Qualifi Level 5 Diploma in Cyber Security

Digital Investigations and Forensics

Level 5: Diploma in Cyber Security
UeCampus Study Guide

Academic Module Study Guide Online Learning

Unit Overview: Three Chapters

Chapter 1

Core Principles of Digital Investigations

Defining digital forensics, investigation process, evidence types, chain of custody, legal frameworks, anti-forensics

Chapter 2

Tools & Techniques for Investigations

Forensic imaging, file system analysis, network forensics, mobile/IoT, memory forensics, professional tools

Chapter 3

Planning for Forensics Teams

Team building, lab accreditation, forensic readiness, reporting, expert testimony, emerging trends

The Subdisciplines of Digital Forensics

Computer Forensics

File systems, deleted files, email, browser history, timeline

Mobile Forensics

Smartphones, tablets, app data, GPS, encryption

Network Forensics

PCAP, IDS logs, flow data, intrusion detection

Memory Forensics

RAM analysis, malware, rootkits, encryption keys

Cloud Forensics

AWS/Azure/GCP, multi-tenancy, jurisdictional issues

IoT Forensics

Smart devices, CCTV, vehicles, proprietary formats

Database Forensics

Transaction logs, metadata, fraud detection

Multimedia Forensics

Image/video authenticity, deepfakes, EXIF data

Digital evidence is relevant in over 90% of all criminal investigations — not just cybercrime (UK Home Office)

The Four ACPO Principles

1. No action should change data that may be relied upon in court
2. If accessing original data is necessary, the person must be competent and able to explain their actions
3. An audit trail of all processes must be created and preserved — an independent third party should achieve the same result
4. The person in charge has overall responsibility for ensuring law and principles are followed

ACPO guidelines now maintained by NPCC — essential knowledge for all UK digital forensics practitioners

The Digital Forensic Investigation Process

Identification

Recognise incident, identify evidence sources, scope assessment

Collection & Preservation

Order of volatility, write blocking, forensic imaging, hash verification

Examination & Analysis

File system analysis, keyword search, timeline, data carving,
malware analysis

Reporting & Presentation

Executive summary, methodology, findings, conclusions, chain of custody

Every action must be documented: who, what, when, where, why, and how — a backup that cannot be verified is worthless

Types and Sources of Digital Evidence

Evidence Categories

- Active data – visible files, emails, databases
- Latent data – deleted files, slack space, swap files
- Archival data – backups, cloud archives
- Volatile data – RAM, processes, connections (lost at power-off)
- Metadata – timestamps, author info, GPS coordinates

Evidence Sources

Computers	Files, registry, event logs
Mobile Devices	Calls, SMS, app data, GPS
Servers	Access logs, databases, email
Network Devices	Router/firewall/IDS logs
Cloud Services	Stored files, API logs
IoT Devices	Sensor data, video, logs
CCTV	Video, timestamps, motion

Locard's Exchange Principle: 'every contact leaves a trace' — every digital interaction creates recoverable artefacts

Chain of Custody and Evidence Integrity

Maintaining Chain of Custody

- Document every transfer: who, when, why
- Use tamper-evident evidence bags
- Store in secure, access-controlled location
- Calculate SHA-256 hashes at every stage
- Work only on forensic images, never originals
- Photograph evidence in situ before collection
- Maintain detailed evidence log with exhibit refs

Hash Verification

Cryptographic hash functions are the cornerstone of digital evidence integrity.

SHA-256 computed at collection and at every subsequent stage proves evidence is unaltered.

If hashes match = data identical.
If hashes differ = integrity compromised.

MD5 has known collision vulnerabilities — always use SHA-256 alongside.

A broken chain of custody can cause critical evidence to be ruled inadmissible — potentially collapsing an entire case

Forensic Imaging and Data Acquisition

Physical Image

Bit-for-bit copy of entire device including unallocated space. Gold standard. Formats: E01, dd, AFF4.

Logical Acquisition

Files/folders visible to OS only. Faster but misses deleted data and slack space.

Live Acquisition

Data from running system including RAM, processes, connections. Essential for encrypted systems.

Cloud Acquisition

Data from cloud services via account credentials or legal process. Jurisdictional challenges.

