Training Course on Forensic Artifacts of Containerized Applications

Professional Development Training Course Outline

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

Course Introduction

Introduction

The rapid adoption of containerized applications and orchestration platforms like Kubernetes has revolutionized software deployment, offering unparalleled agility and scalability. However, this dynamic and often ephemeral environment presents significant new challenges for digital forensic investigations and incident response. Traditional host-centric forensic methodologies often fall short in complex container ecosystems, where processes are isolated, file systems are layered, and containers can be short-lived. Training Course on Forensic Artifacts of Containerized Applications provides an essential deep dive into forensic artifacts of containerized applications, equipping digital forensic investigators, incident responders, and DevOps security professionals with the unique methodologies and practical skills needed to effectively collect, preserve, analyze, and report on digital evidence from compromised containers and their orchestration layers. Participants will learn to navigate the intricacies of container runtimes, image layers, volumes, and orchestration logs, transforming transient data into cohesive actionable intelligence.

This intensive program moves beyond basic container knowledge, focusing on the nuances of container image analysis, live container forensics, persistent storage examination, and the critical role of orchestration platform logs (e.g., Kubernetes audit logs) in reconstructing an attack. Through extensive hands-on labs, real-world container compromise scenarios, and the application of cutting-edge open-source and commercial container forensic tooling, attendees will gain proficiency in examining Docker, Kubernetes, and other container technologies for signs of malware, data exfiltration, privilege escalation, and supply chain attacks. By the end of this course, you will be capable of leading complex investigations in the cloud-native landscape, building robust, legally defensible cases and fortifying your organization's security posture against threats targeting containerized environments.

Programme Curriculum

Training Course on Forensic Artifacts of Containerized Applications

Introduction

The rapid adoption of containerized applications and orchestration platforms like Kubernetes has revolutionized software deployment, offering unparalleled agility and scalability. However, this dynamic and often ephemeral environment presents significant new challenges for digital forensic investigations and incident response. Traditional host-centric forensic methodologies often fall short in complex container ecosystems, where processes are isolated, file systems are layered, and containers can be short-lived. Training Course on Forensic Artifacts of Containerized Applications provides an essential deep dive into forensic artifacts of containerized applications, equipping digital forensic investigators, incident responders, and DevOps security professionals with the unique methodologies and practical skills needed to effectively collect, preserve, analyze, and report on digital evidence from compromised containers and their orchestration layers. Participants will learn to navigate the intricacies of container runtimes, image layers, volumes, and orchestration logs, transforming transient data into cohesive actionable intelligence.

This intensive program moves beyond basic container knowledge, focusing on the nuances of container image analysis, live container forensics, persistent storage examination, and the critical role of orchestration platform logs (e.g., Kubernetes audit logs) in reconstructing an attack. Through extensive hands-on labs, real-world container compromise scenarios, and the application of cutting-edge open-source and commercial container forensic tooling, attendees will gain proficiency in examining Docker, Kubernetes, and other container technologies for signs of malware, data exfiltration, privilege escalation, and supply chain attacks. By the end of this course, you will be capable of leading complex investigations in the cloud-native landscape, building robust, legally defensible cases and fortifying your organization's security posture against threats targeting containerized environments.

Course Duration

5 Days

Course Objectives

1. Understand Container Architecture: Comprehend the components of containerization (Docker, containerd, runc), images, layers, and volumes.
2. Master Container Orchestration Forensics: Analyze the forensic implications of Kubernetes, OpenShift, and other orchestration platforms.

3. Conduct Forensically Sound Container Acquisition: Safely acquire container images, running container states, and associated host artifacts.
4. Perform Container Image Analysis: Deconstruct container image layers to identify embedded malware, vulnerabilities, and unauthorized changes.
5. Investigate Live Container Activity: Extract and analyze running processes, network connections, and volatile memory from active containers.
6. Examine Container Logs & Auditing: Interpret container runtime logs, application logs, and Kubernetes audit logs for malicious activity.
7. Analyze Persistent Storage & Volumes: Forensically examine mounted volumes, bind mounts, and persistent storage solutions used by containers.
8. Trace Container Privilege Escalation: Identify methods and evidence of privilege escalation within containers and to the host.
9. Detect Container Escape Attempts: Uncover indicators of attackers breaking out of containers to compromise the underlying host.
10. Identify Container Supply Chain Compromises: Analyze container build processes, registries, and CI/CD pipelines for evidence of injected malware or backdoors.
11. Leverage Specialized Container Forensic Tools: Proficiency in using open-source (e.g., crictl, Docker CLI, Kube-forensics, container-diff) and commercial tools.
12. Correlate Host & Container Artifacts: Integrate findings from the container, its host, and orchestration logs for a holistic view of the attack.
13. Generate Actionable Forensic Reports: Produce clear, concise, and legally defensible reports on containerized application forensic investigations.

