Training Course on Cloud Forensics for AWS Environments

Professional Development Training Course Outline

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

Course Introduction

The rapid evolution of cloud computing has brought unprecedented scalability, flexibility, and efficiency to organizations worldwide. However, with this technological advancement comes the growing need for robust cloud forensics training, especially within Amazon Web Services (AWS) environments. As cyber threats escalate and data breaches become more sophisticated, mastering cloud forensics has become essential for cybersecurity professionals, incident responders, forensic analysts, and AWS practitioners. Training Course on Cloud Forensics for AWS Environments offers a deep dive into AWS-native security tools, forensic readiness, incident detection, data preservation, and chain of custody management in cloud-native architectures.

This hands-on course is designed to equip learners with real-world skills in cloud evidence acquisition, log analysis, AWS CloudTrail forensics, S3 bucket investigations, and IAM activity audits. Participants will gain cutting-edge knowledge to conduct secure, compliant, and effective forensic investigations within AWS. Each module integrates real-world case studies, showcasing how cloud forensics plays a critical role in cyber incident response, data breach investigations, and regulatory compliance such as GDPR, HIPAA, and SOC 2.

Programme Curriculum

Training Course on Cloud Forensics for AWS Environments

Introduction

The rapid evolution of cloud computing has brought unprecedented scalability, flexibility, and efficiency to organizations worldwide. However, with this technological advancement comes the growing need for robust cloud forensics training, especially within Amazon Web Services (AWS) environments. As cyber threats escalate and data breaches become more sophisticated, mastering cloud forensics has become essential for cybersecurity professionals, incident responders, forensic analysts, and AWS practitioners. Training Course on Cloud Forensics for AWS Environments offers a deep dive into AWS-native security tools, forensic readiness, incident detection, data preservation, and chain of custody management in

cloud-native architectures.

This hands-on course is designed to equip learners with real-world skills in cloud evidence acquisition, log analysis, AWS CloudTrail forensics, S3 bucket investigations, and IAM activity audits. Participants will gain cutting-edge knowledge to conduct secure, compliant, and effective forensic investigations within AWS. Each module integrates real-world case studies, showcasing how cloud forensics plays a critical role in cyber incident response, data breach investigations, and regulatory compliance such as GDPR, HIPAA, and SOC 2.

Course Objectives

1. Understand cloud forensics fundamentals in AWS environments
2. Identify and collect forensic evidence using AWS-native tools
3. Analyze AWS CloudTrail, S3, VPC, and Lambda logs for anomalies
4. Implement forensic readiness within AWS security architectures
5. Maintain integrity and chain of custody for cloud-based evidence
6. Automate evidence collection using AWS Lambda and Step Functions
7. Conduct incident triage and threat attribution in AWS
8. Perform memory and disk forensics on EC2 instances
9. Secure forensic data against tampering using encryption and IAM
10. Apply cloud forensic principles to ransomware and insider threat cases
11. Understand legal and regulatory implications of cloud forensics
12. Simulate AWS data breach investigations using real-world scenarios
13. Integrate cloud forensics in DevSecOps and continuous monitoring

Target Audience

1. Cloud Security Engineers
2. Cybersecurity Analysts
3. Digital Forensics Professionals
4. Incident Response Teams
5. AWS Cloud Practitioners
6. IT Risk & Compliance Officers
7. Penetration Testers
8. Security Operations Center (SOC) Analysts

Course Duration: 5 days

Course Modules

Module 1: Introduction to AWS Cloud Forensics

- Overview of cloud forensics in public cloud infrastructure
- AWS Shared Responsibility Model in digital investigations
- Legal and compliance considerations in AWS forensics
- AWS services relevant to forensic analysis
- Differences between traditional and cloud forensics
- **Case Study**: Overview of a GDPR investigation in an AWS-hosted environment

Module 2: Forensic Readiness in AWS

- Planning and implementing AWS forensic strategies
- Designing for evidence preservation and secure logging
- Creating an incident response plan within AWS
- Integrating AWS Config, GuardDuty, and Security Hub
- Setting up logging and monitoring policies for compliance

- **Case Study**: Preparing for forensic investigation in a PCI-DSS AWS workload

Module 3: Evidence Identification and Collection

- Capturing volatile and non-volatile data in EC2 instances
- Working with snapshots, volumes, and CloudTrail data
- Using AWS APIs and CLI for evidence gathering
- Network traffic analysis via VPC Flow Logs
- Preserving integrity: hashing, timestamps, and encryption
- **Case Study**: Insider threat investigation involving AWS S3 access logs

Module 4: AWS Log Analysis Techniques

- AWS CloudTrail, Config, and CloudWatch log correlation
- Filtering and querying logs for suspicious activities
- Using Athena and CloudTrail Lake for log analytics
- Detecting privilege escalation and brute force attacks
- Automating detection using AWS Lambda scripts
- **Case Study**: IAM role abuse detection via CloudTrail log patterns

Module 5: EC2 Forensics and Memory Acquisition

- Snapshotting EBS volumes for forensic imaging
- Capturing and analyzing memory from EC2 Linux/Windows
- Volatility and Rekall use in cloud memory forensics
- Malware detection in ephemeral cloud environments
- Securing forensic data with IAM policies and encryption
- **Case Study**: Crypto-mining malware found in EC2 instance memory

Module 6: S3 and Object Storage Investigations

- Investigating unauthorized access to S3 buckets
- Auditing bucket policies, ACLs, and access logs
- Detection of data exfiltration and public exposure
- Forensic recovery of deleted objects in S3
- Alerting using EventBridge and CloudWatch
- **Case Study**: Credential dump and ransomware staging in S3

Module 7: Automation and Response in AWS

- Building serverless forensic pipelines using Lambda
- Automating evidence collection using Step Functions
- Playbooks for common incident scenarios
- AWS Systems Manager for secure data retrieval
- Integrating SOAR tools for cloud-native response
- **Case Study**: Automating malware response in a hybrid AWS network

Module 8: Advanced Threats and Compliance Forensics

- Detecting APTs and persistent threats in AWS
- Using AWS Macie and Detective for threat hunting
- Mapping AWS forensic controls to frameworks (NIST, ISO)
- Cross-account investigation and auditing
- Chain of custody reporting and compliance documentation
- **Case Study**: HIPAA audit and multi-account AWS investigation

Training Methodology

- Interactive lectures using real AWS environments
- Hands-on labs with sandboxed AWS infrastructure
- Scenario-based learning with guided forensic walkthroughs
- Group case study analysis and incident simulation
- Post-training knowledge checks and certification assessment

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	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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