DERU

Time-Sensitive Digital Evidence Technical Guide

Investigator Companion to the Time-Sensitive Digital Evidence Assessment and Digital Evidence Case Assessment Checklist

Purpose

A practical guide for investigators who may not have extensive digital-forensic training. Use it to identify digital evidence that may disappear, change, be overwritten, or become inaccessible; determine what must be addressed first; document what you learn; and recognize when specialized assistance is needed.

Digital Innocence Initiative
Digital Evidence Review Unit (DERU)

Version 1.1 | August 2026

How to Use This Guide

This guide is designed to be used with the DERU Time-Sensitive Digital Evidence Assessment and the Digital Evidence Case Assessment Checklist. The checklist helps the investigator identify possible sources and track the case baseline; this guide explains why a source may be urgent, what technical questions matter, what to document, what not to do, and when to obtain qualified assistance.

> **Core Rule**
> If retention, overwrite behavior, device stability, account access, or the method needed to preserve or collect the evidence is unknown, treat the source as potentially time-sensitive until current guidance is confirmed.

- Use the checklist first to identify every possible source. Do not limit the assessment to evidence already mentioned in discovery.
- For each source, identify the controller or custodian, the relevant date/time range, the loss mechanism, and the next action.
- Address sources at risk of loss before routine collection planning.
- Preservation and collection are different. A preservation request may reduce the risk of deletion, but it does not give the defense the evidence.
- Do not perform a forensic examination simply because the device or account is accessible. Initial triage is different from a full forensic examination.
- When a source exceeds your training, authority, or technical capability, stop and obtain qualified assistance.

> **This is not a seizure or extraction manual**
> An investigator should not improvise isolation, unlocking, password attempts, forensic extraction, device repair, or technical acquisition procedures. The goal is to recognize the issue, prevent avoidable loss, document the condition, and get the right person involved.

1. The 10-Minute Time-Sensitive Evidence Triage

At the beginning of a case, or whenever a new fact is learned, run this short triage before doing anything else with digital evidence.

1. What happened, where did it happen, and what exact time period matters?
2. Who was present or involved, and what devices, accounts, vehicles, businesses, cameras, networks, or systems were likely around them?
3. Which sources could be overwritten, deleted, reset, replaced, remotely changed, or become inaccessible?
4. Who controls each source right now: client, witness, business, provider, platform, law enforcement, government agency, employer, school, hotel, transportation company, or another third party?
5. What action could reduce the risk of loss without altering the evidence?
6. Does the defense need legal process, a preservation request, consent, discovery, a subpoena, a court order, or technical assistance?
7. What is the earliest known or suspected deadline?
8. What evidence should reasonably exist but has not yet been identified, preserved, obtained, or produced?

Think in time windows

Do not ask only what happened at the exact moment of the alleged event. Identify a reasonable period before, during, and after the event. Digital evidence often establishes travel, preparation, absence, communications, device use, or later conduct outside the narrow event window.

2. What Makes Digital Evidence Time-Sensitive?

Digital evidence is time-sensitive when delay can reduce the amount, quality, availability, context, or reliability of the evidence. The risk is not limited to formal retention periods.

Risk mechanism	Common examples	Why it matters
Automatic overwrite	DVR/NVR video, body camera systems, logs, rolling buffers, network equipment, vehicle systems, some business systems	Old data is replaced by new data as storage fills.
User or account deletion	Messages, posts, cloud files, photos, email, app data	A user, administrator, or account process can delete or alter data.
Disappearing/ephemeral content	Stories, disappearing messages, temporary media, expiring links	The platform or application is designed to remove content.
Device change	Phone reset, replacement, OS update, app update, battery failure, damage	The device state can change and previously accessible artifacts may disappear.
Remote access or synchronization	Cloud accounts, phones, computers, tablets, connected devices	Another device or account action may delete, sync, revoke, lock, or alter data.
Retention/policy expiration	Providers, businesses, government systems, commercial platforms	Stored records may be deleted according to policy or system design.
Log rotation	Routers, servers, access systems, apps, enterprise systems	Older events are automatically purged as new events are recorded.
Loss of context	Video clips, screenshots, exports, forwarded media	The selected item survives but surrounding records, metadata, or original files are lost.
Tool/technology change	Locked devices, unsupported phones, encrypted apps, damaged storage	A current extraction may be limited; future tools may recover more, but continued device use can also destroy recoverable data.

