Best Practices for Digital Forensics

Joshua L. Brunty, CHFI, SCERS, FTK/ACE-AME
Assistant Professor
Department of Integrated Science
Marshall University
1 John Marshall Drive
Huntington WV 25755
304.696.5602

May, 2013

I. Introduction

Computers and other digital devices are becoming pervasive in modern society. Due to this, it was inevitable that the investigation of such mediums would begin to feature as heavily in crime and law. Since the late 1970s the amount of crime involving computers has been growing very quickly, creating a need for constantly developing forensic tools, software, and best practices.

From its inception, the science of digital forensics has grown both in popularity and support. Digital evidence is being recognized much more easily in courts and organizations understand the need for proper forensic processes when investigating employee malpractice. Initially the field grew out of the work and needs of practitioners rather than from academics and scientists, which led to early digital investigations, tools and practices being ad-hoc and uncertain. Since the early 21st century proper practices and guidelines have helped to formalize the field.

Digital forensics is, at its root, a forensic science encompassing the recovery and investigation of material found in digital devices. A frequently cited definition for Digital Forensic Science is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. In addition, digital forensics may be subdivided into three general subsets: 1) Traditional digital forensics (e.g hard drives, media storage, and filesystems); 2) network forensics (e.g. networks, routers, servers, tapes); and 3) mobile, handheld, and embedded forensics (e.g. mobile phones, mobile tablets). Due to the variance of

the types of evidence that may be encountered within a digital forensics investigation, the fleeting nature of such electronic evidence, and the ever-evolving nature of technology, it is nearly impossible to develop standards and best practices that will not need to evolve over time. With that said, it is the intention of this chapter to focus on the standard best practices in the field of digital forensics, and provide a solid foundation to build evolving standards upon. In addition, this chapter will discuss best practices and innovations in developing technologies such as embedded devices and cloud computing.

II. Basic Application

At its core, digital forensics is founded upon the scientific method, and focuses on the following forensic elements of ***identification, testing/validation, acquisition/preservation, examination/analysis, interpretation, documentation*** and ***presentation/reporting*** of digital evidence in order to ensure such evidence is forensically sound. Although the methodology of handling different types of evidence varies in nature (i.e. mobile phones require different search/seizure principles compared to a laptop computer) the aforementioned forensic elements are the same.

Identification:

Before information can be collected and preserved, the sources of potential data must be identified. An investigator should understand the structure and organization of the electronic evidence before proceeding in a digital forensics investigation. In addition, the investigator should be properly trained on how to identify and seize various types of digital evidence before executing search and seizures involving digital evidence.

Testing/Validation:

With the field of digital forensics growing at an almost warp-like speed, there are many issues out there that can disrupt and discredit even the most experienced digital forensics examiner. One of the issues that continue to be of utmost importance is the validation of the technology and software associated with performing a digital forensic examination. The science of digital forensics is founded on the principles of repeatable processes and quality evidence. Knowing how to design and properly maintain a good validation process is a key requirement for any digital forensic examiner. This article will attempt to outline the issues faced when drafting tool and software validations, the legal standards that should be followed when drafting validations, and a quick overview of what should be included in every validation.

According to the National Institute of Standards and Technology (NIST), test results must be repeatable and reproducible to be considered admissible as electronic evidence. Digital forensics test results are repeatable when the same results are obtained using the same methods in the same testing environment. Digital forensics test results are reproducible when the same test results are obtained using the same method in a different testing environment (different mobile phone, hard drive, and so on). NIST specifically defines these terms as follows:

Repeatability refers to obtaining the same results when using the same method on identical test items in the same laboratory by the same operator using the same equipment within short intervals of time.

Reproducibility refers to obtaining the same results being obtained when using the same method on identical test items in different laboratories with different operators utilizing different equipment.

In the legal community, the Daubert Standard can be used for guidance when drafting software/tool validations. The Daubert Standard allows novel tests to be admitted in court, as long as certain criteria are met. According to the ruling in Daubert v. Merrell Dow Pharmaceuticals Inc. the following criteria were identified to determine the reliability of a particular scientific technique:

1. Has the method in question undergone empirical testing?
2. Has the method been subjected to peer review?
3. Does the method have any known or potential error rate?
4. Do standards exist for the control of the technique's operation?
5. Has the method received general acceptance in the relevant scientific community?

The Daubert Standard requires an independent judicial assessment of the reliability of the scientific test or method. This reliability assessment, however, does not require, nor does it permit, explicit identification of a relevant scientific community and an express determination of a particular degree of acceptance within that community. Additionally, the Daubert Standard was quick to point out that the fact that a theory or technique has not been subjected to peer review or has not been published does not automatically render the tool/software inadmissible. The ruling recognizes that scientific principles must be flexible and must be the product of reliable principles and methods. Although the Daubert Standard was in no way directed toward digital forensics validations, the scientific baselines and methods it suggests are a good starting point for drafting validation reports that will hold up in a court of law and the digital forensics community.

