



SANS Institute

Information Security Reading Room

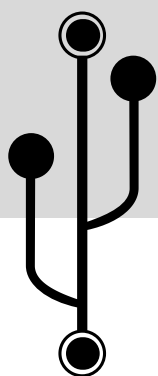
Six Steps To Successful Mobile Validation

Heather Mahalik

Copyright SANS Institute 2021. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

SIX STEPS TO SUCCESSFUL MOBILE VALIDATION



Authors: Heather Mahalik, John Bair, Alexis Brignoni, Stephen Coates, Mike Dickinson, Mattia Epifani, Jessica Hyde, Vladimir Katalov, Scott Koenig, Paul Lorentz, Christophe Poirier, Lee Reiber, Martin Westman, Mike Williamson, Ian Whiffin, and Oleg Skulkin



Cellebrite



ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS



MAGNET
FORENSICS®



OXYGEN
FORENSICS

MSAB



GRAYSHIFT

paraben®
corporation paraben.com

Belkasoft
forensics made easier





Digital forensics is a complex and ever-changing field that requires a lot of testing, tools and validation. This paper is written by experts in smartphone forensics who have many years' experience in research, tool development, validation, testimony and who care about educating the community on the recommended steps to ensure mobile data is extracted, examined and reported in a manner that is trusted.

The authors of this paper stand shoulder to shoulder even though our backgrounds, organizations and jurisdictions differ. Many tools and methods exist to support smartphone forensics and no one tool is perfect. Depending on your mission or investigation, not all steps may be required. Equally, as a summary document, the steps listed here cannot be exhaustive and more research or guidance could be necessary.

You, the investigator, should decide which steps are required to obtain what you have authority for or simply what answers the question at hand. We hope this paper guides you down a path to ensure your smartphone examinations are completed successfully.

The six steps below were created to reassure you on common methods for mobile validation. First and foremost, you need to document everything you do and consider preservation of evidence. How you handle the device matters. Make sure you understand how to protect the data and document every step of the way.

STEP I

DETERMINE ALL POSSIBLE EXTRACTION METHODS FOR YOUR SEARCH AUTHORITY

- A.** It is necessary to ensure that the seizure is legally authorized via consent, warrant, title, etc.
- B.** Think before you start and consider the order of extraction. Time is often the critical factor and there are cases when you may need to review some data manually (which may take just a few seconds) and only then make a decision which method to use.
- i.** Learn as much as possible about the target device to be able to choose the most appropriate extraction method and tool(s). For many devices, several different methods exist, and they often complement each other. Evaluate all possible risks for each, and start with the safest method and work to the most comprehensive (which may be the most risky), if time allows. It may be helpful to have a logical acquisition even if full file system can be obtained.
 - ii.** Keeping the device powered on and network isolated increases the chances of accessing the device, so please try to accommodate that. Note that some devices will turn on when plugged in, enabling them to be remotely wiped when they connect to network.
 - iii.** Read the tools or vendors product guides and help files. They contain lots of useful information that will help you deciding the way forward with your seized device.
 - iv.** If the device is not supported by your tools, contact the vendors and ask if there is a possible solution coming in future planned release.
 - v.** For eDiscovery cases be mindful of necessary upstream ingestion needs (Nuix, Relativity, etc.), and possible conversion(s) necessary from forensic tools. Keep in mind this may not only apply to eDiscovery investigations.
 - vi.** Ideally, interact with the device as little as possible prior to carrying out any extraction, given the possibility of triggering database changes, altering logs and usage records. Ensure that interaction with the target device which may change settings or data is necessary, proportionate, and deliberate.
 - vii.** Understand that exploits and specialized techniques are often required to recover data from smartphones. Be aware that some exploits will require the device to be restarted several times.
 - viii.** Understand what each extraction method will obtain from the device. Read the tool support notes wherever possible.
 - ix.** If data is not extracted, double-check all the connections and power. If still unsuccessful attempt to extract with another tool or another extraction method. Additionally, it may make sense to continue research and request support for devices that are not easily extracted from a vendor. If support is updated, additional extractions can then be obtained.

STEP I CONT.

