Digital Forensic Examination of Deleted Data and Electronic Evidence

Posted on September 17, 2018

View this essay online:
https://academic-master.com/digital-forensic-examination-of-deleted-data-and-electronic-evidence/

Introduction

Digital forensic examination is a controlled evidentiary process rather than a simple search for deleted files. In the hypothetical training scenario, investigators possess a laptop and mobile phone linked to a senior government official and are asked to examine communications, deleted archives, contacts, and possible transfer activity. Those facts are case assumptions, not proof of guilt or motive. The examiner's role is to preserve evidence, acquire data through validated methods, recover and interpret relevant artifacts, correlate independent sources, and report findings that another qualified examiner could reproduce. Scope should be defined before examination begins through the applicable warrant, consent, policy authorization, or other legal authority. Investigators need to know which devices and accounts are covered, the relevant dates, known identifiers, and the questions the examination is intended to answer. Modern devices contain large volumes of unrelated personal information, so technical capability to access data does not automatically create legal authority to examine everything available on the device.

Preservation and Acquisition Come Before Interpretation

Preservation begins with chain of custody and careful documentation of who collected each device, when and where it was collected, its condition, identifying information, and every later transfer. For a powered-off computer, a forensic image is commonly created through a validated acquisition process so that examination occurs on a copy rather than on the original storage medium. Cryptographic hashes can demonstrate that the acquired image remains unchanged. A powered-on computer requires a different decision because volatile memory may contain running processes, encryption keys, mounted volumes, network connections, or other evidence that disappears when power is removed. Capturing volatile data changes the system, so the action must be justified and documented. Mobile devices add risks from remote wiping, synchronization, and encryption. Isolation may be necessary, but investigators must consider whether power loss could lock the device or make data inaccessible. The correct method depends on device state, security configuration, legal scope, and the evidentiary objective. (SWGDE, 2025)

Deleted Data Is Not Automatically Recoverable

Deleted-data recovery depends heavily on storage technology and what occurred after deletion. Ordinary deletion on some file systems may remove or alter metadata while leaving data blocks available until they are reused, allowing recovery from unallocated space, file-system journals, backups, shadow copies, temporary files, caches, or carved data. It is misleading to claim that overwritten files can generally be recovered. When physical blocks have actually been overwritten, recovery is usually far less plausible, while solid-state drives can remove data through TRIM and internal garbage collection. Encryption can also make recovered blocks unusable without the required keys. Compressed archives should be examined for file signatures, metadata, creation and access times, partial content, and relationships with other artifacts. If sensitive or classified material is involved, the examiner should minimize unnecessary reproduction and follow appropriate handling rules. A defensible report states exactly what was recovered, from which artifact, and with what limitations rather than making broad claims about deleted information.

Cloud and Network Evidence Require Corroboration

Evidence of transfer to a cloud or file-sharing service requires more than a browser-history entry showing that a service was visited. Local artifacts such as cloud-client databases, recent-file lists, shell commands, application logs, browser records, sync histories, or operating-system events may indicate upload activity, but provider-side records can add account identity, file versions, timestamps, access addresses, sharing history, and deletion events. Strong conclusions emerge when independent sources converge. For example, an archive created on the laptop, an upload event recorded by the client, a matching provider-side record, and corresponding organizational network logs create a stronger timeline than any source alone. Timestamp interpretation also requires care because time zones, clock drift, synchronization delay, and provider formatting can create apparent inconsistencies. Investigators should preserve original values, document conversions, and explain uncertainty. Similar filenames are weak evidence of identity, while cryptographic hashes or other reproducible metadata can support a stronger technical relationship between files. (SWGDE, 2025)

Separate Artifact Findings from Investigative Conclusions

Forensic analysis should distinguish artifact-level findings from investigative and legal inference. A message record can establish that a particular device database contains text associated with specified participants and a timestamp. Interpreting that text as arranging a meeting is one level of inference. Concluding that the meeting formed part of a conspiracy is a broader investigative or legal

judgment that usually requires evidence beyond the digital artifact itself. The same discipline applies to a contact label, deleted archive, or cloud-service visit. Examiners should test plausible alternative explanations rather than searching only for evidence that supports the investigative theory. Timeline analysis can combine messages, file-system metadata, logons, removable-media history, cloud records, network logs, and application artifacts, but each source has limitations. Tool validation is equally important because forensic software can omit data or parse artifacts incorrectly. A commercial product does not eliminate the examiner's responsibility to understand what was acquired, how the tool interpreted it, and how important findings were independently verified.

Conclusion

A professional digital-forensic report should identify the authority for examination, evidence received, acquisition method, hashes, tools and versions, procedures, findings, limitations, and final disposition of evidence. Screenshots can illustrate important artifacts but should not replace preserved source data or documented extraction methods. Conclusions should remain restrained and reproducible. The examiner may be able to report that specific messages were recovered, that an archive existed and was deleted, or that local and provider artifacts are consistent with transfer activity. The report should also state when secure erasure, encryption, missing credentials, damaged storage, unsupported applications, or expired provider logs prevent stronger conclusions. Good digital forensics is therefore not defined by recovering the greatest quantity of data. It is defined by lawful scope, preservation, validated acquisition, transparent analysis, minimization, corroboration, and honest reporting of uncertainty. In a politically sensitive hypothetical case, technical discipline is especially important because forensic evidence should clarify what devices demonstrate without being used to manufacture conclusions about guilt or motive.

References

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

Scientific Working Group on Digital Evidence. (2025). Best Practices for Computer Forensic Acquisitions.

Scientific Working Group on Digital Evidence. (2025). Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers.