available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

ELSEVIER

Digital Investigation

Editorial

What does "forensically sound" really mean?

A debate in our community over what constitutes forensic treatment of digital evidence is underway with significant repercussions for both practitioners and the growing number of attorneys and courts that rely on the results of digital examinations. This debate risks putting form over substance by imposing a methodological paradigm that detracts from, rather than enhances, the understanding of analytical results.

Purists argue that forensic acquisitions should not alter the original evidence source in any way. Yet, others point out that the act of preserving certain sources of digital evidence necessarily alters the original. For instance, collecting the contents of memory from a live computer generally requires the acquisition tool to be loaded into memory, which overwrites some volatile data. Similarly, using remote forensic tools necessarily establishes a network connection, executes instructions, and makes other alterations on the evidentiary system. Even when acquiring data from an IDE hard drive using hardware write blockers, the drive may have to be temporarily reconfigured to access data in a host protected area.

The dilemma of altering the original evidence in order to collect and analyze it is not a new one in forensic science. As a sanity check, looking at methods in traditional forensic disciplines, such as DNA analysis, can be helpful. When an examiner collects samples of biological material, the process generally scrapes or smears the original evidence. Forensic analysis of the evidentiary sample alters the sample even more because DNA tests are destructive. Despite the changes that occur during preservation and processing, these methods are considered forensically sound and DNA evidence is regularly admitted as evidence. The measure of forensic soundness, therefore, does not require the original to be left unaltered.

Setting an absolute standard that dictates "preserve everything but change nothing" is not only inconsistent with other forensic disciplines but also is dangerous in a legal context. Conforming to such a standard may be impossible in some circumstances and, therefore, postulating this standard as the "best practice" only opens digital evidence to criticisms that have no bearing on the issues under investigation. Focusing on whether an item of digital evidence was altered in any manner, rather than in a manner that affects the reliability or authenticity of the results, distracts from the substantive aspects of the evidence. Thus, distinguishing between sound forensic procedures versus unrealistic paradigms is important.

1. Paradigms versus best practices

In the inaugural issue of this journal, Carrier and Grand presented the proof-of-concept Tribble device for acquiring memory from a computer with the push of a button. However, this device has to be pre-installed in the victim system prior to an incident. Until equipment like the Tribble become commonplace and post-shutdown acquisition of physical memory has been thoroughly tested, the current best practice is to load a program into memory, save the contents of physical memory onto removable media or a remote system, and calculate an MD5 hash of the acquired data.

Also in the first issue, I evaluated features of Network Forensic Analysis Tools specifically designed to acquire network traffic as evidence. While many organizations have intrusion detection systems or some form of network-level logging that can be useful in a digital investigation, often they were not designed with evidence collection in mind. When a monitoring system used to collect network traffic generates its own traffic on the network, thereby introducing data into the stream, the collection and analysis must take this into account, but the presence of that data does not reduce the value of the network traffic as a source of evidence. Provided the digital investigator can give reasonable assurance that the evidence was not substituted, contaminated, or tampered with, the traffic captured by the monitoring device is still a useful source of digital evidence.

Situations frequently arise when it is necessary to preserve of digital evidence using tools that were not designed for forensic purposes. In the last issue, LaVelle presented a graphical interface to Robocopy for acquiring files from a network server in a way that preserves date-time stamps and maintains a log of any errors that occur during the copy process. Similarly, the Microsoft Exmerge utility can be configured to maintain a detailed audit log when acquiring current mailboxes from Exchange servers. Although the Robocopy and Exmerge programs are not forensic tools *per se*, provided they used appropriately and hash values of all acquired files are calculated after they are preserved, the results are generally considered to be forensically sound.

In some cases, when digital investigators are performing certain tasks, data are only displayed on the screen for a moment, making it necessary to preserve such transient digital evidence in some way. Methods for capturing this transient digital evidence may vary. For example, the HyperTerminal program available on most Microsoft Windows systems may be used to record in a log file the results of an examination of routers, firewalls, and other network devices. In addition, a second digital investigator observing the collection process can jot down each action and its result while the evidence is being collected. This approach has the added benefit of immediate peer review and collaboration.

Another example of real time evidence gathering is an IRC or IM chat session in which digital investigators keep a running log of their conversation with a suspect. However, if a significant amount of information is being displayed onscreen, it may be desirable to record a visual representation of events. A visual recording can be created using an application such as Camtasia that captures onscreen events and can replay them at a later time, much like video tape. Although these and other programs are useful for collecting digital evidence, they do not perform integrity checks and other audit logging that can be used to authenticate the data. Therefore, it is necessary to take additional steps to document the evidence. For instance, when preserving an IRC log file, documentation may include the time of collection, the log file's metadata (e.g. size, date-time stamps), and the MD5 value of the acquired data.

2. Documentation and trustworthiness

One of the keys to forensic soundness is documentation. A solid case is built on supporting documentation that reports on where the evidence originated and how it was handled. In addition to characteristics of the evidence source, such as a computer hardware clock or the number of sectors of a hard drive, an audit log and chain of custody enable an independent examiner to authenticate the evidence and assess its integrity and completeness.

When a digital investigator does not maintain documentation, a court may nevertheless admit his or her digital evidence based upon testimony about its authenticity and integrity. In *United States v. Tank*, a case related to the Orchid/Wonderland Club investigation, defendant argued that the authenticity and relevance of Internet chat logs were not adequately established. One of the points the defense argued was that the chat logs could be easily modified. The government offered a number of witnesses to establish that the logs were authentic. The court held that "printouts of computer-generated logs of 'chat room' discussions may be established by evidence showing how they were prepared, their accuracy in representing the conversations, and their connection to the defendant."

3. Conclusions

From a forensic standpoint, the acquisition process should change the original evidence as little as possible and any changes should be documented and assessed in the context of the final analytical results. Provided the acquisition process preserves a complete and accurate representation of the original data, and its authenticity and integrity can be validated, it is generally considered forensically sound. Imposing a paradigm of "preserve everything but change nothing" is impractical and doing so can create undue doubt in the results of a digital evidence analysis, with questions that have no relation to the merits of the conclusions.

Eoghan Casey
Stroz Friedberg, LLC 1150 Connecticut Avenue NW, Suite 200,
Washington, DC 20036, United states
E-mail address: eoghan@digital-evidence.net

1742-2876/$ – see front matter

doi:10.1016/j.diin.2007.05.001