

Book 1 - Foundation of Digital Forensics

1.	FUNDAMENTALS OF DIGITAL FORENSICS INVESTIGATION	2
2.	ELECTRONIC DATA ACQUISITION – LEGAL COMPLIANCE AND REQUIREMENTS	22
3.	COMPUTER PROCESSING CRIME AND INCIDENT SCENES.....	47
4.	FUNDAMENTALS OF FILE SYSTEMS	70
5.	OVERVIEW OF COMMON TOOLS FOR DIGITAL FORENSICS.....	97
6.	NETWORK FORENSICS ARTEFACTS.....	123
7.	MOBILE DEVICE FORENSICS	150
8.	DIGITAL FORENSICS WRITING REPORTS	175

1. Fundamentals of digital forensics investigation

Scope Template															
Number	1														
Title	Fundamentals of digital forensics investigation														
Introduction	The scope of this topic is introducing the history of digital forensics and explaining the importance of electronic evidence for solving various problems. It also explains the digital forensic terminology, goals of forensic analysis, the digital forensics process, and challenges for digital forensics.														
Outcomes	LO.1: Explore the changes in society associated with the advent of technological changes and the introduction of the Internet. LO.2: Explain the role of digital forensics in criminal and corporate investigations, auditing, and in the general area of IT security. LO.3: Define digital forensics and outline how to prepare for computer investigations. LO.4: Identify the challenges associated with the enforcement and prosecution of computer crime in society. LO.5: Outline features of examples of cybersecurity incidents and the motivation of the threat actors behind specific security incidents. LO.6: Describe the processes involved in digital forensic investigations.														
Topics	1.1. Digital Forensics Overview 1.1.1 Definition of Digital Forensics 1.1.2 History of Computer Crimes 1.1.3 Digital Forensic Terminologies 1.2. Goals of Forensic Analysis 1.3. The Digital Forensics Process 1.4. Challenges for Digital Forensics Investigation 1.5. Chapter's Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>1 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>5 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>2 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>5 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>1 hr</td> </tr> <tr> <td>Total</td> <td>13 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> Ch. 1, Guide to Computer Forensics and Investigations (5th Edition). By Bill Nelson, Amelia Phillips, Christopher Stuart, 2016. Chs. 1 & 2, Computer Forensics and Cyber Crime: An Introduction (3rd Edition). By Marjie T. Britz, 2013. Ch. 1, A Practical Guide to Computer Forensics Investigations (2nd Edition). By Darren R. Hayes, 2019. 	Task	Time	Preparation (Introduction and On-line Planning):	1 hr	Textbook Content:	5 hr	Thinking (On-line discussions, Review questions)	2 hr	Tutorial Work:	5 hr	Related Course Work:	1 hr	Total	13 hours
Task	Time														
Preparation (Introduction and On-line Planning):	1 hr														
Textbook Content:	5 hr														
Thinking (On-line discussions, Review questions)	2 hr														
Tutorial Work:	5 hr														
Related Course Work:	1 hr														
Total	13 hours														

Content Template	
Section Number	1.1
Section Title	Digital Forensics: An Overview
Introduction	In this section, we start our journey towards the fundamentals of the digital forensics course by introducing some definitions, terminology and fundamental concepts related to digital forensics and investigation. In the next sections, we continue our study and introduce the digital forensics process, goals of forensic analysis and shed light on some challenges that forensic examiners face when preparing and processing crime scenes.
Content	<p>Historically, the Internet and its offered services are experiencing periods of great progress and improvement. This achievement has created opportunities for e-commerce, distance learning, education, research, entertainment, and public discourse. Also, this worldwide connectivity has greatly improved the way we live, work, and communicate by overcoming the key traditional limitations of telecommunication systems. For example, the increased automation of the printing process and the introduction of digital mass media and storage greatly enhanced information sharing by increasing the availability, integrity, and confidentiality of huge data sources.</p> <p>Unfortunately, this digital revolution has a downside; it has led to criminal innovation and created a new forum for both terrorist activities and criminal behavior. It has been further increased by adapting new technologies, wireless communications, social networking, and smart phones, which has complicated the investigative landscape even further. This issue has led to exacerbating the vulnerabilities of government, organizations, institutions, and individuals alike.</p> <p>The following definitions are commonly used with digital crime.</p> <ul style="list-style-type: none"> • Computer-oriented crime: It is a form of criminal behavior that uses a <i>computing machine and/or a computer</i> network to carry out illegal activities. • Cyber-crime: It is the set of activities carried out by individuals to encompass misuse or abuse of computing systems or any electronic device. • Digital crime: It is the set of criminal behavior carried out by individuals to access unauthorized information for the purpose of destroying data or carrying out illegal activities and operations. • Digital forensics: This concept was firstly defined in 2001 by the Digital Forensics Research Workshop (DFRWS) as "<i>The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations</i>"^[1]. Some experts have argued that sometimes digital investigators behave like a computational archaeologist or a digital geologist. "<i>Digital archaeology is about the direct effects from user activity, such as file contents, file access time stamps, information from deleted files, and network flow logs. ... Digital geology is about autonomous</i>

	<p><i>processes that users have no direct control over, such as the allocation and recycling of disk blocks, file ID numbers, memory pages or process ID numbers</i>"^[2].</p> <p>The digital forensic process encompasses several operations that obtain and analyze digital data for the purpose of extracting digital evidence of a crime scene. In general, these operations are almost the same as the traditional criminal investigation process. Nevertheless, the investigation scene might be different and it depends on the case under consideration.</p> <p>In Section II, we list the main goals of forensic analysis. Section III overviews the digital forensics process. In Section IV, we discuss the main challenges for digital forensics investigation. We conclude and summarize in Section V.</p>
--	---

Content Template	
Section Number	1.2
Section Title	Goals of Forensic Analysis
Introduction	This section discusses the main goals of any given forensic examination analysis.
Content	<p>It was stated that forensic analysis goals vary per case. The analysis phase can be used to prove or disprove assumptions against individuals, organizations, or entities, or it can be used to investigate information security crimes locally on the existing system or globally over the Internet.</p> <p>The main target of the digital forensic process is to extract facts that can be used to re-create the truth of an event. This means that a set of actions might be taken on a computing system that leave traces of that activity on several locations on the system such as system logfiles, system registry, and Cookies. More complex actions are likely to create longer-lasting impressions on the system. The main entity in the digital forensic analysis is the digital device related to the security crime under investigation. The digital device can be computers, tablets, cellular phones or other data storage devices that is either used to commit a crime, to target an attack, or is a source of information for the analyst.</p> <p>Furthermore, in many digital investigation cases, determining whether the digital evidence under consideration is consistent or not is one of the purposes of the examination. Digital investigators must be aware of all processes and systems that are used to test this consistency.</p> <p>Digital investigation involves several other goals such as:</p> <ul style="list-style-type: none"> – Assist in following up, in a legally sound manner, all criminal cases involved in the same digital evidence. – Preserve the integrity of seized digital evidence. – Help in training the public community. – Provide technical assistance in the proper safeguarding of system assets.

Content Template	
Section Number	1.3
Section Title	The Digital Forensics Process
Introduction	In this section, we overview the generic process used by digital forensics investigators.
Content	<p>In enterprise network environments, security experts are divided into tightly coupled groups to secure enterprise networks and their assets. Some experts analyze system vulnerabilities to mitigate incidents, others manage Intrusion Prevention and/or Detection Systems (IPS/IDS), and others conduct computer digital examinations. The latter is the main focus of this chapter.</p> <p>The process of digital forensics can be split into three main activities: <i>data acquisition, data analysis, and results presentation.</i></p> <ul style="list-style-type: none"> – Data acquisition: This is a set of activities carried out by digital investigators to collect and process the data that are stored on various types of digital media such as Hard Disk Drives (HDDs), optical storage devices such as CD or DVD, Personal Digital Assistants (PDAs), cameras, and smart phones, etc. The acquisition process should first consider the creation of multiple copies of the original data and make sure that they contain good historical records of all activities and logs being extracted from the media. – Data Analysis: This refers to the set of activities being carried out by investigators to identify, analyze and interpret the collected data. At a minimum it includes locating the set of items of interest located on the digital media and trying to narrow this set as necessary. This reduced set of items is then given further analysis and processing. Examples of these operations are the analysis and examining of file system contents, processing of log files, extracting statistical results, and so on. Finally, the digital investigators interpret the obtained facts and results based on their own experience. – Results Presentation: This refers to the process that is followed by the examiner of sharing his/her results obtained from the analysis phase for policy makers. This process mainly consists of generating a report of actions associated with all discovered artifacts and their analysis. Furthermore, the presentation phase can include the investigator defense plan and the possible implementation challenges. <p>The results obtained from this phase can used further for doing additional acquisitions in an iterative process. In this way, each process generates more analytical artifacts that are fed as inputs to other processes in a feedback manner. This feedback iterative process can have several iterations for long-lasting criminal investigations.</p>

Content Template	
Section Number	1.4
Section Title	Challenges for digital forensics investigation
Introduction	In this section we give an overview of the major challenges and problems forensic examiners face when preparing and analyzing investigations, including the main ideas and questions they must consider prior or during the digital forensic process.
Content	<p>Nowadays, listing all the challenges faced by the forensic investigators and law enforcement is not an easy task. In fact, with the ever-growing development of new technologies, a huge volume of stored data is exists with heterogeneous forms and are accessible using various types of communication technologies. Therefore, digital forensic examiners are facing a critical set of challenges and problems. Among the most important ones are:</p> <ol style="list-style-type: none"> 1. Proliferation of Device technology: Personal computers, mobile devices, embedded systems, and IoT equipment use various types of computing systems, telecommunication facilities and different file management processes. This will increase the burden on investigators for doing digital investigations. Moreover, inspecting heterogeneous electronic devices can cause other problems related to data correlation and integrity. 2. Paucity of resources and staff training: This is considered to be one of the main challenges. Due to the lack of experts, investigators only learn the basics on how to use specific software without being provided with any professional skills for their working and techniques for allowing them to use alternatives or more than one tool. 3. Cloud forensics: Data now are stored on the cloud on different nodes across the Internet. This issue leads to data being managed and administrated by several authorities. This new computing paradigm forces investigators to be aware of the local laws for collecting digital evidence on the cloud. This can also increase the amount of time being spent and the complexity of forensic tools needed. 4. Data and Device Encryption: Each device has its own challenges. For example, for devices using MS Windows, a fully encrypted disk can be retrieved by snatching a memory dump to get the decryption key. For Android devices the process mainly depends on both the installed OS version and the manufacturing company. Here, how to actually locate the encrypted data adds an extra burden on the investigation process. 5. Setup environment: In some cases, the amount of setup required before true analysis can be undertaken is considered a challenge. If the examiner simply looks to determine a known file type, he/she still needs to identify the OS file system and determine the partitions on the image. Nevertheless, some common tools like Autopsy and FTK can automatically find partitions and recognize file systems. In this case, the effect of this setup work is not that important and does not directly affect the overall purpose of the investigation.

	<p>6. Legal and ethical issues: Since every user owns his/her data and digital device, forensic examiners face ethical and legal issues of accessing and collecting the required information. Cases may occur in which the required information owned by the suspect and stored on his/her device cannot be accessed due to legal stipulations.</p> <p>To summarize this section, we conclude that each one of the aforementioned challenges is designed to open a window for developing new mechanisms, forensic software and methods that address these gaps and enhance forensic analytical capabilities. These enhancements include, but are not limited to, utilizing network traces and services, disks and flash memories, and cell phones.</p>
--	---

Content Template	
Section Number	1.5
Section Title	Chapter Summary
Introduction	In this section, the main concepts outlined in the previous sections are summarized.
Content	In the first section of this chapter we introduced a brief overview of what we mean by digital forensics, some terminology, and concepts. In section 1.2, we discussed the main goals of any given forensic examination analysis. In Section 1.3, we explained the generic process used by digital forensics investigators. In the next section we looked at the main forensic challenges and problems that forensic examiners face when preparing and analyzing a case, including the main ideas and questions they must consider prior or during the digital forensic process.

Activity Template	
Number	1.1
Title	Using Internet resources
Type	Research
Aim	LO.1 & LO.2 The aim of this activity is to teach students how to find well-known digital forensic IT companies.
Description	Use a Web search engine, such as Google, Bing or Yahoo!, and search for companies specializing in computer forensics. Select three and write a two-to three-page comparative summary of what each company does.
Timeline	Internet search: 1 hr. Writing report: 2 hrs.
Assessment	Each student is required to submit his/her report and this will be evaluated based on their contribution. Students will be discouraged from a cut and paste exercise.

Activity Template	
Number	1.2
Title	Review scientific papers
Type	Research & Reflection
Aim	LO.3 & LO.4 The aim of this activity is teaching students how to find scientific papers related to digital forensics and summarize, introducing their main findings.
Description	Search the Internet for articles on computer crime prosecutions. Find at least two. Write one to two pages summarizing the two articles and identify key features of the decisions you find in your search.
Timeline	Internet search: 1 hr. Paper review: 4 hrs.
Assessment	Each student is required to submit his/her review and then discuss his/her findings in the class.

Activity Template	
Number	1.3
Title	Conduct internal computing investigations and forensics examinations
Type	Reflection
Aim	LO.3 to LO.6 In this activity, you work for a large corporation's IT security company. Your duties include conducting internal computing investigations and forensics examinations on company computing systems.
Description	<p>This activity is adopted from Ref [1]. As an employee, you are asked by your company manager to conduct a digital investigation scene. Your main task is to examine a USB drive owned by a former employee who currently works in another competitive firm. The company has some doubts that this former employee stole some confidential documents that consist of 24 files with the text "data".</p> <p>To process this forensic scene, follow these steps:</p> <ol style="list-style-type: none"> 1. Start ProDiscover → open project name C2Prj02 → save it in your work folder (DigitalForensic\Activitites\Activity1). 2. Click Action → Add → ImageFile → C2Prj02.eve. 3. Click expand Content View → Expand Images → Click the pathname containing the image file → Examine the files that are listed. 4. Open the search dialog box → Click the Content Search tab → Select the Disk(s)/Image(s) → click the drive you're searching → Click Content Search Results to specify the type of search. 5. Open the Search dialog box again → click the Cluster Search tab → run the same search → click Cluster Search Results → view the search results pane. 6. Once finished, write a one-page report to the company manager explaining what you have found.
Timeline	Understand project idea: 1 hr Implement project steps: 1 hr
Assessment	Each student will be assessed based on his/her successful implementations of the above steps and his/her extracted information. As well as , each student is required to submit a one-page answer report and then discuss it in the class as open session.

Activity Template	
Number	1.4
Title	Analyze Case Study
Type	Reflection
Aim	LO.1 to LO.6 In this activity, you will review a case study taken from a computer forensics firm. Write an outline for how the firm should approach the case.
Description	As a digital investigative expert, you were hired by an insurance company to conduct a forensic analysis for an arson investigative scene. The suspects have been arrested, but the company wants to make sure that there are no victims. For the purpose of this activity, you were given two files to work with. The first one named CasePrj0201a.doc which is a small letter from the police department, and the other file named CasePrj0201b.doc which is a letter from the insurance company that explains what should be investigated. Your main task is to review these two files to decide which course of actions that your company should take. Write a one-page forensic report explaining how your company should handle this case.
Timeline	Understand case study: 1 hr. Write a one-page report: 2 hrs.
Assessment	Each student is required to submit a one-page answer report and then discuss it in the class as open session. His/her answer will be evaluated based on the course of actions suggested to handle the case.

Activity Template	
Number	1.5
Title	Write a one-page investigation report
Type	Review & Reflection
Aim	LO.1 to LO.6 In this activity, you will review a case study taken from a computer forensics firm. Write an outline for how the firm should approach the case.
Description	You work in a specific firm as a digital forensic manager. Your company faces a forensic case for one of its former employees who was fired from his/her job for inappropriate files discovered on his/her desktop computer. He/she claimed that never accessing these files. What steps should you follow to conduct this case? Write a one- to two-page report describing this case besides other relevant resources that should be investigated.
Timeline	Understand case study: 1 hr. Write the report: 2 hrs.
Assessment	Each student is required to submit an answer report and then discuss it in the class as open session. His/her answer will be evaluated based on the correct course of actions suggested to handle the case.

Think Template (MCQs)	
Number	1.1
Title	Fundamentals of digital forensics investigation
Type	Choose correct answer
Question	<p>The triad of computing security includes which of the following?</p> <p>(A) Detection, response, and monitoring</p> <p>(B) Vulnerability assessment, detection, and monitoring</p> <p>(C) Vulnerability assessment, intrusion response, and investigation</p> <p>(D) Vulnerability assessment, intrusion response, and monitoring</p>
Answers	Answer: (C)

Think Template (MCQs)	
Number	1.2
Title	Fundamentals of digital forensics investigation
Type	True or False
Question	Digital Forensics and data acquisition refer to the same concepts (A) True (B) False
Answers	Answer: (B)

Think Template (MCQs)	
Number	1.3
Title	Fundamentals of digital forensics investigation
Type	Fill in the blanks
Question	<p>List three common types of digital crime.</p> <p>(A) _____</p> <p>(B) _____</p> <p>(C) _____</p>
Answers	<p>(A) Internet Pornography</p> <p>(B) Espionage</p> <p>(C) Abuse of Internet Property</p>

Think Template (MCQs)	
Number	1.4
Title	Fundamentals of digital forensics investigation
Type	Fill in the blanks
Question	<p>What are some initial assessments you should make for a computing investigation?</p> <p>(A) _____</p> <p>(B) _____</p>
Answers	<p>(A) Talk to others involved in the case about the incident.</p> <p>(B) Was there any evidence seized by the law enforcement or security officers?</p>

Think Template (MCQs)	
Number	1.5
Title	Fundamentals of digital forensics investigation
Type	Choose the correct answer
Question	Laws and procedures for PDAs are which of the following? (A) Well established (B) Still being debated (C) In the law books (D) None of the above
Answers	Answer: (B)

Extra Template	
Number	1.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	1.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

2. Electronic data acquisition – legal compliance and requirements

Scope Template															
Number	2														
Title	Electronic data acquisition – legal compliance and requirements														
Introduction	The scope of this chapter is introducing data acquisition formats, methods and tools. Students will learn about the three forensic data acquisition formats: raw, proprietary, and Advanced Forensic Format (AFF) and the four methods of acquiring data for forensics analysis which are disk-to-image file, disk-to-disk copy, logical disk-to-disk or disk-to-data file. This chapter also explains static and live acquisition to collect digital evidence when a computer is turned on or off. They will also learn how to use several acquisition tools and methods that work in Windows and Linux and how to search for newer and better tools to ensure the integrity of your forensics acquisitions. Finally, it overviews a generic procedure used to <i>validate</i> the <i>data acquisition</i> process.														
Outcomes	LO. 1: List digital evidence storage formats LO. 2: Explain ways to determine the best acquisition method LO. 3: Describe contingency planning for data acquisition LO. 4: Explain how to use acquisition tools LO. 5: Describe how to validate data acquisitions LO. 6: List other forensics tools available for data acquisition														
Topics	2.1 Understanding Storage Formats for Digital Evidence 2.2 Acquisition Methods 2.3 Computer Forensics Acquisition Tools 2.4 Validating Data Acquisitions 2.5 Chapter's Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>2 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>7 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>3 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>6 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>3 hr</td> </tr> <tr> <td>Total</td> <td>20 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> Ch. 3, Guide to Computer Forensics and Investigations (5th Edition). By Bill Nelson, Amelia Phillips, Christopher Steuart, 2016. Ch. 4, A Practical Guide to Computer Forensics Investigations (2nd Edition). By Darren R. Hayes, 2019. 	Task	Time	Preparation (Introduction and On-line Planning):	2 hr	Textbook Content:	7 hr	Thinking (On-line discussions, Review questions)	3 hr	Tutorial Work:	6 hr	Related Course Work:	3 hr	Total	20 hours
Task	Time														
Preparation (Introduction and On-line Planning):	2 hr														
Textbook Content:	7 hr														
Thinking (On-line discussions, Review questions)	3 hr														
Tutorial Work:	6 hr														
Related Course Work:	3 hr														
Total	20 hours														

Content Template	
Section Number	2.1
Section Title	Understanding Storage Formats for Digital Evidence
Introduction	In this section, we will talk about the data acquisition process. We will mainly discuss various formats for digital evidence storage and determine the best acquisition method for each one of them. In the subsequent sections, we will talk about how to carry out static acquisition using several tools and methods and describe how to validate data acquisitions.
Content	<p>As previously mentioned in Chapter 1, the analysis of digital evidence poses challenges to forensics investigators. Working with digital media and electronic information is important for the successful implementation of case disposition. In this regard, forensic data acquisition can be defined as the process of collecting digital evidence from electronic media by making multiple copies of data being investigated.</p> <p>In general, there are two types of data acquisition methods: <i>static acquisitions</i> and <i>live acquisitions</i>. Both methods and their data integrity requirements are similar. In static acquisition, any data stored on digital media remains the same regardless of the number of acquisitions being performed upon it. <i>i.e.</i>, making a second or third static acquisition for the preserved original media should produce the same outcome. Whereas making multiple copies of live acquisition while a computer is running will collect new data instances because of the dynamic nature of the system. Therefore, by using live acquisition investigators cannot carry out repeatable processes, and repeatability helps to validate digital evidence.</p> <p>Although hardware components may provide the required platform to acquire and analyze data, it still needs third party forensic software to be more effective. Five broad categories of software tools are cited in the literature that can be used to assist in the analysis process they are:</p> <ul style="list-style-type: none"> – Data preservation, duplication, and verification tools – Data recovery/extraction tools – Data analysis tools – Data reporting tools – Network utilities <p>There are three main generic formats being extensively used to store data on a computer. Two of these formats are open source, known as raw and Advanced Forensic Formats (AFF), and the third is proprietary which is based on vendors' unique features. In addition, a number of proprietary formats are available nowadays, and most of computer forensics analysis tools can read various types of them. In the following we will give more details on these three formats, discuss some of their advantages, and limitations.</p> <p>Raw format: This is the oldest version of data format that has been used. It mainly makes a duplicate copy of the disk by performing bit by bit copying from one disk to another. For practical purposes to preserve digital evidence, software vendors modified this process with the ability to write bit-stream data to files that creates simple sequential files of the media. The output of these files is in raw format. Raw format outperforms other file formats (like AFF and EWF) in terms of throughput, <i>i.e.</i>, has high transfer data rate between media. Some of its disadvantages are:</p>

- It is inefficient in using storage capacity; it needs high storage volumes on disk with a minimum capacity equaling the size of the original media.
- It has some efficiency issues when dealing with unhealthy sectors on the media. This means that, when applied on weak media it will have a low level of threshold of retry reads of raw data on these bad media spots.
- Many commercial forensic tools have a higher threshold value of retry reads to verify that all relevant data is gathered in a proper way.

Some of the current acquisition tools come with built-in mechanisms to generate raw format acquisitions with validation checksum by using for example Cyclic Redundancy Check (CRC-32), Message Digest 5 (MD5), and Secure Hash Algorithm (SHA-1 or newer versions) and hashing functions.

Advanced Forensic Format (AFF): This new open-source format has no implementation restrictions and it has started to gain recognition among computer forensics investigators. Although the AFF is open source, many existing software vendors are starting to include it in their tools. AFF format has the following features:

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

Proprietary formats: As previously mentioned, many vendor computer forensics tools can store collected data in specific formats. These formats are complementing vendor's analysis software. Vendors' proprietary formats have several advantages compared to other formats such as:

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

Their main disadvantages are:

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

It is worth mentioning that the EWF format started as a proprietary format but then was published and now many tools support it.

Table 1 lists the main differences among Windows file systems:

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

Table 1: The main differences between FAT32 and NTFS Microsoft Windows file systems.

Content Template	
Section Number	2.2
Section Title	Acquisition Methods
Introduction	This section discusses the types of acquisition methods used in the digital investigation process and gives some guidelines on how to select among them based on the investigation scenario under consideration.
Content	<p>Four methods are generally cited by the literature to acquire data they are:</p> <ol style="list-style-type: none"> 1) Disk-to-image file 2) Disk-to-disk copy 3) A logical disk-to-disk 4) A sparse copy of a folder or file <p>Disk-to-image method is considered as the most common and flexible method for doing investigations. By using it, investigators can create several copies of a suspect's media which are constructed by using bit-for-bit replications mechanism. Moreover, they can also use other forensic tools, such as SMART, ProDiscover, X-Ways Forensics, FTK, ILook, and Autopsy, to read the most common types of disk-to-image files they created. These software tools treat the disk-to-image file as though it is the original disk.</p> <p>Sometimes investigators face problems of making a disk-to-image file. One of the main challenges is hardware and/or software incompatibilities. This becomes more complicated when investigators face old disk drives. In this case, they might have to create a disk-to-disk copy instead of disk-to-image copy. Several tools are available – like EnCase and SafeBack- that can copy data exactly from an older disk to a newer one. These tools can adapt their functionality to match data on the original suspect drive. They do that by modifying disk hardware features such as cylinder, head, and track configuration.</p> <p>In the case that the extracted data is stored in a large drive, the data capture process can take several hours. To overcome this issue, some vendors suggest the use of sparse data acquisition that gathers only specific types of files. In this case, the overall performance will be improved especially when the process needs to examine only some parts of the suspect's disk drive.</p> <p>Some compression methods can be used to reduce file size to fit with the disk drive storage space. Common tools for archiving such as WinRAR, PKZip and WinZip use lossless compression to reduce file size without affecting the image quality.</p> <p>One of the ways to test the data consistency of a file is to carry out a hashing method such as MD5 or SHA-1. This should be done before and after applying the compression. In this case, if the compression process is done correctly, both copies should have the same hashing value, otherwise the compressed file is corrupted. Another method of doing this is to use a backup using tapes, such as Super Digital Linear Tape (SDLT) or Digital Audio Tape/Digital Data Storage (DAT/DDS) especially when working with large drives.</p> <p>Finally, as a standard practice that must be followed, especially for those investigators who don't produce duplicate copies of their evidence due to the time and resource limitations, is to produce at least two duplicate images of the evidence they collect. Moreover, if they have more than one</p>

	<p>software tool, they can try to make the first copy using one tool and the other one with another tool.</p> <p>To summarize this part, we conclude that to determine the best acquisition method that can be used for digital investigation purposes, examiners must consider the following key points:</p> <ol style="list-style-type: none">1) The size of the data volume2) The method of retaining the data as evidence or referring it to its owner3) The time required to carry out the acquisition4) The location of the digital evidence.
--	--

Content Template	
Section Number	2.3
Section Title	Computer Forensics Acquisition Tools
Introduction	In this section, we discuss a number of artifacts that are unique and specific to three well-known operating systems (OS) they are: Microsoft Windows, Linux, and MAC OS X. Then, we provide an overview of some of the well-known acquisition tools that run on top of them.
Content	<p>Windows Systems</p> <p>Windows is the most popular OS and therefore occurs most frequently in forensic examinations. As a result, it has many well-known artefacts. It mainly supports two types of primary file systems: File Allocation Table (FAT) and New Technology File Systems (NTFSs). FAT systems can be of different flavors supported by a special type of OS. Some drivers are also available that allow the NTFS volumes to be accessed by other operating systems like Linux and Mac OS X.</p> <p>File Allocation Table (FAT): This file structure is one of the simplest systems and was totally supported by the family of Microsoft operating systems, i.e.; MS-DOS and Windows. Its simplicity comes from the fact that it possesses few data structures. It can be FAT16, FAT32, and exFAT. In this system, the volume is divided into clusters with a specific size. For example, for FAT16, the cluster size ranges from 512-bytes to 64 KB. It is also supported by any removable storage devices such as thumb drives and flash cards. Furthermore, as it's an old and generic system, it is supported by other operating systems, thus it makes it easy for investigators to move it from one system like Linux to another one like Windows. For example, if the investigator is conducting the analysis via a Linux system, he/she can save the collected information to access them easily from a Windows system later on. Despite the aforementioned advantages, FAT systems suffer from security issues compared to other systems.</p> <p>New Technology File System (NTFS): Currently, the NTFS system is the most popular system used in Microsoft OS. This popularity comes from its ability to set Access Control Lists (ACLs) on file objects and having built-in file compression mechanisms. In this regard, the Master File Table (MFT) is the richest source of information required by an investigator when working with the NTFS file system. The size of each MFT entry is 1024 bytes, which makes it straightforward to parse. Furthermore, each MFT record begins with ASCII strings of either FILE or BAAD and followed by one or more attributes, each with their own identifiers and structures.</p> <p>Some Challenges of Windows acquisition tools</p> <p>In general, Windows acquisition tools have the following drawbacks:</p> <ul style="list-style-type: none"> – When using Windows OS they can easily corrupt the evidence drive, investigators must apply well-tested write-blocking hardware devices to protect them. – Some Windows forensics tools face several challenges when trying to acquire data from protected areas of the HDD. – There are some legal and ethical issues in some countries of how to use the write-blocking devices for the data acquisition process. <p>Linux systems</p>

Over the past two decades, Linux has become a popular operating system and found its way into a large number of applications and environments such as networking devices and powerful supercomputing clusters. Some versions of Linux OS have come a long way from their humble roots as a free Unix-like system for personal computers. Most of them share a common standard Linux file system, directory structure, system artefacts and user activity. Most current Linux systems use the Ext4 file system and older systems used Ext3 and Ext2.

In general, any Ext file system has two main components that make up its layering structure they are the superblock and the group descriptor table. The superblock is a data structure type that is located in the first 1024 Bytes of the Ext file system. It maintains information about the layout of the file system, its block and inode allocation information, as well as timestamps. Whereas, the group descriptor table is located after the superblock and contains allocation status information for each block group found on the file system.

In addition to the Ext family of file systems, others are found but are rarely used in Linux file systems. None of these systems are currently supported by The Sleuth Kit but can be tested logically using generic Linux file system tools. These formats are: ReiserFS, XFS, JFS, YAFFS2 and JFFS2. Table 2 below lists the main differences between Linux file systems.

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

Table 2: The main differences between EXT4, XFS, and BTRFS and Linux file systems.

MAC OS X systems

The OS X file system implementation is called *HFS+* or *Mac OS Extended*. HFS+ is the successor to the Hierarchical File System (HFS) that was mainly used in pre-OS X Mac OS. Currently, two versions of the HFS+ exist that support journaling (*HFSJ*) and case-sensitive file names (*HFSX*).

The core structure of the HFS+ contains the volume header that stores information related to the file system, its allocation block size, volume creation timestamp, and the location of special files that are necessary for HFS+ operation, etc. As in the Linux system, the volume header is located in the first 1024 Bytes and the backup copy is located at the end of the volume.

	<p>HFS+ mainly uses allocation blocks as data units. The size of each allocation block is initially identified in the volume header with 4KB. Furthermore, allocation blocks can be grouped into smaller pieces called <i>clumps</i> that are similar to the block allocation in the Linux Ext file systems. Here, file data are addressed in terms of <i>extents</i>. It is simply a pointer of 4-byte size that points to the starting allocation block and another 4-byte value that indicates the length of the extent.</p> <p>Also, HFS+ files contain several data streams called <i>forks</i> associated with them. The two main forks are:the <i>data fork</i> and the <i>resource fork</i>. Generally, the data fork contains the actual file content, while the resource fork contains nonessential information about the file. Additional forks can be created whenever needed based on the application specific purposes.</p> <p>More information is available in the following Apple technical document "Technical Note TN1150: HFS Plus Volume Format."</p>
--	---

Content Template	
Section Number	2.4
Section Title	Validating Data Acquisitions
Introduction	In this section, we will talk about digital evidence validation methods and list some of their weakness and advantages.
Content	<p>An important part of computer forensics is validating digital evidence. A forensic hash is a standard approach that is commonly used for this validation. It is a form of a checksum. A checksum uses a mathematical formula that simply sum the assorted bits in a message to provide a value. Hashing mechanisms generate a binary or hexadecimal digital fingerprint of a file. They use more complex mathematical functions of checksum algorithms.</p> <p>In the context of digital forensics, a forensic hash is the process of applying a mathematical function to the acquired data to produce a unique hash value. Both MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) are two common algorithms used in digital forensics. They were first introduced to check the integrity of the downloaded files from the Internet, i.e., two files with different filenames are considered identical if they have similar hash values.</p> <p>This hash process is normally applied during the acquisition of the evidence to verify the integrity of the collected data and the forensic analysis procedure. This way, if there is any intentional or unintentional attempt to modify any part of a digital evidence, the hash algorithm will produce a completely different hash value.</p> <p>A number of forensic tools with built-in hashing capabilities are available nowadays. Some tools outperform others in terms of computer resource consumption.</p> <p>Normally, the above-mentioned hashing algorithm methods are available as standalone programs or are integrated into many acquisition tools or kits. For example, the Windows system has built-in an MD5 hashing tool and third-party programs exist such as Breakpoint Software Hex Workshop or X-Ways WinHex. Commercial computer forensics kits also come up with built-in validation techniques such as FTK, ProDiscover, and EnCase. In ProDiscover tool, the .eve files include metadata of the acquisition file and the hash value of the HDD. Image data loaded into the Pro-Discover tool is first hashed and then compared to the hash value in the stored metadata. If the hash does not match, ProDiscover sends notifications announcing that the acquisition process is corrupt, and the evidence can't be considered as a reliable.</p> <p>In general, many forensics tools do not contain metadata for raw format image files. As mentioned previously, a separate manual check of the validation process is highly recommended and must be conducted for all raw acquisitions at the time of analysis. The generated validation file for raw format acquisitions is essential to the check the consistency of digital evidence.</p> <p>As an example, in FTK Imager, when an investigator selects the Expert Witness (.e01) or SMART (.s01) format, additional options for validation are automatically displayed. This validation report also lists the SHA-1 and MD5 hash values. The MD5 hash value is added to the proprietary format image. When this image is loaded into the SMART, FTK, or X-Ways Forensics, the</p>

	<p>MD5 hash is compared to the image to verify whether the acquisition is correct.</p> <p>Regarding Linux and UNIX operating systems, things are different. Here, there are several open source commands and functions that can be used to validate data. For example, the two Linux shell commands dd and dcfldd have several options that can be combined with other commands for doing validation purposes. The dcfldd command has also additional options that validate data collected from the acquisition process. Validating acquired data with the dd command requires using other helpful shell commands. Current Linux systems use two hashing algorithm utilities to validate data, they are md5sum and sha1sum. Both utilities can compute hashes of a single file, multiple files, individual or multiple disk partitions, or an entire disk drive.</p>
--	--

Content Template	
Section Number	2.5
Section Title	Chapter Summary
Introduction	In this section, we summarize the main concepts outlined in the previous sections and shed light on the upcoming topic.
Content	<p>In this chapter we talked about the forensics data acquisitions process. We introduced three different digital storage formats: raw, proprietary, and AFF. Next, we looked at the four methods of acquiring data for forensics analysis which are disk-to-image file, disk-to-disk copy, logical disk-to-disk or disk-to-data file, or sparse data copy of a folder or file. Then, we listed some useful forensic tools run on Windows, Linux and Mac OS.</p> <p>By the end of this chapter, we concluded that investigators always need to validate data acquisition with built-in tools, functions, or mechanisms, or by using forensics acquisition kits either open source or commercial. Besides, every considered operating system has its own mechanisms, tools, and artifacts that must be considered for validating data acquisition using MD5 or SHA-1 hashing functions, or the Linux md5sum or sha1sum commands.</p>

Activity Template	
Number	2.1
Title	Create a USB Drive using Linux Operating System
Type	Reflection
Aim	LO.1 In this activity, students will learn how to prepare a USB drive and create a FAT32 disk partition using Linux systems.
Description	For the purpose of this activity, students will need a Linux distribution CD and a USB drive to work with. The main task is to format the disk drive as FAT32 in Linux. Students may refer to the following Internet resource, or any other relevant resources of their choice that contain the necessary steps that must be followed. <i>https://www.garron.me/en/go2linux/format-usb-drive-fat32-file-system-ubuntu-linux.html</i>
Timeline	Implement the activity: 1 hr.
Assessment	The student's work is assessed based on his/her successful implementation of the required steps.

Activity Template	
Number	2.2
Title	Acquire Data from a USB Partition using Linux commands
Type	Reflection
Aim	LO.1, LO.5 & LO.6 In this activity, students will learn how to use Linux operating system commands to acquire data and validate it.
Description	<p>Students will use built-in Linux commands such as dd and md5sum to acquire and validate data. For this activity, students need a Linux distribution CD and a USB drive formatted with FAT32 (See Activity 1). The main tasks are to perform the data acquisition using each one of the following commands: dd, dcfldd, and dc3dd. After that, students will perform a validation of the acquired image files using md5sum command. Students may refer to the following Internet resources for more information.</p> <p><i>http://www.cyber-forensics.ch/acquiring-data-with-dd-dcfldd-dc3dd/</i> <i>https://www.howtoforge.com/linux-md5sum-command/</i></p>
Timeline	Implement activity: 2 hr.
Assessment	The student's work is assessed based on his/her successful implementation of the required steps.

Activity Template	
Number	2.3
Title	Use data acquisition tools to analyze a given case study
Type	Reflection
Aim	LO.3, LO.4, & LO.5 The aim of this activity is to provide students with some practical skills on how to use data acquisitions methods and tools studied in this topic to analyze a given case study.
Description	As a digital forensic expert, a business company has contracted with you to conduct an internal fraud. The company has several TBs of data stored on the network. The company manager has some doubts that one of the employees illegally tried to steal some sensitive data to another competitive company. Your main duties are to analyze this case -you can refer to system and network admins for more information- and write a two-page report to the manager explaining the problems you expect to face and how to rectify them. As well as which acquisition method and strategies should you use?
Timeline	Understand case study: 1 hr. Write report: 3 hrs.
Assessment	The student's work is assessed based on his/her successful implementation of the required steps.

Activity Template	
Number	2.4
Title	Analyze a computer forensic scene given as a case study
Type	Reflection
Aim	LO.2 to LO.5 In this activity, you will use the data acquisitions methods and tools that you have already studied in this topic to review a case study taken from a computer forensics scene.
Description	Your forensic firm is currently doing an investigation on a heinous murder in a residential building. As a member of the investigative group, your manager assigned you a task of having only a few minutes to acquire a several GBs of data on a suspect's computer. Within this time constrain, write a two-pages report that outlines the procedure and available options that must be taken to preserve the data.
Timeline	Understand case study: 1 hr. Write report: 3 hrs.
Assessment	The student's work will be evaluated based on his/her submitted report, the course of options suggested to handle the case, and report's discussion in the class.

Activity Template	
Number	2.5
Title	Use Internet search engines to research of the well-known digital forensic tools
Type	Search & Reflection
Aim	LO. 4 and LO.6 In this activity, you will use Internet search engines and the vendors listed in this topic to collect information about current data acquisitions tools.
Description	<p>For the purpose of this activity, students will use Internet resources to search for popular forensics tools. For each chosen tool, students will collect the following relevant information:</p> <ul style="list-style-type: none"> - Vendor Website - Tool Name - License Type - Supporting Platforms - Developers - Forensic model/s - Other relevant features <ul style="list-style-type: none"> • Supporting formats (Raw, AFF, Proprietary, etc.) • Compressing Methods • Remote network acquisition capabilities • Validation methods (MD5, SHA-1, etc.) <p>Students should prepare spreadsheets that contain the above information of each tool.</p>
Timeline	Search through the Internet: 3 hr. Prepare Spreadsheets : 3 hr.
Assessment	The students will be divided into groups of three students at maximum. Each group is required to submit the comparative spreadsheets and present it in the class as open discussion session.

Think Template (MCQs)	
Number	2.1
Title	Electronic data acquisition – legal compliance and requirements
Type	Choose the correct answer
Question	With remote acquisition, what problems should you be aware of? A. Data transfer speeds B. Access permissions over the network C. Antivirus, antispysware, and firewall programs D. All of the above
Answers	Answer: (D)

Think Template (MCQs)	
Number	2.2
Title	Electronic data acquisition – legal compliance and requirements
Type	True or False
Question	Computer forensics and data recovery refer to different activities. (A) True (B) False
Answers	Answer: (A)

Think Template (MCQs)	
Number	2.3
Title	Electronic data acquisition – legal compliance and requirements
Type	Fill in the blanks
Question	<p>What are two advantages and two disadvantages of the raw format?</p> <p>(A)_____</p> <p>(B)_____</p> <p>(C)_____</p> <p>(D)_____</p>
Answers	<p>The two main advantages are:</p> <p>(A) In some cases, it has fast data transfer speeds</p> <p>(B) It ignores minor data read errors on the source drive.</p> <p>The two main disadvantages are:</p> <p>(A) It requires as much storage space as the original disk.</p> <p>(B) It does not contain hash values in the raw file or metadata.</p>

Think Template (MCQs)	
Number	2.4
Title	Electronic data acquisition – legal compliance and requirements
Type	Fill in the blanks
Question	<p>Name the three formats for computer forensics data acquisitions.</p> <p>(A) _____</p> <p>(B) _____</p> <p>(C) _____</p>
Answers	<p>(A) Raw Format</p> <p>(B) Proprietary Formats</p> <p>(C) Advanced Forensic Format</p>

Think Template (MCQs)	
Number	2.5
Title	Electronic data acquisition - legal compliance and requirements
Type	True or False
Question	In a Linux shell, what is the dcfldd command which is used to list the suspect drive as /dev/hda1? _____
Answer	<i>dcfldd if=image_file.img of=/dev/hda1</i>

Think Template (MCQs)	
Number	2.6
Title	Electronic data acquisition - legal compliance and requirements
Type	True or False
Question	<p>Digital investigators usually apply static data acquisition when the suspect's computer operating system is write-protected and can't be altered.</p> <p>(A) True (B) False</p>
Answers	Answer: (A)

Extra Template	
Number	2.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	2.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

3. Computer Processing Crime and Incident Scenes

Scope Template															
Number	3														
Title	Computer Processing Crime and Incident Scenes														
Introduction	<p>The scope of this topic is:</p> <ul style="list-style-type: none"> (i) teaching students how to process and manage incident scenes, and the necessary investigation approaches for computing systems, (ii) introducing students to the rules of evidence and describing the differences between a business (private entity) and a law enforcement organization (public entity) in needs and concerns, (iii) explaining how to apply standard crime scene practices and rules for handling evidence in corporate and law enforcement computing investigations. 														
Outcomes	<p>LO.1: Describe how to collect evidence at private-sector incident scenes LO.2: Explain guidelines for processing law enforcement crime scenes LO.3: List the steps in preparing for an evidence search LO.4: Describe how to secure a computer incident or crime scene LO.5: Explain guidelines for seizing digital evidence at the scene LO.6: Explain how to obtain a digital hash LO.7: Review a case to identify requirements and plan your investigation LO.8: Explain why documentation is so important.</p>														
Topics	<p>3.1. An Overview of Digital Evidence 3.2. Private-Sector Incident Scenes 3.3. Preparing for a Search 3.4. Securing a Crime Scene 3.5. Seizing Digital Evidence at the Scene 3.6. Storing Digital Evidence 3.7. Chapter Summary</p>														
Study Guide	<table border="1" style="width: 100%;"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>1 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>8 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>1 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>6 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>2 hr</td> </tr> <tr> <td>Total</td> <td>18 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> 4. Ch. 4, Guide to Computer Forensics and Investigations (5th Edition). By Bill Nelson, Amelia Phillips, Christopher Stuart, 2016. 5. Ch. 12, Computer Forensics and Cyber Crime: An Introduction (3rd Edition). By Marjie T. Britz, 2013. 6. Ch. 4, A Practical Guide to Computer Forensics Investigations (2nd Edition). By Darren R. Hayes, 2019. 	Task	Time	Preparation (Introduction and On-line Planning):	1 hr	Textbook Content:	8 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	6 hr	Related Course Work:	2 hr	Total	18 hours
Task	Time														
Preparation (Introduction and On-line Planning):	1 hr														
Textbook Content:	8 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	6 hr														
Related Course Work:	2 hr														
Total	18 hours														

Content Template	
Section Number	3.1
Section Title	An Overview of Digital Evidence
Introduction	The main objective of this section is introducing students to the general guidelines for processing a digital investigation scene.
Content	<p>To handle a crime scene in an efficient manner, investigators must understand the criminal rules of search and seizure. Each country has its own criminal investigations rules, regulations, and procedures on how to process a crime scene. One of the main challenges that investigators face nowadays is how to establish recognized standards for digital evidence processes. For example, evidence might be distributed over multiple locations and tens or even hundreds of software or hardware components of evidence can be found. This includes HDDs, smart phones, and other computing devices. If certain law enforcement procedures have been agreed in some of these countries, the digital evidence might be viewed confidently like any other jurisdiction event. The Scientific Working Group on Digital Evidence (SWGDE) proposed a set of international standards on how to recover, preserve, and even examine digital evidence scenes. Students are recommended to review these standards to get an overview of common regulations shared by most countries. Furthermore, they must be trained to understand digital evidence resolution and analysis processes.</p> <p>Among the most important operations that digital evidence experts usually carry out when handling the evidence of a digital crime are:</p> <ul style="list-style-type: none"> • List all digital assets of a crime scene. • Systematically gather digital information from different available resources • Reduce the risk of losing evidence by documenting it. • Make a deep analysis to identify and organize digital evidence. • Regenerate the case circumstances. <p>Dealing with digital evidence is different than that of physical evidence because it can be easily modified. These changes can and must be detected by comparing the original data with a duplicate copy. Investigators can also use other methods with the help of segmentation or categorization of records into so called <i>computer-generated records</i> and <i>computer-stored records</i>. The first type can be defined as an any type of data that can be maintained by the system and its components, i.e., They are generated from computer processes or algorithms without user intervention such as log files and notifications triggered by management systems. Whereas, computer-stored records store electronic data on a computer main memory or an external digital device such as a USB drive. Some records may contain both types, such as Microsoft Excel sheets that contain computer-generated records such as a mathematical formula in a spreadsheet and computer-stored records generated by the user.</p>

Content Template	
Section Number	3.2
Section Title	Private-Sector Incident Scenes
Introduction	In this section we go forward and discuss digital evidence processing steps in private-sector organizations that include small to medium businesses, large corporations, and non-government organizations or agencies.
Content	<p>For customer privacy issues, the private market requires special treatment when dealing with digital evidence and crime scenes. Normally, organizations belonging to the private sector such as Internet Service Providers (ISPs) can examine computer crimes and service abuse carried out by their employees but not by customers. This is because ISPs have the responsibility to preserve the privacy of any customer's sensitive information they have, especially for some sensitive applications such as email and Web.</p> <p>Crimes in the private sector often take place at the workplace, e.g. an office or manufacturing area. This way, all events triggered by computers that are intended to violate the company's security policy must be under a controlled company management authority. Usually a business maintains a database of its assets. This database makes it possible to find data and applications which run on suspect devices. This could help in identifying the best forensics tools and procedures that are required to conduct the analysis. As an example, ISP companies deploy a common Web browser, such as Google Chrome for PCs or Safari for smart phones. By figuring out the name of the browser, investigators can conduct standard procedures to identify and retrieve digital evidence.</p> <p>Normally, investigators approve digital examinations only to named employees who are violating the company assets and operations such as stealing intellectual property. If investigators identify crime evidence during the investigation, they first need to identify whether the incident has a criminal law implication or not. During this process, examiners might have to consult company legal advisors to determine whether the situation is a potential crime. An example of a company policy violation issue is when an employee observes another employee's Web history. In some digital crime scenes, investigators can utilize the data found in log files which are stored in a proxy server to conduct a forensic investigation analysis.</p>

Content Template	
Section Number	3.3
Section Title	Preparing for a Search
Introduction	This section discusses the generic tasks that digital forensics examiners must perform before they search for computers or digital evidence in order to preserve the integrity of any digital crime evidence.
Content	<p>An important step in the digital investigation process is to prepare for evidence search and seizure. Generally, before starting a digital forensic task, an examiner will have to consult with or interview a number of people, including the victim, managers, the police department, etc. In addition to that, he/she can do the following tasks:</p> <ol style="list-style-type: none"> 1) Identifying the nature of the case under consideration: Examiners must initiate their investigations by identifying the structure of the crime scene they are dealing with. This includes determining whether it relates to the private or public sector. 2) Identifying the type of software or hardware: The second task is to determine the types of operating system and hardware devices. This allows the examiner to estimate the size of the suspect storage and determine how many digital devices have to be processed. 3) Determining whether an investigator can retain suspect's device: Determining whether examiners can remove a suspect's device from the scene mainly depends on the type of case, the location of the evidence and the law enforcement rules. 4) Obtaining more detail of the crime scene location: Getting more information about the location of the crime scene will help in gathering more evidence from the crime scene. Safety and environmental issues are the main concerns that investigators must properly handle during this process. This can be done prior to arrival at the digital crime incident by identifying the main hazards and procurement procedures to maintain safety. 5) Determining the person in charge: Normally, investigators seek for an established line of authority and normally only one person is needed to respond for digital evidence. Many cases need an investigation team to collect all the evidence quickly and connect with the managers to make sure that the members of the group process all digital evidence details. 6) Getting help from technical experts: Examiners of digital crimes may need additional support from technical experts to help them in analyzing crime scenes. Identifying the required technical expertise mainly depends on the type of case. 7) Determining the list of required tools: An investigator can start listing what tools he/she needs at the crime scene once the information has been collected. Two kits of tools might be in use: an initial-response field kit and an extensive response field kit. The initial-response field kit is the first one being used by the investigator due to its simple design and ease of transport. With this simple kit, an investigator can collect the data he/she needs and return to the investigation lab in a short amount of time. 8) Assembling an investigation team: The last task is to create a complete team of experts with the needed skills to assess the facts

	quickly, make the investigation plan, gather the needed resources and information, and collect data from the crime scene.
--	---

Content Template	
Section Number	3.4
Section Title	Securing a Crime Scene
Introduction	In this section, we will give a brief overview about the importance of securing crime scenes to keep information about the incident confidential and to preserve the integrity of evidence.
Content	<p>Investigators must secure crime scenes to preserve their confidentiality because information made public could negatively affect the investigation process. During the investigation process, examiners must use several mechanisms to secure the crime scene, such as using barrier tape to prevent others from entering the scene's location or taking photos with mobile devices. Therefore, accessing to the digital crime evidence should be allowed only to those people who have the right permission or some reasons to be there. One way of securing the incident location is to enlarge the controlled area beyond the exact location of the crime scene. In this way, uninterested people are kept away from what is really happening at the scene.</p> <p>In many crime scenes determining the security perimeter requires other specialists and detectives other than digital investigators themselves. The latter's main responsibilities are collecting physical evidence and defining a scene's security perimeter. For crime scenes involving mostly computers, the computers can be either a primary or secondary crime scene that contains evidence to be handled. In general, electronic devices such as computers may also have other peripheral devices that are considered as actual physical evidence, such as fingerprints on keyboards. Digital crime labs can use special tools to handle them. However, even well-trained experts to search crime scenes can intentionally or unintentionally modify some aspects of the crime scene.</p> <p>Digital investigators must also be aware of what they are doing and what they are touching either physically or virtually. They should take steps to ensure that no data is inadvertently modified before it has been forensically imaged. Even booting a computer can modify hundreds of timestamps.</p>

Content Template	
Section Number	3.5
Section Title	Seizing Digital Evidence at the Scene
Introduction	This section is intended to teach students the generic steps that must be taken during the processing of a civil or criminal investigation.
Content	<p>Depending on company internal policies, in most cases investigators do not have the credentials to work on other employees' machines and peripherals. In this case, investigators must follow standards for seizing digital data (See: www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf, or <i>ISO 27037</i>). The following are some guidelines that must be followed by digital investigators to seize digital evidence at the crime scene.</p> <ul style="list-style-type: none"> - Use logic to determine what are the steps that must be taken when processing a crime scene. - Document all actions. - Include timestamps of all activities in chronological order. - Make systematic updates of all documents as the processing is going on. - Make sure that only authorized staff can access the crime scene location. - Secure the crime scene perimeter. - Making sure not to miss anything in the crime location without investigation. - Refer all media and journalists to a public information media department. - Start by recording the overall crime scene, and then taking photos, videos of the area around the digital crime scene. - Make sure to check the used connections and devices with software as part of their license agreement. - Record the crime area and all access points to the machines, such as doors and windows. - Make a rough a sketch of all objects, their interconnections, and distances between them. - Check the status of each device to determine whether it is powered on or off . - Use standard digital forensic operations to kill the computer's power to make sure that data doesn't become corrupt. This operation is still typically available for legacy Windows OSs, but for new versions of Windows, UNIX, and Linux systems, investigators should first do an orderly shutdown before using this feature. <p>Once the scene has been recorded, examiners should apply the following steps to complete the process:</p> <ol style="list-style-type: none"> 1) To ensure the integrity of collecting digital evidence information, minimize the number of investigators. 2) Use unique attributes like current date and time, serial numbers and name of the person, to tag all the collected information. 3) Keep two log files of the collected information for auditing purposes. 4) Maintain a good control and management of the collected digital evidence information.

