

Lecture 1

Digital Forensics Analysis (ACCA7031_LON)

Session 1 · Introduction to Digital / Cyber Forensics

Learning objectives

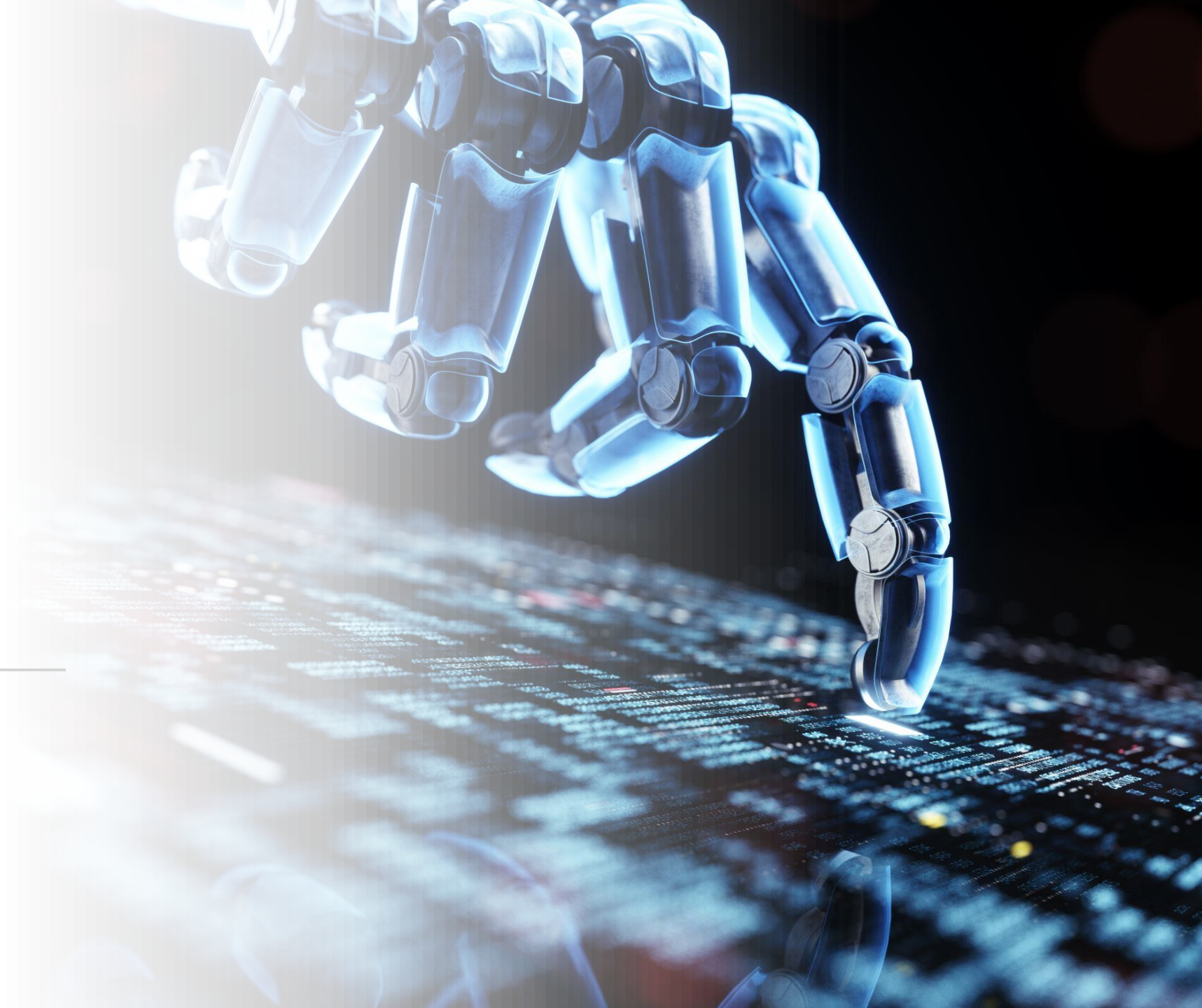
- Understand the cyber forensics domain
- Know the types of cyber crime and tools used
- Differentiate law enforcement and corporate investigation
- Understand why a digital forensics laboratory is needed
- Name the major tools and frameworks used in DFIR

ROADMAP

Topics 1–10, then a case study.



