Ensuring Admissibility of Mobile Evidence in Court

By Brendan Morgan

Admissibility of mobile device evidence can be tricky to ensure. Mobile forensics is unlike traditional computer forensics in many ways, and it can be difficult to explain the differences to judges, attorneys, and members of a jury.

For example, it isn't possible to perform a true forensic image of the device's memory. Because the device must be powered on to perform the extraction, mobile forensics processes makes changes to the evidence device. Although the process doesn't change user data, it does alter the information within the device's operating system. Other processes, including the way the mobile device stores data across its flash memory chip, can present additional complications.

The key to good testimony is good process backed up by good documentation. Additionally, building a strong relationship with the forensic examiners you rely upon can make all the difference in the way you communicate with them—and, in turn, the way they communicate with you, judge, and jury—while they are on the stand.

Good Process Starts at the Crime Scene

Preservation, chain of custody, and legal authority can present bigger challenges to law enforcement over other forms of evidence. Mobile devices are so ubiquitous in our everyday lives that many first responders don't think twice about picking one up on the scene and thumbing through its contents or expecting forensic examiners to do the same.

Yet, these practices can get mobile device evidence suppressed. In *State v. Michael Patino* (12-263 [R.I. 2014])[1], first responders' failure to properly secure their evidence resulted in getting all incriminating text messages, and the confession they elicited, thrown out. The state's Supreme Court later readmitted text messages obtained from a consensual search of a witness' device.

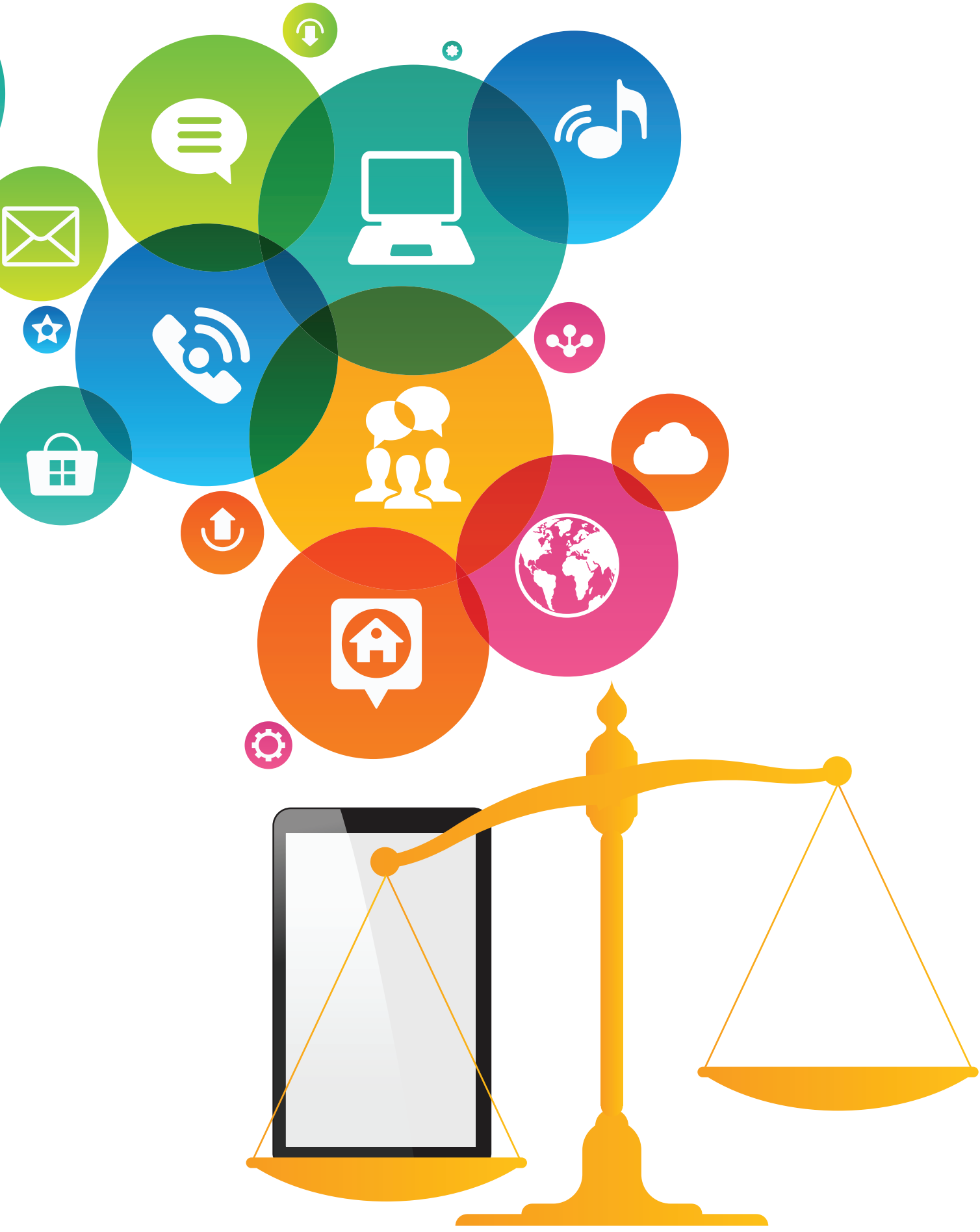
First responders must be trained to preserve, document, and control mobile devices in the manner in which they would any other kind of evidence. Documenting devices' position and condition, the presence of any physical evidence on the devices, and steps taken to preserve the data on the device should all be part of standard procedure. So should a protocol for bagging and tagging the evidence and logging its chain of custody.

