Training Course on Cloud Forensics for Azure 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

In the evolving landscape of digital transformation, cloud computing plays a vital role in how organizations manage data, applications, and infrastructure. With the increased adoption of Microsoft Azure, security incidents and cyber threats targeting cloud assets have surged. Training Course on Cloud Forensics for Azure Environments equips IT professionals, cybersecurity analysts, and digital forensic investigators with in-demand skills to identify, collect, preserve, and analyze digital evidence within Azure ecosystems. The course offers hands-on techniques using Microsoft tools and best practices tailored for Azure.

As cyberattacks grow in sophistication, understanding cloud-native forensic techniques, log analytics, and threat intelligence integration in Azure is critical. This course bridges the gap between traditional forensic practices and cloud-based environments, with a special focus on compliance, legal frameworks, and incident response. Through real-world case studies, guided labs, and modular learning, participants will emerge with practical skills essential to securing cloud assets and performing accurate forensic investigations in Microsoft Azure environments.

Programme Curriculum

Training Course on Cloud Forensics for Azure Environments

Introduction

In the evolving landscape of digital transformation, cloud computing plays a vital role in how organizations manage data, applications, and infrastructure. With the increased adoption of Microsoft Azure, security incidents and cyber threats targeting cloud assets have surged. Training Course on Cloud Forensics for Azure Environments equips IT professionals, cybersecurity analysts, and digital forensic investigators with in-demand skills to identify, collect, preserve, and analyze digital evidence within Azure ecosystems. The course offers hands-on techniques using Microsoft tools and best practices tailored for Azure.

As cyberattacks grow in sophistication, understanding cloud-native forensic techniques, log analytics, and threat intelligence integration in Azure is critical. This course bridges the gap between traditional forensic practices and cloud-based environments, with a special focus on compliance, legal frameworks, and incident response. Through real-world case studies, guided labs, and modular learning, participants will emerge with practical skills essential to securing cloud assets and performing accurate forensic investigations in Microsoft Azure environments.

Course Objectives

1. Understand core principles of cloud forensics in Azure environments.
2. Master Azure Security Center and Microsoft Defender for Cloud tools.
3. Conduct incident response using Azure-native services.
4. Perform forensic imaging and data acquisition from virtual machines.
5. Analyze and interpret Azure Activity Logs, Log Analytics, and Kusto Query Language (KQL).
6. Identify and collect chain-of-custody-compliant evidence in the cloud.
7. Integrate threat intelligence for forensic investigations.
8. Use automation in evidence gathering with Azure Logic Apps and Playbooks.
9. Assess compliance with GDPR, HIPAA, and other regulatory standards.
10. Deploy Azure Sentinel for threat detection and forensic analysis.
11. Explore forensics in multi-tenant and hybrid cloud environments.
12. Mitigate insider threats and ensure data sovereignty and integrity.
13. Apply machine learning tools for predictive forensics in cloud incidents.

Target Audiences:

1. Cybersecurity Analysts
2. Incident Responders
3. Cloud Security Engineers
4. Digital Forensic Investigators
5. Azure Administrators
6. IT Compliance Officers
7. Penetration Testers
8. Risk and Governance Professionals

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cloud Forensics in Azure

- Fundamentals of cloud computing and Azure architecture
- Differences between on-prem and cloud forensics
- Azure's Shared Responsibility Model
- Legal and compliance considerations
- Data volatility in the cloud
- **Case Study: Investigating a Suspicious Login in Azure Active Directory**

Module 2: Azure Logging and Monitoring for Forensics

- Understanding Azure Activity Logs and Diagnostic Logs
- Azure Monitor and Log Analytics Workspaces
- Creating alerts and data retention policies
- Introduction to Kusto Query Language (KQL)
- Forensic value of telemetry data
- **Case Study: Tracing a Privilege Escalation Attack Using Logs**

Module 3: Evidence Acquisition from Azure Virtual Machines

- VM snapshotting and disk acquisition
- Memory forensics in Azure environments
- Use of Azure Automation and Logic Apps for evidence collection
- Chain-of-custody procedures in cloud environments
- Exporting forensic images to secure storage
- **Case Study: Memory Dump Analysis of a Compromised Azure VM**

Module 4: Azure Sentinel and Threat Detection

- Overview of Azure Sentinel SIEM
- Setting up workbooks and analytic rules
- Leveraging MITRE ATT&CK framework
- Using built-in threat intelligence connectors
- Creating incident response playbooks
- **Case Study: Automated Threat Detection of Ransomware in Azure**

Module 5: Compliance and Legal Considerations

- Overview of GDPR, HIPAA, CCPA compliance in Azure
- Managing audit logs and regulatory requirements
- Legal hold and eDiscovery in cloud
- Jurisdiction and cross-border data concerns
- Role of compliance in forensic readiness
- **Case Study: Handling a Legal Discovery Request for Cloud Logs**

Module 6: Insider Threats and Data Breaches

- Common insider threat patterns in cloud environments
- Behavioral analysis and anomaly detection
- Limiting data exposure and data exfiltration detection
- Zero Trust implementation in Azure
- Real-time alerting and risk mitigation
- **Case Study: Insider Leak of Sensitive Files from OneDrive**

Module 7: Advanced Forensic Tools and Automation

- Using PowerShell and CLI for automation
- Azure Logic Apps and Functions in investigations
- Machine learning for predictive forensics
- Automation in evidence collection and triage
- Integrating forensic workflows with DevSecOps
- **Case Study: Automated Workflow to Capture Evidence During an Attack**

Module 8: Final Capstone and Live Forensic Simulation

- Live simulation of a breach in Azure
- Step-by-step incident response and investigation
- Collaborative team analysis and decision making
- Report writing and presenting forensic findings
- Debrief and lessons learned
- **Case Study: Full End-to-End Cloud Forensics Exercise in Azure**

Training Methodology

- Instructor-led interactive sessions with certified Azure security experts

- Hands-on lab exercises using Azure Sandbox environments
- Real-world case studies and scenario-based simulations
- Group-based collaborative forensic exercises
- Quizzes, assignments, and final capstone 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
19 Oct 2026	23 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
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