Training Course on Server Log and Application Log 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 ever-evolving cybersecurity landscape, server log analysis and application log forensics play a crucial role in detecting, analyzing, and responding to cyber incidents. Training Course on Server Log and Application Log Forensics equips cybersecurity professionals, IT administrators, and digital forensic analysts with the skills needed to monitor, analyze, and investigate log data from various environments such as cloud platforms, web servers, databases, and enterprise applications. With the exponential growth of cyber threats, log forensics has emerged as an essential discipline for uncovering attack patterns, insider threats, data breaches, and system anomalies.

This hands-on course focuses on real-world scenarios and provides participants with the ability to leverage industry-standard tools for log collection, correlation, and forensic reporting. By the end of this course, attendees will be proficient in recognizing malicious behavior, conducting timeline reconstructions, and generating comprehensive forensic reports to support incident response, legal investigations, and compliance. With a strong emphasis on SIEM integration, log parsing techniques, cloud log forensics, and advanced threat detection, this course is ideal for those aiming to fortify their cyber defense infrastructure.

Programme Curriculum

Training Course on Server Log and Application Log Forensics

Introduction

In today’s ever-evolving cybersecurity landscape, server log analysis and application log forensics play a crucial role in detecting, analyzing, and responding to cyber incidents. Training Course on Server Log and Application Log Forensics equips cybersecurity professionals, IT administrators, and digital forensic analysts with the skills needed to monitor, analyze, and investigate log data from various environments such as cloud platforms, web servers, databases, and enterprise applications. With the exponential growth of cyber threats, log forensics has emerged as an essential discipline for uncovering attack patterns, insider threats, data breaches, and system anomalies.

This hands-on course focuses on real-world scenarios and provides participants with the ability to leverage industry-standard tools for log collection, correlation, and forensic reporting. By the end of this course, attendees will be proficient in recognizing malicious behavior, conducting timeline reconstructions, and generating comprehensive forensic reports to support incident response, legal investigations, and compliance. With a strong emphasis on SIEM integration, log parsing techniques, cloud log forensics, and advanced threat detection, this course is ideal for those aiming to fortify their cyber defense infrastructure.

Course Objectives

1. Understand the fundamentals of log file architecture and forensic data integrity.
2. Master log correlation techniques for cyber threat analysis.
3. Identify and analyze security events using SIEM platforms.
4. Perform real-time log monitoring for anomaly detection.
5. Investigate web server logs for evidence of attacks.
6. Extract and decode application log artifacts.
7. Utilize machine learning tools for log-based threat intelligence.
8. Conduct cloud-native log forensics (AWS, Azure, GCP).
9. Implement log retention policies and ensure compliance readiness.
10. Reconstruct attacker timelines using log sequence analysis.
11. Leverage open-source forensic tools like ELK Stack and Graylog.
12. Detect insider threats through behavioral log analysis.
13. Develop comprehensive forensic reports for litigation and auditing.

Target Audience

1. Cybersecurity Analysts
2. IT Security Managers
3. Digital Forensics Investigators
4. SOC (Security Operations Center) Teams
5. Incident Response Professionals
6. Compliance & Risk Officers
7. System & Network Administrators
8. Cloud Security Engineers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Log Forensics

- Basics of log formats and types
- Log life cycle and integrity
- Role of logs in digital investigations
- Overview of forensic-ready systems
- Regulatory relevance of logs
- **Case Study:** Log analysis in a financial breach case

Module 2: Server Log Architecture

- Apache, NGINX, and IIS log formats
- System log structure (Linux, Windows)
- Event viewer & syslog parsing
- Centralized log management overview
- Common indicators in server logs

- **Case Study:** Tracing lateral movement via server logs

Module 3: Application Log Analysis

- Identifying application vulnerabilities via logs
- Parsing proprietary log formats
- Application crash forensics
- SQL injection & log evidence
- Integrating logs into SIEM
- **Case Study:** Mobile banking app breach analysis

Module 4: Log Collection and Preservation

- Centralized vs. decentralized logging
- Secure transport of logs (TLS, Syslog-ng)
- Chain of custody procedures
- Hashing and timestamping
- Archival strategies for forensic readiness
- **Case Study:** Compliance audit failure due to improper logging

Module 5: Web Server Log Forensics

- Access log and error log analysis
- Detecting XSS, LFI, and RFI attacks
- Identifying bot traffic and scraping
- Time-based log filtering
- Filtering malicious user-agent strings
- **Case Study:** Detecting DDoS via Apache logs

Module 6: Event Correlation and Timeline Reconstruction

- Identifying sequences in multi-source logs
- Mapping user actions across platforms
- Creating attack timelines
- Visual log analytics tools
- Pivoting techniques for threat hunting
- **Case Study:** Insider exfiltration reconstruction via logs

Module 7: SIEM and Log Analysis Tools

- Introduction to ELK Stack (Elasticsearch, Logstash, Kibana)
- Graylog and Wazuh basics
- Building dashboards for forensic alerts
- Integrating logs with threat intel feeds
- Use of Splunk for log-based investigations
- **Case Study:** Cloud data breach triage using SIEM

Module 8: Cloud Log Forensics

- AWS CloudTrail and CloudWatch analysis
- Azure Monitor and Sentinel logs
- Google Cloud Logging
- Correlating IAM and API logs
- Detecting shadow IT via logs
- **Case Study:** Unauthorized S3 access investigation

Module 9: Insider Threat Detection Using Logs

- Behavioral analytics
- Correlating login anomalies with activity
- USB, printing, and data export logging
- Use of UEBA tools
- Alerting on access patterns
- **Case Study:** Privileged access abuse detection

Module 10: Forensic Reporting and Legal Considerations

- Elements of a forensic log report
- Legal admissibility of logs
- Reporting templates and tools
- Expert witness considerations
- Presenting technical findings to non-technical audiences
- **Case Study:** Report submission in civil litigation

Module 11: Malware Detection via Logs

- Suspicious process creation events
- Registry and startup log entries
- Command and control detection
- Correlating antivirus alerts with logs
- Endpoint logging tools (Sysmon, EDR)
- **Case Study:** Malware infection detection using Windows logs

Module 12: Log Analysis in Mobile Environments

- Android and iOS app logs
- Device and emulator forensic techniques
- Logcat and system logs
- Cloud sync log inspection
- Network activity tracing
- **Case Study:** Chat app metadata recovery

Module 13: Log Forensics in Industrial Systems (ICS/SCADA)

- Unique log formats in OT environments
- Device-level event analysis
- Logging standards in critical infrastructure
- Detecting anomalies in HMI and PLC logs
- Challenges in air-gapped systems
- **Case Study:** ICS intrusion analysis via historian logs

Module 14: AI and ML in Log Forensics

- Training machine learning models on logs
- Anomaly detection algorithms
- NLP for log parsing
- Reducing false positives in alerts
- Pattern recognition in logs
- **Case Study:** AI-assisted phishing campaign detection

Module 15: Capstone Project and Simulation

- Log investigation lab
- Multi-stage attack scenario

- Incident timeline reconstruction
- Report writing and presentation
- Peer and instructor review
- **Case Study:** Simulated APT attack on a hybrid cloud network

Training Methodology

- Hands-on Labs using real-world forensic tools
- Interactive Simulations and scenario-based exercises
- Group Discussions and collaborative log reviews
- Expert-led Lectures with real-life case examples
- Capstone Projects with feedback
- Quizzes and Knowledge Checks for skill validation

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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