Dispelling Common Myths of "Live Digital Forensics"

By
Matthew J. Decker, DFCP,
Warren G. Kruse II, DFCP,
Bill Long, DFCP,
Greg Kelley, DFCP

Introduction

We are all familiar with the story of Icarus, the figure from Greek mythology that soared high into the sky on wings made from feathers and wax, and who ignored the words of his father who warned "do not fly too close to the Sun." As the story goes, Icarus did fly too close to the Sun, the wax melted, his wings failed, and Icarus plummeted to his death. An entertaining and metaphorically rich story. Of course the story wasn't written to hold up under the scrutiny of scientific knowledge and an application of reasonableness, so the fact that the story is a myth is readily obvious, at least today.

Scientifically, we now know that it actually gets colder as one flies higher, so lofting wax high into the atmosphere would be a poor way to try to melt it. We also know that the average distance to the Sun is about 93 million miles, so it's hardly relevant that Icarus flew "closer" to the sun during his fateful flight, assuming he stayed within the breathable atmosphere. Barring such scientific facts, one should reasonably determine that using wax to assemble a collection of feathers will leave you with a wing that you cannot pick up, much less strap on and use to flap your way to freedom, so even a reasonable person with limited scientific knowledge should have a difficult time believing that the story is an actual account of events.

What's the point? The point is we are capable of determining myth versus reality via application of reasonableness and science; exactly what the Court expects of those testifying as experts. As Digital Forensics Practitioners in the United States we are obligated to apply the scientific method to our field of expertise, and draw reasonable conclusions from our methods.

The purpose of this paper is to identify and dispel a number of commonly encountered myths regarding “Live Digital Forensics” that have generated some confusion in our profession. Hopefully, we can provide some clarity on the issue, and offer a path to resolution. Let’s begin with the documented obligations placed upon testifying experts, including Digital Forensics experts, by the U.S. Court.

Obligations of a Digital Forensics Practitioner

Digital Forensics Practitioners in the United States are obligated:

- to offer opinions formulated in accordance with the Daubert Principles (Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993) 509 U.S. 579, 589), Frye Standard (Frye v. United States, 293 F. 1013 (D.C. Cir. 1923), or similar state statutes, as appropriate to

the Court. Note: Daubert is the most commonly accepted standard. Supreme Court cases General Electric Co. v. Joiner (522 U.S. 136 1997), and Kumho Tire Co. v. Carmichael (526 U.S. 137 1999) have been important in refining the application of Daubert.

- to adhere to the Federal Rules of Evidence (FRE) (http://www.law.cornell.edu/rules/fre/), or equivalent state rules as appropriate to the Court.

This appears to be a very short list, but the above represent the primary resources used by the U.S. Court to scrutinize experts, their evidence, and their opinions. One of the fundamental criterions mandated in Daubert is application of the scientific method by the expert in order to scrutinize their presentation of relevant scientific evidence in Court. This is important because it applies equally to all scientific, technical, and engineering evidence to be presented in a court of law, including Digital Forensics evidence. Before we delve into specific instances of myth versus reality pertaining to live digital forensics, you may want to review a few definitions that we need to know and understand.

Definitions We Need to Know

Forensic – Belonging to, used in, or suitable to courts of judicature or to public discussion and debate. (Online Source: http://www.merriam-webster.com/dictionary/forensic, Sept 13, 2011)

Digital Forensics - Preservation, collection, analysis and reporting upon digital data, such that the findings and conclusions are suitable for use in a court of law.

Digital Forensic Process - A process or method that satisfies the documented obligations placed upon testifying experts by the Court, such that the expert opinions derived from the process are suitable for use in a court of law.

Writings and recordings - "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation. (Federal Rules of Evidence; Article X, Rule 1001, para 1).

Original - An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original". (Federal Rules of Evidence; Article X, Rule 1001, para 3). *Special Note:* This is the only use of the word “computer” you will find in the entire FRE.

Common Myths

Without further adieu, we present to you some of the most common myths we have encountered in the realm of Live Digital Forensics, followed by an explanation of the reality.

Myth #1
A Digital Forensics Practitioner conducting live forensics upon a system will inevitably alter that system in some manner, thus live forensics cannot be conducted as a truly forensic process.

Reality: While true that conducting live forensics upon a system will inevitably alter that system in some manner, the flawed statement, here, is that this precludes the process from being a truly forensic process. In fact, there is no such requirement levied by the Court. In almost every other forensic discipline, we destroy or adulterate the evidence during the collection and analysis process. Mr. Ovie Carroll offers the following comparative comment regarding the preservation and collection of volatile evidence among several forensic disciplines:

> "Prior to collection, several types of evidence are volatile. Tire tracks and blood are susceptible to deterioration or total destruction due to weather. The casting of a tire track in dirt or the swabbing of blood with a wet cotton swab both modify or adulterate the evidence during the collection. Latent fingerprints, made from the transfer of the oils from a person's fingers, begin deteriorating from the moment they are left. It is critical to the preservation of evidence to take actions to preserve, as best as possible, these and many other types of evidence, but in doing so, the evidence itself is adulterated or modified. In some instances, analysis of evidence destroys at least a portion of the evidence as is common in drug testing. Some forms of digital evidence are likewise modified during the collection process. The collection of RAM and other forms of volatile data require some modification to the data in order to collect it. Some forms of digital evidence are in a constant state of movement, such as RAM on a running computer system or in some cases, data stored on solid-state memory. Like in the physical world, current technology is not available to collect some forms of evidence without modifying, adulterating or even perhaps destroying a portion of the evidence. The failure to take actions to preserve such volatile evidence, actions that will modify, adulterate or destroy a portion of the evidence, will in and of itself result in the modification or destruction of the evidence. As evidence collectors, we are trained to use steps necessary to collect evidence in a manner that best preserves its state as we discovered it. "
>
> ***Ovie L. Carroll, DFCP***

