in the 5:00 a.m. time frame, either slightly before or slightly after 5:43 a.m.

Q Okay.

So nothing in the 10:00 time frame, correct?

A Correct.

Q All right.

And when you conducted an extraction of Ms. Watkins' phone, did you see evidence of calls in the 10:00 time frame Eastern Standard Time?

A No, I did not.

Q All right.

When you looked at her CDR, did you see evidence of something in her CDR that would have implied a 10:00 call?

A There were line items for a 10:00 call.

Q Okay. Now, to be clear, while you rely on these CDRs, it's not something that you would put yourself out as an expert, correct?

A That is correct, I am not an expert in CDRs.

Q You use them to reconcile differences, however, correct?

A Yes, to validate the data in my extractions.

Q Now, when I brought this to your attention, was this the first time you had seen this discrepancy as to the respective CDRs and extractions?

A Yes.

Q Did you take time to review the CDRs and attempt to reconcile for your expertise why that would have occurred?

A I did.

Q Was there a phone number listed as -- on the 10:00 ones?

And if we can pull up Watkins 52 for the witness only, please.

Are you able to see that, ma'am?

A Yes, sir.

Q Can you go to 3 of 13, please.

And back to page -- yeah, there you go. 13.

In looking at this document, ma'am, what anomalies did you note as to why there may have been confusion as to whether or not there were calls in the 10:00 Eastern Time frame?

THE COURT: Mr. Fischer, I'm sorry -- I'm sorry, Mr. Crisp, could you just orient the jurors as to what this is.

MR. CRISP: Sure. I'm sorry.

BY MR. CRISP:

Q Ma'am, what are we looking at?

A These are the call detail records for Ms. Watkins' phone.

Q Okay.

And as it pertains to the issue of the anomaly as to the 10:00 phone calls, what did you discover?

A There are three calls in the 10:00 a.m. range that have a different number in the dialed digits column.

Q Now, in your experience, what does that mean?

A It could be that the call was routed through some kind of provider number.

Q Okay. And why would that happen?

A I honestly -- I don't know why calls are routed.

Q All right. You talked about historically, certain providers and cell phone providers had done this in the past, is that accurate?

A I have -- yes, I have seen that in the past.

Q Okay. And why have they done that -- why was it done in the past?

A The way cell phone technology used to work is that it would send a call through your home tower before it would hit the local tower near where you were.

It's been several years since I've looked at that. I'm not well-versed in it nowadays.

Q All right. So the phone number that you think may be a routing number, what is that number?

A (937) 727-9469.

Q Did you see evidence of that number in any of the extraction that you conducted in Ms. Watkins' phone?

A I did not.

Q Did you see any evidence of that number in Mr. Caldwell's CDR?

A I did not.

Q His phone extraction?

A I did not.

THE COURT: Sorry -- Mr. Crisp, I'm sorry, what was that number again?

MR. CRISP: It is (937)727-9469.

THE COURT: All right. Thank you.

MR. CRISP: And to be clear -- Your Honor, at the point I'm going to move to admit Watkins 52.

MS. RAKOCZY: No objection.

THE COURT: All right. Watkins 52 will be admitted.

(Defendant Watkins Exhibit 52 received into evidence.)

MR. CRISP: If we can publish that to the jury.

Thank you.

BY MR. CRISP:

Q So can an individual go in and delete a phone call from their phone?

A Yes, they can.

Q And if you delete a phone call from a phone, would it show up on an extraction?

A Potentially.

Q If I delete a phone call from my phone and you get a CDR of my phone, would that deleted phone call show up on the CDR?

A Yes.

Q Am I able, as a user, to go and delete records from the cell phone provider?

A No, you're not.

Q So regardless of what I do with my phone, a phone call is still going to show up on a CDR if it was made, is that fair to say?

A That's fair.

Q Okay.

And to be clear, all but one of these calls, as I see it, was made from Mr. Caldwell's phone to Ms. Watkins' phone?

A That is correct.

Q Okay.

And based on your expertise and knowledge and the extraction you conducted as far as both of these phones, is it fair to say you would indicate to a reasonable degree of forensic certainty that there were no phone calls made in the 10:00 time frame between these two phones?

A In comparing to the extractions, I would say that, yes.

Q Okay.

Any question about that?

A No.

Q Okay.

All right. I want to also, before we move on from that, I want to talk about the final call that was made at 2:00, around about 2:08, 2:07. What can you tell me about that call?

A It was noted in the extraction as being a missed call.

Q As a what, ma'am?

A As being a missed call.

Q Okay.

And how was an extraction able to say whether it's missed or not?

A If it actually has device connectivity and the user answers the call.

Q Okay.

So a missed call is, without being too redundant or obvious, is one that you call me, it rings, it rings, it rings, I never pick it up?

A That is correct.

Q And I want to pull up Watkins 13, please.

Just for the witness.

THE COURT: Mr. Crisp, how long do you anticipate direct examination will be?

MR. CRISP: I'm sorry, Judge.

THE COURT: How much longer for your direct?

MR. CRISP: If you want take a break now, we can.

THE COURT: That's what I'm trying to figure out.

MR. CRISP: Another 15, 20 minutes.

THE COURT: Why don't we take a quick break. I know our court reporter has been working since 8.

MR. CRISP: Roger that.

THE COURT: Let's take our morning break. It's 10:30. We will resume at 10:45. Thank you very much.

COURTROOM DEPUTY: All rise.

(Jury exited the courtroom.)

THE COURT: Ms. Cain, you can step down. I'll ask you not to discuss your testimony with anyone during the break. Thank you.

MR. FISCHER: Your Honor, could I, for the record --

THE COURT: Ms. Cain, you can be excused.

Be seated, everyone.

MR. FISCHER: For the record, now that Mr. Caldwell, we have rested, can I make a Rule 29 motion and for all the previous reasons or --

THE COURT: Sure.

MR. FISCHER: That are on the record and it's preserved, I just want to be clear.

THE COURT: Okay.

MR. FISCHER: Thank you, Your Honor.

THE COURT: Thank you, Mr. Fischer.

All right. Thanks, everybody. See you in 15 minutes.

(Recess from 10:31 a.m. to 10:46 a.m.)

THE COURT: Please be seated, everyone. Thank you, all.

Ms. Cain, come on back up. Thank you.

(Pause)

COURTROOM DEPUTY: Jury panel.

(Jury entered the courtroom.)

THE COURT: All right. Please have a seat, everyone.

Okay. Welcome back, everybody.

Mr. Crisp.

MR. CRISP: Thank you, Your Honor.

BY MR. CRISP:

Q Ma'am, are you able to see what is on the screen?

A I am.

MR. CRISP: And, Your Honor, for the record, this has been marked as Watkins 13. And I move for its admission at this time, please.

MS. RAKOCZY: No objection.

THE COURT: Watkins 13 will be admitted.

(Defendant Watkins Exhibit 13 received into evidence.)

BY MR. CRISP:

Q So, ma'am, is this a compilation of the call logs we discussed?

A It is, from the extraction.

Q Okay.

And I believe earlier you said that there are approximately five calls that you think occurred between those two individuals?

A Correct.

Q And does this accurately reflect the five calls that occurred?

A It does.

Q Okay.

So if I can shift a little bit, just for the witness, please, if we can have Watkins 5.

And, Your Honor, I do not intend to admit this report. This is just for edification.

Now, the amalgamated report that we discussed, what did you do and how did you compile that?

A I'm sorry, are we speaking about the Signal report?

Q Yes, ma'am.

A Okay.

I was requested for one specific chat, to look on all of the devices that I examined and find where that chat appeared across the devices.

And then on every device it appeared on, I combined that into one report so that the entire chat was in one location.

Q All right.

And so my understanding is that there were approximately four phones with which you did this, right?

A I did.

Q And it would have been in Kellye SoRelle's Stewart Rhodes', Michael Greene's, and Mr. Harrelson's, who's first name is escaping me right now, I apologize, but --

A That is correct.

Q And there were no records as it relates to Mr. Harrelson's phone.

A No. The group chat was on his device but there was not content.

Q Okay.

I apologize.

So there were no input from him on the chat?

A Yes, his membership -- listed his membership on that chat in his phone.

Q And is that why, as far as this amalgamated report, you really only see three participants.

A That is correct.

Q And what I would like to do now is show you Watkins 8, please.

Now on the screen is Watkins 8.

MR. CRISP: And, Your Honor, for --

THE COURT: Mr. Crisp, I'm sorry to interrupt.

I don't think I heard her identify which Signal chat she did this for. Did she --

MR. CRISP: Which chat group?

THE COURT: Yes.

MR. CRISP: Fair enough, Your Honor. Thank you.

THE COURT: Could you just --

BY MR. CRISP:

Q Ma'am, let's clarify that. Which group did you do this amalgamated report for?

A I believe it was called "D.C. Op Jan. 6, 21."

Q Thank you.

Now, in looking at what's on --

MR. CRISP: Your Honor, I'm going to move for the admission of Watkins 8, 9, and 11. This is 8, so if I can do that upfront.

MS. RAKOCZY: No objection.

THE COURT: All right. 8, 9, and 11 will be admitted.

(Defendant Watkins Exhibits 8, 9 and 11 received into evidence.)

BY MR. CRISP:

Q Do you recognize Watkins 8?

A I do.

Q And is this essentially an extraction from what we looked at earlier of Watkins 5?

A Yes, it is.

Q Okay.

So essentially we've cut and pasted sections of that entire report for efficiency purposes?

A That is correct.

Q All right. If this is not published to the jury, if we could please do so.

I want to go over what the columns are marked as.

So "source" column means what?

A That is the device owner of the phone that this line item was taken from.

Q Okay.

So the first one says "source," and there you have "Greene." Is this Mr. Greene's phone?

A That's correct.

Q And the second one, so that would have been Rhodes' phone and SoRelle's phone, right?

A Yes, sir.

Q Let's jump over to "remote party name." What does that connote?

A That corresponds with the remote party column and that is the sender of any particular message on here.

Q All right.

Let's talk about some distinctions between and the application Signal. You're familiar with that?

A I am.

Q And how are you familiar with that?

A I routinely see it as on all of my -- on many of my cell phone extractions that I do.

Q When it's on an Apple phone versus an Android phone, are there differences in how you're able to -- how you extract that information, how you compile that information and so on?

A There are differences.

Q Can you tell the jury what those are, please, and why.

A The main difference is the database that actually houses the information corresponding to these Signal messages in an iPhone, the generic date field is the date the message was sent.

In an Android database for Signal, the generic date field is the date the message was received.

Q So did Mr. Rhodes and Ms. SoRelle have an iPhone?

A They did.

Q Did Mr. Greene have an Android or iPhone?

A He had an Android.

Q So as to the point you discussed earlier, if you have a person from an Android phone sending to an Apple phone and you do an extraction, and in the Signal app, let's assume it's all through Signal, at 1:00, when would the Android sender show the sent time?

A 1:00.

Q When would the Apple recipient show the receipt time?

A 1:00.

Q Now, do we know, based on how this is done, whether or not the Android phone -- I'm sorry, the Apple phone actually received it at 1:00?

A No, we don't. This is just the sent time of the message.

Q Let's turn it around.

Apple sender at 1:00, Android recipient.

The sent time for Apple sender would be 1:00, right?

A That is correct.

Q What time would the Android recipient show in receipt time?

A The actual time that that message was received.

Q Okay.

So Android -- and as to how this is -- these extractions are done through Signal with Androids, you can show with greater specificity, shall we say, in using an Android phone in terms of send and receive times?

A Assuming that you have the sent time from another location, yes, from another source.

Q All right.

So if the Android recipient didn't receive it until 1:10, that would actually show up on this kind of extraction as 1:10?

A That is correct.

Q Okay.

And in this particular case, do you see any discrepancies between send receipt times between the receivers and senders?

A I do not.

Q Okay.

And as to Mr. Greene, we indicated he is an Android user so it's fair to say that when Mr. Rhodes sent the message, "Correction. That's C Street," so on at 11:35, and this is all in Eastern Standard Time?

A This is, yes.

Q Did you convert that from UTC to Eastern Standard?

A My report was in UTC, but I confirmed that what you have shown me here was correctly converted into Eastern Standard Time.

Q So simultaneous send/receipts fair to say?

A Yes.

Q We can have -- I'm sorry.

One moment, Judge.

Watkins 9, please.

Now, have you seen this exhibit as well?

A I have.

Q And same thing here, these are copies of or cut and pastes from your report?

A Yes, with the timestamp converted to Eastern Standard Time.

Q Roger.

Okay.

Now, let's go with the first one with Greene, it's from Rhodes, so it's Stewart -- I'm sorry, it is

Michael Greene's phone with the sender being Stewart Rhodes in the first row, yes?

A Yes.

Q And here you have "Pence is doing nothing as I predicted."

The receipt time for Mr. Greene is reported as 1:36, is that accurate?

A Yes, it is.

Q Do we know when Mr. Rhodes sent that?

A If you look further down on Rhodes' -- where Rhodes is the sourced device, that same message is on the first line and it's 1:25:41 p.m.

Q And Ms. SoRelle has the receipt date as 1:25 as well, right?

A Her time stamp date, that is the date that -- because she has an iPhone that is also the date the message was sent.

Q We don't know if she actually received it at 1:25?

A Not on this report, no.

Q Is there a way of actually making a determination as to when she would have received it?

A At this time, none of the tools available to us parse any other date other than these generic time stamps. It is possible that we could have created a custom-coded solution to potentially pull those dates out if they were available in the database. I do not know if they are.

Q Okay.

Now, can you tell me why there would have been an approximately 11 minutes and few odd seconds delay between the send/receipt between Mr. Rhodes and Mr. Greene?

A There are a couple of different potential reasons. The first reason being if the phone was powered off or in airplane mode and it wasn't connected to any network, then the application obviously couldn't receive any messages at that time.

The second explanation is if his phone was powered on but say perhaps he had turned off the ability for the app to refresh in the background so, which means that if the app is not actively open, it isn't actively reaching up to the server and pulling down those messages.

And then in that case, you would need to actually open the Signal app in order for it to sync and bring down those messages.

The third is that potentially the notifications were turned off on the device and that device refresh was off, and so those two kind of align in that the messages would not be received until the user opened the Signal app on their device.

Q Is network delay also a possible reason?

A It is, yes.

Q As we sit here right now, there's at least four reasons why there would have been a delay in the receipt from -- to Mr. Greene?

A That is correct.

Q In all of those instances, however, just so I'm clear, what we can definitively say from this is that you can say Mr. Greene would not have seen that message in the first row until 1:36 Eastern?

A That is correct.

Q Now, these discrepancies that are listed later in the rest of the remaining phone conversations are also consistent with your report?

A They are.

Q Okay.

Now, let's go down to the third one that's from Whiplash, it says, at 2:14, "They have taken ground at the Capitol." That is his send date because he's sending the message, correct?

A That is correct.

Q And Mr. Rhodes has that time receipt as what time?

A Well, he has his generic time stamp, which on the iPhone is time sent as the same time, which is 2:14:43 p.m.

Q And that is because that's going to reflect, as we said earlier, sent date, not necessarily receipt date?

A Correct.

Q All right.

If we can go to Watkins 11.

Now, Watkins 11, as you'll see here in a moment, ma'am, is the report that we discussed earlier that deals with a large chunk of messages that have a two plus hour delay.

And we'll probably have to blow that up a little bit so if we can do that.

So what we're looking at here are the first party here, the sending party -- or the source phone is going to be Mr. Rhodes on the first block, is that fair?

A That's correct.

Q And then if we can scroll down to the bottom block, please, and this is going to be Mr. Greene.

So if we can scroll back up to Mr. Rhodes' messages, here you have messages that he is showing having been sent in the 2:41 through 3:31 time frame. Is that correct?

A That is correct.

Q If we can scroll down to Mr. Greene's phone, please.

And these are the same messages but these are showing a receipt date of approximately anywhere from two plus hours upwards of three hours' difference?

A That is correct.

Q Correct? Okay.

Now, in your review of Mr. Greene's phone, if we could scroll back up to Mr. Rhodes' time frame, you recall -- do you recall seeing messages that Mr. Greene was either sending or receiving from other parties in the 2:40, 2:41, 2:45 time frame?

A I do.

Q And he was, to your recollection, receiving messages from others intermittently in that same time window.

A He was.

Q So what does that tell you?

A The most likely explanation is that the Signal app was open during that time.

THE COURT: I'm sorry, was what? I didn't hear her.

THE WITNESS: Was open during that time.

BY MR. CRISP:

Q And he was using it, right?

A And he was using it.

Q So the likely explanation as to why he's not receiving these messages from Mr. Rhodes would either be a send delay from Mr. Rhodes or just a network busy issue overall?

A That is correct.

Q Okay.

MR. CRISP: The Court's indulgence one moment, Your Honor.

BY MR. CRISP:

Q Ma'am, I'm sorry, I was reminded I forgot to ask something on Watkins 9.

If we can pull that up real quickly.

All right, ma'am, I want to direct your attention to -- if we can go to Mr. Rhodes as a source phone and it's going to be the one -- third row, this is where Mr. Rhodes is asking Whip, "What's your location, I'm trying to get to you," and that was from him, right?

A That was from Mr. Rhodes, yes.

Q And it was sent then to, do we know who?

A The entire group of the "D.C. Op Jan. 6, 21."

Q When can we tell when Mr. Greene received that message?

A According to his device, Mr. Greene received that message at it 2:24:21 p.m.

Q All right. So we're talking a difference of about 18 minutes or so, yes, before Mr. Greene actually saw that message?

A Yes.

Q All right.

MR. CRISP: Ma'am, I don't have any additional questions.

Thank you, Judge.

THE COURT: Thank you, Mr. Crisp.

MR. CRISP: I believe government counsel does.

THE COURT: All right.

MS. HALLER: With the Court's indulgence, we would just have a few questions on direct. Just one moment.

THE COURT: Any objection?

MS. RAKOCZY: In light of expediency, Your Honor, no.

THE COURT: Ms. Haller, do you have questions?

MS. HALLER: Yes, Your Honor.

- - -

DIRECT EXAMINATION

BY MS. HALLER:

Q Good morning.

A Good morning.

Q I'm Juli Haller, and I represent Kelly Meggs in this case, and I'm sorry I've lost my voice a little bit so just bear with me.

(Pause)

Forgive me.

If we can just go over some of the chats. You said that you helped doing the analyzing data based off of the cell phones.

As for the chats, did you review the "Old Leadership" chat as one of the chats in this case?

A I did extract data containing that for the "Old Leadership" chat. I'm not too familiar with the content inside that chat.

Q Okay.

But when you extracted data, do you recall whether or not you checked for when various defendants sent their last message?

A I did prepare a report that said certain key individuals and certain group chats, when they did have the first and last message, yes.

Q Okay.

I'm going to show what I think that report might be.

A Okay.

Q And you tell me --

Just for the witness if that's --

So this did have a Government's Exhibit number, but we're going to call it KM79 at this time.

And just to show it to the witness.

Ms. Cain, would you be able to identify this document where it's about defendants' entry to and exit from key Signal chats?

A Yes, this is my report.

MS. HALLER: At the time, we would like to move in Exhibit 1 -- or KM79, please. And publish it to the jury.

MS. RAKOCZY: No objection, Your Honor.

THE COURT: KM79 will be admitted.

(Defendant Exhibit KM79 received into evidence.)

BY MS. HALLER:

Q Going down to the pink section where it says Kelly Meggs, would it be correct to say that the last message from Kelly Meggs in what's called the "Old leadership" chat is 12/18/2020?

A That is correct.

Q Okay.

And as for his other chats, looking at the "D.C. Op Jan. 6", what time or what's the date of his last known message?

A January 8th, 2021.

Q And -- thank you.

Looking at the "OK FL D.C. Op Jan. 6" chat, what does it say for the date or what did you determine to be the date of his last known message?

A His last known message was January 7th, 2021.

Q And looking at the -- sorry, I can't see what the -- the OK FL hang out, what did you determine to be the last date of his message?

A January 7th, 2021.

Q Thank you.

And the last one "Vetted OK FL hangout" chat, what did you determine to be his last message?

A January 20th, 2021.

Q Okay. Thank you.

And then the only --

Okay. So now looking at what we would, just for the witness, show -- what we would mark as KM80. And if we can just show the witness -- thank you.

Looking at this excerpt from a cell phone -- can we make it a little bigger -- I'm not sure --

Would you be familiar with what these individuals called themselves, their monikers?

A I know that Mr. Meggs is OK Gator 1.

Q Okay.

And I'm showing you an excerpt from -- would you be able to identify from the visual whether it's an iPhone or Android?

A Not from this visual, no.

Q Okay.

Did you review Isaac's phone as a way to extract a chat which was the "OK FL D.C. Op Jan. 6" chat?

A I did not review Mr. Isaacs' phone.

Q Oh, okay. So you didn't extract?

A I did not.

Q Okay. And then you will not -- you wouldn't be familiar with Isaac' phone at all?

A That is correct.

Q Okay.

MS. HALLER: Then that is all I have. Thank you for your time.

THE COURT: All right, Ms. Rakoczy.

MS. HALLER: Thank you, Your Honor.

THE COURT: Thank you, Ms. Haller.

- - -

CROSS-EXAMINATION

BY MS. RAKOCZY:

Q Good morning, Examiner Cain. How are you?

A Great. Thank you.

Q I just have a few questions for you this morning.

I'd like ask you a couple of questions about what Mr. Crisp asked you about with respect to call detail records that you looked at.

Could you just explain the difference between call record data that you see on a phone versus call record data that you get from cell phone providers?

A Sure.

When we look at a phone extraction, all of the messages that are -- that come to that phone, either sent or received or missed and that you can visibly see on the interface of that device, that would be something that would be available in a phone extraction.

Call detail records come from a phone provider and they detail any call that actually goes through one of the cell towers on their system.

So, for instance, if I say I called someone and they look at their phone and they do not see that call, maybe they're in airplane mode, maybe for some other reason, and they can't see that on their actual phone, then that call would be not be reflected on the extraction but it could be on the provider's records.

Q Okay.

Now, when you're looking at the data on someone's actual phone or device, is it possible for the user of the device to delete the record of a phone call from their phone?

A It is.

Q Is it possible for them to delete it from the records that the phone companies keep?

A To my knowledge, it is not.

Q Okay.

Let's talk about Signal, the Signal app. Can you make calls through the Signal app?

A You can.

Q And could that data -- would that data be stored by a person's phone?

A It would.

Q Could the user of the phone delete a record of a Signal call that had been made on their phone?

A They could, yes.

Q Now, would the cell phone companies keep a record of a call made through the Signal app?

A No, they would not.

Q So is it fair to say if you and I had a Signal call and I deleted the record of that from my phone, there wouldn't also be a record of that that the cell phone providers would have, correct?

A There would not be a record.

Q There would be no record of that call, correct?

A Correct.

Q How about with are there other apps on people's cell phones that people can use to make calls?

A There are.

Q And can people go into their phones then and delete the record of those communications?

A Yes, you can.

Q And would the cell phone providers have any record of those communications through apps?

A No, they would not.

Q If we could talk a little bit now about the questions you were asked about the analysis you performed of this "D.C. Op Jan. 6" Signal chat, you were talking a little bit about the difference between the way that Android phones store the timestamp on messages versus iPhone messages.

Can you remind us again just what it means when you say that an Android phone has received a message?

A Sure.

It is the time that the message actually leaves the Signal server and hits that device.

It could be, like we said earlier, dependent on several factors as to when it hits the device, but it's when that device receives it and is notified that there is a message.

Q Okay.

And you testified on direct examination that there were some differences between the time that certain messages were sent by, say, Stewart Rhodes' phone and when they were marked as having been fully received by the Michael Greene phone. Do you remember that?

A That is correct.

Q Could we bring up the screen Watkins Exhibit 8, please.

Do you see Exhibit Watkins 8 on the screen now?

A I do.

Q Now, these were two messages that were originally sent by the Stewart Rhodes phone; is that correct?

A That is correct.

Q Okay.

And is it fair to say that these two messages that Mr. Rhodes sent were both received by Mr. Greene's phone at the same time they were sent?

A Yes, it is, that is correct.

Q Okay.

So no delay at all on these two messages?

A Correct.

Q That's including a message that Mr. Rhodes sent at

2:43 p.m. saying, "Come to the south side. Just left of dome"?

A That is correct.

Q Okay.

If we could take that down, please. Thank you.

Could we bring up Watkins Exhibit 9.

Now, these are a few messages that were sent by both Mr. Rhodes and Mr. Greene's phone in the period of roughly 1:25 to 2:15 p.m. or 2:24 p.m.; is that right?

A That is correct.

Q Okay.

So the first message I think that we're talking about is "Pence is doing nothing as I predicted"; is that right?

A Yes, it is.

Q And that was a message that Mr. Rhodes' phone sent?

A Yes, it is.

Q And Mr. Rhodes' phone suggests that he sent that message at 1:25 p.m., is that right?

A That is correct.

Q And this exhibit is in Eastern Time, right?

A It is.

Q And you triple-checked that and made sure that it really was 1:25 p.m. Eastern Time?

A I did.

Q Okay.

And that message was received by Mr. Greene's phone at 1:36 p.m., correct?

A That is correct.

Q And so just a nine-minute delay; is that right?

A Yes, ma'am.

Q And the fact that we have that timestamp of 1:36 p.m., that means that the phone got it at that point, right?

A Yes, ma'am.

Q Okay.

And then the next message we're talking about was sent by Mr. Rhodes' phone at 1:38 p.m.; is that right?

A That is correct.

Q And that was the message "All I see Trump doing is complaining. I see no intent by him to do anything. So the patriots are taking it into their own hands. They've had enough"?

A Correct.

Q Okay.

And that was also sent at 1:38 p.m. Eastern, right?

A Yes, ma'am.

Q Okay.

And that was received by Mr. Greene's phone, according to the records at the top, just four minutes later, right?

A That is correct.

Q Okay.

And then Mr. Greene's phone is the next one, I think, to send messages, at about 2:14 and 2:15 p.m.; is that right?

A That's correct.

Q And you told us on direct that the fact that we're seeing these red received times on Mr. Greene's phone relatively close in time to when they were sent, Mr. Rhodes' messages, that means that it appears as though Mr. Greene has the app open and is using it, right?

A That's correct.

Q And so then at 2:14 and 2:15 p.m., Mr. Greene's phone says, "They've taken -- they have taken ground at the Capitol. We need to regroup any members who are not on mission," correct?

A Yes, ma'am.

Q And we can't really tell exactly when Mr. Rhodes and Ms. SoRelle's phone received that because they're Androids, right?

A IPhones, yes.

Q Or iPhones, sorry. Thank you for correcting me.

The last message in this is then the message that Mr. Rhodes sends at 2:15 p.m.; is that right?

A Yes, ma'am.

Q And that's when he says, "I'm on the Supreme Court side of the Capitol. Whip or Landon, where are you," right?

A Yes.

Q And Mr. Greene's phone, it looks like he gets that no later than nine minutes later, is that fair?

A That's correct. That is correct.

MS. RAKOCZY: Ms. Rohde, we can take that one down.

Can we bring up Watkins 11, please.

BY MS. RAKOCZY:

Q Now, these are a series of messages that were sent by Mr. Rhodes entirely, right, are these messages sent by Mr. Rhodes' phone?

A Yes.

Q Okay.

And these were sent, it looks like between 2:41 p.m. Eastern time and 3:30 p.m. Eastern Time, fair to say?

A Yes, ma'am.

Q And you checked these as well and these are all the correct Eastern Time timestamp that Mr. Rhodes' phone sent these messages?

A Yes, ma'am.

Q Okay.

Now, we see that Mr. Greene's phone doesn't show a received time for these messages until like the 5:30, 5:45 p.m. time frame; is that correct?

A That's correct.

Q But we do not have those corresponding messages that Mr. Greene is sending in this time period, right?

A Not on this report, no.

Q Okay. So you can't say one way or the other -- well, let me ask you this.

Isn't it true that it could be the case that Mr. Greene had his app closed and that's why he's not getting these messages?

A It could be, yes.

Q Okay.

So we don't know that there was some kind of a delay causing these messages to be -- to show a 5:00 p.m. receipt date, right?

A Correct, we do not know the reason for the delay.

Q Okay. So we can't really tell anything about why Mr. Greene's phone is getting these messages later, correct?

A Correct.

Q Okay.

Thank you, Ms. Rohde. If we could take that down.

We then were -- you then were in the looking at, when Ms. Haller was asking you questions about an exhibit that you made that I think was Watkins or Mr. Meggs' 79. Do you remember that?

A Is that the Signal membership chart?

Q When people came and left chats?

A Yes, ma'am.

Q Okay.

Could I have the Court's indulgence one minute.

MS. RAKOCZY: If we could bring up on the screen and publish, I believe we're now looking at the exhibit that Ms. Haller was just showing. I think it's KM79.

BY MS. RAKOCZY:

Q Do you see this chart, Ms. Cain?

A Yes, ma'am.

Q Okay.

And this is something you prepared; is that right?

A It is.

Q Okay.

If we could just zoom in on the peach or pink colored series of rows that say "Kelly Meggs."

Okay. So these are some chats that defendant Kelly Meggs was a participant in; is that right?

A That is correct.

Q And it's the "Old Leadership" chat, "D.C. Op Jan. 6, 21," "OK FL "D.C. Op Jan. 6," "OK FL

Hangout," and "Vetted OK Hangout:; is that right?

A That's correct.

Q Okay.

Now, you have at first the first row is -- says "joined chat," is that right?

A That is correct.

Q What does that mean?

A When you become a member of a Signal group, Signal stores a membership list of that group on their server.

When your device connects to that group, it sends down a realtime version of that membership list.

So if I create a group at 1:00 and there are five members on it and then another member joins at 2:00, there would be a refresh of that membership group, both at 1:00 and 2:00. So it is continually refreshing its membership list when you open that app.

Q And then I see you also noted when you saw or when the first known message was sent by Mr. Meggs in each of these chats, is that right?

A That's correct.

Q And so sometimes I see, like in the third column for the "OK FL D.C. Op Jan. 6" chat, I noticed that you put an "unknown" for the join-chat date. Why did you put that there, if you remember?

A I was not able, across any of the devices, to find an incoming membership list that noted when he entered that chat, which just shows that it was -- he likely entered it before any of my extractions also joined that chat.

Q Okay.

But you did note that the first message that you saw Mr. Meggs' phone sending to this chat was on January 2nd of 2021; is that correct?

A That's correct.

Q Okay.

So now can you explain to us the last two rows, the last known message versus the last known membership?

A Yes.

The last known message is exactly what it sounds like, the last message that Mr. Meggs sent in participation with that group. It's the last message that he posted in that group chat.

The last known membership is based on those membership lists.

So, for instance, that same chat that you were talking about, OK Florida D.C. Op January 6th, in that third column, it says down there that Mr. Meggs is still a member at the time of the Stone extraction.

So Mr. Stone's device was extracted in December of 2021. He still had that Signal group present on his device and was still receiving regular membership updates to that group list at that time.

Mr. Meggs was still showing up in his member list as a member of that group at that time.

Q If you don't have someone's phone, can it be challenging to say with certainty when for sure they left a Signal group chat?

A It can be, yes.

Q And if you have someone's device but they've deleted Signal content or some Signal content from their phone, can that make it challenging to know when they left or whether they left a Signal group chat?

A It can make it challenging, yes.

Q Did you look at the data from Kelly Meggs' cell phone?

A I did.

MS. HALLER: Objection, Your Honor; outside the scope.

THE COURT: It's overruled.

BY MS. RAKOCZY:

Q I'm sorry, what did you say about whether you looked at his phone?

A I did look at Mr. Meggs' data.

Q Okay.

And did you notice whether there was any Signal data on that phone?

A The Signal application was installed on his device, and there were messages; however, they were very limited, there was not many of them at all, and they were much later in the course of 2021.

Q And do you recall that you found that the Signal data, in fact, had sort of -- did not exist prior to some date in January of 2021?

A That is correct, there was not data from January 2021.

MS. RAKOCZY: Thank you, Your Honor. I have no further questions.

THE COURT: Okay. Mr. Crisp, any redirect?

MR. CRISP: I do, Your Honor. If I may have the Court's indulgence real quick, please.

- - -

REDIRECT EXAMINATION

BY MR. CRISP:

Q Ma'am, I'm going to throw a little bit of curveball here because I didn't expect to have to go down this road here, but I am going to show you what's been marked as --

Sorry, I'm getting different marching orders at the moment.

Let's start with 6740, please.

And then have Watkins 13 in conjunction with that, please.

So, ma'am, what I want to make sure about is, you see the two exhibits?

A I do.

Q All right. On your left, this is published -- these are already admitted so they should be published -- on the left is going to be what is Government 6740, on the right is going to be Watkins 13. Is that correct?

A That's correct.

Q Okay.

Now, what I want to make sure we're clear about here is when you're looking at the CDRs, okay, you had testified earlier both on direct and on cross, that an individual cannot delete phone calls from a CDR?

A That is correct.

Q All right.

And when you looked at Mr. Caldwell's CDR, did you see any call to that 937 number that you kind of referred to as a ghost number?

A I did not.

Q And Mr. Caldwell had Signal on his phone, right?

A I do not recall if he had Signal on his device.

Q Did you look at his extraction?

A I did.

Q All right. So you have no reason to believe that when we talked about whether or not you had ever seen that phone number, that you had ever seen that on Mr. Caldwell's phone?

A I had never seen that phone number on his phone.

Q Okay.

Did you ever see that phone number that you referenced as a ghost number -- and when I saw ghost, that's essentially a routing number, right?

A Well, it was a number that it was not identifiable to me, I don't know the source of that number.

Q To your understanding based on the CDR and based on the extractions, do you have any reason to believe that it was actually a legit number that was ever dialed?

A It would not appear so, no.

Q Okay.

So the likelihood that it was a number that was either in a Signal app based on your review of all the records in this case is extremely row?

A It is. Signal records do not appear on call detail records.

Q But Signal, if you have it on your phone, is still visible, right?

A It is still visible.

Q And if you have it on your phone and it hasn't been removed, you're still going to see the numbers that have been called?

A That is correct.

Q Okay.

And I want to just, there's one final thing as to Government's 6740, at the phone call that took place at approximately 2:08:25. I'd like to compare that to Watkins 13.

The actual length of that call was approximately what, do you know?

A According to the extraction, it was a missed call so the length was zero.

Q Okay.

So it wouldn't have been a 26-second phone call, would it?

A No, it would not have.

Q Okay. Thank you.

So, ma'am, we're going to have to go through this somewhat methodically, but I'm going to show you what's been marked as Watkins 10 alpha through 10 Charlie, so 10A, B, C.

Let's start with 10 alpha, please.

Now, again these are extractions or these are copies of the extractions in similar format as the earlier exhibits?

A Yes.

Q All right.

And do you remember discussing with me yesterday the issue of how we could determine whether or not an individual was able to receive messages during a time period if you can cross-reference it from send receipts from other parties?

A I believe so.

Q Okay.

And if my question is unclear, I'm kind of winging it here, so I apologize, if you don't understand, I'll try and rephrase it.

So, for example, there's a question about whether or not Mr. Greene had his phone open or on or the app open in that two to three-hour window that a glut of messages was received at the 1730 or 5:30 p.m. time frame, right?

A Yes.

Q If the individual is receiving messages from other parties at 2:41, 2:42, 2:43, what would that tell you?

A It would indicate that the app was most likely open.

Q Okay.

If we can go down to, I believe it is 10 Charlie.

Yeah, I think we're just going to have to stick with one at a time, please.

But I don't believe the government objects to its admission?

MS. RAKOCZY: No objection.

THE COURT: 10 -- Watkins 10A, B and C will be admitted.

(Defendant Watkins Exhibit 10A, B and C received into evidence.)

BY MR. CRISP:

Q Again, we are looking at essentially the same format, extraction from the amalgamated report you conducted?

A Yes.

Q Okay.

Do you remember me going over some of these messages from third parties to Mr. Greene's phone?

A Yes.

Q Do you remember seeing these messages from -- and again, so third column is listed as remote party?

A That is correct.

Q Which means what?

A That is the person sending the message.

Q Okay.

And first column is, we know this is Mr. Greene's phone because that's the source phone, right?

A That's correct.

Q All right.

And what are you able to tell me from this report?

A That his device was receiving messages between the first and last timestamp, 2:58 and 3:12 p.m.

Q Okay.

So can we say whether or not his phone was on?

A His phone was on.

Q Can we say whether or not he had the notifications -- well, whether the app was open?

A Um --

Q During this time period?

A It is likely that he had the app open, however, he could have had the app closed and had the background refresh happening even if the app was closed down.

Q In that event, would the messages that came in at 17:30 would also have hit in this time period, too, correct?

