Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/digital-forensics-faq/

PLANNING THE ENGAGEMENT

Scoping Digital Forensics to Control Cost and Time

An examination scoped to the first legal question delivers facts that direct the next step, quickly and in proportion to the dispute. Define the question and the sources first and collect second, then call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why a Focused Scope Delivers Critical Answers Sooner

When an internal compliance issue, trade secret dispute or regulatory inquiry arises across a multi office corporation, a focused technical scope moves faster and costs less than imaging fifty employee laptops and loading terabytes of server data into a review queue. Digital forensics is most powerful when it is scoped around the specific factual questions that the legal department, internal audit or the board of directors must answer first.

Matching the Legal Question to the Highest Value Artifact Sources

Working directly under the direction of retained attorneys, internal auditors and corporate IT security leaders, Global Digital Forensics structures enterprise engagements in disciplined, phased milestones. In phase one, we map the timeline of the disputed event against the exact devices and cloud tenants that record that behavior, often starting with rapid cloud audit log preservation and targeted forensic imaging of the two or three primary custodian laptops and smartphones. By analyzing high speed operating system artifacts, USB connection histories and cloud download telemetry first, we frequently deliver decisive answers within days, allowing the client to expand or narrow the scope based on hard technical facts rather than guesswork.

What a Scoped Examination Can Answer

A scoped examination answers factual questions about what happened on identified systems during an identified period: which files were accessed, copied or deleted, which accounts signed in from where, which messages were sent and what they contained, which devices were connected, what software ran. Those answers are drawn from artifacts whose scope we state, and they are the facts needed before deciding whether to expand, settle, report or litigate. The scope is a set of questions, and the first phase answers the ones that most change the next decision.

Intent and motive are read from the record together with interviews, documents and context, and counsel weighs them. Deleted data is recovered where it remains on the media, and for overwritten data the examiner turns to backups, synced copies and recipients. Tying an account to the person behind it combines the

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

account record with corroborating evidence. The scoping conversation also confirms which logs were enabled and within retention, so the case is built on the sources that exist and plans around the rest. We describe at the scoping stage which sources the examiner will read, because that shapes the questions worth asking.

A forensic examination plays a defined part in the whole matter. It supplies the technical facts that the internal investigation led by counsel or audit relies on, in a form that can be tested and, if needed, presented. Our digital forensics FAQ in the resources library answers the common definitional questions, and the process guide walks through the stages from first call to report so the people directing the matter know what each stage produces. Setting that expectation early keeps the engagement aligned with the decision it serves.

Proportionality Under Rule 26(b)(1) as a Scoping Tool

Federal discovery is bounded by proportionality. Rule 26(b)(1) limits discovery to matter “proportional to the needs of the case,” considering the importance of the issues, the amount in controversy, the parties' access to information, their resources, the importance of the discovery in resolving the issues and whether the burden or expense outweighs the likely benefit (Federal Rule of Civil Procedure 26). The same factors are a sound guide to scoping a forensic examination even when no court is involved, because they force the question of which sources are likely to resolve the issue and at what cost.

In practice that means ranking sources by how directly they bear on the question. For a suspected data exfiltration, the departing employee's laptop image, the cloud audit log of downloads and sharing, and the USB and personal email records come first, and the file server and the colleagues' mailboxes come later when the first phase points there. For a suspected financial manipulation, the accounting system's audit trail and the controller's mailbox come first. The order is driven by the question, and the first phase is designed either to be decisive or to redirect the work toward the sources that will be.

Proportionality also protects the client from the opposing side's demands. When an adversary insists on imaging every device in a department, a written scope that explains which sources were examined and why, and what the examination of those sources showed, is the basis for resisting the demand or negotiating it down under Rule 26. Our audit and discovery preparation guide describes how organizations prepare that record before a dispute, and the preparation pays for itself the first time a disproportionate request arrives. A documented scope is a concrete answer to that demand.

