Book 2 - Digital Forensic Procedures

1. Introduction to Digital Forensics

Scope Template	
Number	1
Title	**Introduction to Digital Forensics**
Introduction	This topic introduces digital forensics in general. The topic shows the meaning of digital forensics and the types of digital forensics. The chapter then defines digital evidence and shows the subdisciplines of digital forensics.
Outcomes	1- To know the meaning of digital forensics 2- To know the types of digital forensics 3- To understand what is digital evidence and its importance 4- To understand the subdisciplines of digital forensics and their meaning
Topics	**1- Introduction** **2- Digital Forensics** **3- Digital Forensics scientists** **4- Types of digital forensics** **5- Digital Evidence** **Digital forensics subdisciplines**
Study Guide	

Content Template	
Section Number	1.1
Section Title	Introduction
Introduction	This section introduces digital forensics and its relation to scientific methods and legal methods. The section shows how digital forensics changes over time because of emerging technologies. The section also outlines the differences between scientific methods and legal methods.
Content	This book is an introduction to digital forensics procedures. It gives an overview of forensic science and its application to the digital artefacts that we continuously create through our interactions with computers and mobile devices. It is known that forensic science is applying science to the data in a legal manner [1]. The 'forensics' element refers to the courts part and how courts make their decisions while the 'science' part refers to the use of the scientific method in investigation [2].

In order to understand the background of forensics science, we briefly explain what is a scientific method. Science aims at producing explanations of phenomenon around us in the form of laws or rules. Examples of the laws are Newton laws of movements and gravity laws. These laws can be described by scientific and mathematical formulae. These laws and rules can be universally accepted and generalized to similar cases unless someone proves that these laws are incorrect.

Scientists are usually able to derive a scientific law by following a process known as the scientific method. The scientific method consists of steps that are:

- making observations regarding a specific issue
- forming a hypothesis to explain the observations
- testing the hypothesis
- examining and analyzing the results of the testing
- stating that the hypothesis is a scientific law that holds good for a given range of the phenomena
- or disproving the hypothesis

Scientific law may change over time, and the change requires the agreement of the scientific community. A scientist can extend another scientist's law or change it based on new findings. These changes help us to understand the emerging phenomenon and helps new societies to adapt to the change. The same applies in legislation because new criminal practices emerge [1][3]. Also, because of the large number of new methods of detection, such as fingerprints that can be used as a proof in the law.

Forensics science therefore is very similar to the scientific method as it focuses on the discoveries of phenomena that add a value to investigations which end in the court for legal proceedings [2]. Also, specialist tools and standard operating procedures are usually developed over time, and their development causes the emergence of new legal methods. Further, specific methods are used by a forensic scientist or investigator who examines a particular case for finding evidence and reports the evidence to the legal representative. The final result of many forensics investigations is often to help prove if a person is guilty or innocent in a criminal trial.

Scientific methods usually differ from legal methods and both have different requirements and decision-making process [4]. The court's job is to make a formal judgment on specific issues between different parties in the criminal courts. The legal methods are used to determine whether the prosecution has evidence which is accepted and can identify that a crime has been committed. One of the fundamental rules of court operation is that once a decision is made, that decision is final. This holds true unless there are profound and reasonable justifications for appeal. The reason for this is that it would be unfair to someone to be accused of a crime, if a court is allowed to change the decision based on further investigations after several months. This is sometimes referred to as the "fiction of certainty" [4][2].

Content Template	
Section Number	1.2
Section Title	**Digital Forensics**
Introduction	This section states the definition of digital forensics. The section also presents the history of digital forensics.
Content	Digital forensic scientists are professionals who analyze and collect data from a computer or other digital devices. Other terms that are used in this book are digital forensics investigator and digital forensics expert. The term digital forensic scientist extends the definition of forensic scientist to the digital domain. There are different specialisms of forensic science that a student of digital forensics needs to know and distinguish from the digital forensics scientist, and these are [1], [3]: **1- Forensic Pathology** which is a specialty of medicine and a sub-specialty of pathology for studying problems of unnatural death. **2- Forensic DNA** which is the use of biological science to determine the ID of individuals by using genetic samples such as blood, semen and saliva or by DNA. **3- Forensic Engineering** which is the use of engineering principles to investigate accidents of aircraft, vehicles, electrical faults, fire, or metal fatigue. **4- Forensic Accounting** which focuses on tracing any financial inconsistencies within a company's account. **5- Forensic Dentistry** which is the use of information for identifying human remains through teeth examination and dental prostheses **6- Forensic Anthropology** which is the study of human beings in relation to their physical character, such as gender, age, nutritional status, ethnicity, stature, disease processes, and skeletal trauma. **7- Forensic Toxicology** which determines the existence and the number of drugs, poisons or toxins in body. Scientists from the above specialisms need to be very precise and accurate in their work. It is the same for the digital forensic scientists since they need to perform their work accurately as their actions are subjected to scrutiny in the court by the judiciary. The presence of a standard structured process provides digital forensic scientists with a suitable mechanism to be followed during the investigations.

Content Template	
Section Number	1.3
Section Title	Types of digital forensics
Introduction	This section discusses the types of digital forensics. It also shows the differences between these types.
Content	Digital forensics is evolving continuously deals with ongoing developments in the world. This causes it to include many sub-disciplines that are [1]: 1. **Computer Forensics** which focuses on electronic evidence that can be found in computer or other digital devices in terms of identification, preservation, collection, analysis and reporting the evidence for supporting the investigations and legal proceedings. 2. **Network Forensics** which focuses on electronic evidence related security attacks, intrusions, worms, virus or malware attacks in term of monitoring, capturing, storing and analyzing of network activities. 3. **Mobile Devices Forensicss**which focuses on electronic evidence from mobile phones, smartphones, GPS devices, SIM cards, PDAs, and tablets. 4. **Digital Image Forensics** which focuses on photographic evidence in terms of extraction of the required information from images. 5. **Digital Video/Audio Forensics** which focuses on sound and video evidence in terms of collection, analysis and evaluation of recordings. 6. **Memory forensics** which focuses on obtaining evidence from a running computer by RAM live acquisition. In practice, this classification can be changed because of staff skill sets, available lab space, contractual requirements, and other factors. For example: smartphones without SIM cards can be considered computers. Another example is whether to consider memory cards found in smartphones and tablets indicate computer forensics or mobile forensics. Also, tablets with keyboards can be considered laptops and can be considered as computer or mobile forensics. This classification is not the final one because digital forensics will continue to expand as new types of digital devices and electronic data are created so often.

Content Template	
Section Number	1.4
Section Title	**Digital Evidence**
Introduction	This section explores the meaning of digital evidence. It also shows how the evidence should be collected and what are the components of the digital evidence.
Content	The main task of the digital forensic scientists and investigators is to collect digital evidence so that they can present it in the court and assist in determining the result of the case. Digital evidence is a form of electronic data, either it is a transaction, a document, or media such as an audio or video recording [1]. Transactions can include a financial record created during purchasing an item, paying a bill, writing a check, and withdrawing or depositing money. Nowadays, almost every transaction in our daily life is kept in electronic format and becomes digital evidence [3]. Several examples can be found in our life, such as doctor visits, getting medical prescriptions, marriage certificates, registering a new born child and purchasing or selling houses. Digital evidence requires three basic elements that are necessary during the collection [1]: 1- Source: the artifacts and the metadata that can show where the information came from. For example, embedded watermarks in some images can identify its origination or authenticity. Establishing source is very important for forensics information as it can make or terminate a case. 2- Format: Evidence must be stored in its original format and digital forensics investigator should utilize all available tools to maintain the format of the evidence. 3- Type: evidence can have different types, such as email, a document, spreadsheet, or text message. Electronic data can become digital evidence if they are stored in a place that is ultimately accessible. The data must also be recoverable by a forensics investigator. Nowadays, the big challenge is not related only to finding the digital evidence, but also to storing the evidence, getting access to that storage, and the ability to recover that evidence for a civil or criminal action.

Content Template	
Section Number	1.5
Section Title	**Digital forensics subdisciplines**
Introduction	This section presents the most well-known subdisciplines that can be encountered while working on digital forensics cases.
Content	**1.5.1 incident response** Digital forensics scientists and investigators consider incident response to be a subdiscipline of digital forensics [1], [2]. In network security, a network security breach or attack, hacking, intrusion detection, malware, and rootkits are considered "an incident". These attacks are caused by a hacker, or from a worm, a virus such as Trojan horse, or other malware. An incident response expert is specialized in identifying possible attacks and determining whether the attack has reached to other parts of the network [1]. The incident response expert also finds ways to contain the attack, and eliminate any malicious code. The duty of the incident response experts also is to educate information technology (IT) workers on how to protect the computer network within an organization by using the appropriate security measures. **1.6.3 Cell phone forensics** Nowadays, cell phones are widely spread so the examination of cell phones has become very popular and similar to the examination of computers. So, cell phone forensics as a subdiscipline of digital forensics has come to mean the examination of cell phones and the records created by cell phone service providers like call detail records and cell phone billing information [1]. Because cell phones contain much valuable information, examining them can recover electronic evidence that has of great value in the court. Examples of cell phone data are the contacts, text messages, audio recordings, images, videos, and e-mail. Even deleted data from a cell phone can be recovered as well and used as evidence [1], [3]. However, because there are several types and models of cell phones, recovering data from a cell phone is specific to each type and requires special tools to deal with that type. The good news is that modern cell phones are becoming very similar to computers, e.g. smartphones, so recovering data from these devices is becoming very similar to the process in computers. One set of important data within cell phones is related to call records that contain information about the numbers that were called from a particular cell phone, the date and time of the calls, the duration of the call, and the cell site information for cell phones [4]. Cell site information is important because the general location of a person and their movement can be identified based on their cell phone activity. However, using cell phone records and cell phone activity to establish a legal case for a person or its use as evidence requires critical analysis of the cell phone data. **GPS forensics**

Global positioning systems (GPS) have also become very popular and used in most cars and phones nowadays. Therefore, GPS forensics has emerged as a subdiscipline to include the examination of GPS data and records. The examination of GPS is useful to find information such as recently visited places, favorite places, and navigated addresses. These GPS records and information can form valuable evidence, even if the GPS unit cannot be displayed in the court. Also deleted data from GPS units can be recovered as well [1].

Examples of using GPS as evidence could be based on a person suspected of a crime, the GPS records can assist in determining if the person actually went to the location of the crime, or the GPS can reveal whether the person was near the incident place in the vehicle. Another example is when a suspected person is accused of committing a murder at one location, and then placing the body at another location in a one-hour timeframe. The GPS can help in locating all events in this case. However, the GPS units may have some errors in the tracking process due to GPS malfunction, poor transmission, and unclear sky view [1]. So, the data of the suspected person obtained by GPS may not be true or related to the crime which requires careful analysis in all cases.

Social media forensics

Social media websites and programs have become very popular and widely spread in the world these days. The social media websites such as Facebook, Twitter, and LinkedIn are commonly used and contain a lot of data about people. Some people may have accounts with multiple social media sites. For example, some people have a Facebook account to communicate with their friends and family, and a LinkedIn account for business and professional use.

Any type of communication on social media inevitably leads to electronic evidence. Therefore, social media forensics has become very necessary. The social media forensics subdiscipline focuses on examining social media communication and the artifacts left on cell phones and computers used for that communication [1]. For example, when a forensics investigator performs examinations on a computer or a social media software, valuable and necessary data for a specific case can be found.

Media device forensics

There are different media devices, such as digital audio recorders, digital music players, personal data assistants, USB memory drives, and portable hard drives. The forensics examination of media devices can find useful data and form important evidence [1]. Other useful data that can be found on media devices are the files that have been transferred to or from them and the time and date when these transfers took place. Deleted data from media devices can also be recovered and used as evidence. For example, a deleted file from a digital audio recorder can be recovered.

The media devices are important in digital forensics because these devices can be used to steal or hide data [1], [2]. For example, music players are usually used to play music, but because of their memory capacity, they can be used to transfer important forensic data to other places.

Digital video and photo forensics

Digital video and photo forensics focuses on the examination of photos or videos for finding electronic evidence. A forensics investigator needs to understand that a photo is a still image while a video is a sequence of still images [1]. A movie is actually thousands of images that are played within a timeframe. To find useful evidence, digital video and photo forensics should allow for enhancement and analysis of the individual images.

The main difference between photo and video forensics is that with a photo, enhancement is made one time, while with a video, thousands of enhancements are made at a time [1]. Indeed, enhancement of videos and photos requires much care because incorrect enhancement can damage the evidence within the photo or the video.

Digital camera forensics

A traditional film camera that was very popular few decades ago used to contain only the actual picture taken. On the other hand, a digital camera contains the pictures taken and much information about the pictures themselves embedded as metadata. This metadata such as the model of the camera and the time of taking the picture can form forensics evidence. Therefore, it is important for the digital forensics to focus on such adomain.

As with other digital media devices, digital camera pictures, if deleted, can be recovered. Actually, often the digital picture is enough in front of court as evidence even if the camera was not found. Through a computer, an investigator can examine digital pictures taken with a digital camera and use the metadata within the pictures to link them back to the originating camera [1].

Digital audio forensics

Digital audio forensics includes the enhancement and analysis of audio recordings created with any type of recording device [1]. Audio forensics aims to verify the integrity of audio recordings. A digital forensics investigator needs to know the techniques used to enhance audio and the software used for voice pattern recognition. For example, if the quality of recording is poor, the audio track should be enhanced so that voices would become clearer, or background noise would be eliminated. The voice pattern recognition software allows the use of audio recording for identifying the voices of particular people.

Computer game forensics

Today, the most popular form of games is the multiplayer games. There are tens of millions around the world who play multiplayer online games. People spend large amounts of their time on computer games and online games. Such a person actually lives the life of the game once he/she logs in and builds their game character. Different events can be designed by the player including good and bad events.

	The information inside online and computer games indeed form digital evidence [1], [2]. In digital forensics, the actual amount of time a person has spent playing as one of the characters can be detected in the game itself by typing a command into the game interface. Online and computer games usually store much information about the players. Information in games includes information about each session, the length of that session, the in-game chat logs, and the characters for each account in the game. Another set of computer games are those on game consoles, such as li Xbox, Nintendo Wii, or Sony PlayStation. These devices are all computers because they contain a hard drive, and they have an operating system. The information stored on these devices can be recovered, including deleted information from a gaming console. Such information can be used as evidence since the players have identities within the game itself or online. Some games are also connected with emails and social networks which leaves much information to be collected as forensics evidence.

Activity Template	
Number	1.1
Title	Write an article about the history of digital forensics in your country?
Type	• Research
Aim	- To understand the meaning of digital forensics - To know the types of digital forensics
Description	Each student needs to write an article about the history of digital forensics in his country. Students must describe when digital forensics started and what is the current situation. Students should list some of the laws related to digital forensics.
Timeline	One week
Assessment	Students need to produce an article of at least three pages. The main elements in the article are: 1- The history of digital forensics 2- The laws in the country facilitating the work of digital forensics 3- The challenges facing digital forensics in their country

Activity Template	
Number	1.2
Title	Write an article about computer games forensics?
Type	Describe whether this will be in the form of: • Research
Aim	To know the subdisciplines of digital forensics
Description	Students need to find how information is stored in computer games, what form this information takes and can this information form actual digital evidence?
Timeline	One week
Assessment	Students need to produce an article of at least three pages that describes what is digital evidence in computer games, data types, storage places, the laws related to finding evidence in the computer games.

Template (MCQs)	
Number	1.1
Title	introduction
Type	• Choose correct answer
Question	The term digital forensics as introduced at the beginning means the protocols to study cases on computers
Answers	1- True **2- False**

Think Template (MCQs)	
Number	1.3
Title	**Digital Forensic scientists**
Type	- Choose the correct answer
Question	The science that determines the existence and the number of drugs, poisons or toxins in body is called:
Answers	Forensic Pathology Forensic Accounting **Forensic Toxicology** Forensic Anthropology

Think Template (MCQs)	
Number	1.4
Title	Types of digital forensics
Type	- Choose the correct answer
Question	The type of digital forensics that focuses on electronic evidence related to security attacks, intrusions, worms, viruses or malware attacks is called:
Answers	Mobile forensics **Network forensics** Memory forensics Computer forensics

Think Template (MCQs)	
Number	1.5
Title	**Digital evidence**
Type	- Choose the correct answer
Question	The digital forensic investigator is allowed to legally change the format of the electronic file collected as evidence
Answers	True **False**

Think Template (MCQs)	
Number	1.6
Title	**Digital forensic subdisciplines**
Type	- Choose the correct answer
Question	The digital forensic subdiscipline that aims to find an evidence related to a person's location is termed:
Answers	Media device forensics Social media forensics **GPS forensics** Computer games forensics

References	
Number	1.1
Title	*Digital Forensics for Legal Professional*
Topic	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Type	• L. E. Daniel, Larry E. and Daniel, *Digital Forensics for Legal Professionals*, 1st ed. Elsevier Inc., 2012.

References	
Number	1.2
Title	*The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*
Topic	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Type	• J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2014

References	
Number	1.3
Title	*Computer Forensics and Digital Investigation with EnCase Forensic v7*
Topic	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Type	• S. Widup, *Computer Forensics and Digital Investigation with EnCase Forensic v7*, 1st ed. McGraw-Hill Education, 2014

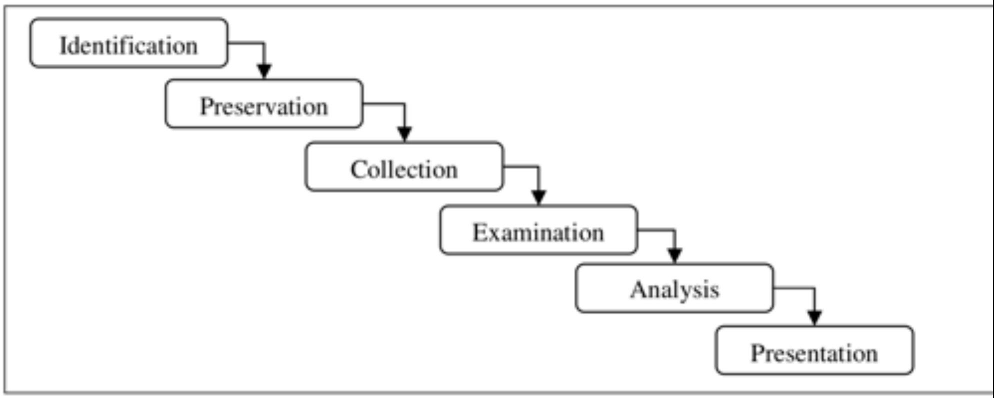
References	
Number	1.4
Title	*Digital Forensics*
Topic	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Type	• A. Årnes, *Digital Forensics*, 1st ed. Wiley, 2017

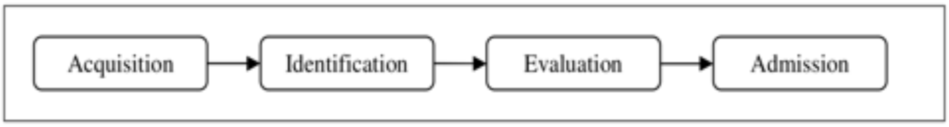
References	
Number	1.5
Title	A Road Map for Digital Forensic Research
Topic	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Type	• Digital Forensic Research Conference, "A Road Map for Digital Forensic Research," 2001

2. Digital Forensics Process

Scope Template	
Number	2
Title	**Digital Forensics Process**
Introduction	This topic introduces the digital forensic process. It shows the stages of the digital forensic process and explains each stage. The section gives guidelines to digital forensic investigators on how to collect evidence, preserve it , analyze it and present it to the court.
Outcomes	To know the digital forensic process that is related to how to collect evidence, preserve it, analyze it and present it to the court of law
Topics	1- Introduction 2- Digital Forensic Research Workshop model 3- Computer forensic investigation process (1984) model 4- Details of digital forensic stages 5- Acquisition best practice
Study Guide	

Content Template	
Section Number	2.1
Section Title	Introduction
Introduction	This section introduces the digital forensics process and the model used to describe the investigation process.
Content	There are different models that describes the digital forensic process. Examples of these models are (Hassan 2011): 1- Digital Forensic Research Workshop (DFRWS) Model 2- Computer Forensic Investigative Process (CFIP) (1984) model 3- Abstract Digital Forensics Model (ADFM) (2002) 4- Integrated Digital Investigation Process (IDIP) (2003) model 5- Enhanced Digital Investigation Process Model (EDIP) (2004) 6- Computer Forensics Field Triage Process Model (CFFTPM) (2006) 7- Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) (2009) model Some of these models are too detailed and others are too general. Sometimes, it is difficult for new forensic investigators to select the right investigation model. Therefore, in this chapter, we review the DFRWS and the CFIP models as they share many common stages with other models.

