COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Forensic Evidence from Cloud Infrastructure: AWS, Azure and Google Cloud

Control-Plane Logs, Storage, Compute and the Evidence in the Account, Not the Server

When the business runs on cloud infrastructure, there is no server to image. The application lives across storage buckets, databases, virtual machines and managed services in an AWS, Azure or Google Cloud account, and the evidence lives not in a machine but in the account: the control-plane logs recording every action taken through the provider's interfaces, the storage-access logs, the identity and access records, the configuration history, and the snapshots and backups the platform keeps. This is a different discipline from imaging a laptop. The examiner works through the provider's own logging and export mechanisms, reasons about ephemeral compute that may no longer exist, distinguishes the control plane (who did what to the infrastructure) from the data plane (what the applications did with the data), and preserves evidence that is billed by the hour and deleted by policy. This guide sets out for UK lawyers what each of the three major platforms records, how to preserve and collect it, who controls access, and how infrastructure evidence is deployed in disputes from data breaches to shareholder claims to the departing engineer who took the account with them.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Cloud-infrastructure investigations are a growing part of its work: breach reconstruction from control-plane logs, disputed configuration changes, departing-engineer access, and the preservation of ephemeral and billed evidence in AWS, Azure and Google Cloud: worked through the providers' own logging and snapshot mechanisms and reported under CPR Part 35, with the FSR Code declaration where criminal proceedings follow.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | CLOUD-INFRASTRUCTURE FORENSICS | CONTROL-PLANE LOG ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: CLOUD-INFRASTRUCTURE EVIDENCE LIVES IN THE ACCOUNT, NOT THE MACHINE: THE CONTROL-PLANE LOG RECORDS WHO DID WHAT TO THE INFRASTRUCTURE, THE DATA-PLANE LOGS RECORD WHAT HAPPENED TO THE DATA, AND BOTH ARE BILLED, RETAINED BY POLICY AND PRESERVABLE ONLY THROUGH THE PROVIDER'S OWN MECHANISMS, APPLIED EARLY

The control plane (§3): every action taken through the provider's console, command line or API is recorded in a management event log: AWS CloudTrail, Azure Activity Log and Microsoft Entra logs, Google Cloud Audit Logs: with the identity, action, resource, source IP, time and result: the definitive record of who created, changed, accessed or deleted infrastructure, and the first thing preserved in any cloud dispute. **The data plane (§4):** storage-access logging (S3 access logs, Azure Storage logs, Cloud Storage audit logs) recording object reads, writes and deletes; database audit logs; and application logs shipped to the provider's logging service: what the running systems did with the data, distinct from what administrators did to the infrastructure. **Compute and snapshots (§5):** virtual machines and containers that may be long gone (auto-scaled away, terminated, redeployed), with their evidence surviving only in snapshots, machine images, block-storage volumes, backups and the logs they shipped while alive: the ephemeral-evidence problem that makes cloud compute forensics a race against automation. **Preservation and collection (§6):** the provider's hold and retention mechanisms engaged before policy deletes the logs; log and snapshot export to preserved storage; and the access question: who holds the account's root or administrative credentials, because the party that controls the account controls the evidence: with legal process reaching the provider or the controlling party where they are adverse. **Deployment (§7):** breach reconstruction (guide 99 at cloud scale), disputed configuration and deletion changes attributed through the control-plane log, the departing engineer who retained access or took infrastructure, and intellectual-property and shareholder disputes over what a cloud estate contained: all evidenced from logs that were billed by the hour and are already ageing.

- **The account is the evidence:** no machine to seize: the control-plane log is the crime scene and the witness.
- **Control plane and data plane differ:** who changed the infrastructure is a different log from what the data did.
- **Compute is ephemeral:** the server may be gone; its snapshot, image and shipped logs are what survive.
- **Logging is a choice, billed:** what was recorded depends on configuration and cost, established per account.
- **Access is control:** whoever holds the account holds the evidence: the first strategic question is who that is.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: there is no server to image

Traditional computer forensics has an object: a disk, seized, imaged and examined. Cloud infrastructure has no such object. The "server" is a virtual machine that exists as configuration until the moment it runs, may be created and destroyed automatically many times a day, and shares physical hardware the provider will never let anyone image. The data sits in storage services accessed over the network. The whole estate is defined by settings in an account and observed through logs the provider generates. To ask "can we image the server?" is to misunderstand the medium: there may be no server tomorrow, and there was never one to seize.

