

DF-010 Quick Reference

One handout for all five modules. Keep it next to you while you do the activities.

Module 1: Digital evidence

Digital evidence is information, stored or transmitted in digital form, that can help prove or disprove a fact in an investigation.

Where it lives	Computers and servers · phones and tablets · cloud accounts and email · messaging apps · CCTV and DVR units · network and access control systems (router logs, firewall logs, door entry records)
Two layers	Created by the user: documents, photos, messages, emails. Recorded by the system: logs, timestamps, file history, connection records. The system layer is often more useful.
Metadata	Data about data: when a file was created, modified and (on some systems) opened; which account or device produced it; sometimes where a photo was taken.
Volatile	Lost when power is lost: memory, running processes, open network connections, the clipboard.
Non-volatile	Stays when power is off: hard drives, SSDs, USB drives, cloud storage, backups.

First rule: do not poke around on the original. Even opening a file can change its timestamps.

Module 2: How an investigation runs

1. **Identify** what evidence might exist and where.
2. **Preserve** it from change.
3. **Collect** (acquire) a repeatable copy.
4. **Examine** what you collected.
5. **Analyze** what it means.
6. **Report** what you found and how.

Before touching any device: settle your **authority** (who allowed you to look) and your **scope** (at what exactly). Write both down and stay inside them.

Order of volatility (capture the most short-lived first): processor registers and cache, then memory and network state, then temporary files, then disk, then logs held on other systems, then archives and backups.

Live vs powered-off acquisition: live can capture memory and running state but means interacting with the system; powered-off is stable and repeatable but volatile data is lost. Decide on purpose, and write down why.

References to know by name: ISO/IEC 27037, NIST SP 800-86, RFC 3227. Standards use slightly different stage names; the shape is the same.

Notes: who was present and who handled what; the device and its state; the time of each action with the time zone; where it was found; why you acted. Photograph what you can.

Module 3: Chain of custody and hashing

Chain of custody is a written record of who held an item, when, where and why, from seizure until it is presented. A handover that is not written down did not happen, as far as the record is concerned. Fill the record in at the time, not afterwards. Use the separate template for the activity.

Hash: a short, fixed-length fingerprint of a file. Change one character and the hash changes completely. Use **SHA-256** for new work. MD5 and SHA-1 are weak against deliberate collisions; do not rely on them alone.

Windows PowerShell	Get-FileHash file.txt -Algorithm SHA256
Windows Command Prompt	certutil -hashfile file.txt SHA256
Linux	sha256sum file.txt
Mac	shasum -a 256 file.txt

Work on copies. A write blocker (hardware or software) lets you read a drive without altering it. After copying, hash the original and the copy and compare. If they match, you have a verified copy.

Module 4: Legal basics for India (general education)

This is not legal advice. Laws change and your situation may be different. Check the current text of any law and speak to a qualified lawyer before you rely on it.

Information Technology Act, 2000	Defines electronic records and creates offences, including unauthorised access (s.43), computer-related offences (s.66, with 66C identity theft and 66D cheating by personation), publishing obscene material (s.67), and Examiner of Electronic Evidence (s.79A).
Bharatiya Sakshya Adhiniyam, 2023	Replaced the Indian Evidence Act; in force since 1 July 2024. Electronic records are admissible; the conditions and the certificate are in section 63, which replaces the old section 65B.
BNSS and BNS	The Bharatiya Nagarik Suraksha Sanhita replaced the CrPC; the Bharatiya Nyaya Sanhita replaced the IPC. For this course you need the names only.
Personal data	The Digital Personal Data Protection Act, 2023 applies in phases, with most obligations from 13 May 2027. Handle personal data lawfully, and only as far as your authority allows.

Plan for the evidence certificate from the start. Authority and consent differ by route (employer under written policy, a private person, law enforcement). In every case, document who authorised what.

Module 5: Tools and the case note

Imaging and triage	FTK Imager, Autopsy
Network	Wireshark
Memory	Volatility
Mobile	Cellebrite UFED, Magnet AXIOM
Cloud and enterprise	Audit, email and identity log tools

Facts vs opinions. A fact is what you observed, with times and sources. An opinion is what you think it means, clearly labelled and kept separate. Never write guilty or innocent.

One-page case note: Case ID, date and examiner · authority and scope · items received, with hash values · what was done, in order · what was found, as observed facts · limitations (what you could not check).

Ethics: stay within scope; if you find something outside it, stop and report it to whoever authorised the work; report what you find, not what people hope to hear; keep client and case data confidential.

Next courses: DF-020 (networking and OS basics), DF-030 (first look at forensic tools), DF-101 (foundations), then network, mobile, memory or cloud forensics.