Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/common-digital-evidence-mistakes/

EXECUTIVE GUIDE ON PRACTICAL GUIDANCE FOR EXECUTIVES AND LEGAL TEAMS

Five Mistakes That Destroy Digital Evidence Before We Arrive

The first few days shape how the evidence reaches the examiner, and the people best placed to protect it are the well meaning people inside the organization. The five decisions that matter most, and how to make each one well.

Written for the executives and lawyers who make the first decisions after a problem surfaces.

Electronic information can decide a matter when it reaches the examiner in a condition that supports conclusions. Its usefulness depends on the question being asked, the lawful authority to collect, the source it came from, the method used to collect it and a clear account of every change and exclusion along the way. In more than three decades of casework at Global Digital Forensics, the same handful of early decisions has shaped the record more than any adversary, and the best time to make them well is before the first file is touched. A matter specific source plan, agreed early, settles most of them.

Making Every Collection a Documented Collection

When something goes wrong, the first instinct is to have someone in IT pull the files. An IT employee can be an appropriate collector when trained, authorized and equipped for the task; what matters is how the work is done and how it is documented. A documented collection keeps the timestamps, message headers, earlier versions, attachments and application context that show how a record was used, all of which opening, printing or resaving a file can alter. Material handled informally often remains usable, and documenting each step keeps the examiner's conclusions broad and gives the other side a clear account of every change.

Record the source account or device, the time of collection, the method, any filters applied and every transfer that followed. Retain original formats where they exist and be ready to explain the integrity checks that were run. If data has already been copied, keep that copy. Preserve it, document the actions taken and let a computer forensics examiner assess what the sources hold and whether a further acquisition would help. The examiner checks each source for recoverable artifacts and reports what the work finds, and counsel evaluates the legal duties and the consequences of any collection issue.

If a copy has already been made, tell a senior examiner exactly what was done as your first step; the free consultation exists for that call.

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

Preserving First, Then Deciding How Far to Analyze

Preservation and examination are different decisions, and making them separately is the most valuable habit on this list. Relevant logs run on retention schedules set outside the legal department, devices are reissued on the IT calendar and cloud content follows license and retention policy, so preservation keeps pace with those clocks. A limited preservation step retains the sources while the parties decide whether a broader analysis is proportionate. Protecting the material now keeps every option open while the question of trial is settled.

Be precise about what a preservation step produces. A forensic disk image preserves the acquired sectors of a drive, and a live system or a cloud export uses its own method with its own scope, so document the data obtained and the collection period for each acquisition. Ask for acquisition, processing, analysis and reporting to be estimated separately. Cost and urgency follow from the actual sources, the access available and the work required.

If logs or devices are due for deletion or reissue this week, call (800) 868-8189 and preserve the sources first; the decision on how far to go follows once they are held.

Choosing a Scope That Tests the Disputed Facts

The right scope includes the sources needed to test the other side's explanation and stays proportionate, keeping cost, delay and privacy exposure in line with the question. Begin with the conduct in question, the period over which it happened and the systems that were involved. A departing employee's messages, file activity and sharing logs each answer a different part of the same question, and a financial dispute may require the structured transaction data together with the software rules that produced it.

Work from an initial source map with agreed custodians and justified date ranges, and state plainly which sources were excluded, how any samples were selected and what would justify expanding the work. Each deliverable is labeled for what it is, so a targeted export reads as a targeted export and a complete device examination as a complete examination. Tool support varies by version, platform and artifact, and UNIX, Mac and mainframe sources in particular deserve a direct question about coverage. Ask the examiner to explain the proposed coverage and how the results will be validated before the work begins.

Ask us for a written source map before any collection begins; the first conversation is free and it is where the map starts.

Issuing Preservation Instructions With an Operational Plan

Counsel issues the preservation instructions, and they take effect when the people who run the systems carry them out. Technical owners need to identify the retention settings, scheduled deletions, device replacements, backup rotations and account lifecycle events that could affect the relevant sources, and someone needs to record what has already happened and who can authorize and implement each action. A hold notice preserves the record once it is translated into system changes.

When a problem is suspected, get source specific handling instructions first, then decide whether to power down, disconnect or reconfigure a device. The right instruction keeps volatile data accessible and operations running, and it covers how the device is used in the meantime, since continued use changes the record too.

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

Life safety and urgent containment always take priority. Keep a log of every response action so that later analysis can separate what the responders did from the activity being examined.

Once the hold notice has gone out, bring the technical owners to a free planning call with an examiner to turn it into system changes.

Selecting an Examiner by Examining the Proposed Work

Ask who will perform the acquisition and the analysis, what relevant experience they bring, which tools and versions they intend to use and how they will check the results that matter. Ask how the examiner's credentials and tools apply to the particular system in front of you, and expect a clear plan for the work, with the courtroom result left to the court. Request a scope that separates collection, processing, interpretation and reporting, with its assumptions and decision points written down.

Agree on the deliverables before the work starts: an acquisition inventory, handling records, the relevant native data, a chronology or report in which each finding traces to its source, and expert assistance if that is retained. The report should set out the scope of the collection and weigh each alternative explanation against the evidence. Our examiners' credentials and court experience are listed on the About page, and the technical file an expert should be ready to defend is described in our guide to preparing the digital expert's file for scrutiny.

On the first call, ask who would perform the acquisition and who would testify, and we name both.

What to Bring to a First Conversation

Prepare the question, the deadline, the sources you know about, the people authorized to grant access and the actions already taken. The goal of that first discussion is a proportionate plan that preserves useful material and produces a result that can be explained to a court, a regulator or a board. Admission and weight are decisions for the court, and the legal scope of the matter belongs with the legal team. Our part is to preserve and explain the technical record they work from. Global Digital Forensics has served AmLaw 100 firms and Fortune 1000 companies since 1992 from sixteen US offices and an international line, and the initial consultation is free. Call (800) 868-8189.

Technical background: NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. The NIST publication covers integrating forensic techniques into incident response. For service and client questions, see the Digital Forensics FAQ, and for how a matter moves from a question to a report, see the digital forensics process.

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.