Digital Forensic Examination of Deleted Data and Electronic Evidence

Posted on September 17, 2018

This digital forensic examination is based on a hypothetical training scenario involving a laptop and mobile phone assigned to a senior U.S. government official. The scenario alleges that investigators discovered a text message arranging a lunch meeting on February 15, 2016, a contact labelled “Red Ralph,” deleted compressed files containing sensitive material, and evidence suggesting that files may have been uploaded to a file-sharing service. These facts should be treated only as case assumptions for the forensic exercise. They do not establish the guilt of any real public official or foreign actor, and the examiner’s role is not to decide motive or criminal liability. The examiner’s responsibility is to preserve, recover, authenticate, analyze, and report digital evidence in a reproducible manner.

Modern digital forensics places much greater emphasis on validated acquisition, chain of custody, tool testing, cloud evidence, mobile-device isolation, and minimization than older “recover everything and search later” models. NIST’s forensic-science program and the Scientific Working Group on Digital Evidence (SWGDE) now maintain standards and best-practice documents covering computer acquisition, mobile-device evidence, cloud-service evidence, focused collection, and forensic examination. The appropriate method therefore depends on the device, legal authority, encryption state, volatility of the data, and the specific questions investigators have been authorized to answer.

Examination Scope

The case should begin with a written examination request. At minimum, the examiner needs the legal authority for the search, the devices or accounts included within scope, relevant date ranges, known identifiers, and the investigative questions. In this scenario, the central questions are whether the mobile device contains communications related to the specified meeting or relevant contacts; whether the laptop contained compressed or classified files that were deleted; whether those files can be recovered or reconstructed; whether system or application artifacts indicate transfer to an external file-sharing service; and whether timestamps and account identifiers link the recovered artifacts into a defensible timeline.

Evidence source	Primary forensic question	Important artifacts

Mobile phone	Were relevant communications or contacts present?	SMS/MMS, messaging databases, contacts, call logs, notifications, app data, backups, device/account identifiers
Laptop storage	Were sensitive archives created, accessed, deleted, or transferred?	File-system metadata, deleted directory entries, unallocated space, shell history, recent files, archives, browser history, cloud-client databases
Cloud/file-sharing account	Was material uploaded, shared, downloaded, or deleted?	Provider logs, file versions, account activity, IP records, timestamps, sharing permissions, deleted-item records
Network or organizational logs	Can device activity be corroborated independently?	Authentication, proxy, firewall, VPN, DNS, DLP, endpoint, and identity-provider logs

The scope should be narrow enough to comply with the warrant, consent, policy authorization, or other legal basis. Modern digital devices can contain years of unrelated personal and professional information. SWGDE's current guidance on focused collection and minimization recognizes that investigators may need to limit seizure or examination to information relevant to the authorized purpose. Technical ability to access data is not the same as legal authority to examine it.

Evidence Preservation

The most important early objective is to avoid changing the original evidence unnecessarily. The examiner should document who collected each device, when and where it was collected, its condition, identifying information, and every transfer of custody. Evidence packaging and storage should protect against physical damage, unauthorized access, and accidental modification.

For a powered-off computer drive, a common approach is to create a forensic image through a validated acquisition process and then perform examination on the copy rather than the original medium. Cryptographic hash values should be recorded for the acquisition and used to demonstrate that the forensic image has not changed. Current SWGDE guidance on computer forensic acquisitions, updated in 2025, emphasizes appropriate hardware and software, documentation, validation, error handling, and preservation of acquisition results.

A powered-on computer creates a different problem because volatile evidence may disappear if power is removed. Random-access memory can contain running processes, encryption keys, network connections, command history, malware artifacts, mounted encrypted volumes, or other information unavailable after shutdown. Live acquisition may therefore be justified in some cases, but it changes

the system and must be documented carefully. The decision should follow the investigative objective and agency procedures rather than an automatic rule to “always pull the plug” or “always capture RAM.”

Mobile devices require another set of decisions. A smartphone may receive new messages, remote-lock commands, remote wiping instructions, or cloud synchronization after seizure. Investigators should document the device state and apply an appropriate isolation method while considering whether power loss could activate encryption or make acquisition more difficult. SWGDE’s 2025 mobile-device best-practices document covers collection, preservation, handling, and acquisition, while NIST continues to maintain tool-testing specifications for mobile acquisition. The acquisition method may be logical, file-system, physical, backup-based, cloud-assisted, or another validated technique depending on device model, operating system, security configuration, and legal authority.

Tool validation is essential because forensic software can fail or interpret artifacts incorrectly. NIST’s Computer Forensics Tool Testing program publishes specifications and test results to help laboratories understand tool capabilities and limitations. Using a commercial product does not remove the examiner’s obligation to understand what the tool actually acquired, what it omitted, and how its parsing was verified.

Deleted Data Recovery

The original article suggests that overwritten files can generally still be recovered from a modern hard drive. That statement is too broad and can be misleading. Deletion, formatting, overwriting, encryption, solid-state-drive garbage collection, and secure erasure are different events. Whether data can be recovered depends on the storage technology and what has happened since the file was deleted.

On many file systems, ordinary deletion initially removes or changes metadata that points to file content while some underlying data blocks may remain until reused. Investigators may therefore recover whole or partial files from unallocated space, deleted directory records, file-system journals, volume shadow copies, backups, temporary files, application caches, or other artifacts. File carving can reconstruct some content from recognizable headers and data patterns even when original filenames or directory metadata are gone.

Recovery becomes far less likely when the relevant physical blocks have actually been overwritten. On solid-state drives, TRIM and internal garbage collection can also remove data that traditional magnetic-drive recovery assumptions expected to persist. Full-disk encryption further changes the analysis because raw recovered blocks may be useless without the relevant keys. A defensible report should therefore state exactly what was recovered and from which artifact rather than claiming that “deleted data can always be restored.”

