DIGITAL FORENSICS FUNDAMENTALS BY ELYAS

GitHub • https://github.com/elyasec0 | GitHub Pages • https://elyasec0.github.io | X • https://x.com/elyasec0 | LinkedIn • https://www.linkedin.com/in/elyasec0

CYBERSECURITY | IUTT

Forensics Science:

is the application of science principles and methods to support:

- Investigation Agencies
- Legal Decision-making

Contents "Digital Forensics Fundamentals"

Chapter 1:

Digital Forensics: A part of forensics science.

Digital forensics is a specialized field that applies computer science and investigative techniques to analyze digital evidence for legal purposes. It combines technical expertise with legal knowledge to ensure that evidence is collected, preserved, and analyzed in a way that is admissible in court.

Power of Digital Forensics:

Digital forensics can support in revealing crimes and tracking traces such as:

1. Fraud.
2. Child Exploitation
3. Terrorism
4. Drug Trafficking
5. Homicide

Digital Forensics and Security Practices:

Digital Forensics overlaps with other cybersecurity fields such as:

1. **Incident Response – Handles detection and recovery from attacks.**
2. **Threat Hunting – Searches for hidden threats using forensic data.**
3. **Security Monitoring – Watches systems for anomalies or breaches.**
4. **Reverse Engineering & Malware Analysis – Studies malicious code to understand and prevent attacks.**

1. Relation Between Digital Forensics & Incident Response(D F I R)

DFIR stands for Digital Forensics & Incident Response — two closely connected fields that often work together during cybersecurity incidents.

- In many organizations, there are separate teams for Incident Response (IR) and Digital Forensics (DF), but both must understand each other's roles to work effectively.

Similarity:

Both IR and DF focus on analyzing artifacts and collecting evidence related to cybercrimes.

Differences:

- Incident Response (IR): Performs rapid analysis to find the root cause, focusing on containment and eradication of threats.
- Digital Forensics (DF): Conducts deep, detailed analysis to preserve, document, and present evidence, often taking longer.

Main Steps in Digital Forensics:

1. Acquisition – Safely capturing the data.
2. Preservation – Ensuring evidence integrity.

If legal action is expected, forensic artifacts must be securely preserved to remain valid in court.

Example:
In a ransomware attack from another company trying to damage servers, IR stops the attack, while DF collects and analyzes evidence for possible legal investigation.

2. Digital Forensics & Threat Hunting

- Threat Hunting is done in the SOC to find hidden cyber threats.
- It searches for traces in artifacts like logs or network data.
- Both Forensics and Hunting analyze artifacts using hypotheses.
- Difference: Hunting focuses on detection, not preservation.
- Forensics focuses on preserving evidence for legal use.
- Both work together during compromise assessments.

3. Digital Forensics & Malware Analysis

Both fields are connected in analyzing malicious activities.

Similarity:

- Both **extract artifacts** from infected systems.
- Both **identify Indicators of Compromise (IOCs)** to trace and understand attacks.

Investigations Triad:

- **Vulnerability/Threat Assessment & Risk Management**
  - Tests and verifies the integrity of stand-alone workstations and network servers.

- **Network Intrusion Detection & Incident Response**
  - Detects intruder attacks using automated tools and monitoring firewall logs.
- **Digital Investigations**
  - Manages investigations and conducts forensic analysis of systems suspected to contain evidence.

Digital Forensics & Legal Considerations:

1. **Legal Value of Evidence**
   - **Digital evidence must be collected, preserved, and documented properly.**
   - **Treated like physical evidence to be admissible in court.**
2. **Key Steps**
   - **Acquisition: Capture data without altering it (e.g., Write Blocker, imaging, hash).**
   - **Preservation: Maintain integrity and chain of custody.**
   - **Documentation: Include collector, date/time, tools, system specs, and hash.**
   - **Relevance: Evidence must directly relate to the case.**
3. **Roles & Responsibility**
   - **Only authorized personnel (forensic experts, investigators, judicial officers).**
   - **Experts should be qualified, accountable, and follow legal guidelines.**
4. **Collaboration with Security Teams**
   - **Work with Incident Response, Threat Hunting, Malware Analysis.**
   - **Understand each team's role, but Forensics ensures legal admissibility.**
5. **Reporting & Documentation**
   - **Comprehensive documentation from collection to analysis.**
   - **Copies/screenshots must include date, collector, system info, tools, hash.**
   - **If original cannot be preserved, document full examination on original device.**
6. **Standards & Best Practices**
   - **ISO/IEC 27037, 27041 – Guidelines for digital evidence handling.**
   - **NIST SP 800-101 / 800-86 – Computer & mobile device forensics.**
   - **Chain of Custody – Continuous accountability to protect admissibility.**

