DF Lecture 2 Notes

Sure! Here's your **comprehensive and well-formatted version** of **Lecture 02: Introduction to Digital Forensics (Continued)** prepared neatly for exam revision. All definitions and concepts have been preserved **exactly as in your notes**, with **better organization, formatting, and readability**.

LECTURE 02: INTRODUCTION TO DIGITAL FORENSICS (CONTINUED)

Dr. Zunera Jalil
📧 *zunera.jalil@au.edu.pk*
🗓️ *18/02/2025*

📌 Digital Forensics

> **Definition (Ken Zatyko – Former Director of Defense Computer Forensics Laboratory):** Digital Forensics is the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) **after**:

- Proper search authority
- Chain of custody
- Validation with mathematics (hash function)
- Use of validated tools
- Repeatability
- Reporting
- Possible expert presentation

📌 NIST's Definition of Digital Forensics

> **NIST SP800-86** *(Guide to Integrating Forensic Techniques into Incident Response)*
> "The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."
> 🔗 NIST Guide SP800-86

📌 Digital Forensics Standards

✅ ISO 27037

> "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence"
> 🔗 ISO Standard

✅ CART (Computer Analysis and Response Team)

- FBI's team formed in **1984**
- Handles cases involving digital evidence
  🔗 CART Information

📌 Fourth Amendment to the U.S. Constitution

- Protects individuals from unlawful search and seizure
- Courts consider whether a separate digital search warrant is necessary
- Many investigators include digital devices in search warrants to avoid admissibility issues

---

📌 Digital Forensics vs. Other Disciplines

🔄 Digital Forensics vs. Network Forensics

- **Network Forensics**: Focuses on how attackers gain network access
- **Digital Forensics**: Focuses on data retrievable from storage media (hard drives, etc.)
- Investigates:
  - Logins, accessed URLs, login methods & locations
  - File changes, copies, tampering

🔄 Digital Forensics vs. Data Recovery

- **Digital Forensics**: Seeks hidden/deleted data as **evidence**
- **Data Recovery**: Retrieves accidentally deleted or lost data with a **known objective**

🔄 Digital Forensics vs. Disaster Recovery

- **Digital Forensics**: Extracts **inculpatory or exculpatory** evidence
- **Disaster Recovery**: Uses forensic techniques to recover lost data for the client

---

📌 Digital Investigation Process

🔹 Investigators work in teams to ensure digital security

- Triad model: Different groups/departments handle specific tasks
- **Digital Investigations Group**: Analyzes systems suspected of containing incident/crime-related evidence

---

📌 Laws and Legal Frameworks

⚖️ Case Law

- Used when no existing statute covers the digital situation
- Each case is evaluated on its **own merit**

📌 Developing Digital Forensics Resources

- Knowledge across platforms: DOS, Windows 9x, Linux, Mac, Mobile OS
- Join forums like **CTIN (Computer Technology Investigators Network)** for collaboration

---

📌 Digital Investigations Types

🏛️ 1. Public Investigations

- Involve government agencies
- Governed by criminal law and must follow **Fourth Amendment**

🏢 2. Private/Corporate Investigations

- Involve private entities
- Governed by internal policies, not criminal law
- Common issues:
  - Policy violations
  - Civil litigation

📌 Law Enforcement Investigations

🔹 Criminal Case Examples

- Burglary, murder, molestation, fraud
- Computers are **tools**, like lockpicks in burglaries

🔹 Legal Process (3 Stages):

1. **Complaint**
2. **Investigation**
3. **Prosecution**

🔹 Key Terms

- **Affidavit**: Sworn statement to request a search warrant

- Must be notarized and approved by a judge

📌 Corporate Investigations

🔹 Common Corporate Crimes

- Email harassment
- Falsification of data
- Discrimination
- Embezzlement
- Espionage
- Sabotage

📌 Reducing Litigation Risk

📘 1. Establishing Company Policies

- Clear policies allow internal investigations

📢 2. Displaying Warning Banners

- Inform users their data and activities are not private
- Gives the company authority to monitor

👤 3. Designating Authorized Requesters

- Only certain departments should be allowed to initiate investigations:
  - Corporate Security
  - Ethics Office
  - Equal Employment Office
  - Auditing
  - Legal Department

🔍 4. Conducting Security Investigations

- Types:
  - Abuse/misuse of assets
  - Email/Internet abuse

📱 5. Distinguishing Personal vs Company Property

- Personal devices (phones, laptops) should not connect to corporate systems
- Prevents data mingling

Let me know if you want this converted into a PDF, printed notes, or if you'd like a flashcard or quiz version for revision!

