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

EVIDENCE PRESERVATION

How Legal and IT Teams Stop Spoliation When an Employee Departs

Evidence in a departure or trade secret dispute is best protected inside routine offboarding, before a technician boots the laptop, a script wipes the phone or a license revocation starts a deletion timer. Quarantine the devices and hold the accounts first, and call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Robert Knudsen, Computer forensics and cybersecurity examiner, Global Digital Forensics

Where Offboarding Meets Digital Evidence Inside an Enterprise

In the vast majority of corporate trade secret disputes, employment lawsuits and internal compliance inquiries, the critical moment for digital evidence comes during routine corporate offboarding rather than at the hands of sophisticated hackers. When a key executive or engineer resigns, human resources notifies IT, a helpdesk technician boots up the returned laptop to check its condition or copy desktop folders, and an automated script revokes the user Microsoft 365 license and wipes their corporate iPhone for reassignment. Within forty eight hours of that uncoordinated handoff, thousands of operating system timestamps are altered, solid state garbage collection purges deleted files and the thirty day cloud mailbox deletion timer begins ticking.

Establishing Defensible Preservation Gates Between HR, IT and Legal Counsel

Global Digital Forensics partners with general counsel, outside litigators, internal auditors and IT security leaders to build documented forensic preservation gates into offboarding. Whenever a departing employee worked with sensitive intellectual property, client lists or executive strategy, their returned hardware goes straight into physical quarantine, powered off and with the user profile left closed. At the same time, IT administrators must suspend the custodian login credentials and revoke active session tokens while leaving the underlying cloud license and data containers intact under a formal litigation hold so a certified forensic examiner can create a verified bit for bit image and cloud export.

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

What a Device Shows After an Unplanned Boot

Counsel often calls after the helpdesk has already logged into a returned laptop, and the first question is what the device still holds. Usually a great deal, and the changes the boot made are specific. Booting a Windows machine into the user's profile updates registry hives, writes new prefetch entries, rolls event logs and may trigger an update or an indexing pass that changes file access timestamps. On a solid state drive, the boot can also prompt TRIM to release blocks that deleted files occupied, so the examiner turns to cloud copies and sync logs for those files. What remains is substantial: the user's documents, browser history, USB device history in the registry, LNK files and jump lists that show which files were opened, cloud sync client logs and the event logs that survived.

After an uncontrolled boot, the record is where the examiner looks for what the departing employee opened, copied and connected in the weeks before departure, and the technician's session is accounted for in every timeline. We identify the technician's logon, the duration of that session and every artifact it touched, and we exclude or annotate those entries so a timeline presented to a court assigns the helpdesk's activity to the helpdesk and the custodian's activity to the custodian. That accounting prepares the report for the cross examination question about who was logged in.

After reprovisioning, the examination moves to the cloud accounts, backups and server logs, which the examiner preserves in place of the reimaged laptop. OneDrive and Google Drive activity logs, Microsoft 365 audit records of downloads and sharing, and email records are held apart from the device when the account was placed on hold. Our trade secret and departing employee forensics page describes the device and cloud sources that are correlated in these matters and why both are needed. Where the device has been reissued, the cloud record is where the examiner looks for the answer to the question counsel asked.

The Trade Secret Statute Rewards Reasonable Measures

The Defend Trade Secrets Act defines a trade secret in part by the owner's conduct. Information qualifies only if “the owner thereof has taken reasonable measures to keep such information secret” (18 U.S.C. 1839(3)), and the civil remedy in 18 U.S.C. 1836 depends on that definition. A company that documents how it controlled access to its designs or customer data, and preserves the record of what the departing employee took, has evidence on both elements. The offboarding record is evidence on both: the access controls that were in place and the forensic preservation that shows what left.

Preservation also protects the employer on the other side of the same dispute. When a departing employee later alleges wrongful termination or retaliation, or when a new employer is accused of receiving trade secrets, the employer's own conduct in handling the departed employee's devices and accounts is examined. A documented quarantine, a hash verified image and a cloud export made before any administrator reviewed the content are evidence that the employer preserved the record whole and as found. Under Rule 37(e), the question is whether reasonable steps were taken, and a written preservation gate is the clearest answer.

The statute and the rule together make the point that preservation is a legal position rather than an IT task. We encourage general counsel to write the preservation gate into the offboarding procedure itself, so HR's notice of a sensitive departure triggers quarantine and hold automatically rather than depending on someone remembering to call legal. Our guide to common digital evidence mistakes lists the situations this gate is

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

designed for, and most of them are procedural rather than technical. A procedure written once and followed every time costs less than a single spoliation motion, and it is the evidence of reasonable steps that counsel will want to show.

