B3 Creating Deleted File Recovery Tool Testing Images

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 some of the issues in the creation of test data for testing computer forensic tools used to recover deleted files from digital evidence and strategies used by the Computer Forensics Tool Testing (CFTT) project to address the issues.

The presentation will impact the forensic science community by increasing awareness of what impact tool test strategies have on the ability to reveal anomalies in tool behavior. The presentation will aid the forensic practitioner in the preparation of test data sets for testing forensic tool capabilities for the recovery of deleted files.

The CFTT project at the National Institute of Standards and Technology develops methodologies for testing computer forensic tools. This presentation covers creating test data images for testing digital forensics tools that recover deleted files using residual meta-data after a file is deleted to recover file name and file content.

A file system is used to store data for access by a computer. This 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 these 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:

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

This basic approach requires refinement so that the tool testing can produce verifiable results; the following issues need to be addressed:

1. The content of the image file needs to be documented. In particular, the following should be noted:
   - Active files and blocks allocated to each active file
   - Deleted files and content history for blocks allocated to a deleted file and time of file deletion
   - MAC (modify, access & create) times for each file
   - File attributes
   - Each operation (create, append or delete) on files.
2. Identification of conditions within a file system that are relevant to tool behavior and should be present in test images.
3. Development of techniques to bring about the relevant conditions.

Four programs were created to aid documentation of image file content as follows:

- **not-used** writes the text message “not used” to each sector of the storage device. This is run as a first step before the file system is created.
- **mk-file** is used to create files. Each block of the file is tagged with the file name and a sequence number. Blocks allocated to a file are easy to identify and track.
- **ap-file** is used to append to an existing file. This appends blocks to the file already created and continues the block numbering where it left off.
- **layout** scans an image file and classifies blocks as files, metadata or not used.

These four programs simplify classification of blocks from an image file as either *allocated to a file*, *never been used* or *file system metadata*.

This presentation gives an overview of the issues in creating deleted file recovery test images and techniques that can be used to address
the issues.

Digital Evidence, Software Testing, Deleted File

 ** Presenting Author*