Digital Forensics

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

Lab Assignment - 1

Activity 1:

- Identify the tools (Open Source and Freeware) which can be used to acquire and analyse data from all storage devices including memory

  - Some of the Best Available Open Source and Freeware tools

    1. Wireshark
    2. NMAP
    3. Oxygen Forensic Suite
    4. The Sleuth Kit
    5. SIFT
    6. Volatility
    7. Free Hex Editor Neo
    8. MVT
    9. Autopsy
    10. FAW
    11. USB Write Blocker
    12. NFI Defraser
    13. ExifTool
    14. Dumpzilla
    15. Caine
    16. Crowd Response
    17. Xplico
    18. ForensicUserInfo
    19. Paladin
    20. The Coroner's Toolkit

A. The Sleuth Kit – analyze disk images and recover files

- The Sleuth Kit (TSK) is a library and collection of command line file and volume system forensic analysis tools that allow you to investigate and analyze volume and file system data. With this software, investigators can identify and recover evidence from images acquired during incident response or from live systems. The software is open source, which allows investigators to verify the actions of the tool or customize it to specific needs.

- The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence.

- The volume system (media management) tools allow you to examine the layout of disks and other media. TSK supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools.

- TSK allows users to analyze a disk or file system image created by 'dd', or a similar application that creates a raw image. These tools are low-level and each performs a single task. When used together, they can perform a full analysis.

- TSK is based on The Coroner's Toolkit.

Features include:

- ✓ Analyzes raw (i.e. dd), Expert Witness (i.e. EnCase) and AFF file system and disk images.
- ✓ Supports the NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, and ISO 9660 file systems
- ✓ Tools can be run on a live system during Incident Response. These tools will show files that have been "hidden" by rootkits and will not modify the A-Time of files that are viewed.
- ✓ List allocated and deleted ASCII and Unicode file names.

- ✓ Display the details and contents of all NTFS attributes (including all Alternate Data Streams).
- ✓ Display file system and meta-data structure details.
- ✓ Create time lines of file activity, which can be imported into a spread sheet to create graphs and reports.
- ✓ Lookup file hashes in a hash database, such as the NIST NSRL, Hash Keeper, and custom databases that have been created with the 'md5sum' tool.
- ✓ Organize files based on their type (for example all executables, jpegs, and documents are separated). Pages of thumbnails can be made of graphic images for quick analysis.
- ✓ 'md5' and 'sha1' tools to generate hashes of files and other data.
- ✓ hfind creates an index of a hash database and perform quick lookups using a binary search algorithm.
- ✓ ils lists all metadata entries, such as an Inode.
- ✓ blkls displays data blocks within a file system (formerly called dls).
- ✓ fls lists allocated and unallocated file names within a file system.
- ✓ fsstat displays file system statistical information about an image or storage medium.
- ✓ ffind searches for file names that point to a specified metadata entry.
- ✓ mactime creates a timeline of all files based upon their MAC times.
- ✓ disk_stat discovers the existence of a Host Protected Area.

B. Write Blockers

Digital evidence is our major issue of concern in Forensic investigation. Forensic investigators need to absolutely assure of the fact that the data they obtain as digital evidence is not altered during the capture, analysis, and control.

In the courtroom everyone including attorneys, judges, jurors need to feel confident that digital evidence has not been tampered and is legitimate. How can you be assured that digital evidence has not tampered?

What are Write Blockers?

Write Blocker is a tool designed to prevent any write access to the hard disk, thus permitting read-only access to the data storage devices without compromising the integrity of the data. A write blocking if used correctly can guarantee the protection of the chain of custody.

NIST has issued a set of general guidelines for write blocking requirements:

1. The write-blocker tool shall not allow a protected drive to be changed.

2. The write-blocker tool shall not prevent any operations to a drive that is not protected.

3. The write-blocker tool shall not prevent obtaining any information from or about any drive.

What are the different types of Write Blockers?

Write Blockers are basically of 2 types:

Hardware Write Blocker and Software Write Blocker. Both types of write blockers are meant for the same purpose that is to prevent any writes to the storage devices. Let's discuss each type of write blocker in detail.

■ Hardware Write Blocker:

Hardware write blockers are used to intercept and block any modifying command from ever reaching the storage device. Some of its features include:

- ✓ They offer monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device.

- ✓ They provide built-in interfaces to a number of storage devices.

- ✓ Hardware write blockers can connect to other types of storage with adapters.

- ✓ Hardware devices that write block also provide a visual indication of function through LEDs and switches. This makes them easy to use and makes functionality clear to users.

Challenges of using Hardware Write Blockers:

Let’s discuss some of the challenges of using hardware-based write blockers.

- ✓ Hardware write blocking devices are very expensive.
- ✓ They are awkward to use since they require a physical connection and a different connector for each type of interface for IDE, SCSI, USB, etc.
- ✓ Hardware write blockers are comparatively slower as they need to perform protocol conversions.

■ Software Write Blocker:

Software write blockers are installed on a forensic workstation. According to NIST’s specification on software Write Blocker, a software write blocker tool operates by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface.

They provide the ability to simultaneously write block as many disk devices as are connected to a computer without the need for multiple expensive hardware write blocking devices.

Some of the features that are provided by different write blocking tools are:

- ✓ The user can control automatic write blocking policies for fixed and/or removable disks.
- ✓ The user can have write blocking tool remember each fixed device’s blocked or un-blocked status for ease of use on media repeatedly used on a workstation/laptop.

✓ Some of the write blocking tools provide a GUI interface that allows the user the ability to block and unblock any disk or flash storage device.

Benefits of using Software Write Blockers:

There are some benefits in using Software Write Blockers instead of Hardware Write Blockers.

✓ They offer faster imaging than using hardware-based write blockers.

✓ Software write blockers are more affordable than the hardware ones as they don’t need a separate physical connector to be attached to the device for write blocking.

Activity 2:

➢ Identify the tools (Open Source and Freeware) which can be used for analyzing emails.

■ Some of the common techniques which can be used for email forensic investigation are

1. Header Analysis
2. Server investigation
3. Network Device Investigation
4. Sender Mailer Fingerprints
5. Software Embedded Identifiers

■ Some of the available tools for analyzing emails

1. EmailAnalytics
2. Sortd
3. ActiveInbox
4. Todoist
5. The Email Game

- EmailAnalytics :

  - EmailAnalytics is the most comprehensive app on this list, and probably the closest to an actual “analytics” app.

  - EmailAnalytics provides analytics for Gmail, pulling data from your Gmail account about how many emails you have in various folders, how many emails you send per day, who you’re frequently emailing, and how your conversations usually unfold.

  - It’s all the data you need to positively determine how you’re spending your time and how that time expenditure can be improved in the future.