Digital Forensics

Lectures 0-1 & Lab 01 - Complete Exam Guide

Simplified for Beginners with Examples

Course: F20FO/F21FO
Heriot-Watt University Dubai

Academic Year 2025-26

Contents

1 LECTURE 0: Course Introduction

1.1 What This Course Is About

KEY EXAM POINT

For the Exam: Know what Digital Forensics means and why it matters.
Digital Forensics = Finding and analyzing digital evidence from computers, phones, and networks to solve crimes or security incidents.

DEFINITION

Digital Forensics is the scientific examination of data from digital devices (computers, phones, tablets, networks) that can be used as evidence in legal cases or investigations.

1.1.1 Main Topics You'll Learn

1. **Digital Evidence** - What counts as evidence? How do we collect it?
2. **Forensic Tools** - Software used to analyze devices
3. **Computer Security** - Protecting systems vs. investigating breaches
4. **Chain of Custody** - Legal tracking of evidence
5. **Incident Response** - What to do when an attack happens

1.2 Assessment Structure - MEMORIZE THIS!

KEY EXAM POINT

100% Coursework - No final written exam, but you have 4 assessments throughout the semester.

Assessment	Weight	Week	What It Tests
Class Test 1	20%	Week 5	Topics 1-2 (Intro to DF, Evidence)
Coursework 1	20%	Week 7	Practical forensic analysis
Class Test 2	20%	Week 10	Topics 3-4 (Advanced concepts)
Coursework 2	40%	Week 12	Complete forensic investigation
TOTAL	**100%**		

Table 1: Assessment Breakdown - Know These Percentages!

WORKED EXAMPLE

How to Calculate Your Final Grade:
Let's say you get:

- Class Test 1: 75/100 = 75%
- Coursework 1: 85/100 = 85%
- Class Test 2: 80/100 = 80%
- Coursework 2: 90/100 = 90%

Step-by-step calculation:

$$\begin{aligned}\text{Final Grade} &= (0.20 \times 75) + (0.20 \times 85) + (0.20 \times 80) + (0.40 \times 90) \\ &= 15 + 17 + 16 + 36 \\ &= 84\%\end{aligned}$$

Result: You pass with a B grade (typically 70-79% is B, 80+ is A).

1.3 Important Course Logistics

Item	Details
When	Every Monday, 6:30 PM - 10:00 PM
Lectures	6:30-7:45 PM (Weeks 1-5), 7:30-8:45 PM (Weeks 7-11)
Labs	8:00-10:00 PM (Weeks 1-5), 9:00-10:30 PM (Weeks 7-11)
Week 6	No class - Consolidation week (catch up on work)
Week 12	Coursework 2 demos
Office Hours	Monday 5:30-6:30 PM (book via email)
Instructor Email	r.soobhany@hw.ac.uk

Table 2: Course Schedule at a Glance

COMMON MISTAKE - AVOID!

Common Mistakes Students Make:

- Not checking Heriot-Watt email daily (instructor does NOT use MS Teams)
- Forgetting Week 6 is a break - use it to catch up!
- Not attending labs - they start Week 1 and are crucial for coursework

1.4 Learning Outcomes - What You Must Know

KEY EXAM POINT

By the end of this course, you should be able to:

1. **Chain of Custody** - Explain how evidence is tracked legally
2. **Perform DF Analysis** - Use tools to extract and analyze data

3. **Incident Response (IR)** - Know the workflow when attacks happen
4. **Use DF Tools** - Hands-on with software like Autopsy, FTK Imager
5. **Identify Artifacts** - Find traces left by operating systems and apps

