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 Lab2: Computer Forensics technics and tools

2.1 introduction
2.2 Computer Forensics technics
2.3 Computer Forensics tools
2.4 Main functions of Computer Forensics tools
2.5 Other Forensics tools

2.1 introduction

Forensic techniques and tools are used to extract forensic evidence from computers and computer network systems. Using appropriate forensic techniques and tools helps the forensic examiners to extract and analyze forensic evidence.

However The main purpose of the digital forensic tools is to create an image of the suspect drive to an image file. Later, the image will be analyzed in separate environments. On the other hand, due the reliability and under time specific environment live forensic is required to deal with threats at runtime.

2.2 Computer Forensics technics

The common forensic techniques used during computer forensic investigations are :

1. Data Recovery

As most of the computer system operations are data driven, data forensic become the most typical setting for forensic professionals.

There are various technics used for data recovery. Generally, they can be used in two forms: **in-place** data recovery (the forensic tool can be used to repair or fix the error on the disk drive) and **read-only recovery** (the forensic tool can be used to restore the recovered files somewhere on the disk).

2. Cross-Drive Forensics

Cross-drive forensic technics can be used to analysis and compare the information found on multiple hard drives. This type of forensic investigation can be used in different types of intrusion detection such as anomaly and host-based intrusion detection.

2.2 Computer Forensics technics (Cont.)

3. File Forensics

Files forensics is very important and extensively used technic in computer forensics by means of various file forensic tools. As physical file data cannot always be erased by most operating systems, the files data can be reconstructed easily from the hard drive. The following illustrates different kinds of file forensic techniques and methods:

- File Analysis and File Filtering
- String Searching and File Fragments
- File Carving

4. Live Forensics

Live forensic technics are used to extract evidence directly from the normal or standard interface which focus on computer systems that are always powered on. The aim of this method is to avoid losing volatile data while acquiring the evidence.

2.2 Computer Forensics technics (Cont.)

5. Password Forensics

Password forensics is important in the investigation process. In fact, it will help to reach and access to a potentially valuable source of evidence.

A password system can provide the first line of defence and protection for computer and file systems. The issue is associated with the management of the password and protecting the password itself from being lost.

In the case of losing the file or system password, the easy and safe way is to recover the password by cracking it. There are many methods can be used in this case such as brute force, reduce the number of possible passwords, etc. On the other hand, the issue will continue with the recovery of encrypted files.

6. Email Forensics

Using e-mail forensic technics, the email header metadata such as the IP address of the source, delivery details such as time and data as well as the computer name can be analyzed and extracted. This information is very useful to trace and establish the true source of the email.

2.3 Computer Forensics tools

Forensic examiner (investigator) needs to learn many forensic tools as possible. Although there are very common tools, it is almost mandatory for the forensic examiner to have hands on the most common forensic tools.
Digital investigation tools have become relatively easy to use and that reduces the time needed to conduct an investigation.
The following table surveys the most common digital forensic tools. The tools are discussed in terms of features and relevant operating platform.

Digital Forensic Tools	Operating Platform	Features
Encase	Windows	Multi-purpose forensic tool
Drive spy	DOS/Windows	Inspects slack space and deleted file metadata
Wire shark	Cross-platform	Open-source packet capture/analyze
Autopsy	Windows/UNIX	Smartphone and hard disks forensics
CAINE	GNU/Linux	Computer aided investigative environment

2.3 Computer Forensics tools (Cont.)

Volatility	Cross-platform	Open source memory forensic
Windows-Scope	Window	Memory forensic
Magnit AXIOM	Cross-platform	Mobile device forensic
XRY	Cross-platform	Mobile device forensic
Snort	Unix/window	Detect network intrusion and perform protocol analysis
TcpDump	Unix	Network monitoring, protocol debugging, data gathering
SANS Investigative Forensics Toolkit	Ubuntu	Multi-purpose forensic operating system
Registry Recon	Windows	It rebuilds the windows registries from anywhere on a hard drive and parses them for deep analysis
Digital Forensics Framework	Unix-like/ Windows	Framework and user interfaces dedicated to Digital Forensics