Phases of an Enterprise Engagement and the Decisions Between Them

The first phase is triage and preservation. We identify the systems and accounts most likely to hold the answer, preserve them in a defensible manner, and hold everything else in place for later collection if the work calls for it. Preservation is broad and collection is narrow, which keeps the option to expand while the budget goes to the sources that matter first. At the end of this phase the client has an inventory of what exists, what has been preserved and what is at risk, and can decide on the first analytical question with that inventory in hand.

The second phase is targeted analysis. The preserved sources are examined against the first question, and the findings are reported in a short written update that states what was found, what the artifacts support, what remains under examination and which source the examiner would read next. This is a decision point. Counsel

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

may conclude the matter is resolved, expand to the sources the findings point toward, or change the question. Because each expansion is a decision rather than a default, the engagement stays proportional to what is learned, and the budget follows the facts.

The third phase is the deliverable the matter needs, which may be a memorandum for the board, a report for a regulator, a declaration in support of a motion or trial testimony. The form determines how the file has been kept from the start, which is why we ask about the likely deliverable in the first conversation. Our computer forensics and expert witness pages describe the two ends of that range, and the massive data discovery case study describes a matter in which raw supplied data was organized into correlated timelines so the legal team could work from it.

What Drives Cost and Timing in an Enterprise Matter

Cost in a forensic engagement is driven by volume, variety and the form of the deliverable. Volume is the number of custodians, devices and accounts and the size of each. Variety is the mix of platforms: a Windows laptop and a Microsoft 365 mailbox are routine, while a mix of macOS, Linux servers, mobile devices, Google Workspace, Slack and a line of business application each require their own methods. The deliverable matters because a memorandum for internal audit and a Rule 26 report with testimony require different levels of documentation, validation and preparation.

Timing is driven by access and by the providers. Encrypted devices require recovery keys from the management console. Cloud exports are rate limited by the provider and large mailboxes take time to export regardless of the examiner's urgency. Custodians in several time zones and administrators who must be scheduled add days. And retention windows set the deadline for preservation whether or not analysis is ready to begin. We lay those drivers out in the written proposal so you can see why a phase takes the time it does and where the schedule can be compressed.

The way to control both is the phased structure described above and a clear point of contact on the client side who can authorize access, schedule administrators and relay decisions. Organizations that have prepared through a forensic readiness plan or an incident response retainer start with the inventory already built and the access already arranged, which shortens the first phase considerably. Either way, the initial consultation is free and produces a written proposal before any analysis begins. Organizations starting fresh move quickly too, with the first phase building the inventory a readiness plan would have provided, as the written proposal sets out.

What to Bring to Your Initial Scoping Call

Before calling our team, jot down the core factual question you need answered, the date range of the disputed activity, the types of laptops, phones and cloud platforms involved, and any upcoming court or regulatory deadlines. Our step by step guide to the digital forensics process shows how a matter moves from that first call to a report or testimony.

Call Global Digital Forensics 24/7 at (800) 868-8189 for a free initial scoping consultation with a senior forensic examiner.

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

Matching the Legal Question to the First Source to Examine

A scoped first phase is designed either to be decisive or to redirect the work. This table pairs a common opening question with the sources that bear on it most directly, so legal and internal audit can see what a proportional first phase would preserve and examine. Read it as the ranking proportionality under Rule 26(b)(1) would suggest. The later sources are held in place and collected when the first phase points toward them.

Common opening questions and the highest value sources a first phase examines for each.

Opening question	First sources to examine	Held for a later phase
Did a departing employee take data	Custodian laptop image, cloud download log, USB and webmail records	File server and colleagues' mailboxes
Was an account compromised	Sign in logs, audit log, inbox rules and consents	Endpoint images of secondary hosts
Was a document altered	The file metadata, the master file table, the application records	Backup copies and recipient versions
Was financial data manipulated	The accounting system audit trail and the controller mailbox	The wider transaction archive
Where did an intruder enter	Authentication logs and the mail or web gateway records	Lateral hosts the first phase identifies
What did a phone record	A full file system extraction of the device	Carrier records and synced devices

The massive data discovery case study describes two terabytes of raw data organized into correlated timelines so the case could proceed from hard facts, the phased and scoped approach this guide recommends.

