International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/51k68z79

Article – e003

A Critical Review of Evidence Acquisition and Preservation in Software-as-a-Service Environments: Customer-Controlled Forensic Capabilities and Provider Dependencies

Brian Mwangi[1] ✉, Peter Kamau[2]

[1,2] Student, Master of Science, University of Nairobi, Kenya

Received: 20/08/2026 **Revision Received:** 20/09/2026 **Accepted:** 29/09/2026

ABSTRACT

Software-as-a-Service (SaaS) environments present distinctive challenges for digital forensic investigations because customers generally control user accounts, organizational configurations, and selected audit capabilities but do not control the underlying infrastructure. Consequently, the availability, completeness, and preservation of forensic evidence depend on both customer-managed settings and provider-operated systems. This critical narrative review examines the forensic implications of that division of control, focusing on evidence generation, accessibility, retention, preservation, and reliability. It evaluates the limitations of customer-accessible audit records, the significance of provider-controlled evidence, and the difficulties associated with acquisition through administrative interfaces and application programming interfaces. We distinguish routine administrative export from defensible forensic preservation and examine how licensing, retention settings, application design, and provider cooperation shape an investigation. A five-dimensional analytical framework is proposed to assess whether an organization can generate, access, retain, preserve, and substantiate evidence relevant to an incident. The framework can support forensic readiness assessments and incident investigations, but it is not a validated numerical scoring system. The analysis demonstrates that customer access to SaaS audit functionality does not establish complete forensic visibility and that reliable investigation requires a documented understanding of evidentiary boundaries, collection procedures, and provider dependencies.

KEYWORDS: Software-as-a-Service; cloud forensics; digital evidence; forensic readiness; audit logs; evidence preservation; chain of custody; cloud service providers

1 Introduction

Cloud computing has changed the location, administration, and ownership of information systems used by organizations. Under the Software-as-a-Service model, customers access provider-hosted applications while the provider manages substantial portions of the supporting infrastructure, software deployment, and service operations. Customers no longer need to run the application infrastructure themselves, but they also lose much of the access needed to acquire and preserve digital evidence. Traditional forensic investigations may involve direct examination of storage devices, operating systems, memory, network infrastructure, and application logs. In SaaS environments, customers commonly lack equivalent access to the underlying systems. Instead, they rely on administrative interfaces, application programming interfaces (APIs), audit exports, retention controls, and provider assistance.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

The central challenge is not simply that evidence resides in the cloud. It is that the authority to generate, retain, access, and preserve evidence is distributed between the customer and the service provider. A customer may possess administrative privileges within an application but remain unable to examine provider-side authentication processing, backend service activity, infrastructure logs, or internal event-processing mechanisms. Even evidence exposed through a customer-facing interface may be subject to licensing restrictions, configurable retention periods, pagination limits, delayed ingestion, or incomplete event coverage. Those limits affect investigations of unauthorized access, insider misuse, account compromise, data theft, and disputed user activity.

Cloud forensic literature has long identified challenges concerning evidence location, acquisition, integrity, and the dependence of investigators on cloud service providers. These concerns are particularly important in SaaS because customers typically possess less infrastructure-level visibility than users of Infrastructure-as-a-Service environments. Even so, not all SaaS investigations require unrestricted access to provider infrastructure. Customer-accessible evidence may be sufficient to establish particular facts, provided that the evidence is relevant, complete enough for the question being examined, and collected through a defensible process. The principal issue is therefore determining what can actually be established from the evidence available to the customer, rather than assuming that administrative access provides comprehensive forensic capability. We address five questions:

1. What categories of forensic evidence are ordinarily accessible to SaaS customers?
2. Which investigative activities depend on provider-controlled systems or cooperation?
3. How do audit configuration, licensing, and retention affect evidence availability?
4. What distinguishes administrative data export from defensible forensic acquisition and preservation?
5. How can organizations assess their practical forensic readiness before an incident occurs?

The article develops a five-dimensional framework covering evidence generation, accessibility, retention, preservation, and reliability.

2 Review Approach and Scope

2.1 Review design

We use a critical narrative review approach, synthesizing cloud forensic research, forensic acquisition studies, relevant technical standards, and published SaaS audit and retention documentation. The aim is not to calculate a pooled measure of forensic effectiveness. Instead, the review examines how the SaaS service model affects the availability and evidentiary value of customer-accessible information. The reviewed material encompasses general cloud forensic principles and SaaS-specific technical constraints. Findings from studies involving particular applications or service configurations are interpreted within their original contexts rather than generalized to all SaaS platforms.

2.2 Scope of analysis

We focus on investigations performed by or on behalf of a SaaS customer. Relevant evidence includes application audit records, identity and access events, administrative changes, user activity records, application content, available version histories, and exports produced through supported customer interfaces. Provider-controlled evidence is considered where its absence or availability affects the conclusions an investigator can reasonably draw. We do not assume that customers possess unrestricted access to infrastructure-level artifacts, hypervisor data, physical storage, or provider-internal logs.

2.3 Analytical distinctions

The analysis separates five questions that are often treated as interchangeable:

1. Was a relevant event recorded?
2. Can the customer retrieve the record?

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

3. Will the record remain available for the required period?
4. Can the record be preserved in a defensible manner?
5. Can its meaning, provenance, and integrity be adequately established?

Those questions guide the framework developed below.

2.4 Limitations of the review approach

We did not conduct a systematic review or meta-analysis, and the proposed framework has not yet been validated as a standard assessment tool. Provider capabilities and retention policies may also change over time. Product-specific statements must be interpreted according to the applicable service, license, configuration, and documentation version.

3 SaaS Architecture and the Division of Forensic Control

3.1 Customer-controlled resources

In SaaS environments, customers generally control some combination of user identities, organizational policies, role assignments, application configuration, stored content, and administrative audit functions. The precise scope of this control varies by product and subscription. Customer administrators may be able to retrieve sign-in events, inspect account changes, export documents, review sharing activity, or configure selected retention policies. Such access can be valuable during an investigation. Yet administrative authority within the application should not be confused with ownership or control of the underlying infrastructure.

3.2 Provider-controlled resources

The provider generally controls application hosting, backend services, infrastructure maintenance, and internal operational monitoring. Depending on the service, the provider may also control the generation, processing, filtering, and storage of audit events that are subsequently exposed to customers. Investigators therefore depend on the provider for part of the evidence. A customer may receive an audit record describing an event without access to the systems that originally generated the record or the internal processes through which it was processed. The investigator must therefore evaluate the record's documented semantics and collection context rather than presume complete visibility into its creation.

3.3 Shared responsibility and forensic responsibility

The shared-responsibility concept is commonly used to explain security obligations in cloud computing. Still, responsibility for securing a system does not always imply the ability to investigate every aspect of that system. A customer may be responsible for configuring identity controls while depending on the provider for access to particular authentication records. Likewise, a provider may maintain the infrastructure while offering customers only a limited set of application-level audit events. Forensic responsibility must be evaluated in terms of actual evidentiary capability.

3.4 Implications for investigative conclusions

The division of control affects the strength of conclusions investigators can reach. For example, an application audit record may establish that a particular account performed a recorded operation. It may not, without additional evidence, establish the identity of the human operator, the condition of the endpoint, or the complete sequence of backend actions. A missing audit event may reflect inactivity, but it may also reflect disabled logging, limited event coverage, retention expiry, or incomplete access. Investigative reports should distinguish these possibilities.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

4 Customer-Accessible Evidence Sources

4.1 Application audit records

Application audit records are among the most important evidence sources available to SaaS customers. Depending on the service, such records may describe user authentication, file access, document sharing, administrative changes, permission modifications, and other supported activities. Audit records can help investigators establish sequences of events, identify affected accounts, and correlate activity across users and applications. At the same time, audit functionality is not necessarily comprehensive. Different products may record different event categories, and a single product may expose additional records only under particular licensing or configuration conditions.

Pichan, Lazarescu, and Soh [1] identify the forensic difficulties associated with cloud logging, including collection complexity, volatility, authenticity, and the distributed location of log sources. Their analysis demonstrates why the existence of logging infrastructure does not automatically ensure that investigators can obtain all relevant records. Marty [2] similarly treats logging as a proactive design requirement: applications must generate and retain records that answer anticipated investigative questions before an incident occurs. This is particularly important in SaaS, where a customer cannot later reconstruct provider-side events that were never exposed or recorded.

4.2 Application content and version histories

Customer-accessible content can provide evidence of the information stored or exchanged through a SaaS application. Examples include documents, messages, attachments, and application-specific records. Where supported, version histories may help establish changes to content over time. Yet an exported current document and a complete history of actions affecting that document are different forms of evidence. A file export may preserve its present contents without reproducing every earlier version, sharing event, or administrative operation. Investigators must therefore determine whether the acquired material represents a current state, a historical state, or a sequence of recorded changes.

Quick and Choo [3] investigated the collection of data from Dropbox, Google Drive, and Microsoft SkyDrive through browser and client-based methods. Their experiments found no changes to file contents during upload, storage, and download in the tested services. However, they also demonstrated the importance of interpreting file timestamps in relation to the collection method and service behavior. The correct conclusion is not that cloud acquisition necessarily alters file contents. Rather, file-content integrity and metadata interpretation must be evaluated separately. Martini and Choo's ownCloud experiments [4] further demonstrate that relevant cloud-storage evidence may be distributed across client and server artifacts. Because their study involved an open-source storage service with access to both sides of the environment, its acquisition opportunities cannot be assumed to exist in provider-operated SaaS platforms.

