

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

Defendant.

DECLARATION OF SEAN MORRISSEY

I, Sean Morrissey, hereby declare pursuant to 28 U.S.C. § 1746 as follows:

1. I am an Apple iOS Mobile Forensics expert, I submit this Declaration in support of the Defendant's Motion *in limine* to preclude the government from offering certain non-expert testimony and evidence during the trial of the above matter.

2. I have been retained by defense counsel for the Defendant to aid in reviewing the discovery materials, with particular focus on several cell phone forensic extractions provided in discovery. In preparing this Declaration, I have reviewed, among other things, the forensic extractions from the iPhones and a number of other phone extractions provided in the discovery materials to defense counsel. I have also reviewed various search warrant applications and other materials.

3. As detailed below, the process of conducting a cell phone forensic extraction and analysis of the underlying data is a process that is complex and requires technical expertise to perform correctly. Moreover, specialized expertise is required to interpret the results of the extraction.

QUALIFICATIONS

4. I am a nationally recognized iOS and mobile device data security and forensics expert. My CV is annexed hereto as Exhibit A.

5. My career in mobile forensics began in approximately 2006 when I was hired by the United States Department of Defense as a computer forensics instructor to develop and teach courses on Macintosh / Advanced Windows forensics.

6. As part of my responsibilities in that role, I developed and wrote curriculum and research on Mac OS forensics that was utilized by the Federal Law Enforcement Training Center, Secret Service, Special Forces, US Army CID, Navy NCIS, military intelligence, and various other high-level Government organizations.

7. After leaving the Department of Defense, I was hired by the US State Department as a computer/mobile forensic examiner where I continued to develop extensive expertise in mobile forensics, with a concentration on Apple iOS.

8. After leaving the US State Department, I started my own mobile forensic software business, Katana Forensics, LLC and served as its founder and CEO. In that capacity, I oversaw the development of complex mobile forensic software designed to access and recover mobile forensic data, including text messages, deleted data, and other app usage information.

9. A part of my responsibilities with Katana Forensics included providing training to law enforcement officers around the United States as well as internationally in how to properly handle mobile devices and obtain evidence in the most forensically sound manner possible. I have trained thousands of law enforcement officers around the globe on proper techniques for handling digital forensic evidence, and specifically, mobile devices. In this capacity, I also served as an instructor at the US Secret Service Academy approximately four times yearly.

10. I have authored multiple textbooks on Apple iOS Forensic analysis, including *iOS Forensic Analysis*, ISBN 978-1430233428, which was published by APRESS in 2010, and is a widely read textbook on Apple iOS Forensic analysis. My other publications include: *Mac OS X iPod and iPhone Forensic Analysis* ISBN 978-1597492973 (2008), and *Defense Against the Dark Arts*, ISBN 978-143-9821190 (2011).

11. Through my training, experience and life's work, I have developed an extensive expertise in mobile forensic device recovery and analysis, specifically concentrated on Apple iOS devices.

THE GRAYKEY EXTRACTION OF CELLPHONE #5 ([REDACTED] IPHONE)

12. Part of the discovery materials in this case included a forensic extraction and relation examination data for a phone labeled in the discovery as "Cellphone #5 (107 pct)".

13. That cell phone is an iPhone 14 Pro Max running iOS version 16.6 and named "[REDACTED]". I am able to determine that information from reviewing the Cellebrite "Extraction Summary" from within the Cellebrite Reader program. A copy of the Cellebrite extraction summary for Cellphone #5 is annexed hereto as **Exhibit B**.

14. A second cell phone seized from Ms. [REDACTED] was also provided in the discovery materials and labeled as "Cellphone #6 (107 pct)". That cell phone is an iPhone XS running iOS 16.5 and named "[REDACTED]". A copy of the Cellebrite extraction summary for Cellphone #6 is annexed hereto as **Exhibit C**.

15. The contents of Cellphone #5 (the "[REDACTED] iPhone") was initially extracted utilizing a tool that is available only to law enforcement called GrayKey. That process began at 13:29:16 UTC on January 2, 2024 and was performed by an examiner with the

name “[REDACTED]”. A GrayKey Progress report detailing this process is annexed hereto as **Exhibit D**.

16. GrayKey is a proprietary technology and its precise inner-workings are a closely guarded secret. GrayKey essentially works by exploiting a security vulnerability in the Apple iOS (mobile) operating system to permit the installation of a software agent on the phone. That software agent permits GrayKey to access the iPhone at the file system level and then perform an extraction of its contents.

