

Recovery and analysis of deleted email from Google Takeout and Microsoft Outlook

Tanushka Yadav¹, Dr. Munish Kumar Mishra², Dr. Lav Kesharwani³, Dr. Suchit Ashish John⁴, Abhinav Anand⁵

¹M.Sc (Forensic Science) Student, Department of Forensic Science, SHUATS, Prayagraj-211007, U.P., India

²Professor, Department of Forensic Science, SHUATS, Prayagraj-211007 U.P., India

³Professor, Department of Forensic Science, SHUATS, Prayagraj-211007 U.P., India

⁴Professor and Head, Department of Forensic Science, SHUATS, Prayagraj-211007 U.P., India

⁵Digital Forensic Analyst, Cyint Technologies, New Delhi -110020, India

Abstract

Email communication represents an important source of digital evidence because email messages may contain message content, headers, timestamps, sender and recipient information, attachments, and other metadata. Deletion of a message from a user interface does not necessarily mean that all corresponding artifacts have been removed from locally stored or exported mailbox data. This study presents a comparative forensic examination of deleted email artifacts from Google Takeout and Microsoft Outlook using SysTools Viewer. Sample email communications were prepared and selected messages were deleted. Gmail data were acquired through Google Takeout and examined in MBOX format, while Microsoft Outlook data were synchronized locally and examined in OST format. The resulting mailbox files were loaded into SysTools Viewer for examination of mailbox structure, deleted messages, headers, metadata, attachments, timestamps, sender and recipient information, and message content. Four sample emails were deleted in the experimental work and all four were reported as recovered. Both platforms provided recoverable forensic artifacts, although differences were observed in acquisition method, storage format, mailbox organization, and platform-specific metadata. Outlook provided additional artifacts such as CC/BCC information, read/unread status, message size, and native folder hierarchy, whereas Google Takeout provided an exported Gmail archive in MBOX format. The findings demonstrate a practical workflow for examining email evidence across cloud-exported and locally synchronised mailbox environments, emphasising that recoverability depends on the mailbox state, the timing of export or synchronisation, and the deletion process.

Keywords: Email forensics; deleted email recovery; Google Takeout; Microsoft Outlook; MBOX; OST; SysTools Viewer; digital evidence; metadata

Date of Submission: 17-09-2026

Date of Acceptance: 01-10-2026

I. Introduction

Email is one of the most widely used forms of digital communication and is used in personal, academic, business, governmental, and legal environments. An email contains more than visible message text: headers, timestamps, sender and recipient information, routing information, attachments, and other metadata can provide evidence about communication events. Because of this combination of content and technical information, email is an important source of digital evidence in cybercrime and other investigations. Email forensics focuses on the identification, acquisition, preservation, recovery, examination, and interpretation of email-related evidence. Previous research has examined email headers, deleted messages, mailbox formats, forensic tools, visualization, automated analysis, and the use of email evidence in investigations. (Fagalde2006) examined recovery of deleted Outlook messages and PST data, while (Tiwari et al.2011) described a systematic approach to email evidence involving acquisition, preservation, recovery, analysis, and presentation. (Banday2011) emphasized header and metadata analysis, including correlation with server and network records. (Devendran et al.2015) comparatively evaluated email forensic tools and highlighted that different tools provide different strengths. Despite this body of work, a practical comparison of deleted-email artifacts from a cloud-export mechanism and a locally synchronised desktop mailbox, examined with the same software workflow, remains useful. Google Takeout exports Gmail data as MBOX archives, whereas Microsoft Outlook can maintain locally synchronised mailbox information in OST files. These different acquisition and storage environments may influence which artifacts remain available for forensic examination. The present study therefore investigates the recovery and analysis of deleted email artifacts from Google Takeout and Microsoft Outlook using SysTools Viewer. The study specifically compares the two environments with respect to acquisition, storage format, recoverability, mailbox structure, metadata, attachments, and other forensic artifacts.

II. Material And Methods

The experiment was conducted in a controlled environment using a Windows 11 personal laptop with 8 GB RAM and approximately 447 GB of available SSD storage, together with a stable Internet connection. The software resources were Microsoft Outlook, Google Takeout, and SysTools Viewer for OST/PST and MBOX examination. Sample email accounts were used with prior consent of the account holders, and test emails included normal messages, messages containing attachments, and deleted messages. Microsoft Outlook was configured with the experimental email account and synchronized so that mailbox folders were available locally. The account settings and synchronization options were checked, and the mailbox was allowed to complete synchronization. The Outlook data-file location was identified and the local mailbox data were copied to a separate working folder. The resulting OST data were opened in SysTools OST Viewer, which processed the mailbox and displayed folders and available email records for examination. The experimental Google account was accessed and Google Takeout was opened. Mail data were selected for export and an export archive was requested. After the export was made available, the downloaded ZIP archive was extracted and the mailbox data were located. The MBOX file was then loaded into SysTools MBOX Viewer and processed for examination. The mailbox structure, messages, metadata, attachments, and deleted-message records were inspected. Forensic Examination includes identification of the mailbox file type (MBOX or OST), Loading of the working copy into the appropriate SysTools Viewer, Examination of mailbox and folder structure, identification of deleted or recoverable email records, Examination of sender and recipient information, subject, date/time, Message-ID, headers, and other metadata and Examination of attachments and their associated messages. Comparison of artifacts available from Google Takeout and Microsoft Outlook.