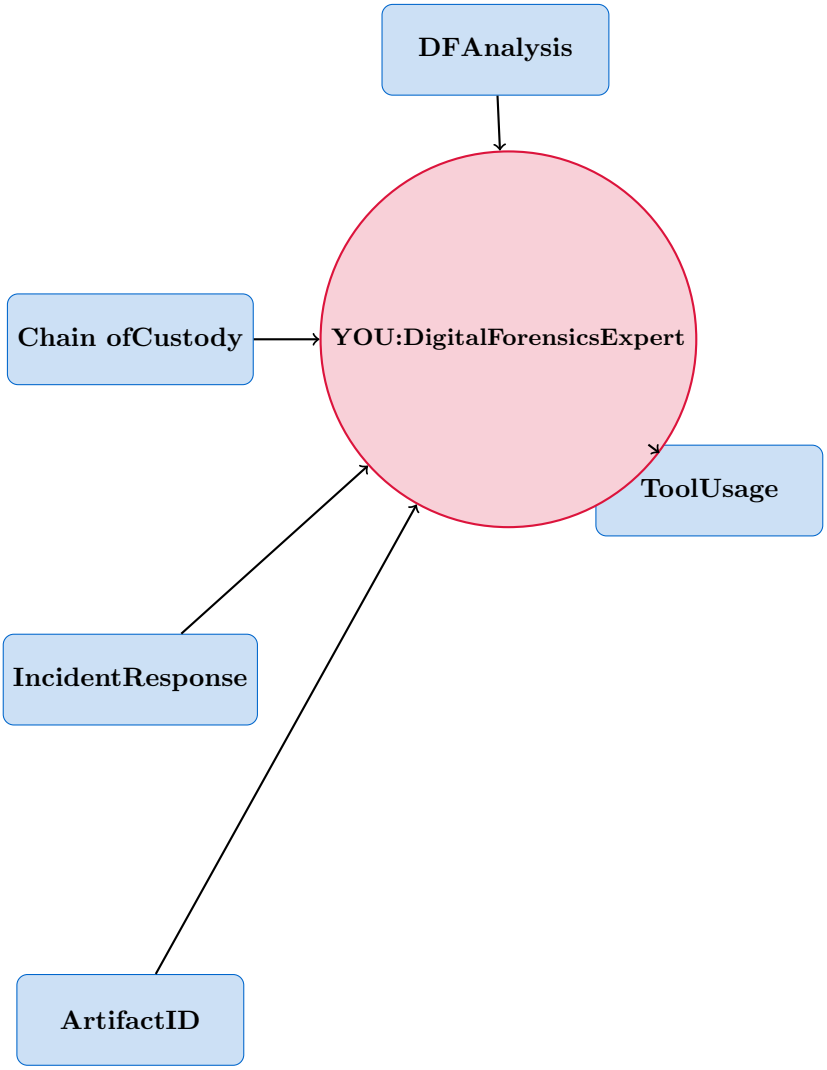

Figure 1: Your Goal: Master These 5 Core Skills

2 LECTURE 1: Introduction to Digital Forensics

2.1 Computer Security Fundamentals

DEFINITION

Computer Security = Protecting information and systems from danger, damage, or unauthorized access.
Think of it like locking your house - you want to keep bad guys out and your valuable stuff safe.

2.1.1 The CIA Triad - MOST IMPORTANT CONCEPT!

KEY EXAM POINT

EXAM ALERT: The CIA Triad appears in almost every exam. Know each component with examples!

Component	Simple Meaning	Real Example
Confidentiality	Only authorized people can see the data	Your bank account info should only be visible to you and the bank
Integrity	Data cannot be changed without permission	Your exam grade can't be altered by other students
Availability	Data is accessible when needed	You can access Netflix whenever you want (if you pay)

Table 3: CIA Triad Explained Simply

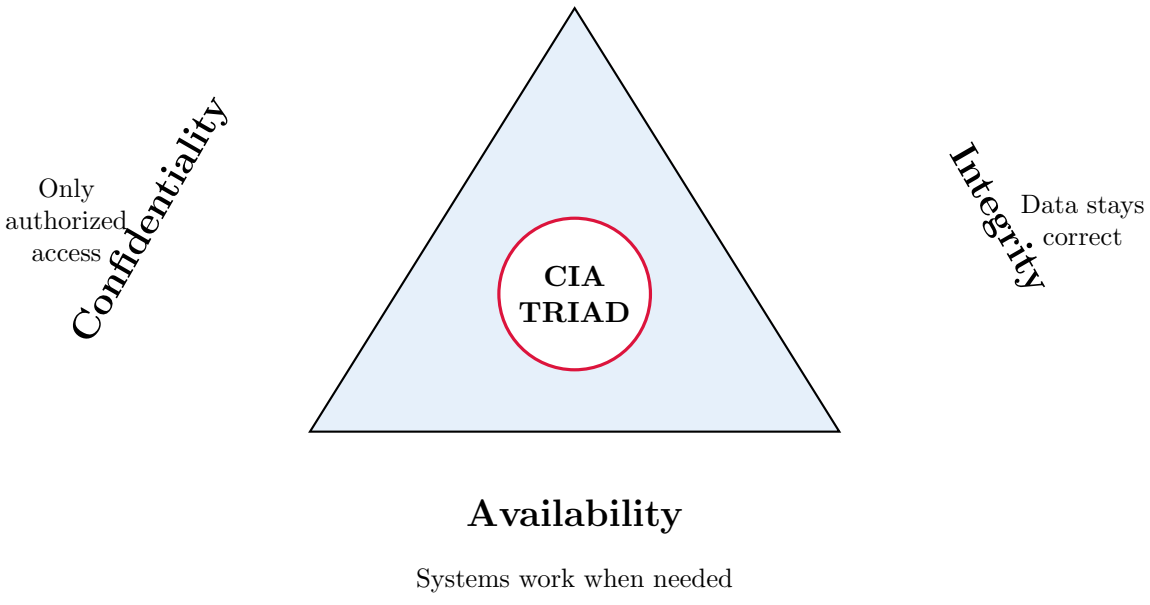

Figure 2: The CIA Triad - Memorize This Triangle!

WORKED EXAMPLE

CIA Triad in a Hospital System:

- **Confidentiality Breach:** A hacker steals 10,000 patient medical records
  - Impact: Privacy violation, lawsuits, loss of trust
- **Integrity Breach:** Someone changes a patient's blood type from O+ to AB-
  - Impact: Patient could die from wrong blood transfusion
- **Availability Breach:** Hospital servers crash, doctors can't access patient files
  - Impact: Delayed treatment, emergency care disrupted

Which is worst? All are serious, but integrity breaches can be life-threatening!

2.1.2 Additional Security Goals

Goal	What It Means (Simple English)
Authentication	Proving you are who you say you are (like showing ID)
Authorization	Determining what you're allowed to do (student vs. teacher permissions)
Accountability	Keeping records of who did what (like CCTV cameras)
Non-repudiation	You can't deny you did something (like a signed contract)

Table 4: Beyond CIA: Other Security Goals

2.1.3 Computer Security vs. Digital Forensics

KEY EXAM POINT

Key Difference for Exams:

- **Computer Security:** PREVENTING attacks (before they happen)
- **Digital Forensics:** INVESTIGATING attacks (after they happen)

Think: Security = Lock your door. Forensics = CSI after a break-in.

Figure 3: Timeline: Security → Incident → Forensics

2.2 Computer Crime and Cyber Threats

2.2.1 Why Should You Care?

KEY EXAM POINT

Data Has Value! Modern criminals steal data instead of physical goods.