A One would think so.

Q And barring a network delay?

A Correct.

Q Okay.

But if he's receiving messages from some other parties and it's refreshing in this 2:58, 3:12, 3:12 window, the messages that had been sent at 2:41 from the earlier chat we looked at would have hit in this window as well?

A They could have. They did not.

Q And the likely explanation is a network delay?

A Yes.

Q Okay.

MR. CRISP: Your Honor, we're going to pull up Watkins 9, please.

BY MR. CRISP:

Q All right.

And, again, just for expediency purposes, first block is Mr. Greene's phone, right?

A Yes, sir.

Q All right.

And he is sending messages, there's two messages he sent at both the 2:14 at 2:15 time frame, right?

A Yes, there are, yes.

Q All right.

And from that, you're able to determine that he was actually utilizing the app or somebody or some entity was utilizing the app from his phone?

A Yes.

Q Okay.

So if he's sending a message at 2:15, he should have received the message from Mr. Rhodes that was sent at 2:06, right, at 2:15, if it were anything other than a network delay?

A That's a reasonable conclusion, yes.

MR. CRISP: Thank you, ma'am. No further questions.

might go longer than the government expects. I expect, particularly with that witness, to go quite a while.

THE COURT: Okay.

(Jury entered the courtroom.)

THE COURT: Thank you. Be seated. Thank you for your patience.

Ms. Hughes.

MS. HUGHES: The government calls digital forensic examiner, Katherine Cain.

THE CLERK: Please raise your right hand.

KATHERINE CAIN,

called as a witness, being first duly sworn, was examined and testified as follows:

THE WITNESS: I do.

THE CLERK: Have a seat.

THE COURT: All right. Welcome. Remove your mask if you're comfortable doing so.

Ms. Hughes, ready when you are.

DIRECT EXAMINATION

BY MS. HUGHES:

Q. Good afternoon. Could you please introduce yourself to the ladies and gentlemen of the jury by stating and spelling your full name?

A. Jennifer Katherine Cain, C-A-I-N.

Q. Where do you work?

A. For the Federal Bureau of Investigation.

Q. What is your title?

A. I am a senior digital forensic examiner.

Q. In which section?

A. I am a part of the CART team, which stands for Computer Analysis Response Team.

Q. How long have you been with the FBI?

A. Next month will be ten years.

Q. What are your duties as a CART examiner?

A. We handle all types of digital evidence, which is any kind of electronic storage media, to include laptops, computers, mobile devices, tablets, and anything that can store data for any of those systems.

Q. What is your educational background?

A. I have a degree from the University of North Carolina, Chapel Hill in business and a master's in cybersecurity with a concentration in digital forensics from the University of South Florida.

Q. What kinds of trainings are you required to do to become a CART examiner with the Federal Bureau of Investigation?

A. Sure. Our original process is a two-year process in about 400 hours of classroom and hands-on instruction, and then after we are certified, we have about a hundred hours of additional training we have to complete each year.

Q. Do you conduct any trainings, Examiner Cain?

A. I do.

Q. What trainings?

A. I teach our new examiners in training. I teach incident response and digital -- digital forensic fundamentals, sorry.

Q. Have you been qualified as an expert in federal court?

A. I have.

Q. In which jurisdiction?

A. The District of Columbia.

Q. And have you been called by an expert by the defense?

A. I have.

Q. In connection with this matter, were you asked to examine several mobile devices, seized from multiple defendants and subjects?

A. I was.

Q. And as part of your analysis, were you asked to determine if the Signal application was presently located on any given device?

A. I was.

Q. Did you examine an iPhone associated with Joseph Hackett? And this is government's -- for identification, this is Government's Exhibit 66.

A. I did.

Q. Did you examine a Motorola cell phone associated with David Moerschel? And again, this an identification number of

Exhibit 130.

A. I did.

Q. And did you examine a Motorola Moto cell phone associated with Edward Vallejo? And this is government's identification Exhibit Number 210.

A. I did.

Q. For each of these three devices, did you look to see if Signal was still on the phone?

A. I did.

Q. What was your conclusion?

A. Signal was not present on any of the devices.

Q. Now, did you also examine a device associated with an individual named Roberto Minuta?

A. I did.

Q. From looking at that phone, when could you tell the phone was set up?

A. The phone artifacts suggest on or around February 20th of 2021.

Q. And for January 6, 2021, what does that mean for the Signal messages that would have been sent in January of 2021?

A. It would not be possible for them to be present on that phone.

Q. And so for any messages that were sent in the January 2021 time frame, they would not be on the phone that you examined in connection with Mr. Minuta?

A. That is correct.

Q. Okay. So we're going to focus on the three phones then, the cell phones from Mr. Moerschel, Mr. Hackett, and Mr. Vallejo.

Before we talk about each of these phones in depth, what, in general, do you do when you extract the data from a phone?

A. So we have a variety of commercial tools available to us. So the first thing we look at the device is, we manually review it and determine the best tool. We then extract the information off of that device, so that we can look at a copy of the phone itself without having to constantly look at the phone. And then we process that information into a meaningful way and provide reports.

Q. What is Signal?

A. Signal is an encrypted chat application. You can download it for your mobile device, iPhone and Android, and your desktop computer, and it -- you are able to microphone calls, video calls, and send messages, both privately and in a group scenario.

Q. What does a Signal extraction look like and the data you would review from a phone?

A. It's a database. They store all their information in the database.

Q. And if Signal on a device has been deleted, what does that mean in terms of the data that would be stored in your Signal -- in your Signal profile?

A. When you remove the Signal application from your phone, the database is also removed entirely from that phone.

Q. So there's no data that's stored say in the cloud?

A. That is correct.

Q. Let's turn first to your examination of the iPhone associated with Mr. Hackett. First of all, what was the iPhone that was associated with Mr. Hackett?

A. It was an iPhone 6S Plus.

Q. And was Signal on that phone, that iPhone 6S Plus?

A. No, it was not.

Q. Were you asked to review iCloud search warrant returns in connection with this phone?

A. I was.

MS. HUGHES: If we could please bring up just for the witness, Government's Exhibit 9705. And if we could just zoom in on the top, please.

Q. (BY MS. HUGHES) Is this a fair and accurate version of some of the cells and rows that were in that search warrant return?

A. It is.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9705.

MS. HALIM: No objection.

THE COURT: 9705 will be admitted.

Q. (BY MS. HUGHES) Okay. So first, what are we looking at here, what is this chart?

A. This is -- it comes straight from Apple. It is related to Mr. Hackett's Apple identifier, and this particular spreadsheet are update and redownload data details for two different applications.

MS. HUGHES: Okay. And if we could just zoom in on the top here, Ms. Badalament, thank you.

Q. (BY MS. HUGHES) Okay. So you said update and download details. Is that what it says here: Report description, update and redownload details related to DSID?

A. Yes.

Q. What is a DSID?

A. That is the identifier that Apple internally assigns to someone when they sign up for an iCloud account.

MS. HUGHES: Okay. If we could zoom out, please.

Q. (BY MS. HUGHES) Now, the left-hand column --

MS. HUGHES: If we could just zoom in on this column to begin with.

Q. (BY MS. HUGHES) What is this global unique ID?

A. That is an identifier for Mr. Hackett's iPhone.

Q. The physical iPhone?

A. The physical iPhone.

Q. Does this global unique ID correspond with the physical iPhone? And that would be, for identification purposes, Government's Exhibit 66, the physical phone that you examined, does that relate to the phone?

A. It does.

MS. HUGHES: If we could please zoom out. And, Ms. Badalament, if we could now focus on this section, and just for Signal, please. So -- sorry. Thank you so much.

Q. (BY MS. HUGHES) Okay. So these entries, are there dates and times that are associated with specific update and download entries?

A. There are.

Q. And what is the general date range of these update and download entries?

A. Around, it looks, August 2020 through January 2021.

Q. And what does it say in terms of the content, what is the application that is being updated, what does this column correspond to here?

A. Signal private messenger.

MS. HUGHES: If we could please zoom out, thank you, Ms. Badalament.

Q. (BY MS. HUGHES) Are there, in fact, two phone numbers that are connected with Mr. Hackett?

A. There are.

Q. Why are there two numbers associated with Mr. Hackett?

A. When we looked at his Signal username, he actually has two accounts registered with Signal.

Q. And what do you attribute to there being these two phone numbers? Are there two phones?

A. No. One of the phone numbers is for the actual iPhone that we have, and the other phone number is a Text Me phone number.

Q. What is Text Me?

A. It's a third-party application that you can download to your Android or iPhone device, and it enables you to create a second phone number that you can then use on that same device.

MS. HUGHES: If we could please bring up what's already been admitted into evidence Government's Exhibit 2426. If we could zoom at the top here. Thank you, Ms. Badalament.

Q. (BY MS. HUGHES) What is this document?

A. This is a return from the Text Me company, attributed to the account associated with Mr. Hackett.

Q. And what is the username on this account?

A. John Willow 232581.

Q. And this e-mail, johnwillow23@protonmail.com have you seen this e-mail elsewhere?

A. I have.

Q. Where did you see this e-mail?

A. Proton Mail was an application on that same iPhone, and this was the account associated with it.

Q. And for the user information for the Text Me, what is the model associated with this account?

A. IPhone 6S Plus.

Q. And what is the date of activation?

A. November 17th, 2020.

Q. What was the withdrawal date?

A. February 6, 2021.

MS. HUGHES: And we can zoom out, thank you, Ms. Badalament. If we can go back now to 9705, which is already in evidence, and if we can now focus on the Text Me portion of these iCloud search warrant returns.

Q. (BY MS. HUGHES) So again, do these entries relate to the same global identifying number that we referenced previously that's associated with the device, Government's Exhibit 66?

A. It does, yes.

Q. And are these entries for the update and download entries associated with Text Me?

A. Yes, they are.

Q. What's the first entry associated -- the update associated with Text Me?

A. November 17th, 2020.

Q. And what was the date of the activation that was found in that user information from Text Me?

A. Also November 17th, 2020.

Q. In the course of your -- of this investigation, did you review whether or not Mr. Hackett, in fact, used Signal?

A. I did, yes.

Q. How were you able to determine that Mr. Hackett, in fact, had used Signal?

A. We had identified other devices in which Signal was present, and his name and username was a participant in those chats.

Q. And from your examination of these devices, were you able to summarize the groups and the messages that he sent to these various groups?

A. I was, yes.

MS. HUGHES: If we could please bring up just for the witness, Government's Exhibit 9700. And if we could go to page 2. Thank you, Ms. Badalament.

Q. (BY MS. HUGHES) Are these the summaries of his -- of Mr. Hackett's group membership that you were just discussing?

A. They are, yes.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9700.

MS. HALIM: No objection.

THE COURT: 9700 will be admitted.

Q. (BY MS. HUGHES) Starting with the first page, how did you compile this chart?

A. I -- we looked at Signal across other phone applications that still had the Signal chat app installed, and then looked for Mr. Hackett's phone number and the accounts, which then led us to the messages in these particular Signal groups.

Q. And what is meant -- there's a notation on this chart that says "source." What does source refer to?

A. That is the device containing the Signal chat application in which that message was present.

Q. So when you say, "First known message to this DC Operation Intel Team," the source from this is from Stuart Rhodes's phone; is that right, for that first row?

A. Yes, that is correct.

Q. And does this number here -- is this his Apple iPhone number, or is this his Text Me number?

A. That is his iPhone number.

Q. What was the first date of the message sent to Signal -- to a Signal group associated with his iPhone number?

A. July 25th, 2020.

Q. And this was to the OK FL Hangout?

A. Yes, ma'am.

Q. And what is the last date that a message was sent that you were able to find associated with this number?

A. January 20th, 2021.

Q. Is that for the DC Operation Intel Team?

A. Yes, ma'am.

Q. And was there anything -- did you have a chance to look actually at this message that was sent on January 20th?

A. I did. It was not actually a message sent by the user, it was an update to the account, and possibly just notated in that group.

Q. So what was the last message you saw that he sent that actually was -- included content?

A. November 17th, 2020.

Q. And this was to both the Grey Team OK FL and the OK FL Hangout?

A. Yes, ma'am.

MS. HUGHES: If we could please go to page 2 of Government's Exhibit 9700.

Q. (BY MS. HUGHES) What is this number associated with?

A. That's the Text Me number.

Q. And what is the first date of a number -- of a message sent using this number?

A. November 17th, 2020.

Q. And could you remind me, what was the date that the Text Me account was activated?

A. Also November 17th, 2020.

Q. What was the last date that a message was sent on using this Text Me number?

A. January 9th, 2021.

Q. And could you please read the groups that were associated with this Text Me number?

A. Sure. The Miami Rolling Stone OP, OK Florida, OK Florida Vetted Leadership, OK Florida DC OP Jan 6, OK SE Region Open Forum, OK FL Hangout, Vetted OK FL Hangout, Temp OK FL Leadership.

Q. Thank you.

MS. HUGHES: If we could please go now to Government's Exhibit 2413, already in evidence. If we could go to page 29, thank you, Ms. Badalament. And if we could just focus on this number here for a moment, the IMEI. Sorry, I can't see it. The IMEI, the number on the left.

Q. (BY MS. HUGHES) Did you have a chance to compare this IMEI number to the IMEI that is associated with the physical phone, Government's Exhibit 66?

A. I did.

Q. And are they the same?

A. They are the same.

Q. How did you compare these numbers?

A. The first 14 ident- -- numbers in this string, that comprises the mobile identity equipment number, and they match, they are a match.

MS. HUGHES: If you could zoom out, please, Ms. Badalament.

Q. (BY MS. HUGHES) And on Government's Exhibit 2413, page 29, does it appear that there are numerous entries in

January 2021 for calls using that physical phone?

A. Yes, there are.

MS. HUGHES: Okay. We can bring that down, thank you, Ms. Badalament.

Q. (BY MS. HUGHES) We're going to now talk about David Moerschel. Was Signal found on Mr. Moerschel's phone, the phone that you examined?

A. No, it was not.

Q. And that, again, is, for identification purposes, Government's Exhibit 130.

MS. HUGHES: If we could please just bring up for the witness, Government's Exhibit 9701. And there are three pages, Ms. Badalament, if you could just scroll through them.

Q. (BY MS. HUGHES) Is this, what you're seeing on your screen now, an excerpt of the Cellebrite report from Mr. Moerschel's phone?

A. It is, yes.

Q. And is this a fair and accurate excerpt of some of those entries?

A. Yes.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9701.

MR. WEINBERG: No objection.

THE COURT: Government's 9701 is admitted.

Q. (BY MS. HUGHES) Okay. So there was no Signal found on this phone; correct?

A. Correct.

Q. But were there Text Messages found on the phone?

A. There were.

Q. Starting on page 1, please, what is the earliest text messages you found on the phone?

A. August and October of 2019.

Q. And again, is this just a summary? Are there actually many, many, many more text messages?

A. There are. These are just the first.

Q. Okay. So August and October 2019 are the earliest ones?

A. Yes, ma'am.

MS. HUGHES: If we could please go to page 2.

Q. (BY MS. HUGHES) Are these the last messages you found on his phone?

A. They are.

Q. And what are the date of the last messages found on his device?

A. May 26, 2021.

MS. HUGHES: If we could please go to page 3.

Q. (BY MS. HUGHES) Does this focus on the time period of November to January, 2020 to 2021?

A. It does.

Q. What is the next message sent after November 13th, 2020?

A. January 16th, 2021.

Q. So where -- where were the messages between November 13th, 2020 and January 16th, 2021, were they on the phone?

A. There were no messages in that time frame.

Q. As with Mr. Hackett, for Mr. Moerschel, were you able to conclude that he was, in fact, a Signal user, that he had a Signal profile?

A. Yes.

Q. How were you able to determine that for Mr. Moerschel?

A. The other devices that we examined that contained the Signal application contained Mr. Moerschel's Signal identifiers, including his phone number.

Q. And did you again create a summary of the groups Mr. Moerschel was a member of?

A. I did.

MS. HUGHES: Could we please bring up just for the witness, Government's Exhibit 9701, page 4.

Q. (BY MS. HUGHES) And is this the summary you created in connection with Mr. Moerschel?

A. It is.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9701, page 4.

MR. WEINBERG: No objection.

THE COURT: 9701 is admitted.

Q. (BY MS. HUGHES) How many groups was Mr. Moerschel a member of?

A. Four.

Q. And what was the earliest message he sent -- pardon me, the earliest date he sent a message?

A. December 13th, 2020.

Q. And what was the last date we know he sent a message?

A. January 7th, 2021.

Q. And just to be clear, could there be messages we don't know exist?

A. Yes.

Q. So these are just the messages we know from the devices we have collected over the course of the investigation; is that right?

A. That's correct. That is correct.

Q. Now, how many groups was Mr. Moerschel a member of?

A. Four.

Q. And finally --

MS. HUGHES: You can bring that down, thank you, Ms. Badalament.

Q. (BY MS. HUGHES) Mr. Vallejo, was Signal found on Mr. Vallejo's Motorola Moto phone? That's Government's Exhibit 210.

A. It was not.

Q. What -- or how many groups was Mr. Vallejo a member of?

A. Just one that we found.

MS. HUGHES: If we could please bring up just for the witness, Government's Exhibit 9702, and for page 1, seeking to admit just page 1 at this time.

Q. (BY MS. HUGHES) Is this one of the messages you reviewed that Mr. Vallejo sent?

A. Yes, it is.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9701 [sic], page 1.

THE COURT: It will be admitted.

Q. (BY MS. HUGHES) Okay. So who -- first of all, you said that Mr. Vallejo was part of one group. What was that group?

A. DC OP Jan 6/21.

Q. And how did Mr. Vallejo -- what was his username? How would he appear if you were chatting with him on Signal?

A. Just as you see here, as Ed Vallejo.

Q. Is that a name that he would have given himself?

A. For this instance, yes, it is.

MS. HUGHES: If we could please bring up page 2 just for the witness. Apologies, page 3, Ms. Badalament, thank you.

Q. (BY MS. HUGHES) Is this how his username is associated with this phone in a cell phone extraction?

A. It is.

Q. Is this a fair and accurate excerpt from that extraction?

A. Yes, it is.

MS. HUGHES: My apologies, I believe I misspoke. I said 9701. This is 9702. My apologies.

The government seeks to admit and publish Government's Exhibit 9702, page 3.

THE COURT: Admitted.

Q. (BY MS. HUGHES) Okay. So you were just -- you were just describing how his username is associated with a phone number. Can you explain what we're looking at right now on 9702, page 3?

A. Sure. This is from a Signal database, and that database, inside it has a table that tracks all the identifiers associated with its users, and the full name, Ed Vallejo, is associated here with phone number 602-434-6843.

Q. Whose device was this from?

A. Mr. Rhodes.

Q. Stuart Rhodes?

A. Yes, ma'am.

MS. HUGHES: If we could please go just for the witness to Government's Exhibit 9702, page 2.

Q. (BY MS. HUGHES) In addition to Signal messages, did you also review Text Messages that were sent on that number, 602-434-6843?

A. I did.

Q. Did you notice -- or did you note the number of messages that Mr. Vallejo sent in any given month on that number?

A. I did, yes.

Q. And is this exhibit in front of you an accurate summary of those messages sent in 2019, 2020, and 2021?

A. Yes.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9702, page 2.

THE COURT: All right. 9702, page 2 is admitted.

Q. (BY MS. HUGHES) Focusing your attention on this time period, November/December/January 2020 to January 2021, approximately how many Text Messages were sent from November 2020 through January 2021?

A. Approximately 1,400.

Q. And why have we not reviewed -- we started by talking about Mr. Hackett's iCloud search warrant. Why have we not reviewed an iCloud search warrant in connection with Mr. Moerschel and Mr. Vallejo when analyzing their Signal usage?

A. Those two particular devices are Android devices, they are not iPhones, so they back up to their Google accounts. And Google just does not store the same types of data that Apple does. So whereas you can get Apple store data on any given device, that's just not available on the Google platform.

MS. HUGHES: And if we could back up just for a moment to Government's Exhibit 2414.1, page 11.

Q. (BY MS. HUGHES) Did you have an opportunity to compare this?

MS. HUGHES: And we're missing the top column, so if you could actually go to page 1 first, Ms. Badalament, my apologies, and just identify which row is the IMEI row. The IMEI row would be the row that is three from the right.

And we can now go back to page 11.

Q. (BY MS. HUGHES) Did you have an opportunity to compare whether this IMEI -- this IMEI corresponded with any of the physical phones that you examined?

A. It did.

Q. And which phone did this correspond with?

MS. HUGHES: My apologies, Ms. Badalament, you might have to zoom out. If you could just zoom in on just a small portion of it.

A. I'm sorry, I don't have them committed to memory as to which of the four devices.

MS. HUGHES: If we could go to the top of this exhibit.

Q. (BY MS. HUGHES) So this device -- we've gone through Mr. Hackett's. That was Government's Exhibit -- my apologies, 2413 was Mr. Hackett's. Were you asked to evaluate whether an IMEI corresponded with another physical device?

A. Yes, I was.

Q. Which device were you asked to correspond an IMEI with the physical device for?

A. With his iPhone.

Q. With whose iPhone?

A. Oh, Mr. Hackett.

Q. And this is a different exhibit. This is Government's Exhibit 2414. My apologies, they all look very similar.

A. Okay.

Q. There are two CDR records you were asked to look at and correlate with physical phones.

A. Yes.

Q. We've gone over Mr. Hackett's phone. Did you look at a different phone and compare it with the IMEI?

A. Yes, I did.

Q. Who?

A. Mr. Moerschel.

Q. Mr. Moerschel.

A. Yes.

Q. Now, going back to page 11, for this exhibit, this is Government Exhibit 2414 --

MS. HUGHES: If we could please go to page 11.

Q. (BY MS. HUGHES) Did there appear to be entries in the January time period that showed that this phone was indeed active, was making calls in the January time frame?

A. Yes, there are.

Q. And is this the same phone that you examined -- you examined the physical phone for?

A. Yes. The IMEIs are a match.

Q. In addition to looking at various text messages, did you also summarize how many -- just in terms of raw numbers, how many Signal messages Mr. Vallejo, Mr. Hackett, and Mr. Moerschel sent in these groups that you're able to identify?

A. I did.

Q. And did you create a summary chart summarizing those number of chats that were sent?

A. I did.

MS. HUGHES: If we could please bring up just for the exhibit [sic], Government's Exhibit 9704.

Q. (BY MS. HUGHES) And is this a fair and accurate representation of the summary you created?

A. It is, yes.

MS. HUGHES: Government seeks to admit and publish Government's Exhibit 9704.

THE COURT: All right. 9704 is admitted.

MS. HUGHES: Okay. If you could just zoom in on the chart itself, Ms. Badalament, thank you.

Q. (BY MS. HUGHES) Okay. So first of all, there are two entries for Mr. Hackett, one with the number ending in 9396 and one for an entry ending 2509. Does this refer to his iPhone number and then is Text Me number?

A. It does.

Q. How many messages approximately in total did Mr. Hackett send from July 25th, 2020 through January 20th, 2021?

A. Just under 400.

Q. And for Mr. Moerschel, for the time period of December 13th, 2020 through January 7th, 2021, approximately how many messages did Mr. Moerschel send?

A. 150.

Q. And for Mr. Vallejo, from January 5th, 2021 through March 7th, 2021, approximately how many messages did Mr. Vallejo send?

A. 140.

Q. And did you find any of these messages on any of the three devices you examined?

A. No, I did not.

MS. HUGHES: No further questions.

THE COURT: Okay. Any cross-examination?

CROSS-EXAMINATION

BY MR. WEINBERG:

Q. Good afternoon, how are you?

A. Great. Thank you.

Q. That was a lot of data?

A. Yes.

Q. All right. So you'll have to excuse me, I'm not very good with data, but I just have a couple questions. Okay?

Mr. Moerschel's phone is what kind?

A. It's a Motorola.

Q. Okay. Is it fair to say that that type of phone doesn't have a lot of memory compared to like, let's say, the iPhone 14?

A. They're all older devices, yes, so they're not as robust as today's devices.

Q. Okay. And you looked through the Cellebrite; correct?

A. I did.

Q. Okay. And in the Cellebrite, it has a list of all of the text messages and everything like that, correct?

A. It does.

Q. Okay. We can agree that in Mr. Moerschel's phone, he had numerous other gaps where text messages were not on his phone. Would you agree with that?

A. There were some other gaps where there were no messages.

Q. So we can agree that from 8/24/2019 to 9/28/2019, that's about a five-week period there were no messages besides two spam messages?

A. I don't recall that exactly, but that sounds logical.

Q. Okay. And then between 10/10/2019 and 5/22/2019, there are no messages besides four spam messages, correct?

A. I -- I don't remember the exact dates that there were no messages, but there were indeed time gaps like that, yes.

Q. Okay. So -- and there was also one more gap from 8/11/2020 to 9/23/22020, about a six-week gap where there are no messages on his phone?

A. Okay.

Q. Okay. So it's your understanding that he deleted those messages on those three other four- to five-week to six-week spans, is that --

A. They are not on the device.

Q. Okay. Then I do have a question about one of your exhibits. I think it was 9701.

MR. WEINBERG: Could we pull that up? I think it was page 4, maybe. Okay.

Q. (BY MR. WEINBERG) Just a quick question. This data, what time zone is that?

A. I believe this is in UTC.

Q. Okay. So for UTC, that would mean five hours back; is that right?

A. If we're comparing it to Eastern Standard Time, yes, sir.

Q. Okay. From like to --

A. From here, in D.C.

Q. Okay. All right. So that would mean -- I'm not very good at math, but at 14:35, that would mean five hours prior is when he left the group?

A. Is the last -- not necessarily when he left the group, but when the last --

Q. Message?

A. -- message that he posted to that group, yes.

Q. Okay. Great.

MR. WEINBERG: I don't have any other questions. Thank you.

CROSS-EXAMINATION

BY MS. HALIM:

Q. Agent, good afternoon. You have some familiarity with the Signal app; is that correct?

A. Yes, ma'am.

Q. All right. So if a person is on Signal and sends a message, and later decides that he or she wants to get rid of that message, there is a function where you can just delete an individual message; correct?

A. There is, as long as you're the creator of that message.

Q. If you're the creator, correct. So an author of a message could say go back a day, a week, or a month and say, I don't like that message, I'm going to delete that specific message?

A. Yes.

Q. And when that happens, you know from your review that what you then see on Signal, is you still see the person's name and it just says messages deleted; correct?

A. Yes.

Q. All right. Now, when you reviewed Mr. Hackett's messages from other people's -- from the Signal on other people's phones, never once did you see that in connection with a message that he authored; correct?

A. I didn't specifically look for that, so I can't answer to it.

Q. Okay. But you didn't -- you -- in preparation for your testimony, as the FBI agent who did the digital forensic analysis, you don't recall ever seeing that, do you?

A. I didn't specifically look for it.

Q. But what you did see, regardless of what you were looking for, what you saw, what you absorbed and observed, you did not see messages that were individually deleted by Mr. Hackett, what you saw?

A. No, I did not see on Signal the words, "This message has been deleted by the user."

Q. But you did see that in connection with other people, correct?

A. Occasionally, yes.

Q. Yeah, so you have seen it, as your job as the digital forensic examiner in this case, in this investigation, were individual authors did, in fact, delete specific messages?

A. Yes, ma'am.

Q. All right. Now, Mr. Hackett's phone was seized by the FBI on May 28th, 2021. Does that sound right?

A. That sounds accurate, yes.

Q. And so your examination couldn't have begun prior to May of 2021, right?

A. That is correct.

Q. And by the time --

MS. HALIM: Oh, thank you. Did you do this, Scott? Thank you so much.

Q. (BY MS. HALIM) By the time that you -- when you analyzed Mr. Hackett's phone, Signal, the application, was not on the phone at all, correct?

A. That is correct.

Q. Now, Signal is an application like many other applications that a person can have a smartphone, right?

A. Yes.

Q. And Signal's an application that only works on a smartphone, correct?

A. You can also download it for a desktop computer as well.

Q. A desktop computer, but not like an old decrepit phone?

A. Right. You have to have data and Wi-Fi capabilities, yes.

Q. Thank you.

Now, I'm going to be specific to iPhones, because that's what I know, okay. So if I were to go to my iPhone and if I had Signal on it, and I wanted to delete it, I would press and hold, right, and I'd get the little jiggly box with an X, right?

A. Yes, ma'am.

Q. I would press the X, correct?

A. Yes, ma'am.

Q. And then typically, a message is going to pop up, are you sure you want to delete this, yes or no, right?

A. Yes, ma'am.

Q. And then sometimes you would even get a second message, are you really, really sure, because if you delete this, it's going to wipe out everything, right?

A. Yes, ma'am.

Q. And then you say yes or no, correct?

A. Yes.

MS. HALIM: If we could -- Justin, could you please pull up Government's Exhibit 9704.

Q. (BY MS. HUGHES) This is the summary of the number of messages, correct?

And I see for Mr. Hackett, you have tabulated or counted a total of 390 messages sent between July 25th, 2020 and January 20th, 2021, correct?

A. January 9th, but yes, 2021.

Q. Well, if you look at that first one, the very first box, does it not say 1/20/2021?

A. Oh, I'm sorry, yes.

Q. So the all-encompassing dates for the two boxes that pertain to Mr. Hackett are from July 25th, 2020 to January 20th, 2021, correct?

A. Yes.

Q. And we don't have any information here as to when those 390 messages specifically were sent, correct?

A. Not on this slide, no.

Q. And to make it even more specific, we don't have the number of messages between November 3rd and January 20th, correct?

A. November 3rd, no.

Q. Right.

Did you look at any of the Signal messages? Was that something that you did as part of your role for the FBI?

A. Yes, it was.

Q. Do you recall a number of messages from Mr. Hackett to the effect of, Welcome, from Sarasota?

A. I do not.

Q. You don't recall that?

A. I don't --

Q. You don't recall to the tune of 50 or more messages, Welcome, from Sarasota?

A. I do not.

Q. Okay. Thank you, Agent.

MS. HALIM: I have no further questions.

MR. SHIPLEY: I have no questions. Thank you.

THE COURT: Okay. Mr. Peed.

MR. PEED: Your Honor, I have an objection. I want to have the witness testify about the total DC OP chat file, and the government's objecting, so I don't know...

(Bench conference on the record.)

THE COURT: Mr. Peed.

MR. PEED: I want to have the witness identify the total number of pages and the total DC Signal OP chat from Stuart Rhodes's phone, the page that Vallejo's first message appears on, and then the number of Vallejo messages between January 5th and January 8th, and the number of Vallejo messages between January 5th and January 20th, and the last Vallejo message date.

THE COURT: Okay. I can't hear you, Ms. Hughes.

MS. HUGHES: He can ask her is it fair to say x amount, date, but what he wants to have her do is a worksheet it looks like, and have her look at some document that's over 300 something pages, we cannot -- we don't know what this -- if his version compares to our version or what this is and to have to do this on the fly. So if he wants to ask those dates, I object to the worksheet exercise with this document that she's never seen before. We object.

MR. PEED: I believe this document is extracted from Stuart Rhodes's phone.

THE COURT: What are you going to ask her to do? Are you going to ask her to look through 300 pages and count up Mr. Vallejo's Signal messages?

MR. PEED: No, Your Honor. I'm going to ask if she's worked with this document and if she does the search function, then enter Ed Vallejo's handle. And then it will bring up all 144 messages. And then identify these dates, it should take about five minutes.

MS. HUGHES: She's not seen this document before. So if he wants to fill in the answers, the government does not have an objection, but doing this kind of worksheet format with something she's never seen before, is --

MR. PEED: I guess it's news to me that she hasn't seen this, because I thought this was from discovery.

MS. HUGHES: You sent me an e-mail with this document. I'm not sure what this is. And apologies, I have not had time to look through all 360 pages.

MR. PEED: So what I have is the DC OP chat pulled from what I believe is discovery, if she has not seen this document --

THE COURT: I'm still lost, what are you trying to accomplish with her with this 300-plus page document?

MR. PEED: The relative to the total what page of the document does Mr. Vallejo's first message come in. And then the number of messages she -- her chart only has from January 5th to the end. I want to establish how many messages between January 5th and January 8th, and then January 5th to January 20th, you know, key points in the time line --

THE COURT: How is she going to do that while she's standing there, is she just going to count up the number of messages looking page-by-page?

MR. PEED: We're going to do it together and she's going to create an exhibit --

THE COURT: No, we're not going to do that. You want to do that, you can call your investigator or somebody else on the stand to do that. We're not going to waste the jury's time while you try to create an exhibit on the fly. So you can do that in your own case, call your investigator who's going to do the same exercise and do it that way.

(The following proceedings were had in open court.)

MR. PEED: Can you pull up 9702, second page?

CROSS-EXAMINATION

BY MR. PEED:

Q. Okay. You went over these. This is the number of messages -- of SMS messages recovered from Mr. Vallejo's phone, correct?

A. That is correct.

Q. And could you just notate with the screen the messages in January of 2021?

A. 668.

Q. Okay. That number was greater than December and greater than in February, right?

A. That is correct.

Q. And the FBI was able to review or possess all 668 of those messages, right?

A. Yes.

Q. Because they were on Mr. Vallejo's phone when he gave his phone to the FBI, right?

A. Yes.

Q. Now, Mr. Vallejo's phone was searched by the FBI in June of 2021, correct?

A. I believe that is correct, yes.

Q. All right. And so that would be over five months after the events of January 6th, right?

A. Yes.

Q. Mr. Vallejo had a Moto E5 Cruise, correct?

A. That sounds correct, yes.

Q. And he was using that same Moto E5 Cruise up through the point where the FBI asked for it, correct?

A. That is my understanding.

Q. The same one he came with to D.C.?

A. Yes.

Q. And the same one he was using going back to 2019?

A. Yes.

Q. Right. That Moto E5 Cruise has a manufacturer or release date of -- has a general release date of July of 2018, correct?

A. That sounds accurate.

Q. And it's an Android 8 device, right?

A. I'm not sure of what operating system it was running, but it was running an Android operating system.

Q. Okay. It has a hard drive space of 16 gigabytes, right?

A. I'm not sure what the specs were on this particular phone, but that does sound accurate.

Q. Okay. It had RAM of -- 2 gigabytes of RAM, right?

A. Sure.

Q. Fairly cheap little phone, right?

A. I -- it's a smartphone. It is less expensive than some of its other counterparts, but I don't know how you classify cheap.

Q. I guess I'll put it this way, 2 gigabytes on an Android device is about the minimum you can have on it to run effectively in 2020, right?

A. Sure. Yes.

Q. The Android operating system takes up about 3 to 4 gigabytes on most phones, right?

A. I don't know.

Q. Now, you said that the Signal -- Signal is a phone app, right?

A. It is.

Q. And messages on Signal app can be stored on the user's device; they're not stored in the cloud, right?

A. That is correct, until the time move go through the Signal server until the time they are delivered to the device.

Q. Now, you said that -- I think the last question to you was did the FBI find Signal on any of the phones that we've been discussing, right?

A. Yes.

Q. Okay. Signal also has a desktop application, correct?

A. It does.

Q. And when a user downloads a Signal desktop application, they can sync it with their phone, right?

A. You can.

Q. Okay. When you sync it with your phone, the messages that are stored on your phone are then synced to your computer, right?

A. No, they are not. It's if you send a message from your phone, that message is on your phone, and if you send a message on your computer, that message is on your computer.

Q. But if you link it with a QR code, it will be synced between those devices, won't they?

A. To my knowledge, it does not sync the complete history of Signal. It could sync a particular set of data in the chat that you were discussing between the two devices.

Q. Okay. So if someone with -- syncs their phone to their computer or to the Signal desktop app, and they were in the DC OP chat, that chat group would appear on their Signal desktop app, correct?

A. Potentially. Parts of it could, yes.

Q. And the FBI did not search to see if Mr. Vallejo had these messages on a computer, for example, correct?

A. I was not involved with looking at his computer or even if he possessed one, no.

Q. All right. And you'd agree with me that if you have a phone with two gigabytes of RAM, and its memory is running out, it will run slower, correct?

A. Sure.

Q. And that deleting things will make it run more quickly, generally, right?

A. Sure. Yes.

Q. And Mr. Vallejo's last message was -- that you brought up, is March 7th, 2021, right?

A. For Signal?

Q. Yes.

A. Yes, if that's what I had on my chart, then yes.

Q. That is two months after January 6th, right?

A. It is.

Q. And there had been arrests in January 6 cases before then, correct?

A. Correct.

Q. There had been arrests of people we've heard names about like Mr. Caldwell, correct?

A. Correct.

Q. All right. And two months -- Mr. Caldwell was arrested in January of 2021, right?

A. I don't recall the date of his arrest.

Q. But before March 7th, right?

A. I don't recall the date of his arrest.

Q. Okay.

MR. PEED: No further questions. Thank you.

