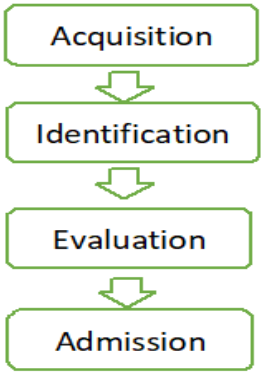
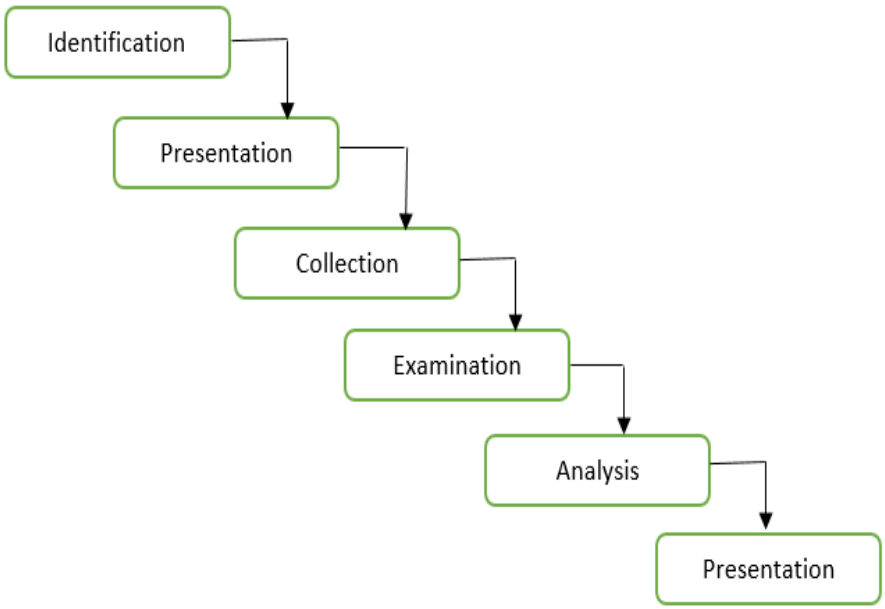
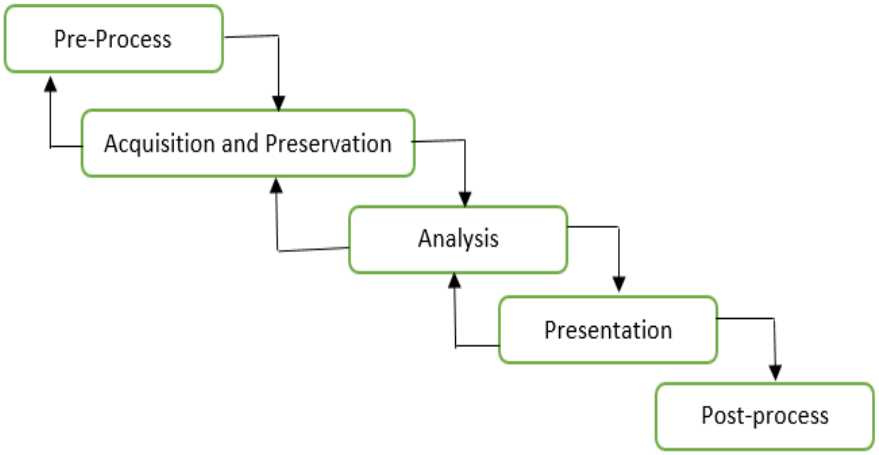
Book 5 - Digital Investigation Techniques and Tools

1. Digital Forensic Techniques and Tools

<table>
<tr><td colspan="2">Scope</td></tr>
<tr><td>Number</td><td>1</td></tr>
<tr><td>Title</td><td>Digital Forensic Techniques and Tools</td></tr>
<tr><td>Introduction</td><td>Digital forensic technologies and tools are developed to capture digital evidence, investigate digital devices and perform relevant network analysis. As such, the analysis and investigation encompass hard and soft components of digital devices. Although the number of the proposed processes and models are varying, this chapter introduce the commonly shared processes, models and standards for digital forensics to inform on how, where, and when to appropriately apply the proper model and tool.</td></tr>
<tr><td>Outcomes</td><td>At the end of this Module you should be able to:
• Understand the concept of digital forensic process;
• Demonstrate good knowledge of the common forensic techniques and tools;
• Apply a systematic approach to an investigation using forensic techniques and tools;
• Identify the main advantages and disadvantages of common forensic techniques;
• Demonstrate clear understanding of network forensic analysis.</td></tr>
<tr><td>Topics</td><td>- Introduction
- Digital Forensic Process
- Digital Forensic Models
- Digital Forensic Techniques and Tools
- Digital Forensic and Network Analysis</td></tr>
<tr><td>Study Guide</td><td>Instructions on how to study this unit:
• Required study time:
You should plan to spend approximately 25 hours studying this unit. You may find it convenient to break up your study as follows:
<table>
<tr><th>Activity</th><th>Time</th></tr>
<tr><td>Preparation</td><td>3 hours</td></tr>
<tr><td>Content Review</td><td>1 hour</td></tr>
<tr><td>Set Textbook Content</td><td>1 hours</td></tr>
<tr><td>Software/Hardware Review</td><td>8 hours</td></tr>
<tr><td>Thinking (Review questions, MCQs):</td><td>5 hours</td></tr>
<tr><td>Tutorial</td><td>2 hours</td></tr>
<tr><td>Related Course Work</td><td>5 hours</td></tr>
<tr><td>Total</td><td>25 Hours</td></tr>
</table>
• Required hardware/software:
✓ Digital Forensics Lab.
✓ Microsoft Internet Explorer version 5 or higher.
• Required external resources including links and books:
✓ E- Library.</td></tr>
</table>

Content	
Section Number	1.1
Section Title	**Introduction**
Introduction	This Section introduces digital forensic investigation and equipment for the reader with fundamental understanding for digital forensics. The subsequent sections present a selected number of digital forensic models and tools to be reviewed. The reviewed tools and models are chosen to present the state of art of the current digital forensic models and tools.
Content	Gathering digital evidence from computers, networks, and storage media has become a vital weapon against different types of software and hardware attacks and forbidden threats. Generally, the practice of collecting, analyzing and reporting digital evidence in a way legally admissible in court is known as digital or computer forensics and the experts who practice this kind of science are known as forensic examiners. However, the acquisition, analysis, and reporting of the digital evidence depends on the nature of the crime scene, types of available evidence and the digital forensic tools employed. As there are loads of data and events encounter certain digital evidence, digital forensic examiners may apply different type of digital forensic techniques and tools. On the other hand, the accumulative number of digital activities using different kinds of digital devices have tightened and complicated the process of analyzing and the cleanse of target data. As such, evaluating digital forensic evidence is not an easy task due to the following reasons: ☐ The lack of clear and relevant data. ☐ The time required for sifting through the evidence data sets. ☐ The constant change of the network data, cloud data, digital media devices. ☐ The realistic measurement of the false alarm versus the detection rate as well as the capability of detecting new or hidden events. ☐ The manipulation of features and data attributes.

Content	
Section Number	1.2
Section Title	**Digital Forensic Process**
Introduction	Forensic examiners use scientific methods to identify and extract digital evidence. Forensic examiners generally follow clear information and communication technologies based forensic process and technique based on well-defined procedures.
Content	The following Figure 1 illustrates the common phases of digital forensic process.  Figure 1. Digital Forensic Process **Acquisition phase** At this stage, an approval must be obtained in order to acquire the evidence. In addition, a detailed description of the data sources shall be provided and presented. As such, software or hardware Write Blocking tools can be used to ensure that the image of the evidence drive cannot be modified during investigation. **Identification phase** At this stage, the format of the evidence need to be moderated to human readable format. The evidence data sets shall be normalized and cleaned to be further used. The usage of cleaned evidence can be tangible using software tools or logical for the analysis of case. However, the format of evidence depends of the relevant evaluation of the evidence. For example, if the evaluation is human based then the evidence should be human readable and if the evaluation is computer based then the evidence should be computer readable format. **Evaluation Phase** At this stage, an evaluation on the prearranged evidence will take place in order to decide whether the acquired evidence is relevant to court case or not. As such, the evaluation step should ensure that the collected evidence is sound and reproducible. **Admission Phase** At this stage, the acquired evidence shall be documented such that to make sure that the give evidence data is actually readable and acceptable in the court of law. Relevant reporting format can be followed and to be contingent to the case.
Content	
Section Number	1.3
Section Title	**Digital Forensic Models**

Introduction	At the early beginning, the general investigation process was proposed. Later, number of investigation models were introduced. However, forensic examiners generally follow valid and case pertinent forensic procedure.
Content	The straightforward forensic model as defined in the Digital Forensics Research Workshop known as DFRWS [1] investigation model is comprised of six phases as per the following in Figure 2.  Figure 2. DFRWS Investigation Model [1] In addition to the above, there are a good number of proposed investigation models. As an example of these models, the following Figure 3 illustrates the Generic Computer Forensic Investigation Model [1].  Figure 1. Generic Computer Forensic Investigation Model [1]
Content	
Section Number	1.4
Section Title	**Digital Forensic Techniques and Tools**
Introduction	Forensic examiner needs to learn as many forensic techniques and tools as possible. Although there are very common techniques and tools, it is almost mandatory for the forensic examiner to have hands on the most common forensic techniques and tools. The following section presents the most common digital forensic techniques and tools.
Content	**Forensic Techniques**

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. The common forensic techniques used during computer forensic investigations are described and discussed below.

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 software tools used for data recovery. Generally, these tools can be used in two forms: in-place and read-only recovery. In in-place data recovery, the forensic tool can be used to repair or fix the error on the disk drive were as in 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 tools can be used to analysis and compare the information found on multiple hard drives. This type of forensic investigation can be used in different type of intrusion detection such as anomaly and host-based intrusion detection.

3. Live Forensics

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

In the environment where time-efficiency is required, the forensic process should deal with active and runtime threats. As such, web and packet capture forensics allow for live and instant forensics. Live forensics is useful when we would like to deal with the threat on the spot. However, in live forensic we still follow the same procedures and steps such as identifying and analyzing the threat with instant response time. Therefore, this method can be used to construct defense line.

4. File Forensics

Files forensics is very important and extensively used technique 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

In order to determine the file details such as to determine whether the file is an executable or not executable, it is important to analyze the details of the file. This method reveals what an attacker may hide irrespective to the format of the file. On the other hand, filtering known, and unknown files help investigators to ignore irrelevant files. Generally, this method makes the investigation process faster.

- String Searching and File Fragments

This method is helpful as it allows the investigator to locate data that may be relevant to the case or have evidential value. Searching for special sequence of character may speed up the investigation process. However, it is of great important to properly choose the keywords and strings in the proposed search. For example, if you want to look for a file that contains sample of power supply adapter, avoid using the term "sample" in your search; instead,

focus on "adapter" as you might have other files containing the word "sample," while very few files include "adapter"

- File Carving

File carving is a method used for searching and reconstructing deleted materials from the known file headers and other means such as the contents and by using statistical methods. In general, as the deleted file content is located in the unallocated space of the drive the operating systems may lose portion or control on the entire content. However, by extracting meaningful content and structured data, we can still recover files especially when the file directory or entry is totally corrupted.

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 defense 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. Recovering password can be achieved by cracking the password. 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 tools, 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. .

Forensic Tools

Forensic tools development is growing rapidly at educational and private sectors. The developers aim to produce an ultimate special purpose forensic tool. As such, there are many open and closed source forensic tools exists for direct use. Generally, forensic examiners use well-known, specialized and reliable forensic tools for clear and reliable forensic evidence acquisition.

The major 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.

Although forensic tools perform similar function, the difference between traditional and time specific forensic tools is the response time which make it suitable for the environment were active response forensic tools is required. However, hardware and software based forensic tools generally perform the following main functions:

1- Acquisition. Such as and not limited to:
- Physical and logical data copy
- Data acquisition
- Command-line acquisition
- GUI Acquisition
- Remote acquisition
- Verification

2- Validation. Such as and not limited to:
- Hashing

- Filtering
- Analyzing headers

3- Extraction. Such as and not limited to:
- Keyword searching
- Data Viewing
- Decompressing
- Decrypting
- Bookmarking
- Carving

4- Reconstruction. Such as and not limited to:
- Disk-to-disk copy
- Image-to-disk copy
- Partition-to-partition copy
- Image-to-partition copy

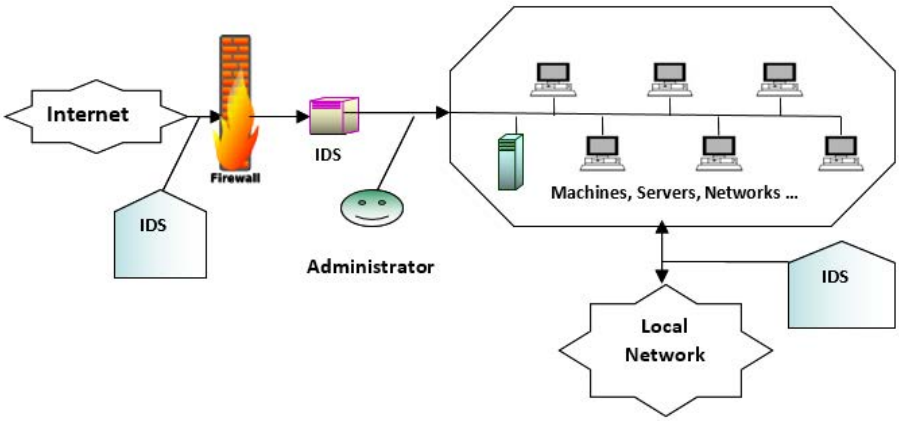
5- Reporting. Such as and not limited to:
- Log report
- Report generator

The following table surveys the most common digital forensic tools. The tools are discussed in terms of features and relevant operating platform.

Table 1. Forensic Tools

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
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

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

Content	
Section Number	1.5
Section Title	**Digital Forensic and Network Analysis**
Introduction	Digital forensic analysis describes the process of the cleaning and presenting of digital evidence. For example, steganographic analysis on stored files can be used to acquire steganographic contents. These contents are data and information of an actual data storage device like the hard drive. By comparing a large volume of stenographic contents, forensic examiner can exclude data files, which are not correlated to the forensic case. Therefore, the number of interpreted evidence-based data files are small and has greater significance as compared with the larger volume of data files being examined. Enterprise Forensic Toolkit software like FTK and Encase can be used to compare the data files signatures and derive comparative evidence. The following section present the most common network analysis tools and techniques for digital forensics.
Content	With the growth of the Internet, the location of data files become associated with the local network and the Internet in general. Therefore, external threats started to increase rapidly and badly. As a solution, Intrusion Detection Sensors (IDS) are very popular security and network analysis tools used for detection and protection of host and network intrusions. The following diagram in Figure 4 illustrates the conventional IDS deployment.  Figure 4. Conventional IDS Deployment [2] The main functions of Intrusion detection systems include: ☐ Detect and protect against host and network-based intrusions; ☐ Monitor system and network activities; ☐ monitor operating systems logs and application programs; ☐ Alert network administrators against suspicious network activates; ☐ Provide detailed reports about the network status; ☐ Evaluate host and network configurations; ☐ Monitor legitimate system activities; ☐ Provide defense in depth monitoring system. The deployment of IDS technologies has introduced new strength for the security of information systems. Generally, Intrusion detection sensors are classified as:

	Network based intrusion detection sensors Typically, a network-based IDS process system activity based on network data and make a decision to evaluate the probability of action of these data to decide whether these activities are normal or intrusion. Network intrusion detection sensors are associated with monitoring events occurring on computer network usually by capturing and analyzing network packets. As such, the basic function of is to analyze and detect any attempts to compromise the confidentiality, integrity, availability, or to avoid security measures of computer network. **Host based intrusion detection sensors** Host-based IDS scans resources on the host machines for security related information such as application logs, system activities, and file system modification logs. **Signature Intrusion detection systems** Signature-based IDS looks for specific signatures that match a known attack scenario. This approach is successful of detecting attacks of previously known signatures i.e. detecting against known attacks. **Anomaly intrusion detection systems** Anomaly-based IDS work on the notion that any intrusive usage behavior deviates enough from normal system usage behavior. This is also meaning that a threshold can be established for normal profile, and any deviation from the threshold is considered as anomalous. Usually this approach is for detecting unknown attack signatures. Deploying the IDS main engine for actual network connection would result in many benefits such as reducing false negative, understanding of an attacks severity, and increasing the detection accuracy. Moreover, anomaly and Denial of Service (DoS) detection can be combined together; as they both work to find any abnormal events in the network traffic flow which will add defense mechanisms against new attacks i.e. newly arising attacks. However, most of the new security systems recommend the deployment of combined and specialized sensors at various network locations according to the security necessity and needs.

Activity	
Number	1.1, 1.2, 1.3
Title	Introduction and process models
Type	Review questions
Aim	To discuss and understand the concept of digital forensic investigation.
Description	1- Discuss how computer forensics and data recovery may or may not refer to the same activity? 2- Determine the resources needed for digital investigation. 3- Compare between the phases of digital computer forensic models in term of similarity and requirements.
Timeline	One Hour
Assessment	Classroom discussion

Activity	
Number	1.4
Title	Digital Forensic Techniques and Tools
Type	Research and reflection questions
Aim	To exhibit and apply different computer forensic tools in digital investigation.
Description	1- What are the main function for computer forensic tools? 2- Search for and download two open source and popular forensic tools, and write a short report on the tools main functions. Illustrate with examples. 3- A father called to report that his 10-year-old son has run away from school. He has access to his son's e-mail inbox and reported that a number of e-mails reveal that his son was in contact with former young female teacher. Write a short report on how to proceed and provide clear roadmap to digitally investigate the case. 4- Create an image for one of your own flash drives without creating the possibility of accidentally damaging the drive contents. Create directory listings of all files in the image and show bit-by-bit image of the device including deleted files and slack space data. Write a report show the entire process followed.
Timeline	3 Hours
Assessment	Lab discussion

Activity	
Number	1.5
Title	Digital Forensic and Network Analysis
Type	Review Questions
Aim	To discuss and understand network forensic analysis.
Description	1- Differentiate between the following terms: - Anomaly and misuse intrusion detection sensors - Host-based and network intrusion detection sensors 2- Explain the terms false positive and false negative for intrusion detection and which one is dangerous and why?
Timeline	One Hour
Assessment	Classroom discussion

Think Template (MCQs)	
Number	1.3, 1.4, 1.5
Title	Digital forensics and network analysis
Type	Choose correct answer
Question	1. The digital forensic process consist of: a) Acquisition of data b) Identification of evidence c) Evaluation and Admission d) All of the mentioned 2. ... can be considered as systematic tracking of incoming and outgoing traffic and it is crucial when developing data map of digital evidence. a) SIM Cards b) Network Forensics c) Drive Slack d) Win Registry 3. During investigation we refer to logical drives which means we refer to the system … a) SIM Card b) EEPROM c) PDA's d) Partition 4. … gives us a road map to data on a disk. a) SIM Card b) EEPROM c) PDA's d) File system 5. … is a database that stores hardware and software configuration information, network connections, user preferences, and setup information. It can contain valuable info about current/past applications and user created information. a) SIM Card b) EEPROM c) Windows Registry d) File system 6. Unused space in a cluster between the end of an active file and the end of a cluster. (Includes RAM and file slack) a) Drive Slack b) EEPROM c) Windows Registry d) File system 7. … are areas of files and disks data that are not apparent to the user, and sometimes not even to the operating system. a) Hidden data b) Missing data c) Exceptional data d) File system data 8. Which tool is needed for computer forensic examiner job? a) WireShark b) Snort c) Encase d) Depend on the forensic case, forensic examiner may use several well-known tools for single forensic case. 9. What are major components of IDS? a) Analysis Engine b) Event provider c) Alert Database

	d) All of the mentioned 10. What is the common approach to classify an IDS? a) Zone based b) Host & Network based c) Network & Zone based d) Level based 11. What are characteristics of anomaly based IDS? a) It models the normal usage of network as a noise characterization b) It doesn't detect novel attacks c) Anything distinct from the noise is not assumed to be intrusion activity d) It detects based on signature 12. What is major weakness of anomaly based IDS? a) These are very slow at detection b) It generates many false alarms c) It doesn't detect novel attacks d) None of the mentioned 13. What are characteristics of signature based IDS? a) Most are based on simple pattern matching algorithms b) It is programmed to interpret a certain series of packets c) It models the normal usage of network as a noise characterization d) Anything distinct from the noise is assumed to be intrusion activity 14. What are weaknesses of signature based IDS? a) The ability to detect novel attacks b) They generate false alarms c) They have to be trained again for every new pattern to be detected d) All of the mentioned 15. What are characteristics of Host based IDS? a) The host operating system logs in the audit information b) Logs includes logins, file opens and program executions c) Logs are analyzed to detect tails of intrusion d) All of the mentioned 16. What are weaknesses of the host based IDS? a) Unselective logging of messages may increase the audit burdens b) Selective logging runs the risk of missed attacks c) Very fast to detect patterns d) Originally programmed for new patterns 17. What are strengths of the host based IDS? a) Attack verification b) System specific activity c) No additional hardware required d) All of the mentioned 18. What are characteristics of Network based IDS? a) They look for attack signatures in network traffic b) Filter decides which traffic will not be discarded or passed c) It is programmed to interpret a certain series of packet d) It models the normal usage of network as a noise characterization 19. What are strengths of Network based IDS? a) Cost of ownership reduced b) Malicious intent detection c) Real time detection and response d) All of the mentioned
Answers	1. The digital forensic process consist of: d) All of the mentioned 2. ……can be considered as systematic tracking of incoming and outgoing traffic and it is crucial when developing data map of digital evidence. b) Network Forensics

	3. During investigation we refer to logical drives which means we refer to the system … d) Partition 4. … gives us a road map to data on a disk. d) File system 5. … is a database that stores hardware and software configuration information, network connections, user preferences, and setup information. It can contain valuable info about current/past applications and user created information. c) Windows Registry 6. Unused space in a cluster between the end of an active file and the end of a cluster. (Includes RAM and file slack) a) Drive Slack 7. … are areas of files and disks data that are not apparent to the user, and sometimes not even to the operating system. b) Missing data 8. Which tool is needed for computer forensic examiner job? d) Depend on the forensic case, forensic examiner may use several well-known tools for single forensic case. 9. What are major components of IDS? d) All of the mentioned 10. What is the common approach to classify an IDS? b) Host & Network based 11. What are characteristics of anomaly based IDS? a) It models the normal usage of network as a noise characterization 12. What is major weakness of anomaly based IDS? b) It generates many false alarms 13. What are characteristics of signature based IDS? a) Most are based on simple pattern matching algorithms 14. What are weaknesses of signature based IDS? d) All of the mentioned 15. What are characteristics of Host based IDS? d) All of the mentioned 16. What are weaknesses of the host based IDS? a) Unselective logging of messages may increase the audit burdens 17. What are strengths of the host based IDS? d) All of the mentioned 18. What are characteristics of Network based IDS? a) They look for attack signatures in network traffic 19. What are strengths of Network based IDS? d) All of the mentioned

Extra	
Number	1
Title	Digital forensic techniques and tools
Topic	1.2, 1.3, 1.4, 1.5
Type	• Book/Chapter (ISBN) 1- A Practical Guide to Computer Forensics Investigations, Pearson publishing 2015. ISBN-13: 978-0-7897-4115-8 ISBN-10: 0-7897-4115-6 2- Computer Network Intrusion Detection: An Integrated approach using self-organizing maps and fuzzy cognitive maps. LAP LAMBERT Academic Publishing 2011. • Offline content (Full reference) 1- Common phases of computer forensics investigation models, International journal of computer science and information technology (IJCSIT), Vol 3, No 3, June 2011. 2- A Survey about network forensic tools, International journal of computer and information technology (ISSN: 2279-0764). Volume 2 - Issue 1, January 2013 3- Network Forensic Frameworks: Survey and research challenges. Digital Investigation 7 (2010) 14-27. 4- Comparative analysis of digital forensic models, Journal of Advances in Computer Networks, Vol. 3, No. 1, March 2015. • Online content (URL) - https://niccs.us-cert.gov/ - https://resources.infosecinstitute.com/

2. Digital Forensics Evidence Acquisition

Scope Template	
Number	2
Title	Digital Forensics Evidence Acquisition.
Introduction	Digital evidence become important as non-digital one in nowadays crimes, computer systems holding digital evidence have two states, "live" if the computer is running, and "dead" if the computer is shut down at the moment responding investigator approaching. Each state of them has different methods of data acquisition. This topic provides the reader with knowledge about different methods of data acquisition.
Outcomes	1. Reader will be familiar with different states of computer systems holding digital data. 2. Reader will have knowledge about different methods of data acquisition for each computer state.
Topics	* Introduction * Simple File Copying * Dead Box Approaches * Live Box Approaches
Study Guide	Instructions on how to study this unit. • Required study time is 4 hours. • Required hardware: PC, Hard drives, Tableau SATA/IDE Bridge Hardware and write blocking device. • Required software: Upcopy, Robocopy, FTK Imager, Raptor Forensics Boot Operating System, -Response Enterprise, TrueCrypt, X-Ways Capture, Vmware

Task	**Time**
Preparation (Introduction and On-line Planning):	1hr
Disk-based Content:	2.5hrs
Set textbook Content:	1
Thinking (On-line discussions, Review questions)	1hr
Tutorial Work:	2.5hrs
*Related Course Work:	1hrs
Total	**09 hours**

Content Template	
Section Number	2.1
Section Title	Introduction.
Introduction	This section is an introductory to the digital evidence acquisition discipline, objectives of this section are: 1. Introduce challenges of evidence acquisition. 2. Introducing major steps of evidence acquisition process. 3. The main digital evidence acquisition approaches will be studied in this chapter.
Content	Digital evidence is information of value to an investigation that is stored and transmitted in a digital form. Digital evidence may be found in magnetic storage media such as hard disks, floppy disks, flash drives, random access memory (RAM). The challenge faces the investigator is to know where to look for the digital evidence and what digital information is most important to the investigation in order to appropriately collect it. Since digital evidence can be altered or damaged easily, through improper handling during collection or examination. Creating a working copy of the examined data is critical. It is always preferable to work on a copy, or a forensic image, than touch the original storage media to prevent changing the original evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. There is no single procedure for collecting evidence, investigator must use a suitable methodology to acquire digital evidence depending upon the type of digital evidence, the type of investigation, where the evidence located, and whether the suspect has been already identified The investigator should know which tool to use in order to identify and capture the evidence without losing its integrity and value. There are several steps involved in acquiring the evidence as outlined in the following list: • Identification: is an important step that preceding evidence collection. In identification step key people involved in the case and best sources of potential evidence are identified. Investigator needs extensive knowledge of computer hardware and software, including operating systems, file systems, and cryptographic algorithms. Evidence has to be identified among normal files, and may be found in slack space, unallocated space, registries, hidden files, encrypted files, password-protected files, system logs, etc. Evidence can be found on any number of media sources such as hard drive, floppy disk, CD-ROM, PDA, cell phones, flash drives. Search for evidence should also consider physical evidence in a non-digital format that may be of value e.g. notebooks, pieces of paper with potential passwords • Collection/Preservation: The identified evidence has to be collected from available components. The use of computer may cause loss of valuable information so the collection of evidence must not be delayed. It is critical to make identical copy of the original evidence by making an exact bit-by-bit copy using special "forensic" software and/or hardware. The imaging process is intended to copy all blocks of data from the investigated to the practitioner's target device, a full bit-for-bit copy is the preferred forensic process. The created file called a forensic image file and it can be in various formats, including .AFF, .ASB, .E01, and.dd or raw image files, and virtual image formats

such as .VMDK and .VDI. Evidence could be altered easily while the copy is being made. The imaging utility must not introduce new data into the original evidence or the copy. Creating a forensic image is accomplished using a hardware write protection device (See Figure 2.1), which can be described as an adapter that connect a hard drive through a USB cable to a computer. Hardware write protection devices prevents modifications to the evidence hard drive, since the device only allows data to be read from the evidence source. The investigator must be able to prove in court that the copy is a valid one, and show that the imaging process is repeatable.

Figure 2.1 Tableau SATA/IDE Bridge Hardware write blocking device (Adapted from: URL Wikipedia, https://en.wikipedia.org/wiki/Forensic_disk_controller).

- Transportation and Storage: All the recovered evidence from the investigated system should be physically secured. The package contains the evidence has to be sealed to prove that it has not been tampered with during transportation.

A chain of custody document must be associated with every piece of evidence. Chain of custody is a process used to maintain and document the chronological history of the investigation. The chain of custody tracking document for a piece of evidence records information such as who handled the evidence, what procedures were performed on the evidence, when the evidence was collected and analyzed, where the evidence was found and is stored, why this material was considered as evidence, and how the evidence collection and maintenance was done. Maintaining a chain of custody of the evidence collected is crucial to protect the integrity of the evidence and argue that the evidence was not tampered while in custody.

The acquisition of digital evidence has different implications and objectives as compared to the method of seizure and preservation of non-physical evidence. One of these differences is that, some evidence will be lost, for example, if a running computer is shut down, all memory contents will be lost., The investigator must make a choice of an acquisition method. Depending upon the goals of the investigation, specific measures in data acquisition must be taken. Investigators should be aware of options of evidence seizure. As to the best method to seize electronic evidence, it is up to the investigator to decide

	which method is most reasonable when approaching the computer systems at each scene. Each case is different. Each computer system configuration is different. The totality of the circumstances at the time will determine which method will be a reasonable choice. In next sections you will be introduced to Simple File Copying method of collecting evidence data. Dead box approaches of collecting data on turned off evidence computer, and Live box approaches of collecting data on running computers.

<table>
<tr><td colspan="2">Content Template</td></tr>
<tr><td>Section Number</td><td>2.2</td></tr>
<tr><td>Section Title</td><td>Dead Box Acquisition</td></tr>
<tr><td>Introduction</td><td>Evidence computers can be turned off ("Dead Box") or running computers ("Live Box") at the time responding investigators approaching, each case has different data acquisition method. This section objectives is to

1. provide reader with knowledge of data acquisition methods of dead box analysis.

2. provide reader with knowledge about the data acquisition tools of dead box.</td></tr>
<tr><td>Content</td><td>If the investigation includes a turned off computer, the investigator should copy the hard drive using write-blocker device without turning the device on.

Creating a dead box image is accomplished using a hardware write protection device, which can be described as an adapter that connect a hard drive through a USB cable to a computer. hardware write protection devices prevents modifications to the evidence hard drive, since the device only allows data to be read from the evidence source.

In conjunction with hardware write blockers, forensic analysts use applications specifically developed for creating forensic images. Table 2.1 lists several examples of commonly used imaging software applications

Table 2.1 Examples of Software Developed to Create Forensic Images of Media

<table>
<tr><td>FTK Imager</td><td>http://www.accessdata.com</td></tr>
<tr><td>Encase Forensics</td><td>http://www.guidancesoftware.com</td></tr>
<tr><td>X-Ways Forensics</td><td>http://www.x-ways.net</td></tr>
<tr><td>ProDiscover</td><td>http://www.techpathways.net</td></tr>
<tr><td>Guymager</td><td>http://guymager.sourceforge.net/</td></tr>
<tr><td>SMART Linux</td><td>http://www.asrdata.com</td></tr>
<tr><td>Macquisition</td><td>http://www.blackbagtech.com</td></tr>
</table>

Most of these forensic imaging applications can also be used on a live machine if necessary. Figure 2.2 shows an example of FTK Imager from Accessdata, which can create forensic images with hardware write blockers in the ‘dead box’ approach as well as be able to capture volatile memory and hard drive imaging from a live machine.</td></tr>
</table>

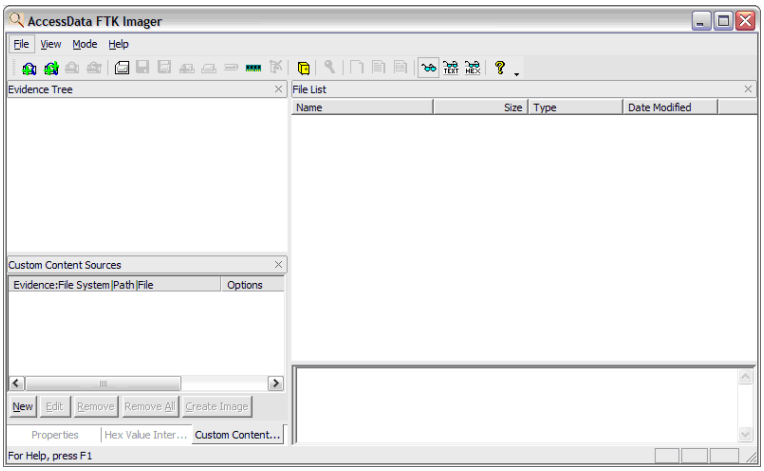


Figure 2.2 FTK Imager from Accessdata, dialog box for creating an image of physical media (http://www.accessdata.com).

<table>
<tr><td colspan="2">Content Template</td></tr>
<tr><td>Section Number</td><td>2.3</td></tr>
<tr><td>Section Title</td><td>Live Box Acquisition</td></tr>
<tr><td>Introduction</td><td>Data resides in live box computer systems continuously changes by operating system and running applications or by interacting users. Objectives of this section is to

1. provide student with knowledge of data acquisition methods of dead box analysis.

2. provide student with knowledge about the data acquisition tools of dead box.</td></tr>
<tr><td>Content</td><td>Decision of the appropriate data collection method must be taken without any delay in the case of approaching a running computer system ("Live box"), as the operating system in addition to the open applications changes the data on the evidence drives and physical memory. Depending upon the needs of the investigation, the order of capturing different volatile has to be decided, and even the order of volatility has to be taken into account to capture data before it vanishes while you are capturing other data, for example, the data in the physical memory has different volatile order, for example, data resides in Random Access Memory ("RAM") volatile in nanoseconds, due to changes occurs in RAM by the operating system and running applications or by interacting user with the system. On the other hand, data resides in hard drives volatile for indefinite time.

Live acquisition involves collecting volatile data information, where live acquisition involves capturing memory as an image file.

Obtaining volatile physical memory may best be conducted with batch files or scripts to automate the process. Table 2.2 lists several applications suited for physical memory acquisition can be used by investigators, before RAM acquisition is conducted, investigator must try to determine the operating system and use the suitable software or use a software that suitable for any OS. It is not a good practice to try several software tools during live acquisition. A trusted software tool should be used, otherwise the integrity of the evidence is violated and will not be accepted in the court.

Table 2.2 Examples of Physical Memory Acquisition Tools
<table>
<tr><td>X-Ways Forensics</td><td>http://www.x-ways.net</td></tr>
<tr><td>X-Ways Capture</td><td>http://www.x-ways.net</td></tr>
<tr><td>ProDiscover</td><td>http://www.techpathways.net</td></tr>
<tr><td>FTK Imager</td><td>http://www.accessdata.com</td></tr>
<tr><td>Winen</td><td>http://www.guidancesoftware.com</td></tr>
<tr><td>Mdd</td><td>http://www.sourceforge.net/projects/mdd/</td></tr>
<tr><td>Memoryze</td><td>http://www.mandiant.com</td></tr>
</table>

Since the standard amount of RAM in personal computers now commonly ranges from 4GB to 32GB and higher, the amount of data contained therein is substantial, and the relevance of this data to investigation is very high, such</td></tr>
</table>

as list of programs ran in this session or may contain decrypted data (if data on hard disk is encrypted).

Given this amount of memory, it is also known that intruders have the ability to install rootkits or malicious software (malware) within RAM and that the code to these malware program will only execute in memory. By not capturing the physical memory, it is likely never to be known if a malware existed only in RAM, or created files on the disk.

If a malware exists in the system, it is possible that this same malware will interfere with forensic applications used to examine and acquire memory dump. An example of such case is when a malware disguises its existence by altering "running program list" and remove its process from the list. a solution to minimize malware interference during a live acquisition of memory or hard drive can be by acquiring the data remotely. Remote acquiring is conducted by connecting a forensic workstation to the suspect machine via a network or network cable, forensic applications can be run on the trusted forensic workstation rather than the suspect machine. Although typically, a small amount of code from the forensic program needs to be installed onto the suspect machine, the actual forensic applications will be run on the trusted machine, thereby reducing the amount of modifications to the suspect computer and risk of interference from the evidence system.

A unique and effective utility to facilitate this process is F-Response (http://www.f-response.com). F-Response allows examiners to connect their forensic workstations to suspect machines remotely. The connection to the suspect machine is Read-Only, in that the forensic examiner cannot modify the suspect machine's data (other than the changes that are made naturally by the suspect's operating system). Using F-Response, the hard drive(s) can be imaged as can the Physical memory.

As F-Response simply (yet ingeniously) provides a secure and Read-Only connection, it does not have the functionality to acquire data. This is an intentional feature not supplied as the forensic examiner can use virtually any application to acquire data through the F-Response connection. The ease of accessing systems remotely with F-Response can be seen in Figure 2.3.

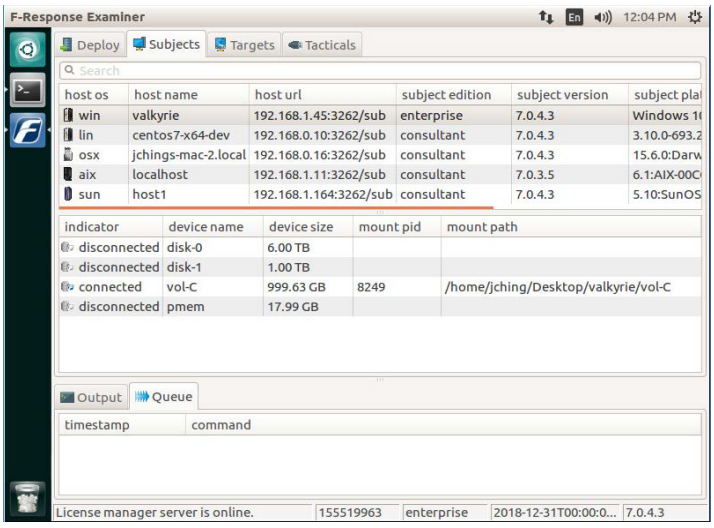


Figure 2.3 F-Response Enterprise, http://www.f-response.com.

Data encryption that is suspected or known to be employed can prevent acquisition of some or all of the data. Data encryption can encompass one or more files, folders, volumes, partitions, or even the entire hard drive. If an image is created of an encrypted file or hard drive, the decryption key will be needed to decrypt and analyze the encrypted data. Without the decryption

key, the likelihood of recovering the encrypted data may be slim to none, depending upon the complexity of the encryption and decryption key.

Encryption programs, such as VeraCrypt seen in Figure 2.4, are plentiful and freely available on the Internet. VeraCrypt gives any computer user the option to encrypt their entire operating system or a specific container of files. Commercial products, such as the Microsoft Operating System, also offer full disk encryption as part of the operating system.

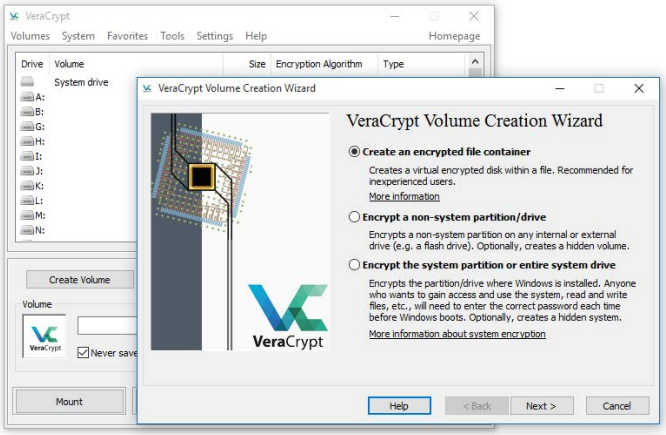


Figure 2.4 VeraCrypt, http:// www.veracrypt.fr.

Other operating systems, such as Linux, generally allow the user to encrypt their entire system or individual files as well. There are few operating systems that do not come with encryption programs by default. Any system that does not come with encryption programs by default most likely is able to have third party encryption programs to be used.

Ignoring encryption possibilities on a suspect computer will eventually lead to extremely short forensic examinations because when encrypted, there is little that can be done to examine an encrypted system without the decryption keys. You can assume that nearly any live system can be encrypted, either in whole or part, as many current operating systems include encryption as a system feature. There are also countless encryption programs that are freely available to accomplish encryption. the live acquisition of RAM may help sense it may contain decryption keys.

With full disk encryption, once the computer has been shut down, the decryption key will be needed, otherwise, it could take weeks or years to decrypt, with the possibility of being virtually unable to decrypt. Several forensic applications, such as X-Ways Capture seen in Figure 2.5, can be run on the investigated computer to not only determine if encryption is employed, but to also image the system's physical memory and subsequently, the evidence hard drive(s) should encryption be detected on the live system.

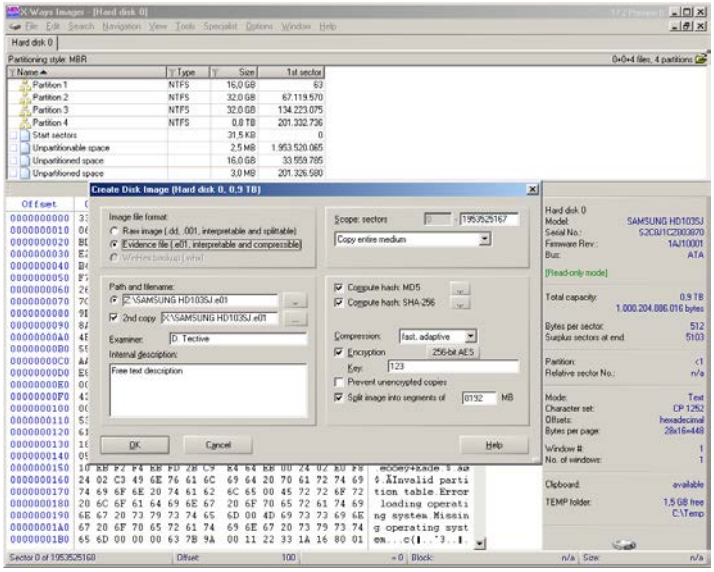


Figure 2.5 X-Ways Capture, http://www.x-ways.net.

As described so far, the clock continues to tick away when investigated computers are running and choices are being weighed. Yet another factor that can literally add hours to the process and modify the evidence even more are applications that may be running on the suspect machine. Commonly used programs, such as word processing programs, are not so much the concern as are other programs.

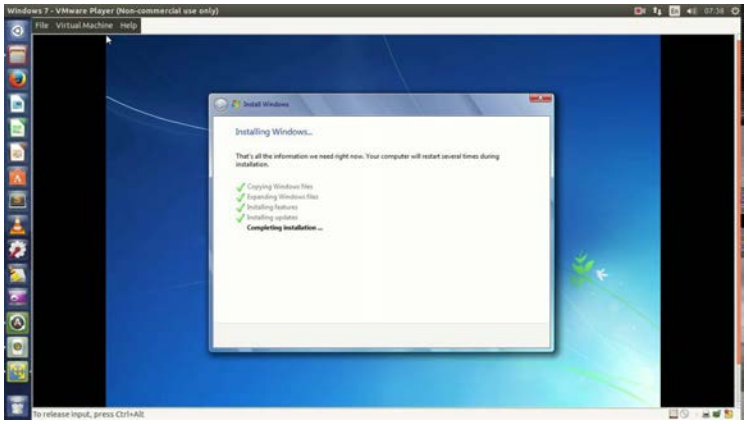
Data wiping programs that may be open are a serious concern and need to be addressed quickly to prevent evidence destruction by shutting the computer down immediately. Virtual machine applications also pose a problem, if a virtual machine is running on your evidence system.

Virtual machine applications, such as developed by Vmware (http://www.vmware.com) and VirtualBox (http://www.virtualbox.org), allow for entire operating systems to be operated as guest systems within the host operating system. As an example, a computer with a physical hard drive running Microsoft Windows, can also run the VirtualBox application which can run a separate operating system as a guest system, or several simultaneous guest systems. The guest operating system maintains its own data within its own files. In effect, an examiner that approaches a running suspect machine that is seen to have a running virtual machine on the desktop now has to decide acquisition methods of two systems.

The guest virtual machine will have many of the same considerations of data collection as the host machine. It is possible to temporarily suspend the virtual machine operating systems with some types of virtual machine applications such as vmware, storing the physical memory in file. This stored physical memory can be examined as if it were imaged. Other virtual machine applications do not suspend or store physical memory, which gives the investigator more difficult decisions on how to proceed.

Given the nature of a virtual machine containing all its data internally, it is conceivable that all evidence needed for the investigation could be contained solely within the virtual machine and not exist on the host system. This evidence could consist of Internet history, running processes, or email. The collection of a running virtual machine from a running suspect computer increases the risks of system crashes, lost data, and altered data.

However, this is expected and unavoidable and the investigator must make a decision based on the facts of that particular situation. Figure 2.6 shows an

	Ubuntu host operating system with a Windows 7 guest virtual system. The approach to this one system is actually an approach to two individual systems.  Figure 2.6 Ubuntu "host" and Windows 7 "virtual machine guest." Other problematic programs and processes that will interfere in the collection of evidence include peer-to-peer networking applications, open remote connections, active file deletion or file copying, and active program installations. Closing some programs, such as Internet Explorer, may cause user created data to be written to the drive, which may be beneficial to the examination. Some applications may lose data when they are closed on a running system. Each of these can contribute to a substantial loss of pertinent electronic evidence and create obstacles to the investigator's process of collection. All of the choices made will require explanations in reports and may be testimony for the choices made. Right or wrong, you have to make a decision based on what you know at the time.

Activity Template	
Number	2.2
Title	Use of FTK Imager
Type	Reflection
Aim	The aim of this activity is to be familiar with FTK Imager.
Description	Student is provided with a USB stick of small size such as (64 MB), and then he asked to execute the following steps: 1. copy some files to the USB stick. 2. format it using quick format. 3. Create an Image using FTK Imager. 4. Check the hashes for the Images. 5. Locate the files on the USB image.
Timeline	1.5 hour.
Assessment	assessment is based on execution of the required steps.

Activity Template	
Number	2.3
Title	acquire image of data using hardware write blocking device
Type	Reflection
Aim	The aim of this activity is to be familiar with imaging using write blocking devices.
Description	Student will be provided with a small size USB stick and he will be asked to acquire an image using a hardware write blocker.
Timeline	1 hour.
Assessment	assessment is based on successful execution of acquiring an image using hardware blocker (by comparing hash value)

Activity Template	
Number	2.4
Title	Acquiring image of data using F-Response
Type	Reflection
Aim	The aim of this activity is to be familiar with F-Response software which a tool of Live box data acquisition method.
Description	Install F-Response and use it to image a workstation hard drive.
Timeline	1 hour.
Assessment	Checking the hash values.

Think Template (MCQs)	
Number	2.1
Title	Introduction
Type	Choose correct answer
Question	Digital evidence can be found in:
Answers	* RAM * Keyboard * CD-Rom drive Correct answer: Ram

Think Template (MCQs)	
Number	2.2
Title	Simple File Copying
Type	Fill in the blanks
Question	Simple file copying is not advised since it will alter the ..... of the files.
Answers	* metadata * content * type * size Correct answer: metadata

Think Template (MCQs)	
Number	2.3
Title	Dead Box Approaches
Type	• Rank options
Question	Rank the following steps in order to image a dead box computer using a forensic boot USB
Answers	*Change the BIOS boot order of the hard drive to the last *Unplug all hard drives cables *Connect USB boot drive *Reconnect the hard drive, and boot the system to your forensic disk. *Change the BIOS boot order of the USB to the first *Run the computer and check that the forensic USB boots *Save your changes, exit, and shut down the computer Correct answer: *Unplug all hard drives cables *Change the BIOS boot order of the USB to the first *Change the BIOS boot order of the hard drive to the last *Save your changes, exit, and shut down the computer *Connect USB boot drive *Run your computer and check that the forensic USB boots *Reconnect the hard drive, and boot the system to your forensic disk.

Think Template (MCQs)	
Number	2.4
Title	Live Box Approaches
Type	• Match Pairs
Question	Match the following software tools with appropriate functionality
Answers	Software List: * F-Response * TrueCrypt * X-Ways Functionality List: * Data Encryption * Acquire encrypted unlocked volumes * Remotely Imaging Correct Answer: * F-Response: Remotely Imaging * TrueCrypt: Data Encryption * X-Ways: Acquire encrypted unlocked volumes

Extra Template	
Number	2.1
Title	Placing the Suspect Behind the Keyboard.
Topic	Digital Forensics Evidence Acquisition.
Type	ISBN: 978-1-59749-985-9

Extra Template	
Number	2.2
Title	Handbook of Digital Forensics and Investigation
Topic	Digital Forensics Evidence Acquisition.
Type	ISBN: 978-0-12-374267-4

3. Internet Investigation

Scope Template	
Number	3
Title	Internet Investigation.
Introduction	This chapter entitled "Internet Investigation", is an introductory chapter about the application of digital forensics to the internet. Section one is a revision about the internet and networking terms, and it describes how the internet works. The reader can find the definition, types of internet crime, and the dangers of internet crime in section two. Internet investigation requires the detective to collect and document digital evidence which is discussed briefly in section three. Using domain IP tools, OSINT, cashed web pages repositories, deep and dark web as investigation tools are explained with examples in section four. The internet user as regular user or investigator sometimes needs to access the internet anonymously, how to work anonymously and what does it mean are discussed in section five. Finally, in the last section of this chapter you can find an introduction about the importance of internet security and some tips and techniques to avoid and prevent possible internet crimes and internet security issues.
Outcomes	1. Explain the web and internet terms. 2. Explain the importance if the internet security and safety. 3. Identify the source of digital evidence, and what are the correct methods and steps to collect the evidence. 4. Use a collection of free tools to extract information from the internet. 5. Use a collection of free tools, and some methods to work hidden on the internet and avoid the internet crimes.
Topics	1. How does the internet work? 2. Introduction to Internet Crime. 3. Collecting and Documenting Digital Evidence. 4. Using Internet Investigation Tools. 5. Working Hidden on the Internet. 6. Internet Crimes Prevention.
Study Guide	Instructions on how to study this unit. • Required study time: 13 Hours. • Unit comprehensive reading. • Refer to external resources for more details such as the references appeared in the text • You are required to have a PC or laptop with internet connection and web browser to be able to try the examples and do the activities. • You are required to install an anonymous browser like Tor, Epic, Comodo Dragon or SRWare iron.

Content Template	
Section Number	3.1
Section Title	How does the internet work?
Introduction	This section gives introductory information about the internet. At the beginning of the section, we define the web and the internet and show the importance of using the internet. The section also describes some aspects and requirements of establishing connection between the host and the server like IP, protocols and DNS services.
Content	Using internet applications has become one of the regular days activities to a large number of people. For example, checking electronic mail, or post some ideas on social network pages, or manage your bank account and more. So, the internet becomes very important for almost everybody. Suppose you have an electronic device such as personal computer or smart phone, and you used it to access your Facebook page that stored on some device somewhere, then your device becomes a part of the internet. In another word, the internet is a collection of billions of electronic devices connected to each other's to exchange information. Your device plays a client role to fetch information and use services from other devices which play server role on the internet. In addition to the client and server there are a lot of devices and software needed to complete the connection between the client and the server. The World Wide Web which shortly called the web is one of the most important applications of the internet. The web is the collection of websites we can access through the internet like www.googl.com, www.youtube.com, www.facebook.com, www.ptuk.edu.ps etc. Different websites have different purposes and was built for specific reason. Simply the purpose of the web could be anything such as online banking, education, social media and electronic newspaper and more. In short, the web is a collection of files and data stored on some device called server that can be accessed from another device called a client through the internet to read, update, save or delete some of the files or data according to the client privileges. Each electronic device connected to the internet should have its unique address to identify it and give it an address to be accessed from the other devices. If a device on the internet wants to send a message to another device, then it should use the IP address to label the message with in order to reach to its destination.

Content Template	
Section Number	3.2
Section Title	How does the internet work?
Introduction	This section gives introductory information about the internet. At the beginning of the unit, we define the web and internet and show the importance of using the internet. The section also describes some aspects and requirements of establishing connection between the host and the server like IP, protocols and DNS services.
Content	When the client wants to take a service from a server, then it sends a request message to the server. Any message should contain the destination IP address and the source IP address. So the request should be labeled by the IP address of the server as destination IP address and the client IP address as the source IP address. When the server send its response to the client labeled by the server IP address as source IP address and the client IP address as the destination address. But when we want to access a website, we simply type the web site address on the web browser, so what happen. In fact, there is a distributed data base keeps the IP addresses it its corresponding hostname called DNS. Therefore when we ask a website using its host name, the domain name will be translated to IP address using the DNS then complete the request using the IP address. (Kurose and Ross, 2012) The message should pass through the transmission medium and interconnecting devices, and that needs a special treatment on client while sending as well on the severer while receiving. A collection of rules called protocols known a TCP/IP protocol stack is responsible to make any transformation on the message as necessary to be transmitted and received to its destination successfully. (Sheldon, 1997) In brief, the internet is collection of interconnected devices over the world. The main objective of the internet is exchanging the information between the interconnected devices. The interconnected devices use several hardware and software to accomplish the communication and exchange the information between them using client/server architecture.

Content Template	
Section Number	3.3
Section Title	Introduction to Internet Crime
Introduction	By reading this section, the reader will be able to define the internet crime and list its elements. In addition, this section discusses the different internet crimes classes based on its elements, targets, and objectives.
Content	The internet crime is any criminal activity using the internet as the communication medium, this crime could be very simple such as illegal download for a music file, or it could be very serious such as illegal accessing bank accounts and steel millions of dollars (Arora, 2016). According to (Arora, 2016) the internet crimes categorized into three classes. First, internet crimes target the individuals. Second, internet crimes target the property. Finally, internet crimes targets government, organizations or society. The internet crime where the victim is a person behind the target device is a crime against individual. In this type of crimes individual persons are affected. For example, if a person is cheated by fishing e-mail to get some information, or his system hacked and the hacker gets some personal files from the victim device. The aim of this type of crimes is harming the others personally like blackmail the victim, or squeezing him to do something. In other words, any user of the internet is exposed to the internet crime and be one of the internet crimes victim, in this case we could classify the crime into crime against individual (Arora, 2016). The internet crime against property, on the contrast of the crime against individual this type of crimes targets the property its aim to exploit, damages the resources over the internet. For example, if someone theft an internet access from his neighbor then this behavior comes under crimes against property. In conclusion, crimes against property target resources available on the Internet, not the individuals themselves(Arora, 2016). But what about the third class of the internet crimes. Suppose an attack targets government web site, and sensitive information were stolen, then this attack classified under the third class. Steeling users' information like password, credit card numbers and other information by hacking some organization servers is another example of the third class. Another example of this class of crimes is denial of service attack (Arora, 2016).

Content Template	
Section Number	3.4
Section Title	Collecting and Documenting Digital Evidence
Introduction	Each investigation requires collecting, storing and analyzing evidence. This section explains, in brief, the digital evidence, where we can find the digital evidence, how to collect the evidence, how to store the evidence correctly, and how to analyze them.
Content	Usually the digital evidence is related to the electronic crimes. However, digital evidence could be use in the investigation in any crime. For example, suspect's digital devices such as his/her PC, mobile phone and digital camera may contain very important information that can help the investigators to track and study the suspect behavior. For example, the suspect's digital devices may contain his location at the crime time or his activities before and after the crime and more. Digital evidence can be extracted from almost any electronic device such as computer hard drive, flash card in a digital camera and mobile phone even if the user deletes the files or clears the data from his electronic device. Digital forensic investigators use a variety of methods and tools to discover, collect, reserve, analyze and present the evidence found on the digital devices to be used as digital evidence. (Casey, 2011) The activities that the investigators should follow in the collecting and documenting the digital evidence is listed in the following:("Digital Evidence and Forensics," https://www.nij.gov:443/topics/forensics/evidence/digital/pages/welcome.aspx (accessed 3.1.18).) • Try to access the device that used in the crime. • Collect the data from the device as much as possible while the devise still on in the crime scene; because some data may no longer available once the device is shut down. For example, we should collect the live data like RAM and connections. • Unplug the device or remove the battery. • Label each part and document the model and serial number of the device. • Take all the storage devices and hard driver and packing them with antistatic evidence bag. • The evidence should not be changed in any way at any step. • Everything should be documented.

Content Template	
Section Number	3.5
Section Title	Collecting and Documenting Digital Evidence (cont.)
Introduction	Each investigation requires collecting, storing, analysis evidence. This section explains, in brief, the digital evidence, where we can find the digital evidence, how to collect the evidence, how to store the evidence correctly, and how to analyze them.
Content	After the evidence is collected from the suspect device, the digital forensics examinershould handle the evidence as following: • Identifying the relevant evidence i.e. the data that is related to the crime. • Preserving the evidence using the most accurate method suitable to the type of data and device. For example, we may make multiple copies of the evidence. Another example we may use read only storage device to store a copy of the evidence. • Analyze the evidence. For example using the metadata as analyzing method. • Presenting the evidence at the court room using the suitable presentation tools such as screen audio system etc.

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools
Introduction	This section discusses the importance of the internet as a source of information about crimes, and show how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cached Web pages repositories, and Deep and Dark web.
Content	The internet contains a lot of information. Using the proper searching techniques and tools, we can get very useful information even if this information is protected in some level. For example, we can search online databases using some information about a suspect or victim, and then try to retrieve all related data about him to be used later in the analysis step to find possible evidence. Search engines like Google and AltaVista could be used as online investigation tool. It could be used to search and find messages, e-mail and forum post of the suspect. In this section we are going to talk about three of internet investigating tools. Domain and IP tools, opens source intelligence, Cashed websites repositories and dark web **Domain and IP Tools** An online database such as Whois services is an example of a rich source of online information. Whois services can be used to have some information about the domain and domain owner (Casey, 2011). We can also know the IP address of the domain and then use this IP to know the location of this IP, the owner name and some other information, or we can use the IP to identify the location of the website or service visitors. Example: using www.whois.com to get some information about the domain www.wt-elite.net. The retrieved information is shown in Table 3.1 and Table 3.2 :

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools.
Introduction	This section discusses the importance of the internet as a source of information about crimes and shows how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cached Web pages repositories, and Deep and Dark web.
Content	

Table 3.1 Domain Information Retrieved Using Whois

DOMAIN INFORMATION	
Domain	wt-elite.net
Registrar	Domain.com, LLC
Registration Date	2016-03-05
Expiration Date	2019-03-05
Updated Date	2018-02-18
Status	clientTransferProhibited clientUpdateProhibited
Name Servers	ns1.ipage.com ns2.ipage.com

Table 3.2 : Domain Registrant, Administrative and Technical Contact Details Retrieved Using Whois

	REGISTRANT CONTACT	ADMINISTRATIVE CONTACT	TECHNICAL CONTACT
Name	Yazeed Sleet	Yazeed Sleet	Yazeed Sleet
Organization	Yazeed Sleet	Yazeed Sleet	Yazeed Sleet
Street	Ibn-Sena	Ibn-Sena	Ibn-Sena
City	Jenin	Jenin	Jenin
State	NA	NA	NA
Postal Code	201	201	201
Country	PS	PS	PS
Phone	+1.7259727930	+1.7259727930	+1.7259727930
Email	yazeed_sleet@yahoo.com	yazeed_sleet@yahoo.com	yazeed_sleet@yahoo.com

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools.
Introduction	This section discusses the importance of the internet as a source of information about crimes, and show how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cached webpage repositories, and the deep and dark web.
Content	In the previous example the registrant, administrative and technical contract have the same information, some other domains may have different information for each. Try this example using some domain names you know. The website and mobile application developers can collect and document the user activities including the user IP address, access date and time, visited and used services and more. The DNS service in responsible to map a domain name to its associated IP address, so this is an example of online database. So we can get the IP address that is associated to a domain easily using many online available services like http://www.domaintoipconverter.com/ by providing the domain name we get the IP address. Another way to get IP address of a domain is using the nslookup command. Gets the IP address of a domain using nslookup command. 1. Start the command prompt. 2. Type nslookup and press enter. 3. Type the domain name you that you want to get its IP address like www.*****.com and press enter. Using the IP-Based geolocation, we can get the ISP (internet service provider), latitude, longitude, region, city and country of the internet connected device using its IP address, we can also get the name of the IP owner if the IP address is fixed or if the address associated with a domain. Several geolocation databases are available online like IP2loaction, DB-IP, MAxMind and IPlocation. Some of the geolocation databases are free for use and some are paid. Most of these data bases provide the websites and mobile applications developers with API to enable them to integrate the IP-Based Geolocation service with the application they develop.

