2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

CHAPTER TWO

Introduction to Digital Forensics and Digital Evidences

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Introduction to Digital Forensic

- Forensic science is a well-established science that plays a critical role in criminal justice systems.
- Forensic science is often referred to as forensics.
- Digital forensics is also referred to as digital forensic science, a branch of computer forensic science that includes the restoration and inspection of material detected in digital devices, often in relation to a cybercrime.
- Digital Forensic is a series of steps to uncover and analyze electronic data through scientific method.The major goal of the process is to duplicate original data and preserve original evidence then performing the series of the investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Need of Digital Forensic

- The meaning of the word “forensics” is “to bring to the court”.
- It is necessary for network administrator and security staff of networked organizations to practice computer forensics and should have knowledge of laws, because rate of cyber crimes is increasing greatly.
- the major goal of computer forensics is to recognize, gather, protect and examine data in such a way that protects the integrity of the collected evidence to use it efficiently and effectively in a case.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Rules of Digital Forensic

Rule 1. An examination should never be performed on the original media.

Rule 2. A copy is made onto forensically sterile media. New media should always be used if available.

Rule 3. The copy of the evidence must be an exact, bit-by-bit copy (Sometimes referred to as a bit-stream copy).

Rule 4. The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified (Use a write blocking device when possible).

Rule 5. The examination must be conducted in such a way as to prevent any modification of the evidence.

Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Types of Digital Forensic

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, that is, worms, virus, or malware attacks, abnormal network traffic and security breaches.
3. **Mobile Devices Forensics** – the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets, and game consoles. Mobile device forensics involves the recovery of digital evidence or data from mobile devices.
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.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Ethical Issues

- "Ethics" is derived from the ancient Greek word ethikos, meaning "moral, showing moral character". Ethics in digital forensics field can be defined as a set of moral principles that regulate the use of computers; some common drawbacks of computer forensics include intellectual property resources, privacy concerns, and the impact of computers on the society.
- Ethical decision-making in digital forensics work comprises of one or more of the following:
  1. Honesty toward the investigation.
  2. Prudence means carefully handling the digital evidences.
  3. Compliance with the law and professional norms.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

General Ethics Norms for Investigator in Digital Forensic Field

Before starting the investigation in the digital forensic field, the investigator should satisfy the following points.

1. Should contribute to the society and human being.
2. Should avoid harm to others.
3. Should be honest and trustworthy.
4. Should be fair and take action not to discriminate.
5. Should honor property rights, including copyrights and patents.
6. Should give proper credit to intellectual property.
7. Should respect the privacy of others.
8. Should honor confidentiality.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Unethical Norms for Digital Forensic Investigation

The investigator should not:

1. Uphold any relevant evidence.
2. Declare any confidential matters or knowledge learned in an investigation without an order from a court of competent jurisdiction or without the client's consent.
3. Express an opinion on the guilt or innocence belonging to any party.
4. Engage or involve in any kind of unethical or illegal conduct.
5. Deliberately or knowingly undertake an assignment beyond his or her capability.
6. Distort or falsify education, training or credentials.
7. Display bias or prejudice in findings or observations.
8. Exceed or outpace authorization in conducting examinations.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Digital Forensic Investigations

- Digital investigations, DFIs, forensic examination, and forensic investigations have been used to describe an investigation where a digital device forms part of the incident.
- A DFI is thus a special type of investigation wherever scientific procedures and techniques used can permit the results, that is, the digital proof, to be allowable in a court of law.
- The results of a DFI should have a legal basis. Proof cannot be directly read, and a few tools are employed to look at the state of the information.
- Digital forensic investigation or DFI is a special type of investigation where the scientific procedures and techniques used will be allowed to view the results – digital evidence – to be admissible in a court of law.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Introduction to Digital Evidences

- Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device.
- Evidence can be stated as any information that can be confident or trusted and can prove something related to a case in trial, that is, indicating that a certain substance or condition is present.

Figure 2.1 Examples of digital devices.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Introduction to Digital Evidences

The Best Evidence Rule:

- The best evidence rule is that the original or true writing or recording must be confessed in court to prove its contents without any expectations.
- We define best evidence as the most complete copy or a copy which includes all necessary parts of evidence, which is closely related to the original evidence.
- It states that multiple copies of electronic files may be a part of the "original" or equivalent to the "original".