4.3 Identity and access evidence

Identity-related records may provide information about account authentication, sign-in activity, access attempts, and administrative changes. Identity records are especially useful when an account may have been compromised or used without permission. Still, an authentication event is not proof of the identity of the individual operating the account. Credentials may be shared, stolen, or used through compromised devices. Also, SaaS applications may depend on external identity providers, creating additional evidentiary sources outside the application itself. An investigation may therefore require correlation between application activity, identity-provider records, endpoint evidence, and other available information.

4.4 Endpoint artifacts associated with SaaS applications

Although SaaS infrastructure is provider-operated, client devices may retain locally accessible artifacts associated with application activity. Such artifacts may include cached content, application databases, configuration information, and traces of communications. Bowling et al. [5] examined Microsoft

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Teams artifacts on Windows, Android, and iOS devices. In their tested environment, manual examination partially or fully recovered 77.6% of populated artifacts, whereas the automated forensic tools recovered 13.8%. The reported percentages apply only to the applications, devices, artifacts, and tools tested in that study. They are not general recovery rates for SaaS platforms. The study demonstrates that customer-side or endpoint acquisition can supplement cloud-accessible evidence, while also showing that automated forensic tools may not identify all recoverable artifacts.

4.5 Evidence correlation

Different evidence sources may describe related events from different perspectives. An application audit record may identify a document access operation, while an identity record may describe the authentication session associated with the account. Endpoint artifacts may provide further contextual information. Correlating these sources can strengthen an investigation, but correlation requires careful attention to timestamps, identifiers, event semantics, and the possibility of missing records. The existence of multiple records does not establish their independence, particularly when they originate from a common provider-controlled event-processing system.

5 Evidence Accessibility and Acquisition Constraints

5.1 Administrative interfaces

Many SaaS services provide administrative portals through which authorized users can search and export selected records. Administrative interfaces can provide useful evidence during incident response. At the same time, their investigative limitations should be evaluated before an incident. Search restrictions, export limits, available filters, event coverage, and account permissions can influence the completeness of collected material. A successful export confirms that a particular dataset was retrieved through the interface. It does not establish that the dataset contains every relevant event.

5.2 API-based acquisition

APIs may allow investigators to retrieve application content and audit information programmatically. Compared with manual portal exports, API-based acquisition may support repeatable collection procedures and systematic processing of larger datasets. Still, APIs can impose pagination, request limits, permissions, query restrictions, and restrictions on historical data. A collection process must therefore account for incomplete pages, failed requests, retry behavior, and changes to records during collection. Investigators should document the API endpoint, query parameters, time range, account permissions, response status, and collection time. Where supported, the collection should retain original responses as well as normalized analytical copies.

The completeness of an API collection must be established through the documented behavior of the interface and the results of the collection procedure, not inferred merely from a successful response.

5.3 Provider-controlled evidence

Some potentially relevant information may not be exposed through customer interfaces. Provider-only evidence may include internal service logs, backend processing events, infrastructure records, and information kept only in provider-operated systems. The availability of such evidence may depend on contractual arrangements, provider policy, legal processes, and the technical ability of the provider to retrieve it. Pichan, Lazarescu, and Soh [6] examine broader cloud forensic challenges involving technical access and investigative dependencies. Their analysis reinforces the importance of distinguishing the theoretical existence of evidence from the practical ability to acquire it.

NISTIR 8006 organizes cloud-forensic challenges across technical, organizational, and legal categories and specifically identifies problems involving data collection, logging, time, location, integrity, and provider dependence [7]. These broader findings explain why customer-facing SaaS exports represent only one part of the potential evidence environment.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

5.4 Trust in provider-mediated acquisition

Dykstra and Sherman [8] examined the technical and trust issues associated with forensic acquisition in Infrastructure-as-a-Service environments. Although their study concerns a different cloud service model, its discussion of trust boundaries is relevant to SaaS investigations. Where an investigator cannot directly observe the underlying evidence source, confidence in the acquired material depends partly on the systems and processes used to produce it. Yet techniques evaluated for Infrastructure-as-a-Service cannot be transferred directly to SaaS. The customer-accessible control plane, available artifacts, and provider responsibilities differ.

5.5 Access limitations and investigative uncertainty

The inability to retrieve a record may have several explanations. The event may never have been generated, may not be exposed to the customer, may have expired, or may be inaccessible because of permissions or subscription restrictions. Each possibility leads to a different evidentiary conclusion. Investigators should therefore avoid equating unsuccessful retrieval with evidence that the underlying activity did not occur. An explicit account of inaccessible or unavailable evidence is essential to the transparency of forensic conclusions.

6 Retention and the Risk of Evidence Loss

6.1 Retention as a forensic constraint

Retention determines how long records remain available through the relevant service or storage mechanism. In SaaS environments, retention may be influenced by provider defaults, subscription level, customer configuration, and the category of evidence involved. Different records within the same service may have different retention periods. As a result, a general statement that a SaaS platform retains audit data for a particular duration may be misleading unless the relevant event types and conditions are specified.