Sure! Here's a continuation in the **same clean, structured, and easy-to-study format** as before:

PREPARING DIGITAL FORENSIC INVESTIGATION: SYSTEMATIC APPROACH

Steps for Preparing a Case:

- Make an initial assessment of the case type
- Determine a preliminary approach/design
- Create a detailed checklist
- Identify and gather required resources
- Obtain and create a copy of the evidence drive
- Identify possible risks
- Plan mitigation strategies
- Test your approach/design
- Analyze and recover digital evidence
- Investigate recovered data

- Complete a comprehensive case report
- Conduct a final critique of the case

EXAMPLE: DIGITAL FORENSICS CASE 1

Scenario:

- Steve Billings, a manager, receives customer complaints about George Montgomery's performance.
- George and another employee, Martha, are both missing without notice.
- IT confiscates George’s hard drive and storage media.
- Goal: Find clues related to George’s behavior and absence.

SOLUTION: DIGITAL FORENSICS CASE 1 (1/5)

Case Assessment:

- Conversations with coworkers reveal George is running a side business using company computers.
- **Focus of Investigation:** Potential misuse of company resources.

Details:

- **Situation:** Employee resource abuse
- **Nature:** Personal business on company systems
- **Specifics:** Registering domains and setting up websites for clients
- **Company Policy:** No expectation of privacy on company systems
- **Evidence Type:** USB drive (NTFS file system)
- **Location of Evidence:** George’s assigned workstation

SOLUTION: DIGITAL FORENSICS CASE 1 (2/5)

Abuse of Company Resources:

- Evidence of personal business activity
- Keywords to search for: Websites, domain names, ISPs
- USB drive formatted with NTFS
- Focus: Recover relevant data from USB drive

SOLUTION: DIGITAL FORENSICS CASE 1 (3/5)

Tools Needed:

- Reliable digital forensic tool for:
  - Creating forensic copy (bit-by-bit duplication)
  - Finding deleted and hidden files

SOLUTION: DIGITAL FORENSICS CASE 1 (4/5)

Planning the Investigation:

1. Acquire and tag evidence (USB)
2. Fill out an evidence custody form
3. Transport to the digital forensic lab
4. Place in a secure evidence container
5. Prepare forensic workstation
6. Retrieve evidence from storage
7. Make a forensic image (bit-by-bit copy)
8. Return original evidence to secure storage
9. Begin analysis on copied image

Evidence Forms:

- **Single-Evidence Form**

- **Multi-Evidence Form**

SOLUTION: DIGITAL FORENSICS CASE 1 (5/5)

Securing the Evidence:

- Use anti-static bags and padding for transport
- Clearly label and tag evidence
- Seal with tape and write initials
- Insert dummy disks in drives during transportation to avoid damage

---

ACTIVITY TIME – 10 MINUTES

Group Discussions:

- **Group A:** Employee Termination & Internet Abuse Cases (Page 32)
- **Group B:** Email Abuse Investigation (Pages 33-34)
- **Group C:** Attorney-Client Privilege Investigation (Pages 34-35)
- **Group D:** Industrial Espionage Investigations (Pages 36-37)
- **Group E:** Interviews & Interrogations in High-Tech Investigations (Pages 37-38)

DATA RECOVERY WORKSTATIONS AND SOFTWARE

FORENSIC WORKSTATION (1/2)

Supported Operating Systems:

- MS-DOS 6.22
- Windows 95/98/Me
- Windows NT/2000/XP/Vista/7/8/10
- Linux

- Mac OS X/macOS

FORENSIC WORKSTATION (2/2)

Essential Hardware/Software:

- Write-blocker device
- Forensic acquisition tools
- Forensic analysis tools
- Target drive (for image)
- Spare PATA/SATA/USB ports

Additional Useful Items:

- NIC (Network Interface Card)
- FireWire 400/800 ports
- SCSI card
- Disk editor, text editor, and graphics viewer tools
- Specialized viewing tools

BIT STREAM COPIES

- Bit-by-bit or forensic copies are exact images of the entire disk or partition
- Commonly known as “acquiring an image” or “making an image”
- Ensures all sectors, including deleted files, are copied

ANALYZING DIGITAL EVIDENCE

- Deleted files can still exist on disk until overwritten
- Forensic tools (e.g., **Autopsy**) help retrieve deleted files

- Useful for extracting hidden or fragmented evidence

🔗 Autopsy Download (v4.3.0)

COMPLETING THE CASE

Final Report Should Include:

- Who, What, When, Where, Why, and How
- Explanation of digital processes and evidence found
- Logs from forensic tools showing analysis steps

READING REFERENCES

Textbook 1:

- *Guide to Computer Forensics and Investigations*
  Edition: 6th
  Chapter: 1 – *Understanding the Digital Forensics Profession and Investigations*

Textbook 2:

- *Fundamentals of Digital Forensics: Theory, Methods and Real-Life Applications*
  Edition: 2nd
  Chapter: 1

Let me know if you'd like a summarized cheat sheet or a visual diagram to go with this too!