III. Results

Google Takeout produced Gmail data in MBOX format. The MBOX file was successfully opened in SysTools MBOX Viewer and the mailbox structure was displayed. The examination showed that the exported archive retained email records available at the time of export. Recovered records included sender and recipient addresses, subject, transmission date and time, message body, message identifiers, labels/folders, and attachments. In the experimental work, four sample emails were deleted and all four deleted emails were reported as recovered. While Microsoft Outlook generated a locally synchronized OST mailbox. SysTools OST Viewer recognised the mailbox and displayed folders including Inbox, Sent Items, Deleted Items, Drafts, and Archive. Recovered information included sender, recipient, CC/BCC, subject, message body, date and time, attachment information, message size, and read/unread status. These artifacts provided additional information for reconstructing mailbox activity and communication history.

Table no.1 Recovered Email Artifacts From Google Takeout and Microsoft Outlook

Artifact	Google Takeout	Microsoft Outlook
Sender information	Available	Available
Recipient information	Available	Available
Subject	Available	Available
Date and time	Available	Available
Email header	Available	Available
Attachments	Available	Available
Folder information	Available	Available
Message status	Available	Available
CC/BCC	Limited	Available
Read/unread status	Not available	Available
Message size	Limited	Available

Metadata examination identified sender address, recipient address, date, time, subject, and Message-ID in both environments. It records examination of CC/BCC, attachment names, and file size. These metadata elements assist in reconstructing communication sequences and linking messages to participants. Timestamps provide a basis for chronological reconstruction, while sender and recipient fields support identification of communication relationships. SysTools Viewer displayed attachments associated with recovered messages. It records PDF documents, JPEG and PNG images, and text documents among the attachment formats examined. Attachment names, sizes, and their association with the corresponding messages remained available for examination.

Table no. 2 Comparative Analysis Of Google Takeout and Microsoft Outlook

Parameter	Google Takeout	Microsoft Outlook	Forensic Interpretation
Data Source	Cloud Gmail Export	Local Outlook Mailbox	Different acquisition methods
Storage Format	MBOX	OST/PST	Different forensic file formats
Data Acquisition	Manual export	Automatic synchronization	Outlook provides quicker acquisition
Deleted Email Recovery	Recoverable only if included in export	Recoverable from OST/PST depending on deletion status	Outlook offers greater recovery potential
Email Headers	Available	Available	Useful for sender verification and routing analysis
Sender/Recipient Details	Available	Available	Supports communication reconstruction
CC/BCC Information	Limited	Available	Outlook provides more complete metadata
Attachments	Preserved	Preserved	Both maintain evidential attachments
Folder Structure	Gmail Labels	Native Outlook Folders	Outlook preserves mailbox hierarchy
Read/Unread Status	Not available	Available	Indicates user interaction with messages
Message Size	Limited	Available	Additional evidential value in Outlook
Keyword Search	Through Viewer	Through Viewer	Both support forensic searching
Evidence Integrity	Read-only analysis	Read-only analysis	Original files remain unchanged
Overall Forensic Value	Good	Excellent	Outlook provides more comprehensive artifacts

The comparison demonstrates that both platforms can provide useful forensic artifacts, but their acquisition and storage architectures are different. Google Takeout provides an exported snapshot of Gmail data in MBOX form, whereas Outlook provides a locally synchronized mailbox database in OST format. It indicates that Outlook supplied a broader set of platform-specific artifacts, including CC/BCC information, read/unread status, message size, and native folder hierarchy. Google Takeout nevertheless provided a useful export mechanism for preserving Gmail data for examination. Recoverability should not be interpreted as guaranteed: it depends on whether the relevant information remained in the exported or synchronized data and on the timing and manner of deletion.

IV. Discussion

The results support the established forensic principle that deletion from a user-facing email interface does not necessarily eliminate every residual artifact from associated storage. The present study recovered deleted email records from both examined environments and identified metadata and attachments that could assist in reconstructing communication events. This finding is consistent with (Fagalde 2006), described recoverable Outlook email information, and with (Tiwari *et al.* 2011), emphasized systematic recovery and analysis of email evidence. The importance of metadata observed in this study is consistent with (Banday 2011) and (Nurse *et al.* 2015), emphasized the forensic value of headers and technical email information. Sender and recipient information and timestamps in the present study supported reconstruction of communication history, while message identifiers and attachment information added further evidential context. The use of SysTools Viewer differs from studies that compared multiple forensic suites. (Devendran *et al.* 2015), for example, showed that different forensic tools have different strengths and limitations. The present study does not establish that SysTools Viewer is superior to FTK, EnCase, MailXaminer, Aid4Mail, or other forensic suites. Instead, it demonstrates that the selected viewer was capable of examining the particular MBOX and OST datasets generated in this experiment. This distinction is important because a viewer should not be presented as a substitute for a complete forensic acquisition suite. The comparative platform analysis is relevant to the cloud-versus-local evidence problem identified in earlier email forensic research. Google Takeout requires an export operation and therefore reflects data available through that export, whereas Outlook's OST reflects synchronized local mailbox information. Consequently, an investigator should consider both the source platform and the acquisition state when interpreting whether an email can be recovered.

V. Conclusion

This study demonstrates a practical approach for the forensic recovery and examination of deleted email artifacts from Google Takeout and Microsoft Outlook using SysTools Viewer. Gmail data were exported in MBOX format and Outlook data were examined in OST format. In the experimental work, four sample deleted emails were reported as successfully recovered. Both environments preserved useful forensic information including

sender and recipient details, subjects, timestamps, headers, message identifiers, attachments, and mailbox organization. The comparison showed that the two platforms differ in acquisition method and storage architecture and that Outlook provided additional platform-specific artifacts such as CC/BCC information, read/unread status, message size, and native folder hierarchy. The findings also indicate that deleted-email recovery is condition-dependent and should be interpreted in relation to export timing, synchronization status, storage format, and deletion method. The contribution of the present work is therefore not the development of a new forensic tool, but the practical comparative examination of two email environments through a consistent forensic workflow.

References

- [1]. Al-Makkawi, T., Alsarhan, A., Al-Na'amneh, Q., Aljaidi, M., Almaiah, M., AlJamal, M., Alqura'n, R., & Aljawarneh, M. (2025). Open-source forensics tools for recovery of deleted data in unconventional ways. In *Cryptography, biometrics, and anonymity in cybersecurity management. IGI Global*.
- [2]. Banday, M. T. (2011). Techniques and tools for forensic investigation of e-mail. *International Journal of Network Security & Law*, 3(6), 227–241.
- [3]. Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A comparative study of email forensic tools. *Journal of Information Security*, 6(2), 111–117.
- [4]. Fairbanks, J. (2024). POST: Email archival, processing and flagging stack for incident responders.
- [5]. Fagalde, K. (2006). Forensic processing of Outlook email: Recovering deleted email files and messages. *Guidance Software User Conference Proceedings*.
- [6]. Ghafarian, A., Mady, A., & Park, K. (2020). An empirical analysis of email forensics tools. *International Journal of Network Security & Its Applications*, 12(3), 1–15.
- [7]. Hadjidj, R., Debbabi, M., Lounis, O., Ghorbani, A., & Benredjem, D. (2009). Towards an *integrated e-mail forensic analysis framework*. *Digital Investigation*, 6(3–4), 124–137.
- [8]. Hamdi, S. D., & Radhi, A. M. (2019). Integrated cyber forensic for e-mail analysis framework. *International Journal of Computer Science and Information Security*, 17(5), 104–112.
- [9]. Hatole, P. P., & Bawiskar, S. K. (2017). Literature review of email forensics. *Imperial Journal of Interdisciplinary Research*, 3(4).
- [10]. Iqbal, F., Binsalleeh, H., Fung, B. C. M., & Debbabi, M. (2010). Mining writeprints from anonymous e-mails for forensic investigation. *Digital Investigation*, 7(1–2), 56–64.
- [11]. Jeong, C., Lee, K.-G., & Lee, S. (2011). Recovery techniques for deleted email items in digital forensic context. *Communications in Computer and Information Science*, 185, 115–122.
- [12]. Joshi, V., & Vinodkumar. (2025). Analyzing the effectiveness of email forensic software in cybercrime detection. *KSV E-Journal*, 2(1).
- [13]. Kayarkar, P. V., Ricchariya, P., & Motwani, A. (2013). Review on email forensics using sequence mining. *International Journal of Engineering Research & Technology*, 2(12).
- [14]. Meyer, A., & Roy, S. (2019). Do metadata-based deleted-file-recovery (DFR) tools meet NIST guidelines? *Digital Investigation*, 28, S132–S140.
- [15]. Mrityunjay, Chauhan, U., & Gupta, S. (2017). Novel approach for email forensics. *International Journal of Engineering Research & Technology*, 5(10), ICCCS-2017.
- [16]. Nikkel, B. (2004). E-mail authentication and forensic analysis. *Digital Investigation*, 1(3), 223–233.
- [17]. Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G., & Whitty, M. (2015). Investigating the leakage of sensitive personal and organisational information in email headers. *Journal of Internet Services and Information Security*, 5(1), 22–40.
- [18]. Singh, V. N., & Shalini. (2013). Forensic investigation of email artefacts by using various tools. *International Journal of Engineering Research & Technology*, 2(12).
- [19]. Stadlinger, J., & Dewald, A. (2017). A forensic email analysis tool using dynamic visualization. *Journal of Digital Forensics, Security & Law*, 12(1), 7–14.
- [20]. Tiwari, L. K., Samaddar, S., & Dwivedi, C. K. (2020). E-mail forensics for real life application in evidence building. *International Journal of Advanced Research in Computer Science*, 11(3), 34–38.