	<p>Finally, to finish the analysis and processing of evidence, examiners should gather all documents and digital media related to the investigation. This includes the following:</p> <ul style="list-style-type: none">– Physical component– Software component– Digital media storage such as USB drive– Handwritten notes
--	---

Content Template	
Section Number	3.6
Section Title	Storing Digital Evidence
Introduction	In this section we will talk about the different types of media being used to save digital evidence along with the storage devices to secure them.
Content	<p>Normally, investigators use different types of media to store digital evidence. Choosing the best media usually depends on the storage duration of the digital evidence. For example, in criminal situations, investigators need to store information as long as they can. Examples of media that can be used in this case are DVDs, DVD-Rs, DVD-RWs, or magnetic tapes that are mainly used to store big data. Figure 1 shows some of these types, and Figure 2 gives a brief comparative study among the most relevant ones. Unlike DVDs, tape drives can store tens of Gigabytes, but writing/reading data to/from them are very slow. If the user uses these tapes, he/she must test the stored data by making copies to a HDD.</p> <div style="text-align: center;"> </div> <p>Fig. 1: Examples of Storage media that can be used for digital investigation purposes.</p> <p>Recently, some disk manufacturers such as Quantum Corp have presented a new tape drive system with higher speed and capacity called Super Digital Linear Tape (SDLT) [1]. This type of systems is typically manufactured for archiving purposes, i.e.; it can store data up to several Tera Bytes of information.</p> <p>For security purposes, data can be copied and stored in more than one storage media to prevent data loss, and more than one forensic tool can be also used to double check the verification process. For example, investigators can apply the dd command in Linux to create the first image and another tool like ProDiscover to create another image. Also, some hardware copiers can easily create two copies of a disk at the same time. One approach is to create two copies of a hard disk and then replace the hard disk with one of the copies and then keep the original hard disk as the evidence and the second copy for analysis.</p>

Comparison of methods of secondary storage

Type	Speed	Method of Data Access	Relative Cost / MB
Magnetic tape	Slow	Sequential	Low
Floppy disk	Slow	Direct	Low
Fixed disk	Fast	Direct	High
Compact discs	Medium	Direct	Low
Optical disks	Fast	Direct	Medium
Flash drive	Fast	Direct	High

Fig. 2: Storage media comparative table

[1] https://en.wikipedia.org/wiki/Digital_Linear_Tape

Content Template	
Section Number	3.7
Section Title	Chapter Summary
Introduction	In this section we will summarize the main concepts presented in the previous sections.
Content	In Section 1, we provided an overview of the digital evidence process, the main management tasks, and the necessary investigation needs for computing systems. Section 2 introduced the rules of evidence and described the main differences between private and public entities. In Section 3, we explained in detail how to conduct the standard crime scene practices and rules of thumbs for handling evidence in corporate and law enforcement computing investigations. Also, in this section we discussed the generic tasks that digital forensics examiners must perform before they search for computers or digital evidence that preserves both the security and integrity of any digital evidence. In Section 4, we gave a brief overview about the importance of securing crime scenes to preserve the evidence and to keep information about the incident or crime confidential. Section 5 summarized the main guidelines on how to process a crime scene and what steps to take when processing a civil or criminal investigation. Finally, Section 6 reviewed the different types of media being used to save digital evidence along with the storage devices to secure them.

Activity Template	
Number	3.1
Title	Use the investigation methods to analyze an incident scene
Type	Reflection
Aim	LO.1 to LO.5 The aim of this activity is to use the investigation methods and techniques to analyze an incident scene.
Description	Consider the following case: You are working in a company as a digital forensic examiner, the CEO has received an e-mail about a serious assault that violates the company internal policy. He forwarded the email to you and asked for an immediate action. Write a two-page report outlining the list of actions you should do to handle this case.
Timeline	Write report: 3 hrs.
Assessment	The student's work will be evaluated based on his/her submitted report and the course of options suggested to handle the case.

Activity Template	
Number	3.2
Title	Use the investigation methods to analyze an incident scene
Type	Reflection
Aim	LO.1 to LO.5 The aim of this activity is to use the investigation methods and techniques to analyze an incident scene.
Description	As you are a Bitcoin forensics expert, you are conducting a digital forensic examination on a suspect's computer who may use the Bitcoin network to sell illegal goods. Currently, his/her computer has some running Bitcoin software and online sessions through a DSL connection. Write a two-page report outlining the necessary information that you must gather to package the evidence. Students may refer to the following Internet resource or to some other resources for Bitcoin concepts and terminology. <i>https://bitcoin.org/en/</i>
Timeline	Understand Basics of Bitcoin: 4 hrs. Write the report: 3 hrs.
Assessment	The students will be divided into groups of three students at maximum. Each group is required to submit the comparative spreadsheets and present it in the class at an open discussion session.

Activity Template	
Number	3.3
Title	Calculate hash values of given files
Type	Reflection
Aim	LO.6 The aim of this activity is to provide students with some practical skills on how to calculate and compare the hash values of given files.
Description	<p>This activity was adopted from Ref [1]. Students will have hands-on experience of the FTK manager forensic tool. They will create files and calculate their hash values. They will make some modifications to the content of files and recalculate the hash values again to compare the files. To do this activity, students need a Windows-running machine and a USB drive. Follow the following steps:</p> <ol style="list-style-type: none"> 1. Create a folder (Activity_3.3) on the USB drive → Open Notepad → Write "Working with hash values" → Save the file as test1.txt → Exit Notepad. 2. Start FTK Imager → File→ Add Evidence→ Select Source dialog box→ Click Logical Drive option button. 3. Select Drive Selection list arrow → USB drive → Finish. Expand USB drive → Right-click test1.txt → Export File Hash List → Save the file → Exit FTK Manager. Note (FTK Imager saves it as a test1.csv) 4. Start Notepad → Open test1.txt] → modify text → save file→ exit Notepad. 5. Start FTK Imager again → Repeat Steps 2 and 3→ Save the file as changed hash. 6. Repeat all steps for other files.
Timeline	Implement Activity : 1 hr.
Assessment	The student's work will be evaluated based on his/her submitted report and their understanding of hashing.

Activity Template	
Number	3.4
Title	Analyze a case study of an incident scene
Type	Reflection
Aim	LO.7 & LO.8 In this activity, you will use the crime investigation methods and tools to review a case study taken from a computer forensics scene.
Description	This activity was adopted from Ref [1]: Consider that you work as a digital investigator in a police department in your town. Your department manager receives a bomb threat claim in an anonymous e-mail for one of the local schools. Consequently, he/she sent you to conduct the investigation having information from a subpoena about the last known ISP where the anonymous e-mail originated, and that the message was sent from a residence in the school's neighborhood. Also, the school's Web server has been under an attack by an unknown computer attacker. The manager has got a warrant for the search and seizure of a computer at the residence the ISP identified. Your main task is to prepare a list of items that must be included in an initial-response field kit to ensure the preservation of computer evidence when the warrant is carried out.
Timeline	Understand the case study: 1 hr. Outline the action plan: 2 hr.
Assessment	The student's work will be evaluated based on his/her submitted report, the course of options suggested to handle the case, and report's discussion in the class.

Activity Template	
Number	3.5
Title	Analyze a case study of a crime scene
Type	Reflection
Aim	LO.1 to LO.8 In this activity, you will use the crime investigation methods and tools that you have already learnt in this topic to review a case study taken from a crime scene.
Description	Consider the case that you are police officer conducting a murder investigation in a big company in your town. Suppose that the primary suspect in a murder investigation (Person X) works at a local company and is reported to have two computers at work in addition to one at home. Write a two-page report stating what you would do if the company had its own computer forensics and investigations department and what you would do if the company did not.
Timeline	Understand the case study: 1 hr. Write a report: 2 hr.
Assessment	The student's work will be evaluated based on his/her submitted report, the course of options suggested to handle the case, and report's discussion in the class.

Think Template (MCQs)	
Number	3.1
Title	The CIA Model
Type	Fill in the blanks
Question	<p>What are the three main components of the Triad model?</p> <p>(A)_____</p> <p>(B)_____</p> <p>(C)_____</p>
Answers	<p>(A) Confidentiality</p> <p>(B) Integrity</p> <p>(C) Availability</p>

Think Template (MCQs)	
Number	3.2
Title	Computer Processing Crimes and Incident Scenes
Type	True or False
Question	<p>One of the main differences between private-sector and public-sector investigations is that the former focuses on policy violations, whereas the later involves criminal investigation agencies.</p> <p>(A) True (B) False</p>
Answers	(A) True

Think Template (MCQs)	
Number	3.3
Title	Computer Processing Crimes and Incident Scenes
Type	Choose the correct answer
Question	Which of the following techniques might be used in covert surveillance? (A) Keylogging (B) Data sniffing (C) Network logs (D) All of the Above
Answers	(A) & (B)

Think Template (MCQs)	
Number	3.4
Title	Computer Processing Crimes and Incident Scenes
Type	True or False
Question	<p>In some countries, if a company doesn't distribute a computing use policy stating an employer's right to inspect employees' computers freely, including e-mail and Web use, employees have an expectation of privacy.</p> <p>A. True</p> <p>B. False</p>
Answers	(A) True

Think Template (MCQs)	
Number	3.5
Title	Computer Processing Crimes and Incident Scenes
Type	Fill in the blanks
Question	List two hashing algorithms commonly used for forensic purposes. (A) _____ (B) _____
Answers	(A) MD5 (B) SHA-1

Extra Template	
Number	3.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	3.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

4. Fundamentals of File Systems

Scope Template															
Number	4														
Title	Fundamentals of File Systems														
Introduction	The aim of this topic is to provide students with an overview of how data is stored and managed on current and legacy Operating Systems (including Windows, Linux, and Macintosh), and how their file systems are structured. In addition, it discusses storage hardware devices such as Hard Disk Drive (HDD) and Solid-State Drive (SSD).														
Outcomes	LO.1: Describe Microsoft Windows file structures and New Technology File System (NTFS) LO.2: Explain Macintosh file structures. LO.3: Explain the Linux disk structures. LO.4: Explain how Hard Disk Drive (HDD) and Solid-State Drive (SSD) operate. LO.5: List some options for decrypting drives encrypted with whole disk encryption														
Topics	4.1. Microsoft Windows File Structure 4.2. Linux File Structure 4.3. Macintosh File Structure 4.4. Chapter's Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>1 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>8 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>1 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>15 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>3 hr</td> </tr> <tr> <td>Total</td> <td>28 hours</td> </tr> </tbody> </table>	Task	Time	Preparation (Introduction and On-line Planning):	1 hr	Textbook Content:	8 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	15 hr	Related Course Work:	3 hr	Total	28 hours
	Task	Time													
	Preparation (Introduction and On-line Planning):	1 hr													
	Textbook Content:	8 hr													
	Thinking (On-line discussions, Review questions)	1 hr													
	Tutorial Work:	15 hr													
	Related Course Work:	3 hr													
	Total	28 hours													
<p>Reading Material</p> <ol style="list-style-type: none"> Chs. 6 & 8, Guide to Computer Forensics and Investigations (5th Edition). By Bill Nelson, Amelia Phillips, Christopher Stuart, 2016. File System Forensic Analysis (1st Edition). By Brian Carrier, Addison-Wesley Professional, ISBN: 0321268172, 2005. 															

Content Template	
Section Number	4.1
Section Title	Microsoft Windows File Structure
Introduction	In this section we will give a brief review of the structure of Microsoft Windows file systems, namely FAT and NTFS. We will explain how data is stored and managed in these systems and outline the various activities performed by an operating system during the startup process to preserve the digital evidence from modifications.
Content	<p>A file system plays a crucial role in any Operating System (OS); it outlines how data is stored on the disk drive. For a digital investigation process knowing how to manipulate file systems has several benefits such as:</p> <ul style="list-style-type: none"> – In some cases, investigators have to login to computing devices to gather some information related to their investigations, so that he/she can access and modify file system settings as needed. – To ensure that data cannot be modified or altered during the investigation process, investigators must know how to access, monitor or even modify several system settings. – In some cases when digital forensic investigators need to work on a computer for forensic evidence, they need to work on the hidden partitions of the disk drive because it might contain files or parts of files that will help them during the investigation process. <p>The main system settings of an OS are normally stored into pieces of hardware inside the computer. These hardware devices are:</p> <ul style="list-style-type: none"> • Complementary Metal Oxide Semiconductor (CMOS) • Basic Input/Output System (BIOS) • Extensible Firmware Interface (EFI) • Unified Extensible Firmware Interface (UEFI) <p>In brief, CMOS stores timing information when the device is offline. While, the system BIOS, EFI, or UEFI contains system software that performs input/output at the hardware level. The main difference between these programs is that BIOS is used on older computers. When BIOS was designed, x86 was the most modern system available.). In this regard, to easily locate and load the OS into the RAM, MBR can be used that contains the necessary information to active this purpose. UEFI replaces BIOS in newer computers. It uses a so called Globally Unique Identifier (GUID) partition table which replaces the Master Boot Record (MBR) partitioning scheme with more advanced features.</p> <p>System users can access the setup programs by using several methods. Many BIOS manufacturers use the Del key to open the CMOS window; others use Ctrl+FI, F2, or F10. Each BIOS manufacturer’s screen has its own format. Users may refer to devices commercial Web sites to get more information.</p> <p>Investigators working in the digital forensics field should also be familiar with the structure of the HDD, and how information is being stored and located on them. Figure 1 shows the physical components of the HDD besides other relevant low-level parts such as tracks, cylinders, and sectors. Students should review all of these concepts before proceeding to the next topics.</p>

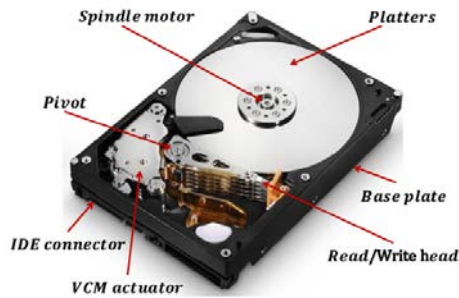


Fig.1: Main components of a Hard Disk Drive (HDD).

A Solid-State Storage (SSD) device is another type of hard drive that is mainly used in USBs, laptops, tablets, and cell phones. They have several key advantages compared to the traditional HDD. Figure 2 summarizes the main differences between SSD and HDD drive storing technology.



 SSD vs. HDD 		
0.1 ms	Access Times SSDs exhibit virtually no access time	5.5-8.0 ms
SSDs deliver at least 6000 io/s	Random I/O Performance SSDs are at least 15 times faster than HDDs	HDDs reach up to 400 io/s
SSDs have a failure rate of less than 0.5%	Reliability This makes SSDs 4-10 times more reliable	HDDs failure rate fluctuates between 2-5%
SSDs consume between 2 and 5 watts	Energy Savings This means that on a large server, approximately 100 watts are saved	HDDs consume between 6 and 15 watts
SSDs have an average I/O wait of 1%	CPU Power You will have an extra 6% of CPU power for other operations	HDDs average I/O wait is about 7%
The average service time for an I/O request while running a backup remain below 20 ms	Input/Output Request Times SSDs allow for much faster data access	The I/O request time with HDDs during backup rises up to 400-500 ms
SSD backups take about 6 hours	Backup Rates SSDs allow for 3-5 times faster backup for your data	HDD backups take up to 20-24 hours

Fig. 2: Comparison of the key differences between HDD and SSD disk drives.

It is worth noting that one of the main challenges that face digital forensic examiners when dealing with SSD drives compared to the HDD is that, since all SSD-based memory devices have a "wear-leveling" feature, deleted data cannot be recovered immediately, it might be lost forever. But, recovering data from HDD is easy. This is due to the fact that when data is deleted on a HDD, only the references to it are removed, which leaves the original data in unallocated disk space. Using an appropriate forensics tool, data can be recovered easily. Therefore, when dealing with SSD, its highly recommended that when recovering data from an unallocated disk drive making a full copy

of the data is very important. Without doing this, the wear-leveling feature automatically overwrites the unallocated space.

Microsoft Windows File Structures

Recall that Windows OS has two main file systems: FAT and NTFS (Refer to Table 1, Section 2.3 for more information). To easily understand these two file systems, it is necessary to have a look at the structure of the HDD where the file system is normally stored. A HDD can be logically partitioned into several sections, called logical drives, or partitions. Partitions can be primary - up to three primary partitions can be supported by Windows, and an extended partition that contains other logical partitions. Also, unallocated spaces can be used to store data ^[2]. In this way, it will not be shown by Windows. However, digital examiners could use disk editing utilities such as WinHex or Hex Workshop to access the unallocated area of the volume. By using these utilities, they can also examine a partition's physical level because they enable them to navigate critical parts of a specific file.

The physical structure of the HDD is divided into a number of sectors, and each sector is logically grouped into a number of clusters; each with size ranges from 512 Byte to 32 Kbyte, i.e., sectors are a hardware concept whereas clusters are usually defined by the file system. A Master Boot Record (MBR) is a special type of boot sector that is normally located at the very beginning. It holds file system area and boot record information as well as it contains executable codes for loading the OS. For more information on the structure of the HDD and the MBR, students may refer to Ref ^[3].

Working with FAT systems

The FAT system is simply a file structure that is used by the OS to manage files on volumes. It can be described as a map of all clusters that form the data area. It writes each file's data sequentially, i.e., it starts from cluster #1, cluster #2, and so on. In this context, If the FAT system allocated two or more clusters of a given file, then the FAT table entry will contain the address of the second cluster, the second cluster entry points to the third, and so forth. A FAT entry like this forms a linked list commonly called a cluster chain.

It is worth pointing out that the FAT system does store information about the location of the first cluster that was allocated for a given file. This information is normally stored in the directory. The directory entry for each file contains a value called a cluster address. This is a pointer to the first entry in the FAT for a given file. This FAT entry in turn points to the first cluster in the volume's data area that has been allocated to the file. Also, directory entry were used to store additional metadata such as stored file passwords, access rights, and owner IDs. Among other relevant information.

Working with NTFS systems

As previously mentioned in Chapter 1, NTFS has several improvements compared to the FAT file systems.

These include:

- (1) with FAT, the data is stored in the directory entry, and the FAT, and the data area, whereas in NTFS, just the MFT and data area are used. And with small files, the data is stored in the MFT itself,
- (2) NTFS gives more file details such as file credentials and other features,
- (3) By using NTFS users will have more control over all system files and directories,
- (4) it is also a journaling file system that keeps tracking all of the transactions and processing operations.

This will help the system to finish the ongoing transaction or return to the last optimal settings when a power failure has happened.

In the NTFS, the boot sector starts at sector #0 and can expand to 16 sectors. Then, it comes the Master File Table (MFT). NTFS stores all files and directories in separate records of 1024 Bytes each, where each record contains metadata about the file, the data of the file or links to these data. There are mainly two methods to store information in an MFT record: resident and non-resident. Small files, about 512 Bytes or less, are stored in the MFT and referred to as resident files since their metadata is stored in the MFT record. While, for larger files (greater than 512 Bytes) the system stores them outside the MFT record and assigns logical addresses. It is referred to as non-resident since the file's data is preserved in a separate file outside the MFT record. All MFT records start with header IDs that identify their states of whether they are resident or non-resident attributes.

The header information also contains additional data that determines where the first attribute ID starts. Also, each attribute ID has a length value in that defines where it ends and where the next attribute starts. Please refer to the following link that contains more detailed information on how the MFT is configured, <http://technet.microsoft.com/en-us/library/cc781134.aspx>.

Also, another NTFS feature that is worth mentioning is that it provides compression capabilities to improve data storage on disk drives. The only difference with FAT compression is that with NTFS users can compress files, folders, or entire volumes, whereas with FAT (FAT12/FAT16), compression is only accepted at the volume level. Microsoft has introduced a built-in encryption mechanism to the NTFS file system, called Encrypting File System (EFS)^[4]. EFS uses private or public key methods that are generally used in files and folder encryption. The encrypted data can be only decrypted using the owner's private key and the public key set by a certification authority.

Microsoft Windows Registry

Windows registry is a hierarchical database that stores software and hardware configuration parameters, network connections, usernames and passwords and setup information, among other information. It can contain valuable evidence that might be helpful for investigative purposes. Digital forensic investigators should have good technical skills for exploring system registries in all types Windows systems. The number of files the registry uses mainly depends on the Windows version. In legacy Windows Me, it uses only two files, *User.dat* and *system.dat*. In newer versions of Windows, it has at least six files they are *Ntuser.dat* (there is an *NTUSER.dat* file for each user on the system), *System.dat*, *SAM.dat*, *Software.dat*, *Security.dat*, and *Default.dat*. During the investigation process, when investigators are examining registry data from a suspect drive after they reviewed it in a forensics tool, they might need to know the location of these files. To get more information about this process see <http://support.microsoft.com/kb/250410>.

Microsoft Startup Tasks

In some crime scenes, investigators must keep digital information on the HDD just as it was before. Also, in some scenarios, trying to incorrectly login to a suspected device could corrupt the digital evidence. Fig. 3 illustrates the main steps that Microsoft Windows will follow during the boot up process.

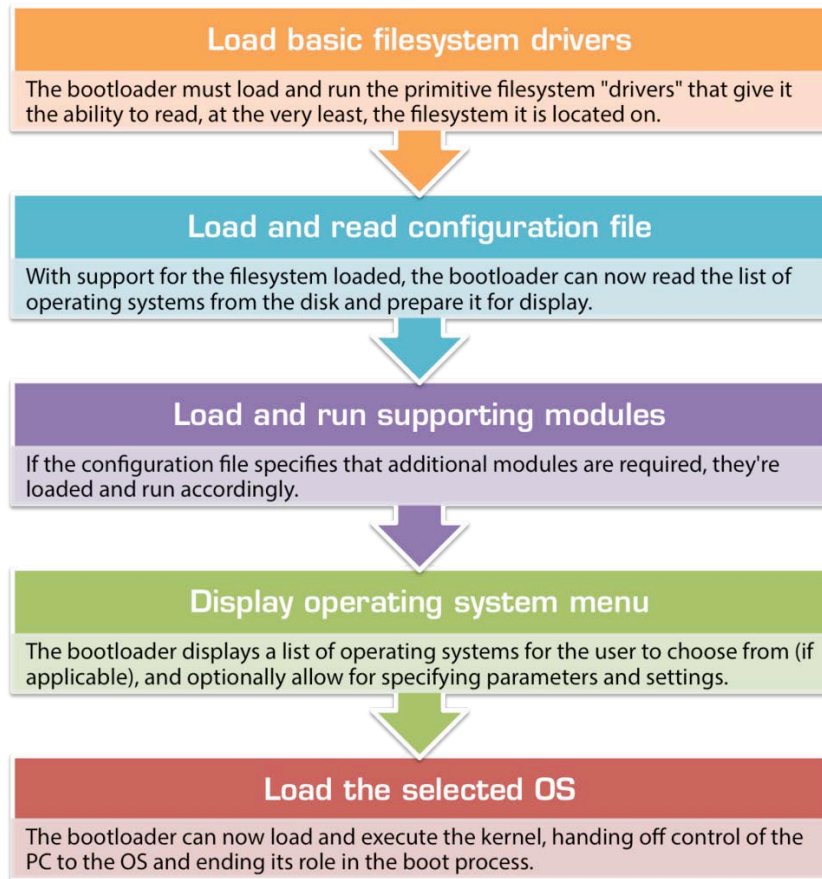


Fig. 3: Microsoft Windows boot process.

It is worth mentioning that, in Windows Vista and later, the boot process uses a boot configuration data (BCD) store which is registry file in the Boot BCD folder that is maintained to control the boot process. To access this file, investigators use the BCD Editor. In Windows 8, the BCD contains the boot loader that initiates the bootstrap process when Windows boots. In older versions of Microsoft Windows like Windows XP, the Ntldr program replaced other programs like bootmgr.exe, winload.exe, and winresume.exe.