On-scene examinations may need to go further than simple preservation, too. Many of the activities that have historically taken place via computer—peer-to-peer file sharing, email, and live streaming video—are now taking place via mobile devices and often occur through third-party applications. Thus, investigators may be faced with the need to collect evidence as part of an on-scene triage or preview process designed to determine which media contain evidence and which are less relevant to an investigation.

The ability not just to preserve but also to extract and view data is important in these situations. First responders should be prepared to articulate what types of content they believe is evidence, and in what time frames they believe the evidence to exist, when seeking a search warrant, conducting a consent search, or searching under exigent circumstances.

Proper Process in the Lab

The inability to understand how to properly use forensic tools and how they function carries a number of risks



for forensic examiners. Among them:

- **Damaging or altering original evidence.** Some of the tools used to extract mobile-device evidence aren't technically forensic. This could result in the destruction of the original evidence.
- **Failure to examine evidence thoroughly.** To be sure, mobile devices often contain gigabytes of data, and most cases involve more than one mobile device. Investigators need to be able to narrow the scope of data they must analyze—but not to the point where they're potentially missing exculpatory data. Rather than only looking for SMS messages, examiners should also look for messages sent and received using messaging apps. Examiners should also narrow their search not just to data types but also to time and date ranges. It's important to analyze the totality and context of communications activity within those time frames and how it relates to other facts of the case.
- **Misinterpreting data.** Mobile devices store data in different ways, and a single image stored multiple times may simply be the result of a data storage process known as "wear leveling"—captured during a forensic extraction before the device was able to clean up the duplicate copies. Misinterpretation of these duplicates could lead to multiple counts of (for example) possession of child pornography where none is deserved.
- **Preparing inaccurate reports of findings.**

Evidence being ruled inadmissible is just one possible outcome of these mistakes. The examiner who makes them also risks losing credibility in the court's eyes and opens himself to potential civil liability.

Admissibility of mobile forensic evidence comes down to the examiner's ability to certify that she used a sound set of analysis protocols. These protocols or methodologies ensure:

- The examiner has validated his/her forensic tools, including each new release or update for those tools. (Note: Regular updates do not mean that a mobile forensics tool is inherently unreliable. As long as each update is validated, and the examiner recognizes any bugs and takes steps to roll back updates that are identified as having bugs, the tool can be looked upon as reliable.)
- The examiner can repeat her own process and can reproduce results using that same process. In other words, the examiner shouldn't plan only to validate his tools, but also his findings. This process can include hand-scrolling techniques, the use of more than one forensic tool, and/or—for smartphones—database verification and analysis.
- The examiner can demonstrate, via the process of hashing, that evidence files are true and accurate copies of the original items seized.
- The examiner stays within the scope of legal search authority. This includes limiting a forensic examination only to the evidence of the crime named in the search warrant and obtaining a new search warrant if any evidence of a different crime is encountered.

Mobile forensics examiners must also be prepared to testify to forensic hardware and software vendors' proprietary methods, in particular their extraction and decoding techniques. While some information is necessarily restricted to protect the vendors' intellectual property, vendors should provide some basic information that indicates their tools' internal processes are forensically sound. Additional information may come from vendor-specific training and networking with peers online and through professional associations.

Helping Forensics Examiners Help You

To maximize the chance of digital evidence being admitted, it is essential to develop positive relationships with the forensic examiners who are preparing the evidence and the documentation. Ideally, form this relationship before a big case. A strong relationship will foster the examiner's ability to offer creative solutions to help build your case.

Be prepared to provide the examiner with information on your needs, including your timeline, strategy, anticipated cross-examination questions, trial prep schedule, and objectives. Ask him to explain his report of findings in layman's terms. If you have a hard time understanding the technical intricacies of mobile-device evidence, chances are judges and juries will too. Help him refine his explanation to the point where it makes sense to you and where you could explain it to a judge.

Have him demonstrate the process of recreating and validating his findings. It should be possible for an examiner to use his own documentation to walk you through his process and explain why he made the choices he made, including what tools he used and how the process led to his conclusions.

Ask the mobile examiner to assist you with the creation of exhibits. Many mobile forensics tools include visual analytics, including the ability to plot Wi-Fi, tower, and GPS location data on maps; view messages and calls in conversation and time-line order; and show frequency of contacts. It may even be possible for examiners to create playback video of some of these analytic tools.

Ask him to help you address possible defense expert theories regarding the evidence and its provenance. Both forensic reports and exhibits must be authenticated to be admissible.

Make sure your examiners are prepared to provide copies of their chain-of-custody documentation, their legal authority for their search of the items they analyzed, testimony as to how their forensic tools function and their methodology in using those tools, and finally, a detailed and defensible report of their findings.

Final Thoughts

When you're relying on digital forensics examiners to make your case, be sure to make them active participants in your pretrial prep meetings. Be sure they have a true understanding of how their mobile forensic tools function and that they can explain it in layman's terms, backing up their explanations with thorough documentation.

Once you put them on the stand, be sure that they can testify not just to their process but also to how they can be sure their process led to results they can authenticate. This includes validation of both tools and findings, as well as peer review.

Mobile forensics can be complicated, and your job is to help judges and juries understand, but this is not a Sisyphean task. Build relationships with examiners early, before you need them, and let this foundation guide you through building your court case. ⊙

Brendan Morgan serves as a senior instructor and developer at Cellebrite USA Inc. Before joining Cellebrite in May 2014, Brendan served as detective/forensics examiner/federal task force officer for the city of Hoover, Alabama, assigned to the U.S. Secret Service Electronic Crimes Task Force and the U.S. Secret Service National Computer Forensics Institute. Brendan also served as an investigator with the State of Alabama Office of Prosecution Services–Alabama Computer Forensic Laboratories, and as a detective sergeant in Alabama, where he performed civil and criminal investigations, including bank fraud, crimes against intellectual property, forgery, health insurance fraud, network intrusion, and more. He has more than 16 years of law enforcement experience.

Endnotes

[1]www.courtlistener.com/opinion/2716863/state-v-michael-patino/

Additional Resources

1. *United States v. Marsh,* No. 13-258, 13-2549, 568 F. App'x 15 (2014 U.S. App. 2nd Cir.); 2014 U.S. App. 2nd Cir. LEXIS 10054 (U.S. App 2nd Cir. May 30, 2014). Please refer to Federal Rules Of Appellate Procedure Rule 32.1 governing the citation to unpublished opinions: U.S. Supreme Court certiorari denied by *Marsh v. United States,* 2014 U.S. LEXIS 6674 (U.S., Oct. 6, 2014); U.S. Supreme Court certiorari denied by *Anderson v. United States*, 2014 U.S. LEXIS 6917 (U.S., Oct. 14, 2014).

OVERVIEW: In convictions of a conspiracy that did not involve more than 500 grams of powder cocaine or crack under 21 U.S.C.S. § 846, the jury charge was not defective because it clearly set forth the elements of conspiracy, and it fairly and accurately encompassed the theory of the defense.

2. *United States v. Flores-Lopez,* No. 10-3803, 670 F.3d 803, (2012 U.S. App. 7th Cir.); 2012 U.S. App. 7th Cir. LEXIS 4078; 55 Comm. reg. (P & F) 701 (U.S. App. 7th Cir. Argued Jan. 25, 2012, Decided Feb. 29, 2012).

OVERVIEW: Warrantless search of defendant's cell phone incident to his arrest did not violate the Fourth Amendment because the search, limited to finding the phone number for the cell phone, was minimally invasive.

3. *United States v. Martinez,* No. 13cr3560-wqh, 2014 S.D. Cal. App. LEXIS 99705, (S.D. Cal. App. Decided July 22, 2014).

4. *Total Safety U.S., Inc. v. Rowland,* Civil Action No. 13-6109 § B(4), 2014 E.D. La. LEXIS 59236, (E.D. La. Decided April 29, 2014).

5. *United States v. Halgat,* 2:13-cr-241-apg-vcf, 2014 D.C. Nev. LEXIS 55778, (D.C. Nev. Decided April 22, 2014).

6. *United States v. Zaavedra,* No. 12-cr-156-gkf, 2013 N.D. Okla. LEXIS 174493, (N.D. Okla. Decided Dec. 9, 2013).

7. *United States v. Mayo,* No. 2:13-cr-48, 2013 D.C. Vt. LEXIS 158866, (D.C. Vt. Decided Nov. 6, 2013).

OVERVIEW: Warrantless search of vehicle passenger's cell phones was unreasonable under Fourth Amendment because cell phones properly seized pursuant to search-incident-to-arrest exception or automobile exception could not be searched without warrant, but suppression was not warranted because good faith exception applied.

8. *United States v. Dixon,* Criminal Action No. 1:12-cr-205-1-ode-ecs, 984 F. Supp. 2d 1347 (N.D. Ga. 2013); 2013 N.D. Ga. LEXIS 163674, (N.D. Ga. Decided Aug. 29, 2013. Adopted/Motion granted Nov. 15, 2013).

9. *United States v. Dixon,* Criminal Action No. 1:12-cr-205-ode-ecs, 2013 N.D. Ga. LEXIS 125385, (N.D. Ga. Decided July 29, 2013); magistrate's recommendation at *United States v. Floyd,* 2013 U.S. Dist. LEXIS 136966 (N.D. Ga., Aug. 27, 2013); magistrate's recommendation at *United States v. Dixon,* 2013 N.D. Ga. LEXIS 163674 (N.D. Ga., Aug. 29, 2013); motion denied by *United States v. Dixon,* 2013 N.D. Ga. LEXIS 125169 (N.D. Ga., Sept. 3, 2013); magistrate's recommendation at *United States v. Wilson,* 2013 N.D. Ga. LEXIS 155712 (N.D. Ga., Sept. 20, 2013).

10. *United States v. Davis,* No. 11-60285-cr-Rosenbaum, Fed. R. Evid. Serv. (Callaghan) 574 (S.D. Fla. 2013); S.D. Fla. LEXIS 70371 (S.D. Fla. May 17, 2013).

OVERVIEW: Defendants' motion to reconsider the denial of defendants' motion in limine was denied because the witness was qualified where the witness had regularly analyzed cellular telephone records, and, for the past three years, the witness had done nothing but analyze cellular-telephone records in support of criminal investigations.