ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

Master of Science(Cyber Security) (MSCS)

Computer Forensics
(CSP-18)

Block

1 Introduction to Computer Forensics

EXPERT COMMITTEE

Dr. P.K Behera **(Chairman)**
Reader in Computer Science
Utkal University
Bhubaneswar, Odisha

Dr.J.RMohanty **(Member)**
Professor and HOD
KIIT University
Bhubaneswar, Odisha

Sri PabitranandaPattnaik **(Member)**
Scientist-E, NIC
Bhubaneswar, Odisha

Sri Malaya Kumar Das **(Member)**
Scientist-E, NIC
Bhubaneswar, Odisha

Dr. Bhagirathi Nayak **(Member)**
Professor and Head (IT & System)
Sri Sri University, Bhubaneswar,Odisha

Dr.Manoranjan Pradhan **(Member)**
Professor and Head (IT & System)
G.I.T.A
Bhubaneswar, Odisha

Sri Chandrakant Mallick **(Convener)**
Consultant (Academic)
School of Computer and Information Science
Odisha State Open University
Sambalpur, Odisha

Master of Science(Cyber Security) (MSCS)

Course Writers
Aseem Kumar Patel
Academic Consultant
Odisha State Open University,Sambalpur

Material Production

Dr. Manas Ranjan Pujari
Registrar
Odisha State Open University, Sambalpur

Unit Structure

UNIT I: INTRODUCTION TO DIGITAL FORENSIC

1.1 Learning Objectives

After completion of this unit, we will be able to:

- Learn What is Digital Forensic and types
- Know the past and evolution of digital forensics
- Describe various types of cybercrime
- Realize the benefits of computer forensics
- Identify about forensics readiness
- Implement forensics readiness plan

1.2 Introduction

Digital forensics, the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/netbooks, tablets, smartphones, etc., was little-known a few years ago. However, with the growing incidence of cybercrime, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations.

As a rule of thumb, "Forensic is the scientific tests or techniques used in connection with the detection of crime." - ***Wikipedia***.

Case Scenario

Suppose Mr X is the computer forensics investigator in Odisha and he has been appointed to inspect data-stealing case in an MNC in Bhubaneswar. The general manager of the organization has confidence in that some of his employees are involved in the case including the network crack and the transfer of the confidential data. Mr X has started his investigation, Analyze, Evaluate the case and collected the evidence and then he submitted his final report to the Authority. According to the report, four employees were found accountable for data theft/ data-stealing. Based on this report, a case has been lodged against them.

In the situation mentioned above, the organization was the client, Mr X was the service provider and the service that was being provided is called computer forensics & digital investigation services.

1.3 Definition of Computer Forensics

Computer Forensics is the process of using scientific techniques during the identification, collection, examination and reporting the evidence to the court. So what computer forensics is all about?

According to Dr H.B. Wolfe, computer forensics is, "A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media that can be presented in a court of law in a coherent and meaningful format."

If we further define computer forensics then, it is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.

The scope of computer forensics is not limited to investigating a crime only. Apart from this, computer forensics can be used for:

- Data recovery
- Log monitoring
- Data acquisition (from the retired or damaged devices)
- Fulfil the compliance needs

1.4 Cybercrime

Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Dr. Debarati Halder and Dr K. Jaishankar define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation-state is sometimes referred to as cyberwarfare.

Digital forensics is traditionally associated with criminal investigations and, as you would expect, most types of investigation centre on some form of computer crime. This sort of crime can take two forms; computer-based crime and computer-facilitated crime.

1.4.1 Computer-based crime

This is criminal activity that is conducted purely on computers, for example, cyber-bullying or spam. As well as crimes newly defined by the computing age it also includes traditional crime conducted purely on computers (for example, child pornography).

1.4.2 Computer facilitated crime

Crime conducted in the "real world" but facilitated by the use of computers. A classic example of this sort of crime is a fraud: computers are commonly used to communicate with other fraudsters, to record/plan activities or to create fraudulent documents.

Not all digital forensics investigations focus on criminal behavior; sometimes the techniques are used to incorporate (or private) settings to recover lost information or to rebuild the activities of employees.

1.5 Evolution of Computer Forensics

Most of the experts agree that the field of computer forensics began to develop more than 40 years ago.

