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

ANSWERS FOR ATTORNEYS AND BUSINESS LEADERS

Digital Forensics FAQ for Attorneys and Businesses

When the evidence sits on a phone, in a mailbox or in a departed employee's cloud account, the first questions are practical, can you collect it remotely, can my client keep using the device, what will it cost and how long will it take. Senior examiners answer them below, the way we would on the first call.

What a Digital Forensic Examination Can Establish

Digital forensics preserves and examines the information held on computers, mobile devices, email systems and cloud platforms, then connects it. Global Digital Forensics correlates file activity, messages, sign ins and sharing records to test what actually happened and to explain the evidence behind each conclusion and the scope it covers.

A useful examination begins with a business or legal question, and the devices follow from it. That question governs which sources we collect, which period we examine and what the report must answer. Our computer, email and cloud forensic service brings those sources together so the timeline reflects every relevant source together.

Start with the question your matter has to answer, and tell a senior examiner what it is; the sources and the scope follow from there.

What Happens After You Call Global Digital Forensics

The first conversation is a discussion of the matter: the question, the people and organizations involved, the devices or accounts that may hold the answer and your deadline. From that we propose a scope and a cost, explaining the collection, analysis and reporting options, including the flat rate Core Analysis service when the matter is a departure review. You see the plan before anything is engaged, and the initial consultation is free.

Once engaged, we coordinate access, collect the evidence using documented procedures, verify its integrity with hash values and analyze the relevant activity. You receive a report you can read, the supporting records behind it and whatever expert or discovery assistance the matter needs, from the same examiners who did the work. Global Digital Forensics has worked this way for law firms and businesses since 1992.

Want the plan before you commit to anything? Call (800) 868-8189 and describe the matter; the proposal comes first, and the engagement follows once you have read it.

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

Consult a Senior Examiner on Your Evidence Before Anything Changes

Tell us what happened and which devices or accounts may hold the answer. A senior examiner will explain the collection options and the next step, and the initial consultation is free.

Evidence Preservation and Reporting Built for Scrutiny

Professional collection retains the original messages, attachments, file information and relevant logs together with a record of how each item was handled. The chain of custody identifies the source and every transfer, and integrity checks let anyone who needs to verify the evidence compare it against the hash values recorded at collection.

The report connects each finding to its supporting evidence. A timeline can show a file being created, attached to an email and shared through cloud storage, with every entry traced to its source record. The result is an explanation that works in a client discussion, a discovery conference, a deposition or at trial.

For the technical background on evidence handling, see NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. We fit the examination plan to the evidence that is available and the assignment in front of us. For questions about organizational authority, sources and operations, see the organizational scoping guide.

If the way a finding traces to its source record matters to your case, ask us to walk through the report format before the collection is scoped.

Choose the Service Your Matter Needs

Open the service that matches your source, Microsoft 365, Google Workspace, a mobile device, a departed employee's files or an eDiscovery collection, or read the profiles of the examiners who would handle your matter.

FREQUENTLY ASKED

Ten Answers on Collection, Cost and Testimony

Can you collect evidence remotely, or does someone have to ship us the device?

Often we can collect remotely. When the authorized person has lawful authority and the source is supported, we plan the collection of email, cloud accounts and supported computers and phones with that person, run it over a secure connection and document the method and its scope in the custody record. Some devices and sources call for hands on acquisition, and we tell you which before anything moves.

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

Can my client keep using their phone while you collect it?

In many cases, yes. Our supported remote workflow collects a phone through a link and a computer connection, normally with the client continuing to use the device, and the collection itself can take anywhere from a few minutes to overnight depending on the setup. Get handling instructions from us first for any device that may hold evidence, so ongoing use, deletion or a reset is planned around the collection. The model, the device state, encryption, authority and the question determine the plan.

Can users keep working in their email account during collection?

Routine remote collection of a supported mailbox usually permits continued use. A legal hold, a compromised account, a provider setting or a narrow collection window can shape that answer, so we agree access, preservation and any restrictions for the actual account before the collection begins.

Can you tell whether a departing employee took proprietary information?

An examination looks for the records consistent with access, copying, messaging or sharing: file activity, USB connections, cloud synchronization, email and sharing logs. Tying that activity to one person combines those records with account ownership, retention coverage, access logs and other corroboration, and the report sets out how each attribution was made. For employee exits, executive departures and partner separations, our Core Analysis service preserves the sources and produces an activity timeline for a flat rate within an agreed scope. The report states each finding at the level the record supports.

Can you determine whether an email is authentic or has been altered?

We examine the available original messages, their headers, attachments, mailbox records and the related server and provider logs, and we tell you what those sources support. The strength of the conclusion follows from the sources available and how they corroborate one another. We explain the findings and the support behind each one, and the court decides what the evidence is worth.

How much does a forensic examination cost?

Cost follows the questions you need answered, the number and type of sources, the volume of data and the deliverables you want, and we discuss each of those before engagement so there are no surprises. A focused scope keeps collection and review in proportion. For departures and separations, ask about Core Analysis, which is priced at a flat rate for its agreed scope. The initial consultation is free.

Can you help with an eDiscovery stipulation when the budget is limited?

Yes. We work with retained counsel on the technical collection requirements, keyword and date proposals, processing and production specifications, and we use software GDF owns to keep processing and hosting proportionate for small and midsize matters. Scope, access, review responsibilities and hosting determine the estimate.

What do I actually receive at the end of the examination?

The deliverables we agree at the start, which can include a collection inventory, chain of custody records, an activity timeline in which each entry links to its source record, the relevant native data, a forensic report written in plain English and supporting exhibits. When we are retained as experts, you also receive expert reports, declarations and deposition or trial testimony.

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

Can your experts explain the findings in court?

Yes, when retained and qualified for the assignment. Our examiners have testified in federal and state courts, hold credentials including the CISSP, EnCE, CCE and CHFI, and prepare reports built to withstand cross examination. The court decides qualification, admissibility and weight, and the examiner who did the work is the examiner who explains it.

How do you approach deleted information?

We start with where deleted material and the records around it may still reside. Device state, storage behavior, backups, cloud versions, retention settings and other sources all bear on recovery, and we assess those before choosing a method. We tell you plainly what that assessment finds, and the plan sets out the feasible collection and recovery work and its scope.

Talk Through Your Evidence Question With an Examiner

Find regional collection and engagement information for our sixteen US offices or meet the forensic team. Ask about the collection method and the report format that fit your matter, and bring the question, the sources you know about and the deadline.

Those three things, the question, the sources and the deadline, are all the free first conversation needs.

Call Before Devices Are Reissued or Logs Expire

Our 24/7 hotline is (800) 868-8189. Call to discuss your next step and to arrange secure information sharing.

Web Addresses for the Sources Cited

1. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://csrc.nist.gov/pubs/sp/800/86/final

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.