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

EXECUTIVE GUIDE ON A GUIDE FOR LEGAL TEAMS AND EXECUTIVES

How a Forensic Examination Reaches the Witness Stand

Anyone retaining a forensic examiner benefits from seeing how one works. This guide walks through the five phases of a digital forensic examination, what each one produces and where the decisions that shape the evidence get made.

Written for the attorneys, general counsel and executives who need to understand what a forensic examination involves before they retain one.

A digital forensic examination is a sequence of decisions, each of which shapes what the evidence can later support, made by an examiner prepared to explain every one of them under oath. Global Digital Forensics has run that sequence for law firms and businesses since 1992, on everything from a single laptop to mainframe transaction systems and cloud tenants. The phases below describe how we work and why each one protects the client who retained us.

Phase One Plans Around the Question, the Authority and the Deadline

Every examination begins with four facts: what question the matter needs answered, who has lawful authority to collect the data, which sources could hold the answer and when the answer is due. We sit down with the technical owners and retained counsel to separate preservation, acquisition, processing, analysis and reporting into distinct decisions, because each has its own cost, its own timing and its own clock.

The written plan records the access we are assuming, the data on the shortest retention clocks, the operational constraints of the business and the conditions under which the work would expand. You see the shape of the engagement before any device is touched, which is also where most disputes about scope and proportionality are settled cheaply. For the preservation decisions that matter most early, read our guide to Common Digital Evidence Mistakes.

Phase Two Acquires the Data in a Way That Can Be Explained Later

The right acquisition method depends on the source. A forensic disk image captures the acquired sectors of a drive, a targeted endpoint collection pulls defined artifacts from a running system, and an authorized provider export retrieves what a cloud service makes available. For each we record the device or account identifiers, the condition of the source, the time of collection, the tools and settings, any filters applied and every transfer that follows, and we run integrity checks whose hash values tie every working copy to the data as collected.

We identify, acquire, authenticate, analyze and report on digital devices, electronic media, hard drives and cloud storage. Our examiners document evidence handling and verify acquired data with cryptographic hashes.

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

Choosing the acquisition method comes first. Ask us which method suits your source, then power on the device or run the export.

Phase Three Extracts the Records That Bear on the Dispute

Once the sources are preserved, the examiner identifies the files, messages, application records, logs and structured data inside them that could answer the question. Each source brings its own conditions, including encryption, overwriting, retention settings, hardware damage and formats outside the standard tools. We select and validate methods suited to the actual source, and where a source calls for more than ordinary tools we build custom processing with its assumptions and checks written down so they can be tested.

This is the phase where experience with the specific system pays for itself. An examiner who has worked inside IBM mainframe databases, mobile operating systems and cloud tenants knows where each one keeps its records and how to read the spaces between them, which is why we match the team to the sources before the work starts.

When the source is a mainframe, an unusual platform or a damaged device, call (800) 868-8189 and we will tell you whether we have worked inside it before.

Phase Four Correlates the Sources and Tests the Alternatives

A disputed event is settled by records read together, far more often than by a single timestamp, account name or isolated document. Analysis correlates the relevant sources so that each record is read against the others: the file system against the application logs, the message against the login record, the device against the cloud account. We check time conventions, processing artifacts, missing records and the alternative explanations that the other side will raise, and we corroborate material conclusions wherever the available evidence permits.

Throughout, we keep observed artifacts separate from interpretation. The report states what the data shows, then states what we conclude from it and why, so the reader and the court can see the distance between the two. That discipline prepares each finding for cross examination, and it is why our examiners have testified in federal and state courts.

Ask us to walk you through how a report keeps observed artifacts apart from the conclusions they support; the first consultation is free.

Phase Five Reports the Findings and Explains Them in Testimony

The agreed report can include source inventories, methods, the relevant records, timelines, charts and exhibits. Every finding traces to the underlying data, and material uncertainty is stated plainly, because a report that matches its evidence is one the examiner can stand behind at deposition. We write for the reader who will act on it, whether that is trial counsel, a board or a regulator.

When we are retained for testimony, the examiner who did the work is the one who explains it. We describe the methods and conclusions, counsel addresses the legal use of the findings, and the court decides admissibility and weight. The record we build is one the examiner can defend line by line. Our digital forensics expert witness page describes how testimony engagements are scoped.

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

If testimony is likely, ask now who would do the work and who would take the stand, because at GDF they are the same person.

Choose the Examiner for the Systems in Your Matter

Select a team for the actual systems and questions in the assignment. Ask about the proposed examiner's relevant experience, the access that will be available, the tool support for the devices in question and the deliverables you should expect. Our examiners' credentials, court experience and training are listed on the About page, and the published case studies describe selected work. They describe that work within its published scope, and your matter is assessed on its own systems and facts, which is the standard we would apply to anyone else's expert.

Put those questions to us first: (800) 868-8189 reaches a senior examiner who will answer them for the systems in your matter.

Secure Handling and Documented Methods From the First Call

Before any material moves, we agree secure handling, access restrictions, reporting recipients and retention for the assignment. Commercial and proprietary forensic tools are used alongside documented custom processing, and reproducibility rests on explaining the relevant methods, inputs, settings and validation. Private material travels through the agreed secure channel, and we will set that channel up with you before anything is sent.

Global Digital Forensics has served AmLaw 100 firms and Fortune 1000 companies since 1992, and the initial consultation is free. Bring the question, the deadline and what you know about the sources, and a senior examiner will tell you which phases the matter needs and what each one will produce. Call (800) 868-8189.

Technical reference: NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. The NIST publication addresses integrating forensic techniques into incident response and informs the method for each matter.

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.

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

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.