1. What is cyber forensics?





Crime scene forensics



Crime scene forensics

Scene sealed off with tape

Photograph the scene before touching anything

Fingerprints and DNA

Footprints in rain: fragile, collect first

Sealed, labelled evidence bag

Analyse samples, keep the original safe

Piece together a torn, burnt document

Signed chain of custody form

Analogy: a physical crime scene vs a digital one

Crime scene forensics

Crime scene sealed off with tape

Photograph the scene before touching

Fingerprints and DNA

Footprints in rain: fragile, collect first

Sealed, labelled evidence bag

Analyse samples, keep the original safe

Piece together a torn, burnt document

Signed chain of custody form



Digital forensics

Device isolated; write-blocker attached

Record screen and state; document everything

Hashes, metadata, logs and timestamps

RAM: volatile, capture first

Forensic image (E01) with a hash

Analyse the image, keep the original sealed

Carve deleted files from fragments

Chain of custody / acquisition log

1. What is cyber forensics?

- Application of law to the cyber domain
- Forensic science applied to computers, mobiles, networks and clouds
- Identify, preserve, analyse and present digital evidence
- Evidence must be acceptable in legal proceedings
- Sources: hard disk, RAM, external storage, network logs, cloud

IN ONE LINE

Finding, protecting and explaining digital evidence so it stands up in court.

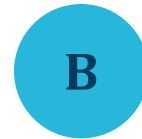


Scenario:

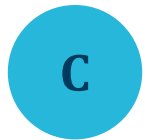
An employee is suspected of leaking files. The IT manager plugs in the laptop and browses through the folders to look for evidence.



It is too slow



Browsing can change data such as timestamps and weaken the evidence



Laptops cannot be examined



Only police may look at laptops



Answer

Just opening files can change access times and other data, which can make the evidence unreliable in court. Investigators work on protected copies instead.

Terminology check: research these

In pairs: define each term in one sentence and give a simple example.

DFIR

Chain of custody

Write-blocker

Forensic image

E01

Hash value

Acquisition

Volatile memory (RAM)

Electronic discovery

Carving

Bookmarking

Email spoofing

Answers: definitions and examples (1/2)

DFIR

Digital Forensics and Incident Response: investigating digital evidence and responding to security incidents.

Example: After ransomware hits, the team contains it and works out how it got in.

Chain of custody

A documented record of who handled evidence, when and why, from seizure to court.

Example: A signed log shows a laptop moved from officer to lab to locked storage.

Write-blocker

A hardware or software tool that lets a drive be read but blocks any writes to it.

Example: A suspect USB is read through one so its timestamps do not change.

Forensic image

A bit-for-bit copy of a drive, including deleted and unallocated data.

Example: Analysts work on the image; the original stays sealed.

E01

Expert Witness Compression Format: a compressed image format that stores case details and hashes.

Example: FTK Imager saves the file as Case1234_USB_E01.

Hash value

A fixed-length digital fingerprint of data; any change gives a different value.

Example: Source and image hashes match, so the copy is identical.

Answers: definitions and examples (2/2)

Acquisition

Collecting or copying digital evidence, physically (whole disk) or logically (selected files).

Example: Imaging the entire USB is physical; copying one folder is logical.

Volatile memory (RAM)

Temporary memory that is lost at power-off; holds running programs and connections.

Example: Capture RAM from a live PC before shutting it down.

Electronic discovery

Collecting, reviewing and producing electronic documents for legal proceedings.

Example: A court orders a firm to hand over all relevant emails.