In the Daubert vs. Merrill ruling, The US Supreme Court defined scientific methodology as “the process of formulating hypotheses and then conducting experiments to prove or falsify the hypothesis.” The Scientific Method refers to a body of techniques for investigating

phenomena, acquiring new knowledge, or correcting and integrating previous knowledge. To be termed scientific, the method must be based on gathering, observing, or investigating, and showing measurable and repeatable results. Most of the time, the scientific process starts with a simple question that leads to a hypothesis, which then leads to experimentation, and an ultimate conclusion. To exemplify, if you are validating a particular hardware write blocking device you may want to start with the simple question "Does this tool successfully allow normal write-block operation to occur to source media?" Since it is assumed that the write-blocking device supports various types of media (SATA, IDE, and so on) you may be required to list the various requirements of the tool. Because if this, it is good practice for an examiner to use the scientific method as a baseline for formulating digital forensic validations. It is recommended that forensic examiners follow these four basic steps as a starting point for an internal validation program:

1) Develop a Scope of Plan

Developing the scope of the plan may involve background and defining what the software or tool should do in a detailed fashion. Developing the scope of the plan also involves creating a protocol for testing by outlining the steps, tools, and requirements of such tools to be used during the test. This may include evaluation of multiple test scenarios for the same software or tool. To illustrate, if validating a particular forensic software imaging tool, that tool could be tested to determine whether or not it successfully creates, hashes, and verifies a particular baseline image that has been previously setup. There are several publically available resources and guides that can be useful in establishing what a tool should do such as those of NIST's Computer Forensic Tool Testing Project (CFTT) available from http://www.cftt.nist.gov. The CFTT also publishes detailed validation reports on various types of forensic hardware and software ranging from mobile phones to disk imaging tools.

2) Develop a Controlled Data Set

This area may be the longest and most difficult part of the validation process as it is the most involved. This is because it involves setting-up specific devices and baseline images and then adding data to the specific areas of the media or device. Acquisitions would then need to be performed and documented after each addition to validate the primary baseline. This baseline may include a dummy mobile phone, USB thumb drive, or hard drive depending on the software or hardware tool you are testing. In addition to building your own baseline images, Once baseline images are created, tested, and validated it is a good idea to document what is contained within these images. This will not only assist in future validations, but may also be handy for internal competency and proficiency examinations for digital examiners.

3) Conduct the Tests in a Controlled Environment

Outside all the recommendations and standards set forth by NIST and the legal community, it only makes sense that a digital forensics examiner would perform an internal validation of the software and tools being used in the laboratory. In some cases these validations are arbitrary and can occur either in a controlled or uncontrolled environment. Since examiners are continuously bearing enormous caseloads and work responsibilities, consistent and proper validations sometimes fall through the cracks and are validated in a somewhat uncontrolled “on-the-fly” manner. It’s also a common practice in digital forensics for examiners to “borrow” validations from other laboratories and fail to validate their own software and tools. Be very careful with letting this happen. Keep in mind that in order for digital forensics to be practicing true scientific principles, the processes used must be proven to be repeatable and reproducible. In order for this to occur, the validation should occur within a controlled environment within your laboratory with the tools that you will be using. If the examiner uses a process, software, or even

a tool that is haphazard or too varied from one examination to the next, the science then becomes more of an arbitrary art. Simply put, validations not only protect the integrity of the evidence, they may also protect your credibility. As stated previously, using a repeatable, consistent, scientific method in drafting these validations is always recommended.

4) Validate the Test Results against Known and Expected Results

At this point, testing is conducted against the requirements set forth for the software or tool in the previous steps. Keep in mind that results generated through the experimentation and validation stage must be repeatable. Validation should go beyond a simple surface scan when it comes to the use of those technologies in a scientific process. With that said, it is recommended that each requirement be tested at least three times. If there are any variables that may affect the outcome of the validation (e.g. failure to write-block, software bugs) they should be determined after three test runs. There may be cases, however, where more or fewer test runs may be required to generate valid results.

Real world laboratory use, controlled internal tests utilizing scientific principles, and peer review should all be leveraged in a validation test plan. As the field of digital forensics continues to grow and evolve as a science the importance of proper scientific validation will be more important than ever.

Acquisition/Preservation:

The digital forensic acquisition process is a set of three principles that lie at the core of digital forensics and may be paraphrased as follows: 1) acquire the evidence without altering or damaging the original; 2) establish and demonstrate that the examined evidence is the same as that which was originally obtained; and 3) analyze the evidence in an accountable and repeatable fashion. Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed

by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion later in the process.

At the time of acquisition it is common for hash values (analogous to a digital fingerprint) to be created for the entire disk and for each of the digital objects (files) contained within it. If a digital object is subjected to the same hashing algorithm at a later date and the same hash value is obtained, it may be concluded that the object has not changed. Other functionalities include: file viewing, analysis of file signatures, date-time interpretation, identification of known files (e.g. operating system files) by means of hash libraries, data extraction, file export, searching, indexing, bookmarking, timeline visualization, logging, and reporting, all of which are to be undertaken according to forensically sound principles. In addition, principles such as network isolation of mobile phones and wireless devices (to prevent evidence alteration to occur over a wireless network) are also becoming prevalent in the digital forensics acquisition process. This can be achieved through "faraday shielding" which utilizes wire mesh bags, cans, and even aluminum foil to isolate a device from a wireless network until preservation of the evidence contained on the device can take place.