By the 1970s, electronic crimes were increasing, especially in the financial sector. Most computers in this era were mainframes, used by trained people with specialized skills who worked in finance, engineering, and academia. White-collar fraud began when people in these industries saw a way to make money by manipulating computer data. One of the most well-known crimes of the mainframe era is the one-half cent crime. Banks commonly tracked money in accounts to the third decimal place or more. They used and still use the "rounding

up" accounting method when paying interest. If the interest applied to an account resulted in a fraction of a cent, that fraction was used in the calculation for the next account until the total resulted in a whole cent. It was assumed that sooner or later every customer would benefit.

Some computer programmers corrupted this method by opening an account for themselves and writing programs that diverted all the fractional monies into their accounts. In small banks, this practice amounted to only a few hundred dollars a month. In large banks with many branch offices, however, the amount reached hundreds of thousands of dollars.

The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents.

In 1984, FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.

By the early 1990s, specialized tools for computer forensics were available. In 1988, the International Association of Computer Investigative Specialists (IACIS), an international non-profit corporation composed of volunteer computer forensic professionals introduced training on software for forensics investigations. However, no commercial GUI software for computer forensics was available until ASR Data created Expert Witness for Macintosh. This software could recover deleted files and fragments of deleted files. One of the ASR Data partners later left and developed EnCase, which has become a popular computer forensics tool.

It was followed by the formation of International Organization on Computer Evidence (IOCE) in 1995, which aims to brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

With the rise in cybercrime, the G8 nations realized the importance of computer forensics, and in 1997 declared that - Law enforcement personnel must be trained and equipped to address high-tech crimes. In 1998, G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. In the same year, INTERPOL Forensic Science Symposium was held. The First FBI Regional Computer Forensic Laboratory established in 2000 at San Diego.

As computer technology continued to evolve, more computer forensics software was developed. "ILook", is a Cyber forensic tool maintained by the IRS Criminal Investigation Division and limited to law enforcement, can analyze and read special files that are copies of a disk. Access Data Forensic Toolkit (FTK) has become a popular commercial product that performs similar tasks in the law enforcement and civilian markets.

Computers are getting more powerful day by day, so the field of computer forensics must rapidly evolve. Previously, we had many computer forensic tools that were used to apply forensic techniques to the computer. However, we have listed a few best forensic tools that are promising for today's computers:

- SANS SIFT
- ProDiscover Forensic
- Volatility Framework
- The Sleuth Kit (+Autopsy)
- CAINE (Computer Aided Investigative Environment)
- Xplico
- X-Ways Forensics

In this material, we will try to discuss as many tools as possible but you should also refer to trade publications and Web sites, such as www.ctin.org (Computer Technology Investigators Network) and www.usdoj.gov (U.S. Department of Justice), to stay updated.

1.6 Different types of digital forensics

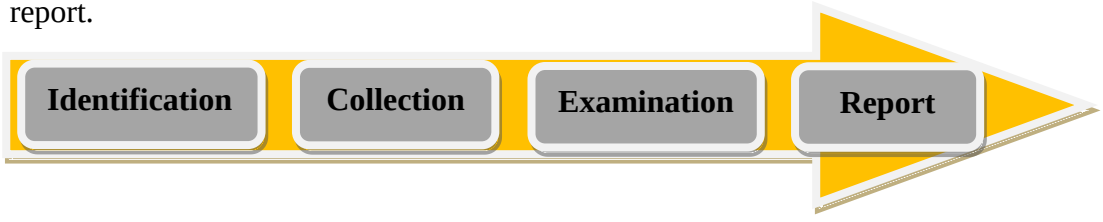
Digital forensics is a constantly evolving scientific field with many sub-disciplines. Some of these sub-disciplines are:

1) **Computer Forensics**: the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.
2) **Network Forensics**: the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
3) **Mobile devises Forensics**: the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.
4) **Digital Image Forensics**: the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
5) **Digital Video/Audio Forensics:** the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
6) **Memory forensics:** the recovery of evidence from the RAM of a running computer, also called live acquisition.
7) **Cloud Forensics:** Cloud Forensics is actually an application within Digital Forensics which oversees the crime committed over the cloud and investigates on it.