THE COURT: Redirect, Ms. Hughes.

REDIRECT EXAMINATION

BY MS. HUGHES:

Q. Ms. Badalament, if we could please begin -- you were asked a series of questions about Mr. Moerschel and how there were chunks of time that were missing in Mr. Moerschel's text messages out of his extraction. Do you remember those questions?

A. I do.

Q. And specifically in your testimony you discuss that there were no messages found between November 13th, 2020 and January 16th, 2021, correct?

A. That is correct.

Q. Does January 6, 2021 fall within that time span?

A. It does.

Q. You were asked by Mr. Peed, Mr. Vallejo's attorney, about there being voluminous text messages found on Mr. Vallejo's phone. In your experience, what is the difference in terms of encryption between a text message and Signal messages?

A. Well, text messages go through your phone provider, and that's all controlled by your cellular phone provider, and Signal is an encrypted chat app in which you select these as you're going to exchange text messages with.

Q. So text messages compared to Signal messages, which one is more secured?

A. Signal messages.

Q. Finally, you were asked a series of questions by Ms. Halim, Mr. Hackett's attorney, that many of the messages he sent were sort of welcome -- welcome in nature. Do you remember those questions?

A. I do.

MS. HUGHES: If we could please bring up what's already been admitted into evidence as Government's Exhibit 6776, page 13.

MS. HALIM: Objection.

THE COURT: Can I see it?

(Bench conference on the record.)

MS. HUGHES: She made it seem like it was all welcome, so this is -- I believe, actually, this is precisely the issue Your Honor flagged.

THE COURT: Well, I don't want to reverse engineer what I was trying to avoid, which is opening the door to every single message that --

MS. HUGHES: This is the only message the government intends, Your Honor.

THE COURT: No, no, I know, but if you introduce this -- look, this is already in evidence, you're going to be able to make whatever argument you want. I think it's really outside the scope. And unfortunately -- or not unfortunately, in my view, based on my thinking, opened the door to the admission of all these Signal messages that she's identified and can be presumably collected from other phones. So I'm going to sustain the objection.

MS. HUGHES: I understand.

(The following proceedings were had in open court.)

MS. HUGHES: If we could please go to Government's Exhibit 9704, Ms. Badalament. And you can zoom in.

Q. (BY MS. HUGHES) You were asked a series of questions that Mr. Hackett said a bunch of times, you're welcome, welcome. In the date range -- first of all, you testified that January 20th, that this was, in essence, not a real message. What was that message again?

A. It was a system message indicating that the user's profile had just been updated in some form.

Q. And so from July 25th, 2020 to January 9th, 2021, five months and some change, did Mr. Hackett send approximately 400 messages?

A. Yes.

Q. And after January 9th, do we have any evidence that he sent a single message?

A. No, we do not.

Q. And you've reviewed some of his messages, not all of them, correct?

A. That is correct.

Q. Were all of them, Welcome?

A. No, they were not.

MS. HUGHES: No further questions.

THE COURT: Okay. Ms. Cain, thank you very much for your time and testimony. You may step down.

Okay. Ladies and gentlemen, we actually are going to have a early dismissal today. We've come to the end of our day. So we will adjourn and resume tomorrow at 9:30. We look forward to seeing you then. Thank you.

(Jury left the courtroom.)

THE COURT: All right. Please be seated, everyone.

All right. Let's just talk about scheduling. So it sounds like we should have the better portion of the day tomorrow. And then that puts us to Wednesday. So who's prepared to start Wednesday?

MS. HALIM: Our agreement was if there's no agreement, we go in order.

MR. SHIPLEY: Well, I have an opening, Judge, obviously.

its next witness.

MR. KENERSON: Thank you, Your Honor.

The government calls Jennifer Kate Cain.

THE COURT: Can I ask -- can the government remove the exhibit? Presumably, they're not going to use this with this particular exhibit.

MR. KENERSON: This map exhibit?

THE COURT: Yes, sir.

DEPUTY CLERK: Please raise your right hand. Do you solemnly swear or affirm that any information or testimony you shall present to the Court and to the jury in the case now on trial will be the truth, the whole truth and nothing but the truth?

THE WITNESS: I do.

DEPUTY CLERK: Thank you. You may be seated.

COURT REPORTER: Can you take your mask off for me, please?

DIRECT EXAMINATION ON QUALIFICATIONS

OF JENNIFER KATHERINE CAIN

BY MR. KENERSON:

Q. Good afternoon, ma'am.

A. Good afternoon.

Q. I'm going to try and keep this microphone as close to me as I can. I'm going to ask you to do the same. Can you please introduce yourself to the jury by telling us your name and spelling your last name, please?

A. Jennifer Katherine Cain, C-a-i-n.

Q. Do you go by Jennifer or do you go by a different name?

A. I go by my middle name Kate.

Q. Thank you.

Are you employed currently?

A. I am, with the Federal Bureau of Investigation.

Q. Also known as the FBI?

A. Yes, sir.

Q. What's your current job title at the FBI?

A. I am a senior digital forensic examiner.

Q. Did you have any educational or professional experience prior to joining the FBI?

A. Yes. I have a bachelor's in business administration from the University of North Carolina and a masters in cybersecurity with a concentration in digital forensics from the University of South Florida.

Q. Now you said you are a senior digital forensic examiner. How long have you been with the FBI at this point?

A. I have been with the FBI 10 years.

Q. Of those 10 years, for how many were you a digital forensic examiner?

A. Almost six.

Q. Out of those six, how often or how long have you been a senior digital forensic examiner?

A. One year.

Q. Can you tell us what are the duties within the FBI of a digital forensic examiner?

A. Sure. We handle all aspects of digital evidence, which is to include computers, laptops, tablets, mobile devices and any kind of electronic storage media that could attach to those devices.

Q. What is the difference in terms of duties between a digital forensic examiner and a senior digital forensic examiner?

A. We undergo an additional certification to be a senior examiner. You have to have a certain number of years in the position as well as contributions to the community, teaching classes, undergoing an additional examination and providing a research project.

Q. Now did you have to undergo any sort of training back six years or more than six years ago when you first became a digital forensic examiner?

A. Yes. To become certified, it's about a two-year process and roughly 400 hours classroom in-person and instructor-led training.

Q. Now once you get certified and become a digital forensic examiner, are you required to keep current on updates in technology?

A. Yes. So each additional year after the initial certification we receive about 100 hours of advanced forensics training.

Q. Now you also mentioned a little bit about your background. Is there anything about your professional background prior to joining the FBI that's relevant to your work here today?

A. Yes. Before I joined the FBI, I worked for Johns Hopkins University Medical Center, the All Children's Hospital as a database administrator and a system administrator, which essentially means that I ran all of the database operations for the hospital healthcare system, the electronic system.

Q. What about that master's degree you mentioned? Is that helpful to you in your role here today?

A. It is. My concentration was in digital forensics, so my courses were geared towards that.

Q. Do you ever -- you mentioned you did this 400 hours before becoming certified and 100 hours a year since becoming certified. Is that within FBI, outside FBI or a combination?

A. It's a combination.

Q. Have you -- you've mentioned the number of hours of training that you have attended. Have you ever given training as an instructor?

A. I have.

Q. Can you tell us about that?

A. Yes. Currently, I serve as one of the instructors for our digital forensics trainees and I teach incident response and acquisition as well as digital forensic fundamentals.

Q. Now, you mentioned earlier that some of the duties of digital forensic examiner involve examining electronic evidence. Did I hear you correctly on that?

A. Yes, sir.

Q. Approximately how many cell phones have you been involved in processing in your role as a forensic examiner?

A. About 1,000.

Q. And approximately how many computers?

A. Three to 400.

Q. And have you also had a chance to review as part of your duties information provided by companies like Apple and Google related to electronic accounts that those companies hold?

A. I have.

Q. Approximately how many of those?

A. About 100.

Q. Does the FBI have any sort of an audit process to ensure the quality of the work that you perform?

A. We do. We have an internal department dedicated towards quality -- our quality standards as well as our education and training. And this department puts together a standard operating procedure or SOPs for all of us to follow. And then we are required to complete an exam each year to refresh our certification in those standard operating procedures.

Q. And in terms of the actual casework that you conduct, examinations of phone, computers and the like, is there anyone -- is there any process in place to checkup to ensure that the work that you're doing is also up to standard?

A. Yes, we have -- in -- all of our work is subject to peer review and technical and administrative reviews, and those are templates that follow the standard operating procedures. And we submit roughly 20 to 50 percent of our work for approval and review.

Q. And could you just tell us a little bit about what that process is like for the work that you do submit to it?

A. Sure. We turn over all of the -- any notes and final reports that we create during the course of any complete examination, and another examiner goes in, ensures that we have reviewed the correct legal authority, followed the CART request that the agent has put in for that specific case. They review the way that we perform the extraction on any given piece of evidence, how we processed it and the reports that we created for accuracy.

Q. Thank you. And we'll get to some of the terms that you just mentioned in there in a moment.

But in the course of your work, have you become familiar with the workings of encrypted applications, like Telegram, WhatsApp and Signal?

A. I have.

Q. How did you become familiar with those apps?

A. I use them both personally and professionally as well as I see it routinely in my case work and I do my own testing and validation of any new applications that are relevant to my case work.

Q. When you say "testing and validation," can you tell us what you mean by that?

A. Sure. I have a variety of test phones, both Androids and iPhones, that any time a new chat application comes up that's of interest to us forensically, I create accounts. I test sending messages or whatnot back and forth between the accounts.

Then I go through what we would consider a full examination of that phone by extracting my test devices, processing them and then comparing the output to what I actually see on the device itself.

Q. And why is going through that sort of testing important for the work that you do?

A. Well, we have a variety of in-house and commercial tools that help us during the processing process. And I like to know that the tools that I am using represent that data accurately.

Q. And again, we'll get to some -- what you mean by some of these terms, like "tools," in just a moment.

And have you, in addition to conducting this testing that you've described, reviewed information that's put out by the companies like Signal, WhatsApp and Telegram?

A. I do.

Q. What types of information have you reviewed that's been put out by the companies?

A. I follow them on their websites, and typically they each have some type of platform, such as a blog, where they issue new features and monthly updates, as well as I read the release notes of all of the different applications as they hit the Google Store and the App Store.

Q. And why is it helpful to you to read the release notes and these blogs in your line of work?

A. Because with every new edition of any application, the features are always changing which means that what you can do on the app is changing, which then in turn means what we look at forensically on that device is also changing.

Q. Ms. Cain, have you testified before?

A. I have.

Q. How many times?

A. Twice.

Q. And were those both in this courthouse here in D.C.?

A. They were.

Q. Have you been qualified as an expert previously?

A. I have.

Q. How many times?

A. Once.

Q. Was that for the government or for the defense?

A. For the defense.

Q. Has any court ever declined to recognize you as an expert?

A. No.

MR. KENERSON: Your Honor, at this point, I would seek to qualify Examiner Cain as an expert in digital forensic analysis.

THE COURT: All right. Let me hear from -- actually, we are at a decent time now to stop and I can see that the court reporter would like me to do that. So let's take -- well, maybe a little bit longer but at least our usual 10-minute break for the court reporter and we'll go from there.

Ma'am, you may step down as well.

Second, as for this Friday, I was able to bump matters so we have Friday morning until 12:30 this Friday.

Next Friday, we will not sit. Next Friday we will not sit. Not --

(Jury entered the courtroom.)

THE COURT: Ladies and gentlemen, you all may be seated. A couple of scheduling notes, so I don't forget them, this Friday will be a half day, a half day. We will go until either noon or 12:30, something on that order of magnitude.

And then next Friday, the 17th, I think it's the day before the long weekend -- I will just make absolutely sure of that. Yes, correct. We will not sit that day. We will not sit that day.

All right. Very well. Let me recognize Mr. Jauregui for some initial questions from the defendants.

MR. JAUREGUI: Thank you, Your Honor.

CROSS-EXAMINATION ON QUALIFICATIONS
OF JENNIFER KATHERINE CAIN

BY MR. JAUREGUI:

Q. Good afternoon, Ms. Cain.

A. Good afternoon.

Q. My name is Sabino Jauregui and along with my colleague, Nayib Hassan, we represent Enrique Tarrio.

I am just going to ask you a few questions, if I may, please.

A. Sure.

Q. When you testified on direct, you spoke about some of your training and experience. Let me just ask you if you are a member of some of these certifying organizations. Are you a member of the International Association of Computer Investigative Specialists?

A. No.

Q. Okay. Are you a member of the National Computer Forensic Institute?

A. No.

Q. Okay. Are you a member of the American Academy of Forensic Sciences?

A. No.

Q. Okay. Are you a member of the Forensic Specialties Accreditation Board?

A. No.

Q. Okay. I did see that you had some SANS computer forensic training; is that correct?

A. That is correct.

Q. And you did have also some NCASE; is that true?

A. Access data.

Q. And that's vendor-provided training. Correct?

A. Vendor provided, yes, sir.

Q. But you weren't a member of any of these international or national organizations in your field. Correct?

A. None that you mentioned, no.

Q. Now, would it be fair to say that these accreditations and your training, they expire after a certain amount of time?

A. Yes, I believe they all have term limits.

Q. Okay. And would it be fair to say that the last independent certification that you had, the last time you updated that was in 2020?

A. 2020 was the last SANS course that I took that had a certification with it, yes.

Q. So you are two years and something overdue on that one?

A. No, it remains certified for three years.

Q. Okay.

A. And I'm scheduled to renew it with a course in April.

Q. Okay. Thank you.

Would it be fair to say that most of your training and education is actually through the FBI?

A. No, it's about half and half.

Q. About half and half? Okay.

A. Uh-huh.

Q. And you haven't received any more academic training at a university or anything like that since you graduated from your masters?

A. No, not since my masters.

Q. You graduated from your masters what year?

A. 2017.

Q. 2017. Thank you.

Now, would it be fair to say you are a jack of all trade, everything computer forensic; would that be fair?

A. Yeah.

Q. You don't specialize in any one area in computer forensics?

A. We don't have designations. However, in the Bureau, I am known for specializing in mobile forensics.

Q. Okay.

Have you ever taught any courses at any university or any college?

A. No.

Q. And you don't have any academic appointments, do you?

A. No.

Q. Have you ever won any awards besides at the FBI, any independent awards by peers in your field?

A. No.

Q. Have you ever been published in the Digital Investigation journal?

A. No.

Q. How about in the Forensic Science Communications journal?

A. No.

Q. And that's actually an FBI journal. You've never been published there?

A. Not that I am aware.

Q. Have you been published in the International Journal of Digital Crime and Forensics?

A. No.

Q. The International Journal of Digital Evidence?

A. No.

Q. Have you ever been published in the International Journal of Forensic Computer Science?

A. No.

Q. Have you ever been published in the Journal of Digital Forensic Practice?

A. No.

Q. Have you ever been published in the Journal of Digital Forensics, Security and Law?

A. No.

Q. How about the Journal of Forensic Sciences?

A. No.

Q. Lastly, the Small Scale Digital Device Forensics Journal?

A. No.

Q. And you've only testified just once in your entire career as an expert. Correct?

A. As an expert, yes.

Q. And when you testified as an expert in that case, you were talking about call logs, why their phone calls were made and received; that kind of thing?

A. That, as well as signal and encrypted chat application.

Q. Thank you.

Now, you are not an expert in the Telegram application, are you?

A. Not yet.

Q. Would it be fair to say that your methodology in examining Telegram has never been subjected to peer review or publication. Correct?

A. That is not correct.

Q. Okay. You mean at the FBI?

A. Oh, yes.

Q. So you've only been peer reviewed by your colleagues at the FBI?

A. That is correct.

Q. I'm sorry. My fault. My question. It was inartful.

Have you ever been peer reviewed by independent computer experts in the field, not working at the FBI?

A. No.

Q. Now, you've also taken multiple courses on how to testify in court and you are doing beautifully today. Correct?

A. Thank you. Yes.

Q. Okay.

MR. JAUREGUI: Judge, that's all I have.

THE COURT: All right. Very well.

MR. JAUREGUI: Thank you.

THE COURT: Let me just ask Mr. Kenerson, are there any further questions or should I discuss --

MR. KENERSON: (Inaudible.)

THE COURT: Very well.

(Sidebar discussion.)

MR. JAUREGUI: Judge, I think it is clear that she is not an expert. She testified herself she is not an expert in Telegram.

Not only that, she has not been published in a single journal or peer-reviewed article. She has never taught a course substantively in anything, never been published in anything and never been qualified as an expert in any of the fields that Mr. Kenerson wants her to testify to as an expert, to give an opinion testimony or conclusion of any kind.

THE COURT: Mr. Kenerson?

MR. KENERSON: Just -- at least maybe I misunderstood him, but I understood Mr. Jauregui's question about Telegram to be whether she had been qualified as an expert to testify in Telegram. I didn't take it as kind of a more general, are you an expert in Telegram?

But even that aside, I don't think anything that Mr. Jauregui has done has cut into her qualification to testify as an expert in the area of digital forensic analysis. She has the requisite experience, the training, the peer review from the FBI, as the Court noted ahead of time.

I just don't -- I don't see anything that Mr. Jauregui brought out to undercut the qualifications that she laid out during the government's voir dire to testify as an expert in the area of digital forensic analysis.

THE COURT: I agree with you, Mr. Kenerson. The -- you know, she wasn't published in a lot of different journals. That could have been one question, but instead, it was 20. But in any event, all the other training and experience she has gives her the -- makes it clear to me that she can be qualified as an expert as requested.

And as for her answer on the Signal point or Telegram, I guess it was, I think, really, if I understand her answer, to have been sort of about a narrow topic, not her broader question of whether testifying about that topic within her broader expertise, that whether she can do that. In fact, I've looked through, for example, the information Ms. --

MS. HERNANDEZ: Hernandez.

THE COURT: -- Hernandez -- I'm sorry, that's right, it can only be -- ^there's only on the defense side.

Ms. Hernandez had provided me, and it's very clear to me she knows a lot about Telegram and the back-and-forth of extracting data, in the limits of what she can know about certain things. So I think I will qualify her once Mr. Kenerson asks me that question.

(Sidebar discussion concluded.)

MR. KENERSON: Thank you, Your Honor.

So as we stated before the break, we would proffer Ms. Cain as an expert in the area of digital forensic analysis.

THE COURT: All right. She will be qualified, as you requested.

DIRECT EXAMINATION OF JENNIFER KATHERINE CAIN

BY MR. KENERSON:

Q. Examiner Cain, let me ask you just a couple basic background-type questions.

One of the things that you mentioned during my initial questioning of you was something called CART. Are you familiar with that?

A. Yes.

Q. What's CART?

A. It stands for Computer Analysis Response Team.

Q. And is that a term used within the FBI?

A. It is.

Q. Can you just tell us what the Computer Analysis Response Team does?

A. That -- all of the forensic -- the digital forensic examiners at the FBI, that is our unit. So it is the unit responsible for digital forensics.

Q. Now, as a general matter, what is your goal when you conduct analysis of electronic evidence?

A. Well, um, ultimately, the goal is to work with the case agent to understand the scope of any particular case we are working on and how it relates to the device that we are looking at in question.

So ultimately my goal is to extract the artifacts from that device and present it to the case agent in a way that they can take it to their investigative team for review.

Q. And when you say "extract," what does the term "extract" mean in this context?

A. So the first part of digital forensics is actually making a copy of the device. We typically do not work with the device itself. We try to extract the data, the file system, off of that device and then do our analysis on a copy of that.

Q. Okay.

Now, does the FBI have protocols in place for ensuring the integrity of electronic evidence from when, say, a phone is recovered in the field to when you start your analysis of it?

A. Yes.

Q. Can you tell us what those protocols are?

A. Sure. We followed the typical evidence chain of custody procedures, so when an electronic device is seized under a search warrant or on consent, the seizing agent will put that device inside one of our evidence bags. They seal it up and sign it. And then at some point that will come to our computer lab, at which point we would take custody of it.

Q. And are there any procedures that you follow to ensure whether something that comes to you in the lab is -- has been not -- excuse me -- has not been tampered with between when it's been recovered and when you start your work on it?

A. Sure. When we get physical devices, they always come to us sealed, and so we will break the seal in order to know that it hasn't been tampered with since it was last sealed.

Q. Now, once you now have received a piece of electronic equipment that you are going to analyze, can you just walk us through what processes you go through at that point?

A. Sure. The first step is to take a physical inventory of the device, so actually looking at it to see what type of device it is. Is it an Android or an iPhone? Is it powered on? Is it powered off? Do we have the code for the device? Is there any physical damage that would potentially limit our access to it, such as a cracked screen or a battery that doesn't charge?

So by taking kind of inventory of what the physical device looks like, then that allows me to assess which tool would be best to copy the data, to extract the data off of that device.

Q. Now, can you just walk us physically through the process? How is it that you create an extraction from a phone?

A. We have a variety of in-house and commercial tools available to us. Most of them come with their own hardware and software; that is to say they come to us as a unit, perhaps a computer or a laptop.

We actually power on the device and hook the device up to that hardware in which the tool would interact with the mobile device in order to pull the data off of it.

Q. Now, you mentioned this term "tool." What does the word "tool" mean in this context?

A. Any commercial or in-house tool, such as a software program such as -- I believe the devices that we looked at for this particular case were used with GrayKey and Cellebrite.

Q. Now, what is the difference between a commercial tool and an in-house tool?

A. In-house is just something that we have developed. It's not available publicly for people to purchase.

Q. When you say "we," the FBI?

A. The FBI.

Q. Now, you've been talking so far about extractions of a phone. Is there any difference between the process you would do with a phone versus what you would do with a computer?

A. There is a slight difference. Most computers, we can actually take them apart and remove the hard drive and then we would hook up the hard drive to our tools so we don't actually have to interact with the computer to pull the data off of it.

However, as I just stated, that's not the case with mobile devices. They actually have to be powered on in order for our tools to interact with the device.

Q. And what about search warrant returns that you discussed a little bit earlier that you might get from electronic account providers, like Apple and Google? How does that process differ from what we have been talking about?

A. The data will come to us in some sort of containerized format. And then it appears -- from there on, the process is the same as it is with any cell phone or computer as we just need to look at the type of data that is contained in that file and determine the best way to process it and provide it to our agents for review.

Q. Now, once you have created this extraction that you have just described, what is the process at that point to safeguard the integrity of that extraction?

A. Once we get an extraction, we typically will -- either the tool will create a hash value or we will create the hash value upon conclusion of that. And what that is is a digital fingerprint, basically.

We have -- any -- there's a variety of tools that we use to do it, but it takes all of the content contained in that file and it performs algorithms on it over and over again to reduce it down to just one identifier, and then that's our hash value.

Then if anything were to change inside that file, even adding a period, it would change that entire value. So we always verify those to make sure that they match and that indicates that the content has not been altered.

Q. Now, is the -- the extraction that you created, is that -- you mentioned the phone is treated as evidence. Is the extraction also treated as evidence?

A. It is. We would check a copy of the extraction into evidence additionally. We call that derivative evidence.

Q. And do you also keep a copy that you can work on?

A. We do. I don't work on the master copy that we check into evidence. I have a working copy that I perform on.

Q. Now, once you've created this forensic extraction, the first version that comes straight out of the phone from one of these tools that you've just described, can anyone, any layperson, just open that file and see what is in it?

A. Not necessarily. You really need a specialized tool in order to convert it to a readable format.

Q. So a second tool?

A. After the extraction, yes, a second tool to do the processing on it.

Q. Can you tell us a little bit about the process of creating that first extraction into something that a layperson can look at and understand what they are seeing?

A. Sure. When we get the file system in the phone, it is exactly that. It is a file system in the phone. It is not necessarily what you would look at when you turn on your device. You can't open this extraction and see text messages. All of the applications are stored in their native state, which typically are databases.

So we use a variety of tools to turn that file system, to turn all those databases and the datapoints into what we would typically see on a phone into a useable format for analysis.

Q. Now, you mentioned that there's a copy that is checked into evidence and a copy that you work on. For the copy that you work on, is that available to anyone in the FBI or is that more limited in distribution?

A. It's very limited. We each -- when I receive a case on my local network, I put it in a case file and only I have access to that. And then as additional examiners or agents need access to that, I am able to add them to the access list and give them access. So it's not something that just anyone could go in and get.

Q. So let's say you're working on an extraction. You decide that you need to give another examiner access to that extraction. How would that second examiner be able to know that what they are looking at is a true and accurate copy of what was taken out of the phone originally?

A. All they would have to do is calculate the hash value for that, and as long as it matched, that means that the contents had not been changed and they would be okay to begin working on it.

Q. I want to ask you a couple of questions about the application Telegram. Are you familiar with that application?

A. I am.

Q. Can you tell us, what is Telegram?

A. Telegram is an encrypted chat application where a user can create an account, either on a mobile device or a computer, and exchange messages both publicly and privately with other users. They can also hold video and voice calls and send and receive attachments such as videos, images, documents, audio files.

Q. And you mentioned that Telegram is encrypted. Can you just tell us what you mean by the term "encrypted"?

A. Sure. Encrypted data is essentially data that has been concealed. It appears scrambled, for instance, while it is in transit, moving from one phone to another phone. And the only people that can unlock and unscramble the encrypted message are the ones with the keys.

Q. So if -- with Telegram, if a message is sent from phone A to phone B and it is kind of intercepted midstream, would the person who intercepts it be able to see what the message was?

A. No.

Q. So let me ask you just a couple questions about Telegram. So if someone wants to put Telegram on their phone and start using it, what's that process?

A. You would go to the Google store or the App store, depending on what type of phone, what type of device you have, download the application. And then once you open the application, Telegram will prompt the user through the account creation.

Q. Now, if you and I have Telegram accounts, can I send you a message and vice versa?

A. Yes.

Q. And for all intents and purposes, would that look any different to the two of us than a normal text message?

A. No, it would have your name and a timestamp in the message.

Q. Does Telegram also have the ability to create what is called group chats?

A. Yes.

Q. Can you tell us what the difference between a group chat and that hypothetical where you and I are just sending messages back and forth would be?

A. Sure. The intention of group chats is to add more that two people, though you could create it beginning with two people.

Once a group chat is created, the owner -- the creator becomes the administrator of the group and can add, in certain settings, additional details to that group, such as a group description, a group name, a group image.

Q. And can groups be made private?

A. They can. There are two types, both public and private groups.

Q. And what is the difference?

A. With a private group, you can only add a member by one of the current members sending out an invitation to join that group.

With a public group, you can actually search for the name of the group in the Telegram app and request access that way.

Q. Now, if you extract a device that has Telegram on it and there are group chats in that, what type of information are you able to see about the group chats?

A. We can see the name, the administrator of the group, the group description and the members of that group.

Q. And if there were, for example, two chats on a given phone that had the name "trial," would you be able to tell the difference between those two, as a forensic examiner?

A. Yes. When anybody creates a group, Telegram automatically assigns it a unique identifier, which is just a number 10 or 11 digits in length. That number is never repeated and it is unique to that group. So you could change the group name potentially infinite amounts of times, but because that group number stays the same, those groups would stay different.

Q. Now, you mentioned there is both -- depending on whether you have an Android or whether you have an Apple phone, you have to go to the Google store versus the Apple store, is there any difference in your ability as a forensic examiner to review data from Telegram based on whether the device in question was an Apple device or an Android device?

A. There is. The iPhone Telegram database and the Android Telegram database are completely different. They look and function nothing alike. Even though to the end user, Android and iPhone users can exchange messages seamlessly, the databases are actually different and store a little bit different information. So at this time, we can get just slightly more information out of the Android for the group members.

Q. And what types of information can you get out of Android that you cannot, at this point, get out of Apple devices?

A. For certain groups, the number of administrators and who those administrators are, as well as a membership list of that group, regardless of if that person participated in the group chat.

Q. Now, I want to ask you just a couple questions about group chats and how you can analyze those when people are on Telegram.

Let's say you and I are in a group chat, same Telegram group chat with a few other people. If you were to analyze my phone and your phone at the same time, would you expect what you saw in the forensic extraction to be the same between those two?

A. Potentially. Potentially not.

Q. And when you say potentially not, what types of things would cause them to not be the same?

A. Well, the main thing would be when the devices were extracted.

MS. HERNANDEZ: I'm sorry, can she repeat the answer? I couldn't hear.

THE WITNESS: Sorry. The main thing would be when the devices were extracted. For instance, if users came and went, were added or removed from that group during those two time periods or if messages were added or deleted during those two time frames, then those chats could potentially appear different, yes.

Q. And so, say, a hypothetical, my phone is extracted on Monday. Yours is extracted on Thursday, three days later. What would happen if messages were deleted in that time period?

A. Well, they -- we would see them on your device, but we would not see them on my device extracted three days later.

Q. And kind of the reverse, for the device that was extracted first, the group chat continues on, other people say things in the interim, what would you expect the difference between phone A and phone B to be?

A. Well, we wouldn't see the devices on your device, Phone A from Monday, but we would see all that added content that had come in Tuesday and Wednesday until the second device had been extracted.

Q. Now, I want to ask you a couple questions about Telegram groups. Within private groups, is there more than one type of private group?

A. There are groups and super groups.

Q. Okay. And we'll ask you some questions about super groups in a second, but I just want to ask about kind of regular groups.

A. Regular private groups. Okay.

Q. So go back to the hypothetical, you and I have a Telegram chat, we add a third person to that chat.

A. Uh-huh.

Q. Will that new member be able to see messages that were sent prior to when he or she was added?

A. No, you can only see messages from the point that you were added, on.

Q. And you mentioned earlier an administrator having some powers. Can you just tell us again, within a group, what powers does an administrator have?

A. They can add and remove members. They can set a group photo or a group description and add additional administrators too.

Q. Do they also have any influence over who can and cannot be invited to a group?

A. They do. They can set it so that only they can allow other people to join the group or they can allow all members inside that group to invite members in.

Q. And are administrators able to tap other people in the group to be administrators as well?

A. They can.

Q. Is a group limited to one administrator or can you have more than one?

A. You can have more than one.

Q. Now, again, talking about these regular groups, what happens if a user who was just a group member leaves a chat?

A. If they leave the chat, Telegram will prompt them with just a little bubble that comes up on the screen and it says, Do you want to delete this chat or do you want to delete this chat and leave the group? So there is a difference between those two.

Q. And can you just tell us what the difference is?

A. Sure. If they choose just to delete the chat, then that content and the group would be removed from the device, but they would still be a member of that group. So at any point in the future, if chats resumed, then that chat could potentially come back onto the device because they are still a member of that group.

Q. And what about in the second option that you discussed, where they choose to exit the group and -- I'm sorry. What was the prompt?

A. It was delete the group and remove themselves from the group. Essentially the same thing. They would be -- the chat would be erased from their device and they would no longer be a member in that group.

Q. Now, let's say a group member does not want to leave a group totally, but wants to delete a message they had posted to that group, what would happen then?

A. They get a similar pop-up, but the pop-up would say, Do you want to delete this message for just you or would you like to delete this message for the entire chat?

Q. So let me ask you about each of those options. If they choose, Delete this message for just you, what happens?

A. Then that message would be gone from their device only.

Q. And what if they were to choose, Delete this message for everyone in the chat?

A. It would be deleted for everyone in the chat.

Q. So again, hypothetical, you and I are in a group. I want to delete a message and I choose, Delete this message for everyone in the chat. Later your phone is imaged. Would that message be found on your phone?

A. Most likely not, no.

(Brief pause.)

Q. Now, so far we have been talking about messages that a given user posted.

A. Uh-huh.

Q. Let's say we are in a group and I want to delete a message that you have posted. Do I have that ability?

A. No. You can only delete messages that you personally authored.

Q. What about an administrator?

A. In a group, an administrator cannot do that either. They can only delete the messages that they create.

Q. And when you say "in a group," you are talking about a group, as opposed to super group?

A. That is correct.

Q. Okay. Now we've been asking about these regular groups so far. Can you tell us what the difference is between a group and a super group in the Telegram context?

A. Well, Telegram created super groups as groups started to get larger, so that is their main focus, is for more administrative control over group settings and group content when you have a large number of users. So that's the reason that they exist, basically.

Q. And so how does a group within Telegram get designated as a super group?

A. There are two ways. The first way is as the users -- or the members of that group, as it starts to reach 200, Telegram will automatically flip it over to a super group.

And the second way is that at any time, the administrator of a group can go in and actually just edit that group and force it into a super group by just clicking on that option.

Q. And are there any differences in functionality between groups and super groups?

A. There are for the administrator, yes.

Q. What are those differences?

A. The administrator can -- first off, they can remove messages from all of the devices, not just the ones that they author. They can remove any user's message and it would remove it from all devices.

They also have the ability to set the group to --

if a new member comes on, then they can read all of the content prior to them joining; that's something not available in regular groups. They also have the ability to set a link or a QR code that users can send out to invite people to join groups.

Q. Now, you mentioned that this can happen in one of two ways, either a group size approaches 200 or the administrator goes in and says, I want to change this to a super group. Do I have that right?

A. Yes.

Q. Now, if I were just a user in one of those groups where the change happened, would I necessarily notice any difference on my device?

A. Most likely not. It would all appear in the same chat thread for you.

Q. Now, that's for the user. For you as a forensic examiner, looking at that phone later, are you able to tell the difference?

A. Yes. So when a group is created, it is given a unique identifier, a unique number by Telegram. When it is converted to a super group, it's actually given a different unique identifier.

So in the database, that chat can appear as two different groups, just because the group will have one ID and the super group will have a different ID. However, it will appear as one group on the end user's device.

Q. Now, I think you mentioned that an administrator of the super group can delete a message for everyone, not just messages that they themselves post; is that right?

A. That's correct.

Q. Now, what about users in super groups? Are they still limited to their own messages?

A. They are still limited to their own messages, yes.

Q. Now, I want to ask you a little bit about images that you either created or reviewed in connection with this case. Forensic extractions, excuse me. Did you create a forensic extraction from a phone recovered from an individual known as -- named Paul Ray?

A. Yes.

Q. And have you been able to examine, using the hash value protocol we discussed earlier, phones from Enrique Tarrio, Ethan Nordean, Nicholas Ochs, Matthew Greene, Gabriel Garcia, Zachary Rehl, Ronald Loehrke and Jeremy Bertino?

A. Yes.

Q. And for the ones that you did not yourself conduct the extraction of, were you able to verify the accuracy of the extraction that you looked at?

A. Yes. The extractions were sent to me over our forensic network and upon receipt, I verified the hash values to ensure all of them matched, which they did, indicating that none of the data had been altered inside.

Q. And have you also been able to review the results of information provided by Google in response -- or related to an account registered to Joe Biggs?

A. Yes.

Q. Same question. Were you able to verify the accuracy when you looked at it?

A. Yes, I verified the hash value.

Q. Now, you mentioned I think early on in your testimony that part of what you do is you take data out of a phone. It's in some format that is not necessarily readable to a layperson, and then you try to get it into a format that is useable to, say, agents in the field who don't have your training; is that correct?

A. Yes.

Q. Okay. Do the tools that you use to make that happen allow agents to then create what we might call reports of just individual chat strings?

A. Yes. They can export out any series of artifacts from that into a report.

MR. KENERSON: Ms. Rhode, if we could have up just for the witness Government Exhibit -- demonstrative Exhibit 1131. And if we could just click through so the witness and defense counsel can see a little bit of this.

MS. RHODE: (Complied.)

BY MR. KENERSON:

Q. Do you recognize this demonstrative exhibit?

A. I do.

Q. Does that aid your testimony to the jury in describing kind of the process of how these reports are created and then assembled?

A. Yes.

MR. KENERSON: Your Honor, I move for the exhibit -- admission of 1131 as a demonstrative exhibit.

THE COURT: It will be admitted and permission to publish it to the jury.

(Government's Exhibit 1131 was admitted.)

BY MR. KENERSON:

Q. All right. So what we have up here on the screen looks like something in a column labeled Phone and something labeled A. What does that represent?

A. That represents any phone, just the phone itself.

Q. So the actual physical device recovered from wherever it was recovered?

A. Yes, the physical device.

Q. All right.

MR. KENERSON: If we could click to the next one, Ms. Rhode.

BY MR. KENERSON:

Q. What does what just came on the screen represent?

A. So that's a disk. That represents the extraction or a copy of the data that we have pulled off of that device.

Q. And now, in the column labeled Chat ID Number 123546789, what would that represent?

A. So then we would take the extraction, the file system, and turn that data into a readable format in order to analyze it. So that would represent, for instance, chat messages back and forth between users.