Content Template	
Section Number	2.2
Section Title	**Digital Forensic Research Workshop (DFRWS) model**
Introduction	This section explains the main components of the digital forensic research workshop model.
Content	The first Digital Forensic Research Workshop (DFRWS) states that the digital forensic process consists of six stages (Hassan 2011). T The DFRWS model is shown in Figure 1.  Identification Preservation Collection Examination Analysis Presentation Figure 1: the DFRWS model for digital forensics The DFRWS model contains the following stages (Hassan 2011): 1. **Identification:** This is the first stage in which all potential sources of evidence in the form of information, devices, data location, and key custodians are identified. 2. **Preservation:** This is the phase of preserving all related electronically stored information (ESI) by first protecting the scene of the crime, capturing all necessary pictures of the scene and documenting any necessary information that is related to the evidence. 3. **Collection:** This is the phase of collecting all of the necessary digital information for the investigation by imaging, copying or printing the content of electronic devices from the scene of the crime. After that the electronic devices should be removed from the scene of the crime. 4. **Examination:** This is the phase in which the evidence is tracked and validated, and the deleted or encrypted data are recovered. 5. **Analysis:** This is the phase that can be described as the in-depth systematic search of evidence using well-designed techniques and methodology. Analysis aims at drawing conclusions based on the outputs of the previous phase (examination). 6. **Presentation:** This is the phase in which the results of the analysis phases are reported, and this phase should enable other forensic examiners to reproduce and obtain the same forensic results. A crucial activity that usually accompanies the first five stages is contemporaneous note-taking. This is the detailed documentation of what a digital forensic scientist has done.

Content Template	
Section Number	2.3
Section Title	**Computer Forensic Investigative Process (1984) model**
Introduction	This section lists the components of the Computer Forensic Investigative Process (1984) model and defines these components
Content	This is another digital forensic investigation model Pollitt (M. M. Pollitt 1995)(Pollitt 2007). The terminology used in this model is more abstract than the previous model. This model is shown in figure 2.  Figure 2: The Computer Forensic Investigative Process (1984) The sub-stages of the model describe the process of obtaining, preserving and presenting electronic evidence and can be summarized as follows (M. M. Pollitt 1995)(Pollitt 2007): 1- Acquisition is the phase of collecting electronic data. The Acquisition phase demands that evidence should be acquired in an acceptable format with the appropriate approval of the authorities. 2- The Identification phase includes the tasks to determine and find the electronic components from the acquired evidence. Note that this stage is a little different from the identification stage in the DFRWS model. 3- The Evaluation phase includes the tasks to determine whether the electronic components found in the previous phase can become legitimate evidence. 4- The Admission phase also known as the presentation phase, the acquired and extracted evidence is presented in the court.

Content Template	
Section Number	2.4
Section Title	**Details of digital forensic stages**
Introduction	This section explains the stages of the digital forensic process. The section shows the differences between all stages and outlines the guidelines for the investigators
Content	In this section, we discuss the most common stages in the DFRWS and the CFIP models and show how a digital forensic investigator or scientist can accurately follow the process. **2.4.1 Identification** This is the first stage in the digital forensic process DFRWS model that should take place before any digital forensic examination begins. This stage is very similar to the acquisition stage in the CFIP model. Identification is the task performed by an investigator to search, detect, and document digital evidence (Daniel, Larry E. and Daniel 2012). During this phase, the digital evidence first responder (DEFR) must investigate all devices found at the crime scene including those actually used in the crime and those devices that may seem irrelevant in the beginning (Daniel, Larry E. and Daniel 2012). In this stage, the key players and custodians should be determined. Also, the investigator should identify the best sources of electronic evidence. This information should be collected for the following reasons (Sammons 2014): 1- any essential evidence that might affect a case must not be missed 2- the scope of the case can be modified according to the actual needs 3- the investigation costs should be estimated in advance and future sources of evidence should have a low impact on the cost. Example of Identification tasks includes the act of seizing a computer found in the crime scene and taking custody of a computer. The other task can be about making a forensic copy of hard drives. Making forensic copies of evidence is referred to as "acquiring" instead of copying in the digital forensic field. Because the word copy does not mean that the it was made in a forensically sound manner (Daniel, Larry E. and Daniel 2012). During the identification, there is a high possibility that evidence is damaged or destroyed. For example, turning on a computer can modify hundreds of evidentiary items, such as files, date, time, and Internet history. It can also destroy files that could be recovered from the computer hard drive (Daniel, Larry E. and Daniel 2012). The identification stage consists of several sub-stages that are interviewing, identifying, revising and measuring twice and all of these must be documented as shown in figure 3.

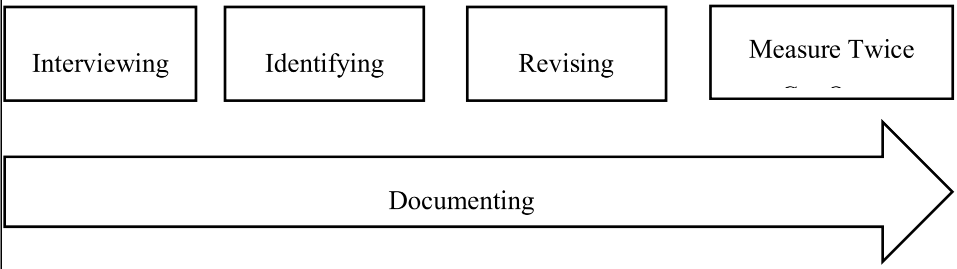


Figure 3: timeline of the identification sub-stages

Interviewing

The interview is the first step in the identification stage. Interviews are very important for the success of a digital forensic examination. Once all relevant devices necessary to collect data are determined, the next step will be interviewing all of the following: (Sammons 2014; Widup 2014):

1. Custodians
2. Site administrators
3. Other users.

Identifying

Here, the digital forensic scientist needs to focus on the important tasks including (Sammons 2014; Widup 2014):

1. obtaining legal authorization for making a search
2. contacting administrators for identifying devices and custodians
3. determining the number and the type of all involved devices including flash drives, scanners, printers, microphones and memory cards
4. determining the types of electronically stored information (ESI), such as photographs, files, documents, emails, spreadsheets, text messages, databases et cetera.
5. determining who is the source of ESI and the way of transferring the ESI, for example, email addresses and IP addresses.
6. determining the storage media of information, such as offsite location, backup media, cloud, or remote locations
7. determining if there are devices involved with remote login capabilities
8. determining the types of the different operating systems
9. determining whether all devices require continuous electric power

Documenting

In this sub-stage, the digital forensic scientist needs to document the following (Daniel, Larry E. and Daniel 2012):

- information related to interviews, such as the names and titles of individuals
- information related to the number and types of devices found during the collection
- information related to the locations from which peripheral devices were found in or removed from
- information related to the form of network in the scene
- information related to the file types involved
- information related to any off-site and remote storage
- information related to the different types of software

Revising

The digital forensic scientist may find that additional electronic evidence that is not included in the original plan needs to be collected. If this occurs, the digital forensic scientist needs to obtain a legal warrant, if necessary, and then an amended consent form, or make other changes to the original scope of the task.

Measure Twice, Cut Once

Every digital forensic case has a scope and cannot include everything because of the limited time and budget. Therefore digital evidence needs to be examined with respect to the scope of the case. At the very beginning of the investigation, the digital forensic scientist needs to accurately set the right scope of the case, make a specific list of the needed digital evidence. Otherwise, the time and the costs of the investigation will be very large and will not be affordable by the organization (Hassan 2011).

2.4.2 Preservation

Preservation is the phase in which a chain of custody is created from the time the case begins to the end when evidence is returned back to the owner or destroyed (Daniel, Larry E. and Daniel 2012). Preservation is also known as the protection of digital evidence exactly as it was found in the scene without any modification or change so that it can be analyzed later. This is because evidence can only be valid if the custody chain is kept without any change and without any break (Årnes 2017). Also, the chain of custody log should include each instance related to any piece of evidence, including the device containing the evidence, the transport of evidence, the storage of evidence, and the time when the evidence is examined or checked by forensic examiners or others (Daniel, Larry E. and Daniel 2012).

In real life, relevant data can be lost due to the continuous use of devices. For example, employees can leave a company and their computers remain in use. After several months, it will be too late to preserve their computer if a crime took place in that company. Preserving a former employee’s electronic devices can thus be considered business best practice (Daniel, Larry E. and Daniel 2012).

2.4.3 Collection

In this phase, devices and duplication of an exact copy of the original electronically stored information (ESI) is collected for preserving digital evidence (Daniel, Larry E. and Daniel 2012). The forensic collection of data can involve the process of switching off electronic devices and sending them to a forensic team. This is called *Dead box forensic collection* which collects data from the devices after they were turned off and is an important part of the digital forensic process (Daniel, Larry E. and Daniel 2012). Turning off the device or isolating ESI should be done in a way that will not change evidence. However, in certain cases this may cause the loss of valuable evidence.

Emerging technology now allows for *live box forensic collection* or simply a *live collection* which is the collection of data from an active device before switching it off. The live collection is important because forensic examiners may never have another chance to collect valuable evidence if that device is switched off (Daniel, Larry E. and Daniel 2012).

Forensic collection includes the following (Årnes 2017; Daniel, Larry E. and Daniel 2012):

1- Photographing the evidence before the collection or duplication
2- Identifying information related to devices, such as serial numbers and manufacturer
3- Putting tags on every collected item for tracking
4- Placing tamper-proof tape over power outlets, CD-ROM drives, USB ports, and floppy disk trays
5- Putting each item in a bag or a secure container that is sealed with tamper-proof tape
6- Placing each collected item in secure areas.
7- Recording any evidence that is released or destroyed in the chain of custody

Locations of electronic evidence

Here is a non-exhaustive list of typical devices that need to be collected as a digital evidence (Daniel, Larry E. and Daniel 2012; Widup 2014):

- Desktops and Laptops
- Smartphones and Tablets
- External hard drives
- Flash memory drives
- Camera cards
- Backup Tapes and Servers, RAIDs
- Surveillance systems
- GPS devices and units
- MP3 music players
- Computer and online game stations.

Forensic examiners must never underestimate the importance of any electronic device. Further, Forensic examiners need to cope with new technology as new forensic ESI can be found in these new devices such as automatic electronic defibrillators, voice recorders, Internet of things (IoT) and vehicles.

Preparing devices for data collection

Some considerations need to be taken before the collection starts (Daniel, Larry E. and Daniel 2012; Sammons 2014; Widup 2014). If devices are already switched off, forensic examiners **must not turn them on**. Forensic examiners should follow the following steps for forensically and proper data collection:

1. Determining whether a device is on or off by looking for lights, listening for sounds, feeling for vibrations and heat. A laptop, smartphone, or tablet may be in sleep mode. If the device is a laptop or desktop, the mouse should be moved without clicking any buttons. If the smartphone or tablet's screen is greasy or dirty, the home button should be pressed or the screen should be swiped.
2. If the device is on, the forensic examiners needs to check if the device is locked, if the user interface is accessible, if the device is encrypted and the password is known, and if the battery is charged.

3. If a laptop, smartphone, or tablet or is on, the airplane mode should be activated
4. The forensic examiners should record device model numbers, serial numbers and passcodes
5. The forensic examiners should take pictures and start a chain of custody document
6. If a device *must* be switched off to preserve ESI, the forensic examiners should switch the device off properly using the "shut down" command
7. If the forensic examiners suspect destructive programs, such as formatting, deleting, removing or altering data, is running, he should switch off the device immediately and remove the plug
8. The forensic examiners should check for any removable media such as CDs/DVDs, SD cards, flash drives, and Sticky notes.

Once a device is switched off, it should be transferred to a lab for the purpose of acquisition and analysis. The forensic examiners should package all components and label all devices. The forensic examiners should put the device in an anti-static bag and tightly secure it in a box. The forensic examiners should keep the evidence away from magnets, moisture, and extreme temperature.

2.4.4 Analysis

Forensic digital analysis is the phase in which the in-depth search and examination of electronically stored information (ESI) take place (Daniel, Larry E. and Daniel 2012). The main purpose of analysis is identifying information that can support or undermine the case in a civil or criminal court (Daniel, Larry E. and Daniel 2012). Thus, analysis is the phase of locating and collecting evidence from the collected items for any specific and unique case.

The outcome of the examinations and investigations is largely influenced by the analysis quality which requires high individual skills, the appropriate tools, and the training of the forensic examiners (Daniel, Larry E. and Daniel 2012). The training of the forensic examiners can have a great impact on the success of the examination particularly because evidence has many forms and comes from different locations and devices. Here, a computer expert must be distinguished from the forensic expert. The computer expert understands many aspects of computer usage and data while a trained forensic expert has good knowledge in recovering data as well as in the appropriate examination techniques (Daniel, Larry E. and Daniel 2012).

Analysis of digital evidence is not only determining if a file or e-mail message can be found in a hard drive. But also, it includes outlining how that file or message reached the hard drive, who put that file or message on that hard drive (Daniel, Larry E. and Daniel 2012). The best legal outcome is usually obtained by analyzing a forensic image or copy of the collected device as opposed to the source or the original device.

The scope of analysis is about identifying the key players and location of the electronically stored evidence. The scope is about: Who, When, What, Where and Why as the main questions in the examination (Sammons 2014). The initial scope should be identified clearly although this is not possible at all times.

Analysis may have limitations due to privacy, conflicting or opposing interests. In cases involving opposing interest, a court may limit the scope of information to be analyzed or even collected. The digital forensic analyst should be informed about these limitations to ensure that the limitations are possible to be handle particularly in considering how the ESI is stored and how forensic software processes the data (Daniel, Larry E. and Daniel 2012).

2.4.5 Presentation

Presentation is the last phase in which the examiner's findings as forensic evidence is reported and presented to court (Årnes 2017; Daniel, Larry E. and Daniel 2012; Hassan 2011). The presentation includes a formal report on the identification of all related information. It also includes depositions of experts, the creation of affidavits, and court testimony. Ultimately, the report and all related information will be viewed by executives, lawyers, law enforcement, judges and juries. Therefore, the report should be concise and clear, and must contain sufficient details for describing a defensible process (Daniel, Larry E. and Daniel 2012).

A well written report should include the collection methods used, the steps taken to preserve the evidence, and how the evidence was verified (Daniel, Larry E. and Daniel 2012). Objective findings are the most important rule in writing a report. Although examiners can give opinions or examples when necessary, any conjecture should be clearly identified. A well-organized report should present digital analysis and evidence and can contain (Daniel, Larry E. and Daniel 2012):

1- Executive Summary
2- Findings
3- Appended Reports
4- Conclusion

While the content of a digital forensics report should include the following (Daniel, Larry E. and Daniel 2012):

1- Examiner background and experience
2- Examination tools
3- Methods used to verify, recover and extract the data
4- the examiners findings
5- Actual data recovered that can support the examiner findings.

Content Template	
Section Number	2.5
Section Title	**Acquisition best practices**
Introduction	This section shows the best practice in acquisition and what investigators need to know and perform to obtain appropriate evidence.
Content	The main task of the digital forensic scientists and investigators is to collect digital evidence so that they can present it in the court and assist in determining the result of the case. Digital evidence is a form of electronic data, either it is a transaction, a document, or media such as an audio or video recording [1]. Transactions can include financial records created during purchasing an item, paying a bill, writing a check, and withdrawing or depositing money. Nowadays, almost every transaction in our daily life is kept in electronic format and becomes digital evidence [3]. Several examples can be found in our life, such as doctor visits, getting medical prescriptions, marriage certificates, registering a new born child and purchasing or selling houses. Digital evidence requires three basic elements that are necessary during the collection [1]: 4- Source: the artifacts and the metadata that can show where the information came from. For example, embedded watermarks in some images can identify its origination or authenticity. Source is important forensic information that can make or terminate a case. 5- Format: Evidence must be stored in its original format and digital forensic investigator should utilize all available tools to maintain the format of the evidence. 6- Type: evidence can have different types, such as email, documents, spreadsheets, text message et cetera. Electronic data can become digital evidence if they are stored in a place that is ultimately accessible. The data must also be recoverable by a forensic investigator. Nowadays, the big challenge is not related only to finding the digital evidence, but also to storing the evidence, getting access to that storage, and the ability to recover that evidence for a civil or criminal action.

Activity Template	
Number	2.1
Title	Determine the input and the output of the six phases in the DFRWS model? You can imagine a scenario of a digital crime, try to investigate the crime, collect the evidence and report the evidence to the court in a legally sound matter.
Type	• Research
Aim	To understand the digital forensic process that is related to the collection of evidence, preservation, analysis and presentation to a court of law
Description	Each student needs to write an article about the input and the output of each phase and each student must link the output to the evidence.
Timeline	Two weeks
Assessment	Students need to produce an article of at least three pages. The main elements in the article are: 4- The input and the output of each phase of the digital forensic process 5- The ability to analyze the data 6- The final presentation of the evidence

Think Template (MCQs)	
Number	2.1
Title	introduction
Type	- Choose correct answer
Question	The digital forensic process models are limited to seven
Answers	3- True **4- False**

Think Template (MCQs)	
Number	2.2
Title	**Digital Forensic Research Workshop (DFRWS) model**
Type	Choose correct answer
Question	The phase in which all electronic evidence can be validated and finally prepared for the court is:
Answers	Preservation Collection **Analysis** Presentation

Think Template (MCQs)	
Number	2.4
Title	**Detail of digital forensics stages**
Type	Choose correct answer
Question	Seizing a computer that is found in the crime scene is from:
Answers	The identification phase The presentation phase Examination phase Preservation phase

Think Template (MCQs)	
Number	2.4
Title	**Detailed of digital forensics stages**
Type	Choose correct answer
Question	The scope of the case can be changed
Answers	**True** False

Think Template (MCQs)	
Number	2.4
Title	**Detailed of digital forensics stages**
Type	Choose correct answer
Question	Documenting all events from the crime scene should start in the preservation phase
Answers	True **False**

Think Template (MCQs)	
Number	2.4
Title	**Detailed of digital forensics stages**
Type	Choose correct answer
Question	Evidence is presented to the court in the form of a report that may contain the software and the hardware
Answers	**True** False

Think Template (MCQs)	
Number	2.45
Title	**2.5 Acquisition best practices**
Type	• Choose correct answer
Question	Using a USB cable to transfer data from the original evidence to the copy machine directly is a:
Answers	Forensic method **Non forensic method** Semi-forensic method

Extra Template	
Number	2.1
Title	*Digital Forensics*
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	Årnes, André. 2017. *Digital Forensics*. 1st ed. Wiley.

Extra Template	
Number	2.2
Title	*Digital Forensics for Legal Professionals*
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	Daniel, Larry E. and Daniel, Lars E. 2012. *Digital Forensics for Legal Professionals*. 1st ed. Elsevier Inc.

Extra Template	
Number	2.3
Title	Common Phases of Computer Forensics Investigation Models
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	Hassan, Yunus Yusoff and Roslan Ismail and Zainuddin. 2011. “Common phases of computer forensics investigation models.” *International Journal of Computer Science & Information Technology* 3(3).

Extra Template	
Number	2.4
Title	Computer Forensics: An Approach to Evidence in Cyberspace
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	M. M. Pollitt. 1995. "Computer Forensics: An Approach to Evidence in Cyberspace." Pp. 487–91 in *the National Information Systems Security Conference*. Baltimore,.

Extra Template	
Number	2.5
Title	An Ad Hoc Review of Digital Forensic Models
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	Pollitt, Mark M. 2007. "An Ad Hoc Review of Digital Forensic Models." Pp. 43–52 in *Proceedings - SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering*. Washington,.

Extra Template	
Number	2.6
Title	*The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	Sammons, John. 2014. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. edited by Syngress.

Extra Template	
Number	2.7
Title	*Computer Forensics and Digital Investigation with EnCase Forensic V7*
Topic	2.1, 2.2, 2.3, 2.4, 2.5
Type	Widup, Suzanne. 2014. *Computer Forensics and Digital Investigation with EnCase Forensic V7*. 1st ed. McGraw-Hill Education.

