Training Course on Digital Forensics in Hybrid Environments

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

The rapid shift towards hybrid cloud architectures has revolutionized how organizations store and manage data, but it has also introduced unprecedented complexities for digital forensic investigations. Blending on-premises infrastructure with multiple cloud service providers (e.g., AWS, Azure, GCP) creates a distributed and dynamic environment where traditional forensic methodologies often fall short. Training Course on Digital Forensics in Hybrid Environments is specifically designed to equip forensic professionals with the advanced skills required to navigate these intricate ecosystems. Participants will learn to identify, acquire, analyze, and present digital evidence seamlessly across disparate physical and virtualized platforms, ensuring comprehensive and legally defensible investigations in the hybrid attack surface.

This immersive program will delve into the unique challenges presented by multi-cloud data sovereignty, shared responsibility models, and the ephemeral nature of cloud resources. Through practical labs and real-world case studies, attendees will master techniques for correlating evidence from diverse sources – from endpoint logs to cloud audit trails – to reconstruct complex attack scenarios. Gain the expertise to perform cross-platform forensic analysis, understand the nuances of cloud native forensics, and become an indispensable asset in securing and responding to incidents within any hybrid enterprise. This course is crucial for anyone seeking to maintain digital investigative integrity in the era of distributed computing.

Programme Curriculum

Training Course on Digital Forensics in Hybrid Environments

Introduction

The rapid shift towards hybrid cloud architectures has revolutionized how organizations store and manage data, but it has also introduced unprecedented complexities for digital forensic investigations. Blending on-premises infrastructure with multiple cloud service providers (e.g., AWS, Azure, GCP) creates a distributed and dynamic environment where traditional forensic methodologies often fall short. Training Course on Digital Forensics in Hybrid Environments is specifically designed to equip forensic professionals with the advanced skills required to navigate these intricate ecosystems. Participants will learn to identify, acquire, analyze, and present digital evidence seamlessly across disparate physical and virtualized platforms, ensuring comprehensive and legally defensible investigations in the hybrid attack surface.

This immersive program will delve into the unique challenges presented by multi-cloud data sovereignty, shared responsibility models, and the ephemeral nature of cloud resources. Through practical labs and real-world case studies, attendees will master techniques for correlating evidence from diverse sources – from endpoint logs to cloud audit trails – to reconstruct complex attack scenarios. Gain the expertise to perform cross-platform forensic analysis, understand the nuances of cloud native forensics, and become an indispensable asset in securing and responding to incidents within any hybrid enterprise. This course is crucial for anyone seeking to maintain digital investigative integrity in the era of distributed computing.

Course Duration

5 Days

Course Objectives

1. Define Hybrid Forensic Challenges: Articulate the unique complexities of digital forensics in hybrid cloud environments (e.g., data dispersion, jurisdictional issues, multi-tenancy).
2. Master Cross-Platform Evidence Acquisition: Acquire forensically sound digital evidence from a mix of on-premises servers, endpoints, and diverse cloud platforms.
3. Navigate Cloud Service Provider (CSP) Specifics: Understand the forensic capabilities, logging mechanisms, and legal processes of major CSPs (AWS, Azure, GCP).
4. Correlate Disparate Data Sources: Effectively combine and analyze evidence from traditional systems with cloud audit logs, network flow data, and security event information.
5. Perform Cloud Native Forensics: Utilize cloud-native tools and APIs for evidence collection, analysis, and incident response within cloud environments.
6. Address Data Sovereignty & Jurisdictional Issues: Apply best practices and legal considerations for handling digital evidence across international boundaries in hybrid setups.

7. Identify & Analyze Containerized Workloads: Perform forensics on container technologies (Docker, Kubernetes) and their impact on evidence persistence.
8. Investigate Serverless Computing Incidents: Understand and investigate security incidents involving serverless functions and ephemeral resources.
9. Develop Hybrid Investigation Playbooks: Create structured methodologies and workflows for end-to-end forensic investigations in hybrid environments.
10. Leverage Automation for Hybrid Collection: Implement automated solutions for efficient and scalable artifact collection across on-premises and cloud infrastructures.
11. Analyze Hybrid Network Traffic: Correlate network data from traditional firewalls, cloud security groups, and virtual networks for comprehensive visibility.
12. Mitigate E-Discovery Complexities: Address the challenges of electronic discovery in hybrid environments, including data identification and preservation.
13. Present Hybrid Forensic Findings: Articulate complex technical findings from hybrid investigations clearly and defensibly in reports and testimony.

Organizational Benefits

1. Enhanced Incident Response Capability: Faster and more effective response to security incidents across hybrid infrastructures.
2. Reduced Investigation Costs: Streamlined processes and targeted evidence collection minimize resource expenditure.
3. Improved Legal Defensibility: Ensure forensically sound and admissible evidence from complex hybrid environments.
4. Mitigated Compliance Risk: Adherence to regulatory requirements for data handling and investigations in distributed systems.
5. Strengthened Security Posture: Deeper understanding of attack vectors and vulnerabilities unique to hybrid environments.
6. Optimized Cloud Security: Better utilization of cloud security features for proactive threat detection and incident readiness.
7. Proactive Threat Hunting: Ability to identify and track threats across interconnected on-premises and cloud systems.
8. Cross-Functional Collaboration: Fosters better understanding and cooperation between traditional IT, cloud operations, and security teams.
9. Protection of Critical Assets: Safeguard intellectual property and sensitive data regardless of its location (on-prem or cloud).
10. Reputation Management: Swift and effective handling of breaches in hybrid environments minimizes reputational damage.