Original Evidence:

- we define original evidence as the truth or real(original) copy of the evidence media which is given by a client/victim.
- We define best incidence as the most complete copy, which includes all the necessary parts of the evidence that are closely related to the original evidence.
- There should be an evidence protector which will store either the best evidence or original evidence for every investigation in the evidence safe.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Rules of Digital Evidence

- Rule of evidence is also called as law of evidence.
- It surrounds the rules and legal principles that govern all the proof of facts.
- The rules must be:

1. Admissible: The evidence must be usable in the court.
2. Authentic: The evidence should act positively to an incident.
3. Complete: A proof that covers all perspectives.
4. Reliable: There ought to be no doubt about the reality of the specialist's decision.
5. Believable: The evidence should be understandable and believable to the jury.

Rule 103: Rule of evidence

1. Maintaining a claim of error.
2. No renewal of objection or proof.
3. Aim an offer of proof.
4. Plain error taken as notice.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Rules of Digital Evidence

- Evidence collection should always be performed to ensure that it will withstand legal proceedings. Key criteria for handling such evidence are outlined as follows:

1. The proper protocol should be followed for acquisition of the evidence irrespective of whether it physical or digital. Gentle handling should be exercised for those situations where the device may be damaged (e.g., dropped or wet).
2. Special handling may be required for some situations. For example, when the device is actively destroying data through disk formatting, it may need to be shut down immediately to preserve the evidence. On the other hand, in some situations, it would not be appropriate to shut down the device so that the digital forensics expert can examine the device's temporary memory.
3. All artifacts, physical and/or digital should be collected, retained, and transferred using a preserved chain of custody.
4. . All materials should be date and time stamped, identifying who collected the evidence and the location it is being transported to after initial collection.
5. . Proper logs should be maintained when transferring possession.
6. . When storing evidence, suitable access controls should be implemented and tracked to certify the evidence has only been accessed by authorized individual.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Characteristics of Digital Evidence

1. Locard's Exchange Principle :

- According to Edmond Locard's principle, when two items make contact, there will be an interchange.
- When an incident takes place, a criminal will leave a hint evidence at the scene and remove a hint evidence from the scene. This alteration is known as the Locard exchange principle.

2. Digital Stream of Bits

- Cohen refers to digital evidence as a bag of bits, which in turn can be arranged in arrays to display the information.
- The information in continuous bits will rarely make sense, and tools are needed to show these structures logically so that it is readable.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 **Types of Evidence**

2.11 Challenges in Evidence Handling

Types of Evidence

There are many types of evidence, each with their own specific or unique characteristics. Some of the major types of evidence are as follows:

1. Illustrative evidence
2. Electronic evidence
3. Documented evidence
4. Explainable evidence
5. Substantial evidence
6. Testimonial

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

2.9 Characteristics

2.10 **Types of Evidence**

2.11 Challenges in Evidence Handling

Types of Evidence

1.Illustrative Evidence:

Illustrative evidence is also called as demonstrative evidence. It is generally a representation of an object which is a common form of proof. For example, photographs, videos, sound recordings, X-rays, maps, drawing, graphs, charts, simulations, sculptures, and models.

2. Electronic Evidence:

Electronic evidence is nothing but digital evidence. As we know, the use of digital evidence in trials has greatly increased. The evidences or proof that can be obtained from an electronic source is called as digital evidence (viz., emails, hard drives, word-processing documents, instant message logs, ATM transactions, cell phone logs, etc.)

3. Documented evidence:

Documented evidence is similar to demonstrative evidence. However, in documentary evidence, the proof is presented in writing (viz., contracts, wills, invoices, etc.). It can include any number of medias. Such documentation can be recorded and stored (viz., photographs, recordings, films, printed emails, etc.).

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 **Types of Evidence**
2.11 Challenges in Evidence Handling

Types of Evidence

4. Explainable Evidence (Exculpatory):
Exculpatory evidence is evidence favorable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt. It is the opposite of inculpatory evidence, which tends to present guilt.
This type of evidence is typically used in criminal cases in which it supports the dependent, either partially or totally removing their guilt in the case. It is also referred to as exculpatory evidence.

5. Substantial Evidence:
A proof that is introduced in the form of a physical object, whether whole or in part, is referred to as substantial evidence. It is also called as physical evidence. Such evidence might consist of dried blood, fingerprints, and DNA samples, casts of footprints, or tires at the scene of crime.

6. Testimonial Evidence:
It is a kind of evidence spoken by a spectator under oath, or written evidence given under oath by an official declaration, that is, affidavit. This is one of the common forms of evidence in the system.

2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Challenges in Evidence Handling

1. Authentication of Evidence

The evidences that are collected by any person/investigator should be collected using authenticate methods and techniques because during court proceedings these will become major evidences to prove the crime. In other words, for providing a piece of evidence of the testimony, it is necessary to have an authenticated evidence by a spectator who has a personal knowledge to its origin.

2.1 Digital Forensic

2.2 Need

2.3 Rules of Digital Forensic

2.4 Types

2.5 Ethical Issues

2.6 Investigations

2.7 Digital Evidences

2.8 Rules of Digital Evidence

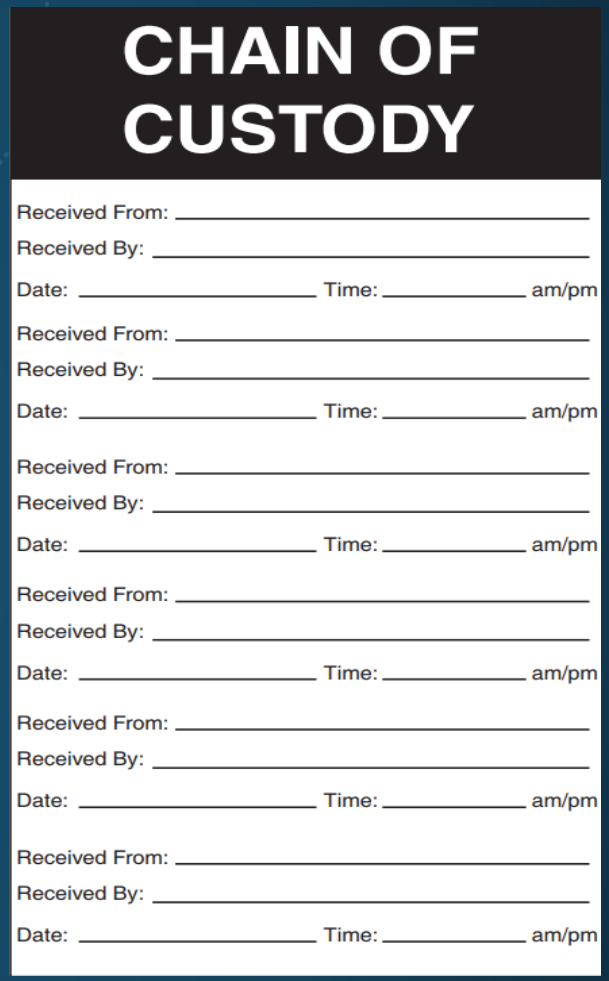
2.9 Characteristics

2.10 Types of Evidence

2.11 Challenges in Evidence Handling

Challenges in Evidence Handling

2. Maintaining the chain of custody means that the evidences collected should not be accessed by any unauthorized individual and must be stored in a tamper-proof manner. For each item obtained, there must be a complete chain of custody record. Chain of custody is nothing but the requirement that you may be able to trace the location of evidence from the moment it was collected to the moment it was presented in a judicial proceeding



2.1 Digital Forensic
2.2 Need
2.3 Rules of Digital Forensic
2.4 Types
2.5 Ethical Issues
2.6 Investigations
2.7 Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics
2.10 Types of Evidence
2.11 Challenges in Evidence Handling

Challenges in Evidence Handling

3. Evidence Validation

The challenge is to ensure that providing or obtaining the data that you have collected is similar to the data provided or presented in the court. Several years pass between the collection of evidence and the production of evidence at a judiciary proceeding, which is very common. To meet the challenge of validation, it is necessary to ensure that the original media matches the forensic duplication by using MD5 hashes. The evidence for every file is nothing but the MD5 hash values that are generated for every file that contributes to the case. The verify function within the Encase application can be used while duplicating a hard drive with Encase. To perform a forensic duplication using dd, you must record a MD5 hash for both the original evidence media and binary files or the files which compose the forensic duplication.