DF Lecture 2 Notes

LECTURE 02: INTRODUCTION CONT’D

Dr. Zunera Jalil
📧 *zunera.jalil@au.edu.pk*
📅 *18/2/2025*

Digital Forensics

> 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

> *— (Ken Zatyko, former Director of the Defense Computer Forensics Laboratory)*

Digital Forensic – NIST’s Definition

> “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 SP800-86** *(Guide to Integrating Forensic Techniques into Incident Response)*
> 🔗 https://csrc.nist.gov/publications/detail/sp/800-86/final

---

Digital Forensics Standards

ISO 27037

> "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence"
> 🔗 www.iso.org/standard/44381.html

CART

- FBI Computer Analysis and Response Team
- Formed in 1984 to handle digital evidence
  🔗 https://www2.fbi.gov/hq/lab/org/cart.htm

The Fourth Amendment to the U.S. Constitution

- Protects personal security from search/seizure.
- Ongoing legal developments affect digital evidence search protocols.
- Search warrants for computers often included to avoid admissibility issues.

Digital Forensics vs Other Disciplines

Digital Forensics vs Network Forensics

Network Forensics:

- How attackers access networks
- Uses log files: login times, accessed URLs, login methods/locations

Digital Forensics:

- Investigates hard drives and storage media
- Determines tampered/copied/examined files
- Tracks user actions and changes

Digital Forensics vs Data Recovery

Digital Forensics:

- Recovers hidden/deleted data for legal evidence
- Search for *any possible evidence*

Data Recovery:

- Retrieves data deleted by accident or due to failure
- Know *what you're looking for*

Digital Forensics vs Disaster Recovery

Digital Forensics:

- Recovers and uses deleted/hidden data as legal evidence
- Inculpatory or exculpatory evidence

Disaster Recovery:

- Uses forensic techniques to retrieve *lost* data
- Focus: Business continuity

Digital Investigation

- Investigators secure computers/networks.

- Digital investigation teams analyze incidents or crimes.

Brief History of Digital Forensics

History (1/6)

- **One-half cent crime**: Programmers redirected interest rounding errors to their accounts.
- **1970s**: Rise in electronic crimes (mainly financial).
- **1980s**:
  - PCs, DOS emerged.
  - Tools created by govt agencies (C/Assembly).
  - Used by IRS, Royal Canadian Police.

History (2/6)

- **Mid-1980s**:
  - Xtree Gold (recover lost/deleted files)
  - Norton DiskEdit (top deleted-file tool)
  - Apple Mac SE + 60MB EasyDrive

History (3/6) - (4/6)

- **1990s**: Forensics tools available
  - IACIS training
  - IRS created search-warrant software
  - **ExpertWitness (Mac)** - GUI tool
  - EnCase developed later
  - Large disks = complex challenges

History (5/6) - (6/6)

- **Current Tools**:
  - iLook (IRS, law enforcement only)

    - EnCase
    - AccessData FTK *(Most popular, public use)*

Laws and Resources

Case Law

- Rapid tech evolution = outdated laws
- Use previous similar cases when statutes are absent

Developing Digital Forensics Resources

- Learn multiple platforms: DOS, Windows, Linux, macOS, mobile OS
- Join groups like CTIN (monthly meets)

Preparing for Digital Investigations

Digital Investigations (1/2)

- Two types:
    - Public Investigations
    - Private/Corporate Investigations

Digital Investigations (2/2)

Private:

- For companies/government agencies
- Governed by **internal policies**
- Focus: Policy violations, civil litigation

Public:

- Law enforcement
- Governed by **legal standards & criminal law**

Law Enforcement Agency Investigations

Understanding Investigations (1/4)

- Criminal cases: Fraud, molestation, burglary
- Digital tools = crime tools (e.g., like a lockpick)

Following Legal Process (1/3)

- 3 stages:
  1. Complaint
  2. Investigation
  3. Prosecution

Following Legal Process (2/3)

- Begins with a **complainant's allegation**
- Police file report → investigation
- Prosecutor handles case if strong enough evidence
- May request **affidavit** for search warrant

Following Legal Process (3/3)

Affidavit:

- Sworn statement for evidence
- Judge signs the **search warrant** for collection

Corporate Investigations

Understanding Private Sector Investigations

- Involves:
  - Email harassment
  - Falsifying data

  - Discrimination
  - Embezzlement
  - Sabotage
  - Espionage

How to Reduce the Risk of Litigation

(1/5) - Company Policies

- Easy-to-read, well-defined
- Empower investigators to act

(2/5) - Warning Banners

- On login/screens
- Removes expectation of privacy

(3/5) - Authorized Requester

- Defined by management
- e.g., Security, Ethics, Legal, EEO, Auditing

(4/5) - Security Investigations

- Internet/email abuse
- Distinguish between company and criminal cases

(5/5) - Personal vs Company Property

- Restrict personal devices
- Avoid data mixing

Preparing Digital Forensic Investigation

Systematic Approach

1. Initial case assessment
2. Design investigation strategy
3. Create checklist
4. Identify & mitigate risks
5. Obtain and copy evidence
6. Analyze & investigate
7. Report and critique

Example Case (George Montgomery)

Scenario:

- Employee (George) underperforming, missing
- Another employee (Martha) also missing
- Manager requests hard drive analysis

Solution (1/5): Case Assessment

- Co-workers say George used company resources for personal business
- Policy: No privacy on company systems
- USB drive found (NTFS)

Solution (2/5): Finding Evidence

- Look for:
  - Websites, ISPs, domain registrations
- NTFS USB drive → suspicious content

Solution (3/5): Tools Needed

- Reliable forensic software for:
  - Duplicating drive
  - Recovering deleted/hidden files

Solution (4/5): Investigation Plan

- Acquire, tag, and store USB
- Fill evidence form (chain of custody)
- Prepare workstation
- Make forensic copy
- Analyze copy using forensic tools

Evidence Forms:

- Single Evidence Form
- Multi-Evidence Form