The Virtual Gaze: Decoding the Paradox of Elastic Evidence and Multi-Tenant Jurisdiction in 2026 Cloud Forensics

Amarnath M
Assistant Professor, Department of Digital and Cyber Forensic Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.

***Abstract*—The migration of global data infrastructures to virtualized environments has necessitated a fundamental evolution in Digital Forensic Science (DFS). This article examines the transition from the traditional "box-at-the-scene" model to a modern, log-centric approach dictated by the complexities of cloud architecture. As physical hardware becomes increasingly abstracted through Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, investigators must navigate unique challenges such as multi-tenancy, data fragmentation, and the inherent ephemerality of serverless instances. The study details a three-dimensional forensic framework—Technical, Organizational, and Legal—to address these complexities. It explores critical methodologies including snapshot analysis, API-based telemetry collection, and remote live forensics, which are essential for preserving the "Order of Volatility" in non-persistent environments. Furthermore, the article analyzes the "Jurisdictional Thicket," highlighting the legal deadlock between the extraterritorial reach of the U.S. CLOUD Act and the privacy mandates of the EU's GDPR and Brazil's LGPD. Ultimately, the paper argues that the future of DFS relies on a synthesis of AI-driven data reconstruction and a deep understanding of the Shared Responsibility Model. By mastering these virtualized frontiers, the forensic community ensures that the "binary witness" remains an objective narrator of human intent in an era of borderless, ephemeral data.**

Keywords*— *Cloud Forensics, Shared Responsibility Model, Ephemeral Instances, Jurisdictional Thicket.

I. INTRODUCTION: THE END OF THE PHYSICAL DRIVE

In traditional digital forensics, the investigative process is often tethered to the "box-at-the-scene" model. This approach is straightforward: an investigator physically seizes a hard drive, applies a hardware write blocker to prevent any accidental modification, and creates an exact bit-stream image for analysis. However, as of 2026, the mass migration to Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) has rendered this physical-centric model nearly obsolete for enterprise-level investigations.

The Shift from Physicality to Virtualization

In the cloud, the concept of a "drive" is a logical abstraction rather than a physical reality. Data is no longer confined to a single spinning platter or silicon chip under the investigator's hand. Instead, it is governed by three core cloud principles that disrupt traditional forensic acquisition:

a) Resource Pooling & Multi-Tenancy: On a single physical rack in a data center, the data of a suspect coexists with the data of thousands of innocent users. Traditional "bit-stream" imaging of the physical hardware is legally impossible, as it would constitute an unreasonable seizure of third-party privacy.

b) Data Fragmentation & Replication: To ensure high availability, cloud providers replicate data across multiple geographic regions. A single document might exist in fragments across servers in Virginia, Dublin, and Singapore, making the "location of evidence" a fluid, global concept.

c) On-Demand Self-Service (Elasticity): Cloud resources are "ephemeral." A virtual server can be spun up to launch a cyberattack and then "deprovisioned" seconds later. Once the instance is deleted, the underlying physical memory and storage blocks are immediately reallocated and overwritten, causing the evidence to evaporate instantly.

The New Forensic Frontier: API and Log-Centric Analysis

Because investigators can no longer "bag and tag" the hardware, the primary focus of Digital Forensic Science (DFS) has shifted toward orchestrated data reconstruction. Rather than examining "dead" files on a disk, 2026-era investigators focus on:

1. Management Plane Telemetry: Analyzing API logs (such as AWS CloudTrail or Azure Activity Logs) to see who created, modified, or deleted a resource and from what IP address.
2. Virtualized Snapshots: Using cloud-native tools to create point-in-time snapshots of virtual disks, which act as the modern equivalent of a forensic image without touching the physical server.
3. Identity-Centric Forensics: Since infrastructure is now "code," the "who" is often more important than the "where." Investigators track Identity and Access Management (IAM) tokens to reconstruct a suspect's movement through a virtual environment.