17. Using the GrayKey process, a full file system extraction of the phone’s content is performed by GrayKey. This differs from a hardware level bit-for-bit copy because it does not include the entire content of the iPhone’s internal storage. The GrayKey process can only extract limited data or a full file system extraction based on the unlock state of the phone. From the [REDACTED] iPhone, law enforcement was able to obtain a full file system extraction.

18. Although the Department of Homeland Services (“DHS”) has previously performed testing on a much earlier version of GrayKey and issued a report.¹ However, the DHS Report does not perform any validation testing on data recovered from the Telegram application. Even a later January 2024 report issued by DHS still did not validate Telegram data.²

¹ Department of Homeland Services, February 2022: Test Results for Mobile Device Acquisition Tool: GrayKey OS v1.7.3.19461530 App Bundle v2.2.2, available at: https://www.dhs.gov/sites/default/files/2022-06/22_0615_st_test_results_for_mobile_device_acquisition_tool-graykey.pdf (last accessed June 30, 2025).

² The 2024 DHS Report tests Magnet GrayKey, the report is available at: https://www.dhs.gov/sites/default/files/2025-03/25_0324_st_test_results_for_mobile_device_acquisition_tool-magnet_graykey_v4.1.0-axiom_examine_v8.0.0.pdf (last accessed June 30, 2025).

THE CELLEBRITE ANALYSIS OF THE [REDACTED] IPHONE

19. Once the filesystem extraction of the [REDACTED] iPhone is completed, the content of the filesystem is forensically analyzed using Cellebrite, a leading mobile forensics tool.

20. Analyzing the [REDACTED] iPhone data with Cellebrite results in the creation of a .UFDR file, i.e. a Universal Forensic Extraction Device Report. That file contains the forensically extracted and analyzed data in a “human-readable” format, although the review and interpretation of that data requires specialized skill and expertise. This is the format in which the data was produced to counsel for Mr. [REDACTED], and ultimately the format in which I reviewed the content of the [REDACTED] iPhone.

21. The processes underlying Cellebrite’s analysis of the phone data is complex. Cellebrite programmatically parses the iPhone system files from various databases and files contained within the iPhone, such as SQLite databases, plists (property lists), system log files, system library files, among many other filetypes.

22. Some of the data within various iPhone databases is stored in a non-human readable format such as BLOB, (Binary Large Object), or other data formats. That data needs to be decoded in order to be readable, which is a process programmatically undertaken by Cellebrite.

THE “SAVAGE”³ GROUP CHAT FROM THE [REDACTED] IPHONE

23. From the [REDACTED] iPhone, I have reviewed the underlying data that the government repeatedly refers to in its search warrant applications as “The Savages

³ While the government refers to the chat as “Savages” the associated title of the chat appears to be “Savage” and not “Savages”.

Telegram Group Chat”. An excerpt of a May 14, 2025 search warrant application that references this group chat is annexed hereto as **Exhibit E**.

24. Other than the deleted chat discussed below beginning at paragraph 28, the fragments of this chat that were recovered from the [REDACTED] iPhone were not recovered from the Telegram database file directly, but were instead recovered from a separate iPhone SQLite database file called “knowledgec.db”. The knowledgec database file stores a variety of information about the cell phone’s usage, background processes and other information about the operation of the phone, including application notifications. It is of significant value to forensic investigations because it contains a variety of information about a phone’s activity at any specific point in time. **Exhibit F** hereto is a screenshot taken from the Cellebrite Reader application demonstrating that the “Savage” chat was recovered from the Knowledgec.db file.

25. The conversation fragments recovered from the knowledgec.db file contain only incoming messages to the [REDACTED] iPhone and not any outgoing messages because the relevant information recorded in the knowledgec.db file is from incoming message notifications to the [REDACTED] iPhone. That incoming message notification would include the text of the incoming message, which was recorded in the knowledgec.db file.

26. Outgoing messages from the [REDACTED] iPhone were not recorded in the database because they did not result in a notification on the phone.

27. I have reviewed the following statement by United States Secret Service Officer [REDACTED] [REDACTED] contained in a May 14, 2025 sworn declaration in support of a search warrant:

“when viewing an individual’s Telegram account on their mobile device, often times the only visible messages are incoming messages, and the

outgoing messages are not saved on the app. Thus, [REDACTED] may have sent messages over Telegram to [REDACTED] and/or [REDACTED] that law enforcement officers are unable to see based solely on their review of the [REDACTED] Cellphones.”⁴

This statement is inaccurate and is indeed inconsistent with the data recovered from the government’s own investigation of the [REDACTED] iPhone, which contains approximately 195 *other* Telegram group chats, the vast majority of which all contain outgoing messages from the username “[REDACTED]” dating back to August 26, 2019. The government’s representation that “outgoing messages are not saved on the [Telegram] app” is fundamentally incorrect.