3. Digital Forensics in the Legal System

Scope Template	
Number	3
Title	**Digital Forensics in the Legal System**
Introduction	This chapter discusses the ways of using digital forensics evidence in legal matters. The chapter shows how the evidence is used in civil and criminal trials during all stages including the pre-trial and post-trial phases.
Outcomes	5- To know how the digital evidence is used in court
Topics	6- Introduction 7- Mitigation 8- Pre-Trial Motions 9- Trial preparation 10- Example Trial Questions 11- Trial Phase
Study Guide	

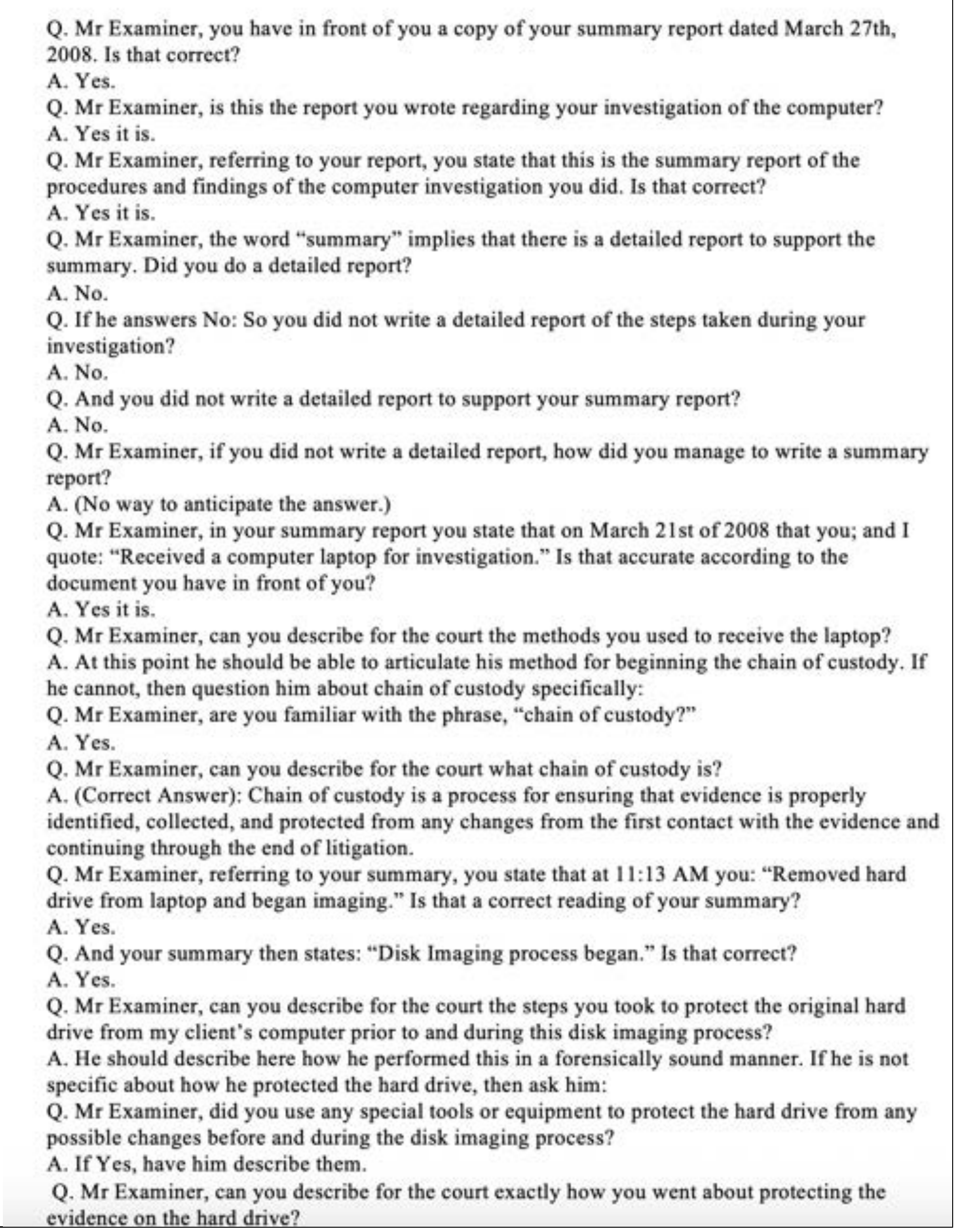
Content Template	
Section Number	3.1
Section Title	Introduction
Introduction	This section is an introduction to the chapter and gives the outline of the chapter.
Content	This chapter discusses the ways of using digital forensics evidence in legal matters. The chapter shows how the evidence is used in civil and criminal trials during all stages including the pre-trial and post-trial phases. The chapter also shows the role of the digital forensic investigator. Forensic examinations are important because they can sometimes cause changes to the case even without going to the trial, for example, charges may be dropped, sentences may be reduced, and civil matters may be settled. Digital forensics investigators therefore play an important role during the case because they present useful evidence and they can assist attorneys in preparing the examination and the analysis of opposing experts. This chapter begins by explaining mitigation, and then the pre-trial motions. The chapter gives examples of questions that are asked during the pre-trial and trial for civil and crime cases.

Content Template	
Section Number	3.2
Section Title	Mitigation
Introduction	This section explains what is meant by *mitigation* in digital forensics and shows an important case study to let student understand the importance of evidence in any digital forensic case
Content	The mitigation refers to using the evidence for pre-sentencing hearings [1]. So, the investigator role is to perform forensic examinations for the purpose of mitigation purposes. in mitigation, the pre-sentencing digital forensic examination can reveal several mitigating factors which may change the sentence of a client [2]. **Case study: Pre-sentence mitigation in an internet predator case** [1] This is an example of mitigation used in real life. The client in this case was a man who was 64 years old and was charged in federal court for illegal transactions. The sentence of the court was 25 years. Part of the illegal transactions was using the Internet for child pornography. Three images of pornography were found on his computer and these images where used for sentence enhancement. The defendant claimed that someone had offered to provide him with an underage girl while he was chatting with others on the Internet. Based on that claim, the judge had offered to reduce the sentence if the evidence of that chat could be found. A digital forensics expert was brought in by the defense attorney to check if the claims made by both sides could be verified. After the digital forensics expert had examined the computer, three of the four images were not related to child pornography. It was also found that the other image which could be child pornography had been placed on the man's computer through the Microsoft Messenger Service. The Microsoft Messenger Service used to be in the Windows 98 operating system and ran on startup as a service. This service was automatic and was not controlled by the computer user. Receiving spam messages through this service, including files, was very common among the messenger users. The digital forensic expert also found that the images were placed on the man's computer four years before the sentence and the man had never opened these images. Regarding the claim that the man was offered the provision of an underage girl, the expert was able to find and reconstruct the Yahoo chat logs on the computer hard drive. This allowed the expert to present the chat text in which the offer had been made. The expert was able to find also the city and telephone number of the person who made that offer. Based on the digital forensic evidence provided to law enforcement, the sentence of the client was reduced from 25 years to 14 years as the child pornography was eliminated from his case.

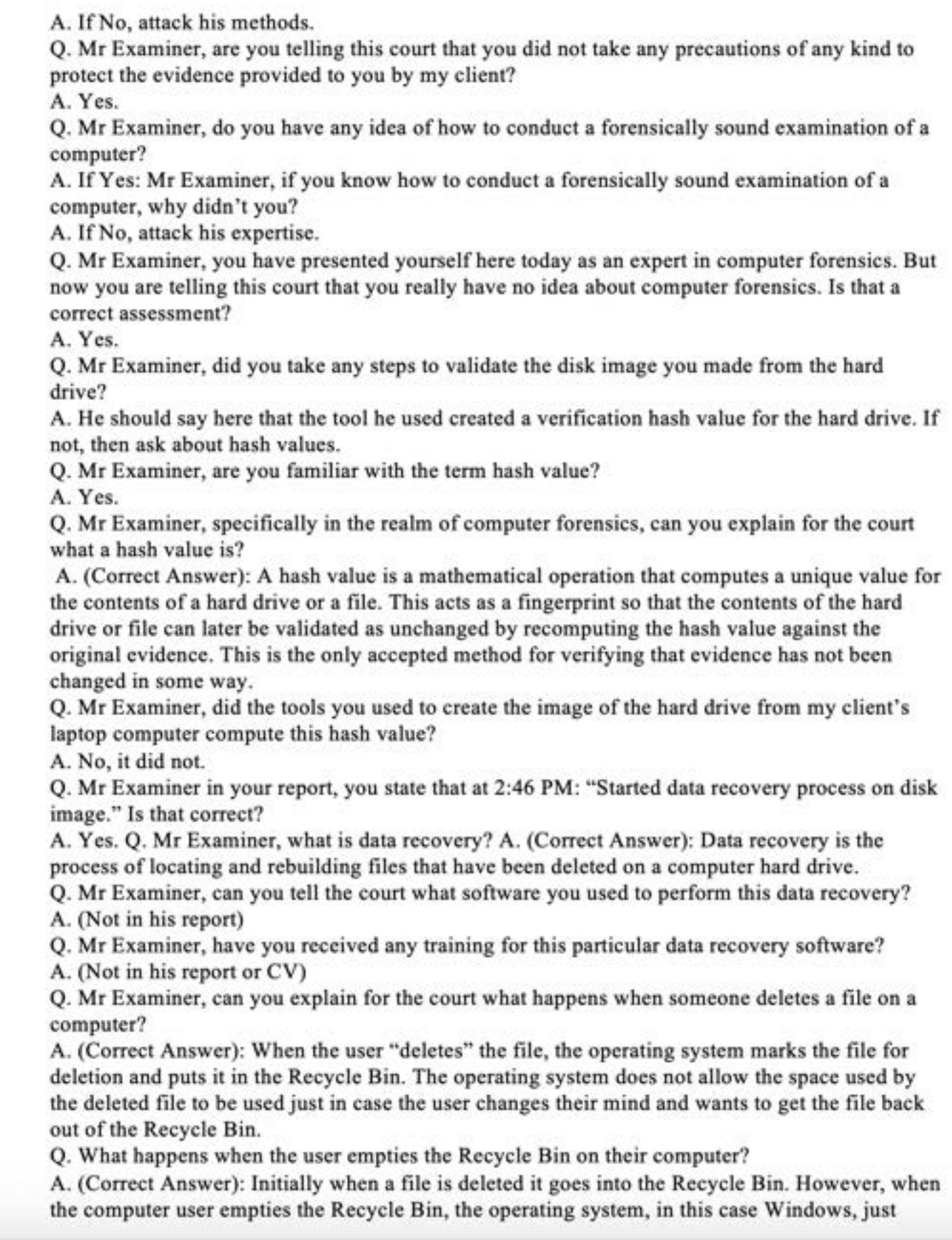
Content Template	
Section Number	3.3
Section Title	**Pre-Trial Motions**
Introduction	This section explains the duties of digital forensic experts in the pre-trial phase.
Content	Digital forensics experts can significantly assist attorneys during the pre-trial phase. This assistance includes: testifying in the opposition or the support of motions, discovery or spoliation of compliance motions, and motions to dismiss civil actions [1][3]. The digital forensic expert can definitively assist with the technical issues and provide evidence in support of the motion. During the pre-trial motion, the digital forensic expert can also testify in hearings for the support of the evidence at a specific issue. Once an attorney decides to seek the help from the digital forensic expert, the expert can also help during the preparation for the trial by providing questions for the attorney to use for the examination of the opposing expert. That can be possible if the attorney has got the report of the opposing expert and the findings of the engaged expert.

Content Template	
Section Number	3.4
Section Title	**Trial preparation**
Introduction	This section gives what is needed for the trial phase
Content	The preparation for the trial includes different acts from the digital forensic expert. The first act is related to the questions set that will assist in identifying the facts that clarify the issues at hand for the jury [1], [4]. The other act is to anticipate the testimony made by the opposing expert and to prepare for rebuttal testimony. The expert needs to help the attorney to predict the opposing expert response to the questions and prepare a reply to each response. The digital forensic expert is recommended to be at the table to listen to the testimony and provides the attorney with new questions according to the expert's responses. However, the expert can only be at the table if in the case the judge, and the jurisdiction allow for that. If the expert cannot be at the table, he can take notes and pass the notes to the attorney once it is allowed.

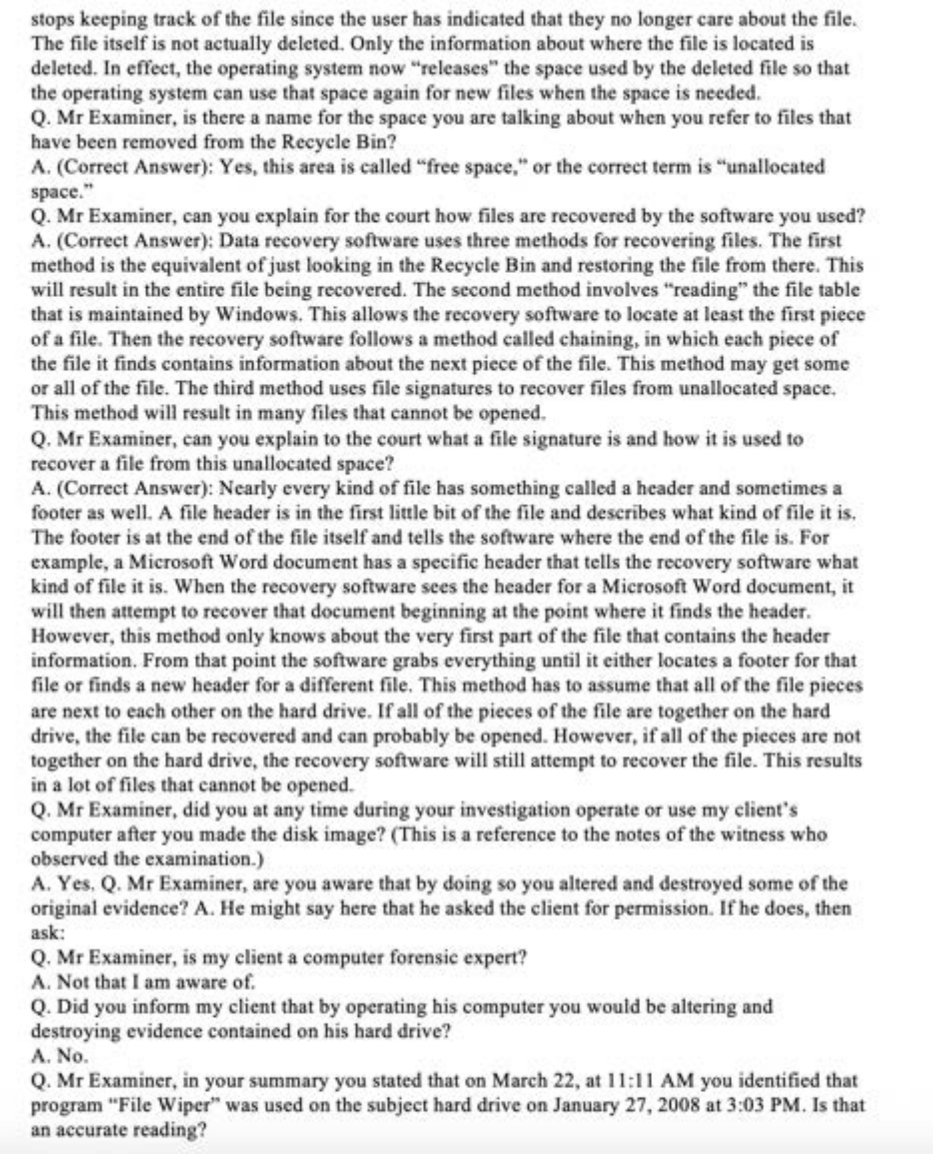
Content Template	
Section Number	3.5
Section Title	**Example Trial Questions**
Introduction	In this section, two example question sets; The first one is for a civil hearing and the second one is for a criminal trial.
Content	These example question sets shown in Figure 1 and Figure 2 are taken from the source [1] and are designed to be part of trial preparation. In this section, two example question sets; The first one is for a civil hearing and the second one is for a criminal trial. These examples are from real-world cases and the opposing expert is called Mr Examiner. **3.5.1 A civil case example** In this example, the client was accused of destroying evidence by using a file destruction software program. This question set shown in Figure 1 was used at a court hearing to question the plaintiff's expert on his investigations of the defendant's computer. The court has issued a preservation order previously for this case. The main issue was the discovery of the file destruction program. The plaintiff's contention was that [1]: *"Not all responsive discovery documents were produced and that the file destruction program was used as a method by the defendant to destroy evidence."* The defendant's claim was that [1]: *"The file destruction program was used only to remove sensitive information in the normal course of business and had been removed from the computer immediately after the issue of the preservation order."*

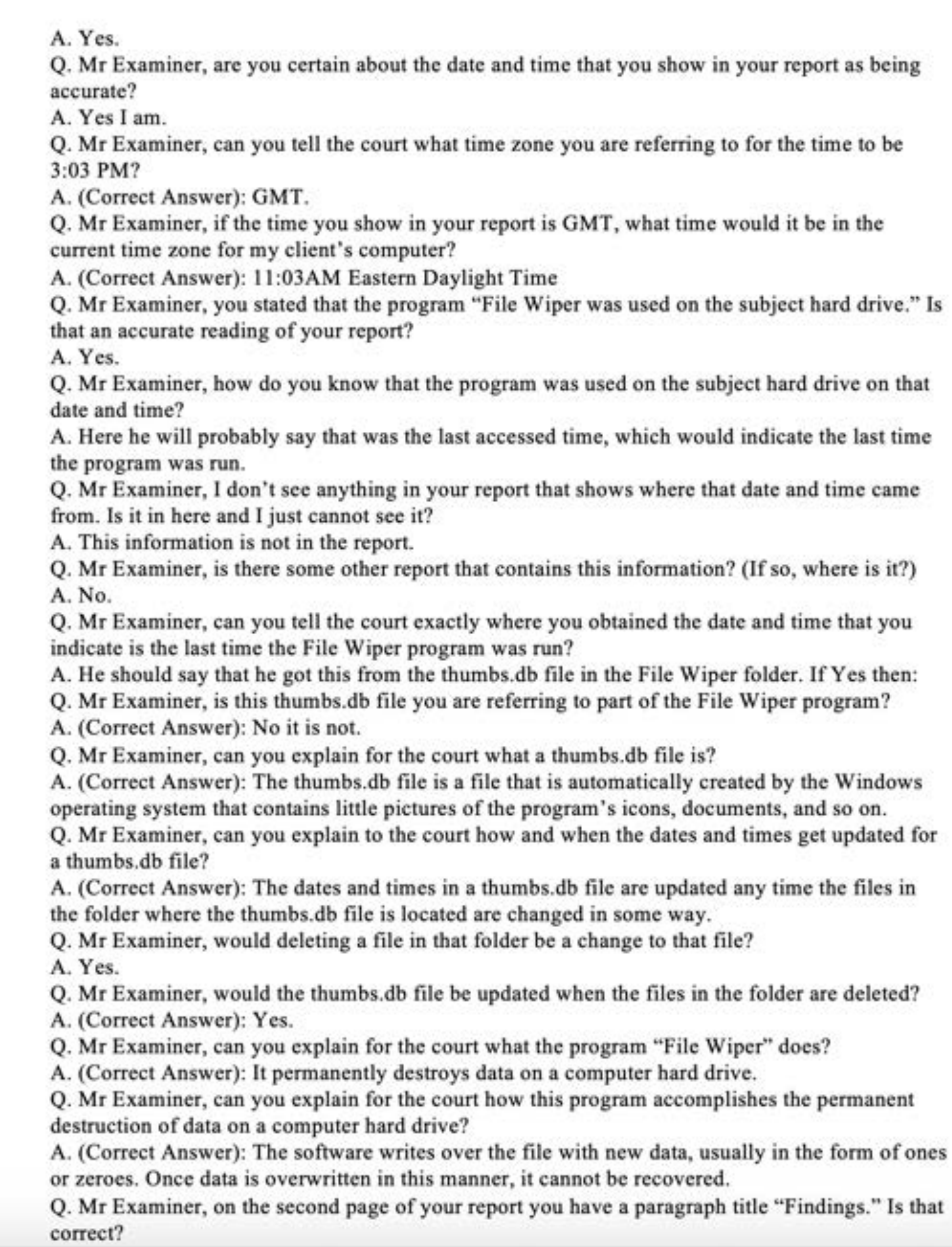


Q. Mr Examiner, you have in front of you a copy of your summary report dated March 27th, 2008. Is that correct?
A. Yes.
Q. Mr Examiner, is this the report you wrote regarding your investigation of the computer?
A. Yes it is.
Q. Mr Examiner, referring to your report, you state that this is the summary report of the procedures and findings of the computer investigation you did. Is that correct?
A. Yes it is.
Q. Mr Examiner, the word "summary" implies that there is a detailed report to support the summary. Did you do a detailed report?
A. No.
Q. If he answers No: So you did not write a detailed report of the steps taken during your investigation?
A. No.
Q. And you did not write a detailed report to support your summary report?
A. No.
Q. Mr Examiner, if you did not write a detailed report, how did you manage to write a summary report?
A. (No way to anticipate the answer.)
Q. Mr Examiner, in your summary report you state that on March 21st of 2008 that you; and I quote: "Received a computer laptop for investigation." Is that accurate according to the document you have in front of you?
A. Yes it is.
Q. Mr Examiner, can you describe for the court the methods you used to receive the laptop?
A. At this point he should be able to articulate his method for beginning the chain of custody. If he cannot, then question him about chain of custody specifically:
Q. Mr Examiner, are you familiar with the phrase, "chain of custody?"
A. Yes.
Q. Mr Examiner, can you describe for the court what chain of custody is?
A. (Correct Answer): Chain of custody is a process for ensuring that evidence is properly identified, collected, and protected from any changes from the first contact with the evidence and continuing through the end of litigation.
Q. Mr Examiner, referring to your summary, you state that at 11:13 AM you: "Removed hard drive from laptop and began imaging." Is that a correct reading of your summary?
A. Yes.
Q. And your summary then states: "Disk Imaging process began." Is that correct?
A. Yes.
Q. Mr Examiner, can you describe for the court the steps you took to protect the original hard drive from my client's computer prior to and during this disk imaging process?
A. He should describe here how he performed this in a forensically sound manner. If he is not specific about how he protected the hard drive, then ask him:
Q. Mr Examiner, did you use any special tools or equipment to protect the hard drive from any possible changes before and during the disk imaging process?
A. If Yes, have him describe them.
Q. Mr Examiner, can you describe for the court exactly how you went about protecting the evidence on the hard drive?