Consequently, the forensic scientist has evolved from a hardware technician into a specialist in virtualized architecture, navigating a world where the "silent witness" is a stream of encrypted bits flowing through a borderless, global network.

II. THE THREE DIMENSIONS OF CLOUD FORENSICS

To effectively investigate a cloud-based incident, Digital Forensic Science (DFS) must move beyond a purely technical scope. Investigators utilize a three-dimensional model—originally proposed by researchers to address the unique complexities of distributed computing—which categorizes the investigation into Technical, Organizational, and Legal layers.

I. Technical Dimension

The technical dimension involves the actual tools, procedures, and expertise required to perform the forensic process in a virtualized environment. In 2026, this dimension is characterized by a shift from hardware interaction to software-defined evidence collection.

a) Evidence Segregation: In a multi-tenant environment, the technical challenge is to "carve" out a suspect's data without infringing on the privacy of other tenants sharing the same physical CPU cache or storage volume.
b) Elastic Forensics: Investigators must use "elastic" tools that can scale alongside the cloud environment. This includes automated triggers that create a snapshot of a Virtual Machine (VM) the moment a security policy is violated.
c) Volatile Data Capture: Capturing the RAM of a cloud instance is critical, as it may contain decrypted keys or active malware. This must be done "live" before the instance is deprovisioned by the user or the provider's automated scaling logic.

II. Organizational Dimension

Unlike traditional forensics, where the investigator often has sole custody of the evidence, cloud forensics is a collaborative effort between at least two parties: the Cloud Service Provider (CSP) and the Cloud Customer.

a) The Chain of Dependency: Many CSPs outsource their underlying infrastructure to larger providers (e.g., a SaaS provider running on AWS). Investigators must navigate this "chain" to find where the actual logs and data reside.
b) Service Level Agreements (SLAs): The SLA is the primary document in the organizational dimension. It defines the "forensic readiness" of the environment—specifying what logs (API, network, or system) the provider is required to preserve and the timeframe in which they must deliver them to the customer or law enforcement.
c) Governance and Internal Staffing: Mature organizations now maintain internal "Cloud Incident Response" teams that act as a bridge between the technical administrators and external forensic experts.

III. Legal Dimension

The legal dimension is perhaps the most complex, as it deals with the "loss of physical location." Because data in 2026 is globally distributed, a single investigation can trigger a jurisdictional thicket.

a) Multi-Jurisdictional Conflict: A suspect in London may use a service headquartered in California with data centers physically located in Germany. Each of these regions

has distinct laws regarding data privacy (such as GDPR) and government access.

b) Search Warrants and "Possession": Legal teams must determine who "possesses" the data. Does a warrant served to the cloud customer suffice, or must it be served to the CSP? Acts like the U.S. CLOUD Act have attempted to streamline this, but international cooperation remains a bottleneck.

c) Chain of Custody in the Virtual World: Proving that a digital snapshot has not been tampered with while being transferred from a provider's data center to an investigator's lab requires high-level cryptographic verification (hashing) and detailed audit trails from the CSP.

III. THE SHARED RESPONSIBILITY MODEL

In cloud forensics, the "crime scene" is defined by the Shared Responsibility Model. This framework is a contractual and operational agreement that delineates which security and administrative tasks are handled by the Cloud Service Provider (CSP) and which fall to the customer. For a digital forensic scientist, this model is the primary map used to determine what evidence is "collectible" and what is "abstracted" away.

I. Infrastructure as a Service (IaaS)

In an IaaS environment (e.g., AWS EC2, Azure VMs), the CSP provides the "virtual iron"—the hardware, storage, and networking—while the customer manages everything from the Operating System (OS) upward.

a) Forensic Depth: This model offers the highest level of forensic visibility. Because the customer owns the OS, the investigator can perform live memory forensics, capture system registries, and analyze local log files (/var/log or Windows Event Logs).

b) Acquisition Method: The primary tool here is the Volume Snapshot. Investigators can "freeze" the state of a virtual hard drive to capture deleted files in unallocated space, much like a traditional bit-stream image.

II. Platform as a Service (PaaS)

In PaaS (e.g., Google App Engine, AWS Lambda, Azure SQL), the CSP manages the underlying infrastructure and the OS. The customer only manages the applications and the data they generate.

a) Forensic Depth: The investigator is "blind" to the OS layer. They cannot see running processes or kernel-level artifacts.

b) Evidence Sources: The investigation shifts to Application-Level Logs and Database Transaction Logs. If a web application is compromised, the evidence is found in the traces left within the development framework or the API calls made to the platform, rather than the server's file system.

III. Software as a Service (SaaS)

SaaS (e.g., Microsoft 365, Salesforce, Slack) represents the most restrictive environment for forensics. The CSP manages the entire stack, providing only a functional interface to the user.

a) Forensic Depth: The investigator has zero access to the underlying hardware, OS, or application code. They are entirely dependent on the Audit Logs provided by the CSP.

b) The "Provider Gap": Evidence is often limited to high-level metadata: login timestamps, IP addresses of successful authentications, and file-access history (who viewed a document and when). If the CSP's internal logging does not capture a specific event, that evidence is effectively non-existent for the investigator.

The transition from IaaS to SaaS represents a steady loss of Forensic Granularity. While IaaS allows for "Deep-Dive" analysis of the binary, SaaS forces the investigator to become a "Log Analyst," relying on the CSP to act as the primary custodian of the digital truth.

IV. TECHNICAL CHALLENGES: MULTI-TENANCY AND EPHEMERALITY

Cloud environments introduce two major technical obstacles that fundamentally break the traditional "seize and search" forensic workflow. These challenges—Multi-Tenancy and Ephemerality—force investigators to abandon bit-stream physical imaging in favor of surgical, logic-based data collection.

I. Multi-Tenancy and Data Segregation

In a cloud infrastructure, "your" data sits on the same physical hardware as the data of a "suspect," a "competitor," or an "innocent bystander." This shared

environment, known as Multi-Tenancy, creates a conflict between investigative necessity and privacy law.

a) The Problem of Physical Seizure: In a traditional lab, an investigator would image an entire 1TB drive. In a cloud data center, that same 1TB of storage might contain fragments from 500 different customers. Seizing the physical disk would result in the illegal mass-seizure of data from hundreds of uninvolved third parties, violating privacy regulations like GDPR or the Fourth Amendment.
b) Logical Acquisition & Cryptographic Silos: Forensic scientists must instead perform Logical Acquisitions. This involves targeting only the specific virtual containers or accounts authorized by a warrant. Modern cloud security often uses Cryptographic Tenancy, where each tenant's data is encrypted with a unique key. The investigator's challenge is to isolate the suspect's "ciphertext" and obtain the specific decryption keys from the Cloud Service Provider (CSP) without triggering "leakage" from neighboring tenants.

II. Ephemeral Instances and "Vanishing" Evidence

Traditional forensics is "post-mortem"—it happens after the computer is turned off. Cloud forensics, however, must often be "live" because cloud resources are inherently Ephemeral (short-lived).

a) Elasticity as an Anti-Forensic Tool: Cloud servers are often designed to be "elastic." They may be spun up automatically to handle a spike in web traffic or to execute a specific malicious script and then be deprovisioned (deleted) immediately after.
b) The Serverless Gap: In "Serverless" architectures (like AWS Lambda or Google Cloud Functions), the execution environment exists only for the milliseconds required to run a piece of code. Once the function finishes, the entire virtual environment is wiped from the physical RAM.
c) The Necessity of Proactive Logging: If an investigator has not enabled automated, centralized logging (such as VPC Flow Logs or SIEM integration) *before* an attack occurs, the evidence—including running processes, network connections, and temporary files—vanishes forever the moment the instance terminates.

The technical reality of the cloud is a race against time and architecture. To succeed, the forensic scientist must move from being a "reactive examiner" of hardware to a "proactive architect" of virtualized data streams.

V. DATA ACQUISITION METHODOLOGIES

To overcome the inherent barriers of cloud architecture, forensic scientists have moved away from physical imaging and toward specialized, software-driven acquisition techniques. These methodologies allow for the collection of evidence while maintaining the integrity required for judicial scrutiny.

I. Snapshot Analysis

Snapshot analysis is the cloud-native alternative to bit-stream imaging. A snapshot is a point-in-time, "frozen" copy of a virtual machine's (VM) disk.

a) The Methodology: When a security breach is detected, the investigator triggers a snapshot command through the Cloud Service Provider's (CSP) management console. This creates a static image of the virtual drive without requiring the server to be shut down.
b) Forensic Utility: Unlike a live system where data is constantly changing, a snapshot provides a stable environment for "dead" analysis. Investigators can search for hidden malware, examine system registries, and attempt to recover deleted files from the virtual file system.
c) Limitations: A snapshot only captures data at rest. It does not include the contents of the RAM or active network connections, meaning volatile evidence may be lost if a snapshot is the only method used.

II. API-Based Collection

In 2026, the "Management Plane" is the most critical source of truth. Every action in the cloud—creating a user, changing a firewall rule, or accessing a database—is an API call.

a) Management Logs: Providers like AWS (CloudTrail), Azure (Activity Logs), and Google Cloud (Audit Logs) record these API calls in near real-time. This provides an

immutable audit trail of the "who, what, and when" of an attack.

b) Metadata Acquisition: API-based collection allows investigators to pull metadata that traditional tools cannot see, such as the geographic region where a resource was created or the specific IAM (Identity and Access Management) role used to authorize a command.

c) Automated Sifting: Because cloud logs can reach petabytes in size, forensic scientists use automated scripts to query these APIs and filter for anomalies, such as a login from an unexpected country or an unauthorized attempt to disable encryption.

III. Remote Live Forensics

Because cloud instances are often ephemeral, waiting for a snapshot is sometimes too slow. Remote Live Forensics involves interacting with the target system while it is still running and connected to the network.

a) Forensic Agents: Investigators deploy lightweight "agents" or servlets (e.g., F-Response or Google's GRR) directly into the running instance. These agents act as a bridge, allowing the investigator to "reach into" the cloud VM from their remote workstation.

b) Volatile Data Capture: This is the only reliable way to capture the Order of Volatility in the cloud. It allows for the extraction of:

1. RAM Dumps: Containing unencrypted passwords and encryption keys.
2. Network Sockets: Showing active connections to a Command-and-Control (C2) server.
3. Process Trees: Revealing malicious code that may be "cloaked" from a standard disk snapshot.

c) Surgical Precision: This technique allows for the collection of specific files or memory segments, which is essential in multi-tenant environments where a full disk capture might be legally prohibited.

VI. THE JURISDICTIONAL "THICKET"

Jurisdiction is arguably the most significant non-technical hurdle in cloud forensics. In a classical investigation, the physical location of a computer determines the governing law. In the cloud, data is fragmented, replicated, and geographically dispersed. If a U.S. company's data is stored in a German data center, and the crime was committed by a user in Brazil, the investigator enters a "thicket" of conflicting legal mandates.

I. The U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data)

Passed in 2018 and heavily refined by executive agreements through 2026, the CLOUD Act fundamentally shifted the focus of jurisdiction from location to control.

a) Extraterritorial Reach: The Act allows U.S. law enforcement to compel U.S.-based technology companies (like Microsoft, Google, or AWS) to provide data even if that data is stored on a server physically located in another country.

b) The "Possession" Rule: If a U.S. provider has "possession, custody, or control" of the data, they must comply with a U.S. warrant. This renders the physical hosting location (e.g., Germany) irrelevant from the perspective of U.S. federal law.

c) Efficiency over MLATs: Historically, investigators used Mutual Legal Assistance Treaties (MLATs)—a process that could take months or years. The CLOUD Act bypasses this, allowing direct subpoenas to providers to meet the speed of digital crimes.

II. GDPR and the "Legal Deadlock"

The European Union's General Data Protection Regulation (GDPR) stands as the primary counter-force to the CLOUD Act. This creates a high-stakes legal dilemma for Cloud Service Providers (CSPs).

a) Article 48 Conflict: Under GDPR, a court order from a non-EU authority (like a U.S. judge) is generally not recognized as a valid legal basis for transferring personal data unless it is backed by an international agreement (like an MLAT).

b) The Deadlock: A CSP may find itself in a "no-win" scenario:

1. If they comply with the U.S. CLOUD Act warrant, they may face massive GDPR fines (up to 4% of global turnover) for an illegal data transfer.

2. If they refuse the U.S. warrant to satisfy GDPR, they face contempt of court and criminal penalties in the United States.

c) The "Comity" Challenge: To mitigate this, providers can file a "motion to quash" a warrant if they can prove that disclosure would violate the laws of a "qualifying foreign government." However, this process is rare and legally burdensome.

III. The Brazilian LGPD Context

In the hypothetical scenario involving Brazil, investigators must also contend with the LGPD (Lei Geral de Proteção de Dados). Much like GDPR, Brazil's privacy law imposes strict requirements on the international transfer of data. As of 2026, Brazil has moved toward institutionalizing enforcement pathways that increasingly intersect with U.S. outcomes, but the lack of a formal "Executive Agreement" under the CLOUD Act means that data acquisition from Brazil remains a manual, complex process involving local judicial authorization.

Ultimately, the "thicket" means that a digital forensic scientist's report is only as strong as the legal authority behind it. Without navigating these jurisdictional boundaries correctly, even the most technically perfect binary evidence can be suppressed in court.

VII. CONCLUSION: SYNTHESIS AND THE FUTURE OF THE VIRTUAL WITNESS

The transition from localized hardware to distributed cloud architectures represents the most significant paradigm shift in the history of Digital Forensic Science. As this analysis has demonstrated, the "science of the binary" is no longer a matter of physical recovery, but one of architectural navigation. The move away from the "box-at-the-scene" model toward a virtualized, log-centric methodology is not merely a technical update; it is a fundamental reimagining of what constitutes evidence and how the chain of custody must be preserved in a borderless digital ecosystem.

The New Standard of Forensic Integrity

In the classical era of forensics, integrity was defined by the physical isolation of a hard drive. In the cloud era of 2026, integrity is defined by the cryptographic verification of orchestration. The shift toward Management Plane Telemetry and Identity-Centric Forensics reflects a reality where "human intent" is evidenced not by a fingerprint on a keyboard, but by the specific IAM token used to spin up an ephemeral instance or modify a global security group.

The Shared Responsibility Model has become the primary legal and technical map for this new landscape. As we have explored, the depth of an investigation is now inversely proportional to the level of service abstraction. While IaaS environments still allow for the "deep-dive" analysis of the binary—imaging virtual disks and carving unallocated space—the rise of SaaS and Serverless computing has forced the forensic scientist to evolve into a sophisticated Data Scientist. In these high-abstraction environments, the "silent witness" is often found in the metadata: the login timestamp, the API request, and the cross-region replication log.

Navigating the Technical and Legal Arms Race

The technical challenges of Multi-Tenancy and Ephemerality have turned the forensic process into a race against the provider's automated scaling logic. The transition to "Live" forensics—capturing RAM and network sockets before an elastic instance is deprovisioned—requires a level of proactivity that was previously unknown in the field. 2026-era investigators can no longer afford to be reactive; they must be integrated into the organization's cloud architecture, ensuring that "Forensic Readiness" is baked into the infrastructure from day one.

Simultaneously, the Jurisdictional Thicket remains the most volatile element of the cloud landscape. The tension between the U.S. CLOUD Act and the EU's GDPR (and similarly, Brazil's LGPD) has placed Cloud Service Providers in a precarious position as global data custodians. As of 2026, the success of a cross-border investigation depends less on the examiner's ability to crack a password and more on their ability to navigate international treaties and privacy redaction protocols. The "Legal Deadlock" is a reminder that in the digital age, technology moves at the speed of light, while the law often moves at the speed of bureaucracy.

Toward an AI-Driven, Automated Frontier

As we look toward the immediate future, the primary challenge facing Digital Forensic Science is the sheer volume of data. We have moved from investigating gigabytes to analyzing petabytes. Manual log analysis is no longer feasible. The next phase of DFS will be defined by the integration of Artificial

Intelligence (AI) and Machine Learning (ML) directly into the forensic pipeline.

AI models are now being deployed to perform "Anomaly Detection" across millions of API calls, spotting the one unauthorized IAM role change that signals an insider threat. Furthermore, AI-assisted redaction is becoming the primary tool for solving the Multi-Tenancy problem—allowing investigators to extract a suspect's data while automatically masking the private information of "neighboring" tenants to remain GDPR-compliant.

However, this automation brings a new requirement for Algorithmic Transparency. For an AI-driven forensic finding to be admissible under the Daubert Standard, the "black box" of the algorithm must be made explainable to a court of law. The forensic scientist of the future must therefore be "tri-lingual"—fluent in the language of computer science, the language of the law, and the language of data ethics

REFERENCE

[1] Amazon Web Services. *AWS Security Best Practices for Forensics*. AWS Whitepapers, 2024, aws.amazon.com/whitepapers/forensics-on-aws/. Accessed 2 Jan. 2026.

[2] ASTM International. *ASTM E3016-18: Standard Guide for Management of Digital Evidence*. ASTM International, 2018, www.astm.org/e3016-18.html.

[3] Bennett, Charles H., and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing." *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175-79.

[4] Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed., Academic Press, 2011.

[5] "Clarifying Lawful Overseas Use of Data (CLOUD) Act." *U.S. Code*, vol. 18, sec. 2523, 2018. *GovInfo*, www.govinfo.gov/app/details/PLAW-115publ141.

[6] "Computer Forensic Tool Testing (CFTT)." *National Institute of Standards and Technology*, 14 Nov. 2023, www.nist.gov/itl/ssd/software-quality-group/computer-forensic-tool-testing-cftt. Accessed 2 Jan. 2026.

[7] Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579. Supreme Court of the United States. 1993. *Google Scholar*, scholar.google.com.

[8] European Parliament and Council. *Regulation (EU) 2016/679 (General Data Protection Regulation)*. 27 Apr. 2016. *EUR-Lex*, eur-lex.europa.eu/eli/reg/2016/679/oj.

[9] Gubbi, Jayavardhana, et al. "Cloud Computing: A Forensic Perspective." *Future Generation Computer Systems*, vol. 35, 2014, pp. 123-34.

[10] ISO/IEC. *ISO/IEC 27037:2012 Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. International Organization for Standardization, 2012.

[11] Lei Geral de Proteção de Dados Pessoais (LGPD). *Lei nº 13.709*. 14 Aug. 2018. *Presidência da República do Brasil*, www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[12] Locard, Edmond. "The Analysis of Dust Traces." *The American Journal of Police Science*, vol. 1, no. 3, 1930, pp. 276-98. *JSTOR*, www.jstor.org/stable/1147012.

[13] National Institute of Standards and Technology. *NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing*. 2011, doi.org/10.6028/NIST.SP.800-144.

[14] Riley v. California. 573 U.S. 373. Supreme Court of the United States. 2014. *Oyez*, www.oyez.org/cases/2013/13-132.