ARTICLE:

Are mobile device examinations practiced like 'forensics'?

By **Gary Kessler, Ph.D.**

Mobile device forensics is sometimes disparaged as not really being 'forensics.' This paper discusses the relationship between digital forensics and other forensic sciences, and the relationship of mobile device forensics to the broader field of digital forensics. It specifically addresses the question of whether mobile device forensics processes – and practices – rise to the level of suitable forensics quality.

Introduction

Mobile device forensics is a subset of the broader category of digital forensics which is, itself, just one of the forensic sciences. While all of the forensic sciences have essentially the same steps in the investigative process, digital forensics has some significant differences from traditional forensic sciences. Furthermore, mobile devices are forensically examined in a different way than 'traditional' computers, which often leads to the misconception that mobile device examinations are somewhat less forensically sound and thorough than examinations of computers. And yet, that observation is not totally baseless.

This paper will examine the question of where mobile device forensics stands as a forensic practice. Section 1 will present working definitions of forensics and science. Section 2 will define digital forensics and set a context for comparing and contrasting digital forensics with the more traditional forensic sciences. Section 3 will define mobile device forensics as a subset of digital forensics, distinguishing the science and practice of mobile device forensics from that of computer forensics. Section 4 will offer some conclusions.

Defining forensics and science

Forensics is a discipline 'relating to or dealing with the application of scientific knowledge to legal problems.'[1] Popular media, from the US television show *Quincy, M.E.* in the 1970s to today's *CSI* and *NCIS*, plus countless other TV shows, movies, books, and newspaper articles, have made even the casual observer recognize the importance of blood, fingerprints, deoxyribonucleic acid (DNA), tool markings, tire tracks, and other latent evidence found at a crime scene to solving crime.

One of the foundations of the forensic sciences is Locard's Exchange Principle, first articulated by Edmond Locard, the founder of the first police forensics laboratory in 1910. The exchange principle says, in essence, that every contact leaves a trace.[2] Put another way – if a person is hit on the head with a branch of a tree, something from the branch is left on the head and something from the head is left on the branch. All of the forensic sciences assume that such contacts and exchanges take place during the commission of a crime. Our job, as forensic scientists, is to find those latent traces, interpret the contacts, and put them together so as to make sense of what actions caused them in the first place.

One common model of the forensics process includes the following six phases:[3]

> *Identification:* Surveying a crime scene to determine potential sources of evidence that might have a nexus to the crime.
>
> *Preservation:* Maintaining the state of potentially probative items to prevent changes, ensuring evidentiary integrity.
>
> *Collection:* Assembling potential evidence in a manner so that the items can be forensically examined on-site (as necessary) or transported to a laboratory facility.

[1] Merriam-Webster, 'Forensic', available at http://www.merriam-webster.com/dictionary/forensic .

[2] Forensic Handbook, available at http://www.forensichandbook.com/locards-exchange-principle/ .

[3] Eoghan Casey and Bradley Schatz, 'Conducting Digital Investigations', in Eoghan Casey *Digital Evidence and Computer Crime* (3rd ed., Amsterdam: Elsevier, 2011); Gary Palmer, A Road Map for Digital Forensic Research Report From the First Digital Forensic Research Workshop (DTR - T001-01 FINAL, DFRWS TECHNICAL REPORT (DFRWS) August 7-8, 2001 Utica, New York), November 6th, 2001 – Final Approved For Public Release, available at http://www.dfrws.org/2001/dfrws-rm-final.pdf .

Examination: Testing each evidentiary item to extract probative information, making it available for analysis. This phase is guided by the legal context of the seizure and search of the items.

Analysis: Application of the scientific method, systematic processes, and critical thinking to look at the totality of the evidentiary information to answer the fundamental investigative questions: who, what, where, when, why, and how. This phase includes the analysis of both incriminating and exculpatory evidence.

Reporting: Document the entire forensics process, particularly explaining how the analysis leads to the conclusions about the crime. The type of investigation – i.e., corporate, civil, or criminal – provides the context for this phase.

The definition of forensics includes reference to scientific knowledge. Science is a systematic structure for understanding a body of knowledge.[4] This knowledge is acquired through the use of the scientific method, the process of hypothesis, experimentation, and testing in order to gain knowledge.[5]

Digital forensics

Introduced in 2008, Digital & Multimedia Sciences (DMS) is the newest section identified by the American Association of Forensic Sciences (AAFS). The DMS section includes forensic practitioners who analyse traditional computer systems (e.g., laptops, desktops, and servers), as well as network traffic, mobile devices, and digital media (such as pictures and other images, audio recordings, and videos).[6]

Locard's Exchange Principle applies in cyberspace as well as it does in physical space. Indeed, it applies so well that there are often hundreds or thousands of digital contacts that examiners may not be able to detect, such as with network servers and data in log files.

Digital forensics employs the scientific method to the process of examinations and analysis, although it is not an application of science to seek greater truths. The scientific method is used in order to find information, provide a context in which to understand the information, and determine the probative value of the information. Digital forensics uses science to find patterns that are supported by digital evidence, consistent with Fred Cohen's Fundamental Theorem of Digital Forensic Examination: 'What is inconsistent is not true.'[7] Indeed, science is the basis of the creation of the tools used for digital forensics examinations.

Digital forensics generally follows the same six-step forensic process as described above. The Association of Chiefs of Police Officers (ACPO) has put forward four principles that are particularly relevant to digital evidence:[8]

1. No action should be taken that will change data that might be subsequently used as evidence.
2. When it is necessary to access original data, the person doing so should be competent and able to explain the necessity and implications of those actions.
3. An audit trail of the processes used in a digital examination must be maintained so that a third-party could use those same processes and achieve the same results.
4. The person in charge of the investigation has responsibility to ensure that all aspects of the examination adhere to the appropriate laws and these principles.

At the practice level, there are some fundamental differences between digital forensics and forensics associated with the more traditional life and physical sciences. Firstly, the traditional forensic examiner compares latent evidence found at a crime scene to known samples. For example, a technician finds fingerprints and compares them to a database of fingerprints, looking for a match. The same is true for DNA, blood, bullets, tool marks, tire tracks, shoe prints, hair, typewriters, handwriting, and other forms of physical evidence. Even forensic pathologists

[4] Merriam-Webster, 'Science', available at http://www.merriam-webster.com/dictionary/science.
[5] Merriam-Webster, 'Scientific method', available at http://www.merriam-webster.com/dictionary/scientific%20method.
[6] Eoghan Casey and Bradley Schatz, 'Conducting Digital Investigations', in Eoghan Casey *Digital Evidence and Computer Crime* (3rd ed., Amsterdam: Elsevier, 2011).
[7] Fred Cohen, *Digital Forensic Evidence Examination* (4th ed., Livermore, California: Fred Cohen & Associates, 2012), 26, available in electronic format at http://www.fredcohen.net/Books/2013-DFE-Examination.pdf.
[8] ACPO, *Good Practice Guide for Digital Evidence* (v5, 2012), available at http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

compare the signs found in a corpse to known syndromes.

Digital forensic examiners (DFEs, also known as digital evidence specialists[9]), however, do not conduct the same type of comparison. DFEs, instead, look at the information found on a computer, cell phone, or other digital device, attempt to reconstruct the device's activities, and then try to determine whose fingers were on the keyboard at the time of various activities. Indeed, the analysis is based upon knowledge of what action would cause a certain trace. This is where science comes into play; a DFE is, in essence, fabricating an experiment to support or refute a theory of what activities occurred. If the experiment contradicts the theory, then the theory is wrong; if the experiment supports the theory, however, it only means that the theory is correct insofar as the current set of facts represents the truth.[10] It is because our knowledge of the facts is not perfect that two experts can (correctly) disagree on the interpretation of certain digital evidence.

Secondly, while the tools of the traditional forensic scientist change and, generally, get better over time, the evidence itself is not in constant flux. Human blood and DNA, for example, have not changed very much in millions of years, although the tools and methods with which to analyse them keep improving.