THE DELETED CHAT

28. Separate from the “Savage” chat portions that were recovered from the knowledgec.db file, there is a portion of a group chat beginning on December 28, 2023 involving [REDACTED], [REDACTED] ([REDACTED]) and [REDACTED] that was recovered which Cellebrite indicates was deleted.

29. This “Deleted Chat” was recovered from an SQLite database from within the Telegram data folder of the [REDACTED] iPhone called “db_sqlite”, which is entirely different from the knowledgec.db file. Db_sqlite is the central Telegram database file. **Exhibit G** hereto is a screenshot from Cellebrite Reader demonstrating that the deleted chat was recovered from the Telegram messenger data folder from the [REDACTED] iPhone, specifically from the db_sqlite file.

⁴ May 14, 2025 Sworn Declaration of United States Secret Service Officer [REDACTED]
[REDACTED], USAO_282801 at fn. 3, Exhibit E hereto.

30. The recovery of deleted Telegram messages or any other deleted data from an iPhone is a complex process that requires parsing together data and information from various database tables to piece together the deleted information.

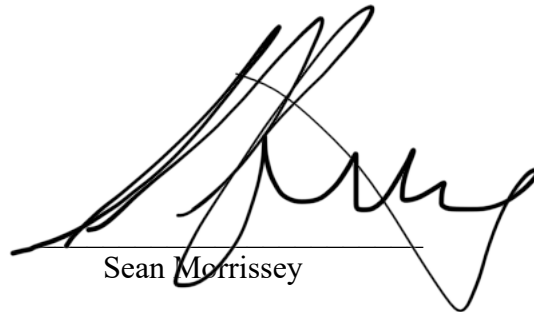
OTHER MEMORIALIZATION OF THE “SAVAGE” GROUP CHAT

31. In addition to the knowlegec.db file, the “Savage” group chat and other fragmented conversations are stored in a separate location of the [REDACTED] iPhone that appears to contain recorded user notifications from an application called DuetExpertCenter. **Exhibit H** hereto is a screenshot from Cellebrite Reader demonstrating that a portion of the “Savage” group chat was also recovered from “DuetExpertCenter” within the [REDACTED] iPhone.

32. While I am continuing the investigate the reasons that incoming notifications would be stored in this database file, it is presently my opinion that that those notifications were incoming notifications to an iOS application called “Duet”, which permits a user to use an external device, such as an iPhone or iPad as a secondary display monitor.

33. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, pursuant to 28 U.S.C. § 1746.

Dated: June 30, 2025
Las Vegas, Nevada



Sean Morrissey

EXHIBIT A

SEAN MORRISSEY

Las Vegas, NV

OPTIV**Jun 2020 – Present****Senior Domain Advisor, Threat, Application Security, and Vulnerability Management**

Drive demand generation across the full portfolio including sales and pre-sales support to best meet the business and technology needs.

- Partner with clients to solutions and communicate the proper solution blueprint on specific custom deals.
- Oversight on proposals and statements of work creation for the proper execution of specific custom deals.

Senior Consultant II, Enterprise Incident Management

Incident Response: experience conducting or managing incident response investigations for organizations, investigating targeted threats such as the Advanced Persistent Threat, Organized Crime, and Hacktivists

- Client facing role for various incidents responsible for inbound calls, client updates, and Reporting.
- Subject Matter Expert for Mobile Device and Mac OS Forensics.
- Selected to an internal project that was responsible for changing the practice from a small boutique firm to engaging in large scale Incident response matters and being selected to be on insurance panels. This project dealt with overhauling management processes and prosecution of incident response engagements. Coordinating with sales and finance teams to meet the needs of future clients. This project also dealt with improving infrastructure and software upgrades.

CROWDSTRIKE**Aug. 2019 – Jun 2020****Manager, Professional Services**

Incident Response: experience conducting or managing incident response investigations for organizations, investigating targeted threats such as the Advanced Persistent Threat, Organized Crime, and Hacktivists

- Program Manager for various incidents responsible for inbound calls, overall project oversight, client updates, and Reporting.
- Subject Matter Expert for Mobile Device and Mac OS Forensics.
 - Responsible for Mobile Assessments and Incidents for High Profile Subjects.
 - Dealing with sensitive data and coordinating with security teams.

STROZ FRIEDBERG**Director, Data Forensics & Incident Response****Feb. 2018 – Jun 2019**

Incident commander and Lead creation of teams of data forensics experts in delivering reactive services to government agencies, expanding market and focus of global data security consulting firm.