6.2 Retention and delayed incident discovery

An incident may be discovered after relevant records have expired. Retention matters most when unauthorized access continued for a long time, detection was delayed, or investigators must reconstruct older account activity. The fact that an organization currently has access to an audit feature does not establish that records from the relevant historical period remain available. Retention capability must be evaluated before an incident, and collection should begin promptly when relevant activity is identified.

6.3 Product-specific retention differences

Microsoft Purview illustrates the importance of distinguishing product capabilities from general SaaS characteristics. Microsoft documentation states that the default retention period for Audit (Standard) changed from 90 to 180 days for records generated on or after October 17, 2023. Audit (Premium) provides longer retention for qualifying records, including a one-year default for specified workloads and appropriately licensed users. Other records may retain the 180-day default unless a suitable policy applies. The applicable retention period therefore depends on record type, licensing, generation date, and relevant policies [9]. The figures are not universal retention periods for Microsoft 365 data, and they cannot be generalized to SaaS services as a whole.

6.4 Independent evidence retention

Where technically and contractually permitted, organizations may export relevant audit records to independently managed storage. Independent storage reduces reliance on the provider's default searchable retention period. Still, independent retention is effective only if collection occurs before the source records expire and the export captures the required event categories. A centralized logging system cannot reconstruct events that were never generated or were unavailable through the collection

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

interface. Organizations should therefore validate both the coverage and the continuity of their collection processes.

6.5 Retention does not establish preservation

Routine retention and forensic preservation serve different purposes. Retention maintains records for an operationally or administratively defined period. Forensic preservation seeks to protect identified evidence from alteration or loss while maintaining sufficient information about its acquisition and subsequent handling. A retained record may still be deleted when its retention period expires unless an appropriate preservation mechanism is applied. Conversely, a downloaded copy may preserve particular contents while failing to capture their complete context. Keeping acquisition, preservation, and export separate is central to a sound evidentiary assessment.

7 Forensic Preservation and Chain of Custody

7.1 Acquisition versus preservation

Acquisition involves obtaining data from an identified source. Preservation involves maintaining the acquired evidence and its relevant context in a manner that supports later examination and evaluation. An administrative export may constitute an acquisition method, but its evidentiary adequacy depends on how the data were selected, retrieved, documented, and maintained. NIST SP 800-86 [10] provides guidance for integrating forensic techniques into incident response, including the importance of systematic evidence handling. Its general principles remain relevant to SaaS, although cloud-specific acquisition constraints require additional consideration.

Martini and Choo [11] proposed an iterative cloud-forensic framework that separates preservation from collection and adapts conventional forensic processes to cloud constraints. For SaaS investigations, that distinction supports documenting both the provider-controlled source and the customer-controlled act of export or acquisition.

7.2 Collection documentation

A defensible SaaS collection process should record the source service, tenant or organizational context, collecting account, permissions, collection method, time range, and date of acquisition. Where an API is used, relevant request parameters and response information should also be retained. The aim is to make the collection process understandable and, where possible, reproducible. At the same time, reproducibility may be limited when source records change or expire. Documentation must therefore distinguish a repeatable collection procedure from a guarantee that the same source data will remain available.

7.3 Integrity verification

Cryptographic hashes can help demonstrate whether acquired files have changed after hashing. They do not, by themselves, prove that the source data were complete, accurate, or unaltered before collection. The difference matters for provider-generated audit records because the investigator did not create the source data. A hash can protect the integrity of the exported record from a particular point onward, but it does not independently verify the provider's internal event-generation process. Integrity assessment must therefore include provenance and collection context as well as post-acquisition protection.

7.4 Chain of custody

Chain-of-custody documentation records the handling and transfer of evidence. In SaaS investigations, this may include the acquisition account, export operation, receiving storage location, subsequent transfers, and access to preserved copies. A complete chain of custody supports accountability and helps establish how evidence was handled. Yet it cannot compensate for missing source records or undocumented limitations in the acquisition method.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

7.5 Time and metadata interpretation

Timestamp interpretation is particularly important when data are obtained through cloud interfaces. The time associated with an event may represent its occurrence, ingestion, modification, export, or another system-defined operation. Quick and Choo [3] demonstrated why collection-related timestamp behavior requires careful examination. Investigators should preserve available original metadata and document any transformations performed during analysis. Where timestamps from multiple systems are correlated, the relevant time zones, precision, and event definitions should be considered.

8 Reliability and Evidentiary Interpretation

8.1 Authenticity and provenance

Evidence reliability depends partly on establishing where a record originated and how it was produced. A provider-generated audit record may carry useful event identifiers and timestamps, but investigators should understand the documented meaning of its fields. The presence of an account identifier does not establish the identity of the person responsible for an action. In the same way, a record of successful access may not independently establish what information a user actually viewed or understood.

