

Carney Forensics

John J. Carney, Esq.
Scandia, MN

Office: 651.695.1757
Cell: 612.386.0453

E-mail: jjc@carneyforensics.com

Web: www.carneyforensics.com

August 28, 2020

Mobile Device Forensic Protocol

1. I am the Chief Technology Officer and lead examiner at Carney Forensics, which is an assumed name of Carney Consulting LLC, a Minnesota limited liability company. Carney Forensics is a digital forensics consulting agency, which has operated in Minnesota for over ten years. My CV is attached which describes my education, experience, credentials, certifications, publications, and testimony history. I will perform the mobile device forensic examination on the device in my lab in the Twin Cities.
2. Recovery of mobile evidence from mobile devices starts by a lawyer requesting it during discovery. Normally that begins with a request for production, but sometimes a motion to compel is necessary. The device produced for examination is the handset, which most people think of as the smartphone itself. Enclosed in the handset is a SIM card. A SIM card is a Subscriber Identity Module which stores network credentials, last tower identity, and the user's phone number. Android smartphones also feature a microSD card, a memory card enclosed within the handset. It stores photograph, video, audio, and sometimes document evidence.
3. I use process guidelines for the forensic examination and production of evidence from mobile devices that's been the standard in the mobile device forensics field for over a decade. While the specific details of the examination of each device may differ, the adoption of consistent examination processes assist the examiner in ensuring that the evidence extracted from each mobile device is well documented and that the results are reasonably repeatable and defensible.

Cellular Phone Evidence Extraction Process

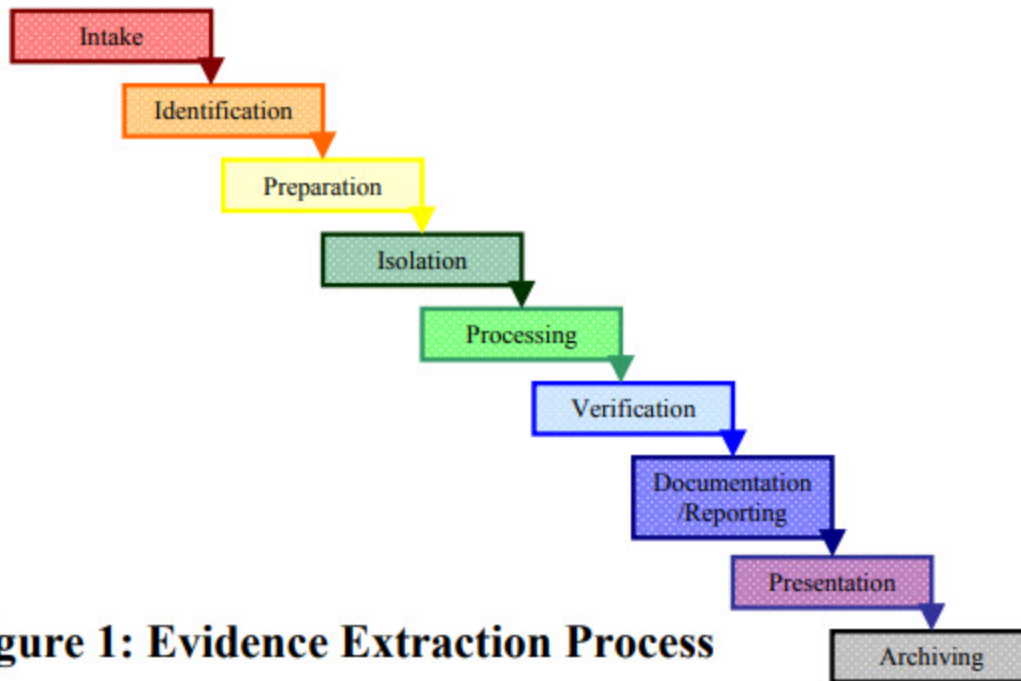


Figure 1: Evidence Extraction Process

4. I use chain of custody documentation for mobile devices with foundation prepared for inbound and outbound transit to and from my digital forensics lab.
5. I protect the integrity of the mobile device evidence in my examinations by employing forensically sound best practices used by certified mobile device forensics examiners as recommended by the U.S. Department of Justice in their “Electronic Crime Scene Investigation: A Guide for First Responders”, Second Edition, April 2008.