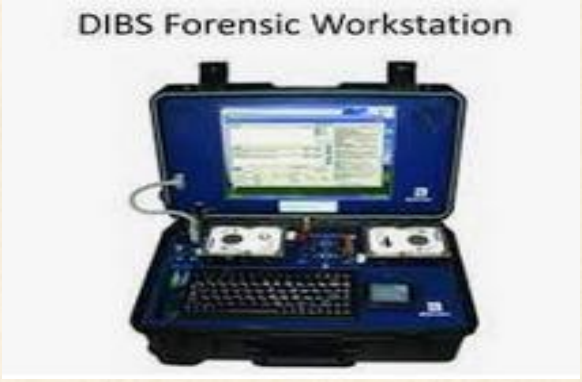
2.3 Computer Forensics tools (Cont.)

Forensic Toolkit (FTK)	Windows	FTK is a multipurpose court cited digital investigations platform built for speed, stability and ease of use
DiskExplorer	Windows	Windows based Disk Editor for Windows and Linux File Systems
WinHex	Windows	Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor
The Coroner's Toolkit	Unix-like	A suite of programs for Unix analysis
COFEE	Windows	A suite of tools for Windows developed by Microsoft
Xways	Windows	Used for disk cloning and imaging
The Sleuth Kit	Unix-like/ Windows	A library of tools for both Unix and Windows
DEFT Zero	Linux	Data and evidence gathering
FTK Imager	Windows	Data preview and imaging tool
FAW (forensic acquisition of websites)	Cross-platform	Online websites forensic

2.4 Main Functions of Computer Forensics Tools

Digital forensic utilities are mainly classified into those aimed at **hardware** or **software**. A **hardware** tool can be a simple one, for example set up for a **single-purpose** component or a more complex one like those necessary for computer systems and servers.

An example of a single-purpose hardware tool is the **Tableau T35es-R2 SATA/IDE eSATA**. It is used to access a **SATA** or an **IDE disk** drive with one device. **Expert systems** and **DIBS Advanced Forensic Workstations** are some examples of digital forensic hardware tools mainly deigned for complete systems.



Software forensic tools can be also sub-divided. There are **command-line** and **GUI** based tools, **SafeBack** is an example of a command-line disk acquisition tool that was mainly designed for hard disk drive imaging. Other tools are designed to perform several different tasks like **PassMark Software OSForensics, AccessData FTK, Technology Pathways ProDiscover, X-Ways Forensics, Autopsy**. Software forensic tools are also commonly used for data copying purposes.

Hardware and software forensics tools share common specific functions. The following set of functions are being used as guidelines to evaluate digital forensics tools.

2.4.1. Data acquisition

One of the first tasks that digital forensic investigators should care about is how to acquire data from a device and make sure to preserve the original disk drive. This can be done by making a replica of the main HDD to save the digital evidence, if there is any, from damage or corruption. Data acquisition has several sub-functions they include the following:

- **Physical data copy**
- **Logical data copy**
- **Data acquisition format**
- **Command-line acquisition**
- **GUI acquisition**
- **Remote, live, and memory acquisitions.**

Software acquisition can be done either **physically** or **logically**. Physical acquisition is to make a full copy, bit-by-bit acquisition, of the whole HDD (used to find deleted files or folders), whereas in the logical acquisition only a disk partition is copied (it involves accessing files and folders). Furthermore, some software acquisition methods have built-in mechanisms to make a full image of the whole HDD. Usually, the crime scene determines which type of acquisition methods an investigator should use to achieve the intended goals.

2.4.2. Validation and Verification

Validation and **verification** are two main functions that are mainly used for testing purposes. Here, validation is specifically used to confirm that a tool is functioning as expected without unexpected results, and verification assures that any two datasets (the original drive with the image) are completely identical. This process can be done with the help of hashing algorithms.