1.7 Stages of Computer Forensics Process

The overall computer forensics process is sometimes viewed as comprising of four stages:

- **Assess the situation/ Identification:** Analyze the scope of the investigation and the action to be taken.
- **Acquire the data/ Collection:** Gather, protect, and preserve the original evidence.
- **Analyze the data/Examination:** Examine and correlate digital evidence with events of interest that will help you make a case.
- **Report the investigation:** Gather and organize collected information and write the final report.



Assess the situation/ Identification

The first process of computer forensics is to identify the scenario or to understand the case. At this stage, the investigator has to identify the need of the investigation, type of incident, parties that involved in the incidence, and the resources that are required to fulfil the needs of the case.

Acquire the data/ Collection

The collection (chain of custody) is one of the important steps because your entire case is based on the evidence collected from the crime scene. The collection is the data acquisition process from the relevant data sources while maintaining the integrity of data. Timely execution of the collection process is crucial in order to maintain the confidentiality and integrity of the data. Important evidence may lose if not acted as required.

Analyze the data/Examination

The aim of the third process is to examine the collected data by following standard procedures, techniques, tools and methodology to extract the meaningful information related to the case. At this stage, the investigator searches for the possible evidence against the suspect, if any. Use the tools and techniques to analyze the data. Techniques and tools should be justified legally because it helps you to create and present your report in front of the court.

Report the investigation

This is the final and most important step in the investigation process. At this step, an investigator needs to document the process used for the above steps. The investigation report also consists of the documentation of how the tools and procedures were being selected. The objective of this step is to report and present the findings justified by the evidence. Every step mentioned above can be further divided into many parts and every part has its own standard operating procedures (SOP), we will discuss this in detail in the next unit.

1.8 Need of computer forensics

1. The world has become a global village since the beginning of computer, digital devices & the internet. Life seems impossible without these technologies, as they are necessary for our workplace, home, street, and everywhere. Information can be stored or transferred by desktop computers, laptop, routers, printers, CD/DVD, flash drive, or thumb drive. The variations and development of data storage and transfer capabilities have encouraged the development of forensic tools, techniques, procedures and investigators.
2. With the ever-increasing rate of cybercrimes, from phishing to hacking and stealing of personal information not only just limited to a particular country but globally at large, there is a need for forensic experts to be available in public and private organizations. To be able to handle this, it's vital for network administrator and security staff of networked organizations to have the knowledge to make sure that they have the laws relating to this on their fingertips. This would ensure that should need for the service avail itself, then they would come in and rescue the situation.
3. The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics. They should be taken as the main element of computer and network security. It would be a great benefit for a company if it has knowledge of all the technical and legal aspects of this field. It will be of help in the provision of evidence and prosecution of the case in the court of law.
4. New laws aimed at the protection of customer's data are continuously being developed. Should they lose data, then naturally the liability goes to the company. Such cases, if they occur will automatically result in the company or organization being brought to the court of law for failure to protect personal data, this can turn out

to be very expensive. But through the application of forensic science, huge chunks of money can be saved by the firms concerned.

It simply means that there is a necessity in investment in either employing an expert in computer forensic in the firms or having part of their staff trained into this project so as to help in detection of such cases.

1.9 Rules of Computer Forensic

There are certain rules and boundaries that should be kept in mind while conducting an investigation.

Matthew Braid, in his AusCERT paper, 'Collecting Electronic Evidence after a System Compromise' has provided the rules of computer forensics:

1) **Minimize or eliminate the chances of examining the original evidence:**
   Make the accurate and exact copy of the collected information to minimize the option of examining the original. This is the first and the most important rule that should be considered before doing any investigation, create duplicates and investigate the duplicates. You should make the exact copy in order to maintain the integrity of the data.

2) **Don't Proceed if it is beyond your knowledge**
   If you see a roadblock while investigating, then stop at that moment and do not proceed if it is beyond your knowledge and skills, consult or ask an experienced to guide you in a particular matter. This is to secure the data, otherwise, the data might be damaged which is unbearable. Do not take this situation as a challenge, go and get additional training because we are in the learning process and we love to learn.

3) **Follow the rules of evidence**
   You might be worried because we have not discussed any rule of evidence yet, but the next topic will be about evidence. The rule of evidence must be followed during the investigation process to make sure that the evidence will be accepted in court.

4) **Create Document**
   Document the behaviour, if any changes occur in evidence. An investigator should document the reason, result and the nature of change occurred with the evidence. Let say, restarting a machine may change its temporary files, note it down.

5) **Get the written permission and follow the local security policy**
   Before starting an investigation process, you should make sure to have written permission with instruction related to the scope of your investigation. It is very important because during the investigation you need to get access or need to make copies of the sensitive data, if the written permission is not with you then you may find yourself in trouble for breaching the IT security policy.

6) **Be ready to testify**
   Since you are collecting the evidence then you should make yourself ready to testify it in the court, otherwise the collected evidence may become inadmissible.

7) **Your action should be repeatable**
   Do not work on trial-and -error, else no one is going to believe you and your investigation. Make sure to document every step taken. You should be confident enough to perform the same action again to prove the authenticity of the evidence.

8) **Work fast to reduce data loss**
   Work fast to eliminate the chances of data loss, volatile data may be lost if not collected in time. While automation can also be introduced to speed up the process, do not create a rush situation. Increase the human workforce where needed.

Always start collecting data from volatile evidence.

9) **Don't shut down before collecting evidence**
   This is a rule of thumb since the collection of data or evidence itself is important for an investigation. You should make sure not to shut down the system before you collect all the evidence. If the system is shut down, then you will lose the volatile data. Shutdown and rebooting should be avoided at all cost.

10) **Don't run any program on the affected system**
    Collect all the evidence, copy them, create many duplicates and work on them. Do not run any program, otherwise, you may trigger something that you don't want to trigger. Think of a Trojan horse.

1.10 Computer Forensics Team

As per Irfan Shakeel in his Book "Introduction to Computer Forensics & Digital Investigation" mention about the key people that a computer investigation firm should have. Which is as follows.
Law enforcement and security agencies are responsible for investigating computer crime, however, every organization should have the capability to solve their basic issues and investigation by themselves.

Even an organization can hire experts from small or mid-size computer investigation firms. Also, you can create your own firm that provides computer forensic services. To do so, you need a forensics lab, permission from the government to establish a forensics business, the right tools with the right people and rules/policies to run the business effectively and efficiently.

Without this ability, it is very hard for an organization to determine the fraud, illegal activities, policy, or network breach or even they will find it hard to implement the cybersecurity rules in the organization. The need for such abilities may vary and it depends on the nature of business, security threats and the possible loss.

Here are the key people that a computer investigation firm should have:

- **Investigators:** This is a group of people (number depends on the size of the firm) who handle and solve the case. It is their job to use forensic tools and techniques in order to find evidence against the suspect. They may call law enforcement agencies if required. Investigators are supposed to act immediately after the occurrence of the event that is suspected of criminal activity.
- **Photographer:** To record the crime scene is as important as investigating it. The photographer's job is to take photographs of the crime scene (IT devices and other equipment).
- **Incident Handlers (first responder):** Every organization, regardless of type, should have incident handlers in their IT department. The responsibility of these people is to monitor and act if any computer security incidence happens, such as breaching of network policy, code injection, server hijacking, RAT or any other malicious code installation. They generally use a variety of computer forensics tools to accomplish their job.
- **IT Engineers & technicians** (other support staff): This is the group of people who run the daily operation of the firm. They are IT engineers and technicians to maintain the forensics lab. This team should consist of a network administrator, IT support, IT security engineers and desktop support. The key role of this team is to make sure the smooth organizational functions, monitoring, troubleshooting, data recovery and to maintain the required backup.

- **Attorney:** Since computer forensics directly deal with investigation and to submit the case in the court, an attorney should be a part of this team.

First Responder (Incident Handlers)

The first responder and the function of the first responder are crucial for computer forensics and investigation. The first responder is the first person notified, and act to the security incident. The first responder toolkit will be discussed in the upcoming chapters, but at this stage, I will discuss the roles and responsibilities of the first responder.

The first responder is a role that could be assigned to anyone, including IT security engineers, network administrator and others. The person who is responsible to act as a first responder should have knowledge, skills and the toolkit of first responders.

The first responder should be ready to handle any situation and his/her action should be planned and well documented. Some core responsibilities are as follows:

- Figure out or understand the situation, event and problem.
- Gather and collect the information from the crime scene
- Discuss the collected information with the other team members
- Document each and everything

First responder or incident handlers should have the first-hand experience of Information security, different operating systems and their architectures.

1.11 Forensics Readiness

There are several reasons for this field ‘s growth; the most significant being that computers are everywhere. You‘d be hard-pressed to find a household today without at least one computer. And it is not just computers that computer forensic examiners get involved with. Computer forensic examiners analyze all types of technical devices like cell phones, iPods, Tablets, PDAs, and text messaging. Computer forensic examiners analyze all of these electronic devices! Cyber forensics is a rapidly changing field. There are new technologies coming out daily that are becoming smaller, but storing more and more data. This leads to why cyber forensics is import. In computer- related crimes, such as identity fraud, it is becoming easier to hide data. With the proper analysis of digital evidence, better security can be made to protect computer users, but also catch those who are committing the crimes. Organizations have now realized the importance of being prepared to fight cybercriminals with their forensic readiness plan ready.

1.11.1 What is Forensics Readiness?

Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whereas minimizing the costs of an investigation. Digital evidence can be in the form of log files, emails, back-up disks, portable computers, network traffic records, and telephone records etc.

CESG Good Practice Guide No. 18, *Forensic Readiness*, defines forensic readiness as: “The achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law.

Modern digital technologies not only present new opportunities to business organizations but also a different set of issues and challenges that need to be resolved. With the rising threats of cybercrimes, many organizations, as well as law enforcement agencies globally, are now establishing proactive measures as a way to increase their ability to respond to security

incidents as well as create a digital forensic ready environment.

Forensic readiness as defined by Mohay (2005) as the extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations.

1.11.2 Goals of Forensic Readiness

Some of the important goals of forensics readiness are:

- to gather admissible evidence legally and without interfering with business processes;
- to gather evidence targeting the potential crimes and disputes that may adversely impact an organisation;
- to allow an investigation to proceed at a cost in proportion to the incident;
- to minimise interruption to the business from any investigation; and
- to ensure that evidence makes a positive impact on the outcome of any legal action.

1.11.3 Benefits of Forensic Readiness

Forensic readiness can offer an organisation the following benefits:

- evidence can be gathered to act in an organisation's defence if subject to a lawsuit;
- comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cybercriminal);
- in the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- a systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- a structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- forensic readiness can extend the scope of information security to the wider threat from cybercrime, such as intellectual property protection, fraud, extortion etc;
- it demonstrates due diligence and good corporate governance of the company's information assets;
- it can demonstrate that regulatory requirements have been met;
- it can improve and facilitate the interface to law enforcement if involved;
- it can improve the prospects for a successful legal action;
- it can provide evidence to resolve a commercial dispute; and
- it can support employee sanctions based on digital evidence (for example to prove a violation of acceptable use policy)

1.11.4 Steps for Forensic Readiness Planning

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence;
2. Identify available sources and different types of potential evidence;
3. Determine the evidence collection requirement;
4. Establish a capability for securely gathering legally admissible evidence to meet the

requirement;

5. Establish a policy for secure storage and handling of potential evidence;
6. Ensure monitoring is targeted to detect and deter major incidents;
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;
9. Document an evidence-based case describing the incident and its impact; and
10. Ensure legal review to facilitate action in response to the incident.

An IT auditor performing a forensic readiness assessment should check to see that the above points can be deduced from the forensic readiness policy of an organization.
The remainder of this section gives a brief description of each of the ten steps.

1. **Define the business scenarios that require digital evidence:** The first step in forensic readiness is to define the purpose of an evidence collection capability. The rationale is to look at the risk and potential impact on the business from the various types of crimes and disputes. What is the threat to the business and what parts are vulnerable? This is, in effect, a risk assessment, and is performed at the business level. The aim is to understand the business scenarios where digital evidence may be required and may benefit the organisation the event that it is required. In general, the areas where digital evidence can be applied include:
   - reducing the impact of computer-related crime;
   - dealing effectively with court orders to release data;
   - demonstrating compliance with regulatory or legal constraints;
   - producing evidence to support company disciplinary issues;
   - supporting contractual and commercial agreements; and
   - proving the impact of a crime or dispute.

   In assessing these scenarios, this step provides an indication of the likely benefits of being able to use digital evidence. If the identified risks, and the potential benefits of forensic readiness, suggest a good return on investment is achievable, then an organisation needs to consider what evidence to gather for the various risk scenarios.

2. **Identify available sources and different types of potential evidence:** The second step in forensic readiness is for an organisation to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. Computer logs can originate from many sources. The purpose of this step is to scope what evidence may be available from across the range of systems and applications in use. Some basic questions need to be asked about possible evidence sources to include.
   - Where does data generated?
   - What format is it in?
   - How long is it stored for?
   - How is it currently controlled, secured and managed?
   - Who has access to the data?
   - How much is produced?

- Is it archived? If so where and for how long?
- How much is reviewed?
- What additional evidence sources could be enabled?
- Who is responsible for this data?
- Who is the formal owner of the data?
- How could it be made available to an investigation?
- What business processes does it relate to?
- Does it contain personal information?

Email is an obvious example of a potentially rich source of evidence that needs careful consideration in terms of storage, archiving & auditing and retrieval. But this is not the only means of communication used over the internet, there is also instant messaging, web-based email that bypasses corporate email servers, chat-rooms and newsgroups, even voice over the internet. Each of these may need preserving and archiving. The range of possible evidence sources includes:

- equipment such as routers, firewalls, servers, clients, portables, embedded devices etc.
- application software such as accounting packages etc. for evidence of fraud, ERP packages for employee records and activities (e.g. in case of identity theft), system and management files etc.
- monitoring software such as intrusion detection software, packet sniffers, keyboard loggers, content checkers, etc.
- general logs such as access logs, printer logs, web traffic, internal network logs, internet traffic, database transactions, commercial transactions etc.
- other sources such as CCTV, door access records, phone logs, PABX data etc. and back-ups and archives.

3. **Determine the Evidence Collection Requirement:** It is now possible to decide which of the possible evidence sources identified in step 2 can help deal with the crimes and disputes identified in step 1 and whether further ways to gather evidence are required. This is the evidence collection requirement. The purpose of this step is to produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring information systems through an agreed requirement for evidence. One of the key benefits of this step is the bringing together of IT with the needs of corporate security. IT audit logs have been traditionally configured by systems administrators independently of corporate policy and where such a policy exists there is often a significant gap between organizational security objectives and the 'bottom-up' auditing actually implemented. The evidence collection requirement is moderated by a cost- benefit analysis of how much the required evidence will cost to collect and what benefit it provides (see above). The critical question for successful forensic readiness is what can be performed cost-effectively. By considering these issues in advance and choosing storage options, auditing tools, investigation tools, and appropriate procedures it is possible for an organisation to reduce the costs of future forensic investigations.
4. **Establish a capability for securely gathering legally admissible evidence to meet the requirement:** At this point, the organisation knows the totality of evidence available and

has decided which of it can be collected to address the company risks and within a planned budget. With the evidence requirement understood, the next step is to ensure that it is collected from the relevant sources and that it is preserved as an authentic record. At this stage legal advice is required to ensure that the evidence can be gathered legally and the evidence required can be met in the manner planned. For example, does it involve monitoring personal emails, the use of personal data, or
fishing trips on employee activities? In some countries, some or all of these activities may be illegal. Relevant laws, in the areas of data protection, privacy and human rights, will inevitably constrain what can actually be gathered. Some of the guidelines are:

- monitoring should be targeted at specific problems.
- it should only be gathered for defined purposes and nothing more, and
- staff should be told what monitoring is happening except in exceptional circumstances.

Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage. As well as preventative measures such as secure rooms and swipe card access it is also prudent to have records of who has access to the general location and who has access to the actual machines containing evidence. Any evidence or paperwork associated with a specific investigation should be given added security by, for example, storing in a safe. Additional security of logs can also be achieved through the use of WORM storage media.

5. **Establish a policy for secure storage and handling of potential evidence:** The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required. It concerns the long-term or off-line storage of information that might be required for evidence at a later date. A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence. In the parlance of investigators, this is known as continuity of evidence (in the UK) and chain of custody (in the US). The continuity of evidence also includes records of who held, and who had access to, the evidence (for example from swipe control door logs). A significant contribution to the legal collection of evidence is given by the code of practice on the legal admissibility and weight of information stored electronically, published by the British Standards Institution. This document originated from a perceived need for evidence collection in the paperless office. The problem is addressed is if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability? The current edition broadens the scope to all information management systems, Ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication such as those where information is transmitted over networks such as email systems for example. It points out that methods of storage, hardware reliability, operation and access control, and even the programs and source code, may be investigated in order to determine admissibility. A closely related international standard is being developed as ISO 15801. The required output of this step is a secure evidence policy. It should document the security measures, the legal

advice and the procedural measures used to ensure the evidence requirement is met. Upon this document rests the likely admissibility and weight of any evidence gathered.