Organizational Benefits

1. Rapid Cloud-Native Incident Response: Swiftly detect, contain, and remediate security incidents within containerized environments.
2. Minimized Breach Impact: Reduce potential financial and reputational damage from data loss or system compromise in containers.
3. Enhanced Forensic Capability: Develop in-house expertise to investigate the unique complexities of containerized applications.
4. Improved Security Posture: Insights from investigations inform better security controls and best practices for container adoption.
5. Stronger Compliance & Audit Readiness: Demonstrate robust incident handling for regulatory requirements in cloud-native deployments.
6. Protection of Critical Applications: Safeguard core business applications and data running within containers.
7. Better Supply Chain Security: Identify and mitigate risks stemming from compromised container images or build processes.

8. Optimized Tooling & Processes: Leverage specialized container forensic tools and methodologies effectively.
9. Reduced Downtime: More efficient and targeted investigations lead to quicker recovery from container compromises.
10. Competitive Advantage: Position as a leader in securing and responding to incidents in cutting-edge cloud-native architectures.

Target Participants

- Digital Forensic Investigators
- Incident Response Team Members
- DevOps Security Engineers
- Cloud Security Architects
- Cybersecurity Analysts (SOC Tier 2/3)
- Application Security Engineers
- Container Platform Administrators
- Threat Hunters
- Penetration Testers (interested in container post-exploitation)
- System Administrators managing container environments

Course Outline

Module 1: Containerization Fundamentals & Forensic Overview

- **Introduction to Containers:** Docker, runc, containerd, namespaces, cgroups.
- **Container vs. VM Forensics:** Key differences and new challenges.
- **Container Orchestration:** Kubernetes concepts (Pods, Deployments, Services, Namespaces).
- **Forensic Implications:** Ephemeral nature, layered file systems, shared kernel.
- **Case Study:** Understanding a simple container compromise scenario.

Module 2: Container Image Forensics

- **Docker Image Structure:** Layers, manifest, base images.
- **Image Layer Analysis:** Inspecting individual layers for added/modified files.
- **Vulnerability Scanning of Images:** Identifying known CVEs in image components.
- **Detecting Image Tampering:** Unauthorized changes, embedded malware.
- **Case Study:** Analyzing a suspicious container image for hidden malware.

Module 3: Live Container Forensics

- **Process Analysis:** Identifying running processes within containers (`docker top`, `crictl top`).
- **Network Connections:** Analyzing established connections (`netstat`, `ss` within container).
- **Volatile Memory Acquisition (Container):** Challenges and techniques for capturing container RAM.
- **File System Exploration (Live):** Using `docker exec` and `nsenter` for live file system access.
- **Case Study:** Investigating a running container showing signs of compromise.

Module 4: Container Logging & Auditing

- **Container Runtime Logs:** Docker logs, containerd logs.
- **Application Logs within Containers:** Best practices for collecting and analyzing.
- **Kubernetes Audit Logs:** Events related to API server requests (creation, deletion, updates).
- **Container Security Auditing Tools:** Falco, Open Policy Agent (OPA).
- **Case Study:** Tracing unauthorized access to a Kubernetes API via audit logs.

Module 5: Persistent Storage & Volume Forensics

- **Types of Container Volumes:** Bind mounts, Docker volumes, Kubernetes persistent volumes.
- **Forensic Acquisition of Volumes:** Imaging and analyzing underlying storage.
- **Data Recovery from Volumes:** Undeleting files from persistent storage.
- **Volume Snapshotting:** Using cloud provider snapshots for forensic copies.
- **Case Study:** Recovering deleted data from a compromised container's persistent volume.

Module 6: Host-Level Artifacts for Container Forensics

- **Container Runtime Files:** Docker daemon logs, /var/lib/docker directory structure.
- **Container Network Interfaces:** Analyzing docker0, CNI plugins, and network bridge configurations.
- **Linux Host Forensics Review:** Relevant kernel logs, auditd, process activity.
- **Correlating Host & Container Data:** Linking container events to host-level processes.
- **Case Study:** Identifying a container escape by analyzing host-level system calls.

Module 7: Orchestration Platform Forensics (Kubernetes Deep Dive)

- **Kubernetes Components & Logs:** Kube-API server, Kubelet, etcd, controller manager logs.
- **Pod & Deployment Forensics:** Analyzing YAML definitions for malicious configurations.
- **Network Policies & Service Mesh Forensics:** Understanding traffic flow and potential exfiltration.
- **Admission Controllers & Mutating Webhooks:** Detecting malicious injections during deployment.
- **Case Study:** Investigating a compromised Kubernetes Pod used for cryptomining.

Module 8: Tools, Best Practices & Emerging Trends

- **Container Forensic Tooling:** Dive into docker cp, docker export, docker commit, kubectl debug.
- **Specialized Tools:** container-diff, Dive, crictl, Kube-forensics.
- **Developing Container Incident Response Playbooks:** Strategy for rapid containment.
- **Future Trends:** Serverless forensics, WebAssembly, eBPF for deep visibility.
- **Case Study:** Comprehensive investigation and reporting for a containerized application breach.

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.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

Start Date	End Date	Location	Price
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
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