Checklist for Preparing for a Computer Forensics Scoping Call

Gather the device details, account owners, access arrangements and deadlines an examiner needs to plan your matter.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/computer-forensics-scoping/

A useful first call establishes the question, the sources that may answer it, the authority to act and the next deadline. Preparing takes a short conversation with the people closest to the matter. Write down what they know, note the devices and accounts involved, and leave each device as it is so the examiner sees it in its current state. Bring that list to the first call and we will set the plan from there.

Define the issue and the immediate decision

Write the event or dispute in a short factual description. Identify what you need the examination to help determine: file movement, account access, deletion, authenticity, chronology or another specific issue. Record the relevant period and the deadline. Separate an allegation from an observed fact. If you have an opposing report or a proposed collection protocol, note its existence and arrange secure sharing rather than pasting it into a public form.

Ask who will use the result and in what form. A preliminary triage discussion, a defined technical examination, a report for counsel and potential testimony are different assignments. Identify the person authorized to agree on scope and cost, and the legal or business owner who can resolve a question during the work.

Identify computers, storage and physical custody

List the computers, servers, virtual machines, external drives and other media that may be relevant. Record known operating systems, asset identifiers, locations, owners and current custodians. State whether each item is company supplied or personally owned, and whether it is currently running, stored, damaged or in another party's possession. Leave each device in its current power state while you build the list.

Document relevant handling already performed: use after the event, attempted recovery, copying, resets, repairs, encryption changes or an earlier collection. Name the person who can explain each action. If a device is about to be reassigned, wiped or shipped, make that timing clear on the call. A prompt preservation decision may be more urgent than a detailed examination plan.

Map email, collaboration and cloud records

Identify the actual email service, such as Microsoft 365, Google Workspace or another provider, and any reseller relationship. List relevant accounts, shared mailboxes, cloud drives and collaboration spaces. Ask whether an archive, retention policy, legal hold or backup exists and who can demonstrate its coverage. Record each control separately, since each one covers its own set of records.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Record who has administrative access and what logs may still be available. Include outside IT providers and the owner who can authorize their work. If records have already been exported, note the source, dates, method and known filters. A screenshot or forwarded message helps explain the issue, and the examiner traces it back to its native source.

Separate mobile ownership from account registration

List relevant phones and tablets separately from computers. Ask whether each is company owned, personally owned or managed through a bring your own device arrangement. Identify the person or organization controlling the Apple, Google or Samsung account associated with the device. Ownership of the handset, account registration, unlock access and authority to collect are separate facts.

Ask whether mobile device management is in place, whether a work profile is used and whether any wipe, retirement or account removal action is pending. Record who can arrange authorized access and who approves handling, so the examiner can select the collection method.

Confirm encryption and access arrangements safely

Ask whether the computer uses BitLocker, FileVault or another encryption mechanism. Record whether an authorized recovery method is available and who controls it. The examiner arranges a secure handoff for the key itself. Ask an administrator to confirm the recovery record for each relevant device.

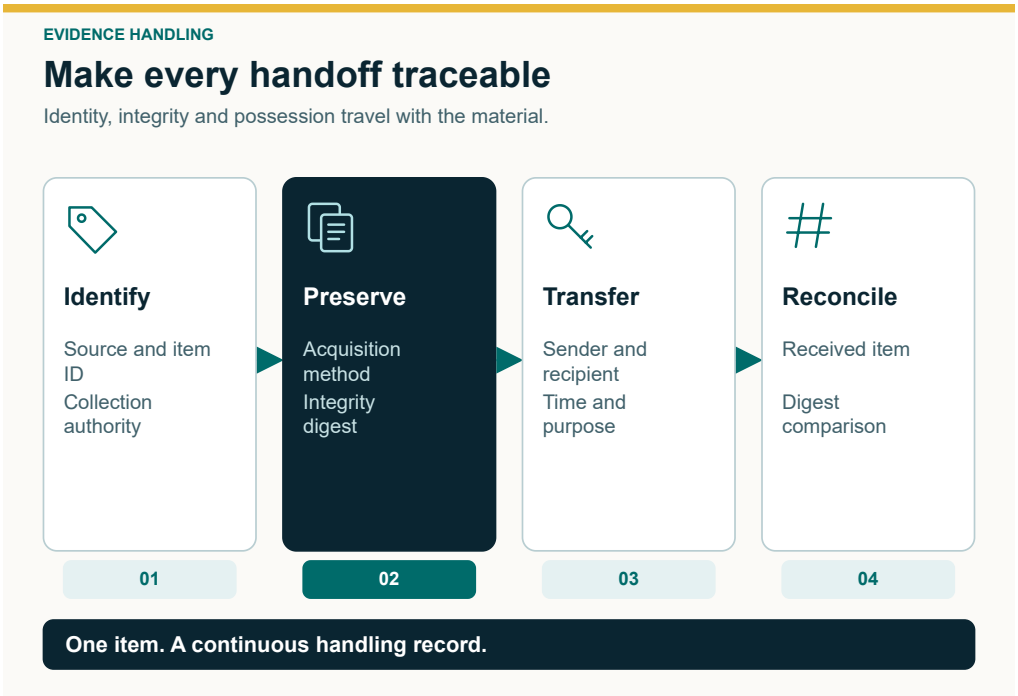
Identify the credentials, permissions or provider assistance the collection will use, and note any personal information, protected records or unrelated data that call for special handling. With the scope of access agreed with counsel, the examiner selects the acquisition methods that fit it.

Prepare the source and exception register

Use one row per source with the following fields: source description, owner, custodian, location, relevant period, availability, preservation risk and person who can confirm the answer. Mark unknown information plainly. Add a short handling history and the date each answer was confirmed. Keep the completed register in the location the business approves.