APR.
08

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice



NIJ

Special

REPORT



Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

www.ojp.usdoj.gov/nij

6. I use forensically sound, generally accepted processes, methods, and tools under the written principles and standards, also best practices, recommended by the U.S. National Institute of Standards and Technology (NIST), the Sedona Conference, the Scientific Working Group on Digital Evidence (SWGDE), and the American Academy of Forensics Sciences (AAFS), the latter organization of which I am a voting member.
7. NIST published a reputable document entitled "Guidelines on Mobile Device Forensics", NIST Special Publication 800-101, Revision 1, which states on page 48:

"The examination process uncovers digital evidence, including that which may be hidden or obscured. The results are gained through applying established scientific based methods and should describe the content and state of the data fully, including the source and the potential significance."

Guidelines on Mobile Device Forensics

Rick Ayers
Sam Brothers
Wayne Jansen

<http://dx.doi.org/10.6028/NIST.SP.800-101r1>



8. I use standard network isolation techniques to protect the mobile device including use of a Faraday bag to house the device and to protect it from radio frequency (RF) signals. I also enable airplane mode on the mobile device at my first opportunity to protect physical memory from evidence contamination from nearby cell towers, Wi-Fi networks, and Bluetooth devices.
9. Mobile device experts must isolate and protect their devices to prevent evidence contamination and overwriting deleted data. This practice is so important that the U.S. Government has written federal standards for all practitioners' use in their examinations of mobile devices to support federal investigations and litigation in federal courts. Please see the above mentioned standards from the U.S. Department of Justice and the National Institute of Standards and Technology (NIST).
10. Also a prestigious digital forensic trade organization named Scientific Working Group on Digital Evidence (SWGDE) has written standards on mobile device forensics which describes best practices for evidence handling and data isolation. Included in SWGDE standards for mobile device examinations is a practice of documenting and reporting any incoming phone evidence that contaminates the device during examination.



Scientific Working Group on Digital Evidence

5.4 Documentation

Documentation should meet the requirements of the organization's policies and should at least contain information on evidence handling, examination information and a report of findings.

- Evidence handling documentation should include but is not limited to:
 - Copy of legal authority.
 - Chain of custody.
 - Detailed description and/or photographs of the phone (e.g., phone number, make, and model).
 - Photographs or documentation of any visible damage.
 - Information regarding the packaging and condition of the phone.
- Examination documentation should be preserved according to policy and include:
 - Sufficient detail to enable another examiner, competent in the same area of expertise, to repeat the findings independently.
 - Tools and software used in the examination.
 - Documentation of any anomalies in the data acquisition (e.g., acquisition disruptions, faulty cables, and incoming data).
 - Substantive communication notes regarding the case.

11. Last, Minnesota's Bureau of Criminal Apprehension (BCA) serves as an example for Minnesota digital forensic examiners to adhere to these federal and trade standards for mobile phone isolation to protect digital evidence. A recent example is shown in BCA mobile device forensic examiner Shawn Hughes' digital forensic report describing his examination of a defendant's iPhone.

Description of Evidence:

Exhibit 0.1

- T-Mobile Apple cell phone, model no.: iPhone A1549, IMEI: 359234061519742

Processing:

The Exhibit 0.1 cell phone was placed into a Ramsey faraday enclosure to prevent possible data alteration from the receipt of wireless transmissions. The cell phone was powered on and then connected to a CelleBrite Universal Forensic Extraction Device (UFED) Touch. The CelleBrite UFED Touch assists specialists in the acquisition of data from mobile devices such as cell phones, tablets, GPSs, etc. Specialist Hughes performed a file system extraction of data from the cell phone using the CelleBrite UFED Touch.

The resulting file containing the extracted data were then processed using the software CelleBrite Physical Analyzer (PA) v4.1. The CelleBrite PA software assists specialists in the parsing of data from mobile device extractions. The CelleBrite PA software performed a number of automated tasks such as parsing text messaging, detailing call logs, etc. The CelleBrite PA software was used to generated a report containing the processing results.

The generated report was recorded to disc and provided to the McLeod County Sheriff's Office along with all original evidence.

All examinations are concluded and no further examination is requested at this time.

12. When a mobile device enters my lab I screen it initially for any hardware damage or malfunction. Examples include broken screen, discharged or defective battery, water damage, or a damaged data port. The latter is important because device data extraction involves connecting the mobile device to my forensic workstation using an USB cable. If the device cannot connect, it cannot be extracted.
13. I use best of breed, world class repair facilities in both Ohio and New Hampshire operated by mobile forensic hardware experts who regularly speak at national digital forensic conferences and testify in court. I have used Binary Intelligence in Franklin, Ohio on several repair and data recovery cases including an Appellate Public Defender post conviction case, State of Minnesota v. Nidjia Dean Nicks, in which I performed joint mobile device forensic examinations with the Minneapolis Police Department. I have used FlashFixers in Portsmouth, NH on numerous occasions for repairs and data recovery work on other electronic devices.

14. I pursue recovery of all digital evidence, both live and deleted, on mobile devices in my lab. I employ my three best mobile device forensic tools to examine it. I use the latest release of Cellebrite's UFED 4PC (Universal Forensic Extraction Device) to extract the device and UFED Physical Analyzer to process and analyze it. Cellebrite's UFED hardware and software are used by investigators in both the public and private sectors worldwide. Over 90,000 hardware units have been sold to law enforcement at local, county, state or provincial, and federal levels; corporate legal and security teams; private investigators and consultants; and military field personnel in over 100 countries. Securities, customs and border protection, immigration, and various task forces all use UFED to investigate narcotics, human trafficking, fraud, homicide, sexual assault, and numerous other types of cases.
15. UFED's extraction processes are generally accepted as a valid scientific process due to its read-only transfer of data from source device to target drive. Cellebrite's UFED tools have been referenced in many judicial opinions and orders in federal cases at both district and appellate levels in jurisdictions across the U.S.
16. Cellebrite's UFED hardware and software have been independently tested at least seven times by the U.S. National Institute of Standards and Technology (NIST) and once by the U.S. Department of Justice's National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence.
17. The National Institute of Standards and Technology evaluated Cellebrite UFED hardware and software in 2009, 2010, 2012, 2016, 2017, 2018, and 2019 as part of its Computer Forensic Tool Testing Project. In all those years, the UFED completely and accurately acquired all supported objects, with few anomalies.
18. The National Institute of Justice study, completed in July 2012, tested seven devices as part of the NIJ Research, Development, Testing and Evaluation Process. It concluded: "Cellebrite's UFED performed consistently well during the testing. Connectivity issues between the UFED and phones tested were rare. In these tests, the UFED only had difficulty connecting to certain GSM phones that did not contain a SIM card, and these issues most likely could be remedied by creating a cloned SIM card."
19. UFED Physical Analyzer features a fast and convenient malware scanner that uses the latest Bitdefender signatures to determine the cybersecurity status of the mobile device file system and identify any viruses, spyware, Trojans, worms, or other computer exploits. Bitdefender is a global leader in cybersecurity and generally accepted within the digital forensics community worldwide.
20. I cross validate my mobile evidence handset results with Oxygen Forensic Detective by examining the mobile device with it and then comparing and contrasting it with the Cellebrite UFED evidence. Law enforcement and government agencies, institutions, corporations, and private investigators rely on Oxygen Forensic products to ensure evidence availability when mobile device data analysis and recovery are required. Oxygen Forensic customers include various U.S. and European federal and state agencies, such as the U.S. Department of Defense, U.S. Department of Justice, U.S. Department of Homeland Security, U.S. Department of Transportation, U.S. Postal Service, U.S. Internal Revenue Service, U.S. Supreme Court, European Commission, London Metropolitan Police, French National Police and Gendarmerie, German Federal Criminal Police Office, Italian Financial Guard, and the

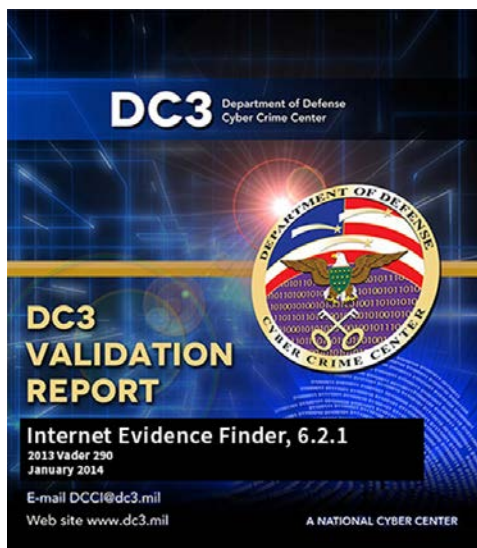
Spanish Civil Guard. Also, Big Four, national consulting firms like PricewaterhouseCoopers and Ernst & Young are Oxygen Forensic customers.

21. I also cross validate my Cellebrite UFED's Subscriber Identity Module (SIM) card evidence results with Magnet Forensics' AXIOM. I extract and process the SIM card a second time and compare and contrast my mobile evidence results between the two mobile device forensics tools and the forensic examinations I perform with each.

22. Magnet Forensics' computer and mobile device forensics tools are trusted and used by over 3,000 law enforcement agencies in 92 countries to assist in their investigations. Magnet Forensics AXIOM tool has been independently tested in October of 2018 by the U.S. National Institute of Standards and Technology (NIST).

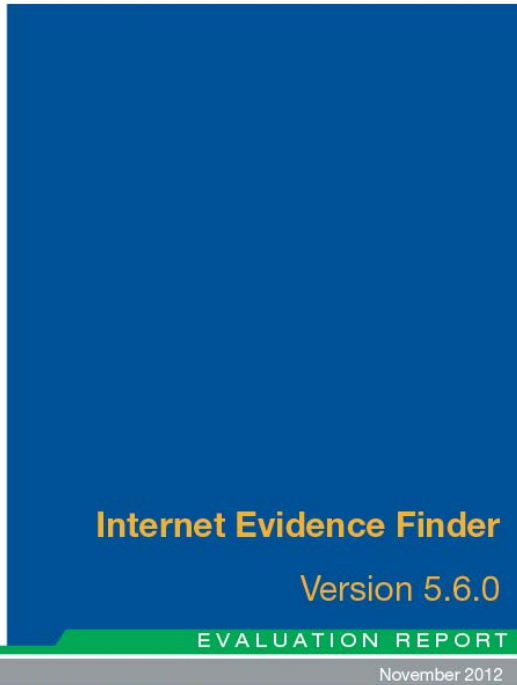
23. Magnet Forensics' prior mobile device forensic tool, Internet Evidence Finder (IEF), which I used for five years before using AXIOM, has been validated by the United States Defense Cyber Crime Institute (DCCI). DCCI is the research, development and evaluation arm of the Department of Defense that tests tools tailored to the requirements of digital forensic examiners and incident responders. DCCI is a part of the Department of Defense Cyber Crime Center (DC3). The DCCI report evaluated IEF on 42 criteria to determine the circumstances under which computer crime investigating agents assigned to Defense Criminal Investigative Organizations (DCIOs) may employ IEF for digital forensic investigation and analysis. DCCI's findings included:

- IEF is forensically sound and does not modify evidence files upon reading them.
- IEF successfully produces the same results after being run against the same dataset multiple times.
- IEF successfully recovers data from several Internet related artifacts.



24. Internet Evidence Finder has also been independently tested by the U.S. Department of Justice's National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence. The National Institute of Justice study, published in November 2012, tested IEF on several systems and drives as part of the NIJ Research, Development, Testing and Evaluation Process.

25. The NIJ study concluded: “In every instance that IEF was run, it was able to discover Internet artifacts. IEF consistently found information that was not expected to be found. IEF provides a very clear idea of how the computer under examination has been used over a long period of time. IEF also discovers evidence that an investigator may have not thought to initially look for. Manually performing the searches that IEF automatically performs would take an investigator a great deal of time, effort and knowledge. IEF clearly demonstrates a tool that would enhance the efficiency of justice. There is no doubt IEF is a superior tool and should be a part of every investigator’s toolbox.”



26. I cross validate photographic and video results with Phil Harvey’s versatile and respected ExifTool which excels at recovering identity and foundation metadata from media evidence. When necessary, I also use advanced photograph and video analysis services to authenticate the veracity of media content and to enhance visual recognition and fidelity. Last, I cross validate Microsoft Office and PDF document forensic results using the PayneGroup’s authoritative Metadata Assistant tool.

27. I use a native form of production to produce or export mobile evidence to the parties for their review in criminal and civil cases. It is far superior to other primitive forms of production

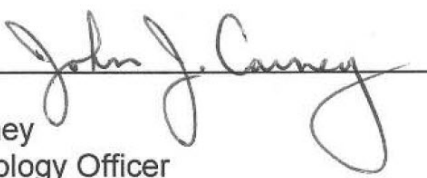
because it cost effectively supports full text search and a thorough inspection of all available metadata with no additional effort.

28. Once the mobile device is extracted and processed using mobile device forensic tools I generate a mobile evidence summary document for use by the parties. It serves as an evidence inventory and names the evidence artifacts (contacts, calls, texts, photos, videos, etc.) and the quantity of each on the smartphone. It highlights the evidence available for analysis, but also evidence previously unknown to the parties. I send it to the legal team to start a conversation about the goals of the examination for the mobile device. My analysis is guided by the legal team's decisions in a prioritized goal of the examination. Together we educate each other on case facts and the emerging evidence strategy and collaborate on identifying which evidence types merit analysis time and attention.
29. After analysis I use my mobile device forensic tools to generate reports responsive to the legal team's goal of the examination. For instance, one report might be a chronology of text messages with content and descriptive metadata. A second report might contain photographs from the particular date of an incident to be litigated. My mobile device forensic reports are generated in PDF, Microsoft Word, or Microsoft Excel formats. They present embedded photographs, also attachments and links to be opened and reviewed. Most legal teams have Microsoft Office and Adobe Acrobat tools for working with these report formats.
30. Mobile device forensic reports can also be a web browser document which the legal team reviews using browser software like Chrome, Firefox, Edge, or Safari on a PC, Mac, smartphone, or tablet. Browser reports are searchable, can easily display links in native format, also attachments, and show a coherent tabular presentation of evidence metadata. Most legal teams are skilled at using browsers on their computers and mobile devices.
31. Alternatively, mobile device forensic reports can be a data set for part or the entire mobile device's evidence in native form. I can share these with the legal team who can then review the evidence on their Microsoft Windows workstation using mobile evidence reader software I provide with no license fee. I can provide it also to the opposing party and third party defendants with no license fee. The software is reasonably easy to use and does not require extensive training classes or certifications. User documentation and online videos are available at no charge to ease the learning curve.
32. Cellebrite's UFED Reader provides capabilities to review mobile evidence, metadata, and timelines. The user can search, analyze, filter, and bookmark it. The user can also generate his or her own custom mobile evidence reports for subsequent review by a client or for production to the court or opposing party. And the user can capture screens and record videos to quickly and clearly document and explain mobile evidence investigative processes, build visual reports easy to present and share, and communicate with others more effectively.

33. Magnet Forensics AXIOM Examine provides capabilities to review mobile evidence and metadata in a portable case file. The user can search and filter evidence, also add his or her own comments, tags, media categorizations, and bookmarks. The user can generate his or her own custom mobile device forensic reports for relevant evidence of interest and for previously tagged or bookmarked evidence. The user can also build and review timelines composed of mobile evidence.

34. I use an online, encrypted, digital distribution system to transfer a mobile evidence package to the parties in most timely manner available. For legal teams with more time available I generate a ready-to-review USB flash drive containing the mobile evidence and ship it by U.S. Post.

35. I strictly adhere to any protective orders issued by the court. Disposition of mobile evidence takes place after the dispute has been resolved by settlement or trial and all appellate actions have been exhausted. Upon receiving written notification from counsel, I wipe the mobile evidence and other evidentiary documents from production, archival, and backup storage.



John J. Carney
Chief Technology Officer
Carney Forensics