[2] <https://www.disk-partition.com/disk-partiton/create-hidden-partition-on-usb-drive.html>

[3] <http://www.file-recovery.com/downloads/filerecovery.pdf>

[4] <https://docs.microsoft.com/en-us/windows/win32/fileio/file-encryption>

Content Template	
Section Number	4.2
Section Title	Linux File Structure
Introduction	In Section 4.1, we briefly explored Microsoft Windows file systems. This section continues this exploration by examining Linux file structures. In addition, it introduces some hands-on approaches to identifying Linux file structures with tools such as X-Ways Forensics, OSForensics, and WinHex.
Content	<p>Linux maintains an official kernel among all of its distributions including Ubuntu, Red Hat, and Debian. The Linux kernel is usually accompanied by components such as a GUI, several open-source applications that are developed and maintained by companies and users. Linux is only the core of the OS.</p> <p>File Structures in Ext4</p> <p>A wide range of file system standards are supported by Linux. The oldest one was called Second Extended File System (Ext2) and then came Third Extended File System (Ext3) which replaced Ext2 in most Linux distributions. The main difference between them is that Ext3 was using a journaling file system having built-in file recovery mechanisms. Nowadays, in all current Linux distributions, the fourth Extended File System (Ext4) is considered the standard file system. In addition to supporting all features of the former file systems, Ext4 has its own main features. They are:</p> <ul style="list-style-type: none"> - It supports a large partition size with several TBs in size - It has an improved management of large files - It has a more flexible approach for adding file system features <p>The Linux file system consists of four main parts:</p> <ol style="list-style-type: none"> 1. Boot block: It contains the instructions for startup - the bootstrap code. 2. Superblock: It is part of the Linux metadata that contains information about the file system. 3. Inode block: This block contains the first data after the superblock, and it is given all file allocation units. Inodes can be created or deleted like directories or files. Accessing control to the files or directories is managed by the links between their associated inodes. 4. Data block: The data block stores directories and files on a disk drive. This location is linked directly to inodes. <p>The following information is assigned to an inode associated with all created files and directories on a Linux file system.</p> <ul style="list-style-type: none"> • The mode and type of the file or directory • The number of links to a file or directory • The UID and GID of the file's or directory's owner • The number of bytes in the file or directory • The file's or directory's last access time and last modified time • The inode's last file status change time • The block address for the file data • The indirect, double-indirect, and triple-indirect block addresses for the file data • Current usage status of the inode

- The number of actual blocks assigned to a file
- File generation number and version number
- The continuation inode's link

One of the main Linux features that is not found in Windows is that it keeps track of bad sectors, which is referred to as the bad block inode. Inode #2 is the root inode, and the bad block inode is inode #1. Some forensics tools might ignore inode #1 and might fail to restore useful information. The `badblocks` command can be used to find bad blocks. `mke2fs` and `e2fsck` commands can be also used to check the device for bad blocks. They have other useful functions such as creating a file system and determining the block size in Bytes.

Hard Links and Symbolic Links

A hard link is as a pointer that allows users to access the same file using different filenames, all refer to the same inode and physical location on the disk drive, i.e. users with different login information could access the same physical file. If one user changed the file, the changes would be apparent when another user opened the file again. Users can use the `ln` command to create a hard link on Linux systems. But, to do that all files pointing to the same inode have to be on the same physical drive, not on another volume.

Symbolic links are also pointers. But, unlike the hard links, they can point to items on other disk drives or other parts of the network by using an absolute path. They have their own inode that is different from the inode of the item they point to. Furthermore, they are easier to identify on a running Linux system than hard links are and identify their destination by name and path. If both the name and path no longer exist, the symbolic link stops working.

Content Template	
Section Number	4.3
Section Title	Macintosh File Structure
Introduction	In this section, we cover Mac file structure and forensics procedures in Mac.
Content	<p>Mac OS X is the last family of OSs reviewed in this chapter. It is mainly built upon a core system called Darwin with a BSD UNIX distribution. Mainly, there are two file systems being used in Apple's OS. They are: Hierarchical File System (HFS), and Extended Format File System (HFS+). The main difference between them is that HFS was limited to support 65,536 block - 512 Bytes/block, and HFS1 increased it to 4 Billion and more. Consequently, HFS1 supports smaller file sizes on larger volumes, which enhances the disk usage.</p> <p>Both file systems have two descriptors for the physical and logical End-of-a File (EOF). The first one refers to the number of bytes allocated on the volume for a file. The second one represents the actual ending of a file.</p> <p>Mac File Structures</p> <p>In Mac OS, a normal file has two main components:</p> <ol style="list-style-type: none"> 1. Data fork: It typically stores user created information such as text or spreadsheets. Also it stores other user's applications that can read/write from/to the data fork. 2. Resource fork: It stores file's metadata and other application-specific information such as menus, icons, executable code, and controls. <p>Both forks share common contents for all files like resource map, resource header information for each file, window locations, and icons.</p> <p>A volume is a storage medium for hard disks that is being utilized to store files or directories. Each volume has both logical and allocation blocks. A logical block is a collection of data with 512 Bytes maximum. Allocation block is a group of consecutive logical blocks that is used to save a file. Depending on the file size, one allocation block can include several logical blocks.</p> <p>The HFS system uses a clumps technique to reduce file fragmentation, which are groups of contiguous allocation blocks that are managed to be a minimum for larger files. The first two logical blocks, namely 0 and 1, of this system are called boot blocks that contain startup instructions for a given system.</p> <p>Previous versions of Mac OSs used the Master Directory Block (MDB) for HFS, where all the volume's information is stored in the MDB and written to it when a specific volume is initialized. When the OS mounts a volume, it writes some information from the MDB to a Volume Control Block (VCB) and stores them in system memory. When a user unmounts the volume, the VCB is automatically removed. The MDB copy is continually updated when the extents overflow file or catalog increases in its size. The extents overflow stores any file information not found in the MDB or a VCB. The catalog maintains the relationships between files and directories on a volume.</p>

For digital forensics investigations in Mac OS X, examiners must know where file system components are located and how both files and file components are stored.

There are three applications formats used in the HFS system: plaintext, plist files (XML and binary) and the SQLite database. Text editors can be used to work with plaintext files. While, to view Plist files, users can use special editing programs such as PlistEdit Pro. These files are mainly considered as preference files for installed applications on a system which are stored in location /Library/Preferences. Finally, to view the SQLite database, one can use the SQLite Database Browser tools.

Among Mac OS files that might contain information useful for a digital forensics analysis process are:

- /System/Library/CoreServices/SystemVersion.plist: This file contains the installed version of the OS version.
- /Library/Preferences/SystemConfiguration/NetworkInterfaces. Plist: This file shows information about network connections.
- /private/var/db/DirectoryService/flatfile.db: It shows a list of user's information on a system.
- /private/var/db/dslocal/nodes/Default/users: This file contains user's plist files in the Mac OS X version.
- /private/var/db/shadow/hash: It contains user account passwords.

Several programs can be used inside the HFS system to encrypt and decrypt a user's directory such as FileVault. FileVault consists of two keys: master and recovery. Version 2 is available that encrypts the whole disk drive using 128 Bit AES encryption algorithms. Investigators can also find so called keychain files that show what applications and files require passwords in a variety of places. This information can be found following this path /System/Library/Keychains and /Library/Keychains.

In Mac OS X, deleted files are stored in the trashes folder. However, if a file is deleted using the Command Line Interface (CLI), it doesn't show up in the trash.

BlackBag Technologies have produced software to examine the Mac OS X file system. This company provides acquisition tools for newer version of Mac OS like OS 9 and OS X and have a forensic boot media named MacQuisition for making an image of a Mac HDD. They have also written a guide for forensic examination of Macs. For more information about the tools please refer to the following company web site (<https://www.blackbagtech.com/software-products.html>)

Normally, the tool that examiners use depends on the format of the file image. For example, if he/she used EnCase or FTK forensics to generate an Expert Witness image, he/she should apply one of these programs to analyze the content of the image. Otherwise, he/she can use any one of the following:

- X-Ways Forensics
- BlackBag Technologies Macintosh Forensic Software (OS X only)
- Guidance Software EnCase
- SubRosaSoft MacForensicsLab (OS X only)
- AccessData FTK

Students should get hand-on experience with these tools and try to differentiate between their functions and usage. As an example of their usage, BlackBag

	<p>Technologies Mac forensic software and SubRosaSoft MacForensicsLab have a nice feature of enabling or disabling the automatic mounting when the HDD is connected via an external USB or FireWire device. This feature will help users to connect a suspect disk drive to a Mac without a write-blocking device.</p>
--	--

Content Template	
Section Number	4.4
Section Title	Chapter Summary
Introduction	In this section, we summarize the main concepts outlined in the previous sections.
Content	<p>This chapter reviewed three main families of operating systems: Microsoft Windows, Linux, and Macintosh. It mainly focused on their file systems structures and how they store and manage data. In Section 1, we started the discussion by reviewing the two main Microsoft Windows file systems: FAT and NTFS. We also outlined the main tasks Windows OS performs, and reviewed some concepts such as the Master Boot Record (MBR), the registry in Windows, the main components of the HDD.</p> <p>Section 2 overviewed the Linux file systems: Ext2, Ext3, and Ext4, and outline the main differences among them. It also listed the main components defining the file system: boot block, superblock, inode block, and data block. In addition, it also talked about several core concepts of Linux such as inode, hard links and symbolic links.</p> <p>The last OS discussed in this chapter (in Section 3) was Mac OS. We mentioned its two main file systems: HFS and HFS1 and outlined the main difference among them. We also talked about the structure of a file which consists of two parts: a data fork and a resource fork. In addition, we talked about several main concepts of Mac OS such as clumps and Plist files.</p>

Activity Template	
Number	4.1
Title	Compare contents of several files at the hexadecimal level
Type	Reflection
Aim	<p>LO.1 & LO.2</p> <p>The aim of this activity is to teach students how to become familiar with different file types and compare various files to determine whether they are different at the hexadecimal level or not.</p>
Description	<p>In this activity, students will compare files created in Microsoft Office to determine whether the files are different at the hexadecimal level. Students can use Windows and follow the following steps:</p> <ol style="list-style-type: none"> 1. Create a Word document with some text → save it → and exit. 2. Create an Excel sheet with some numbers → save it → exit. 3. Download Hex Workshop (http://www.hexworkshop.com/) 4. Start the Hex Workshop → open the doc. file you created in Step (1). 5. In Hex Workshop, navigate the Editor pane to find Offset, Hex, and Text columns. In a separate document write the information you captured in these columns.

	6. Repeat Step (5) for the Excel sheet you created in (2) 7. Compare the printouts extracted from Steps (5 and 6) and describe any differences you found in the MS Office header.
Timeline	Understand the activity: 1hr. Implement the above steps: 1hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps.

Activity Template	
Number	4.2
Title	Explore the Master File Table (MFT)
Type	Reflection
Aim	LO.1 & LO.4 The aim of this activity is to introduce students with the necessary practical skills on how to explore the Master File Table (MFT) of Microsoft Windows to locate date and time values in the metadata of a file they create.
Description	<p>In this activity, students will explore the Master File Table (MFT) and learn how to locate date and time values in the metadata of a file they create. To implement this activity, students need the following components:</p> <ul style="list-style-type: none"> • ProDiscover Basic (Download it using the following link) http://prodiscover-basic.freedownloadscenter.com/windows/ • WinHex Demo (Download it using the following link) https://www.x-ways.net/winhex/ <p>Follow the following steps:</p> <ol style="list-style-type: none"> 1. Create a folder on your C Drive → Create .txt file with some random text → save the file in your work folder. 2. Start ProDiscover Basic → Go to PhysicalDrive0 → Type c-drive → Click to expand Content View, Disks, and PhysicalDrive0 → o to Work area → Right-click \$MFT → click Copy File → Navigate to your work folder → Click Save. Students may refer to this YouTube link to help them navigate the tool (https://www.youtube.com/watch?v=f5czUMeazo) 3. When the \$MFT file has been copied to your work folder, exit ProDiscover Basic, saving the project if prompted. 4. Start WinHex Demo → Click the Open toolbar button. → Navigate to your work folder → Open \$MFT file → Click Search → name of text file created in (2) → Click the Format Code list arrow → click Unicode. Students may refer to the following YouTube link to help them navigate the tool) (https://www.youtube.com/watch?v=AIeaSM0d_6M) 5. Data Interpreter window → click Options → Click the Win32 FILETIME (64 bit) → Go to WinHex window → Click at the beginning of the record, on the letter F in FILE → Drag down till the counter reaches 50, release the mouse button. 6. Move the cursor one position to the left and record the date and time of the Data Interpreter's FILETIME values. 7. Repeat Steps 5 and 6, using the offset positions plus 1 Byte to see the values for the remaining date and time positions. Write down these values. When you're finished, exit WinHex and hand in the date and time values you recorded.
Timeline	Understand the activity: 1hr. Implement the above steps: 1hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps.
Activity Template	
Number	4.3
Title	Perform an OS X file system analysis
Type	Reflection and Search
Aim	LO.3 & LO.4

	The aim of this activity is to introduce students with the necessary practical skills on how to explore the OS X file system, its functions, and tools available in BlackBag Technologies Macintosh Forensic Software.
Description	<p>This activity was adopted from Ref [1]. In this activity, students will perform an OS X file system analysis to become familiar with the functions and tools available in BlackBag Technologies Macintosh Forensic Software. To successfully implement this activity, students need the following components:</p> <ul style="list-style-type: none"> • Macintosh (OS X 10.2) (https://support.apple.com/downloads/mac-os-x-10.2.2) • BlackBag Technologies - Download Demo Version from here (https://www.blackbagtech.com/) <p>To prepare for this activity, do the following:</p> <ol style="list-style-type: none"> A. Make sure the following files have been extracted to your work folder: GCFI-OSX.001 through GCFI-OSX.007. B. Rename each GCFI-OSX image file in the Macintosh Disk Image format with .dmg and .dmgpart extensions. C. Start Finder, and locate and double-click the first file, GCFI-OSX.dmg (previously GCFI-OSX.001), to mount the disk image. <p>Follow these steps for the partition mapping data on this OS X drive:</p> <ol style="list-style-type: none"> 1. Start BlackBag → click PDISKInfo on the BlackBag Forensic Suite ToolBar → Click the Suspect Device list arrow → Click the .dmg file. (https://www.youtube.com/watch?v=5nVShcqf05I) 2. Click the Partition Map → Type the root password for your Macintosh system → Save the PDISKInfo output by clicking Save Report → Type GCFI-OSX-partprt.txt → click Save. 3. In the Where drop-down list box, click the folder where you want to save it. If the ReportSaved dialog box opens, click OK. When you're finished, exit PDISKInfo. 4. Repeat these steps, clicking the PMAPInfo and IORegInfo buttons on the BlackBag Forensic Suite ToolBar, and save the report each utility creates. For the IORegInfo utility, click All Information. 5. Continue the analysis of this drive to learn how the DirectoryScan, File-Searcher, and VolumeExplorer utilities work. When you have finished, write a short paper describing the results of each function.
Timeline	Understand the activity: 1hr. Implement the above steps: 2hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps, and the short paper that will be submitted after completing the activity.

Activity Template	
Number	4.4
Title	Analyze an image file with Sleuth Kit and Autopsy tools
Type	Research
Aim	LO.4, LO.4, & LO.5 The main purpose of this activity is to teach students how to become familiar with Sleuth Kit and Autopsy tools. Students will convert an image file to a raw dd image, and then analyze it with these two tools.
Description	<p>This activity was adopted from Ref [1]. For this activity, students will convert the image file GCFI-datacarve-FAT.eve to a raw dd image by using ProDiscover Basic, and then will analyze it with Sleuth Kit and Autopsy tools. To successfully implement this activity, students need the following:</p> <ul style="list-style-type: none"> • A PC running Windows with ProDiscover Basic installed (https://prodiscover-basic.software.informer.com/8.2/) • A Linux or UNIX system with Sleuth Kit and Autopsy installed (https://www.sleuthkit.org/), (https://www.sleuthkit.org/autopsy/) <p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Start ProDiscover Basic → Go to Image Conversion Tools → Click Convert ProDiscover Image to 'DD' → Click the location in your work folder where you saved GCFI-datacarve-FAT.eve → Click OK → Exit ProDiscover Basic. 2. Start Sleuth Kit and Autopsy → Click New Case → Fill in your information (using GCFI-datacarve-FAT for the case name) → Click New Case. 3. Click Add Host → Enter your information → Click Add Host → Click Add Image → click Add Image File → Type the full pathname and the GCFI-datacarve-FAT.dd image filename in the Location text box → click the Partition option button → Click the Copy option button for the import method → Click Next. 4. Go to the Image File dialog box → Click Add → click the Analyze button. 5. Click File Analysis → Click Generate MD5 List of Files → Save the list as GCFI-datacarve-FAT-MD5.txt in your work folder → Close the MD5 Results window. 6. Click File Type → click Sort Files by Type → Print the Results Summary frame of the Web page. 7. Click Image Details → Print the frame containing the results. 8. Write a report describing the information each function asks for and what information it produces so that you can begin building your own user manual for this tool.
Timeline	Understand the activity: 1hr. Implement the above steps: 2hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps, and the short report that will be submitted after completing the activity.

Activity Template	
Number	4.5
Title	Use online resources to research for popular tools that allow Linux to perform read and write access to an NTFS-formatted drive.
Type	Search
Aim	LO.1, LO.3 to LO.5 The aim of this activity is to teach students on how to use online resources to research for popular tools that allow Linux to mount and perform read and write access to an NTFS-formatted drive.
Description	The purpose of this activity is to provide students with more technical information on how to mount NTFS partitions on the Linux operating system to perform read and write access. To do that, students will use the Internet resources to gather information. After that, they will write a two-page report outlining all the necessary steps, available drivers and software that are needed to be installed in any Linux distribution. (Hint: See www.linux-ntfs.org or http://sourceforge.net/projects/linux-ntfs/ to start your research.)
Timeline	Search through the Internet: 1hr. Write a report: 2hr.
Assessment	The student's work will be evaluated based on the submitted report and its alignment with the activity's objectives.

Think Template (MCQs)	
Number	4.1
Title	Fundamentals of file systems
Type	Choose the correct answer
Question	How many bytes does a disk drive sector typically contain? (A) 256 (B) 512 (C) 1024 (D) 2048
Answers	(B) 512

Think Template (MCQs)	
Number	4.2
Title	Fundamentals of file systems
Type	Choose the correct answer
Question	<p>Virtual machines have which of the following limitations when running on a host computer?</p> <p>(A) Internet connectivity is restricted to virtual web sites.</p> <p>(B) Applications can be run on the virtual machine only if they're resident on the physical machine.</p> <p>(C) In some case, the capability of a virtual machine is constrained by the host computer's peripheral configurations, such as mouse, keyboard, CD/DVD drives, and other devices.</p> <p>(D) Virtual machines can run only OSs that are older than the physical machine's OS.</p>
Answers	(C)

Think Template (MCQs)	
Number	4.3
Title	Fundamentals of file systems
Type	True or False
Question	Metadata of NTFS normally uses 16-bit Unicode for character code representation instead of the 8-bit configuration that ASCII uses. (A) True (B) False
Answers	(A)

Think Template (MCQs)	
Number	4.4
Title	Fundamentals of file systems
Type	Fill in the blanks
Question	<p>List three pieces of information found in metadata in the Linux file system.</p> <p>(A) _____</p> <p>(B) _____</p> <p>(C) _____</p>
Answers	<p>(A) User ID (UID)</p> <p>(B) File Size</p> <p>(C) File Permission</p>

Think Template (MCQs)	
Number	4.5
Title	Fundamentals of file systems
Type	Choose the correct answer
Question	EFS can encrypt which of the following? (A) Files, folders, and volumes (B) Certificates and private keys (C)The global Registry (D) Network servers
Answers	(A)

Think Template (MCQs)	
Number	4.6
Title	Fundamentals of file systems
Type	Choose the correct answer
Question	<p>How does Mac OS 9 reduce disk fragmentation?</p> <p>(A) Clumps are used to group contiguous allocated blocks.</p> <p>(B) The MDB is reconfigured by File Manager.</p> <p>(C) Data is written to the extents overflow file.</p> <p>(D) Disk Arbitration is used to reorganize data on the volume.</p>
Answers	(A)

Think Template (MCQs)	
Number	4.7
Title	Fundamentals of file systems
Type	Choose the correct answer
Question	In UNIX OSs, drives, monitors, and NICs are treated as which of the following? (A) Objects (B) Tar devices (C) Files (D) Mount devices
Answers	(C)

Think Template (MCQs)	
Number	4.8
Title	Fundamentals of file systems
Type	Fill in the blanks
Question	List three features that NTFS has that FAT does not. (A) _____ (B) _____ (C) _____
Answers	(A) Unicode characters (B) Security (C) Journaling

Extra Template	
Number	4.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	4.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

5. Overview of Common Tools for Digital Forensics

Scope Template															
Number	5														
Title	Overview of Common Tools for Digital Forensics														
Introduction	The scope of this topic is to introduce students to the background of common software and hardware forensics investigations tools. It will also explain how to select tools for computing investigations based on specific criteria.														
Outcomes	LO.1: Explain how to evaluate needs for computer forensics tools LO.2: Describe available computer forensics software and hardware tools LO.3: Apply forensics tools to analyze case studies LO.4: List some considerations for computer forensics hardware tools LO.5: Compare forensics tool functions LO.6: Describe methods for validating and testing forensics tools														
Topics	5.1 Main Functions of Computer Forensics Tools 5.2 Computer Forensics Software Tools 5.3 Computer Forensics hardware Tools 5.4 Forensics Software Validation Protocols 5.5 Chapter's Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>1 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>6 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>1 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>8 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>2 hr</td> </tr> <tr> <td>Total</td> <td>18 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> 1. Chs. 6 & 7, Guide to Computer Forensics and Investigations (5th Edition). By Bill Nelson, Amelia Phillips, Christopher Steuart, 2016. 2. Part II & Part III, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (1st Edition). By Michael Hale Ligh, Andrew Case, and Aaron Walters, 2014. 	Task	Time	Preparation (Introduction and On-line Planning):	1 hr	Textbook Content:	6 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	8 hr	Related Course Work:	2 hr	Total	18 hours
Task	Time														
Preparation (Introduction and On-line Planning):	1 hr														
Textbook Content:	6 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	8 hr														
Related Course Work:	2 hr														
Total	18 hours														

Content Template	
Section Number	5.1
Section Title	Main Functions of Computer Forensics Tools
Introduction	This section discusses the main functions of software or hardware digital forensic tools. We list the main criteria used to select tools for digital investigations.
Content	<p>Digital forensic utilities are mainly classified into those aimed at hardware or software. A hardware tool can be a simple one, for example set up for a single-purpose component or a more complex one like those necessary for computer systems and servers. An example of a single-purpose hardware tool is the Tableau T35es-R2 SATA/IDE eSATA. It is used to access a SATA or an IDE disk drive with one device. Expert systems and DIBS Advanced Forensic Workstations are some examples of digital forensic hardware tools mainly deigned for complete systems. Software forensic tools can be also sub-divided. There are command-line GUI based tools, SafeBack is an example of a command-line disk acquisition tool that was mainly designed for a specific task. Other tools are designed to perform several different tasks like PassMark Software OSForensics, AccessData FTK, Technology Pathways ProDiscover, X-Ways Forensics. Software forensic tools are also commonly used for data copying purposes.</p> <p>Hardware and software forensics tools share common specific functions. The following set of functions are being used as guidelines to evaluate digital forensics tools. As will be shown later, every function has several subfunctions specific to data analysis, data recovery, and data quality assurance.</p> <p>1. Data acquisition</p> <p>One of the first tasks that digital forensic investigators should care about is how to acquire data from a device and make sure to preserve the original disk drive. This can be done by making a replica of the main HDD to save the digital evidence, if there is any, from damage or corruption. Data acquisition has several subfunctions they include the following:</p> <ul style="list-style-type: none"> - Physical data copy - Logical data copy - Data acquisition format - Command-line acquisition - GUI acquisition - Remote, live, and memory acquisitions. <p>Software acquisition can be done either physically or logically. Physical acquisition is to make a full copy of the whole HDD, whereas in the logical acquisition only a disk partition is copied. Furthermore, some software acquisition methods have built-in mechanisms to make a full image of the whole HDD. Usually, the crime scene determines which type of acquisition methods an investigator should use to achieve the intended goals.</p> <p>2. Validation and Verification</p> <p>Validation and verification are two main functions that are mainly used to for testing purposes. Here, validation is specifically used to confirm that a tool is functioning as expected without unexpected results, and verification assures that any two datasets (the original drive with the image) are completely identical. This process can be done with the help of hashing algorithms. The Scientific Working</p>

Group on Digital Evidence (SWGDE) has some online datasets used as benchmarks for testing digital forensics tools. As an example, consider the forensics tool EnCase. This tool prompts the user to obtain the MD5 hash value of acquired data, and FTK is used to validate the generated MD5 and SHA-1 hash sets during the process of acquiring digital data. Also, some hardware acquisition tools have facilities to simultaneously apply both the MD5 and CRC-32 hashing algorithms to acquire the data. Examples of such tools are Image MASSte and Solo-4. It is highly recommended to use the tool with built-in hashing function mechanisms for verification purposes. The hashing mechanisms itself depends on the investigation process. But, in most cases when it is being used it produces a unique hexadecimal value for ensuring that the original data is unchanged. The National Software Reference Library (NSRL) is a good resource that can be used by investigators to get technical details about the best hashing values being used for various OSs, and images that investigators can download from: www.nsrll.nist.gov/Downloads.html.

3. Extraction

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

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

All these subfunctions can give digital investigators good flexibility in exploring the data. Data analysis, recovery, and encrypting, or decrypting files are considered major challenges that need special treatment by investigators.

From the point of view of a digital investigation, encrypted files and systems are a big challenge. This is due to the fact that many password recovery tools are freely available with built-in mechanisms to generate potential password lists (Brute-force attack).

4. Reconstruction

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

(1) to analyze the different activities that occurred during the crime scene, and
(2) to share the disk drive with other investigators who are working on the same problem. This allows them to engage in more extensive testing and analysis of the digital evidence,

(3) it is also done if a disk drive has been infected by malware or any malicious software.

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

- Disk-to-disk copy
- Partition-to-partition copy
- Image-to-disk copy
- Image-to-partition copy

- Disk-to-image copy
- Rebuilding files from data runs and carving

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

5. Reporting

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

- Bookmarking or tagging
- Log reports
- Report generator

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

Table 1: Comparisons of forensics tools functions [1].

