COMPUTER FORENSICS AND SLEUTH KIT

Overview

- A brief history of Computer Forensics
- File Systems Structures
- The Sleuth Kit
- Demo

Computer Forensics

- Analytical techniques to identify, collect, preserve and examine evidence/information which is digitally stored
- Forensics is the gathering of obscured data usually as to be used as evidence in a legal setting
- Computer Forensics deals with the retrieval of lost data
- Requires a knowledge of computer organization and the right tools for the job!

Computer Crimes and Laws

- Prior to 1980s – computer crimes were dealt with existing laws
- 1978 – Florida passed first bill
- 1980s-1990s: Law enforcement agencies set specialized organizations
- 1984 - FBI sets up Computer Analysis and Response Team
- Most people employed to do the digging were just computer enthusiasts
- They developed ad-hoc tools that were the starting point of many forensics software

Standardization

- 1992 – first use of term “Computer Forensics”
- *Scientific Working Group on Digital Evidence* - 2002 paper *Best Practices for Computer Forensics*
- ISO 17025, General requirements for the competence of testing and calibration laboratories published in 2005

What are the goals of Computer Forensics?

- To be able to retrieve data that has been lost due to a complication
- To get data that has been erased on purpose by a person of interest
- Preserve the integrity of any evidence you collect

What Computer Forensics can do

- To identify anything that may have been removed from the user perspective, hidden away in the file system
- To recover that data so the user is able to view its contents
- Analyzing the drive to see how the user had interacted with it

Techniques

- Cross-Drive Analysis
- Live Analysis
- Deleted Files
- Stochastic Forensics
- SteganoGraphy

Cross Drive Analysis

- Correlates information found on multiple hard drives
- Used to identify social networks
- Anomaly detection - visits a site from his laptop frequently and never visited the site from his desktop

Live Analysis

- Use CF tools or SysAdmin tools to extract data from within operating system
- Useful for obtaining keys to encrypted hard drives and in some cases imaging the system before its shut down

Deleted Files

- Pointers to files are deleted
- The file still exists and is recoverable
- Sleuth Kit can do that

Stochastic Forensics

- Reconstruct Digital activity lacking artifacts
- Digital Artifact - Undesired alteration of data
- Used to analyze insider data thefts
- i.e. Uber and Google - Anthony Levandowski
- Large copying of data causes meta data of files to change and as such is detectable

Steganography

- Hide data in an image
- Could be sensitive government docs that criminal stole
- Can use a hash of the original image to compare if available

Types of Data to Recover

- Persistent Data, data that stays on when there is no power to the system
- Files that stay on the system because they are needed for later operations
- Volatile Data, data that the system may be lost because the system does not need it anymore
- Ex: delete files and temp files

Volatile Data

- Machine active; power down; info in ram lost
- Live analysis tools: COFEE, windd, WindowScope
- Cold Boot Attack:- machine powered off; freeze it to -60 to make residues stay
- Mouse Jigglers and UPS
- Easiest way is to save ram to disk
-

Types of Drive Formats

- NTFS (New Technology File System), the native windows file system
- HSF+ (Hierarchical File System), the native Mac file system
- exFAT (Extended File Allocation Table), older windows file system used in 2006
- Fat32, the legacy windows file system, simple and robust

What are the differences?

- Maximums – File name characters and file sizes are limited by the format in sectors of the drive
- Encryption – Native encryption of files and folders may not be supported
- Compatibility – Certain drives will only have certain abilities on certain operating systems

File System Structure

- Metadata – Information that lets you know what kind of system the drive is formatted to
- Inodes – Pointers to data within the drive that the system can quickly look through to search for something specific
- Data – The actual data that is stored within the drive

The Sleuth Kit

- An open source tool that allows the user to analyze disk images and recover them
- A command line tool, allowing users to analyze in their terminal
- A c library that allows the user to call upon it for scripts

Img_stat

- Img_stat displays the basic information of the drive
- Image type
- Size of the drive

```
root@kali:~/Desktop# img_stat backup.img
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 4026531840
```

Mmls

- Mmls presents the layout of the drive
- Offsets
- Partition Table

```
root@kali:~/Desktop# mmls backup.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000127   0000000128   Unallocated
002:  000:000   0000000128   0007864319   0007864192   NTFS / exFAT (0x07)
```

Fsstat

- Fsstat is a more detailed look at the file system than img_stat's basic information
- File System Information
- Metadata
- Content Information

```
root@kali:~/Desktop# fsstat -o 128 backup.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: D8A8FE3AA8FE16AA
OEM Name: NTFS
Volume Name: Bababooey
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
```

Fls

- Fls lists out all the files and directories in a drive
- Shows the state of the file
- Displays the information of the file

```
root@kali:~/Desktop# fls -o 128 backup.img
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-1:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
```

Ils

- Lists out inode information of the file system
- Inode numbers
- Time stats
- Permissions

```
root@kali:~/Desktop# ils -o 128 backup.img
class|host|device|start_time
ils|kali||1518379210
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
41|f|0|0|1518100556|1518100562|1518100556|1518100562|777|1|16
```

Istat

- Information on a data block by specifying the inode number of the file
- File information
- Access times

```
root@kali:~/Desktop# istat -o 128 backup.img 41
MFT Entry Header Values:
Entry: 41        Sequence: 2
$LogFile Sequence Number: 4207040
Not Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 264  ()
Created:        2018-02-08 09:36:02.284980300 (EST)
File Modified:  2018-02-08 09:35:56.204621800 (EST)
MFT Modified:   2018-02-08 09:35:56.204621800 (EST)
Accessed:       2018-02-08 09:36:02.284980300 (EST)
```

Icat

- Icat reads a files contents from the specified inode number
- Can read deleted files using this method
- $ icat [file] [inode]