WORKED EXAMPLE

Traditional Crime vs. Cyber Crime:

2.2.2 How Much Data Exists?

DEFINITION

Data Units - Understanding big numbers:

- 1,000 Kilobytes (KB) = 1 Megabyte (MB)
- 1,000 MB = 1 Gigabyte (GB) - A movie is about 2-4 GB
- 1,000 GB = 1 Terabyte (TB) - A large hard drive
- 1,000 TB = 1 Petabyte (PB) - All Netflix content
- 1,000 PB = 1 Exabyte (EB)
- 1,000 EB = 1 Zettabyte (ZB) - All data on the internet

KEY EXAM POINT

Mind-Blowing Fact: By 2025, the world generates approximately **180 Zettabytes** of data annually. That's 180 trillion gigabytes!

WORKED EXAMPLE

Data Generated Every Single Minute (2024):

- Google: 5.9 million searches
- YouTube: 3.5 million videos viewed
- Emails: 251 million sent
- TikTok: 16,000 videos uploaded
- Netflix: 363,000 hours streamed
- Instagram + Facebook: 139 million Reels played
- Data breaches: 4,080 records compromised

Why This Matters: More data = more targets for criminals = more work for forensic investigators!

2.2.3 Real-World Cyber Attack Examples

KEY EXAM POINT

Exam Tip: Know at least 2-3 real cyber attack examples with details (company, date, impact).

Organization	Date	Attack Type	Impact
Southern Water	Feb 2024	Data Breach	5-10% of customers affected; personal data stolen
Jaguar Land Rover	Aug 2025	Ransomware	£1.9 billion cost; 5-week shutdown; 5,000 suppliers affected
NHS (Synnovis)	Jun 2024	Ransomware	Blood test delays; patient data stolen and published
CrowdStrike	Jul 2024	Faulty Update	8.5 million Windows devices crashed; airlines, hospitals disrupted
TfL London	Sep 2024	Data Breach	5,000 customers affected; bank details potentially stolen

Table 6: Major UK Cyber Attacks 2024-2025

WORKED EXAMPLE

Case Study: Jaguar Land Rover (JLR) Attack
What Happened:

1. Attackers used ransomware (malicious software that locks files)
2. Exploited vulnerabilities in third-party supplier software
3. Moved "laterally" (sideways) through connected systems
4. Locked critical production and logistics systems

Financial Impact Calculation:

- Total cost: £1.9 billion
- Production stopped: 5 weeks = 35 days
- Cost per day: £1,900,000,000 ÷ 35 = £54.3 million per day

Lessons Learned:

- One weak supplier can compromise the entire chain
- Ransomware can cause more damage than data theft
- Recovery takes much longer than the attack itself

Step 1: Criminals send innocent-looking emails with Zeus Trojan malware

↓

Step 2: Victim opens email → malware installs secretly

↓

Step 3: Malware records keystrokes (passwords, account numbers)

↓

Step 4: Criminals take over bank accounts

↓

Step 5: Money transferred to "mules" with fake IDs

↓

Step 6: Mules keep 10%, send 90% to criminals

Figure 4: How the Zeus Trojan Attack Works

2.2.4 Zeus Trojan Attack - Step-by-Step

WORKED EXAMPLE

Zeus Attack Money Flow Calculation:
If criminals steal $100,000:

- Mule keeps: $100,000 × 10% = $10,000
- Criminals get: $100,000 × 90% = $90,000

If they attack 100 small businesses at $50,000 each:

- Total stolen: 100 × $50,000 = $5,000,000
- Criminals keep: $5,000,000 × 0.9 = $4,500,000

2.2.5 What Valuable Data Do YOU Hold?

COMMON MISTAKE - AVOID!

Think About Your Own Devices:

- Bank account info / Credit cards
- Social media accounts
- Personal photos and messages
- Passwords (email, shopping sites)
- Passport/ID scans
- Work emails and documents

If your phone was hacked, what could a criminal do with this data?

2.2.6 Security Measures - What You Should Do

Security Measure	How It Helps	DF Impact
Strong passwords	Prevents unauthorized access	Can slow forensic investigation
Encryption	Scrambles data so it's unreadable	Makes evidence recovery harder
Antivirus/Firewall	Blocks malware	Helps detect attacks
Physical locks	Prevents device theft	Doesn't stop remote attacks
Backups	Recover deleted data	Provides alternative evidence source

Table 7: Security Measures and Their Forensic Implications

KEY EXAM POINT

Important Paradox: Security measures (like encryption) that protect you ALSO make it harder for forensic investigators to analyze evidence - even when legally required!

2.3 Digital Evidence and Forensics

2.3.1 Three Ways Devices Are Involved in Crime

DEFINITION

Devices can play 3 different roles in criminal investigations:

Role	Description	Example
1. Device Used to Conduct Crime	The computer/phone is the tool used to commit the crime	Sending threatening emails, creating fake documents, distributing illegal content
2. Device is Target of Crime	The device itself was attacked	Ransomware attack, DDoS attack, data breach
3. Device Contains Evidence	Device wasn't involved in crime but has useful information	Smartphone GPS shows suspect's location during robbery

Table 8: Three Device Roles in Digital Crime

WORKED EXAMPLE

Car Accident Investigation - Physical vs. Digital Evidence:

Physical Evidence:

- Skid marks on road
- Car damage patterns
- Witness statements
- Photos of scene
- Paint transfer between cars

Digital Evidence:

- ECU (Engine Control Unit) data
- GPS location history
- Dashcam footage
- Phone usage records
- Traffic camera recordings

What ECU Can Tell You:

- Speed at moment of impact: e.g., 85 km/h
- Whether brakes were applied: Yes/No
- Airbag deployment time
- Seat belt usage

2.3.2 What is Digital Forensics?

DEFINITION

Digital Forensics is the scientific examination of data from digital devices and networks that can be used as evidence.
Four Main Stages:

1. **Acquisition** - Collect the data (making exact copies)
2. **Identification** - Find relevant evidence
3. **Evaluation** - Analyze what it means
4. **Presentation** - Explain findings in court/reports

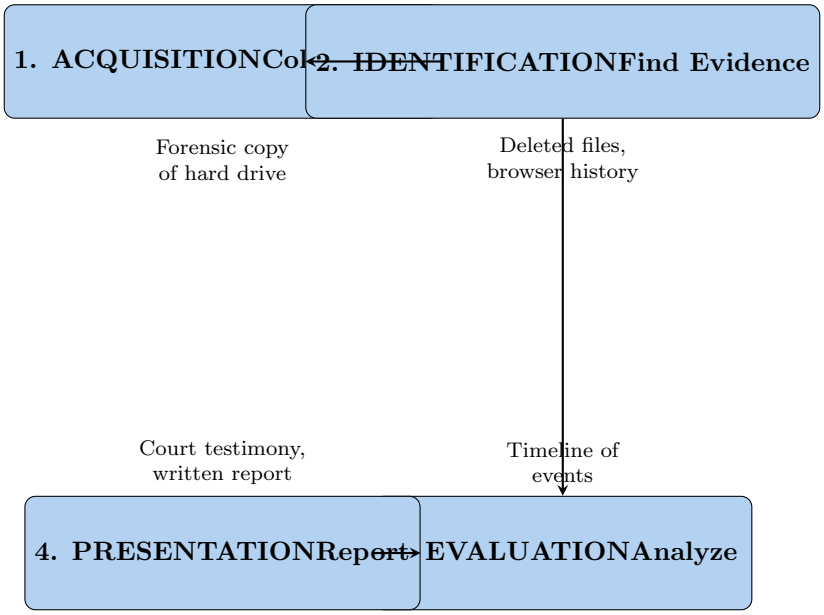

Figure 5: The Digital Forensics Process - Know These 4 Steps!

KEY EXAM POINT

Digital Forensics Requires Three Disciplines:

1. **Computing** - Technical skills with hardware, software, networks
2. **Forensic Science** - Evidence handling, scientific methodology
3. **Legal Knowledge** - Laws, chain of custody, admissibility rules

You need ALL THREE! Being a computer expert isn't enough.

2.3.3 Digital Evidence - Key Concepts

DEFINITION

Digital Evidence = Data stored or transmitted in digital form that can support or refute a theory in a legal case.
Sources Include:

- Computer systems (hard drives, RAM)
- Mobile devices (phones, tablets, smartwatches)
- Storage media (USB drives, SD cards, CDs)
- Networks (internet traffic, emails)
- IoT devices (smart home devices, fitness trackers)
- Vehicles (car computers, GPS systems)

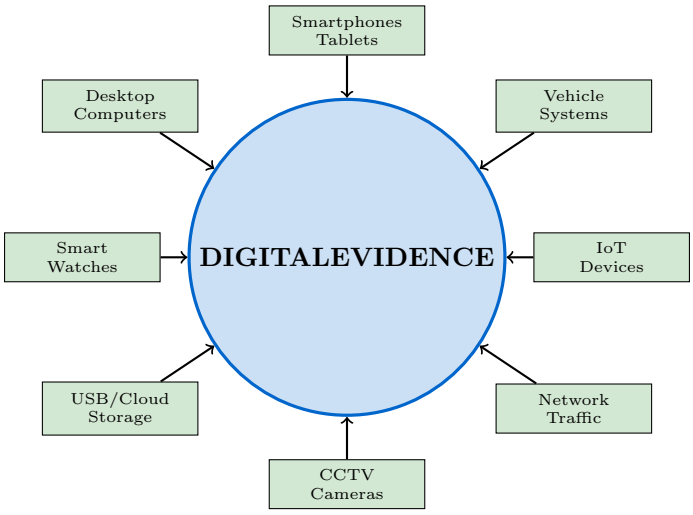

Figure 6: Sources of Digital Evidence

2.3.4 Chain of Custody

KEY EXAM POINT

CRITICAL FOR EXAMS: Chain of Custody = Documented trail showing who handled evidence, when, and why.
Without proper chain of custody, evidence cannot be used in court!

DEFINITION

Chain of Custody is the chronological documentation showing:

- Who collected the evidence
- When it was collected
- Who had access to it
- Where it was stored
- Any transfers between people
- How its integrity was maintained

WORKED EXAMPLE

Chain of Custody Example - Seized Laptop:
What This Proves:

- Nobody tampered with the laptop
- Evidence remained secure
- Every person who touched it is accountable
- Can be trusted in court

2.3.5 Challenges in Digital Forensics

COMMON MISTAKE - AVOID!

Common Challenges You MUST Know:

1. **Deleted Data**
   - Problem: Suspect deletes incriminating files
   - Solution: Forensic tools can recover deleted data (if not overwritten)
2. **Encryption**
   - Problem: Data is scrambled, unreadable without password
   - Solution: Password cracking, finding encryption keys, legal orders
3. **Anti-Forensic Techniques**
   - Problem: Criminals use tools to destroy evidence
   - Solution: Quick response, live forensics, cloud backups
4. **Data Volume**
   - Problem: Modern devices have terabytes of data
   - Solution: Keyword searches, targeted analysis, automation
5. **Volatile Data**
   - Problem: RAM (memory) data disappears when device turns off

- Solution: Live forensics - capture data before powering down

WORKED EXAMPLE

Deleted File Recovery - How It Works:
When you "delete" a file:

1. Operating system marks the space as "available"
2. But the actual data is still on the disk
3. It only gets overwritten when new data needs that space

Analogy: Imagine a library catalog. Deleting a file is like removing the book's card from the catalog - the book is still on the shelf, you just can't find it easily anymore.
Recovery Chance Calculation:

- Deleted 1 hour ago, device unused: 95% recovery chance
- Deleted 1 day ago, light use: 70% recovery chance
- Deleted 1 week ago, heavy use: 20% recovery chance
- Deleted + disk overwritten: 0% recovery chance

2.3.6 Areas of Digital Forensics

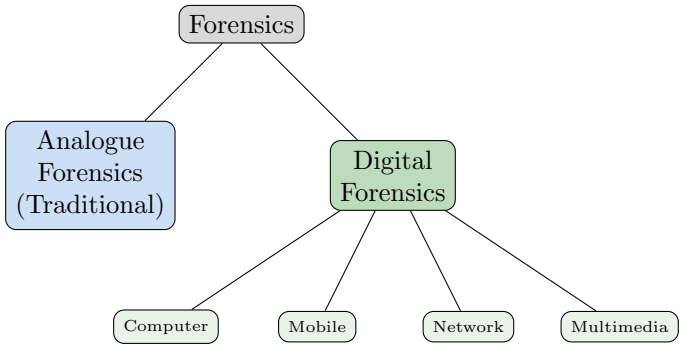

Figure 7: Forensics Branches - Know the Main Types

Type	Focus	Example
Computer Forensics	Desktop/laptop computers, hard drives	Analyzing suspect's PC for illegal files
Mobile Forensics	Smartphones, tablets, wearables	Extracting deleted texts from iPhone
Network Forensics	Internet traffic, packets, logs	Tracing hacker's connection route
Multimedia Forensics	Images, videos, audio files	Detecting if photo was manipulated
Database Forensics	Database systems, SQL logs	Finding unauthorized data changes

Table 10: Specializations in Digital Forensics

KEY EXAM POINT

Exam Fact: 80% of all criminal investigations in Europe involve mobile devices! Why? Everyone has a phone, and it contains:

- Location data (GPS)
- Communications (texts, calls, social media)
- Photos and videos
- Contacts and relationships
- Financial transactions (mobile banking, payment apps)

2.3.7 Incident Response and Blue Teams

DEFINITION

Incident Response (IR) = The process of handling a security breach or cyber attack. **Blue Team** = Defensive security team that protects systems and responds to attacks. (Note: Red Team = Offensive team that tests security by attacking it - like ethical hackers)

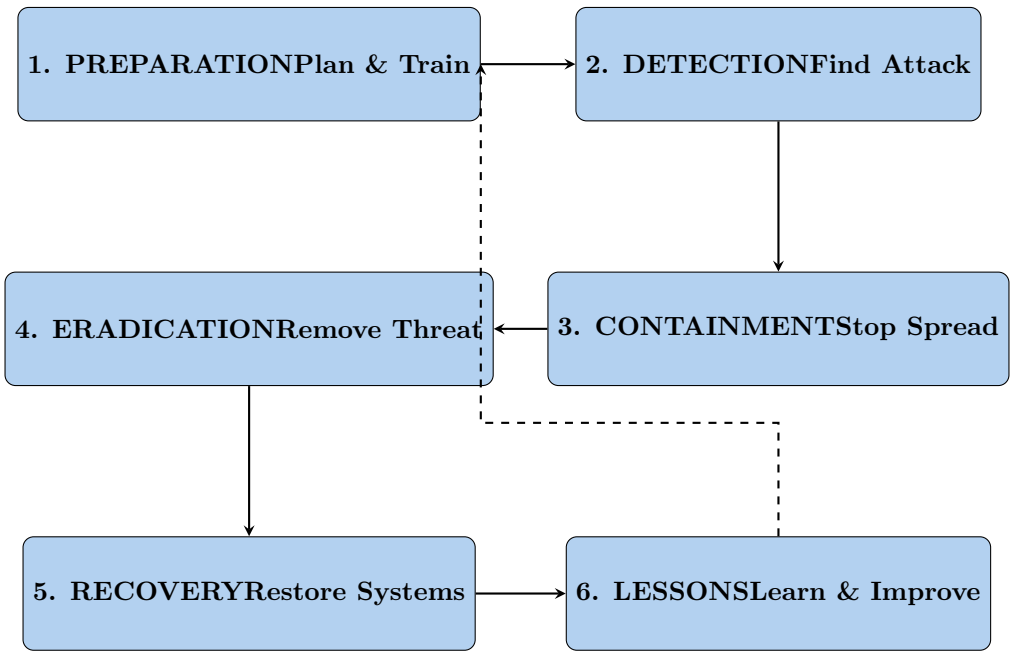

Figure 8: Incident Response Lifecycle - Continuous Process

WORKED EXAMPLE

Blue Team Incident Response Example:
Scenario: Ransomware attack detected at 2:00 AM

1. **Detection (2:05 AM):** Antivirus alerts to suspicious file encryption
2. **Containment (2:15 AM):**
   - Disconnect infected computers from network
   - Prevent spread to other systems
   - Isolate backup servers
3. **Eradication (3:00 AM):**
   - Identify and remove ransomware
   - Change all passwords
   - Patch vulnerabilities
4. **Recovery (8:00 AM):**
   - Restore files from backups
   - Verify system integrity
   - Bring systems back online gradually
5. **Lessons Learned (Next Week):**
   - How did ransomware get in? (Phishing email)
   - Update security awareness training
   - Implement email filtering

Time Calculation:

- Detection to containment: 10 minutes
- Containment to eradication: 45 minutes
- Full recovery time: 6 hours

KEY EXAM POINT

Blue Team Skills (You Need to Know):

- Digital forensics techniques
- Understanding of vulnerabilities and threats
- Forensic and security toolkits
- Good communication skills (for reports, testimony)
- Incident management procedures

Digital Forensics and Computer Security work together in incident response!