3. Assign an Urgency Level

Urgency is based on the chance of loss, not on how important the evidence appears at first glance. A source can be highly probative and still stable; another source may be uncertain but require immediate action because it can disappear.

Level	Meaning	Examples
URGENT	Act now / same-day attention	Known or likely imminent overwrite; disappearing content; active device at risk of remote change; rapidly changing system; evidence owner preparing to replace/reset device; known short deadline.
HIGH	Prompt action	Meaningful but not clearly imminent loss risk; third-party records with unknown retention; provider/platform records; business video; account logs; vehicle or access-control data.
NORMAL	Track and schedule	Stable evidence already forensically acquired, preserved, or securely held; still verify completeness and underlying source data.

When uncertain, move the source up

Unknown retention or unknown system behavior should not be treated as stable. Confirm current information with the custodian, provider, applicable policy, or technical resource.

4. The Seven Questions to Ask About Every Digital Source

1. What is the source? Identify the actual device, account, system, database, camera, provider record, file, or forensic source—not just a report or screenshot.

2. Who controls it? Identify the current custodian and anyone else who can alter, delete, revoke, reset, or replace it.

3. What period matters? Record the date, time, timezone, and a reasonable before/during/after window.

4. What can it contain? Identify the categories of data that could corroborate, contradict, locate, identify, authenticate, or lead to another source.

5. How can it be lost? Retention, overwrite, deletion, reset, remote access, sync, replacement, damage, log rotation, legal-process delay, or loss of credentials.

6. What action is needed now? Preserve, document, obtain legal process, request discovery, secure the device, contact the custodian, or obtain technical assistance.

7. What proves the source is complete? Ask for native/original data, metadata, logs, audit records, system information, extraction type, date range, and any indication that data was unavailable or not collected.

5. Source Evidence, Forensic Output, and a Summary Are Not the Same Thing

A recurring discovery problem is treating a report, spreadsheet, screenshot, map, or exhibit as though it is the underlying evidence. Investigators should identify the original source and determine whether the defense has it.

Layer	Examples	Investigator question
Source evidence	Phone, computer, forensic image, native file, extraction database, provider return, DVR export, account archive, original recording	The material from which the analysis originates.
Forensic output	Tool report, parsed database, export, bookmark set, map, timeline, log, examiner worksheet	May depend on tool version, settings, filters, parsing, and examiner choices.
Summary/presentation	Narrative report, selected messages, screenshots, clip, spreadsheet, chart, presentation map	May omit context, excluded data, limitations, failed collection attempts, or alternative interpretations.

Baseline question

For every digital exhibit or report, ask: What is the underlying source, was it preserved, what method was used to obtain it, and does the defense have the source material needed to independently evaluate it?

6. Source-Specific Technical Guide

Use the following sections with the source categories on the assessment form and case assessment checklist. The objective is not to turn the investigator into a forensic examiner. It is to make sure the right questions are asked before evidence disappears.

A. Surveillance and Recorded Video

Potential sources include business cameras, residential cameras, doorbells, apartment systems, government cameras, transit systems, schools, body-worn and dashboard cameras, jail video, venue systems, vehicle cameras, rideshare or delivery video, and cloud-based security systems.

- Identify every camera that could cover the approach, departure, parking area, adjacent street, entrance, hallway, elevator, or nearby route—not only the camera pointed directly at the scene.
- Identify the controller and the recording system: local DVR/NVR, memory card, cloud service, central security office, law-enforcement system, or third-party monitoring company.
- Ask the actual retention/overwrite period for that system and camera. Policies and real storage behavior may differ.
- Record the system clock shown on the recording and compare it with a known accurate time when possible. Do not assume the displayed timestamp is correct.
- Request the native/original-quality export when possible, with surrounding footage, metadata, audit information, and any proprietary player required to view it.
- Preserve a reasonable period before and after the event. Motion-triggered systems may have gaps; note whether recording was continuous or event-based.
- Document camera location, field of view, obstructions, lighting, frame rate/quality if known, and whether a clip is a copy, transcode, screen recording, or social-media repost.

> **Do not rely on a phone video of a monitor**
>
> A phone-recorded playback or screenshot may be useful as an emergency reference, but it is not a substitute for the native recording. Keep pursuing the original source and document if it is no longer available.

B. Mobile Devices

Phones and tablets can contain communications, location artifacts, photographs, videos, app data, browser activity, account tokens, device history, paired-device information, and cloud synchronization. They are also easy to alter unintentionally.

- Record make, model, visible condition, screen state, power state, battery condition, SIM/eSIM information if known, phone number, device identifiers available without manipulating the device, and who currently controls it.
- Do not browse through apps, open messages, change settings, update the operating system, reset the device, remove accounts, guess passcodes, or connect the device to a computer unless directed by trained personnel.
- Do not change power or network state simply because a generic rule says to turn a device on, off, or place it in airplane mode. The correct action depends on device state, encryption, lock status, remote-access risk, and available expertise.

- Identify paired devices and linked accounts: smartwatch, tablet, laptop, vehicle, cloud backup, email, messaging desktop client, photo synchronization, and other devices that may contain related data.
- If the device is locked, damaged, unstable, recently reset, subject to remote wipe, or important deleted data may exist, get qualified forensic assistance promptly.

Understanding Mobile Extraction Levels

The phrase “phone extraction” does not mean that everything on the phone was obtained. Different acquisition methods can produce dramatically different data. Tool terminology varies, and the most complete method available depends on the exact device, operating-system version, security state, and forensic tool.

Acquisition type	What it generally means	Investigator concern
Manual / screen review	Examiner views information on the device and records or captures selected content.	Fast but limited; changes can occur; hidden, deleted, database, and system artifacts may be missed.
Logical / backup-style acquisition	Obtains data exposed through supported device services or backups.	May capture common user data but can omit protected app data, system databases, deleted artifacts, or inaccessible files.
File-system acquisition	Obtains files and directories available through a forensic method.	Often provides more application and system data than logical acquisition.
Full file-system acquisition	Broader access to protected file-system areas when supported.	Can materially expand app databases, logs, and system artifacts; availability varies by device and OS.
Physical / low-level acquisition	Attempts to acquire storage at a lower level where technically possible.	Modern encryption often limits usefulness or availability; terminology can be misleading if the examiner does not explain the method.
Cloud / account acquisition	Obtains data from synchronized accounts or cloud services rather than only the handset.	Can reveal backups, synchronized content, account history, or data absent from the local device; scope depends on credentials, tokens, provider behavior, and legal authority.

> **Important: extraction capability changes**
> A failed, partial, logical-only, or older extraction should not automatically be treated as the final word. Commercial tools, device support, exploit methods, and advanced unlocking capabilities change rapidly. Preserve the original device and acquisition files so a later, more complete examination remains possible.

- Ask the examiner to identify the tool and version, acquisition method, device/OS version, whether the device was locked or unlocked, whether the extraction was complete, what failed, what categories were unavailable, and whether a later re-extraction could produce more.
- Ask for the underlying extraction/source data, not only a PDF report or selected messages. Parsing and reporting tools can change what is visible.

C. Cellular-Provider Records and Cell-Site Evidence

Cellular-provider evidence is not one record type. Investigators should identify the provider for the relevant historical date and determine which categories could exist. A current carrier may be different from the carrier that handled the number during the event.

Record category	What it may contain	Do not assume
Subscriber/account	Subscriber name, account identifiers, billing or service details, activation information	Links a number/account to a subscriber or service period; does not establish who physically used the phone at a particular moment.

Record category	What it may contain	Do not assume
Call/text detail	Incoming/outgoing event records, timestamps, numbers, duration, message event records where retained	Usually metadata, not the content of ordinary SMS messages; provider formats vary.
Data/session records	Network data sessions, IP assignments, session times, network elements where retained	Can show device/network activity and may include cell-site associations depending on the provider and record type.
Historical cell-site / sector	Serving cell-site and sector information associated with recorded network events	Shows network association, not a precise GPS point. Interpretation requires provider-specific and RF context.
Tower/sector reference data	Site addresses/coordinates, sector identifiers, azimuth/orientation, technical reference information	Needed to interpret cell-site identifiers and maps; reference data should match the relevant historical period when possible.
Advanced/network-based location	Provider-generated location estimates or network location records beyond ordinary historical cell-site records, when available	May be more precise than traditional CSLI but requires careful interpretation of method, accuracy, and time.

