Training Course on Software Defined Networking (SDN) 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 the ever-evolving realm of cybersecurity, Software Defined Networking (SDN) has emerged as a transformative approach for optimizing and securing complex network infrastructures. However, the dynamic and programmable nature of SDNs presents unique forensic challenges, requiring specialized techniques to monitor, investigate, and respond to network incidents in real-time. Training Course on Software Defined Networking (SDN) Forensics is designed to equip professionals with cutting-edge skills in identifying, analyzing, and mitigating threats in SDN environments. The course delves into critical areas such as OpenFlow protocol forensics, control plane manipulation, malicious flow rule injection, and controller compromise analysis, ensuring participants gain a deep understanding of SDN-based cyber threats.

With cloud-native architectures, 5G, and IoT devices relying heavily on SDN frameworks, cybersecurity experts must evolve their approach to digital forensics and incident response. This course blends hands-on labs, real-world case studies, and open-source forensic tools to provide a comprehensive learning experience. Attendees will gain actionable knowledge to detect anomalous SDN behaviors, perform packet-level investigations, and uncover attack paths within programmable networks. By the end of this program, learners will be prepared to conduct robust network forensic investigations across modern SDN deployments.

Programme Curriculum

Training Course on Software Defined Networking (SDN) Forensics

Introduction

In the ever-evolving realm of cybersecurity, Software Defined Networking (SDN) has emerged as a transformative approach for optimizing and securing complex network infrastructures. However, the dynamic and programmable nature of SDNs presents unique forensic challenges, requiring specialized techniques to monitor, investigate, and respond to network incidents in real-time. Training Course on Software Defined Networking (SDN) Forensics is designed to equip

professionals with cutting-edge skills in identifying, analyzing, and mitigating threats in SDN environments. The course delves into critical areas such as OpenFlow protocol forensics, control plane manipulation, malicious flow rule injection, and controller compromise analysis, ensuring participants gain a deep understanding of SDN-based cyber threats.

With cloud-native architectures, 5G, and IoT devices relying heavily on SDN frameworks, cybersecurity experts must evolve their approach to digital forensics and incident response. This course blends hands-on labs, real-world case studies, and open-source forensic tools to provide a comprehensive learning experience. Attendees will gain actionable knowledge to detect anomalous SDN behaviors, perform packet-level investigations, and uncover attack paths within programmable networks. By the end of this program, learners will be prepared to conduct robust network forensic investigations across modern SDN deployments.

Course Objectives

1. Understand the architecture and components of Software Defined Networking (SDN).
2. Analyze the forensic implications of SDN's control and data plane separation.
3. Conduct packet analysis and flow tracking in SDN environments.
4. Perform forensic analysis using SDN-specific tools like Wireshark, OpenDaylight, and Ryu.
5. Detect and investigate malicious flow rule injections and DDoS attacks via SDN.
6. Investigate SDN controller logs and behavior for forensic evidence.
7. Evaluate flow table manipulation and identify abnormal flow patterns.
8. Conduct timeline reconstruction and incident response in programmable networks.
9. Develop skills in using open-source forensic toolkits tailored for SDN.
10. Perform forensic readiness planning in SDN-integrated cloud infrastructures.
11. Interpret real-time network traffic anomalies in SDN environments.
12. Apply threat hunting strategies for SDN-enabled networks.
13. Produce digital forensic reports with a focus on legal admissibility.

Target Audience

1. Network Forensics Analysts
2. Security Operations Center (SOC) Teams
3. Penetration Testers & Red Teamers
4. Cybersecurity Consultants
5. IT Risk and Compliance Officers
6. Cloud Security Engineers
7. Network Administrators & Engineers
8. Law Enforcement & Digital Forensics Investigators

Course Duration: 5 days

Course Modules

Module 1: Introduction to SDN and Forensics Fundamentals

- Overview of SDN architecture and technologies
- Introduction to network forensics principles
- Comparison between traditional and SDN forensics
- Role of SDN controllers in data capture
- Common SDN-based attack surfaces
- **Case Study:** Analysis of a flow spoofing incident in SDN

Module 2: SDN Components and Attack Vectors

- Understanding controllers, switches, and APIs
- Threat modeling in SDN environments

- Attack taxonomy specific to SDN architecture
- Identifying weak points in controller-switch communication
- Leveraging APIs for forensic traceability
- **Case Study:** Exploitation of OpenFlow for DDoS attacks

Module 3: OpenFlow Protocol Forensics

- Deep dive into OpenFlow packet structure
- Detecting malicious flow rule installations
- Analyzing flow table anomalies
- Collecting OpenFlow logs and messages
- OpenFlow version-specific forensic tactics
- **Case Study:** OpenFlow hijacking during a cloud breach

Module 4: SDN Controller Forensics

- Forensic acquisition from ONOS, Ryu, and OpenDaylight
- Parsing controller logs and traffic
- Reverse engineering controller configurations
- Identifying privilege escalation in controllers
- Log correlation for incident reconstruction
- **Case Study:** Controller compromise via northbound API injection

Module 5: Flow Rule Manipulation and Anomaly Detection

- Techniques to trace flow rule lifecycle
- Investigating stealthy rule insertion
- Traffic shaping and packet drop analysis
- Flow statistics for behavioral analysis
- Alerting on anomalous SDN behavior
- **Case Study:** Insider manipulation of critical flow entries

Module 6: SDN Forensic Tools and Automation

- Overview of forensic tools: Wireshark, Snort, Ryu forensic modules
- Automating log extraction and parsing
- Building custom detection scripts
- Using SIEMs with SDN data feeds
- Visualization and reporting dashboards
- **Case Study:** Automated flow monitoring during a ransomware incident

Module 7: Legal, Ethical, and Regulatory Aspects

- Chain of custody in programmable environments
- Legal considerations for SDN evidence collection
- Admissibility of SDN forensic data in court
- Regulatory compliance and SDN audit trails
- Ethics in programmable network investigations
- **Case Study:** Legal defense of forensic evidence from SDN logs

Module 8: Real-World Incident Response and Forensic Reporting

- Coordinated response to SDN-based intrusions
- Playbooks for SDN forensic readiness
- Documentation and evidence preservation
- Collaborative forensics in hybrid environments

- Report generation and stakeholder communication
- **Case Study:** Forensic investigation of multi-vector attack on SDN data center

Training Methodology

- Hands-on lab sessions using SDN testbeds and tools
- Real-world simulations and case-based learning
- Interactive lectures with forensic demos
- Group exercises and peer analysis
- Instructor-led walkthroughs of SDN attack scenarios
- Capstone project with final forensic investigation report

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
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
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