3 LAB 01: Linux and VirtualBox

3.1 Why Linux for Digital Forensics?

KEY EXAM POINT

Most professional forensic tools run on Linux because:

- Free and open source
- Powerful command-line tools
- More control over system
- Many forensic tools are Linux-based

3.2 Virtual Machines - Essential Concept

DEFINITION

Virtual Machine (VM) = Software that lets you run a "guest" operating system inside your "host" operating system.
Example: Running Linux inside Windows, or Windows inside macOS.

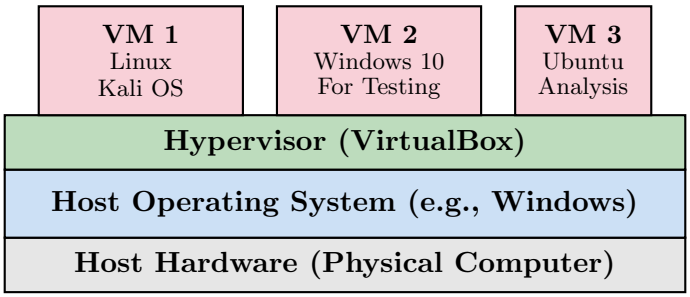

Figure 9: Virtual Machine Architecture - One Computer, Multiple Operating Systems

WORKED EXAMPLE

Why Use VMs in Digital Forensics?

1. **Safety:** Analyze malware without risking your real computer
2. **Isolation:** Keep evidence separate from your personal files
3. **Snapshots:** Save VM state, restore if something goes wrong
4. **Portability:** Move entire investigation to another computer
5. **Testing:** Try risky procedures without consequences

Real Scenario: You need to analyze a USB drive that might contain malware:

- DON'T plug it into your main computer directly
- DO create a VM, snapshot it, then plug USB into VM
- If malware activates, just delete the VM and restore snapshot

3.3 Disk Images - Two Types

KEY EXAM POINT

Don't Confuse These Two!

1. **VM Disk Images** - For installing operating systems in VMs
2. **Forensic Disk Images** - Copies of evidence drives

Type	File Format	Purpose	Used By
VM Images	.ISO	Install operating system in VM	VirtualBox, VMware
	.VDI, .VMDK	Store VM's virtual hard drive	VirtualBox, VMware
Forensic Images	.DD (raw)	Bit-by-bit copy of drive, includes deleted data	Forensic tools
	.E01 (EnCase)	Compressed copy with hash verification	EnCase, FTK

Table 11: Disk Image Types - Know the Difference!

DEFINITION

Key Differences:
ISO Image:

- Logical copy (only active files)
- Like copying only the books listed in a library catalog
- Doesn't include deleted data or unallocated space

DD/E01 Image:

- Physical copy (every single bit)
- Like photocopying every page in the library, including blank pages
- Includes deleted data, slack space, unallocated areas

WORKED EXAMPLE

Why Forensic Images Are Different:
Imagine a 500 GB hard drive:

- Used space: 300 GB (active files)
- Free space: 200 GB

ISO-style copy: Only copies the 300 GB of active files
DD forensic image: Copies all 500 GB, because the "free" 200 GB might contain:

- Deleted files that can be recovered
- Fragments of old documents
- Browser history remnants
- Critical evidence the suspect tried to hide

Size Comparison:

- ISO: 300 GB
- DD: 500 GB (always same size as original)
- E01 (compressed): ˜350 GB (smaller due to compression, but still has all data)

3.4 Essential Linux Commands

KEY EXAM POINT

Memorize These Commands - They Appear in Labs and Exams!

Command	What It Does	Example
`ls`	List files in current directory	`ls -la` (detailed list with hidden files)
`cd`	Change directory	`cd /home/user/Documents`
`pwd`	Print working directory (where am I?)	`pwd` shows `/home/user`
`mkdir`	Make new directory	`mkdir evidence`
`cp`	Copy files	`cp file1.txt backup/`
`mv`	Move or rename files	`mv old.txt new.txt`
`rm`	Remove (delete) files	`rm unwanted.txt`
`cat`	Display file contents	`cat report.txt`
`grep`	Search for text in files	`grep "password" log.txt`
`find`	Find files	`find / -name "evidence.dd"`
`chmod`	Change file permissions	`chmod 755 script.sh`
`sudo`	Run command as administrator	`sudo apt install tool`
`dd`	Create disk image (forensic)	`dd if=/dev/sda of=image.dd`

Table 12: Essential Linux Commands for Digital Forensics

WORKED EXAMPLE

Real Forensic Scenario - Using Linux Commands:
You need to find all files containing the word "confidential" on a suspect's drive:

```
# Step 1: Mount the forensic image
sudo mkdir /mnt/evidence
sudo mount evidence.dd /mnt/evidence

# Step 2: Search for files with "confidential"
grep -r "confidential" /mnt/evidence > results.txt

# Step 3: List all PDF files
find /mnt/evidence -name "*.pdf" > pdf_files.txt

# Step 4: Check results
cat results.txt
```

What Each Command Does:

- `mkdir`: Creates folder to access evidence
- `mount`: Makes the image accessible like a normal drive
- `grep -r`: Searches recursively through all files
- `find`: Locates all PDF files
- `cat`: Displays your findings

COMMON MISTAKE - AVOID!