- Identify the exact phone number, provider, account, device identifiers if known, and the relevant date/time range.
- Request or preserve each needed category specifically. A generic request for “phone records” may not capture all available categories.
- Document the provider response, date range, record type, missing intervals, unavailable categories, and any preservation confirmation.
- Obtain underlying provider records and supporting tower/sector information. A map or analyst chart is a presentation, not the source evidence.
- Check timezone conventions, timestamp format, daylight-saving issues, sector identifiers, historical tower changes, and provider-specific terminology before drawing timeline conclusions.

Cell-site is not GPS

Historical cell-site evidence generally reflects the network connection recorded for an event. It should not be described as placing a phone at an exact address. Mapping, RF coverage, tower selection, network design, load, terrain, and the underlying record type may matter. Seek qualified assistance for material location conclusions.

D. Cloud Accounts, Email, Backups, and Stored Content

- Identify the provider, account identifier, username/email/phone number, linked devices, recovery accounts, and whether another person can access or administer the account.
- Potential evidence includes backups, synchronized photos/videos, documents, email, deleted/recently deleted material, account activity, login history, device lists, IP records, application backups, file versions, and sharing information.
- Preserve account data and the physical devices separately. A cloud preservation does not preserve everything that may exist only on the device, and preserving the device does not preserve every cloud record.
- Do not assume current cloud contents are identical to what existed at the relevant time. Synchronization, deletion, versioning, and account settings matter.
- Document account status, recovery methods, storage settings, linked devices, and whether data is locally stored, cloud-only, or synchronized.

E. Social Media and Messaging Applications

- Identify the platform, profile/account identifier, visible profile URL/address, username history if known, linked phone/email, and devices used to access it.
- Potential evidence includes public posts, private messages, group chats, reactions, edits, deleted content, disappearing media, stories, login/activity records, linked devices, backups, attachments, metadata, and account connections.
- Capture enough context to show the conversation, sender/recipient identity, timestamps, preceding/following messages, group membership, and how the content was located.
- A screenshot is a lead and sometimes an emergency preservation method, but it may omit metadata, edited/deleted history, attachments, message identifiers, or context. Pursue native/platform/device records when material.
- Consider linked desktop/web clients, tablets, cloud backups, notification records, downloaded media, and recipient devices as independent sources.
- Disappearing-message settings and retention can change by conversation or user. Treat unknown behavior as time-sensitive.

F. Location and Movement Evidence

Location evidence can come from many unrelated systems. Never assume that one missing source means no location evidence exists.

Source family	Possible evidence
Device/app	Map/navigation history, app location records, photo/video metadata, device system artifacts, fitness or travel apps
Cellular provider	Historical cell-site, data sessions, network-based location records where available
Vehicle	Navigation destinations, infotainment, telematics, paired-phone records, vehicle cameras, tolling, event systems
Commercial/transport	Rideshare, delivery, transit, toll, parking, rental vehicle, airline, lodging
Network/proximity	Wi-Fi association, router/access-point logs, Bluetooth devices, access-control systems
Public/private sensors	ALPR/LPR, traffic cameras, building cameras, doorbell cameras, smart-home systems

- Build a movement timeline using independent sources. One source may provide a location; another may provide time, direction, vehicle, device presence, or corroboration.
- Ask whether the data is a measured GPS coordinate, a network estimate, a cell-site association, a user-entered destination, a cached location, or a business transaction. These are not equivalent.
- Preserve provider, device, app, vehicle, and third-party sources separately.
- For mapping, RF, accuracy, geofence, or provider-location interpretation, obtain qualified assistance.

G. License-Plate Reader (LPR/ALPR) and Roadway Data

- Identify whether the system is law-enforcement, municipal, tolling, parking, commercial, private, or vendor-hosted.
- Potential records include plate reads, vehicle images, camera location, direction, timestamp, confidence or read information, hot-list alert data, query/audit logs, and system metadata.
- Retention can be policy- and system-specific. If the system is known or likely, act promptly and verify current retention directly.
- Preserve a reasonable window and nearby cameras/locations, not only the exact plate read relied upon by one party.

- A “no hit” does not necessarily establish that a vehicle did not pass. Coverage, camera operation, image quality, plate visibility, query settings, retention, and system participation can affect results.

H. Vehicles, Wearables, and Connected Devices

- Vehicles may contain infotainment history, paired phones, call/contact data, navigation destinations, telematics, diagnostic/event records, camera data, key/fob events, and cloud-connected manufacturer data.
- Wearables may contain activity, steps, workouts, heart-rate/activity timestamps, location, notifications, messages, alarms, and paired-phone information, depending on device and settings.
- Connected-home sources can include door locks, alarms, cameras, speakers, thermostats, lighting, garage systems, access logs, and account activity.
- Record manufacturer, model, account, serial/device identifiers if readily available, current power/connection state, paired devices, and recent changes.
- Avoid unnecessary use. Vehicle and IoT acquisitions can be specialized; preserve related cloud accounts and obtain technical assistance before examination when needed.

I. Law-Enforcement and Government-Held Digital Evidence

Government-held evidence can itself be time-sensitive, and the defense should evaluate both what was collected and what reasonably should have been collected.

Category	Examples
Recorded media	Body camera, dash camera, interview room, jail, pole camera, drone, surveillance, RTCC feeds
Dispatch/operations	911 audio, CAD/dispatch, radio, AVL/GPS, incident-management systems
Location/vehicle	LPR/ALPR, traffic systems, vehicle location, agency GPS
Forensic/device	Seized device, forensic image, extraction, tool report, examiner notes, failed attempts, passwords/credentials obtained
Provider/platform	Search-warrant returns, carrier records, cloud returns, social-media returns, preservation responses
Analytical systems	Timelines, maps, link analysis, investigative databases, real-time crime-center products

- Identify participating agencies, units, task forces, analysts, forensic examiners, and outside vendors.
- Ask what systems and tools were used, what date ranges were queried, what filters were applied, what failed, and what data was excluded or unavailable.
- Request source files, native media, metadata, forensic images/extractions, examiner notes, logs, audit history, tool/version information, and provider returns where material.
- Compare what law enforcement collected with what should reasonably exist. Missing underlying evidence, incomplete date ranges, or a report without source data should be documented and followed up.

J. Computers, Removable Media, Networks, and Business Systems

- Potential sources include desktops, laptops, servers, external drives, USB devices, memory cards, browser history, documents, databases, downloads, cloud-synced folders, application logs, network shares, email clients, and remote services.

- Network and business systems may contain login logs, DHCP/IP assignments, Wi-Fi association records, VPN logs, badge/access logs, audit trails, POS transactions, inventory, timestamps, and user activity.
- Some logs rotate quickly. Ask the administrator how long each log type is actually retained and whether backups, centralized logging, or archived copies exist.
- Do not casually open files or browse a computer that may become evidence. Access can change timestamps, application state, synchronization, and logs.
- Do not change the power state of an important computer without direction from trained personnel. A running system may contain volatile evidence, while interaction can also change evidence.

K. Audio, Video, Photographs, and Digital Media Files

- Locate the earliest or original source: recording device, camera card, phone, cloud account, newsroom system, social platform, messaging thread, or editing project.
- Request the native file rather than only a streamed, compressed, converted, enhanced, or social-media copy.
- Document the file origin, transfer path, filenames, timestamps, metadata, surrounding files, edits, conversions, enhancements, and who handled it.
- If authenticity, editing, synchronization, deepfake/manipulation, or enhancement is disputed, preserve all available versions and obtain qualified media-forensic assistance.

L. Commercial, Financial, Employment, School, Hotel, and Access Records

Digital evidence often exists in ordinary operational systems that investigators do not initially think of as “forensics.” These sources can be particularly time-sensitive because retention is driven by business operations, not litigation.