Chapter 2: Forensics Basics first steps:

Digital Forensics Process

- **Identification:** Locate potential sources of evidence (devices, data custodians, locations).
- **Collection (Acquisition):** Gather digital information relevant to the investigation.
  1. Artifacts: Extracted digital proofs with potential impact on investigation.
  2. Evidence: Any collected item from the crime scene that may or may not be relevant.
- **Preservation:** Protect electronically stored information (ESI), document evidence, and capture visual images of the scene.
- **Analysis:** Systematic, in-depth examination of evidence related to the incident.
- **Reporting:** Reports follow proven methodology, reproducible by competent examiners.

Forensics as a Practitioner

1. Attitude & Mindset
   - Willing to accept opinions.
   - Work consistently following a methodical approach.
   - Maintain clarity in communication.
2. Consulting Skills
   - Ask the right questions:
     - **What** do you need?
     - **Why** do you need it?
     - **When** do you need it?
     - **How** long will it take?
     - **From** whom?
3. Technical & Research Skills
   - Computer fundamentals: Strong understanding of systems and networks.
   - Research capability: Ability to investigate, analyze, and learn new tools or techniques.
   - Understanding EXE files and other formats for analysis.

Forensics Methodology – Three Cornerstones

1. Three Cornerstones of Forensics Methodology

- **Hypothesis / Prediction** – Form initial assumptions.
- **Validation** – Peer review or cross-check by another analyst.
- **Proof** – Evidence to support or refute the hypothesis.

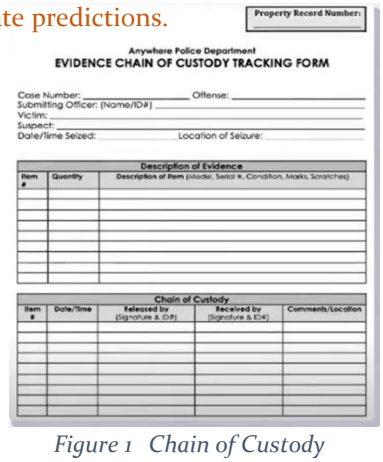
2. Example: Methodology Steps

Field Work:

1. Get Authority – Obtain permission to investigate.
2. Collect Basic Information – Identify relevant data sources.
3. Determine Acquisition Points – Decide what to collect.
4. Acquisition – Capture data safely.
5. Coding / Recording / Label – Organize and label collected data.
6. Preservation / Submission – Maintain integrity and chain of custody.
7. Reporting / Hypothesis – Document findings and validate predictions.

Lab Work:

- **Acquire:** Artifact → Label → Chain of Custody.
- **Cloning:** Make exact copies for analysis.
- **Extraction:** Extract relevant data from artifacts.
- **Analysis:** Examine evidence in depth.
- **Proof:** Confirm or refute initial hypothesis.


Property Record Number:

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____

Submitting Officer: (Name/ID#) _____

Victim: _____

Suspect: _____

Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Figure 1 Chain of Custody

Digital Forensics Types

Non-volatile Forensics:

Focuses on data that remains stored even after the system is powered off.

1. File system and OS forensics
2. Storage forensics
3. Image, video & audio forensics
   - Example: Detecting **deepfake videos** by analyzing image metadata, compression artifacts, and inconsistencies using forensic tools.
4. Mobile device forensics

Volatile Forensics:

Focuses on data that disappears when the device is powered off or rebooted.

1. Memory forensics
2. Network forensics

Types of Digital Artifacts:

- Digital artifacts are traces of user activity or system operations that can provide evidence during an investigation

1. **Download & Temporary Files – Contain cached or recently accessed data.**
2. **Web Browser History – Tracks visited websites, search terms, and timestamps.**
3. **Printer Logs – Record printing history, document names, and timestamps.**
4. **Registry (Windows) – Store configuration and user activity data.**
5. **Deleted Files – May still exist in unallocated space and can be recovered.**
6. **Emails – Contain sender, receiver, timestamps, and message content.**
7. **SMS – Provide communication evidence from mobile devices.**
8. **Photos taken by digital cameras – Often include metadata (EXIF) such as location, time, and device information.**
9. **Event Logs – Record system and security events, user logins, and errors.**
10. **Applications & Package Reveal software usage, installation dates, and activity logs.**
11. **Social Media and OSINT (Open-Source Intelligence) – Publicly available posts, profiles, or digital footprints.**

Chapter 3: Digital forensic lab tools and equipment:

Digital Forensics Labs

A **Digital Forensics Lab** can range from a **large professional facility** (e.g., Police Department, CERT) to a **small personal setup** on your home computer.