8.2 Completeness

Completeness concerns whether the available records adequately represent the activity relevant to an investigative question. It is not necessarily possible to demonstrate absolute completeness in a SaaS environment. The investigator may lack access to provider-internal evidence or may be unable to determine whether particular event categories were recorded. For this reason, completeness should be assessed relative to the specific question being investigated.

8.3 Consistency and corroboration

Evidence from different sources can provide corroboration. For example, identity records, application audit events, and endpoint artifacts may collectively support an account of suspicious activity. Still, inconsistencies may arise from different timestamp definitions, asynchronous logging, incomplete coverage, or changes in application behavior. Investigators should examine these explanations before treating discrepancies as evidence of malicious activity.

8.4 Reliability of automated tools

Automated forensic tools can assist with collection and interpretation, but their results depend on supported applications, artifact formats, and software versions. The Microsoft Teams investigation by Bowling et al. [5] demonstrates that manual examination recovered artifacts that the tested automated tools did not identify. The result does not mean that manual examination is always better. It establishes that tool performance must be assessed against the relevant application, environment, and artifact types.

8.5 Reporting evidentiary limitations

Forensic reports should distinguish established observations from inferences. They should identify relevant unavailable records, collection restrictions, retention gaps, and uncertainties concerning event attribution. A conclusion should not be expressed with greater confidence than the supporting evidence permits. Clear reporting matters when investigators rely on provider-generated records but cannot inspect the systems that created them.

9 A Five-Dimensional Framework for SaaS Forensic Capability

9.1 Framework rationale

The reviewed evidence indicates that SaaS forensic capability cannot be adequately described by a single question such as whether audit logging is enabled. An organization may generate relevant

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

records but lack access to them. It may have access but retain them for an insufficient period. It may retain records but lack a defensible preservation process. Alternatively, it may preserve records successfully while being unable to establish their meaning or completeness. The proposed framework therefore separates five dimensions:

1. Evidence generation.
2. Evidence accessibility.
3. Evidence retention.
4. Evidence preservation.
5. Evidence reliability.

The five dimensions are related, but each answers a different question. The NIST Cloud Computing Forensic Reference Architecture describes forensic readiness at a broader level [12]. The framework proposed here narrows the assessment to capabilities that a SaaS customer can actually use. It also complements organizational readiness research. Alenezi, Atlam, and Wills [13] group readiness factors into technological, legal, and organizational dimensions. Their work is primarily IaaS-focused and does not validate the five dimensions proposed here, but it supports assessing readiness before an incident rather than assuming that evidence will be obtainable afterward.

9.2 Dimension 1: Evidence generation

Evidence generation concerns whether the SaaS service records activities relevant to an investigation. The principal question is whether the required events are produced at all. For example, an investigation into unauthorized file sharing may require records of sharing-link creation, permission changes, and file access. A service that records sign-ins but not relevant file operations may be insufficient for this investigation. The assessment should therefore identify the required event categories and compare them with documented logging coverage.

9.3 Dimension 2: Evidence accessibility

Evidence accessibility concerns whether the customer can retrieve the relevant records. Accessibility covers administrative permissions, supported interfaces, licensing restrictions, and access to historical data. The existence of provider-side logs does not establish customer accessibility. Where access requires provider cooperation, that dependency should be documented.

9.4 Dimension 3: Evidence retention

Evidence retention concerns whether relevant records remain available for the required investigative period. The assessment should identify applicable retention periods and determine whether they align with likely detection and investigation delays. It should also distinguish provider-managed retention from independently maintained copies. A long retention period for one record category cannot be assumed to apply to all categories.

9.5 Dimension 4: Evidence preservation

Evidence preservation concerns the ability to protect acquired records and document their handling. Relevant considerations include export procedures, preservation of original formats, integrity verification, acquisition documentation, access controls, and chain of custody. The ability to download a file does not establish that all associated metadata and historical context have been preserved.

9.6 Dimension 5: Evidence reliability

Evidence reliability concerns whether the acquired material can support defensible conclusions. The assessment should consider provenance, event semantics, timestamp interpretation, completeness, consistency, and opportunities for corroboration. A reliable collection process cannot establish facts that the available records do not contain. Likewise, the presence of multiple records does not eliminate the need to assess their origin and interpretation.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

9.7 Framework summary

Dimension	Principal assessment question	Representative evidence
Generation	Are relevant activities recorded?	Audit event coverage and logging configuration
Accessibility	Can the customer obtain the records?	Portal permissions, API capabilities, export restrictions
Retention	Will the records remain available?	Retention policies, licensing, independent log storage
Preservation	Can the records be protected and documented?	Acquisition records, hashes, original exports, custody documentation
Reliability	Can the records support defensible conclusions?	Provenance, event definitions, metadata, corroboration

9.8 Relationships between dimensions

The five dimensions are not independent in practice. For example, the absence of evidence generation makes subsequent accessibility and preservation impossible for that event category. Insufficient retention can prevent acquisition even where access permissions are adequate. A preservation procedure may protect an export without resolving uncertainty about its completeness. The framework should be applied to specific investigative questions rather than used as a generic checklist of product features.