Before the call, identify the three most urgent decisions: preserving an expiring source, obtaining authority or coordinating access. Have the relevant IT or legal owner available if possible. Ask the examiner what to preserve now, what to leave as it is, which secure transfer method to use and what goes into a written scope. A useful scoping call ends with clear next steps, and you can book it at (212) 561-5860 or through the free consultation.

© 2026 Global Digital Forensics, Inc. All rights reserved.



Each source, collection, transfer and analysis step is recorded so the examiner can account for the evidence.

Information Gathering Q&A Checklist

Use this Q&A with the people who own the systems and the relevant legal or business decisions. Mark unknown or not applicable answers explicitly. Record an owner, a confirming source and the date.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

Who is directing the matter and who can authorize technical access?

Identify directing counsel, the business decision maker, the IT security owner and any outside administrator. Record the immediate deadline, relevant period and known preservation risk. Record who authorizes the examination scope for each device and account, which can differ from who holds the device or administers the account.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Who provides the email service and who administers it?

Identify Microsoft 365, Google Workspace, an internal Exchange environment, a hosted service or a combination. Record the tenant or organization reference, relevant domains, mailbox owners, aliases, shared mailboxes and the MSP or administrator responsible. Identify available preservation and export permissions and any licensing question that needs confirmation.

Answer:

Owner, source, date and open questions:

Does the company have archiving, backups or preservation holds in place?

Name each service and distinguish an archive or journal from a backup, a retention policy and a matter specific hold. Identify what each covers, the available dates, deletion or rotation rules and who can export or restore records. Record whether preservation has actually been verified, rather than treating the existence of a subscription as proof of coverage.

Answer:

Owner, source, date and open questions:

Does the company supply the computers or do employees use their own?

Record company owned, personally owned, leased and shared equipment separately. Identify the assigned user, operating system, asset or serial reference and present location. Note any employee owned computer used for business and the applicable access agreement. Record permission to examine personal material separately from company ownership.

Answer:

Owner, source, date and open questions:

Are mobile devices company owned, employee owned or a mixed arrangement?

Identify the phone or tablet, assigned user, model and operating system where known, and who currently holds it. Distinguish the owner of the handset from the owner of the cellular service account. Record whether work data is separated into a managed profile and whether a replacement, return or wipe is already scheduled.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Whose Apple, Google or Samsung account is registered or signed in on each phone?

Record each relevant account as personal, company controlled or unknown, and identify who can lawfully arrange access. For Apple devices, note any organization enrollment and known Activation Lock status separately from the signed in Apple Account. For Android devices, distinguish personal and work profiles and note relevant Google and Samsung accounts separately. Answer from what is visible now, leaving each account signed in as it is. [Apple guidance on Activation Lock and device management; Android Enterprise guidance on work profiles]

Answer:

Owner, source, date and open questions:

Does the company use MDM and what does it actually manage on these devices?

Name the management service, administrator and enrollment mode, including supervision or work profile details where applicable. Record the last known device contact and any pending retire, lock or wipe command. A device listed in a management console can also hold personal applications, messages or backups, and the examiner looks for them on the device itself. Preserve the management record as it stands.

Answer:

Owner, source, date and open questions:

Can the company recover the BitLocker or other encryption keys for each relevant computer?

Ask whether recovery material is actually available for the identified device and drive, where it is escrowed and who has authorized retrieval permission. Possible locations include Microsoft Entra ID, Active Directory or another approved store. Note FileVault or other encryption separately. Confirm key availability for each device and record where the key is held. [Microsoft BitLocker recovery overview]

Answer:

Owner, source, date and open questions:

Who controls identity, administrator access and multifactor authentication?

Identify the identity provider, relevant privileged accounts, outside administrator and person who can approve an export or collection. Note access dependencies such as an unavailable administrator or authentication device. Identify shared or delegated access so the examiner can attribute account activity to the right individual.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Which cloud storage, collaboration and messaging services contain relevant work?

Identify shared drives, Teams, SharePoint, OneDrive, Slack, Google Chat and other platforms actually used for the relevant work. Note external ownership, linked documents, personal accounts used for business and any unsupported or unavailable source. List linked files and separate conversations alongside the mailbox so each one is collected in its own right.

Answer:

Owner, source, date and open questions:

What activity logs and endpoint records are available now?

Ask the responsible administrator which email, identity, endpoint, cloud sharing, USB, security and data protection records exist for the relevant period. Record actual date coverage, export permissions, known gaps and the next expiration or rotation point.

Answer:

Owner, source, date and open questions:

What has already changed on the devices or accounts?

Record password resets, access restrictions, account deletions, mailbox conversions, software installations, cleanup activity, repairs, cloud sync changes and any device reset or wipe. Identify who acted, when and why. Include informal handling or earlier collections so the examiner can distinguish relevant historical activity from changes made during the response.

Answer:

Owner, source, date and open questions:

What has happened to the device or account since the event?

Record use, repairs, exports, resets and the people who can confirm them.

Answer:

Owner, source, date and open questions:

Which source may change or expire before the next decision?

Identify the preservation risk and the owner who can address it.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Primary sources and further reading

Sources checked November 3, 2026.

1. Microsoft BitLocker recovery overview https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview
2. Apple guidance on Activation Lock and device management https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web
3. Android Enterprise guidance on work profiles https://support.google.com/work/android/answer/6191949?hl=en

Get a Free Consultation

The first call is a free consultation with a senior examiner. We review the matter, the evidence and the deadline, and outline the collection and analysis it needs. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.