A. If No, attack his methods.
Q. Mr Examiner, are you telling this court that you did not take any precautions of any kind to protect the evidence provided to you by my client?
A. Yes.
Q. Mr Examiner, do you have any idea of how to conduct a forensically sound examination of a computer?
A. If Yes: Mr Examiner, if you know how to conduct a forensically sound examination of a computer, why didn't you?
A. If No, attack his expertise.
Q. Mr Examiner, you have presented yourself here today as an expert in computer forensics. But now you are telling this court that you really have no idea about computer forensics. Is that a correct assessment?
A. Yes.
Q. Mr Examiner, did you take any steps to validate the disk image you made from the hard drive?
A. He should say here that the tool he used created a verification hash value for the hard drive. If not, then ask about hash values.
Q. Mr Examiner, are you familiar with the term hash value?
A. Yes.
Q. Mr Examiner, specifically in the realm of computer forensics, can you explain for the court what a hash value is?
A. (Correct Answer): A hash value is a mathematical operation that computes a unique value for the contents of a hard drive or a file. This acts as a fingerprint so that the contents of the hard drive or file can later be validated as unchanged by recomputing the hash value against the original evidence. This is the only accepted method for verifying that evidence has not been changed in some way.
Q. Mr Examiner, did the tools you used to create the image of the hard drive from my client's laptop computer compute this hash value?
A. No, it did not.
Q. Mr Examiner in your report, you state that at 2:46 PM: "Started data recovery process on disk image." Is that correct?
A. Yes. Q. Mr Examiner, what is data recovery? A. (Correct Answer): Data recovery is the process of locating and rebuilding files that have been deleted on a computer hard drive.
Q. Mr Examiner, can you tell the court what software you used to perform this data recovery?
A. (Not in his report)
Q. Mr Examiner, have you received any training for this particular data recovery software?
A. (Not in his report or CV)
Q. Mr Examiner, can you explain for the court what happens when someone deletes a file on a computer?
A. (Correct Answer): When the user "deletes" the file, the operating system marks the file for deletion and puts it in the Recycle Bin. The operating system does not allow the space used by the deleted file to be used just in case the user changes their mind and wants to get the file back out of the Recycle Bin.
Q. What happens when the user empties the Recycle Bin on their computer?
A. (Correct Answer): Initially when a file is deleted it goes into the Recycle Bin. However, when the computer user empties the Recycle Bin, the operating system, in this case Windows, just

	 stops keeping track of the file since the user has indicated that they no longer care about the file. The file itself is not actually deleted. Only the information about where the file is located is deleted. In effect, the operating system now "releases" the space used by the deleted file so that the operating system can use that space again for new files when the space is needed. Q. Mr Examiner, is there a name for the space you are talking about when you refer to files that have been removed from the Recycle Bin? A. (Correct Answer): Yes, this area is called "free space," or the correct term is "unallocated space." Q. Mr Examiner, can you explain for the court how files are recovered by the software you used? A. (Correct Answer): Data recovery software uses three methods for recovering files. The first method is the equivalent of just looking in the Recycle Bin and restoring the file from there. This will result in the entire file being recovered. The second method involves "reading" the file table that is maintained by Windows. This allows the recovery software to locate at least the first piece of a file. Then the recovery software follows a method called chaining, in which each piece of the file it finds contains information about the next piece of the file. This method may get some or all of the file. The third method uses file signatures to recover files from unallocated space. This method will result in many files that cannot be opened. Q. Mr Examiner, can you explain to the court what a file signature is and how it is used to recover a file from this unallocated space? A. (Correct Answer): Nearly every kind of file has something called a header and sometimes a footer as well. A file header is in the first little bit of the file and describes what kind of file it is. The footer is at the end of the file itself and tells the software where the end of the file is. For example, a Microsoft Word document has a specific header that tells the recovery software what kind of file it is. When the recovery software sees the header for a Microsoft Word document, it will then attempt to recover that document beginning at the point where it finds the header. However, this method only knows about the very first part of the file that contains the header information. From that point the software grabs everything until it either locates a footer for that file or finds a new header for a different file. This method has to assume that all of the file pieces are next to each other on the hard drive. If all of the pieces of the file are together on the hard drive, the file can be recovered and can probably be opened. However, if all of the pieces are not together on the hard drive, the recovery software will still attempt to recover the file. This results in a lot of files that cannot be opened. Q. Mr Examiner, did you at any time during your investigation operate or use my client's computer after you made the disk image? (This is a reference to the notes of the witness who observed the examination.) A. Yes. Q. Mr Examiner, are you aware that by doing so you altered and destroyed some of the original evidence? A. He might say here that he asked the client for permission. If he does, then ask: Q. Mr Examiner, is my client a computer forensic expert? A. Not that I am aware of. Q. Did you inform my client that by operating his computer you would be altering and destroying evidence contained on his hard drive? A. No. Q. Mr Examiner, in your summary you stated that on March 22, at 11:11 AM you identified that program "File Wiper" was used on the subject hard drive on January 27, 2008 at 3:03 PM. Is that an accurate reading?



A. Yes.

Q. Mr Examiner, are you certain about the date and time that you show in your report as being accurate?

A. Yes I am.

Q. Mr Examiner, can you tell the court what time zone you are referring to for the time to be 3:03 PM?

A. (Correct Answer): GMT.

Q. Mr Examiner, if the time you show in your report is GMT, what time would it be in the current time zone for my client's computer?

A. (Correct Answer): 11:03AM Eastern Daylight Time

Q. Mr Examiner, you stated that the program "File Wiper was used on the subject hard drive." Is that an accurate reading of your report?

A. Yes.

Q. Mr Examiner, how do you know that the program was used on the subject hard drive on that date and time?

A. Here he will probably say that was the last accessed time, which would indicate the last time the program was run.

Q. Mr Examiner, I don't see anything in your report that shows where that date and time came from. Is it in here and I just cannot see it?

A. This information is not in the report.

Q. Mr Examiner, is there some other report that contains this information? (If so, where is it?)

A. No.

Q. Mr Examiner, can you tell the court exactly where you obtained the date and time that you indicate is the last time the File Wiper program was run?

A. He should say that he got this from the thumbs.db file in the File Wiper folder. If Yes then:

Q. Mr Examiner, is this thumbs.db file you are referring to part of the File Wiper program?

A. (Correct Answer): No it is not.

Q. Mr Examiner, can you explain for the court what a thumbs.db file is?

A. (Correct Answer): The thumbs.db file is a file that is automatically created by the Windows operating system that contains little pictures of the program's icons, documents, and so on.

Q. Mr Examiner, can you explain to the court how and when the dates and times get updated for a thumbs.db file?

A. (Correct Answer): The dates and times in a thumbs.db file are updated any time the files in the folder where the thumbs.db file is located are changed in some way.

Q. Mr Examiner, would deleting a file in that folder be a change to that file?

A. Yes.

Q. Mr Examiner, would the thumbs.db file be updated when the files in the folder are deleted?

A. (Correct Answer): Yes.

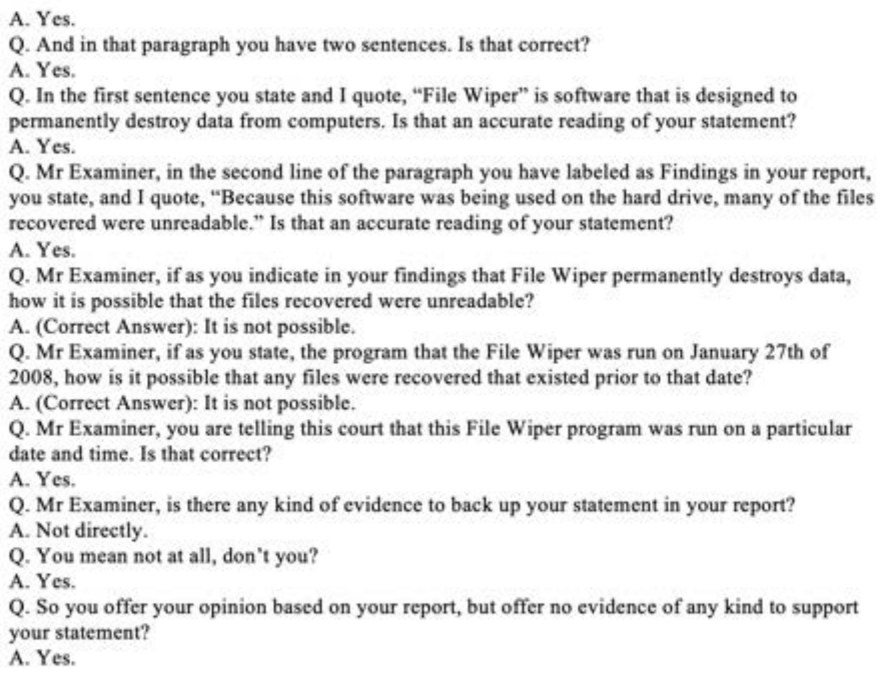
Q. Mr Examiner, can you explain for the court what the program "File Wiper" does?

A. (Correct Answer): It permanently destroys data on a computer hard drive.

Q. Mr Examiner, can you explain for the court how this program accomplishes the permanent destruction of data on a computer hard drive?

A. (Correct Answer): The software writes over the file with new data, usually in the form of ones or zeroes. Once data is overwritten in this manner, it cannot be recovered.

Q. Mr Examiner, on the second page of your report you have a paragraph title "Findings." Is that correct?



A. Yes.
Q. And in that paragraph you have two sentences. Is that correct?
A. Yes.
Q. In the first sentence you state and I quote, "File Wiper" is software that is designed to permanently destroy data from computers. Is that an accurate reading of your statement?
A. Yes.
Q. Mr Examiner, in the second line of the paragraph you have labeled as Findings in your report, you state, and I quote, "Because this software was being used on the hard drive, many of the files recovered were unreadable." Is that an accurate reading of your statement?
A. Yes.
Q. Mr Examiner, if as you indicate in your findings that File Wiper permanently destroys data, how it is possible that the files recovered were unreadable?
A. (Correct Answer): It is not possible.
Q. Mr Examiner, if as you state, the program that the File Wiper was run on January 27th of 2008, how is it possible that any files were recovered that existed prior to that date?
A. (Correct Answer): It is not possible.
Q. Mr Examiner, you are telling this court that this File Wiper program was run on a particular date and time. Is that correct?
A. Yes.
Q. Mr Examiner, is there any kind of evidence to back up your statement in your report?
A. Not directly.
Q. You mean not at all, don't you?
A. Yes.
Q. So you offer your opinion based on your report, but offer no evidence of any kind to support your statement?
A. Yes.

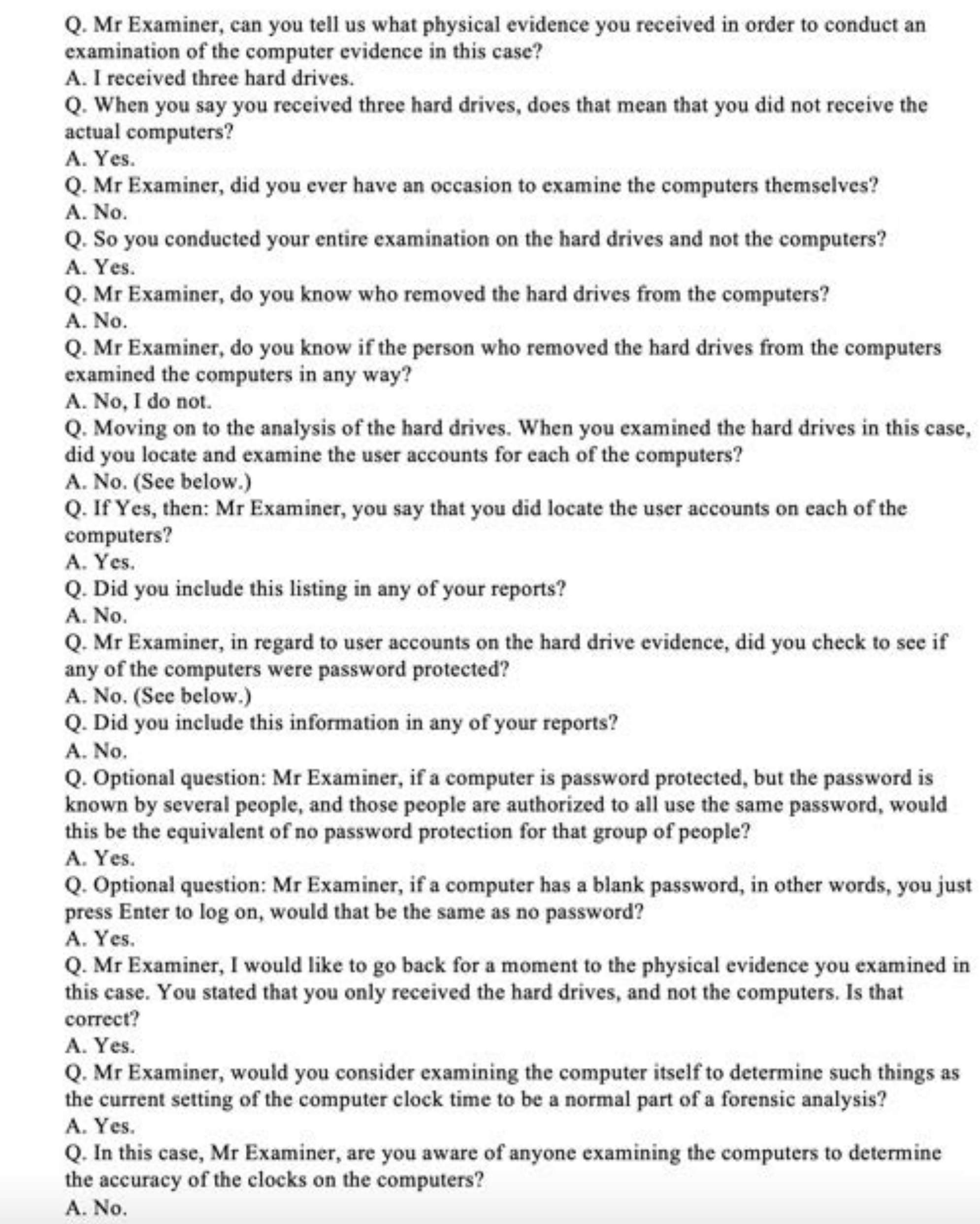
Figure 1: civil case example [1].

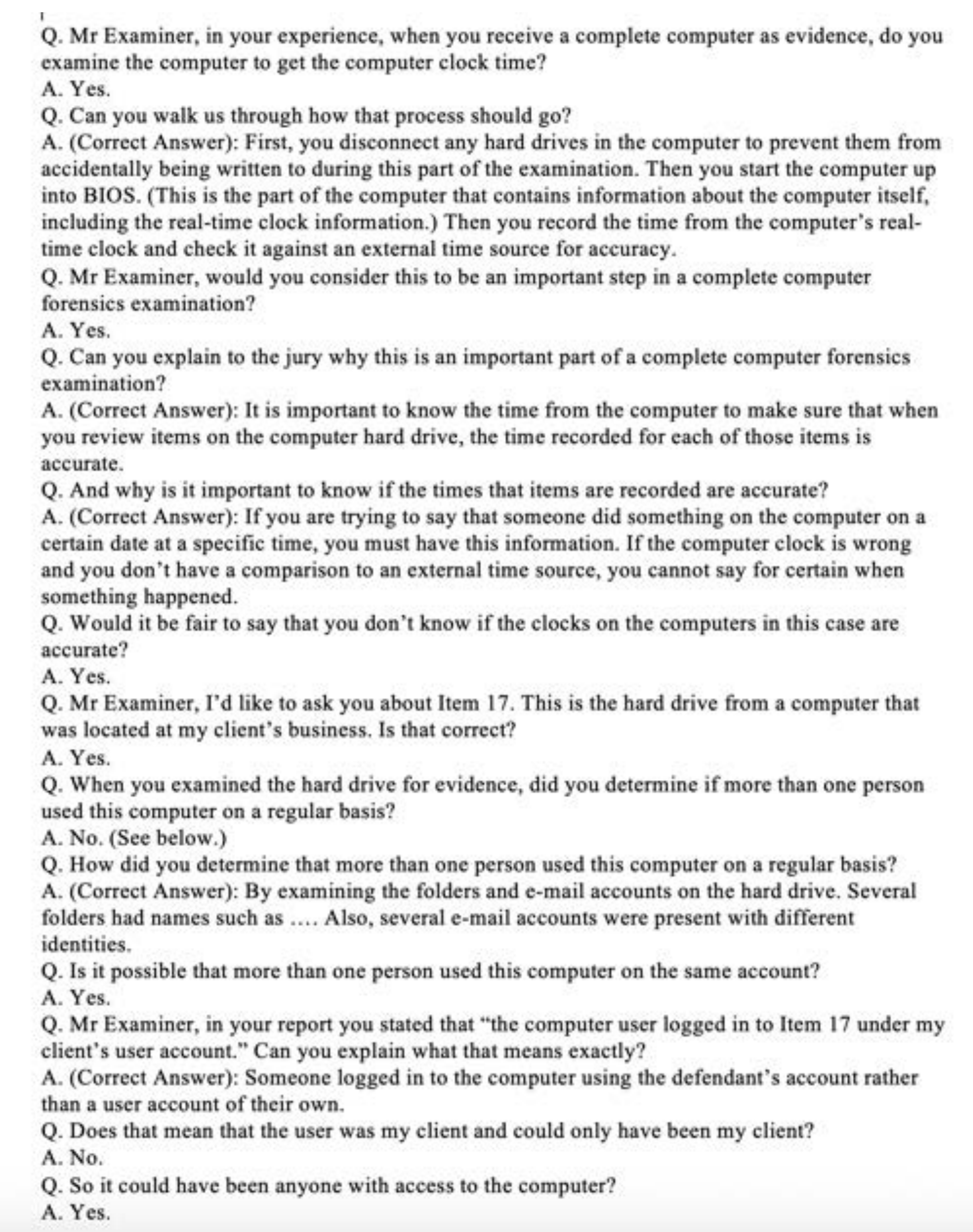
3.4.2 Criminal trial example

Criminal and civil matters share several characteristics and evidence types. The evidence in many criminal cases depends on user attribution and timelines [1][3]. In other words, who was at the computer when the crime happened, and who was given access to the computer? It is also critical for evidence formation to know when for example, someone performed a map search, performed an Internet search, performed online chat, downloaded a file.

When trying to prove that a person performed illegal actions on a computer, the expert needs to find who had accounts and if those accounts were secured using passwords [1]. This is useful to prove that only one person or multiple people could have performed the actions on the computer, such as search, download and chat. Another common issue in many cases is if the computer clock was changed to hide when some actions occurred.

If the forensic expert fails to know the exact time of any act on the computer, the evidence cannot be considered reliable and may be asked to repeat the investigations. The set of questions shown in Figure 2 was prepared for a death penalty trial. At the end and because the case did not go to trial, the defendant received 17 years as part of a plea bargain.

	 Q. Mr Examiner, can you tell us what physical evidence you received in order to conduct an examination of the computer evidence in this case? A. I received three hard drives. Q. When you say you received three hard drives, does that mean that you did not receive the actual computers? A. Yes. Q. Mr Examiner, did you ever have an occasion to examine the computers themselves? A. No. Q. So you conducted your entire examination on the hard drives and not the computers? A. Yes. Q. Mr Examiner, do you know who removed the hard drives from the computers? A. No. Q. Mr Examiner, do you know if the person who removed the hard drives from the computers examined the computers in any way? A. No, I do not. Q. Moving on to the analysis of the hard drives. When you examined the hard drives in this case, did you locate and examine the user accounts for each of the computers? A. No. (See below.) Q. If Yes, then: Mr Examiner, you say that you did locate the user accounts on each of the computers? A. Yes. Q. Did you include this listing in any of your reports? A. No. Q. Mr Examiner, in regard to user accounts on the hard drive evidence, did you check to see if any of the computers were password protected? A. No. (See below.) Q. Did you include this information in any of your reports? A. No. Q. Optional question: Mr Examiner, if a computer is password protected, but the password is known by several people, and those people are authorized to all use the same password, would this be the equivalent of no password protection for that group of people? A. Yes. Q. Optional question: Mr Examiner, if a computer has a blank password, in other words, you just press Enter to log on, would that be the same as no password? A. Yes. Q. Mr Examiner, I would like to go back for a moment to the physical evidence you examined in this case. You stated that you only received the hard drives, and not the computers. Is that correct? A. Yes. Q. Mr Examiner, would you consider examining the computer itself to determine such things as the current setting of the computer clock time to be a normal part of a forensic analysis? A. Yes. Q. In this case, Mr Examiner, are you aware of anyone examining the computers to determine the accuracy of the clocks on the computers? A. No.



Q. Mr Examiner, in your experience, when you receive a complete computer as evidence, do you examine the computer to get the computer clock time?

A. Yes.

Q. Can you walk us through how that process should go?

A. (Correct Answer): First, you disconnect any hard drives in the computer to prevent them from accidentally being written to during this part of the examination. Then you start the computer up into BIOS. (This is the part of the computer that contains information about the computer itself, including the real-time clock information.) Then you record the time from the computer's real-time clock and check it against an external time source for accuracy.

Q. Mr Examiner, would you consider this to be an important step in a complete computer forensics examination?

A. Yes.

Q. Can you explain to the jury why this is an important part of a complete computer forensics examination?

A. (Correct Answer): It is important to know the time from the computer to make sure that when you review items on the computer hard drive, the time recorded for each of those items is accurate.

Q. And why is it important to know if the times that items are recorded are accurate?

A. (Correct Answer): If you are trying to say that someone did something on the computer on a certain date at a specific time, you must have this information. If the computer clock is wrong and you don't have a comparison to an external time source, you cannot say for certain when something happened.

Q. Would it be fair to say that you don't know if the clocks on the computers in this case are accurate?

A. Yes.

Q. Mr Examiner, I'd like to ask you about Item 17. This is the hard drive from a computer that was located at my client's business. Is that correct?

A. Yes.

Q. When you examined the hard drive for evidence, did you determine if more than one person used this computer on a regular basis?

A. No. (See below.)

Q. How did you determine that more than one person used this computer on a regular basis?

A. (Correct Answer): By examining the folders and e-mail accounts on the hard drive. Several folders had names such as …. Also, several e-mail accounts were present with different identities.

Q. Is it possible that more than one person used this computer on the same account?

A. Yes.

Q. Mr Examiner, in your report you stated that "the computer user logged in to Item 17 under my client's user account." Can you explain what that means exactly?

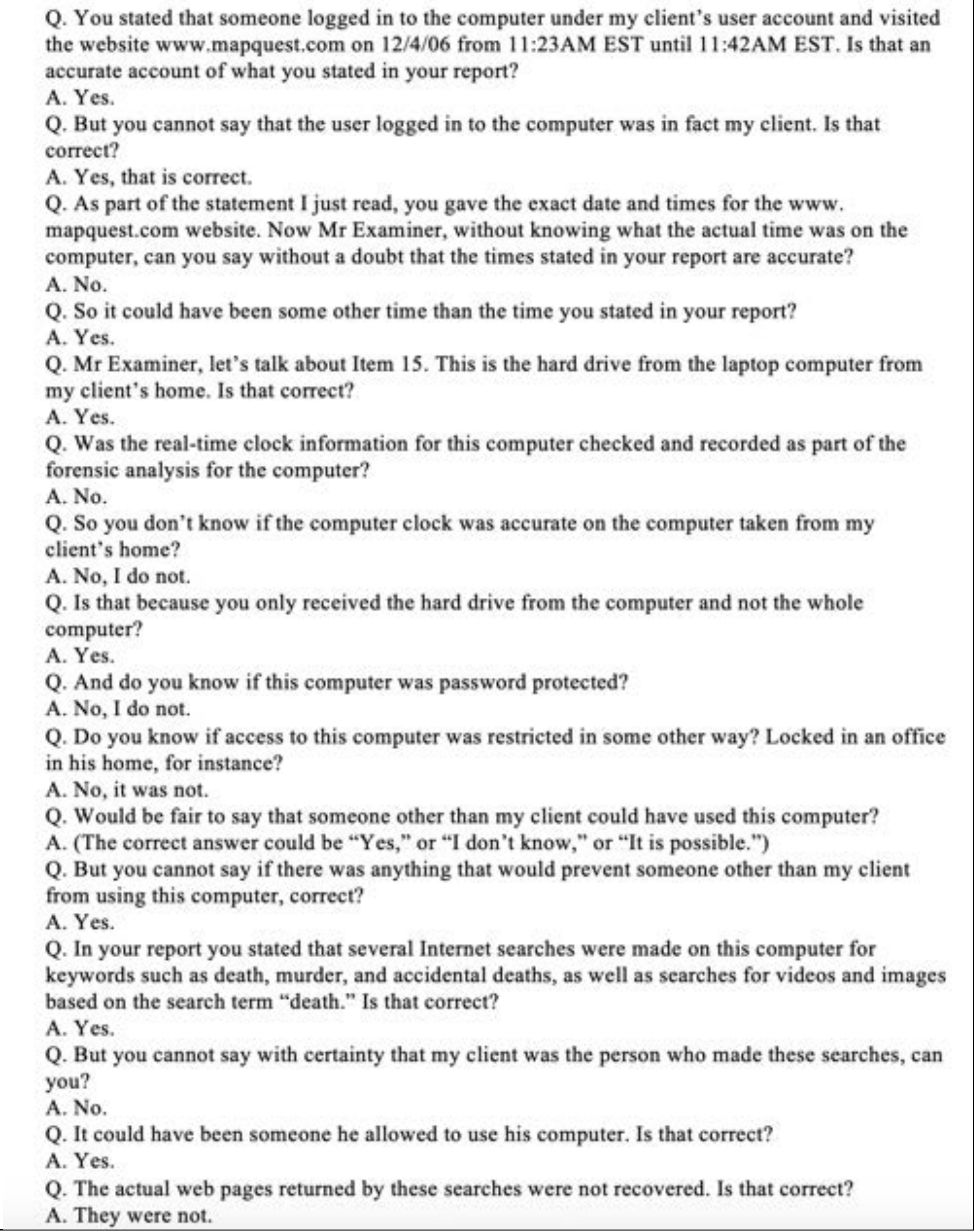
A. (Correct Answer): Someone logged in to the computer using the defendant's account rather than a user account of their own.

Q. Does that mean that the user was my client and could only have been my client?

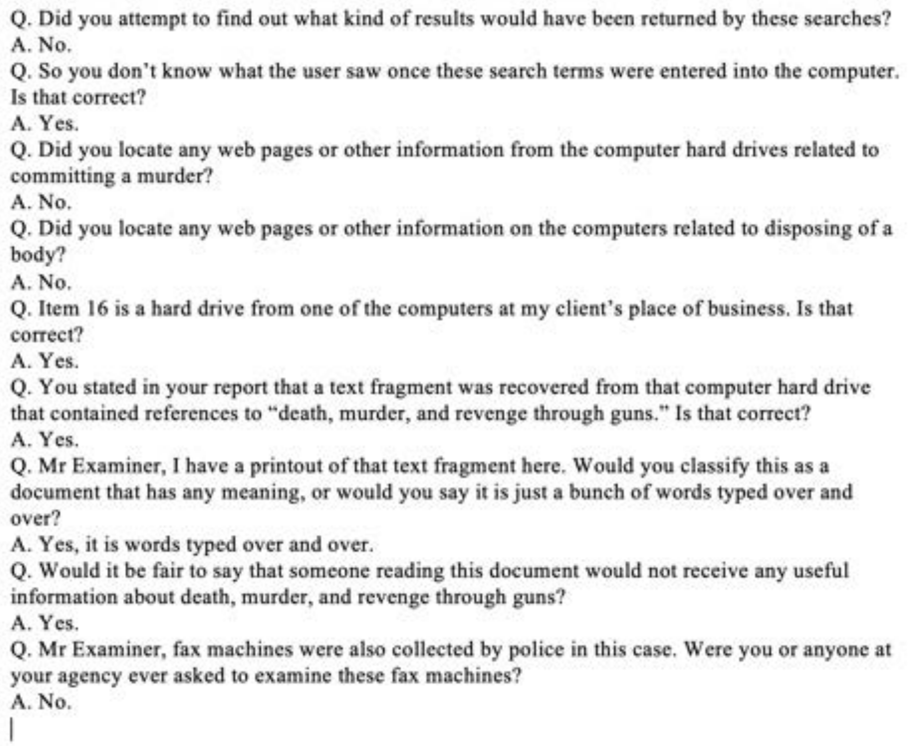
A. No.

Q. So it could have been anyone with access to the computer?

A. Yes.



Q. You stated that someone logged in to the computer under my client's user account and visited the website www.mapquest.com on 12/4/06 from 11:23AM EST until 11:42AM EST. Is that an accurate account of what you stated in your report?
A. Yes.
Q. But you cannot say that the user logged in to the computer was in fact my client. Is that correct?
A. Yes, that is correct.
Q. As part of the statement I just read, you gave the exact date and times for the www.mapquest.com website. Now Mr Examiner, without knowing what the actual time was on the computer, can you say without a doubt that the times stated in your report are accurate?
A. No.
Q. So it could have been some other time than the time you stated in your report?
A. Yes.
Q. Mr Examiner, let's talk about Item 15. This is the hard drive from the laptop computer from my client's home. Is that correct?
A. Yes.
Q. Was the real-time clock information for this computer checked and recorded as part of the forensic analysis for the computer?
A. No.
Q. So you don't know if the computer clock was accurate on the computer taken from my client's home?
A. No, I do not.
Q. Is that because you only received the hard drive from the computer and not the whole computer?
A. Yes.
Q. And do you know if this computer was password protected?
A. No, I do not.
Q. Do you know if access to this computer was restricted in some other way? Locked in an office in his home, for instance?
A. No, it was not.
Q. Would be fair to say that someone other than my client could have used this computer?
A. (The correct answer could be "Yes," or "I don't know," or "It is possible.")
Q. But you cannot say if there was anything that would prevent someone other than my client from using this computer, correct?
A. Yes.
Q. In your report you stated that several Internet searches were made on this computer for keywords such as death, murder, and accidental deaths, as well as searches for videos and images based on the search term "death." Is that correct?
A. Yes.
Q. But you cannot say with certainty that my client was the person who made these searches, can you?
A. No.
Q. It could have been someone he allowed to use his computer. Is that correct?
A. Yes.
Q. The actual web pages returned by these searches were not recovered. Is that correct?
A. They were not.



Q. Did you attempt to find out what kind of results would have been returned by these searches?
A. No.
Q. So you don't know what the user saw once these search terms were entered into the computer. Is that correct?
A. Yes.
Q. Did you locate any web pages or other information from the computer hard drives related to committing a murder?
A. No.
Q. Did you locate any web pages or other information on the computers related to disposing of a body?
A. No.
Q. Item 16 is a hard drive from one of the computers at my client's place of business. Is that correct?
A. Yes.
Q. You stated in your report that a text fragment was recovered from that computer hard drive that contained references to "death, murder, and revenge through guns." Is that correct?
A. Yes.
Q. Mr Examiner, I have a printout of that text fragment here. Would you classify this as a document that has any meaning, or would you say it is just a bunch of words typed over and over?
A. Yes, it is words typed over and over.
Q. Would it be fair to say that someone reading this document would not receive any useful information about death, murder, and revenge through guns?
A. Yes.
Q. Mr Examiner, fax machines were also collected by police in this case. Were you or anyone at your agency ever asked to examine these fax machines?
A. No.

Figure 2: Criminal trial example [1]

Content Template	
Section Number	3.6
Section Title	**Trial Phase**
Introduction	This section identifies the duties of the digital forensic expert in the trial phase
Content	At the end when a case goes to trial, all digital evidence has to be reported by both sides, if available, through digital forensic experts. This part of the report was discussed in chapter 2 at the presentation stage section. During the direct and the cross examination in the trial phase, the digital forensic expert can assist in understanding the opposing expert responses and in preparing new set of questions and answers.

Activity Template	
Number	3.1
Title	Investigate a civil case or a criminal case and prepare a question set for that case. Use the examples in figure 1 and figure 2 in chapter 3 to prepare the questions.
Type	• Research
Aim	To know how digital forensic evidence is used in the court
Description	Each student needs to write an article about the case he is investigating, the digital evidence used and what questions have to be asked.
Timeline	Two weeks
Assessment	Students need to produce an article of at least three pages. The main elements in the article are: 7- The case and how the students obtained it 8- The evidence and how the student can present it 9- The questions and their relation to the case and the evidence

Think Template (MCQs)	
Number	3.1
Title	Mitigation
Type	Choose correct answer
Question	Mitigation can be used during the trial phase
Answers	5- True **6- False**

Think Template (MCQs)	
Number	3.2
Title	**Digital evidence through the trial life time**
Type	- Choose correct answer
Question	The digital evidence expert can present the evidence during:
Answers	1. Mitigation stage 2. pre-trial stage 3. trial stage **4. all stages**

Think Template (MCQs)	
Number	3.3
Title	**Pre-trial motion**
Type	• Choose correct answer
Question	The digital forensic expert can present his question set to the court even without authorization from the attorney
Answers	• True • **False**

Reference	
Number	3.1
Title	*Digital Forensics for Legal Professionals*
Topic	3.1, 3.2, 3.4, 3.5, 3,6
Type	Daniel, Larry E. and Daniel, Lars E. 2012. *Digital Forensics for Legal Professionals*. 1st ed. Elsevier Inc.

Reference	
Number	3.2
Title	An Ad Hoc Review of Digital Forensic Models
Topic	3.2
Type	Pollitt, Mark M. 2007. "An Ad Hoc Review of Digital Forensic Models." Pp. 43–52 in *Proceedings - SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering*. Washington,.

Reference	
Number	3.3
Title	*Computer Forensics and Digital Investigation with EnCase Forensic V7*
Topic	3.4 ,3.3
Type	Widup, Suzanne. 2014. *Computer Forensics and Digital Investigation with EnCase Forensic V7*. 1st ed. McGraw-Hill Education.

Reference	
Number	3.4
Title	Computer Forensics: An Approach to Evidence in Cyberspace
Topic	3.3, 3.4, 3.5
Type	M. M. Pollitt. 1995. "Computer Forensics: An Approach to Evidence in Cyberspace." Pp. 487–91 in *the National Information Systems Security Conference*. Baltimore,.

4. Digital forensic expert

Scope Template	
Number	4
Title	**Digital forensic expert**
Introduction	This chapter explains the meaning of an expert as the term "expert" refers to the examiner, investigator and scientist although the term "expert" is a legal term and is only valid in a court of law. The chapter also shows the difference between a computer expert and a digital forensics expert. Then the chapter shows how to select a digital forensics expert, what is expected from an expert and the investigations made by an expert.
Outcomes	To understand the job of digital forensics expert
Topics	1- Introduction 2- What is the digital forensic expert? 3- Why the digital forensic expert is needed? 4- When is the digital forensic expert needed? 5- The difference between a Computer Expert and Digital Forensics Expert 6- How to select an expert 7- What is expected from an expert
Study Guide	

Content Template	
Section Number	4.1
Section Title	Introduction
Introduction	This section is an introduction to the chapter and shows the objectives of the chapter.
Content	Digital forensics is an area of specialty that requires technical and legal knowledge in addition to investigative skills. On the other hand, Computer expertise area is a specific area covering technical understanding of computer planning, implementation, support, diagnosis, and repair. This chapter explains the meaning of an expert as the term "expert" refers to examiner, investigator and scientist although the term "expert" is a legal term and is only valid in a court of law. The chapter also shows the difference between computer expert and digital forensic expert. Then the chapter shows how to select a digital forensic expert, what is expected from an expert and the investigations made by an expert.

Content Template	
Section Number	4.2
Section Title	**What is the digital forensic expert?**
Introduction	This section defines the digital forensic expert
Content	Section 700 of the Federal Evidence Rules and specifically Rule 702 is used by the federal system to describe expert witness testimony. *"Testimony by Experts:* *If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.* [1]

Content Template	
Section Number	4.3
Section Title	**Why the digital forensic expert is needed?**
Introduction	This section shows the importance of the digital forensic expert in the field
Content	Although the answer to this question may appear clear, it is noted that experts are not called in every case. The reason for that is people may think the case is too simple, such as searching in internet history, which does not deserve the payment for a digital forensic expert [1][2]. If an expert asks for a high rate of remuneration, the question should be: will this investment give good results for the client? Sometimes, the fee is nothing compared to a client's freedom or the large amount of money that the client may lose. For example, in many criminal cases where the client faces loss of freedom or loss of life, the cost of hiring a digital forensics expert should not even be considered. Another example, millions of dollars can be the price for a case in civil courts, paying a digital forensics expert a relatively small amount of money is nothing compared to the total loss of money. Why would someone think to hire an expert? Mainly because any forensic case requires proper collection and preservation of digital evidence, efficient and precise analysis of digital evidence, and accurate interpretation of the examinations results [1]. The accurate interpretation of digital evidence is important and there can be different interpretations of a single piece of evidence. A good expert should consider all variables and the entire body of digital evidence so that his/her conclusion is in the right direction. The need for an expert is clearer in in complex cases involving multiple computers, many computer users, and complicated timelines [3]. Without a competent expert, the client can face a difficult time made by the opposing side's expert. In such situations, an expert is needed to act as an equalizer; that is, to determine if the opposing expert has performed a proper forensic examination and to verify their claims.

Content Template	
Section Number	4.4
Section Title	**When the digital forensic expert is needed?**
Introduction	This section explains when the digital forensic expert should be hired and the importance of time during the investigations
Content	A digital forensics expert needs to be hired when the client determines that any type of electronic evidence will be required for the case[1]. The earlier the engagement of a digital forensic expert the better because the clients may have evidence that must be collected early or a large volume of evidence that has to be analyzed. This is because collecting and analyzing digital evidence can take an amount of time that cannot be predicted at the beginning. For example, collecting and analyzing evidence from large hard drives is obviously more time-consuming than small ones. The digital forensic expert should also be hired when cases involving deleted items that are the reason for a spoliation claim [1][2]. The recovery of deleted files and finding who and when deleted the files is a complex process and may consume much time. The process demands searching in hard drives, caches and even raw data which requires special tools and high skills. Also, making a forensic copy of the evidence is a time-sensitive operation [1][3]. As your studies have shown electronic devices must not be kept running because this may cause a change to evidence and some evidence can be lost. Any delay in completing forensic collections can also cause the evidence to be intentionally destroyed or damaged normally because the client such as big companies may have periodic disk-cleaning operations. The digital forensic expert should have the ability to be on time and to do things on time [3]. The client and his expert should act together to meet the deadlines set by the attorney. The opposing side may have got the evidence and the analysis earlier. So, the expert has to take quick action to perform the necessary collection and analysis. The attorney may not give the expert enough time to examine the evidence; and in this situation the expert and the client may lose if they do not act judiciously. Failing to hire an expert early and at the right time may result in incomplete analysis, increased expenses, and non-compliance with court orders that may result in penalties or inadmissibility of evidence that is critical to the case [1].

Content Template	
Section Number	4.5
Section Title	**The difference between the Computer Expert and Digital Forensic Expert**
Introduction	In this section, the difference between a computer expert and a forensic expert is explained in detail.
Content	**4.5.1 Computer Expert** Computing is a very broad term and includes different technologies such hardware, software, security, and networking. When a person has knowledge of one computer field, that does not mean the person can practice other fields with professionalism. For example, a software expert may not have any knowledge of networking or hardware. Also, the knowledge of computing can be superficial and only at a hobby and not professional level. There are different specialties in the field of computing. For instance, a software expert is the person who performs functions and could be the person who actually develops software applications from scratch for end users. Or she/he can be just the person who provides simple support for a specific piece of software. In a large company, it is likely that you will find specialists who provide support, upgrading, and maintenance of e-mail servers or backup servers, or database servers. At the same time, there are others who work on network security and network protection from viruses and malware. Another term used in the software business is website developers that deal with the mechanics of web applications and cooperate with designers to determine the final interface and look of the website. The computer hardware field includes the maintenance side which focuses on computer repair or building computers from component parts. Nowadays assembling a computer from a motherboard, compatible memory, processor, DVD drive and hard drive is easy and takes little time. These days most components are built on the motherboard and the technician does not need to manually set jumper switches on the motherboard for adjusting the processor speed and also does not need to install several add-in cards for video, modem, audio, and networking. A computer expert's main focus is on installing, maintaining, and repairing computer systems. Figure 4. 1 shows the main focus of the computer expert.

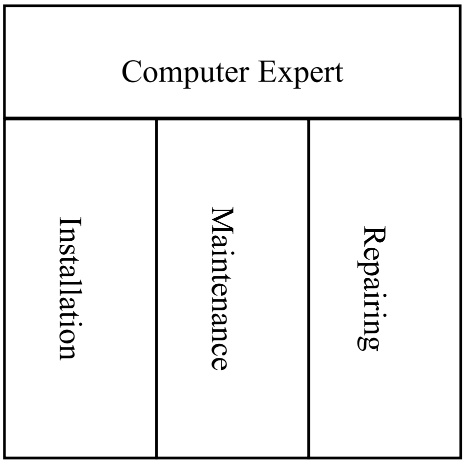


Figure 4.1: The focus of the computer Expert

The hardware expert is similar to the software expert as both deal with the same tasks no matter what the system is. While both may have the skills to recover lost data, they cannot be considered computer forensic experts because they have no knowledge on how to extract evidence and present it for the court as will be shown in the coming section.

4.5.2 The Digital Forensics Expert

Digital forensic experts may have a lot of background knowledge on computing and may have not. Some forensic expert come from a police background and got training on computers while other came from the computer field and got training on the forensic part [1].

A computer forensics expert or examiner is trained to use specialized tools and programs to perform data recovery and to analyze the data in a forensic style [2]. Therefore, a computer forensics expert focuses on the examination of recovered data to obtain useful evidence for the case. So, the computer forensics expert must be able to identify and collect facts about the data, not only recovering the data. Further, the computer forensic expert is trained on handling evidence, working within the law, and presenting the findings in a legal style.

Figure 4.2 illustrates the focus of digital forensics experts on the areas of technical knowledge, investigative techniques, and the legal system.

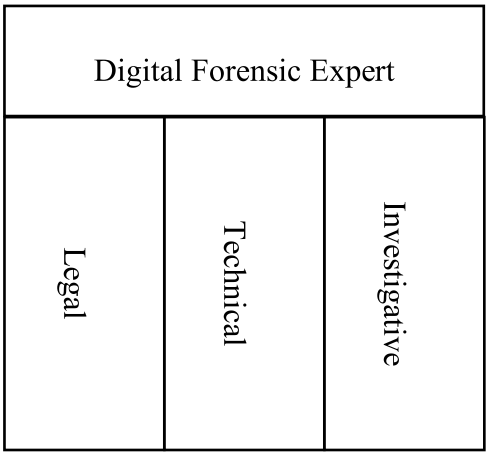


Figure 4.2: The focus of the computer Expert

Case study

An example that shows the main difference between computer expert and forensic expert is:

"*suppose that a client is accused of deleting data from a hard drive after a preservation hold has been put in place. Furthermore, add in the fact that when the computer is examined, a file-wiping software program is discovered to have been on the computer*." [1]

Examiner 1, who was a computer expert with no forensics background acted by firstly examining the hard drive and running file recovery software on the hard drive. In this way, he recovered hundreds of deleted files. But because of the file-wiping software installed on the computer, he was not able to open the files. He stated that in his report.

Examiner 2, who was a trained forensics examiner, acted by also examining the hard drive on the client's computer. The difference here is that Examiner 2 initially removed the hard drive and made a forensic copy without switching the computer on. He then examined the hard drive forensic copy and also recovered hundreds of deleted files. He noted that there was a directory in which the file-wiping software was installed. Inside that directory, he found that the only remaining file was a system file with a date that was two days after the court hearing on the preservation order. After that he downloaded a copy of the same file-wiping program onto a clean test computer and then ran the software and subsequently uninstalled the software to find out how it worked and what it did when it was uninstalled. Examiner 2 determined that the file-wiping software deletes files by overwriting them with zeroes. When he examined the raw data on the hard drive forensic copy, he found that sets

	of zeroes were missing on the hard drive meaning that the files were overwritten. Examiner 2 concluded that the file-wiping software had never been run against the client’s drive to remove files of interest because if the file-wiping program had been run on the drive, there woud be a sequence of zeros in the raw data on the hard drive [1].

Content Template	
Section Number	4.6
Section Title	**How to select an expert?**
Introduction	This section shows how a client can hire an expert and gives guidelines for a client to follow and for experts to consider
Content	Digital forensic experts must be first qualified as a digital forensic expert. An expert in digital forensics usually obtains a forensic certificate which is should not be easy to obtain and may be expensive. Some courts may not demand the forensic certificate as long as the person involved can provide strong forensic experience [1]. It is not enough to have knowledge of computing as experts should also have good public speaking experience. Experts need to be able to present themselves at the court professionally and they should not have trouble explaining any complex technical concepts in a simple and easy-to-understand way. Prior to court, experts should have testimony experience as any lack of testimony experience can certainly cause issues within the case [1] [2]. Also, experts should have references to back up their expertise. Experts must have also knowledge and training in forensic methods and processes. If for example the hired expert does not have the skill for dealing with cell phone cases, problems will be caused to the client requiring such skill. These problems become more complicated when the opposition expert has the skills and discovers that the hired expert has incorrectly dealt with the evidence. Also, experience is required because there are more complex cases than just recovering simple data [2]. Some cases may involve financial records, multiple persons, data hiding techniques and complex relationships. Usually the government have an expert in criminal cases who performs the examinations and produces the evidence. The hired expert must not only repeat what the government expert did, but also, she/he should make their own examination to validate any prosecution clams. Therefore, an expert should have experience and training on complex cases in civil or criminal courts.

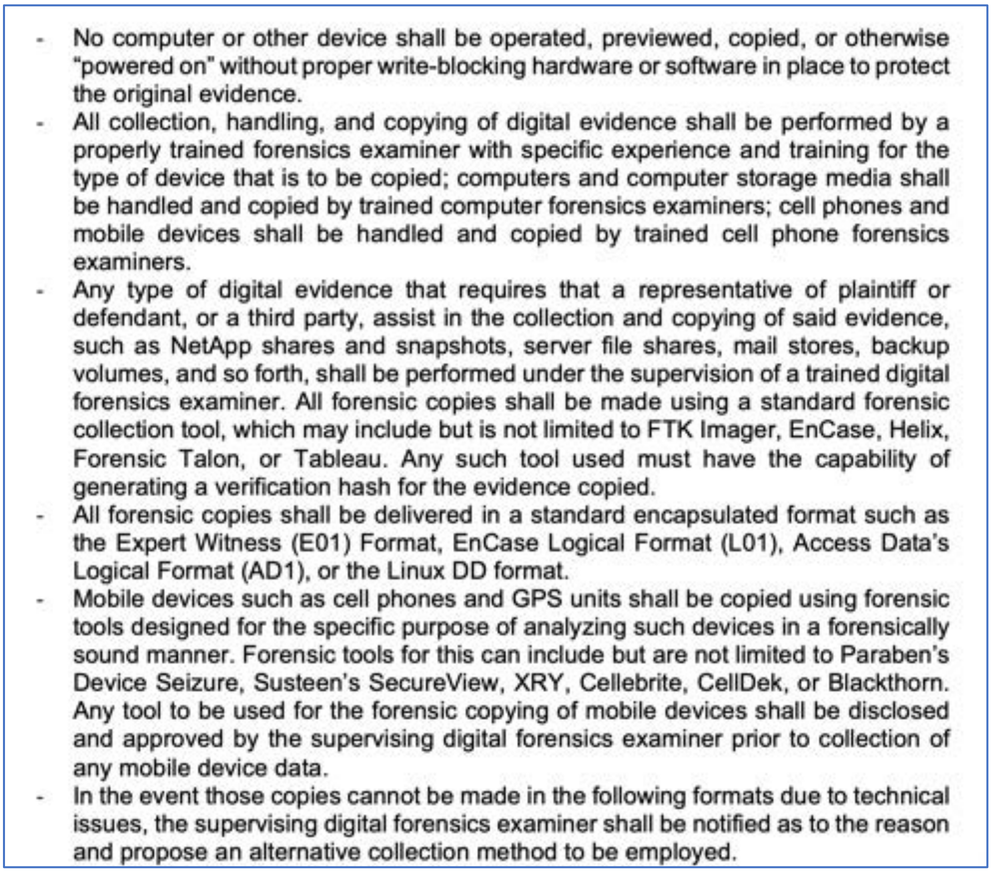
Content Template	
Section Number	4.7
Section Title	**What is expected from an expert?**
Introduction	This section explains the details of digital forensic tasks and shows practical examples of some cases.
Content	Several points are expected from an epxert which can be explained as follows: **4.7.1 General expectation** Generally, the main task of the expert is obtaining evidence through motions or orders and performing all actions related to the evidence [2]. The expert should be able to determine the type of the evidence and identify the evidence itself. The expert needs to analyze the evidence and present the results to the court. Also, the expert needs to review the opposition expert's evidence and work. An expert should also assist the attorney in reviewing warrant affidavits and assessing the merits of a case [3]. Engaging an experienced expert is important in assisting during the pre-trial motions by revealing the way in which the evidence was collected and preserved and by analyzing the cause in search warrant affidavits [1]. The expert is also needed for assisting in the assessment of cost that is required for processing different types of evidence. **4.7.2 Investigation of Digital Evidence** What does investigation mean? investigating a computer includes determining the action that someone has made on the computer [1]. The digital forensic investigation aims to prove that the person accused is the same person who performed the action on the computer. In digital forensics, the investigation aims to find every piece of evidence and determine who created that evidence. So, the investigation deals with the questions: what, when, how, and who in relation to the evidence. The investigation also determines if something has been deleted, when it was deleted, who deleted it, and who owns it [3]. Sometimes it is not easy to prove who deleted the file. For example, some personal computers do not have passwords protecting the individual accounts, so it is not easy to establish whether the owner of the personal computer is the one who actually deleted the file. Once the actual investigation and examination start, the process of searching for evidence becomes more complicated. Therefore, an expert has not only to locate the evidence, but also she/he needs to find all the facts surrounding that evidence. Examples of questions that need to be answered in such cases include: "*Who was logged on to the computer at the time the evidence was created? Was the account password protected? Is the date accurate? Is it relevant? Was the original evidence protected when this item was located to ensure that the evidence*

wasn't modified or planted? Did the person who examined the computer have a legal right to do so?" [1]

4.7.3 Providing forensic protocols

The other task of a digital forensic expert is to provide a set of protocols that are necessary in ensuring that all evidence was collected properly. Sometimes a third party may take the responsibility of collecting, copying and preserving the evidence. An example of protocols that are used for evidence collection by an opposition party or a third party is as follows:

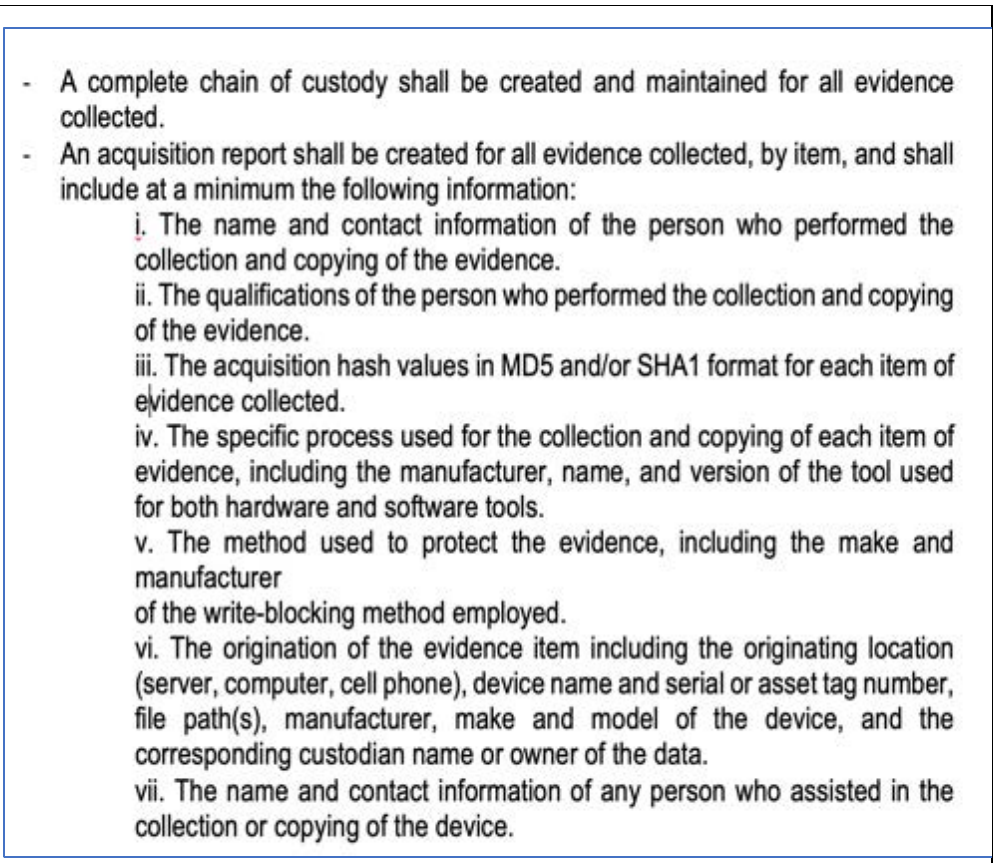
1- A forensically sound method that complies with the best practice should be used to copy the media for producing the evidence. Figure 4.3 shows a copy of protocols that are usually used for media copying by third or opposition parties as described in [1].



- No computer or other device shall be operated, previewed, copied, or otherwise "powered on" without proper write-blocking hardware or software in place to protect the original evidence.
- All collection, handling, and copying of digital evidence shall be performed by a properly trained forensics examiner with specific experience and training for the type of device that is to be copied; computers and computer storage media shall be handled and copied by trained computer forensics examiners; cell phones and mobile devices shall be handled and copied by trained cell phone forensics examiners.
- Any type of digital evidence that requires that a representative of plaintiff or defendant, or a third party, assist in the collection and copying of said evidence, such as NetApp shares and snapshots, server file shares, mail stores, backup volumes, and so forth, shall be performed under the supervision of a trained digital forensics examiner. All forensic copies shall be made using a standard forensic collection tool, which may include but is not limited to FTK Imager, EnCase, Helix, Forensic Talon, or Tableau. Any such tool used must have the capability of generating a verification hash for the evidence copied.
- All forensic copies shall be delivered in a standard encapsulated format such as the Expert Witness (E01) Format, EnCase Logical Format (L01), Access Data's Logical Format (AD1), or the Linux DD format.
- Mobile devices such as cell phones and GPS units shall be copied using forensic tools designed for the specific purpose of analyzing such devices in a forensically sound manner. Forensic tools for this can include but are not limited to Paraben's Device Seizure, Susteen's SecureView, XRY, Cellebrite, CellDek, or Blackthorn. Any tool to be used for the forensic copying of mobile devices shall be disclosed and approved by the supervising digital forensics examiner prior to collection of any mobile device data.
- In the event those copies cannot be made in the following formats due to technical issues, the supervising digital forensics examiner shall be notified as to the reason and propose an alternative collection method to be employed.

Figure 4.3: protocols for media collection by third party or opposing party

2. Documentation Requirements: there are also protocols to be followed for preparing the documentation by the third party. An example of such protocols is shown Figure 4.4 as appears in [1].



- A complete chain of custody shall be created and maintained for all evidence collected.
- An acquisition report shall be created for all evidence collected, by item, and shall include at a minimum the following information:

    i. The name and contact information of the person who performed the collection and copying of the evidence.

    ii. The qualifications of the person who performed the collection and copying of the evidence.

    iii. The acquisition hash values in MD5 and/or SHA1 format for each item of evidence collected.

    iv. The specific process used for the collection and copying of each item of evidence, including the manufacturer, name, and version of the tool used for both hardware and software tools.

    v. The method used to protect the evidence, including the make and manufacturer
    of the write-blocking method employed.

    vi. The origination of the evidence item including the originating location (server, computer, cell phone), device name and serial or asset tag number, file path(s), manufacturer, make and model of the device, and the corresponding custodian name or owner of the data.

    vii. The name and contact information of any person who assisted in the collection or copying of the device.

Figure 4.4: the set of protocols for the documentation made by third party or opposing party

Such protocols are critical because when a non-expert is hired to perform collections, he may not use any forensic tool for protecting the evidence and for making forensic copies. This cannot be known until the case gets to the court. So, the protocols can prevent such situations.

4.7.4 Examination

This task is performed by the digital forensic expert when the evidence has been collected. The expert needs to perform analysis and an examination of the evidence. Based on information collected during the previous process, which was provided by the attorney, the client, and the review of an opposition expert's report, the expert needs to perform the following [1][3]:

1. Verifying the work of the opposition expert.

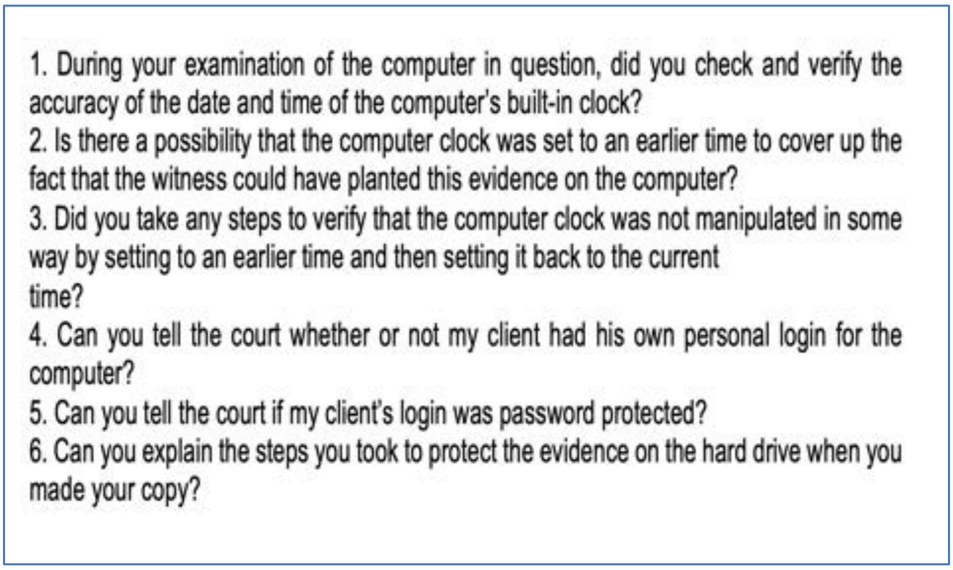
2. Performing independent analyses on the evidence for ensuring that the evidence is accurate

3. advising on the findings and on the merits of the digital evidence in the case.

4. Assisting the client with trial preparation.

4.7.5 Court Preparation

The court preparation involves reviewing the opposition expert's reports. A series of questions needs to be created by the expert to help the attorney examine the opposition expert's opinion about the case. Some examples of such questions appear in [1] and shown in Figure 4.5.



1. During your examination of the computer in question, did you check and verify the accuracy of the date and time of the computer's built-in clock?
2. Is there a possibility that the computer clock was set to an earlier time to cover up the fact that the witness could have planted this evidence on the computer?
3. Did you take any steps to verify that the computer clock was not manipulated in some way by setting to an earlier time and then setting it back to the current time?
4. Can you tell the court whether or not my client had his own personal login for the computer?
5. Can you tell the court if my client's login was password protected?
6. Can you explain the steps you took to protect the evidence on the hard drive when you made your copy?

Figure 4.5: example of questions to be asked about the opposition expert's report

In the court also, the expert may need to testify and should provide testimony to the ownership of the files, ownership of the computers, the collection and handling of the evidence, the software installed on the computer, and date and time logs of the computer activities.

Activity Template	
Number	4.1
Title	Review the section "what is expected from an expert" and write a report about what the expert should do for the case: "A man is accused of using bitcoin in internet gambling"
Type	• Review
Aim	To understand the job of a digital forensic expert
Description	Each student needs to write a report about the tasks to be performed by the digital forensic expert
Timeline	Two weeks
Assessment	Students need to produce an article of at least three pages. The main elements in the article are: 10- Identify who is the expert to be hired 11- Explain the tasks of the expert to be performed on the case 12- Describe the expert's tasks and digital forensic process

Think Template (MCQs)	
Number	4.1
Title	Digital forensic expert
Type	Choose correct answer
Question	Having in-depth knowledge of computers and software in general is a prerequisite for a digital or computer forensics examiner.
Answers	7- True **8- False**

Think Template (MCQs)	
Number	4.2
Title	**How to select an expert**
Type	Choose correct answer
Question	An expert may not have a certificate as the experience is enough
Answers	**1- True** 2- False

Think Template (MCQs)	
Number	4.3
Title	**Digital forensic expert**
Type	Choose correct answer
Question	The digital forensic expert should not be able to provide any justification about the use of a specific method in evidence collection
Answers	True **False**

Think Template (MCQs)	
Number	4.4
Title	**What is expected from an expert**
Type	Choose correct answer
Question	The digital forensic expert should provide protocols for the opposition expert in civil cases only
Answers	True **False**

Think Template (MCQs)	
Number	4.5
Title	**Digital forensic protocols**
Type	Choose correct answer
Question	There are digital forensic protocols related to data copying from any media
Answers	**True** False

Extra Template	
Number	4.1
Title	*Digital Forensics for Legal Professionals*
Topic	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
Type	Daniel, Larry E. and Daniel, Lars E. 2012. *Digital Forensics for Legal Professionals*. 1st ed. Elsevier Inc.

Extra Template	
Number	4.2
Title	*Computer Forensics and Digital Investigation with EnCase Forensic V7*
Topic	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
Type	Widup, Suzanne. 2014. *Computer Forensics and Digital Investigation with EnCase Forensic V7*. 1st ed. McGraw-Hill Education.