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

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

In summary, Table 1 shows a comparison of some digital forensic tool functions discussed above. It is worth noting that, investigators may develop their own comparative table by adding other functions as necessary to determine which tools perfectly fit with the case they are working with.

	Also, it is highly recommended to refer to some nonprofit organizations' websites like NIST's Computer Forensics Tool Testing (CFTT) program, and ASTM International's E2678 standard when working and testing digital forensics tools.
--	---

Content Template	
Section Number	5.2
Section Title	Computer Forensics Software Tools
Introduction	This section explores the various commands and programs that are being used in the data acquisition process. We focus on those that use the command-line interface as well as GUI interfaces and those implemented in both Windows and UNIX/Linux systems.
Content	<p>As previously mentioned in Section 5.1, digital forensics investigators have the freedom to select the tool that achieves their objectives and goals. The selected tool can be either command-line or GUI based so long as it is compatible with the suspect's operating system.</p> <p>Command line tools (CLI) are preferable in systems with limited resources since they do not require a lot of system resources. Some command-line forensic software is specific to Microsoft Windows systems. Others are implemented for Linux platforms or Macintosh. Examples of Windows based CLI tools are those created by private companies like NTI, Digital Intelligence, DataLifter, and ByteBack. Linux has several built-in command-line tools like dcfldd and dd programs.</p> <p>Command-line forensics tools are rarely used in current versions of Windows. The Microsoft DOS was extensively explored as a CLI tool for doing normal tasks, but it has been rarely used for digital forensics analysis due to its age. Nevertheless, the first tools that are mainly used for the purpose of data extraction and analysis from floppy of HDD were based on MS-DOS, such as Norton DiskEdit. This tool was mainly based on manual processing with limited capabilities. Currently many desktops come up with an installed version of Microsoft Windows. Therefore for machines running Windows, software developers now have GUI forensics tools to help investigators in their examination. Current tools have more powerful features such as data search and import capabilities, hash value mechanisms data recovery.</p> <p>Linux platforms are becoming more popular nowadays for both home and business usage. This popularity is due to the fact that most Linux distributions are open source and are popular in developing users applications and services. However, these advantages put a burden on their users to obtain more technical experience of the Linux terminal and its digital investigative environment. In the following section we briefly list some of the well-known Linux digital forensics tools and provide a description of their functions and capabilities.</p> <p>1. SMART</p> <p>SMART is a powerful digital forensics tool having the following features</p> <ul style="list-style-type: none"> – It is compatible with almost all Linux distributions such as Fedora, SUSE, Debian, UBUNTU. – It has the capability to work with different file formats. – It includes several plug-in utilities to ease the update process. – It supports multithreading OSs and hardware. – It can be used to mount different file systems. – It has the hex viewer with color-code values to mark the start and end of a file. – It has the capability to report features and data logging capabilities.

2. Helix 3

The unique feature of this tool is that it can be used on live data acquisitions. This function can be done by inserting the Helix media into the suspect's computer to extract data while the system is running. Investigators might need to retrieve active contents like the suspect's user profile, from a computer or server that can't be turned off or seized. Thus, this tool can help in achieving this task.

3. Autopsy and Sleuth Kit

Autopsy and Sleuth Kit tools are considered as part of the Kali Linux kit. This tool is one of the main tools extensively used by digital investigators when working with Linux machines. Sleuth Kit is a forensics tool that is mainly designed for Linux systems, and Autopsy is its GUI browser interface. Both are accessed from Kali kit. Students will get hands on experience in the activity part on how to use these tools to analyze given crime scenes.

Content Template	
Section Number	5.3
Section Title	Computer Forensics Hardware Tools
Introduction	In this section, we overview some hardware tools and utilities that are used for digital forensic investigative purposes.
Content	<p>Many hardware manufacturers design and produce various types of forensic workstations and devices with a variety of features to meet the digital investigation needs. But, in general, there are three types of forensic workstations. They are:</p> <ul style="list-style-type: none"> - Stationary workstation - Portable workstation: A laptop with all input and output devices that can be utilized as a stationary workstation - Lightweight workstation: A laptop with a minimum set of peripherals that can be easily carried out and used in crime locations. <p>There are several considerations investigators must care about when buying an investigative workstation. The most important one is diversity of the investigative environment. For example, some digital forensics operations force the investigator to keep the workstation running all the time (24/7) without slowdown periods. This case could happen when investigators must analyze huge datasets coming from different locations and having different formats and characteristics. To choose an appropriate workstation that perfectly fits with this case, investigators must choose machines with enduring hardware physical equipment.</p> <p>Investigators must carefully analyze their environment to carefully choose hardware needs. Several factors can help investigators to choose such as:</p> <ul style="list-style-type: none"> - Equipment costs and available budgets - Stations running time periods - Impact of hardware failures - Cost of hardware support in the long run - Cost of replacing the workstations <p>Based on the above points, investigators must create a plan to balance their needs and the suggested machine specifications. This way, they can save time and money. It is also highly recommended for future plans that investigators must use more than one hardware configuration as this will help them facing any diverse investigations to streamline the workstation to achieve the target needs.</p> <p>If an investigator has the necessary technical hardware skills, then he/she can build his/her own forensic workstation. Otherwise, investigators must ask for help. Some hardware vendors offer a designed workstation for digital forensics. Example like the Digital Intelligence or hardware mounts from ForensicPC. Also, investigators are not forced to purchase all equipment from one vendor, they can choose components from several vendors and match them to get the hardware capabilities they need.</p> <p>Software or hardware write-blockers can be also used to maintain digital evidence on HDDs by avoiding the "write new data" commands. Examples of software write-blockers are PDBlock from Digital Intelligence. Hardware write-blockers are mainly located between the suspect HDD and the forensic</p>

	workstation. They intentionally prevent an OS from trying to write new data to the blocked drive.
--	---

Content Template	
Section Number	5.4
Section Title	Forensics Validation Protocols
Introduction	In this section, we will discuss the common validation methods available for testing digital forensics tools. We will also explain how to develop new validation protocols and mechanisms.
Content	<p>As previously mentioned, one of the main non-profit organizations that considers digital forensics is the National Institute of Standards and Technology (NIST). It is continually publishing articles, suggesting tools, and creating reports, and procedures utilizing the ISO 17025 criteria for testing and validating forensics software. For the successful validation of digital forensics tools, investigators must achieve the following criteria:</p> <ul style="list-style-type: none"> - Classify the available digital forensics software in groups - Identify the main requirements and the technical features of each group - Create several tests to validate the tool. - Identify a number of cases that can be used to test the forensic tool. - Specify how to test the validation method - Combine the test results into a report <p>ISO 5725 is another international standard that could be also used for testing purposes. NIST has created the NSRL project that contains common hash values for vendor property tools and OS files. The primary hash algorithm that the NSRL used was SHA-1. It creates digital signatures called the Reference Data Set (RDS). Investigators may also use more than one tool to verify their obtained results or validate software or hardware upgrades. This is can be done by performing the same tasks with two similar tools. One method that can be followed to a tool is to use disk editing tools, such as WinHex, or Hex Workshop. These tools have a nice interface that typically shows information like files, slack, file headers, amongst other data. In the activity part, students will work on hands-on projects that help them apply these concepts to validate some digital forensics software tools.</p> <p>Digital forensics examiners can also use the following testing steps to validate the GUI forensics tool.</p> <ol style="list-style-type: none"> 1. Perform the investigation with one GUI tool. 2. Repeat step (1) with a disk editing service to check whether the GUI tool 3. Get the hashing value of both results (the GUI tool and the disk editing service), 4. Compare both values obtained in (3) to cross check the hash value obtained from both tools. <p>Finally, for all things to be consistent, investigators must keep the OS and the digital forensics tools up to date. This requires installing all new system releases and patches and keeping the OS in a healthy condition all the time, and also checking the tools' Web for new updated versions or patches.</p>

Content Template	
Section Number	5.5
Section Title	Chapter's Summary
Introduction	This last section summaries the points presented in this chapter.
Content	<p>The topics of this chapter introduced some theoretical and practical skills of common software and hardware forensics investigative tools. It also explained how digital investigators use specific criteria to select the appropriate tool from many other options.</p> <p>In Section 1, we started this chapter by discussing the generic functions of any digital forensics tool. This includes data acquisition, data validation and verification, data extraction, data reconstruction, and data reporting. Section 2 talked about software forensic tools. Some tools run in a command-line interface, others use a GUI interface, and some others support both interfaces.</p> <p>In section 3, we discussed the hardware requirements for digital forensics workstations, such as write-blockers that are mainly used to preserve the integrity of the digital evidence. Before purchasing or building a forensic workstation, investigators must take into their account the location of which data should be acquired to determine the suitable hardware configurations.</p> <p>The different validation mechanisms are summarized in Section 4. Mainly, most of these mechanisms suggested and maintained by international non-profit organizations like the National Institute of Standards and Technology (NIST) is a good reference to consider that contains a number of tutorials and guidelines to verify the various types of forensic tools. It is highly recommended to refer to these standards to understand how the validations mechanisms are performed.</p>

Activity Template	
Number	5.1
Title	Use the AccessData FTK forensics tool to analyze data stored in a USB drive
Type	Reflection
Aim	LO.1 to LO.4 The aim of this activity is to give students the practical skills of using some forensics tools. For this activity, students will work on the AccessData FTK tool to analyze the contents of a disk drive.
Description	<p>In this activity, students will use Microsoft Word and Excel to create and delete files on a USB drive. After that, they will use the AccessData FTK forensics tool to analyze the drive. Students can download the FTK tool and other relevant tutorials following this link</p> <p>https://accessdata.com/products-services/forensic-toolkit-ftk</p> <p>Follow the following steps:</p> <ol style="list-style-type: none"> 1. Create a work folder on your USB drive → Create a new word document with some random text → Wipe the data → Save the file in the work folder → Exit Word. 2. Create a new Excel sheet with some random numbers → save it in the work folder → Exit Excel. 3. Delete both files from the USB drive. 4. Start AccessData FTK → enter the work folder name as the case path → Go to Add Evidence dialog box → Click the Add Evidence button → Click the Local Drive → Click Continue. 5. Make sure the USB and Logical Analysis are selected → Click Evidence Information dialog box → Select time zone → Click Finish. Now, the FTK processes the data on the USB. 6. Click the Deleted Files button → View file contents and explore what you have seen → Close all open windows and exit FTK.
Timeline	Understand the activity: 1hr. Implement the above steps: 1hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps.

Activity Template	
Number	5.2
Title	Use the SecureClean tool to remove all traces of data from the USB drive
Type	Reflection
Aim	LO.1 to LO.4 The aim of this activity is to give students the practical skills of using forensics tools for crime investigation purposes. For this activity, students will work on the AccessData FTK tool to analyze the contents of a disk drive.
Description	<p>Students will use the SecureClean tool to erase the USB drive that has some stored data. Students can refer to following link to install SecureClean tool and download other relevant material.</p> <p style="text-align: center;">www.whitecanyon.com/secureclean.php.</p> <p>To remove all traces of data from your USB drive using the SecureClean tool, follow the following steps:</p> <ol style="list-style-type: none"> 1. Create a new work folder on your USB drive. 2. Start SecureClean → White-Canyon → point to SecureClean 4 → Click Clean My Computer. 3. Go to Drive List section → Click to clear the check boxes → Click the check box corresponding to your USB drive → Click Deep Clean → Done. 4. Start AccessData FTK (Refer to the Activity 5.1) → Click the Add Evidence button → click the Local Drive option button → Click Continue. 5. Make sure the USB drive is selected → In the Evidence Information dialog box → Click to select time zone → Click OK → Click Finish. 6. Go to the Overview tab → Click the Unknown Type button → Click the F~S0001T~P file and note that it contains no data. 7. Click the Unknown Type button again. Explain what you have seen → Exit the FTK
Timeline	Understand the activity: 1hr. Implement the above steps: 1hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps.

Activity Template	
Number	5.3
Title	Use FTK and Hex Workshop tools to verify that a given USB drive contains evidence.
Type	Reflection
Aim	LO. 1 to LO.4 The aim of this activity is to give students the practical skills of using forensics tools to analyze a given data source to find crime evidence.
Description	<p>This activity was adopted from Ref [1]. In this activity, students will create a test drive by planting evidence in the file slack space on a USB drive or small disk partition. Then they will use FTK and Hex Workshop to verify that the drive contains evidence. Follow these steps:</p> <ol style="list-style-type: none"> 1. Format the USB Drive → Create a "Activity_5.3" folder on it → Create a new Word and type "Testing for string Namibia" → Save the file as "file1.doc". 2. Create a new Word document → Type "Testing for string XYZX" → Save the file as "file2.doc" → Exit. 3. Start Hex Workshop → Create a chart with two columns with Labels "Item" and "Sector". 4. In Hex Workshop → Open the USB drive → Open file1.doc → Scroll down until you see "Testing for string Namibia." 5. Click the tab corresponding to your USB or disk drive → Click at the beginning of the right column → Click Edit → Find "Text String" → Type "Namibia" → Click the Either option button → Click OK. 6. In the Item column, write file1.doc → In the Sector column, write the sector number as shown on the Hex Workshop title bar → Scroll to the bottom of the sector → Type Murder She Wrote near the end of the sector in the right pane → Click the Save toolbar button. 7. Click the file1.doc tab → Click Edit → Type Murder in the Value text box → Click OK → Click Edit → Click OK → Close the file. Write down the information you found 8. Open file2.doc → Go to "Testing for string XYZX" → Click the tab for your USB drive → Click at the beginning of the right column → Click Edit → Type XYZX → Click OK. On your chart, write file2.doc as the filename in the Item column, and in the Sector column. 9. In the tab for the USB drive, type I Spy near the end of the sector in the right pane, in the slack space → Save → Verify that "I Spy" doesn't appear as part of the file by clicking the file2.doc tab and searching for this string twice. Close the file2.doc file and exit Hex Workshop.
Timeline	Understand the activity: 1hr. Implement the above steps: 1hr.
Assessment	Each student's work will be evaluated based on the successful implementation of the above steps.

Activity Template	
Number	5.4
Title	Use Internet resources to search for popular forensics tools to make a comparative study among their main features.
Type	Research
Aim	LO.4 to LO.6 The aim of this activity is to teach students how to use online resources to research for popular forensics tools that are available for computing systems and compare their features.
Description	<p>In this activity, students will use Internet resources to gather information about the following 8 popular forensics tools available nowadays.</p> <ul style="list-style-type: none"> • The Sleuth Kit (+Autopsy) • AccessData FTK • Guidance Software EnCase • ProDiscover Forensic • Volatility Framework • CAINE • Xplico • X-Ways Forensics <p>Your main task is to create a comparative table among all of them. You can include as many comparative features as you can: This may include tool technical features, main strongest points, main weakness points, supported files formats, supported platforms, either commercial or open source, etc.</p>
Timeline	Search through the Internet: 2hr. Create the table: 2hr.
Assessment	The students will be divided into groups of three students at maximum. Each group is required to submit the summary report and present it in the class at an open discussion session.

Activity Template	
Number	5.5
Title	Write a procedure to verify a new forensics software package
Type	Research
Aim	LO.5 & LO.6 The aim of this activity is to teach students how to use online resources to search for popular forensics software verification procedures.
Description	Consider the following case: You work in the police department as a digital forensic expert. Two days ago, the police department purchased a new forensic software tool. To make sure it works very well, the department has assigned you the task of checking this tool to verify its operation. Your main task is to provide the department with a structured procedure on how to verify this newly purchased software package. Write a two-page report outlining the procedure you plan to use to check this tool.
Timeline	Search through the Internet: 2hr. Write a report: 2hr.
Assessment	The students will be divided into groups of three students at maximum. Each group is required to submit the summary report and present it in the class at an open discussion session.

Think Template (MCQs)	
Number	5.1
Title	Overview of Common Tools for Digital Forensics
Type	Fill in the Blanks
Question	<p>The five major tasks performed by most computer forensics tools, both hardware and software are:</p> <p>A. _____</p> <p>B. _____</p> <p>C. _____</p> <p>D. _____</p> <p>E. _____</p>
Answers	<p>A. Acquisition</p> <p>B. Validation</p> <p>C. Extraction</p> <p>D. Reconstruction</p> <p>E. Reporting</p>

Think Template (MCQs)	
Number	5.2
Title	Overview of Common Tools for Digital Forensics
Type	Choose the correct answer
Question	<p>One of the following forensics organization has created criteria for testing computer forensic tools</p> <ul style="list-style-type: none"> A. NIST B. SANS C. DFA D. HTCIA
Answers	Answer: (A)

Think Template (MCQs)	
Number	5.3
Title	Overview of Common Tools for Digital Forensics
Type	True or False
Question	The standards for testing forensics tools are based on ISO 17025. A. True B. False
Answers	Answer: (A)

Think Template (MCQs)	
Number	5.4
Title	Overview of Common Tools for Digital Forensics
Type	Fill in the blanks
Question	Forensic software tools are grouped into _____ and _____ applications.
Answers	Command Line (CL) and Graphical User Interface (GUI)

Think Template (MCQs)	
Number	5.5
Title	Overview of Common Tools for Digital Forensics
Type	Choose the correct answer
Question	When considering new forensics software, you should do which of the following? A. Uninstall other forensics software. B. Reinstall the OS. C. Test and validate the software. D. None of the above.
Answers	Answer: (C)

Think Template (MCQs)	
Number	5.6
Title	Overview of Common Tools for Digital Forensics
Type	True or False
Question	NIST testing procedures are valid only for government agencies. A. True B. False
Answers	Answer: (B)

Think Template (MCQs)	
Number	5.7
Title	Overview of Common Tools for Digital Forensics
Type	Choose the correct answer
Question	<p>When validating the results of a forensics analysis, you should do which of the following?</p> <ul style="list-style-type: none"> A. Calculate the hash value with two different tools. B. Use a different tool to compare the results of evidence you find. C. Repeat the steps used to obtain the digital evidence, using the same tool, and recalculate the hash value to verify the results. D. Do both A and B. E. Do both B and C. F. Do both A and C. G. Do none of the above.
Answers	Answer: (D)

Extra Template	
Number	5.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	5.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

6. Network Forensics Artefacts

Scope Template															
Number	6														
Title	Network Forensics Artefacts														
Introduction	The main objectives of this Chapter are to <i>(i)</i> introduce students to network forensics procedures that protect network's resources and information; <i>(ii)</i> To provide students with some information about virtualization and virtual machine components; and <i>(iii)</i> introduce the use of live acquisitions to capture an image while a machine is running, which is necessary in many situations.														
Outcomes	LO.1: Discuss the standard procedures being used for conducting virtual machines forensic analysis LO.2: Overview of the current network intrusions and unauthorized access problems. LO.3: Explain the standard procedures being used in network forensics and network-monitoring tools LO.4: Explain the live acquisition process														
Topics	6.1 Network Forensics Overview 6.2 The TCP/IP Reference Model 6.3 Virtual Machine Acquisition 6.4 Live Acquisition Process 6.5 Chapter's Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>1 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>5 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>1 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>8 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>3 hr</td> </tr> <tr> <td>Total</td> <td>18 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> Ch. 12, Guide to Computer Forensics and Investigations (5th Edition). By B. Nelson, A. Phillips, C. Steuart, 2016. Ch. 8, A Practical Guide to Computer Forensics Investigations (1st Edition). By Darren R. Hayes, 2014. 	Task	Time	Preparation (Introduction and On-line Planning):	1 hr	Textbook Content:	5 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	8 hr	Related Course Work:	3 hr	Total	18 hours
Task	Time														
Preparation (Introduction and On-line Planning):	1 hr														
Textbook Content:	5 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	8 hr														
Related Course Work:	3 hr														
Total	18 hours														

Content Template	
Section Number	6.1
Section Title	Networks Forensics Overview
Introduction	In this section, we talk about network forensics. We mainly focus on shedding light on the importance of network traffic and its contents to defend against network attacks and help in easy management of the system as well
Content	<p>With the recent increase in network attacks, viruses, trojans, and social media attacks, digital forensics examiners should know how to deal with crime scenarios which use computer networks. Here, we define the network forensics process as a procedure of collecting, processing and analyzing raw network traffic to help in tracking ongoing attacks and suggesting mitigation plans. The collected information can be useful in analyzing system status to help in determining how attackers are getting into the system and what type of data was copied, modified, or deleted. To do that, well defined procedures should be clearly stated for data acquisition before, during or after the occurrence of the attack. The followed procedures must be based on two things (1) the network infrastructure and design, and (2) the organization's requirements and functions.</p> <p>In this regard, digital investigators should review the reports presented by the NIST organization to get more information about how to integrate forensic techniques into the network incident resolution process. In general, several tasks must be applied to protect networked systems from any security breach. This include:</p> <ul style="list-style-type: none"> • Updating all system software, all security patches and antivirus software • Applying physical and personal security measures. • Making sure all company's employees are well trained and aware of the current security trends. • Choosing proper security equipment such as Intrusion Prevention Systems (IPSS) and firewalls. • Applying various penetration tests regularly and couple them with the implemented risk management plan. • Ensuring fast mitigation of any system attack that occurs. • Being aware of all assessment and monitoring procedures for disaster recovery plans. <p>Network Forensics: Standard Procedure</p> <p>In addition to the above points, the standard procedure that is normally used for computer network forensics contains the following guidelines:</p> <ol style="list-style-type: none"> 1. Install an official image of the OS on the network with all standard applications. 2. Check the vulnerability issues on your system frequently to mitigate the attack quickly or prevent other attacks from taking place on the network. 3. Make a forensic image of the compromised system. 4. Make a forensic image of the compromised drive and store it securely.

5. Make a consistency check to ensure that the forensic image is a copy of the original installation image. Of course, this can be done by comparing hash values of common files.

Following the above steps, investigators can keep working with the image copy to find the deleted or hidden files and partitions. They may also have to restore the drive to easily work with some types of viruses and malware that an attacker has installed on the system. As an example, consider the situation where attackers might have intentionally sent a Trojan horse script that allows them to login to systems and steal some sensitive files. After that, they can use a rootkit software to perform reconnaissance tasks on the network with the purpose of collecting system's vulnerabilities that will help them to attack the system again.

Network Log Files

A computer network is a collection of network servers, routers, firewalls, and other network devices which are connected together using some transmission media. Through the daily operation of the network these devices generate hundreds or even thousands of alerts or notifications that are stored in log files located in several places across the network. These alerts contain technical information that can be used for digital forensics analysis since they record traffic going in or out of the network.

Several methods can be used to explore log files and interpret their information. One such method is running the tcpdump program on Linux system. Figure 1 shows a sample of a record taken from the Linux syslog files. It shows the main fields and their meanings.

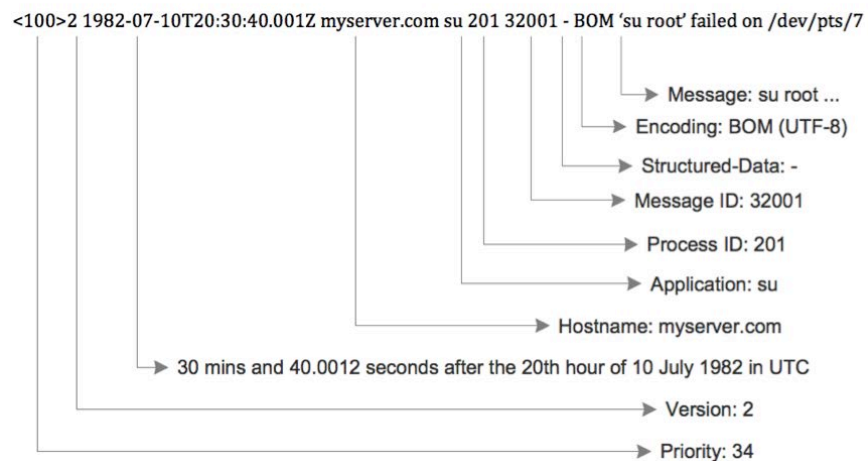


Fig. 1: Attributes of a sample record obtained from Linux syslog files.

It's worth noting that the format of a logfile may differ from system to system and application to application. Thus, when working with a specific application or system, it is highly recommended to refer to the vendor's Website to get more information about the structure of the logfile it generates. Event correlation methods such as filtering, aggregation, and clustering can be applied to preprocess, analyze, merge data obtained from several logfiles to extract useful patterns.

Network Management Tools

Network administrators normally use several management tools, either open source or commercial, to manage, administrate and monitor the network.

Examples of such tools are RegMon, FileMon, and PsTools. Some of these are software kits that contain a group of tools for doing several tasks. For example, network administrator can explore contents of the PsTools files to check whether an employee accessed a file without authorization.

Also, and as a daily operational task, network administrators use packet sniffing tools (such as Wireshark, www.wireshark.org) to monitor and analyze packets which are transmitted and received through the network. Some analyzers apply certain sniffing mechanisms to capture packets, some others have built-in mechanisms to analyze the captured data.

There are a large number of packets sniffing tools. Most of them can use the Pcap (packet capture) generic format, such as tcpdump and Wireshark. Pcap has two other versions: Libpcap (for Linux) and Winpcap (for Windows). Therefore, to achieve the purpose of the investigations, investigators must choose the appropriate tool. For example, consider the case of handling the TCP SYN flooding attack. Here, attackers keep sending TCP requests asking for the server to establish a new fake TCP connection. The aim of attackers is to overload the server by sending many fake TCP connection requests rapidly to overload the sever and then stop the service. Although the server can manage huge number of requests, it can deal with only a dedicated number of established connections due to its limited resources. To mitigate this attack, investigators must be interested in those packets having the SYN flag set to 1 as response to a connection request process. To find these packets, investigators can use several specialized packet sniffers such as tcpdump and tethereal (a network protocol analyzer) having built-in mechanisms to explore the TCP header to locate those packets having SYN flag set.

Tcpslice is a well-known network sniffing tool that is mainly used to extract information from large Libpcap files. Tcpreplay suite can be also used to analyze Libpcap format files. Tcpslice is another tool that can be used to generate Libpcap statistics link average and maximum transfer rates, number of packets transmitted and received in a given period of time, etc.

