# MASTER STUDY NOTES

Topic 2: Digital Forensics & Digital Evidence

F20FO/F21FO – Digital Forensics

Exam-Ready Edition

Academic Year 2025-26

## Contents

**1 Introduction & Learning Outcomes 2**

1.1 Topic Overview - The Big Picture 2

**2 What is Digital Forensics? (MUST MEMORIZE) 2**

2.1 Core Definitions - Exam Critical 2

2.2 ELI5 Explanation: What is Digital Forensics? 3

2.3 Key Points from Definitions - EXAM FOCUS 3

2.4 Terminology: Digital vs Computer Forensics 4

**3 The Digital Forensics Process - CRITICAL FOR EXAMS 4**

3.1 Three-Phase Model (Simplified) 4

3.2 Four-Phase Model (Detailed - More Common in Exams) 4

3.3 Detailed Breakdown of Each Phase 5

3.3.1 Phase 1: Acquisition 5

3.3.2 Phase 2: Identification 6

3.3.3 Phase 3: Evaluation/Analysis 6

3.3.4 Phase 4: Presentation 7

3.4 Process Comparison Table - EXAM GOLD 7

**4 Digital Forensics Goals - What DF Can Do 8**

4.1 Three Main Goals (Memorize These) 8

4.2 Detailed Explanation of Each Goal 8

4.2.1 Goal 1: Deleted File Recovery 8

4.2.2 Goal 2: Timeline Analysis 9

4.2.3 Goal 3: Metadata Extraction 10

4.3 How DF Achieves These Goals 11

**5 Digital Forensics Evolution - Historical Timeline 11**

5.1 Why Study History? (Exam Relevance) 11

5.2 Complete Timeline (MEMORIZE KEY DATES) 12

5.3 Key Milestones Explained (ELI5) 13

5.3.1 Pre-Digital Era (Foundation of Forensic Science) 13

5.3.2 Digital Era Begins 13

5.3.3 The Professionalization Era (1990s) 14

5.3.4 Modern Era (2000s - Present) . . . . . . . . . . . . . . . . . . . . . . . 16
5.4 Timeline Visualization for Memorization . . . . . . . . . . . . . . . . . . . . . . 17

**6 Why Do We Need Digital Forensics? 17**
6.1 Six Critical Reasons (Exam Common) . . . . . . . . . . . . . . . . . . . . . . 17

# 1 Introduction & Learning Outcomes

**What You MUST Know for the Exam**

After studying this topic, you should be able to:

1. **Define and understand** key concepts in digital forensics
2. **Appreciate and explain** the importance of chain of custody in handling digital evidence
3. **List and apply** guidelines for dealing with digital evidence (especially ACPO)
4. **Identify and explain** different imaging toolkits and their purposes

## 1.1 Topic Overview - The Big Picture

This topic covers three main areas that are heavily tested on exams:

Digital Forensics Evolution
Digital Investigations & Evidence
Digital Forensics Tools

# 2 What is Digital Forensics? (MUST MEMORIZE)

## 2.1 Core Definitions - Exam Critical

**Definition 1 (Most Common)**

**Computer/Digital Forensics** is the *scientific examination and analysis* of data held on, or retrieved from, device storage media in such a way that the information can be used as **evidence in a court of law**.

**Definition 2 (Alternative)**

Computer forensics is the practice of **collecting, analysing, and reporting** on digital data in a way that is **legally admissible**. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

## 2.2 ELI5 Explanation: What is Digital Forensics?

### Like a Crime Scene Investigator... But for Computers

Imagine you're a detective at a crime scene:

- At a physical crime scene: You collect fingerprints, DNA, footprints
- In digital forensics: You collect files, emails, browser history, deleted data

**The Goal is the Same:** Find proof (evidence) that shows:

1. **WHAT** happened (what crime occurred)
2. **WHEN** it happened (timeline)
3. **WHO** did it (suspect identification)
4. **HOW** they did it (method/technique)

**But there's a catch:** Digital evidence is:

- **Fragile** - Easy to accidentally delete or change
- **Invisible** - Can't see it with your eyes like a fingerprint
- **Massive** - A single hard drive can have millions of files

That's why we need **scientific processes** and **special tools**!