Extra Template	
Number	4.3
Title	*Digital Forensics*
Topic	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
Type	A. Årnes, *Digital Forensics*, 1st ed. Wiley, 2017.

5. Digital evidence discovery

Scope Template	
Number	4
Title	**Digital evidence discovery**
Introduction	This chapter explains the process of digital evidence discovery in civil cases and criminal cases. The committed reader can learn the challenges of both types of cases and understand the methods of collecting evidence related to each types.
Outcomes	To understand the digital evidence discovery in civil and criminal cases
Topics	1- Introduction 2- Evidence in criminal cases 3- Evidence in civil cases 4- Evidential Discovery of Computers and Storage Media
Study Guide	

Content Template	
Section Number	5.1
Section Title	Introduction
Introduction	This section is an introduction to the chapter and explains the objectives of digital evidence discovery.
Content	The discovery of digital evidence is not an easy task. The digital forensic expert must perform a comprehensive investigation and examination to get useful information. Also, the expert should help the client and the court by creating discovery motions tailored to the evidence required in the case. So, in this chapter, we discuss the process of creating discovery motions for digital evidence.

Content Template	
Section Number	5.2
Section Title	**Evidence in criminal cases**
Introduction	This section explains the evidence discovery in criminal cases, the challenges, and the methods used for evidence discovery.

Content

In criminal cases, the evidence is kept out of use and maintained in the custody of law enforcement when a discovery motion is created. However, the digital forensic expert needs to get access to the forensic images and to the chain of custody documentation in order to start the examination [1].

5.2.1 Common challenges in criminal cases

Criminal cases poses some challenges to the digital forensic experts that can be summarized as [1][2]:

1. Sometimes the expert cannot get a copy of the evidence and all forensic examination must be performed at the law enforcement facility and under the supervision of law officers.
2. Sometimes the evidential items are returned to owners by law enforcement before an expert can examine them. For example, a cellphone can be returned to its owner before the forensic examination.
3. It will be also challenging if the documentation made by the law enforcement examiner are not requested in the discovery motion.
4. Sometimes the evidence cannot be found because the law enforcement agents did not use the proper tools to copy the evidence.
5. Some forms of evidence are difficult to obtain, such as a global positioning system (GPS) device data or data from cloud computing companies.

5.2.2 Discovery of Digital Evidence in Criminal Cases

Several types of digital evidence can be found in criminal cases. The expert needs to know how to find the needed evidence so that she/he can defend the client effectively [1]. So an expert should review the initial discovery of the case and then determine what should be collected from the available digital evidence. Therefore, it is important that the expert should be hired as early as possible so that she/he can identify the required evidence and request them in the discovery motion.

5.2.3 Source of evidence in criminal cases

Criminal cases have different characteristics, but they share the advantage that it is easy to define the method that can be used to determine the evidence during the discovery. Initially when the process of discovery and fact-finding starts, the digital forensic examiner must consider the facts provided by the prosecution and any third party. The examiner has to pay attention to all collected items [1], [3]:

1- Search Warrant Returns

The meaning of the search warrant returns is the list of "*all evidence collected by law enforcement when they execute the warrants*". Digital forensic examiners have to search for all possible evidence by considering the items in the inventory. The examiner has look for all devices that can reveal evidence, such as computers, cell phones, cameras, music recorders, video games, GPS units, and storage devices.

2- Paper Discovery

Digital forensic examiners have to be aware of the evidence that can be collected based on the witness statements, third party documents, and investigative reports. All of these can form the evidence documented on paper. Also, paper discovery may include documents from devices such as cell phone call records, web pages and social media records, e-mails printouts, computer screenshots and GPS location records. Special care has to be taken when dealing with these documents because evidence can be missed easily at this stage.

5.2.3 Building the Motion

In criminal cases, some items may not look important to the expert and some items may not seem related to the case [1]. For building the motion, the examiner needs to include these items in the motion. For example, the law enforcement agency may collect items with potential digital evidence without examining those items. Such items are collected because the warrant allows for the collection of everything electronics, such as facsimile machines, video tapes, cameras, CD-ROMs, music players, movie cameras, and game controllers.

Another category is the improper evidence that was collected by incorrect methods or evidence that was not requested at all. The expert should review this evidence to identify its type. An example of this occurs in the case of the collection of call details even though they are not requested from the law enforcement body.

5.2.4 Discovery motion specifics

There are different and important specifics that are included in the discovery motion and the digital forensics expert should pay to attention for [4]:

1- The Inventory: this refers to all items requested by the defense and that can contain any digital data. It does not matter whether these items were examined or copied by the prosecution's experts.

2- Defense material: this refers to the items supplied by the defense to help completing the discovery. For example, the defense may provide sanitized hard disks or storage devices for the forensic copies upon the request of the law enforcement agency.

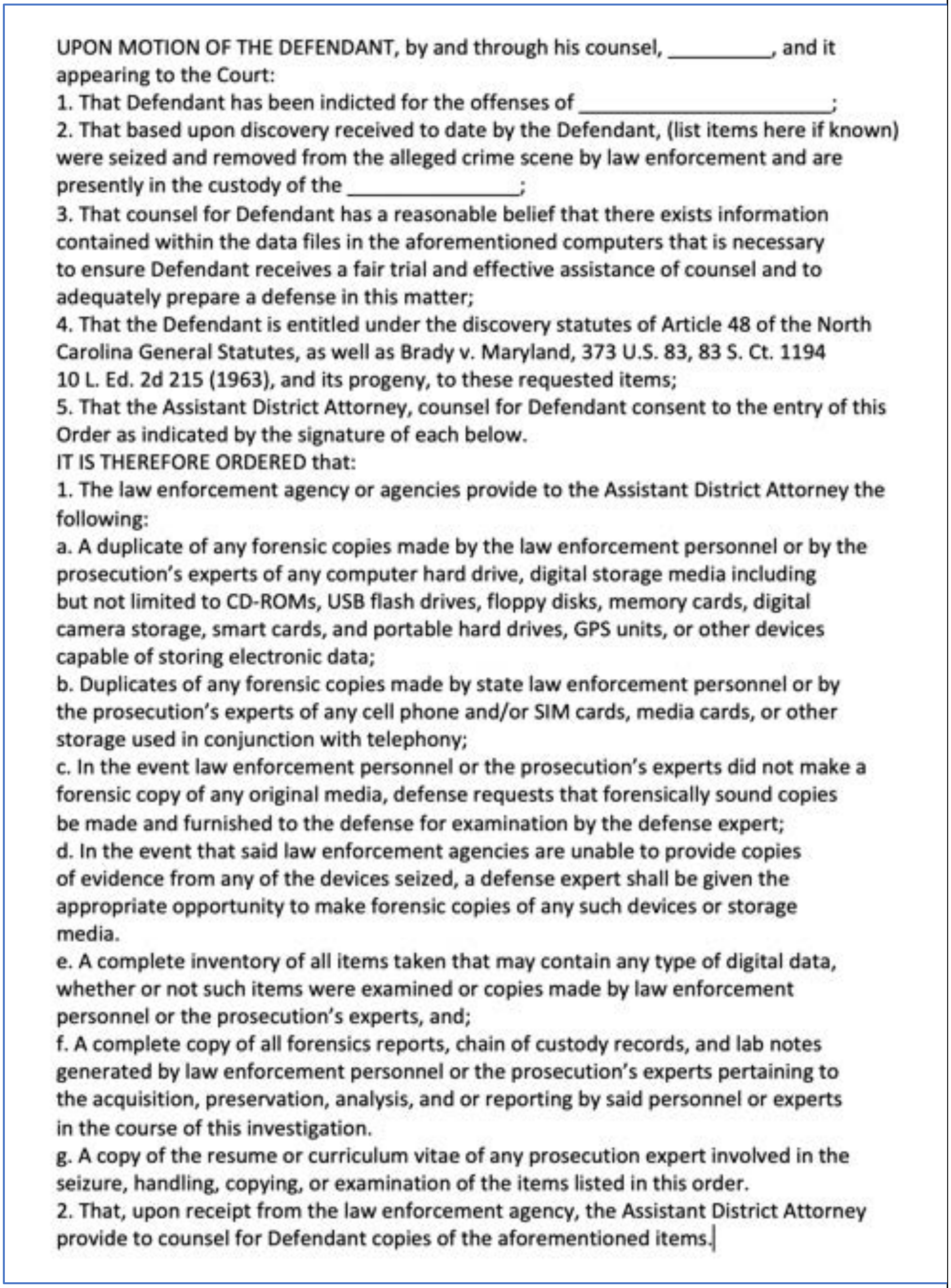
3- Forensic Copy Format: this refers to the preferred format for the forensic copies. One of the preferred formats is "*EnCase (E01) Expert Witness Format*" which is a self-contained set of files and can be opened by most available forensic tools. This format can be converted into other formats easily, so it is widely used.

4- Supplemental Documents: this refers to the materials requested by the defense including copies of all forensics reports, lab notes, and chain of custody records produced by the prosecution's experts during any digital forensic stage: collection, preservation, analysis and presentation. Further, the defense may request resumés or curriculum vitae of prosecution experts involved in the examination process.

5- Computers and digital items: this refers to the defense requests for a duplicate of any forensic copies produced by the prosecution's experts. This can include any computer hard drive and any digital storage media such USB flash drives, DVDs, CD-ROMs, floppy disks, digital camera storage, portable hard drives and smart cards. Also, the defense can ask for a copy of the data on portable devices such as cell phones, GPS, media players, audio and video recorders, and SIM cards.

6- Non-collected forensic images: this refers to the request of the defense for copying original media that was not copied by the prosecution's experts as the defense expert may believe that there is still digital evidence which may help finding the truth.

The process of ordering the collection of digital evidence is a formal consent order due to the sensitivity of the criminal cases. An example of the consent order that is used by the state of North Carolina is shown in Figure 5.1.



UPON MOTION OF THE DEFENDANT, by and through his counsel, __________, and it appearing to the Court:
1. That Defendant has been indicted for the offenses of ________________________;
2. That based upon discovery received to date by the Defendant, (list items here if known) were seized and removed from the alleged crime scene by law enforcement and are presently in the custody of the ________________;
3. That counsel for Defendant has a reasonable belief that there exists information contained within the data files in the aforementioned computers that is necessary to ensure Defendant receives a fair trial and effective assistance of counsel and to adequately prepare a defense in this matter;
4. That the Defendant is entitled under the discovery statutes of Article 48 of the North Carolina General Statutes, as well as Brady v. Maryland, 373 U.S. 83, 83 S. Ct. 1194 10 L. Ed. 2d 215 (1963), and its progeny, to these requested items;
5. That the Assistant District Attorney, counsel for Defendant consent to the entry of this Order as indicated by the signature of each below.
IT IS THEREFORE ORDERED that:
1. The law enforcement agency or agencies provide to the Assistant District Attorney the following:
a. A duplicate of any forensic copies made by the law enforcement personnel or by the prosecution's experts of any computer hard drive, digital storage media including but not limited to CD-ROMs, USB flash drives, floppy disks, memory cards, digital camera storage, smart cards, and portable hard drives, GPS units, or other devices capable of storing electronic data;
b. Duplicates of any forensic copies made by state law enforcement personnel or by the prosecution's experts of any cell phone and/or SIM cards, media cards, or other storage used in conjunction with telephony;
c. In the event law enforcement personnel or the prosecution's experts did not make a forensic copy of any original media, defense requests that forensically sound copies be made and furnished to the defense for examination by the defense expert;
d. In the event that said law enforcement agencies are unable to provide copies of evidence from any of the devices seized, a defense expert shall be given the appropriate opportunity to make forensic copies of any such devices or storage media.
e. A complete inventory of all items taken that may contain any type of digital data, whether or not such items were examined or copies made by law enforcement personnel or the prosecution's experts, and;
f. A complete copy of all forensics reports, chain of custody records, and lab notes generated by law enforcement personnel or the prosecution's experts pertaining to the acquisition, preservation, analysis, and or reporting by said personnel or experts in the course of this investigation.
g. A copy of the resume or curriculum vitae of any prosecution expert involved in the seizure, handling, copying, or examination of the items listed in this order.
2. That, upon receipt from the law enforcement agency, the Assistant District Attorney provide to counsel for Defendant copies of the aforementioned items.

Figure 5.1: Example Language for A Consent Order for Digital Evidence [1].

Content Template	
Section Number	5.3
Section Title	**Evidence in civil cases**
Introduction	This section explains the evidence discovery in civil cases, the challenges, and the methods used for evidence discovery.
Content	Civil cases have different characteristics and different challenges than the criminal cases which makes the discovery motion methods different. The way to access the evidence in civil cases also is different from the criminal cases [1], [3]. - Sometimes in e-discovery cases, the digital evidence items are accessed online because these items are on devices that cannot be switched off. Even if the devices can be examined offline and the evidence can be fully acquired, the time to examine such evidence is often limited to a few hours or less. Careful planning and well-defined scheduling must be done for forensically collecting the evidence of interest. - In civil cases, some parts of the chain of custody documentation may be missed, or the chain may be completely absent. Therefore, the digital forensic examiners who want to examine civil cases should be expert in such cases and should know how to get access to the evidence when creating discovery motions. **5.3.1 Common challenges in civil cases** there are several challenges faced by the digital forensic expert in civil cases. These challenges can be summarized as [1]: 1. Sometimes the chain of custody for a digital evidence is poorly preserved and documented. So, the digital forensic expert needs to know how the evidence was collected and treated and needs also to know the other experts who worked on the same evidence. 2. Sometimes it is difficult to get an access to evidence because the evidence resources are online such as computer servers. 3. In some cases, the evidence was altered or destroyed because of the lack of experience of the opposition digital forensic expert. So, the client expert may not get any documentation regarding the opposition expert and the opposition examinations. 4. In many cases the clients collect the evidence by themselves or hire a computer expert to do so. Therefore, the evidence does not follow the forensic standards because the evidence can be altered, authentication is missing and copying the evidence is not possible. 5. The format of the evidence is not easy to use by the receiving party, such as some database files, backup tape, and some forensic images. 6. The evidence is controlled by a third party, such as phone service providers, Internet service providers, cloud computing providers, or data backup and storage providers. **5.3.2. Discovery of Digital Evidence in Civil Cases** In civil cases, the discovery of evidence is challenging for several reasons [1]:

- the expert needs to figure out what evidence may exist in the case, where it may reside, and who controls it.

- There is a higher chance for evidence to be lost or destroyed in a civil case than in a criminal case. This is because the persons involved in the case have some knowledge that the electronic data can be examined and lead to the provision of evidence.

- In civil cases, there i a high possibility of litigation holds, cost shifting, spoliation, and sanctions against parties that fail to abide by the discovery orders.

5.3.3 Rules Governing Civil Discovery

There are general rules that govern the civil discovery around the world. In the USA federal cases are provided in the Federal Rules of Civil Procedure (FRCP) [1]. These Federal Rules of Civil Procedure are Rules 26, 29, 34, and 45.

5.3.4 Electronic Discovery in Particular

Rule 34(a) of the Federal Rules of Civil Procedure states [1]:

"A party may serve on any other party a request within the scope of Rule 26(b):

1- to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:

a- any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or

b- any designated tangible things; or

2- to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it."

The rule implies that the expert has the power to search anything in electronic form for the purpose of collecting evidence. The term "anything" is far too wide, so the expert must describe during the discovery motion the evidence items, such as computer hard drives, documents, cell phones, e-mail, databases, pictures, drawings, diagrams, etc. The expert must satisfy the judge that the request is reasonable.

5.3.5 The Importance of Time

There is a major risk of losing digital evidence over time. After evidence is created on a device, many activities can occur on that device which may cause evidence alteration or damage. The digital forensic expert needs to work on the evidence as soon as possible because computer hard drives may crash, companies delete data according to their business routines, video surveillance systems are scheduled to overwrite the data storage, people frequently buy new phones and throw away the old ones [1]. There are many activities that can lead to evidence damage in our daily life.

5.3.6 What to collect

The digital forensics expert needs to use a specific method for figuring out what should be collected in a civil case: The method can be specified by the: What, Who, How, Where, and Who approach [1]. These questions help form the investigation to locate and collect electronic evidence. These questions can be summarized as follows:

- **What happened?**

Litigation requires a "what happened?". This is about "*someone or something did or did not do something that has resulted in injury or harm to another party, whether that result is physical or financial harm. Was it a person or persons involved or was it an inanimate object*?" The expert needs to figure out the case and the harm caused by the case to others. The expert starts to think about the evidence and people involved in the case.

- **Who was involved?**

Because litigation implies that someone did something to others. So the expert starts to think "*who are the parties that had some interaction with or instrumentality concerning the alleged subject of the litigation?"* Once the expert identifies these parties by name or by responsibility, the discovery order should be used to determine from whom to collect the data. After that, the identities of people in possession of electronic evidence are disclosed.

- **How would electronic evidence be involved?**

Nowadays, life is increasingly digitized, and almost everything can create an electronic record. One can think about many such examples of electronic records. All these records and the way they are created should be considered once a case occurs. The expert needs to know if the records were created directly by the people involved in the process or by an automated process. The expert needs to consider all the electronic devices involved in the case. For example, in a supermarket once a case occurs, the expert may need to collect data from some employees' or customers' cell phones, from alarm systems, surveillance systems, ATM machines, computers, credit card machines, and devices that are capable of creating and preserving digital data.

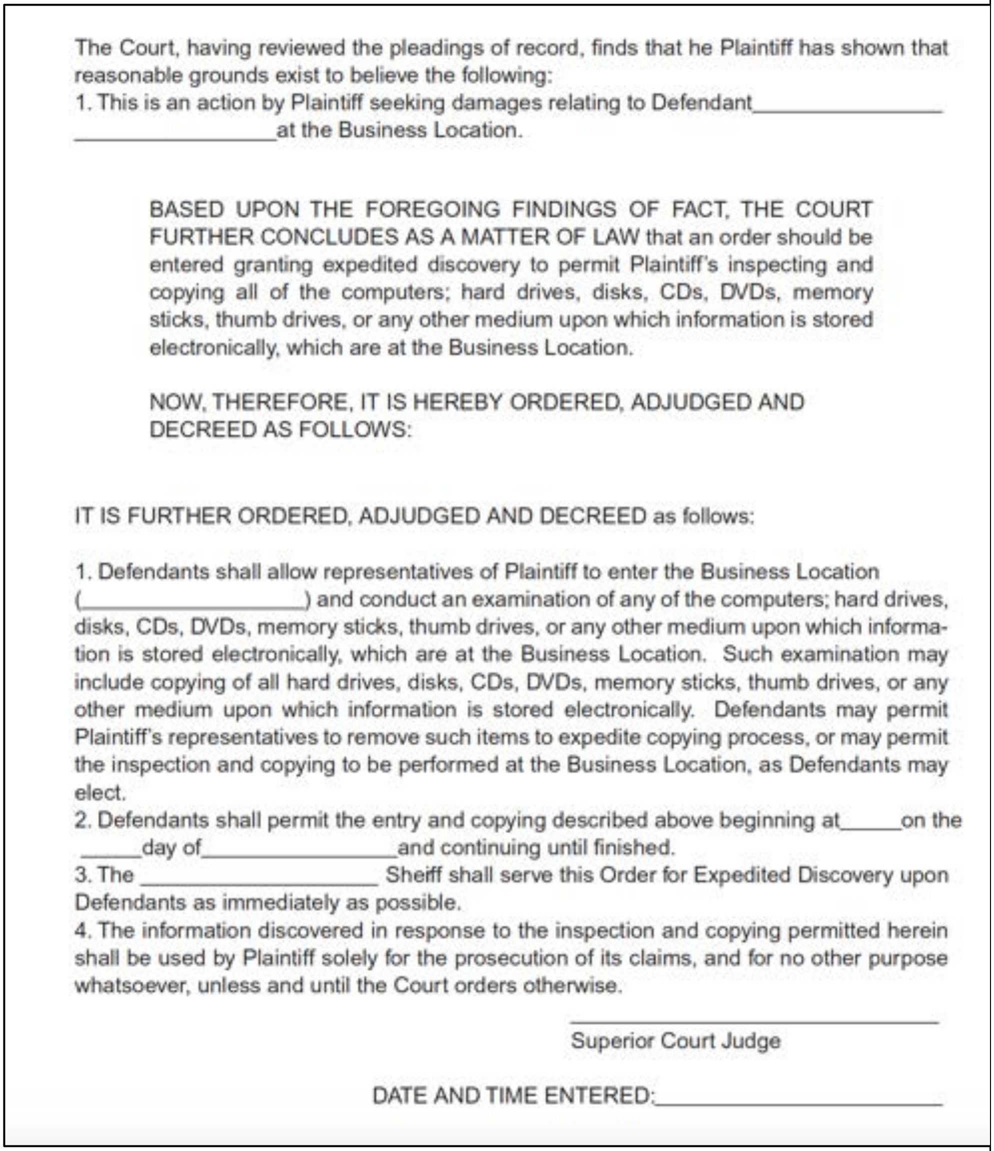
- **Where might electronic evidence be stored?**

Electronic evidence is stored in many places that range from individual computers, networks and the internet to cloud systems. Activity 2 in this book aims to search for the different categories of storage devices.

