Forensic Evidence From Cloud Infrastructure AWS Azure Google Cloud

Forensic evidence from cloud infrastructure, such as AWS, Azure, and Google Cloud, resides in the account, not the server. This guide details how control-plane and data-plane logs record actions and data events, and how these are preserved through provider mechanisms.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/forensic-evidence-from-cloud-infrastructure-aws-azure-google-cloud

CLOUD INFRASTRUCTURE · A GUIDE FOR UK LAWYERS Forensic Evidence from Cloud Infrastructure: AWS, Azure and Google Cloud Control-Plane Logs, Storage, Compute and the Evidence in the Account, Not the Server COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES CLOUD-INFRASTRUCTURE FORENSICS

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: CLOUD - INFRASTRUCTUREEVIDENCELIVESINTHEACCOUNT, NOT THE MACHINE: THE CONTROL - PLANELOGRECORDSWHODIDWHATTOTHE INFRASTRUCTURE, THEDATA - PLANELOGSRECORDWHATHAPPENEDTOTHEDATA, AND BOTHAREBILLED, RETAINEDBYPOLICYANDPRESERVABLEONLYTHROUGHTHE PROVIDER ' SOWNMECHANISMS, APPLIED EARLY

§ 02 · FIRST PRINCIPLES The problem in plain English: there is no server to image

§ 03 · THECONTROLPLANE The control plane: who did what to the infrastructure

§ 04 · THEDATAPLANE The data plane: storage, databases and what the applications did

§ 05 · COMPUTE, SNAPSHOTSANDTHEEPHEMERAL - EVIDENCE PROBLEM Compute, snapshots and the ephemeral-evidence problem

§ 06 · PRESERVATION AND COLLECTION Preservation and collection: holds, exports and who controls access

§ 07 · DEPLOYMENT Deployment: breaches, configuration disputes and the departing engineer

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION PLANE

HISTORY + CONTROL- NETWORK- PROVIDER + OPERATING PLANE LOG FLOW LOGS DESTINATION END POINT S DATA- CONFIG LOGS SNAPSHOTS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEOPENBUCKETANDTHELOGTHATHADITALL EXAMPLE2 · THE PRODUCTION DATABASE THAT WAS DELETED, ANDTHEIDENTITYTHAT DIDIT EXAMPLE3 · THEENGINEERWHOTOOKTHEINFRASTRUCTURE, NOT JUST THE DATA

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · CLOUD - INFRASTRUCTUREPRESER VAT IONNOTICE

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The cloud-infrastructure checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Our systems are all in AWS. Can you image the server? Someone deleted our production database. Can we prove who? We think data was taken from cloud storage, but there is no access log. Is it hopeless? A former engineer still had access to our cloud account. How serious is that? How long do we have before the evidence disappears? Does it matter which of AWS, Azure or Google Cloud we use?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 end point.

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 what ever 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 end point s 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, export in g 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. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 15 of 17