How to Begin and What Happens on the First Call

Our Preservation Checklist: Quarantine the Device, Hold the Account sets out the items to secure in the order they expire. Have the core factual question, the date range, the custodians and the devices, accounts and platforms they used, any deadlines from a court, regulator or board, what has already been preserved or changed and who holds administrative access. The examiner asks what decision the answer will inform, what the sources are likely to show, whether a hold has issued, who directs the matter and what form the deliverable must take. The conversation produces a written proposal that names the sources to preserve immediately, the first analytical phase and its question, the decision points that follow, the deliverable and the cost and timing drivers specific to your environment. The initial consultation is free. Call (800) 868-8189 at any hour, or request a call through the contact form.

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

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics.

Authorities cited in this guide: Federal Rule of Civil Procedure 26. Supplies the proportionality language in 26(b)(1) quoted in the guide, current text at Cornell LII. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Establishes the collection, examination, analysis and reporting phases the engagement structure follows, final publication August 2006. NIST SP 800-101 Revision 1, Guidelines on Mobile Device Forensics. Establishes the mobile acquisition methods referenced when phones are among the sources in scope, Revision 1 published May 2014. Federal Rule of Civil Procedure 37(e). Sets the reasonable steps standard that makes broad preservation and narrow collection the defensible structure, current text at Cornell LII.

FREQUENTLY ASKED

Running the Engagement Day to Day

How much does a digital forensics examination cost?

It depends on the number of custodians, devices and accounts, the mix of platforms, the volume of data, whether logs and devices were preserved before we were called, the number of questions to be answered and the form of the deliverable, from an internal memorandum to a report and testimony. A single device with one question is a small engagement and a multi custodian, multi platform matter with expert testimony is a large one. The initial consultation is free, and the written proposal states the drivers for your matter before analysis begins.

How long does an enterprise forensic engagement take?

Preservation is immediate because retention windows keep running. The first analytical phase is scoped to the question that most changes the next decision and is designed to be short. Overall timing then depends on device encryption and key availability, provider export rate limits, the number of custodians and administrators to be scheduled, the volume of data and the deliverable. We state those drivers in the written proposal and report progress at each decision point so counsel controls the pace.

Do we have to image every computer in the department?

Rarely, and the stronger start is a focused one. Preservation is broad, meaning holds and retention changes that keep evidence in place, while collection and analysis begin with the sources most likely to answer the first question. If the findings point to other custodians, the scope expands by decision rather than by default. A written record of that reasoning also supports resisting a disproportionate demand from an opposing party.

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

Who in our organization should be the point of contact for the examiner?

Someone who can authorize access, schedule administrators and relay counsel's decisions quickly, often a member of the legal department or an internal audit lead, with a named technical contact who holds administrative rights to the systems in scope. The examination should run under the direction of counsel where litigation is possible, and the point of contact arranges secure transfer for evidence and coordinates containment steps with preservation.

Will the findings be usable if the matter goes to court?

The findings are prepared so they can be. Preservation is documented with hashes and custody records, methods are recorded with tool versions and validation, and conclusions are tied to the artifacts that support them, which is the foundation a court expects under the rules of evidence. Whether a particular finding is admitted is the court's decision and counsel's argument. Telling us at the outset that testimony is possible lets us keep the file to that standard from the first day.

Web Addresses for the Sources Cited

1. Federal Rule of Civil Procedure 26: https://www.law.cornell.edu/rules/frcp/rule_26
2. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://csrc.nist.gov/pubs/sp/800/86/final
3. NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics: https://csrc.nist.gov/pubs/sp/800/101/r1/final
4. Federal Rule of Civil Procedure 37(e): https://www.law.cornell.edu/rules/frcp/rule_37

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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