Carving

Rebuilding deleted files from raw data fragments using file signatures.

Example: Recovering a deleted photo from unallocated space.

Bookmarking

Tagging evidence in a forensic tool so it is included in the report.

Example: Bookmark the sent email so it appears in the final report.

Email spoofing

Forging sender details so an email looks like it came from someone trusted.

Example: In M57-Jean, a fake "Alison" address tricked Jean.

2. Skills and the profession

- Three skill sets: legal procedures and laws of evidence, computer technology, investigative techniques
- Value of evidence depends on all three
- Extra qualities: technical skills, communication, investigator mindset, self-motivation
- Roles: private investigator, corporate compliance, law enforcement

THREE SKILL SETS

Law · Technology ·
Investigation

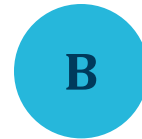


Scenario:

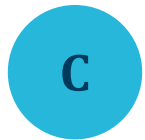
A very talented IT technician finds deleted emails on a drive, but has never learned the rules of evidence and cannot explain the findings clearly.



The evidence may lose its value despite being found



Nothing, technical skill is enough



The drive will run faster



The case will end sooner



Answer

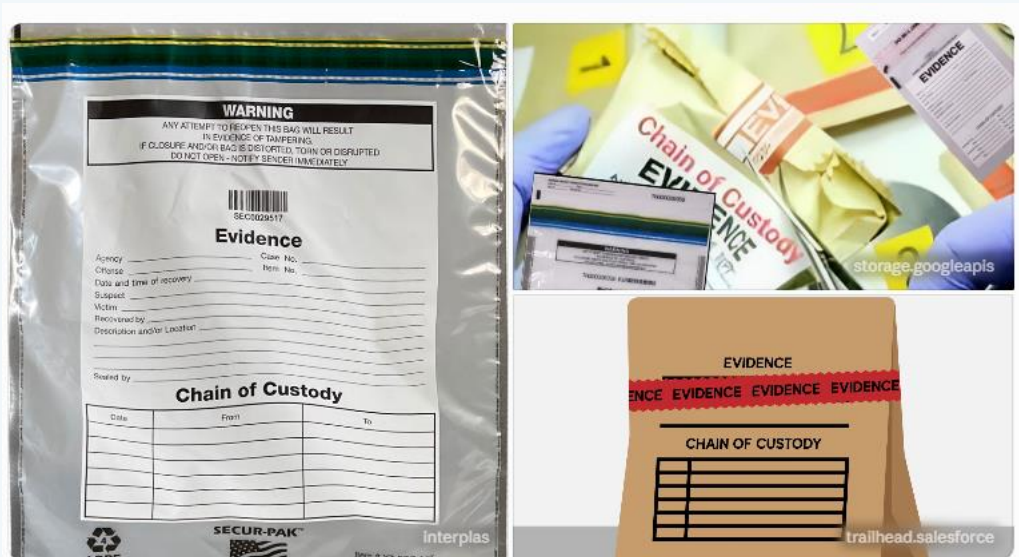
Value depends on legal knowledge, technical skill and investigative technique together.
Missing one weakens the whole case.

3. The forensic process

- Identification → Collection → Preservation
- Examination → Analysis → Presentation
- Requires deep knowledge of hardware and software
- Avoid accidental destruction or invalidation of evidence

WORKFLOW

Preserve before you examine.



?

Scenario: what would you do?

Sam starts opening and analysing files on a suspect laptop straight away, before making any protected copy.

A

Presentation

B

Preservation

C

Identification

D

Reporting



Answer

Preservation, protecting the original, was skipped. Analysis should be done on a verified copy so the original stays unchanged.

4. Types of forensics

- Computer forensics: computers and storage media
- Mobile forensics: recovery from mobile devices
- Network forensics: monitoring and analysing traffic
- Database forensics: databases and their metadata
- Printer forensics: identifying the printing device

FIVE BRANCHES

Different evidence,
different techniques.

