Training Course on Cloud Forensics for Google Cloud Platform (GCP)

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's digital age, cloud forensics has emerged as a critical component in cybersecurity and digital investigations, especially for platforms like Google Cloud Platform (GCP). As organizations migrate to cloud infrastructure, they must equip their IT and security teams with robust investigative techniques to detect, analyze, and respond to cloud-based threats. Training Course on Cloud Forensics for Google Cloud Platform (GCP) offers a comprehensive guide into GCP forensic techniques, aligning with modern compliance standards, data protection laws, and incident response protocols in cloud environments.

This training will help learners build expertise in identifying, preserving, analyzing, and presenting digital evidence on GCP. With increasing incidents of cloud breaches, cybercrime, and insider threats, mastering GCP forensic procedures is no longer optional—it's essential. Whether you're in law enforcement, cybersecurity, IT operations, or a cloud architect role, this course equips you with actionable, hands-on knowledge using real-world cloud forensics case studies and tools.

Programme Curriculum

Training Course on Cloud Forensics for Google Cloud Platform (GCP)

Introduction

In today's digital age, cloud forensics has emerged as a critical component in cybersecurity and digital investigations, especially for platforms like Google Cloud Platform (GCP). As organizations migrate to cloud infrastructure, they must equip their IT and security teams with robust investigative techniques to detect, analyze, and respond to cloud-based threats. Training Course on Cloud Forensics for Google Cloud Platform (GCP) offers a comprehensive guide into GCP forensic techniques, aligning with modern compliance standards, data protection laws, and incident response protocols in cloud environments.

This training will help learners build expertise in identifying, preserving, analyzing, and presenting digital evidence on GCP. With increasing incidents of cloud breaches, cybercrime, and insider threats, mastering GCP forensic procedures is no longer optional—it's essential. Whether you're in law enforcement, cybersecurity, IT operations, or a cloud architect role, this course equips you with actionable, hands-on knowledge using real-world cloud forensics case studies and tools.

Course Objectives

1. Understand the fundamentals of cloud forensics and its application in Google Cloud environments.
2. Learn about GCP infrastructure and service models relevant to forensic investigations.
3. Master incident response planning and execution within GCP.
4. Identify and collect forensically sound data from GCP services like Compute Engine, Cloud Storage, and Cloud Logging.
5. Analyze log data, API interactions, and system metadata to track malicious activity.
6. Utilize digital forensics tools and open-source platforms to investigate GCP threats.
7. Explore threat hunting strategies using GCP-native tools such as Cloud Audit Logs.
8. Implement chain of custody and legal compliance techniques for cloud evidence.
9. Gain skills in forensic imaging and snapshot analysis of cloud-based virtual machines.
10. Detect data exfiltration and lateral movement in the cloud using behavioral analytics.
11. Perform timeline reconstruction and incident documentation in GCP environments.
12. Apply machine learning-driven forensic techniques in modern cloud investigations.
13. Prepare comprehensive forensic reports with a focus on court-admissible evidence.

Target Audience

1. Cloud Security Engineers
2. Cybersecurity Analysts
3. Digital Forensics Investigators
4. GCP Cloud Architects
5. Incident Response Teams
6. IT Security Managers
7. Law Enforcement & Legal Experts
8. Cloud System Administrators

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cloud Forensics in GCP

- Overview of cloud forensics and its evolution
- Key differences between traditional and cloud-based investigations
- GCP architecture and shared responsibility model
- Legal and ethical challenges in GCP investigations
- Overview of GCP compliance standards (HIPAA, GDPR, etc.)
- **Case Study**: Investigating a simulated insider data breach in Google Cloud

Module 2: GCP Forensic Readiness and Incident Response

- Planning forensic readiness in GCP environments
- Building an incident response (IR) framework for GCP
- Tools and playbooks for cloud-based IR
- GCP-native logging and monitoring tools
- Setting up alerts and proactive threat detection
- **Case Study**: Real-time IR drill using Google Cloud’s security suite

Module 3: Evidence Identification and Acquisition

- Locating digital evidence in Compute Engine, GKE, and Cloud Storage
- Cloud Audit Logs and Admin Activity Logs usage
- Preserving data integrity during collection
- Snapshotting and imaging virtual machines in GCP
- Secure evidence export and storage
- **Case Study**: Investigating data theft through VM compromise

Module 4: Log Analysis and Metadata Forensics

- Parsing and filtering GCP logs for anomalies
- Understanding GCP API calls and network traces
- User behavior analysis and anomaly detection
- Reconstructing attacker timelines using Stackdriver
- Automating log analysis with BigQuery and Cloud Functions
- **Case Study**: Uncovering a cross-project privilege escalation

Module 5: GCP Threat Hunting and Detection

- Setting up threat hunting strategies on GCP
- Leveraging AI and ML tools for threat detection
- Indicators of compromise in cloud environments
- Using VPC Flow Logs and Packet Mirroring
- Integrating third-party SIEM solutions with GCP
- **Case Study**: Identifying a cryptojacking attack on cloud resources

Module 6: Chain of Custody and Legal Compliance

- Documenting evidence handling in the cloud
- Applying international forensic standards (e.g., ISO/IEC 27037)
- Managing cross-border data concerns in GCP
- Ensuring admissibility of cloud evidence in court
- GCP tools supporting legal compliance audits
- **Case Study**: Preparing a forensic report for a legal proceeding

Module 7: Reporting and Presentation of Forensic Findings

- Writing structured forensic investigation reports
- Best practices for presenting evidence to stakeholders
- Tools for visualization of forensic findings
- Using templates and GCP dashboards for reporting
- Verifying report authenticity and consistency
- **Case Study**: Mock presentation of findings from a GCP compromise

Module 8: Advanced Techniques and Emerging Trends

- Cloud-native forensic automation
- Forensics in serverless and containerized environments (e.g., Cloud Run)
- Future of AI in digital forensics
- Integration of blockchain for evidence traceability
- Evolving threats and forensic challenges in multi-cloud setups
- **Case Study**: Detecting and responding to a multi-cloud APT attack

Training Methodology

- Instructor-led virtual or in-person training sessions

- Real-world case study walkthroughs for every module
- Hands-on labs using GCP sandboxes
- Access to cloud forensic toolkits and scripts
- Group-based assignments and incident simulations
- Quizzes and assessments after each module

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100

Start Date	End Date	Location	Price
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com