Conversely, both the tools and evidentiary sources in digital forensics are constantly changing. The tools of digital forensics are software and hardware; these are constantly being upgraded with new drivers and software releases. The operating system platforms of the tools – Linux, Mac OS, and Windows – are also frequently updated. In addition, the targets of the examination are also changing, with application software and operating systems frequently updated. In that regard, digital forensic examiners are dealing with two moving targets.

Finally, the six-step forensic process does not specifically account for another major difference with digital forensics, namely the necessity, at times, to do a *live* analysis of digital devices. There are several circumstances under which digital evidentiary sources cannot be safely shut down and transported to the laboratory for analysis. For example, there is often valuable information in a computer's random access memory (RAM) – such as usernames, passwords, or pass phrases – that will be lost when the system is powered down, so RAM is imaged while the computer is still powered on; of course, the very act of imaging RAM means that imaging software needs to be loaded into RAM, thus changing its contents. Similarly, what is called *live imaging* needs to be performed on mobile devices, encrypted disks (assuming that they are mounted and accessible), when capturing network traffic, for cloud-based investigations, and when examining Internet-based sites. Principle 2 of the ACPO Guide applies to these circumstances; i.e., the examiner obtaining access to original data must be competent to explain the necessity and implications of doing so.

Mobile device forensics

Mobile device forensics is a subset of digital forensics and refers to the preservation, data acquisition, examination, and analysis of mobile digital devices such as cell phones, smartphones, music players, tablets, Global Positioning Systems (GPS), and other types of mobile devices.[11] The author long ago predicted that mobile device forensics would yield more probative information per byte examined than computer forensics; since the advent of smartphones in 2009, this prediction has shown itself to be true – smartphones are incredibly special devices filled with intimate details of a person's life and activities, tracking people more finely than most users appreciate.

The evolution of cell phones, in particular, has been particularly astounding. Early adopters of cell phones (1993) were fortunate to get dial tone; cell phones were voice-only devices, had no 'apps,' and essentially no accessible RAM with user information. Ten years later saw cell phones that started to have many apps to support the communications function; call history, an address book, the Short Message Service (SMS), and the display of images and videos were common features, and these devices had on the order of 100 MB of RAM for examination. Early smartphones started to appear with computer-like applications and cameras. By 2013, 'cell phones' had evolved into

[9] See Stephen Mason and Andrew Sheldon, 'Proof: the investigation, collection and examination of digital evidence' in Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).

[10] Fred Cohen, *Digital Forensic Evidence Examination* (4th ed., Livermore, California: Fred Cohen & Associates, 2012), 26, available in electronic format at http://www.fredcohen.net/Books/2013-DFE-Examination.pdf .

[11] Eoghan Casey and Bradley Schatz, 'Conducting Digital Investigations', in Eoghan Casey *Digital Evidence and Computer Crime* (3rd ed., Amsterdam: Elsevier, 2011).

smartphones, or 'portable internet terminals'. In addition to multi-core processors, RAM sizes on the order of 64 GB, and traditional voice features, these devices have cameras, audio and video recorders, a plethora of sensors, web browsers, myriad personal apps, office productivity software, games, GPS, social media, maps, navigation, and tens of thousands of other programs.

Mobile device forensics compared to computer forensics

While the mobile device and computer forensics processes are the same, the actual procedures are very different.[12] One of the most fundamental differences is the way is which data is forensically acquired from the systems. Historically, once a computer is powered down upon seizure, it is not restarted. Data is retrieved from a computer's hard drive via a process called imaging, whereby the drive is connected to a forensic workstation via a cable and write-blocking mechanism. The imaging process makes a forensically correct copy of every sector on the drive, including unallocated space (i.e., ostensibly 'deleted' data).[13]

While mobile devices are generally powered down (and removed from any WiFi, data, or other communications networks) upon seizure, data acquisition requires the device be powered on. Indeed, data acquisition might retrieve only existing files on the device or every byte in RAM; the amount of data recovered is largely dependent upon the device manufacturer and model, operating system version, features and options selected by the carrier, and capability of the acquisition tools.

