FORENSIC

Legal Informatics and Multimedia

Forensic Analysis for Computer Systems

Plan of the Labs:

1. Electronic data acquisition
2. Computer Forensics technics and tools
3. Volatility Framework
4. Autopsy (**Sleuthkit)**
5. FTK (Forensic ToolKit)
6. Guidance software EnCase & ProDiscover Forensic

Course Lab1: Electronic data acquisition

1.1 Introduction
1.2 Storage Formats for Digital Evidence
1.3 Acquisition Methods
1.4 Operating systems file structures
1.5 Windows evidence acquisition challenges

1.1 Introduction

The analysis of digital evidence poses challenges to forensics investigators. Working with digital media and electronic information is important for the successful implementation of case disposition.

- ✓ Forensic data acquisition can be defined as the process of collecting digital evidence from electronic media by making multiple copies of data being investigated

1.2 Storage Formats for Digital Evidence

There are two types of data acquisition methods:

- ✓ Static acquisitions and
- ✓ Live acquisitions.

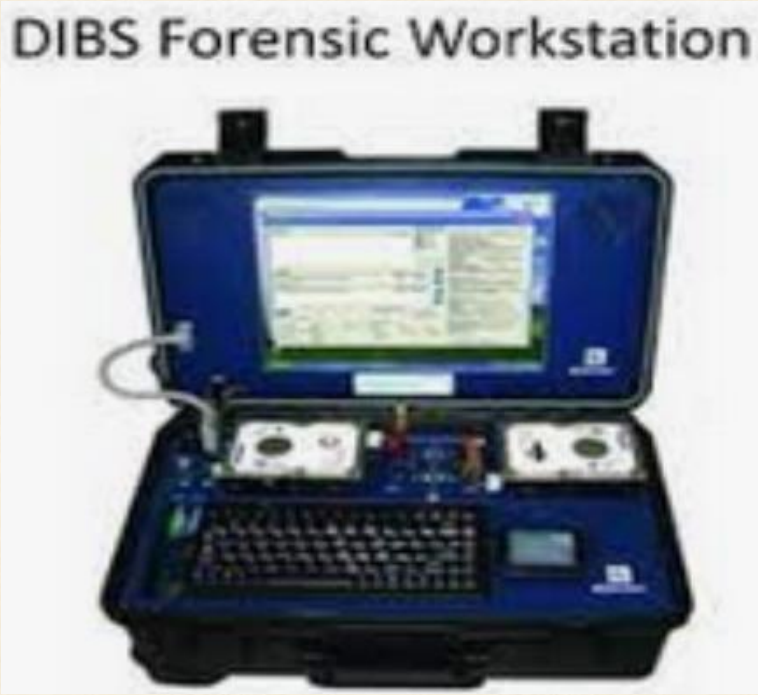
In *static acquisition*, any data stored on digital media remains the same regardless of the number of acquisitions being performed upon it (i.e., making a second or third static acquisition should produce the same outcome).

Whereas making multiple copies of *live acquisition* while a computer is running will collect new data instances because of the dynamic nature of the system. Therefore, by using live acquisition investigators cannot carry out repeatable processes, and repeatability helps to validate digital evidence.

1.2 Storage Formats for Digital Evidence (Cont.)

Hardware components provide required platforms to acquire and analyze data, but they still need third party forensic software to be more effective. For this purpose five categories of software tools are cited in the literature:

- Data preservation, duplication, and verification tools
- Data recovery/extraction tools
- Data analysis tools
- Data reporting tools
- Network utilities



1.2 Storage Formats for Digital Evidence (Cont.)

There are three main formats that are extensively used to acquire and store data. Two of them are open source, known as *raw* and *Advanced Forensic Formats (AFF),* and the third is proprietary which is based on vendors' unique features:

Raw format: It mainly makes a duplicate copy of the disk by performing Bit by Bit copying from one disk to another.

- For practical purposes to preserve digital evidence, software vendors modified this process with the ability to write bit-stream (or bit sequence) data to files that creates simple sequential files of the media.
- Raw format outperforms other file formats (like AFF and EWF) in terms of throughput, i.e., has high transfer data rate between media.

Despite this, it is inefficient in using storage capacity; it needs high storage volumes on disks.

1.2 Storage Formats for Digital Evidence (Cont.)

Advanced Forensic Format (AFF): This new open-source format has no implementation restrictions and it has started to gain recognition among computer forensics investigators.

AFF format has the following features:

- ✓ Investigators can create compressed or uncompressed image files
- ✓ It is scalable in storage capacity without any restrictions on file sizes.
- ✓ Provides a space in the created image file to store metadata descriptions.
- ✓ It is an open source that runs on multiple computing platforms.
- ✓ Has several mechanisms to test internal consistency and self-authentication

1.2 Storage Formats for Digital Evidence (Cont.)

Proprietary formats: Many vendor computer forensics tools stores collected data in specific formats. These formats are complementing vendor's analysis software. They have several advantages compared to other formats such as:

- ✓ Efficient in using Disk drive storage space by using options of compressing image files.
- ✓ Have built-in mechanisms to split an image into smaller pieces or segments for archiving purposes.
- ✓ Have built-in mechanisms for checking data integrity.
- ✓ Have metadata features that can be integrated into the image file, such as timestamps

Their main disadvantages are:

- ✗ They are vendor proprietary formats, which means that its unable to share an image between different vendor computer forensics analysis tools.
- ✗ They have some limitations in file size. Typically, forensic tools that use proprietary formats can produce a segmented file having 2 GB maximum segment size.

1.3 Acquisition Methods

Generally, there are four methods for data acquisition which are:

1) Disk-to-image file
2) Disk-to-disk copy
3) A logical disk-to-disk
4) A sparse copy of a folder or file

1.3 Acquisition Methods

1) Disk-to-image method is considered as the most common and flexible method used by investigators,

- ✓ In this method we can create several copies of a suspected media which are constructed by using bit-for-bit replications mechanism.
- ✓ Moreover, they can also use other forensic tools, such as **SMART, ProDiscover, X-Ways Forensics, FTK, ILook,** and **Autopsy**, to read the most common types of disk-to-image files they created.

1.3 Acquisition Methods (Cont.)

2) **Disk-to-disk copy :** It is a solution of making a disk-to-image file where we have hardware and/or software incompatibilities problems. This becomes more complicated when investigators face old disk drives. In this case, they might have to create a disk-to-disk copy instead of disk-to-image copy. Several tools are available – like **EnCase and SafeBack-** that can copy data exactly from an older disk to a newer one.

3) **A logical disk-to-disk :** The above tools can adapt their functionality to match data on the original suspect drive. They do that by modifying disk hardware features such as cylinder, head, and track configuration. This last represents a logical disk-to-disk operation.

1.3 Acquisition Methods (Cont.)

4) A sparse copy of a folder or file : In the case that the extracted data is stored in a large drive, the data capture process can take several hours. To overcome this issue:

- ✓ we can use a sparse data acquisition that gathers only specific types of files.
- ✓ In this case, the overall performance will be improved especially when the process needs to examine only some parts of the suspect's disk drive.

Beautiful practices:

- ✓ Using of compression methods to reduce file size to fit with the disk drive storage space, such as **WinRAR, PKZip and WinZip** which use lossless compression to reduce file size without affecting the image quality.
- ✓ Performing hashing operation to test the data consistency by carry out a hash such as **MD5 or SHA-1**. This should be done before and after applying the compression

1.3 Acquisition Methods (Cont.)

- ✓ Producing at least two duplicate images of the evidence they collect. In this case and if they have more than one software tool, they can try to make the first copy using one tool and the other one with another tool.

- ✓ Acquired data should be validated, thus an important part of computer forensics is validating digital evidence. A forensic hash is a standard approach that is commonly used for this validation. It is a form of a checksum*.

*A checksum uses a mathematical formula that simply sum the assorted bits in a message to provide a value. Hashing mechanisms generate a binary or hexadecimal digital fingerprint of a file. They use more complex mathematical functions of checksum algorithms

1.3 Acquisition Methods (Cont.)

A number of forensic tools with built-in hashing capabilities are available nowadays. Some tools outperform others in terms of computer resource consumption.

The above-mentioned hashing algorithm methods are available as standalone programs or are integrated into many acquisition tools or kits. For example:

- ✓ Windows system has built-in an MD5 hashing tool and third-party programs exist such as **Breakpoint Software, Hex Workshop or X-Ways/WinHex**.
- ✓ Commercial computer forensics kits also come up with built-in validation techniques such as **FTK, ProDiscover, and EnCase.**

1.4 Operating systems file structures

We present in this section the artifacts (file structures) that are unique and specific to two well-known OS which are: Microsoft Windows, and Linux.

Windows Systems : Windows is the most popular OS and therefore occurs most frequently in forensic examinations.
As a result, it has many well-known artefacts. It mainly supports two types of primary file systems:

- ✓ File Allocation Table (FAT) and
- ✓ New Technology File Systems (NTFS).

1.4 Operating systems file structures (Cont. Win Os)

File Allocation Table (FAT): This file structure is one of the simplest systems and was totally supported by the family of Microsoft operating systems, i.e.; MS-DOS and Windows. Its simplicity comes from the fact that it possesses few data structures. It can be **FAT16, FAT32, and exFAT.**

As it's an old and generic system, it is supported by other operating systems (Linux & Mac Os), thus it makes it easy for investigators to move it from one system like Linux to another one like Windows. Despite the aforementioned advantages, FAT systems suffer from security issues compared to other systems.

1.4 Operating systems file structures (Cont. . Win Os)

New Technology File System (NTFS): Currently, the NTFS system is the most popular system used in Microsoft OS.

- ✓ This popularity comes from its ability to set Access Control Lists (ACLs) on file objects (permissions control) and having built-in file compression mechanisms.
- ✓ The Master File Table (MFT) is the richest source of information required by an investigator when working with the **NTFS** file system.
- ✓ The size of each MFT entry is 1024 bytes, which makes it straightforward to parse.

1.4 Operating systems file structures (Cont. . Win Os)

The following table lists the main differences between Windows file systems:

FEATURE	FAT32	NTFS
Max. Partition Size	2TB	2TB
Max. File Name	8.3 Characters	255 Characters
Max. File Size	4GB	16TB
File/Folder Encryption	No	Yes
Fault Tolerance	No	Auto Repair
Security	Only Network	Local and Network
Compression	No	Yes
Conversion	Possible	Not Allowed
Compatibility	Win 95/98/2K/2K3/XP	Win NT/2K/XP/Vista/7

1.4 Operating systems file structures (Cont. Linux Os)

Linux systems : Linux Os has become a popular operating system and found its way into a large number of applications and environments such as networking devices and powerful supercomputing clusters.

- ✓ Some versions of Linux OS have come a long way from their humble roots as a free Unix-like system for personal computers.
- ✓ Most of them share a common standard Linux file system, directory structure, system artefacts and user activity.
- ✓ Most current Linux systems use the **Ext4** file system and older systems used **Ext3** and **Ext2**.

1.4 Operating system file structures (Cont. Linux Os)

Any **Ext** file system has two main components that make up its layering structure they are:

- ✓ The **superblock** : It represents a data structure type that is located in the first 1024 Bytes of the **Ext** file system. It maintains information about the layout of the file system, its block and node allocation information, as well as timestamps.

- ✓ The **group descriptor table:** Which is located after the superblock and contains allocation status information for each block group found on the file system.

1.4 Operating systems files structure (Cont. Linux Os)

In addition to the **Ext** family of file systems, others are found but are rarely used in Linux file systems. None of these systems are currently supported by The SleuthKit but can be tested logically using generic Linux file system tools. These formats are: ReiserFS, XFS, JFS, YAFFS2 and JFFS2.

Table below lists the main differences between Linux file systems.

Feature	EXT4	XFS	BTRFS
Architecture	Hashed B-tree	B+ tree	Extent based
Introduced	2006	1994	2009
Max volume size	1 Ebytes	8 Ebytes	16 Ebytes
Max file size	16 Tbytes	8 Ebytes	16 Ebytes
Max number of files	4 billion	2^{64}	2^{64}
Max file name size	255 bytes	255 bytes	255 bytes
Attributes	Yes	Yes	Yes
Transparent compression	No	No	Yes
Transparent encryption	Yes	No	Planned
Copy-on-Write (COW)	No	Planned	Yes
Snapshots	No	Planned	Yes

1.5 Windows evidence acquisition challenges

Windows evidence acquisition have the following drawbacks:

- When using Windows OS they can easily corrupt the evidence drive, investigators must apply well-tested write-blocking hardware devices to protect them.
- Some Windows forensics tools face several challenges when trying to acquire data from protected areas of the HDD.
- There are some legal and ethical issues in some countries of how to use the write-blocking devices for the data acquisition process.

1.5 Windows evidence acquisition challenges

The general challenges faced by Computer Forensics are:

- The increase of PC's power and extensive use of Internet access.
- Easy availability of hacking tools.
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes the investigation task very difficult.
- Any technological changes require an upgrade or changes the solutions.