Training Course on Container Forensics

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 rapidly evolving cloud-native environments, containerization has become the cornerstone of DevOps and microservices architecture. While technologies such as Docker and Kubernetes offer scalability, speed, and portability, they also introduce complex security challenges and new attack surfaces. With cyber threats targeting container workloads, the need for skilled professionals in container forensics is more urgent than ever. Training Course on Container Forensics is designed to equip security analysts, forensic investigators, and DevOps teams with hands-on knowledge in investigating compromised containers, detecting advanced persistent threats (APTs), and implementing incident response strategies across containerized ecosystems.

This course delves deep into forensic techniques and investigative frameworks tailored for container environments. Participants will master key skills such as container log analysis, memory acquisition, file system investigation, audit trail reconstruction, and orchestrator (Kubernetes) forensics. Using real-world case studies, threat intelligence, and lab simulations, this program enhances capabilities in identifying indicators of compromise (IOCs), reverse engineering container images, and conducting forensic readiness in CI/CD pipelines. Designed with trending topics in cybersecurity and digital forensics, this course also integrates cloud-native forensics, runtime threat detection, and compliance auditing as core learning pillars.

Programme Curriculum

Training Course on Container Forensics

Introduction

In today’s rapidly evolving cloud-native environments, containerization has become the cornerstone of DevOps and microservices architecture. While technologies such as Docker and Kubernetes offer scalability, speed, and portability, they also introduce complex security challenges and new attack surfaces. With cyber threats targeting container workloads, the need for skilled professionals in container forensics is more urgent than ever. Training Course on Container Forensics is designed to equip security analysts, forensic investigators, and DevOps teams with hands-on knowledge in investigating compromised containers, detecting advanced persistent threats (APTs), and implementing incident response strategies

across containerized ecosystems.

This course delves deep into forensic techniques and investigative frameworks tailored for container environments. Participants will master key skills such as container log analysis, memory acquisition, file system investigation, audit trail reconstruction, and orchestrator (Kubernetes) forensics. Using real-world case studies, threat intelligence, and lab simulations, this program enhances capabilities in identifying indicators of compromise (IOCs), reverse engineering container images, and conducting forensic readiness in CI/CD pipelines. Designed with trending topics in cybersecurity and digital forensics, this course also integrates cloud-native forensics, runtime threat detection, and compliance auditing as core learning pillars.

Course Objectives

1. Understand the fundamentals of container technology (Docker, Kubernetes) and attack surfaces.
2. Perform live and static forensics on compromised containers.
3. Capture and analyze container logs, audit trails, and runtime data.
4. Identify Indicators of Compromise (IOCs) in container environments.
5. Conduct forensic analysis of Kubernetes clusters and nodes.
6. Reverse engineer container images to uncover malicious layers.
7. Use open-source container forensics tools effectively (e.g., Falco, Sysdig, Dive).
8. Apply threat intelligence to container investigations.
9. Automate container forensics in CI/CD and DevSecOps pipelines.
10. Map MITRE ATT&CK tactics and techniques to container threats.
11. Develop compliance-driven forensic documentation and reporting.
12. Integrate cloud-native forensics into AWS, Azure, and GCP environments.
13. Build a forensic readiness plan for microservices-based infrastructure.

Target Audience

1. **Cybersecurity Analysts** – Enhance skills in real-time container breach detection and investigation.
2. **Digital Forensics Investigators** – Learn specialized techniques for Docker and Kubernetes environments.
3. **Cloud Security Engineers** – Strengthen cloud-native container forensics and monitoring.
4. **DevSecOps Professionals** – Integrate forensics with CI/CD pipelines and security automation.
5. **IT Incident Responders** – Acquire skills to respond to container-based threats and security incidents.
6. **SOC Analysts** – Improve response workflows and alert triaging in containerized infrastructure.
7. **Penetration Testers & Ethical Hackers** – Understand post-exploitation traces in container breaches.
8. **Compliance & Risk Officers** – Gain awareness on evidence handling and forensic audits in regulated environments.

Course Duration: 5 Days

Course Modules

Module 1: Introduction to Container Security & Forensics

- Overview of Docker and Kubernetes architecture
- Threat landscape for containerized environments
- Differences between traditional and container forensics
- Common attack vectors in container ecosystems
- Overview of forensic methodologies for containers
- **Case Study:** Analysis of a container supply-chain attack (SolarWinds-style exploit)

Module 2: Log Analysis in Docker and Kubernetes

- Log sources: Docker logs, Kubernetes audit logs, journald
- Tools: EFK/ELK stack, Loki, Fluentd

- Timestamp correlation and container lifecycle logging
- Detecting anomalies and privilege escalation attempts
- Techniques for log retention and chain of custody
- **Case Study:** Investigating privilege escalation through Kubernetes audit logs

Module 3: Memory and Process Forensics in Containers

- Challenges in memory acquisition from ephemeral containers
- Using tools like Volatility with container images
- Identifying injected code and rogue processes
- Capturing and analyzing core dumps
- Memory forensics for runtime container analysis
- **Case Study:** Memory dump analysis of a cryptojacking container

Module 4: File System & Volume Forensics

- Investigating Docker image layers and filesystem diffs
- Persistence mechanisms within container volumes
- Hidden files and malicious binaries analysis
- Use of Dive, Binwalk, and container diff tools
- Immutable infrastructure and ephemeral data considerations
- **Case Study:** File system analysis of an image used in data exfiltration

Module 5: Kubernetes Cluster Forensics

- Forensics on control plane and worker nodes
- Kubelet, etcd, API server logs investigation
- RBAC misconfiguration and role escalation traces
- Container orchestration attack detection
- Evidence collection from pods, services, and namespaces
- **Case Study:** Post-incident analysis of a Kubernetes node breach

Module 6: Threat Hunting & MITRE ATT&CK Mapping

- Mapping container events to MITRE ATT&CK for Containers
- Threat detection with Falco and Sysdig rules
- IOC enrichment with threat intelligence feeds
- TTP correlation for adversary emulation
- Building detection rules in Kubernetes-native environments
- **Case Study:** Hunting for container breakout attempts using Falco

Module 7: CI/CD & DevSecOps Pipeline Forensics

- Integrating forensics into CI/CD pipelines
- Detection of poisoned container builds
- GitOps artifacts and audit trails investigation
- Supply chain compromise detection
- Automation of evidence collection post-deployment
- **Case Study:** Forensic response to a malicious GitHub Actions runner in CI

Module 8: Reporting, Compliance, and Forensic Readiness

- Legal considerations and forensic soundness
- Documentation and evidence handling best practices
- Compliance with NIST, ISO, GDPR, HIPAA standards

- Building a container forensics response playbook
- Reporting frameworks for audits and legal defense
- **Case Study:** GDPR compliance audit after a Kubernetes data breach

Training Methodology

- Hands-on labs using simulated container breach scenarios
- Live instructor-led sessions covering theoretical foundations
- Tool-based walkthroughs with Falco, Sysdig, Dive, Volatility, and ELK stack
- Group activities to solve real-world forensic case challenges
- Knowledge checks and quizzes after each module
- Final capstone project involving multi-step container incident investigation

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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