A second fundamental difference is that once a computer is shut down, its state is preserved because it is never turned back on. Mobile devices must be powered on in order to recover the data, in turn altering the state of the device. This is actually analogous to imaging the RAM on a running computer; once the RAM copy is made, the computer is shut down and the contents of the hard drive do not subsequently change, but the state of the running computer was changed when the RAM image was created.

A third difference between computers and mobile devices relates to the sheer volume of devices. Today's computers are limited to essentially three different operating systems (OSs), namely Linux/Unix, Mac OS X, and Windows (including the various versions that are in common use). Mobile devices, however, have four major operating systems – Android, Blackberry, iOS, and Windows (and their variants) – plus a handful of proprietary operating systems. In the computer world, Mac OS X and Windows computers are all essentially standardized, while Linux and Unix come in myriad variations; similarly, Blackberry, iOS, and Windows mobile devices are standardized while Android device features can vary widely by manufacturer. Indeed, the function of a telephone's hardware might vary by manufacturer and service provider; Tracfone, for example, generally disables the data transfer capability of the Universal Serial Bus (USB) port of its devices, using it only for power and charging.

The tools used to examine and analyse mobile devices also function differently than computer forensics tools. Most mobile device tools both acquire the data and parse the results. While the raw binary file might be imported into another analysis tool, most mobile device tools perform both functions. In the computer forensics environment, imaging and analysis are two separate and distinct operations.

Indeed, data acquisition of computers is a very different process than acquiring mobile telephone data. Because computer hard drives are largely standardized, the imaging process is well understood, with many standard hardware and software tools. Acquiring a cell phone requires the proper cable and a method that allows kernel access to the device's software and hardware. Access to the mobile device's RAM often requires more privileged access to the device than is needed for the imaging of a hard drive. Indeed, DFEs often 'hack' their way into an Android or iOS system by requiring Developer or Safe mode access, employing boot loaders, 'jailbreaking' the device, uploading client software to the device, obtaining direct access to the application program interface (API) commands, or other methods are less than straightforward and might make unknown changes to the device.

[12] Gary C. Kessler and Richard P. Mislan, 'Cellular Phones', in J.A. Siegel & P.J. Saukko, eds, *Encyclopedia of Forensic Sciences* (2nd ed., Waltham: Academic Press, 2013), 298-302; Richard P. Mislan, Eoghan Casey and Gary C. Kessler, 'The Growing Need for On-Scene Triage of Mobile Devices', *Digital Investigation*, 6 (2010), 3-4, 112-124.

[13] For a high-level overview of how computers and computer-like devices are structured, see George R. S. Weir and Stephen Mason, 'The sources of digital evidence' (Chapter 1) in Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).

Mobile device examinations as forensics

Mobile device forensics is practiced very differently from the classic computer forensics. Given that mobile devices are usually not imaged as thoroughly as a hard drive, and because mobile devices are powered 'on' instead of 'off 'during the data acquisition phase, the forensic quality of the analysis of a mobile device could fairly be questioned.

A review of the definition of forensics, however, makes it clear that the current state of the art of mobile device forensics meets the spirit and meaning of the term. The U.S. National Institute of Standards and Technology (NIST) has been involved in testing digital forensics tools since the early 2000s.[14] Among the essential requirements of these tools is that the results of an examination be both repeatable and reproducible; i.e., when following the same procedures, results found in one examination should be able to be found in a second examination and results found by one examiner in one laboratory should be able to be found by another examiner in another laboratory.[15] This is wholly consistent with ACPO Principle 3.

NIST has carefully crafted out methodologies and procedures to test computer and mobile device forensics tools to ensure that they meet these and other quality standards.[16] Several NIST publications demonstrate the efficacy of mobile device forensics methods, processes, and tools.[17] Mobile device forensics tools and techniques have been shown to meet the test of providing quality evidence from which conclusions can be drawn. Of course, as with any scientific or technical evidence, and as noted above, two experts might draw different conclusions from the same data. Yet, even with these guidelines for tool testing, it is difficult for the tools to keep up with the capability of the devices. New mobile devices are introduced at a faster pace than the testing can keep up with, and the capabilities of even one particular device might vary from carrier to carrier. The datasets and images used for tool testing, then, quickly become obsolete.

The problem of keeping the tools current is exacerbated by the fact that there are tens of thousands of apps for smartphones, but even the best tools routinely can only parse several hundred of the more popular ones.

The practice of mobile device forensics

Why, then, raise the question of whether mobile device forensics is *forensics*? In the author's experience and observation, the practice of mobile device forensics does not uniformly rise to the level of the available science. In part, this is due to the fact that there is no widespread appreciation for the fact that a mobile device – particularly a smartphone – is not a telephone, in the traditional meaning, but a portable computer in every sense of the word.[18] Indeed, many of the major mobile device forensics tools are deceivingly simple to use; i.e., by combining data acquisition and parsing, it appears that the tools seize everything from the device and interpret the contents with a simple cable connection and the push of a button.

This results in several problems with the practice of mobile device forensics. First, while no agency would ever consider giving an untrained person a computer forensics tool and allow him or her to examine a hard drive, many agencies give a relatively untrained person access to a mobile device forensics tool and tell him or her to examine a smartphone.

Second, the perceived simplicity of the tools makes some undertrained examiners overly dependent upon what the tools can do, making it difficult to apply critical thinking to the results. Mobile device forensic tools can commonly interpret many of the common data structures, such as the contact list, SMS messages, GPS points, call history, images, videos, audio recordings, e-mail, and browser history, but provide, at best, raw databases for other applications. Often, the examiner takes at face value whatever the tool reports, sometimes to the extreme of believing

[14] Barbara Guttman, James R. Lyle and Richard Ayers, 'Ten Years of Computer Forensic Tool Testing', 8 *Digital Evidence and Electronic Signature Law Review* (2011), 139-147.
[15] *General Test Methodology for Computer Forensic Tools, Version 1.9* (Gaithersburg, Maryland: National Institute of Standards and Technology, 2001), available at http://www.cftt.nist.gov/Test%20Methodology%207.doc.
[16] 'CFTT Methodology Overview Web page', available at http://www.cftt.nist.gov/Methodology_Overview.htm.
[17] Rick Ayers, Sam Bothers and Wayne Jansen, *Guidelines on Mobile Device Forensics*, Special Publication 800-101, Revision 1 (Gaithersburg, Maryland: National Institute of Standards and Technology, 2014), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications /NIST.SP.800-101r1.pdf ; James Lyle (ed.), *Computer Forensics Tool Testing Handbook* (Gaithersburg, Maryland: National Institute of Standards and Technology, 2012), available at http://www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf .
[18] Gary C. Kessler and Richard P. Mislan, 'Cellular Phones', in J.A. Siegel & P.J. Saukko, eds, *Encyclopedia of Forensic Sciences* (2nd ed., Waltham: Academic Press, 2013), 298-302; Richard P. Mislan, Eoghan Casey and Gary C. Kessler, 'The Growing Need for On-Scene Triage of Mobile Devices', *Digital Investigation*, 6 (2010), 3-4, 112-124.

that if the tool does not find something, then that data is either not present or not accessible. This problem is exacerbated if the examiner only knows how to use a single tool or method.

Third, there are many ways to acquire information from a mobile device, such as manual examination, logical acquisition, file system acquisition, physical acquisition, use of Joint Test Action Group (JTAG) testing points, and chip-off forensics. Only a trained DFE can determine which method should be employed to best and most accurately acquire data from a given device. Indeed, multiple acquisitions might be required since one method might acquire some data off a telephone and another method acquire additional data. It is essential that the examiner understands how the different methods work and why one method might be more fruitful than another; this is particularly true when one of the hacking methods described earlier is employed.

