Internet and Web Forensics

1. Internet Forensics

A specialized area of digital forensics that investigates crimes or incidents occurring over the Internet, such as:

- **online attacks**
- **suspicious network traffic**
- **Domain Name System (DNS) manipulation**
- **social media or web-based activities**

Goal: Reconstruct events and produce legally admissible evidence.

الهدف: إعادة بناء الأحداث وإنتاج أدلة مقبولة قانونًا.

2. Digital Footprints البصمات الرقمية

Traces left by a user or system on the Internet:

- **Active footprints: what you choose to share. (posts, comments, messages)**
- **Passive footprints: what systems collect automatically.(logs, cookies, IPs, metadata)**

A **cookie** is a small piece of data that websites save on your browser to remember your actions, preferences, or login information.

These footprints help investigators identify *who did what, when, and how*.

3. Role of AI in Internet Forensics

AI helps investigators by:

- **Anomaly detection: find unusual login attempts, traffic, or behavior**
- **Media forensics: detecting deepfakes or modified images**

- **Predictive analysis: identifying attack patterns before they happen**
- **Automated data processing: handling huge logs, PCAPs, and cloud data**

Note A **PCAP** (Packet Capture) is a file format used to **store network traffic** captured from a network interface.

Goal: AI improves speed and accuracy but does not replace human judgment.

4. Legal Considerations

Investigators must:

- **Collect evidence legally (court order / warrantمذكرة).**
- **Preserve integrity using forensic methods (hashing, write blockers).**
- **Follow cybercrime and privacy laws.**

5. Ethical Considerations

- **Protect privacy: access only data relevant to the investigation.**
- **Keep objectivity and avoid bias.**
- **Use tools responsibly and document all actions transparently.**

6. Key Challenges in Internet Forensics

- **Fast data deletion and volatility**
- **Heavy encryption tools•**
- **Global jurisdiction and legal fence الاختصاص العالمي والحواجز القانونية •**
- **Complex cloud and IoT systems**
- **Anti-forensic techniques (log wiping, fake metadata)**
- **Huge data volume and variety**
- **Tool limitations and lack of standards for cloud/web evidence**

6.1. Global jurisdiction

This means different countries have different laws, and it's not always clear which country's law applies when something happens on the internet.

6.2. Legal fence

These are problems or limits caused by laws, such as:

- **countries not sharing data,**
- **slow legal processes,**
- **privacy rules that stop access to information,**
- **different countries having conflicting laws.**

7. Key Steps in Internet Forensics

1. **Identification: determine what systems and data are involved**
2. **Preservation: secure evidence, ensure no tampering**
3. **Collection: gather logs, PCAPs(Packet Capture), cloud data**
4. **Analysis: reconstruct events, identify attackers or actions**
5. **Presentation: write a clear forensic report with conclusions and evidence**

8. WAF(Web Application Firewall) Technologies for Web Security

Block Attacker: stop dangerous requests before they reach your system.

WAFs: block attacks like SQLi, XSS

- **Vulnerability Scanners: find system weaknesses**
- **Password Cracking Tools: test password strength ethically**
- **Fuzzing Toolsادوات التشويش: detect unknown vulnerabilities**

- **Testing Approaches: black-box and white-box testing for secure applications**