Furthermore, the acquisition of a live system using generally accepted practices may yield some really valuable evidence that would not otherwise be available, such as volatile physical memory or decrypted drive contents, and the acquired image will contain "Original" evidence in accordance with Article X, Rule 1001, para 3 of the FRE. Bear in mind too, that you may have to use the evidence you collect in court. To say that data collected and processed in a case is "not really forensics" is to say that "this evidence is not suitable for use in a court of law."

Myth #2
Actions taken by a Digital Forensics Practitioner must not change the data held on a digital device's storage media if such data is to be relied upon in a court of law.

Reality: The Court places no such demand on the Digital Forensics Practitioner. If the scientific method applied by the practitioner holds this requirement to be true, then it is the practitioners' forensic process that is perhaps too rigid and in need of alternatives. If your Forensic Process precludes you from collecting valuable evidence and using it in a court of law, then by all means fix your process. If opposing counsel's expert utilizes and presents a sound methodology for having acquired, analyzed and reported upon the evidence, then the evidence will almost certainly be admissible even if some minimal but necessary change was made on the evidentiary device.

Myth #3
Actions taken by a Digital Forensics Practitioner must produce an evidence image that can be repeatedly collected whilst producing an identical hash value, thus "Live forensics" and "Mobile Phone forensics" can't really be considered "forensics." Because the evidence image must be collected live, they can't be repeatedly collected in a forensically sound manner as you will not obtain an identical hash value for each subsequent image.

Reality: There is no such requirement levied by the Court. Hash values assist Digital Forensics Practitioners in a number of ways, but are not required by the Court for any purpose. A common use of image hash values is in support of Article IX, Rule 901, para 9 of the FRE, which describes an acceptable means for authenticating and identifying evidence that includes a process or system that produces an accurate result. Hash algorithms are not specifically named, but fall into this category as an acceptable means to identify and authenticate digital evidence. If your Forensic Process mandates that your collected images must produce a hash value that is reproduced upon collection of subsequent images from the same device, then your Forensic Process is outdated and overly rigid. It's time to fix your process.

NIST (National Institute of Standards & Technology), the federal technology agency that works with industry to develop and apply technology, measurements, and standards, does not perpetuate the myth that "Mobile Phone Forensics" isn't truly forensics. NIST defines Mobile Phone Forensics as "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods." (Source: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf) NIST also makes a distinction between "forensic tools" versus "non-forensic tools". NIST Special Publication 800-101, pg 15, states "Both forensic and non-forensic software tools often use the same protocols to communicate with the device. However, non-forensic tools allow a two-way flow of information to enhance or customize one's cellular device (e.g., to add customized phone rings, wallpaper, themes, etc.), while forensic tools are designed specifically to acquire data from the device without altering device content and to calculate integrity hashes over the acquired data." It is important to note that "forensic tools" may also allow a two-way flow of information to the device, but for a very specific purpose, and with controlled results. This two-way flow of information is permissible and may be required, because for a live acquisition to be performed the forensic tools may require a specially crafted application be placed on the phone under

inspection. The application is designed to minimize the amount and types of data written to the phone such that the probative value of the acquired data is maintained. You could not, for example, use a forensic tool to add customized phone rings, wallpaper, themes, contacts, etc, because the forensic tool prohibits these types of changes on the attached device. This fact is just one area which distinguishes "forensic tools" from "non-forensic tools" for live acquisitions.

Conclusion

Live Digital Forensics is a critical capability for Digital Forensics Practitioners, today, and will only become more critical as time marches on. Why? Because hard drives will become larger and less expensive, ever greater quantities of data will be stored electronically, encrypted data will demand live collection of some kind, data in the cloud will require live collection, and new products and technologies will emerge that require live collection. At least one hard drive product available today is marketed with a capability to *wipe itself* if removed from its native location and connected elsewhere, such as to a write-blocking device.

Naturally, there has been some confusion in the profession even among some of the most established forensic organizations in the community as to how to handle "live" data. This is likely because their existing Forensic Processes and Procedures are outdated, and in some cases actually contain instructions that preclude a forensics practitioner following a documented process from understanding that the "live" data is, in fact, "forensic" data when collected and processed in accordance with proper tools and techniques. To follow proper protocol using proper tools and techniques, and then to say that the data collected and processed in a case is "not really forensics" is to say that "this evidence is not suitable for use in a court of law," and for digital forensics practitioners that is not acceptable. Fortunately, it is also not true.

If your forensic processes preclude you from using some form of digital evidence in a court of law then you might consider that it's not the state in which you encountered the evidence that's at the root of your problem. You might solve your problem upon consideration of updating your forensic processes while remaining in compliance with the documented obligations placed upon testifying experts by the applicable Court.