D40 Computer Forensic Tool Quirks Uncovered During Testing

James R. Lyle, PhD, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899*

After attending the presentation, attendees will be made aware of several unexpected behaviors exhibited by computer forensic tools used in the acquisition of digital evidence. The practitioner can then either avoid the conditions that generate the behavior or take steps to mitigate the results.

The presentation will impact the forensic community by increasing awareness in the community of some tool behaviors that are unexpected and may have implications for examination of digital data and presentation of results.

The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology develops methodologies for testing computer forensic tools. The authors have applied the developed test methodologies to several tools in the areas of disk imaging and write blocking.

Disk imaging involves acquiring an image of either a physical hard drive or a disk partition, also called a logical drive. A disk imaging tool functions by reading each sector from the drive to be examined and creating either an image file or a clone of the original on a similar device. An image file contains all information to exactly reconstitute the original hard drive. While an image file may be stored as a bit for bit copy of the original, it is usually compressed in some way to save space. During testing of disk imaging tools it was observed that under the correct conditions for some tools the following behaviors:

- a tool incorrectly determines the size of a hard drive to be acquired,
- the last sector of a hard drive is not acquired,
- the last sector of a partition (logical drive) is not acquired,
- a few sectors near the end of an NTFS partition are acquired incorrectly,
- hidden areas of a hard drive are not acquired,
- a tool tries alternate read instructions if a faulty sector is encountered,
- readable sectors adjacent to a faulty sector are not acquired, and
- a restored hard drive is not identical to the original acquisition.

Write Blocking is used to protect original digital data from modification during acquisition or preliminary inspection to determination relevance to an investigation. A write blocking tool functions by inserting itself between the data to protect and the application accessing the data. Any operations that might change the data are intercepted and blocked. Write blocking can be implemented either in hardware or software. While there are advantages and disadvantages to both, hardware write blocking devices are more widely used. Usually access to digital data from a storage device is by a command set that implements some access protocol. Typical examples are BIOS commands, ATA commands and SCSI commands. These command sets usually implement several read and several write commands. During testing of write block software and hardware we have observed the following:

- blockers are designed in one of two ways: either (1) to block any write commands and allow any other commands, or (2) allow any read commands and block anything else, access protocols change over time and new commands are introduced, and some blockers may allow acquisition of protected data but, an operating system may not be able to mount a file system from a protected drive and hence a preliminary examination may not be possible.

Digital, Software, Testing