Key Imaging Tools:

FTK Imager (free, GUI) • dd / dcfldd / dc3dd (Linux CLI) • Guymager (open-source GUI) • EnCase Forensic Imager • Magnet ACQUIRE (free, multi-platform)

File System and Network Forensics

Windows NTFS Artefacts

- MFT – central file index; deleted files retain entries
- Registry – config, USB history, recent docs, network
- Event Logs – logins, security events, app errors
- Prefetch – app execution history, run count, timestamps
- LNK files – shortcuts recording original path, volume ID
- ADS – Alternate Data Streams can hide data

Network Evidence Sources

- PCAP – full packet capture (Wireshark, tcpdump)
- NetFlow/sFlow – summarised connection records
- Firewall/proxy logs – allowed/blocked connections
- IDS/IPS alerts – Snort, Suricata, Zeek
- DNS logs – C2 communication, DNS tunnelling
- DHCP logs – IP-to-device mapping at specific times

Linux: inodes, journal, /var/log/, bash_history, cron jobs • macOS: APFS snapshots, Spotlight index, FSEvents, Unified Logs

Mobile, IoT, and Memory Forensics

Mobile Extraction Methods

- Manual – view & photograph screen
- Logical – files via USB/backup
- File system – full FS (root/jailbreak)
- Physical – bit-for-bit (chip-off, JTAG)
- Cloud – iCloud, Google, WhatsApp

Memory Forensics

- Running processes & hidden malware
- Open network connections (C2)
- Encryption keys in RAM
- User credentials & tokens
- Fileless malware (memory-only)
- Tools: Volatility 3, Rekall, AVML

IoT Forensics Challenges

- Proprietary data formats
- Limited device storage
- Manufacturer cooperation needed
- Diverse platforms & protocols
- Smart speakers, vehicles, medical devices as evidence

In 2016, prosecutors sought Amazon Echo data in an Arkansas murder case — one of the first cases highlighting IoT forensic potential

Professional Forensic Tools and Platforms

Commercial Platforms

EnCase Forensic	Industry standard; law enforcement
Magnet AXIOM	Computer, mobile, cloud, vehicle
Cellebrite UFED/PA	Mobile forensics market leader
X-Ways Forensics	Lightweight; European LE popular
Oxygen Forensic	Mobile + cloud + visualisation

Open-Source Tools

Autopsy / Sleuth Kit	Disk forensics platform
Volatility 3	Memory forensics framework
Wireshark	Network packet analyser
Zeek (Bro)	Network security monitor
SIFT Workstation	SANS forensic Linux distro
Plaso / Log2Timeline	Super timeline generation
YARA	Malware pattern matching

UK Legal and Ethical Framework

PACE 1984

Search & seizure powers for police

Computer Misuse Act 1990

Criminalises unauthorised access to computer systems

RIPA 2000

Surveillance, interception, key disclosure (Part III)

Data Protection Act 2018

UK GDPR compliance; data minimisation in investigations

Forensic Science Regulator Act 2021

Mandatory quality standards for digital forensics in CJS

Ethical Principles for Investigators:

Objectivity (report all evidence) • Competence (work within expertise) • Confidentiality (protect investigation details) • Proportionality (minimal intrusion) • Privacy (examine only relevant data)

Building a Forensics Team and Laboratory

Key Team Roles

- Forensic Team Lead / Manager
- Digital Forensic Examiner (DFE)
- Incident Responder
- Malware Analyst
- Network Forensic Analyst
- Mobile Device Examiner
- eDiscovery Specialist

Lab Requirements

- Restricted, logged physical access
- Secure evidence storage with environmental controls
- Faraday cage/bags for mobile examination
- CCTV monitoring of all areas
- Isolated forensic network
- ISO 17025 accreditation (UK mandatory for CJS)

Key certifications: GCFE, GCFA, EnCE, CCO/CCA, ACE, CompTIA CySA+, CISSP

Emerging Trends and Future Challenges

Encryption by Default	Full device encryption on iOS, Android, Windows makes acquisition significantly harder without keys
Cloud-First Architectures	Evidence resides with third-party providers across jurisdictions; requires legal processes and cooperation
AI & Deepfakes	AI-generated content challenges authenticity verification; detection tools still maturing
Fileless Malware	Operates entirely in memory; no disk trace; requires memory forensics capabilities
IoT Proliferation	Billions of devices with non-standard OS, proprietary protocols, limited tool support

The Forensic Science Regulator Act 2021, evolving data protection legislation, and 5G/edge computing continue reshaping the landscape

Key Takeaways

- Digital forensics spans 8 subdisciplines: computer, mobile, network, memory, cloud, IoT, database, and multimedia forensics
- The four ACPO principles are the UK foundation: no data change, competent access, audit trails, and overall responsibility
- Investigation follows four phases: Identification → Collection & Preservation → Examination & Analysis → Reporting
- Chain of custody with SHA-256 hash verification at every stage is essential for evidence admissibility
- Order of volatility: collect most volatile data first (RAM) before least volatile (hard drives, backups)
- Write blockers prevent any modification to original evidence — always work on forensic images
- Professional tools span commercial (EnCase, AXIOM, Cellebrite) and open-source (Autopsy, Volatility, Wireshark)
- ISO 17025 lab accreditation is mandatory for digital forensics in the UK criminal justice system
- Emerging challenges: encryption by default, cloud evidence, AI deepfakes, fileless malware, IoT proliferation