**Chapter One**

**Digital Crime**: illegal activity happened on digital information in one of digital resources such as computer, network.

sell to third party or use for black mail and this can be only be detected and stopped with digital forensics.

**Digital Forensics**: branch of forensics science involved with the use of scientific techniques towards the preservation, collection, validation, identification, analysis, interpretation, and presentation of digital evidence derived from digital resources for the purpose of facilitating the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions.

**Why Digital Forensics:**

* To track and punishment the cybercriminals ملاحقة ومعاقبة مرتكبي الجرائم الالكترونية
* To collect evidence of cybercrimes in a forensically way جمع الادلة على الجرائم الالكترونية بطريقة قانونية
* To estimate and reduce the impact of criminal activity on the victimتقدير وتقليل التأثير المحتمل على الضحية من الجريمة
* To minimize the losses to the organization تقليل الخسائر التي تتكبدها المنظمة
* To protect the organization from similar attack in future.

**Cases to use Digital Forensics:**

Theft of Company Secret Data, Theft of Personal Information and Digital Data, Financial Crimes, Embezzlementاختلاس, Harassmentتحرش, Child Pornography.

**Cyber Crime:** an unauthorized system/network access by a third party, the person who carried out a cyberattack is termed as hacker/ attacker

**Cyberattacks have several negative effects such as follows:**

* data breaches, resulting in data loss or data manipulation اختراق البيانات ما يؤدي لفقدانها او تعديلها
* financial losses خسائر مالية
* lose customer trust. فقدان ثقة العملاء
* reputational damage سوء السمعة

**Main Types of Cyber Attack:**

* **Malware Attack** This is one of the most common types of cyber attacks Malware refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.
* **Phishing Attack** It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment By doing so, attackers gain access to confidential information and account credentials They can also install malware through a phishing attack
* **Password Attack** It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Air crack, Cain, Abel, John the Ripper, Hash cat, etc There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks
* **Man in the Middle Attack (MITM),** is also known as an eavesdropping attack in this attack, an attacker comes in between a two-party communication, i e the attacker hijacks the session between a client and host by doing so, hackers steal and manipulate data
* **SQL Injection Attack**

**Types of Cyber Attacks:**

* **Internal Attacks:** Breach of trust by disgruntled or unsatisfied employees within the organization. Exp, Espionage, Changes of the data record, trojan
* **External Attacks:** Attackers hired either by internal or external entities to destroy the organization reputation. SQL Attacks, Phishing, DDOS.

**Challenges Cybercrimes present to investigators:**

1. **Speed:** Advancement in technology has boosted the speed with which cybercrimes are committed, whereas investigators require authorization and warrants before starting legal procedure.
2. **Anonymity:** cyber criminals can easily hide their identity by masquerading as some other or by hiding their Ip address using proxies.
3. **Volatile nature of evidences** most of digital evidences can be easily lost as it is in the form of volatile data such as logs, records and others.
4. **Evidence size and complexity.**
5. **Anti-digital forensics** Attackers are increasingly using encryption and data hiding techniques to hide digital evidences.
6. **Limited legal understanding** many victims are unaware of the law violated during the incident and fail to defend their claim.

**Civil vs Criminal investigation:**

|  |  |
| --- | --- |
| Civil | Criminal |
| Investigators show information to another party to solve the problem | Investigators follow a set of standard forensics process |
| بحث الادلة في الاجهزة يتم بالتفاهم بين الطرفين | امر من المحكمة بالبحث عن الادلة في الاجهزة |
| Informal report | Formal report |
| المدعي مسؤول عن جمع وتحليل الادلة | وكالات خاصة مسؤولة بجمع وتحليل الادلة |
| عقوبات مالية | عقوبات مالية او سجن او كليهما |

**Administrative investigation** refers to an internal investigation by an organization to discover if its employee, client and partners are abiding by the rules or policies Violation of company policies

**Rules of Forensics Investigation:**

* Comply with standards.
* Use recognized tool for analysis.
* Securely store the evidences during the investigation.
* Limit access to original evidences.

**Enterprise Theory of Investigation (ETI):**

ETI become the standard model which used through the investigation process by FBI when conducting investigation against major criminal organization.

Rather than viewing criminal acts as isolated crimes, the ETI attempts to show that individuals commit crimes in furtherance of the criminal acts solely to benefit their criminal enterprise.

**Digital Evidence**: includes all such information that is either stored or transmitted in digital form and has probative value.

**Main characteristic of digital evidence:**

* Hidden
* Believable, means that the collected evidence must be understandable.
* Reliable
* Complete
* Admissible

**Types of digital evidence:**

• Volatile Evidence: refers to the temporary information on a digital device that requires constant power supply and is deleted if the power supply is interrupted Important volatile data include system

time, logged on users' info, open files, network information.

• Non-Volatile Data: refers to the permanent data stored on secondary storage devices, such as hard disk drive, memory cards.

**Source of evidence:**

* User-created files: media, documents, database files.
* User-protected files: compressed files, encrypted files, hidden files.
* Computer-created files: Log files, cookies, system files.