The Preservation Engagement, Step by Step

The first phase is quarantine and hold, and it happens before we arrive. Returned devices are bagged, labeled with the date, custodian and the name of the person who received them, and stored powered off. Mobile devices go into airplane mode or a shielded container so they stay isolated from remote wipe commands. Accounts are suspended, with sessions revoked and credentials disabled, while the license, mailbox and cloud storage remain intact under a litigation hold. We walk administrators through those steps on the first call because each one closes a path by which evidence changes.

Imaging and export follow. Laptops are imaged bit for bit through a write blocker or, where the drive is encrypted, through a documented live acquisition with the recovery key from the endpoint management console, and every image is hashed and verified. Phones are acquired through full file system or logical extraction depending on the model, or remotely through our supported collection link when the device is with the custodian, a process that usually runs from a few minutes to overnight depending on setup. Cloud mailboxes and drives are exported in native format with their audit records. Each step is recorded in a chain of custody log.

Analysis is scoped to the question counsel asks. A departure matter usually begins with the final weeks of USB connections, cloud uploads, personal email forwarding, large file access and application installs, correlated across the device image and the cloud audit record. We report findings with the artifacts that support each, and we note which sources cover each period. The computer forensics page describes the laboratory process, and the digital forensics process guide explains how the engagement moves from preservation to report. Findings are reported in writing at the end of the first phase so counsel can decide whether to expand the scope or conclude.

Who Acts Before the First Call

Human resources holds the trigger. The moment a departure, termination or internal complaint involves someone with access to sensitive information, HR should notify legal and IT together, before the exit interview if possible, so the preservation gate opens before the employee's last session. HR also holds the signed acceptable use policy and device agreements that establish the company's right to examine its own equipment, and those documents should be located and preserved with the devices, because opposing counsel will ask for them early. A standing checklist for sensitive departures keeps the notice from depending on any one person's memory.

IT holds the devices and the accounts. The instruction is simple and often counterintuitive: keep the laptop powered off, keep the phone as it is, keep the account, and keep the license active. Suspend sign in, revoke sessions, change the password to one no one knows, place the mailbox and drive on hold, pull the BitLocker or FileVault recovery key from the management console and record it with the device, and stop any automated reprovisioning job that is scheduled to run. Endpoint management consoles often show the device's last check in and location, which should be captured before the device is enrolled elsewhere.

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

Legal holds the decision. Counsel decides whether the matter warrants imaging, which custodians are in scope, and whether the analysis proceeds under a litigation hold with the expectation of a report or testimony. Counsel also directs the engagement so the examiner's work is performed at counsel's request, and counsel manages communication with the departed employee and any new employer. Our expert witness page describes how the preserved record becomes a declaration or testimony when the dispute proceeds. Counsel's early direction also keeps the examiner's work product structured for the deliverable the matter will eventually need, whether that is a letter to the new employer or a declaration in support of an injunction.

Immediate Action Checklist Before Touching a Returned Device

If a suspicious departure or internal dispute is unfolding right now, instruct your IT staff to stop all laptop reprovisioning, gather the device BitLocker or FileVault recovery keys from your endpoint management console and isolate any returned mobile devices in Airplane Mode. Read our guide to the five digital evidence mistakes counsel must avoid, or call Global Digital Forensics 24/7 at (800) 868-8189 to coordinate rapid, defensible device and cloud preservation. The initial consultation is free.

What an Unplanned Boot Leaves in Place

Counsel often calls after a technician has already signed into a returned laptop. This table lists the artifact families an examiner looks for in a departure matter, whether each tends to persist through an uncontrolled boot, what it can establish and where the examiner looks next. It complements the narrative above by showing how much a booted device still holds, and why the cloud record is read alongside it. The second column describes a tendency, which the examiner confirms on the image.

Artifact families on a returned Windows laptop, their resilience to an uncontrolled boot and the corroborating source for each.

Artifact family	After a helpdesk boot	What it can establish	Where the examiner looks next
USB device history in the registry	Usually survives	A device with a given serial was connected and when it was first and last seen	File system artifacts for any copy to the device
LNK files and jump lists	Survive, with new entries from the technician	Which files and folders were opened from which profile	Logon records and badge data for the person at the keyboard
Browser history and downloads	Usually survives	Personal webmail, cloud upload pages and downloads	The service's own log for the content uploaded
Windows event logs	May roll with new entries	Logon sessions, service installs, device events	Forwarded or exported logs for earlier periods
Prefetch and application execution records	Survive, with new entries added	Programs run, including wiping and archive tools	File system and journal records for each affected file
Deleted files on a solid state drive	Often released by TRIM after boot	Recovered content from blocks still allocated	Cloud copies and backups for released blocks

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

Artifact family	After a helpdesk boot	What it can establish	Where the examiner looks next
Cloud sync client logs	Usually survive	Files synced, shared or removed from OneDrive or Drive	The provider's audit records for other accounts
Cloud audit records	Unaffected by the device	Downloads, sharing and sign ins for an account placed on hold	Secondary copies in a SIEM or archive for earlier periods

The drug diversion case study describes examiners creating forensically sound copies of seized drives under documented acquisition and handling procedures, the same chain of custody discipline this guide asks of a returned device.

How to Begin and What Happens on the First Call

Before the call, our Preservation Checklist: Quarantine the Device, Hold the Account sets out the items to secure in the order they expire. Have ready the custodian's name and role, the date of departure or notice, the devices issued and their current location and state, the cloud accounts involved, whether any device has been booted or wiped, and whether a hold has issued. The examiner asks what the concern is, what the employee had access to, what has already happened to the devices and accounts, who the administrators are and whether counsel is directing the matter. You receive immediate preservation instructions for IT and a written proposal naming the devices and accounts to be preserved, the acquisition method for each, the questions the analysis will address and the timing factors, including whether remote phone collection is available. The initial consultation is free. Call (800) 868-8189 at any hour.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST SP 800-86 and NIST SP 800-101 Revision 1.

Authorities cited in this guide: 18 U.S.C. 1839, Definitions (Defend Trade Secrets Act). Supplies the reasonable measures element of the trade secret definition quoted in the guide, current text at Cornell LII. Federal Rule of Civil Procedure 37(e). Sets the reasonable steps standard for preservation of electronically stored information, current text at Cornell LII. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Establishes the collection, examination, analysis and reporting structure the preservation engagement follows, final publication August 2006. NIST SP 800-101 Revision 1, Guidelines on Mobile Device Forensics. Establishes the isolation and acquisition practices for mobile devices described in the engagement steps, Revision 1 published May 2014.

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

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Evidence Preservation

IT already logged into the returned laptop. Is the evidence ruined?

Usually the device still holds a great deal. The technician's session changed registry hives, event logs and some timestamps and may have triggered TRIM on deleted files, but documents, browser history, USB device records, shortcut files and cloud sync logs typically survive. The examiner identifies the technician's logon and accounts for it in every timeline so the custodian's activity is separated from the helpdesk's. Power the device off now, record who used it and when, and preserve it as it stands.

How long should we keep a departed employee's laptop before reissuing it?

Long enough for counsel to decide whether the departure carries risk, and when it does, until a verified forensic image exists. Once a hash verified image is made and stored, the physical device can usually be reissued, because the image is the evidence. For departures that involve access to trade secrets, client lists or pending disputes, imaging before reissue is the conservative path. The decision belongs to counsel, and an image is a small cost that keeps every option open.

Can you collect a phone that is still with the departing employee?

Where counsel has arranged the employee's cooperation and the authority to collect, yes. Our supported remote collection works through a link and a computer connection, normally with the phone continuing in use, and usually runs from a few minutes to overnight depending on the device and setup. The alternative is physical collection on site or at one of our offices. Either way the acquisition is hashed and documented so the method can be explained in a declaration if the collection is challenged.

Do we need a litigation hold before imaging a device?

Imaging can proceed on its own, and a hold accompanies it when litigation is reasonably anticipated, because the hold is what pauses retention policies, offboarding scripts and license deletions on the cloud side of the record. The device image preserves one source. The hold preserves the mailbox, drive and audit logs that the image is correlated against. Counsel decides when the duty attaches, and we help translate the hold into the specific technical actions each administrator must take.

Does the company need the employee's consent to examine a company device?

That is a legal question for counsel, and the answer usually turns on the acceptable use policy, device agreements and the law of the jurisdiction rather than on forensics. Our role is to preserve the device in a way that works under any answer, so counsel has the option once the authority is settled. We also recommend locating and preserving the signed policies with the device, because they are often the first thing opposing counsel asks about.

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

Web Addresses for the Sources Cited

1. 18 U.S.C. 1839(3): https://www.law.cornell.edu/uscode/text/18/1839
2. 18 U.S.C. 1836: https://www.law.cornell.edu/uscode/text/18/1836
3. Rule 37(e): https://www.law.cornell.edu/rules/frcp/rule_37
4. NIST SP 800-86: https://csrc.nist.gov/pubs/sp/800/86/final
5. NIST SP 800-101 Revision 1: https://csrc.nist.gov/pubs/sp/800/101/r1/final

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 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.