- C.** Obtain extractions from external components of the mobile device.
 - i.** UICC (SIM) cards - remove after the extraction of the device and acquire separately using your tool of choice.
 - ii.** SD cards and the like should be acquired inside the device first and then should be removed, write-protected and acquired outside of the device, assuming time allows.
 - a.** In the instance of adoptable or encrypted storage, it will need to be acquired through the device.
- D.** If legally authorized, extract cloud data.
 - i.** Explain to the judge/attorneys/client why cloud data is just as relevant as the data on the device.
 - ii.** Social media and applications store data in the cloud that may not be accessible on the device.
 - iii.** Data recovered from a smartphone may lead to the discovery of possible cloud data and potential keys enabling access to cloud repositories.
 - iv.** Try to obtain warrant for data from Online providers if the data is relevant to your investigation. (i.e. Google, Facebook, etc.)
 - v.** Be aware that acquiring cloud data can raise alarms on the suspect's account. Act quickly once started.
- E.** If using an acquisition technique that is either new, unconventional or known to be unreliable, begin with a less invasive acquisition (such as a logical) so that in the event of a technique going wrong you are not left with nothing.
 - i.** Understand if the tool or method is using native extraction methods (iTunes or ADB backup).
 - ii.** If proprietary methods are used by the tools, make sure you understand how the tool functions and ask the vendor, where needed. When possible, test the methodology on an exemplar device before attempting the method on evidence. This may not always be possible.
 - iii.** Understand the configuration options that have been set for your extractions. (i.e. options settings that have been selected for the extraction, since this will impact not only how you acquire the data, but how you will review the data).

STEP I CONT.

F. Obtain acknowledgment (preferably written) from the investigator in charge (ideally after consultation with prosecutors) and/or device owner if you believe there is a potential for device bricking, warranty invalidation, or physical damage to the device.

- i. If a method has not been tested and publicly researched, try the method on a test device.
- ii. Obtain all extractions possible before attempting an extraction that could potentially damage a device. In some instances, it is advantageous to wait for an extraction method to be developed before attempting a methodology that could cause permanent physical damage to the device.

G. Use more than one tool or method to extract data that may be the focal point or key artifact of the crime. Understand that mobile log and system data (clock, etc.) constantly changes (user created artifacts should not change assuming the device is properly isolated), and two data extractions may not be exactly the same, nor necessary.

H. Always check which applications are installed on the device and determine the level of support your chosen tools offer.

- i. Different levels of extraction and support exist depending on device, chipset, OS version, and application version.
- ii. Document the versions of tools used to ensure your report stands valid based upon the level of support for applications at the time of examining the evidence.
- iii. Be aware that processes such as application downgrade may be necessary to recover data, changing application versions and requiring restarts of the device.
- iv. Manual verification may be required to ensure all applications are accounted for.

STEP 2

PROCESS THE DATA IN MORE THAN ONE TOOL

A. Make sure you update your tools regularly. Be sure to read the release notes and check if the added support fixes a bug or provides the necessary support for your device.

- i. Updating tools and verifying the updates can take extended periods of time.
- ii. When tools update, new bugs may be introduced. Make sure you verify against old versions or correlate artifacts to other tools and scripts to ensure data is being presented as expected.

B. Compare artifact results across more than one tool for anything that is considered essential evidence, whether exculpatory or inculpatory. These artifacts should be your priority for validation. Refer to step 3 when data is inconsistent. (Native application artifacts, contacts, calls, messages, browser, images).

- i. Make sure you know how the tool you are using will represent the data. Ask if you aren't sure if the tool is decoding and aggregating data or not.
- ii. Be sure to check the source of the data if there are any discrepancies between tools.
- iii. Different tools might parse different data types from same application.
- iv. Most tools support import of extractions from other tools and are able to decode them. Use it to verify your primary tools findings, this can be done after the device is returned to confirm your findings.
- v. Verify the duplicated data between different tools and concatenate data from the tools to give the most accurate representation of the application data.
- vi. Combine the results of different tools for tricky cases where different techniques can give additional results: carving, data evasion techniques like photovault, secure messaging that can leave remnants on the device, etc.
- vii. Make sure you reference and refer to CASE and FORMOBILE guidance.

C. Learn the intricacies of your tools.

- i. Be familiar with how your tools deduplicate, filter and show results.
- ii. Be familiar with how keyword searching works in your tools so that you understand the results.
- iii. Be familiar with file formats and how they are represented by the tools (SQLite, logs, plists, etc.).
- iv. Be familiar with the way your tool handles timestamps (default time zone, automatic conversion or not, etc.). Be aware that not all applications store all timestamps related to the device time. Mobile apps can utilize time offsets that are not related to UTC or the time zone of the device (i.e. Apple leverages Pacific Time for some artifacts).

D. If available, know your tool's capabilities to parse unsupported application's data in a semi-automatic way, but understand the limitations and deep dive where necessary.

E. Make sure your tool settings are correct to recover deleted artifacts, parse unsupported applications, provide connections, etc. Make sure to verify after every update.

F. Compare the list of installed applications to the list of applications supported by the tool(s) you are using.

STEP 3

DEEP DIVE FORENSICS: WHERE THE PUSH BUTTON STOPS AND FORENSIC EXAMINATIONS BEGIN

- A.** Do the artifacts make sense?
 - i. Are they legible?
 - ii. Does the timeframe correlate to the crime?
 - iii. Are they contextual?
- B.** Compare to the source/device.
- C.** Do not forget removable media (UICC (SIM) and MicroSD Cards).
- D.** Manually verify key artifacts on the handset and photograph them or use a tool to photograph them - what is the time set to?
 - i. It is wise to note the time zone for where the device was derived and the time zone of your lab (i.e. Device seized in Eastern Time but sent to a lab in Central Time).
- E.** Leverage community tools and scripts.
- F.** Create sample files for keyword searching to ensure the tools are properly showing results.
- G.** Work closely with investigators on the case to help develop timelines and filters.
- H.** Take your time and research - always ask for help, when needed. Avoid reinventing the wheel without at least being aware existing research has already been done.
- I.** Make sure you understand all potential application data sources and data formats, so you can extract and analyze data unsupported by your toolset. Resources like SANS posters may be helpful:
 - i. [iOS Third-Party Apps Forensics Reference Guide Poster](#)
 - ii. [FOR585 Poster](#)
 - iii. [The Ultimate List of SANS Cheat Sheets](#)

STEP 4

VALIDATION:

(TYPES: VISUAL, CROSS-TOOL,
CALL DETAIL RECORDS, CCTV,
CARVING, REPLICATION)

- A.** Follow the source file for the artifact.
 - i.** The source should be identified and reported if the artifact is important to your investigation.
 - ii.** The source file should be followed and verified for critical evidence.
 - iii.** The source should be provided for future validation/verification purposes.
 - iv.** On encrypted devices, tracing the data to its source hex data, is not trivial. Be prepared to answer questions on why decoded data can not be viewed in hex viewer in the raw data dump. The same might apply on translation layers as well.
- B.** Examine databases, plists and relevant files in their native format or in a file viewer. This should be done after an extraction has been obtained.
- C.** Validate timestamps - are the timestamps shown in the device local time or UTC? Cross check for daylight saving time, time zone changes, time sync, etc.
 - i.** Know where the timestamp comes from (handset vs mobile network).
 - ii.** Time zones can be tricky. Make sure you do not assume the user stayed in one location.
 - iii.** Make sure your tool is extracting relevant timestamps. Verify on the device, if necessary.
- D.** Don't fear Hex and know how to keyword search in Hex. If you are not familiar with looking at raw data with Hex viewers, find training that will further your understanding in this area. This applies to other structures found on mobile devices including SQLite databases, plists, Realm and Level databases, Protobuf and others you may encounter on the device.
- E.** Reach out for support and to get your questions answered (there is no stupid question as the field is wide and changing rapidly). Be sure to use tool vendors support for any product-specific questions you have.
- F.** Reach out for community support.
- G.** Create test data to replicate your findings when the data may cause confusion. Even more important when cross time zone data exists, you are reporting on/researching a non-supported application or when you have found "the smoking gun" and want to be sure to corroborate using all available sources of information.
- H.** Take ample notes pertaining to validation steps taken.
- I.** Retain all research and documentation created should it be required to be provided or referred to at a later stage by a third party.
- J.** Ensure understanding of recovered data. Not all recovered data is user deleted. A great reference for this is: [Standardization of File Recovery Classification and Authentication](#)

