Chapter 11

Data Analysis Techniques

Ed Crowley

Topics

- How to locate and organize all pieces of computer media and assemble them before you begin any interpretation of the contents.

Topics

- Restoring:
  - A forensic duplication
  - A qualified forensic image
- Recovering
  - Previously deleted files
  - Unallocated space and slack space
- Generating file lists
- Performing string searches

Forensic Analysis Preparation Issues

Whether you restore the duplicate or analyze it in its native format depends on several factors:

- Organization's analysis policies and methodologies
  - Tools vs. forensic suites
- Original data format
- Current file systems vs. exotic or little known types.
- Original data condition
- Valid and accurate image vs. image of a damaged drive
- Need to review the user's operating environment in its native state?

Three Methods

1. Duplicate image can be restored to another medium, producing a mirror or restored image.
   - Then, you can use DOS tools
2. You can analyze the duplicate image in Linux
   - Allows Linux to apply the native file system rules to the duplicate image
- You can allow a forensic tool suite to perform the functions of interpreting, presenting, and examining the forensic duplication.

Restoring a Forensic Duplicate

- When restoring a drive, it is essential to first wipe the destination hard drive clean.
- A specific tool such as Eraser from www.heidi.ie/eraser
- DD also work s.

Restoring a Qualified Forensic Duplication of a Hard Disk

- Knowing how to transform a suspect's hard drive utilizing a proprietary file format into a form that you can work with is an important skill.
- Tools include:
  - EnCase
  - SafeBack
  - FTK

Preparing a Forensic Duplication for Analysis in Linux

- Linux an ideal forensic analysis environment.
- You may also utilize a set of patches and tools provided by the NASA Computer Crime Division.
  - Contains a modified kernel and loopback mounting code that allows the system to recognize multiple partitions within a forensic duplicate image.
  - Allows you to analyze duplicate file without restoring it to another hard drive.

Examining the Forensic Duplicate File

- Challenging.
- Physical layer information.
- Needs to be overlayed with file system rules to view the contents of the duplicate in its native format.

Associating the Forensic Duplicate File with the Linux Loopback Device

- Assigning the /dev/loopa device to the dd_Image.full.bin file allows you to access the forensic duplicate file as if it were a stand alone device.
- To prevent the kernel from writing to the forensic duplicate, set the “read only” flags in two places.
  - First change the permissions of the file with the chmod command.
  - The second read only flag that is set is set when the image is mounted.

Reviewing Image Files with Forensic Suites

- With EnCase or the Forensic ToolKit (FTK), the process of creating a new case and populating it with forensic duplicates is fairly straight forward.

Tools

EnCase

- When acquiring evidence files in EnCase for the first time, you must create a new case.

Forensic Toolkit (FTK)

- Reviewing Forensic Duplicates
- While the interface and evidence import processes are a bit more complicated than EnCase, it can outperform EnCase when dealing with email store files and complex string searches.
- Currently, FTKs ability to handle compound files, such as Microsoft OLE, Outlook, and Exchange files is unparalleled.

Converting a Qualified Forensic Duplicate to a Forensic Duplicate

- FTK will convert the qualified forensic duplicate created by EnCase or SafeBack into a true bit for bit duplicate of the original.
- Load a QFD with FTK's explorer.

Recovering Deleted Files on Windows Systems

- It is desirable to scour unallocated space on a restored forensic image in order to undelete or recover as many files or file fragments as possible.

Recover

- Any evidence that had been deleted by malicious users
  - Simply erased by those who wished to cover up their misdeeds

Deleted Files

- Almost never does an O/S delete file data entirely
  - Usually just marks files for deletion
- Files remain intact until new data overwrittes the physical area where the deleted file's data are located.
  - Or a shredder overwrites sectors
- EnCase and FTK have utilities for recovering files.
  - Old Norton utilities also work (FAT)
  - You can also employ a hex editor.

Linux File Recovery Tools

- Supports a wide variety of file systems including:
  - FAT (12, 16, 32)
  - NTFS
  - HPFS
  - Macintosh
  - OS/2
  - EXT2, EXT3,
  - UFS (Solaris).
- Recovers file slack and unallocated space.
  - Enhanced loopback kernel makes it easy to identify slack, and unallocated drive space.
- Provides an efficient, effective, and accurate undelete utility.
- Provides keyword search capabilities.
- Performs all functions in a read only state on the file system being processed.
- Handles compressed drives
- Provides extensive auditing and logging of all forensic activities
- Provides for data validation and integrity.

File Recovery Factors

Potential Factors

- New files created on the partition
- Existing files growing larger
- New software installed on the partition
- If the partition contains a network share, network users may unknowingly modify the volume when accessing shared files.
- Applications running on the computer may update the partition.

Potential Factors

- If the partition stores the %systemroot% directory, Windows may modify the partition for internal housekeeping tasks.
- If the partition contains the web browser cache, it may be modified when a browser is started.
- If the volume contains the “TEMP” directory, it may be modified by installation software.
- System startup/shutdown, which includes many of the above elements, may also reduce the likelihood of data recovery.

Using FatBack to Recover Deleted Files

- Fatback offers a great way to perform file recovery on FAT12, FAT16, and FAT32 file systems from a Linux forensics platform.

Features include

- Long filename support
- Recursive undeletion of directories
- Lost cluster chain recovery
- Ability to work within single partitions or entire disks.

Using TASK to recover Deleted Files

- The Sleuth Kit (TSK)
  www.sleuthkit.org
- TSK is an open source forensic toolkit used to analyze Microsoft and Unix file systems.
- Only works with a single partition.

For a FAT file recovery test see:

http://www.sleuthkit.org/informer/sleuthkit-informer-14.html

http://dftt.sourceforge.net/test6/index.html

Autopsy Forensic Browser

- An HTML-based graphical interface for the Sleuth Kit's command line tools
  - Makes investigating a system easier and faster.

Features

- Initiating string and regular expression searches
- Recovering deleted material
- Creating a timeline of events, by examining the modified, access, and changed times of files
- Importing hash databases of "known good" files so that you can perform hash comparisons with the evidence files.

Autopsy

- On Back Track.
- Client/server architecture.
- Runs on many Unix systems.
- Client can run on any platform with an HTML browser.
- Begins by selecting New Case

Using Foremost to Recover Lost Files

- Foremost is a Linux program used to recover or “carve out” files based on the file headers and footers.
- Foremost can be configured to create a directory for all HTML pages, another directory that contains all Word documents, a directory that contains all GIF images, …

Recovering Deleted Files on Unix Systems

- Can be a challenge.
  - Many people do not even attempt.
  - Considered more art than science
- Grep and string search
- A more scientific approach would use debugfs on files stored on the ext2 file system.

Using debugfs to Relink a file to Lost+Found

- Debugfs is an interactive file debugger used to examine and to change the state of the ext2 file systems.
- Currently, provides the best means for recovering files on media using the ext2 file system
- See example page 273 …

Recovering Unallocated Space, Free Space, and Slack Space

File slack

- Unused space within a file allocation unit (cluster).

RAM slack

- Analogous concept applying to paging system's 4K pages

Unallocated space

- Area of the hard drive not currently allocated to a file.

Free space

- Portion of the hard drive media that is not within any currently active partitions.

Slack Space Tools

- NTI has a tool NTFSGETS for writing all of slack space to a single file.
- Both EnCase and FTK automatically reveal slack space and unallocated space on the qualified forensic duplication.

Generating File Lists

- Critical to analyze the contents of a hard drive.
- Done by creating file listings that contain:
  - Full path of each file found on the evidence media.
  - Last written and modified time/date stamps for each file
  - Creation time/date stamps, if they exist
  - Last access time/date stamps
  - Logical size of each file
  - An MD5 hash of each file

Listing File Metadata

- Good policy is to have in house tools that populate a data base for rapid time/date stamp correlation.
- CATALOG is a command line Linux tool that creates file lists.

Identifying Known System Files

- It is very helpful to identify and exclude from review the known operating system files.
- You can do this by getting their hash values
- You can get CDs with MD5 hashes from NIST
  - Use these to exclude known good files from your examination.

Preparing a Drive for String Searches

- Reducing the amount of data requiring review during analysis is critical.

Some challenges:

- Numerous proprietary file formats promote additional complexity when trying to perform string searches on the contents of a HD.
  - .pst and .ost, .dbx, Registry files, event log files, browser history files, and others require special tools for proper forensic analysis
- Numerous compressed file formats render traditional string searching ineffective
- Encrypted files or password protected files cannot be reviewed until unencrypted

Before Conducting Effective, Complete String Searches

- Identify all compressed files, decompress them
- Identify all encrypted files, unencrypt them
- Identify all compressed files in email stores and decompress them
- Remember that it is not uncommon to have compressed files contained within compressed files.

Performing String Searches with Grep

- Grep is a powerful, highly effective, and free utility for Unix environments.
- You can also use FTK, EnCase, and Task and Autopsy to do string searches

Questions?