What there is, instead, is a comprehensive record of actions. Because everything in the cloud happens through the provider's interfaces, and because providers log those interfaces for their own operational and billing reasons, the account contains a detailed history of who did what, to which resource, from where, and when. That history is the evidence. But it is generated continuously, retained only as long as configuration and cost allow, and controlled by whoever holds the account credentials. The examiner's work is to identify the relevant logs and snapshots, preserve them through the provider's own mechanisms before they age out, reason about the compute that no longer exists, and attribute actions to identities and then people. This guide is that work, plane by plane and platform by platform.

§ 0 3 · THE CONTROL PLANE

The control plane: who did what to the infrastructure

- **The management event log:** AWS CloudTrail, Azure Activity Log and Google Cloud Audit Logs (Admin Activity) record every management action: create, modify, delete, configure, access-grant: with the calling identity, action, target resource, source IP, user agent, timestamp and outcome: the authoritative "who did what to the infrastructure" record, and the first preserved.
- **Identity and access records:** AWS IAM and its sign-in records, Microsoft Entra sign-in and audit logs, Google Cloud IAM and identity logs: authentication events, role assumptions, permission changes and federated-identity use: the identity layer that joins an action to an account and a session (guide 105 §7).
- **Configuration history:** AWS Config, Azure Resource Manager change history and Google Cloud asset inventory: the state of resources over time and the record of each change: what the estate looked like on a given date and when a setting (a permissive bucket policy, an open security group) changed and by whom.
- **Key and secret access:** key-management-service logs (AWS KMS, Azure Key Vault, Cloud KMS) recording use of encryption keys and secrets: who could decrypt what, and when keys were used, created or deleted: relevant to both breach and destruction (guide 110 §5).
- **The federation and cross-account trap:** actions taken through assumed roles, federated identities and cross-account access attribute to the assumed role or the federating identity: the human behind them found from the identity provider's logs (guide 105) and the session context, not from the control-plane entry alone.

§ 0 4 · THE DATA PLANE

The data plane: storage, databases and what the applications did

- **Object-storage access logs:** S3 server-access logging and CloudTrail data events, Azure Storage analytics and diagnostic logs, Google Cloud Storage data-access audit logs: object-level reads, writes, deletes and permission changes: what was taken from or written to storage, distinct from the control-plane act of configuring the storage: often off by default and enabled only where configured, per §6.
- **Database audit logs:** managed-database audit and query logging (RDS, Azure SQL, Cloud SQL and the managed NoSQL and warehouse services): connections, queries and data access: who read or changed which records, where auditing was enabled.
- **Application and platform logs:** logs shipped to the provider's logging service (CloudWatch Logs, Azure Monitor, Cloud Logging) by applications, load balancers, functions and gateways: the application-level narrative, retained per the log group's policy.
- **Network-flow logs:** VPC flow logs, NSG flow logs and VPC Flow Logs recording connections between resources and to the internet: the egress and lateral-movement record (guide 99 §5, guide 111 §5) at infrastructure scale.
- **The default-off problem:** much data-plane logging is disabled by default because it is voluminous and billed: the honest first finding in many matters is that object-level access was never logged, and the §8 alternates (snapshots, application logs, the destination) must carry the case.

§ 0 5 · COMPUTE, SNAPSHOTS AND THE EPHEMERAL-EVIDENCE PROBLEM

Compute, snapshots and the ephemeral-evidence problem

- **Virtual machines as evidence:** a running instance's disk can be captured by snapshotting its block-storage volume (EBS, Azure managed disks, persistent disks) and analysing the snapshot like a disk image: the closest cloud analogue to imaging a machine, available only while the instance or its volume still exists.
- **The ephemerality problem:** auto-scaling terminates instances, deployments replace them, and container tasks live for seconds: the machine that held the evidence may have ceased to exist before anyone thought to preserve it, leaving only the snapshots, machine images and logs it shipped while alive: the race guide 99's volatility principle runs, at cloud speed.
- **Snapshots and images:** existing snapshots, custom machine images and their creation history: point-in-time captures that may hold the state of a system as it was, and whose own creation and deletion are control-plane events (§3): the recoverable past of an ephemeral present.
- **Backups and managed recovery:** the platform's backup services and any third-party backups: the estate's redundancy (guide 95 §5) at infrastructure scale, holding prior states of storage and databases.
- **Containers and serverless:** container images in registries, task definitions and function code and configuration in the account, plus the logs each shipped: the evidence of workloads that leave no persistent machine at all: read from their definitions and their logs.