1. Secure Facility
   - The lab must be physically secure to protect digital evidence.
   - Only authorized personnel should have access.
2. Evidence Lockers
   - Used to **store collected evidence** safely.

     Examples of protection methods:

     - **RF Shielding / Faraday Bags** – Prevents wireless communication or tampering.
     - **TEMPEST (Transient Electromagnetic Pulse Emanation Standard)** – Prevents electromagnetic leaks.

       ➢ **TEMPEST Forms:**

       1. Faraday Bags
       2. Shielded Enclosures
3. Minimize Static Electricity
   - Use **antistatic pads** on desks.
   - Maintain **clean floors and carpets** to prevent static discharge.
4. Maintain Two Trash Containers
   - **General Waste:** Non-investigation materials.
   - **Sensitive Waste:** Shredded or securely destroyed investigation-related items.
5. Microscopy / Microscope Tools
   - **Used to inspect or recover data from** damaged disks or media**.**
6. Floor Planning
   - **Small Organization: Single-room setup with basic equipment.**
   - **Large Organization: Dedicated rooms for acquisition, analysis, and secure storage.**
7. Lab Accreditation
   - **Forensic labs can be accredited by:**
     1. **ANSI National Accreditation Board (ANAB) – Ensures lab meets international standards.**

Forensics Workstation (Small Lab Setup)

You can build a small digital forensics lab using your own laptop or PC. This setup is known as a Forensics Workstation.

1. **Hypervisor:**
   Used to create and manage **virtual machines** for testing and analysis.
2. **Workstation (Host System):**
   A computer running **Windows** or **Linux** (preferably a **Linux Live Distro** such as Kali, Parrot, or CAINE).
3. **Write Blocker Device:**
   Prevents modification of original evidence during acquisition.
   a. **Hardware Write Blocker:**
      A physical device connected between the suspect drive and the workstation.
   b. **Software Write Blocker:** "LINK"
      A software-based tool that blocks write operations to the source media.
4. **Digital Forensics Acquisition Tool:**
   Used to **capture or image** the suspect drive (e.g., FTK Imager, dd, Guymager).
5. **Digital Forensics Analysis Tool:**
   Used to **examine, recover, and analyze** the collected evidence (e.g., Autopsy, Sleuth Kit, X-Ways).
6. **Target Drive:**
   A clean, empty disk used to **store the copied data** from the suspect drive.
7. **Spare PATA or SATA Ports:**
   Allows you to connect multiple storage devices for acquisition.
8. **Cloners:**
   Devices or tools used for **disk-to-disk duplication** without altering data.

Digital Forensic OS Toolkit

Any Live CD **(bootable operating system) can be used for forensic work,** as long as it includes the proper tools**.**

- **SANS SIFT (SANS Investigative Forensic Toolkit)** – Used by professionals for advanced analysis.
- **CAINE Live (Computer Aided INvestigative Environment)** – User-friendly and comes with many preinstalled tools.
- **Tsurugi Linux** – Focused on digital forensics and incident response with powerful analysis features.

Forensics Tools for Acquisition and Analysis

Category	Acquisition Tools	Purpose	Analysis Tools	Purpose
Disk / File Imaging	FTK Imager	Collect and image drives safely	Autopsy	Full forensic analysis platform
Memory (RAM)	LIME	Capture live memory data	Volatility	Analyze memory dumps
Network Traffic	TCPdump	Capture live network packets	Wireshark	Analyze captured network traffic
Deleted Data	Foremost	Recover deleted or lost files	—	—
Windows Registry	—	—	RegRipper	Extract and analyze Windows Registry data
Image / Audio Metadata	—	—	EXIF Viewer	Analyze metadata (e.g., GPS, camera info)
System Logs	—	—	LogParser Studio	Analyze OS and application log files

All tools should be used in a controlled forensic environment to ensure evidence integrity and legal admissibility.

Daubert Standard

The Daubert Standard **is used in some U.S. courts to determine whether expert testimony and digital forensic evidence are scientifically valid and admissible.**
It is widely accepted because it aligns with established rules of evidence**.**

➢ Daubert Criteria for Evidence:

1. **Testing**
   The forensic report must clearly describe **how the testing was performed** in the case, including tools, procedures, and steps.
   All methods should be **well-documented and reproducible**.
2. **Error Rate**
   The report should mention the **expected or measured error rate** for the method used.
   In legal practice, a forensic expert appointed by the court usually determines an acceptable rate (e.g., **less than 10%**).

3. **Reviewed**
   The results or methodology must be **reviewed by another expert or analyst** to confirm accuracy and eliminate bias.
4. **Accepted**
   The method or approach should be **recognized and accepted by the scientific and forensic community**, ensuring reliability in court.

➢ Practical Considerations for Forensic Analysts

1. **Get Proper Authority**
   - Ensure you have a valid **contract**, **job role**, or **official order** before starting.
2. **Stick to the Scope**
   - Do not exceed the investigation boundaries — many cases are lost due to **scope breaches**.
3. **Determine Analysis Location**
   - Some cases require that **data never leave the investigation site**. Always confirm before acquisition or analysis.
4. **Document Everything**
   - Maintain a **detailed timeline** and record all steps taken during the investigation.
5. **Notify and Communicate Properly**
   - Even with authority, remember you may not have **decision-making power** — always notify before critical actions.
6. **Use a Secure Facility or Safe Environment**
   - Work on **clean disks**, within **controlled and secure forensic labs**.
7. **Maintain Professionalism Under Pressure**
   - Your role is **critical**; stay calm, think before speaking, and give **clear, concise answers** when questioned.

The Daubert Standard ensures that forensic evidence presented in court meets the highest scientific and legal reliability.

Chapter 4: Acquisition and Preservation Phase:

Evidence Lifecycle:

- **Acquisition → Preservation → Cloning → Analysis → Presentation**
- **Why Acquisition?**
  1. **You can't work on the suspect machine, otherwise you will tamper the evidence.**
  2. **Forensics is based on hypothesis (trial and error).**
  3. **Organizations won't accept keeping an asset out of production for long.**
  4. **Acquisition enables cloning, allowing multiple investigators to work in parallel.**
  5. **Cloning is a separate step with its own conditions to preserve the law of evidence.**
- **Most Important Tasks in Acquisition.**
  1. **List the collection points.**
  2. **Decide which acquisition tools will be used.**
  3. **Preserve integrity of evidence using hash calculation.**
- **Acquisition Process Order.**
  1. Follow the **Order of Volatility**.
  2. Start with the **most volatile** component.
  3. End with the **most static** component.
     - **Volatility Order:**

       Registers → CPU Cache → RAM → Hard Disk → External/Secondary Storage

Types of Acquisition:

- **Live Acquisition**
  1. **Must be done at a specific time.**
  2. **Collects volatile data.**

     Example: Memory (RAM).
- **Static Acquisition**
  1. **Can be done anytime.**
  2. **Example: Hard Disk.**
  3. **Dead Acquisition: a subset of static acquisition where there's no interaction with the OS.**

Disk Acquisition

❖ Acquisition Methods

1. Full Acquisition

1. **Disk to Image**
   - **Copies the entire disk into one image file (like .dd or .E01).**
2. **Disk to Disk**
   - **Copies all data from the suspect's disk to another physical disk.**

2. Partial Acquisition

3. **Logical**
   - **Captures specific files, folders, or partitions — not the whole disk.**
4. **Sparse**
   - **Collects only relevant or changed data blocks from the disk.**

❖ Copy / Cloning

Copying or cloning means creating an exact duplicate of the suspect's drive to another one.

❖ Imaging / Copying

Imaging creates a file image (.dd, .E01, .aff, etc.) that contains all the data from the original disk.

❖ Three Formats of Disk Images

1. **Raw Format** "Example: **.dd, .img**"
   - **Advantages:**
     - **Fast data transfers.**
     - **Ignores minor data read errors on the source drive.**
2. **Proprietary Formats (Closed Source)**
   - **Advantages:**
     - **Supports compression to save space.**
     - **Can integrate metadata (case info, hash, time, etc.).**
     - **Can split the image into smaller segments.**
   - **Disadvantages:**
     - **Limited sharing between tools because it's closed-source.**
   - **Examples:**
     - **EWF – Expert Witness Format used by EnCase.**
     - **IDIF – used by ILook Investigator.**
     - **sgzip – used by PyFlag.**

3. **Advanced Forensics Format (AFF)** ***(Open Source)***
    - **Features:**
        - **Compression**
        - **Encryption**
        - **Metadata support**
    - **Advantages:**
        - **Open source and supported on multiple OS and tools.**
    - **File Extensions:**
        - **.afd → Advanced Forensics Data**
        - **.afm → Advanced Forensics Metadata**

❖ Consideration During Acquisitions:

1. **Size of the source disk**
    - **The larger the disk, the more time and storage are required for imaging.**
2. **Compression**
    - **Lossy: Some data is lost during compression (❌ not recommended).**
    - **Lossless: No data is lost; used by tools like EnCase and ILook.**
3. **Time to perform the acquisition**
    - **The process can take hours depending on disk size and hardware.**
4. **Create a duplicate copy of your evidence image file**
    - **Always keep an exact backup of your acquired image for safety.**
5. **Use different tools or techniques**
    - **To validate results, acquisition should be verified using different tools.**
6. **Be prepared to deal with encrypted drives**
    - **May require the suspect's decryption key.**
    - **Windows uses BitLocker for full disk encryption.**
    - **Consider using hardware acquisition tools for protected disks.**
    - **Don't forget to copy the Host Protected Area (HPA) of the disk as well.**

❖ Preservation / Validation:

1. **Proofing that artifacts are not changed during custody is important**
    - **Evidence integrity must be proven at all stages.**

2. **Hash functions are used as a digital fingerprint**
    - **Hashing ensures that no alteration has occurred.**
3. **Challenge with preservation**
    - **Hashing is the last line of defense to prove data integrity.**
4. **Recommended algorithms**
    - **SHA-2 → for digital forensics evidence.**
    - **MD5 / SHA-1 → may still be used for verification or penetration testing.**

Chapter 5: Analysis phase:

- **Preparation before Analysis**
    - ❖ **Verify all tools and OS updates.**
    - ❖ **Confirm the integrity of acquired data before starting.**

- **Windows System Analysis**
    - ❖ **Registry & System Files: Extract and examine using:**
        1. **FTK Imager – for offline registry extraction.**
        2. **Registry Explorer & Regripper – automatic system information extraction.**
        3. **ShellBag Explorer – track user folder activity.**
    - ❖ **Key artifacts: user accounts, installed software, connected devices, browser history, timestamps, deleted files.**

- **Linux System Analysis**
    - ❖ **Examine main directories: /home, /etc, /var/log, /tmp, /mnt, /root.**
    - ❖ **Important files:**
        1. **.bash_history – command history**
        2. **.bashrc / .profile – environment settings**
        3. **/etc/passwd & /etc/shadow – user credentials**
        4. **/var/log & /etc/rsyslog.d – system and auth logs**
        5. **/etc/crontab – scheduled tasks**

Browser Artifacts

- Extract user activity from browsers like Firefox.
- Tools: Autopsy (1) – analyze history, cookies, and downloads.

Autopsy Case Management (Windows & Linux)

- Create a new case and add data source.
- Analyze evidence: deleted files, registry, system logs, user activities.
- Generate reports with detailed timelines.
- (1) Autopsy.pdf file will be attached here for reference.

Analysis Tools Summary

Task	*Windows Tools*	*Linux Tools*
Registry Extraction	FTK Imager, Registry Explorer, Regripper	N/A
System & Log Analysis	LogParser Studio	Autopsy, direct log parsing (`/var/log`)
Memory Analysis	Volatility, LIME	Volatility, LIME
Network Traffic	Wireshark, TCPdump	Wireshark, TCPdump
Deleted Files	Foremost, Autopsy	Foremost, Autopsy
Browser Artifacts	Autopsy, Firefox SQLite parsers	Autopsy, Firefox SQLite parsers
Case Management & Reporting	Autopsy	Autopsy
Software / Disk Tools	Software Write Blocker	Software Write Blocker

References:

- **Autopsy.pdf – FILE (1)**
- **Link of Course: Digital Forensics Fundamentals**
- **Books / Guides:**
  1. *Guide to Computer Forensics and Investigations, Sixth Edition*

GitHub • https://github.com/elyasec0 | GitHub Pages • https://elyasec0.github.io | X • https://x.com/elyasec0 | LinkedIn • https://www.linkedin.com/in/elyasec0