Q. And before we get -- one question going back to extraction. In addition to chats like this, would that also have other information on the phone, like photos, videos, things like that?

A. Yes.

Q. Now, in this representation of Chat ID 123456789, there's two bubbles with nothing in them. Is that out of the ordinary for you to see?

A. No, it usually represents some type of missing or deleted data.

Q. Okay. So if phone A is all that you have recovered, would this be -- what we see on the screen be the most complete representation of that chat ID that you could put together?

A. Yes.

MR. KENERSON: Ms. Rhode, if you could click one more time.

BY MR. KENERSON:

Q. So you see that what is labeled as a combined chat is just exactly what is in phone A. Correct?

A. Uh-huh. Yes.

Q. Okay. So let's say FBI recovers Phone B.

MR. KENERSON: If we could click a couple more times.

BY MR. KENERSON:

Q. And creates an extraction. Can they also -- once you have processed that data into something that an agent in the field can look at, can that agent look for that same chat string?

A. Yes.

MR. KENERSON: And if we could click again.

BY MR. KENERSON:

Q. So seeing what just came up on the screen under Chat ID 123456789, if an agent in the field saw that and they knew of the existence of phone A, what types of steps could they take?

A. Knowing that the chat IDs matched and that the timestamps and the direction of the messages were consistent between the two chats, they could combine those chats.

Q. And we don't have timestamps on here, but can you tell us why it's important for the timestamps to match?

A. That would indicate that those are actually the same message.

Q. Okay. Now, assuming the timestamps do match, would an agent or yourself be able to put those two chats together and get a fuller picture of what Chat 123456789 would have looked like before any data went missing?

A. Yes.

MR. KENERSON: If you can click again.

BY MR. KENERSON:

Q. So what we see over in the fourth column right there, that puts together those chats, would that be something that if it is put together in the way that we've described, you would believe would be accurate?

A. Yes.

MR. KENERSON: Now, Ms. Rhode, if we could click once more. And different hypothetical now, Phone B comes in. If we could go through to where the chat comes up.

BY MR. KENERSON:

Q. If phone B comes in and that last blue bubble is blank on Phone B as well, such that when you put them together, there is one blank, would that surprise you?

A. No, that looks accurate.

Q. So would it be common or uncommon for the best version of a chat that can be put together from the phones recovered to still contain some blanks?

A. That is to be expected, yeah.

Q. What types of things can cause a message, for example, like the one in the bottom right of combined Chat 123456789, to be missing from every phone recovered in the course of an investigation?

A. The most likely explanation is that it's been deleted.

MR. KENERSON: Thank you. We can take this exhibit down.

BY MR. KENERSON:

Q. Have you been able to, Ms. Cain, analyze -- review a number of reports of the types that we just discussed?

A. Yes.

Q. Or chat threads labeled Government's Exhibits 500 through 550, 5-5-0, for identification purposes?

A. Yes.

Q. And those came to you as -- well, how did they come to you?

A. As zip files.

Q. And what is a zip file?

A. It's a container file in which it kind of just packages up everything inside into one file.

Q. Okay. And did each of those exhibits, 500 to 550, refer to one chat thread?

A. There were multiple chat threads.

Q. Each exhibit, so like 500 was one --

A. Oh, each exhibit was one individual chat thread, yes.

Q. And within those zip files, did some of them contain versions of the chat thread from multiple devices?

A. They did, yes.

Q. Did you compare -- did you have a chance to compare each of those files in those zip files to the original extractions we discussed for the phones?

A. I did.

Q. And that's the phones that you testified that you either extracted yourself or compared the hash values and looked at the extraction?

A. That is correct.

Q. And in keeping with the example we have been using before, Phone A and Phone B, if that zip file contained something labeled Phone A and something labeled Phone B, did you compare the report from phone A to the phone A extraction?

A. Yes, I did.

Q. And the report from Phone B to the Phone B extraction?

A. Yes, I did.

Q. And all of those files -- the zip files and the files within the zip files, were you able to determine whether they matched the original extraction?

A. They all matched the original extraction.

Q. Can you just tell us a little bit about how you did that comparison?

A. Sure. Each of the zip files has source extraction information in it, meaning the name of the device that it was taken from, so I opened that extraction that had been processed and compared line by line that to ensure that the messages in those exports matched the actual message in our programs.

Q. So let me ask you a question in another way. The Government's Exhibits 500 to 550, the zip files you reviewed, do they all represent fair and accurate copies of chat strings on -- in those zip files recovered from the phones they were on?

A. They do.

Q. Of those exhibits, do any of them contain super groups?

A. They did, yes.

Q. For example, was Exhibit 505, Ministry of Self Defense Op, was that a super group?

A. Yes.

Q. Exhibit 503, Ministry of Self Defense Main, was that a super group?

A. Yes.

Q. Exhibit 507, also Ministry of Self Defense Main, was that a super group?

A. Yes.

Q. And Exhibit 509, Boots on Ground, was that a super group?

A. Yes.

Q. Now, we've talked a little bit about tools that might allow a layperson to review an extraction in an intelligible way. Right?

A. Yes.

Q. Now, is Cellebrite an example of that?

A. It is.

Q. What is Cellebrite?

A. It's a commercial tool that the government has used and bought licenses for.

Q. And what does it do?

A. It turns the data in the file system extraction into a meaningful format in order for us to review it.

Q. Were most of the phone extractions that you mentioned done in Cellebrite?

A. Most of them were, yes.

Q. I am going to ask you a couple questions about the Boots on Ground chat. Have you had a chance to -- have you had a chance to look at that chat?

A. Yes, I have.

Q. And let me ask you about Cellebrite, at least as it existed at the time these phones were extracted, if someone were in a group and was a member, but did not say anything, would that person show up in the participant list created by Cellebrite?

A. No. When Cellebrite creates their participant list, they generate the names and identifiers from the people that actually contributed messages and content to that group.

Q. Now, are you able to tell, by looking at something other than the Cellebrite participant list, whether someone was in a group?

A. Potentially, yes. As I mentioned --

MR. PATTIS: Potentially, yes, sounds speculative.

THE COURT: We'll let the witness complete her answer. So overruled.

THE WITNESS: If -- as I said before, with the Android devices, we can extract membership lists. So if that group existed on one of our Android devices, then I could look at the membership list of that group on the Android device and get a list of people who were members, but maybe not necessarily contributed content to that group.

BY MR. KENERSON:

Q. What about if you had the actual device of a member who may not have said anything?

A. Yes. If the device owner was a member of the group, by the nature of that chat existing on that device, that person would be a member.

Q. And let me ask you about what happens in Telegram when someone is invited to a group.

A. When a user is -- joins a group after a group creation, there is a system message that says, New person has joined the group, and it till say the user's name.

Q. And are you able to view that message in Cellebrite?

A. Yes.

Q. So if someone is invited to the group, but does not say anything, would that system message still be visible to you?

A. Yes.

Q. Now, have you had a chance to look at the Telegram chat Boots on Ground?

A. I did.

Q. And I think you said you reviewed the forensic extraction of Matthew Greene's phone; is that right?

A. I did, yes.

Q. Did -- when you reviewed that, did you see any evidence one way or the other whether Mr. Greene was in Boots on Ground?

A. I did. Mr. Greene's phone was an Android. So I was able to see in his membership table that he was listed as a member in Boots on Ground.

Q. And what about from reviewing the extraction? Did you see any evidence one way or the other whether he had been invited to that group?

A. When I reviewed Mr. Nordean's device, in Boots on Ground chat on Mr. Nordean's device, there was a system message that said Mr. Greene's user name or user ID had joined the chat on January 15th, I believe, at 6:35 p.m.

Q. Now, did you ever see any information as to whether an individual with the Telegram handle NobleLead was in Boots on Ground?

A. I did.

Q. And can you tell us about that?

A. So when a user joins the group after the group creation, a system message comes across and says that, This user has joined the group. When they are added during the group creation, while the administrator is actually going in and creating the group, you have the option to add members right off the bat as the group is being created. Those will not leave system messages.

However, when a user leaves the chat, a system message is created. I was able to find a system message for NobleLead leaving that chat.

MR. KENERSON: And if we could have the demonstrative back up just for the witness for a moment, please.

And, Ms. Rhode, you can go to the last slide of that.

BY MR. KENERSON:

Q. And looking at that, would -- do you recognize what you see on the screen?

A. I do.

Q. Would using what you see on the screen help you explain your testimony you just gave to the jury?

A. It would.

MR. KENERSON: Your Honor, I would ask that this portion also be admitted as a demonstrative.

Number again?

MR. KENERSON: 1131.

THE COURT: All right. It will be admitted and permission to publish.

(Government's Exhibit 1131 was admitted.)

MS. HERNANDEZ: So, your Honor, these are demonstrative evidence? Is that what I understood the government --

THE COURT: They've -- correct. They have -- it is a demonstrative; is that correct, Mr. Kenerson?

MR. KENERSON: Yes.

THE COURT: All right. Very well.

BY MR. KENERSON:

Q. All right. Can you explain to us what we are looking at at the top of these two blue bubbles?

A. This is a screenshot of a Cellebrite report and these are system messages.

Q. And system messages are the type that you just discussed that happen when people either enter or leave a group?

A. Yes.

Q. And the one at the top, can you tell us what we are looking at in the one at the top here?

A. That is a system message saying that the Peer ID 1480174105 joined the group via a link on January 5th, 11:35 p.m., UTC, which would translate to January 5th, 6:35 Eastern Standard Time.

Q. And you mentioned a bunch of numbers and a peer ID. What is a peer ID?

A. When a person creates account on Telegram, much like a group is given a numerical identifier, each person's user name, each account you create is also given a numerical identifier. This one that begins with 148 is associated with Mr. Greene.

Q. Thank you.

And -- now, there's one below that says system message, Enrique Florida Pb left the group and it gives some dates. Can you tell us what we are looking at there?

A. Yes. It is also a system message on January 14th, 2:34 a.m., so January 13th, 9:34 p.m. Eastern Standard Time. It says, Enrique Florida Pb left the group.

Q. These are both from the Boots on Ground chat?

A. Yes.

Q. Now, I asked you, I think, about the Telegram handle NobleLead, and we are looking at something that says Enrique Florida Pb. Can you tell us why this says Enrique Florida Pb?

A. When you create an account on Telegram, you are assigned a unique identifier and you are also able to create a user name and a display name for yourself.

However, when your friends find you and you join groups on Telegram, they are -- and if you are stored in their phone contact with a different name and you allow Telegram to sync up with your contact list, Telegram will actually display what your phone displays for that same person.

So while NobleLead is the user name that he selected during account creation, this is -- Enrique Florida Pb is what is displayed on Mr. Nordean's device.

Q. Thank you.

And I think you mentioned that -- were you able to find something like you found for Mr. Greene, an invite system message for Mr. Tarrio?

A. No, I was not.

Q. And what does that tell you?

A. That he was added during the group creation as it was being created, so he did not get a system message for joining the group.

MR. KENERSON: Thank you, Ms. Rhode, we can take this exhibit down.

BY MR. KENERSON:

Q. Are you familiar with the term "orphan files" that has been used in this investigation in relation to Telegram?

A. Yes.

Q. What is that?

A. For this investigation, we have considered an orphan file to be any type of attachment, such as a video, image, document or audio file that has been sent as an attachment in any given message, but the original message is no longer present on the device.

Q. And how -- can you just tell us how a file can become orphaned, such that the original message is not available by the time that you are looking at the phone?

A. If the message has been deleted.

Q. Excuse me. Let's say you come across an orphaned audio file. Are you able to tell which of those applications it was originally associated with?

A. No. Oh, sorry. Yes.

Q. How are you able to tell that?

A. When all of these applications create media attachments, they are all containerized, meaning if Signal create -- has an attachment in it, it is forced to stay in the Signal path file of the device.

If Telegram has an attachment with a media file in it, when it saves to the phone, it's also forced to save in the Telegram portion of the device.

Each of the devices are containerized and so all of the media within them stays within those certain paths.

Q. Now, if you do learn that, say, a particular orphaned file is associated with Telegram, but there's no associated chat left on the device, are you able to say definitively what chat that file was originally associated with?

A. No.

Q. Now, have you had a chance to look at a number of orphaned files recovered from some of the devices that we have discussed?

A. I have.

Q. And did you have a chance to look at what is called metadata associated with those files?

A. I did, yes.

Q. What is metadata?

A. For these particular files in this scenario, the metadata is essentially just data about the data. So these are file system dates as they relate to when that particular attachment was saved to the device.

Q. And as you sit here today, do you recall the specific dates and metadata in question for those files?

A. Not from memory, no.

Q. Were you able to -- well, did you send a couple of emails memorializing that metadata?

A. I did.

Q. Would it aid your testimony if you were able to refer to those emails in the course of that testimony?

A. It would, yes.

MR. KENERSON: Your Honor, I provided defense counsel a copy of these, but I would ask that Ms. Cain be permitted to refer to her, essentially, notes while testifying about the metadata.

THE COURT: All right. Counsel would like -- one counsel would like to be heard at sidebar.

(Sidebar discussion.)

MS. HERNANDEZ: The government earlier mentioned Paul Ray I think and a couple other names that are not the defendants in the case. I guess the Government alleges that those people are co-conspirators or tools or some other category, so --

THE COURT: I think at a minimum, it just means that they found relevant evidence on their phone.

MS. HERNANDEZ: Well, I just wanted to make an objection subject to the government at some point linking it up -- as I was going to say, whether they are tools or co-conspirators or however else.

THE COURT: I don't believe -- well, I actually don't know. But has any of the evidence that we have been talking about, Mr. Kenerson, come from any of the phones that Ms. --

MS. HERNANDEZ: Hernandez.

THE COURT: -- Hernandez has mentioned?

MR. KENERSON: I guess it depends on what evidence we have been talking about. Are we talking about the course of her testimony or the PDFs?

THE COURT: I'm talking about the PDFs.

MR. KENERSON: I believe so. I believe at least some level of the evidence that wound up going into those PDFs came from some of those phones, yes.

THE COURT: Well, I mean -- I guess -- Ms. Hernandez, that sounds like an objection you can make as the -- either could have made or might make as a particular exhibit is coming into evidence.

It doesn't -- these are -- we know who sent -- we knew who the sender was for all of these messages. That it happened to be captured on someone else's phone strikes me as not, you know, a bar to its admission.

MS. HERNANDEZ: I wasn't sure exactly -- I know the government mentioned those names. I was not sure how they would interact or how they affected the evidence that the government was going to introduce. So I just wanted to lodge the objection and if they -- if it becomes an issue, we'll figure it out. I just --

THE COURT: All right.

MS. HERNANDEZ: To the extent that any of the evidence is coming in from those devices, I am just lodging the objection.

THE COURT: All right. Mr. Pattis?

MR. PATTIS: Briefly, Judge. Mr. Kenerson read those names pretty quickly. I didn't want to interrupt the flow because I didn't think it was material. Could he give us those names again, please?

MR. KENERSON: I'm happy to do so. It might be more efficient to do it just off the record where I am not flipping through my notes again, but if we want to do it now, I'm happy to do it now too.

MR. PATTIS: It doesn't matter to me. It's just a gap in my notes and now that the issue has come up.

THE COURT: We only have 15 more minutes with the jury, so let's get back to the testimony and we can tie up these loose ends after we are done.

MR. PATTIS: Yes, sir.

THE COURT: All right.

(Sidebar discussion concluded.)

MR. KENERSON: I think the request before the break was to allow Examiner Cain to refer to her notes when discussing the metadata.

THE COURT: All right. Without objection, it will be permitted.

MR. KENERSON: All right. If I may approach the witness --

THE COURT: You may, sir.

MR. KENERSON: -- with what's been marked for identification as Government's Exhibits 1134, 1135 and 1136.

Ms. Rhode, if we can bring up Government's Exhibit 1104, which I believe is already in evidence.

DEPUTY CLERK: 1104 was ID'ed, but it wasn't admitted.

MR. KENERSON: To the extent it hasn't been admitted, I think I would move for its admission -- we can go on the phones --

THE COURT: All right.

(Sidebar discussion.)

THE COURT: What is 1104, Mr. Kenerson?

MR. KENERSON: 1104 was one of the four audio files that was played during Mr. Greene's testimony.

THE COURT: Oh, all right. I don't know why -- Ms. Harris, you don't see it in evidence?

DEPUTY CLERK: 1104, 5, 6, nor 7. I have them all ID'ed, but not received in evidence.

THE COURT: They were all Mr. Pezzola's files. Correct?

MR. KENERSON: Well, they were -- Mr. Greene identified the voice as Mr. Pezzola's, yes.

THE COURT: Right.

All right. Is there any objection to their admission now?

MS. HERNANDEZ: On behalf of Mr. Rehl, I think if that's some of the items that were not co-conspirator statements, we would object.

THE COURT: Well, it doesn't -- they're coming in one way or the other. Right? I mean, again, I think, at the time we discussed them and the jury heard them, we talked about -- I would have mentioned to all of you that, if you think a limiting instruction is appropriate based on the particulars of the statement, you all let me know and I'll consider it and give it.

So they're coming in one way or the other. You know, if you -- the question of whether these were co-conspirator statements or not, I don't think the parties have addressed but --

MS. HERNANDEZ: My recollection was the Court said you would give a limiting instruction once the parties got together and offered something.

THE COURT: Right. On any -- so, so is there any objection to their admission with subject to whatever you want to argue in terms of what the limits might be?

MS. HERNANDEZ: Not that -- in that manner, Your Honor.

THE COURT: All right.

MR. METCALF: Your Honor, Steven Metcalf. I don't remember how I handled this when they were first introduced with Mr. Greene. So I just want to reserve me basically taking a look into that for -- to address to the Court a little bit later on if I need to.

THE COURT: If you mean a limiting instruction, I suppose, although as to your particular client, I think it's going to be hard for there to be a limiting instruction. They're his statement.

MR. METCALF: Understood. I just don't know if I objected at the time.

THE COURT: It doesn't -- whether you did or did not, they're moving their admission now and I don't know of a reason why they wouldn't be admissible.

MS. HERNANDEZ: It might not be -- I thought one of them was some call with his wife or about his wife having --

THE COURT: Well, I had inquired about the content and whether it was potentially objectionable and it was not.

So, Mr. Kenerson, those will be admitted subject to whatever the limiting instruction the parties present to me.

(Sidebar discussion concluded.)

MR. KENERSON: Okay. So we'd move for the admission of Exhibits 1104 to 1107.

THE COURT: All right. They will be admitted and permission to publish.

(Government's Exhibits 1104 to 1107 were admitted.)

MR. KENERSON: And starting with 1104, Ms. Rhode.

(Audio played.)

BY MR. KENERSON:

Q. Now, do you recognize that as being one of the orphaned files you reviewed?

A. I do, yes.

Q. Which phone was that from?

A. Mr. Greene's device.

Q. Now, did you get a chance to look at the metadata associated with that file?

A. I did.

Q. What was the metadata associated with that file's creation?

A. May I refresh my recollection?

Q. Sure.

A. It was created on Mr. Greene's device on January 3rd at 1:30 p.m. Eastern Standard Time.

Q. January 3rd of what year?

A. 2021.

Q. Now, the fact that it was created on Mr. Greene's device at that date and time, what is that -- what would cause that to be created then?

A. If -- when Mr. Greene's device received the message containing that attachment and saw it on his phone, that is when the file would be added to the file system and that's when that time stamp would be created.

Q. Thank you.

MR. KENERSON: Now, 1105, please, Ms. Rhode.

(Audio played.)

BY MR. KENERSON:

Q. Examiner Cain, did you recognize that?

A. Yes, sir.

Q. Is that one of the files that you reviewed?

A. Yes, from Mr. Greene's device.

Q. What was the metadata associated with that file's creation?

A. May I refresh my recollection?

Q. Please.

A. It was January 5th, 2021 at 5:34 p.m.

Q. Thank you.

MR. KENERSON: 1106, please.

(Audio played.)

BY MR. KENERSON:

Q. Do you recognize that?

A. Yes.

Q. What device was that one from?

A. Mr. Greene's device.

Q. And what does the metadata say about the creation time of that file?

A. May I refresh?

Q. Please.

A. It was January 5th, 2021, at 7:56 a.m.

Q. All right.

MR. KENERSON: And lastly in this series, Ms. Rhode, 1107, please.

(Audio played.)

BY MR. KENERSON:

Q. Do you recognize that?

A. I do.

Q. Is that one of the files you reviewed?

A. It is, yes.

Q. Which device was that from?

A. Also Mr. Greene's device.

Q. What did the metadata say about the creation date of that file?

A. May I refresh?

Q. Please.

A. It was January 5th, 2021 at 7:58 a.m.

MR. KENERSON: Ms. Rhode, can we have Exhibit 551 start, play just a couple of seconds and then stop?

(Audio played.)

You can stop there before we play the whole thing.

BY MR. KENERSON:

Q. Do you recognize that file, Examiner Cain?

A. I do.

Q. Is that one of the files you reviewed?

A. It is.

Q. Could you tell us which, if any, of the phones you found that one in?

A. It was on Mr. Loehrke and Mr. Ray's device.

MS. HERNANDEZ: Objection.

THE COURT: Overruled at the moment. Overruled as to this testimony.

MR. KENERSON: I move for the admission of Exhibit

551.

THE COURT: I'm sorry. Maybe we do need to go to the phone so I understand something.

(Sidebar discussion.)

THE COURT: Mr. Kenerson, this is a new document or a new exhibit?

MR. KENERSON: That is correct. This is a new exhibit. She has testified that she recovered it from Mr. Ray's device. I expect a later witness will testify that that's Ethan Nordean's voice. You know, I -- if the Court wants us to wait to admit it until then, that's fine but it's -- I expect a different witness will testify it's Ethan Nordean's voice, and she will testify as to the metadata associated with that file.

THE COURT: Why don't we just then -- just to make this easy, why don't you just lay the foundation but not move its -- of course, she has to hear it and the jury will hear it, but nonetheless, why don't we just wait until admitting it until that later witness connects the dots.

MR. KENERSON: Sure.

THE COURT: All right.

(Sidebar discussion concluded.)

BY MR. KENERSON:

Q. All right. Examiner Cain, from what you heard, did you recognize that to be a file that you examined -- or excuse me, that you -- an orphaned file you found on one of the phones?

A. I do, yes.

Q. Associated with -- you testified to the phones it was in but associated with which application?

A. The Telegram application.

THE COURT: I'm sorry. Again, again, I can't have the examination be competing with other people in the courtroom. Mr. Kenerson?

MR. KENERSON: Associated with --

MS. HERNANDEZ: Your Honor, could they keep their voice up? What you're hearing is we're trying to -- we can't hear what's being said. I apologize.

THE COURT: It's ironic because it makes it harder for me to hear as well.

All right. So Mr. Kenerson and if the witness -- both witness and attorney, if you'll try to keep your voices up.

BY MR. KENERSON:

Q. Sorry. It was, I think you were saying, it was recovered from two different phones associated with which application?

A. Telegram.

Q. And let's ask you, first, about Mr. Ray's device. What did the metadata say in terms of the creation date in

Mr. Ray's device?

A. May I refer to my notes?

Q. Please.

A. The date was January 7, 2021 at -- sorry -- 7:23 p.m.

Q. And what about in Mr. Loehrke's device?

A. That was -- can I refer to my notes?

Q. Please.

A. Mr. Loehrke's device was January 6th, 2021 at 9:38 a.m.

Q. What types of things would cause one -- was it the same file on both phones?

A. It was the same file.

Q. What types of things would cause there to be that type of discrepancy in the creation date between the two phones?

A. If the message wasn't received on one of the devices until later, then that could cause that day to be later. Also, Mr. Ray's device is the date that it was later on. If he had interacted with that file, perhaps forwarded it to some other group or to someone else, that could also modify the dates in there.

Q. Now, um, I think I forgot to ask you this with respect to 1104 to 1107. What application were those files associated with in Mr. Greene's phone?

A. Telegram.

Q. Thank you.

Now, with respect to 551, you said it was on two phones. Was it an orphaned file in both of them?

A. It was, yes.

MR. KENERSON: Your Honor, just looking at the clock, this would be about where I move into a different topic.

THE COURT: All right. Very well.

Ladies and gentlemen, we'll conclude for the day. Thank you very much for your attention as always. We will see you tomorrow morning.

(Jury exited the courtroom.)

THE COURT: All right, ma'am. You may step down.

(Witness stepped down.)

THE COURT: And everyone may be seated.

All right. So the only item I want to go through right now with the parties is just give you a, kind of -- I will put on the record a more detailed basis for this ruling later on.

But in the interest of time, in the interest of letting the government know what's in and what's out on the Telegram stuff, I'm just going to run through a bunch of objections that I have sustained, either in whole or in part, so that you all know and the government can adjust

So those were newly discovered and a discrete issue.

THE COURT: All right. Very well.

Let's bring in the jury and the witness.

Mr. Kenerson, were we at the end of your -- had you completed your direct?

MR. KENERSON: No, I had not. I had not much more, but some more.

(Thereupon, Examiner Jennifer "Kate" Cain entered the courtroom and the following proceedings were had:)

THE COURTROOM DEPUTY: Jury panel.

(Whereupon, the jury entered the courtroom at 9:42 a.m. and the following proceedings were had:)

THE COURT: You all may be seated.

Ladies and gentlemen, welcome back. We'll continue with the Government's direct examination.

MR. KENERSON: Thank you.

(JENNIFER "KATE" CAIN, GOVERNMENT WITNESS,
PREVIOUSLY SWORN.)

CONTINUED DIRECT EXAMINATION

BY MR. KENERSON:

Q. Good morning, Examiner Cain. How are you?

A. Great. Thank you.

Q. I want to switch topics from where we were yesterday. You said one of the phones you examined was one belonging to an individual named Jeremy Bertino. Is that right?

A. That is correct.

MR. KENERSON: And, Ms. Rohde, if we could bring up, just for the witness, Government's Exhibit 1137.

BY MR. KENERSON:

Q. And do you recognize what's on your screen?

A. I do.

Q. What do you recognize that as?

A. This is a video found on Mr. Bertino's device that he had screen recorded and then sent to someone else in a text message.

Q. And can you tell what -- well, what is a screen recording of?

A. When the user goes and actually takes a video of everything that is happening on the device.

Q. Okay. Does this show any particular application?

A. This is the Telegram app.

Q. And is this -- have you had a chance to view this video in its entirety before your testimony here today?

A. I have.

Q. Does this fairly and accurately represent what was recovered from Mr. Bertino's phone?

A. It does.

MR. KENERSON: Your Honor, I'd move for the --

MS. HERNANDEZ: I'm sorry. Your Honor, one of the screens isn't working, so we --

THE COURTROOM DEPUTY: I'll send an email to John.

THE COURT: Oh, it's on. All right. Very well.

You may proceed, Mr. Kenerson.

MR. KENERSON: I'd move for the admission of Exhibit 1137.

THE COURT: All right. It will be admitted. And permission to publish.

(Whereupon, Government's Exhibit No. 1137 was entered into evidence.)

BY MR. KENERSON:

Q. And before we start playing, you said this was a screen recording. Can you tell us how a user would create a screen recording such as this?

A. There is a setting in the iPhone that you -- the user can go to and click "screen record," and then everything after that point will be recorded.

Q. And is that -- and so what we are looking at here is a video file, not a still shot. Correct?

A. That is correct.

Q. And if someone takes a video record as opposed to a still shot of a screen, what's the difference?

A. Well, a still screen shot is just an image of how it looks at that time. A video is actually the user interacting with the device. So if the user opens an application, you'll see it open. If they scroll down, you'll see the screen scroll down. You'll see everything the user sees on that device as it's happening.

Q. So is this how a user would see this chat if they scrolled through it on their phone at the time the screen capture was created?

A. Yes.

Q. Now, was this file particularly associated with Telegram or was it found somewhere else on Mr. Bertino's device?

A. It was found in the camera roll of his device.

Q. Okay. And so you mentioned that this is how Telegram would appear to a user of Telegram. If you were looking at the Telegram application through your forensic tools, is this how it would appear to you?

A. No, it wouldn't. We build the data as similar and as close as possible, but it actually doesn't look like the application does.

Q. Okay. Now, on this, is there any significance to which side the chat bubbles are coming from?

A. The ones on the left-hand side are all of the incoming text messages -- or messages. And then the ones on the red -- sorry -- on the right side in green, those are all of the outgoing messages, just like they appear in regular text messaging.

Q. Now, let me ask you something about, as an example, the message that I'm circling right now, which has Captain Trump at the top and then Noblebeard, the Immortal, under it at -- it looks like 12:34 p.m. What does that -- the message displaying in that manner signify?

A. So the author of this message is Captain Trump, and the message is an audio file. And when you see the blue bar like that, he's actually replying specifically to a voice message that Noblebeard, the Immortal, left.

Q. Thank you.

Now, up at the top, it says: Parler comment on post, Carol Jean, and then some words.

What is that denoting?

A. Those are the IOS notification banners that are coming across in realtime as the screen is being recorded.

Q. So notifications on the user's iPhone as he's recording?

A. Yes.

MR. KENERSON: Ms. Rohde, can we play until ten seconds.

(Whereupon, segments of Government's Exhibit No. 1137 were published in open court.)

BY MR. KENERSON:

Q. Now, we just saw the video scroll through at a certain pace. Are you able to control the pace of how this scrolls as we play the video?

A. I am not, as someone watching the video. That would have been controlled by the person recording the video.

Q. And we just saw a bubble of a man who said something about storming the Capitol Building. Under that bubble, there is something that says 12:56 p.m. What does that 12:56 p.m. mean?

A. That was the time the message was sent.

Q. And have you had a chance, Examiner Cain, to compare -- first of all, did you have a chance to look at these messages and see whether you can link them up to any of the chats that you looked at?

A. I have, yes.

Q. Which chat was this recording from?

A. This chat was called New MOSD.

Q. And did you have a chance to look at the copies of that chat that were -- you were able to review from the forensic extractions and see whether the messages in this chat were present in any of the versions that you looked at?

A. I did.

Q. And did you take some notes from that?

A. I did.

Q. Would it aid your testimony to be able to refer to those notes?

A. That would help. Thank you.

MR. KENERSON: Your Honor, if I may approach the witness.

THE COURT: You may, sir.

MS. HERNANDEZ: Objection. Is there a question that she can't recall so that she needs to look at the notes?

THE COURT: I think this is the same -- let me hear counsel.

(Whereupon, the following proceedings were had at sidebar outside the presence of the jury:)

THE COURT: Mr. Kenerson, is this the same issue we went through yesterday?

MR. KENERSON: Yes. This is one of the three documents I brought to her yesterday. We just did not get to this point in the testimony.

THE COURT: All right. Do you have any objection, Ms. Hernández? It's just refreshing her -- it's as to particular details. Mr. Kenerson isn't using the technically formal refresh procedure, but I think -- I thought everyone had agreed that they didn't have an objection to this in this case.

MS. HERNANDEZ: Is he asking her about the metadata? I didn't hear him say that. I thought he was just going to ask her questions about everything. He said, You took notes.

If it's about the metadata, I have no objection. But I thought the question was broader than that.

MR. KENERSON: It's going to be whether certain messages were recovered from any of the chats she looked at.

THE COURT: Ms. Hernández, this is, broadly speaking, I would say, about metadata, about where things were recovered from, what the metadata shows, where things were recovered from. Do you have any objection to this, then?

MS. HERNANDEZ: I'll let him proceed. If there's a problem that I see, I'll object again, your Honor. Thank you.

THE COURT: Mr. Pattis?

MR. PATTIS: I'm looking at the exhibit. I don't know how far -- what the Government intends to do. But there's a notation -- there are notations from someone who calls themselves cracker, nigger, faggot. Are we getting into that here?

THE COURT: Mr. Kenerson?

MR. KENERSON: It is literally already on the screen right now. This was the subject of -- I'm not going to ask her any questions about that, but this was the -- kind of a subject of a pretrial motion *in limine*, and this was in the Government's opening as well.

THE COURT: Well, what do you mean, Mr. Pattis?

MR. PATTIS: I'll withdraw it. I forgot -- I had forgotten the pretrial order. My mistake.

I apologize to your Honor.

THE COURT: That's all right. I wasn't sure whether you meant that screen name or another -- the content of what the person says.

Mr. Kenerson, you may proceed.

(Whereupon, the following proceedings were had in open court:)

MR. KENERSON: Your Honor, if I may approach the witness with what has been marked as Government's Exhibit 1136 for identification.

THE COURT: You may, sir.

BY MR. KENERSON:

Q. Examiner Cain, is what I just handed you the notes that you created in connection with this exhibit?

A. They are, yes.

Q. Now, the chat bubble that we've just been discussing at 12:56 p.m., was that message recovered on any device that you examined?

A. No, it was not.

Q. And what about the message right above it that says -- and I'll just say it directly -- "Fuck then" -- that comes from the right of the screen?

A. May I refer to my notes?

Q. Yes, please.

A. No, it was not.

MR. KENERSON: Ms. Rohde, can we play until 30 seconds now.

(Whereupon, segments of Government's Exhibit No. 1137 were published in open court.)

MR. KENERSON: Thank you.

BY MR. KENERSON:

Q. Now, that second bubble video that has a timestamp of 12:58 p.m., was that recovered from any device you examined?

A. May I refer to my notes?

Q. Please.

A. No, it was not.

Q. Now, under that, there's two messages coming from the right, one that says, "Form a spear," and one that says, "Holy fuck, do it, boys."

Were either of those recovered from any --

THE COURT: I'm sorry, Mr. Kenerson. I just -- can you keep your voice up?

And can the witness -- can you keep your voice up, please?

And can those at counsel table keep their voices down.

BY MR. KENERSON:

Q. So the two messages underneath the bubble at 12:58 p.m. -- one says, "Form a spear"; one says, "Holy fuck, do it, boys" -- were either of those recovered from any device that you examined?

A. No, they were not.

MR. KENERSON: Can we play until one minute and one second, please -- or play to the end, I suppose.

(Whereupon, segments of Government's Exhibit No. 1137 were published in open court.)

BY MR. KENERSON:

Q. Examiner Cain, the chat bubble from the right with the individual with the beard at 1:00 p.m., was that recovered from any device you examined?

A. May I refer to my notes?

Q. Sure.

A. No, it was not.

Q. What about the two underneath? We'll start with, first, "Fuck, I'm so mad I'm not there."

Was that recovered from any device you examined?

A. No, it was not.

Q. What about, "More videos, Bro"?

A. No, it was not.

Q. What about the bubble from the left at 1:02 p.m.? Was that recovered from any device you examined?

A. No, it was not.

Q. Now, what about the one underneath it, "Push inside. Find some eggs and rotten tomatoes"?

A. Yes, it was.

Q. Which devices was that recovered from?

A. They were found on Mr. Rehl and Mr. Nordean's device.

Q. Now, it looks like we are at the end of the video at this point. Correct?

A. That is correct.

Q. Now, what, if any, conclusions can you draw as an examiner from the fact that the messages that we just discussed that weren't found on any device were not found on any device you examined?

MS. HERNANDEZ: Objection. Relevance.

THE COURT: Overruled.

THE WITNESS: These messages that were not found on the device had been deleted.

BY MR. KENERSON:

Q. Can you draw any conclusions as to who would have deleted them?

A. The user that posted the video.

Q. Why do you come to that conclusion?

A. Because when we found this chat on two different devices, the missing messages were gone from both of those devices. Therefore, if the user had selected just to remove it from their own device, then they would still be present on the other two devices. And since they weren't, the conclusion is that they removed them from all the devices for the chat.

Q. Now, in addition to --

MR. KENERSON: Ms. Rohde, we can take this exhibit down.

BY MR. KENERSON:

Q. You said you also had a chance to review the extraction from Mr. Rehl's phone. Is that right?

A. That is correct.

Q. And did you have a chance to look at exhibits labeled Government's Exhibit 400A, 400D, as in delta, P, as in Paul, R, X, as in x-ray, G, as in gamma, P, as in Paul, Q, T, JJ, 402B, 403G and 403H?

A. I did. Yes.

Q. Were all of these found on Mr. Rehl's device?

A. They were.

Q. And do they appear to depict events from January 6th, 2021?

A. They do.

MR. KENERSON: Your Honor, I'd move to admit those exhibits.

THE COURT: They will be admitted.

(Whereupon, Government's Exhibit Nos. 400A, 400D, 400P, 400R, 400X, 401G, 401P, 401Q, 401T, 401JJ, 402B, 403G and 403H were entered into evidence.)

BY MR. KENERSON:

Q. Now, we talked about metadata yesterday. Did Mr. Rehl's device have metadata associated with those files?

A. It did.

Q. Did you create a chart that includes some of that metadata?

A. I did, yes.

MR. KENERSON: Ms. Rohde, if we could have, just for the witness, Government's Exhibit 1132.

BY MR. KENERSON:

Q. Do you recognize what's on your screen?

A. I do.

Q. What is that?

A. This is the metadata that I extracted out of the device that corresponds with the exhibits that you just named and are listed here.

Q. Thank you.

And I need to correct how I read those exhibits. I said -- let me just read them over one more time: 400A, 400D, 400P, 400R, 400X, 401G, 401P, 401Q, 401T, 401JJ, 402B, 403G and 403H.

That's what's on the chart. Correct?

A. That is correct.

MR. KENERSON: And for the record, those are the exhibits I'm moving to admit.

THE COURT: All right. And so those will be admitted to the extent there was any discrepancy.

(Whereupon, Government's Exhibit Nos. 400A, 400D, 400P, 400R, 400X, 401G, 401P, 401Q, 401T, 401JJ, 402B, 403G and 403H were entered into evidence.)

MR. KENERSON: And I would also move at this point for the admission of Exhibit 1132.

THE COURT: It will be admitted.

(Whereupon, Government's Exhibit No. 1132 was entered into evidence.)

MR. McCULLOUGH: And seek permission to publish.

THE COURT: And permission to publish.

BY MR. KENERSON:

Q. Now, looking at the first column of this chart, does that represent the exhibit number in court that we just read out?

A. It does, yes.

Q. The second column that says Photo Title, what does that represent?

A. It's the name of the image or the video.

Q. The image as found where?

A. In the device.

Q. In Mr. Rehl's device?

A. In Mr. Rehl's phone. Yes.

Q. Okay. Now, Photo Taken Date/Time, what does that represent?

A. That is the actual creation date of the video or picture listed. It comes from the EXIF data. So it actually is embedded in the file itself so that if it's moved to a different -- you know, saved somewhere else other than the device, that creation date is embedded inside the file itself so it will always remain the same.

Q. And you used the term EXIF data. Can you just tell the jury what that means?

A. Sure. It's actually a standard for photographers. When digital cameras became popular, it's a way for them to store all of the camera settings such as the aperture and the lens. And so among those are things that are relevant forensically, like the date the photo was taken and created and the type of camera that took it and the latitude and longitude of the photo as well.

Q. Now, speaking of latitude and longitude, that's what the next two columns represent. There's only, it appears, that data for one photo. Does that indicate that was the only photo that has that data?

A. It does. Saved as EXIF data, yes.

Q. Okay. And then what does the camera make denote?

A. These photos were taken with an Apple iPhone. Several of them with an iPhone 11 Pro and one with an iPhone 8.

Q. Now -- and what's the source of that data?

A. That is also in the EXIF data.

Q. And same question about the camera model.

A. Same. It's embedded in the photos itself, in the EXIF data.

Q. Now, the bottom two, 403G and 403H, do not have a camera make or a camera model. Is that because there was no EXIF data that indicated that?

A. That is correct. Telegram and most social media strip most of the EXIF data from the photos to make the size smaller. However, it does retain the creation date of the video or image.

Q. And were you able to tell which, if any, of these exhibits were taken by the camera on Mr. Rehl's phone?

A. Yes. Mr. Rehl's phone was an Apple iPhone 11 Pro. So wherever it says iPhone 11 Pro, those were taken with his actual device.

Q. Now, with respect to 402B, that says it was taken from an iPhone 8. Are you able to tell how that photo got onto Mr. Rehl's phone?

A. Yes. He received that photo via a text message.

MR. KENERSON: Ms. Rohde, can we put up 402B.

BY MR. KENERSON

Q. So that was the photo he received via text message?

A. It is, yes.

Q. Thank you.

MR. KENERSON: If we can go back to the chart.

MS. HERNANDEZ: Your Honor, I didn't hear

Mr. Kenerson's question. Was it received by Mr. Rehl, did he say? Or sent by Mr. Rehl?

THE COURT: This was -- the question was about whether he received it.

MS. HERNANDEZ: Thank you.

BY MR. KENERSON:

Q. Now, you mentioned that Telegram and most social media sites don't necessarily include camera make and model. 403G and 403H, what application were those associated with?

A. Those are from Telegram.

Q. And are those orphaned files like we were discussing?

A. They are.

MR. KENERSON: Ms. Rohde, can we play 403G, please.

(Whereupon, Government's Exhibit No. 403G was published in open court.)

BY MR. KENERSON:

Q. So was that video found on Mr. Rehl's device?

A. It was.

Q. Now, did you also have a chance to take a look at information provided by Google in connection to an account subscribed to by Joseph Biggs?

A. I did.

Q. How, for you, as a forensic examiner, does reviewing that type of data differ from reviewing phone data or computer data?

A. It's very much the same. It comes to us usually in a container format, like a zip file. And inside there, just depending on the type of return it is, it has some type of file system structure to it. It could contain anything from text files to phone backups. And so we generally treat it with the same process we treat all of our digital extractions.

Q. And did you also -- first, did that information provided by Google include photos and videos?

A. It did.

Q. Did it also include metadata?

A. It did.

Q. Did you have a chance to create a chart that included some of that metadata linked to the photos?

A. I did.

MR. KENERSON: Ms. Rohde, if we could have 1133, please, just for the witness.

BY MR. KENERSON:

Q. And do you recognize 1133?

A. I do.

Q. What is that?

A. This -- when the Google return came back, each of these images or movies had a file with it that contained the metadata or EXIF data out of each of those files. And so because they were all individually, I combined them onto one sheet, and that's the sheet that you see here.

Q. And did you have a chance to look at the exhibits in that chart? And I'll read them out: 404C, as in cat, 404F, as in Frank, 404G, as in gamma, 404K, as in kilo, 404N, as in Nancy, 404Q, 404V, as in Victor, 404W, 404X, 404Z, as in zebra, 404DD, 404EE, 404LL, 404V, as in Victor, V, as in Victor, 405I, 405M, as in Mary, 405N, as in Nancy, 405AA, 405BB, 405FF, and 405HH.

Did you have a chance to look at those exhibits?

A. I did.

Q. And did you have a chance to compare them to the data provided by Google?

A. Yes.

Q. Do they appear to be fair and accurate representations of the data provided to you by Google in connection with the account subscribed by Mr. Biggs?

A. Yes.

MR. KENERSON: Your Honor, I'd move for the admission of the exhibits I just read out.

MR. PATTIS: No objection on behalf of Mr. Biggs.

THE COURT: They will be admitted. And permission to publish.

(Whereupon, Government's Exhibit Nos. 404C, 404F, 404G, 404K, 404N, 404Q, 404V, 404W, 404X, 404Z, 404DD, 404EE, 404LL, 404VV, 405I, 405M, 405N, 405AA, 405BB, 405FF, and 405HH were entered into evidence.)

BY MR. KENERSON:

Q. And does this chart, 1133, fairly and accurately represent the metadata provided by Google?

A. It does. Google provided the photo taken time in UTC, and I did convert it to Eastern Standard Time for this chart.

MR. KENERSON: I would move the admission of 1133 as well.

THE COURT: It will be admitted. And permission to publish.

(Whereupon, Government's Exhibit No. 1133 was entered into evidence.)

MR. KENERSON: Thank you.

BY MR. KENERSON:

Q. Examiner Cain, I'm going to ask you a couple of questions like we asked with the data associated with Mr. Rehl.

The first column, that's the court exhibit name that we just read out. Is that right?

A. Correct.

Q. All right. The second column, Photo Title, what's the source of that data?

A. That is the actual name of the file on the device -- or in the Google return.

Q. Now, the Photo Taken Date/Time, what does that represent?

A. That's the EXIF data for the time that that file was created.

Q. And what about the EXIF latitude and EXIF longitude? What was the source of that data?

A. This is also in the EXIF data, and it is embedded in the actual photo itself.

Q. And just in a very broad sense, are you familiar with generally what those latitudes and longitudes on there correspond to?

A. Yes. Washington, D.C.

MR. KENERSON: And I'm going to ask Ms. Rohde to play just a couple of those. If we could have 404F, please.

(Whereupon, Government's Exhibit No. 404F was published in open court.)

MR. KENERSON: And if we could return to the chart really quick, Ms. Rohde.

BY MR. KENERSON:

Q. 404F, what we just watched, what does the metadata indicate in terms of the date and time of that?

A. January 6th, 2021, 12:55:54 p.m.

MR. KENERSON: Ms. Rohde, if we could have 404Z, as in zebra.

(Whereupon, Government's Exhibit No. 404Z was published in open court.)

MR. KENERSON: Thank you.

Ms. Rohde, if we could go back to the chart.

BY MR. KENERSON:

Q. 404Z, as in zebra, what was the date and time of -- associated with that exhibit?

A. January 6th, 2021, at 1:16:25 p.m.

Q. Now, these photos and videos that are represented in this chart -- well, first of all, let me ask you, there's -- I have not yet asked you about the final column that is labeled "is trashed." What does that represent?

A. These photos were deleted and in the trash bin.

Q. What's the source of that data?

A. The Google returns.

Q. And if a Google return lists "true" for "is trashed," what does that mean?

A. It means that the user deleted that file.

Q. Now, were these the only photos and videos in Mr. Biggs's iCloud account from January 6th, 2021?

A. No, they were not.

Q. Approximately how many more were there?

A. Roughly 40 to 50.

Q. And about what percentage of those had "true" labeled for "is trashed" in the Google return?

A. 100 percent.

Q. Thank you.

MR. KENERSON: I don't have any further questions, your Honor.

THE COURT: All right. Cross-examination for Mr. Nordean.

CROSS-EXAMINATION

BY MR. SMITH:

Q. Good morning, Ms. Cain.

A. Good morning.

Q. I just have a few questions about some of your testimony on direct. I'm Nick Smith. I'm representing Ethan Nordean.

So you testified about how groups work in Telegram, the Telegram application. Right?

A. I did.

Q. Okay. And you also testified about how users -- Telegram users gain access to those groups. Right?

A. Yes.

Q. Okay. And you testified about some of the digital forensics tools that your team and you use to analyze messages that were extracted from Telegram. Correct?

A. Yes.

Q. Okay. So let's assume that a Telegram user has been admitted to a group and gains access to messages going forward in that --

A. Okay.

Q. -- group.

The user can then open the window in the Telegram application and look at messages that are being sent within that group window. Is that sort of how that works?

A. Look at all the messages in that group chat?

Q. Yes.

A. Is that what you mean by window?

Q. Yes.

A. Then yes. Yes.

MR. SMITH: Ms. Rohde, would you help me bring up Government Exhibit 1137? I would do that, but that's not one that we have digitally. And not to play the videos, but just to show the display for the chats.

Okay. Can we publish that to the jury, Ms. Harris?

Thank you.

BY MR. SMITH:

Q. Ms. Cain, can you see the -- do you remember testifying about this image on Telegram?

A. Yes, I do.

Q. Okay. So is this sort of -- does this look, appear -- if you were a Telegram user and you were admitted to a group chat and you were to open that group chat and look at messages, is this roughly how that would appear to a user in the chat window?

A. It is. There are some settings. You can change the colors. But this is how it would look, yes.

Q. Okay. So is this a group chat that we're looking at right here?

A. It is.

Q. Okay. So in our hypothetical, let's say that a Telegram user is admitted to this group chat. Okay?

A. Okay.

Q. And let's say we are the user right now looking at this window. Okay?

The user would be able to scroll through these messages going back and forth and look at all of them. Right?

A. That's correct.

Q. But the tools that you've been discussing that allow you to analyze these messages, those tools can't tell you when a user has looked at any given message within this window. Correct?

A. No. In the winter of 2021, Telegram did not do read receipts for individual users in a group chat.

Q. And if I'm -- correct me if I'm mistaken, but did you testify about read receipts on direct?

A. No, I did not.

Q. Okay. What is a read receipt?

A. When the user looks -- actually opens up and the phone is recorded as digitally have -- seeing the message.

Q. And how does a read receipt display on this? How would you know whether a user -- if you had access to a user's phone and the user was admitted into a Telegram group, how would you tell, from looking at their phone, that they've read a particular message? What would be the visual item?

A. Well, in group messages in 2021, the read receipts were for -- if any person in that one group had seen that message, then a checkmark would appear. So if you look in one of these -- any of these green bubbles in here, you can see that there is a check-checkmark in the bottom right-hand corner. That indicates that at least one group member has received that. It does not indicate which group member or how many group members. It just indicates that someone, just one at least in the group, has seen it.

Q. Okay. Thank you for that. That was very helpful.

So let's -- I'm going to give you another hypothetical here. I'm going to draw on the screen. So let's say -- can you see that I've circled the user Captain Trump, and there appears to be a message from them?

A. Well, this is a message from Mr. Bertino's account in direct reply to Captain Trump.

Q. Sorry. I should have clarified that.

So this message I've circled in green, the user here we're looking at from the perspective of is Bertino. Is that correct?

A. That is correct. Yes.

Q. Okay. So if we're in the perspective of Bertino here, can we -- you can see that Bertino in this message is responding directly to one from Captain Trump. Correct?

A. That is correct.

Q. So we can make a fair inference that Bertino has seen that message from Captain Trump, because he's responding to it. You could make that inference.

A. Sure. Yes.

Q. It could be a mistake if someone is texting in response -- if Bertino is texting to Captain Trump there, it could be mistaken, but we can also make an inference that Bertino has seen that message from Captain Trump because he's responding directly to it. Correct?

A. Yes. He would have had to select that message in order to reply directly to it.

Q. Okay. Now, let's take a slightly different -- let's ask a slightly different question here. I'm circling a message from someone else, someone -- it appears to be -- this appears to be from a user called Aaron of the Bloody East.

A. That is correct.

Q. Okay. So that message I've circled was posted by Aaron of the Bloody East, whoever that may be.

A. Yes.

Q. On this window, just taking this window as our universe, we don't see that Bertino, the user, has responded to that message. Correct?

A. No. That is Aaron of the Bloody East.

Q. Right.

A. So that is an incoming message.

Q. And we don't see that Bertino, the user of this chat, is responding to that particular Aaron of the Bloody East message. Correct?

A. That is correct.

Q. Okay. So with the technology as it stood in these Telegram chats in this case, we don't know whether Bertino, the user, viewed that message. Correct?

A. No. All we can show is that his device received it.

Q. Okay. And so I guess one might make an inference that if Bertino -- let's remove that circle and let's draw Bertino's message that we were -- I've drawn a circle around Bertino's message again. You can see that Bertino's message is immediately below, in physical space, the Aaron of the Bloody East message. Correct?

A. Correct.

Q. So one might make an inference that the user there, Bertino, has seen that message because it's directly above. Correct?

A. You could. Yes.

Q. Yes.

So in your review of Telegram groups in this case, is it fair to say that some of them have hundreds or thousands of messages?

A. Across all their chats?

Q. Yes.

A. Yes.

Q. Okay. So the inference one might make about Bertino seeing -- Bertino seeing a message that's directly above one of Bertino's messages might not be the same kind of inference you'd make about Bertino, the user here, seeing a message that was, say -- let's say it was hundreds or thousands of messages above that one. Correct?

A. I don't presume to know what he -- you know, how he viewed his messages. I just know that the device received them.

Q. Well, so -- you've qualified as an expert in digital forensics and you've -- I think you said you've reviewed thousands of --

A. I have. Yes.

Q. Okay. So I guess I'm asking you based on your experience about -- are you familiar with the habits of users in chat apps?

A. I am. Yes.

Q. Okay. So is it fair to say that the inference one might draw about what Mr. Bertino, the user here, has seen is different for a text that's immediately above -- a chat that's immediately above where the user responds to a message and a chat that's, say, hundreds of messages above that -- a chat that the user has responded to? Do you understand my question?

A. I believe so. Yes. I mean, because he is responding directly to Captain Trump, I think it's safe to say that he has definitely received that message.

Q. Okay. So let's say -- let's assume this were -- we're in a group chat window here. Right? And let's say the group chat had hundreds of messages in it, like some of these. Okay?

A. Uh-huh.

Q. Then let's say there was a user who didn't send any messages at all in the chat group. None. Would you make an -- is there any tool that you have that allows you to say that that person who's been admitted to a chat group but has not sent any messages there -- is there any tool that allows you to show that that user has seen anything in the chat group?

A. No. I can just tell if the device has received them or not.

Q. Okay. So you've testified about a few -- the names of a few chat groups in this case that you've -- where you've analyzed the Telegram data. Right?

A. Correct.

Q. The original MOSD group was one of those?

A. There is -- I don't believe the title was original MOSD. There was one --

Q. Ministry of Self-Defense?

A. Yes. There was one called Ministry of Self-Defense.

Q. And I think -- have -- have you been characterizing this as maybe the first Ministry of Self-Defense group or the original Ministry of Self-Defense group?

A. Yes. There are, in fact, two groups with that name. And there was one that was created first. Yes.

Q. And the second one was what you were characterizing as a super group?

A. That is correct.

Q. Okay. So those are two groups we have there, the first MOS -- Ministry of Self-Defense, or MOSD, group, and then the super group. Correct?

A. Yes.

Q. Did you also testify about a chat group called the MOSD op group -- O-P, for operations, I guess?

A. Yes.

Q. So did there come a time when you had conversations with the prosecutors about whether particular Defendants in this case had communicated in those chat groups?

A. Yes. I looked for membership in those groups.

Q. And you looked for membership by particular Defendants to see whether they were involved in these groups?

A. Yes.

Q. Okay. So isn't it the case that you advised the Government that Mr. Nordean was not involved in any of -- did not send messages in any of those three groups I've just listed?

MR. KENERSON: Objection to what she advised.

THE COURT: Sustained.

BY MR. SMITH:

Q. Did there come a time when you learned that Mr. Nordean did not send messages in those three groups I just mentioned -- and to recall your memory, the original MOSD group, the super group and the MOSD op group?

A. I believe he did not contribute actual messages to the MOSD op group. However, I believe he contributed messages to the others.

Q. Can you recall any of those messages?

A. Not off the top of my head, no.

Q. Okay. Do you know whether -- has the Government made an inquiry with you about any of those messages that Mr. Nordean apparently sent in the other two groups?

A. Not specifically. I know that I have --

Q. Do you recall seeing any of them?

A. I do recall seeing some of them. Yes.

Q. And what were those?

A. I don't remember the content, but I know there were quite a few in the Ministry of Self-Defense larger group.

Q. So if I told you that the Government has conceded in this case Mr. Nordean did not send any messages in that group, you would say they're mistaken about that?

MR. KENERSON: Objection. Vague. Which group?

THE COURT: Sustained as to vagueness.

BY MR. SMITH:

Q. So if I were to inform you that the Government has taken the position that the original MOSD group -- in the original MOSD group and the super group, Mr. Nordean has not sent any messages, you would say that's inconsistent with your memory?

MR. KENERSON: Again, objection. Vague. Which group?

THE COURT: Overruled.

THE WITNESS: I know that -- I know he has sent messages in one of the Ministry of Self-Defense groups. I am not sure whether it was the smaller one or the larger one. I know he did not contribute messages to the Ministry of Self-Defense op group.

BY MR. SMITH:

Q. Okay. So let's -- let's cover Telegram handles. I don't know if that was the term you used, handle or nickname or -- so what I'm referring to is people will -- users in Telegram will use pseudonyms to identify themselves sometimes. Correct?

A. Usernames. Correct.

Q. Username. And the username is not -- sometimes is not the same as the legal name of the user. Right?

A. That is correct.

Q. Okay. So just for an example, your name is Kate Cain. You could appear in Telegram as something other than Kate Cain?

A. Correct.

Q. Okay. So there's no -- you testified about an identification number that each user has, like a -- kind of like a snowflake, has a unique fingerprint for each user. Correct?

A. That is correct. Yes.

Q. Okay. But there's no way in the application for a user to look behind the Telegram name and the identification number and find the legal name of a user. Is that right?

A. No, not the legal name. Not unless they chose to provide it.

Q. Okay. So it would be possible for individuals to communicate on Telegram without having any way to determine who that person is -- what the legal name of that person is. Correct?

A. Well, you are required to register your Telegram account with a phone number. And so we can use that as attributable to a certain person because you must verify -- when you create the Telegram app, it sends you a text message verification. So we do know the phone number associated with most Telegram accounts. Yes.

Q. Thank you. So that is very informative.

But I was asking about someone who's not law enforcement. So when you say "we" -- you know, you have access to certain data because you have search warrants and grand jury subpoenas. I'm asking about somebody who's a civilian user.

Say you and I are both civilian users of Telegram. Okay?

A. Yes.

Q. And we're not using our legal names when we communicate with each other.

A. Okay.

Q. Okay? And there is no way in the Telegram application for me, a civilian user, who does not have search warrants and grand jury subpoenas -- there's no way for me to look behind your Telegram name and find that you are Kate Cain.

Correct?

A. You can choose to expose the phone number or have it hidden. So --

Q. You could choose -- so a user can choose --

A. The user chooses.

Q. A user can also choose not to reveal their phone number and their legal name. Correct?

A. Correct.

Q. And if you and I are communicating on Telegram and we choose not to use our legal names and our phone numbers, there would be no way for me to know who I'm talking to in the real world. Correct?

A. Correct.

Q. Okay. So if you and I are communicating in Telegram and we've chosen not to use our real names, if I was using the name Captain Trump and you were using Sergeant Trump, for example, okay, I can't be sure it's you and I who are speaking unless we communicate outside of Telegram using another medium, like the telephone, for example. Right?

A. Sure.

Q. Okay. So -- are you familiar with what chatbots are?

A. In what context?

Q. In the context of social media use.

A. Somewhat familiar.

Q. What are they?

A. You can have, essentially, artificial intelligence create posts and create content. I mean, I'm just vaguely familiar with them.

Q. Are they algorithms that allow -- are they algorithms that mimic human speech --

A. Yes. That's fair --

Q. -- that are not controlled by humans?

A. That's fair to say. Yes.

Q. Okay. And you testified that you're an expert in social media use. Correct?

A. In digital forensics behind social media applications. Yes.

Q. And have you -- in the thousands of phones and computers that you've conducted forensics on, have you familiarized yourself with social media use on those devices?

A. Yes.

Q. Okay. So is it fair to say that chatbots are a relatively prevalent phenomenon on social media?

A. They are used. Their uses are limited these days, as most social media blocks the ability to use them nowadays.

Q. Does Telegram?

A. It does, as of this fall. Yes.

Q. This fall?

A. Yeah.

Q. But it wasn't at the time?

A. No. Not at the time.

Q. Okay. You testified about Telegram encryption. Right?

A. I did.

Q. Okay. So other -- that -- explain what -- did you testify that the users in Telegram chat groups are communicating through an end-to-end encryption system?

A. No, I did not.

Q. What did you testify about encryption?

A. Telegram, by default, uses encryption anytime the message is in transit. And we consider it a client side to a user side encryption, meaning you create a message on your device. It is sent to the Telegram server. And while it is being sent to the Telegram server, it is encrypted. And then once the Telegram server delivers that message, as it's being sent to the recipient, it is also encrypted. So anytime that message is in transit, it is encrypted and locked with those keys and cannot be accessed with anyone without those keys.

Q. So there were a wide range of commercially available chat applications that feature encryption. Correct?

A. There are. Yes.

Q. Like WhatsApp is one?

A. Yes.

Q. Signal?

A. Yes.

Q. Telegram is another?

A. Yes.

Q. So -- you said you're familiar with these applications. Right?

A. I am.

Q. So you're familiar that billions of users around the world use encrypted chat apps to communicate?

A. Yes.

Q. Okay. So it's not intrinsically a proof of criminal activity if individuals are speaking through a chat app that's encrypted?

A. No.

Q. I think you testified that you yourself use Telegram, perhaps?

A. Yes.

Q. Okay. So you testified about -- what are some of the tools from the toolbox you used to analyze the messages from?

A. We have a variety of in-house tools and commercial tools available to us. I think the ones we spoke about earlier was Cellebrite's Physical Analyzer.

Q. And you used the tool Cellebrite here to manage your extraction of Telegram devices. Right?

A. Some of them.

Q. But you didn't use -- would you say the vast majority of them?

A. Yes. I would say.

Q. Okay. But Cellebrite is actually not equipped to handle extracting Telegram messages, is it?

A. No, that's not correct.

Q. That's not correct?

A. No.

Q. Have you ever taken the position with the Government that it was not adequate for extracting Telegram messages in this case?

A. I have taken the position that it was not adequate for a programming project, that -- we had a team developing an in-house commercial tool to parse Telegram messages, and they wanted to build it based off of Cellebrite's platform, and I said that that was not an appropriate use of the tool.

Q. Okay. And have you taken the position in this case that using Cellebrite to extract Telegram messages gets you wonky message extraction?

A. Up until a certain point -- I believe 7.38 -- was that it gave some wonky messages. Everything used here in this case today was 7.42 and above. So those messages are accurate.

Q. Can you explain what you mean by -- what's that distinction about?

A. Sorry. That's a version distinction. So we are currently on Cellebrite .60. So that's, you know, a range of about 22 different versions over the last two years.

You know, as -- there are 4 billion apps in the -- or 4 million apps in the Google store and 3 million apps in the Apple store, and so our tools don't parse all of them. You know, they -- our commercial tools focus on what is relevant to the digital forensics community, what is relevant to the casework of the people buying their product.

And so early on, in those earlier versions, you know, as Telegram was just being used and just being parsed by the digital forensic community, there were some limiting capabilities. Sure.

Q. So --

A. But every release adds new functionality.

Q. So did there come a time when you took that position that Cellebrite would get you wonky Telegram messages with respect to the prosecutors in this case? Did you inform them of that?

A. With respect to this case?

Q. Yes.

A. No. To our programming team, who is developing a solution, I told them they should not base their solution on an old version of Cellebrite.

Q. Okay. And how are you sure that the current version of Cellebrite is any different from -- has resolved the problems that you identified yourself with wonky message extraction on Telegram?

A. I provide -- I do testing and validation on all of my tools, and pretty much every version I use undergoes some type of testing and validation by both my unit and personally by myself.

Q. So it's not the case that you have taken the position that Cellebrite itself, just Cellebrite period, not a specific version, is the very worst tool for extracting Telegram messages? You've never taken that position?

A. I told that to our programming team when they were writing a solution. Yes. I told them they should not use that particular version of Cellebrite to parse those messages in a tool that they were currently building, that there were others ways to build the tool more effectively. Yes.

Q. Okay. So your position is that you were not -- your position before was not that Cellebrite, period, is ineffective at extracting Telegram messages?

A. No. Not at all.

Q. Okay. So --

MR. SMITH: Your Honor, I'm going to bring up an email from Ms. Cain on February 9th, 2022. This is impeachment material.

MR. KENERSON: Objection. Can we go to the phones?

(Whereupon, the following proceedings were had at sidebar outside the presence of the jury:)

THE COURT: Let's just do this. It would be helpful for me to see the document while we're having this discussion, but we don't want to bring it up for the witness.

MR. SMITH: I can proffer for your Honor that -- she took the position that she formally advised the Government that it was a specific version of Cellebrite that would produce wonky Telegram extraction. And the email says Cellebrite, period, produces wonky Telegram extractions.

THE COURT: Mr. Kenerson?

MR. KENERSON: I think she's already -- I don't think that there is anything inconsistent with her testimony there. I mean, the Court can see the email. But I think her testimony has been, yes, I said those things. That's what was in the process. I don't think there's anything inconsistent to impeach her with at this point.

MR. SMITH: Your Honor, the inconsistency is she just -- we went through a colloquy several times where I asked her, Is it Cellebrite itself that produces wonky extractions or is it a particular version? The witness said, a particular version.

The inconsistency is, in this statement she made, it's Cellebrite, period.

THE COURT: I think -- look, again, if you give her a chance -- I think it's at least arguable it's inconsistent. The witness has to be given the opportunity, though, to explain the statement. When it comes -- and we've sort of tabled the question of whether these things come into evidence.

But I think Mr. -- and to be clear, when you say, "taken the position," the impeachment is about prior statements, not prior positions. The witness has --

MR. SMITH: This is a prior statement. Thank you, your Honor.

And, your Honor, under the D.C. Circuit precedent, we're entitled to publish it to the jury under 613(b), because this is -- the best evidence, the D.C. Circuit has held, of an inconsistent statement is the statement itself.

THE COURT: I'm not sure there is an inconsistency. You can show it to her and ask her about it.

MR. SMITH: That's all we're asking for.

MR. KENERSON: On the question of what can be published to the jury, I think to the extent that there is an inconsistent statement, this is just that statement. It's not the entire email and not the entirety of her -- I think it needs to be redacted if it's going to be shown to the jury.

THE COURT: That's fair. That's a fair point.
Isn't it?

MR. SMITH: Your Honor, we will draw a line above the irrelevant and immaterial information that has no bearing on this case earlier in the email. But, your Honor, the jury has to have some context. If I redact everything except the word "Cellebrite," then the jury won't see what the statement is.

THE COURT: Obviously. But I mean, if we're going to put up -- it's a fair request from the Government. I want you to show it to Mr. Kenerson before we continue so at least we can have -- we don't waste more time with this redaction issue.

MR. SMITH: Okay, your Honor.

THE COURT: Thank you.

Mr. Smith, the other thing we could do -- I know you've set up the impeachment. If you have more to do -- we're coming up on a break. If you want to, we can circle back during the break and do your redaction cleanly when we come back.

MR. SMITH: That works, your Honor. Thank you.

(Whereupon, the following proceedings were had in open court:)

BY MR. SMITH:

Q. So apologies for that.

MR. SMITH: Your Honor, how many minutes before --

THE COURT: I think we're about ten or 15 minutes away from a break for the court reporter.

BY MR. SMITH:

Q. Ms. Cain, I'll come back to that question after a break.

So you testified about the means by which a user can delete, who within that chat group can delete messages. You testified about the potential ways that could occur. Right?

A. Yes.

Q. Okay. And you said that one way that can happen is when the user deletes their own message. Correct?

A. Correct.

Q. Okay. And you testified that in the case of -- there might be a distinction when it comes to administrators, group chat administrators, deleting messages between super groups and smaller groups. Correct?

A. That is correct.

Q. And I think you testified that in the case of a super group, which has a certain number of members in it, an administrator of a chat can delete any message they choose to delete within that group. Correct?

A. They can. Yes.

Q. But you testified that when it comes to groups that are not super groups, a smaller number -- that the administrator of the chat cannot delete messages. Right?

A. That is correct.

Q. That's not correct. Right? So --

A. No, that is correct. As of the winter of 2021, administrators of a small group cannot delete messages for the entire group that they did not author.

Q. So it -- how do you know that? Is that -- well, scratch that. Let me rephrase the question.

Have you reviewed Telegram user protocols and instructions from the Telegram company?

A. I have.

Q. And don't they indicate that at any time, both in the winter of 2021 and the present, that a user -- that an administrator of a chat group of any size can always delete messages?

A. They can always delete their own messages and delete for everyone.

Q. Don't those -- don't those Telegram instructions indicate that they can always delete anyone's message?

A. No, they do not.

Q. Okay.

MR. SMITH: Your Honor, I think we would want to use that impeachment material now.

THE COURT: All right. Let's just take our break just a few minutes early.

Ladies and gentlemen, we're going to take a quick break for the court reporter's sake. Ten minutes. We'll come back and pick up the cross-examination then.

(Whereupon, the jury exited the courtroom at 10:42 a.m. and the following proceedings were had:)

(Thereupon a recess was taken, after which the following proceedings were had:)

THE COURTROOM DEPUTY: Jury panel.

(Whereupon, the jury entered the courtroom at 10:58 a.m. and the following proceedings were had:)

THE COURTROOM DEPUTY: We're back on the record on Criminal Matter 21-175, the United States of America versus Ethan Nordean, et al.

MR. SMITH: Your Honor, just an update. We have an agreement with the Government on the proper redactions. It looks like there's a crayon on the page, but...

THE COURT: Very well.

(The witness retakes the witness stand.)

MR. SMITH: Permission to publish the redacted email on the jury screen?

THE COURTROOM DEPUTY: Do you have an exhibit number?

MR. SMITH: It's called impeachment material. The judge has indicated that these are not --

THE COURT: Well, let's identify it by a number.

MR. SMITH: We can identify it as Nordean Exhibit No. 4.

THE COURT: All right.

THE COURTROOM DEPUTY: Exhibit 4.

Permission to publish?

THE COURT: Yes. Permission to publish is granted.

BY MR. SMITH:

Q. Ms. Cain, I'm sorry for how this looks, but do -- you see this appears to be an email with some green redactions. Right?

A. It is. Yes.

Q. And do you see that the "from" line says from Jennifer Katherine Cain?

A. I do.

Q. And it says: Sent Wednesday, February 9th, 2022?

A. I do.

Q. Okay. Now, there's a couple of points I would like to direct your attention to here.

In the middle paragraph, the second paragraph -- I've drawn a yellow line next to it. And you appear to be referencing parsing Telegram extractions through Cellebrite. And you indicate here that, "I don't have any other cases on your list, but I can pretty much say with certainty that they will be missing or have wonky Telegram data as well if you relied solely on Cellebrite to parse it."

Then I would direct your attention to the last sentence in the next paragraph, with the yellow line next to it, where you say, "However, the issue is that Cellebrite simply cannot handle Telegram the way that some of our other tools can. It's the very worst, actually."

So you testified that there was a particular Cellebrite version that had created a wonky or missing Telegram extraction?

A. I did.

Q. Here, it appears you're saying, "The issue is that Cellebrite cannot handle Telegram the way some of our other tools can. It's the very worst, actually."

A. Yes.

Q. Would you like to explain?

A. Sure. This is an email I wrote to our programming team, who I had been working with for the better part of a year. They were trying to create a custom solution to parse Telegram. The version that we were working with, since we had been working on it for over a year, was 7.38. That did parse Telegram -- what I consider wonky. And the way I determined that is the effectiveness for my case agent to be able to go in there as a nontechnical person and review that data.

So the way -- for instance, the way they parsed it at the time was they did not parse the group name; they only parsed the group identifier.

And as this case has heavily relied on the names of these Telegram groups, it's not attractive for me to present a solution -- to present a report to my case agents in my investigative review by saying, this is group No. 4097987677. You know, they like to see, this is group Ministry of Defense.

And so those earlier versions, while technically not incorrect -- all the messages were there, the dates and times were correct, the sender, whether it was incoming or outgoing, was correct, the content of the message itself was correct, the attachment was correct -- none of that was in question.

What was in question was the fact that it wasn't optimally suited for a non-technical person to review that data. For instance, I'd love to see it separate into a section called private chats and then for the user to be able to go down and see a section called groups, and then maybe super groups, and then channels. I like to see a division. I like to lay it out very easy for the investigative team. That is my job, is to take hard-to-understand technical data and present it in a way that is very easy for a non-technical person to understand.

The way that Cellebrite parsed it back in 7.38 is not the easiest way for a non-technical person to read that data. So I did not think that we should develop a tool that was not only going to be used on this case, but future cases, based on an output that I just couldn't hand to my case agents and let them run with it.

So this was to that programming team. We actually came up with other solutions --

MR. JAUREGUI: Your Honor, objection. Narrative.

THE COURT: Overruled. The witness can complete her answer.

THE WITNESS: So when I came to this case and this came up as a question, I took all of the Cellebrite reports that correspond to the devices that were used in this case and I simply validated them all. I opened them all up. I reran them in a multitude of different programs, including parsing the database myself in some instances. I compared the data that Cellebrite was parsing back to the actual device and the way it was displaying in the Telegram app itself on that actual device.

And I came up with the -- just that all of the data was technically correct, and that the only thing that, you know, from a forensic standpoint that I wanted to do was add those group names in.

So what I ended up doing is, because they parse it in Cellebrite and it only showed the group number, I created a master list of all of the group IDs and their corresponding group names, and I turned that over to the case agents so they were able to review all of their data in the best way and easiest way possible.

BY MR. SMITH:

Q. Thank you.

So I have one final question for you. You indicated that the version of Cellebrite that you're testifying today that was problematic with respect to Telegram extraction, that was 7.38, you said. Right?

A. Yes, it was.

Q. Okay. Do you see the first line in your email right there? It says, "I can rerun it through Cellebrite. I've been working with Cellebrite's programming team to fix the portions of Telegram, so some fixes have gone through as the 7.52 version."

You appear to be referring to the later version right there. Right? 7.52?

A. In this email for the changes that we had talked about.

Q. Yes. And then, several sentences below, after having obtained 7.52, that version, nevertheless, you say, "The issue is that Cellebrite simply cannot handle Telegram the way that some of our other tools can. It's the very worst, actually."

So you made that statement after receiving 7.52.

Right?

A. Well, after I said, "So some fixes have gone through as of 7.52," the next sentence says, "I can run it in 7.52," which has been redacted. So I had not actually run it in 7.52.

Q. Just so you understand, the Government asked me to redact that.

A. I understand.

Q. Okay.

MR. SMITH: Thank you for your testimony. Thanks.

THE COURT: Counsel for Mr. Biggs.

CROSS-EXAMINATION

BY MR. PATTIS:

Q. I'll be very brief, ma'am.

My name is Norman Pattis. Dan Hull and I represent Joe Biggs. How are you?

A. Well. Thank you.

Q. You graduated University of South Florida in 2017. Correct?

A. Yes, sir. For my master's.

Q. University of North Carolina, 2003. Correct?

A. Yes, sir.

Q. Tell us about your first job, your internship with the Disney World Company.

A. Out of college, I took an internship in the hospitality industry with Walt Disney World. I worked in a variety of hotels down there in recreation.

Q. Were you giving people tours, like where they could meet Mickey, Goofy, Mary Poppins?

A. I did not, no.

Q. Okay. Because, as you testified -- the way you look at the jury and testify, I sort of feel like I'm on one of those intern tours when you go to Disney World.

A. I wish. But no.

Q. Me, too. Bye.

MR. PATTIS: Nothing further.

THE COURT: Counsel for Mr. Rehl.

CROSS-EXAMINATION

BY MS. HERNANDEZ:

Q. Good morning.

A. Good morning.

Q. My name is Carmen Hernandez and I represent Zachary Rehl. You know his name --

THE COURT: Use the microphone, please.

MS. HERNANDEZ: I need a lavalier.

BY MS. HERNANDEZ:

Q. I'm going to ask you a number of questions. I'll stipulate that you know more about technology than I do. Let's start there.

A. Okay.

Q. Let me show you --

MS. HERNANDEZ: Ms. Rohde, could you pull up Government's Demonstrative Exhibit -- I think it's 1131.

BY MS. HERNANDEZ:

Q. I'm going to show you the Government's demonstrative exhibits. I believe they're 1131 or 32. Ms. Rohde is pulling it up for us.

MS. HERNANDEZ: You can just do one of the later ones -- the one that has all the info on it.

BY MS. HERNANDEZ:

Q. So I want to start there. And this is supposed to demonstrate what happens when you -- you got a phone. You extracted -- or someone extracted the information from the phone. That's the second column. Is that correct?

A. Yes, ma'am.

Q. And when we say extracted the information from the phone, it's literally this little device takes the information that is on the phone and -- does it download it into, like, this hard drive or something?

A. It creates a containerized file, either an extraction or a binary file. And we just save it to another location. So that just represents just a location that we have saved that copy to.

Q. Okay. And in theory, it's supposed to have all the information that was on the phone that you extracted?

A. Depending on the type of extraction that we get, it could differ from device to device. Yes.

Q. Okay. And does that mean you can extract only certain information, if that's the only information you're looking for?

A. When we do an extraction, whatever is available for that type of extraction, we would get it all.

Q. All of it?

A. Yes.

Q. Okay. And then there's this next column, which is supposed to represent, I guess, some messaging on -- is this the way it would look on Telegram?

A. Well, we've used the common iPhone green bubble/blue bubbles here. It doesn't necessarily look exactly like that. We've obviously left out date stamps and message ID numbers. But -- it's just a visual, yes.

Q. But it's a visual -- so this visual, this type of visual -- I understand it's missing dates and names and whatever -- is this what you would find on the phone itself or is this what you would find once you extracted it?

A. When we extract the phone, we get the data from each application. Most commonly, these are stored in databases.

Q. So that means you would get, like -- words like "hello" and "hi," but the extraction doesn't show these little bubbles. Is that correct?

A. The extraction would not show the bubbles. No.

Q. Okay. But if, instead of the extraction, if you were -- let me back up one other question.

Although -- you've extracted phone information. Correct?

A. Yes.

Q. And one of the phones you extracted was Mr. Rehl's phone. Correct?

A. Yes, ma'am.

Q. You still have the phone?

A. I don't personally have the phone.

Q. Okay. The Government -- someone still has the phone. Someone --

A. I assume so, yes.

Q. -- over here still has the phone?

A. I assume so, yes.

Q. If I or if you were provided that phone and you opened -- would you be able to open a Telegram chat?

A. Possibly, yes. It depends on a couple of factors.

Q. Okay. And if you open that Telegram chat on the phone, would it appear as -- in this third column?

A. Well, this is a representation. But a chat would appear with -- you know, visually similar to this.

Q. Okay. So visually similar to this. And we've all agreed that it would have words in these bubbles and maybe a date and the name of the person?

A. Yes.

Q. But the information that you've extracted -- so the phone would give you a representation that is much more similar to this chat ID, third column. Is that correct?

A. That is correct.

Q. Whereas the information you extract -- and I'm not suggesting you're doing anything wrong -- it's just that's the way technology works. When you extract, you're just extracting the words.

A. We get all of the raw data. So we get much more than you see on the device itself or represented in these chat bubbles.

Q. And this particular demonstrative appeared to be a conversation maybe between two people?

A. Yes.

Q. And this would -- if this were all you were dealing with, this would allow you to say -- let's say this were Mr. Rehl's phone. Would Mr. Rehl be in green?

A. No. He probably would be in blue, because the outgoing messages are usually on the right-hand side.

Q. Okay. So if this were, for example, a chat between Mr. Rehl and his wife, for example, then you would be able to see Mrs. Rehl and Mr. Rehl and you would be able to clearly say they were having a conversation between the two?

A. Uh-huh.

THE COURT REPORTER: Is that yes?

THE WITNESS: Yes, ma'am. Sorry.

BY MS. HERNANDEZ:

Q. Now, obviously, you've talked about these chat groups that you have in this. And these chat groups can contain -- what's the outer number that some of these chat groups you've looked at in this case? How many people?

A. I think just above 100.

Q. Okay. So in a chat that contained 100 people, the raw data that you got obviously would not be -- but you would have a large amount of raw data?

A. We do. Yes.

Q. And you wouldn't be able to identify in the same way as you can with two people who they're talking -- that they're talking to each other. Correct?

A. We would see the chat. It would be that this message belongs in this particular chat group.

Q. But you would not be able -- let me break that up into two boxes.

In your raw data extraction, you would know that there's 100 people in this chat. Correct?

A. Yes, ma'am.

Q. This is an example. At any one time, all or some of those 100 people would be posting?

A. Yes, ma'am.

Q. But you would not necessarily know whether they were responding to each other. Is that correct?

A. If a message was in direct reply to another message? Is that what you're asking?

Q. Yes.

A. We can get that information out of the database.

Q. Sometimes?

A. Yes.

Q. So in other words, if I -- if the message was, "What time is it," and the very next message said, "It's 3:43" --

A. Yes, ma'am.

Q. -- you could infer that the 3:43 is a response to "What time is it?"

A. That would be logical. Yes.

Q. Okay. But some of these messaging threads -- is that the right terminology?

A. Sure. Yeah. That works.

Q. Some of these messaging threads aren't so clear that it's a direct response. Would you agree?

A. In the chat database?

Q. Yes.

A. There is a column that tracks if a message is in direct reply to another message.

Q. Okay. Let's talk about that.

When you say there is -- I'm sorry. There is a what that tracks it?

A. The database tracks it.

Q. You said there is something that tracks whether it's a direct response.

A. Yes. Potentially there's a table with a record.

Q. And would that be -- would I need the phone to see if it's a direct response?

A. We could see that in the database.

Q. You could see that in the database?

A. Yes, ma'am.

Q. You could see that in Cellebrite?

A. Not earlier versions. That is a functionality that they added this past year in one of their releases. Yes.

Q. So do you know whether you've reextracted Mr. Rehl's phone using this new database?

A. We did not -- well, we don't -- it's not reextracting. It would be reprocessing that extraction. We would still work off of that original copy of the device.

Q. So as to Mr. Rehl's phone, do you know whether you reprocessed it with this new upgraded format?

A. No, we did not. I believe it came out in November or December past, when we had made all of our final exhibits for this.

Q. So today, you could go back and reprocess -- tell me if this is true. Today, if you wanted to go back and reprocess, you could reprocess the information from Mr. Rehl's data and actually see which messages he responded to or which he didn't respond to?

A. Well, it wouldn't be -- it would be if the user directly replied, took the action of selecting a message and then replying directly to that message.

Q. Okay.

A. Yes.

Q. So maybe you can -- before I go on, so let me -- so the program that you used, or the model number or however you want to define it, you used when you extracted Mr. Rehl's phone on Cellebrite did not have this function that you're describing for the jury today?

A. At the time, no. None of our forensic tools did.

Q. So the information that we -- and the Cellebrite extraction that you did, I believe you know was provided to the defense. Correct?

A. Yes, ma'am.

Q. Okay. So the Cellebrite extraction that we have -- we, the defense counsel and Mr. Rehl -- does not contain this new function that you're describing today. Correct?

A. I do not believe it does. No.

Q. So what we have doesn't -- what we have -- and I believe it's what the Government has, what the prosecutors have also -- does not let us determine whether any particular person was responding to another person. Correct?

A. In direct response, no.

Q. It doesn't. But today, you have the -- is it the technology to actually determine that?

A. I believe so. I believe one of the Cellebrite releases that came out at the very end of last year, either November or December, I believe they added that capability in.

Q. Okay. So using the old system, which is the one we're all working on, if you have a large chat with a lot of people, the only way you could tell, from the Cellebrite extraction, whether the responses were directly to another person or not is, would you say, by inference?

A. Yes. That's accurate.

Q. And again, by inference, the example, "What time is it," says one person, and the next person, seconds later says, "It's 4:36 p.m."?

A. Yes, ma'am.

Q. And so that would be inference that he's responding to that?

A. Yes, ma'am.

Q. But under the old system, which is what we have, unless you can draw that inference, the answer could be to what someone posted two weeks ago. Correct?

A. Yes, ma'am.

Q. Or could be just an idle comment that isn't even related to anything previously posted?

A. We just wouldn't be able to tell.

Q. You couldn't tell. Okay.

So if I get a string of messages one right after the other that were posted all on the same day, that still wouldn't be able to tell you whether they were responses to each other under the system that -- under the extraction that you've provided to us?

A. Correct.

Q. Okay. Thank you.

So let me -- before I go on, Telegram is -- there are millions of users in the United States and in the world who use Telegram. Is that correct?

A. I believe so. Yes.

Q. It's not -- did I hear you say that you have Telegram also?

A. Yes, ma'am. I test all of our applications.

Q. Okay. So you just have it on your phone just to test it, not because you use it?

A. I -- yes. I test it. That's why I have it.

Q. Do you also use it?

A. I use it extensively for testing.

Q. Okay. You also mentioned other -- like WhatsApp?

A. Yes, ma'am.

Q. And that's another messaging app?

A. Yes, it is.

Q. I'm getting better at this. That's another messaging app --

A. Yes, ma'am.

Q. -- that people can use to communicate?

A. Yes.

Q. For example, WhatsApp, I -- I use it because you can make international calls without having to pay a toll or something like that. Is that right?

A. I believe so. Yes.

Q. Okay. So that's a useful tool?

A. Yes.

Q. And it doesn't -- and these multiple -- did you say there's like 3,000 apps?

A. There's 4 million apps in the Google store and almost 4 million -- or 3 million apps in the iTunes store.

Q. So these apps are just apps that are out there that people can use. They don't denote any -- in any particular case -- they don't mean that you're a criminal if you use these particular apps. Correct?

A. I don't know why anyone -- no.

Q. So it's just an app that you can -- one of many apps that people -- that the young ones use to communicate with each other these days. Is that correct?

A. It is an app. Yes.

Q. Okay. So one of the things you spoke about was orphaned files?

A. Yes, ma'am.

Q. Okay. And tell me a little bit about an orphaned file. I tried to follow, but I'm not sure. How does an orphaned file -- how is an orphaned file created or why does it exist?

A. For this particular case, the term "orphaned file" means any kind of attachment. It's a known attachment from the Telegram database, so it's an image, video, audio file or document that we know has been transmitted as an attachment, but we don't actually have the message that corresponds with that attachment being sent.

Q. And I do understand correctly that if you have an orphaned file -- let me back up.

So an orphaned file is someone at some point, using Telegram, say, for example, sent another person or sent a chat, an email -- I'm sorry -- say a video or a photograph?

A. Yes, ma'am.

Q. And would that file that was sent -- could it have been sent to an individual or to a whole chat group?

A. Either one. We would not know.

Q. Okay. So if it's orphaned, the reason it's orphaned is because the original message is no longer found on Telegram?

A. That's correct. We consider the message the parent. So it's a child without a parent.

Q. So you have this video, for example, out there. And did I also understand, from some of the information that we've been provided, that these orphaned files, you cannot tell when it was created?

A. We can tell based on the type of file it was. There are certain things, such as when I talked about EXIF data earlier, on videos and images -- the creation date is embedded in that EXIF data, so we can tell the creation date.

Q. So, for example, if I took a picture right now, there would be some information on that photograph that showed that the picture was taken today?

A. Yes, ma'am.

Q. Okay. So even on those orphaned files, you would know when the picture was taken; is that correct?

A. For a picture or a video. Yes.

Q. Okay. But for those orphaned files, you would not know when it was transmitted; is that correct?

A. That is correct.

Q. So if I took a photograph -- let's say I took a photograph today and, for whatever reason, it became orphaned. You would not be able to know -- you would not be able to tell us whether it was sent today or it was sent seven weeks from today?

A. Well, forensically, we could narrow down that window based on the EXIF data and the other metadata of that file.

Q. So how far can you narrow it?

A. It just depends on the file. For instance, we take a picture today. The EXIF data would have a creation date embedded in that file. And then I send that message through Telegram to my friend.

When my friend's phone gets that message, the attachment is added to that device's file system, and that file system will have a date on it. So if I sent it today -- if I took it today, I sent it today, I would have that embedded in the actual image itself. And then, on my friend's device, if he looked at it this afternoon, that same image would have a file system date on his device of, say, 3:00 p.m. this afternoon, so I would know that that image had been transmitted sometime between my creation date at 11:00 a.m. and his file system date of 3:00 p.m. So I could narrow that window down based on those two types of dates.

Q. So if your friend didn't open the video until two weeks from the day you sent it --

A. Yes, ma'am.

Q. -- then the window would be two weeks?

A. Yes, ma'am.

Q. So you couldn't narrow it any further?

A. No, ma'am.

Q. Okay. And is that because you're using Cellebrite or is that just because it's an orphaned file?

A. That's just the forensic science between how the date stamps work in image files and how file system date stamps work.

Q. So even if you went back to the original phone, the receiving phone and the -- or the receiving device and the sending device, you still wouldn't be able to narrow it more than as you've described?

A. Correct, because the message is gone.

Q. Okay. So one of the videos that was shown to you by the Government -- and I'm going to need Ms. Rohde's help again. So the Government played a video, 403G, for you.

MS. HERNANDEZ: Ms. Rohde, could you take this down?

So 403G -- could you please pull it up. I'm sorry, Ms. Harris.

MR. KENERSON: This screen is still showing the PowerPoint.

THE COURTROOM DEPUTY: That's what I have, too. But it's set on "Plaintiff."

MS. HERNANDEZ: Do I have to delete this maybe?

THE COURTROOM DEPUTY: I'll reset it. It's still coming up.

THE COURT: Also, for the record, could the Government identify the exhibit that -- I think, when we first brought up the prior exhibit that Ms. Hernández was asking questions about, I'm not sure it was identified for the record.

MR. KENERSON: The demonstrative is 1131.

THE COURT: 1131. Very well.

MS. HERNANDEZ: Thank you, your Honor.

BY MS. HERNANDEZ:

Q. So the Government played this video for you. It's 403G.

MS. HERNANDEZ: Could you play it.

(Whereupon, Government's Exhibit No. 403G was published in open court.)

BY MS. HERNANDEZ:

Q. So your testimony on direct --

MS. HERNANDEZ: Thank you.

BY MS. HERNANDEZ:

Q. Your testimony on direct was that was -- that you found that video on Mr. Rehl's phone?

A. I believe so. Yes. I don't recall the exact device. But if that is what I said prior, then yes. Yes, it is.

Q. Let me show you -- and I believe this is Government's Exhibit 32 and it's already -- it's Government's

Exhibit 1132. And I have a paper copy.

So this is the exhibit that the Government showed you. And I believe that video is 403G, this one. Correct?

A. Yes, ma'am.

Q. And your testimony was that this was taken from Mr. Rehl's phone?

A. Yes, ma'am.

Q. And you're showing the photo was taken January 6 at 2:34 p.m.?

A. Yes, ma'am. Video.

Q. But you're not showing any other information with respect to that video?

A. Correct. When --

Q. So --

A. Telegram will strip most of that EXIF data out due to size restrictions.

Q. So you cannot tell us when that video was received by Mr. Rehl?

A. No, I cannot.

Q. And do you know how he received it?

A. Through the Telegram app.

Q. Through the Telegram. But you don't know whether it was posted on a chat?

A. I don't know where the original message is. No.

Q. Or whether it was sent to him as an attachment?

A. No. The original message has been deleted.

Q. Or whether he saw it on the 'net, for example?

A. Well, no. It would have been sent to him as an attachment.

Q. As an attachment through Telegram?

A. Through Telegram.

Q. But according to this, you were unable to determine when it was sent to him?

A. Correct. I just have the date the video was created.

Q. Or when he actually received it?

A. I do not know.

Q. Or when he opened it. Or how about if he opened it? Can you tell if he opened it?

A. No. But the file exists on his device, so I know that he did receive that message.

Q. You know that he received it. You don't know when he received it and you don't know whether he actually viewed it?

A. No, because the original message has been deleted.

Q. Okay. And is there anything -- can you rule out some things? So let me ask you this: Can you rule out whether that was sent to him contemporaneously? And by that, I mean at -- January 6th at 2:34 p.m.

A. No. That is a possibility.

Q. But it's also -- it's just a possibility?

A. Yes.

Q. It could have been sent to him three days later?

A. Yes. The message has been deleted.

Q. And you can't determine how the message was deleted?

A. I do not know how the message was deleted.

Q. And when you say the message was deleted, that doesn't mean he deleted the message. Correct?

A. No. It's most likely whoever authored that message.

Q. Whoever authored that message --

A. -- is most likely --

Q. -- the person who would have deleted the -- the post or the chat? I don't know how -- what's the term?

A. That is the most likely scenario.

Q. Okay. Thank you.

You were also shown a number of -- I believe you were shown Government's Exhibit 1136. I believe you have a copy of 1136 in front of you.

A. I do.

Q. And I have a copy here.

And I believe you were asked a number of questions about how this was deleted from all the -- several devices. Is that correct? Do --

A. Yes, ma'am.

Q. -- you recall?

A. Yes, ma'am.

Q. And I believe you were asked questions -- it was deleted from all the devices, I believe was what you answered?

A. For the messages that do not appear in this chat thread, yes.

Q. So -- and you -- let me -- I believe what you said, with respect to 1136, was that it was not -- the 12:56 p.m. message, it was not recovered from any device. Is that correct?

A. May I refer to the notes?

Q. Yes. And if you need anything else to refer to.

A. Yes, ma'am. The video at 12:56.

Q. Okay. And the video at 12:56 was this thing here. And you believe that that was a video sent by Mr. Bertino. Is that correct? Or recorded by Mr. Bertino?

MR. KENERSON: Objection. Both misstates and kind of vague as just referring to "here" without noting for the record --

MS. HERNANDEZ: I'm sorry.

BY MS. HERNANDEZ:

Q. That's the 12:56 message that we're talking about that you just said was not recovered on any device.

A. Oh, the 12:35?

Q. No. I thought it was at 12:56. I'm sorry. I'm pointing to the wrong thing. The 12:56 was the one that I understood you to say was not recovered from any device.

A. Oh, okay. The video. 12:56 video message. Yes.

Q. That was sent by Mr. Bertino? Do you know?

A. It appears that the video message was from Mr. Donohoe.

Q. Okay. It was Mr. Donohoe.

And do you know -- it appears that someone on the ground in D.C. on January 6th was videotaping some of what was going on. Do you recall these videos that you played?

A. I recall the videos that we entered. Yes.

Q. And is that accurate the way I'm describing? Somebody on the ground on January 6th of 2020 was recording some of what was -- 2021 -- was recording -- somebody on the ground on January 6th, 2021, was recording some of what was going on outside the Capitol?

A. Yes. We had a number of videos.

Q. I mean, we know a lot of people were recording. But I'm talking with respect to this particular exhibit, 1136, that you were shown, someone on the ground was recording some of this information and posting it on this chat?

A. Yes.

Q. And do you know -- the person who was doing this recording, was that -- if you know, was that Mr. Donohoe?

A. I believe for this message it was.

Q. Okay. And you indicated that the messages -- that the reason they weren't recovered from any device is that you believe the message had been deleted?

A. That is correct.

Q. And I believe you were asked your opinion, since it was deleted from all the devices, does that mean that the administrator for this group was the one who deleted it?

A. I don't remember if this was a group or a super group.

Q. Okay.

A. I just know that the message went -- whoever selected to delete it, instead of deleting it for just the device, selected to delete it and remove it from all of the users.

Q. And what does that tell you about who could have deleted it?

A. The user could have deleted it.

Q. The user could have deleted it?

A. And -- sorry. I don't recall if this was a super group. But then in that case, the administrator could have also deleted it.

Q. Okay. And can you tell from here who -- which group it was?

A. I believe it was the New MOSD chat.

Q. Okay. And is there any document that would tell you who was the administrator for New MOSD that you could look at?

A. I do not recall if I recorded that in writing.

Q. Okay. But essentially -- so the fact that it was deleted from all the devices would indicate to you that one person with some administrative capacity deleted it?

A. Or the person that authored that message.

Q. Or the person that authored it. Because otherwise, you would find it in one of the other devices. Is that correct?

A. That's true. I mean, there is the possibility that the two devices we have that contain this chat, that both of those users selected to remove that message from their device. I cannot rule that out as a possibility.

Q. Okay. And at one point, I believe you indicated that some of these messages were found on Mr. Rehl's phone but not on other devices. Correct?

A. That is correct.

Q. And that means he didn't delete them. If they were found on his device but not on others, that means he -- he had not deleted them from his device?

A. Correct.

Q. Okay. You talked a little bit about encryption.

MS. HERNANDEZ: I can take this down.

BY MS. HERNANDEZ:

Q. Encryption is something that is fairly common with the internet; is that correct?

A. Depending on certain chat applications. It is widely used today.

Q. And the reason for encryption, the primary reason, is to secure data. Correct?

A. Correct.

Q. I mean, the average person who sends an email through any number of -- Hotmail, AOL, whatever -- ordinarily, those applications have encryption in them. Correct?

A. Those do not --

Q. So if I send you --

A. -- use encryption.

Q. Those do not?

A. Not by default. No.

Q. But you can choose it?

A. Certain providers allow you to.

Q. Retail stores use -- like, if I go online and purchase something from a retail store, it's likely that the information I'm sending is encrypted?

A. I can't speak to that.

Q. Banks?

A. I don't know how their systems are run. I really can't speak to the encryption services that they use.

Q. Do you know of any encryption -- Department of Justice, when they send an email to you, that's encrypted?

A. I believe it is.

Q. Any other entities that you're familiar with that encrypt their -- their information so -- at least in transmitting the information. Correct?

A. Yes, ma'am.

Q. That's much more common, in transmitting the information, it's encrypted?

A. Correct.

Q. And that's done so that the entire world, except maybe the hackers and the 13-year-old boys in this country, can't read what you're writing. Correct?

A. It's to secure the data in transit. Yes.

Q. Okay. And in fact, there's a lot of websites where you go on and the prefix is HTTPS.

A. Yes.

Q. When the S is added to the end of that HTTPS, that's because -- that means it's secure?

A. It does. The protocol used to transmit.

Q. And that's likely to -- let me write this so that you can see that. And you can see that -- HTTPS, that's what we're talking about?

A. Yes, ma'am.

Q. And you can go on any number of websites and, if you see that S, it denotes that there's some security in the --

A. That's what the S stands for. Yes.

Q. Okay. And again, that's pretty common and ordinary in today's world?

A. Yes.

Q. And would you say that's much different or the same as what the Telegram encryption is?

A. Well, this is a totally different type of --

Q. Encryption?

A. -- securing data. This is not technically encryption. It's the protocol used to transmit the website contents, so...

Q. But do you agree with me that the encryption used by Telegram is fairly common and ordinary for a number of these apps?

A. They do use a combination of established encryption protocols. Yes.

Q. Okay. And the theory is that encryption keeps the internet somewhat safe or secures Internet privacy?

A. For your data, yes.

Q. And in fact, there's a number of federal regulations that demand that kind of encryption. Correct?

A. I would assume so.

Q. Like if you are communicating with an M.D. or a hospital or something with health insurance -- with the HIPAA regulations, usually those people have to -- hospitals and doctors, doctors' offices, have to have encryption to secure the information being transmitted. Correct?

A. I would assume so.

MS. HERNANDEZ: Just a moment, your Honor.

BY MS. HERNANDEZ:

Q. I know there was some questions about your view of Cellebrite and how useful it was in extracting Telegram information.

Am I correct that there are other programs that extract information that may be more suited -- may have been more suited to extracting Telegram when the extraction in this case took place?

A. Every -- we use a variety of commercial tools, and they all have their strengths and weaknesses. So it's a personal preference.

Q. But you identified, I think, an entity named Oxygen -- or a program named Oxygen?

A. That is the tool I used for one of the devices. Yes.

Q. And you believe that was, at least in some instances, a better fit to extract Telegram data?

A. For that particular device, it was.

Q. And that particular device, is it because it's Android versus Apple?

A. That's a large part of it. Yes.

Q. And just -- Apple is the iPhone?

A. It is, yes.

Q. And Android is?

A. Any non-iPhone, aside from the Windows phone, most of them run on a version of the Android platform.

Q. And again, that's -- and I may be misstating, but that's basically a -- it's like the brand -- maybe "brand" is not the accurate description, but the difference between Apple and whatever else -- the other one is essentially the manufacturer?

A. It's the operating system.

Q. The operating system. But certain manufacturers -- Apple uses Apple whatever, technology, whereas the other phone companies might use a different -- anyone other than Apple uses a different system. Correct?

A. Relatively speaking, yes.

Q. And I think I'm at the end of my questions. I just want to make sure.

So one of the concerns with Cellebrite is that while it extracts information, when it displays it, it loses some of the information that is found in Telegram itself?

A. It displays the messages. However, you know, databases store many types of different information. And as we see the need to include more, we request enhancements from those programs to include additional functionality.

Q. But you lose the ability to see -- what's a pinned message on Telegram?

A. A pinned message?

Q. Pinned, P-I-N-N-E-D.

A. In a super group, in a larger group like that, the administrator can -- it looks like a little pin tack that you'd use on a bulletin board. And that essentially puts that message at the top of the chat so that, when new users come on, they see that this somehow has been flagged for an important message and that they should read it. And so no matter when they come in the chat, no matter how the history is set, even if that message was made and pinned two years ago, anybody new coming in can see that because it's been designated as important.

Q. And -- I mean, if you use Facebook or Twitter or something, you can pin certain messages. That's a similar concept?

A. They each have their own version, I believe. Yes.

Q. Which means, I want you all to know that I have -- that I gave birth last week or that I got married a year ago or whatever?

A. Sure.

Q. And you lose that ability to see whether a message was pinned when you just extract?

A. No. Cellebrite parses the pinned messages.

Q. It does?

A. It does.

Q. How about -- I should probably leave some of this for some of my more technically adept people, but let me -- co-counsel. But just one last question on Cellebrite. The Cellebrite program that you used when you extracted the information in this case was not as -- would you say it was not as good as the current version?

A. It's always adding functionality.

Q. So the current version is -- has more functions than the one that you used at the time that you downloaded this -- that you extracted this info?

A. It does potentially display more data. Yes.

Q. And again, if I -- is there some -- there is some information on the device itself, on the phone, that, if I had the phone here, I could ask you to go to a particular message and you could provide me more information about whether that message was responding to a particular message or that type of thing than you can from the Cellebrite extraction. Am I correct on that?

A. That's something we could determine from the device itself or from the database, the Telegram database.

Q. I know. But what I'm asking you, is that accurate, that if you had the device itself and you could -- if you had the device itself right now, if you had Mr. Rehl's phone right now, you could go to -- the phone should still have the Telegram app on it?

A. It should. It just depends on a variety of circumstances.

Q. Okay.

A. The type of extraction we got and how it interacted with that device, if we were provided the PIN or passcode to that device. If it had been removed or placed into airplane mode since the extraction, that could have an effect. But in a perfect scenario, we could look at the device and see that.

However, we are able to get a lot more data from the database itself than we can by looking at the device itself.

For instance, all of these orphaned files, they would not be present -- if you were to just open up the Telegram application on the device, you couldn't see those. Those were items that we pulled out of the Telegram application itself. So you wouldn't -- the end user wouldn't be able to see them. So in that case, reviewing the physical device would not --

Q. Let me go back to the orphaned video files that we discussed earlier. I understood that Cellebrite timestamps may or may not have any correlation whatsoever to when the actual message containing the video was sent. Is that accurate?

A. So the -- when you say the Cellebrite timestamp, that's most likely referring to the file system timestamp. As we discussed in our earlier scenario, if I were to send a video and it had a creation date embedded in it and then, when it hit that other user's device, that file system timestamp -- in my scenario, I had -- I sent a message -- I composed it at 11:00 a.m. The device received it at 3:00 p.m. I could not say from the file system timestamp that the message was received at 3:00 p.m.

Q. But you -- and that's different, I guess -- and I think you said this already, but I just want to make sure. The embedded timestamp does tell you when it was created. That's -- on an orphaned file, that's pretty much -- and particularly, the one I showed -- the one that we played, the only thing you have on that is the time it was created?

A. For videos and images, we would have the creation date embedded in the file and then, on any other devices that it was present on, we would have the file system timestamp.

Q. But the one we played -- and there was an exhibit that went along with that -- only had the time it was created. Do you remember that?

A. Yes, ma'am. I don't believe we pulled any other dates surrounding that.

Q. Okay. One last thing. You looked at a number of chats. Is that correct? A number of Telegram chats?

A. I did.

Q. And there were a number -- and you know the Defendants in this case. Correct? You know the names of the Defendants in this case?

A. Yes, ma'am.

Q. And some of the chats -- some of the Defendants in this case were not in all the chats. Would you agree with me with that?

A. I believe that's accurate.

Q. Like, for example, there's a chat that's identified as the Elders chat. Are you familiar with that chat?

A. Yes, ma'am.

Q. Mr. Rehl was not in that chat?

A. I don't -- sorry. I don't recall from memory who was present -- a member of which chat.

Q. Okay. If I showed you something --

MS. HERNANDEZ: I will mark this as Mr. Rehl Exhibit 40, which is a list of chats that the Government produced.

And if I may approach.

THE COURT: It will be marked for identification purposes?

MS. HERNANDEZ: Yes, your Honor.

THE COURT: Very well.

BY MS. HERNANDEZ:

Q. Mr. Kenerson gave me that, just so you can be confident.

A. Thank you.

Q. And are there a number of chats that Mr. Rehl did not belong to?

A. May I?

Q. Yes, please.

A. Yes. There are a number of chats.

Q. Can you identify what those are?

A. May I read from this?

Q. Yes, please.

A. Mr. Rehl was not a member of Skull and Bones, 2020-2021, the MOSD Vetting chat, which was renamed to Noble-MOSD Vetting chat.

Q. And Vetting, that's V-E-T-T-I-N-G?

A. V-E-T-T-I-N-G, yes.

The chat called Elders; the chat -- MOSD Prospect chat, which we referred to in our exhibits as East Coast Prospect; OG Pickle Back Crew; Space Force chat; WB Stream chat.

Q. Thank you.

One last question. I understood you didn't do all the extractions yourself. It was a team effort?

A. It was a team effort. Yes, ma'am.

MS. HERNANDEZ: Thank you very much for your time.

May I get the exhibit back?

THE COURT: You may, ma'am.

Counsel for Mr. Tarrio.

MR. JAUREGUI: Thank you.

CROSS-EXAMINATION

BY MR. JAUREGUI:

Q. Good morning again, Ms. Cain.

A. Good morning.

Q. Almost good afternoon.

A. Good afternoon.

Q. Ms. Cain, who's the lead FBI agent on this case?

A. The lead agent that I worked with is Special Agent Nick Hanak, H-A-N-A-K.

Q. Is he here today?

A. Yes, he is.

Q. Now, Cellebrite was developed in Israel. Correct?

A. I believe so.

Q. And they sell this product, the Cellebrite product, to Russia, China, Myanmar, Iran, some pretty oppressive governments. Correct?

A. I don't know who they sell it to.

Q. Now, Cellebrite has two parts; is that correct?

A. Could you elaborate more?

Q. Sure. The first part is the UFED, which stands for the universal forensic extraction device. Correct?

A. That is one of their products.

Q. Okay. And that extracts data from a mobile device and backs it up to a Windows PC. Correct?

A. I actually don't use that product, so I'm not familiar with how it works.

Q. Which product is the one that you use?

A. I used -- with this case, we used Cellebrite Premium.

Q. Got it.

And the latest version of that is 7.60. Correct?

A. Cellebrite Premium, I'm not sure what the latest version is. It's probably somewhere between 7.58 and 7.60.

Q. Okay. And you're an expert in computer forensics. Correct?

A. Yes.

Q. You didn't bother to look up what the latest version of the most important tool in this case is?

A. I believe a version came out last week, and I'm just not sure which version that is.

Q. Understood.

And Cellebrite itself has various trainings and classes. Correct?

A. They do.

Q. Okay. And you've taken, I assume, the Cellebrite mobile forensics fundamentals course.

A. I have not.

Q. Okay. I assume you took the Cellebrite certified operator course.

A. I did not.

Q. Well, then, you must have taken the Cellebrite certified physical analyst course.

A. I did not.

Q. How about the Cellebrite -- since we're talking about Premium -- the Cellebrite certified Premium operator course?

A. I did take that.

Q. Great.

Did you take the Cellebrite in-system programming course?

A. No.

Q. How about the Cellebrite advanced smartphone analysis course?

A. No.

Q. Did you take the Cellebrite Apple fundamentals course?

A. No.

Q. How about the Cellebrite Android fundamentals course?

A. No.

Q. Then you definitely didn't take the Cellebrite advanced forensics course?

A. No.

Q. Now, in this case, I think it's very important -- you're saying you did not do the extractions in this case or you only did some extractions?

A. Only some of them.

Q. Out of the gentlemen here in court, which extractions did you do?

A. None of their devices.

Q. You didn't do a single extraction of a single Defendant in this case?

A. No. I believe they were all done by different divisions.

Q. Is that because you're in Knoxville, Tennessee?

A. I am now. When I began work on this case, I was in the Tampa division.

Q. Now, you've testified before, and you compared an extraction to a blood draw at a doctor's office. Correct?

A. I believe I did. Yes.

Q. You get a phone, just like a nurse or a doctor at a hospital or at a medical setting, and under controlled conditions, they draw somebody's blood. Correct?

A. Yes.

Q. And the reason you draw the blood in these controlled conditions is because you don't want any contamination in that blood. Correct?

A. Well, I believe you draw it so that you can test it.

Q. Of course.

But if you draw it incorrectly, if you contaminate the blood, once you take it to the lab, the results aren't going to be correct. Wouldn't you agree?

A. That's correct. You would not want to contaminate it.

Q. And in one of the most important cases in the United States of America, you decided it was not important to do the extractions yourself?

A. Oh, no. It is a generally accepted practice, especially when we have cases that span the entire country -- we have 56 field offices -- it's neither practical nor probable for me to visit every single one of those divisions when we have CART-trained examiners in every single field office that can do it locally.

Q. So I can order something from Amazon and have it the same day, but the FBI cannot send you a phone next-day air for you to do the extraction yourself. Is that what you're telling the ladies and gentlemen of the jury?

A. No. It's more preferable to have the local division do it. We wouldn't want any outside factors to come in. It's important that, if it comes in powered on or if we have the code, that we take the best steps to preserve that evidence. And so I wouldn't risk sending a phone across the country just so I could extract it when my team in, say, Seattle has the exact same capabilities and tools to extract that locally and just get it done on the same day.

Q. I'm glad you said that.

And the reason is, because when you do the extraction, you have to make sure that the phone is not connected to the outside world. Correct?

A. We try to.

Q. Right.

A. We always try.

Q. Right. Well, I mean, it's easy. You turn it on, you immediately put it into airplane mode, you turn the Wi-Fi off, those kind of steps. Correct?

A. Well, you do have to have the passcode, nowadays, to turn airplane mode off [sic]. So we try to preserve it in any way we can.

Q. Understood.

And as you sit here today, you cannot testify to the ladies and gentlemen of the jury that you have any personal knowledge whatsoever of the extraction process. Correct? You're just relying on somebody else's work, are you not?

A. We all follow the standard operating procedures to extract the device. And so when they created that extraction, they -- the examiners provided a hash value. And then when I received that extraction, when they copied it over to my network, I verified it, confirming that what they had done matched.

Q. Where are the handwritten lab notes that accompany the summary report of the extraction?

A. Where are the what?

Q. The handwritten notes that, under procedure, are supposed to accompany the extraction.

A. We don't -- we're not required to take handwritten notes.

Q. Okay. Aren't you supposed to create a summary report that describes the date and times that the action was taken in the extraction?

A. Our tools generate reports that say that for us. Yes.

Q. And where is that report? Did you provide that to the Government?

A. Those reports should come with the extractions themselves. The tools generate them. I know that, in this case, we used a variety of tools, both Cellebrite Premium and Grayshift GrayKey. And in those extractions, there are attached files that document that process.

Q. I'm talking about your forensic report or the forensic report of the person that actually did the extraction. Have you seen the forensic report of the actual person that did the extraction?

A. I looked at what they wrote up into our case file. Yes.

Q. Okay. And did you provide that to the Government?

A. I do not have a copy of that today.

Q. Do you know if it was provided to the Government, is my question.

A. I do not know.

Q. Did you create a forensic mobile phone submission form, as is required?

A. That is not a form that I am familiar with.

Q. Do you know if the person that actually did the extraction created that form?

A. That's not a term I've ever heard before.

Q. Now, Cellebrite can extract live data and hidden data.

Correct?

A. By live data, you mean what you would see displayed on the device?

Q. Yes.

A. Then yes.

Q. Now, live data is typical user info, like SMS, MMS, video, email, et cetera. Correct?

A. Sure.

Q. There's also hidden data. Correct?

A. There can be. Yes.

Q. And that typical hidden data is web history, email headers, picture data. Correct?

A. Well -- I'm sorry. I now don't follow what you mean by hidden data.

Q. Okay. Let me move on.

There's two types of extractions. Correct?

A. There are many types of extractions.

Q. Right. There's a logical extraction, which is what we're dealing with here. Correct?

A. No. That is not correct.

Q. Okay. What are we dealing with here?

A. Well, depending on the different devices, most -- for most of the devices in this case, we got full file system extractions.

Q. Would that be a physical extraction?

A. We use the term interchangeably. Some of our tools call it a physical extraction; some of them call it a full file system. They're kind of used interchangeably. Neither are -- you could say that. Yes.

Q. Right. But you would agree with me a logical and a physical extraction are two different things. Right?

A. They are two different things.

Q. Okay. And since you didn't do the extraction, you don't know what kind of extraction was done in this case. Correct?

A. Oh, no. I know what type of extraction was done.

Q. Because of the hash value that you testified earlier?

A. Well, no. That doesn't tell me the type of extraction. The accompanying report that comes with the extraction itself tells me what type of extraction it is.

Q. And that --

A. I believe it's also in the name of the extraction [indiscernible].

Q. -- will then --

THE COURT REPORTER: I'm sorry? Say that again.

THE WITNESS: The accompanying printout that our tools generate tell the type of extraction that it is. And also, most of our tools report the type of extraction in the actual extraction name itself.

BY MR. JAUREGUI:

Q. And the extraction is through Cellebrite?

A. The extraction is what?

Q. This extraction report you're speaking about, that's through Cellebrite?

A. It's the tool that generates it. So it would have been Cellebrite Premium generates a log file, and our Grayshift GrayKey generates a summary report in a PDF format.

Q. That's what I'm trying to figure out. When you say the report that's generated, are you talking about the report generated through Cellebrite or through GrayKey?

A. Yes.

Q. Which one is it?

A. Both.

Q. Both.

And in this case, you have both reports?

A. I reviewed all -- yes. I reviewed -- that came along with each extraction. Yes.

Q. Thank you.

Now, these extractions and these reports, they're not 100 percent reliable, are they?

A. Well, they're log files of how the system interacted with the device.

Q. How the tool interacted with the device. Right?

A. Yes.

Q. Now, you know -- you said you followed the releases, the updates on social media and the tools' websites, so on and so forth. Correct?

A. Yes, sir.

Q. And you know, of course, that Moxie Marlinspike, who's the creator of Signal, he had Cellebrite. You know that. Right?

A. I know that Signal and Cellebrite have interacted with each other. Yes.

Q. Okay. But you know that the tool was hacked by the founder of Signal?

A. It wasn't --

Q. It's a famous hack case. You've heard about it. Right?

A. It wasn't hacked. But I know to what you are referring, yes.

Q. You know what I'm talking about?

A. I do.

Q. Thank you.

Now, you're saying you did not personally extract Mr. Tarrio's phone. Correct?

A. That's correct.

Q. Okay. Now, isn't it true that Grayshift GrayKey is actually better at processing Telegram than Cellebrite?

A. Well, Grayshift GrayKey doesn't process anything. It's only a tool used to extract the data from the device.

Q. Right. But the question was, it works better than Cellebrite. Correct?

A. No. The extraction that you would get from Cellebrite Premium, if it was a full file system extraction, and the full file system extraction you would get from GrayKey would be nearly identical.

Q. Okay. And the reason you use Cellebrite is what? It's easier to use for the agents -- for the Government?

A. It's just depending on availability. Right now, we only have GrayKey for iPhones and we have Cellebrite Premium that works on Androids and iPhones. And as of today, all of our divisions are equipped with both of those. Back in 2021, each division typically only had one or the other just based on availability at the time.

Q. Okay. And you would agree with me there's a big difference between the Apple IOS and the Android systems. Correct?

A. Yes. There's a big difference in their operating systems.

Q. And, actually, the Android even varies by phone. I have a Samsung, and on the Samsung, there's all this bloatware, and actually, there's an extra kernel on top of the Android operating system. Correct?

A. I can't speak to the bloatware, but yes, Samsung would be different than, say, LG. They all use the Android platform, but they are slightly different operating systems.

Q. Okay. Now, my colleagues asked you about the different messaging apps, Signal, WhatsApp. Those are all encrypted. Correct?

A. They are.

Q. And even the simple Apple iMessage, that is also encrypted. Correct?

A. The iMessage is, yes.

Q. Now, on Telegram, it's also encrypted, but it's not end-to-end encryption. Correct?

A. Not by default.

Q. Okay. And not only that, but in these group chats, it's not even encrypted at all. Correct?

A. No. They are encrypted.

Q. Okay. Just not end-to-end encrypted?

A. Not end-to-end encrypted.

Q. Now, when a person does the extraction, they control all the factors, correct, as to the variables that they want to extract from the phone. Right?

A. No. When we do a full file system extraction, because of the way that our tool interacts with the device, we have to pull all of the data off. We do not get to select which portions. We copy the entire file system.

Q. And you know that because somebody wrote it on a report. Correct?

A. Because I know that's how the tools work. Yes.

Q. Okay. But when they use the tool, you would agree with me that the tool has endless variations and variables in it. Correct?

A. Not the extraction tools, no. When we hook it up to our extraction tool, it identifies the chipset in the certain device, the type of device it is, the chipset. And then the tool makes the determination on how to best extract that. It's not interactive with the user. The tool does it.

Q. So you can't pick a timeframe on the tool; is that what you're telling me?

A. For extraction, no. We would extract the entire device.

Q. Okay. Now, you did look at Mr. Tarrio's extraction. Correct?

A. I did.

Q. Okay. And you saw that he communicated through multiple mediums, text messages, Telegram and other applications. Correct?

A. I saw that there were many applications on there.

Q. And in the Telegram application, you saw he had countless threads and group chats and private and individual chats. Correct?

A. There were a number of messages and chats. Yes.

Q. And actually, he had about 32 and a half million unread messages. Do you remember that?

A. I do not remember that.

Q. You don't remember that.

Do you know how many unread messages he had?

A. No, I do not. But I know it was not 32 million.

Q. Okay. How many do you think it was?

A. I don't know, but I know that the total number of artifacts that we reviewed for that case did not reach anywhere near 32 million, so I know there weren't 32 million unread chats.

Q. And is there an easy way to look that up after -- you know, between -- you know, during lunchtime? Can you look that up through a Cellebrite report, perhaps?

A. No, not here, because the data set that we have provided has been scoped to the parameters of the search warrant. So it would not include --

Q. Okay.

A. -- the entirety of his --

Q. When you say that the data was scoped to the search warrant, what does that mean?

A. When we provided the final reports, we selected data that was relevant to the case here today.

Q. So you used a timeframe. Correct?

A. That was part of the consideration, but not the entire consideration.

Q. Got it.

So you were able to limit that to variables that you picked out in the tool. Correct?

A. For the final reports, yes.

Q. Got it.

Now, isn't it true that when data is not collected in a forensically sound manner, you inherently change the metadata?

A. I'm sorry. I'm just not sure what you mean by that question.

Q. Sure. If the extraction was not done correctly, the metadata could be contaminated. Isn't that true?

A. I'd have to see an example.

Q. Well, you'd have to see the phone and extract it, I guess. Right?

A. I would, yes.

Q. And just by seeing the extraction, you can't check the integrity of the data on the actual phone. Correct?

A. Well, as our tools are extracting the data, they take a hash value of the data that it expects to extract, and then, once it's done, it takes the hash -- that same hash value of the data that's come out, and that's how we receive that.

Q. But wouldn't it be best practice to have that report and then you have the phone with you to compare them both to make sure they're the same?

A. I did as part of my process, Yes.

Q. Yeah. But you didn't have the phone, did you?

A. I did not have the physical device. I did have the extraction with that. Yes.

Q. Understood.

So if the extraction was done incorrectly, the data is dead on arrival. Isn't that true?

A. I would assume -- I have -- I'd have no way to know that. I know that the data I looked at in this case, all the hash values matched; all the extractions were valid.

Q. I understand.

Now, you had already testified that you're not an expert in Telegram. So let me ask you just as to your personal knowledge. When using Telegram, when you use a reply or a swipe reply function, a review byline is created that allows two users to directly communicate without disrupting the flow of the overall chat with unnecessary confusion. Correct?

A. I'm not -- I'm not sure what --

Q. I'll break it up into pieces. I'm sorry. It's a long question.

You know what using a reply or a swipe reply is in Telegram. Correct?

A. Yes. When you reply directly to another message.

Q. Okay. When that happens, there's like a little review box that opens up. Correct?

A. There is.

Q. Okay. And that's done so that, as you're speaking back and forth, it doesn't create any kind of disruption in the conversation. Right?

A. I don't know the intent of it. I know that it does then display that message as your reply is in direct response to this other reply.

Q. Okay. When you extract that in Cellebrite, it doesn't show that. Correct?

A. In the earlier versions it didn't. As we discussed with Ms. Hernández, I believe the version that came out in November or December now does display that data.

Q. Okay. And again, you don't know if, in this new latest version, if it does that, because you haven't really looked at it. Correct?

A. No. I know that as of the version that came out in November or December, it does.

Q. It does. What version is that, to be clear?

A. I believe it was as of 7.58 or 7.59. I'm not sure of the exact version number. Just in the last few months.

Q. Understood.

But the version that we're working with, that Mr. Kenerson and I are working with, is that old one. Right?

A. Not the very first one that I had referenced, but somewhere in the 40s, the 7.40s.

Q. 7.40s or something?

A. Yes.

Q. And -- I mean, that's important. I mean, I get an update on my phone every few weeks. I can't even drive my car if I don't get it updated. Isn't that important for us to be working on the most updated Cellebrite version tool?

A. We try to use the latest tools. Yes.

Q. Okay. Now, extraction creates a complication in terms of the contextual conversation. Correct?

A. I'm sorry. Can you repeat that?

Q. Sure. You already said that in the extraction in Cellebrite, we can't see swipe replies or replies. So if we can't see that, it creates a big contextual complication. We don't really know who's responding to what or to whom. Correct?

A. Sure.

Q. Now, it's really problematic when you're using Telegram to explain a person's state of mind. Correct?

A. I don't have any knowledge of using Telegram to explain a state of mind.

Q. Well, the user interface factors in most of how the user conducts themselves. Isn't that true?

A. I'm sure that's personal to each person.

Q. Okay. And actually, some data gets missed if it's in a different format, like in a voice chat. Correct?

A. I don't -- I don't understand what you mean by "data missed."

Q. Well, isn't it true that in a lot of these Telegram messages the voice chats are missing?

A. We do have a lot of voice chats that have been deleted, yes.

Q. Yeah. And there's a lot of missing GIFs or photos, things that add context. Correct?

A. Yes. A lot of messages have been deleted.

Q. Okay. And, actually, there's missing messages that haven't been deleted. Isn't that true?

A. I --

Q. Not every single missing message was deleted. Isn't that true, Ms. Cain? Some of it are just artifacts that Cellebrite can't recognize correctly. Isn't that true?

A. No. The reply -- the message would still be there. It just wouldn't show that it was in direct reply to another message.

Q. I'm not talking about the replies; I'm talking about missing messages. Missing messages in a thread.

A. Uh-huh.

Q. Okay? You've seen those in these Telegram chats, correct, where there's just empty spaces?

A. Yes.

Q. Okay. Not every single empty space was a deleted message. Isn't that true?

A. No. That's -- if the message is missing and all that remains is the timestamp, then that is a deleted message.

Q. Isn't it true it could be a pinned message of some kind that Cellebrite can't recognize correctly?

A. No. Cellebrite parses pinned messages.

Q. It shows up as a big red X?

A. I think it has, like, a little icon and it says Pinned Message.

Q. Okay. But you can't actually see the pinned message. Isn't that true?

A. Well, it would be the message inside that container.

Q. Okay. Now, when looking backwards at these messages, without the user interface, we're pretty much guessing what the intent was. Correct?

A. I don't speak to the intent of these messages. My job is to provide the technical data in a useable format.

Q. And are you the person with the most technical knowledge in this prosecution team?

A. I did parse these Telegram chats and provide technical advice based on them, yes.

Q. Did anybody above you provide technical advice to the Government in this case?

A. Not to my knowledge.

Q. Okay. So you're the Government's tech person in this case. Would that be fair?

A. For this case, yes.

Q. Thank you.

Now, isn't it true that Telegram allows for editing and deleting of comments after being sent?

A. Individual messages?

Q. Yes.

A. I'm not sure if you can edit them back in the winter of 2021.

Q. Okay. Are you aware you can do that now?

A. I did not know that. No.

Q. Okay. So you didn't know that I can send a message, somebody can reply to my message, and then I can go back and change the initial message? You didn't know you could do that in Telegram?

A. I don't know if you could do that in the winter of 2021. No.

Q. Now, when checking to see if a comment has been read by other users, a double-checkmark will appear next to the comment. Correct?

A. That's correct.

Q. One checkmark means that the comment was sent and is ready for others to view and respond in the actual application. Correct?

A. That sounds correct. Yes.

Q. Now, we can't see any of these checkmarks in Cellebrite. Correct?

A. I don't recall if they included them or not, no.

Q. Okay. Would something refresh your recollection? Perhaps a Cellebrite report?

A. If we have those available.

Q. I do.

A. Sure.

MR. JAUREGUI: Ms. Harris, this is going to be Tarrio Exhibit 6. If we could just publish it just to the witness, please.

BY MR. JAUREGUI:

Q. Now, Ms. Cain, I'm showing you some Telegram messages between my client, Tarrio, and Lieutenant Shane Lamond, the head of the intelligence of the Metropolitan --

MR. KENERSON: Objection.

BY MR. JAUREGUI:

Q. -- Police Department.

THE COURT: Hold on. Is the witness being asked to refresh her memory about something?

MR. JAUREGUI: That's it, Judge.

THE COURT: All right. So why don't you just ask her the question about the topic at hand.

MR. JAUREGUI: Thank you.

BY MR. JAUREGUI:

Q. I'm going to show you this Telegram. I'm just going to scroll there.

Do you see these Telegram messages --

A. I do.

Q. -- between my client and Lamond? Are there any --

MR. KENERSON: Objection.

THE COURT: Sustained.

BY MR. JAUREGUI:

Q. Are there any checkmarks there?

A. There are no checkmarks.

Q. Okay. So in the Cellebrite version that we have, it doesn't display checkmarks, one or two, to determine whether something has been read?

A. Well, this is also not a group chat. This is an individual chat between two users.

Q. Okay. Does it show the checkmarks, yes or no?

A. It does not.

Q. Okay. Would it be fair to say, if it doesn't show it in an individual chat, it won't show it in a group chat? I could find you a group chat if you'd like.

A. I would prefer that you found a group chat. Yes.

Q. Sure.

MR. JAUREGUI: If we could publish this to the witness, please.

BY MR. JAUREGUI:

Q. Now, this is a group chat between Lamond --

MR. KENERSON: Objection.

THE COURT: I'm sorry, sir. Just ask your question about whether this refreshes the witness's recollection about the topic you've asked.

MR. JAUREGUI: Understood.

BY MR. JAUREGUI:

Q. I'm showing you some Telegram messages between different people -- we won't name who they are -- in a group chat. Any checkmarks on any of these?

A. No. But that's also not a group chat.

Q. It's not a group chat?

A. No.

Q. What is this? It's a group text?

A. It's two individuals.

Q. Oh, sorry. I have it as multiple people. I have it as -- I'll move along.

I have that one as three people. You didn't see three people there?

A. Well, it doesn't necessarily make it a group chat. It could still be a private message and not an official group with a name.

Q. Got it. Got it.

I'm showing you another Cellebrite report. Is this a group chat?

A. It is.

THE COURTROOM DEPUTY: What number is this?

MR. JAUREGUI: This is Tarrio Exhibit 50.

THE COURTROOM DEPUTY: 50.

BY MR. JAUREGUI:

Q. Did I finally score on this one? Is this one a group -- group chat?

A. Group chat. Yes.

Q. There's a lot of people on this one. Right? How many people do you think are in this one?

A. I have no idea.

Q. Hundreds, maybe?

MR. KENERSON: Objection. Are we refreshing at this point?

THE COURT: Does this refresh your recollection?

BY MR. JAUREGUI:

Q. Does this refresh your recollection, Ms. Cain?

THE COURT: About?

BY MR. JAUREGUI:

Q. About whether --

A. It does. There are no checkmarks.

Q. There's no checkmarks?

A. There are no checkmarks.

Q. Thank you.

Now, what this proves is that simply extracting the phone doesn't give you an accurate picture of what's happening on Telegram. Correct?

A. No. Extracting the phone will get all of the data off of the phone. The next portion is to then process that data into a readable format. So, yes, extracting the data still does get a complete picture of the data off of the phone.

Q. You mean you're getting a copy of the data of the phone. Correct?

A. That is correct, in the extraction.

Q. Right. But what I'm trying to say is the Cellebrite that we're all using does not give a real picture of the communications on Telegram. Isn't that fair?

A. I would say that's not accurate. I would say it does give a good picture of the communications, as it has every group in it, every private message; it has the users that contributed a message, the message itself, a timestamp, the name of the attachment, the attachment itself. So it has all of the key features included in order to read any given chat thread.

Q. So a good 50, 60 percent, let's say 70 percent -- that's good enough for court. Right?

A. No. I would say more like 95.

Q. 95 percent. Okay. Not 100 percent. I guess I got you there. Not 100 percent, right, of the communication?

A. I mean, maybe later versions -- I could put in some enhancement requests.

Q. It's a shame we didn't use that later version, huh, Ms. Cain?

Isn't it true that when somebody joins a group chat, they miss entire sections of the conversations that came before then?

A. There is a setting in the super groups where the administrator can choose to show the history from all time or choose to just show the history from when that person joins the chat. The default is to just show when that person joins onward.

Q. Got it.

And in the extraction, you can't tell that using Cellebrite. Correct?

A. You can't tell what?

Q. What you just said. That -- the administrator can activate a setting as to what a user can see. You can't tell whether the administrator activated that setting on Cellebrite. Correct?

A. Oh, no. I do not know that.

Q. Again, we're just guessing, right, on Telegram, whether the administrator did or did not do such a thing?

A. I could look in the database for an individual chat and find that information.

Q. But you didn't do that in this case. Correct?

A. Not for this one. No.

Q. I understand.

Now, this leaves us to try and piece together the original context based on our speculation. Isn't that right?

A. I'm not sure what your question is.

Q. Well, I just asked you, When somebody joins a group chat, do they know what was said before they got there? And you basically said no. Correct?

A. That is correct. They would just see messages going forward in the default setting.

Q. Got it.

So if they start writing, we don't even know what they're responding to. Correct? Because we don't know whether they did a swipe reply. Correct?

A. Well, if they just joined the chat, I would assume they're not responding to anything, because they haven't seen anything.

Q. Right.

A. So they would be replying to nothing.

Q. Right. But they can't do it the minute they get there. They can do a swipe reply. You just can't show it on the Cellebrite. Correct?

A. Well, if you join the chat and you can't see the history, then you can't reply to a previous message because there are no previous messages.

Q. Got it.

Isn't it true that Cellebrite processes the database inaccurately sometimes?

A. In my testing, in validation of the earlier versions of Cellebrite, I did find that Cellebrite was duplicating some of the records. And the way that databases work is they have a write-ahead log, which is called the WAL file, and when a user sends a new message, it writes that to the WAL file first, and then that's moved over to the database at a later time.

And so we noticed that, in the earlier versions of Cellebrite, they were processing and displaying some messages twice. So they were just duplicating messages. So the content was accurate; the timestamp was accurate; who the message was from was accurate. We were just seeing it in the database two times. And obviously, that person didn't send the exact same message at the exact same time twice because we were seeing it for several messages.

Q. And you actually told that to Agent Hanak in an email. Correct?

A. I did. I wanted him to be able to correctly interpret the data.

Q. Right. And you even told him, Cellebrite doesn't report with enough accuracy. Correct? That's why I hadn't sent you Paul Ray's phone before, even though you guys were clamoring for it. Correct?

A. For his device, I processed it with a different tool because, at that date and time, and the number of groups that he was a member in, I felt that the interface was more appropriate as a review tool. Yes.

Q. And you even said Cellebrite has weird ways of displaying the pinned messages. Correct?

A. Oh, we did have a question about one of the ways that the pinned messages were displayed. It put an icon -- it created an icon. Essentially, instead of just saying at the bottom of the bubble, "This message was pinned," it created a little pin icon as -- to draw attention to the fact that that message had been pinned. It's just a programming preference. They wanted to be able to draw attention, so they assigned an icon to it.

Q. Okay. And you also told Agent Hanak that whenever there's extensive group threads, they may not be parsed correctly, nor coherently, in Cellebrite. Correct?

A. When -- we have a lot of groups and super groups for these particular devices, and because each one of those has a unique identifier, and because Cellebrite doesn't display the chat by the group name, but it displays the chat by the group identifier, one chat thread could appear as two. So I wanted to just make sure that I drew the case agent's attention to that so that, if they were to look at any particular group, they knew that, for some groups, they needed to look at two chat threads in order to see the whole picture of that.

THE COURT: All right. Ladies and gentlemen, we're going to break for lunch. We will see you on the other side of our break. Thank you again for your attention and patience.

(Whereupon, the jury exited the courtroom at 12:35 p.m. and the following proceedings were had:)

THE COURT: You may step down from the witness stand.

Madam Court Reporter, do you have another ten minutes in you?

THE COURT REPORTER: Yes, Judge.

THE COURT: So we'll wait for Ms. Harris to return, and then I'll hear from you on the overnight issue, if you will.

Just in case the issue ripens today, why don't I hear from the parties on the issue that you all -- that was raised overnight, I guess, first by the Government and then Ms. Hernández responding in kind about what the Government wants to do with these additional exhibits. Whoever from the Government, I will hear from you. Then I will hear from it's appropriate to ask the question for that reason. So, I would move -- move beyond all this. I would sustain an objection as to foundation and scope.

But, again, this witness isn't going anywhere. If I rule all that admissible, of course, you'll be able to put it in in your case one way or another.

MR. JAUREGUI: Thank you.

Judge, please note any objection.

THE COURT: It is noted for the record. Very well.

(Open court:)

JENNIFER "KATE" CAIN,

CROSS-EXAMINATION (Cont.)

BY MR. JAUREGUI:

Q. Good afternoon, Ms. Cain.

A. Good afternoon.

Q. I think we were talking about Telegram, right, before?

A. Yes.

Q. Okay. Now I would like to show you a short little demonstration that I did on my phone with my -- the very talented Ms. Katinsky over there. I have Telegram on my phone. I'm going to just show you a video, and I would like you to just take a look at it. Okay?

MR. JAUREGUI: This is titled Demonstrative Aid 1A; is that all right?

THE COURTROOM DEPUTY: 1A?

MR. JAUREGUI: Sure.

BY MR. JAUREGUI:

Q. You know what kind of phone this is?

Is that a hint?

A. Oh, it's an Android.

Q. Yeah.

THE COURT: Counsel, has this demonstrative been shown to the government?

MR. JAUREGUI: It has, Judge. During lunch, I showed them.

THE COURT: Very well.

MR. JAUREGUI: Let me just get to the Telegram app here.

If we could publish, please, Ms. Harris.

THE COURTROOM DEPUTY: Permission to publish?

THE COURT: Permission to publish is granted.

BY MR. JAUREGUI:

Q. Does that look like the Telegram app to you?

A. It does.

Q. Great. I'm going to show you a short little video.

If the jury could please pay attention and look at it.

(Video played.)

Did you see that video?

A. I did.

Q. You said earlier that you didn't know whether messages could be edited after the fact. Now you know they can, correct?

A. In this current version, yes. I do not know if that was available in January 2021.

Q. Okay. Wouldn't it have been your specific job, as a computer forensic expert of the FBI, to find out if, back then, when the crime was allegedly committed, whether that option was available?

A. Well, as you can see from the video you just showed me, when a video -- when a message is edited, it actually changes the message itself and says "edited" at a specific time --

Q. Right.

A. -- instead of "sent" on a specific time. So, there would be indicators in the database if something had been edited after the fact. There would be a timestamp associated with that.

Q. On the phone, not on Cellebrite, correct?

A. Not on Cellebrite. In the database, in the extraction itself. That's something that we look at in the extraction itself.

Q. Thank you for your honesty.

Isn't it true that on Cellebrite, there's no pulls data, correct?

A. There's no what? I'm sorry.

Q. Pulls data. The pulls.

A. There's no pulls data?

Q. Right. When you pull a message. You don't know what pulling a message is?

A. I don't know what the context of that means, no.

Q. Okay. And there's no edit history on Cellebrite, correct?

A. I did not see -- in the January 2021 versions of Telegram, I did not see an edited column in the database, no.

Q. Okay. And, actually, there's no muting history, either, on Cellebrite, correct?

A. There is. You can mute history.

Q. On Cellebrite?

A. I'm sorry. Notifications, you can mute them, yes.

Q. Okay. But can you please listen to my question carefully.

Is there mute history on Cellebrite? Yes or no?

A. No, it doesn't show if the chat has been muted.

Q. Thank you.

And even more importantly, there's no admin logs on Cellebrite; isn't it?

A. Admin what?

Q. Admin logs?

A. Admin locks?

Q. Logs. Logs. L-o-g-s. Administrative logs.

A. Logs?

Q. Yes, on Cellebrite.

A. I don't believe Telegram has administrative logs.

Q. You don't believe or you don't know?

A. I've never seen an administrative log for Telegram.

Q. Isn't it true that sometimes the times in Cellebrite are inaccurate?

A. For Telegram specifically?

Q. Yes.

A. No, I have never seen an inaccurate time tamp.

Q. Isn't it true that you can get added to chats without your consent?

A. You can be added to a chat, yes.

Q. And that explains all the spam that I get on Telegram, right? People just add me though their groups; is that the cause?

A. The public groups, if you've interacted in some way, then you can be automatically added to some.

Q. Thank you.

Can you tell on Cellebrite whether or not a message has been forwarded?

A. I don't believe on the earlier versions you could.

Q. Okay. And, actually, you can't even tell whether a user is a chatbot or not on Cellebrite, correct?

A. Whether a user is a chatbot?

Q. Yes.

A. No.

Q. And, actually, some of the messages that the government has in their exhibits were actually chatbots. Did you know that?

A. Not that I recall.

Q. Do you know what Group Guardian is?

A. Group Guardian?

Q. Yeah.

A. Is that a -- is that a specific Telegram group?

THE COURT: Counsel, please, just for the court reporter's sake, again, counsel and the witness, each wait until the other is done speaking.

MR. JAUREGUI: My apologies, Judge.

BY MR. JAUREGUI:

Q. Have you heard of a chatbot whose name is Group Guardian?

A. No, I have not.

Q. Now, Tarrio created the Ministry of Self-Defense on December 31st, 2020, correct?

A. I don't recall the exact date of the group creation.

Q. So then you don't know when it became a super group, either, correct?

A. I believe I took notes regarding that, or conversed with my case agent regarding those things, but I don't have them committed to memory, no.

Q. Does the government have the notes? Do you know?

A. Potentially.

MR. JAUREGUI: Eric, do you have the notes?

(Off-the-record discussion between counsel.)

MR. JAUREGUI: May I have a minute, Judge, please, for a paper?

THE COURT: Yes, sir. Yes.

MR. JAUREGUI: May I approach, Your Honor?

THE COURT: You may, sir -- well, you may.

MR. JAUREGUI: Thanks.

BY MR. JAUREGUI:

Q. I'm showing you what's been shown to you before. Hopefully this will refresh your recollection as to when Tarrio created the MOSD.

Did he create it on December 31st, 2020?

A. I'm sorry. This one doesn't have the date the chat was created.

Q. Okay. And do you know when it became a super group? I guess not, right?

A. I don't recall from memory, no.

Q. Okay. And do you know when the group IDs were changed?

A. When the super group conversion happened is when --

Q. And when that conversion happens, there's two different IDs, right?

A. Yes.

Q. Now, let's talk about the Boots on the Ground chat. You did review that with the government, correct?

A. I did.

Q. And that was important because the government wasn't sure whether or not Enrique was actually in that group, correct?

MR. KENERSON: Objection to characterization of why it's important.

MR. JAUREGUI: Well, I'll take the blame.

BY MR. JAUREGUI:

Q. It's important for me to find out when Enrique was in that Boots on the Ground. And you looked into that, correct?

A. I did research it.

Q. Okay. And the reason that was important is because there's actually no messages or any interaction by Enrique in that group Boots on the Ground, correct?

A. He does not contribute any messages, no.

Q. And, actually, there's not even a system message that he joined the group, correct?

A. No. Because he would have been added at the group creation, which does not create a system message.

Q. Thank you.

And we don't even know if he had even seen that group, correct?

A. I do not know if he saw it.

Q. Thank you for your honesty, Agent.

Now, Ms. Cain, did you create any exhibits whatsoever in this case?

A. No. I reviewed the exhibits.

Q. Okay. And the exhibits were manufactured by who?

A. Our investigative team put them together.

Q. And the government people at this table here?

A. They are -- the case agent and his team. You would have to ask him for the participants.

Q. Got it. So Agent Hanec is the one that created the exhibits in this case.

A. He was my contact that I spoke to about this. Again, I don't know who created each individual exhibit, no.

Q. Got it. And whatever exhibit Agent Hanec created was based on your data?

MR. KENERSON: Objection. Characterizes.

THE COURT: Sustained.

BY MR. JAUREGUI:

Q. Okay. The exhibits created by the prosecution team was based on your data?

A. It was based on the Cellebrite reports for those devices.

Q. Okay. I saw you make a big differentiation there. I asked you about the data, and you said: No, it was based on Cellebrite reports.

So what you're telling the jury is, just to be clear, the exhibits were manufactured, created, based on Cellebrite reports; is that correct?

A. That is correct.

Q. Did you preview these exhibits with that elaborate peer-review process you have at the FBI?

A. I did not.

Q. Any future mistakes on these exhibits, who's fault are they?

MR. KENERSON: Objection.

THE COURT: Sustained.

BY MR. JAUREGUI:

Q. If there's mistakes on the exhibit, they're not your fault, are they?

MR. KENERSON: Objection.

THE COURT: Sustained.

MR. JAUREGUI: And I have no more questions. Thank you, Ms. Cain.

THE COURT: All right. Counsel for Mr. Pezzola.

MR. ROOTS: Thank you.

CROSS-EXAMINATION

BY MR. ROOTS:

Q. Special Agent Cain, my name is Roger Roots. I represent Mr. Dominic Pezzola, along with my co-counsel, Mr. Steven Metcalf. My colleagues have mostly asked most of the questions that I wanted to ask, so I will just briefly touch on some of these.

Ms. Hernandez, representing Mr. Rehl, asked you: Isn't it true that millions of people use Telegram?

It's actual 500 million users worldwide, correct?

A. I don't know the exact number.

Q. That would be more than the total number of people in the United States.

A. I'm not sure.

Q. And hundreds of millions more use other encrypted apps, such as Signal, correct?

A. Signal is a widely used application, yes.

Q. And Signal would be described as a competitor of Telegram?

A. Potentially. They perform, generally, the same chat functions.

Q. WhatsApp is another encrypted app used by millions?

A. Yes.

Q. So, I believe Mr. Smith asked you a question: There's nothing criminal about using an encrypted communication, correct?

A. No.

Q. I'll go even further. If so many hundreds of millions of people use those, there's nothing shady about it, is there?

A. I don't presume to know why people use them. I just know that they are widely used, yes.

Q. And you use them yourself?

A. I do.

Q. So if witnesses were to come into this room and sit on the witness stand and say, These defendants have used encrypted communications, that wouldn't mean anything remotely unusual about them, would it?

MR. KENERSON: Objection. Argumentative.

THE COURT: Overruled.

BY MR. ROOTS:

Q. Along the same lines, how private do you think these apps are? If someone is in a club or a group that is controversial, or a club that has enemies, if he's aware that in that chat group there are dozens of strangers that he's never met, he wouldn't necessarily think he's protected with a lot of secrecy and privacy, would he?

A. I don't presume to know how people use their devices or what they would think about the privacy.

Q. Now, you testified that you are a FBI digital forensics expert?

A. My title is senior digital forensic examiner.

Q. How many of those are in the FBI?

A. I think there's roughly 400.

Q. 400 senior digital forensic examiners?

A. I believe about 100 of us are senior level.

Q. And I'm trying to understand. Do you all work in about the same place?

A. Well, we have 56 field division offices, so we are dispersed throughout those offices.

Q. So, I heard you mention maybe Tampa and maybe Knoxville or somewhere, Nashville. Do you work in those buildings -- the FBI buildings in those communities?

A. I did. I worked in the Tampa division until last January, and the last year I've worked in the Knoxville division.

Q. And how many other digital forensics FBI examiners are there in your office?

A. I have three in my current Knoxville office, and we had six in Tampa.

Q. Do you know anything about the D.C. FBI office division?

A. I work with their examiners. I've never visited their location.

Q. Do you know how many there are?

A. I do not.

Q. So, I believe you just said there are 400 FBI digital forensic, would you say, not senior, but agents?

A. No. It's a combination of agents and professional staff.

Q. And are they all doing what you were doing, or are they doing different things?

A. We all follow the same standard operating procedure.

Q. Did you -- did you go through the FBI training, Quantico, all the basic training, and that kind of thing?

A. We have our own digital forensic training, and so that is the training that I attended.

Q. You mentioned a programming team. Does the FBI program software?

A. Sure. Yes.

Q. The FBI creates actual software?

A. Yes.

Q. You mentioned developing a tool. The FBI developed actual tools for examining things?

A. Yes.

Q. How many people in the FBI are designing software?

A. I couldn't say. I'm not sure what the number is.

Q. Now, would you call what you do surveillance?

MR. KENERSON: Objection.

THE COURT: Overruled.

A. I would not.

BY MR. ROOTS:

Q. What's the distinction between what you do and surveillance? What's the distinction?

A. I look at devices in the past tense, essentially.

Q. Okay.

A. They must be seized upon consent or search warrant and have some type of legal authority, and the moment that that -- they come into our possession, the device activity ceases. So, I am not looking at any kind of live, interactive data. All the data I look at is historical.

Q. Okay. So you do your digital forensics of devices in the past tense, after -- after occurrences have already happened?

A. I do.

Q. And the FBI obviously has surveillance people that examine communications in realtime, correct?

A. I cannot speak to that.

Q. Couple of my colleagues asked you some questions about the fact that you can be put into a chat group uninvited, correct?

A. Someone can add you to a chat group without your permission.

Q. Without your permission. Without your even -- against your will?

A. No. You would accept the invitation to join the chat group.

Q. Okay. At least two of my colleagues asked about chatbots. I believe you said those are artificial intelligence entities on these chats that post comments?

A. To the best of my knowledge.

Q. So, if you were in a club that has enemies, you were involuntarily put in a chat with strangers, how comfortable would you be thinking that you're going to plot to overthrow the government in such a group?

MR. KENERSON: Objection. Speculation. Foundation. 403.

THE COURT: Sustained.

BY MR. ROOTS:

Q. Let's ask a different question, maybe from a different angle. Suppose an organization that wanted to harm the Proud Boys, such as the federal government, wanted to harm the Proud Boys, could they create a chat group, put chatbots in the chat group, put, perhaps, plants, individuals that are put there with the sole purpose of harming others in the chat group, and then try to concoct a case based on such things?

MR. KENERSON: Objection. Speculation. Relevance. Foundation. 403. Argumentative.

THE COURT: Sustained.

MR. ROOTS: Thank you so much. No further questions.

THE COURT: All right. Any redirect from the government?

MR. KENERSON: Thank you, Your Honor.

REDIRECT EXAMINATION

BY MR. KENERSON:

Q. Examiner Cain, Mr. Jauregui asked you some questions about an edit function, correct?

A. Yes.

Q. Have you ever seen any evidence that -- of editing going on back in 2021?

A. I did not. The database did not contain any indicators that editing was possible back then.

Q. You were asked a number of questions, as well, about whether these -- the phones at issue that you've testified about were extracted using the latest version of Cellebrite. Do you remember those questions?

A. I do.

Q. Could you tell us about how many releases of Cellebrite have happened between January 2021 and today?

A. Do you refer to Cellebrite extracting or Cellebrite processing? Because they have different tools.

Q. Processing.

A. At least 20 different versions have come out in the last two years.

Q. And is it -- would it be standard operating procedure for the FBI to reimage -- or reprocess, excuse me, a phone every single time there's a new update to Cellebrite?

A. No, it wouldn't.

Q. Mr. Jauregui also asked you a question about what might happen if someone improperly extracted a phone and then you were looking at it. Do you remember those questions?

A. I do.

Q. Did you see any evidence of improper extraction in any of the phones in this case?

A. I did not.

Q. You were also asked a question about end-to-end encryption, and I think you said that Telegram was not end-to-end encrypted. Did I understand that correct?

A. It is not end-to-end encrypted by default. Groups can never be end to end --

MR. PATTIS: Objection, Your Honor. This is a narrative, no question.

THE COURT: Overruled.

A. Groups can never be end-to-end encrypted; however, direct messages between two users, private conversations, they have the ability to turn into secret chats, and those chats can be end-to-end encrypted.

Q. And can you just explain what the difference is between end-to-end encryption and the type of default encryption that Telegram uses?

A. End-to-end encryption --

MS. HERNANDEZ: Objection, Your Honor.

(Bench discussion:)

MS. HERNANDEZ: Your Honor, my concern is we're going into an area that wasn't explored in direct, and I don't want to end up with situation where -- asking to recross the end-to-end encryption we're talking about. I know there were questions about encryption, but end to end is a different animal.

THE COURT: I recall questions about end to end, but I could be wrong.

Mr. Kenerson, what is your --

MR. KENERSON: There were questions about end to end on cross, and I would think she's entitled to explore that difference because Mr. Jauregui, I think, left the impression that there might be some difference between them that's meaningful, and I would like to explain that.

MR. JAUREGUI: Judge, I did ask a question about end to end.

MS. HERNANDEZ: I hadn't, so I my missed that.

THE COURT: Very well.

(Open court:)

THE COURT: Objection is overruled.

BY MR. KENERSON:

Q. Can you explain the difference between end-to-end encryption and the type of encryption that Telegram generally uses?

A. Sure. End-to-end encryption is from the first device, it is encrypted immediately after it is written. It passes through the Telegram servers, also encrypted, and then is delivered to the recipient, also in an encrypted state. It is encrypted the entire time and can only be decrypted by the two end users on the either side of that using the encryption key.

The type of default encryption that Cellebrite uses is a client-to-end-user encryption, which means that from the -- when the message is created, it is encrypted until it is received on the Telegram servers. And it is -- when it is at rest on the Telegram servers, it is in a decrypted state.

Their servers are distributed across hundreds of countries all over the world so that a piece of your data lives on each one of those 200 servers, so it's not all together. So for all intents and purposes, it might as well be encrypted because it's been split up.

And then it leaves Telegram servers in an encrypted state to its final destination, where it will be decrypted on the end user's device.

Q. Thank you, Examiner Cain.

I think you were also asked whether you had taken some courses put out by Cellebrite itself. Do you remember those questions?

A. I do.

Q. Can you remind us how many hours per year of training you must complete to keep your certification?

A. We do about 100 hours of advanced forensic training.

Q. And that's per year?

A. Per year, yes.

Q. I believe Ms. Hernandez asked you some questions about orphan files and what data is available and what you can tell based on certain properties associated with those files. Do you remember that?

A. Yes.

Q. And I think that you had said to her that there is EXIF data associated with images and videos and that can help you learn things about those files, correct?

A. That is correct.

Q. What is the difference between images and video and audio files in terms of what data is available to you?

A. Well, as I kind of mentioned before, the EXIF data was established for photographers, originally, to use so that they could memorialize their camera settings in digital photos. Audio files are not inherently a photographer's use, so EXIF data is not attached to an audio file. So, that's why it's only available in video and images.

Q. And I think you also, with Ms. Hernandez, looked at a spreadsheet that you had created with some information about who was in what groups to refresh your memory. Do you remember that?

A. I do.

Q. It's sitting in front of you right now. I think it's Rehl Exhibit 40?

A. It is.

MR. ROOTS: Your Honor, at this point, I move this into evidence under Rule 612(b).

MS. HERNANDEZ: I don't -- we only used it to refresh her recollection, Your Honor. I'm not sure why it comes in and how it's relevant.

THE COURT: Well --

MS. HERNANDEZ: That document was marked up by me, too.

THE COURT: Let's -- let's just take this up -- let's take this up between witnesses, whether that will be admitted.

BY MR. KENERSON:

Q. Let me ask you, if private groups -- private Telegram groups, I think you had some conversations with Mr. Jauregui about maybe being automatically added to a public channel; is that right?

A. I believe so, yes.

Q. What's the difference in terms of automatic addition to a public channel versus automatic addition to a private group?

MR. JAUREGUI: Objection. Vague. We don't know what version of Telegram we're talking about.

THE COURT: All right. Counsel can account for that in a rephrased question.

BY MR. KENERSON:

Q. In January -- or, not January, but in and around the time period we're talking about here, 2021 or so, was there a difference between the ability to be added to a private group versus automatically added to a channel?

A. Yes. Channels are public facing. A channel has a creator and -- or, an administrator, and when they post, it's not an interactive conversation. It's a one-way communication where the person that hosts the channel just posts video -- just posts comments or media, and people essentially just follow it. They don't interact in a group setting with it.

So if you're automatically added to a channel, it's just like following a channel. Just like following someone on Twitter, per se.

Q. And when you had that example with Mr. Jauregui about being added to a channel as a result of maybe somehow interacting with it, were you talking about public channels or private groups?

A. With those, that would be a public channel -- and all channels are public by default -- or a public group.

Q. Okay. And can you remind us the process of how someone can get invited to a private group?

A. You must be invited to a private group. So, someone sends you an invitation to join. You accept that invitation to join the group.

Q. And within a group, who can send those invitations to join?

A. The administrator can always send those invitation, and then they can set a setting either allowing or disallowing the other users of that group to also be able to send invitations out.

Q. So people who are in a private group, if I understood you correctly, must be either invited by an administrator or someone the administrator has designated?

A. Yes.

Q. Now, you had a lot of conversations with Mr. Smith and a couple of the other defense counsel about whether Cellebrite parses all data associated with Telegram messages. Do you remember those conversations?

A. Yes.

Q. Now, you've had a chance to review, I think, those zip files that we discussed labeled Government 500 through Government's Exhibit 550?

A. I did.

Q. And based on your understanding of Cellebrite as it existed at the time of these extractions, do you have any concern about the accuracy of those reports, in terms of accurately reporting the messages and the timestamps and the senders and things like that?

MR. PATTIS: I think that's compound, the items versus reports. So, objection.

THE COURT: I'll sustained as to compound.

BY MR. KENERSON:

Q. So for the exhibits that you reviewed labeled 500 through 550, based on your knowledge of Cellebrite as it existed at the time of the extractions, do you have any concern about the accuracy of that data?

A. No. The data was accurate.

Q. And any concern that Cellebrite would not capture messages, for example?

A. No.

Q. Any concern that Cellebrite would not capture the sender?

A. No.

Q. Any concern that Cellebrite would not capture timestamp?

A. No.

Q. Let me ask you, for more clarification, question on the issue of who can join private groups.

In a super group, does the administrator have the ability to create a link?

A. They do.

Q. And what would be the functionality of that link?

A. When the administrator creates a link, then, I believe, anyone in that group can send the link out to add people. So, once that link is created, that functionality becomes available.

Q. Okay. So, in a super group, if the administrator creates a link, other group members can invite people by that link?

A. They can.

Q. Okay. Thank you.

MR. KENERSON: I do not have any other questions. Thank you, Your Honor.

THE COURT: All right. Can I have just counsel pick up the telephone for a moment.

(Bench discussion:)

THE COURT: All right. Just before we have the witness leave the stand, Mr. Kenerson, let me just ask Ms. Hernandez, do you -- the document that has been used to refresh her recollection, I guess I want to know whether -- I think technically, under the rule, I had always been of the view that the -- generally, the writing used to refresh recollection did not come in.

However, as I think has come up in other context in this case, the adverse party -- if an adverse party uses it, the adverse party, under 612, can -- can introduce into evidence a portion that relates to the witness's testimony. I'm not sure if the sponsoring -- the sponsoring party, the non-adverse party can do that.

On the other hand, if it's -- if you all have seen this, you all have had her use it to refresh her recollection, you all may not object, if you don't want to.

So let me just ask, Ms. Hernandez, do you object to the document coming into evidence?

MS. HERNANDEZ: Your Honor, this is a document generated by the government, and I used it similarly to the way the government used the metadata documents. I mean, it just lists the different groups, it lists everybody else. I don't know how the other defendants feel about introducing it, one; and, two, I only asked about Mr. Rehl's participation.

And that particular document, I believe, has my notes on it, or at least my highlights on it, because I think I had highlighted Mr. Rehl. I don't know what other information is on there. It is the government's -- the government generated the document, so to the extent Your Honor is talking about adverse party, I don't know whether that even fits this definition.

THE COURT: The witness is the government's witness, so, I think technically, under the rules, I don't know that they have the right to admit the document. However, if all the defendants think that what's on there is accurate and no one objects, I will admit it.

But, I want to know whether you maintain your objection or whether the government might have to either address this as a legal matter or ask certain questions that could, for example, have the document admitted in some other -- for some other reason. For example, if she were to just testify that everything in there is accurate and she helped put it together as a demonstrative, or something like that.

I haven't seen the document, so I don't know. But, while the witness is on the stand, I think we could clean this up. The question is just whether you do object to the government's request to admit it. Whether any defendant does.

MS. HERNANDEZ: Your Honor, maybe, could we -- I think we would stipulate that if everybody is okay with it, it could come in, but let the other defendants see it later on, so they -- whether they have any objections or not.

THE COURT: All right. I mean, how about this: Mr. -- so, we'll -- just, again, if the government wants to ask any questions of the witness while she's here that might lay the foundation for it to come in some other way. I want to give them the opportunity to do that, rather than have to have the witness come back.

MS. HERNANDEZ: What I'm suggesting is if nobody objects, I don't think anybody would say you have to bring the witness back just to admit it. I mean, I think we would all agree, if nobody objects, it would just come in.

MR. JAUREGUI: For Tarrio, we object, Judge. I don't even know what that document is, to be honest with you. I haven't had a look at it.

THE COURT: I thought you used it to fresh her recollection, if I recall.

MR. JAUREGUI: I did. But I don't -- I didn't look at it.

MS. HERNANDEZ: It doesn't have the information you needed, so you couldn't use it.

THE COURT: Mr. Kenerson, how do you want to proceed?

MR. KENERSON: Your Honor, I think we got to have an adequate basis to admit it, but I would take the Court's invitation to ask a couple of foundational questions so we can have a legal argument later, depending on what her answers are.

THE COURT: Let's do that. All right.

(Open court:)

BY MR. KENERSON:

Q. Examiner Cain, just a couple more questions.

That document that you have in front of you, I think that Ms. Hernandez showed you --

A. Yes.

Q. -- can you tell us what this is?

A. This is a chart I created of the Government Exhibits 500 through 544, it appears. It's a variety of Telegram group chats. In it I've put the name of the exhibit, the kind of colloquial name that we were calling it internally, because there's a couple with very similar names. The actual Telegram chat name as given -- as assigned to the group. And then the Android and IOS group number and super group number, if applicable, and then a list of the five subjects and whether or not they were members or administrators in each of these groups.

Q. Now, with the exception, I think, of, you said, some of it was, what? We have colloquially referred to the chats as -- what's the source of the data for that spreadsheet?

A. The Telegram databases.

Q. The -- the extractions?

A. From these extractions, yes.

Q. Thank you.

MR. KENERSON: I don't think I have anything further.

THE COURT: All right.

Sorry one more.

BY MR. KENERSON:

Q. For the data that came from those databases, does the data in your chart fairly and accurately describe what was in the databases?

A. It does.

MR. KENERSON: Thank you.

THE COURT: All right. Very well.

(Bench discussion:)

MR. PATTIS: Can it be circulated briefly between counsel? I didn't look at it when it was shown to her. I want to look at it.

THE COURT: I'm not admitting it now.

MR. PATTIS: Okay. You did say that. I apologize.

THE COURT: Very well.

(Open court:)

THE COURT: Ma'am, you can step down. Thank you very much for your testimony.

Government may call its next witness.

MR. MULROE: Your Honor, the United States calls Peter Dubrowski.

THE COURTROOM DEPUTY: Will you please raise your right hand.

PETER DUBROWSKI,

was called as a witness and, having been first duly sworn, was examined and testified as follows:

THE COURT: Counsel, to begin, you may want to retrieve -- there's an item at the -- with the witness right now.

MR. McCULLOUGH: Permission to approach, Your Honor?

Let's talk a little bit about what your expectation is after that. Who you are calling next?

MR. DREHER: Sure. Yeah. I think that we are going to call next -- so we have three witnesses. It's only the third of whom that really needs to testify today. She has chemotherapy tomorrow. So we have three witnesses that we think we can do this afternoon.

THE COURT: Okay. For this afternoon?

MR. DREHER: Yeah.

THE COURT: Okay.

MR. DREHER: Captain Shawn Patton with the Capitol Police and then an FBI CART examiner and an FBI special agent.

THE COURT: Okay. All right. Anything else you all want to raise now?

MR. SHIPLEY: Nothing, Your Honor.

THE COURT: Okay. I'll see y'all around 2:20. I'll do my best to get it finished by then.

MR. DREHER: Your Honor, before we begin with our next witness, the parties did reach four stipulations --

THE COURT: Okay.

MR. DREHER: -- which I have marked as Government's Exhibits 400 through 403. So 400, 401, 402 and 403. And my thought at this time since it's a bench trial is that I wouldn't read these into the record, but I would admit them --

THE COURT: Okay.

MR. DREHER: -- provide them to the Court so that the Court can file them.

THE COURT: Good.

MR. DREHER: And then that the parties -- I mean we have our own version. So even before they hit the docket, if we need to read some portion of it or refer to it, I think we have our own copies.

THE COURT: That's fine.

MR. DREHER: Permission to approach?

THE COURT: Yes. All right. Thank you very much.

MR. DREHER: And then the other sort of just housekeeping matter is we provided the wrong version -- we've provided the correct version of Exhibit 175 to defense counsel. We provided the wrong version in the Court's two exhibit binders. So at the break I just printed two copies of that particular exhibit.

THE COURT: Okay.

MR. DREHER: All right. And I think with that, the government is prepared to call FBI Senior Digital Forensic Examiner Jennifer Kate Cain.

THE COURTROOM DEPUTY: Raise your right hand.

Thereupon,

JENNIFER CAIN,

Having been called as a witness on behalf of the government and having been first duly sworn by the Deputy Clerk, was examined and testified as follows:

DIRECT EXAMINATION

BY MR. DREHER:

Q Can you please introduce yourself to the Court?

A My name is Jennifer Katherine Cain. I'm a senior digital forensic examiner for the Federal Bureau of Investigation.

Q And what are your duties in that role?

A I work with CART, the Computer Analysis Response Team and we are responsible for handling all aspects of digital evidence to include computers, laptops, phones and any kind of external media that would attach to those devices.

Q And have you undergone any training or certifications to become a senior digital forensic examiner?

A I have.

Q Can you just provide a very brief overview of the type of classroom training or, sorry, how many hours of classroom training you have to undergo?

A Sure. To become certified originally, we do around 400 classroom hours of training and then each additional year, we are required to undergo a hundred hours of advanced forensics training.

Q Thank you. During the course of your time as a senior digital forensic examiner, how many cell phones roughly do you think you've processed?

A Approximately a thousand.

Q And how many computers do you think you processed?

A Between three and four hundred.

Q Okay. All right. What does F.B.I. CART generally do?

A We are responsible for all aspects of digital evidence. So we take in any kind of digital device. It follows the standard chain of custody evidentiary rules. We take in those devices. We physically inventory them. We extract them. We turn those extractions into meaningful readable usable formats for our case agents and our investigative team to review and then we write reports on the analysis and the findings.

Q Okay. And when you obtain a digital device in the field, what processes does the FBI use to ensure the integrity of the data inside that device? So, for example, a cell phone from when it's taken in the field to when someone like you reviews it.

A When we extract the device, we get a file -- a containerized file usually in the form of a zip file and we get -- we calculate a hash value for that file, which is essentially a digital fingerprint, meaning that at any point in time, no matter how you calculate that hash value, it will always come to the same value. And so we use that hash value to verify that the contents of that particular extraction have not changed from the start of the exam to the conclusion of the exam.

Q All right. Are you familiar with the telephone application called Telegram?

A I am.

Q What is that?

A It is an encrypted chat application.

Q All right. What does it mean for it to be encrypted?

A Essentially that means that the data is scrambled while it's in transit. So only the parties that are communicating that message can see the contents.

Q Have you reviewed extractions of cell phones that had the application, Telegram, on it?

A I have.

Q Have you done any testing yourself of the application even outside of your review of those kinds of devices?

A I do.

Q Can you just talk a little bit about how you do that testing?

A Sure. I have a variety of test phones, both Android and IPhones. Whenever I get a new application such as Telegram, I create user accounts on both those devices and then use the application to the full extent possible meaning sending messages, sending attachments like media and documents. Then I take those phones through our full examination process where I actually extract them, run them through all the tools that we could use that are available to us and then make sure that the data that our tools is producing matches what I actually put into the application into the device itself.

Q All right. Based on your experience in working with the application, are users of the Telegram application able to send both direct messages to a single other user, but then and also be part of a group that can send messages to one another?

A They are. Yes.

Q Do those appear differently in the phone? Can you tell the difference between the two?

A The only way you would really tell the difference is when you are talking to one other individual, the name of that chat is the other individual that you are communicating with. When you're communicating in a group, the name of that chat is the group name.

Q All right. When somebody signs up with a Telegram account, how does Telegram identify that user in the application?

A Telegram assigns a unique identifier. It's typically nine or ten digits long. The user themselves would assign themself a username. But the Telegram assigned identifier is the unique identifier.

Q Okay. So there's a nine or ten-digit I.D. number and then there's also a username that the user can create?

A That is correct.

Q Is there also a display name?

A There is a display name.

Q All right. And what's the difference between a display name in Telegram and the first two things you mentioned?

A So when someone communicates with another party, if that party has them stored as a contact in their phone, then the display name would then be the contact name. So, for instance, my name is Jennifer Cain, but I go by my middle name, Kate. I would originally appear in Telegram as Jennifer Cain. But in your device, if you have me saved, I could appear as Kate Cain.

Q Okay. Can users change their unique identifier?

A No, they cannot.

Q Can they change their display name?

A Yes. They can.

Q Okay. What about group chats? Are there identifying features for group chats as well?

A When a chat, a group chat is created, Telegram assigns it a unique numerical identifier and it is approximately ten or eleven digits long.

Q So if you see a group chat on multiple different devices, are you able to verify that it's the same chat across those devices?

A We can.

Q All right. And even apart from the unique identification number for that group chat, how else might you look at different chats and verify that it's the same chat on those devices?

A The content of the messages inside that chat. For instance, the number of messages the users that are a member of that group and then the messages themselves based on if it is identical from the person that wrote the message and the time stamp and the content is identical across multiple devices, that's an indication that it's the same group in all of those devices.

Q All right. Can Telegram chats or like can a Telegram message be deleted?

A It can.

Q All right. And how does that process work? Like what happens when you delete a message -- if you're a user and you delete one of the messages that you've sent, what happens?

A When the user goes to delete a message, they receive a pop-up that says do you want to delete for just you or would you like to delete this for every member in the group. If the user selects just them, it will be removed from their device only. If the user selects remove from all -- remove for all users, then it will delete across the board for all of the users.

Q And if a user -- let's say the two of us are in a group chat. And you delete a message that you sent, how would that appear on my phone then when I look at that group chat?

A It will have been removed from the chat.

Q Are there ever chats that are just empty?

A There are. Yes.

Q Okay. And can you just explain what that indicates?

A Sure. So the Telegram data is stored in the database and when a message is sent, it essentially removes that entry from the database. However, if a message is sent with an attachment, it actually is stored in two different locations in that database. And so it would remove it from the attachments location, but might not necessarily clean it up in the main table. So messages that have attachments sent to them could appear as blank messages. It would have the user that sent the message and the time stamp. But then -- and it could indicate whether it was a video or a document or an audio file, but the file would actually be gone.

Q Okay. And I just want to clarify for the record. I think you said if a user sends a message, it could remove it from the underlying tables. Did you mean if a user deletes?

A Deletes. Sorry. Yes.

Q Thank you. And so when you as part of the extraction process end up reviewing messages from a digital device, how would it appear to you when you're reviewing if someone had deleted a message in a group chat?

A The user and the time stamp would be there. But the content -- there would just be no content to that message.

Q All right. What about editing messages? Are you aware of the ability of whether there was an ability in Telegram to edit a message as of let's say December and January of 2021?

A At that time there was not the ability to edit messages.

Q And I meant of course December 2020 --

A 2020.

Q -- to January 2021. Yes. Okay. Let me ask you whether you extracted data from the digital devices of four individuals as part of the investigation in this and other cases. Enrique Tarrio, Ethan Nordean, Zachary Rehl and Nicholas Ochs.

A Yes.

Q Okay. Did each of those extractions contain Telegram data from the application, Telegram?

A It did.

Q All right. Did you create reports relevant to this case -- for this case of the Telegram messages from those extractions?

A I did.

Q And is the Telegram user -- and this will be a nine digital number so I apologize for that. Is the Telegram user 1387834575 in each of those extractions of Telegram data?

A It is.

Q For that Telegram user I.D., what username did the user assign to that Telegram user?

A Loach_Gan_Eagla.

Q And then do you recall what the or do you know what the display name that that user used across those four devices?

A Yes. Sergeant Peppers and also Loach Gan Eagla depending on the extraction.

Q Okay. So the display name might be one of those two things, something like or sorry, either Loach Gan Eagla --

A Eagla. Sorry. Yes.

Q Or username something like Sergeant Pepper?

A Yes.

Q All right. And did those Telegram reports that you reviewed, did they contain chat groups with multiple people?

A They did.

Q Did you verify that the Telegram user that we've been talking about was in each of those chat groups as well?

A I did.

Q All right. I'm going to show you now Government Exhibit 175. All right. Do you recognize -- just looking at the first page of this, do you recognize what this is?

A This is the device belonging to Mr. Nordean and it has Telegram chats from that device.

Q Okay. Is this the device or a Cellebrite report?

A Sorry. This is the report that I created from the device.

MR. DREHER: All right. The government moves to admit Government's Exhibit 175.

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q All right. Let's take a look at Government's Exhibit 180. Looking again at the first page, do you recognize what this is?

A I do.

Q All right. What is it?

A This is the report that I created from Mr. Tarrio's device.

MR. DREHER: At this time, Your Honor, the government moves Exhibit 180 into evidence.

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q Okay. I'm pulling up Government's Exhibit 185. Looking at the first page, do you know what this is?

A This is the report that I created of Mr. Ochs' phone.

MR. DREHER: The government moves Exhibit 185 into evidence.

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q And then lastly in terms of these reports, let me show you Government's Exhibit 190. Looking at this, do you know what this is?

A This is the report I created from Mr. Rehl's device.

MR. DREHER: Okay. The government moves Government's Exhibit 190 into evidence.

THE COURT: Any objection to 190?

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q All right. And let's go back now to Government's Exhibit 180 and I'm going to look at page 40 here. All right. So on page 40 of Government's Exhibit 180, if I were to zoom in on the first message visible, is there -- in this -- first of all, is this a message sent in the Telegram application?

A It is.

Q All right. And based on what is seen in this report, does that indicate that there's an attachment to that message?

A Yes, it does.

Q And would that attachment have been visible to the users in that chat group?

A Yes, it would.

Q All right. And if I open Exhibit 181 -- well, first let me just ask you if you know. Is Exhibit 181 the video file that was -- that is attached to that message?

A Yes, it is.

MR. DREHER: The government moves for the admission of Exhibit 181, Your Honor.

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q And then if we go to page 50 -- I apologize. So page 51. Again if I pull up the first message on that screen, is there also an attachment to that message?

A Yes, there is.

Q All right. And is Government's Exhibit 182 a copy of the attachment that was attached to that message?

A Yes, it is.

MR. DREHER: All right. The government moves

Exhibit 182 into evidence.

MR. SHIPLEY: No objection.

BY MR. DREHER:

Q If we go back to --

THE COURT: 182 you said?

MR. DREHER: Yes. 182.

THE COURT: Received without objection.

BY MR. DREHER:

Q If I go back to page 7 on Exhibit 180, the third message on that page -- I apologize -- the first message on page 8 of Exhibit 180, is there an attachment to that message?

A Yes, there is.

Q And is Exhibit 183 the native file attachment that was attached to that message?

A Yes, it is.

MR. DREHER: And the government moves Exhibit 183.

MR. SHIPLEY: No objection, Your Honor.

THE COURT: I'm not getting these numbers straight. Is that 180-3?

MR. DREHER: No. It's 183.

THE COURT: Government's 183 then is received without objection.

MR. DREHER: The dash is the pagination of Exhibit 180. So it is actually confusing even to myself as I'm flipping through it.

BY MR. DREHER:

Q Okay. So now if I'm looking at page 35 of Exhibit 180, again the first message, does that message have an attachment to it?

A Yes.

Q All right. And is Exhibit 184 the attachment, the native file attachment that was sent by that user --

A Yes.

Q -- in that message?

A Yes, it is.

MR. DREHER: All right. The government moves to admit Exhibit 184.

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q All right. Just a few more. We're going to look now at Exhibit 185. And I'm going to go to page 4. If we take a look at the second message on -- sent on page 4 of Exhibit 185, is there an attachment to that message?

A Yes, there is.

Q And is Exhibit 186 a copy of that video file that was attached to that message?

A Yes, it is.

MR. DREHER: All right. The government moves Exhibit 186 into evidence, Your Honor.

MR. SHIPLEY: No objection.

THE COURT: Received.

BY MR. DREHER:

Q Do you recognize the individual in that video file? Well, let me ask first. Have you reviewed that video file message prior to your testimony?

A I have. Yes.

Q Do you recognize the individual in that video file?

A I do.

Q Who is it?

A It is Mr. Worrell.

Q What if anything can you as a CART examiner discern about what that means about who the user, Loach Gan Eagla, that sent this message is based on the fact that it has this video attached to it?

A When you take a video in Telegram inside the Telegram application and hold your phone up -- you hold your camera up to your face, Telegram circles the video. It's kind of a trademark of Telegram that the video will be contained in a circle. So it is most likely that this video is taken inside the Telegram app and then posted by this user.

Q And so if, for example, if Mr. Worrell is this user and took a video of himself, that's how it would appear in Telegram. Is that right?

A That is correct.

Q And if Mr. Worrell were not this user, is there any way that his -- that a video of him could be sent by that user in that fashion?

A If he were with that person and took the video while they were logged in. I mean you'd have to be present and have access to this account.

Q Okay. So somebody else would have to allow him to use their Telegram account. Is that right?

A Correct.

Q Okay. Are there other videos featuring Mr. Worrell that were sent by this same user in Exhibits 185 and 190?

A There are. Yes.

Q Do you know just roughly how many? And it's okay, if not.

A I believe maybe eight to ten.

Q Okay. And so am I understanding correctly that in order for Mr. Worrell not to be the user, this particular user, he would have had to have been with that user on each of those occasions --

A That is correct.

Q -- to have them record him?

A Yes. That is correct.

Q All right. Let's now look at Exhibit 175, we'll go back to that one, just to get a sense of how Telegram chats generally work. So if I start with just this page here, page

2 and I zoom in, what is in the sort of the middle of the page? What does that indicate?

A This indicates that this is the start of this particular chat. The chat's name is Boots On Ground.

Q And then what are the list of names and numbers below that?

A These are the participants in that chat. This is anyone who has contributed a message inside this chat.

Q Okay. And so again for every chat that's in Exhibits 175, 180, 185 and 190, did you verify that the same username, Loach Gan Eagla, with that same unique user I.D. was present and listed as a member in each of those chats?

A Yes.

Q Okay. All right. And if we take a look now at page 4? It's only one message on page 4. So I'll zoom in on that. Can you just explain what that message shows or indicates?

A When a user joins a Telegram chat, a system message gets posted to that chat saying what user has joined the group and then the time stamp that they joined it.

Q Okay. So would this indicate that they weren't in the group prior to that date and time. But then thereafter they're in the group?

A That is correct.

Q And if they were in the group from the beginning, if they were part of the group that was -- when it was first created, would there be a message like this showing that they had joined the group?

A There would not. No.

Q Okay. What about when somebody leaves the chat, is there also a notification in there when they leave the chat?

A Yes. There is a system message that says the username has left the chat.

Q All right. And in your review of Exhibits 175, 180, 185 and 190, did you confirm that all the messages in those exhibits were sent prior to any notification that this same user had left the chat?

A Correct.

Q And by this same user, I again mean the user with the username, Loach Gan Eagla?

A Yes.

Q And then lastly, just to give an example for the Court, if we were to go down to page 26 -- I must have the wrong page number here. All right. So if I go to page 15 and I look at the second to last message, is that an example of how a message would appear if it was deleted and had no attachment, for example?

A That is correct. Yes.

Q Okay. Thank you. My able colleague pointed out just one thing that might have been confusing. So I want to clarify that.

If I go back to Exhibit 175, page 4 and I look again at the one message on that page, so as you testified this mentions a username or a user with the username SGT, Sergeant Pepper. Is that right?

A Yes. That is correct.

Q And it indicates the date and time or why don't you tell me what date and time is indicated in terms of when he joined the group?

A January 5, 2021 at 2:08:56 p.m.

Q Okay. Does that necessarily mean that this user's display name was Sergeant Pepper at that time?

A No, it does not. The data can be for this particular system message and any system message is actually tracked by the nine or ten digit number of that user and then our tools assign the display name from the corresponding message -- the corresponding username table. So I verified that this is actually the same user identifier number. However, the display name just depending on the time was Sergeant Pepper or Loach Gan Eagla.

Q Okay. And so if the phone, for example, was seized and extracted after January 5th and in between January 5th and that seizure date the display name had been changed --

A Yes.

Q -- is that when you could have the display name appear, for example, as Sergeant Pepper in this extraction even though on January 5th, it would have appeared to this user as something different?

A Yes.

MR. DREHER: Okay. I don't have any further questions, Your Honor.

CROSS-EXAMINATION

BY MR. SHIPLEY:

Q Good afternoon.

A Good afternoon.

Q It's Ms. Horvath. Right?

A Cain.

Q Yeah. Okay. When there are multiple people in a chat and you found in Telegram that there were multiple people in these chats including Boots On The Ground. Right?

A Yes, sir.

Q When there's multiple people in the chat and they're all firing off messages, you can look at your own phone and see that you have 20 unread messages. Right?

A I'm not sure if it displays the number, but it does display the chat in bold saying that there are unread messages. Yes.

Q And then when the user opens it, all of the unread messages suddenly become read?

A The ones that are displayed in the preview pane. Yes.

Q Okay. But that doesn't mean that the user actually read them. Right?

A It means that they have been seen on the device.

Q That the application has been opened and that particular chat has been opened and then every unread message is converted to a read message?

A The ones that are viewable in that pane at that time.

Q Okay. But the only way to know that somebody actually either sent or read a message is if they sent it and you have Loach or Sergeant Pepper as the sender, then presumably you know that Mr. Worrell had either had sent that message using one of those two usernames. Right?

A Yes, sir.

Q Or if he's replying to a particular message, then the reply will reflect the message it's being replied to. Right?

A It would. Yes.

Q Okay. So in that case, you would know that he read that particular message?

A Yes, you would.

Q But beyond that, you can't really say whether an open message was actually read by the person who has the application on their phone?

A Not necessarily. When the user opens the Telegram application, it will -- it marks all of the messages that are viewable in that pane as read. For instance, if you opened Telegram in February and then you don't open Telegram again until November and there are a million messages, when you open the application in November, it will not mark one million messages read. It will just mark the ones viewable, the latest viewable ones from November as read and so it would just mark that subset.

Q So, for example, if there were ten messages on the screen when you opened it up, those ten would be marked as read?

A That is correct.

Q And then if you scrolled up, every one you brought onto the screen would be marked as read?

A Yes, sir.

Q That doesn't necessarily mean they read every one of them though, does it?

A It means that the device has registered that message.

Q Okay.

THE COURT: And you had the opportunity then to read it?

THE WITNESS: Yes, sir.

THE COURT: But it doesn't mean you actually had read it?

THE WITNESS: Yes. It just means that the message has been seen on the device.

BY MR. SHIPLEY:

Q Now the deletion function, that can be set automatically. Right?

A At the time, you could you not set an automatic deletion like a self-destruct timer.

Q So Telegram did not have the application that allowed you to set it to delete after seven days automatically unless you saved it?

A I believe in the private chats, there was some functionality behind that. However, with what I saw, the timer is actually recorded in the database and none of these group chats had timers set. The fields and the columns in the database that tracked those were empty.

Q So in your CART extraction, you would see if somebody had set an automatic deletion timer. But your analysis showed that no such timers were set.

A That is correct. Yes.

Q Okay. Now I want to -- I just want to make sure I understood the questions. What was marked as Government's Exhibit 180 which I believe was the report of Mr. Tarrio's phone. Correct?

A I'm sorry. I don't remember which individual was which exact number.

Q Okay.

A Okay.

Q They are saying yes.

A Then yes, sir.

Q And then he showed you the example of a video of Mr. Worrell that appears on the Telegram app in Mr. Tarrio's phone.

A Okay. Yes.

Q Okay. Does that mean that he had to use Mr. Tarrio's phone to make that video?

A No, sir. That means that in that specific chat message, the username associated with it, which I believe was Loach Gan Elanga, that is the user that sent and posted that message.

Q Okay. So it just turns up in Mr. Tarrio's phone as something that was stored in his phone having received it?

A That is correct.

Q Now when Mr. Worrell joined or was -- well, when somebody joins a chat, Boots On the Ground, 1-5-21, or Loach which then later becomes Sergeant Pepper, he has to be invited to that. Right?

A For most chats, you do have to be provided a link. I believe all of these were private chats in which case you do have to be provided a link in order to join.

Q So it's nothing that he could just go on and become a member of on his own. Right?

A Not to my knowledge. I believe all of these were private chats.

Q And so the Cellebrite report showed that he joined or was invited to that chat and joined on January 5, 2021?

A That is correct.

Q Does the Cellebrite report show who sent the invitation?

A It does not.

Q Does the Cellebrite report show when he accepted the invitation? Is that the 1-5 date and time?

A That would be the same time stamp. Yes, sir.

MR. SHIPLEY: Thank you. Nothing more.

MR. DREHER: No redirect for this witness, Your Honor.

THE COURT: All right. Thank you. You may step down. Next witness.

MR. DREHER: The government calls FBI Special Agent Kate Camiliere.

Thereupon,

SPECIAL AGENT KATHRYN CAMILIERE,

having been called as a witness on behalf of the government and having been first duly sworn by the Deputy Clerk, was examined and testified as follows:

THE COURTROOM DEPUTY: You may be seated.