STEP 5

REPORTING/SHARING YOUR FINDINGS

- A.** Highlight evidence relevant to the investigation.
- B.** Explain your findings - know and understand what you are reporting.
- C.** Consider data privacy concerns and subsets reports when passed to third parties.
- D.** Provide opinions only when required or legally permitted, if appropriate. And annotate or appropriately mark said comments as opinions.
- E.** Make sure you validate what you report.
 - i.** Even a quick validation works.
 - ii.** If possible, have a colleague review the narrative report as a sanity check.
- F.** Take and keep notes to be prepared for testifying in court sometimes years after your investigation.
- G.** Set the expectations for your report.
- H.** eDiscovery clients may require specific output for their reports.
- I.** Where possible, share your findings within your organization or the DFIR community via a blog or whitepaper. If a blog, consider submitting for peer review via DFIR Review: Publications · [DFIR Review - PubPub](#).

STEP 6 EDUCATION

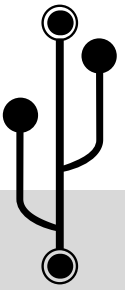
A. DFIR is a fast-moving field and what we practiced yesterday may differ from today (powering devices down and removing battery, removing UICC (SIM) cards vs keeping devices in a powered-on state. We need to adapt.).

B. Stay as current as possible.

- i. Take Training - Vendor training, Vendor-neutral training, self-training, in person or online/on-demand.
- ii. Be familiar with all relevant case law in your jurisdiction and know when you are in 'setting new precedent' territory.
- iii. Create a list of active researchers and follow them.
- iv. If possible, share your own research with the community. If you have faced this issue/question, there is a good chance others will or already have.
- v. Participate in capture the flag (CTF) challenges where test data is provided to enhance your skills in the form of a game/challenge.
- vi. Ask the DFIR community for help.

- 1. Join the DFIR Discord - <https://discord.gg/vQMx5qnb>
- 2. Join community shows like Cached Up (Magnet), Life Has No Ctrl+Alt+Del (Cellebrite) and Forensic Happy Hour (Oxygen).
- 3. Every contribution is valuable: very wide field, fast pace of evolution. Everyone can have its hour of glory (true even for tools...).
- 4. The MDFA group - <https://groups.google.com/forum/#!forum/mobile-device-forensics-and-analysis>
- 5. The SANS FOR585 Alumni group - must be a previous or current student to join.
- 6. Join Vendor community and website groups.
 - i. Reach out to the vendor tech support.
 - ii. Develop scripting and query language skills.
 - iii. Join professional bodies relevant to your discipline.

CONCLUSION



All investigations differ, however the concepts behind proper smartphone handling, extraction, examination, and reporting stand. Some investigations may only require a few steps be taken. For example, if a suspect is in custody and a phone is simply scanned and a quick report is created to see recent communications, steps 3 and 4 would not be required. For a major crimes investigation where the truth may exist on the device or in cloud data, all steps are recommended. Step six is integral - you must know your trade. Smartphone forensics is ever changing and requires testing, validation and training. It is a field that requires us to adapt and adjust to methods and tools that are rapidly changing. DFIR is a mixture of science and art and we are the professionals required to paint the picture.

While everyone may approach investigations in a different manner, these six steps, written by experts in the field are designed to keep you on track. Our hope is that you take this guidance and apply it to your everyday practice. A brief document like this can never provide a complete picture, but it should help you accelerate your journey to professionalism. And if you learned anything from us, you know it's "trust, but verify."

Additional Resources

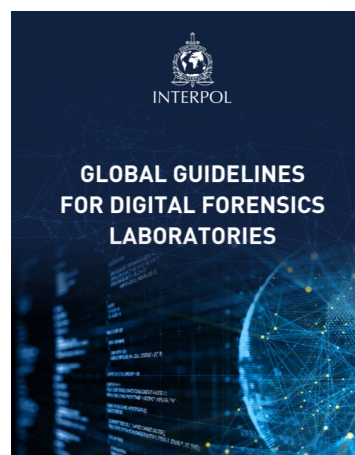
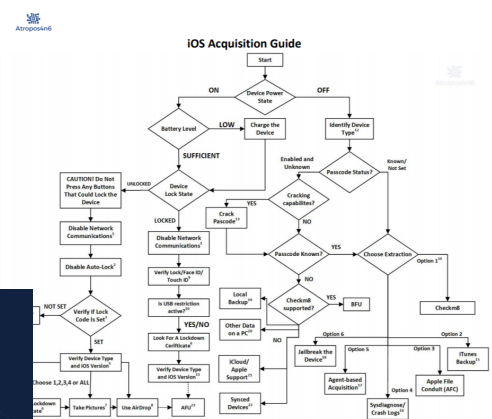
[iOS Acquisition flow chart](#)

[Best practices for mobile device acquisition](#)

[Mobile forensic best practices](#)

[Global Guidelines](#)

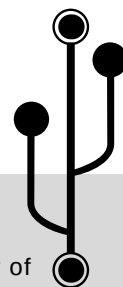
[From Mobile Phones to Court](#)



From mobile phones to court –
A complete FORnsic investigation chain targeting
MOBILE devices
(FORMOBILE)

D3.1 Report on existing practices and
standards

MEET THE AUTHORS



Heather Mahalik: Senior Director of Digital Intelligence, Cellebrite and DFIR Curriculum Lead/Senior Instructor/Author, SANS Institute. Over 19 years experience supporting LE, Government, and DFIR, and co-author of Practical Mobile Forensics.

John Bair: Senior Consultant for an eDiscovery firm in Seattle where he conducts forensic services and expert testimony. Prior to that, John spent 30 years in law enforcement, where his last 13 years were devoted to mobile forensic investigations related to violent crimes.

Alexis Brignoni: FBI Special Agent. Certified Computer Analysis Response Team examiner. Open-source digital forensics tool developer.

Stephen Coates: Detective Constable - Police Officer. Digital Forensic Examiner and Digital Forensics Instructor within Law Enforcement since 2005, specializing in mobile device forensics.

Mike Dickinson: Chief Business Development Officer, MSAB, and former law enforcement.

Mattia Epifani: Digital Forensics Analyst and CEO at Reality Net; SANS Institute Certified Instructor; Researcher at the Italian National Council of Research; Contract Professor at the University of Genoa.

Jessica Hyde: Director, Forensics at Magnet Forensics and Adjunct Professor at George Mason University.

Vladimir Katalov: Executive VP of ElcomSoft, a Moscow-based company. Vladimir drives R&D on mobile and cloud forensics.

Scott Koenig: State Law Enforcement Officer and Digital Forensic Examiner specializing in mobile device forensics.

Paul Lorentz: Technical Account Expert / Sr Solutions Engineer - Cellebrite. Former Law Enforcement. DFIR started off as a hobby then turned into a career path.

Christophe Poirier: Cybersecurity expert in the energy sector, Sworn Forensic Examiner since 2017.

Lee Reiber: Chief Operations Officer, Oxygen Forensics, Inc; Author, Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation; Over 25 years in law enforcement and support of law enforcement DFIR.

Martin Westman: Digital Forensics Product Specialist, MSAB and Digital Forensics Instructor for Law Enforcement since 2004 focusing on Mobile Forensics

Mike Williamson: Technical Forensic Consultant, Magnet Forensics. Former law enforcement. Specializes in digital forensics, software development, and reverse engineering.

Ian Whiffin: Senior Digital Intelligence Expert, Cellebrite. Former Law Enforcement. Specializing in mobile Forensics. DF is my career and hobby.

Oleg Skulkin: Senior Digital Forensic Analyst and Incident Responder, Group-IB and co-author of Practical Mobile Forensics.