System	Potential evidence
Retail / POS	Transactions, receipts, register logs, loyalty accounts, inventory events, cameras, employee logins
Financial / payment	Card transactions, mobile payment events, ATM records, merchant information, account access logs where available
Hotel / lodging	Reservation, key-card/access records, Wi-Fi, parking, cameras, folio/transaction records
Employment	Badge access, time clock, workstation/VPN logs, fleet/GPS, email, scheduling systems, cameras
School / campus	Card access, Wi-Fi, learning systems, cameras, transportation, facility access
Transportation / delivery	Rideshare, delivery, transit cards, tolling, parking, rental systems, fleet telematics

- Ask who administers the system, whether a vendor hosts it, actual retention, timezone, clock synchronization, user permissions, export capability, and whether audit logs exist.
- Preserve both the substantive record and the audit/system context needed to interpret it.

M. Public Web, Online Content, and Open-Source Digital Evidence

- Web pages, livestreams, public posts, marketplace listings, advertisements, online comments, and user profiles can change or disappear without notice.
- Document the URL/address, account/profile name, date/time viewed, how it was located, and enough surrounding context to show what the content represented.
- Capture the content promptly when lawful, but recognize that screenshots may not preserve metadata, source files, edit history, or account records. Pursue the underlying source when material.

- Consider web archives, cached versions, search-engine results, reposts, recipients, downloaded copies, and platform records as separate potential sources.

7. Preservation Is Not Collection

Investigators should treat preservation as a risk-control step and collection as the step that actually obtains the evidence. The appropriate legal process and preservation method vary by source and jurisdiction.

Action	Purpose	Investigator should remember
Preservation	Asks or directs a custodian/provider to keep specified data from being deleted or overwritten, where supported.	Does not automatically disclose the data; may not cover every category; may expire; may require follow-up.
Collection / production	Obtains a copy or forensic acquisition of the evidence through consent, discovery, subpoena, court process, provider process, or technical acquisition.	Must be scoped, documented, and evaluated for completeness.
Forensic preservation/acquisition	Uses trained methods to preserve device/storage data while minimizing alteration and documenting integrity.	Requires appropriate tools, skill, authority, and chain of custody.

Preservation scope matters

Identify the account/device/system, record categories, and date range. A vague preservation request may not preserve every record the defense later realizes it needs. Confirm the recipient, date sent, response, reference number, scope, and follow-up date.

8. Questions to Ask a Custodian or System Administrator

These questions work for businesses, schools, hotels, employers, apartment buildings, transit systems, security companies, and many government systems.

- What exact system contains the data, and is it local, cloud-hosted, or vendor-hosted?
- What is the actual retention or overwrite period for this record type—not just the general policy?
- Does retention vary by camera, device, event type, user, storage capacity, or subscription plan?
- Is the relevant data still present right now?
- Can deletion or overwrite be suspended or the data exported without changing it?
- What is the system timezone, and is its clock synchronized or known to drift?
- What is the native export format, and is a special player/software needed?
- What metadata, audit logs, user logs, or event identifiers exist?
- Are there backups, archives, redundant systems, vendor copies, or related devices?
- Who can modify, delete, or export the data?
- Can the custodian document that a requested record no longer exists, was never retained, or was unavailable?
- Is there a vendor, manufacturer, or technical contact who can explain the system?

9. Build a Digital-Evidence Map Around the Event

A simple way to avoid tunnel vision is to map digital sources around six anchors: people, places, devices, accounts, vehicles, and systems.

Anchor	Prompts
People	Client, complainant, witnesses, third parties, investigators, employees, drivers, account holders
Places	Scene, route, home, work, business, parking, transit, hotel, school, nearby buildings
Devices	Phones, tablets, computers, wearables, cameras, removable media, vehicle systems
Accounts	Email, cloud, social media, messaging, rideshare, delivery, payment, navigation, manufacturer accounts
Vehicles	Client/witness vehicles, rideshare, transit, rentals, fleet, tolling, parking systems
Systems	Cameras, LPR, Wi-Fi, access control, POS, dispatch, RTCC, provider systems, enterprise logs

Use the evidence to find more evidence

Every new digital source should trigger the same loop: add it to the baseline -> assess loss risk -> preserve if needed -> obtain/collect -> triage -> identify new sources -> reassess.