## 2.3 Key Points from Definitions - EXAM FOCUS

### Memorize These 5 Key Points

1. **Many definitions exist** - wording differs, but core concepts are the same
2. **Output is DATA** - DF produces data/information as evidence
3. **Court admissible** - Evidence must be usable in a court of law
4. **Scientific process** - Must follow methodical, repeatable procedures
5. **Similar to other forensics** - Follows same principles as DNA, fingerprint analysis

### 2.4 Terminology: Digital vs Computer Forensics

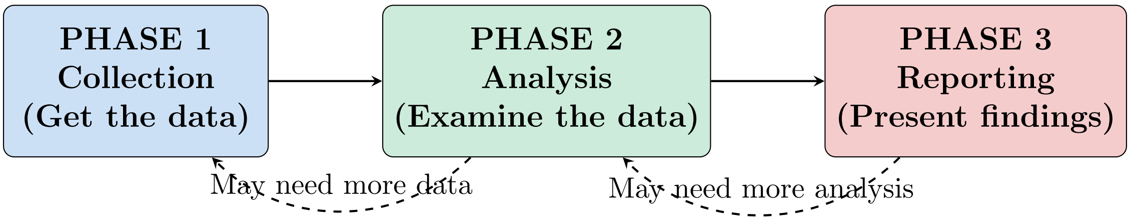
| Term | What it Covers |
|---|---|
| **Computer Forensics** | **Traditional computers only:** PCs, laptops, servers |
| **Digital Forensics** | **ALL digital devices:** Computers + smartphones + tablets + cameras + smart watches + IoT devices + doorbell cameras + cloud systems + networks |
| **Cyber Forensics** | Sometimes used interchangeably with digital forensics |

EXAM TIP

The terms are often used interchangeably. Don't worry about the exact terminology - what matters is that you understand the **scientific process** is the same regardless of which term is used.

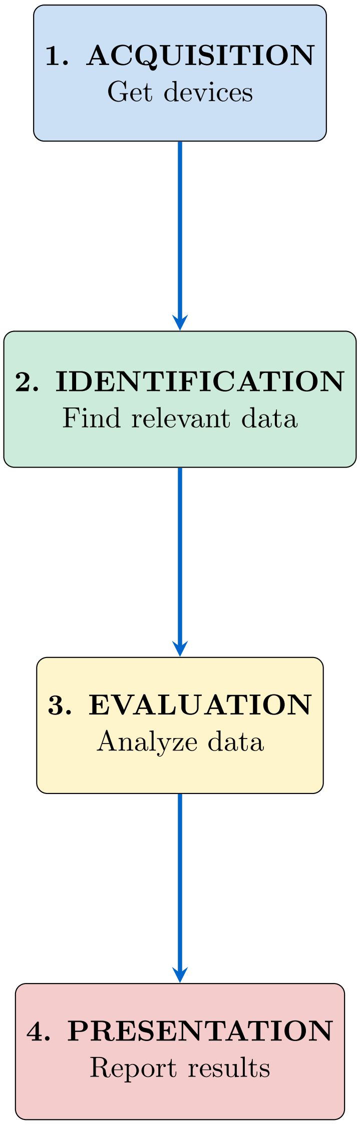
## 3 The Digital Forensics Process - CRITICAL FOR EXAMS

### 3.1 Three-Phase Model (Simplified)



### 3.2 Four-Phase Model (Detailed - More Common in Exams)

The lecture mentions a 4-step process used frequently:



## 3.3 Detailed Breakdown of Each Phase

### 3.3.1 Phase 1: Acquisition

**Acquisition Definition**

**Physically or remotely** obtaining possession of:

- The computer/device
- All network mappings from the system
- External physical storage devices (USB drives, external HDDs, etc.)