Furthermore, acquisition is only part of the issue. After acquiring data from RAM, the zeroes and ones must be parsed. It is well known in the industry that newer software versions are often able to acquire data from telephones that were previously inaccessible and/or to translate and interpret more data than was previously possible, even on older telephones. In the future, a question might be whether we need to reanalyse all of our telephones once the next version of analysis software becomes available.

Finally, the amount of data available on mobile devices and the quantity of mobile devices being examined often leaves little time for the examiner to perform a thorough analysis. It is frequently the case today that a mobile device examiner will do nothing more than acquire the data, parse whatever structures can be interpreted, and then deliver a report (often several hundred pages in length) to an investigator to review in order to find useful information. In these cases, the investigator has no knowledge of what kind of information might be missing from the report and the examiner or analyst has been relegated to the role of technician. And everyone in this scenario has violated at least ACPO Principle 2, because no one knows exactly how the data was acquired and what, if any, changes were made to the device. Some judges are beginning to recognize when an 'examiner' may not be an expert; consider the example of *Bevan v The State of Western Australia*,[19] where all three judges agreed that the constable using extraction tools to obtain data from mobile telephones did not have sufficient knowledge or expertise of the tool to say for certain that text messages were reliably acquired from a mobile telephone. After a second trial, this same point was appealed again. This time, only one member of the court, Buss J, thought the constable did not have sufficient knowledge or experience.[20]

Conclusions

The science behind mobile device forensics and the engineering behind the acquisition and analysis tools are good. The processes and procedures behind the forensics are well established. But too many people involved in the mobile device examinations are untrained or undertrained, from first-responders with inadequate knowledge in how to seize, preserve, and transport mobile devices to examiners who are untrained in the science of mobile devices (i.e., computer science, operating systems, and file systems) to investigators and lawyers who do not truly understand the subtleties of computers in order to interpret the results of a forensics report. This also includes all levels of people involved in the forensics chain who do not appreciate the difference between data acquisition and data parsing/interpretation. The volume of devices and the quantity of information on the devices is so vast that many mobile device forensics laboratories only extract data rather than analyse it.

In some laboratories, mobile device forensics does not rise to the same quality level as computer forensics. But it is the practice of the mobile forensics that is suffering rather than the underlying science; whereas the traditional computer forensic examiners routinely perform the data extraction, examination, and analysis function, mobile device forensics frequently only encompasses data extraction, leaving examination and analysis up to investigators. The risk of this practice is that an understanding of the underlying technical information may be lost and the knowledge and experience required to offer an expert opinion at trial is lost because the 'expert' is not performing the analysis. It is already the case where two experts can reasonably disagree with the digital evidence, so removing an expert from the cycle leaves a larger potential for a miscarriage of justice such as

[19] [2010] WASCA 101.
[20] *Bevan v The State of Western Australia* [2012] WASCA 153.

already has been seen in numerous cases with computer evidence (e.g., *Connecticut v. Amero*[21]).

Like the other forensics sciences, digital forensics – including mobile device forensics – must be practiced by professionals. The acceleration of change in technology mandates that all aspects of digital forensics be performed by well-educated, well-trained, and knowledgeable practitioners. The justice system cannot rely on results that are performed by anyone not so qualified.

Acknowledgement

This paper, in large part, is based upon a presentation titled 'Is Mobile Device Forensics Really 'Forensics'?' and subsequent discussion at the NIST Mobile Forensics Workshop, Gaithersburg, Maryland, USA, June 2014.

Professor Gary C. Kessler, PhD is chair of the Security Studies & International Affairs Department, Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA. A digital forensics practitioner and mobile device forensic examiner, he is a Certified Computer Examiner, Certified Cyber Forensics Professional, and Certified Information Systems Security Professional.

gary.kessler@erau.edu

[21] Alex Eckelberry, Glenn Dardick, Joel A. Folkerts, Alex Shipp, Eric Sites, Joe Stewart, and Robin Stuart, *Technical review of the Trial Testimony State of Connecticut vs. Julie Amero* (2007), available at http://dfir.com.br/wp-content/uploads/2014/02/julieamerosummary.pdf ; for a detailed analysis of this case, see Stephen Mason, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), xxxvi – lxxv.