Digital Evidence Case Assessment Checklist

Purpose: Identify potential digital-evidence sources, recognize evidence at risk of loss, establish the case evidence baseline, identify gaps, prioritize collection, and guide initial triage. Record case-specific details in case notes, the evidence log, or investigation worksheet.

Case / Client	
Case Number	
Assessor / Date	
Relevant Event / Time Period	

ASSESS → PRESERVE → BASELINE → ACT → TRIAGE → REASSESS

1. ASSESS — IDENTIFY DIGITAL-EVIDENCE SOURCES

Start broad. Identify sources from the client, scene, involved parties, third parties, law enforcement, government, providers, and businesses.

CLIENT / DEFENSE-CONTROLLED SOURCES

- ☐ Mobile phones / smartphones
- ☐ External / removable media
- ☐ Cloud storage / backups
- ☐ Social-media accounts
- ☐ Location / navigation
- ☐ Vehicles / connected-car systems
- ☐ Computers / laptops / tablets
- ☐ Email accounts
- ☐ Messaging apps
- ☐ Photos / video / audio
- ☐ Wearables / activity devices
- ☐ Other apps / accounts

SCENE / LOCATION SOURCES

- ☐ Surveillance / security video
- ☐ Business cameras
- ☐ ALPR / license-plate systems
- ☐ Alarm / security systems
- ☐ Smart-home / IoT devices
- ☐ Nearby cameras / locations
- ☐ Doorbell / residential cameras
- ☐ Traffic / roadway cameras
- ☐ Access-control / entry systems
- ☐ Wi-Fi / network systems
- ☐ POS / business systems
- ☐ Other scene source

INVOLVED PARTIES / WITNESSES / THIRD PARTIES

- ☐ Victim / complainant
- ☐ Other involved-person devices / accounts
- ☐ Messages / social media
- ☐ Wearables / vehicle data
- ☐ Ride-share / delivery records
- ☐ Witness devices / accounts
- ☐ Photos / video / audio
- ☐ Location data
- ☐ Employer / business records
- ☐ Other third-party source

For each important source:

- ☐ Who controls it?
- ☐ What time period matters?
- ☐ Could it corroborate / contradict?
- ☐ Where is it?
- ☐ What data might it contain?
- ☐ Could it identify another source?

2. ASSESS — LAW ENFORCEMENT, GOVERNMENT & PROVIDERS

LAW ENFORCEMENT / GOVERNMENT SOURCES

- ☐ Body-worn camera
- ☐ Surveillance / pole camera
- ☐ Cell-site / location records
- ☐ Search-warrant returns
- ☐ Digital forensic reports
- ☐ Cloud / provider returns
- ☐ Investigative databases / analytical systems
- ☐ Dash / patrol vehicle camera
- ☐ 911 / dispatch / CAD records
- ☐ ALPR data
- ☐ Device seizures / forensic extractions
- ☐ Underlying extraction / forensic image
- ☐ Social-media / platform returns
- ☐ Other government source

SERVICE PROVIDERS / PLATFORMS / BUSINESSES

- ☐ Wireless carrier
- ☐ Cloud-storage provider
- ☐ Messaging platform
- ☐ Financial / payment platform
- ☐ Hotel / lodging system
- ☐ Email provider
- ☐ Social-media platform
- ☐ Ride-share / delivery
- ☐ Retail / business system
- ☐ Other provider / business

SOURCE IDENTIFICATION / ASSESSMENT

- ☐ Source confirmed
- ☐ Source likely
- ☐ Custodian / controller identified
- ☐ Relevant date / time identified
- ☐ Potential evidence identified
- ☐ Source reported / referenced
- ☐ Source possible / unconfirmed
- ☐ Location identified
- ☐ Access method identified
- ☐ Related sources identified

☐ Corroboration / contradiction considered
☐ Source documented

3. PRESERVE — TIME-SENSITIVE EVIDENCE

Could the source be lost, overwritten, deleted, changed, or become inaccessible before it can be obtained?

LOSS / ACCESS RISKS

☐ Short or unknown retention period
☐ User deletion
☐ Device loss / reset / replacement
☐ Data changes over time
☐ Known deadline / approaching expiration
☐ Automatic overwrite / continuous recording
☐ Account closure / suspension
☐ Third-party control
☐ Legal-process delay
☐ Other risk

If YES:
☐ Identify what may be lost
☐ Identify responsible person
☐ Document action
☐ Determine preservation action
☐ Identify deadline

☐ **URGENT** — imminent loss / overwrite ☐ **HIGH** — meaningful risk ☐ **NORMAL** — stable source

DERU RULE: Address evidence at risk of loss before routine collection planning.

4. BASELINE — WHAT SHOULD EXIST?

Every identified or suspected source should be accounted for.

SOURCE STATUS

☐ Unknown
☐ Preservation Needed
☐ Collected / Obtained
☐ Missing / Unavailable
☐ Identified
☐ Preserved
☐ Initial Triage Complete
☐ Specialized Review Needed

EXPECTED SOURCE PROMPTS

☐ Devices that should exist
☐ Cameras / video that should exist
☐ Location data that should exist
☐ Native / underlying records
☐ Records referenced by another source
☐ Accounts that should exist
☐ Communications that should exist
☐ Provider / business records
☐ Forensic source data / extraction
☐ Additional source suggested by known facts

MISSING-EVIDENCE CHECK

What should exist based on the facts, but is not currently available to the defense?

☐ Source identified but never requested
☐ LE source referenced; underlying material missing
☐ Third-party source unresolved
☐ Native / underlying data missing
☐ Evidence may have been lost / overwritten
☐ Requested but not received
☐ Client / witness source known but not obtained
☐ Relevant time period incomplete
☐ Extraction / source material missing
☐ Existing evidence indicates another source

5. ACT — PRIORITIZE PRESERVATION / COLLECTION

POSSIBLE NEXT ACTIONS

☐ Preserve immediately
☐ Obtain from witness / involved party
☐ Request from third party
☐ Direct collection
☐ Follow up on retention / availability
☐ Obtain from client
☐ Request from law enforcement
☐ Provider / legal process
☐ Forensic acquisition
☐ Monitor / defer

Prioritize by: evidence value + risk of loss + access constraints + legal / process requirements + deadline.

FOR UNRESOLVED SOURCES

☐ Priority assigned
☐ Deadline identified
☐ Responsible person identified
☐ Action documented

NEW SOURCE? Add to baseline → Assess risk → Preserve → Act.

6. TRIAGE & REASSESS

Initial triage is a first assessment of what was obtained, what appears missing, what it may show, and what should happen next. It is not necessarily a full forensic examination.

INITIAL TRIAGE

☐ Source received matches source identified
☐ Apparent completeness checked
☐ Significant evidence identified
☐ Contradictions / inconsistencies identified
☐ Relevant date / time period confirmed
☐ Missing / inaccessible / corrupted material identified
☐ Potentially exculpatory information identified
☐ Additional evidence sources identified

☐ New investigative questions identified
☐ Evidence baseline updated
☐ Further examination considered
☐ Preservation / collection priorities updated

Evidence reviewed → New source identified → Add to baseline → Assess risk → Preserve → Collect → Triage

FINAL CASE ASSESSMENT

☐ Client / defense-controlled sources assessed
☐ Involved parties / witnesses assessed
☐ Law-enforcement sources assessed
☐ Time-sensitive evidence identified
☐ Digital-evidence baseline established
☐ Collection / action priorities established
☐ New sources incorporated
☐ Scene / location sources assessed
☐ Third-party sources assessed
☐ Government / provider / business sources assessed
☐ Preservation needs addressed
☐ Missing evidence identified
☐ Obtained evidence triaged where appropriate
☐ Follow-up actions identified

FOLLOW-UP / REASSESSMENT

Next review / action date	
Highest-priority unresolved issue	
Responsible investigator / team	

STOP & ASK: What digital evidence should exist that we have not yet identified, preserved, obtained, or evaluated?

Use with case notes, evidence logs, preservation records, discovery review, collection protocols, and applicable legal / process requirements. This checklist is a starting-point assessment and workflow guide; it does not replace jurisdiction-specific law, legal advice, preservation requirements, or forensic protocols.

DERU