**ELI5 Explanation:** This is like gathering all the physical stuff at a crime scene. You:

1. Take the actual computer
2. Note down what it was connected to (networks, other devices)

3. Grab anything plugged into it (USB sticks, external drives)

**Key Questions Asked During Acquisition:**

| Question | Why It Matters |
|---|---|
| Should we focus on static data (hard drive) or temporary memory (RAM)? | RAM contains recent activity but disappears when powered off |
| Should we anticipate encrypted data? | Need special tools/approaches for encrypted drives |
| How much data? How many devices? | Determines resources needed |
| Should data be sought from cloud sources? | Cloud data may be outside jurisdiction |

### 3.3.2 Phase 2: Identification

**Identification Definition**

Identifying what data **could be recovered** and electronically retrieving it by running various computer forensic tools and software suites.

**ELI5 Explanation:** Now that you have the devices, you need to:

1. Scan through ALL the data (even deleted files!)
2. Figure out what's relevant to your investigation
3. Extract/copy that data for examination

**Example:** If investigating drug trafficking, you might search for:

- Text messages mentioning drugs or money
- GPS locations near known drug locations
- Contact lists with known dealers
- Banking/payment apps

### 3.3.3 Phase 3: Evaluation/Analysis

**Evaluation Definition**

Analysis of the information/data recovered to **determine if and how** it could be used.

**ELI5 Explanation:** This is where you:

1. Look at the data you found
2. Try to understand what it means
3. Connect the dots to build a story of what happened
4. Remain **OBJECTIVE** - don't let personal opinions influence your analysis

CRITICAL RULE

**Objectivity is ESSENTIAL:** Your job is to analyze the evidence, not decide if someone is guilty. That's for the court/jury.
You just present the facts: "On June 10th at 3:45 PM, the suspect's phone connected to this tower near the crime scene."

**Iterative Process:** Analysis often leads to more questions:

- Initial search finds drug-related messages
- This leads to discovering multiple user accounts
- Which leads to finding connections to other devices
- Which requires going back to Phase 1 (more acquisition)

### 3.3.4 Phase 4: Presentation

Presentation Definition

Presentation and reporting of evidence discovered in a manner which is **understood by lawyers, non-technical staff/management**, and suitable as evidence.

**ELI5 Explanation:** Write a report that:

1. A lawyer can understand (no jargon!)
2. Clearly shows what you found
3. Explains what it means
4. Can be used in court

**The report might lead to:**

- More questions from lawyers
- Need for additional analysis
- Follow-up investigations

## 3.4 Process Comparison Table - EXAM GOLD

| 3-Phase Model | 4-Phase Model | Core Activities |
|---|---|---|
| Collection | Acquisition | Obtain devices, identify data sources |
| | Identification | Electronically retrieve data |
| Analysis | Evaluation | Examine data objectively |
| Reporting | Presentation | Present findings clearly |

Table 1: Process Model Comparison

Exam Strategy

**If asked about ”the DF process”:**

- You can use EITHER the 3-phase or 4-phase model
- What matters is that you include: **acquiring data, analyzing it, and reporting results**
- Mention it’s an **iterative process** (you might go back to earlier steps)

# 4 Digital Forensics Goals - What DF Can Do

## 4.1 Three Main Goals (Memorize These)

**1. Deleted File**Recovery

**2. Timeline**Analysis

**3. Metadata**Extraction

## 4.2 Detailed Explanation of Each Goal

### 4.2.1 Goal 1: Deleted File Recovery

What is it?

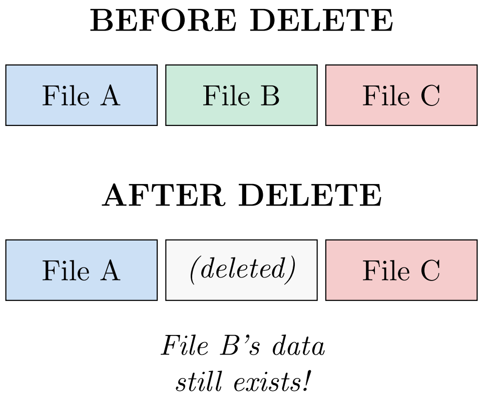
Retrieving files that have been **logically removed** but still leave **recoverable traces** on disk.