Distributed Denial-of-Service (DDoS) Attacks

One of the major computer network attacks is the Distributed Denial-of-Service (DDoS) attacks. In these threats, attackers exploit the network infrastructure and its connected devices to perform their illegal operations. Thousands of users' machines might be in use during the attack, they are referred to as zombies since they unintentionally become part of the attack. A DDoS attack may go beyond the scope of one network; i.e., attackers from different locations may collaboratively work to achieve their purposes.

The HoneyNet project (<https://www.honeynet.org>) was mainly established to help network professionals tackle a DDoS attack. It is implemented by distributing many installed honeypots and honeywalls in different locations worldwide. A honeypot is a computer with some vulnerabilities intentionally setup to trick attackers (like a trap) to gain access to the network, but it contains dummy information. This project was mainly developed to make information widely available worldwide. Its main objectives are awareness, information, and tools.

Another major attack is the zero-day attacks. Here, attackers exploit new or newly discovered system vulnerabilities before software vendors discover them and patches will be available. Penetration tests can be applied here to

	discover unseen vulnerabilities to predict the next steps of the ongoing attack.
--	--

Content Template	
Section Number	6.2
Section Title	The TCP/IP Reference Model
Introduction	To understand packets sniffing tools, students should first review the TCP/IP reference model, its layers, and its well-known protocols. Thus, in this section we review the two common networking architectures: the ISO/OSI and the TCP/IP reference models with more focus on the TCP/IP protocol suite as it is the Internet model.
Content	<p>Network architecture is built using one of following two main reference models: The International Standards Organization / Open Systems Interconnection (ISO/OSI) and Transmission Control Protocol/ Internet Protocol (TCP/IP) reference model. The design of these reference models follows the hierarchical structure in such a way that each layer provides services to the layer above it, and requests services from the layer below it in the hierarchy. Figure 2 shows the number and name of layers of each model. Both have link, network, transport, and application layers, but they differ on the other layers.</p> <div style="text-align: center;"> </div> <p>Fig. 2: The difference between the ISO/OSI and the TCP/IP model</p> <p>The OSI model was mainly proposed to establish standard data communication model that promotes multi-vendor interoperability and extensibility. It has seven layers, each with a set of a built-in functions, protocols, and implementation guidelines for interfaces between layers. Although the protocols associated with the OSI model are now obsolete, the model itself is actually still valid for educational purposes. Unlike, the OSI model, the TCP/IP model has four layers with the majority of its well-know protocols located in the upper three layers. The model itself is not of much use but the protocols are widely used. Therefore, in the next discussion we will look at the TCP/IP model and its implemented protocols.</p>

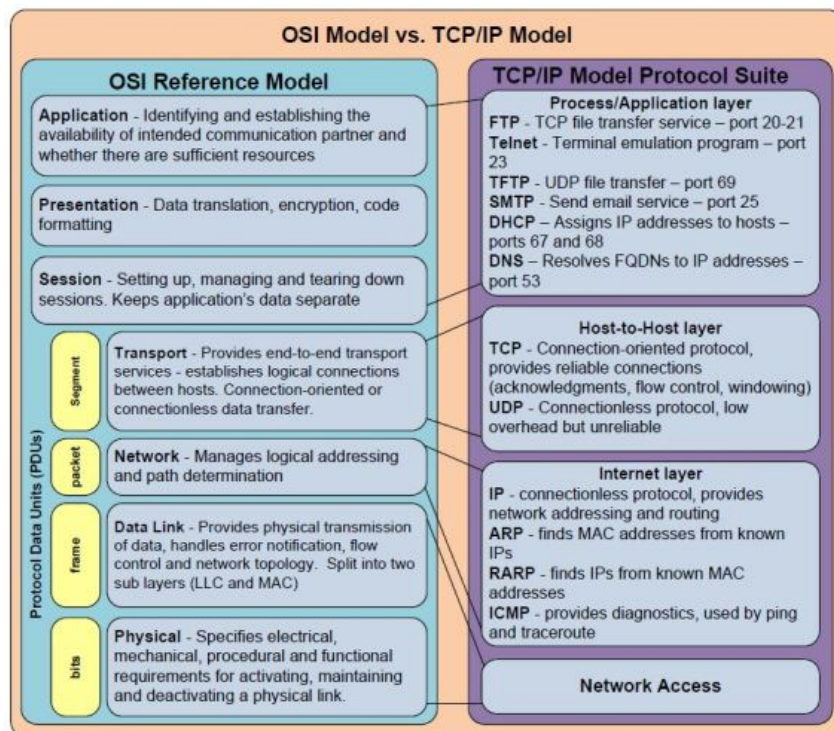


Fig. 3: The TCP/IP protocol suite

Figure 3 shows the TCP/IP protocol suite that shapes the Internet and its common services. IP-based networks have a variety of protocols that provide the different network services. Below is the list of common TCP/IP protocols with their use:

- ✓ FTP (File Transfer Protocol- TCP Ports # 20 & 21): It is TCP protocol used ports 20, 21 to transfer files between to end user devices across the Internet.
- ✓ HTTP (HyperText Transfer Protocol -TCP Port # 80): Its the main protocol used for the Web services; i.e., it allows the Web clients and Web servers to exchange Web resources.
- ✓ SMTP (Simple Mail Transfer Protocol -TCP Port # 25): This protocol is used for email service, i.e., for sending emails between mailing servers.
- ✓ DNS (Domain Name Service - UDP Port # 53): It resolves domain names to their corresponding IP addresses.
- ✓ SSH (Secure Shell – TCP Port # 22): It is a terminal emulation program that allows a secure remote access to servers and other network devices over the Internet.
- ✓ TCP (Transmission Control Protocol): It is a reliable transport layer protocol that manages the connection between any two processes to exchange streams of data.
- ✓ UDP (User Datagram Protocol): It is an unreliable transport layer protocol that manages sending and receiving datagrams over an IP network.
- ✓ IP (Internet Protocol): It is the core protocol of the network layer that specifies format of packets and manages the IP addressing schemes.

- ✓ ARP (Address Resolution Protocol): It's a data link layer protocol that is used convert an logical address (IP address) to a physical address (MAC address).

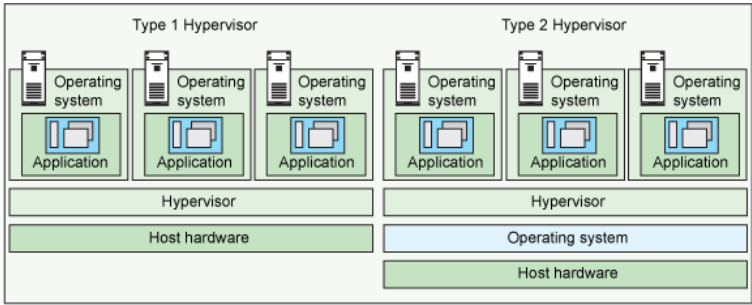
It's worth noting that various packet analyzing tools work at layers 2 or 3 of the TCP/IP model, i.e., they analyze network packets (layer 3 PDU) or network frames (layer 2 PDU). Next, we give some technical details about each layer of the TCP/IP reference model.

- ✓ **The Link Layer:** It is the lowest layer of the model which represents the interface between hosts and transmission media. It has several functions such as determining physical , electrical, and timing properties of signals, encoding/decoding, multiplexing/demultiplexing.
- ✓ **The Internet Layer:** The Internet layer has three big functions: Packet formatting, packet routing, and managing IP addressing scheme.
- ✓ **The Transport Layer:** The main function of this layer to manage the connection between two processes on the source and destination hosts to send and receive data. TCP and UDP are the main protocols belonging to this layer. Figure 4 summarizes the main difference between the them.
- ✓ **The Application Layer:** It is all about network application and services. It defines all the application layer protocols that manage users' applications and services. It is the layer just above the transport layer. The application layer can use either the TCP protocol or the UDP protocol.

Table 1 summarizes the main differences between the TCP and UDP transport layer protocols.

TCP	UDP
Reliable	Unreliable, cepat, dan Low Overhead
Connection-oriented	Connectionless
Acknowledgement	Tanpa Acknowledgement
Mengirim ulang data yang hilang	Tidak ada pengiriman ulang
Sequencing.	Tidak ada sequencing, data diberikan ke layer atas sesuai dengan datangnya data.
PDU disebut Segment	PDU disebut Datagram
Overhead 20 bytes	Overhead 8 bytes.
Web, email, file transfer	Video streaming, VoIP

Table 1: The main differences between the TCP and UDP protocols.

Content Template	
Section Number	6.3
Section Title	Virtual Machine Acquisition
Introduction	This topic talks about the standard procedures of virtual machine forensics analysis and types of hypervisors. It also explains how to work with virtual machines installed on a different system.
Content	<p>Digital forensics investigators must know how to work with virtual machines since they are now a standard part of any IT business company. This importance comes from the fact that since computer hardware/software need large budgets to meet the service needs, companies have to pay more attention to making the best investments for IT infrastructures. Virtual machines enable a well-equipped server to support a small to medium company's needs.</p> <p>Virtual machines are run and managed by a software tool called a Hypervisor. Generally speaking, two types of hypervisor exist: Type 1 and Type 2. Figure 5 shows the main system architecture for both types. In brief, as the figure shows, a type 1 hypervisor interacts directly with the hardware part and mainly loads on physical hardware and doesn't require a separate software OS part. While, a type 2 hypervisor needs an existing OS (such as Windows, Linux) to run.</p>  <p>Fig 5: Type 1 and Type 2 hypervisor system architecture.</p> <p>Furthermore, Type 1 hypervisors are typically loaded on servers with a lot of hardware resources. Whereas Type 2 hypervisors can be used on a normal workstation, or laptop such as running a Windows Server VM on a Linux host. VMs can maintained on a separate network if hardware replacement costs are beyond a company's budget. Table 2 summarizes the performance differences between both types.</p> <p>Technically, installing a type 2 hypervisor on a workstation requires some modifications to the system's BIOS to improve system security and performance. Therefore, CPU vendors such as Intel produced the Virtualization Technology (VT) concepts in some of its CPU Hardware designs.</p>

Feature	Type 1	Type 2
Definition	Hypervisors run directly on the system hardware.	Hypervisors run on a host operating system.
Support	Hardware virtualization.	Operating system virtualization.
Examples	VMware ESXi and Citrix XEN Server.	KVM, Virtual Box, VMware Server and Microsoft Virtual PC.
Efficiency, Availability and Security	Comparatively better than Type 2.	Though inferior, it is used mainly on systems where support for a broad range of I/O devices is important.
Performance	Very high. Resources are not being consumed by a bloated parent operating system.	Steep resource-overhead penalties reduce performance.

Table 2: Hypervisor Type 1 and Type 2 main performance differences.

Virtual Machines Investigation

Detecting whether a virtual machine is on a suspect machine can be challenging for digital forensics investigators. However, the investigative process itself has some similarities with the standard investigative process used on a normal system. Basically, to analyze VM crime scenarios, investigators should first acquire a forensic image of the suspect machine, and system notifications, alerts, or logfiles. They can correlate all of this information and track the virtual machines activities by using the VM's IP address and other systems ID and network protocols. After that they can export and examine the necessary files and information associated with VMs, such as log files, to analyze the crime scene. To get these files, for Windows machines, investigators usually look in the Users or Documents folder, on a Linux system this information can be found in /usr/bin/software-center.

In summary, a digital investigator who is analyzing a forensic scene of VMs can follow the following standard procedure.

- Acquire an image from the host machine.
- Track VM all activities using network information and IP addressing.
- Export all VM associated logfiles, virtual adapters, etc.
- Record the hash values of these associated files.
- Mount the VM as a drive to analyse it.

Content Template	
Section Number	6.4
Section Title	Methods of Acquisition
Introduction	This section gives an overview of the two methods of data acquisition: offline (or dead) and online (or live). We review the advantages and disadvantages of both techniques. We then cover live acquisition as it is the more standard approach.
Content	<p>As previously mentioned in Chapter 3, in most digital forensic examinations, investigators need to work with an exact copy of the original data located on the evidence hard disk. Two types of methods can be followed for creating that image. They are: (i) Live acquisition, and (ii) Offline acquisition. Investigators should use the most appropriate method for a given situation. Indeed, in some circumstances it may make sense to use both. With the help of specialized forensics tools, investigators can extract volatile data from the suspect machine before shutting it down. Offline acquisition is discussed in more detail in Chapter 3. Thus, in the following we give more focus on the second method, live acquisition.</p> <p>Live Acquisition</p> <p>A live acquisition extracts from a system without shutting it down. One of the main challenges that faces investigators when using live acquisition is the Order of Volatility (OOV). This metric specifies the lifetime of information on a computer system. The contents of the RAM might exist for only a short period of time. Other data might last long time, such as files stored on the HDD.</p> <p>When working with live computing systems, investigators should be aware of several issues that might arise. For example, switching the computing system off may cause loss of volatile data stored in primary memory (RAM) such as running processes, network connections and mounted file systems. Thus, these methods are typically beneficial when dealing with active network attacks or intrusions. This way, live acquisition can be set-up before taking a system offline because network attacks might be easily traced only in active processes or memory, for example, some malware might disappear when a system is rebooted.</p> <p>A common way to live digital forensic involves setting up an acquisition software tool into read only mode. Then, using both the tool and writable media to start online acquisition. However, the live acquisition does not apply the same steps as the typical forensic procedure. This is due to the fact that after doing a live acquisition, information might be changed and the taken actions might also change or damage the RAM contents and active processes. In this case, the information can not be regenerated.</p> <p>The General procedure for a live acquisition</p> <p>Like the offline acquisition, implementing a live acquisition requires from investigator to follow a standard procedure that can be summarized as follows:</p> <ol style="list-style-type: none"> 1) Use a bootable forensic media such as DVD or USB drive. Insert the media into the suspect's machine. If the machine is not on the local network, it can be accessed remotely with the help of network forensics tools.

- | | |
|--|---|
| | <ol style="list-style-type: none">2) Make sure to store all activities and actions to logfiles. A network drive is an ideal place that can be used for this purpose.3) Next, copy the contents of the primary memory (RAM) using one of the digital forensic tools such as WindowsScope OSForensics, FTK Imager.4) Make sure to check system healthy status to see whether a rootkit exists. This is also can be done by using special tools such as RootKit Revealer.5) Make sure to check the consistency of every recovered file during the live acquisition by getting a digital hash value. |
|--|---|

Many other tools are available for doing live acquisition, such as Mandiant Memoryze which contains several functions such as listing all network sockets, listing hidden sockets managed by rootkits software, etc., Kali Linux contains password crackers, network sniffers, and freeware forensics tools, and Sleuth Kit tool covers several hundreds of available command-line tools.

Content Template	
Section Number	6.5
Section Title	Chapter's Summary
Introduction	In this section, we summarize the chapter by listing the main key points.
Content	<p>In Section 1, we defined network forensics as a process of collecting and analyzing raw network data which enables network administrators to determine how an attackers gained access to a network's resources and information, we discussed the network forensics procedures and how network generated traffic can be useful for defending against known network attacks, and for other management issues such as performance improvement and management. Section 2 provided an overview of the two common network standards: the ISO/OSI and the TCP/IP reference models with more focus on the TCP/IP model.</p> <p>In Section 3, we briefly explained the Virtual Machine (VM) concept and stated why it is extensively used in current organizations. Therefore, investigators must consider file extensions that indicate the existence of VMs. Also, we looked at the two types of hypervisor for running virtual machines. Type 1 hypervisors contain their own OSs and are loaded directly on physical hardware, whereas, Type 2 hypervisors are applications installed on top of an OS.</p> <p>Section 4 discussed the two Live acquisitions methods: online and off-line, and explained the need to retain volatile contents that are stored in RAM or generated by active processes. Investigators must be concerned with the order of volatility (OOV), which determines how long a piece of information lasts on a system.</p> <p>The next topic will talk about mobile device forensic procedures. It mainly covers the general guidelines being implemented being implemented to acquire information from smartphones or other mobile devices.</p>

Activity Template (Reference Book[1], Hands-On Project 10-1, Page 419)	
Number	6.1
Title	Mount a VM as a drive in the OSForensics tool
Type	Reflection
Aim	LO.1 In this activity, you learn how to mount a VM as a drive in OSForensics
Description	<p>In this project, you mount a VM as a drive in OSForensics. First, you need to create Ubuntuportable VM. The VM will be assigned the next available drive letter on your system in read-only mode. To complete this activity, follow the fooling steps:</p> <ol style="list-style-type: none"> 1. Start the OSForensics. In the left pane, scroll down and click Mount Drive Image to open the PassMark OSFMount utility. 2. In the lower-left corner, click Mount new to open the OSFMount – Mount drive window. 3. Make sure Image file is selected and click the ... button. Scroll to the location of VMware VMs and double-click the Ubuntu-portable.vmdk file. 4. In the "Select a partition in image" window, accept the default option, use entire image file and click OK. 5. Accept the defaults and click OK. This process should take only a few minutes. The .vmdk file should be displayed as a mounted drive. 6. Double-click the drive to display its contents and take a screenshot. Make a note of the new drive letter and click Exit. 7. In the left pane, scroll up and click the Manage Case button. In the right pane click any current case, and then click the Add Device button. 8. In the "Select device to add" dialog box, click the Drive Letter list arrow. The drive letter you noted in Step 5 is listed, and you can add it to a case when you're doing a standard static analysis. Click Cancel. 9. Write a short report of your results and include the screenshots you took.
Timeline	Implement activity: 1 hr.
Assessment	Each student is evaluated based on his/her implementation of the above steps.

Activity Template (Reference Book[1], Hands-On Project 10-5, Page 421)	
Number	6.2
Title	Explore the SANS SIFT tools
Type	Reflection
Aim	LO. 2 & LO. 3 In this activity, you will learn how to explore the SANS SIFT tools.
Description	<p>In this activity, you will explore the SANS SIFT tools.</p> <ol style="list-style-type: none"> 1. Start Portable-VirtualBox, and start the SANS SIFT VM. 2. Open sift-cheatsheet.pdf. It gives instructions on how to mount drives and examine files and has resources for sample images. Take a screen capture of the VM with this file open. 3. Open memory-forensics-cheatsheet.pdf. One of the resources it lists is the volatility tool. Start a Web browser, go to https://code.google.com/p/volatility/wiki/SampleMemoryImages, and write down the resources this tool offers. 4. On the left, scroll down and click DFF (Digital Forensics Framework). Click the second icon from the left to add a local device. Click the VBOX Hard drive device and click OK. If anything had been loaded on the USB drive, this tool would enable you to search for terms and examine the contents. Click File, Exit from the menu. 5. Wireshark is another tool available in the SIFT toolkit. Click the Wireshark icon on the left. In the Capture Help section, click the How to Capture link. 6. Step-by-step instructions open in Firefox. Make note of the warnings, such as making sure you have permission before doing packet captures. Exit Firefox. Write a one to two-page paper summarizing the information in the two cheat sheets you examined and listing warnings for using Wireshark.
Timeline	Implement activity: 2 hr.
Assessment	Each student is evaluated based on his/her implementation of the above steps and his/her submitted paper.

Activity Template (Reference Book[1], Case Project 10-4, Page 422)	
Number	6.3
Title	Use Internet search engines to research for current acquisition tools
Type	Search
Aim	LO.1, LO. 2 & LO. 3 In this activity, you will use Internet search engines and the vendors listed in this topic to collect information about current data acquisitions tools.
Description	Go to http://docs.kali.org/installation/kali-linux-live-usb-install and follow the instructions for installing Kali Linux on a USB drive. Try at least three of the tools it includes and take screenshots of the tools you selected. Write a one- to two-page paper summarizing each tool's functions.
Timeline	Search through the Internet: 1 hr. Prepare report : 2 hr.
Assessment	The student's work will be evaluated based on the written report and its alignment with the case study problem.

Activity Template (Reference Book[1], Hands on Projects 12-1 & 12-2, Page 477)	
Number	6.4
Title	Explore SIMcon mobile forensics software tool
Type	Reflection
Aim	LO. 4 & LO. 5 In this activity, you learn how to explore the SIMcon mobile forensics software tool that can generate information for mobile device investigations
Description	<p>In this case, Sebastian and Nau are suspected of drug dealing, and their phones were seized with the other digital evidence. One of your colleagues has a licensed version of SIMcon. You were able to go to her forensics lab and examine the SIM cards of both phones. In this project, you examine the exported Excel files. To do this activity, follow the following steps.</p> <ol style="list-style-type: none"> 1. Start Excel, and open the Messages_Sebastian's_phone.xls and Messages_Nau's_phone.xls files. 2. If the messages aren't currently in chronological order, change the display to sort them in this order. 3. Establish the timeline for what transpired between these two employees. Note items such as when they respond to each other's messages, dates and times, and what numbers they call. 4. Write a short report summarizing the data you examined and stating any conclusions you can draw from the SMS messages. 5. Start Notepad, and open Report_Nau's_phone.txt. Start a second instance of Notepad, and open Report_Sebastian's_phone.txt. 6. As you examine the reports, find definitions for the following items: International: Mobile Subscriber Identity (IMSI), PLMN selector, HPLMN search period, and Cell Broadcast Message Identifier (CBMI). Note any other items of interest. 7. Explain what "SIM Phase: phase 2 - profile download required" means. 8. You notice "Originating Address (TP-OA): 264813358947" in the report for Nau's phone. The number breaks down into 264-81-3358947. Explain what the first two numbers—264 and 81—designate. 9. Explain what the following originating addresses mean: Originating Address (TP-OA): 123 Originating Address (TP-OA): 131 10. Next, compare the two files and write a report with answers to the preceding questions and include any conclusions you drew about the messages' contents.
Timeline	Implement activity: 2 hr.
Assessment	Each student is evaluated based on his/her implementation of the above steps and his/her submitted paper.

Activity Template (Reference Book[1], Hands on Projects 12-4, Page 478)	
Number	6.5
Title	Use Oxygen Forensics to examine a BlackBerry device
Type	Reflection
Aim	LO. 4 & LO. 5 In this activity, you will learn how to you use Oxygen Forensics to examine a BlackBerry Mobile device.
Description	<p>In this activity, you use Oxygen Forensics to examine a BlackBerry device. If you haven't already done so, go to www.oxygen-forensic.com and request a registration code for downloading the demo version of Oxygen Forensics. (Keep in mind that getting the registration code might take a few days, and plan accordingly.) When you get it, download and install the software. To do this activity, follow the following steps.</p> <ol style="list-style-type: none"> 1. Start a Web browser, if necessary, and go to www.oxygen-forensic.com/en/download/devicebackups. Download the Blackberry 9520 file to your work folder. Unzip the file, which is Greg Bramson's BlackBerry 9520.ofb. 2. Start Oxygen Forensic Suite 2014 and click the Import backup file list arrow. 3. Click Import OFB backup. Navigate to your work folder, click the Greg Bramson's BlackBerry 9520.ofb file, and click Open. 4. In the Oxygen Forensic Extractor v. 5.1.303 dialog box that opens, click Extract. When the extraction is complete, click Finish. 5. When the file opens, click Brooklyn maniac, expand the tree structure, and then click Greg Bramson's BlackBerry 9520.ofb. 6. Notice at the lower right that the listing varies from what you saw for Patrick Payge's Galaxy Mini in the in-chapter activity. The Device Information and File Browser entries are the same, but this BlackBerry device has an entry called Phone Call Logs instead of an Event Log. Click the Device Information icon to see the owner, number, and service provider. 7. Return to the main window by clicking the back arrow at the upper left, and then click the File Browser icon. Click the Geo files tab (scrolling to the right to find it, if necessary), and examine the files listed. What can they tell you about the owner? 8. Click the Images tab and scroll down until you get to the .jpg files. What types of pictures are stored? What can they tell you? 9. Return to the main window and click Messages at the lower right. Examine the messages listed. Combined with the other files and pictures, what sort of timeline can you construct for the owner? 10. Exit the program. Write a two- to three-page paper with your findings.
Timeline	Implement activity: 2 hr.
Assessment	Each student is evaluated based on his/her implementation of the above steps.

Activity Template (Reference Book[1], Case Project 12-1, Page 479)	
Number	6.6
Title	Use Internet search engines to research for current mobile device forensics tools
Type	Search
Aim	LO.4 & LO. 5 In this activity, you will use Internet search engines and the NIST Mobile Device Forensics Guidelines to classify mobile device forensics tools.
Description	Download the most current version of the NIST Mobile Device Forensics Guidelines at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf . Page 17 lists classifications of mobile device tools. For the tools covered in this chapter, determine what type each one is based on these NIST guidelines. Write a one- to two-page paper explaining the uses and limitations of each tool.
Timeline	Search through the Internet: 1 hr. Prepare report : 2 hr.
Assessment	The student's work will be evaluated based on the written report and its alignment with the case study problem.