- **Who has control of the electronic evidence you need to collect**?

Lastly, the digital forensics expert task is to determine "who has control of the electronic evidence". The expert may find that the persons who are directly involved include some third parties such as the cell phone company, the internet provider, and even the cloud data backup company.

To clarify this section, the example in Figure 5.2 specifies what is to be collected, who is going to do the collection, as well as where and when the collection will take place.



The Court, having reviewed the pleadings of record, finds that he Plaintiff has shown that reasonable grounds exist to believe the following:

1. This is an action by Plaintiff seeking damages relating to Defendant________________ ________________at the Business Location.

BASED UPON THE FOREGOING FINDINGS OF FACT, THE COURT FURTHER CONCLUDES AS A MATTER OF LAW that an order should be entered granting expedited discovery to permit Plaintiff's inspecting and copying all of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, which are at the Business Location.

NOW, THEREFORE, IT IS HEREBY ORDERED, ADJUDGED AND DECREED AS FOLLOWS:

IT IS FURTHER ORDERED, ADJUDGED AND DECREED as follows:

1. Defendants shall allow representatives of Plaintiff to enter the Business Location (__________________) and conduct an examination of any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, which are at the Business Location. Such examination may include copying of all hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically. Defendants may permit Plaintiff's representatives to remove such items to expedite copying process, or may permit the inspection and copying to be performed at the Business Location, as Defendants may elect.

2. Defendants shall permit the entry and copying described above beginning at_____on the _____day of________________and continuing until finished.

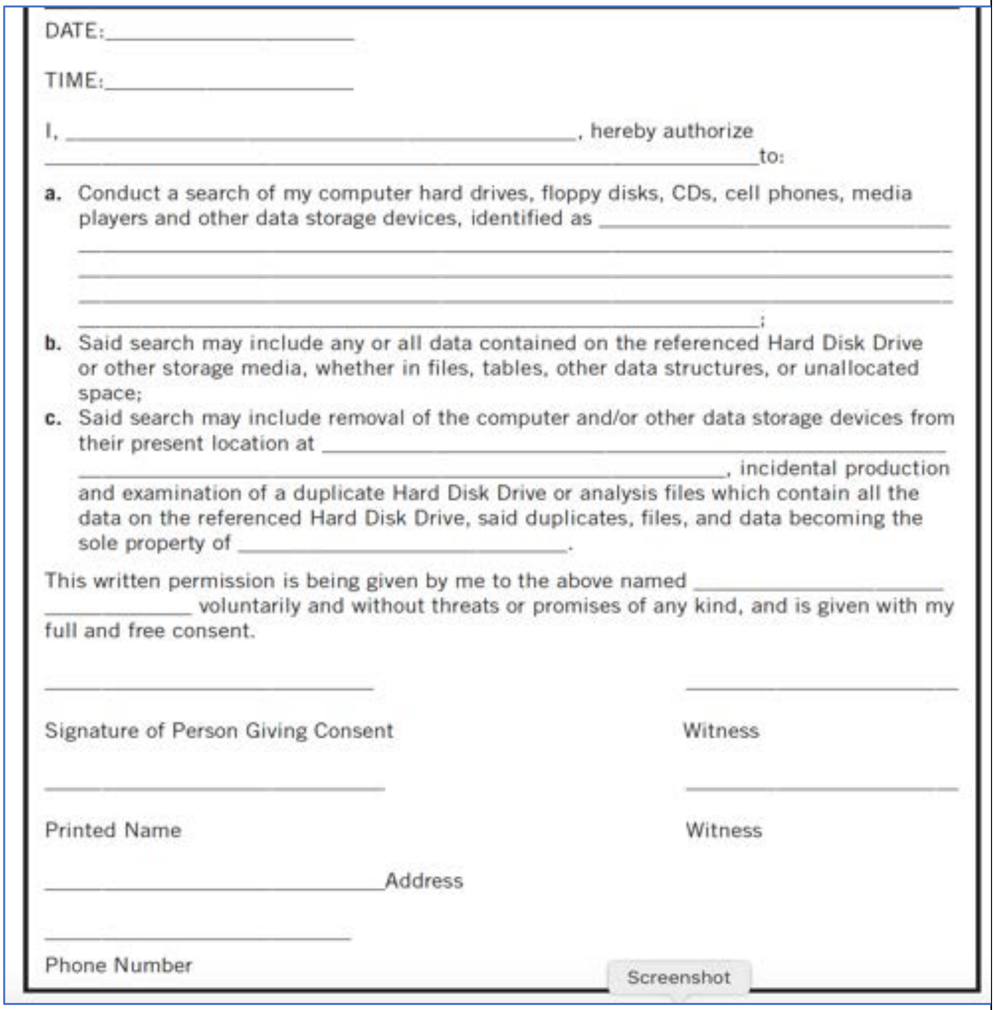
3. The ___________________ Sheiff shall serve this Order for Expedited Discovery upon Defendants as immediately as possible.

4. The information discovered in response to the inspection and copying permitted herein shall be used by Plaintiff solely for the prosecution of its claims, and for no other purpose whatsoever, unless and until the Court orders otherwise.

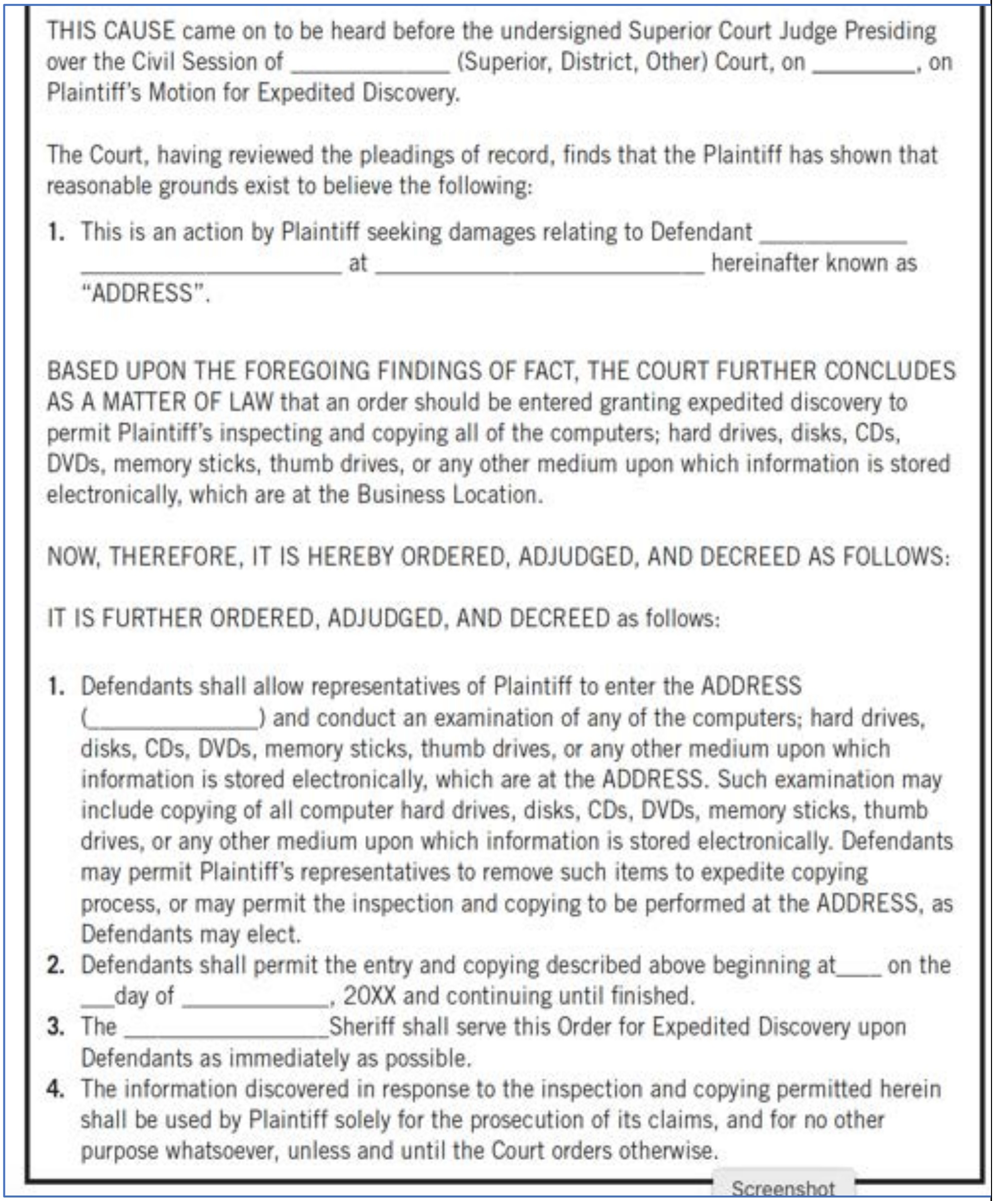
____
Superior Court Judge

DATE AND TIME ENTERED:_______________________

Figure 5.2: Example of a civil order for expedited discovery [1].

Content Template	
Section Number	5.4
Section Title	**Discovery of Computers and Storage Media**
Introduction	This section shows examples of evidence discovery on different storage media. The section also presents examples of the language used for the discovery orders, restraining orders, and a consent to search form.
Content	This section presents examples of the language used for the discovery orders, restraining orders, and a consent to search form. The consent to search form is used by the law enforcement agency to obtain permission that allows the search inside the electronic storage devices without the need to apply for a separate search warrant. This agreement is also used by any private individual to show that a person has agreed and provided the consent to search in a criminal or civil case. These consent forms as in Figure 5.3 are not notarized, but sometimes they can be notarized if for some reason those involved would like to provide additional document authentication.  DATE: ____________________ TIME: ____________________ I, ____, hereby authorize ____ to: **a.** Conduct a search of my computer hard drives, floppy disks, CDs, cell phones, media players and other data storage devices, identified as ____; **b.** Said search may include any or all data contained on the referenced Hard Disk Drive or other storage media, whether in files, tables, other data structures, or unallocated space; **c.** Said search may include removal of the computer and/or other data storage devices from their present location at ____, incidental production and examination of a duplicate Hard Disk Drive or analysis files which contain all the data on the referenced Hard Disk Drive, said duplicates, files, and data becoming the sole property of ______________________. This written permission is being given by me to the above named ____________________ voluntarily and without threats or promises of any kind, and is given with my full and free consent. ______________________ ______________________ Signature of Person Giving Consent Witness ______________________ ______________________ Printed Name Witness ______________________ Address ______________________ Phone Number Figure 5.3: Example of consent to search [1].

A simple order of an expedited discovery is given in the example in Figure 5.4. In this example, it is shown that the collection of evidence is allowed to be made by the opposition party.



THIS CAUSE came on to be heard before the undersigned Superior Court Judge Presiding over the Civil Session of _____________ (Superior, District, Other) Court, on _________, on Plaintiff's Motion for Expedited Discovery.

The Court, having reviewed the pleadings of record, finds that the Plaintiff has shown that reasonable grounds exist to believe the following:

1. This is an action by Plaintiff seeking damages relating to Defendant ____________ ______________________ at ____________________________ hereinafter known as "ADDRESS".

BASED UPON THE FOREGOING FINDINGS OF FACT, THE COURT FURTHER CONCLUDES AS A MATTER OF LAW that an order should be entered granting expedited discovery to permit Plaintiff's inspecting and copying all of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, which are at the Business Location.

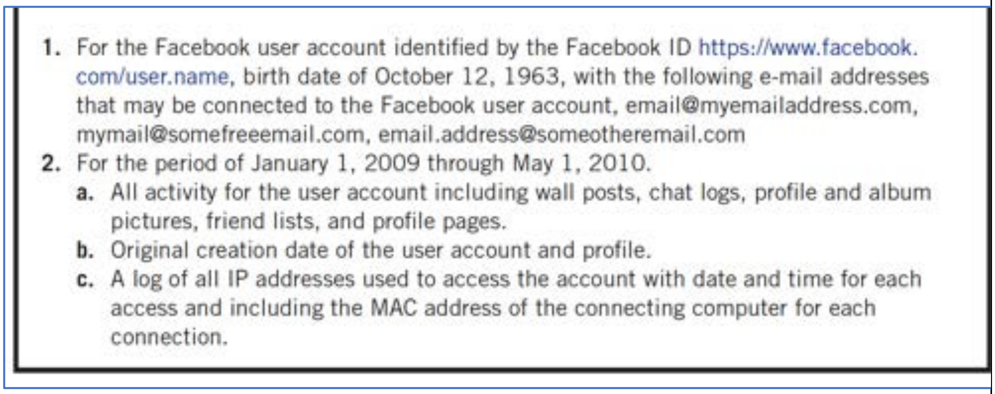
NOW, THEREFORE, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED AS FOLLOWS:

IT IS FURTHER ORDERED, ADJUDGED, AND DECREED as follows:

1. Defendants shall allow representatives of Plaintiff to enter the ADDRESS (______________) and conduct an examination of any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, which are at the ADDRESS. Such examination may include copying of all computer hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically. Defendants may permit Plaintiff's representatives to remove such items to expedite copying process, or may permit the inspection and copying to be performed at the ADDRESS, as Defendants may elect.
2. Defendants shall permit the entry and copying described above beginning at____ on the ___day of ____________, 20XX and continuing until finished.
3. The _________________Sheriff shall serve this Order for Expedited Discovery upon Defendants as immediately as possible.
4. The information discovered in response to the inspection and copying permitted herein shall be used by Plaintiff solely for the prosecution of its claims, and for no other purpose whatsoever, unless and until the Court orders otherwise.

Figure 5.4: example of a simple order for expedited Discovery [1].

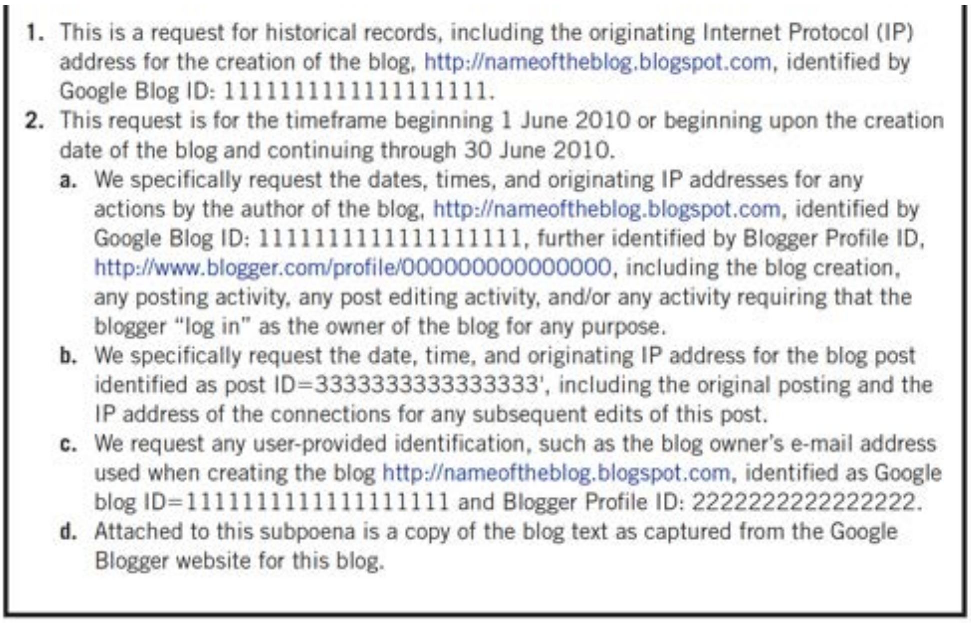
Other types of evidence discovery are related to the type of the device, and each discovery type has its own challenges and process. For example, there is video evidence discovery, audio evidence discovery and social media evidence discovery. While all types share very common procedures in evidence collection, preservation, analysis and presentation, the digital forensics expert has to use different technical language when requesting search or examination. For example, with regards to Facebook the expert needs to include the period of activity during which the case has occurred. The expert needs to provide other information that may help explain the case including e-mail addresses, birthdate, and person's name. The technical language that is used by an expert for getting information from Facebook profile is shown in figure 5.5.



1. For the Facebook user account identified by the Facebook ID https://www.facebook.com/user.name, birth date of October 12, 1963, with the following e-mail addresses that may be connected to the Facebook user account, email@myemailaddress.com, mymail@somefreeemail.com, email.address@someotheremail.com
2. For the period of January 1, 2009 through May 1, 2010.
   a. All activity for the user account including wall posts, chat logs, profile and album pictures, friend lists, and profile pages.
   b. Original creation date of the user account and profile.
   c. A log of all IP addresses used to access the account with date and time for each access and including the MAC address of the connecting computer for each connection.

Figure 5.5: An example of technical language used to obtain Facebook user information [1].

Google can be another example. Google can comply with a request for information regarding a specific post on the Blogger service when the expert provides information to identify the required data. Such information can include web address of the blog, internal ID of the blog, the date and time of the blog post, the individual post ID, the ID of the blog owner. A sample of the technical language used to request data from Google is shown in figure 5.5.



1. This is a request for historical records, including the originating Internet Protocol (IP) address for the creation of the blog, http://nameoftheblog.blogspot.com, identified by Google Blog ID: 111111111111111111.
2. This request is for the timeframe beginning 1 June 2010 or beginning upon the creation date of the blog and continuing through 30 June 2010.
   a. We specifically request the dates, times, and originating IP addresses for any actions by the author of the blog, http://nameoftheblog.blogspot.com, identified by Google Blog ID: 111111111111111111, further identified by Blogger Profile ID, http://www.blogger.com/profile/000000000000000, including the blog creation, any posting activity, any post editing activity, and/or any activity requiring that the blogger "log in" as the owner of the blog for any purpose.
   b. We specifically request the date, time, and originating IP address for the blog post identified as post ID=333333333333333', including the original posting and the IP address of the connections for any subsequent edits of this post.
   c. We request any user-provided identification, such as the blog owner's e-mail address used when creating the blog http://nameoftheblog.blogspot.com, identified as Google blog ID=111111111111111111 and Blogger Profile ID: 222222222222222.
   d. Attached to this subpoena is a copy of the blog text as captured from the Google Blogger website for this blog.

Figure 5.6: An example of technical language used to obtain information from Google [1].

Activity Template	
Number	5.1
Title	What are the rules that govern the discovery of digital evidence in civil cases in your country? Compare these rules and the federal rules in USA?
Type	• Research
Aim	To understand digital evidence discovery in civil and criminal cases
Description	Each student needs to write a report about the rules in his/her country
Timeline	One week
Assessment	Students need to produce an article of at least three pages. The main elements in the article are: 13- Rules in his/ her country 14- Comparison between their country rules and the USA federal rules

Think Template (MCQs)	
Number	5.1
Title	Challenges in criminal cases
Type	Choose correct answer
Question	The data on Drobox or Google drive does not pose a challenge to experts because such data cannot be changed by users
Answers	9- True **10-False**

Activity Template	
Number	5.2
Title	What are the devices that can store digital evidence, please categorize these devices?
Type	• Research
Aim	To understand the digital evidence discovery in civil and criminal cases
Description	Each student needs to write a report about the devices where digital evidence can be stored.
Timeline	One week
Assessment	Students need to produce an article of at least two pages. The main elements in the article are: 1- The name of the device and its function 2- The categories of the device

Think Template (MCQs)	
Number	5.2
Title	**Civil case evidence**
Type	Choose correct answer
Question	The rules governing evidence discovery in civil cases are different and are customized to each country
Answers	**3- True** 4- False

Think Template (MCQs)	
Number	5.3
Title	**Evidence Discovery specifics**
Type	Choose correct answer
Question	Only one format is allowed during the discovery of digital evidence
Answers	True **False**

Think Template (MCQs)	
Number	5.4
Title	**Discovery of evidence in computers and storage media**
Type	Choose the correct answer
Question	Because Google and Facebook provide social media services, the language to request evidence from them is the same
Answers	True **False**

Extra Template	
Number	5.1
Title	*Digital Forensics for Legal Professionals*
Topic	5.1, 5.2, 5.3, 5.4
Type	Daniel, Larry E. and Daniel, Lars E. 2012. *Digital Forensics for Legal Professionals*. 1st ed. Elsevier Inc.

Extra Template	
Number	5.2
Title	*Computer Forensics and Digital Investigation with EnCase Forensic V7*
Topic	5.1, 5.2, 5.3, 5.4
Type	Widup, Suzanne. 2014. *Computer Forensics and Digital Investigation with EnCase Forensic V7*. 1st ed. McGraw-Hill Education.

Extra Template	
Number	5.3
Title	*Digital Forensics*
Topic	5.1, 5.2, 5.3, 5.4
Type	A. Årnes, *Digital Forensics*, 1st ed. Wiley, 2017.

Extra Template	
Number	5.4
Title	*The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*.
Topic	5.1, 5.2, 5.3, 5.4
Type	J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2014.