Common Linux Mistakes:

1. Using `rm` without thinking - deleted files are GONE (no Recycle Bin!)
2. Forgetting `sudo` when you need admin rights
3. Wrong slashes: Linux uses `/` not \
4. Case sensitivity: `File.txt` `file.txt`

3.5 Lab Tasks Summary

KEY EXAM POINT

Lab 01 Objectives:

1. Complete "Learning Linux Command Line" course on LinkedIn Learning
2. Complete "Learning VirtualBox" course on LinkedIn Learning
3. Install a Linux distribution on VirtualBox
4. Save certificates and screenshots in your logbook

WORKED EXAMPLE

Step-by-Step: Installing Ubuntu on VirtualBox

1. **Download VirtualBox:** Get it from `virtualbox.org`
2. **Download Ubuntu ISO:** Get it from `ubuntu.com/download`
3. **Create New VM in VirtualBox:**
   - Click "New"
   - Name: "Ubuntu-Forensics"
   - Type: Linux
   - Version: Ubuntu (64-bit)
4. **Allocate Resources:**
   - RAM: 4096 MB (4 GB) minimum
   - Hard disk: 25 GB minimum
   - Processors: 2 CPU cores
5. **Attach ISO:**
   - Settings → Storage
   - Click empty CD icon
   - Choose your Ubuntu ISO file
6. **Start VM and Install:** Follow Ubuntu installation wizard
7. **Take Snapshot:** After installation, take a snapshot (backup point)

Resource Calculation: If your host computer has:

- 16 GB RAM → Allocate 4-8 GB to VM
- 8 GB RAM → Allocate 2-4 GB to VM
- 4 GB RAM → VMs will be slow, consider upgrading

Rule of thumb: Don't allocate more than 50% of host RAM to VMs.

4 EXAM PREPARATION GUIDE

4.1 Quick Reference: Key Terms

Term	Simple Definition for Exams
Confidentiality	Only authorized people can access data
Integrity	Data hasn't been tampered with or modified
Availability	Systems and data are accessible when needed
Chain of Custody	Documented record of who handled evidence
Digital Evidence	Data from digital devices used in investigations
Digital Forensics	Scientific analysis of digital evidence
Incident Response	Process of handling security breaches
Blue Team	Defensive security team
Virtual Machine	Software that runs an OS inside another OS
Forensic Image	Bit-by-bit copy of storage device
Acquisition	Collecting digital evidence
Authentication	Verifying someone's identity
Encryption	Scrambling data to make it unreadable
Malware	Malicious software (viruses, ransomware, etc.)
Ransomware	Malware that locks files and demands payment

Table 13: Glossary - Learn These Definitions!

4.2 Common Exam Question Patterns

KEY EXAM POINT

Types of Questions You'll See:

4.2.1 Pattern 1: Define and Explain

WORKED EXAMPLE

Q: Define the term "Chain of Custody" and explain why it is important in digital forensics.
A: Chain of Custody is the chronological documentation that records the sequence of custody, control, transfer, and analysis of physical or digital evidence.
Importance:

- Ensures evidence integrity (hasn't been tampered with)
- Makes evidence admissible in court
- Provides accountability (know who handled it)
- Protects against legal challenges

4.2.2 Pattern 2: CIA Triad Application

WORKED EXAMPLE

Q: A hospital's patient database was hacked. The attacker changed patient blood types. Which element of the CIA Triad was violated? Explain the potential consequences.
A: Integrity was violated because data was modified without authorization.
Consequences:

- Patients could receive wrong blood type in transfusions
- Life-threatening medical errors
- Loss of trust in hospital systems
- Legal liability for the hospital
- Need to verify all patient records (expensive and time-consuming)

4.2.3 Pattern 3: Scenario Analysis

WORKED EXAMPLE

Q: An employee is suspected of stealing company data. Their laptop was seized. List the steps a forensic investigator should take.
A:

1. **Documentation:** Photograph laptop, note its condition, time/date
2. **Chain of Custody:** Create log with investigator name, seizure location
3. **Isolation:** Place laptop in Faraday bag (block wireless signals)
4. **Transportation:** Secure transport to forensics lab
5. **Forensic Imaging:** Create bit-by-bit copy using DD or FTK Imager
6. **Hash Verification:** Calculate hash of original and copy to prove match
7. **Analysis:** Work only on the copy, never the original
8. **Reporting:** Document findings, maintain chain of custody throughout

4.2.4 Pattern 4: Compare and Contrast

WORKED EXAMPLE

Q: Compare computer security and digital forensics. How do they differ?
A:

Computer Security	Digital Forensics
Proactive (prevention)	Reactive (investigation)
Happens BEFORE attacks	Happens AFTER attacks
Goal: Stop breaches	Goal: Find out what happened
Uses firewalls, antivirus	Uses forensic tools, imaging
Focuses on protecting assets	Focuses on collecting evidence
May delete logs to save space	Preserves ALL data for analysis

Overlap: Both collaborate in incident response!

4.3 Practice Problems

KEY EXAM POINT

Try These Before the Exam!

4.3.1 Problem Set 1: Calculations

WORKED EXAMPLE

Problem 1: A forensic analyst creates a DD image of a 750 GB hard drive. The drive is 60% full. How large will the image file be?
Solution: DD creates a physical copy, so image size = original size, regardless of how full it is.
Answer: 750 GB
(Common mistake: Students calculate 60% of 750 GB = 450 GB. Wrong! DD copies EVERYTHING including empty space.)

WORKED EXAMPLE

Problem 2: Your final grade is calculated as:

- Class Test 1: 20% (you scored 68%)
- Coursework 1: 20% (you scored 72%)
- Class Test 2: 20% (you scored 75%)
- Coursework 2: 40% (you scored 80%)

What is your final grade? Will you pass (40%)?
Solution:

$$\begin{aligned}\text{Final} &= (0.20 \times 68) + (0.20 \times 72) + (0.20 \times 75) + (0.40 \times 80) \\ &= 13.6 + 14.4 + 15 + 32 \\ &= 75\%\end{aligned}$$

Answer: 75% - You pass with a B grade!

4.3.2 Problem Set 2: True or False

WORKED EXAMPLE

Mark each statement as TRUE or FALSE. Explain why.

1. ISO images include deleted data from a hard drive.

   FALSE. ISO images are logical copies (file-system aware), not physical copies. Only DD/E01 images capture deleted data.

2. Encryption helps computer security but hinders digital forensics.

   TRUE. Encryption protects data from unauthorized access (security), but makes it harder for investigators to analyze evidence (forensics).

3. A Blue Team tries to hack into systems to find weaknesses.

   FALSE. Blue Teams are defensive (protect systems). Red Teams are offensive (attack to test).

4. Chain of custody is only important for physical evidence, not digital.

   FALSE. Chain of custody is CRITICAL for digital evidence to be admissible in court.

5. Availability means data is protected from unauthorized access.

   FALSE. That's Confidentiality. Availability means data is accessible when needed.

4.3.3 Problem Set 3: Short Answer

WORKED EXAMPLE

Q1: List 5 sources of digital evidence in a modern car accident investigation.
A:

1. ECU (Engine Control Unit) - speed, braking data
2. GPS system - location, route history
3. Dashcam footage - video of accident
4. Smartphone records - driver's phone usage during accident
5. Infotainment system - Bluetooth connections, calls

WORKED EXAMPLE

Q2: A company's servers were hit with ransomware. As part of the Blue Team, outline the incident response steps.
A:

1. **Detection:** Identify affected systems via antivirus alerts
2. **Containment:** Disconnect infected servers from network immediately
3. **Eradication:** Remove ransomware, patch vulnerabilities
4. **Recovery:** Restore data from clean backups
5. **Post-Incident:** Analyze how it happened, improve defenses

4.4 Final Exam Checklist

Before Class Test 1 - Can You...

- ☐ Explain the CIA Triad with examples?
- ☐ Describe the difference between computer security and digital forensics?
- ☐ List and explain 3 real cyber attacks from 2024-2025?
- ☐ Define chain of custody and explain its importance?
- ☐ Describe the 4 stages of digital forensics (Acquisition, Identification, Evaluation, Presentation)?
- ☐ Explain the 3 ways devices can be involved in crimes?
- ☐ Differentiate between ISO, DD, and E01 disk images?
- ☐ Describe what a virtual machine is and why it's used in forensics?
- ☐ List the 6 phases of incident response?
- ☐ Execute basic Linux commands (ls, cd, grep, find, dd)?
- ☐ Explain what Blue Team does?
- ☐ Calculate your course grade given test/coursework scores?

4.5 Memory Aids and Mnemonics

KEY EXAM POINT

Use These to Remember Key Concepts:

- **CIA Triad:** "Can I Access?" - **C**onfidentiality, **I**ntegrity, **A**vailability
- **Digital Forensics Process:** "All Investigators Examine Proof"
  - **A**cquisition
  - **I**dentification
  - **E**valuation
  - **P**resentation
- **Incident Response:** "Please Don't Cancel Every Recovery Lesson"
  - **P**reparation
  - **D**etection
  - **C**ontainment
  - **E**radication
  - **R**ecovery
  - **L**essons learned
- **Assessment Breakdown:** "2-2-2-4" (20%, 20%, 20%, 40%)

4.6 Last-Minute Tips

COMMON MISTAKE - AVOID!

Common Mistakes to Avoid:

1. Confusing Confidentiality with Availability
2. Thinking ISO images include deleted data (they don't!)
3. Mixing up Red Team (attack) and Blue Team (defend)
4. Forgetting that DD images are ALWAYS the same size as original
5. Not showing calculations in math problems (show your work!)
6. Writing vague answers - always give specific examples

KEY EXAM POINT

Exam Success Strategy:

- Read questions twice before answering
- Use real-world examples when possible
- Show your calculation steps
- Define terms before using them
- Budget your time (don't spend 30 minutes on one question)
- If unsure, write what you know - partial credit is better than blank

5 APPENDIX: Command Reference

5.1 Complete Linux Command Cheat Sheet

```
# Navigation
pwd                         # Show current directory
ls                          # List files
ls -la                      # List all files with details
cd /path/to/folder          # Change directory
cd ..                       # Go up one level
cd ~                        # Go to home directory

# File Operations
cp source.txt dest.txt      # Copy file
cp -r folder1 folder2       # Copy folder recursively
mv old.txt new.txt          # Rename file
mv file.txt /new/path/      # Move file
rm file.txt                 # Delete file (careful!)
rm -r folder                # Delete folder and contents
mkdir newfolder             # Create directory
touch newfile.txt           # Create empty file

# Viewing Files
cat file.txt                # Display entire file
less file.txt               # View file page by page (q to quit)
head file.txt               # Show first 10 lines
tail file.txt               # Show last 10 lines
tail -f logfile.txt         # Follow file as it grows

# Searching
grep "password" file.txt                # Find "password" in file
grep -r "evidence" /folder              # Search recursively
grep -i "case" file.txt                 # Case-insensitive search
find / -name "*.jpg"                    # Find all JPG files
find /home -type f -size +100M          # Find files larger than 100MB

# Permissions
chmod 755 file.sh           # Make file executable
chmod 644 file.txt          # Standard file permissions
chown user:group file       # Change owner

# System Info
uname -a                    # System information
df -h                       # Disk space usage
free -h                     # Memory usage
top                         # Running processes

# Forensic Commands
dd if=/dev/sda of=image.dd bs=4K        # Create disk image
md5sum image.dd                         # Calculate MD5 hash
sha256sum image.dd                      # Calculate SHA256 hash
file filename.ext                       # Identify file type
strings binary_file                     # Extract readable strings
```