In many cases, these standards of acquisition and preservation are set forth by the Federal Rules of Evidence (FRE), specifically Rules 1000-1003 which outline the baselines and standards of creating duplicates of original evidence. It is common best practice in the field of digital forensics to create a "forensic duplicate" if applicable and perform subsequent examination and analysis from that duplicate to preserve and protect the original electronic evidence. Additionally, The Scientific Working Group for Digital Evidence (SWDGE) has a prominent role in establishing standards for acquiring and preserving digital evidence.

Examination/Analysis:

Simply put, the examination/analysis of digital forensics involves the actual process of the investigation, which can take many forms. When digital forensic examiners analyze digital evidence, it is the job of that examiner to find data (evidence) of probative value. This data may be deleted, overwritten, hidden, fragmented, password protected, and even encrypted. In addition, on any given piece of electronic evidence (hard drive, thumb drive etc.), data can be found in many different locations , which might include the internet cache and browsing history, email, and deleted/partially overwritten files. For this reason, Analysis can be the most time-consuming task, even when the examiner knows exactly what type of evidence is being sought. This is due to the fact that data can take on many different forms and fashions. Data can also be large in nature, which requires the examiner to use various tools and techniques to analyze digital evidence. There is a plethora of commercial and open-source forensic tools available that perform a variety of analysis functions from mobile phones to network forensics. It is important for the digital forensic examiner to be trained to know the availability of such software and hardware tools and know the capabilities of them. This will ensure that no evidence is overlooked in the examination/analysis process.

Reporting:

One of the most overlooked yet key aspects of the digital forensic process is that of reporting. Reporting is a key final phase to any investigation. A skilled investigator aims to balance the technical facts against their own analysis, whilst presenting it in layman terms. Writing a good report is often a skill hard acquired by digital forensic examiners because communicating complicated ideas in simple language is not always easy. How report findings are conveyed depends a lot of who will be reading it. For the most part it is easiest to assume the person

reading any report has no technical knowledge at all, and pitch it to them. A common forensic report might include a summary of findings, description of the analysis undertaken an explanation of terms (i.e. glossary). When producing evidence in a report format, alongside any report it is often required to produce the original evidence. Within a legal setting there is a pre-requisite called the "Best Evidence" rule, which asks for the original copies of evidence. Obviously, with digital evidence this raises the question of "what is the original copy". Viewing the original disk risks modifying the evidence (as discussed in previous sections) and often deleted evidence cannot be presented in original form. For practical purposes courts generally accept forensic duplicates or a report outlining key evidence in the case in question.

III. Future Directions

As digital forensics continues to grow as a practice, so too will the best practices and standards that are currently accepted in the field. Technological trends such as “cloud computing” pose challenges to best practices due to the fact that much of the data is located in an off-site location and cannot be retrieved locally. This not only creates a conundrum on the collection and validation phase, but it also poses legal challenges due to the nature in which the evidence would be seized (i.e. seizing evidence from a remote server). In addition, the concept of internet data and “big data” also create difficulty in setting baseline standards due to the fact that such data are large in volume, and may not be stored locally on a PC or device. It is assumed that social media sites like Twitter and Facebook contain a plethora of probative evidence that can be used by law enforcement, but the challenge of obtaining that evidence in a legally and forensically sound manner is proving to be one of the greatest tasks posed to digital forensic practitioners from this point forward.

References

The following references are useful to those who are interested in gaining more in-depth knowledge about digital forensics:

Digital Forensics Organizations/Projects

1) Scientific Working Group on Digital Evidence (SWGDE)
2) The National White Collar Crime Center (NW3C)
3) National Institute Of Justice (NIJ) Electronic Crime Partnership Initiative (ECPI)
4) International Association of Computer Investigative Specialists (IACIS)
5) American Academy of Forensic Sciences (AAFS) (Digital-Multimedia Sciences Section)
6) High Technology Crime Investigation Association (HTCIA)
7) High Tech Crime Network
8) High Tech Crime Consortium (HTCC)
9) High Technology Crime Investigation Association (HTCIA)
10) SEARCH - The National Consortium for Justice Information and Statistics
11) Digital Forensic Research Workshop (DFRWS)
12) National Institute of Standards & Technology (NIST) Computer Forensics Tool Testing Project (CFTT)

Publications

1) Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition (NCJ 219941)
2) Forensic Examination of Digital Evidence: A Guide for Law Enforcement (NCJ 199408)
3) Investigations Involving the Internet and Computer Networks (NCJ 210798)

4) Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors (NCJ 211314)

Legal Resources

1) Federal Rules of Criminal Procedure
2) Federal Rules of Evidence (FRE)
3) Federal Rules of Civil Procedure