Think Template (MCQs)	
Number	6.1
Title	Network Forensic Artefacts
Type	Choose the correct answer
Question	<p>You can expect to find a type 2 hypervisor on what type of device? (Choose all that apply.)</p> <p>(A) Desktop (B) Smartphone (C) Tablet (D) Network server</p>
Answers	(A), (B) & (C)

Think Template (MCQs)	
Number	6.2
Title	Network Forensic Artefacts
Type	True or False
Question	Tcpslice can be used to retrieve specific timeframes of packet captures. (A) True (B) False
Answers	(A)

Think Template (MCQs)	
Number	6.3
Title	Network Forensic Artefacts
Type	Fill in the blanks
Question	To find network adapters, you use the command _____in Windows and the command _____in Linux.
Answers	ipconfig , ifconfig

Think Template (MCQs)	
Number	6.4
Title	Network Forensic Artefacts
Type	Choose correct answer
Question	<p>When do zero-day attacks occur? (Choose all that apply.)</p> <p>(A) On the day the application or OS is released (B) Before a patch is available (C) Before the vendor is aware of the vulnerability (D) On the day a patch is created</p>
Answers	(B) & (C)

Think Template (MCQs)	
Number	6.5
Title	Network Forensic Artefacts
Type	Choose the correct answer
Question	In VirtualBox, which file contains settings for virtual hard drives? (A) .vbox-prev (B) .ovf (C) .log (D) .vbox
Answers	(D)

Think Template (MCQs)	
Number	6.6
Title	Network Forensic Artefacts
Type	Choose correct answer
Question	Packet analyzers examine what layers of the OSI model? (A) Layers 2 and 4 (B) Layers 4 through 7 (C) Layers 2 and 3 (D) All layers
Answers	(C)

Extra Template	
Number	6.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	6.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

7. Mobile Device Forensics

Scope Template															
Number	7														
Title	Mobile Device Forensics														
Introduction	The scope of this topic is to introduce students to mobile device forensic procedures, and how to retrieve information from a cell phone, smartphone, or other mobile device, as well as gets hands on practice on some of the mobile forensic tools.														
Outcomes	LO.1: Identify the basic concepts of mobile device forensics analysis. LO.2: Explain the standard procedures to acquire data from smartphones. LO.3: Analyze smartphone operating systems. LO.4: Apply forensics tools to retrieve evidence from a smartphone. LO.5: Conduct SIM card forensics.														
Topics	7.1 Understanding Mobile Forensics 7.2 Mobile Device Operating Systems 7.3 Acquisition Procedures for Mobile Devices 7.4 Chapter Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>2 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>6 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>1 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>7 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>4 hr</td> </tr> <tr> <td>Total</td> <td>20 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> Ch. 12, Guide to Computer Forensics and Investigations (5th Edition). By B. Nelson, A. Phillips, C. Steuart, 2016. Ch. 9, A Practical Guide to Computer Forensics Investigations 1st Edition). By Darren R. Hayes, 2014. 	Task	Time	Preparation (Introduction and On-line Planning):	2 hr	Textbook Content:	6 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	7 hr	Related Course Work:	4 hr	Total	20 hours
Task	Time														
Preparation (Introduction and On-line Planning):	2 hr														
Textbook Content:	6 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	7 hr														
Related Course Work:	4 hr														
Total	20 hours														

Content Template	
Section Number	7.1
Section Title	Understanding Mobile Device Forensics
Introduction	This section references mobile device forensics. It mainly focuses on how to retrieve information from a cell phone, or another mobile device
Content	<p>Smart phone technology has developed far beyond what its inventors could have imagined. Now, mobile devices have become one of the main parts of our daily routine. People may store large amounts of information on phones and users spend a lot of their time interacting with them. They can be easily used to navigate the Internet, store images, video, log into bank accounts, make deposits, using a wealth of information both personal and business. Thus, smart phones contain sensitive information that must be kept protected all the time. Most mobile models store the following user and application information:</p> <ul style="list-style-type: none"> ✓ Incoming, outgoing, and missed calls ✓ Multimedia and Short Message Service (MMS & SMS) ✓ E-mail and Web services ✓ Instant messaging (IM) ✓ Pictures, videos, and music files ✓ Calendars and address books ✓ GPS data ✓ Voice recordings and voicemail <p>Despite the usefulness of mobile devices in providing key guidelines for investigations, Mobile investigation is one of the main challenging tasks in digital forensics due to several factors, such as there are no design standards among mobile device vendors, and new brands are not always compatible with previous models. Thus, all existing cables, accessories, software being used for mobile forensics acquisitions can become obsolete quickly.</p> <p>Mobile Phone Basics</p> <p>Mobile communication systems have evolved from the first generation (1G) to the current fifth generation (5G) and are evolving towards the sixth generation (6G). Mobile standards have advanced approximately at the pace of one generation every five years since the 2G. Fig. 5 depicts the evolution of these standards with the main features.</p> <p>The diagram illustrates the evolution of cellular mobile standards from 2G to 5G. It shows a flowchart of standards and a list of key features for each generation.</p> <p>2G</p> <ul style="list-style-type: none"> • Mainly circuit switched, with packet-switching introduced since GPRS • Based on TDMA (and CDMA for CDMA One) <p>3G</p> <ul style="list-style-type: none"> • Circuit and Packet-switched • (Primarily) based on wideband CDMA <p>4G</p> <ul style="list-style-type: none"> • All IP flat architecture with evolved packet core. • Based on OFDM and MIMO • Cooperative processing <p>5G</p> <ul style="list-style-type: none"> • Based on massive MIMO, Small Cell and centralized processing techniques • Integrated wire and wireless full IP networks <p>The flowchart shows the following standards and their relationships:</p> <ul style="list-style-type: none"> 2G: GSM, IS-136, CDMA One (IS-95), GPRS, EDGE 3G: W-CDMA, HSPA 4G: LTE, TD-SCDMA 5G: LTE Advanced, 5G <p>Additional standards shown include CDMA-2000 (by 3GPP2) and Wi-MaX.</p>
	<p>Fig. 5: Evolution of Cellular Mobile Standard from 2G to 5G.</p> <p>The first three generations became obsolete with the appearance of the 4th generation in 2008 when the International Telecommunication Union Radio</p>

(ITU-R) created the necessary requirements for mobile carriers to be considered as 4G. Nowadays, 4G networks can use the following communication technologies:

- ❖ Orthogonal Frequency Division Multiplexing (OFDM)
- ❖ Mobile WiMAX (IEEE 802.16)
- ❖ Ultra-Mobile Broadband (UMB)
- ❖ Multiple Input Multiple Output (MIMO)
- ❖ Long Term Evolution (LTE)

Although mobile carriers use different communications technologies, they share some basic principles in their basic operation. There are three main components that can be used inside a mobile carrier network. They are:

1. Base Transceiver Station (BTS): It defines carrier cells and communicates with mobile phones through radio signals.
2. Base Station Controller (BSC): It's a device with hardware and software components that manages carrier BTS signals, and handles the communication to the Mobile Switching Center (MSC).
3. Mobile Switching Center (MSC): This component plays an important rule in assigning connectivity between customer's calls. It performs this task with the help of a central database that contains customer account and location data, and other key information needed during an investigation.

Inside Mobile Devices

Almost all mobile phones have some basic hardware and software components. Among the software components are a proprietary OS (such as Windows Mobile, Android, and Apple iOS) and users' custom applications. The hardware component consists of almost all of the components found in personal computers with some specific features. The main hardware components are CPU, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, and other accessories like keypads, cameras, GPS devices, LCD display, and network communication technologies like Bluetooth and Wi-Fi.

Technically, smart phones use Electronically Erasable Programmable Read-Only Memory (EEPROM) to store system files. This feature gives users the capability of reprogramming their devices by adding new features, or easily switching between different mobile carrier networks. Furthermore, the installed OS is mainly located in ROM to make it available even if the device is turned off.

Another mobile device that is widely in use nowadays, and is worth mentioning is the Personal Digital Assistant (PDA). They are mainly used for tracking the daily operations in specific markets, such as medical or industrial PDAs. Similar to smartphones, they contain all the necessary hardware and software components, and usually users can retrieve calendar, address book, Web access, and other items as necessary. Besides, a number of extra memory cards can be added to increase storage capacity and carry out other functions. Examples of such cards are Compact Flash (CF), Multimedia Card (MMC) and Secure Digital (SD).

Subscriber Identity Module (SIM) Cards

	<p>A SIM card is like any memory card, it contains a microprocessor and internal memory. It serves these additional purposes:</p> <ul style="list-style-type: none">- Assigns a unique identity to the network subscriber.- Stores user service-related information.- In some cases, it can be used to restore information. <p>There are two types of SIM cards: micro SIM and nano SIM. By switching a SIM card between compatible phones, users can move their provider usage and other information to another phone automatically without having to notify the service provider.</p>
--	---

Content Template	
Section Number	7.2
Section Title	Mobile Device Operating Systems
Introduction	Investigators should know how to work with various types of Operating Systems (OS) including those designed for mobile devices. Thus, in this section we summarize the common mobile OS by listing their main features, their built-in hardware and software security mechanisms, and how the data acquisition process is being carried out.
Content	<p>The purpose of an OS is to efficiently manage all available resources of a computer, mobile device, or any digital device. All OSs have almost the same functions, but their file systems, and structures are proprietary. The main problem that digital investigators face when working with mobile OS is that mobile devices have a variety of OSs compared to legacy workstations. In the following subsections, we give an overview of two main mobile OS Android OS and Apple iOS.</p> <p>Android OS and the File System</p> <p>Android is a Linux-based open source OS that was acquired by Google Inc. in 2005. It is found on a large range of smartphones, tablets, electronic devices, home appliances and in the auto industry. Android phones can now offer a wide range of services and applications to their users. However, the side effect of this tremendous capabilities is the increase in battery consumption rates.</p> <p>Like any other digital device, devices running Android have two types of memory: RAM , a volatile memory that stores running services and online data, and NAND, a nonvolatile flash memory which stores system files and other offline data. Also, since Android is based on the Linux kernel, it supports a number of file systems that include Ext4, FAT32, and YAFFS2 (Yet Another Flash File System 2). The Ext4 file system is found on the Google Nexus S. Whereas, YAFFS2 is an open source file system that was specially developed to be used in NAND flash memory. Currently, apart from the existing file systems, a digital forensic examiner must also review the course code files of the YAFFS2 system. Also, Android OS supports Microsoft FAT32 file system which is mainly found on microSD cards that are common in many Android handsets. VFAT is the Linux file system driver for FAT32 system.</p> <p>The SQLite database is often the most valuable digital evidence found on an Android OS. It is an open source relational database that was designed mainly for mobile devices. Now, the process of developing and managing the SQLite is sponsored by the SQLite Consortium, which includes other software vendors including Oracle, Nokia, Mozilla, Adobe, and Bloomberg.</p> <p>Android OS Evidence</p> <p>Investigators can extract evidence from an Android smartphone in four ways:</p> <ol style="list-style-type: none"> 1. Physical (HW/SW): It is a physical acquisition from a backup or by pushing an exploit to the device. 2. Logical (HW/SW): It is a logical acquisition which recovers only user data but not system files

3. Joint Test Action Group (JTAG): It is an IEEE standard for bypassing security and encryption on a smartphone to obtain a physical dump of the phone data. A full dump of NAND memory can be obtained.

4. Chip-off: This method can be used to access data on a chip when the circuit board has been damaged.

Android OS Security

Mobile Android users can use any one of the following methods to secure their smartphones:

- ✓ **PIN-protection:** A number having a maximum of eight digits. For security issues, after the user tries to login to the mobile device using an invalid PIN number of times, then he/she is requested to enter his/her email account details.
- ✓ **Password:** A password is an Alpha-numeric key that uses more advanced features for constructing the key to give better security. The file data/system/pc.key store the password information. For investigative purposes, investigators can use brute force methods to crack the password or they can use a dictionary attack.
- ✓ **Pattern lock:** This mechanism uses a pattern lock that swipes a 3×3 grid on the smartphone screen to secure the mobile device with gestures. Once applied, it generates 20-byte hex decimal value stored in gesture.key file. Several forensics tools viaForensics can be used to determine the stored pattern lock. The path of this file can be found following this path data/system/gesture.key.
- ✓ **Biometrics:** More advanced third-party solutions rely on biometric facial recognition can be used to unlock the device like a photo of the user's face or fingerprint.

When working with Android OS, investigators should keep the system and its files up-to-date. This requires searching for the latest security vulnerabilities. Security breaches and vulnerabilities are normally posted online to the public. This may provide an opportunity to gain access to valuable evidence.

Examples of Android OS Forensics Tools

A large number of Android forensics tools are available nowadays. Examples like the *viaForensics* software kit which consists of many free modules such as *Santoku*, which enables the investigator to image an Android device, and *AFLogical* which performs a logical acquisition that is stored on a blank SD card.

All Android applications are developed using the Java programming language with a .apk file extension and stored in the Google store after passing the check-list and getting a signed certificate. Every application run on top of the Android OS has a unique user ID and process. This feature prevents data sharing with other applications and hence, the overall security will be enhanced. For forensics analyses, it's worth noting that the amount of information that examiners can retrieve from the application depends on what information that application developer made available.

During the mobile application development process, developers can choose one of the following methods to store data generated by the application:

- [1] Preference
- [2] Files
- [3] SQLite Database
- [4] Cloud System

Technically, the SQLite database stores the most information compared to the other methods. Thus, investigators can have a great source of evidence when working with SQLite databases. Several forensic tools have been developed with their main focus on how to retrieve data from these relational databases: Examples of such tools are:

- ✓ SQLite Database Browser (<http://sqlitebrowser.sourceforge.net/>)
- ✓ SQLite Viewer (www.oxygen-forensic.com/en/features/)
- ✓ SQLite Analyzer (www.kraslabs.com/sqlite_analyzer.php)

Android applications have expanded significantly in both features and data usage. One important application example are those third-party applications that store locational information of user movements. Investigators can benefit from these services and the information they store. Nowadays, Android smartphones come with a GPS built-in application for navigation purposes. The SQLite database associated with navigation is stored in `da_destination.db` file. Facebook is considered one of the most popular applications found on all smartphones. The Facebook account information like contacts, chat logs, messages, photos, and searches are also stored in the SQLite database.

Apple iOS Operating System

The iOS is considered the second most popular mobile OS globally after Android. It is developed by Apple Inc. for its hardware including iPhone, iPad, and iPod Touch. Apple built advanced security into its products to secure its OS design by creating products with integrated hardware, software, and services. This includes advanced features to protect the entire system, secure all applications running on the system, and make sure that all types of data are encrypted and managed seamlessly.

Technically, iOS benefits from many hardware and software features to secure systems. Below are reviews of the most common ones.

- ✓ **Secure Boot:** This process is mainly carried out to protect the system from malicious or otherwise unauthorized software. Its task is to verify that the Bootloader is signed by the Apple root public key before running the OS. After this check is successfully completed, it runs the iBoot, a higher-level bootloader that proceeds loading the iOS kernel as well as the rest of the OS.
- ✓ **Secure Enclave:** It is a coprocessor found in iOS devices that contain Touch ID or Face ID. Each device's Secure Enclave has a unique ID which is used to create a temporary key that encrypts the memory in this portion of the system.

- ✓ **Passcode:** It is used to unlock the mobile device. It is typically four numerical digits. iOS has six-digit passcodes with the option to switch back to four or use an alphanumeric passcode.
- ✓ **Touch ID:** It is a fingerprint scanner that can be used to unlock the mobile device. Touch ID only temporarily stores the fingerprint data in encrypted memory in the Secure Enclave.

In addition to the above security methods, iOS is designed so that all of its core components are secured.

Other security features include:

- iOS has a mechanism to check system security during the startup process from the moment a device is turned on until running all applications and processes.
- iOS ensures that any software updates are authorized.
- The availability of system safeguards that ensure only authorized users can access the mobile device.
- It has strong rules for assigning passcodes and innovative features such as Face ID and Touch ID.
- iOS provides also powerful mechanisms for data security.
- The dedicated hardware processor of the iOS uses AES-256 encryption. In addition, strong encryption keys are also used for file-level data protection.
- iOS protects data during transmission over the network.
- iOS comes with a complete security model for protecting applications against malware and malicious codes.
- Apple Inc. has its own mechanisms to verify the identity of all developers before they can take part in any developer program offered by Apple Inc.
- Apple also reviews mobile applications before uploading to the Apple store to ensure that they have no bugs, they preserve user privacy, and so on.
- iOS provides runtime protection, entitlements, and sandboxing. In this way, mobile users can install and run applications assuring that they access data only in authorized ways.

iOS Forensic Analysis

Technically, four major methods can be used to acquire forensics data from an iOS device. Each method has its own advantages and disadvantages. Thus, Examiners should be aware of all of the four methods. Below we list these methods with a brief summary of each one of them.

- [1] **Acquisition via iTunes Backup:** This method depends on analyzing the latest backups of the iOS device. These backup folders contain several files that may be helpful for forensic analysis and provide information about the device, status, info and manifest.plist files. manifest.plist provides data about the latest backup and the info.plist file contains data that can be used to check whether the backup matches with the device.
- [2] **Acquisition via Logical Methods:** Today, logical acquisition is the most popular method being used for doing forensic analysis. With this method, investigators can easily allocate, recover and

	<p>analyze active files using a built-in synchronization method. This also will allow the investigators to collect digital evidence on call logs, SMS, contacts, photos, etc.</p> <p>[1] Acquisition via Physical Methods: This method has the greatest potential for recovering artifacts of the presented methods. This includes obtaining a bit by bit copy of the original media. Once the physical image has been obtained, examiners can view it and additional items such as deleted items in unallocated space.</p> <p>[2] Acquisition via Jail Breaking: This method is mainly used to replace the firmware partition with a hacked version. This way, an investigator installs software tools that would not normally be on the device. redSn0w is the most popular mechanism for jail breaking. It has a simple wizard that will allow the iOS in a step-by-step process to replace the firmware to begin the artifact extraction process.</p> <p>Finally, investigators working on the iOS device, can use the iPhoneAnalyzer free tool which was created by Crypticbit to obtain data from an iOS backup. This tool provides a way to access the file system from the iOS and also has a simple viewer to preview files. One of the main features of the iPhoneAnalyzer tool is the export all files. This feature converts the binary files to their proper names and locations.</p>
--	--

Content Template	
Section Number	7.3
Section Title	Mobile Device Acquisition Procedures
Introduction	This topic explores how to retrieve digital evidence from a mobile device, and how to conduct SIM card forensics.
Content	<p>Mobile device acquisition procedures are as important as procedures for personal computers. But some new challenges need to be addressed here, such as:</p> <ul style="list-style-type: none"> – A mobile device may lose its power quickly. – Cloud services synchronization issues. – Remote wiping. – Main memory is volatile. <p>Mobile device acquisition procedures can be summarized as follows:</p> <ol style="list-style-type: none"> 1. Make sure to disconnect the suspect’s mobile device from the network as soon as possible. This way the mobile device will not be able to synchronize with applications on a user’s laptop. 2. Make sure to disconnect any personal computer or laptop that may have an Internet access through the mobile device (A mobile device can be used as a hotspot to share Internet access). 3. Collect all these devices to determine whether the hard drive contains any transferred or deleted information. 4. Choose the appropriate time to search or seize the hard disk drive. 5. Make sure to turn off mobile device to save power or a planned attack. 6. Isolate the mobile device from incoming signals with one of the following options: <ul style="list-style-type: none"> – Put the device in airplane mode. – Use the Paraben Wireless StrongHold Bag. – Turn the device off. <p>To determine which acquisition method to use (logical acquisition or physical acquisition), investigators must first know where information is stored in the smartphone. As previously mentioned, a logical acquisition involves accessing files and folders. Whereas, a physical acquisition involves a bit-by-bit acquisition done to find deleted files or folders.</p> <p>To find the stored information, investigators should check the following locations:</p> <ul style="list-style-type: none"> – Internal storage (RAM) – SIM card storage – External memory device – Internet Service Provider (ISP) <p>Regarding the last point, in some cases investigators might need to get some information about the suspect or victim from the ISP, such as timestamps, or locations. However, this step is not always useful since service providers are now using remote wiping to remove a user’s personal information stored on a device to keep his/her data protected when the device is stolen. Remote wiping is necessary in this case to remove an account and its details including contacts, calendar, and other personal information for security purposes.</p>

Technically, investigators can also retrieve some information from SIM cards. The type and amount of retrieved information mainly depends on the service carrier infrastructure. But, in general the following information can be retrieved from the SIM card:

- Identifiers for SIM card and subscriber
- History of calls, data and numbers
- SMS and MMS information
- Some location information

Mobile Device Forensics Methods

The main methods of mobile digital forensics as introduced in the NIST guidelines are:

1. Manual extraction: It involves looking at the device's content manually and inspect it page by page.
2. Logical extraction: A forensic copy of the device is made.
3. Hex dumping and Joint Test Action Group (JTAG) extraction: It uses a modified boot loader to access the RAM contents.
4. The JTAG extraction: It gets information physical components like CPU, flash memory, etc.
5. Chip-off: It requires removing flash memory chip and gathering information at the binary level.
6. Micro read: This method looks at logic gates with an electron microscope.

Examples of Smartphone Forensic Tools

1. AccessData FTK Imager: It performs a logical acquisition and a low-level analysis for Android OS.
2. MacLockPick 3.0: It is similar to AccessData FTK Imager, but it is mainly designed for Apple iOS.
3. Paraben Software: It offers several built-in tools including device seizure and a SIM card reader.
4. BitPim: It has some features to view data on many mobile phone models including LG, Samsung, and others.
5. Cellebrite UFED Forensic System: It retrieves data from smartphones, GPS devices, and tablets.
6. MOBILedit Forensic: It contains a built-in write-blocker.
7. SIMcon: It recovers files on a GSM/3G SIM or USIM card, including stored numbers and text messages.

Content Template	
Section Number	7.4
Section Title	Chapter Summary
Introduction	In this section, we summarize the chapter by listing the key points.
Content	<p>Mobile forensics has become extremely important for digital forensic investigations. This is due to the fact that they can contain a wealth of evidence that will be more important than the evidence obtained from a traditional workstation, since mobile devices are always with users.</p> <p>In Section 1, we talked about mobile device forensics, and focused on how to retrieve information from a cell phone, or other mobile devices.</p> <p>Section 2 continued this topic by overviewing the features of the two common mobile operating systems: Android and IOS. This included the digital evidence acquisition mechanism, common system files, and some security features to protect data, user privacy, and the system kernel and its processes. Section 3 explored how to retrieve digital evidence from a mobile device, and how to conduct SIM card forensics.</p> <p>The next topic shed light on the importance of digital forensics reports, and describes guidelines for writing reports, as well as how to use forensics tools to generate reports.</p>

Activity Template (Reference Book[1], Hands-On Projects 12-1, Page 477)	
Number	7.1
Title	Explore SIMcon mobile forensics software tool
Type	Reflection
Aim	LO. 2, LO. 4 & LO. 5 In this activity, you will learn how to explore the SIMcon mobile forensics software tool that can generate information for mobile device investigations
Description	<p>In this case, Sebastian and Nau are suspected of drug dealing, and their phones were seized with the other digital evidence. One of your colleagues has a licensed version of SIMcon. You were able to go to her forensics lab and examine the SIM cards of both phones. In this project, you examine the exported Excel files. To do this activity, follow the following steps.</p> <ol style="list-style-type: none"> 11. Start Excel, and open the Messages_Sebastian's_phone.xls and Messages_Nau's_phone.xls files. 12. If the messages aren't currently in chronological order, change the display to sort them in this order. 13. Establish the timeline for what transpired between these two employees. Note items such as when they respond to each other's messages, dates and times, and what numbers they call. 14. Write a short report summarizing the data you examined and stating any conclusions you can draw from the SMS messages. 15. Start Notepad, and open Report_Nau's_phone.txt. Start a second instance of Notepad, and open Report_Sebastian's_phone.txt. 16. As you examine the reports, find definitions for the following items: International Mobile Subscriber Identity (IMSI), PLMN selector, HPLMN search period, and Cell Broadcast Message Identifier (CBMI). Note any other items of interest. 17. Explain what "SIM Phase: phase 2 - profile download required" means. 18. You notice "Originating Address (TP-OA): 264813358947" in the report for Nau's phone. The number breaks down into 264-81-3358947. Explain what the first two numbers—264 and 81—designate. 19. Explain what the following originating addresses mean: Originating Address (TP-OA): 123 Originating Address (TP-OA): 131 20. Next, compare the two files and write a report with answers to the preceding questions and include any conclusions you drew about the messages' contents.
Timeline	Implement activity: 2 hr.
Assessment	Each student is evaluated based on his/her implementation of the above steps and his/her submitted paper.

Activity Template (Reference Book[1], Hands on Projects 12-4, Page 478)	
Number	7.2
Title	Use Oxygen forensics to examine a BlackBerry device
Type	Reflection
Aim	LO.3, LO. 4 & LO. 5 In this activity, you will learn how to you use Oxygen Forensics to examine a BlackBerry mobile device.
Description	<p>Go to www.oxygen-forensic.com and request a registration code for downloading the demo version of Oxygen Forensics. (Keep in mind that getting the registration code might take a few days, and plan accordingly.) When you get it, download and install the software. To do this activity, follow the following steps.</p> <ol style="list-style-type: none"> 11. Start a Web browser, if necessary, and go to www.oxygen-forensic.com/en/download/devicebackups. Download the Blackberry 9520 file to your work folder. Unzip the file, which is Greg Bramson's BlackBerry 9520.ofb. 12. Start Oxygen Forensic Suite 2014 and click the Import backup file list arrow. 13. Click Import OFB backup. Navigate to your work folder, click the Greg Bramson's BlackBerry 9520.ofb file, and click Open. 14. In the Oxygen Forensic Extractor v. 5.1.303 dialog box that opens, click Extract. When the extraction is complete, click Finish. 15. When the file opens, click Brooklyn maniac, expand the tree structure, and then click Greg Bramson's BlackBerry 9520.ofb. 16. Notice at the lower right that the listing varies from what you saw for Patrick Payge's Galaxy Mini in the in-chapter activity. The Device Information and File Browser entries are the same, but this BlackBerry device has an entry called Phone Call Logs instead of an Event Log. Click the Device Information icon to see the owner, number, and service provider. 17. Return to the main window by clicking the back arrow at the upper left, and then click the File Browser icon. Click the Geo files tab (scrolling to the right to find it, if necessary), and examine the files listed. What can they tell you about the owner? 18. Click the Images tab and scroll down until you get to the .jpg files. What types of pictures are stored? What can they tell you? 19. Return to the main window and click Messages at the lower right. Examine the messages listed. Combined with the other files and pictures, what sort of timeline can you construct for the owner? 20. Exit the program. Write a two- to three-page paper with your findings.
Timeline	Implement activity: 2 hrs.
Assessment	Each student is evaluated based on his/her the successful implementation of the above steps.

Activity Template (Reference Book[1], Case Project 12-1, Page 479)	
Number	7.3
Title	Use Internet search engines to research for current mobile device forensics tools
Type	Search
Aim	LO.4 & LO. 5 In this activity, you will use Internet search engines and the NIST Mobile Device Forensics Guidelines to classify mobile device forensics tools.
Description	Download the most current version of the NIST Mobile Device Forensics Guidelines at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf . Page 17 lists a classification of mobile device tools. For the tools covered in this chapter, determine what type each one is based on these NIST guidelines. Write a one- to two-page paper explaining the uses and limitations of each tool.
Timeline	Internet Search: 1 hr. Prepare report : 2 hr.
Assessment	The student's work will be evaluated based on the written report and its alignment with the case.

Activity Template	
Number	7.4
Title	Write an essay describing the differences in examining two different cellphones
Type	Search and Reflection
Aim	LO. 2, LO. 3 & LO.5 The aim of this activity is to let students learn how to use Internet resources to write an essay describing the differences in examining two different cellphones.
Description	Write an essay describing the differences between an examination of a CDMA cellphone and a GSM cellphone.
Timeline	Internet search: 1 hr. Write essay: 4 hrs.
Assessment	The student's work will be evaluated based on the written essay and its alignment with case.

Activity Template	
Number	7.5
Title	Write standard operating procedures for examining a cellphone
Type	Search and Reflection
Aim	LO.1 to LO.5 The aim of this activity is to let students learn how to use Internet resources to write a standard operating procedure for examining a cellphone.
Description	Find a smartphone and then write standard operating procedures for examining that cellphone. Include in your essay forensic tools that will work with that particular model.
Timeline	Internet search: 1 hr. Write essay : 4 hrs.
Assessment	The student's work will be evaluated based on the written essay and its alignment with the case.

Think Template (MCQs)	
Number	7.1
Title	Mobile Device Forensics
Type	Choose correct answer
Question	<p>Which of the following best describes the role of the Base Station Controller?</p> <p>(A) Manages the radio signals for Base Transceiver Stations. (B) Assigns frequencies and handoffs between cell sites. (C) Both A and B are correct. (D) Neither A or B is correct.</p>
Answers	Answer: (B)

Think Template (MCQs)	
Number	7.2
Title	Mobile Device Forensics
Type	True or False
Question	A Mobile Switching Center is responsible for switching data packets from one network path to another on a cellular network. (A) True (B) False
Answers	Answer: (A)

Think Template (MCQs)	
Number	7.3
Title	Mobile Device Forensics
Type	Choose correct answer
Question	Which of the following mobile operating systems is an open source operating system based on the Linux 2.6 kernel and is owned by Google? (A) Symbian (B) Android (C) iOS (D) Windows
Answers	Answer (B)

Think Template (MCQs)	
Number	7.4
Title	Mobile Device Forensics
Type	True or False
Question	When acquiring a mobile device at an investigation scene, you should leave it connected to a laptop or tablet so that you can observe synchronization as it takes place. (A) True (B) False
Answers	Answer: (B)

Think Template (MCQs)	
Number	7.5
Title	Mobile Device Forensics
Type	Choose correct answer
Question	<p>Remote wiping of a mobile device can result in which of the following? (Choose all that apply.)</p> <p>(A) Removing account information (B) Enabling a GPS beacon to track the thief (C) Returning the phone to the original factory settings (D) Deleting contacts</p>
Answers	Answer: (A), (C) & (D)

Think Template (MCQs)	
Number	7.6
Title	Mobile Device Forensics
Type	Fill in the blanks
Question	<p>List two ways you can isolate a mobile device from incoming signals.</p> <p>(A) _____</p> <p>(B) _____</p>
Answers	<p>(A) Switch Off</p> <p>(B) Paraben Wireless StrongHold Bags</p>

Extra Template	
Number	7.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	7.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

8. Digital Forensics Writing Reports

Scope Template															
Number	8														
Title	Digital Forensics Writing Reports														
Introduction	The scope of this topic is to introduce students to the importance of digital forensics reports, and describe guidelines for writing reports, as well as how to use forensics tools to generate reports.														
Outcomes	LO. 1: Describe the importance of reports for the digital investigation LO. 2: Overview the main guidelines for writing forensics reports LO. 3: Explain how to generate reports from forensics tools.														
Topics	1. Why writing forensics reports is important? 2. Writing Reports Guidelines 3. Extracting Reports from Software Tools 4. Summary														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td> <td>1 hr</td> </tr> <tr> <td>Textbook Content:</td> <td>3 hr</td> </tr> <tr> <td>Thinking (On-line discussions, Review questions)</td> <td>1 hr</td> </tr> <tr> <td>Tutorial Work:</td> <td>3 hr</td> </tr> <tr> <td>Related Course Work:</td> <td>2 hr</td> </tr> <tr> <td>Total</td> <td>10 hours</td> </tr> </tbody> </table> <p>Reading Material</p> <ol style="list-style-type: none"> 1. <i>Ch. 14, Guide to Computer Forensics and Investigations (5th Edition)</i>. By Bill Nelson, Amelia Phillips, Christopher Stuart, 2016. 2. <i>Ch. 12, Computer Forensics and Cyber Crime: An Introduction (3rd Edition)</i>. By Marjie T. Britz, 2013. 	Task	Time	Preparation (Introduction and On-line Planning):	1 hr	Textbook Content:	3 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	3 hr	Related Course Work:	2 hr	Total	10 hours
Task	Time														
Preparation (Introduction and On-line Planning):	1 hr														
Textbook Content:	3 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	3 hr														
Related Course Work:	2 hr														
Total	10 hours														

Content Template	
Section Number	8.1
Section Title	Why Writing Forensic Reports is Important?
Introduction	In this topic we will explain the importance of writing reports during the digital forensic investigation process, and the set of rules that an investigator must follow to write reports.
Content	<p>A digital forensic report is the most important outcome that can be compiled after completing the forensic examination test. Once done, investigators can benefit from it in several ways, such as:</p> <ol style="list-style-type: none"> 1) Share obtained results between investigators and decision makers for decision making purposes. 2) Save or communicate the obtained facts that might support other investigations 3) Provide justification for collecting more digital evidence 4) Use in legal cases <p>Investigators must prepare the investigation reports taking into consideration all terms and rules of the country law. They first need to analyse the report by themselves to check its consistency and to ensure there are no contradictions with the law. They must expect to be cross-examined about the contents of the report in a court of law. Opposing counsel will eventually look for weaknesses and gaps in the facts presented. Therefore you need to know what facts are core in setting an opinion and what facts are not.</p> <p>Normally, there is no specific format or structure for writing investigative reports. However, investigators should keep a copy of any deposition notice or subpoena so that they can include the following information:</p> <ul style="list-style-type: none"> ✓ Jurisdiction ✓ Style of the case ✓ Format of court documents ✓ Cause number ✓ Date and location of the deposition ✓ Name of the deponent (expert witness) <p>Below are some generic concepts that should be considered before or during the writing process.</p> <ul style="list-style-type: none"> - Limiting a report to specifics: All reports must start by clearly defining the investigation goals. This will reduce the time and cost of the investigation, especially when working with a big dataset. - Audience: Clearly identify the technical knowledge of the intended audience before you begin writing. This will keep you more focused on the specifics. - Types of Reports: Forensics investigators should determine the type of reports they are required to create. There are several types of reports, such as <ul style="list-style-type: none"> • Formal reports (they contain facts) • Preliminary written reports (drafts or tests that haven't been concluded) • Verbal report (for attorney) • Examination plan (expected questions & answers)

	<p>Since the written report is sworn to under oath, investigators should give more attentions to carefully determining what they write.</p>
--	---

Content Template	
Section Number	8.2
Section Title	Writing Reports Guidelines
Introduction	This section describes guidelines on writing reports of the main findings in digital forensics investigations.
Content	<p>A written preliminary forensic report is considered a high-risk document because opposing counsel can find inconsistencies, i.e., if the presented report states something contrary to what an investigator states in his/her final report, they should expect opposing counsel to try to discredit the testimony by using the written report. Below are some guidelines to overcome this issue and make the written report more consistent.</p> <ul style="list-style-type: none"> ✓ Avoid using the terms "preliminary copy" or "working draft". These terms give opposing counsel an opening for discrediting your investigation. ✓ Don't destroy any preliminary reports you have done before a final resolution of the case. In some cases, destroying the report could be considered concealing evidence. ✓ Include in the written preliminary reports the same information you would supply in an informal verbal report. ✓ Give more focus to the final conclusion rather than the preliminary conclusion. ✓ Identify other investigative areas for further analysis. <p>Digital Forensics Report Structure</p> <p>Like any official report or scientific paper, a report structure normally includes some basic sections shown in the following list. The order varies depending on organizational guidelines:</p> <ul style="list-style-type: none"> ○ Report title: Each report should have a title indicating the case under investigation. ○ Abstract: The abstract briefly describes the examination and presents the report's main ideas and results in a summarized form. It should be one or two short paragraphs. ○ Table of contents: This includes the report roadmap, all sections, subsections, etc. It should allow for easy navigation to those parts that readers wish to review. ○ Body of report: This section is the core part of the report, it consumes most time and efforts: It consists of several parts. They are <ul style="list-style-type: none"> - Introduction: This should state the report purpose and show that you are aware of its terms of reference. It contains methods used, limitations, justification why you are writing the report, so make sure you answer the question "What is the problem?" You should also give readers a map of what you are delivering - Discussion sections: Organize discussion sections logically under headings to reflect how you categorise the information and to ensure that your information remains relevant to the investigation.

- **Conclusion:** The conclusion starts by referring to the report purpose, states the main points and draws conclusions.
- **References:** It lists the supporting material to which your work refers.
- **Glossary:** It is a comprehensive list of definitions for non-obvious *terms* and phrases mentioned *in the report*.
- **Acknowledgments:** They enable you to thank all those who have helped in carrying out the investigation.
- **Appendixes:** They contain supplementary material that is not an essential part of the text itself, but which may be helpful in providing a more comprehensive understanding of the investigation.

Writing Reports Clearly

To produce good reports, investigators must be self-critical and assess their writing quality. To do that, they must ask themselves several questions, such as:

Is the report easy to read?

Is the information presented relevant and clearly organized?

Is the language simple and direct so that the meaning is clear, and the text isn't repetitive?

Is the information accurate and consistent?

To answer these questions, a report should be structured in way such that it recites ideas in a logical order that facilitates logical thinking. Make sure the that data flow is consistent from the beginning of the report to the end. Also, collect related sentences into paragraphs, related paragraphs into sections and so on. The report should also be grammatically sound and without syntax and writing errors. Defining acronyms and any abbreviations not used as standard measurement units is particularly important; write the acronyms out in full the first time that they appear in the report.

When writing digital investigation reports, investigators can use many writing tips to pay more attention. Examples of these tips are:

- ✓ Investigators should use a natural language style and format. This way, readers will keep interested of what is going on.
- ✓ They should follow formal writing guidelines, word usage, grammar, and spelling.
- ✓ Be sure to avoid ambiguous sentences and generalized statements or arguments.
- ✓ Do not repeat sentences unless it is necessary, such as key words or technical terms.
- ✓ All verbs will normally be in the past tense.
- ✓ Use active rather than passive voice where appropriate.
- ✓ Avoid including many details and personal observations.
- ✓ Always communicate detached, un-emotional, observations in your report.
- ✓ Always try to identify the weakness in your own examination.
- ✓ Try to include signposts that help readers in scanning the text quickly by marking the main ideas.

Report Layout and Presentation

Typically, investigators use one of the two available numbering systems: *(i)* decimal numbering or *(ii)* legal-sequential numbering.

Decimal numbering system is widely used in writing scientific reports. It divides the report material into sections. It gives each section a unique number, and restarts numbering with each main section. With this system, interested readers can look at the headings to get an overview of how the various parts are related to each other.

The legal-sequential numbering system is a mix of roman and Arabic numerals normally used in legal pleadings. This system is understandable to lawyers but might not be as useful with the lay person because it doesn't indicate section hierarchy and relationship as clearly as the decimal numbering system.

Supporting Material

Investigators can enrich their reports by considering the following improvements:

- ❖ Add graphical material in the form of figures, tables, multimedia content, and equations to help analyze the case.
- ❖ Provide a sequential numbering method to all figures, tables, etc. For example, start numbering figures with Figure 1, Figure 2, Table 1, Table 2, Equation 1, Equation 2, and so forth.
- ❖ Add captions for every added figure, table or equation. This should contain declarative and descriptive information.
- ❖ Assign labels to all axes and include units of measurement.
- ❖ Insert a figure or a table after the paragraph in which it is first mentioned.
- ❖ Use fonts consistently and consistent heading styles, e.g., major headings in bold with initial capitals, minor headings in italics, and so forth.

Dataset Collection Methods

The process of collecting and presenting the used data is technically considered the most important parts of the report. The investigator must supply enough detail for readers to understand their process. This may include examination procedures, materials or equipment, data collection and sources, and analytical or statistical techniques. In this regard, presenting data in a well-organized manner is extremely important, especially if the data collection process becomes the subject of discovery or examination. If any hashing algorithms were used, they must be mentioned in the report. In order to ensure the credibility of the report, investigators must clearly provide a statement of digital analytical case limitations of knowledge and uncertainty.

Report Results

The core part of the report is the results and their analysis. In this part, investigators should describe what they actually found, not what they were looking for. These findings must be stated clearly and consistently. When discussing results, they can use subheadings to divide the whole section into sequential logical parts and make comments on results as they are presented. To make things easier for readers, the discussion can be linked with figures, tables, and equations. In addition, keep the conclusion very short and to the point, it should summarize your findings with clear, concise statements.

List of References

Adding and citing references to sources of material used in the work is necessary. This way, readers can easily track your work, read about some other related topics, and make sure that it is your own work without any plagiarism. When adding references, follow these guidelines:

- ✓ Cite references from trusted resources, such as books, journals, official Web sites, conference proceedings, etc.
- ✓ Add enough citations to the report wherever needed such as when you summarize people's opinions, theories, quotes, or paraphrases.
- ✓ Give detailed information to ease tracking down the information.
- ✓ Choose new or newly published references, i.e., Keep them up-to-date.
- ✓ Apply a standard format, such as use italic font, capital letter or small letter, volume and page numbers, publisher address, etc. For more information, refer to the Modern Language Association (MLA/Harvard) and the American Psychological Association (APA), which are the two most commonly used formatting guidelines.

Appendixes

Investigators can also include an appendix at the end of the report as necessary. They contain additional information that is not essential to be in the report body but including them can support the analysis, such as lengthy information, raw data, figures not used in the body of the report, and anticipated exhibits. If there is more than one appendix, they should be numbered and arranged in the order referred to in the report.

Content Template	
Section Number	8.3
Section Title	Extracting Reports from Software Tools
Introduction	In this section, students will learn how investigators can integrate forensic software-generated reports into the official investigation report that they present to the attorney or client.
Content	<p>In previous chapters, we mentioned a large number of forensic software tools, and students had hands-on experience working with some of these tools, such as X-Ways Forensics, ProDiscover, ILookIX, OSForensics, EnCase and FTK. Normally, these tools produce various types of log files and analysis activities while they are in action. Therefore, reports can also be created that provide supplemental information about the results and analysis. The format of these logfiles are typically text, word processing, or HTML format.</p> <p>Although forensic software reports are considered as the main outcome of the investigation process, investigators should not forget their responsibilities to clearly explain the significance of the evidence they recovered and, if necessary, define any limitations or uncertainty that applies to the results.</p> <p>During the activities, students will work on several forensic tools such ProDiscover and OSForensics to generate reports that will be used for further examination. As you will noticed, some forensic tools have unique features that aren't available in other tools.</p>

Content Template	
Section Number	8.4
Section Title	Chapter Summary
Introduction	In this section we will summarize the main concepts presented in the previous sections.
Content	<p>Nowadays, all courts worldwide require investigators to submit written reports. The reports must include investigator opinions along with the basis for the opinions. They should also answer the questions investigators were retained to answer and keep information that doesn't support specific questions to the minimum.</p> <p>In section 1, we explained the importance of writing reports during the digital forensic investigation process, and set out some of the rules that investigators must follow to provide a well-defined report structure that contributes to readers' ability to understand the information easily.</p> <p>Section 2 described the guidelines on writing forensic reports. Investigators must make sure that their reports include labeled sections and follow numbering schemes consistently. They must ensure that the supporting materials, are also numbered and labeled clearly.</p> <p>Section 3 discussed how investigators can utilize software-generated reports from forensic tools and integrate them into the official investigation report. The tools generate various types of data with different formats text, word processing, or HTML format.</p>

Activity Template	
Number	8.1
Title	Write a report to outline the resources needed for a given scene
Type	Reflection
Aim	LO.1 & LO.2 The aim of this activity is for students to learn how to conduct internal computing investigations to gather data that helps with the evidence collection process.
Description	The county prosecutor has hired you to investigate a case in which the county treasurer has been accused of embezzlement. What additional resources, such as other experts, might you need to collect data for this investigation? Write a one-page paper outlining what resources you should consider helping you with the evidence collection process.
Timeline	Write a report: 2 hrs.
Assessment	Each student is required to submit his/her report and evaluations

Activity Template (Reference Book[1], Hands-On Project 14-1, Page 531)	
Number	8.2
Title	Conduct internal forensics investigations for a crime scene
Type	Reflection
Aim	LO.1, LO.2 & LO.3 In this activity, you work as an forensic investigator for to help in analyzing an incident.
Description	<p>The general counsel for Superior Bicycles, Ileen Johnson, has asked you to locate a file that might contain information about the construction of a new bicycle frame. She tells you that the file she's interested in recovering is named "Materials," but she doesn't know the file extension. Follow these steps:</p> <ol style="list-style-type: none"> 1. Start OSForensics. Click Search Index in the left pane of OSForensics. In the Enter Search Words text box, type Materials. Click the Index to Search list arrow, navigate to and click the drive where you mounted the image, and then click Search. 2. In the Search Index Results window, click the Files tab, and examine the search hits to find any files with the name Materials. 3. Next, click the Emails tab. Right-click each message and click Open to examine its contents. For messages with a file named Materials attached, right-click the filename in the lower pane and click Add Attachment(s) to Case. In the Please Enter Case Export Details window, type File named Materials.rtf in the Export Title input box, and then click Add. 4. Double-click the e-mail with the subject line "Documentation for future plans" containing the Materials.rtf file. In the Documentation for future plans window, click View, Headers. In the lower pane, select the header contents. Right-click this highlighted material and click Copy. Close the Documentation for future plans and the E-mail Viewer windows. 5. In the Manage Case window, click Add Note. Type Header information - Documentation for future plans in the Name text box. In the lower pane, right-click and click Paste to paste the e-mail header information. Click Save. 6. Click Start in the left pane, and then click Generate Report in the right pane. In the Export Report window, click the Copy files to report location option button. Click Browse, navigate to and click your work folder, and then click OK twice. 7. Review the report in your Web browser, and then print it. Turn it in to your instructor, and then exit your Web browser and OSForensics.
Timeline	Understand project idea: 1 hr. Implement project steps: 1 hr.
Assessment	The student's work will be evaluated based on the projects' implementation steps and the extracted information.

Activity Template (Reference Book[1], Hands-On Project 14-2, Page 532)	
Number	8.3
Title	Locate and extract files using a given formats and generate a report
Type	Reflection
Aim	LO.1, OL.2 & LO.3 In this activity, you will review a case study. Your main tasks are to locate, and extract files using specific formats and generate a report.
Description	<p>In this continuation of Activity 1.2, Ileen Johnson has sent you another image file collected from employee Chris Murphy's computer, which uses a different file system than Denise Robinson's computer uses. She's conducting a follow-up investigation of a case that's several years old and deals with some very old file formats. You need to locate, and extract files using these file formats and generate a report for Ileen. For this activity, you use the GCFI-NTFS.dd image file. You need to look for spreadsheet accounting information created with OpenOffice Calc (files with .ods and .sxc extensions) and e-mail correspondence created with Outlook Express (.dbx and .pst extensions). When you find any files with these extensions, add them to the case in OSForensics.</p> <p>Follow these steps to find e-mail messages containing attached spreadsheets:</p> <ol style="list-style-type: none"> 1. Start OSForensics, and create a new case named HOP14-2. Use OSFMount to select the drive for the image file GCFI-NTFS.dd. 2. Click Create Index in the left pane. In the Step 1 of 5 window, click the Use Pre-defined File Types option button, click the Emails, Attachments, Office + PDF Documents, Zip Files, Images, and Plain Text Files check boxes, and then click Next. In the Step 2 of 5 window, click Add. In the Add Start Location dialog box, click the Whole Drive option button, click the list arrow, click the drive letter where GCFI-NTFS.dd is mounted, and click OK. Click Next, and in the Step 3 of 5 window, click Start Indexing. 3. When the indexing has finished, click OK, if necessary, in the message box informing you that errors reading some files might have occurred in the indexing process. 4. Next, click File Name Search in the left pane. In the Search String text box, type *.ods;*.sxc;*.dbx;*.pst, click the ... button next to the Start Folder text box, click the drive where you mounted GCFI-NTFS.dd, click OK, and then click Search. 5. When the search is finished, click the Sorting list arrow, and then click Type. 6. Right-click Inbox.dbx and click View with Internal Viewer. In the E-mail Viewer window, click the Paperclip toolbar icon to sort all messages containing attachments. 7. In the E-mail Viewer window, examine each message. Right-click any message with an .ods or .sxc file attached and click Add Email to Case. In the Please Enter Case Export Details window, type Spreadsheet file found in message in the Export Title text box, and then click Add. 8. Right-click the spreadsheet file in the message header and click Add Attachment(s) to Case. In the Please Enter Case Export Details window, type Found spreadsheet in the Export Title text box, and then click Add. Close the E-mail Viewer window. 9. Click File Name Search in the left pane. If the File List window is blank, move the scrollbar up or down to display the contents. Examine the other .dbx files to determine whether there are more messages with attached spreadsheets. If you find other spreadsheets, repeat Steps 6 through 8. 10. Click File Name Search in the left pane, if necessary. Double-click the first file with an .ods or .sxc extension in the search results to open it. If a file contains spreadsheet data, right-click the file, point to Add to Case, and click File(s). In the Please Enter Case Export Details window, type Spreadsheet not attached to e-mail in the Export Title text box and click Add. 11. Repeat Step 10 for all other spreadsheet files in the search results window. When you're finished, exit OSForensics.

Timeline	Understand project idea: 1 hr. Implement project steps: 1 hr.
Assessment	The student's work will be evaluated based on the projects' implementation steps and the extracted information.

Activity Template (Reference Book[1], Hands-On Project 14-4, Page 534)	
Number	8.4
Title	Write a two-page investigation report.
Type	Reflection
Aim	LO.1, LO.2 & LO.3 In this activity, you will review a case study taken from a computer forensics firm. Write an outline for how the firm should approach the case.
Description	For this activity, print all e-mails and spreadsheets from the case you processed In Activities 1.2 & 1.3. Then write a one- to two-page report addressed to Ileen Johnson that explains the steps you have taken and the evidence you found in your examination. In the conclusion, state your opinion about the nature of the correspondence, based on the e-mails you collected and compared for these cases. Include any supporting materials as appendixes.
Timeline	Write report: 2 hr.
Assessment	The student's work will be evaluated based on the written report and its alignment with the case study problem.

Activity Template (Reference Book[1], Case Project 14-3, Page 534)	
Number	8.5
Title	Recommend a writing guide that examiners can use for all official written reports.
Type	Search
Aim	The aim of this activity is to learn student how Conduct research on the Internet to find information about style manuals and technical and legal writing guides.
Description	Your manager has asked you to research and recommend a writing guide that examiners in your digital forensics company can use for all official written reports. Conduct research on the Internet to find information about style manuals and technical and legal writing guides. You should also research writing guides from professional associations, such as the IEEE. Write a two- to three-page report recommending a style manual or technical/legal writing guide for your company to use and explain the reasons for your recommendations. You might want to combine guidelines from different sources in coming up with recommendations for digital forensics reports.
Timeline	Internet search: 1 hr. Writing report: 2 hrs.
Assessment	Each student is required to submit his/her report and evaluated based on its implications.

Think Template (MCQs)	
Number	8.1
Title	Digital Forensics - Writing Reports
Type	Choose correct answer
Question	Which of the following is an example of a written report? (A) A search warrant (B) An affidavit (C) Voir dire (D) Any of the above
Answers	Answer: (B)

Think Template (MCQs)	
Number	8.2
Title	Digital Forensics Writing Reports
Type	True or False
Question	Consistency is the most important aspect of formatting that should be considered when writing a report. (A) True (B) False
Answers	Answer: (A)

Think Template (MCQs)	
Number	8.3
Title	Digital Forensics Writing Reports
Type	Fill in the blanks
Question	What is a major advantage of automated forensics tools in report writing? <hr/>
Answers	Investigators can incorporate the log files and reports these tools generate into the written reports.

Think Template (MCQs)	
Number	8.4
Title	Digital Forensics Writing Reports
Type	Choose the correct answer
Question	<p>Automated tools help an investigator collect and report evidence, but he/she is responsible for doing which of the following?</p> <p>(A) Explaining your formatting choices (B) Explaining in detail how the software works (C) Explaining the significance of the evidence (D) All of the above</p>
Answers	Answer: (C)

Think Template (MCQs)	
Number	8.5
Title	Digital Forensics Writing Reports
Type	Fill in the blanks
Question	<p>List three items that can be included in report appendixes?</p> <p>(A) _____</p> <p>(B) _____</p> <p>(C) _____</p>
Answers	<p>(A) Explaining report formatting choices</p> <p>(B) Examples of data gathered</p> <p>(C) Explaining in detail how the software works</p>

Extra Template	
Number	8.1
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)

Extra Template	
Number	8.2
Title	The title of the extra resource identified.
Topic	Link to the corresponding section and topic.
Type	<p>Could include:</p> <ul style="list-style-type: none"> • Book/Chapter (ISBN) • Offline content (Full reference required) • Online content (URL)