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

PRESERVATION CHECKLIST

Mobile Preservation Checklist: Airplane Mode First, Questions Later

A phone isolated from every network stops receiving new data, which keeps the space its deleted messages occupied as it is for the examiner. This checklist is the order of isolation, custody and account holds that holds the device as it is until an examiner collects it.

Why Isolation Comes Before Every Other Step

GDF selects and verifies a radio isolation method for the handset, then manages power, charging and acquisition around the device state.

Google Timeline is stored on the individual device, with an optional encrypted backup. GDF maps the relevant handset, account and vehicle sources and correlates the collected records into a documented location chronology.

The Order of Isolation, Custody and Account Holds

We record the isolation method, verification results and handling history with the collected evidence.

Account holds follow immediately, because the accounts are a second place the examiner looks for the data. The mobile device management administrator suspends any pending wipe, retire or selective wipe action for the device so any queued command stays suspended when the phone next sees a network. Counsel or the account owner preserves iCloud or Google backups by disabling automatic deletion and signing in only from existing devices, which keeps the current backup in place for the examiner. Where the matter involves location, counsel notes the carrier and the account so records can be requested by subpoena or with the custodian's consent, and the fleet manager holds any vehicle the phone was paired with in its current state, with sale, service and reset paused. Corporate accounts the phone synchronized are placed on hold on the tenant side exactly as described in our digital evidence mistakes resource.

Who Handles the Phone and Who Keeps It Locked

Counsel decides that preservation is required and documents the instruction, and where the device is personal, counsel negotiates the inspection protocol under which it will be examined. The custodian or the HR representative who receives a company phone performs the isolation and the bagging, records the time and signs the first line of the custody form. The MDM administrator owns the hold on remote commands and the export of the device's enrollment and compliance history, which shows when the phone last checked in and whether a wipe was requested. Counsel or the account owner holds the cloud backups. The examiner alone performs the extraction and documents the tool, the version, the method and the scope of what it reached.

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

The person who most wants to unlock the phone is usually the person best placed to hand it to the examiner. Handing it over unopened keeps the read receipts, database entries and access times as the custodian left them, which is the record an opposing expert will study. Screenshots a colleague has taken are kept as images, and the database behind them is the record the examiner preserves. If someone has already opened the phone or taken screenshots, write down what was done and when, and tell the examiner so the extraction accounts for it from the start.

Habits That Keep the Phone's Record Whole

The first habit is collecting the phone ahead of any reset or trade in, which matters most when a departing employee works through a notice period or a company device is due for scheduled recycling. Under Rule 37(e), the preservation duty runs from the moment it attaches, and a company whose own process holds the device from that moment gives counsel a straightforward account to present. The second habit is network isolation. A phone in airplane mode or a shielded bag stops receiving new messages, so the space the deleted rows occupied stays as it was. The third is securing the passcode. An extraction with the code reaches further than one without it, so the code is written down and sealed for the examiner while the custodian is cooperating.

Scope takes the same care. A personal phone holds far more than any matter needs, and Rule 26(b)(1) proportionality means collections are scoped to date ranges, participants and applications under a written protocol agreed before the device is touched. The scope also follows the question: location data when the matter turns on location, and the account side as well as the handset when the account holds the longer history. Counsel and the examiner settle the questions the collection must answer before it begins, and the protocol records them. Our digital forensics process page describes how that scoping conversation runs.

How GDF Collects, Including Remotely, Under the Direction of Counsel

Global Digital Forensics has examined mobile devices for counsel, insurers and corporate security teams since 1992. Veronica Perez leads our mobile and vehicle evidence work and has taught acquisition methods, including JTAG, chip off and in system programming, to other examiners through the California Department of Justice Advanced Training Center and Teel Technologies. The method follows the device: a logical extraction where that is enough, a full file system extraction where deleted message recovery requires reaching the application databases and their write ahead logs, and hardware methods where a device is damaged or old enough to warrant them. Every extraction is hashed, the tool and version are recorded and the report documents the scope of what was captured so its conclusions can be traced to a source. Our mobile device forensics page describes these methods.

Where the custodian is cooperative and the matter allows, supported remote collection changes the logistics. The owner connects the phone to a computer and follows a link we provide, the collection runs while we supervise, usually from a few minutes to overnight depending on the device and setup, and the owner normally keeps using the phone afterward. That removes shipping, travel and the handoff risks of a device changing hands, and it means an executive can keep working while the record is preserved. GDF mobile evidence has been accepted in court, and the examiner who performs the collection signs the report and the affidavit and is available to testify. The initial consultation is free. If a phone is about to be reset, reissued or traded in, call (800) 868-8189 before it happens.

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

The Checklist at a Glance

The device, account and vehicle sources to hold before a mobile collection, who holds each one, where it lives and how quickly it changes.

Item	Who acts	Where it lives	How fast it expires
The handset	Custodian or HR, airplane mode and power state recorded	Shielded bag or container in a locked cabinet	Deleted rows hold while the phone is isolated
Passcode and account credentials	Custodian, written and sealed for the examiner	Sealed envelope traveling with the custody form	With them, the extraction reaches further
Remote wipe and MDM commands	MDM administrator, suspend wipe and retire actions	MDM console such as Intune or Jamf	Held once suspended, before the phone next sees a network
iCloud or Google account backups	Account owner or counsel, existing devices only	Apple ID or Google account settings	Current backup held while sign ins stay on existing devices
Carrier records	Counsel, by subpoena or customer request	The wireless carrier	Retention varies by carrier and record type
Messaging application data	The examiner, with the apps left closed until then	Application databases on the device	Disappearing message timers run by design
Vehicle infotainment and telematics	Fleet manager, sale, service and reset paused	Infotainment and telematics modules	Held while the vehicle is parked and unpaired
Chain of custody form	Everyone who touches the device, in order	Paper or PDF traveling with the device	Each transfer written down as it happens

FREQUENTLY ASKED

Questions Counsel Ask About This Checklist

Should the phone be powered off or left on?

Isolate it first, then ask the examiner about its power state. A phone left on keeps its current state and is kept charged inside a shielded container, while a phone powered off returns to a fully locked state, so the examiner weighs the two for the specific device. The right choice depends on the model, the operating system version and whether the passcode is available. Record whichever state it is in, the time of isolation and who made the decision.

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

Can we just take screenshots of the messages we need?

Screenshots are a useful quick record of what the custodian saw, and the database behind them is the record the examiner works from. The examiner reads the messaging database for the source timestamps, the delivery and read flags, deleted rows and the structure that shows whether a thread was edited. Preserve the device and let the examiner extract that database. Keep any screenshots already taken and note when they were made.

The employee says the phone is personal. Can we still preserve it?

Counsel decides what can be requested and under what protocol. A personal device that carried corporate email or messages can be within scope, and collection proceeds under an inspection protocol that counsel agree in advance, limited to the date ranges, participants and applications the matter requires. In the meantime counsel sends a preservation request asking the custodian to keep the device as it is.

How fast can a remote collection happen?

Where the custodian cooperates and the matter allows, supported remote collection runs through a link and a computer connection, usually from a few minutes to overnight depending on the device and what is being collected, and the owner normally keeps the phone afterward. The examiner supervises throughout, hashes the extraction and documents the method. It is often the fastest way to preserve a device that stays with its owner.

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.