9.9 Why a numerical score is not proposed

The dimensions do not have established empirical weights. It would be unjustified to assume that a particular improvement in retention compensates for missing evidence generation or that enhanced accessibility offsets unreliable event attribution. The framework supports domain-level assessment rather than a composite numerical score. Its usefulness requires future empirical evaluation.

10 Illustrative Application to a SaaS Account-Compromise Investigation

10.1 Investigation scenario

Consider an organization investigating suspected unauthorized access to a SaaS collaboration account. The organization needs to determine whether the account was accessed without authorization, whether documents were shared externally, and whether relevant content was downloaded. The hypothetical case shows how the framework can organize evidence collection and interpretation.

10.2 Assessing evidence generation

Investigators first determine which authentication, file-access, sharing, and administrative events the service records. They examine the relevant audit documentation and organizational configuration. If file-download events are not generated or are unavailable under the current subscription, that limitation is recorded.

10.3 Assessing accessibility

Investigators identify the interfaces through which relevant records can be retrieved. They determine whether administrative permissions permit access to the required events and historical periods. Where records are available only through provider cooperation, the dependency is identified separately.

10.4 Assessing retention

The investigation establishes whether records remain available for the suspected compromise period. If the relevant events occurred before the applicable retention window, the investigator examines whether independently retained copies exist. An absence of accessible historical records is not treated as proof that no suspicious activity occurred.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

10.5 Assessing preservation

Available records are acquired using documented procedures. The collection process records the relevant time ranges, search parameters, source interfaces, and collection timestamps. Original exports are protected, and subsequent analytical transformations are documented.

10.6 Assessing reliability

The investigator correlates application activity with identity records and available endpoint evidence. A recorded account sign-in may support the conclusion that an account was accessed, but attribution to a particular individual requires additional evidence. Likewise, a sharing event may establish that access permissions were modified without necessarily proving that a recipient viewed the content.

10.7 Investigative conclusion

Using the framework, investigators can separate questions that the available evidence can answer from those that remain unresolved. Its principal value is not to eliminate uncertainty but to make evidentiary capabilities and limitations explicit.

11 Critical Synthesis of the Literature

11.1 Established findings

The literature consistently identifies limitations associated with the distribution of forensic control in cloud computing. Pichan, Lazarescu, and Soh [6] examine technical challenges arising from cloud architecture, while their later logging study [1] addresses the practical difficulties of collecting and using cloud log artifacts. Dykstra and Sherman [8] demonstrate that cloud acquisition raises questions concerning trust and the investigator's dependence on systems outside direct control. Quick and Choo [3] show that cloud collection methods require careful interpretation of metadata, while Bowling et al. [5] demonstrate the value of examining client-side artifacts and the limitations of the tested automated forensic tools.

NIST's cloud forensic reference architecture [12] provides a broader foundation for examining forensic readiness. NISTIR 8006 [7] supplies a detailed challenge taxonomy, while Martini and Choo [11] distinguish preservation and collection within a cloud-specific process. Their ownCloud case study [4] and Marty's logging work [2] add empirical and design-oriented evidence concerning distributed artifacts and proactive log generation. Alenezi et al. [13] further show that organizational readiness includes technological, legal, and organizational preparation. Together, these sources support the conclusion that SaaS forensic capability must be assessed in relation to actual evidence sources, collection methods, and control boundaries.

11.2 Important differences between studies

The studies cover different technical environments. Research concerning Infrastructure-as-a-Service acquisition addresses capabilities that SaaS customers may not possess. Cloud storage investigations focus on particular forms of content and metadata. Client-device studies investigate artifacts retained outside the provider's infrastructure. Cloud logging research addresses broader challenges involving event collection and interpretation. Differences in service model, platform, tools, and access make direct comparison difficult. A successful acquisition technique in one environment does not establish its effectiveness in another.

11.3 Evidence gaps

Several areas require further empirical investigation. First, there is a need for reproducible comparisons of customer-accessible forensic capabilities across major SaaS applications. Second, the completeness of customer-facing audit records requires more systematic examination. Third, acquisition methods should be evaluated for their ability to preserve event semantics, metadata, and historical context. Fourth, investigations should examine the consequences of changes to product licensing, logging

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

behavior, and retention policies. Finally, further research is needed to evaluate the extent to which provider-generated records can be independently corroborated.

11.4 Comparative synthesis

Source	Main contribution	Relevance to SaaS investigations	Limitation
Pichan et al. [1]	Practical cloud logging challenges	Audit availability and usability	Broader cloud context
Quick and Choo [3]	Cloud storage acquisition and metadata	Content and timestamp interpretation	Specific tested services
Bowling et al. [5]	Microsoft Teams endpoint artifacts	Client-side evidence and tool limitations	Specific platforms and tools
Pichan et al. [6]	Cloud forensic challenges and solutions	Control and acquisition constraints	Not exclusively SaaS
Dykstra and Sherman [8]	Acquisition trust boundaries	Provider-mediated evidence	Infrastructure-as-a-Service focus
Microsoft [9]	Product audit retention behavior	Licensing and retention dependencies	Product-specific and changeable
Kent et al. [10]	Forensic procedures in incident response	Collection and preservation principles	General rather than SaaS-specific
Herman et al. [12]	Cloud forensic readiness architecture	Structured capability assessment	Broader cloud architecture
Herman et al. [7]	Cloud-forensic challenge taxonomy	Collection, logging, integrity, and provider dependencies	Broader cloud ecosystem
Martini and Choo [11]	Cloud-specific forensic process	Preservation and collection distinctions	Conceptual framework
Martini and Choo [4]	ownCloud acquisition experiments	Distribution of client and server artifacts	Open-source storage case study
Marty [2]	Proactive cloud application logging	Evidence generation and log design	Requires provider or developer participation
Alenezi et al. [13]	Organizational readiness factors	Technological, legal, and organizational preparation	Primarily IaaS-focused

12 Implications for SaaS Forensic Readiness

12.1 Establishing an evidence inventory

Organizations should identify the SaaS services that support important business processes and determine the evidence available from each service. The inventory should distinguish application content, audit events, identity records, administrative changes, and client-side artifacts. For each category, the organization should document the relevant access method and known limitations. A tested evidence inventory reduces uncertainty during an incident.

12.2 Validating logging coverage

Forensic readiness requires more than enabling an audit feature. Organizations should determine whether the events necessary for anticipated investigations are actually recorded. Where feasible, controlled tests can establish whether particular activities generate the expected audit records. Such tests should account for differences between documented capabilities and actual configurations.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

12.3 Aligning retention with investigative needs

Retention settings should be evaluated against realistic detection and investigation periods. Organizations should also determine whether independent collection is necessary to preserve records beyond provider defaults. The relevant retention policy should be verified for each event category rather than assumed from general product descriptions.

12.4 Preparing acquisition procedures

Investigative procedures should identify authorized collecting accounts, supported export methods, API requirements, and preservation steps. Where APIs are used, procedures should account for pagination, failures, request limits, and record normalization. The aim is to reduce the risk of incomplete or poorly documented collection during time-sensitive incidents.

12.5 Defining provider dependencies

Organizations should understand what evidence cannot be obtained directly. Contractual arrangements and support processes may influence whether additional records can be requested. At the same time, a contractual right to request assistance should not be equated with a guarantee that every desired artifact exists or can be retrieved.

12.6 Exercising forensic readiness

Periodic exercises can test whether relevant records are generated, accessible, and preservable. Exercises may also reveal limitations in permissions, retention, tooling, and documentation. Organizations should repeat these assessments after major application or licensing changes.

13 Research Gaps and Future Directions

13.1 Standardized capability assessments

Future research should develop reproducible methods for evaluating SaaS forensic capability. Such methods should distinguish provider-advertised features from experimentally demonstrated acquisition capabilities.

13.2 Audit completeness and event semantics

More research is needed into the relationship between user activity and customer-visible audit events. Controlled studies could examine whether relevant operations consistently produce records and whether those records preserve sufficient context for forensic interpretation.

13.3 Preservation through APIs

Future investigations should evaluate the completeness and repeatability of API-based acquisition across different SaaS platforms. Particular attention should be given to pagination, historical retrieval, metadata transformations, and the handling of partially failed collections.

13.4 Independent corroboration

Research should examine methods for correlating SaaS audit events with identity, endpoint, and other independently available records. This could improve confidence in event attribution and help identify limitations in provider-generated evidence.

13.5 Framework validation

The proposed five-dimensional framework requires empirical validation. Future studies should evaluate whether it improves the identification of evidence gaps, the consistency of readiness assessments, and the quality of investigative reporting. Until that evaluation is complete, the framework remains a guide rather than a validated measurement scale.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

14 Discussion

The principal finding of this review is that SaaS forensic capability is determined by more than the availability of audit logs or administrative export functions. The division of control between customers and providers influences which events are recorded, which records are accessible, how long they remain available, and whether they can be preserved and interpreted reliably. The literature demonstrates that cloud forensic acquisition is affected by technical architecture and trust boundaries [6,8]. It also demonstrates that evidence collection requires careful attention to metadata and application-specific behavior [3,5]. The findings matter in SaaS because customers usually cannot inspect the infrastructure behind the application. The distinction between evidence generation and evidence accessibility is especially important.

A provider may maintain internal records that are unavailable to customers. Conversely, a customer may possess extensive administrative permissions but lack access to events that the service does not expose. In the same way, retention and preservation must be treated separately. Records may be searchable for a defined period without being protected against expiration during a subsequent investigation. The Microsoft Purview example [9] illustrates how retention depends on product-specific conditions, including licensing and record categories. Provider policies, licensing, and retention settings can determine what evidence still exists when an incident is found. Evidence reliability presents an additional challenge. An acquired record may be protected against subsequent alteration while its completeness or original event semantics remain uncertain.

Forensic integrity therefore involves more than applying a cryptographic hash to an exported file. Investigators must also evaluate provenance, acquisition context, and the conclusions that the available evidence can reasonably support. The proposed five-dimensional framework brings these considerations together. Its contribution is to distinguish evidence generation, accessibility, retention, preservation, and reliability as separate requirements for effective investigation. In practice, the approach gives organizations a clearer view of their forensic readiness and reduces the risk of overstating what they can investigate. Yet the framework remains conceptual. Its effectiveness must be evaluated through controlled studies and practical investigations involving different SaaS services.

15 Limitations

Several limitations should be noted. First, it uses a critical narrative approach and does not claim exhaustive coverage of the literature. Second, some foundational studies examine cloud service models other than SaaS. Their findings are used to explain relevant forensic principles rather than to establish identical technical capabilities across service models. Third, the behavior of individual SaaS applications may change with software updates, licensing arrangements, and provider policies. Fourth, the reviewed evidence includes studies of particular applications, devices, and forensic tools. Their findings should not be generalized beyond the conditions examined. Fifth, the proposed five-dimensional framework has not been empirically validated. Finally, the review does not establish a universal legal standard for evidence admissibility. Legal requirements vary across jurisdictions and investigative contexts.

16 Conclusion

Software-as-a-Service environments create distinctive forensic challenges because customers depend on provider-operated systems for the generation, storage, and exposure of potentially relevant evidence. Customer-accessible audit records, application content, identity information, and endpoint artifacts can support meaningful investigations, but their availability does not establish comprehensive forensic visibility. The critical distinction is between evidence that exists, evidence that the customer can retrieve, evidence that remains available, evidence that can be preserved, and evidence that can support defensible conclusions. The five-dimensional framework proposed in this review organizes these requirements into evidence generation, accessibility, retention, preservation, and reliability.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

It provides a structured basis for assessing practical SaaS forensic capability while making provider dependencies and investigative limitations explicit. Future research should prioritize reproducible assessments of SaaS audit coverage, API-based acquisition, metadata preservation, and independent corroboration. Effective SaaS forensic readiness ultimately requires organizations to understand not only which security features a service provides, but also what evidence those features can actually produce and preserve when an investigation becomes necessary.

REFERENCES

[1] Pichan, A., Lazarescu, M., & Soh, S. T. (2018). Towards practical cloud forensics logging framework. Journal of Information Security and Applications, 42, 18–28. https://doi.org/10.1016/j.jisa.2018.07.008

[2] Marty, R. (2011). Cloud application logging for forensics. Proceedings of the 2011 ACM Symposium on Applied Computing, 178–184. https://doi.org/10.1145/1982185.1982226

[3] Quick, D., & Choo, K.-K. R. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? Digital Investigation, 10(3), 266–277. https://doi.org/10.1016/j.diin.2013.07.001

[4] Martini, B., & Choo, K.-K. R. (2013). Cloud storage forensics: ownCloud as a case study. Digital Investigation, 10(4), 287–299. https://doi.org/10.1016/j.diin.2013.08.005

[5] Bowling, H., Seigfried-Spellar, K., Karabiyik, U., & Rogers, M. (2023). We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems. Journal of Forensic Sciences, 68(2), 434–460. https://doi.org/10.1111/1556-4029.15208

[6] Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation, 13, 38–57. https://doi.org/10.1016/j.diin.2015.03.002

[7] Herman, M., Iorga, M., Salim, A. M., Jackson, R. H., Hurst, M. R., Leo, R. A., Lee, R., Landreville, N. M., Mishra, A. K., Wang, Y., & Sardinas, R. (2020). NIST Cloud Computing Forensic Science Challenges. NIST Interagency Report 8006. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8006

[8] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, S90–S98. https://doi.org/10.1016/j.diin.2012.05.001

[9] Microsoft. (n.d.). Manage audit log retention policies. Microsoft Learn. https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

[10] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

[11] Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71–80. https://doi.org/10.1016/j.diin.2012.07.001

[12] Herman, M., Iorga, M., Salim, A. M., Jackson, R. H., Hurst, M. R., Leo, R. A., Mishra, A. K., Landreville, N. M., & Wang, Y. (2024). NIST Cloud Computing Forensic Reference Architecture. NIST Special Publication 800-201. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-201

[13] Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. Journal of Cloud Computing, 8, 11. https://doi.org/10.1186/s13677-019-0133-z

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)