**ELI5 Explanation - The Pencil Eraser Analogy:**
Imagine you write your name in pencil on paper, then ”erase” it:

- To your eyes, it looks gone
- But if you look very carefully (or use special lighting), you can still see faint traces
- The pencil marks are still there, just very faint

**Same with computer files:**

1. When you ”delete” a file, the computer doesn’t actually erase it
2. It just removes the file’s name from the directory (like removing a library book from the catalog)
3. The actual data is still on the disk until it gets overwritten by new data
4. DF tools can find and recover this data



### 4.2.2 Goal 2: Timeline Analysis

**What is it?**

Helps to reconstruct the **timeline** of file/user actions by examining **metadata** such as:

- Access times
- Modification times
- Creation times

**ELI5 Explanation:** Every file has a "birth certificate" with timestamps:

| Timestamp | Abbrev. | What it tells you |
|---|---|---|
| **Created** | C | When the file was first created |
| **Modified** | M | Last time the content was changed |
| **Accessed** | A | Last time someone opened/viewed it |
| **Changed** | C | Last time metadata was changed |

**Real Exam Example:**

**Scenario: Murder Investigation**

**Question:** The suspect claims they were at home during the murder (8:00-9:00 PM). What does the timeline show?
**Timeline Analysis of suspect's computer:**

- 8:15 PM - Word document "alibi_notes.docx" **created**
- 8:16 PM - Document **modified** (content added)
- 8:45 PM - Document **modified** again
- 9:05 PM - Document **accessed** (read but not changed)

**What this proves:**

- Someone was using the computer during 8:15-9:05 PM
- They were actively creating/editing a document called "alibi notes" (suspicious!)
- This **supports** their claim of being home
- BUT the filename raises questions

### 4.2.3 Goal 3: Metadata Extraction

**What is it?**

Retrieves **embedded information** such as:

- File owner
- Origin device
- Creation tool/software
- GPS location (for photos)
- Camera model (for photos)

This supports **attribution** (who did it) and **contextualization** (understanding the evidence).

**ELI5 Explanation - The Hidden Information:**
Every digital file is like a product with a hidden label that says:

- Made by: [Software name]
- Made on: [Computer/device name]
- Made at: [GPS coordinates, if applicable]
- Made by user: [Username]

**Example - Photo Metadata:**

| Metadata Field | Example Value |
|---|---|
| Camera Make | Apple |
| Camera Model | iPhone 13 |
| Date Taken | 2025-06-10 14:30:22 |
| GPS Latitude | 25.2048° N |
| GPS Longitude | 55.2708° E |
| Software | iOS 16.5 |

**Why This Matters for Exams**

This metadata can prove:

- **WHEN** - Exact time photo was taken
- **WHERE** - Exact location (GPS coordinates point to Dubai, UAE)
- **WHAT device** - iPhone 13 (can be matched to suspect's phone)

If a suspect claims "I was never in Dubai," but a photo from their iPhone has Dubai GPS coordinates... that's strong evidence!

### 4.3 How DF Achieves These Goals

| Tool/Method | What it does |
|---|---|
| **Specialized Tools** | Imaging tools, carving tools, write blockers (covered later) |
| **OS Tools** | Built-in commands to view file systems, metadata |
| **Existing Data** | Metadata, system logs, browser history |

## 5 Digital Forensics Evolution - Historical Timeline

### 5.1 Why Study History? (Exam Relevance)

**Exam Questions Often Ask**

- "When did digital forensics begin?"
- "What were key milestones in DF evolution?"
- "How has DF changed from 1980s to today?"
- "Name important organizations/standards in DF history"

## 5.2 Complete Timeline (MEMORIZE KEY DATES)

**1888** - Francis Galton: First study of fingerprints

**1893** - Hans Gross: First to apply science to criminal investigation

**1910** - Albert Osborn: Documented evidence examination

**1932** - FBI sets up forensic laboratory

**1970s** - Electronic crimes increase (financial sector)

**1980s** - PCs gain popularity, DOS emerges, basic forensic tools

**Mid-1980s** - **Xtree Gold & Norton DiskEdit** appear

**1984** - Scotland Yard Computer Crime Unit & FBI CF departments

**1990** - Computer Misuse Act (CMA) in UK

**Early 1990s** - IACIS formed, commercial DF tools, ExpertWitness

**1993** - First international conference on computer evidence (US)

**1995** - IOCE formed (global law enforcement forum)

**2000** - First FBI RCFL established

**2000-2010s** - Mobile & cloud forensics, live forensics, memory analysis

**2010s-present** - Big data, AI/ML, encryption, IoT forensics

## 5.3 Key Milestones Explained (ELI5)

### 5.3.1 Pre-Digital Era (Foundation of Forensic Science)

**1888 - Fingerprints (Francis Galton)**

**Why important:** First time someone proved you could uniquely identify a person using physical evidence (fingerprints).
**Connection to Digital Forensics:** Just like fingerprints uniquely identify people, digital artifacts (IP addresses, device IDs, file hashes) uniquely identify digital actions.

**1893 - Hans Gross - Scientific Investigation**

**Why important:** First to say "let's use SCIENCE to investigate crimes, not just guesswork."
**Connection to Digital Forensics:** DF follows the same principle - we use scientific methods, not hunches.

**1910 - Albert Osborn - Documentation**

**Why important:** Created the idea of documenting EVERY step of evidence examination.
**Connection to Digital Forensics:** This becomes the "Chain of Custody" in DF (covered later).

### 5.3.2 Digital Era Begins

**1970s - Electronic Crimes Increase**

**What happened:** Banks started using computers → criminals started hacking banks.
**The Problem:** Police didn't know enough about computers to:

- Ask the right questions
- Preserve digital evidence
- Understand what they were looking at

**ELI5:** Imagine investigating a crime scene in a language you don't speak!

**1980s - DOS Era & Early Tools**

**What happened:**

- Personal computers become popular
- Different operating systems emerge (mainly DOS)
- Simple forensic tools created (mostly by government agencies)

**First Real Tools:**

- **Xtree Gold** - Could recognize file types and retrieve deleted files
- **Norton DiskEdit** - Became the best tool for finding deleted files

**ELI5:** These tools were like the first metal detectors - simple but revolutionary!

**1984 - Official DF Departments**

**What happened:**

- Scotland Yard creates Computer Crime Unit
- FBI creates computer forensics departments

**Why important:** This is when digital forensics became an OFFICIAL field, not just IT people helping out.

### 5.3.3 The Professionalization Era (1990s)

**1990 - Computer Misuse Act (UK)**

**What it did:** Made computer crimes ILLEGAL (before this, hacking wasn't technically a crime in many places!)
**Three main offenses:**

1. Unauthorized access to computer material
2. Unauthorized access with intent to commit further offenses
3. Unauthorized modification of computer material

**ELI5:** Before 1990, hacking was like trespassing - wrong, but not always illegal!

### Early 1990s - IACIS & Commercial Tools

**IACIS:** International Association of Computer Investigative Specialists

- Provided **training** on forensic software
- Created **certification** programs

**Commercial Tools:**

- IRS created search-warrant programs
- ExpertWitness for Macintosh
- ASR Data created first commercial GUI software
- Could recover deleted files AND fragments of deleted files

**Why important:** Tools became user-friendly (GUI instead of command-line only).

### 1993 - First International Conference

**What it meant:** DF became a recognized GLOBAL field, not just isolated efforts in different countries.
Experts from different countries could now:

- Share techniques
- Standardize procedures
- Learn from each other

### 1995 - IOCE (International Organization on Computer Evidence)

**Purpose:** Forum for global law enforcement agencies to exchange information about cybercrime investigation.
**Why important:** Cybercrime crosses borders - you need international cooperation!
**ELI5:** If a hacker in Russia attacks a bank in USA, Russian and American investigators need to work together. IOCE helps with that.

**2000 - FBI Regional Computer Forensic Laboratory (RCFL)**

**What it did:** Examination of digital forensics in support of criminal investigations:

- Identity theft
- Hacking
- Viruses
- Malware

**Why important:** Dedicated labs with specialized equipment and trained personnel.

### 5.3.4 Modern Era (2000s - Present)

**2000-2010s: Mobile & Cloud Era**

**New Challenges:**

- **Mobile devices** - Smartphones have different file systems than computers
- **Cloud storage** - Evidence might be on servers in different countries
- **Live forensics** - Analyzing running systems, not just dead storage
- **Memory analysis** - Examining RAM for evidence
- **Network forensics** - Tracking attacks across networks

**ELI5:** Before: Evidence was on one hard drive in one location.
Now: Evidence might be scattered across phones, clouds, networks, multiple countries!

**2010s-Present: Big Data & AI Era**

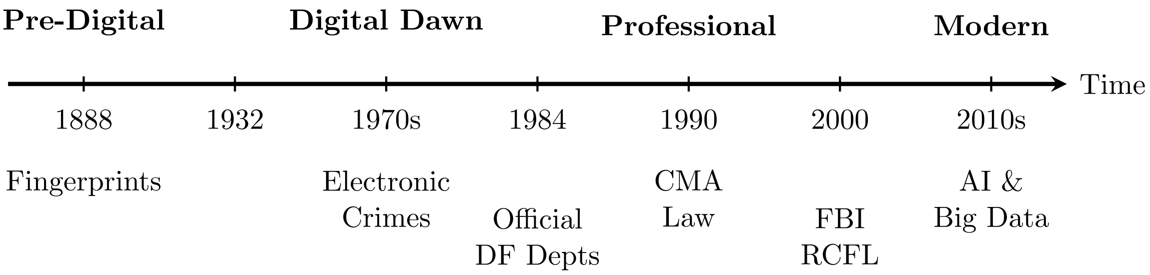
**Modern Challenges & Solutions:**

| Challenge | Solution/Technique |
|---|---|
| Massive data volumes | Big data analytics to process large volumes |
| Finding patterns | Machine learning for pattern recognition and anomaly detection |
| Encrypted data | Advanced techniques for handling encryption & cryptocurrencies |
| IoT devices | Specialized forensics for smart devices (watches, home assistants, cars) |

**ELI5:** A modern investigation might involve:

- Analyzing 10 terabytes of data (too much for humans)
- Breaking encryption
- Examining a smart refrigerator (yes, they have logs!)
- Tracing cryptocurrency transactions

### 5.4 Timeline Visualization for Memorization



# 6 Why Do We Need Digital Forensics?

## 6.1 Six Critical Reasons (Exam Common)

| # | Reason | ELI5 Explanation |
|---|---|---|
| **1** | Ensures overall integrity of computer systems | **Protect organizations:** Like having security cameras - deters crime and helps catch criminals if something happens |
| **2** | Captures important information if systems compromised | **Evidence preservation:** If your system gets hacked, DF helps you understand HOW they got in and WHAT they took |
| **3** | Extracts, processes, and interprets evidence | **Makes sense of technical data:** Turns computer gibberish into understandable evidence |

| # | Reason | ELI5 Explanation |
|---|---|---|
| **4** | Tracks down cyber criminals and terrorists | **Fighting crime:** Helps catch bad guys who commit crimes online |
| **5** | Saves organization money and time | **Efficiency:** Faster investigation = less downtime = less money lost |
| **6** | Tracks complicated cases (e.g., child exploitation) | **Serious crimes:** Some crimes (like CSE) leave primarily digital evidence - DF is essential |

Table 2: Reasons for Digital Forensics

### Exam Tip - Real-World Example

**Question:** ”Why is digital forensics important for modern organizations?”
**Strong Answer Structure:**

1. **State the main reason:** ”Digital forensics is crucial because most criminal activity today involves digital devices...”
2. **Give specific examples:** ”For instance, in child exploitation cases, evidence exists primarily in digital form (images, messages, browser history)...”
3. **Mention consequences:** ”Without DF, organizations cannot effectively investigate incidents, which leads to...”
4. **Include business impact:** ”This saves organizations time and money by enabling faster incident response...”