- Immediately stopped continued losses after \$1.7M data hostage occurrence with a 40-person attack team. Within 24 hours provided client with decrypted data, avoiding millions in day to day losses. Closed backdoors, decrypted data and employed pro-active sources and network testers at forefront, reducing back to “live” time.

- Led team of 12 forensics experts to reduce vulnerability to less than 10% for customer reward programs client experiencing a \$7M loss in sensitive data. Closed unsecured areas of network, repaired connections and fortified firewalls.
- Drove completion of \$70,000 data ransom situation, mitigating losses to one month of data for health pension company after being locked out. Decrypted data, reviewed policies and established hardened firewalls. Led team of 7 people.
- Monitored 1,000,000+ emails over 6-month period of company being bought by a Chinese company, developing both an iOS and Android app, leveraging Amazon Cloud identifying sensitive data being sent to Chinese nationals.
- Selected to be part of a senior group of Directors to test and establish a remote work force

KATANA FORENSICS, LLC Founder and CEO

Jul 2011 – Present

Responsible for business development, sales, personnel and executive leadership for specialized data extraction and analysis of mobile devices for military and government agencies

- Drove sales to \$1.4M annually, conducting extensive business development efforts, technical qualifications and channel development.
- Designed and led development of several software platforms designed to access and recover data, text messages, deleted messages and other app usage.
- Awarded FBI contract(s) valued at \$600k over 4-year period.
- Established online presence for existing and new customers that \$10k in monthly recurring revenue.

Sean Morrissey

- Software in high profile cases including professional sports, Local, State and Federal police agencies and Homeland Security.

US STATE DEPARTMENT

Computer/Mobile Forensic Examiner

Aug 2009 – Oct 2011

Examined mobile devices for data breaches and computer analysis for forensics lab of US Government.

- Developed process and procedures for examining and preparing iPad technology to be used in US State Department.
- Conducted systemwide investigations for forensics, password or visa fraud, data collection, seizure and confiscation, analyzing cellphones mobile devices, extracting critical data for prosecution of suspects.
- Developed new imaging procedures on iMac Air, combined 2 separate programs including a Windows based program, reducing imaging time from days to minutes
- Created new process for recreating suspects phone location and personal movement, building scripts that recreated map of location history of phone via map tiles

US DEPARTMENT OF DEFENSE Computer Forensics Instructor

Jul 2006 – Aug 2009

Developed and delivered classes in Macintosh / Advanced Windows Forensics analysis to military and government agency personnel.

- **Battlefield forensics** – deployable forensics, allowing someone to imaging a phone or computer with minimal technology, reducing time to acquisition and persecution while increasing actionable intelligence.
- *Developed and wrote curriculum and research on iOS forensics*, used by US Academy for Fed Law Enforcement center. Secret service, CID NCIS, special forces, FBI, Military Intelligence,
- Recognized expert globally, spoke at Mobile World Forensics conference with iOS hacking expert .

MPRI Military Advisor / Instructor

Jun 2003 – Nov 2006

Delivered Janus simulation and scenario-based training for Officers of African Militaries as part of peace keeping efforts on the African Continent.

EASTON POLICE DEPARTMENT / TALBOT COUNTY SHERIFFS DEPT Law Enforcement Officer

Jul 1997 – Aug 2003

Conducted peace keeping patrol, criminal and undercover narcotics investigations for local and county police forces.
Awarded Merit Award for identifying and integrating modernizations to Police Department.

UNITED STATES ARMY Special Project Officer / Executive Officer / Operations Officer

1984 - 1997

PUBLICATIONS

<i>IOS Forensics Analysis (ISBN 978-1430233428) –</i>	<i>2010</i>
<i>Mac OS X iPod and iPhone Forensic Analysis (ISBN 978-1597492973)</i>	<i>2008</i>
<i>Defense Against the Dark Arts (ISBN 978-143-9821190)</i>	<i>2011</i>
<i>Mac Editor and Columnist – Digital Forensics Magazine</i>	<i>2010-2012</i>

TEACHING EXPERIENCE

Department of Defense Cyber Crime Center
National Computer Forensics Institute
Federal Law Enforcement Training Center
Katana Forensics, LLC

EXPERT WITNESS TESTIMONY

Commonwealth of PA Vs [REDACTED]

United States Vs Simmons

Major Case Consulting

State of New York Vs Thomas Clayton
State of Louisiana Vs Thomas Lavergne

EDUCATION

Bachelor of Arts – Creighton University – Omaha NE

University of California- Irvine – Project Management Certificate

CERTIFICATIONS

Defense Forensic Examiner – Department of Defense (DOD)
Defense Digital Media Collector – DOD
Paraben Mobile Device Examiner – Paraben