10. Missing Digital Evidence Is an Investigative Issue

The investigator should document evidence that reasonably should exist but is absent from discovery or unavailable to the defense. Absence can be caused by noncollection, failed collection, incomplete production, deletion, overwrite, system limitations, or a decision not to pursue the source.

- Source identified but never requested or collected.
- Law-enforcement report references digital evidence but the underlying file, extraction, return, or recording is missing.
- Relevant date/time range is incomplete.
- Native/source data is missing while only a screenshot, report, clip, or summary was produced.
- Extraction was limited, failed, or used an acquisition method that could not access material categories.
- Provider/business response indicates records were unavailable or outside retention.
- Known device/account/vehicle/camera existed but there is no indication it was assessed.
- Existing evidence points to another source that has not been pursued.

Document unsuccessful attempts

Record when evidence was sought, from whom, what was requested, what response was received, and whether the source was already gone. The history of an unsuccessful preservation or collection effort can itself become important to understanding the case.

11. Evaluating a Law-Enforcement Device Extraction

An investigator does not need to be a forensic examiner to identify whether discovery is sufficient for independent review. Use this screen whenever a police report says a phone or computer was “downloaded,” “dumped,” “extracted,” or “searched.”

- What device was examined, and is the device still preserved?
- Was a forensic image/extraction created, and does the defense have the underlying source data?
- What tool and version were used?
- What acquisition/extraction type was performed?

- Was the device locked or unlocked, and was the acquisition complete?
- What date was the acquisition performed relative to the incident and device seizure?
- Were cloud accounts or backups separately obtained?
- Were deleted data, encrypted app data, file-system artifacts, location artifacts, and system logs available to the method used?
- What failed or was unsupported?
- Were filters, date ranges, search terms, or bookmarks used to create the report provided to the defense?
- Are examiner notes, logs, error messages, screenshots, and tool-generated metadata available?
- Would current tools or a different acquisition method likely provide more data now?

12. When to Get Qualified Assistance

Qualified assistance should be considered early when delay itself can cause loss or when ordinary access could alter the evidence. The investigator's job is to recognize the trigger and frame the question for the specialist.

Trigger	Examples
Device condition	Locked, damaged, unstable, recently reset, remotely accessible, encrypted, unusual hardware, failing storage
Collection method	Specialized tools or authority needed; ordinary use would alter metadata; vehicle/IoT/network acquisition
Mobile extraction	Only logical/manual extraction exists; extraction failed; app data missing; tool support may have changed
Cell-site/location	Mapping, RF coverage, tower/sector interpretation, advanced provider location, timing or accuracy disputes
Media authenticity	Editing, enhancement, synchronization, metadata, manipulation/deepfake, source provenance dispute
Government work	Police examination appears incomplete or cannot be independently evaluated; source data missing
Deleted/encrypted data	Recovery, database analysis, encrypted apps, damaged file systems, low-level acquisition
Complex timelines	Multiple providers, devices, timezones, clocks, data formats, or analytical systems must be reconciled

> **Give the expert a focused assignment**
> Instead of asking "look at the phone," identify the question: Can a more complete extraction be obtained? Does the phone contain location artifacts for the relevant period? Can the original video be authenticated? What does the provider record actually show? What data is missing from the government extraction?

13. What the Investigator Should Document

Good documentation preserves the investigative history and allows another person to understand what was known at each stage.

Field	Record
Source	Specific device/account/system/camera/provider and identifiers
Controller	Person/entity currently possessing or controlling the source
Relevant period	Date/time range and timezone
Risk	Retention, overwrite, deletion, remote access, device change, log rotation, unknown risk

Field	Record
Action	Preservation, contact, legal process, discovery request, collection, expert referral
When/Who	Date and time of action; investigator; recipient; method of contact
Response	Confirmation, tracking/reference number, scope, unavailable records, deadline, follow-up
Condition	Power state, device condition, account state, camera/system status, changes observed
Chain of custody	Who obtained evidence, when, how it was transferred/stored, identifiers/hashes when available
Unresolved issue	What remains unknown, missing, inaccessible, or technically disputed

14. Common Mistakes That Can Destroy or Weaken Digital Evidence

- Waiting for full discovery before identifying time-sensitive third-party evidence.
- Assuming a provider, platform, business, or law-enforcement agency will retain evidence because a case is serious.
- Treating a preservation request as though the evidence has been obtained.
- Requesting only the exact moment of the incident and losing before/after context.
- Taking only a screenshot, selected clip, or report when the native/original evidence still exists.
- Browsing a phone or computer because it is unlocked or accessible.
- Changing power, network, account, sync, or device settings without a device-specific reason and appropriate training.
- Guessing passcodes, repeatedly attempting unlocks, resetting credentials, updating devices, or installing apps/tools.
- Assuming “phone extraction” means a complete extraction.
- Assuming a failed or limited extraction cannot be improved with newer technology.
- Treating a cell-site map as a precise location measurement.
- Failing to identify the historical provider and underlying tower/sector records.
- Accepting a law-enforcement report without asking for the forensic source data and examiner/tool information.
- Failing to document evidence that should exist but is missing or was not preserved.
- Failing to reassess after new evidence identifies another device, account, camera, vehicle, or provider.

15. Investigator Rapid-Reference: What to Do When You Find a New Digital Source

Step	Action	Question
1	IDENTIFY	What exactly is it? Record identifiers and relevant dates.
2	CONTROL	Who has it and who can alter/delete it?
3	RISK	How can it disappear, change, overwrite, or become inaccessible?
4	PRESERVE	What lawful step can reduce the risk of loss now?
5	OBTAIN	What process is needed to actually get the evidence?
6	VERIFY	Did you receive the native/source evidence, full date range, metadata, and supporting records?
7	TRIAGE	What does the initial review show? What is missing? What new source does it identify?
8	ESCALATE	Does the issue require a forensic examiner, cell-site analyst, media expert, legal process, or other specialist?
9	DOCUMENT	Record every action, response, failure, deadline, and unresolved question.

Step	Action	Question
10	REASSESS	Add new sources to the baseline and run the process again.

STOP & ASK

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

16. Plain-Language Glossary

Term	Meaning
Acquisition / extraction	A method used to obtain data from a device, storage medium, or account. Different methods obtain different amounts and types of data.
Artifact	A piece of information created by a device, app, operating system, or service that may show activity or state.
Cloud data	Information stored or synchronized with an online service rather than only on the local device.
CSLI	Cell-site location information: records showing cellular network sites/sectors associated with certain device/network events.
Forensic image	A forensic acquisition of storage or device data made for examination. The exact scope depends on method and technology.
Hash	A computed value used to identify data and support integrity verification. A matching hash strongly indicates the compared digital data is unchanged.
Logical extraction	An acquisition using data exposed through supported interfaces/services; commonly less complete than broader file-system methods.
Metadata	Data about data, such as timestamps, device information, location fields, file properties, message identifiers, or creation/modification information.
Native file	A file in its original or system-generated format rather than a screenshot, transcode, printout, or converted copy.
NVR/DVR	Network/digital video recorder used by surveillance systems. Many systems overwrite older footage automatically.
Preservation	A step intended to reduce deletion or overwrite risk; it is not the same as obtaining the evidence.
Source data	The underlying digital evidence from which a report, export, map, or summary was generated.
Timezone / clock drift	Digital systems may record in local time, UTC, or another convention, and some clocks are inaccurate. Timeline work should verify this.
Volatile data	Information that can disappear when a device is powered off or changes state, such as some memory or active-system data.

17. Closing Action Standard

A complete time-sensitive digital-evidence assessment does not require the investigator to know every forensic technique. It requires a disciplined process: identify broadly, determine who controls the source, recognize how it can be lost, act before the deadline, preserve more than a selected summary when context matters, document every step, and involve qualified assistance when technical interpretation or acquisition exceeds the team's competence.

Final Standard

The investigator should be able to answer four questions for every important digital source: What may exist? Who controls it? When or how can it be lost? What is the next action and deadline?

Use with applicable jurisdiction-specific law, legal process, discovery rules, preservation requirements, provider guidance, forensic protocols, and chain-of-custody procedures. Provider capabilities, retention practices, device support, and forensic-tool capabilities change over time; confirm current information before acting.