cellebrite
delivering mobile expertise

White Paper

# WILL YOUR MOBILE EVIDENCE STAND UP IN COURT?

## 4 Questions to Ask When Evaluating the Forensic Soundness of Mobile Forensics Tools

Just as it is for physical evidence, the admissibility of digital evidence depends on good handling procedures throughout the entire chain of custody. Each link on the chain is responsible for the proper preservation, collection, and documentation practices that demonstrate the evidence is as close as possible to its original state.

When evaluating whether a tool is forensically sound - whether its use can certify that evidence remains unchanged and that the resulting report is a true and accurate representation of what exists on the evidence device - here are four questions to ask[1]:

1. **Is it a tested theory or tool?**
2. **Has it been independently peer reviewed?**
3. **Will its use support both fact and expert witness trial testimony?**
4. **Is it generally accepted within the forensic community?**

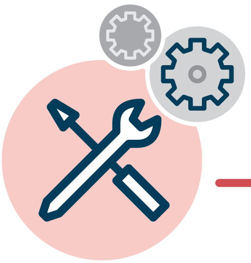
[1] Although no single international standard exists to govern digital forensics practices, courts and forensic practitioners alike have come to rely on a mix of legal precedent and third-party guidelines to govern their practices. This paper relies on two United States legal tests-- Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993) and Frye v. United States. 293 F. 1013 (D.C. Cir 1923) - legal tests in addressing issues that could affect the admissibility of digital mobile device and cloud-based evidence.

# 1 Is it a tested theory or tool?

With the exception of some open source software, mobile and cloud forensics tools are commercial, meaning that their underlying code is proprietary. In the interests of competitive advantage, this code is not open for review. It should be extremely difficult to falsify these tools' results, however, as long as the extraction tool only reads to forensically prepared storage media and not to the evidence device or user account. It should also be possible to validate this type of read-only extraction through a variety of techniques:

1. Manually view results - for instance, the contents of a text message, or an email's date/time stamp - compared to the tool's report. (This will not be possible with deleted data.)
2. Test the tool on two different devices of the same make and model[2]. However, because this risks replicating errors, it is wise to create content on a test device(s) with which to compare evidence extractions - and to use additional validation methods.
3. Compare the tool's results from the evidence device with the results of one or more additional mobile forensic tools.
4. Compare call and text messaging logs with carrier call detail records. Data extracted from cloud-based sources can be compared with app data stored in mobile device memory and/or records obtained from the cloud service provider.
5. For file system and physical mobile device extractions, go into the hexadecimal code and use manual decoding methods to verify results.

In addition to validating that your tool(s) work properly, you should authenticate the evidence, either independently or in collaboration with case investigators, referring to relevant rules of evidence. Hash values, witness statements, and process are explored in great detail in Guidance Software's 2011 EnCase Legal Journal[3].



[2] Examiners should not use their own personal devices. This risks being asked to introduce personal data at trial.

[3] EnCase Legal Journal. Guidance Software. March 29,2011. http://www.guidancesoftware.com/resources/Pages/doclib/Document-Library/EnCase-Legal-Journal.aspx, accessed April 11, 2014

# 2 Has it been independently peer reviewed?

The U.S. National Institute of Standards and Technology (NIST) regularly evaluates digital forensic hardware and software as part of its **Computer Forensic Tool Testing (CFTT) Project[4].** Other government funded bodies, such as the National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE), academic institutions, and private researchers may also conduct independent testing.

NIST's CFTT is ongoing research that evaluates a broad spectrum of digital forensic software and hardware. The CFTT follows a set of standards which NIST itself developed. According to its 2010 and 2012 reports, NIST states:

> ***"Test cases used to test mobile device acquisition tools are defined in Smart Phone Tool Test Assertions and Test Plan Version 1.0. To test a tool, test cases are selected from the Test Plan document based on the features offered by the tool. Not all test cases or test assertions are appropriate for all tools. There is a core set of base cases that are executed for every tool tested. Tool features guide the selection of additional test cases. If a given tool implements a given feature then the test cases linked to that feature are run."***

In general, testing bodies should disclose their test methodology based on test bed and installation procedures. They may or may not reflect how they select test cases. Reports should take care to mention not only how the tool performed overall, but also any errors or anomalies, and what they were if they occurred. Ideally reports should also break out results by logical, file system, or physical extraction for mobile devices, and for cloud-based accounts, whether provider APIs or some other method was used to extract the data.

In your evaluation of these reports, it's important to understand the nature of anomalies and the context of NIST's CFTT reports. First, most mobile forensics tools should be frequently updated to account for new devices, operating systems, apps, etc. as well as to improve performance, introduce new features, and fix bugs.

Second, the CFTT project cannot account for every device make, model, operating system or network protocol that exists; instead, the independent protocol that NIST developed exists to evaluate overall tool performance. Thus, use of the NIST reports should not focus so much on whether the device(s) you are introducing into evidence at trial was also tested by NIST.

[4] Historically cloud forensics tools have not been evaluated as part of the CFTT because none were introduced to market before 2014.

Instead, focus on the reports' broader meaning. Mobile forensics tools should not be found to report content that exists someplace it does not (whether as part of the file system structure or in unallocated space). Mobile forensics tools should also not misreport one type of data as another, for example, a text message as an email.

By contrast, misattribution - reporting a text message as sent when it was actually received, or not reporting part of a message's or image's metadata, even when the content and its location are correct - may have more to do with the device than the forensic tool.

Logical mobile device extractions and cloud-based data extractions, for instance, rely on the device manufacturer's or cloud provider's API to request data. If the API doesn't support the transfer of that particular piece of data, the tool cannot report it. In addition, smartphones' operating systems may make attributions or interpretations (for instance, a cellular tower's location) which the tool does not interpret, but simply reports.

In these cases, focus should be on the fact that the content was found to be on the device and that during a forensically sound extraction, could not have been placed there during a previous extraction or other manipulation. Expert witnesses should be able to help explain how mobile devices store data, how their forensic tools extract and report it, what may result in errors in that process, and again, how they validated their process.

In addition, it should be possible to show that even when a logical extraction misreports data, a physical extraction (when possible for that model) identifies the data's location within the device's memory. At that point, you must use your personal expertise to identify all the data, metadata, and attributes.

Finally, any independent peer-reviewed result reports should be available in the public domain, freely available for download.

# 3 Will the tool's use support both fact and expert witness trial testimony?

As with any digital forensic tool or technique, you should not rely on a single tool to interpret either mobile- or cloud-based data. The tool should make it possible for a trained, experienced examiner to validate what is on the device and where it is located, especially after performing a physical extraction. When the data comes from a cloud-based account and neither the examiner nor the service provider knows where the data physically resides, the artifacts found on the mobile device should help to authenticate the cloud extraction.

Updates should be frequent and readily available, pushed via email alert or from within the tool so that you are encouraged to update (and validate) firmware and/or software regularly.

It's not impossible for a firmware or software update to miss artifacts which a previous version would have extracted or parsed. In these cases, the tool's vendor should make available a robust support system through which you can alert the vendor of any potential problems.

Finally, the tool's report mechanism should make it possible for you to log and document your procedures per your organization's standard operating procedure and digital forensics best practices, thus resulting in a repeatable and reproducible process.

The report should also be easy to explain and, if necessary, demonstrate live or via video in court. This can be valuable in explaining mobile and cloud-based evidence on its own, or the evidence as authenticated with other tools and resources, including other mobile forensics tools, carrier call detail and cloud service provider records, witness interviews, known case details, manual decoding of the hex code, etc.

### Does the tool vendor provide training that adequately prepares the examiner to testify?

While many vendors supply training on the use of their forensic products, whether it prepares examiners to testify in court is another question. Guidelines for evaluating training may start with the first three principles of the Association of Chief Police Officers (ACPO)'s Good Practice Guide for Digital Evidence[5]:

*Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.*

Proper training is developed for every level of investigator, from first responder through examiner and command staff.

*Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*

Arguably this is a common issue in mobile forensics, as the very act of creating a forensic image has the potential to "change" original data, or at the very least that the original data will look different from image to image. Proper training enables the examiner to explain how and why.

*Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*

Good training prepares investigators, again at every level, to document the actions they took and the reasons they took them.

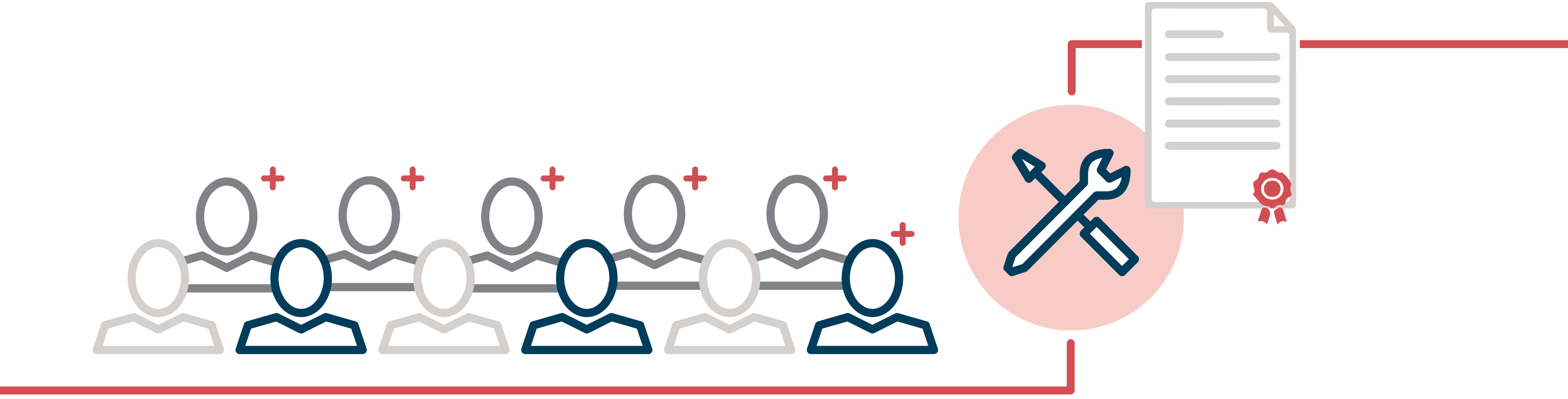
Ideally, a digital forensic tool vendor's training includes certifications that can be referenced on the examiner's curriculum vitae. Certifications should reflect that the examiner was required to go through extensive knowledge and practical testing in order to qualify.

[4] Association of Chief Police Officers of England, Wales & Northern Ireland (ACPO). "Good Practice Guide for Digital Evidence," Version 5 (2011). http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf accessed July 6, 2014

# 4 Is the tool generally accepted within the forensic community?

No independent national or international standard exists for the development of mobile or cloud forensics extraction and analysis tools. However, a mobile or cloud forensics tool's extraction processes should be generally accepted as a valid scientific process owing to validated read-only transfer of data from source device or account to target drive, and mobile physical analysis software's "hex view." Hex view enables you to check the device's underlying data to verify parsed information from a raw "dump" or extraction.

Mobile and cloud forensic hardware and software should be used by a wide variety of investigators in both the public and private sectors worldwide. These investigators may be represented by law enforcement at local, county, state or provincial, and federal levels; corporate legal and security teams; private investigators and consultants; and military field personnel. Securities, customs and border protection, immigration, and various task forces may use the tool to investigate narcotics, human trafficking, fraud, homicide, sexual assault, and numerous other types of cases.



## Navigating a complex and dynamic legal environment

Evaluating mobile and cloud forensics tools needs to take into account the long view, in addition to short-term considerations like cost, ease of use, available training, device support, and so on. The long view anticipates that ultimately, the evidence will end up in court - and examiners need to be able to testify about how it got there. With more courts casting more scrutiny over the search, seizure, and validity of mobile device and cloud-based evidence, be prepared to find the tool that can best bolster your testimony.

# Appendix: Foundational questions

You may find yourself having to answer a wide variety of questions about the evidence you extracted and parsed from mobile devices, and the tool you used to do so. This list is a sampling and is not meant to be exhaustive. Attorneys may come up with their own foundational questions. In addition, some of these should be considered “trick questions” and should be prepared for as such.

- What is this tool?
- Is this tool commonly used by law enforcement to extract data from cell phones (or cloud-based accounts)?
- Are you trained and experienced in using the tool?
- Are you certified to use this tool at the level of extraction you used it for? When did you obtain your certification?
- Are there articles, white papers, or publications about this tool?
- Has the device been accepted as a forensic tool in other courts across the country?
- Is there any one tool that can extract all data from a phone (or account)?
- Is it common for forensic examiners to use multiple tools depending on the phone make/model in question?
- Did you use this tool to extract data in this case?
- Have you validated that the tool is unable to write data to an evidence device (or user account)?
- What type of phone (or cloud-based account) did you examine in this case?
- What type of information did the tool indicate it was capable of extracting from the defendant’s phone (or cloud-based account)?
- Were you able to extract that information using this tool?
- What type of extraction did you perform using this tool?
- Have you validated that the tool extracts the data it says it will extract from this device (or account)?
- Did you also verify that the tool parsed the information correctly? (same number of text messages, contact info, call history)
- During this validation, had the tool changed or deleted any of the data from the cell phone (or account)?
- If the phone is a GSM phone, did you examine the SIM card and the hand set separately?
- If the tool did not extract all the data you extracted from the phone or SIM, what other method did you use to extract that information?

- Was a client used? Was it removed?
- Did you write block the evidence device? How?
- Does this tool hash the evidence?
- Did you capture the RAM?
- Is this conversation from chat, IM, iMessage, or SMS? Is it presented in chronological order?
- Can you explain flash memory, wear leveling, and garbage collection?
- How would an exam conducted today be different from the results in your report from X months ago? Why?

### Cellebrite: Delivering Mobile Expertise

Founded in 1999, Cellebrite is a global company known for its technological breakthroughs in the cellular industry with dedicated operations in the United States, Germany, Singapore, and Brazil. A world leader and authority in mobile data technology, Cellebrite established its mobile forensics division in 2007, introducing a new line of products targeted to the law enforcement sector. Using advanced extraction methods and analysis techniques, Cellebrite's Universal Forensic Extraction Device (UFED) is able to extract and analyze data from thousands of mobile devices, including feature phones, smartphones and GPS devices. Cellebrite's UFED is the tool of choice for thousands of forensic specialists in law enforcement, military, intelligence, security, government and private sector organizations in more than 100 countries.

Cellebrite is a wholly-owned subsidiary of the Sun Corporation, a listed Japanese company (6736/JQ).

To learn more, visit
**www.cellebrite.com**

For more information contact sales