Compressed archives in the scenario require particular attention. Investigators should identify ZIP,

RAR, 7z, or other archive signatures; recover intact or partial archives where possible; examine archive metadata; and correlate their creation, access, extraction, or deletion times with operating-system and application artifacts. Hashes of recovered files can be compared with known organizational copies or approved reference sets. If a file is alleged to contain classified material, the examiner should avoid reproducing unnecessary content in a report and should follow the applicable handling rules for classified information.

The laptop should also be examined for evidence of transfer. Browser history, download and upload records, cloud-sync client databases, recently used file lists, shell commands, link files, jump lists, application logs, thumbnails, operating-system event logs, and endpoint-security records can contribute to a timeline. No single artifact should be treated as conclusive when independent corroboration is available.

Cloud Evidence

If the hypothetical weblog or local artifact suggests that files were sent to a cloud or file-sharing service, local computer evidence is only one part of the analysis. A browser history entry can show that a service was visited without proving a particular file was uploaded. A cloud-client database may provide stronger evidence, but provider-side records can add account identity, file versions, timestamps, access IP addresses, sharing history, and deletion events.

SWGDE's current best practices for cloud-service-provider evidence emphasize acquisition, preservation, provider procedures, legal process, and the need to understand how cloud architecture affects timestamps and metadata. Investigators may need preservation requests or other authorized legal process before provider records expire. Cross-border storage and provider jurisdiction can complicate collection.

Cloud evidence should be correlated with local device evidence. If a recovered archive was created at 14:03, the browser or sync client records an upload event at 14:07, the provider log records the same filename or hash at 14:08, and organizational network logs show a corresponding outbound transfer, the combined timeline is much stronger than any one source alone. Conversely, inconsistent timestamps may indicate clock differences, time-zone conversion, synchronization delay, or an alternative explanation that must be resolved before reporting.

Forensic Analysis

A forensic examiner should not begin with the conclusion that the suspect "exfiltrated classified material" and then search only for confirming evidence. The analysis should test plausible competing explanations. A deleted archive might have been a temporary work product. A cloud-service visit might relate to unrelated files. A contact label such as "Red Ralph" could have no political meaning at all. A lunch message establishes communication but not the content or purpose of the meeting.

The examiner should therefore distinguish facts, technical interpretation, and investigative inference. “The device contains an SMS dated X with the following participants” is an artifact-level finding. “The message arranged a meeting” is an interpretation of the text. “The meeting was part of an illegal conspiracy” is a legal or investigative conclusion that ordinarily falls outside the digital examiner’s role unless supported by separate evidence and explicitly within scope.

Timeline analysis can help connect events without overstating causality. Relevant sources may include mobile messages, file-system timestamps, operating-system logs, cloud records, network logs, user logons, removable-media history, and application artifacts. The examiner should normalize time zones, document clock drift where known, and preserve original timestamps.

Association between files also needs technical support. Files can be linked through hashes, common metadata, archive membership, embedded identifiers, shared directory paths, application histories, or provenance information. Similar filenames alone are weak evidence. Stronger conclusions require reproducible relationships that another qualified examiner could verify.

Reporting Findings

A professional report should identify the case, authority, items received, condition of evidence, acquisition methods, hash values, tools and versions, examination procedures, findings, limitations, and disposition of evidence. Screenshots may illustrate important artifacts, but screenshots are not substitutes for preserved source data and documented extraction methods.

The results section should be restrained. In this scenario, a defensible report might state that investigators recovered specified message records, identified the “Red Ralph” contact entry, recovered or partially recovered particular archives, identified artifacts consistent with deletion, and found local and/or provider evidence consistent with transfer to a named service. Each statement should identify its evidentiary basis.

Limitations should be explicit. An examiner may not be able to recover securely erased content, decrypt a protected volume, prove who physically operated a device at a particular moment, or obtain expired provider logs. Tool limitations, incomplete acquisitions, damaged storage, missing passwords, unsupported applications, and time-zone uncertainty all belong in the report when relevant.

The final review should also ask whether conclusions remain valid if one artifact is excluded. Strong digital evidence often emerges from convergence: device content, metadata, cloud records, network logs, and independent organizational records support the same timeline. When evidence conflicts, the report should preserve that conflict rather than force a definitive narrative.

A modern digital forensic examination is therefore not primarily a process of “recovering deleted files.” It is a controlled evidentiary workflow involving legal scope, preservation, validated acquisition, artifact interpretation, corroboration, minimization, and transparent reporting. In the hypothetical

case presented here, the correct outcome is not a declaration of political guilt. It is a technically defensible account of what the devices and associated services can and cannot demonstrate.

References

National Institute of Standards and Technology. (2014). *Guidelines on Mobile Device Forensics* (NIST SP 800-101 Rev. 1).

National Institute of Standards and Technology. (2025). *Mobile Device Forensic Tool Test Specification, Version 3.3*. Computer Forensics Tool Testing Program.

Scientific Working Group on Digital Evidence. (2025a). *Best Practices for Computer Forensic Acquisitions* (17-F-002-2.1).

Scientific Working Group on Digital Evidence. (2025b). *Best Practices for Computer Forensic Examinations* (18-F-001-2.0).

Scientific Working Group on Digital Evidence. (2025c). *Best Practices for Mobile Device Evidence Collection & Preservation Handling and Acquisition* (18-F-003-2.0).

Scientific Working Group on Digital Evidence. (2025d). *Best Practices for Digital Evidence Collection* (18-F-002-2.0).

Scientific Working Group on Digital Evidence. (2025e). *Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers* (23-F-004-1.1).