n

Standards for Collecting, Preserving & Documenting Electronic Evidence

Digital evidence is inherently fragile — it can be altered, deleted, or rendered inadmissible through poor handling. This guide sets out the minimum standards for collecting, preserving, and documenting electronic evidence to maintain its integrity and admissibility.

Part 1 — Core Principles

Principle	What It Requires
Preservation First	Never work on original evidence. Always create a forensic copy before any examination.
Chain of Custody	Every person who handles evidence must be recorded. Any gap in custody weakens admissibility.
Integrity Verification	Hash values (MD5, SHA-256) must be calculated before and after any examination to prove evidence has not been altered.
Minimal Footprint	Interact with original evidence as little as possible. Use write-blockers for physical media.
Documentation	Document everything — what you did, when, how, and what you found. If it isn't written down, it didn't happen.
Proportionality	Collection must be proportionate to the investigation. Do not collect more than is necessary.

Part 2 — Initial Response Checklist

Before Touching Any Device

■ Photograph the scene before touching anything — show device locations, connections, and power state.

■ Note the time, date, location, and who is present.

■ Identify and record all devices visible — computers, phones, tablets, external drives, USB devices, network equipment.

■ Check if devices are powered on or off. Do NOT change the power state without supervisor guidance.

■ Note any open applications, windows, or content visible on screens (photograph if possible).

■ Secure the scene — prevent others from accessing devices until proper collection procedures are followed.

For Powered-On Devices

- ■ Do NOT shut down unless directed — volatile memory (RAM) may contain critical evidence.
- ■ Photograph the screen showing current state before any interaction.
- ■ Consider using a live acquisition tool to capture volatile memory and running processes.
- ■ If shutdown is necessary: document why, note the time, and where possible use forensic shutdown procedures.
- ■ Record all network connections visible (Wi-Fi network names, IP addresses displayed, VPN status).

For Powered-Off Devices

- ■ Do NOT power on the device — this can alter timestamps and create new artefacts.
- ■ Photograph and bag each device separately with an evidence label.
- ■ Record serial numbers, make, model, and any visible damage or unusual features.
- ■ Disconnect all external connections (cables, peripherals) and bag separately.
- ■ Use anti-static and Faraday bags for mobile devices to prevent remote wiping.

Part 3 — Chain of Custody Form

Complete one form per exhibit. Attach to the physical evidence bag.

Exhibit Number	_____
Case / Reference	_____
Device Description	Make: _____ Model: _____ Serial: _____
Hash Value (SHA-256)	_____
Collection Date/Time	_____
Collection Location	_____
Collected By	Name: _____ Signature: _____

Custody Log

Date / Time	Released By	Received By	Purpose / Location	Signature

Date / Time	Released By	Received By	Purpose / Location	Signature

Part 4 — Evidence Types & Special Considerations

Evidence Type	Collection Method	Key Consideration
Computers / Laptops	Use write-blockers. Create forensic image (bit-for-bit copy). Verify with hash values. Examine image only.	Off = bag without powering on. On = consider live acquisition first.
Mobile Phones / Tablets	Place in Faraday bag immediately to prevent remote wipe. Use specialist mobile forensic tools. Note IMEI/IMSI.	Do not charge uncontrolled. Enable airplane mode if safe to do so.
External Storage (USB, HDD)	Photograph connections before removal. Use write-blocker. Hash before and after image creation.	Label each device with exhibit number before bagging.
Cloud / Online Accounts	Obtain legal authority before access. Use platform-specific preservation requests. Note URL, account ID, date.	Request preservation hold immediately — platforms delete data quickly.
Network / CCTV Footage	Request immediately — CCTV systems overwrite. Note system time vs real time discrepancy. Export to common format.	Document recording format, frame rate, and camera locations.
Email / Messaging	Export in native format where possible (PST, MBOX). Capture headers — they contain routing and authentication data.	Metadata is as valuable as content — preserve both.

Part 5 — Admissibility Requirements

To Ensure Evidence Remains Admissible

- Authenticity: Be able to prove the evidence is what you claim it is (hash verification, chain of custody).
- Integrity: Be able to prove the evidence has not been altered since collection (before/after hash comparison).
- Reliability: Be able to demonstrate that the tools and methods used to collect evidence are accepted and reliable.
- Legality: Be able to confirm the evidence was obtained through lawful means with appropriate authority.
- Completeness: Disclose all relevant evidence — including evidence that weakens your case.

Need a Different Format?

- A printable chain of custody form and Excel evidence log are available on request.
- Email: info@theintelanalystacademy.com.au — Subject: 'Digital Evidence Doc — Format Request'