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools.
Introduction	This section discusses the importance of the internet as a source of information about crimes and show how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cashed Web pages repositories, and Deep and Dark web.
Content	Example2: using the IP address to find the approximate location of the client or the hosting server of a website. 1. Find the IP address of any domain you want, or find your own IP address by search on google using "get my ip". 2. Choose any IP-Based Geolocation database, for example use www.iplocation.net and type the IP address in the search field. The webpage will display the geolocation information of the IP from several databases. Another related service to IP address is tracing email to find its source IP address. Tracing email source requires having the email header. Getting the email header method and steps depends on the email service provider, but it is simple method, you can go to the help of your email service provider and find the steps to get the email header. You can search for the email source using online databases like IPlocation (https://www.iplocation.net/trace-email) by pasting the email header in the search field.

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools.
Introduction	This section discusses the importance of the internet as a source of information about crimes and shows how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cashed Web pages repositories, and Deep and Dark web.
Content	• Open Source Intelligence (OSINT) Open source intelligence is another example on online databases; it is a collection of data produced from public available information. Open source intelligence contains variety type of data such as video, photos and articles from a variety of sources such as social media pages, commercial websites, educational websites and other sources.(George and Kline, 2006; Richelson, 2015) Let us go through an example to show how we can use OSINT as investigation tool. Suppose you have a Facebook profile, you can find the comments in which he was mentioned in, to do this you apply the following steps: 1. Get the profile URL. You can do it simple by search the Facebook for a profile, then open the profile and go to URL address and coy it. 2. Find the profile ID and copy it. You can find the profile ID by going https://lookup-id.com/ and paste the profile URL in the search box and press lookup button. 3. Now you can search for different things using this ID, in this example we want to search for the comments in which the profile owner was mentioned in. to do this go to www.uk-osint.com and select Facebook option, then paste the profile ID in the search box, then press "search for articles your subject is mentioned in ". In other words, Open source intelligence is an online database collected from different sources in different time. In this section we just show one example of OSINT but there are another examples and OSINT sources. You can find several OSINT source on (https://osintframework.com).

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools.
Introduction	This section discusses the importance of the internet as a source of information about crimes and shows how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cashed Web pages repositories, and Deep and Dark web.
Content	**Cashed Web pages Repositories** Website content can change frequently, but there are some services which make copies of the websites or web pages and save them in archive called cached web pages. In this section we will not discuss the caching processes and mechanism; we will show an example of using these services in the following. Suppose you want to know what was on a website, or how the website was look like. You can search cashed Web pages archive for that webpage. In this example we will use Waybak Machine which it is available online on https://web.archive.org. By visiting this site you can search the archive by typing the website you want in the search box. The Wayback will retrieve all the snapshots of the websites grouped in year, month and day, then simply by clicking on the day you want the website of your search will be displayed as it was in day you select. In conclusion, you can explore the history of a website by searching for its cashed web pages even if the website is no longer operating. There are several providers for cashed Web pages archives such as Google, Wayback Machine and archive-it. You may find some of websites are not archived before, or not archived in specific day.

Content Template	
Section Number	3.6
Section Title	Using Internet Investigation Tools.
Introduction	This section discusses the importance of the internet as a source of information about crimes, and show how some tools can be used to extract useful information from the internet. The tools that are discussed in this section are Domain and IP tools, Open Source Intelligence cashed Web pages repositories, and Deep and Dark web.
Content	**Deep and Dark Web** When we use regular search engines and web browsers, we can explore only the surface web. Surface web is the web content that is indexed by search engines, and it can be accessed regularly using any web browser like Google Chrome, Firefox etc. (Dragut et al., 2012) The opposite of the surface web is the deep web. The deep web is the web content that is not indexed by the search engines. Therefore, it will not appear in the search results. Webmail, paid services and the password protected services are examples of deep web.(Dragut et al., 2012) There is also another category of the web content called dark web. The dark web is a part of the deep web, but it cannot be accessed using regular web browsers. The dark web uses the internet connection to connect its users and services, but not all the internet users can access its content. It uses special networks like peer-to-peer network, Tor network, I2P network, and it requires the user to be anonymous on the internet to be able to access the dark. In section 3.7 we will discuss and show how to access the dark web while discussing how to work hidden on the internet.

Content Template	
Section Number	3.7
Section Title	Working Hidden On the Internet
Introduction	This section talks about tracking the internet users in terms of how it is done and what type of activities is tracked, the dangerous and importance of user tracking. In addition, in this section the reader will learn the importance of working hidden on the internet by prevent tracking his activities and information using some available tools for this purpose like regular internet browsers, special internet browser, or change his browsing behaviors.
Content	Working hidden or anonymously on the internet is very useful and very important to stop tracking, detecting and storing your activities on the internet. Browsing history is an example of tracking your activities on the internet. For example, when the you use the web browser to access a website, the web browser save in the history log the visited web pages, the visit time, and some information you may entered in a form. The browser also save some text files coming from a website called cookies. The cookies are used by websites to store information on the client machine about the user like his preferences, last visit time etc. to be used later when the user revisit the website again. There are many tool and techniques to prevent tracking the user. For example, to avoid history log and cookies, you can simply going "incognito" while browsing the internet. In addition to incognito browsing mode there are other simple methods to top tracking the user like deleting all the cookies after finish web browsing, configure the browser to stop sending the location data, stop Google tracking when the user is logged in using his Google account, use anti-tracker tools and disable java and plugins. Using these tools will not make you anonymous, it just stop recording you activities. To work completely hidden on the internet you need to use one an anonymous browser like Tor, Epic, Comodo Dragon and SRWare iron.

Content Template	
Section Number	3.7
Section Title	Working Hidden on the Internet.
Introduction	This section talks about tracking the internet users in terms how it is done and what type of activities is tracked, the dangerous and importance of user tracking. In addition, in this section the reader will learn the importance of working hidden on the internet by prevent tracking his activities and information using some available tools for this purpose like regular internet browsers, special internet browser, or change his browsing behaviors.
Content	Tor browser is a very useful open source tool to enable the user to work completely anonymous on the internet. Tor consists of two parts, the web browser and special encrypted networks. When a client machine sends a request to a web server using Tor browser, the browser does not send the web traffic to the target directly instead it routes the traffic within the Tor network then to the final destination. The connections between the Tor browser and the Tor network and within the Tor network devices are completely encrypted. As a result, using Tor tool will keep your activity and IP address anonymous on the internet. The Tor installation package is available on the Tor web site (https://torproject.org) for free. Download the suitable package for user operating system, install it and start using internet anonymously.(Alvin, 2017) We already discussed the dark web previously, and find that the dark web is an anonymous web and it requires the user to be anonymous in order to be able to access its content. So, to access the deep web content we can use Tor tool. Now we need to find the interesting web site on the dark area of the web, but unfortunately, we cannot find it using regular search engines like Google as we discussed before. We know also that the dark web content belongs to some network does not mean it belongs to another, in this example we are going to see how to access the deep web services within the Tor network. You can easily find many websites domain names of a dark web of the Tor networks on https://thehiddenwiki.org which display large number of domain names grouped into categories with a short description beside each domain name. There are also some search engines you can use to search in the dark web of the Tor network like "not Evil" available on [https://hss3uro2hsxfogfq.onion.to]. Select the domain you want and visit it using Tor. In conclusion working hidden on the internet is not very difficult task with Tor network. You can simply download, install and start surfing the web completely anonymously. In addition to work hidden on the internet using Tor, you can access the dark web using Tor.

Content Template	
Section Number	3.8
Section Title	Internet Crimes Prevention
Introduction	In this section the reader will find the importance of using tools and methods to protect his privacy while surfing the internet to avoid the internet crimes. In this section we list a collection of security tips that the user should follow to keep his data and activities on the internet protected.
Content	We already discussed in this chapter the internet crimes and clarified its definition, types and dangerous. Internet security and defending internet crimes is a wide area of digital forensic and has many tools and methods. In this section we are going to show in brief how we can prevent the internet crimes. Using the suitable and updated internet security tools and methods keep the personal and business private information protected from the internet attacks like illegal data access, illegal data modification, phishing, denial of service attacks and man in the middle attacks. Therefore, we need to use internet security tools and methods to be able to browse the internet and use its services securely. In the following a list of possible internet security tips you can follow to keep your data and behavior on the internet protected. ▪ Review the privacy policy carefully of any service or program you are going to use and ask about anything that is not understood before accepting it. ▪ Do not rush during programs installation by clicking next button. Read every message in the installation steps before clicking next to avoid accepting something or granting some privileges to the program that could be used to threaten your privacy or granting. ▪ Keep the operating system and programs updated. Check for update periodically if the automatic update feature is not implemented and enabled in the program.

Content Template	
Section Number	3.8
Section Title	Internet Crimes Prevention.
Introduction	In this section the reader will find the importance of using tools and methods to protect his privacy while surfing the internet to avoid the internet crimes. In this section we list a collection of security tips that the user should follow to keep his data and activities on the internet protected.
Content	▪ Disconnect all the connectivity while they are not in use. ▪ Use trusted antivirus system. ▪ Use trusted Firewall, and configures it carefully depending on usage and location of network and internet. Some of internet security tools provide the user with antivirus and Firewall in the same application. ▪ Uninstall unnecessary and unused programs and plugins. ▪ Maintain backup of your data and system settings periodically and keep them in a protected location and storage. ▪ Check and review the security settings of your accounts and services, and be sure you understand each one of the security settings and how it will affect your account and privacy before setting it. ▪ Use strong password and change it frequently of at most every 90 days. Strong password should not be driven from known information about you like your birth-date, your sun first name etc. Strong password should be at least 14 characters length and contains upper-case letters, lower-case letters, symbols, numbers and spaces. ▪ Working hidden on the internet as introduced and explained in a previous section.

Activity Template	
Number	3.1
Title	How the internet works.
Type	The student is required to conduct research about the web and internet technologies and the client/server architecture.
Aim	After completing this activity, the student will be able to define the client, server, DNS, ISP, and website, and will be able to explain how these components are collaborating to provide the web services.
Description	In this activity the student is required to write a report that explain how we can have an internet connection and what will happen since we type a website URL till display the website on the browser.
Timeline	• Find and collect the required references and resources such as books and journal. • Find and summarize the related information required to accomplish the report. • Report writing. • This activity will require about six hours.
Assessment	Thisactivity will be assessed based on: • The completeness. • The correctness. • The overall quality. • The followed process.

Activity Template	
Number	3.2
Title	Find domain information using online databases
Type	In this activity the student will use the online databases to retrieve domain information to reflect what was he learns about the online databases and domain information.
Aim	This activity aims to train the student to use some online databases and highlights the importance of such that databases in general and in gathering domain information in specific.
Description	The student should choose three domains at least and two online databases. The student should retrieve the domains' information and compare the results. One comparison among the information retrieved by one database about the chosen domains. And one comparison among two sets of information retrieved by different databases about one domain.
Timeline	This activity will require about one hour.
Assessment	This activity will be assessed based on: • The completeness. • The correctness. • The overall quality. • The followed process.

Activity Template	
Number	3.3
Title	Find the Geolocation of a domain.
Type	In this activity the student will use the DNS service and Geolocationdatabases to get domain IP address and find the approximate location of the domain.
Aim	This activity aims to train the student to use DNS service, and Geolocationdatabases to find the IP address corresponding to the domain and find the location of the IP address.
Description	• The student should choose three domains, and then find its corresponding IP addresses. He should find the locations of the domains in addition to the domains' ISP information. • The student is required to find his machine public IP address, and then use the IP to find his location.
Timeline	This activity will require about one 40 minutes.
Assessment	This activity will be assessed based on: • The completeness. • The correctness. • The overall quality. • The followed process.

Activity Template	
Number	3.4
Title	Internet crimes investigations using OSINT.
Type	The student required to do a research to find some example of OSINT usage in the internet crimes investigations.
Aim	This activity aims to train the student to use OSINT as a source of information and evidence in the internet crimes investigations.
Description	In this activity the student is required to find and write down three internet investigation cases in which we can use OSINT as a source of information. Then, the student should demonstrate to use OSINT in each example.
Timeline	This activity will require about 2 hours.
Assessment	This activity will be assessed based on: • The relevance of the example to the internet crimes. • How the student interacts with the OSINT. • The used OSINT and its suitability to the example it was applied to. • The completeness. • The correctness. • The overall quality. • The followed process.

Think Template (MCQs)	
Number	3.1
Title	How does the internet work?
Type	Choose correct answer
Question	The communication protocol used by the internet is:
Answers	A. HTTP B. www **C. TCP/IP** D. FTP

Think Template (MCQs)	
Number	3.2
Title	How does the internet work?
Type	Choose correct answer
Question	A host on the internet find another host by its:
Answers	A. Postal Address **B. IP Address** C. Electronic Address D. None of the above.

Think Template (MCQs)	
Number	3.3
Title	Introduction to Internet Crime.
Type	Choose correct answer
Question	To be considered a computer crime, what needs to be involved in the crime?
Answers	A. Technology **B. Computers** C. Data D. Networks

Think Template (MCQs)	
Number	3.4
Title	Using Internet Investigation Tools
Type	Choose correct answer
Question	What is the deep web?
Answers	A. The Internet resources that need a subscription to be accessed. B. Information on local database servers that cannot be accessed by the internet. **E. The Internet resources that cannot be indexed by popular search engines** C. A + C

Think Template (MCQs)	
Number	3.5
Title	Using Internet Investigation Tools
Type	Choose correct answer
Question	What kinds of information are commonly invisible to popular search engines?
Answers	A. Webpages that contain only images **F. Webpages skipped on purpose by search engine crawlers** B. Webpages assembled dynamically from online database content C. None of the above

Think Template (MCQs)	
Number	3.6
Title	Internet Crimes Prevention
Type	Choose correct answer
Question	Firewalls are used to protect against:
Answers	A. data driven attacks B. fire attacks C. virus attacks **D. unauthorized access**

Extra Template	
Number	3.1
Title	Computer Networking: A Top-Down Approach
Topic	1. How does the internet work?
Type	Book: Kurose, J.F., Ross, K.W., 2012. Computer Networking: A Top-Down Approach, 6th edition. ed. Pearson, Boston. (ISBN: 978-0-13-285620-1)

Extra Template	
Number	3.2
Title	Encyclopedia of Networking, Electronic Edition
Topic	1. How does the internet work?
Type	Book: Sheldon, T., 1997. Encyclopedia of Networking, Electronic Edition. McGraw-Hill Osborne Media, Berkeley. (ISBN: 978-0-07-882333-6)

Extra Template	
Number	3.3
Title	Exploring and analyzing Internet crimes and their behaviours
Topic	2. Introduction to Internet Crime
Type	Journal Article: Arora, B., 2016. Exploring and analyzing Internet crimes and their behaviours. Perspect. Sci., Recent Trends in Engineering and Material Sciences 8, 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

Extra Template	
Number	3.4
Title	Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet
Topic	3. Collecting and Documenting Digital Evidence
Type	Book: Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press. (ISBN: 978-0-08-092148-8)

Extra Template	
Number	3.5
Title	Digital Evidence and Forensics
Topic	3. Collecting and Documenting Digital Evidence
Type	Online Resource (Web Page): https://www.nij.gov:443/topics/forensics/evidence/digital/pages/welcome.aspx (accessed 3.1.18).

Extra Template	
Number	3.6
Title	Intelligence and the National Security Strategist: Enduring Issues and Challenges
Topic	4. Using Internet Investigation Tools
Type	Book: George, R.Z., Kline, R.D., 2006. Intelligence and the National Security Strategist: Enduring Issues and Challenges. Rowman & Littlefield. (ISBN: 978-0-7425-4039-2)

Extra Template	
Number	3.7
Title	The U.S. Intelligence Community
Topic	4. Using Internet Investigation Tools
Type	Book: Richelson, J.T., 2015. The U.S. Intelligence Community. Avalon Publishing. (ISBN: 978-0-8133-4919-0)

Extra Template	
Number	3.8
Title	Deep Web Query Interface Understanding and Integration
Topic	4. Using Internet Investigation Tools
Type	Book: Dragut, Eduard C., Dragut, Eduard Constantin, Meng, W., Yu, C.T., 2012. Deep Web Query Interface Understanding and Integration. Morgan & Claypool Publishers. (ISBN: 978-1-60845-894-3)

Extra Template	
Number	3.9
Title	Tor Browser: Secrets of the Deep Web, How to Stay Anonymous Online, and Surf the Web Like a Hacker
Topic	4. Working Hidden On the Internet
Type	Book: Alvin, C., 2017. Tor Browser: Secrets of the Deep Web, How to Stay Anonymous Online, and Surf the Web Like a Hacker. CreateSpace Independent Publishing Platform. (ISBN: 978-1-5471-5184-4)

4. Introduction to Database Forensics

Scope Template	
Number	4
Title	Introduction to Database Forensics
Introduction	This chapter provides the reader with an overview of database forensics. This chapter will review the importance and aims of digital forensics, database threats, database threat control methods, database security in the web environment, database attack analysis, and data recovery.
Outcomes	• Understand the importance of investigation of data found on database management systems that might provide evidence of digital crime. • Understand the possible database threats. • Apply some database threats control methods. • Use database tools as forensics tools to detect and analyze possible database attacks. • Understand the relationship between the database servers and the web environment, and how they are affect each other in term of the security. • Understand the importance of database backup and recovery, and how to apply them if an attack is occurred.
Topics	• Introduction. • Importance and Aims of the Database Forensic. • Database Threats. • Database Threats Control Methods. • Detecting and Analysis Database Attacks using Digital Forensics Tools. • Database Security in the Web Environment. • Data Backup and Recovery.
Study Guide	Instructions on how to study this unit. • Required study time: 13 Hours. • Unit comprehensive reading. • Refer to external resources for more details such as the references appeared in the text • You are required to have a PC or laptop to be able to try the examples and do the activities. • You are required to install a DBMS.

Content Template	
Section Number	4.1
Section Title	Introduction
Introduction	This section is about the definition of the database forensics, and it shows the structure of the chapter.
Content	The Database is a collection of data and data about data saved on a computer hard drive. Using database systems provide the developer with a very useful functionalities and benefits in order to be able to manage the data in sophisticated manner such as authentication, concurrency control , data integrity and data consistency.(Malik and Patel, 2016) Database forensic could be defined as the applying the digital forensic techniques and tool to investigate and study the database content and its metadata to find who changed the database, what data was changed and when. In the introduction we said that the data is saved on the computer hard drive, but when applying the digital forensic techniques in the database filed, live analysis should be taken in the consideration to examine the server RAM.(Al-dhaqm et al., 2017) This chapter gives the reader an overview about the database forensics. This chapter reviews the importance and aims of digital forensic, the database threats, the database threats control methods, database security in the web environment, the database attacks analysis and data recovery.

Content Template	
Section Number	4.2
Section Title	Importance and Aims of the Database Forensic
Introduction	In this section, the reader will find a review and general information about the database systems and database applications. This section also tries to highlight the importance and aims of digital investigation and database forensics.
Content	Most of the computing applications contains database which contains very important and sensitive information about the users and enterprise such as university academic portal, online Human Resource Management systems of a company and online baking etc. therefore the data base like a treasure for the hackers, in fact it could be considers as the final destination of the most digital attacks. (Malik and Patel, 2016) As introduced in this section the database provides the application with the data store, so we can find the database in the web-based applications, the desktop applications and the mobile applications. The developer creates and manages the database using one of the available Database Management Systems like ORACLE, MySQL and SQL Server. Therefore, the database plays different roles depending on the type and behavior of the whole application, and it uses different technologies based on the DBMS. Based on the variance of database uses and technologies there are several security issues and attacks. Therefore, we should be concerned about the database security issues to be able to detect, identify, analysis, prevent them and to collect the attacks details of it is occurred. In conclusion, database systems and applications store sensitive and private information like bank-account information. Database security aims to protect the database system from any attack and restore the database, while the database forensic aims to analyses and investigate the database systems if an attack was occurred to find when the attack was occurred, what did the attack do, who is behind the attack, and to revert any an authorized data manipulation operation.

Content Template	
Section Number	4.3
Section Title	Database Threats
Introduction	This section is dedicated to give an overview of the database threats. After reading this section, the reader can define the database threats, categorize the threats based on which part of the database is affected, and give some examples of database threats.
Content	Any database system should provide data privacy, data integrity and data availability. The dataprivacy means that only the authorized users and systems are allowed to see the data, while the integrity means that only the authorized users and systems are allowed to modify the data. The database should be available and ready to serve the authorized users and systems and allow them to perform the interaction any time the need to do and this is what we called data availability of the database. In conclusion, any digital activity affects or violates the data privacy, data integrity or data availability of the database systems will be treated as database threat(Ali and Afzal, 2017).

Content Template	
Section Number	4.4
Section Title	Database Threats
Introduction	This section is dedicated to give an overview of the database threats. After reading this section, the reader can define the database threats, categorize the threats based on which part of the database is affected, and give some examples of database threats.
Content	In addition to the main database threats categories we described, there are some other database threats as listed in the following(Ali and Afzal, 2017)(Malik and Patel, 2016)(Chandrashekhar et al., 2015): • Some database threats could be occurs when an authorized user is granted database privileges that exceed the user job requirements. • Illegal changing the granted privileges to the higher privileges level. • Exploiting the operating system vulnerabilities to gain an unauthorized access to the database. • Exploiting the Database management systems (DBMS) vulnerabilities and misconfiguration. • Sending and executing unauthorized database query which is called SQL injection. • Denial of Service Attack (Dos Attack). • The database backup storage media threats. • Weak authentication and logging policies. In conclusion, there are several types and categories of the databases threats such as threats against data privacy, data integrity and data availability that could affect the database system directly. And there are some threats that affect the database systems indirectly such as attacking the operating system, the database backup media and network.

Content Template	
Section Number	4.5
Section Title	Database Threat Control Methods
Introduction	This section talks about the importance of using control methods to avoid threats. In addition, this section gives some examples of available tools and methods the database manager can use to avoid some types of threats.
Content	Database should be private and modifiable by only the authorized users and systems and that what we have discussed so far in this chapter. Therefore, the database should provide some methods to control user and systems access. The database systems provides such that tools called access controls which determines the types of users, the credential and privileges of individual user or group of users which reflect the enterprise database access policy. Enterprise database access policy should be clear, describes the actual access privileges needs like file access permissions (create, read, update and delete), program execution permissions and data manipulating permissions(Malik and Patel, 2016). Design and implement the database system and its application in such a way to record the database activities such as when a user was logged in, what is his IP address, the operating system, who insert, delete and update the data. Also, we can use the log file of the DBMS which record some of the database activity. The database activity records could have very useful information in the database forensic. Data encryption on the storage media or on the communication media between the client and server is an essential control method of the database threats. By data encryption we ensure that the data is only readable by only the users who have the encryption key to achieve the data privacy of the database(Malik and Patel, 2016).

Content Template	
Section Number	4.6
Section Title	Database Threats Control Methods
Introduction	This section talks about the importance of using control methods to avoid threats. In addition, this section gives some examples of available tools and methods the database manager can use to avoid some types of threats.
Content	Because the database systems and applications are running on the network environment, we should control the network threats that hit the database. There are many useful tools that could be used to control network threats and server threats and protect them from the unusual activities. Such these tools are called Intrusion Detection Systems (IDS). IDS have two main categories the network intrusion detection system and host intrusion detection system. NIDS is used to monitor the traffic on the network, while the HIDS is used to monitor the host operating system to detect, record and reporting any malicious or unusual activities. Therefore the IDS could be useful tool to detect DoS attacks(Bace, 2000)("Intrusion detection system," 2018). In addition, we can use Database Activity Monitor (DAM) and database firewall. DAM operates continuously and in real-time, for monitoring and analyzing database activities. The database firewall us used to monitor the traffic to and from the database server in order to prevent any unauthorized access and modifications of the database. In conclusion, while we are trying to control the database threats, then we need four general control methods the Access Control Management Systems, Database Activities logs, Data Encryption, and Intrusion Detection Systems.

Content Template	
Section Number	4.7
Section Title	Detecting and Analysis of Database Attacks using Digital Forensics Tools
Introduction	This section discusses the types of database infections. Knowing the type of infection help us to find a select suitable digital forensics tool to be used. In addition, this section gives some general example of using digital forensics tools in the database domain.
Content	Fasan and Olivier (Fasan and Olivier, 2012) described the infected databases using three terms compromised, damaged and modified database. The researchers (Fasan and Olivier, 2012) classified the database forensic techniques into three categories based on which infected database types it is applied for. To apply the database forensic correctly we have to know whether the data base compromised, damaged or modified, but unfortunately there is no way know that exactly. Therefore, we should examine the database in all cases compromised, damaged and modified. If the metadata of the database or the software of the DBMS is modified by an attack, then the database is considered compromised. The compromised database keeps operationally working as it was before the attack, but return false information, so it will not be trusted anymore until revert the changes. (Fasan and Olivier, 2012) Fasan and Olivier found that most of the research of the database forensic techniques and research are about the damaged databases. Damaged database means that the database is infected by an attack such as delete, modify or move its content. Damaged databases may still operationally work as it was before the attack, but sure it gives false information. (Fasan and Olivier, 2012)

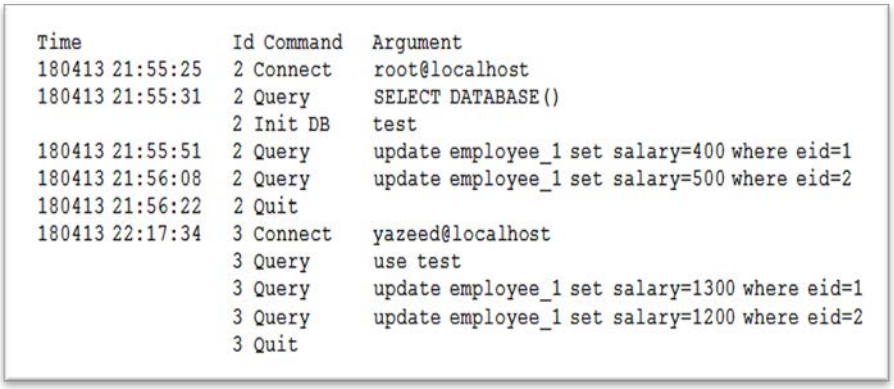
Content Template	
Section Number	4.8
Section Title	Detecting and Analysis of Database Attacks using Digital Forensics Tools
Introduction	This section discusses the types of database infections. Knowing the type of infection help us to find a select suitable digital forensics tool to be used. In addition, this section gives some general example of using digital forensics tools in the database domain.
Content	The database could not be infected by an attack i.e. not compromised nor damaged, but it may be used as a digital forensic tool. Database records and store huge amount of data. We can study and analysis these data to derive some information about an event or subject. The crime is an event against a subject, so we can search the databases that are related to the crime event or crime subject to find some information about the crime. The databases are frequently modified legally by legal business processes, so the database may have different information than it had at the crime time. Fasan and Olivier use the term modified database to refers to those database that have been modified science a specific time, because we need to know what was the content of the database at that time(Fasan and Olivier, 2012). Any database access and modification is done by performing database transaction. Almost all the DBMS and database application have a special file called transaction log file. The transaction log files is a very important component of the database systems and applications because it records all the database transactions ordered sequentially in the same order of its execution. Therefore, the log file will play very important role in the database investigation science it records all the database transaction. By analyzing the database log file we can find what was changed, who changed the database and when. Log file structure and contents is vary from DBMS to another, so we need to refer to the DMBS manual to enable logging, find the log file location read and use the log file. In the last section of this chapter you find an example shows how log file looks like and shows how to use it as part of the database recovery methods. the DBMS is a software server running on hardware server running by operating system in a network environment, sowe can use other digital forensic tools to investigate and analyze the database attacks like using the networks forensics tools and operating systems forensic tools.

Content Template	
Section Number	4.9
Section Title	Database Security in the Web Environment
Introduction	This section explains the relation between the web environment and the database system, and shows the database systems vulnerability through the web environment. In addition, this section explains some tips that can be used to avoid database systems vulnerability through the web environment.
Content	Most of the websites and web-applications we use every day aredesigned specifically for storing and querying data. When we open a webpage and submit or retrieve some information about an object then we actually query a database. To clarify what is actually happen let us study the following scenario. A user visits his bank website that provides online banking. The user enters his credential and click login icon. The request goes from the client machine to the web server. The web server interprets the coming request. But the web server does not contain the information required to identify the user credential, the user and account information is stored on the bank database system. Therefore, the web-server passes a query to the DBMS to get the required information and generate the response then send the response to the client machine. When a user logged in successfully, he can perform many interactions such as print his account statements which is a report from the bank database. In other words, most of the websites and web-applications provide the users with online web-interface to gain access to a database then perform some database transactions based on the user's granted privileges. Suppose that the database is running on a secured server and network, and it is configured correctly regarding to the authentication and access policies. To make this database available online through a website we need to connect the web-server to the database-server which will make the database vulnerable by some threats that are related to internet environment such as DoSattack, SQL injection and packet sniffing. Therefore, we need to have some security tools and methods to secure the web database in addition to the tools that we have discussed in section 0.

Content Template	
Section Number	4.10
Section Title	Database Security in the Web Environment
Introduction	This section explains the relation between the web environment and the database system, and shows the database systems vulnerability through the web environment. In addition, this section explains some tips that can be used to avoid database systems vulnerability through the web environment.
Content	Security methods for web-databases: • Do not deploy and run the database-server and the web-server on the same machine, because the web-server is more likely to be attacked. Therefore running web-server and database-server on separate machines will avoid attacking the database server through the web-server. • Use firewalls to ensure that the database-server and the database are accessible by only the authorized applications and server machines. For example, you can configure the database server to accept the traffic that is coming from a certain machine and IP and deny the other traffic. • Ensure to detect and prevent SQL injection attack. The web-application developer should filter the submitted data and clean it from any SQL injection and use a method that avoids SQL injection like executing the queries using prepared query. In addition we can use web-application firewalls.

Content Template	
Section Number	4.11
Section Title	Database Security in the Web Environment
Introduction	This section explains the relation between the web environment and the database system, and shows the database systems vulnerability through the web environment. In addition, this section explains some tips that can be used to avoid database systems vulnerability through the web environment.
Content	• Ensure that the communication between the client, web-server and the database-server is secured and encrypted. • Ensure that the web-server and the database-server and firewalls are up to date. • Isolates and move the unused data and old data from the database-server into secured storage media. In conclusion and as we have discussed in previous sections, the database threats control methods and techniques depends in general on how do we deploy and run the database systems and how does the database system is connected to the user interface.

Content Template	
Section Number	4.12
Section Title	Data Backup and Recovery
Introduction	A review of database backup definition, types and method is included in this section. This section also talks about recovery methods and shows which recovery method we should use based the occurred database threat.
Content	Database backup and recovery are essential and very important tasks of any database systems. There are many reasons to have database backup and recovery tools and methods such as hardware failure, user error, data corruption; each of these reasons should be treated in different manner. Based on these reasons we should choose the most accurate and suitable recovery techniques to recover the database to the latest correct database. Almost all the database management systems have backup and recovery tools, and each of them has its own specifications and features, but all of them are doing the same task in general. There are three main backup methods: full backup, transaction backup and differential backup.(Elmasri and Navathe, 2006) In this chapter we have discussed some database threats and shown how these threats affect the database privacy, integrity and availability. Some of the database threats affect the database integrity by modifying the database (create, modify and delete item). If an attack is occurred and change the database, then we need to recover the database to revert any illegal data modifications. In the following, you can find two possible methods that could be used as database recover after an attack is occurred.

Content Template	
Section Number	4.13
Section Title	Data Backup and Recovery
Introduction	A review of database backup definition, types and method is included in this section. This section also talks about recovery methods and shows which recovery method we should use based the occurred database threat.
Content	**Method1:** The database management systems record the transactions, errors and other information in files called log files. Almost all the database management systems have transactions log file that contains some information about the transactions that have been performed(Elmasri and Navathe, 2006). Different database management systems have different structure and different content of the transactions log file. **Errore. L'origine riferimento non è stata trovata.** shows a snapshot of a MySQL transactions log file. In the figure below we can see the date and time, the connection id, the user name, and the performed query.  Figure 1 : MySQL Transactions Log File Snapshot Suppose an attack has been occurred and violated the database integrity. By examining the transactions log file having the right information about the attack like the timestamp, the used username and IP address we can identify the transactions that have been performed by the attack. Now we know what items that have been changed, so we can undo these changes.

```
Time              Id Command   Argument
180413 21:55:25   2 Connect    root@localhost
180413 21:55:31   2 Query      SELECT DATABASE()
                  2 Init DB    test
180413 21:55:51   2 Query      update employee_1 set salary=400 where eid=1
180413 21:56:08   2 Query      update employee_1 set salary=500 where eid=2
180413 21:56:22   2 Quit
180413 22:17:34   3 Connect    yazeed@localhost
                  3 Query      use test
                  3 Query      update employee_1 set salary=1300 where eid=1
                  3 Query      update employee_1 set salary=1200 where eid=2
                  3 Quit
```

Content Template	
Section Number	4.14
Section Title	Data Backup and Recovery
Introduction	A review of database backup definition, types and method is included in this section. This section also talks about recovery methods and shows which recovery method we should use based the occurred database threat.
Content	**Method 2:** Perform database backup periodically, then record the legal database transactions. At any time, we want to recover the database we just restore the last saved version of the database and reply all the recorded transactions science the last backup time. The two methods discussed above are general methods to recover database. Applying these methods will depend on the DBMS software. The DBMS has many backup and recovery methods and features which may be different from backup and recovery methods of another DBMS. In conclusion, you have to study the DBMS manual carefully to identify the features and the capabilities of the DBMS and to know how to apply backup plans and recovery.

Activity Template	
Number	4.1
Title	Discuses three real cases of database threats.
Type	The student required to conduct research to find some examples of database threats.
Aim	While doing this activity, the student will read more about the database threats effects, database security, and how to avoid database threats.
Description	In this activity the student is required to find and write down three real cases of database threats. One example of threats against data privacy, the second example about threats against data integrity, and the third example about threats against data availability.
Timeline	• Find and collect the required references and resources. • Find and summarize the related information required to accomplish the report. • Report writing and editing using the academic writing criterions. • This activity will require about five hours.
Assessment	This activity will be assessed based on: • Information and facts correctness and its sequence. • Correct use of the references. • Correct matching between the example and the threat type.

Activity Template	
Number	4.2
Title	Differentiate between compromised database, modified database, and damaged database.
Type	In this activity the student should do a research to differentiate between compromised database, modified database, and damaged database.
Aim	After completing this activity, the student will be able to differentiate between the types of infection of any database attack.
Description	In this activity the student is required to write a report to explain difference between compromised database, modified database, and damaged database.
Timeline	• Required time 2-3 hours. • Find and collect the required references and resources. • Find and summarize the related information required to accomplish the report. • Report writing and editing using the academic writing criterions.
Assessment	This activity will be assessed based on: • Correct matching between the example and the threat type. • The completeness. • The correctness. • The overall quality. • The followed process.

Activity Template	
Number	4.3
Title	Analyze database log file.
Type	In this activity the student will use his knowledge about the DBMS and its structure to use some of the digital forensics.
Aim	This activity encourages the student to utilize the DBMS available tools to be used as forensics tools.
Description	In this activity the student is required to install a DBMS and try to find the activity log file to detect some activities on the database. Then the student should write a short report discussing the importance of the log file for activities analysis.
Timeline	• Required time 4-6 hours. • Install a DBMS on a server. • Create a database with different permission rights for several users. • Access the database and do some modifications using several user accounts and different hosts. • Find the database activity log, and study its structure and content trying to find if a modification has happened, who did the modification and when, what host was used to access the database, and any other useful information. • Write a short report to discuss the importance of the log files for activities analysis.
Assessment	This activity will be assessed based on: • The completeness. • The correctness. • The overall quality. • The followed process.

Activity Template	
Number	4.4
Title	Discuses one example of database attack using web server's vulnerability.
Type	In this activity the student is required to do a research to find and discuses an example of attacking the database through web servers. Then the student should find a solution to prevent such that attacks.
Aim	After completing this activity, the student will realize that if two systems or subsystems are connected, then the attack can exploit vulnerability in one of them to attack the other system.
Description	In this activity the student is required to find and explain oneexample of attacking the database through web servers, and he should propose a solution that can be applied to avoid the attack explained in the example.
Timeline	• Required time 3-4 hours. • Find and collect the required references and resources. • Find and summarize the related information required to accomplish the report. • Report writing and editing using the academic writing criterions.
Assessment	This activity will be assessed based on: • The completeness. • The correctness. • The overall quality. • The followed process. • Correct matching between the example and the threat type.

Think Template (MCQs)	
Number	4.1
Title	Database Threats
Type	Choose correct answer
Question	When the purpose of database application is to make the data available to the authorized users, the database manager is seeking the objective of:
Answers	A. Confidentiality. **B. Availability.** C. Authorization. D. Integrity.

Think Template (MCQs)	
Number	4.2
Title	Database Threats Control Methods
Type	Choose correct answer
Question	Which of the following is not part of database threats control?
Answers	A. Implement the controls. B. Establish an information security policy. C. **Set benchmarks.** D. None of the above.

Think Template (MCQs)	
Number	4.3
Title	Database Security in the Web Environment
Type	True / False
Question	SQL injection is an example of threats that can affect the database through the web.
Answers	**A. True.** B. False.

Think Template (MCQs)	
Number	4.4
Title	Detecting and Analysis Database Attacks using Digital Forensics Tools
Type	Choose correct answer
Question	If we have a database operationally working but gives false information, then we can called it:
Answers	A. Modified database. B. Compromised database C. Damaged database **D. A + B**

Think Template (MCQs)	
Number	4.5
Title	Data Backup and Recovery
Type	Choose correct answer
Question	Which of the following is used to recover the database to the last consistent state?
Answers	A. Backup. B. Recovery **C. A + B** D. None of the above.

Extra Template	
Number	4.1
Title	Database security-attacks and control methods
Topic	• Introduction • Importance and Aims of the Database Forensic • Intrusion Detection
Type	Journal Article: Malik, M., Patel, T., 2016. Database security-attacks and control methods. Int. J. Inf. Sci. Tech. IJIST 6.

Extra Template	
Number	4.2
Title	Database Security: Threats and Solutions
Topic	Database Threats
Type	Journal Article: Ali, A., Afzal, M.M., 2017. Database Security: Threats and Solutions. Int. J. Eng. Invent. 6, 25–27.

Extra Template	
Number	4.3
Title	Analysis of Security Threats to Database Storage Systems
Topic	Database Threats
Type	Journal Article: Chandrashekhar, A.M., Ahmed, S.T., Rahul, N., 2014.Analysis of Security Threats to Database Storage Systems.Int. J. Adv. Res. Data Min. Cloud Comput.IJARDC 3.

Extra Template	
Number	4.4
Title	Intrusion Detection
Topic	Database Threats Control Methods
Type	Book: Bace, R.G., 2000. Intrusion Detection. Sams Publishing. (ISBN: 978-1-57870-185-8)

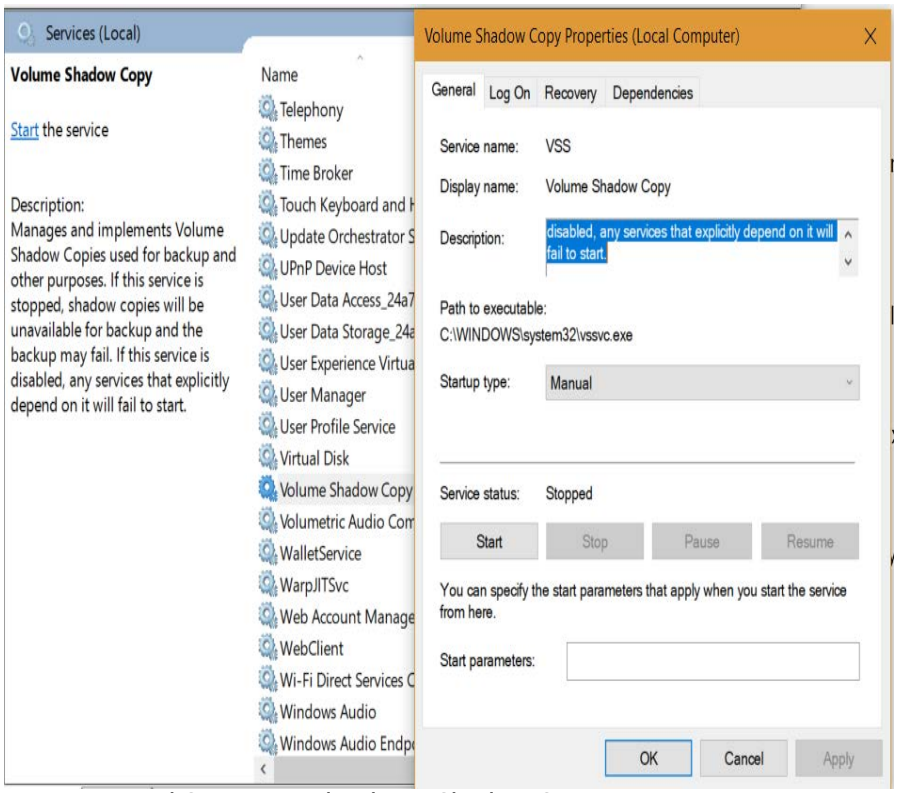
Extra Template	
Number	4.5
Title	On Dimensions of Reconstruction in Database Forensics.
Topic	Detecting and Analysis Database Attacks using Digital Forensics Tools
Type	Conference Paper: Fasan, O.M., Olivier, M.S., 2012. On Dimensions of Reconstruction in Database Forensics., in: WDFIA. pp. 97–106.

Extra Template	
Number	4.6
Title	Database Systems: Models, Languages, Design, and Application Programming
Topic	Data Backup and Recovery
Type	Book: Elmasri, R., Navathe, S.B., 2006. Database Systems: Models, Languages, Design, and Application Programming. Addison-Wesley Longman, Incorporated. (ISBN: 978-0-321-36957-4)

5. Windows Artifacts

<table>
<tr><td colspan="2">Scope</td></tr>
<tr><td>Number</td><td>5</td></tr>
<tr><td>Title</td><td>Windows Artifacts</td></tr>
<tr><td>Introduction</td><td>The largescale use of Windows based systems has made Windows artifacts critical and of great importance for digital forensic examiners. The artifacts can be interpreted as system and user-based activities. It includes file system information, network share information, operating system information, time-zone information, user accounts and Windows event logs. This chapter reviews the common Windows artifacts and prepares the reader to start to identify, compare and analyse relevant user activities.</td></tr>
<tr><td>Outcomes</td><td>At the end of this unit you should be able to:
• Demonstrate clear understanding of Windows Artifacts;
• Identify Window system artifacts, user-based artifacts and evidence locations to answer critical questions on device usage and user activities;
• Perform examination and recovery of common Windows artifacts such as Windows registry, file recovery, volume shadow copy (VSC), Windows volume shadow service (VSS), and Windows event logs using forensic tools;
• Discuss logical and critical answers using variety of free, open-source, and/or commercial forensic tools.</td></tr>
<tr><td>Topics</td><td>- Introduction to Windows Artifacts
- Digital Evidence Collection Using Windows Artifacts
- Windows System Artifacts
- Exploring User Activity with Windows Artifacts</td></tr>
<tr><td>Study Guide</td><td>Instructions on how to study this unit:
• Required study time:
You should plan to spend approximately 25 hours studying this unit. You may find it convenient to break up your study as follows:
<table>
<tr><th>Activity</th><th>Time</th></tr>
<tr><td>Preparation and Content Review</td><td>2 hours</td></tr>
<tr><td>Set Textbook Content</td><td>1 hours</td></tr>
<tr><td>Software/Hardware Review</td><td>10 hours</td></tr>
<tr><td>Thinking (Review questions, MCQs):</td><td>5 hours</td></tr>
<tr><td>Tutorial and Related Course Work</td><td>10 hours</td></tr>
<tr><td>Total</td><td>28 Hours</td></tr>
</table>
• Required hardware/software:
✓ Digital Forensics Lab.
✓ Windows OS 7 or higher version
✓ Current Web Browser.
• Required external resources including links and books:
✓ E- Library.</td></tr>
</table>

Content Template	
Section Number	5.1
Section Title	Introduction to Windows Artifacts
Introduction	Microsoft Windows has become one of the most popular operation systems worldwide. In addition, Microsoft Windows itself can be used as a tool to secure and recover user data and information. The user-friendly environment can provide countless footprints and artifacts made by the user. Therefore, digital forensic examiner must have thorough understanding on how the artifacts are created in Windows and how they can be used to track system and relevant user activity.
Content	With the popularity of Microsoft Windows among system users, a forensic examiner has no choice of escape digging and searching evidences on Windows environment at most of the cases. Thus, it become very superior for digital forensic examiner to have very extensive understanding of the Microsoft Windows and its function. Due to the wide scale use of Windows as an OS it is highly likely that a large amount of an investigators time is spent with these devices and hence the need for a thorough understanding of the topic is very significant for the forensic examiner to cover and or search the hidden tracks. In most of the cases the footprint tacks happen in the system and hidden files. Therefore, the duty of the digital forensic examiner is to find the system relevant artifacts and recover the hidden tracks. In the recent years, plenty of research discussed different ways and means for tracking user footprints and relevant artifacts on Microsoft Windows environment. However, the major forensic challenge is to identify, preserve, collect, and interpret the desired set of evidences in accurate and understandable manner. Generally, Microsoft Windows artifacts can be divided into two main categories as per the following [11]: - System based artifacts which will focus on the events that can be derived by the system. This information can be relevant to files, networks, logs, time zone and more. - User based artifacts in which it focusses on the unique activity of the system user. The following section introduces the common Windows artifacts and illustrate different services provided by Windows to recover the user activities and relevant hidden information. This include deleted data, network and system information, user accounts, event logs and more. The sections also describe the relevant purpose and forensic implication.

Content Template	
Section Number	5.2
Section Title	Digital Evidence Collection Using Windows Artifacts
Introduction	This section introduces common Windows artifacts and illustrate different and basic services provided by Windows to recover the user activities and relevant hidden information. This include deleted data, network and system information, user accounts, event logs and more.
Content	Forensic evidence collection usually varies and depends upon the tool and technique used to collect the evidence. In the following we illustrate the common evidence collection methods based on the common Windows artifacts. 1- Forensic evidence collection based on user created artifacts User created artifact can be generated as data or information contained by the user activity during an operation that may support or relate to certain incident. These artifacts can be taken as file name, MAC address, URL, MD5 and SHA1 file hashes, and more. In addition, user created artifacts can be extracted as file attachment, email, log file, and malware contents. 2- Forensic evidence collection based on volume shadow copy service The volume shadow copy service also known snapshot service implements a framework that allow manual or automatic backups of system files and volumes. The framework act as backbone of the file history, system restore and recovery. The Microsoft Window environment integrate the user services to provide volume backup for creating copies of data. If this service is stopped or failed, shadow copies will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. Figure 1 below illustrates local volume shadow copy properties which can be extracted from Windows system services.  Figure 1. Local Services and Volume Shadow Copy Properties 3- Forensic evidence collection based on system refresh and recovery

Microsoft Windows allows the recovery from different kind of malware or any sort of stability issues by providing the system refresh option. This option allows users to reinstalls Windows and disregard unwanted files to keep the RAM running in smooth fashion. Generally, Windows recovery artifacts include are based on the following major system recovery points:

1- Windows System restore points to undo recent system changes.
2- Windows System refresh points which can be used to reinstall Windows, and keeping files and settings.
3- Windows System reset points to reinstall Windows system, and deleting files and setting.

Restore, refresh and reset are used fix issues associate with Windows system. On the other hand, it can be used help the forensic examiner to present an actual system image before and after the incident. The following Figure 2 and Figure 3 illustrate the system recovery option and some advanced recovery tools in the Windows environment.

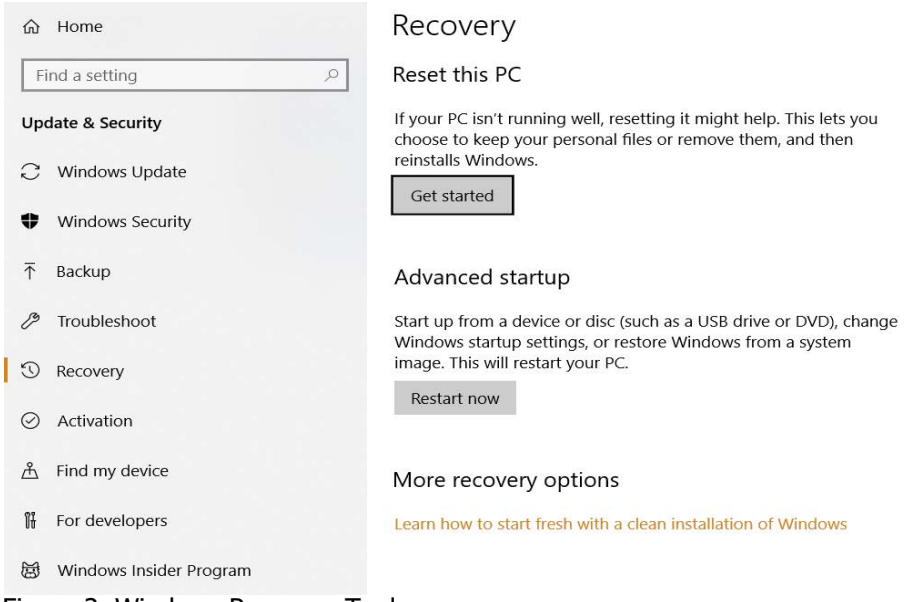


Figure 2. Windows Recovery Tools

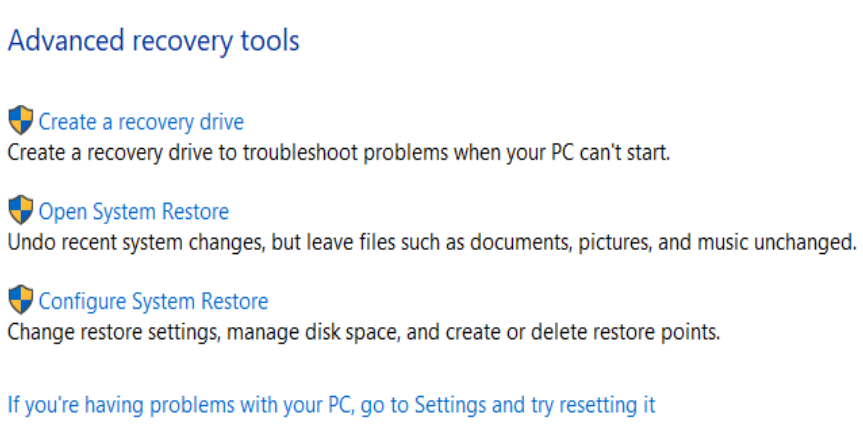


Figure 3. Advanced Recovery Tools

As the artifacts are usually kept on the hard drive, the forensic examiner can use this option to release images from the operating systems relevant to the desired forensic case. Figure 4 below illustrates the control panel which allow the examiner to explore the system available recovery options.

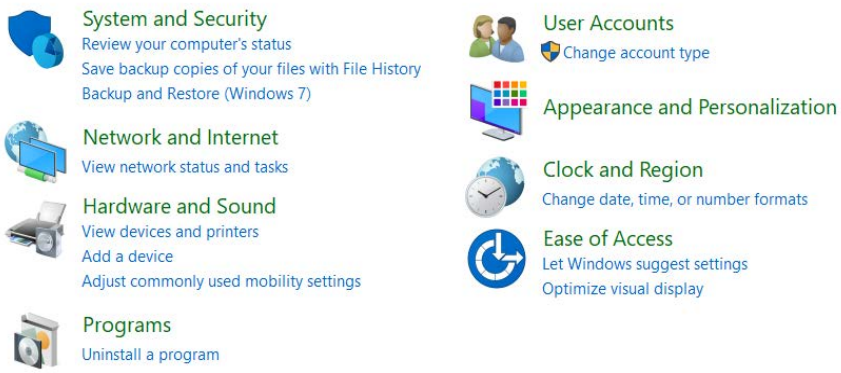


Figure 4. Control Panel

4- Forensic evidence collection based on system restore points

Microsoft Windows allows the request for restore point creation. As such, the previous points and version of Windows are usually stored in the volume drive can be recovered and relevant data can be extracted. Figure 5 below illustrates system properties and system restore configurations in window environment.

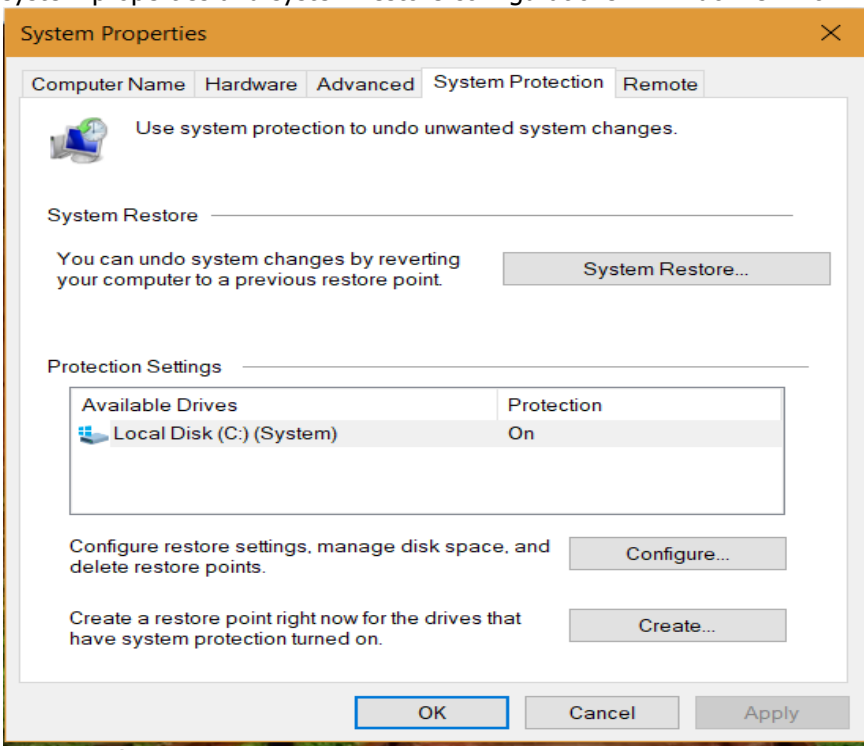


Figure 5. System Properties

Figure 6 illustrate Back up or file restore options on Windows environments. Back up and file restore option can be viewed from the update and security Window.

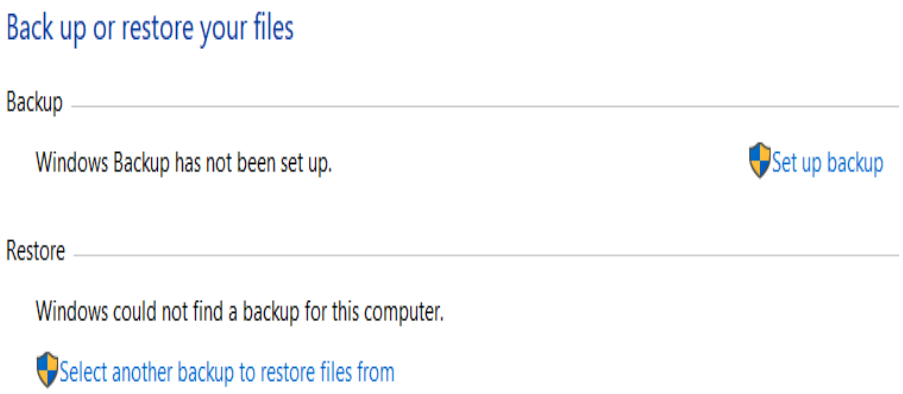


Figure 6. Windows Backup and restore.

5- Forensic evidence collection based on Windows registry

Window system registry is a system database used to store low-level system settings, services, options on user stored data and information, system hardware and software.

Therefore, Window system registry serves as an archive for system and users data. In addition, any changes made to the system and users shall be automatically updated in the registry. Such data stored is critical and can be helpful to the system users. Data and information that can be found on the system registry may include:

- ✓ Most recently used software
- ✓ A list of searches done so far on the system
- ✓ Devices attached to the system such as hard drives, phones, tablets, etc.
- ✓ What and when files are accessed
- ✓ Users and the time they last used the system and more

In addition, manual changes associated with Window system registry can be accomplished using the registry editor. The registry editor allows the user to perform several functions that make up the entire Window system registry such as creating, manipulating, renaming and deleting registry keys, importing and exporting .REG files, exporting data in binary hive format, setting permissions, and remotely editing the registry on another networked computer. The registry editor can be viewed by executing the *regedit* in the run window. Figure 7 below illustrate the registry editor.

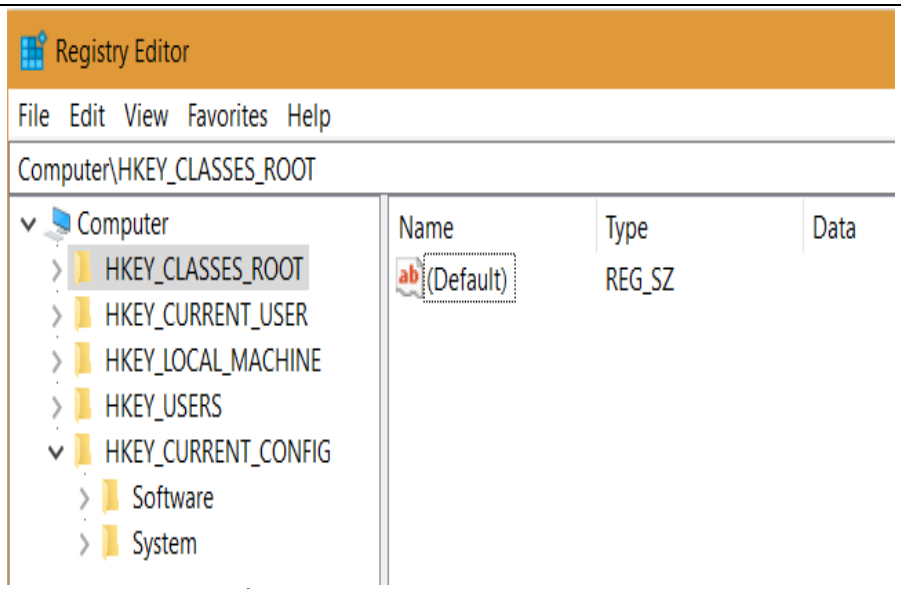


Figure 7. Registry Editor

Registry editors contain enormous amount Window system and user related information which can be used by the digital investigator. For example, registry *hive* is a logical group of keys, subkeys, and values in the registry that has a set of supporting files containing backups and data.

Content Template	
Section Number	5.3
Section Title	Windows System Artifacts
Introduction	Digital forensic investigation normally covers large volume of evidences such as files, downloads, executions, physical local information, USB usage details, user accounts, deleted files and directories. Therefore, Windows system generated artifacts may include several activities which can be read as system or user based artifacts.
Content	One of the most important Windows artifacts are those associated with files. System files are usually hidden from normal user and require deep knowledge of the system and specialized tools to dig, collect, and analyses relevant patterns. Furthermore, Window registry and file prefetching process are considered as potential source of desirable information. Prefetch files are generally used to determine what programs were recently executed on a system. By analyzing a Prefetch file, forensic investigator can determine the executable file name, file path, timestamps, and the volume information. Generally, Window system artifacts include several data patterns and information which can be extracted from file system, network information, user account details and patterns derived from the following window system artifacts: – Desktop – Pinned files – Hiberfil.sys and pagefile.sys – Recycle Bin – Registry – App Data – Favorites and relevant contents – Send to Artifacts – Swap Files – Thumb Cache – HKey Class Root – Cookies – Program files – Meta Data – My Documents – Recent Folder (most recently used) – Restore Points – Print Spooler – Logo – Start menu – Jump lists and Root User Folder The following portion illustrate the most potential Window System artifacts such as file system artifacts, network share artifacts, operating system artifacts, timezone artifacts, user accounts and Windows event logs artifacts. Event logs are unique as they contain details about what is happening on the system as well as user activity. 1- File System Artifacts File system can be assumed as an index, which describe the physical relationship of data elements on the hard drive. However, forensic investigators need to be very familiar with the common file system structure in order to retrieve and recover data elements of particular relationship.

Generally, Window operating system supports wide range of Microsoft developed file systems such as FAT, NTFS, and ExFAT. Some of the common file formats are:

- Word files or documents (.doc)
- Images (.jpg, .gif, .png, etc.)
- Executable files (.exe)
- Multimedia (.mp3, .mp4 and others)
- Acrobat reader files (.pdf)
- Web page files (.html or .htm)
- Notepad or wordpad files (.txt)
- Powerpoint files (.ppt)
- Dynamic Link Library Files (.dll)
- Compressed files (.zip and .rar)

File system artifacts generally provide digital investigator with details about the derived file format, volume, file properties and partitions of the hard drive. In addition, information such as file system type, call history, volume serial number, capacity, sector and cluster information, and more signs of associated with the investigation case. Figure 8 below illustrate call history and app permissions configuration.

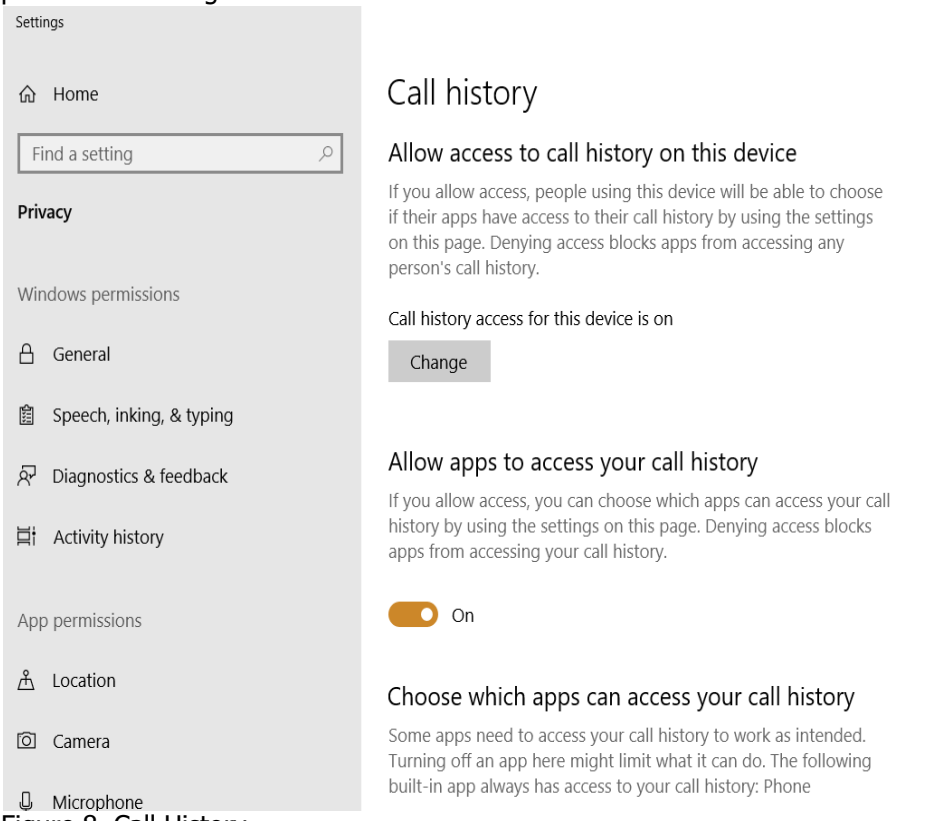


Figure 8. Call History

Digital forensic examiner has the choice to apply different type forensic tools such as Encase to automatically organize files, apply certain retrieval method, and analyze the given file system. However, in certain forensic cases it is fundamental to perform deeper analysis and manually retrieve or parse a given file system using file and registry forensic tools. Deeper forensic may be required to provide essential details for the analysis and recovery for particular piece of data.

Access permission is very important in fornensic investigations. As such, digital examiners must be aware of the legal issues assicuated with access permissions. Form technical point of view, digital investigator should learn

about the access configration and its impact on the investigation process. Figure 9 shows Windows file system access details and how to choose apps that can access certain files with particular format.

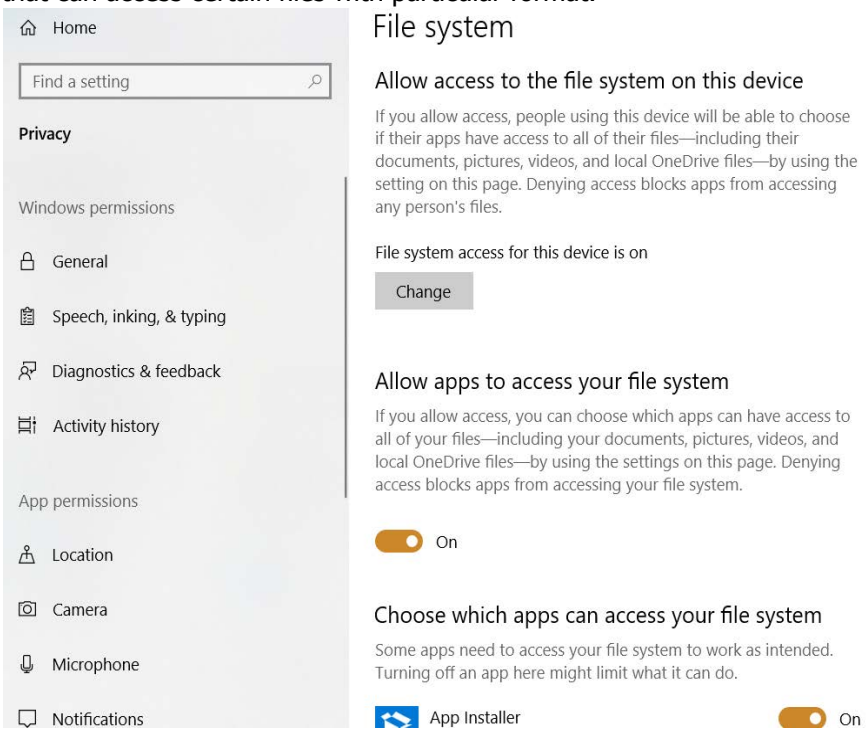


Figure 9. File System

2- Network Share Artifacts

Digital forensic investigators may recover and use network share information as strong evidence. The information which can be pulled from the registry locations such as .REG files and registry hive can benefit to recover many network shared mounted data by the user. However, in most the time forensic investigator needs to use forensic tools. For example, by providing digital investigators relevant network shares for each network user, the revealed information can support additional sources of potential evidence that might be stored on another system on the network. Figure 10 illustrate different sharing options of network profiles from the advance sharing setting in the Window system control panel.

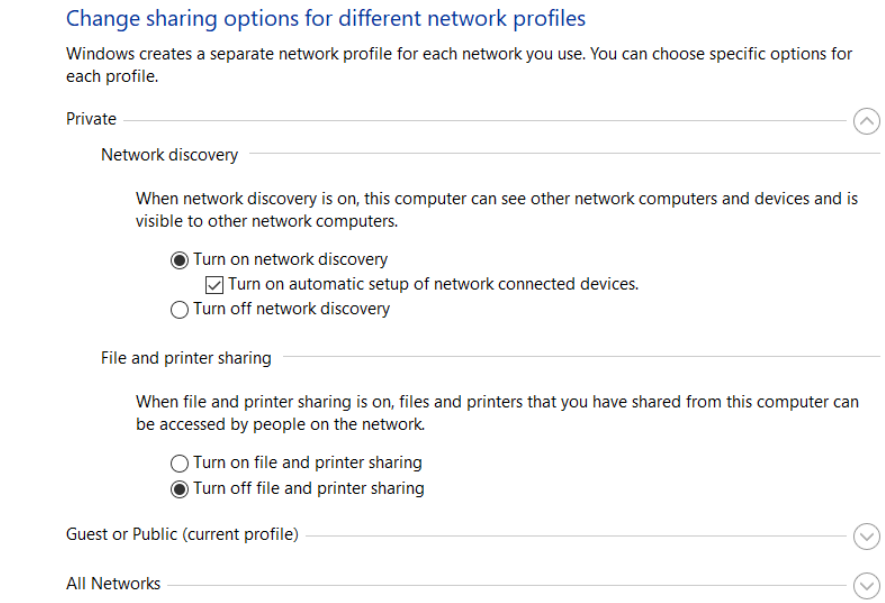


Figure 10. Network Sharing Options

Figure 11 illustrate automatic proxy setup for network and Internet services.

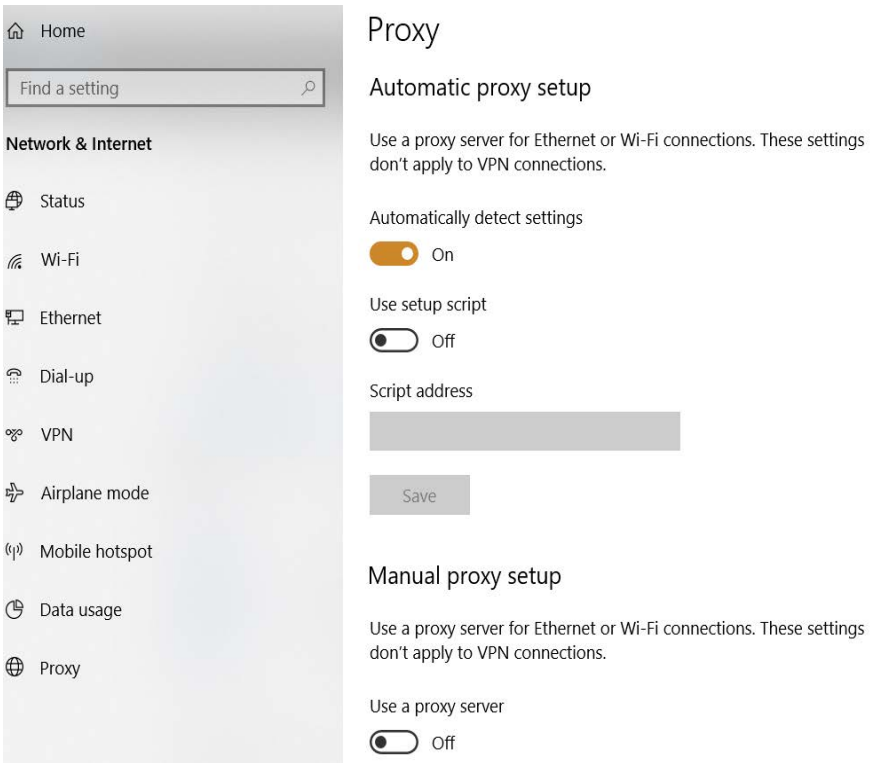


Figure 11. Proxy Setup

3- Operating System Artifacts

The details recovered from the used OS is huge interest to digital investigators to be used as an evidence such as the system version, product ID and Keys, service pack, time stamps and more prints for the operating system in use. The significance of the operating system artifacts is to present details about what is exactly happening on the system as well as the user activity. Figure 12 illustrate the details of the system information as per Window desktop app.

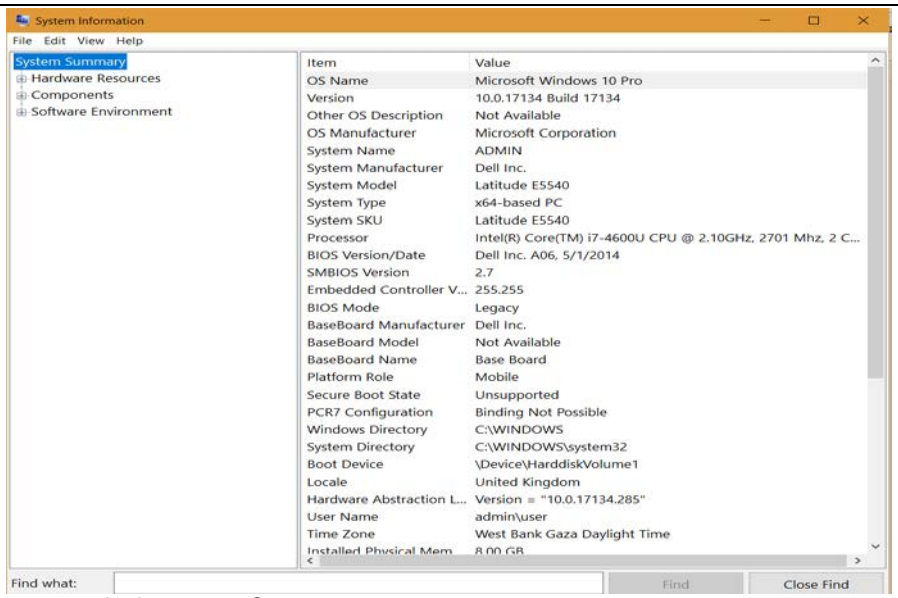


Figure 12. System Information

There are number of valuable scenarios that can be considered from several system footprints such as when the system was simply powered off or unplugged. However, the following system artifacts are of most interest:

- System install date
- Shutdown time
- Events timeline
- Last logon time
- The last time the system was shutdown
- The date the system was installed

Figure 13 below illustrates system details from the setting Window.

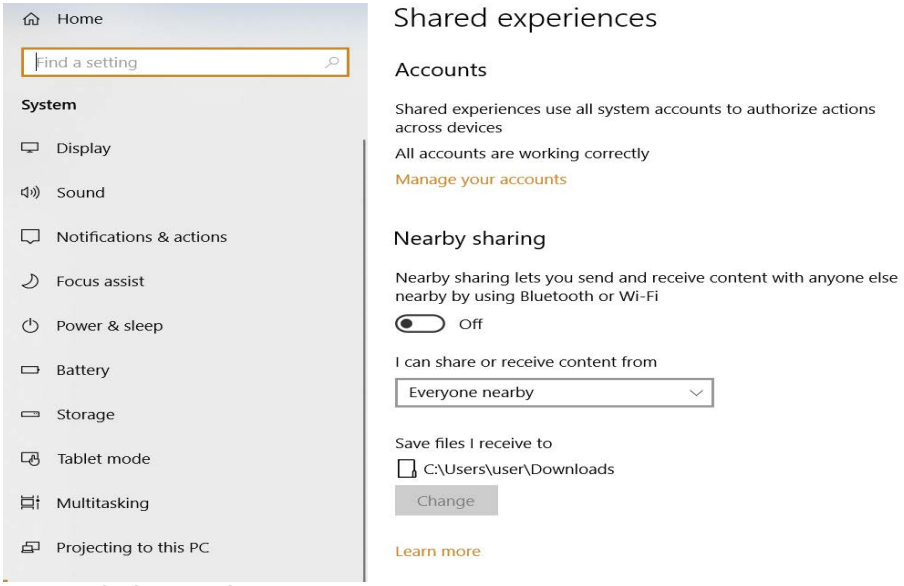


Figure 13. System Setting

4- Timezone Information artifacts

Windows registry store timezone information and a number of timestamps in both local and UTC time. It is vital for the forensic examiner to have deep understanding of the relationship between the stimestamps and system events and how they relate to the local and UTC time format. For example, an

investigator may use the timestamp to determine the correct ordering of a user events and hence determine the sequence of events. Figure 14 illustrate the system date and time events setting which can be viewed from the Window system setting.

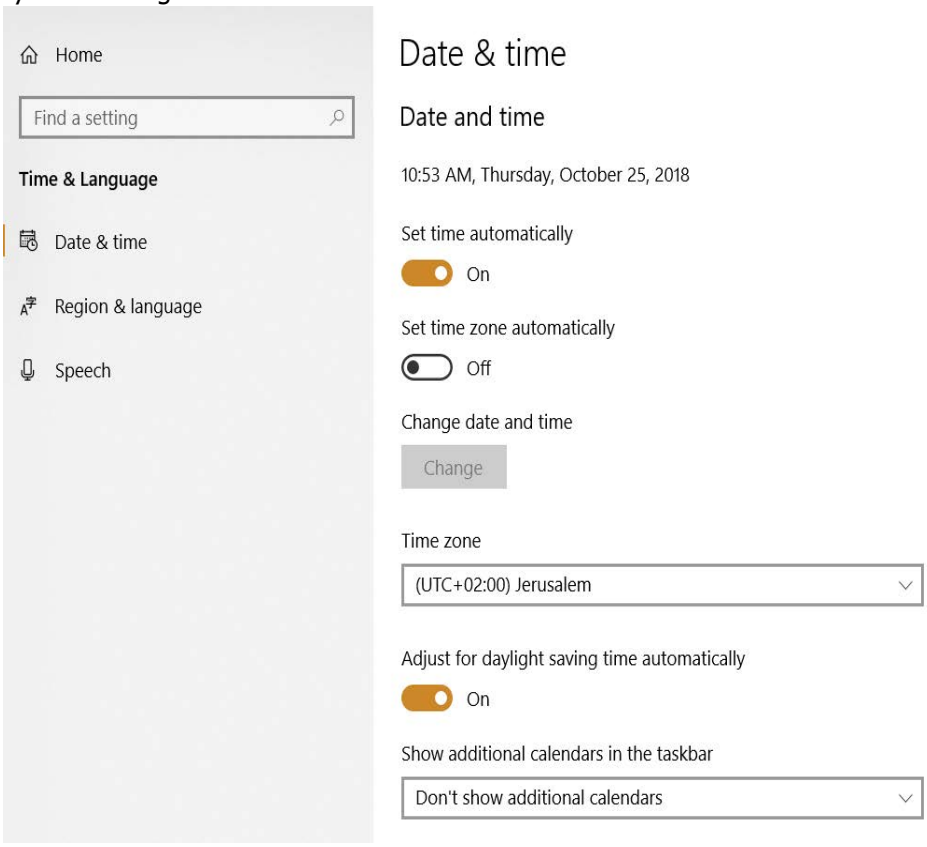


Figure 14. Date and Time Setting

Generally, timezone information is stored in the SYSTEM HIVE or system image, however, forensic examiner need to use sophisticated forensic tools such as Forensic Toolkit (FTK) in order to view the timestamps in relation to the incidents timeline or forensic events. Figure 15 illustrate system event timestamp.

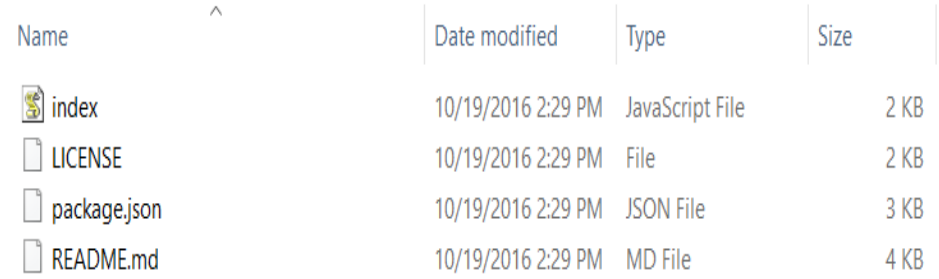


Figure 15. System Event Timestamp

5- User Accounts artifacts

User account information is stored in the registry hive in which we will able to list all of the system default and user created accounts. Using forensic specialized tools such as Encase and FTK, digital investigators can pull interesting user account information such as:

- Account name
- Account type
- Account groups

- Account login and last login
- Disabled accounts
- Passwords and timestamps
- Incorrect logins and domain users

Such information can be go great value to the digital investigator for finding any sort if intrusions in relation to the user account settings. Figure 16 illustrate Windows environment user account control setting from the control panel.

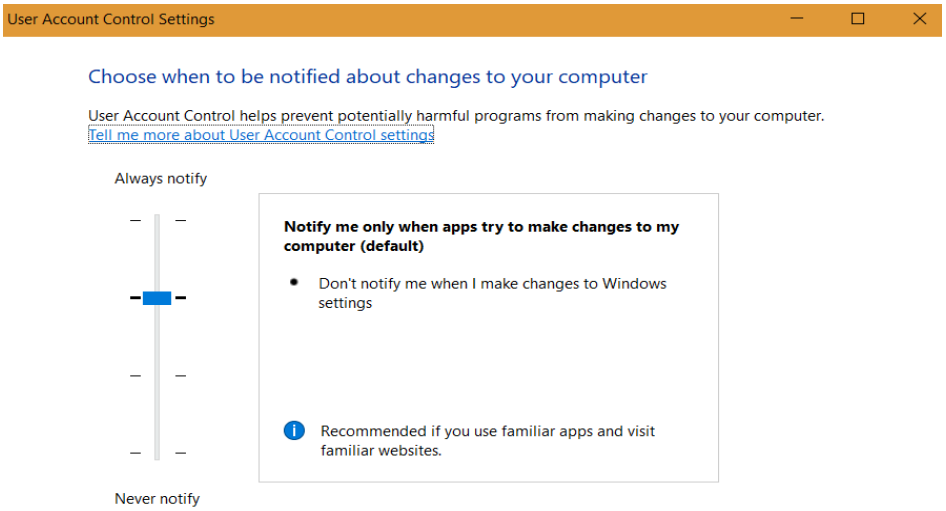


Figure 16. User Account Control Setting

6- Windows Event Logs artifacts

Windows event logs store tons of information about the system and its users. However, the such information can be reached in reference to the logging level (i.e. local vs network) and the version of Windows installed. Windows event logs artifacts can provide digital examiners with the following essential artifacts details:

- Administrative events and their relevant system stamps of interest,
- Application and service logs,
- Success and failure logs
- Security logs,
- Setup logs,
- Forwarded events logs and
- Subscriptions logs

Typically, digital investigator may pull tones of events from the stored window logs but the focus shall be only on those with direct or indirect incident relationship. Therefore, forensic examiner may need to filter these logs using forensic tools to determine specific activates and strong evidence list. Figure 17 illustrates the event logs viewer in Windows environment.

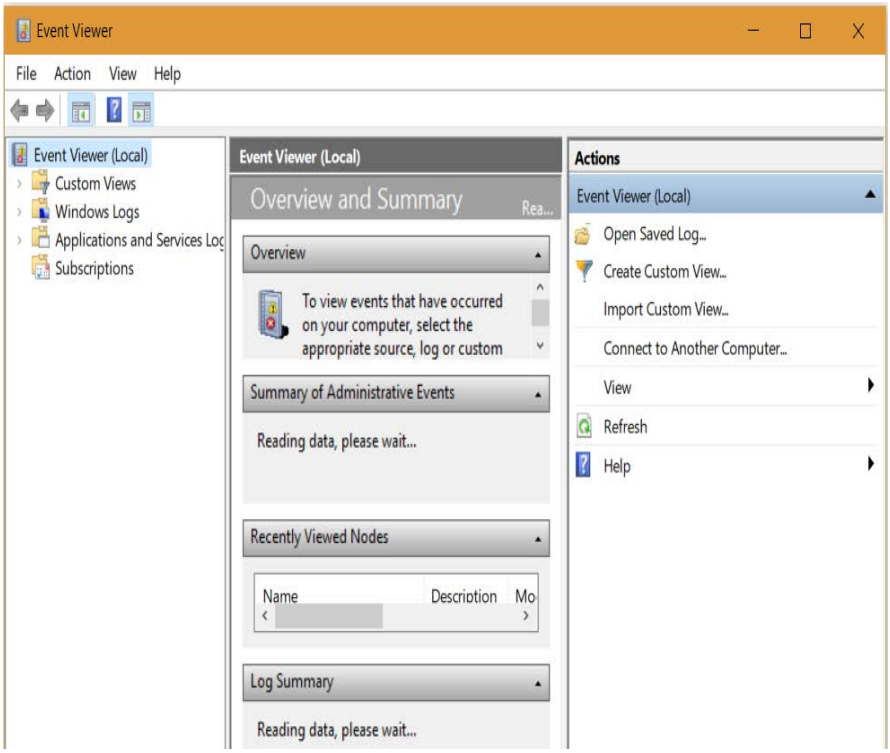


Figure 17. Event Viewer

Content Template	
Section Number	5.4
Section Title	Exploring User Activity with Windows Artifacts
Introduction	In the real world, forensic investigator need to correlate the action of the system user with normal system activities. This may include the user permissions, system term of use, location and so on. Although this type correlation seems vary, each and every event on the computer system actually correlate to a particular user activity. In fact, it depends on the type of the user and relevant account setting. This means that each event is result of whether one particular user involved or not involved in doing something evident and appropriately fit to the forensic case. Therefore, the forensic examiner need to explore the particular details of the user activity, simplifying the events and present the details of the evidence.
Content	Exploring user activities with Windows Artifacts involve characteristics relate directly to the user and others associated with the system. The following list the basic artifacts that combine both system and user's focused artifacts. o File system information and direct links to executable files to provide evidence on how the data is actually stored and retrieved in the system. o Jump lists feature allows an investigator to view recent documents in a program and quickly present the latest user events. o Network share information for sharing resources or enable access of information through more than one device. o Operating system information to provide clear information about the system capability. o Shellbags (registry keys) and startup items to make use of the registry setting. These keys are useful to a forensic investigator to indicate exactly which folder was used and deeply analyze what was exactly happening. o Timezone information to identify the timezone information on the suspect computer. o USB devices history investigation. o User accounts to identify details about the user accounts, deleted user accounts and to determine who logged on to the system. o Windows event logs and Windows prefetch files to determine which applications have been run on a computer, and collect some valuable data on a user's application history. Digital examiner may use direct system extracted artifacts from the Window Operating System or use specific forensic tools for the same purpose. Forensic tools help investigators gain full insight into the details about the system and its users. Overall, digital investigator may derive tons of information about the user and system activities with reference to the above mentioned artifacts. Therefore, digital investigator need to piece and consolidate the collected data and information together to provide clear platform about the forensic case. As such, an investigator would be able to present strong and complete picture of forensic evidence.

Activity	
Number	5.1
Title	Introduction to Windows Artifacts
Type	Review questions
Aim	To demonstrate clear understanding of Windows Artifacts.
Description	4- Discuss the meaning of the term Windows Artifacts. 5- Differentiate between the users and system-based activities. Give an example. 6- Discuss the role of forensic examiner in identifying evidence locations to answer critical questions on device usage and user activities. Give examples.
Timeline	One Hour
Assessment	Classroom discussion

Activity	
Number	5.2
Title	Digital Evidence Collection Using Windows Artifacts
Type	Research and reflection questions
Aim	Perform examination and recovery using forensic tools.
Description	5- Assume that an office secretary has been accused that her computer was compromised. She changed the computer password, yet it seems someone has used it again. As a forensic examiner, what you think might be going on? 6- Assume that you need to investigate a computer drive. The drive contains several files such as password files and files with different extensions. Write a procedure that you will follow to identify the mismatched file headers to extensions and discuss the techniques you can apply to recover passwords from the protected files. 7- Suppose file1.zip was deleted and we need to recover the deleted file. Illustrate the recovery instructions using EnCase or similar available tool. 8- Assume that you need to examine computer whose user is an employee suspected with some illegal transactions. Most of the transactions are attachments and e-mail based. During the investigation, you find several files and one of those files called file2.zip was compressed with zip utility. When you try to open file2.zip using an image viewer, a message is displayed indicating that file2.zip is corrupt. Write a report explaining how to recover file2.zip. 9- Demonstrate FAT and NTFS files partitions recovery using EnCase or similar available tool.
Timeline	Ten Hours
Assessment	Lab discussion

Activity	
Number	5.3, 5.4
Title	Windows System Artifacts
Type	Research questions
Aim	Extract logical and critical answers based on Windows artifacts using variety of free, open-source, and commercial forensic tools.
Description	3- Consider any three common Window system artifacts and determine the similar Windows 10 Official version artifacts locations? Compare your results with Window 7 and Window 8? 4- What types of artifacts are stored by Windows 10 Applications, and where are these artifacts found? 5- What is the difference when forensically analyzing Windows tablet devices and Window desktop devices? Does that have an impact on the law enforcement? Discuss your answer.
Timeline	Ten Hours
Assessment	Classroom and Lab discussion

Think Template (MCQs)	
Number	5.1, 5.2, 5.3
Title	Windows Artifacts
Type	Multiple Choice Question could be in the form of: Choose correct answer
Question	1. Windows artifacts consist of: a) User based activities b) System based activities c) System and user based activities d) None of the above. 2. Common Windows artifacts include: a) User created artifacts b) Volume shadow copy service c) System refresh and recovery d) System restore points and window registry e) All of the above f) None of the above. 3. User account details and patterns can be derived from: a) Recycle Bin Artifacts b) Registry Artifacts c) App Data Artifacts d) Program files Artifacts e) All of the above f) None of the above. 4. System based artifacts focus on the events that can be derived by the system. a) True Statement b) False Statement. 5. What is the file extension name for the Setup logs in Windows 7 (Windows logs)? a) .log b) .etl c) .stp d) .set 5. The Recycle.Bin folder is located within the Windows.old directory, which is accessible once a machine has been Refreshed, as in Windows 8 for example. a) True Statement b) False Statement. 7. Which of the following are Registry data types? (Select as many as applicable) a) REG_DWORD b) REG_WINDOWS a) REG_HEX b) All of the above. 8. By providing digital investigator relevant network shares for each network user, the revealed information can support additional sources of potential evidence that might be stored on another system on the network. a) True Statement b) False Statement. 9. Link files are stored in: a) Windows desktop b) Start Menu c) Send to folder d) Recent folder e) All of the above

	f) None of the above. 10. The system has something called as registry editor and considered as: a) The file which users can read while the system is running. b) Windows page files c) Can be viewed by executing the regedit in the run window d) Database files generated automatically in the folder where the corresponding images exist. e) All of the above f) None of the above.
Answers	1. Windows artifacts consist of: a) User based activities b) System based activities c) System and user based activities d) None of the above. 2. Common Windows artifacts include: a) User created artifacts b) Volume shadow copy service c) System refresh and recovery d) System restore points and window registry e) All of the above f) None of the above. 3. User account details and patterns can be derived from: a) Recycle Bin Artifacts b) Registry Artifacts c) App Data Artifacts d) Program files Artifacts e) All of the above f) None of the above. 4. System based artifacts focus on the events that can be derived by the system. a) True Statement b) False Statement. 5. What is the file extension name for the Setup logs in Windows 7 (Windows logs)? a) .log b) .etl c) .stp d) .set 5. The Recycle.Bin folder is located within the Windows.old directory, which is accessible once a machine has been Refreshed, as in Windows 8 for example. a) True Statement b) False Statement. 7. Which of the following are Registry data types? (Select as many as applicable) a) REG_DWORD b) REG_WINDOWS a) REG_HEX b) All of the above. 8. System users can make any adjustments to the system that would prevent the caching thumbnails. a) True Statement b) False Statement. 9. Link files are stored in: a) Windows desktop b) Start Menu c) Send to folder

	d) Recent folder e) All of the above f) None of the above. 10. The system has something called as registry editor and considered as: a) The file which users can read while the system is running. b) Windows page files c) Can be viewed by executing the regedit in the run window d) Database files generated automatically in the folder where the corresponding images exist. e) All of the above f) None of the above.

Extra	
Number	5
Title	Windows Artifacts
Topic	5.1, 5.2, 5.3
Type	• Book/Chapter (ISBN) 3- Carrier, Brian, File System Forensic Analysis, Addison-Wesley, 2005. 4- Phillip A, Cowen D, Davis C. Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions New York: McGraw-Hill; 2009. 5- Casey E. Handbook of Digital Forensics and Investigation Burlington, MA: Academic Press; 2009. 6- Sammons J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress, second edition, 2014. 7- Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to computer forensics and investigations. Boston, MA: Course Technology Cengage Learning. • Offline content (Full reference) 8- Sutherland I. (2011) An Architecture for the Forensic Analysis of Windows System Artifacts. In: Baggili I. (eds) Digital Forensics and Cyber Crime. ICDF2C 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 53. Springer, Berlin, Heidelberg. • Online content (URL) 9- https://www.infosecinstitute.com/ 10- https://resources.infosecinstitute.com/ 11- https://digital-forensics.sans.org/ 12- https://www.dfrws.org/ 13- https://www.magnetforensics.com/ 14- https://www.sans.org/ 15- http://forensicswiki.org/wiki/Windows

6. Linux forensics

<table>
<tr><td colspan="3">Scope Template</td></tr>
<tr><td>Number</td><td colspan="2">6</td></tr>
<tr><td>Title</td><td colspan="2">Linux forensics</td></tr>
<tr><td>Introduction</td><td colspan="2">This chapter will introduce Linux operating system and basics guides for Linux investigation.</td></tr>
<tr><td>Outcomes</td><td colspan="2">Learning the basics to perform Linux operating system forensic investigation.</td></tr>
<tr><td>Topics</td><td colspan="2">• Introduction.
• Introduction to Linux forensic investigation.
• Linux Forensic.
• Initial data collecting.
• Determine if there is an incident.
• Memory dumping.
• Offline image.
• Start of the analysis.</td></tr>
<tr><td rowspan="9">Study Guide</td><td colspan="2">Instructions on how to study this unit.</td></tr>
<tr><td>Task</td><td>Time</td></tr>
<tr><td>Preparation:</td><td>2hr</td></tr>
<tr><td>Implementation :</td><td>4hrs</td></tr>
<tr><td>Thinking</td><td>2hr</td></tr>
<tr><td>Tutorial Work:</td><td>3hrs</td></tr>
<tr><td>Related Course Work:</td><td>2hrs</td></tr>
<tr><td>Total</td><td>13 hours</td></tr>
<tr><td colspan="2">* Required study time: 13 hours
* Required hardware/software:
Preferred Virtual machine that runs SWIFT operating system.</td></tr>
</table>

<table>
<tr><td colspan="2">Content Template</td></tr>
<tr><td>Section Number</td><td>6.1</td></tr>
<tr><td>Section Title</td><td>Introduction</td></tr>
<tr><td>Introduction</td><td>This section will introduce Linux operating system. It will give a brief overview of Linux file systems and architecture. Also this section provides some popular distributions for Linux operating system.</td></tr>
<tr><td>Content</td><td>Linux is the best-known and most-used open source operating system. As an operating system, Linux is software that sits underneath all of the other software on a computer, receiving requests from those programs and relaying these requests to the computer's hardware. In many ways, Linux is similar to other operating systems you may have used before, such as Windows, OS X, or iOS. Like other operating systems, Linux has a graphical interface, and types of software you are accustomed to using on other operating systems, such as word processing applications, have Linux equivalents.
There are some popular distributions for Linux operating system, such as: UBUNTU, KALI, REDHAT, CENTOS …..etc. Each distribution has its own feature and characteristics, but all of these distributions were built using the same Linux kernel.
Linux treats all devices as a file. As such, an entry is created in the file system for each hardware device recognized by the operating system. For instance, if a standard IDE hard drive is connected to the system, it will be listed under /dev/hdx. These listings start from the letter "a" (or /dev/hda) and increase in alphabetical order. In a similar fashion, each partition of the drive is numbered from "1" on (starting with /dev/hda1, for instance). To see a list of all the partitions that are available for a drive, type the following command: fdisk –l /dev/hdx. Table 6.1 explains Linux operating system file architecture.
<table>
<tr><td>Directory</td><td>Description</td></tr>
<tr><td>/ (root filesystem)</td><td>The root filesystem is the top-level directory of the filesystem. It must contain all of the files required to boot the Linux system before other filesystems are mounted. It must include all of the required executables and libraries required to boot the remaining filesystems. After the system is booted, all other filesystems are mounted on standard, well-defined mount points as subdirectories of the root filesystem.</td></tr>
<tr><td>/bin</td><td>The /bin directory contains user executable files.</td></tr>
<tr><td>/boot</td><td>Contains the static bootloader and kernel executable and configuration files required to boot a Linux computer.</td></tr>
<tr><td>/dev</td><td>This directory contains the device files for every hardware device attached to the system. These are not device drivers, rather they are files that represent each device on the computer and facilitate access to those devices.</td></tr>
<tr><td>/etc</td><td>Contains the local system configuration files for the host computer.</td></tr>
<tr><td>/home</td><td>Home directory storage for user files. Each user has a subdirectory in /home.</td></tr>
</table>
</td></tr>
</table>

/lib	Contains shared library files that are required to boot the system.
/media	A place to mount external removable media devices such as USB thumb drives that may be connected to the host.
/mnt	A temporary mount point for regular filesystems (as in not removable media) that can be used while the administrator is repairing or working on a filesystem.
/opt	Optional files such as vendor supplied application programs should be located here.
/root	This is not the root (/) filesystem. It is the home directory for the root user.
/sbin	System binary files. These are executables used for system administration.
/tmp	Temporary directory. Used by the operating system and many programs to store temporary files. Users may also store files here temporarily. Note that files stored here may be deleted at any time without prior notice.
/usr	These are shareable, read-only files, including executable binaries and libraries, man files, and other types of documentation.
/var	Variable data files are stored here. This can include things like log files, MySQL, and other database files, web server data files, email inboxes, and much more.

Table 6.1: Linux filesystem hierarchy.

Content Template	
Section Number	6.2
Section Title	Introduction to Linux forensic investigation
Introduction	This section introduces several guides and phases that should be followed during Linux forensic investigation.
Content	Before discussing Linux investigation; there are several guides and phases that should be followed during any digital forensic investigation including Linux forensic investigation. In any digital investigation there are numbers of general guiding principles that should be followed, which includes:- • **Maintaining Integrity:** It is of the most importance that evidence not be altered while it is being collected and examined. Forensic investigator should not make any manipulation in the data that he/she wants to investigate. Investigator should make a copy of data and work on that copy. • **Standard Practices:** By following a written procedure accurately there is less explaining to do if you should find yourself in court. You are also less likely to forget something or make a mistake. Also, everything in the investigation should be documented as a reference to guide you during investigation process. In any digital crime, which includes Linux crimes three phases you should follow during your investigation which includes; evidence preservation; such as memory dump, evidence searching; as image search among millions of files, and event reconstruction; such as finding the evidence in more than one place.

Content Template	
Section Number	6.3
Section Title	Linux Forensic
Introduction	This section provides a high level stages for performing a Linux forensic investigation, it also mention the basic tools that should be available and ready to be used by a forensic investigator.
Content	In most cases Linux is the standard choice for anyone working in information security or forensics especially for whom looked for free tools. Many devices all around the world are running some version of Linux. Whether it is the wireless access point that you bought at the local electronics store or the smart temperature controller keeping your home comfortable, they are likely running Linux under the hood. Linux also shares some heritage and functionality with Android and OSX. In general to conduct digital criminals in Linux operating system, you should understand the system in details, for instance how the files are organized in the system, file system types, and you should understand the boot process for this operating system. The majority of Linux forensic investigations "This can be applied to any operating system" are conducted after a suspected breach. Additionally, the high level process for incident response is shown in Figure 6.1

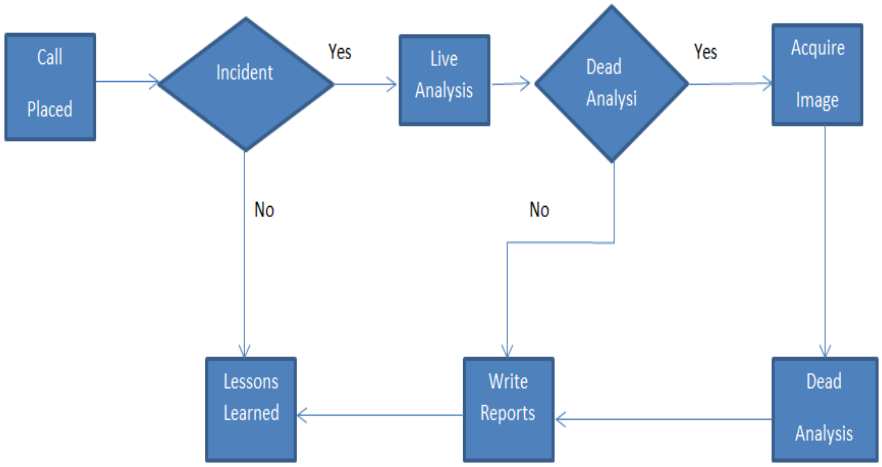


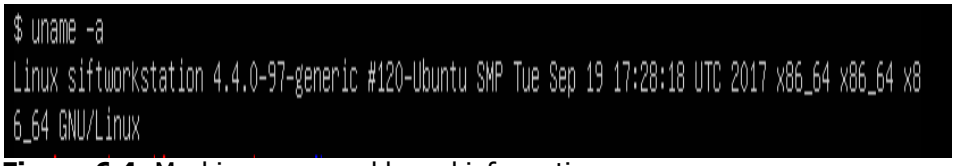
Figure 6.1: Linux forensics process

In order to do Linux forensics effectively you might want to acquire tools, which may include:-

- **Hardware:** USB 2.0 or USB 3.0, Laptop, and other forensic hardware tools for reading damaged disks.
- **Software:** including system binaries, since you should not trust anything in that system. And live Linux USB. Such as SWIFT operating system that bundles with a lot of forensic tools.

Content Template	
Section Number	6.4
Section Title	Initial data collecting
Introduction	In this section we will discuss the initial steps that are required before start Linux investigation.
Content	Before you start an investigation you should minimize the disturbance to a suspicious machine. Figure 6.1, showed that the first step in Linux forensic investigation is to determine if there is an incident or not, and this can be done by conducts the following steps: - • **TALKING TO USERS**: Before you start touching the subject system you should interview the users. Because they know more about the situation than you. You might be able to determine that it was all a false alarm very quickly by talking to the users. Remember to document everything and to take as much information as you can. • **Minimize memory footprint**: By using a tool like NETCAT , we must transfer all basics system information through this tool and save these information in logs files. Information such as; date and time "date command ", hostname "uname –a ", IPs "ipconfig" , Operating system version, open ports, Programs associated with various ports "netstat -anp", Open Files "LSOF -V", Running Processes "PS -ef",Free disks size "df", Routing Tables "netstat –rn , route ", Mounted filesystems "mount", Loaded kernel modules "lsmod", Users past and present, Online users and their past commands "w, last ", users password "/etc/passwd, "/etc/shadow" ,and other suspicious files to our machine to examine them. Remember that NETCAT and the other tools should be within your tools set and mounted to suspicious machine. For instant, Assume we want to transfer a file from suspicious machine to our machine for examination. First we will open a NETCAT session on our forensic machine, see figure 6.2. Then connect to that opened session and transfer the file from the suspicious machine as demonstrated in figure 6.3. You can write a bash script to get all these information easily. Remember you have to transfer all system information using same techniques illustrated before.  **Figure 6.2:** Forensic machine NETCAT command

Figure 6.3: Sending suspicious file from suspicious machine.

Content Template	
Section Number	6.5
Section Title	Determine if there is an incident
Introduction	In this section we will discuss the first steps that should be taken if we found that there was an incident in the suspicious Linux machine.
Content	After collecting the basic system information such as open files, open ports and talking to users, you should start initial analysis for this information in the logs files on your forensic machine to determine if there was an incidence. From our basics analysis, we got information that there was a Linux server which is used by developers and this server is suspected to be manipulated by a user on that system. Also from basics information that we collected we have notice that there is unusual ports opened and unusual processes. The following are some of the important information that was collected and saved in the forensic machine (remember these information is sent to forensic machine using NETCAT). • **Analyzing machine date**: subject system might be in a different timezone from your usual location. • **Operating system version**: You will need to know the exact operating system and kernel version you are running should you later decide to do memory analysis. The results of running this command will be as in figure 6.4  **Figure 6.4:** Machine name and kernel information. • **Network interfaces**: An attacker with physical access could add a wireless interface or USB interface pretty easily. Also you should notice IPs assigned to each network interface. Figure 6.5 illustrates the command used for displaying network interfaces that was sent from the suspicious machine.

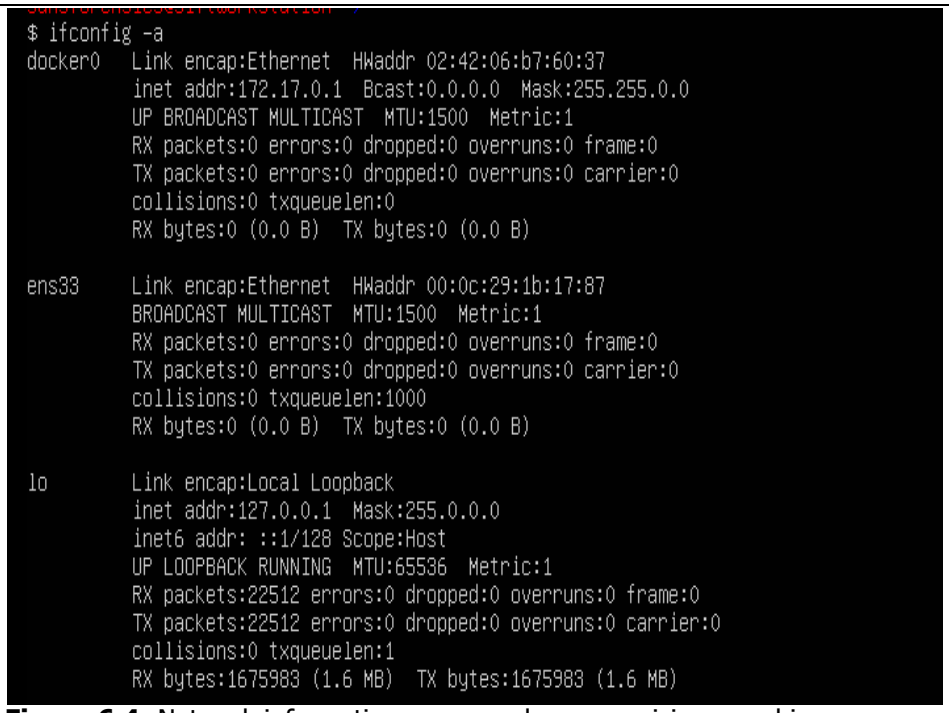


Figure 6.4: Network information command on a suspicious machine.

- **Network connections**: Open ports and programs associated with various ports; Are there any suspicious local network connections? , Are there any suspicious open ports? , Are there any port home to malicious services? These questions can be answered using the command "netstat –anp". See figure 6.6.

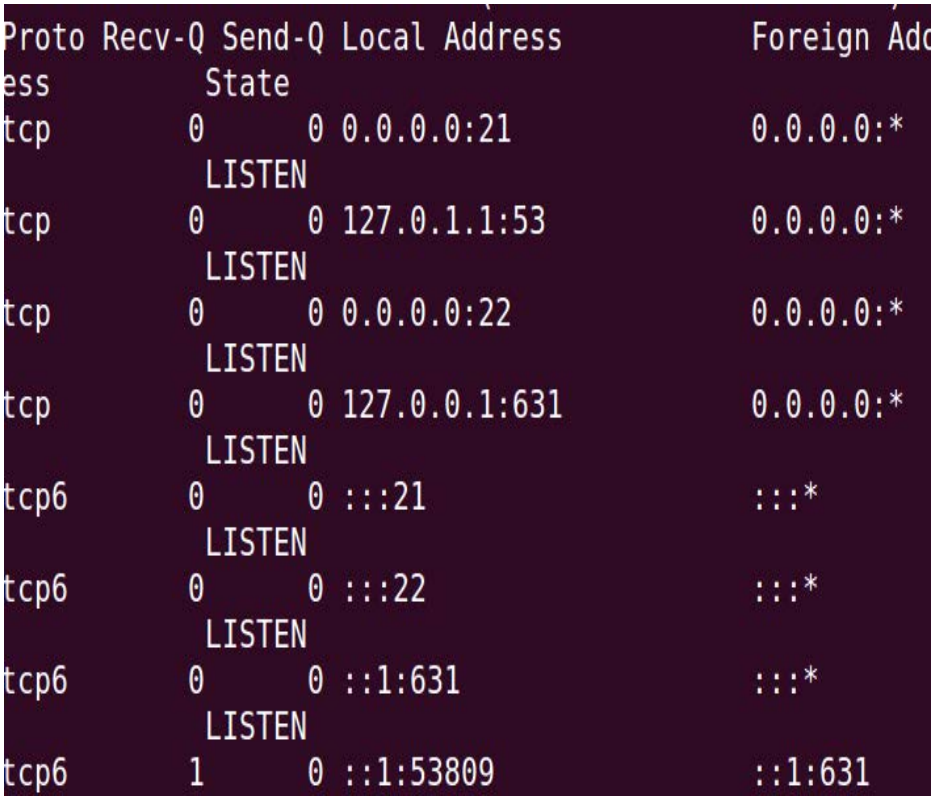


Figure 6.6: netstat command and unusual port 53809 on a suspicious machine.

- **Open files:** it can be insightful to see which programs are opening certain files. Figure 6.7 illustrates the command to view open files.

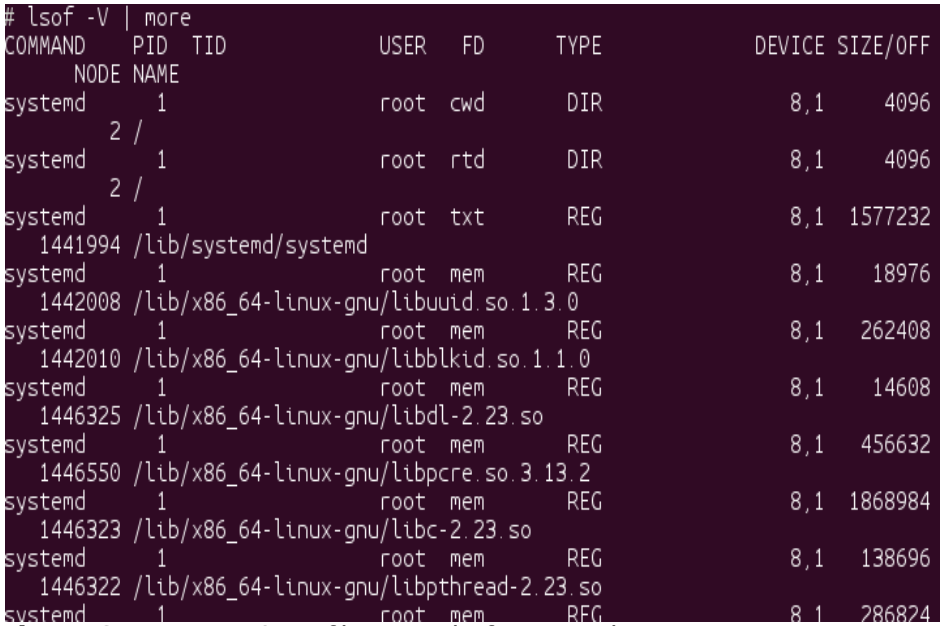


Figure 6.7: Viewing Open files using lsof command.

- **Routing Tables:** Is your traffic being rerouted through an interface controlled and/or monitored by an attacker? Have any gateways been changed? These and other questions can be answered by examining the routing table. There is more than one way to obtain this information. Two of these ways are to use the "*netstat –rn"* and *route* commands. It would be recommend running both commands as a rootkit might alert you to its presence by altering the results of one or both of these commands.

- **Mounted filesystems:** Are any suspicious volumes mounted on the system? Is one of the filesystems suddenly filling up? What are the permissions and options used to mount each partition? Are there unusual temporary filesystems that will vanish when the system is rebooted? The "df (disk free)" and mount commands can answer these types of questions. See figure 6.7.

```
root@siftworkstation -> ~
# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=478364k,nr_inodes=119591,mod
e=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmod
e=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=99776k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relat
ime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xa
ttr,release_agent=/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpu
set)
```

Figure 6.8: Mount command.

- **Loaded kernel modules:** Are there any trojaned kernel modules? Is there any device drivers installed that the client does not know anything about? Figure 6.9 allows you to answer these questions.

```
root@siftworkstation -> ~
# lsmod
Module                  Size  Used by
ipt_MASQUERADE         16384  1
nf_nat_masquerade_ipv4    16384  1 ipt_MASQUERADE
nf_conntrack_netlink    40960  0
nfnetlink              16384  2 nf_conntrack_netlink
xfrm_user              32768  1
xfrm_algo              16384  1 xfrm_user
iptable_nat            16384  1
nf_conntrack_ipv4      16384  2
nf_defrag_ipv4         16384  1 nf_conntrack_ipv4
nf_nat_ipv4            16384  1 iptable_nat
xt_addrtype            16384  2
iptable_filter         16384  1
ip_tables              24576  2 iptable_filter,iptable_nat
xt_conntrack           16384  1
x_tables               36864  5 ip_tables,ipt_MASQUERADE,xt_conntrack,iptable_fi
lter,xt_addrtype
nf_nat                 24576  2 nf_nat_ipv4,nf_nat_masquerade_ipv4
nf_conntrack          106496  6 nf_nat,nf_nat_ipv4,xt_conntrack,nf_nat_masquerad
e_ipv4,nf_conntrack_netlink,nf_conntrack_ipv4
br_netfilter           24576  0
```

Figure 6.9: lsmod command.

- **Users past and present**: Who is currently logged in? What command did each user last run? Who has been logging in recently? Failed login attempted? Figure 6.10 answer these questions.

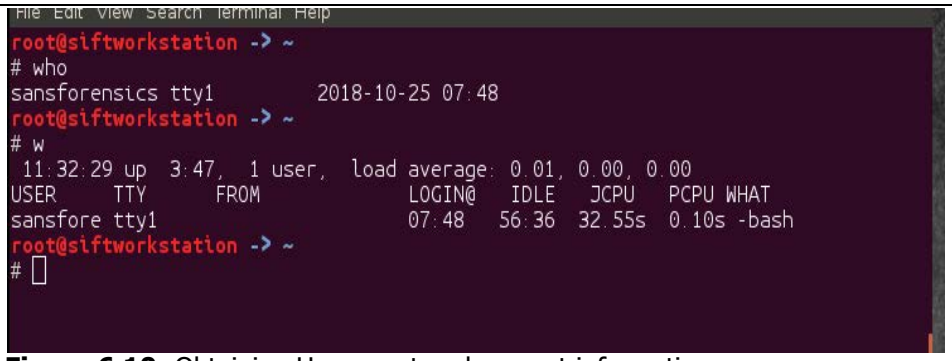


Figure 6.10: Obtaining Users past and present information.

Are there any new accounts created by an attacker? Has someone modified accounts to allow system accounts to login? Was the system compromised because a user had an insecure password? Examining of the */etc/passwd* and */etc/shadow* files help you answer these questions.

Content Template	
Section Number	6.6
Section Title	Memory dumping
Introduction	In this section we will discuss the tools and steps that are required to dump a memory for Linux operating system.
Content	Based on initial data collection and users interview, and you are not sure that everything is good , for examples; you found network interfaces enabled, routing tables manipulated , a lot of open ports, suspicious port and process. If this case you should take the next step which is live analysis to dump the RAM and proceed to dead analysis. The good way to get information from running system is to get a copy of what is in RAM, this is called memory dumping. Before many years dumping memory was so easy. Memory was a gigabyte or less, it was very easy to acquire a memory image in Linux. The device /dev/mem represented all of the physical RAM. This device still exists today, but it is only capable of accessing the first 896 MB of physical RAM. There are hardware devices and software tools for capturing memory. In this chapter we will talk about software tool "LIME" which will be used to dump the memory. **Using LIME:** The Linux Memory Extractor (LIME) is the tool of choice for extracting memory on Linux systems for a couple of reasons. First, it is very easy to use. Second, it is compatible with most volatility memory analysis framework. LIME must be built from source, LIME should be built for the exact kernel version of the subject system "you can obtain the kernel version using the command uname -a". Figure 6.11 shows how to install LIME on the suspicious machine.

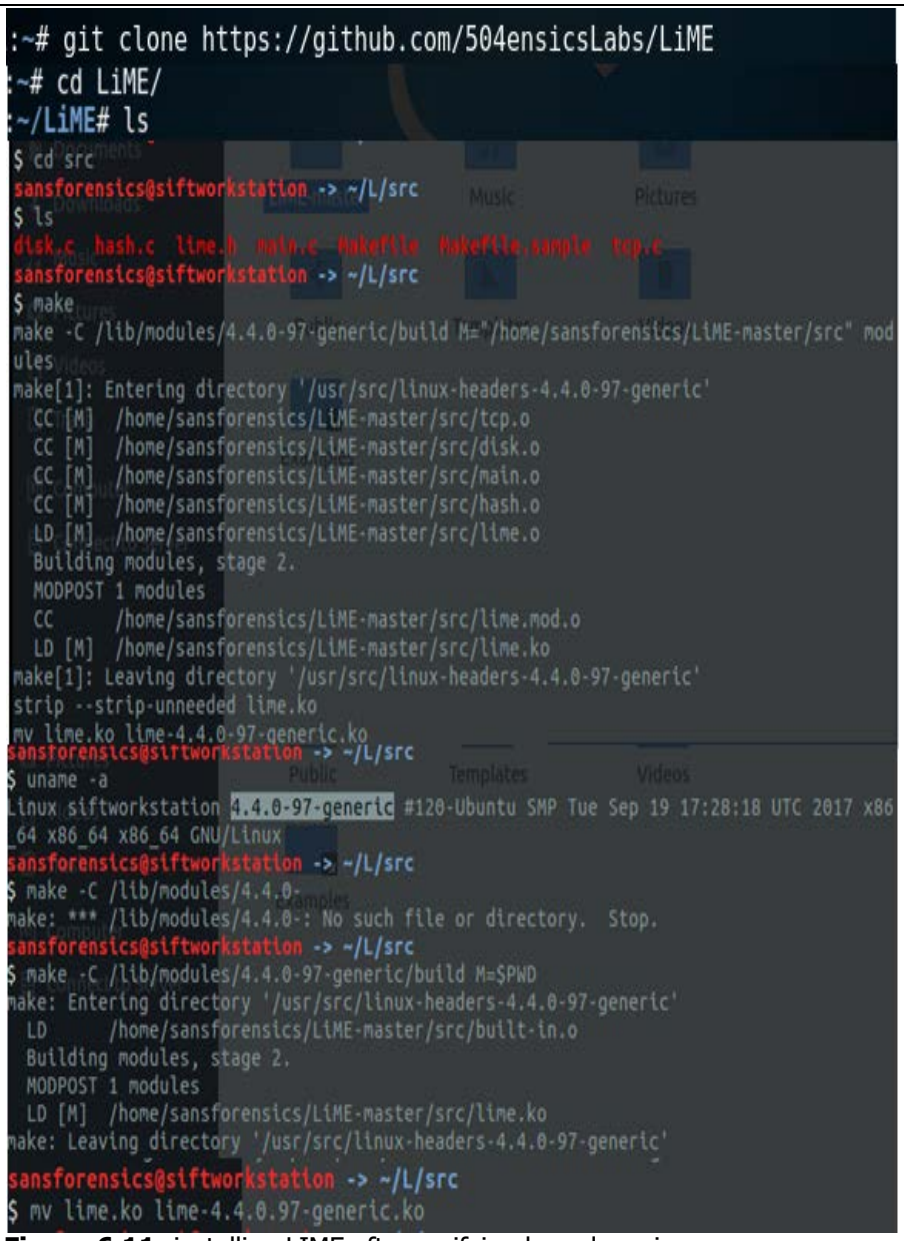
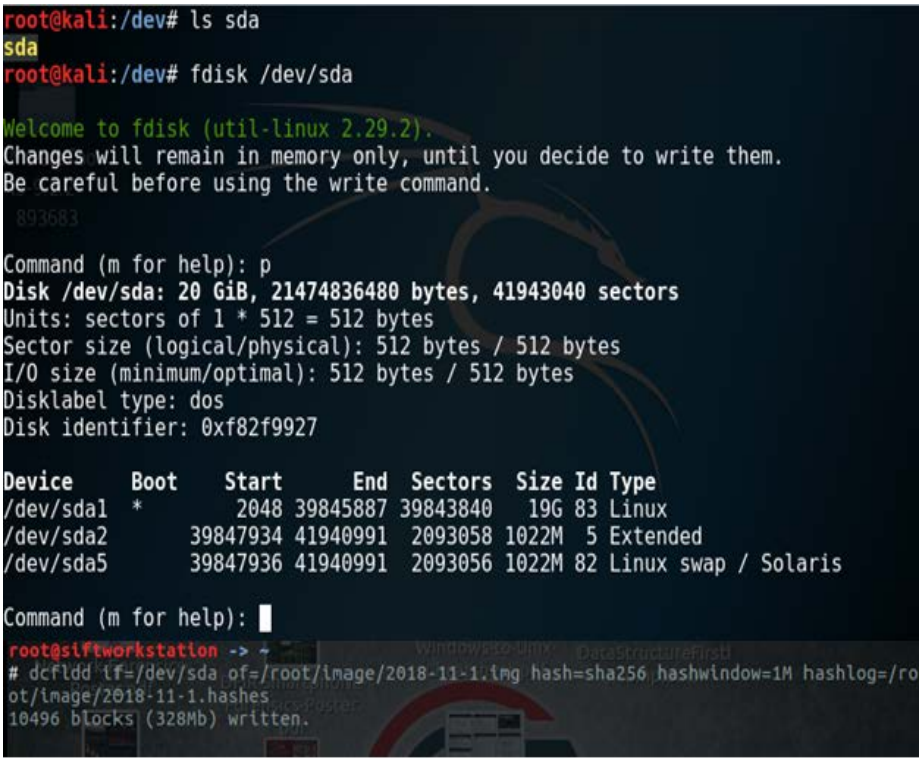


Figure 6.11: installing LIME after verifying kernel version.

After installation we want to dump the memory, before using LIME we must determine the format of memory dumps and the path where you want to dump the memory, the path usually will be your mounted USB flash drive or network path as netcat. There are three format choices: raw, padded, and LiME. Raw format is every memory segment concatenated together. When using the raw format, areas of memory containing blocks of zeros are skipped. Padded is similar to raw, but the zeros are retained so you can know the location of memory chunks, not just their contents. LIME format this format captures memory and stores it in structures complete with metadata, and we will use this format. Figure 6.12 will illustrate how to dump a memory from the suspected machine to our forensic machine. Figure 6.13 shows how our forensic workstation accepts the memory dump, note that it will take sometimes in memory dumping.

Figure 6.12: dumping ram in the suspicious machine.

	 **Figure 6.13**: getting the dumped ram into forensic workstation

Content Template	
Section Number	6.7
Section Title	offline image
Introduction	In this section we will discuss the procedures for offline analysis to the Linux system.
Content	The next step in our forensic investigation process is to perform a dead analysis to the system, by taking an image for the system. There are different tools that we can use to take an image for a Linux system other than live Linux cd, such as dd and dclfdd tool. In our case we are going to take an image using "dclfdd" as illustrated in figure 6.14. It is recommended to view system partition before take the image using "fdisk" command. It is highly recommended imaging the entire drive if it all possible. First, it becomes much simpler to mount multiple partitions. Second, any string searches can be performed against everything you have collected, including swap space, which is created as a separate partition on most modern Linux kernels, and it is used to substitute disk space for RAM memory when real RAM fills up and more space is needed. Finally, there could be data hidden in unallocated space (not part of any partition). There are different type images; Raw, Proprietary with embedded metadata, Proprietary with metadata in separate file and Raw with hashes stored in a separate file. The easiest one is raw, because it takes the media disk as it is.  **Figure 6.14**: creating an image for the entire system. After successfully taking the image and save it in your mounted USB, you have to decide how to shut down the suspicious system. The recommended way in any forensic situation is plug off the system from the power source. Because if you do normal shutdown for the system, this may allow some malwares or rootkits system to clean up themselves and you don't want this. For this, you should clean your files system (for instance flush cashes), then plug off the system from the power supply. Figure 6.15 shows how to clean up file system before unplugs the suspicious system.

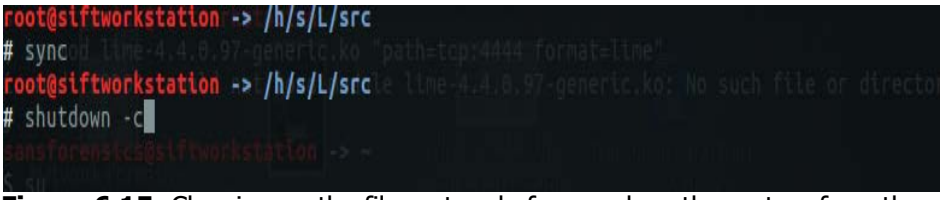


Figure 6.15: Cleaning up the file system before unplugs the system from the power source.

After shutting down the system you have to mount the image to perform a dead analysis. And here you start your comprehensive analysis for the system. In other word, real investigation starts now.

Content Template	
Section Number	6.8
Section Title	Start of the analysis
Introduction	This section will show how to start the analysis for the suspicious image file in our forensic machine.
Content	After getting the image for the suspicious machine ".img file", you should create the image to your forensic machine as a device then mounting this device to start the analysis of that system, figure 6.16 shows how to create the image, and figure 6.17 illustrates the mounting of the image as a hard disk on the forensic machine. You have to notice the type of partition you are mounted (i.e. ext2 or ext3 or ext4).

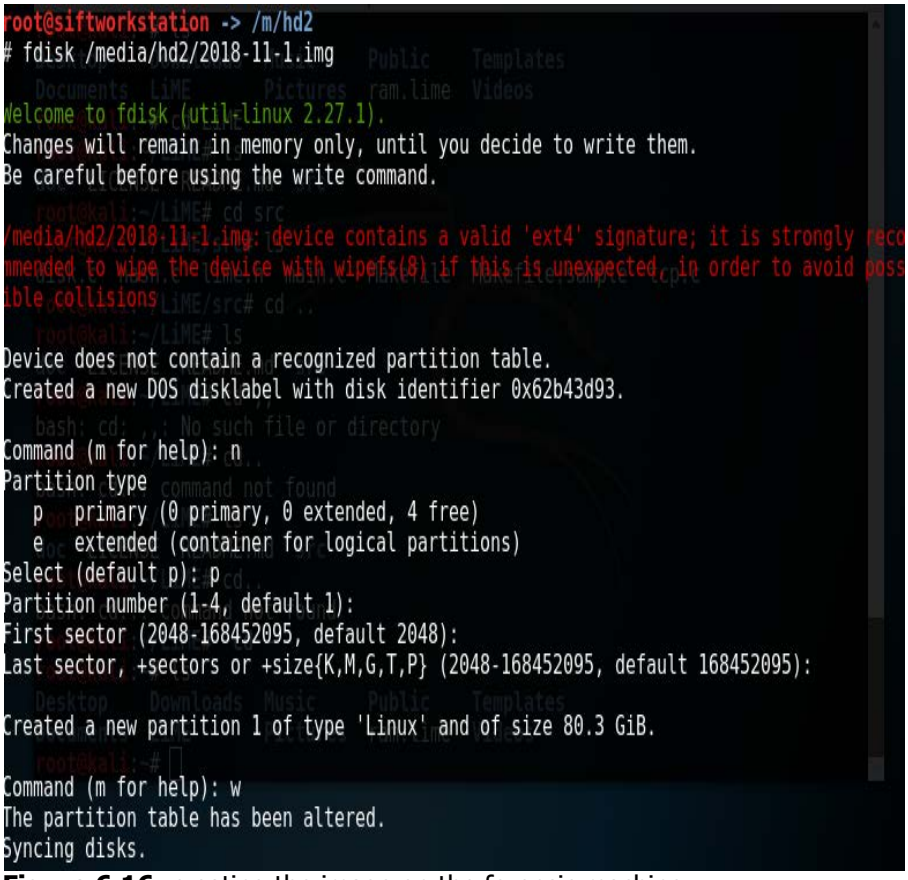


Figure 6.16: creating the image on the forensic machine.

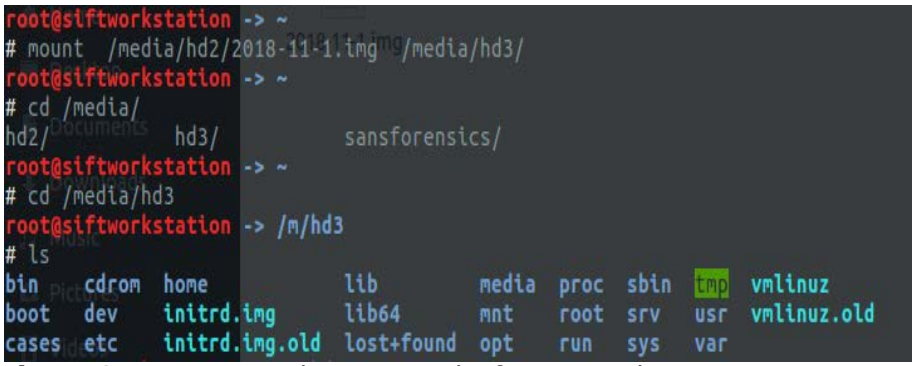


Figure 6.17: mounting the image in the forensic workstation.

	Now we have to EXAMIN BASH HISTORIES, we used a script to extract users' bash command histories. The following code is used to extract user bash histories.
	#!/bin/bash
	#
	# get-histories.sh
	#
	# Simple script to get all user bash history files and .
	# by Dr. Phil Polstra (@ppolstra) as developed for
	# PentesterAcademy.com.
	usage () {
	echo "usage: $0 <mount point of root> [database name]"
	echo "Simple script to get user histories and \
	optionally store them in the database"
	exit 1
	}
	if [$# -lt 1] ; then
	usage
	fi
	# find only files, filename is .bash_history
	# execute echo, cat, and echo for all files found
	olddir=$(pwd)
	cd $1
	find home -type f -regextype posix-extended \
	-regex "home/[a-zA-Z.]+(/.bash_history)" \
	-exec awk '{ print "{};" $0}' {} \; \
	| tee /tmp/histories.csv
	# repeat for the admin user
	find root -type f -regextype posix-extended \
	-regex "root(/.bash_history)" \
	-exec awk '{ print "{};" $0}' {} \; \
	| tee -a /tmp/histories.csv
	cd $olddir
	
	We have to execute this script in the mounted image directory. If you read the script you should notice that the results will be saved in a .csv file in the /tmp directory. Figure 6.18 shows how to run the bash history script. Figure 6.19 examines some of the interested results from .csv that may be helpful in the investigation.

```
root@siftworkstation -> /h/s/Scripts
# ./035-get-histories.sh /media/hd3/
home/sansforensics/.bash_history;sudo apt-get update && sudo apt-get upgrade
home/sansforensics/.bash_history;clear
home/sansforensics/.bash_history;sudo apt-get upgrade
home/sansforensics/.bash_history;sudo apt-get autoclean
home/sansforensics/.bash_history;sudo apt-get autoremove
home/sansforensics/.bash_history;clear
home/sansforensics/.bash_history;exit
home/sansforensics/.bash_history;sudo reboot
home/sansforensics/.bash_history;sudo shutdown -h now
home/sansforensics/.bash_history;sudo shutdown -h now
home/sansforensics/.bash_history;exit
home/sansforensics/.bash_history;sudo shutdown -h now
home/sansforensics/.bash_history;su
home/sansforensics/.bash_history;sudo passwd root
home/sansforensics/.bash_history;su
home/sansforensics/.bash_history;uname -a
home/sansforensics/.bash_history;ifconfig -a
home/sansforensics/.bash_history;netstat -anp
home/sansforensics/.bash_history;startx
home/sansforensics/.bash_history;sudo
home/sansforensics/.bash_history;su
home/sansforensics/.bash_history;apt-get install lime-forensics-dkms
home/sansforensics/.bash_history;su
home/sansforensics/.bash_history;ifconfig
```

Figure 6.18: Extracting bash history commands using bash history script.

Figure 6:19: Examining important events resulted from the bash history script, interested events are highlighted.

Several interesting commands from the john account's bash history are shown in Figure 6.19 It can be seen that this user created the johnn account, copied /bin/true to /bin/false, created passwords for whoopsie and lightdm, copied /bin/bash to /bin/false, edited the group file, move the johnn user's home directory from /home/johnn to /home/.johnn (which made the directory hidden), edited the password file, displayed the man page for sed, used sed to modify the password file, and installed a rootkit. Copying /bin/bash to /bin/false was likely done to allow system accounts to log in. This might also be one source of the constant "System problem detected".
Next we might want to have a look at various system logs files as part of our investigation. These files are located under /var/log. "You should know how Linux saved and archived the log files".
The following script allows you to capture logs files for our analysis and save it in a .CSV file. This script will only capture the current log. After examining the results of current log, and if you feel that you need to returns to archived logs you can run this script against archived version of these logs files.

```
#!/bin/bash
# Simple script to get all logs and optionally
# store them in a database.
```

```
# Warning: This script might take a long time to run!
# by Dr. Phil Polstra (@ppolstra) as developed for
# PentesterAcademy.com.

usage () {
        echo "usage: $0 <mount point of root> [database name]"
        echo "Simple script to get log files and optionally store them to a
database."
        exit 1
}

if [ $# -1t 1 ] ; then
  usage
fi

# find only files, exclude files with numbers as they are old logs
# execute echo, cat, and echo for all files found
olddir=$(pwd)
cd $1/var
find log -type f -regextype posix-extended -regex 'log/[a-zA-Z\.]+(/[a-zA-
Z\.]+)*' \
  -exec awk '{ print "{};" $0}' {} \; | tee /tmp/logfiles.csv
cd $olddir
```

The result of this script will be stored in the /tmp directory. Several of these logs, such as apt/history.log, apt/term.log, and dpkg.log, provide information on what has been installed via standard methods. You can examine them and you will see that user john install an application in the system. It is quite possible that even a savvy attacker might not clean their tracks in all of the relevant log files. It is certainly worth a few minutes of your time to browse through a sampling of these logs. Figure 6.20 shows some important information that was extracted from these logs files "you should notice the date to connect the evidence".

log/fontconfig.log:/usr/share/fonts: caching
log/fontconfig.log:/usr/local/share/fonts: caching
log/fontconfig.log:/.local/share/fonts: skipping
log/fontconfig.log:/var/cache/fontconfig: cleaning cache directory
log/fontconfig.log:/.cache/fontconfig: not cleaning non-existent cache directory
log/fontconfig.log:fc-cache: succeeded
log/wtmp;┐
log/apt/history.log:
log/apt/history.log:Start-Date: 2018-02-18 19:34:14
log/apt/history.log:Commandline: apt-get --yes upgrade
log/apt/history.log:Upgrade: mime-support:amd64 (3.54ubuntu1
log/apt/history.log:End-Date: 2018-02-18 19:34:21
log/apt/history.log:
log/apt/history.log:Start-Date: 2018-02-18 19:34:49
log/apt/history.log:Commandline: apt-get --yes install linux-generic-lts-utopic ubuntu-minimal ubuntu-standard ubuntu-desktop unity-settings-daemon notify-osd libqt4-sql-sqlite unity gnome-ter
log/apt/history.log:Install: dvd+rw-tools:amd64 (7.1-10build1
log/apt/history.log:End-Date: 2018-02-18 19:38:53
log/apt/history.log:
log/apt/history.log:Start-Date: 2018-02-18 19:39:02
log/apt/history.log:Commandline: apt-get --yes install lupin-casper linux-signed-generic-lts-utopic btrfs-tools cifs-utils cryptsetup cryptsetup-bin dmraid dpkg-repack ecryptfs-utils gir1.2-json-1.0 gi
log/apt/history.log:Install: linux-signed-image-generic-lts-utopic:amd64 (3.16.0.30.23
log/apt/history.log:End-Date: 2018-02-18 19:39:50
log/apt/history.log:
log/apt/history.log:Start-Date: 2018-03-05 22:42:39
log/apt/history.log:Install: myspell-en-au:amd64 (2.1-5.4)
log/apt/history.log:Upgrade: firefox-locale-en:amd64 (35.0.1+build1-0ubuntu0.14.04.1
log/apt/history.log:End-Date: 2018-03-05 22:43:17
log/apt/history.log:
log/apt/history.log:Start-Date: 2018-03-05 22:44:10
log/apt/history.log:End-Date: 2018-03-05 22:44:10
log/apt/history.log:
log/apt/history.log:Start-Date: 2018-03-05 22:44:29
log/apt/history.log:Purge: linux-signed-image-generic-lts-utopic:amd64 (3.16.0.30.23)
log/apt/history.log:End-Date: 2018-03-05 22:44:58

Figure 6.20: Examining some important logs, important events are highlighted.

Next we have to examine login and login attempts, the following script will do the job for you. Note that this script is based on last and lastb commands.

```
#!/bin/bash
# Simple script to get all successful and unsuccessful
# login attempts and optionally store them in a database.
#
# by Dr. Phil Polstra (@ppolstra) as developed for
# PentesterAcademy.com.

usage () {
        echo "usage: $0 <mount point of root> [database name]"
        echo "Simple script to get logs of successful and unsucessful logins."
      echo "Results may be optionally stored in a database"
        exit 1
}

if [ $# -1t 1 ] ; then
  usage
fi

# use the last and lastb commands to display information
# use awk to create ; separated fields
# use sed to strip white space
```

```
echo "who-what;terminal-event;start;stop;elapsedTime;ip" | tee
/tmp/logins.csv
last -aiFwx -f $1/var/log/wtmp | \
  awk '{print substr($0, 1, 8) ";" substr($0, 10, 13) ";" substr($0, 23, 24) ";"
substr($0, 50, 24) ";" substr($0, 75, 12) ";" substr($0, 88, 15)}' \
  | sed 's/[[:space:]]*;/;/g' | sed 's/[[:space:]]+\n/\n/' \
  | tee -a /tmp/logins.csv

echo "who-what;terminal-event;start;stop;elapsedTime;ip" | tee /tmp/login-
fails.csv
lastb -aiFwx -f $1/var/log/btmp | \
  awk '{print substr($0, 1, 8) ";" substr($0, 10, 13) ";" substr($0, 23, 24) ";"
substr($0, 50, 24) ";" substr($0, 75, 12) ";" substr($0, 88, 15)}' \
  | sed 's/[[:space:]]*;/;/g' | sed 's/[[:space:]]+\n/\n/' \
  | tee -a /tmp/login-fails.csv
```

The results of executing this script on our mounted image will also be saved in the /tmp directory. Again you have to examine the entries to find something that may be useful; such as comparing the time of login and the time of installing the suspicious software in the system. Figure 6.21: shows the failed login, and Figure 6.22 shows success login. Interesting incidents are highlighted.

```
who-what;terminal-event;start;stop;elapsedTime;ip
john;ssh:notty;Sun Nov 11 03:25:39 2018;Sun Nov 11 03:25:39 2018; (00:00);192.168.60.1
john;ssh:notty;Sun Nov 11 03:23:59 2018;Sun Nov 11 03:23:59 2018; (00:00);192.168.60.1
john;;Sat Nov 10 04:10:34 2018;Sat Nov 10 04:10:34 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:09:28 2018;Sat Nov 10 04:09:28 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:09:19 2018;Sat Nov 10 04:09:19 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:09:03 2018;Sat Nov 10 04:09:03 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:08:54 2018;Sat Nov 10 04:08:54 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:08:49 2018;Sat Nov 10 04:08:49 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:08:45 2018;Sat Nov 10 04:08:45 2018; (00:00);0.0.0.0
john;:0;Sat Nov 10 04:05:39 2018;Sat Nov 10 04:05:39 2018; (00:00);0.0.0.0
lightdm;ssh:notty;Mon Mar  9 21:33:55 2018;Mon Mar  9 21:33:55 2018; (00:00);192.168.56.1
;;;;;
btmp beg;ns Mon Mar  9; 21:33:55 2018;;;
```

Figure 6.21: Failed login report.

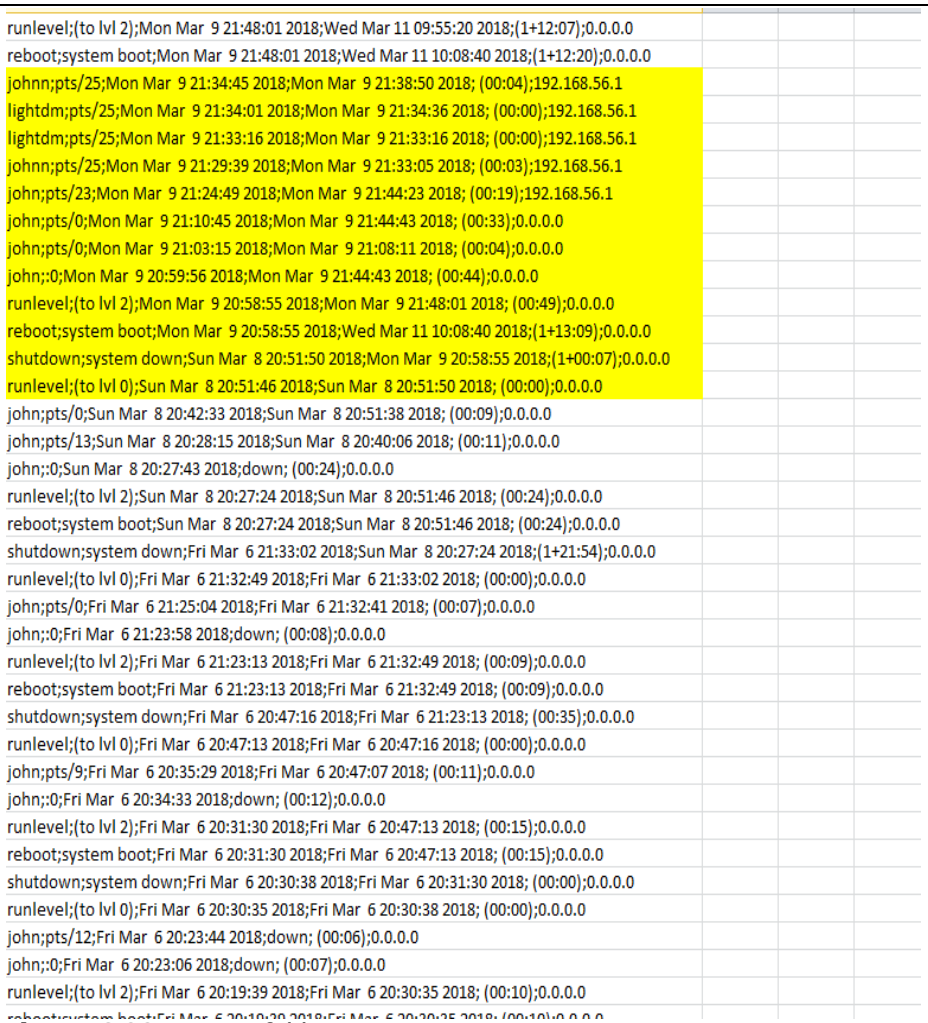


Figure 6.22: successful login report.

From the failed login and success login reports it can be seen that the attacker failed to log in remotely from IP address 192.167.56.1 as lightdm on 2018-03-09 21:33:55. Around that same time the john, johnn, and lightdm accounts had successful logins from the same IP address. The attacker appears to be testing some newly created accounts.

Next we will dig into Linux extended filesystems which will allow us, among other things, to detect data that has been altered by an attacker. Some of the system directories such as /sbin and /bin are highly targeted by attackers. Even the simple ls command can often be enough to detect alterations in these directories. How can we detect tampering in a system directory? When the system is installed, files in the system directories are copied one after the other. As a result, the files are usually stored in sequential inodes. Anything added later by an attacker will likely be in a higher inode number. "Inodes contain all the metadata for a file. They also contain the location of the file's data blocks". The results of running ls -ali bin | sort -n from within the mount directory (subject's root directory) of the subject system are shown in Figure 6.23. Files associated with the Xing Yi Quan rootkit are highlighted. Notice that the inodes are mostly sequential and suddenly jump from 655,549 to 657,076 when the malware was installed.

```
655547 -rwxr-xr-x  1 root root    2039 Jan 10  2018 zles
s
655548 -rwxr-xr-x  1 root root    1912 Jan 10  2018 zmor
e
655549 -rwxr-xr-x  1 root root    5049 Jan 10  2018 znew
657076 -rwxr-xr-x  1 root root   14056 Mar 12  2018 xing
yi_reverse_shell
657094 -rwxr-xr-x  1 root root   27096 Jun 13  2018 nc.t
raditional
657103 -rwxr-xr-x  1 root root   14723 Mar 12  2018 xing
yi_bindshell
657109 -rwxr-xr-x  1 root root    9660 Mar 12  2018 xing
yi_rootshell
```

Figure 6.23: the results of running ls –ali command.

The command ls –aliR bin –sort=size will perform a recursive (-R) listing of a directory with everything sorted by size (largest to smallest). Partial results of running ls -aliR bin –sort=size are shown in Figure 6.24.

```
root@sansforensic:~# ls -aliR  /bin  sort=size
ls: cannot access sort=size: No such file or directory
/bin:
total 10940
655403 -rwxr-xr-x  1 root root  110080 Jan 13  2018 dir
655404 -rwxr-xr-x  1 root root   22896 Feb 12  2018 dmesg
655405 lrwxrwxrwx  1 root root       8 Mar  5  2018 dnsdomai
655406 lrwxrwxrwx  1 root root       8 Mar  5  2018 domainna
655407 -rwxr-xr-x  1 root root   82256 Feb 18  2018 dumpkeys
655408 -rwxr-xr-x  1 root root   31296 Jan 13  2018 echo
655409 -rwxr-xr-x  1 root root   47712 Jul 16  2018 ed
655410 -rwxr-xr-x  1 root root  183696 Jan 18  2018 egrep
655411 -rwxr-xr-x  1 root root 1021112 Mar  9  2018 false
```

Figure 6.24: the results of running ls -aliR bin –sort=size command.

If you look at the highlighted bash and false files from Figure 6.24. Did you notice anything unusual? The only thing /bin/false does is return the value false when called. Yet this is one of the three largest files in the /bin directory. It is also suspiciously the exact same size as /bin/bash. What appears to have happened here is that the attacker copied /bin/bash on top of /bin/false in an attempt to login with system accounts.

Next we have to analyze the memory dump that we took previously, we will use The Volatility framework to do the analysis. "Volatility framework is an open source tool written in Python which allows you to analyze memory images." Before start analysis using Volatility, it needs to setup a profile and the reason for this is that every version of Linux, and every kernel of version could be slightly different in order to make sure that you have the correct exact right structures. This is done by creating your own profile by compiling a specific program; creating a dwarf file; getting a system map file; and zipping everything together. Before making a profile you have to mount the image of the system on your forensic machine.

The following script will create the profile in the mounted image path and output it in a zip file according to your kernel version. But you have to download make and module.c files from VOLATILITY website before running the script. Figure 6.25 illustrate how to create a profile.

```
#!/bin/bash
#
# create-profile.sh
#
# Simple script to create a makefile for a Volatility profile.
# Intended to be used with an image file.
# As developed for PentesterAcademy
# by Dr. Phil Polstra (@ppolstra)
usage() {
echo "Script to create a Volatility profile from a mounted image file"
echo "Usage: $0 <path to image root>"
exit 1
}
if [ $# -lt 1 ] ; then
usage
fi
oldir=$(pwd)
cd ${1}/boot
ver=$(ls System.map* | sed "s/System.map-//" | tr "\n" "|" \
| sed -nr 's/([a-zA-Z0-9\.\-]+\|)*([a-zA-Z0-9\.\-]+\|)$/\2/p' \
| sed "s/|/\n/")
cd "${oldir}"
echo "Version: ${ver}"
PWD=$(pwd)
MAKE=$(which make)
cat <<EOF > Makefile.${ver}
obj-m += module.o
-include version.mk
all: dwarf
dwarf: module.c
${MAKE} -C ${1}/lib/modules/${ver}/build \
CONFIG_DEBUG_INFO=y M="${PWD}" modules
dwarfdump -di module.ko > module.dwarf
${MAKE} -C ${1}/lib/modules/${ver}/build M="${PWD}" clean
clean:
${MAKE} -C ${1}/lib/modules/${ver}/build M="${PWD}" clean
rm -f module.dwarf
EOF
# make the dwarf file
make -f Makefile.${ver}
# copy the System.map file
cp ${1}/boot/System.map-${ver} ./.
# now make the zip
zip Linux${ver}.zip module.dwarf System.map-${ver}
```

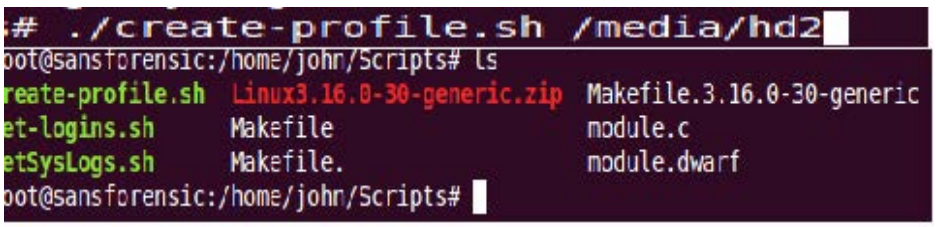


Figure 6.25: creating the profile on the mounted image.

After creating the profile copy it to VOLATILITY path "where you download it" in my case /home/john.Scripts/volatility/plugins/overlays/linux, after that you

can use VOLATILITY to get information about the running processes from the dumped RAM ".LIME file", see figure 6.26.

```
root@sansforensic:/home/john/Scripts/volatility-master# ./vol.py  --profile=LinuxAMD64Paged
Memory   -f /home/john/Scripts/ram.lime linux_pslist
xffff8800368b9e90 ext4-rsv-conver     131          0          0     ..................
xffff88007c1e5180 upstart-udev-br     254          0          0     0x000000007a457000
xffff88007a5b9460 systemd-udevd       261          0          0     0x000000007a54b000
xffff8800368bb2f0 iprt                314          0          0     ..................
xffff8800368b9460 kworker/0:1H        317          0          0     ..................
xffff88007922 0a30 dbus-daemon        505          102        106   0x0000000079d67000
xffff8800792e8a30 ModemManager        552          0          0     0x000000007abf5000
xffff8800792ec750 rsyslogd            567          101        104   0x0000000079d3c000
xffff880079225180 upstart-socket-     610          0          0     0x000000007a479000
xffff880079227010 upstart-file-br     613          0          0     0x0000000078a78000
xffff88007c1e65e0 bluetoothd          642          0          0     0x0000000079258000
xffff8800792e9460 krfcommd            649          0          0     ..................
xffff8800792e8000 systemd-logind      655          0          0     0x0000000079678000
xffff8800792eb2f0 avahi-daemon        658          111        117   0x0000000078830000
xffff8800792edbb0 avahi-daemon        663          111        117   0x000000007a475000
ff88006e880000 xingyi_bindshel     3027 ——    0          0     0x00000005d2be000
```

Figure 6.26: running processes from the dumped ram.

From the figure 6.27 you can see that the rootkit xingyi appears to be loaded at the memory and it is running. Next you have to study the behavior of this rootkit from the same memory dump by trying to study the port that is connected to this process and analyze the traffic using sophisticated tool such as wireshark, I will leave this task for you.
Now you are ready for the final step which is reporting . Your report should normally include an executive summary of less than a page, narrative that is free of unexplained technical jargon, and concrete on recommendations. As from the collected evidence all suspicious goes to user john. But this conclusion is not 100% correct…..?

Content Template	
Section Number	6.9
Section Title	Summary
Introduction	
Content	This chapter introduced a simple Linux forensic investigation. In this chapter we focused on using free tools for Linux investigation. Additionally you have learned that investigation worked by start talking to users, and then analyze basic information, followed by dumping the memory and imaging the system, after that you start the analysis of system, finally reporting the evidence. .

Activity Template	
Number	6.1
Title	Case study
Type	Research
Aim	The aim of this activity is to put the student in a real forensic problem, to measure his/her ability for solving real life forensic scenario.
Description	A web server running apache was hacked, and this web server is hosted at a Linux operating system in a local hosting company, you are called to find out how this system was hacked and compromised? (Hint: use apache access log file to find out the problems. Apache access log is available at "https://bit.ly/2LEKKbu")
Timeline	1 weeks
Assessment	The document will be assessed based on Logic, correctness and overall quality

Activity Template	
Number	6.2
Title	Case study
Type	Research
Aim	The aim of this activity is to put the student in a real forensic problem, to measure his/her ability for solving real life forensic scenario.
Description	Perform a deep network analysis to xing rootkit, you should create your own packet for analysis? (Hint: you can download the rootkit from "https://sw0rdm4n.wordpress.com/2014/11/03/xingyiquan-simple-linux-kernel-rootkit-for-kernel-3-x-and-kernel-2-6-x/" then you have to install it in a Linux machine, finally perform a network sniffing and analysis using wireshark)
Timeline	1 weeks
Assessment	The document will be assessed based on Logic, correctness and overall quality

Think Template (MCQs)	
Number	6.1
Title	Introduction
Type	Fill in the blanks
Question	_____ is one of Linux distribution that is shipped with open source forensics tools.
Answers	SWIFT

Think Template (MCQs)	
Number	6.2
Title	Introduction
Type	Fill in the blanks
Question	_____ command, lists of all the partitions that are available for a drive
Answers	fdisk –l /dev/hdx

Think Template (MCQs)	
Number	6.3
Title	Initial data collecting
Type	Fill in the blanks
Question	_____ and _____, are the required steps before start your investigation.
Answers	• TALKING TO USERS • Minimize memory footprint

Think Template (MCQs)	
Number	6.4
Title	Memory Dumping
Type	Fill in the blanks
Question	You should know _____ before performing Memory dumping "profiling" and analysis.
Answers	the exact operating system and kernel version

Think Template (MCQs)	
Number	6.5
Title	Analysis
Type	Fill in the blanks
Question	_____ is a tool that can be used for memory analysis.
Answers	Volatility framework

Extra Template
Number 6.1
Title The Linux File System Structure Explained
Topic 6.1
Type URL:http://www.linuxandubuntu.com/home/the-linux-file-system-structure-explained

Extra Template
Number 6.2
Title Linux Forensics with Python and Shell Scripting
Topic 6.2,6.3,6.4,6.5,6.6,6.7,6.8
Type Book/Chapter 1 - 8 (ISBN-13: 978-1515037637)

7. Memory Forensics

Scope Template	
Number	7
Title	Memory Forensics
Introduction	This chapter introduces the basics of memory forensics. As memory forensics is very vast topic, this chapter will explain the memory artifacts that can be found on a running computer system, and the importance of their existence to forensic analysis. This chapter also will show what tools you can use to collect artifacts from memory and what tools to use for extracting the collected artifacts. This chapter additionally explains the main stages of memory forensics.
Outcomes	At the end of this chapter, students will be able to: 1- Explain what is memory forensics 2- Understand how memory forensics tools work 3- Define the main artifacts that can be collected and analyzed from memory 4- Understand the memory tools that collect evidence and conduct analysis
Topics	Memory Forensics Basics Memory artifacts The process of memory forensics The memory analysis progression The importance of memory forensics Memory forensics: Tools and Techniques
Study Guide	Instructions on how to study this unit. • Required study time: ○ Preparation: 3 hours ○ Disk-based Content: 2 hours ○ Practical activities: 4 hours • Required hardware/software: Volatility tool • Required external resources including links and books: JungTaek Seo, Seokjun Lee, Taeshik Shon, A study on memory dump analysis based on digital forensic tools, Peer-to-Peer Networking and Applications, Springer, Online Published, June 2013

Content Template	
Section Number	7.1
Section Title	Memory Forensics Basics
Introduction	This section demonstrates the basics of memory forensics and illustrates its importance in digital forensics.
Content	Memory forensics or memory analysis is defined as the examination of volatile data resides in a computer's memory dump. Volatile data is defined as the data resides a computer's short-term memory storage while the computer is running such as browsing history, chat messages, and clipboard contents. Volatile data will immediately be lost when a computer is turned off. For instance, you may lose your work (suppose that you were writing on a word document) when the computer is turned off before saving it to the hard drive of a computer or another non-volatile memory source. A memory dump is known as a replica or a copy of a computer memory data at a time of an incident such as a security compromise, computer system failure or a crash. Identifying the reason of the incident with all specifications and details about what happened can be done with the use of a memory dump in which contains Random Access Memory (RAM) data. Memory dumps allows experts to infer all diagnostic information during the incident since it has a code that responsible for that incident or crash. Thus, memory forensics allows experts or investigators to find buried evidence. RAM is considered as volatile computer data storage. RAM needs power to retain the stored information. RAM maintains its contents only during powered on. All stored data is quickly lost when the power is interrupted. A computer retains information in its memory address to be fetched or retrieved later. All data or information used wheatear by a computer program, or a hardware device will run through the computer's RAM when it is being used. Consequently, RAM analysis is a key task when conducting computer forensics. However, two main reasons show that RAM analysis is not conducted on every computer forensics. 1. **Procedural:** RAM analysis needs to run the target system and execute the collection program, thus leaving an acquisition footprint. Acquisition of system's RAM can give the only proof or evidence that an intrusion was committed since the improvement in malware technology. Soon, the court system will start to believe and to trust that law enforcement have demonstrated footprints during RAM acquisition onto the desired system. Therefore, reports by those examining the acquisition process is the key. 2. **Physical:** Upon shutting down the computer, RAM contents will be lost wiping away all RAM active information. Professionals in information security handle and conduct memory forensics in order to examine, identify and investigate malicious behaviors and attacks which are stealthy enough to avoid leaving data on the computer's hard drive. Memory Forensics aims at capturing the memory contents and it can add a very useful resource to malware analysis incident response, and digital forensics capacity. Although examination of network packet captures and hard disks can leave compelling verification, the reconstruction of events is

	accomplished by the contents of memory forensics. The contents of memory forensics determine what has already happened, what is presently happening, and what would happen with further infection through malware or an intrusion. For instance, a piece of evidence found in RAM could help to associate typical forensic artifacts that may appear different and allow for an integration which could otherwise remain unnoticed. Generally, there are several reasons behind collecting and analyzing the data locates in the computer memory. The memory includes real-time data regarding the operating system such as, all processes being operated, and the mounted file system. Although the encrypted data is commonly decrypted when storing in the computer memory. This method adapts well to the embedded systems as they are barely turned off (i.e. the data stored in the memory is mostly persistent). Thus, performing the analysis effectively on the computer memory can provide vital information. Different kinds of information could be extracted from the memory, such as dynamic link libraries (dll), processes, image identification, process memory, kernel memory, , registry, networking, and malware.

Content Template	
Section Number	7.2
Section Title	Memory artifacts
Introduction	This section illustrates the memory artifacts which can be extracted from a running computer and the importance of their presence to forensic analysis.
Content	RAM artifacts contain all data that is being employed by the computer software or the hardware device. The list of RAM artifacts acquired from a working computer can be entirely huge regarding the investigated forensic case. The input/output of any computer program travels through the memory will stay in RAM. Following points address a list of artifacts that can be found on a running computer system, and the importance of their existence to forensic analysis. 1- **Previous and present network connections.** The information of past and current network connections include remote IP address and the port number for network connections. All of this information is critical because: • It helps finding the remote target in which the malware is connecting with and identifying the destination of a company's ex-filtrated data. • It identifies (via port number) the traffic type which in a connection as a communication vector, for instance FTP, HTTP, SMTP or some ambiguous port recognized by the malware. Figure 1 shows an example of a network connection.

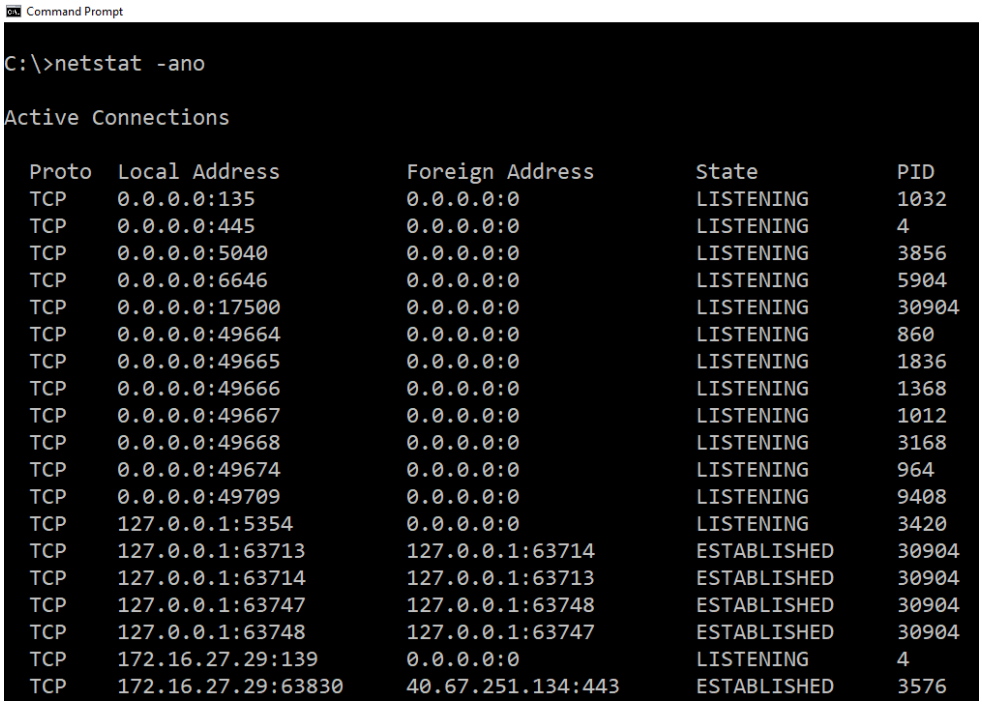


Figure 2. Network Connection

2- **The running processes upon RAM capturing.** Active programs upon RAM capturing can provide investigators with key information regarding how the

computer was being exploit. Visual examination of a computer system desktop or the Task Manager examination (see figure 2) provides details of what is working on a system, for instance Outlook, Limewire or Firefox. However, a running process such as a rootkit (rootkit is defined as a hidden Trojan that enables remote access; it is the keylogger that is transmitting overall user data) will not be revealed from a visual examination.

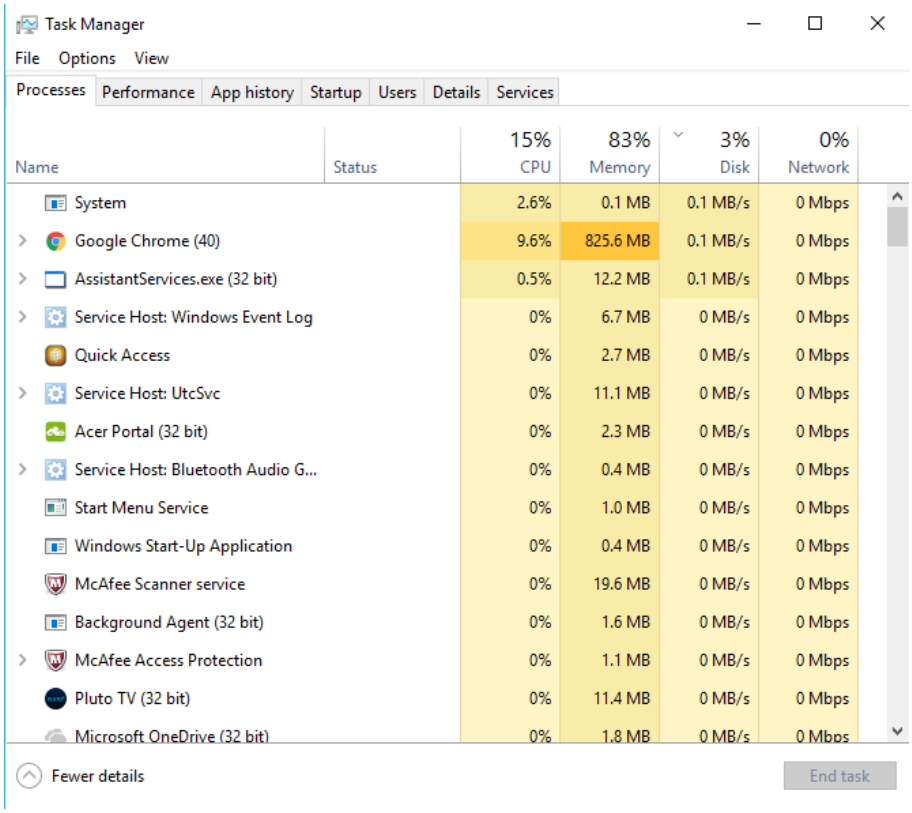


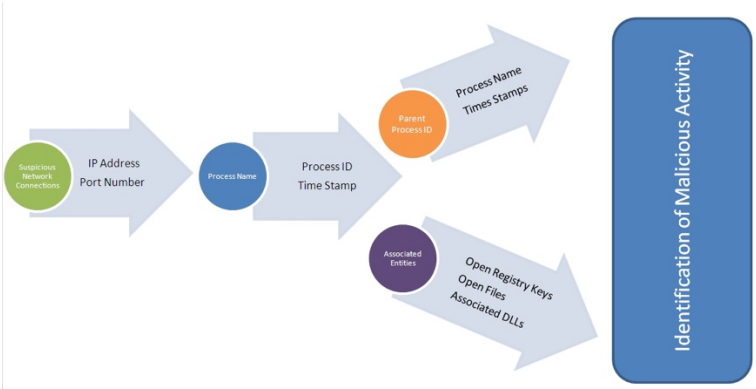
Figure 3. RAM Processes

3- **User names and passwords:** Users enters their credentials (user name and password) to access their internet or Internet Service Provider ISP account. Authentication is the process used to by users' access e-mail accounts, social networks, or their home's wireless access point. A user can investigate in the browser and other memory location where user credentials maintained permanently or temporary. The following tools can be used for password extracting.

- MessenPass
- PasswordFox
- Mail Passview
- Protected Storage PassView
- IE Passview

4- **Loaded Dynamically Linked Libraries (DLL).** Listing the running process' DLLs allows the recognition of a malicious DLL that has added itself to a process. This method is very significant regarding the Zeus botnet.

	5- **Open registry keys for a process.** Envision how critical it would be to be able to distinguish registry keys regarding a malicious process. By having the capacity to link open registry keys to a certain process, an expert could attach functionality to that process, for example encryption, networking capabilities, or being able to link the secure identifier (SID) to the user account who initiated the process. Additionally, it is essential to recognize the technique utilized by the malware to sustain reboot. This data can be recognized from the relation between a process and its registry keys. Note that the registry values will be those that are "open" during the RAM acquisition. However, the registry key that was in charge the malware surviving a reboot may still be listed in RAM and could be found by dumping the address space for that process. In any case, the library key that was in charge of the malware enduring a reboot could in any case be recorded in RAM and could be found by dumping the location space for that procedure. 6- **Open files for a process.** Having the capacity to list open records or files related with a process would uncover any open files that are currently being used by the identified malicious process. This is useful in distinguishing a resident file that is logging keystrokes, or user names and passwords. This is also essential in recognizing a configuration file used by a malicious process, regardless of whether it is encrypted on disk. This file could then be found in memory and its contents read. 7- **Contents of an open window.** • an e-mail client • values into a form field • any keystrokes into Webmail An IM chat client and chat sessions, including participants 8- **Unpacked/decrypted versions of a program.** The capability to carve out an identified malicious process out of memory is considered as one of the most valuable contributions that memory forensics can provide to an analyst. Generally, it is considered as a very hard procedure for analyst to decrypt a malicious file or binary and read its contents, when that file is encrypted on the hard drive. However, all files that are read or executed must decrypt itself in order to be able run. Thus, the malicious file could be identified, carved out of memory, and examined through static analysis or by scanning it with an anti-virus tool. 9- **Memory resident malware.** These malware are very popular as they only reside in a system's memory with no footprints on the system's hard drive. Any data gathered could just be stored in memory before being ex-filtrated to a remote system.

Content Template	
Section Number	7.3
Section Title	The process of memory forensics
Introduction	This section explains the main stages of memory forensics
Content	Figure 3 shows the process of memory forensics. The first step of memory analysis is identification of a suspicious network connection that can be conducting via the use of the available options for connection (i.e. from volatility any active or recently closed network connections) that can be extracted from RAM. A series of WHOIS queries and a few analyses on Google docks may be used to limit the network connections. The process mentioned below (Figure 3) would possibly have to be recurrent persistently to limit the entries on the list further. In fact, the best analysis is the one that correlate data from both the RAM capture and artifacts from the hard drive.  Figure 4. The Process of Memory Analysis Recognizing a malicious network connection can be achieved by: 1- interviewing the owner of the system; 2- analyzing the history files of the internet to identify the frequency IP addresses or domains was visited; 3- Analyzing any network logs "|if any" that capture outbound traffic. Malicious software "malware" often connect with an outside entity on an exact time frame, or intervals. Usually, the communication is done with the identical size of a packet, unless the malicious software "malware" is ex-filtrating data. Recognizing these trends would done very quickly via visual analysis of the network logs using "splunk" or any other tool. Via Volatility, upon extraction of the network connections, all of the connections will be listed with an associated process ID (PID). Thus, by the use of Volatility's *pslist,* an analyst could idenfify the name of the program that was associated with the network connection by mapping each PID to the process name. Occasionally, the program name and its location are a dead giveaway to a seasoned analyst. It is suspicious to find a program initiating a network connection since is not part of the program functionality. Figure 4 below shows the memory analysis progression. Each step is gathering more artifacts in order to build a case. Every step will also include time-stamps that can further increase the case artifacts.

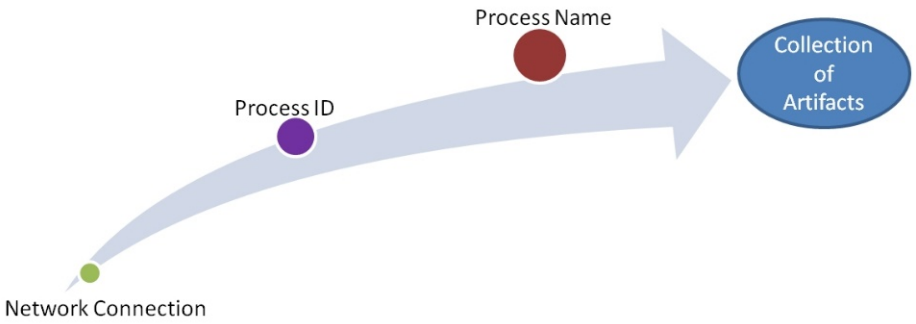


Figure 5. The Memory Analysis Progression

Content Template	
Section Number	7.4
Section Title	The Memory Analysis Progression
Introduction	This section demonstrates the progression of memory analysis
Content	Usually, artifacts consists of: • IP address (port number) • The ID of the process • The associated name of the process The time-stamp is always associated with all above mentioned artifacts to allow investigators conducting timeline examination and correlating with the hard drive artifacts. Always keep in mind that some malware can modify the time stamp of Standard Information Attribute in a try to throw off an investigation. This is often one among the advantages of conducting memory analysis since malware is not yet conducting anti-forensics within RAM. Thus, by knowing the process ID and parent process ID (PPID) (i.e. parent process ID starts the malicious process that initiated the suspicious network connection), analyst will able to identify what was originally executed in which may started the network connection. Note: Volatility can save the output in the format ".dot." Programs such as Graphiz (www.graphviz.org) can read this format. Graphiz is a visualized program that gives a graphical description and visualization of the relationship between PID and PPID. Visualization gives an easy relationship to follow. The following points may be tried for further study: When the id of malware is self-contained, via forensics software a program can be derived from the hard drive. AV scanners can scan process. The analysis step could be done via a static analyzer for instance ollydbg tool or IDA Pro. For encrypted program, Volatility's *procdump can be used.* When the malicious code is injected into a legal procedure, the analyzing and extraction procedures for a file can be done through the use of static analysis. A pre-fetched file for a process/application can be examined. Analyzing the time stamps related to the network connection(s), the ID for the process and the ID of the parent process is necessary. Note: the timestamps from the drive could have been modified, thus, verifying with the time stamp derived from memory to check if there is a match. *Hard drives with no capture can be analyzed via some tools like Virtual Forensic Computing (VFC), Mount Image Pro and VMware. Via these tools a hard drive can be resurrected to gather the RAM.* The image of drive located on the analyst machine is mounted with Live View or Mount Image Pro.

	VFC tool could be used to build an image of VMware. According to the VMware official site: "VMware is a tool applied to open the image and to operate on the "live" system. If the computer system is protected via password, VFC tool has a method to bypass the password authentication process". Now here, pause VMware, and in the location where the VMware image is stored copy out the file with the extension .vmem. This is a copy of the VMware image's RAM. When rebooting a computer, some malware are able to live. These malware would then occur in the RAM sample via the use of VFC. A good practice to let the computer system runs for a while in order to delay the stat-up time for a malware. To capture network traffic packet for inspection, a network sniffer such as Wireshark, tcpdump should also be run. **Note:** When a file is carved out of memory, it is not the same file that is located on the hard drive. It will impact the MD5 hash value.

Content Template	
Section Number	7.5
Section Title	**The Importance of Memory Forensics**
Introduction	This section addresses the importance of memory forensics
Content	Memory forensics aims at providing unique observation into runtime system activity, for example recently executed commands or processes and open network connections. The role of memory forensics appears when examining criminal activity weather insider threats or hackers. Prior to 2004 several generic tools that were not designed for memory forensics such as grep and strings. There were difficulties in using these tools since they were not designed for memory forensics. Michael Ford in 2004 was the first to use the term memory forensics via the use of rootkit tool. Following points address the importance of memory forensics. 1- In order to execute any program (malicious or not), the program needs to be loaded in memory that's make memory forensics crucial for recognizing obfuscated attacks. 2- RAM stores all programs or altered data (created, analyzed, or deleted). Data include: images, encryption keys, network connections, web-browsing history or injected code. 3- In many circumstances, certain artifacts (i.e. critical data related to threats or attacks will exist entirely in system memory) for example account credentials, network connections, encryption keys, chat messages, internet history, running processes, and injected code fragments. 4- Malware programs that only locate in the memory (not the disk) can be developed by attackers. These malwares make the memory virtually invisible to standard computer forensic methods. 5- Firewalls and antivirus software that considered as network-based security solutions cannot detect malware written directly into RAM or a computer's physical memory.

<table>
<tr><td colspan="2">Content Template</td></tr>
<tr><td>Section Number</td><td>7.6</td></tr>
<tr><td>Section Title</td><td>Memory Forensics: Tools and Techniques</td></tr>
<tr><td>Introduction</td><td>This section summarizes all tools and techniques used for memory forensics.</td></tr>
<tr><td>Content</td><td>
Memory Forensics: Tools and Techniques

This section summarizes the tools used in conducting memory forensics: 1) Memory Acquisition tools, 2) Memory Analysis tools.

Memory Acquisition Tools

These tools obtain digital evidence in an acceptable form. The evidence collection tools can be categorized as hardware based and software based acquisition tools.

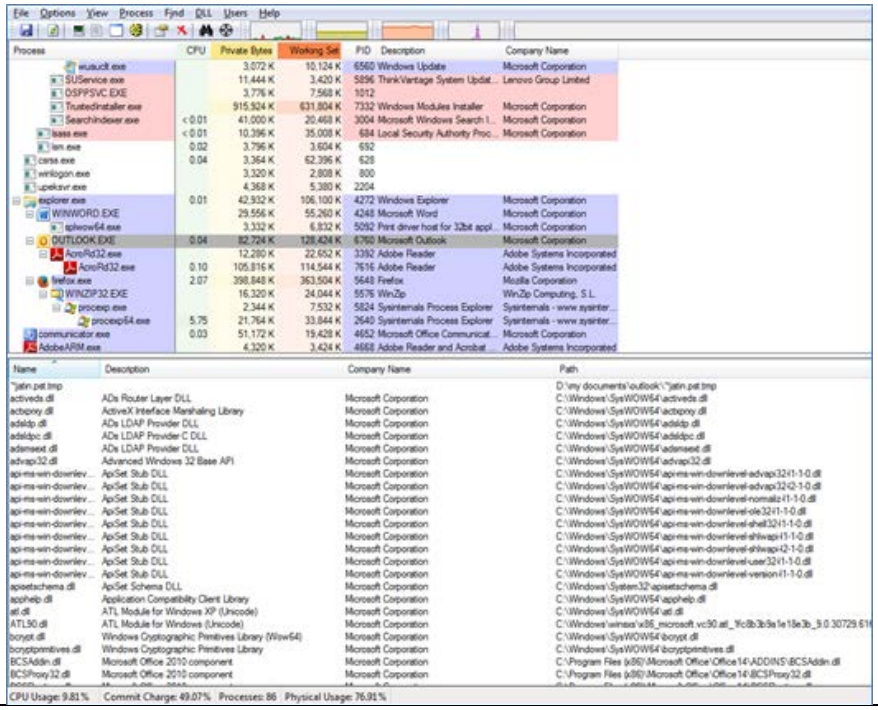
Hardware based acquisition tools: These tools prevent the operating system by means of a physical device. A dedicated communication port will be opened via the dedicated hardware in order to copy the contents of the physical memory. Since there is no interaction with the OS, there is no danger of writing data to the target machine. However, as hardware based technologies exploit Direct Memory Access (DMA) to read physical memory, systems are vulnerable to attacks using this same feature. Table 1 summarizes some hardware based acquisition tools.

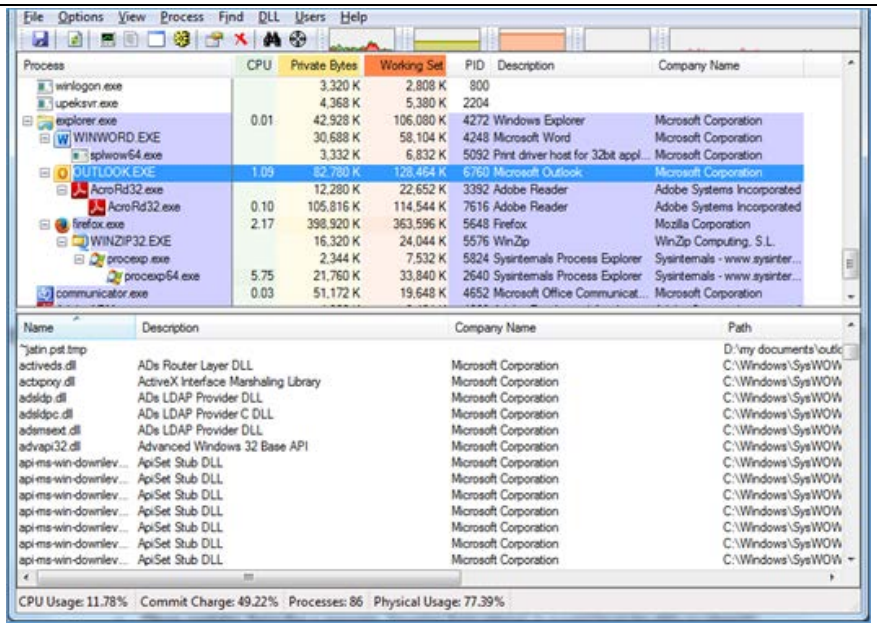
Table 3. Hardware based acquisition tools
<table>
<tr><th>Tool name</th><th>How It works</th><th>Advantages</th><th>disadvantages</th></tr>
<tr><td>Tribble</td><td>This tool makes use of a dedicated Peripheral Component Interconnect card PCI. The card needs installation before incident happening. The PCI card can be detached easily after the incident. Therefore, the system state is maintained to find digital evidence</td><td>Easy of use
no impact on the computer system.</td><td>The main drawback is the installation requirements.
Accessing to physical memory is unauthorized via PCI cards (libraries).
There is possibility to perform Denial of Service attacks (DoS)</td></tr>
<tr><td>FireWire bus or IEEE 1394 bus</td><td>It supports physical access to the system memory via other functionalities for example data-transfer and high speed communication.</td><td>The port of FireWire is popular in many systems.</td><td>For some systems, IEEE 1394 bus presents problems with a part of memory called Upper Memory Area (UMA).</td></tr>
</table>

Software based tools: This section summarizes some software based acquisition tool.
</td></tr>
</table>

	Autopsy (https://www.sleuthkit.org/autopsy/) "is an open source GUI-based digital forensics program that examines and analyzes both hard drives and smart phones effectively. Autospy is popular among thousands of users worldwide in order to explore what actually happened in the computer". MANDIANT Memoryze (https://www.fireeye.com/services.html) "is a memory forensics tool that can get the physical memory from a Windows system and can perform advanced analysis of live memory during running the computer. All analysis can be done either against an acquired image or a live system". Belkasoft Evidence Center (https://belkasoft.com/ec) "is an easy to use tool by investigators to get, acquire, find, search, examine, analyze, save and share digital evidence found in computer and mobile devices. The toolkit extracts digital evidence from several sources via analyzing drive images, hard drives, iOS, memory dumps, Blackberry and Android backups. It also works on UFED, JTAG and chip-off dumps". Evidence Center will automatically examine the source of data and lay out the most essential artifacts for investigator to review, analyze more closely or add to report. 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". HELIX3 (https://www.joomshaper.com/joomla-templates/helix3) "is a live CD-based digital forensic chain developed to be exploited in incident response. It comes with many open source digital forensics tools such as hex editors, data carving and password cracking tools". Memory Analysis tools There are several tools that can be used to conduct memory analysis. 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". 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". 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".

	Platform Independent Tools inVtero.net (https://github.com/ShaneK2/inVtero.net)" is an open source hypervisor/process/kernel detection for Windows, FreeBSD, OpenBSD and NetBSD. inVtero.net is based on interpreting low-level hardware defined constructs which change little over time". 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".

Activity Template	
Number	7.1
Title	Check the dll files using Process Explorer (Microsoft tool)
Type	Practical
Aim	This activity aims at allowing students to list all the DLLs associated with a running process to identify of a malicious DLL that has injected itself into a process. Outcome 3: Define the main artifacts that can be collected and analyzed from memory
Description	This activity should be accomplished upon finishing section 7.2. 1. Dear student, check the dll files using Process Explorer (Microsoft tool). First you have to download process explorer from Microsoft (http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx) and then enable dll view mode. 

	
Timeline	2 hours
Assessment	Each student is required to submit a one-page report. The report will be assessed based on completeness, correctness and overall quality.

Activity Template	
Number	7.2
Title	Memory analysis using volatility tool
Type	Experiment
Aim	This activity shows how forensic analysis of raw memory dump will be performed on Windows platform using standalone executable of Volatility tool. Outcome 4 :Understand the memory tools that collect evidence and conduct analysis
Description	In this activity, forensic analysis of raw memory dump will be performed on Windows platform using standalone executable of Volatility tool. It is common in investigation process that the forensic investigator may find several malicious programs on the compromised hard disk. So, memory analysis becomes very important in such events because malicious program or malware may be running on the compromised system. This activity should be performed upon finishing the whole chapter.
Timeline	2 hours
Assessment	Each student is required to submit a one-page report. The report will be assessed based on completeness, correctness and overall quality.

Think Template (MCQs)	
Number	7.1
Title	Memory Forensics Basics
Type	• Choose correct answer
Question	When shutting down a computer, what information is typically lost? A. Data in RAM memory B. Running processes C. Current network connections D. All of the above
Answers	D

Think Template (MCQs)	
Number	7.2
Title	The process of memory forensics
Type	Fill in the blanks
Question	The first step of memory analysis is ---------- that can be conducted by using one of the connection options from volatility any active or recently closed network connections which can be extracted from RAM.
Answers	identification of a suspicious network connection

Extra Template	
Number	#
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	Could include: • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	7.1
Title	URLs for Software based acquisition tools
Topic	7.6
Type	URLs • https://www.sleuthkit.org/autopsy/ • https://www.fireeye.com/services/freeware/memoryze.html • https://belkasoft.com/ • https://www.wxhexeditor.org/home.php • http://www.e-fense.com/h3-enterprise.php

Extra Template	
Number	7.2
Title	URLs for Memory Analysis tools
Topic	7.6
Type	• Volatility - Volatile Systems - https://www.volatilityfoundation.org/