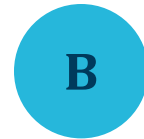


Scenario:

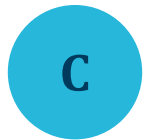
Police seize a smartphone that holds messages related to a fraud case.



Network forensics



Mobile forensics



Database forensics



Printer forensics



Answer

Recovering evidence from a phone is mobile forensics.

5. Electronic discovery

- Produces electronic documents for litigation
- Emails, Word/PPT/spreadsheets, databases, photos
- Collected, prepared, reviewed and distributed
- EDRM: Identification → Preservation/Collection → Processing/Review/Analysis → Production → Presentation

E-DISCOVERY

Volume goes down,
relevance goes up.

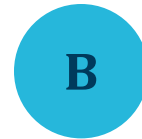


Scenario:

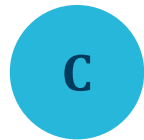
A company is sued and the court orders it to hand over all relevant emails and spreadsheets.



E-discovery



Steganography



Network monitoring



Data carving



Answer

Collecting and producing electronic documents for legal proceedings is electronic discovery.

6. Corporate, law enforcement, private

- Corporate: detection and prevention, minimal business interruption
- Corporate cases: email harassment, data falsification, embezzlement, sabotage, industrial espionage
- Law enforcement: prosecution
- Private: divorce (hidden assets), defence lawyers re-examining evidence

DIFFERENT GOALS

Corporate = stop it. Law enforcement = prosecute.

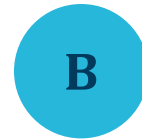


Scenario:

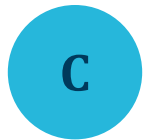
A company finds an employee emailing product designs to a rival and mainly wants it stopped quickly, with the business still running.



Prosecution



Detection and prevention



Divorce proceedings



Counter-intelligence



Answer

Corporate investigations focus on detection and prevention with minimal interruption. If serious, the case may later go to law enforcement.

7. The forensics laboratory

- Where you investigate and store evidence
- Physically secure so evidence is not lost, corrupted or destroyed
- Record activities and findings in a journal
- Goal: reproduce the same results
- Prepare a business case to build a lab

LAB RULES

Secure · Documented ·
Reproducible

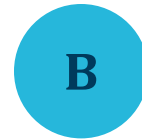


Scenario:

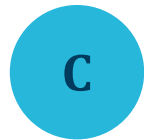
A colleague leaves a seized hard drive in an unlocked drawer in an open-plan office.



Reproducibility



Physical security of evidence



Report writing



Bookmarking



Answer

A lab must be physically secure so evidence cannot be lost, tampered with or destroyed.

Inside a digital forensics lab



Forensic workstation

Imaging and analysis PCs with write-blockers



Evidence storage

Locked, logged storage and evidence bags



Write-blocker bridge

Tableau-style device between drive and PC

8. Tools and acquisition

- Hardware tools: single-purpose components, complete systems
- Software tools: command-line and GUI
- Tasks: acquisition, validation, extraction, reconstruction, reporting
- Acquisition: physical or logical copy, verification
- Write-blockers stop writes to the source disk



WRITE-BLOCKER

A one-way door: read yes, write no.

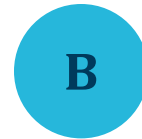


Scenario:

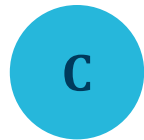
You must copy a suspect USB drive for analysis.



Plug it in a normal USB port



Connect it through a write-blocker



Email the files



Upload it to the cloud



Answer

A write-blocker prevents any changes to the original while it is copied.

9. Validation: hashing and filtering

- Hashing: CRC-32, MD5, SHA
- Filtering based on hash value sets
- Analysing file headers to identify true file types
- Matching hashes prove the copy is identical

HASH

A fingerprint for data. One changed bit = a totally different hash.

What is Hashing?

Hashing is the process of taking some data, such as a text, password, or file, and converting it into a fixed-length string of characters called a hash.

to check that data has not been changed.

