

EVIDENCE FIRST

COMPUTER

Computer First Response & Forensic Acquisition

2027 EDITION · FREE FIELD PREVIEW

**Making expert forensic decision-making
explicit, structured, and usable in
the field.**

**A reversible action buys options.
An irreversible action spends them.**

evidencefirst.guide

The decision before the tool.

Evidence First is a decision-oriented field guide for digital evidence first response and forensic acquisition.

It starts from the state actually observed, compares realistic alternatives, and makes the evidentiary consequences of intervention explicit before an action changes the device, the accessible state, or the options still available.

It is not an encyclopedic forensic manual, an artifact catalog, a command cheat sheet, or a tool-specific handbook.

THE OPERATIONAL QUESTION

What can I preserve? What can I lose? What footprint will I introduce? How reversible is the choice?

One method. Ten questions.

- 01 SCOPE** Define object, authority, limits, and stop/escalation conditions.
- 02 OBSERVE** Record the current observable state before intervention.
- 03 OPTIONS** Identify realistic operational alternatives.
- 04 GAIN** What can the action preserve or obtain?
- 05 LOSS** What can be lost?
- 06 FOOTPRINT** What evidence or state will the action create or change?
- 07 RISK** What evidentiary and operational consequences follow?
- 08 REVERSIBILITY** Can the prior state realistically be reconstructed?
- 09 DECIDE** Choose based on the state actually observed.
- 10 DOCUMENT** Record what was done and why.

**A reversible action buys options.
An irreversible action spends them.**

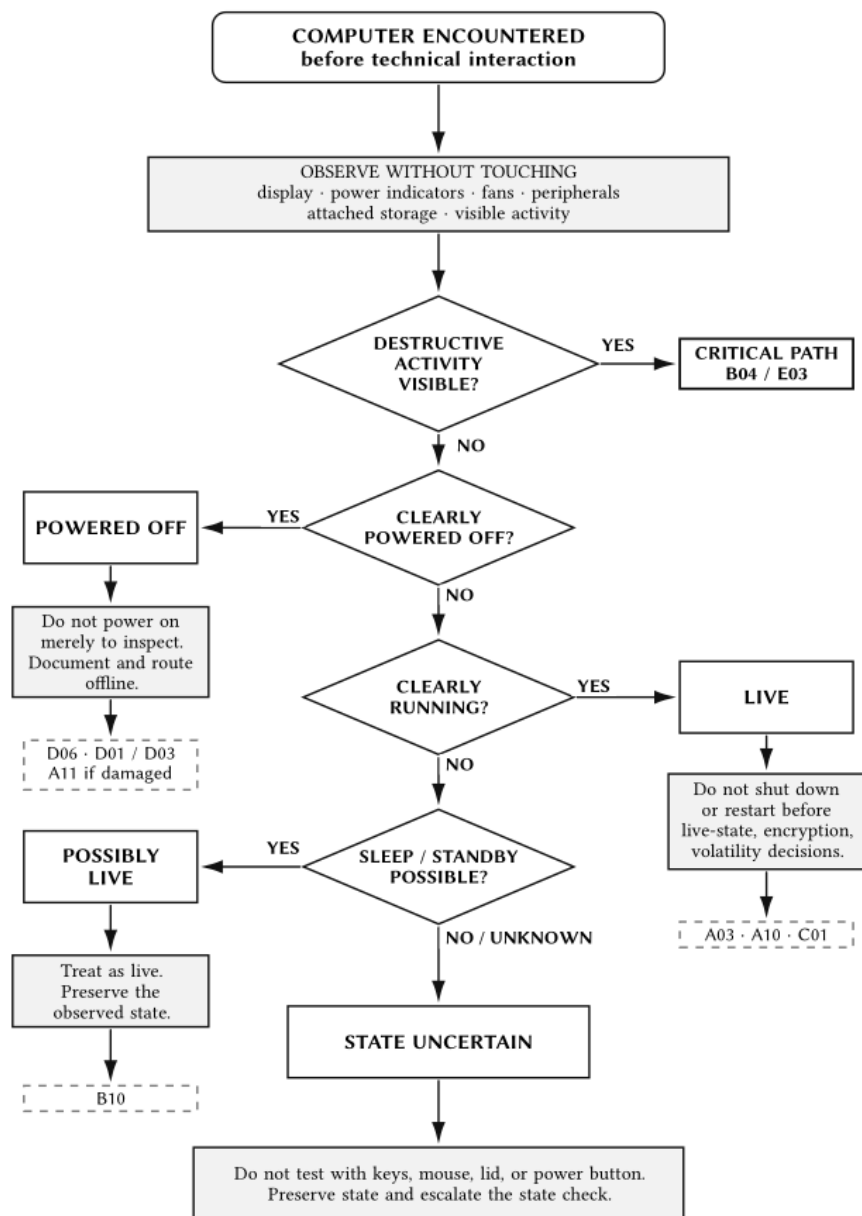
State Map · A01

Computer Found On/Off

VISUAL SUMMARY

STANDARD FLOW NOTATION

Flow notation: rounded box = situation/entry; rectangle = state/consequence/action; diamond = discriminant; arrow = state-dependent path; dashed box = cross-reference. H/M/L = reversibility.



