B8 Computer Forensic Tool Testing Strategies

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

After attending this presentation, attendees will become aware of some of the strategies used by the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) for testing computer forensic tools used in the acquisition of digital evidence.

This presentation will impact the forensic community by increasing awareness that the impact tool test strategies have on the ability of tool testing to reveal anomalies in tool behavior.

The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology develops methodologies for testing computer forensic tools. The developed test methodologies to several tools in the areas of disk imaging and write blocking have been applied and test strategies for testing storage erasing, deleted file recovery, and string searching are being developed. A test strategy should cover all tool features and also give the tool opportunities to fail in easily detectable ways.

For example, good forensic practice is to start by writing zeros to any pieces of media that would be used in an examination of digital data. However, one common way for a tool to fail is to place information in the wrong location. If a block of zeros is transposed with another block of zeros the switch is undetectable. A better practice for media initialization during testing is to write unique content to each disk sector. This has the advantage that out of place data is easy to recognize. If the unique data also includes the original location of each sector then knowing the original location may be helpful in characterization of the tool behavior.

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 of the 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.

Write Blocking is used to protect original digital data from modification during acquisition or preliminary inspection in order to determine relevance to an investigation.

Storage erasing, as considered by CFTT, is for storage device reuse within an organization rather than for disposal or transfer to a destination outside the organization.

This presentation examines selected test cases and test procedures used by the CFTT project to demonstrate the kinds of tool errors that can be revealed by each strategy.

Digital, Tool Testing, Software

 ** Presenting Author*