§ 0 6 · PRESERVATION AND COLLECTION

Preservation and collection: holds, exports and who controls access

- **The access question first:** who holds the account's root and administrative credentials decides who can preserve and collect: a cooperating party's own account is worked with their administrators under instruction; an adverse party's account is reached by order; a departed engineer's personal account holding company infrastructure is reached as in guide 111 §6.
- **Engage retention before policy deletes:** control-plane and data-plane logs have retention periods (a default CloudTrail management-event window, log-group retention settings, activity-log windows) and are deleted on schedule: preservation means extending retention, exporting logs to preserved storage, and disabling lifecycle deletion on the relevant stores: done at once, because the clock is the provider's, not the litigant's.
- **Snapshot the perishable:** snapshots of relevant volumes taken before instances are terminated, and existing snapshots and images protected from deletion: the ephemeral captured while it exists.
- **Documented, reproducible export:** logs and configuration exported through the provider's tools and APIs with the queries, scope and time recorded and results hashed (guide 71): the collection defensible and repeatable, with the provider's role in generating the evidence stated.
- **Provider legal process:** where the account is adverse or inaccessible, the provider's law-enforcement and civil-disclosure channels reach account-existence, ownership and, in some cases, content: on jurisdictional timelines planned early (the provider's data may sit in, or move between, regions).

§ 0 7 · DEPLOYMENT

Deployment: breaches, configuration disputes and the departing engineer

- **Breach reconstruction:** the control-plane and data-plane logs reconstructing an intrusion or misconfiguration exposure: the open bucket, the leaked key, the assumed role, the objects read (guide 99's entry-movement-exfiltration-impact map at cloud scale): the ICO clock (guide 99 §6) running on the finding.
- **Configuration and deletion disputes:** who changed the security group, who deleted the production database, who disabled the logging: attributed from the control-plane log and the configuration history (§3), dated against the duty (guide 106), with the innocent explanations (automation, deployment pipelines, scheduled policy) distinguished from human acts by the calling identity.
- **The departing engineer:** the administrator who left with credentials unrevoked, created back-door access, took infrastructure-as-code and data to a personal account, or reduced the estate on the way out: the control-plane log recording the access and the acts, the exfiltration methods of guide 111 applied to cloud resources, and the access-revocation failure itself a finding.
- **IP, shareholder and value disputes:** what a cloud estate contained and when: the codebase, the data assets, the customer records: read from the account's inventory, storage and configuration history for disputes over ownership, value and representations.
- **Cross-platform and hybrid:** estates spanning two clouds and on-premises, tied together by identity federation: the guide 96 timeline normalising logs across providers and the guide 105 lattice attributing across federated identities: the whole reconstructed from parts in different hands.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a cloud estate records itself in layers that are generated by the provider, retained by policy and controlled by the account holder, and the examination reads whichever survive. The control plane records every management action. The data plane records object and database access where logging was enabled. The identity layer records who authenticated and assumed what. The configuration history records the estate's state over time. Snapshots, images and backups hold the perishable past. Network-flow logs record the connections. And beyond the account: the provider's own records reachable by process, the destination account or new employer where infrastructure or data left, and the endpoints (the engineers' laptops with their command-line histories, credentials and infrastructure-as-code repositories) that operated the cloud from outside. When data-plane logging was off, the snapshot and the application log carry it; when the compute is gone, the log it shipped and the image survive; when the account holder is adverse, the provider and the operating endpoints hold the record; when logs were deleted, their deletion is itself a control-plane event, and the backups predate it.

QUESTION	CONTROL-PLANE LOG	DATA-PLANE LOGS	CONFIG HISTORY + SNAPSHOTS	NETWORK-FLOW LOGS	PROVIDER + DESTINATION	OPERATING ENDPOINTS
Who changed the infrastructure	Y: identity + action	n/a	Y: the change over time	n/a	Provider account records	CLI history, IaC commits
What data was accessed / taken	Access-grant events	Y: object + DB access	Snapshot of the store	Y: egress volume	Y: the destination	Local credentials, downloads
When	Y: timestamps	Y: timestamps	Y: change + snapshot times	Y: flow times	Provider-side times	Endpoint timestamps
Whose identity, whose hands	Y: calling identity	Accessing identity	n/a	Source resource	Account holder	Y: the engineer's own machine
What existed and was lost	Deletion events	n/a	Y: snapshots + backups	n/a	Backup copies	Local repo copies

Fallback strategy in one line: preserve the control plane first because it records everything and expires; where data-plane logging was off, the snapshot, the backup and the destination carry it; and the engineers' own endpoints hold the credentials and the code the account will not show.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE OPEN BUCKET AND THE LOG THAT HAD IT ALL

A company suffered a data breach: customer records from an S3 bucket appeared for sale. The §3 CloudTrail management log, preserved the day the breach was reported, showed the bucket's access policy changed to public four months earlier by a developer's IAM identity during a late-night deployment; the §4 S3 data-event logging, which had fortunately been enabled on that bucket, recorded the subsequent object reads: thousands of GET requests over the following weeks from a cluster of external IPs, and a single large enumeration the night before the data appeared for sale. The §5 analysis needed no ephemeral compute; the storage told the story. The §7 reconstruction (guide 99's map at cloud scale) gave the ICO notification its timeline and scope to the object, and the configuration history dated the exposure precisely. The company's own logging, enabled and preserved in time, was the difference between a defensible breach response and a guess.

EXAMPLE 2 · THE PRODUCTION DATABASE THAT WAS DELETED, AND THE IDENTITY THAT DID IT

During a shareholder dispute, a startup's production database was deleted, and each side blamed the other. There was no server to examine, but the §3 control-plane log was decisive: the deletion was a single API call recorded in CloudTrail with the calling IAM identity, the source IP and the exact time: 03:14, two days after the claim form was served. The identity belonged to a departing technical co-founder whose credentials had not been revoked; the §3 IAM sign-in records placed the session on his known IP; and the configuration history showed automated backups had been silently disabled by the same identity a week earlier: the destruction prepared, then executed. The §5 snapshots that should have existed did not, because of that disablement, but an older manual snapshot predated the disablement and restored most of the data. The deletion, the disablement and the timing, all in the control-plane log, made the spoliation case (guide 110 §7); the co-founder's "it must have been automation" failed against the named identity.

EXAMPLE 3 · THE ENGINEER WHO TOOK THE INFRASTRUCTURE, NOT JUST THE DATA

A departing lead engineer was suspected of taking a fintech's core system to a competitor. The investigation was not only about data but about the infrastructure-as-code that defined the whole platform. The §3 control-plane log showed, in his final fortnight, the creation of a personal access key, the export of the account's infrastructure templates, and read access to the code repositories and secrets; the §7 endpoint examination of his laptop (guide 111 §4) found a personal GitHub account into which the infrastructure repository had been pushed and a personal AWS profile configured; and the §6 process reached both personal accounts, which held the complete infrastructure definition and a partial data export. The control-plane log named the acts and the identity; the endpoint named the destinations; the personal accounts held the material. The springboard relief covered not just the data but the system's blueprint: which, for a cloud-native business, was the more valuable theft.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Asking to image a server:** the medium misunderstood; the control-plane log, which is the evidence, left unpreserved while a non-existent disk is sought.
- **Logs left to their retention:** CloudTrail, activity and log-group windows expiring during deliberation: the control plane's clock, unaddressed: guide 105 §6 at infrastructure scale.
- **Data-plane logging assumed:** object-level access expected to have been recorded when it was off by default: Example 1's near-miss, on the wrong side.
- **Compute left to auto-scale away:** the instance holding the evidence terminated by automation before a snapshot was taken: §5's race lost.
- **Control and data planes conflated:** "who accessed the data" answered from the control-plane log, which records infrastructure actions, not object reads.
- **Automation read as human acts:** deployment-pipeline and scheduled actions attributed to individuals: the calling identity's nature unexamined.
- **Access not secured:** the departing engineer's credentials never revoked (Example 2), the account left under adverse control.
- **The endpoints ignored:** the engineers' laptops with the credentials, CLI histories and code repositories: the cloud operated from outside, that outside never examined.

Technical limitations

- **Logging is configured and billed:** what exists depends on what was enabled and paid for: the investigable record bounded by yesterday's cost decisions, stated per account.
- **Ephemerality is final:** compute gone without a snapshot or shipped log is gone: the report says so and turns to the alternates.
- **Provider access is mediated:** the examiner never touches the hardware; everything is through the provider's interfaces and their integrity, which the methodology addresses.
- **Attribution crosses federation:** assumed roles and federated identities need the identity provider's logs to reach a person (guide 105 §7); the control-plane entry alone names a role.
- **Jurisdiction and data location:** provider data may sit in or move between regions, engaging cross-border and disclosure questions planned early.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which cloud accounts exist, who holds root and administrative credentials, and have any departed staff's credentials been revoked?
- What control-plane and data-plane logging is enabled, with what retention, and can it be extended and exported now?
- What snapshots, images and backups exist, and are any relevant instances at risk of auto-scaling away?

Ask your opponent

- Please preserve and disclose the control-plane management event logs (such as CloudTrail, Azure Activity Log or Google Cloud Audit Logs) for [accounts] during [period], identifying the calling identity, action, resource, source IP, time and outcome of relevant events, and confirm the retention configuration and preservation date.
- Please preserve and disclose the relevant data-plane access logs, configuration history, identity and sign-in logs, network-flow logs, and snapshots, images and backups, and confirm whether object-level and database access logging was enabled during [period].
- Please identify who held root and administrative access to [accounts] during [period] and confirm that no logs, snapshots or resources have been deleted since [date].

Ask your eDiscovery / forensic provider

- What is enabled and retained on this account, and what have we already lost to policy?
- Does the control-plane log attribute the disputed act to a human, or only to a role or automation?
- What survives of the ephemeral compute, and do the engineers' endpoints corroborate the account?

SUGGESTED WORDING · CLOUD-INFRASTRUCTURE PRESERVATION NOTICE

> "You are required immediately to preserve all evidence relating to the cloud infrastructure accounts identified at Schedule 1, and in particular to: (1) extend the retention of, and export to preserved storage, all control-plane management event logs, identity and sign-in logs, data-plane storage and database access logs, network-flow logs and application logs for the period [dates]; (2) preserve the configuration history and all snapshots, machine images and backups, and suspend any lifecycle or automated deletion affecting them; (3) snapshot the block-storage volumes of the instances identified at Schedule 2 before any termination or replacement; (4) preserve and not revoke, alter or delete the identity and access records showing who held and used administrative credentials; and (5) refrain from deleting, reconfiguring or reducing any relevant resource. Preservation must be effected through the provider's own retention and export mechanisms so that authenticity and completeness are maintained, and you must confirm the date and method of each step. These logs and resources are subject to automated deletion and billing-driven lifecycle policies, and evidence lost after the date of this notice may be the subject of an application for adverse inferences and costs."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The cloud-infrastructure checklist

- ☐ Cloud accounts identified; root and administrative access holders known
- ☐ Departed staff credentials revoked; adverse-control risk assessed
- ☐ Control-plane log retention extended and exported first
- ☐ Data-plane logging status established; logs preserved where enabled
- ☐ Configuration history, identity logs and flow logs preserved
- ☐ Relevant volumes snapshotted before auto-scaling or termination
- ☐ Existing snapshots, images and backups protected from deletion
- ☐ Automation distinguished from human acts by calling identity
- ☐ Operating endpoints (engineers' machines) imaged and examined
- ☐ Collection documented, hashed and reproducible per guide 71

Red flags

- Departed administrators whose credentials were never revoked: Example 2.
- Logging or backups disabled shortly before a disputed act: Example 2's preparation.
- Object-level access logging off on sensitive data stores.
- Public or over-permissive storage configurations: Example 1's bucket.
- Personal access keys and profiles created near a departure: Example 3.
- Infrastructure-as-code repositories accessible to leavers.
- Control-plane logs approaching the end of their retention window.

When to involve a digital forensic expert

At once, because the control-plane clock is the provider's and the compute may auto-scale away: preservation of logs, snapshots and access records is same-day work (Example 1's enabled logging, preserved in time); at collection, worked through the provider's mechanisms with the access question resolved and the collection documented; at analysis, where control and data planes are read correctly, automation is separated from human acts, and federated identities are traced to people (Example 2's named call); and at deployment, in breach, configuration-dispute, departing-engineer and IP proceedings under CPR Part 35, with the endpoints examined alongside the account (Example 3). Through **cflab.uk** and **e-discovery.uk**, cloud-infrastructure investigations run from same-day preservation to attributed finding: because in the cloud, the evidence is the account, and the account is already deleting it.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Our systems are all in AWS. Can you image the server?

There is no server to image in the traditional sense (§2): the evidence is in the account: the control-plane log of who did what (§3), the data-plane access logs (§4), and snapshots of any running instance's storage (§5). The right first step is not imaging but preserving those logs and snapshots through AWS's own mechanisms before retention and auto-scaling remove them.

Someone deleted our production database. Can we prove who?

Usually to the identity, often to the person: the deletion is a single control-plane API call recorded with the calling identity, source IP and time (§3, Example 2), and the identity and sign-in logs join it to a session and account. Automation is distinguished from a human by the nature of the calling identity, and the person behind a role is found from the identity provider's logs and the endpoint.

We think data was taken from cloud storage, but there is no access log. Is it hopeless?

Object-level logging is off by default and its absence is a common first finding (§4), but not the end: the control plane records the access-permission changes that enabled it, network-flow logs record the egress volume, snapshots hold the store's prior state, and the destination account (§8) holds what left (guide 111). The case shifts to the alternates, and the report states which carried it.

A former engineer still had access to our cloud account. How serious is that?

Potentially very: unrevoked credentials let a leaver read, take or destroy the estate, and the control-plane log records whatever they did (Example 2, Example 3): the failure to revoke is itself a finding, and the acts are attributed to their identity. Preserve the logs, revoke access, snapshot what is perishable, and examine the leaver's endpoints for the credentials and code they took.

How long do we have before the evidence disappears?

Less than you think: control-plane management-event history has a default window, log-group and activity-log retention is configurable and often short, and compute auto-scales away continuously (§5, §6). Preservation: extending retention, exporting logs, snapshotting volumes, protecting backups: is the first and most time-critical act, because the provider's lifecycle policies delete on schedule regardless of the dispute.

Does it matter which of AWS, Azure or Google Cloud we use?

The principles are identical: control plane, data plane, identity, configuration history, snapshots, retention: but the service names, log formats, default settings and export tools differ per platform (§3-§6), and hybrid and multi-cloud estates need the guide 96 timeline to normalise logs across them. The examiner reads each platform on its own terms and reconciles them into one account of events.

§ 14 · REFERENCE

Glossary

Control plane
The management layer; actions taken to the infrastructure itself.

Data plane
The layer where applications read and write the actual data.

CloudTrail / Activity Log
The providers' records of management events.

Configuration history
The recorded state of resources over time.

Ephemeral compute
Instances or tasks that may exist only briefly.

Flow logs
Records of network connections between resources.

IAM / identity logs
Authentication, role and permission records.

Infrastructure as code
The templates that define a cloud estate.

Snapshot
A point-in-time capture of a storage volume.

Root credentials
The account's highest access, controlling all evidence.

Sources and authoritative references

The cloud-infrastructure disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (cloud-infrastructure forensics, control-plane analysis, breach reconstruction, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (cloud log preservation, snapshot and export collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- AWS, CloudTrail and S3 access logging: docs.aws.amazon.com, CloudTrail · Microsoft, Azure Monitor and Activity Log: learn.microsoft.com, Azure Monitor · Google Cloud audit logs: cloud.google.com, audit logs
- NIST SP 800-86 (forensic techniques) and NIST Cloud Computing Forensic guidance (NISTIR 8006): csrc.nist.gov, SP 800-86 · csrc.nist.gov, NISTIR 8006
- PD 57AD: justice.gov.uk, PD 57AD · CPR Part 35: justice.gov.uk, Part 35 · ICO, personal data breaches: ico.org.uk, report a breach · ISO/IEC 27037: iso.org, 27037

DISCLAIMER

This publication provides general information about forensic evidence from cloud infrastructure as at August 2026. Provider services, log formats, default settings, retention and export tooling change frequently; verify the current position for the platform, account and matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Cloud-infrastructure work at the laboratory starts where the medium demands: not with a disk but with the account, and with the clock. The access question is resolved first (who holds root, whose credentials must be revoked, whether the account is adverse); the control-plane logs are preserved and exported through the provider's own mechanisms before retention deletes them (Example 1's enabled logging, held in time); the perishable compute is snapshotted before automation removes it; and the data-plane, identity, configuration and flow logs are secured where they exist, with the honest first finding stated where they do not. Analysis reads control and data planes correctly, separates automation from human acts by the calling identity, and traces federated identities to people (Example 2's named call), with the engineers' own endpoints examined alongside the account for the credentials and infrastructure-as-code the account will not show (Example 3). Reports run under CPR Part 35, with the FSR Code declaration where criminal proceedings follow. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a cloud dispute has arisen, the control-plane log is on the provider's retention clock now: preservation is today.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace