James R. McGee

Smiths Station, AL 36877 | **james@metadataforensics.com**

Professional Profile:

Reliable and passionate Digital Forensic Examiner with Metadata Forensics with extensive working knowledge in complex digital forensic examinations, felony investigations, interviews and interrogations, and crime scene examinations. Former U.S. Army Criminal Investigation Division Special Agent and Digital Forensic Examiner. Extensive history in providing guidance regarding digital forensics and providing expert advice to senior officials on all aspects of computer crime investigations. Engaged and active contributor in the Digital Forensic Incident Response community. A versatile leader with excellent written and oral communication skills and comprehensive knowledge of the Uniform Code of Military Justice and military operations during a nine-year career in the United States Army.

Core Qualifications

- DoD Certified Cyber Crime Investigator
- Former USACIDC Certified Digital Forensic Examiner
- DoD Certified Digital Media Collector
- Cellebrite Certified Physical Analyst
- Complex Computer and Cyber Investigations
- Conducts Sensitive/Serious Investigations
- Digital Evidence Preservation/Collection
- Strong Verbal and Written Communication
- TS/SCI Security Clearance
- Trained in Defensive Tactics
- DoD Certified Digital Forensic Examiner
- Certified Expert in Digital Forensics
  United States District Court
  Southern District of Georgia
- Magnet Certified Forensics Examiner
- Magnet Certified Cloud Examiner
- Magnet Certified Mac Examiner
- Magnet Certified Video Examiner
- Execution of Subpoenas and Search Warrants
- Over 800 hours of Digital Forensic Training

Experience:

Digital Forensic Examiner
January 2023 to Present
Metadata Forensics, LLC
• Provide thorough and accurate digital investigation services in both civil and criminal legal matters using state of the art technologies and forensic science techniques.
• Conduct forensically sound digital data examinations, collect and document all relevant information, maintain chain-of-custody, and write detailed reports of finding.
• Provide expert consultation and testimony in legal matters when required.

Special Agent - Digital Forensic Examiner
January 2021 to January 2023
Cyber Directorate, Digital Forensics – East, Fort Benning DFE Cell
• Planned, developed, and conducted over 70 digital forensic examinations, consisting of over 100 pieces of evidence, totaling over 20,000 Gigabytes of data.
• Displayed experienced leadership while stepping into a role reserved for a Senior Warrant Officer and produced exceptional results during this time in command. This was furthered in a consistent recognition of leadership ability by higher headquarters and subordinate units for steadfast leadership and direction of examinations.
• Testified in criminal trials as an expert witness and assisted numerous times in trial preparation.
• Reviewed and prepared digital forensic examination reports of felony criminal investigations.
• Processed, analyzed, and examined complex data from numerous device manufactures and operating systems.
• Extensive experience with industry standard forensic tools such as EnCase, Cellebrite, Magnet Axiom, GrayShift, FTK Imager, and open-source software.
• Created and provided training and guidance on digital forensics to all assigned agents of the Southern Field Office.
• Dedicated over 100 hours of personal time to the further development of technical articles which were made available to the digital forensic community around the world.

Special Agent
November 2017 to January 2021
U.S. Army Criminal Investigation Command, 10th MP Battalion (CID), Fort Gordon CID Office
• Investigated felony offenses for Department of the Army with 95% solve rate, in direct support of the U.S. Army Cyber Command and the Fort Gordon Military community.

• Responsible for the conduct of felony investigations including interviews of victims, witnesses, and subjects; processing crime scenes; evaluation of evidence; preparing administrative reports; and testifying before courts and boards.
• Held DoD Certified Digital Forensic Examiner certification while conducting or immediately overseeing over 46 cellular phone extractions, created and provided training on digital forensics to all assigned agents at the Fort Gordon CID Office, and served as the liaison between the office and the Fort Bragg DFE Cell.
• Testified three times in federal court as well as court martial proceedings.
• Performed appointed duties of Alternate Evidence Custodian, Unit Safety Officer, Lead for Motorcycle Mentorship Program, COMSEC, Alternate Voting Assistance Officer, Alternate Recruiting Coordinator, and Alternate Security Manager.
• Maintained liaison with supported commanders, Staff Judge Advocate, civilian and international law Enforcement.

Geospatial Engineer Sergeant
September 2014 to June 2017
United States Army, 1st Cavalry Division, Division Artillery, HHB
• Planned, collected, evaluated, and supervised the production of geospatial products.
• Provided detailed geospatial analysis products for 1st Cavalry Division, Division Artillery and subordinate elements.
• Responsible for the maintenance and accountability of geospatial equipment.
• Facilitated activities pertaining to training on Digital Geospatial Information Systems with geospatial products.

Professional Presentations:

Selected to brief during the 2022 Computer Crime and Digital Forensic Training Forum on own original work, Biome AppIntents – An Alternate Location for Deleted SMS/iMessage Data in Apple Devices. The presentation was regarded with high praise from superiors and peers.

Published Works:

Formulated practical digital forensic validating experiments based on sound hypothesis, then produced as scholarly journal articles which were either approved for publication at the Digital Forensic Research Workshop (DFRWS.org), The Metadata Perspective, or Belkasoft.

Reviewing the new iOS Apple Health Workout Artifact through Magnet AXIOM 7.3 – Published on The Metadata Perspective on August 17, 2023.
Synopsis: This article explores Magnet Forensics AXIOM 7.3 new iOS artifact for Apple Health Workout as well as a custom artifact created to parse Workout data.

Apple Fitness Workout Location Data: Leveraging the healthdb_secure.sqlite Database – Published on The Metadata Perspective on June 21, 2023.
Synopsis: iOS 16 brought many changes for digital forensics and one, seemingly, unexplored area was the increased wealth of location data stored within the healthdb_secure.sqlite database. The location data is stored within the "location_series_data" table of the database for specific workout activity types initiated on the Apple Watch. The data includes: a series identifier, timestamp, latitude, longitude, altitude, speed, course, horizontal accuracy, vertical accuracy, speed accuracy, course accuracy, and signal environment. This article will explore an initial effective, but inefficient, SQL query correlating location data to the ongoing workout; an effective and efficient SQL query correlating location data to the ongoing workout; and finally, a SQL query which provides an analysis as to the actions likely taken by the user for the initiation, pausing, and completion of workouts.

Lagging for the Win: Querying for Negative Evidence in the sms.db – Published by Belkasoft on March 20, 2023.
Synopsis: When sent or received iMessage/SMS/MMS messages are permanently deleted from Apple iPhone's native Messages Application, rows of data are removed from the sms.db – the storage database for the application. When these messages have been removed and data is no longer available, even in the sms.db-wal, this article explores how an examiner/investigator can identify these messages and where they can look for potentially valuable message content. Available for review at https://belkasoft.com/lagging-for-win.

An Alternate Location for Deleted SMS/iMessage Data in Apple Devices – Published at DFRWS.org on November 3, 2022, and a Forensic 4:Cast DFIR Article of the Year 2023 Finalist.

Synopsis: Subjects and persons of interest in criminal investigations are likely to delete data from their devices in an attempt to remove evidence which could be incriminating. With this, the data still present or recoverable on mobile devices can be extremely beneficial to both Law Enforcement Investigators and Digital Forensic Examiners/ Investigators. The sms.db should be reviewed when looking for SMS/iMessage data on an Apple mobile device; however, messages deleted by the user of the device can quickly be overwritten within the database. A new area of focus has been found within Apple devices using iOS 14.0 or later, specifically within the private/var/mobile/Library/ Biome/streams/public/AppIntent/local file path of a Full File System Extraction. Available for review at https://dfir.pubpub.org/pub/yp6efc8q/release/1.

Enriching Investigations with Apple Watch Data Through the healthdb_secure.sqlite Database – Published at DFRWS.org on January 5, 2023.
Synopsis: While an Apple Watch itself offers limited extraction options, the paired device can provide significant data for today's criminal investigations. As I will cover, beneficial location data and activity/heart rate data is maintained within the paired device. Knowing where to locate, how to review, and how to display this data in a readable format can provide the picture required to aid investigations. This process additionally allows the validation of data parsed through other software, if available. This article will focus entirely on the data gained from an Apple Watch through a Full File System Extraction/Advanced Logical File System Extraction of the paired Apple iPhone. Available for review at https://dfir.pubpub.org/pub/xqvcn3hj/release/1.

An Initial Review of the Apple iPhone App Privacy Report – October 19, 2022
Synopsis: According to Apple Support, the App Privacy Report grants visibility to how applications use the privacy permissions granted as well as application network activity. This article will explore data available to review through a Full File System Extraction of an Apple iPhone.

Manual Verification of Absolute Time (Double) Values: Timestamps and Other Usages – November 4, 2022
Synopsis: While the majority of us are familiar with Absolute Time (Double) Values, less of us understand the conversion from a little-endian double precision 64-bit hexadecimal expression to the number of seconds since midnight, January 1, 2001. This article will fully cover the steps within the conversion process, how to reverse the conversion, and the significance for Digital Forensics.

Maximizing iOS Call Log Timestamps and Call Duration Effectiveness: Will You Answer the Call? – November 30, 2022
Synopsis: Call Log Artifacts have long been used to link connections between individuals, aided in pattern of life analysis, and utilized in attempts to establish user attribution data. This article will explore call log timestamps within iOS as they are typically parsed as well as establishing a simple and beneficial parsing change which expands the usefulness of these artifacts. Finally, this article will provide an "at a glance" reading of call durations through an advanced query structure.

Witness Testimony as an Expert at Trial or by Deposition:

- United States of America v. Colten Caudle
  Case No. 1:18-CR-00072-JRH, October 4 – 8, 2021
  Law Enforcement Report: 0076-2018-CID043-004118
  Certified Expert in Digital Forensics
  United States District Court, Southern District of Georgia

- Law Enforcement Report: 0088-2021-CID703-017772
  Deposition in Court Hearing, November 8, 2022

Education:

- Bachelor of Arts, Business Management (3.45 GPA), May 14, 2011
  Grove City College, 100 Campus Drive, Grove City, PA 16127

Job-Related Certifications / Licensure:

- Magnet Certified Video Examiner, December 6, 2022
- Magnet Certified Mac Examiner, November 22, 2022
- Magnet Certified Cloud Examiner, September 16, 2022
- Magnet Certified Forensics Examiner, July 23, 2022
- DoD Cyber Crime Investigator, June 24, 2022
- USACIDC Certified Digital Forensic Examiner, March 25, 2021
- Cellebrite Certified Physical Analyst, August 21, 2020
- Cellebrite Certified Operator, August 9, 2020
- DoD Digital Forensic Examiner, August 30, 2019

Job-Related Professional Training:

- SQLite Forensics with Belkasoft, Belkasoft, January 25, 2023
- DV200 Digital Video Investigations with DVR Examiner, Magnet Forensics Training, December 1, 2022
- AX350 Magnet AXIOM macOS Examinations, Magnet Forensics Training, November 4, 2022
- AX320 Magnet AXIOM Internet & Cloud Investigations, Magnet Forensics Training, September 9, 2022
- AX300 Advanced Mobile Forensics, Magnet Forensics Training, July 29, 2022
- AX250 Advanced Computer Forensics, Magnet Forensics Training, July 22, 2022
- Forensics and Intrusions in a Windows Environment, Defense Cyber Investigations Training Academy (DCITA), June 24, 2022
- AX100 Forensic Fundamentals, Magnet Forensics Training, May 20, 2022
- Technology Evidence in Domestic Abuse, DCITA, May 6, 2022
- Introduction to Advanced Level Courses encompassing 20 Hours, GrayShift, March 15 – 18, 2022
- Various CyberCasts encompassing 39.5 Hours, DCITA, 2020 – 2021
- Cyber Fundamentals 100, DCITA, November 5, 2021
- Cellebrite Mobile Forensics Fundamentals, August 7, 2020
- Windows Forensic Examinations – EnCase, DCITA, July 31, 2020
- Introduction to Cyber Investigations, DCITA, May 14, 2020
- Cyber Threat and Techniques Seminar Pilot, DCITA, February 28, 2020
- Network Intrusions Basics, DCITA, February 12, 2020
- Digital Data Protection, DCITA, January 31, 2020
- Cyber Incident Response Course, DCITA, August 30, 2019
- Introduction to Networks and Computer Hardware, DCITA, April 11, 2019
- Special Victims Capabilities Course, Fort Leonard Wood, November 8, 2019
- CID Special Agent Advanced Leaders Course, Fort Leonard Wood, November 21, 2018
- Structured Child Interviewing, Fort Leonard Wood, June 13, 2018
- Child Abuse Prevention and Investigative Techniques Course, Fort Leonard Wood, June 8, 2018
- Domestic Violence Intervention Training, Fort Leonard Wood, March 2, 2018
- U.S. Army Criminal Investigation Division Special Agent Course, November 7, 2017
- Basic Leader Course, Fort Hood, April 14, 2016
- Geospatial Engineer Advanced Individual Training, Fort Leonard Wood, September 23, 2014
- Basic Combat Training, Fort Leonard Wood, April 18, 2014