The Scientific Working Group on Digital Evidence (SWGDE) has some online datasets used as benchmarks for testing digital forensics tools. As an example, consider the forensics tool **EnCase**. This tool prompts the user to obtain the **MD5 hash** value of acquired data, and **FTK** is used to validate the generated **MD5** and **SHA-1** hash sets during the process of acquiring digital data.

Also, some hardware acquisition tools have facilities to simultaneously apply both the MD5 and CRC-32 hashing algorithms to acquire the data. Examples of such tools are **Image MASSter Solo-4 Forensic** and **Solo-4 G3 PLUS Forensic Enterprise Super Kit**. It is highly recommended to use the tool with built-in hashing function mechanisms for verification purposes.

Super Kit

The National Software Reference Library (NSRL) is a good resource that can be used by investigators to get technical details about the best hashing values being used for various OSs, and images that investigators can download from: https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl.

2.4.3. Extraction

The **extraction** task is considered as the very hard among all tasks. It is responsible for data recovery. **Simple Carver Suite** and **DataLifter** are examples of forensic tools can be used for such an approach. They are mainly designed to work with common datatypes that are taken from the **unallocated HDD space**. DataLifter includes another interesting feature that enables users to add other header values as needed. The extraction function is further divided into several subfunctions:

- **Data viewing**
- **Keyword searching**
- **Decompressing or uncompressing**
- **Carving**
- **Decrypting**
- **Bookmarking**

All these sub-functions can give digital investigators good flexibility in exploring the data. Data analysis, recovery, and encrypting, or decrypting files are considered major challenges that need special treatment by investigators. From the point of view of a digital investigation, encrypted files and mechanisms are a big challenge. This is due to the fact that many password recovery tools are freely available with built-in mechanisms to generate potential password lists (Brute-force attack).

Unallocated free space refers to **a portion of the hard disk that hasn't been allocated to any partition or file system**. It can be used for creating new partitions or expanding existing ones

2.4.4. Reconstruction

The reconstruction function in some forensics tools can be used to regenerate the HDD of the suspect machine for the following purposes:

(1) to analyze the different activities that occurred during the crime scene, and
(2) to share the disk drive with other investigators who are working on the same problem. This allows them to engage in more extensive testing and analysis of the digital evidence,
(3) it is also done if a disk drive has been infected by malware or any malicious software.

Investigators can use any of the following methods to reconstruct the original copy of a disk drive:

- **Disk-to-disk copy**
- **Partition-to-partition copy**
- **Image-to-disk copy**
- **Image-to-partition copy**
- **Disk-to-image copy**
- **Rebuilding files from data runs and carving**

Nowadays, **disk-to-disk** and **partition-to-partition** copies are rarely used. Typically, for security purposes, investigators need to copy an image to another location such as a virtual machine or another computer connected to the network. Some forensics tools can directly create an image from a disk (disk-to-image copy) and store it in the desired location. Examples of such tools would be the **free DD command** found in Linux systems. Some tools work with specific data formats. For example, **.eve** images can be restored only by using the **ProDiscover** tool. Nevertheless, there are some formats like **.E01** or **.001** that can be used by a variety of tools.

2.4.5. Reporting

Performing a forensics HDD analysis requires creating a complete report in various formats, such as Microsoft Word, HTML, or Acrobat PDF. Typically, these reports are not used directly because investigators might work with several printouts extracted from several different applications. The reporting functions includes some other sub-functions that are:

- **Bookmarking (or tagging/labeling)**
- **Log reports**
- **Report generator**

Although forensic software reports are considered as the main outcome of the investigation process, investigators should not forget their responsibilities to clearly explain the significance of the evidence they recovered and, if necessary, define any limitations or uncertainty that applies to the results.

When choosing the best tool, investigators need to develop an action plan to justify their selection. The main goal is to help investigators to choose the appropriate tool that satisfies as many attributes as possible. Among the common features that will help them in their selection are:

- **The type of OS**
- **The portability of the tool**
- **The format of the files**
- **The capability of the tool such as having built-in scripting codes to automate repetitive tasks for reducing time.**
- **Tool vendor information**
- **Open-source or commercial tool**

In summary, Table in next slide shows a comparison of some digital forensic tool functions discussed above. Also, it is highly recommended to refer to some nonprofit organizations' websites like NIST's Computer Forensics Tool Testing (CFTT) program, and ASTM International's E2678 standard when working and testing digital forensics tools.

It is worth noting that, investigators may develop their own comparative table by adding other functions as necessary to determine which tools perfectly fit with the case they are working with.

Function	ProDiscover Basic	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
Acquisition				
Physical data copy	✓	✓	✓	✓
Logical data copy	✓	✓	✓	
Data acquisition formats	✓	✓	✓	✓
Command-line processes				✓
GUI processes	✓	✓	✓	✓
Remote acquisition		✓	✓	✓
Validation and verification				
Hashing	✓	✓	✓	✓
Verification	✓	✓	✓	✓
Filtering		✓	✓	✓
Analyzing file headers		✓	✓	✓
Extraction				
Data viewing	✓	✓	✓	✓
Keyword searching	✓	✓	✓	✓
Decompressing			✓	✓
Carving		✓	✓	✓
Decrypting		✓	✓	
Bookmarking	✓	✓	✓	✓
Reconstruction				
Disk-to-disk copy	✓	✓	✓	✓
Partition-to-partition copy	✓	✓	✓	✓
Image-to-disk copy	✓	✓	✓	✓
Image-to-partition copy	✓	✓	✓	✓
Disk-to-image copy	✓	✓	✓	✓
Rebuilding files	✓	✓	✓	✓
Reporting				
Bookmarking/tagging	✓	✓	✓	✓
Log reports		✓	✓	✓
Report generator	✓	✓	✓	
Automation and other features				
Scripting language				✓
Mount virtual machines		✓	✓	✓
E-discovery		✓	✓	✓

2.5 Other Forensics Tools

For other Hardware based acquisition tools we can cite :

Tribble : This tool makes use of a dedicated Peripheral Component Interconnect card PCI. The card needs installation before incident happening. The PCI card can be detached easily after the incident. Therefore, the system state is maintained to find digital evidence.

FireWire bus or IEEE 1394 bus :It supports physical access to the system memory via other functionalities for example data-transfer and high speed communication.

And for Software based tools:

wxHexEditor (https://www.wxhexeditor.org/) "is a cross-platform, open source hex editor written in C++ and wxWidgets. It works as low level disk editor too and uses 64 bit file descriptors. wxHexEditor does not copy the entire file to the RAM in order to make it faster and opening huge files".

Volatility Framework (https://www.volatilityfoundation.org/) "is an entirely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. It supports a mixture of sample file formats with the ability to convert between these formats: - Hibernation file - Raw linear sample (dd) - Crash dump file. It's functionality can be extended by the use of Volatility plugins".

pdgmail (https://tools.kali.org/forensics/pdgmail) "is a browser email memory tool implemented by python script in order to extract gmail artifacts from memory images".

Belkasoft Evidence Center (https://belkasoft.com/ec) "is a tool by Belkasoft that allows for fetching various artifacts of Instant Messenger from an attached memory image".

Forensics MemDump Extractor (https://www.techipick.com/forensics-memdump-) "is a tool developed by Gem George to extract any kind of files residing in memory dump based on file signature".

WindowsSCOPE Cyber Forensics (http://www.windowsscope.com/product/windowsscope-cyber-forensics-trial/) "is a comprehensive toolkit for capturing and analyzing of Windows physical and virtual memory targeting cyber analysis, forensics/incident response, and education".