6. **Ensure monitoring and auditing are targeted to detect and deter major incidents:** In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatening incidents in a timely manner. This is directly analogous to Intrusion Detection Systems (IDS), extended beyond network attack to a wide range of behaviours that may have implications for the organisation. It is all very well collecting the evidence. This step is about making sure it can be used in the process of detection. By monitoring sources of evidence, we can look for the triggers that mean something suspicious may be happening. The critical question in this step is when should an organisation be suspicious? A suspicious event has to be related to business risk and not couched in technical terms. Thus, the onus is on managers to explain to those monitoring the data what they want to prevent and thus the sort of behaviour that IDS might be used to detect for example. This should be captured in a 'suspicion' policy that helps the various monitoring and auditing staff understand what triggers should provoke suspicion, who to report the suspicion to, whether heightened monitoring is required, and whether any additional security measures should be taken as a precaution. Each type of monitoring should produce a proportion of false positives. The sensitivity of triggers can be varied as long as the overall false-positive rate does not become so high that suspicious events cannot be properly reviewed.

   Varying triggers also guards against the risk from someone who knows what the threshold on a particular event is and makes sure any events or transactions he wishes to hide are beneath it.

7. **Specify circumstances when escalation to a full formal investigation (which may use digital evidence) is required:** Some suspicious events can be system generated, such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness. Each suspicious event found in step 6 needs to be reviewed. Either an event will require escalation if it is clearly serious enough, or it will require enhanced monitoring or other precautionary measures, or it is a false positive. The purpose of this step is to decide how to react to the suspicious event. The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed. The decision criteria should be captured in an escalation policy that makes it clear when a suspicious event becomes a confirmed incident. At this point, an investigation should be launched and policy should indicate who the points of contact are (potentially available on a 24x7 basis) and who else needs to be involved. As with steps 3 and 6, the network and IT security managers and the non-IT managers need to understand each other's position. What level of certainty or level of risk is appropriate for an escalation? What strength of case is required to proceed? A preliminary business impact assessment should be made based on whether any of the following are present:
   - evidence of a reportable crime
   - evidence of internal fraud, theft, other loss
   - the estimate of possible damages (a threshold may induce an escalation trigger)
   - potential for embarrassment, reputation loss

- any immediate impact on customers, partners or profitability
- recovery plans have been enacted or are required; and
- the incident is reportable under a compliance regime.

8. **Train staff, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence:**

   A wide range of staff may become involved in a computer security incident. The aim of this step is to ensure that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. It is also necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence. There will be some issues relevant to all staff if they become involved in an incident. The following groups will require more specialized awareness training for example:
   - the investigating team;
   - corporate HR department;
   - corporate PR department (to manage any public information about the incident);
   - 'owners' of business processes or data;
   - line management, profit centre managers;
   - corporate security;
   - system administrators;
   - IT management;
   - legal advisers; and
   - senior management (potentially up to board level).

   At all times those involved should act according to ‘need to know’ principles. They should be particularly aware whether any staff, such as ‘whistle blowers’ and investigators, need to be protected from possible retaliation by keeping their names and their involvement confidential. Training may also be required to understand the relationships and necessary communications with external organisations that may become involved.

9. **Present an evidence-based case describing the incident and its impact:** The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. The questions go along the lines of who, what, why, when, where and how. Credibility is provided by evidence and a logical argument. The purpose of this step is to produce a policy that describes how an evidence-based case should be assembled. A case file may be required for a number of reasons:
   - to provide a basis for interaction with legal advisers and law enforcement;
   - to support a report to a regulatory body;
   - to support an insurance claim;
   - to justify disciplinary action;
   - to provide feedback on how such an incident can be avoided in future;
   - to provide a record in case of a similar event in the future (supports the corporate memory so that even if there are changes in personnel it will still be possible to understand what has happened); and
   - to provide further evidence if required in the future, for example, if no action is deemed necessary at this point but further developments occur.

10. **Ensure legal review to facilitate action in response to the incident:** At certain points during the collating of the cyber-crime case file, it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions. Legal advisers should be able to advise on the strength of the case and suggest whether additional measures should be taken; for example, if the evidence is weak is it necessary to catch an internal suspect red- handed by monitoring their activity and seizing their PC? Any progression to a formal action will need to be justified, cost-effective and assessed as likely to end in the company's favour. Although the actual decision of how to proceed will clearly be post-incident, considerable legal preparation is required in readiness. Legal advisors should be trained and experienced in the appropriate cyber laws and evidence admissibility issues. They need to be prepared to act on an incident, pursuant to the digital evidence that has been gathered and the case presented in step 9. Legal advice should also recognise that the legal issues may span legal jurisdictions e.g. states in the US, member states in the EU. Advice from legal advisers will include:
    - any liabilities from the incident and how they can be managed;
    - finding and prosecuting/punishing (internal versus external culprits);
    - legal and regulatory constraints on what action can be taken;
        - reputation protection and PR issues; when/if to advise partners, customers and investors;
        - how to deal with employees;
        - resolving commercial disputes; and
        - any additional measures required.

1.12 Summary

1. Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible.
2. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.
3. Computer crime, or cybercrime, is any crime that involves a computer and a network.
4. Activity crossing international borders and involving the interests of at least one nation-state is sometimes referred to as cyberwarfare.
5. The ancient Chinese used fingerprints to identify business documents.
6. Sir Francis Galton established the first system for classifying fingerprints.
7. International Association of Computer Investigative Specialists(IACIS) is an international non-profit corporation composed of volunteer computer forensic professionals dedicated to training and certifying practitioners in the field of forensic computer science.
8. The First FBI Regional Computer Forensic Laboratory established in 2000 at San Diego.
9. The survival and integrity of any given network infrastructure of any company or organization strongly depend on the application of computer forensics.
10. Forensic readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.
11. Monitoring should be targeted at specific problems.

12. Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage.
13. A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence.
14. In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatening incidents in a timely manner.
15. Some suspicious events can be system generated, such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness.
16. The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed.
17. It is necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence.
18. The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible.
19. At certain points during the collating of the cyber-crime case file, it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions.

1.13 CHECK YOUR PROGRESS

1. Fill in the blanks

i. _____was one of the first applications of forensics.
ii. FBI Magnetic Media program was later renamed to _____.
iii. _____is provided by evidence and a logical argument.
iv. At all times those involved should act according to _____principles.
v. IACIS stands for._____
vi. The first step in forensic readiness is to define _____of an evidence collection capability.
vii. It is not just the content of emails, documents and other files which may be of interest to investigators but also the _____associated with those files.
viii. IDS stand for _____.
ix. The decision criteria should be captured in an _____ policy that makes it clear when a suspicious event becomes a confirmed incident.

x. IOCE stands for International_____.

2. State true or false

i. Cybercrime, is any crime that involves a computer and a network.

ii. Computer based crime is criminal activity that is conducted purely on computers, for example cyber-bullying or spam.

iii. The goal of forensic readiness is to gather admissible evidence legally and without interfering with business processes.

iv. FBI Magnetic Media program started in 1994.

v. IOCE aims to bring together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

vi. Logs can originate from only one source in a computer.

vii. The range of possible evidence sources includes equipment such as routers, firewalls, servers, clients, portables, embedded devices etc.

viii. Email is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving and auditing and retrieval.

ix. Staff should not be told what monitoring is happening except in exceptional circumstances.

1.14 Answers to Check Your Progress

1. Fill in the blanks

i. Fingerprinting
ii. Computer Analysis and Response Team (CART).
iii. Credibility
iv. need to know
v. International Association of Computer Investigative Specialists
vi. purpose
vii. metadata
viii. Intrusion Detection Systems.
ix. escalation
x. International Organization on Computer Evidence.

2. State true or false

i. True
ii. True
iii. True
iv. False
v. True
vi. False
vii. True
viii. True
ix. False

1.15 Model Questions

1. What are the four stages of the computer forensic process?
2. What are the uses of computer forensics?
3. What are the objectives of computer forensics?
4. What is the role of a forensic investigator?
5. What is forensic readiness plan?
6. What are the benefits of forensic readiness?
7. What are the various steps involved in forensic readiness planning?
8. What is the continuity of evidence?

1.16 References:

https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf