Digital Evidence and Handling

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form. For example, if you walk into a house with carpeting, dirt from your shoes is left on the carpet, and the carpet leaves fibers on the soles of your shoes. These traces that are exchanged form the basis of what is termed 'trace evidence' in the physical world. In the digital world, there is often very similar trace evidence left when two systems come into contact with each other. For example, if an individual browses a website, the webserver or web application firewall may record the individual's IP address within a collection log. The website may also deposit a cookie on the individual's laptop.

It should be noted, though, that threat actors very easily manipulate digital evidence, so reliance on a single piece of digital evidence without other corroborating evidence should always be tempered with caution; it should be verified before it can be trusted.

DIGITAL EVIDENCE FORMS

To give you an idea of what digital evidence actually is, we've compiled a short list of some common evidence forms.

- E-mails
- Digital Photographs
- Logs
- Documents
- Messages
- Files
- Browser History
- Databases
- Backups
- Disk Images
- Video/audio files

CAN WE TRUST IT?

Digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. Digital evidence is often attacked for its authenticity due to the ease with which it can be modified, although courts are beginning to reject this argument without proof of tampering.

EVIDENCE HANDLING

Proper handling and securing of evidence are critical. Mistakes in how evidence is acquired can lead to that evidence being tainted and, subsequently, not forensically sound. In addition, if an incident involves potential legal issues, critical evidence can be excluded from being admitted in a criminal or a civil proceeding. There are several key tenets for evidence handling that need to be followed, as listed here:

– **Altering the original evidence**: Actions taken by digital forensics examiners should not alter the original evidence. For example, a forensic analyst should not access a running system if they do not have to. It should be noted that

some of the tasks that will be explored have the potential to alter some of the evidence. By incorporating proper documentation and having a justifiable reason, digital forensics examiners can reduce the chance that evidence will be deemed tainted.

– **Using write-blockers**: Although most forensic software tools have built-in software write blockers, you also need an assortment of physical write blockers to cover as many situations or devices as possible. A write blocker is used to keep an operating system from making any changes to the original or suspect media to keep from erasing or damaging potential evidence. Software write blockers work at the operating system level and are specific to the operating system. In other words, a software write blocker works on only the operating system in which it is installed. A physical write blocker works at the hardware level and can work with any operating system because, at the physical level, the write blocker is intercepting (or, in many cases, blocking) electrical signals to the storage device and has no concern about which operating system is in place.

– **Document:** One central theme you will often hear in law enforcement is the phrase: "If you didn't write it down, it didn't happen." This is especially true when discussing digital forensics. Every action that is taken should be documented in one way or another. This includes detailed notes and diagrams. Another way to document is through photographs. Proper documentation allows examiners to reconstruct the chain of events if ever the integrity of evidence is called into question.

Previous Topic
Mark Complete
Next Topic
Back to Lesson