Target Participants

- Digital Forensic Investigators

- Incident Responders
- Cloud Security Architects
- Security Operations Center (SOC) Analysts
- Cybersecurity Engineers
- IT Auditors
- Legal and Compliance Professionals
- Enterprise Architects
- Network Security Specialists
- System Administrators with security responsibilities

Course Outline

Module 1: Understanding Hybrid Environments & Forensic Foundations

- **Defining Hybrid Architectures:** On-premises, public, private, and multi-cloud integration models.
- **The Hybrid Attack Surface:** Unique vulnerabilities and threat vectors across interconnected environments.
- **Challenges of Hybrid Forensics:** Data sprawl, jurisdictional issues, shared responsibility model.
- **Forensic Principles Review:** Chain of custody, integrity, documentation, and legal admissibility.
- **Case Study: Anatomy of a Hybrid Cloud Breach**

Module 2: On-Premises & Endpoint Forensics in a Hybrid World

- **Traditional Endpoint Artifacts:** Windows, Linux, macOS logs, registry, memory, and file system.
- **Integrating Endpoint Detection & Response (EDR) Data:** Correlating EDR alerts with forensic artifacts.
- **Network Forensics on the Edge:** Firewall logs, proxy data, and network device analysis.
- **Virtualization Forensics:** Investigating virtual machines and hypervisor artifacts.
- **Case Study: Tracing an Attack from Cloud to On-Premises Domain Controller**

Module 3: Amazon Web Services (AWS) Forensics

- **AWS Service Overview for Forensics:** EC2, S3, CloudTrail, CloudWatch, GuardDuty, VPC Flow Logs.
- **Acquiring Evidence from AWS:** Snapshotting EC2 instances, S3 bucket analysis, log exports.
- **Analyzing AWS Logs & Artifacts:** CloudTrail events, GuardDuty findings, Config rules.
- **AWS Incident Response & Automation:** Using Lambda, Step Functions for automated collection.
- **Case Study: Investigating Unauthorized Access to an AWS S3 Bucket**

Module 4: Microsoft Azure Forensics

- **Azure Service Overview for Forensics:** Virtual Machines, Storage Accounts, Azure AD, Azure Monitor, Azure Sentinel.

- **Acquiring Evidence from Azure:** Disk snapshots, storage account analysis, diagnostic settings.
- **Analyzing Azure Logs & Artifacts:** Activity Logs, Diagnostic Logs, Azure AD audit logs.
- **Azure Incident Response & Automation:** Azure Functions, Logic Apps for forensic workflows.
- **Case Study: Forensic Analysis of a Compromised Azure VM**

Module 5: Google Cloud Platform (GCP) Forensics & Other Clouds

- **GCP Service Overview for Forensics:** Compute Engine, Cloud Storage, Cloud Logging, Security Command Center.
- **Acquiring Evidence from GCP:** VM snapshots, storage bucket inspection, log extraction.
- **Analyzing GCP Logs & Artifacts:** Audit Logs, VPC Flow Logs, Security Command Center findings.
- **Introduction to Other Cloud Forensics:** Oracle Cloud, Alibaba Cloud (brief overview of unique aspects).
- **Case Study: Investigating Data Exfiltration from GCP Storage**

Module 6: Cross-Platform & Correlative Analysis

- **Data Normalization & Timelining:** Standardizing data formats and creating unified timelines across hybrid sources.
- **Threat Intelligence Integration:** Enriching forensic data with IOCs and threat actor profiles.
- **Advanced Correlation Techniques:** Linking disparate logs, network flows, and system artifacts.
- **Big Data Forensics in Hybrid:** Utilizing tools for large-scale data analysis (Splunk, ELK Stack, Snowflake).
- **Case Study: Reconstructing a Sophisticated Multi-Stage Hybrid Attack**

Module 7: Specialized Hybrid Forensic Topics

- **Container & Orchestration Forensics:** Docker, Kubernetes, OpenShift - evidence collection and analysis.
- **Serverless & Function-as-a-Service (FaaS) Forensics:** Tracing ephemeral actions and execution logs.
- **DevOps & CI/CD Pipeline Forensics:** Investigating compromises in continuous integration/delivery workflows.
- **IoT & Edge Device Integration:** Forensic considerations for edge devices connecting to hybrid clouds.
- **Case Study: Compromise of a Containerized Application & Data Breach**

Module 8: Legal, Ethical & Reporting in Hybrid Environments

- **Jurisdictional Complexities & International Laws:** GDPR, CCPA, CLOUD Act implications for hybrid data.
- **Legal Holds & Data Preservation Strategies:** Ensuring compliance across diverse data locations.
- **Forensic Readiness in Hybrid Environments:** Preparing systems for efficient incident response.
- **Effective Reporting & Presentation:** Crafting clear, defensible reports for legal and technical audiences.
- **Case Study: Preparing Expert Testimony for a Cross-Border Hybrid Incident**

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
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

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

Register Online Now

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