Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/computer-forensics-preservation-checklist/

PRESERVATION CHECKLIST

Preservation Checklist: Quarantine the Device, Hold the Account

Evidence in a device matter is held by simple routine: the laptop stays powered off in its bag, the license stays assigned and the drive stays on the shelf. This checklist is the order of operations that holds the record as it is until an examiner images it.

Why the Device Stays Off Until It Is Imaged

A returned laptop holds its record most clearly in the state it arrived in. Powered off, it keeps the registry hives, prefetch entries, event logs and file access timestamps as the custodian left them, and on a solid state drive it keeps the blocks that deleted files occupied away from the controller's cleanup routines, which run when the machine boots. The strongest record is the one acquired first, imaged through a write blocker, hashed at acquisition and verified when the working copy is made.

GDF works with the authorized Microsoft 365 administrator to preserve the relevant mailboxes, OneDrive records and activity logs.

The Order That Protects the Evidence, Device First and Account Second

Keep an already powered off computer off and place it in documented custody. For a running system, record its condition and contact GDF promptly. Our examiners coordinate the preservation, network isolation and live acquisition plan with the authorized technical team.

The account comes second, within the same day. The administrator blocks sign in and revokes active sessions so the data stays as it is, for the departed employee and everyone else, while the license, the mailbox and the cloud storage stay intact under a litigation hold applied through Purview. The exports that expire first follow: Entra sign in logs with device identifiers and IP addresses, then the unified audit log for the custodian with its FileDownloaded, FileSyncDownloadedFull and sharing events, then any mailbox rules and forwarding addresses. Backups and snapshots are a third tier. Whoever runs the backup platform pauses the rotation so the custodian's last full backup is held, and the endpoint detection, VPN and proxy logs for the custodian are exported ahead of their normal rollover. Each export is hashed and logged. Our digital forensics process page shows how these pieces are later correlated.

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

Who Holds the Device, the Account and the Questions

Counsel owns the decision to preserve and the written instruction that says so. HR or the receiving manager owns the physical device from the moment it is returned until an examiner signs for it. The Global Administrator owns the account hold and the exports, working from a written list so that every source is covered under pressure. The backup and security teams own their own log sources. The examiner owns the acquisition, and the device stays in its bag until then. Writing those roles into the offboarding procedure itself, so a sensitive departure triggers quarantine and hold automatically, is the single change we most often recommend to general counsel, because it puts preservation in motion the moment the departure is recorded.

The people who wait are the ones who want answers fastest, and their questions are taken up from the preserved copies. The manager who wants to know what the employee took looks for that answer in the preserved export, which keeps each file's access timestamps as the custodian left them rather than adding new ones attributed to the company. The helpdesk confirms the laptop works after it is imaged. The administrator's search for the competitor's name runs against the preserved export, where it is recorded as part of the examination. Every one of those steps is taken from a verified image or a preserved export, under the direction of counsel, where it adds to the record.

Routine Habits That Keep the Record Whole

The first habit is holding the hardware. A returned laptop set aside, rather than wiped and reissued to the next hire, keeps the endpoint record of the custodian's final weeks. Where a machine has already been reimaged, the examination moves to the cloud accounts, backups and server logs, which the examiner preserves in place of the reimaged laptop. The second habit is keeping the account. A license left assigned holds the mailbox and drive in place, since the purge timer starts when the license is removed, so the download and sharing history in the audit log has the files themselves to be compared against. The third is leaving the copying to the examiner. A forensic image keeps the original timestamps along with the metadata, LNK files, jump lists and shellbags that show how the files were used, and its hash ties the working copy to the original.

Documentation matters just as much. A device that goes straight to the cabinet with a signed custody form, naming who had it on each day, carries a complete chain of custody to present. And a preservation instruction that reaches the backup administrator, the MDM administrator and the person who runs the VPN, as well as legal, holds every source on the same day. Our guide to digital evidence that withstands cross examination explains why authentication is built at acquisition, well ahead of trial, and the five common digital evidence mistakes describes the procedural steps this checklist is designed to get right.