Multiple Live Devices

FIRST-RESPONSE

MULTI-DEVICE

Situation: Two or more in-scope general-purpose computers are live at the same scene, but time, personnel, or acquisition capacity prevents treating all of them simultaneously.

Which computer must be handled first to avoid spending the most fragile or least reproducible evidence state?

OBSERVE FIRST

- ☐ Destructive activity on any device?
- ☐ Active exfiltration?
- ☐ Unlocked encrypted access unique?
- ☐ System becoming unstable?
- ☐ Active session/mounted dependency?
- ☐ Sleep/timeout imminent?
- ☐ Production/service consequence?
- ☐ Trained operators available in parallel?

OPTIONS & CONSEQUENCES

OPTION	GAIN	LOSS	FOOTPRINT / RISK	REV.
Prioritize most fragile state	Preserves the device whose unlocked, volatile, mounted, or session state is least reproducible	Deferred devices may lock, sleep, time out, disconnect, or otherwise change before collection	Intervention is concentrated on one device; state changes on deferred devices may occur unobserved	M
Parallelize with trained operators	Preserves several volatile/live states within the same time window	Sequence, cross-device context, or contemporaneous relationships may be captured unevenly if coordination fails	Concurrent live actions create multiple simultaneous source changes and require a shared chronology	M
Handle devices in convenient order	Preserves the state of whichever device is reached first without coordination delay	A more fragile device may lock, sleep, disconnect, or lose volatile evidence while waiting	Acquisition footprints still apply; sequencing is not evidence-driven and deferred-state drift increases	M
Change all devices to a common state first	May halt direct user activity and simplify physical control of the scene	Locking, logging off, sleeping, or powering down can destroy unique session, plaintext, RAM, mount, or encryption-access state	Multiple state transitions occur before preservation and may not produce evidentially equivalent states across devices	L

PRIORITIZE FIRST

- Active destructive/exfiltration behavior
- Unique unlocked/encrypted or mounted state
- Instability or imminent sleep/state loss
- Ephemeral session/dependency not reproducible elsewhere

DEFER MORE SAFELY

- Stable system with reproducible access
- No unique volatile dependency identified
- State documented and physically secured
- Service consequence requires coordination — see PRODSERVER

DOCUMENT

- ☐ Initial state of every device before prioritization
- ☐ Priority order, reason, operator assignment, and times

Built for the point of decision.

State-Entry Index

Enter from the condition actually encountered.

Decision Cards

Compare realistic alternatives through GAIN, LOSS, FOOTPRINT, RISK, and REVERSIBILITY.

Procedure Cards

Use compact procedures where the principal decision is already determined.

State Maps

Visualize state-dependent routing without forcing one universal workflow.

Quick Reference

Retrieve compact supporting information without creating unnecessary decision cards.

Field Forms

Record observations, actions, limitations, handoffs, and decision rationale.

One grammar across six domains.

01

Computer

Computer First Response & Forensic Acquisition

02

Mobile Devices

Mobile First Response & Forensic Acquisition

03

Network & Remote Infrastructure

Network First Response & Evidence Collection

04

Cloud & SaaS

Cloud First Response & Evidence Collection

05

Embedded & IoT Devices

Device First Response & Forensic Acquisition

06

Complex Scenes

Cross-Domain First Response & Evidence Coordination

Evidence First — Vol. 1: Computer

Computer First Response & Forensic Acquisition · 2027 Edition

Preorder / publication information

evidencefirst.guide/vol1

Kindle preorder: <https://amzn.eu/d/08CChKmF>

Further reading

Digital Forensics: acquisire subito o aspettare?

Prima bisogna capire cosa rischiamo di perdere — Red Hot Cyber (Italian)

[redhotcyber.com/post/digital-forensics-acquisire-subito-o-aspettare-
prima-bisogna-capire-cosa-rischiamo-di-perdere/](https://redhotcyber.com/post/digital-forensics-acquisire-subito-o-aspettare-prima-bisogna-capire-cosa-rischiamo-di-perdere/)

About the author

Lello Molinaro works across digital investigations, cybersecurity, and digital forensics, with a focus on the operational handling of digital evidence. His work combines field practice with academic study in computer engineering, cybersecurity, and artificial intelligence.

evidencefirst.guide

Current edition · companion resources · references · updates