B19 Deleted File Recovery Tool Testing Results

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

After attending the presentation, attendees will learn about issues revealed while testing meta-databased deleted file recovery computer forensic tools by the Computer Forensics Tool Testing (CFTT) project.

The presentation will impact the forensic science community by increasing awareness in the community of tool test strategies and the ability of tool testing to reveal anomalies in tool behavior. The presentation will aid the forensic practitioner in recognizing the limitations of meta-databased deleted file recovery tools.

The CFTT project develops methodologies for testing computer forensic tools. This presentation reports on tool behaviors observed while testing digital forensics tools against a set of file deletion scenarios.

A file system is used to store data for access by a computer. The data is normally stored within a tree-structured hierarchy of directories and files. When a file or directory is deleted from a file system, the associated *metadata* entry and the stored data are no longer directly accessible to the user and appear to be completely removed. However, in many file systems, e.g., FAT, neither the metadata associated with the file nor the actual content is completely removed. This creates a situation where there is *residual metadata* (metadata remaining after a delete has occurred) that is still accessible by direct access outside the usual operating system methods and can be used to reconstruct deleted files. Many forensic tools exploit the behavior exhibited by file systems of leaving metadata behind after a file is deleted to attempt to recover deleted files. Metadata-based deleted file recovery should not be confused with *file carving*, i.e., scanning unallocated memory for the file signatures present within a file itself to identify a deleted file. The scope of this presentation is limited to metadata-based deleted file recovery tools that use file system metadata from file system structures such as directories or i-nodes to identify recoverable deleted files.

The basic approach to creating a test image is as follows:

1. Create a file system on a secondary storage device.
2. Create some files.
3. Delete some of the created files.
4. Image the storage device.
5. Use the tool under test to attempt to recover the deleted files.

The test images used cover the most widely used file systems, including FAT16, FAT32, ExFAT, NTFS, ext2, ext3, and ext4. The HFS+ file system does not leave enough residual metadata behind after a file is deleted to make recovery practical.

Some of the observations discussed in this presentation include:

- The residual metadata varies with the file system. For example, file names may be completely or partially lost, pointers to file blocks may be overwritten.
- Only the first block of a deleted file is identified for FAT16 and FAT32 file systems. Some tools guess the location of the remainder of the deleted file; this strategy often leads to recovered files that are mixed from several original files.
- The tools sometimes include blocks from active files in a recovered file.
- The tools rarely include blocks that have never been allocated to the current file system, i.e., it is not likely that a block from a recovered file was not a part of some file.
- Some tools attempt to identify overwritten files. The tools often identify (incorrectly) intact files as overwritten.
- Support for ext3 and ext4 is often lacking.
- Sometimes ExFAT is not supported.
- Interpretation of MAC times must be done carefully. Time zone information and actual semantics of the times can vary across file systems and tools.

The test images and image layout documentation are available at the CFReDS project web site http://www.cfreds.nist.gov/dfr-test-images.html. Test reports on specific tools are available for the National Institute of Justice web site http://www.nij.gov/topics/forensics/evidence/digital/standards/cftt.htm

File Recovery, Software Tool, Digital Forensics

 ** Presenting Author*