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

From Quarantine to the Witness Stand

Global Digital Forensics has performed computer forensics examinations for counsel, internal auditors and corporate security teams since 1992, from sixteen US offices and a 24/7 hotline. On a preservation call we walk the administrator through the holds and exports in the order above while the device is still in its bag, then acquire it through a write blocker, verify the image by hash and build the record from there. Robert Knudsen, who leads much of our computer forensics work, has conducted hundreds of computer and mobile examinations supporting matters in federal and state courts, and the examiner who images the device is the one who explains the method. Where the device has already been booted, we identify the technician's session and annotate or set aside everything it touched, so the timeline presented to a court attributes the helpdesk's activity to the helpdesk and the custodian's activity to the custodian.

What the legal team receives is a documented acquisition protocol, a custody record, an inventory of the sources collected and the sources outside the collection, and a report in which each finding traces to its artifact and states that artifact's scope. A LNK file records that a path was opened from a profile, and tying that activity to a person combines the device record with access logs, interviews and other corroboration, which the report sets out. That discipline lets attorneys argue each point with a clear view of the support behind it. Our clients include AmLaw 100 firms and Fortune 1000 companies, and the first conversation is free. If a device is in a drawer and an account is scheduled for deletion, call (800) 868-8189 before the next business day starts, and a senior examiner will tell you what to hold and in what order.

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

The Checklist at a Glance

The device and account sources to preserve before an examiner arrives, who holds each one, where it lives and how quickly it changes.

Item	Who acts	Where it lives	How fast it expires
Returned laptop or workstation	HR or the receiving manager, bagged and powered off	Locked evidence cabinet with a custody form	Held as is until the first boot or a reimage
Microsoft 365 account and mailbox	Global Administrator, block sign in and apply hold	Entra sign in settings and Purview hold	Thirty days after deletion under the Microsoft default
Unified audit log for the custodian	Compliance administrator	Microsoft Purview audit search export	180 days standard, longer by license
Microsoft Entra sign in logs	Global Administrator	Entra portal or SIEM export	Seven or thirty days by license
OneDrive and SharePoint activity	SharePoint administrator	Purview audit events and site activity reports	180 days standard, file versions by site policy
External drives and USB media	Whoever finds them, logged and bagged	Same evidence cabinet, listed on the inventory	Held as is until the drive is reused
Backups and snapshots	Backup administrator, pause the rotation	Backup server or cloud backup console	Held until the next rotation cycle
Endpoint, VPN and proxy logs	Security team, export now	EDR console, SIEM and VPN concentrator	Rolls over by log size or vendor retention

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

FREQUENTLY ASKED

Booted Laptops, Licenses and Custody Forms

The helpdesk already booted the laptop. Is the evidence ruined?

Most of the record is usually still there, and the effect of the boot is specific. The session updated registry hives, prefetch entries and some timestamps, and on a solid state drive it may have released blocks that deleted files occupied. The documents, browser history, USB device history, LNK files, jump lists and surviving event logs usually remain for the examiner. Stop there, bag the device, write down who signed in and when, and let the examiner account for that session openly in the timeline.

Can IT remove the license to save the seat if we export the mailbox first?

Preserve the mailbox, OneDrive records and activity logs with your authorized Microsoft 365 administrator before changing the account or license. GDF confirms the preservation controls and scopes the collection around the matter.

Do we need a forensic image, or is a backup enough?

Preserve the backup as well; it adds a dated copy alongside the device image. Backups capture files on a schedule, and the image adds the system artifacts, deleted space and metadata that show how files were used, copied or removed. A bit for bit image through a write blocker, hashed at acquisition, preserves all of it and yields a copy whose integrity is verified by hash. Preserve the backup, pause its rotation and image the device.

Who should sign the chain of custody form?

Everyone who takes physical possession of the device, in order, with the date, time and reason for the transfer. The form starts with the person who received the returned device and ends with the examiner who acquires it. The other side checks that record first, so each transfer is written down as it happens. Keep the form with the device itself.

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.