ABC

Character	ASCII value
A	65
B	66
C	67

$65 + 66 + 67 = 198$

$198 \div 100 \rightarrow \text{remainder } 98$

ABC → 98

What is Hashing?

Hashing is the process of taking some data, such as a text, password, or file, and converting it into a fixed-length string of characters called a hash.

to check that data has not been changed.

ABD

Character	ASCII value
A	65
B	66
D	68

$65 + 66 + 67 = 199$

$199 \div 100 \rightarrow \text{remainder } 99$

ABD → 99

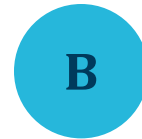


Scenario:

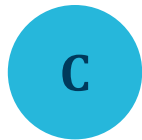
After imaging, the hash of the original drive and the hash of the image do not match.



Carry on, it is fine



The copy is not identical, so investigate and re-acquire



Delete the original



Edit the hash value



Answer

Different hashes mean the data differs. The image cannot be trusted until the problem is resolved.

10. Extraction and reconstruction

- Data viewing, keyword searching, decompressing
- Carving: rebuild fragments of deleted files
- Decrypting: dictionary and brute-force
- Bookmarking: mark evidence as you find it
- Reconstruction: disk-to-disk, image-to-disk copies

CARVING

Rebuild deleted files from raw fragments.

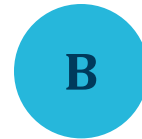


Scenario:

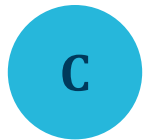
A suspect deleted photos, and you need to recover fragments from the drive image.



Carving



Bookmarking



Decompressing



Hashing



Answer

Carving reconstructs deleted files from fragments found in raw data.

Case study

Case study: M57-Jean

Corporate exfiltration

The setting

M57.biz is a small "virtual" start-up building a body art catalogue. Staff work from home, hotels and cafés, meet only occasionally, and swap most documents by email. That matters because there is no office network to watch, so email and each person's own computer are the main sources of evidence.

What happened

1. A spreadsheet of confidential staff information (names, positions, salaries, SSNs) turns up as an attachment in the "technical support" forum of a competitor's website.
2. It is traced back to CFO Jean's computer.
3. The two executives tell conflicting stories. Alison (the President) says she never asked for it and never received it. Jean says Alison asked him to prepare it for a funding round and email it to her.

Who says what?

- M57.biz: virtual start-up, staff work remotely, documents shared by email
- Spreadsheet with salaries and SSNs found on a competitor's forum
- Alison (President): never asked for it, never received it
- Jean (CFO): says Alison asked him to prepare and email it

QUESTION

Who is telling the truth,
and how would you check?

What the evidence showed

- Jean's hard drive was imaged and examined with a tool such as FTK
- The spreadsheet and the sent email were found
- The email requesting the data came from a spoofed address made to look like Alison's
- Jean unknowingly sent the data to an outsider

LESSON

Evidence resolved a he-said-she-said dispute.

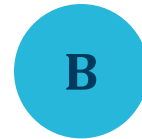


Scenario:

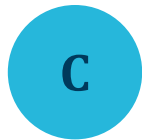
Jean's drive shows he emailed the spreadsheet to an address pretending to be Alison. Alison denies asking for it.



Alison deliberately leaked it



Jean is definitely the thief



An outsider likely spoofed Alison's email and tricked Jean



The competitor's forum created the file



Answer

The evidence points to a spoofed sender address, so an outsider probably impersonated Alison. Good investigators state what the evidence supports and note limits, rather than jumping to blame.

Summary

- What cyber forensics is and why process matters
- Skills, profession and forensic types
- E-discovery; corporate, law enforcement and private cases
- The lab, tools, acquisition, hashing, extraction
- Case study: M57-Jean

NEXT SESSION

Hands-on: acquiring evidence with FTK Imager.

Any questions?

Next: Session 2, Lab 1 acquisition