Training Course on VPN and Remote Access Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s cybersecurity landscape, Virtual Private Networks (VPNs) and remote access technologies have become essential for secure communication and remote work infrastructure. However, these technologies are frequently exploited by threat actors for malicious purposes including data exfiltration, anonymity masking, and unauthorized access. Training Course on VPN and Remote Access Forensics equips cybersecurity professionals with the skills to investigate and analyze VPN-based activities, uncover forensic artifacts, and track malicious behavior across encrypted and distributed networks.

As remote work accelerates globally, so does the need for skilled professionals capable of handling VPN-related incident response, performing deep packet inspection, log correlation, and understanding VPN tunneling protocols from a forensic perspective. This course will provide hands-on, real-world case studies, using industry-grade tools to examine complex cyber incidents involving remote desktop protocols, virtual tunneling, and cross-border threats. Whether defending an enterprise network or conducting a digital investigation, participants will gain comprehensive insight into network traffic analysis, endpoint telemetry, and zero-trust implementation challenges.

Programme Curriculum

Training Course on VPN and Remote Access Forensics

Introduction

In today’s cybersecurity landscape, Virtual Private Networks (VPNs) and remote access technologies have become essential for secure communication and remote work infrastructure. However, these technologies are frequently exploited by threat actors for malicious purposes including data exfiltration, anonymity masking, and unauthorized access. Training Course on VPN and Remote Access Forensics equips cybersecurity professionals with the skills to investigate and analyze VPN-based activities, uncover forensic artifacts, and track malicious behavior across encrypted and distributed networks.

As remote work accelerates globally, so does the need for skilled professionals capable of handling VPN-related incident response, performing deep packet inspection, log correlation, and understanding VPN tunneling protocols from a forensic perspective. This course will provide hands-on, real-world case studies, using industry-grade tools to examine complex cyber incidents involving remote desktop protocols, virtual tunneling, and cross-border threats. Whether defending an enterprise network or conducting a digital investigation, participants will gain comprehensive insight into network traffic analysis, endpoint telemetry, and zero-trust implementation challenges.

Course Objectives

1. Understand the fundamentals of VPN protocols and encrypted remote access.
2. Analyze VPN tunneling techniques (OpenVPN, IPSec, WireGuard) from a forensic standpoint.
3. Perform forensic analysis of remote desktop tools (RDP, TeamViewer, AnyDesk).
4. Trace and analyze anonymized traffic via commercial VPN services.
5. Conduct log forensics on VPN servers and client endpoints.
6. Correlate VPN metadata with user activity using SIEM tools.
7. Detect VPN misuse in cybercrime, fraud, and insider threat cases.
8. Investigate breach paths involving split tunneling and BYOD access.
9. Use packet capture tools (Wireshark, tcpdump) for encrypted traffic analysis.
10. Apply threat intelligence in identifying malicious VPN IPs and domains.
11. Interpret forensic evidence from remote session logs and virtual machines.
12. Report on forensic findings aligned with digital evidence standards.
13. Implement forensic readiness for VPN infrastructure in corporate environments.

Target Audience

1. Digital Forensics Investigators
2. Cybersecurity Analysts
3. Network Security Engineers
4. Incident Response Teams
5. Law Enforcement and Government Cyber Units
6. IT Security Consultants
7. Threat Intelligence Professionals
8. SOC (Security Operations Center) Personnel

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of VPN Technology & Remote Access

- VPN architecture and types (SSL, IPSec, L2TP, WireGuard)
- Remote access models and authentication protocols
- VPN encryption and tunneling methods
- Risks and attack vectors in VPN configurations
- Tools for VPN traffic monitoring
- **Case Study**: Forensic analysis of a misconfigured enterprise VPN breach

Module 2: Analyzing VPN Tunnels & Traffic

- Identifying VPN traffic in network captures
- Detecting anomalies and covert channels
- Deep packet inspection of encrypted VPN sessions
- Analyzing split tunneling and DNS leaks
- VPN traffic fingerprinting using open-source tools

- **Case Study**: Malicious exfiltration via split tunneling

Module 3: Remote Desktop and Access Tool Forensics

- Forensic artifacts from RDP, VNC, and SSH sessions
- Behavioral patterns of remote attackers
- Memory dumps and volatile evidence extraction
- Session recording and keylogging analysis
- Tracing lateral movement via remote tools
- **Case Study**: Insider threat investigation using remote access software

Module 4: VPN Log and Endpoint Analysis

- Collecting and parsing VPN server logs
- Endpoint telemetry for VPN client behavior
- Log correlation using SIEM platforms (Splunk, ELK)
- Time-line reconstruction from VPN metadata
- Detecting evasion tactics like VPN chaining
- **Case Study**: Tracking a credential stuffing campaign via VPN logs

Module 5: VPN Abuse in Cybercrime Investigations

- Role of VPNs in cybercrime (DDoS, fraud, ransomware)
- Mapping malicious IP ranges and VPN exit nodes
- VPN usage in dark web activities
- Leveraging OSINT and threat feeds for attribution
- Jurisdictional challenges in VPN investigations
- **Case Study**: Ransomware attack traced through multi-hop VPN

Module 6: Network Traffic Analysis for VPN Sessions

- Capturing VPN traffic using tcpdump and Wireshark
- Filtering and decoding VPN packets
- Decrypting VPN sessions (where possible) with keys
- Identifying unusual port and protocol usage
- Traffic baselining and anomaly detection
- **Case Study**: Data exfiltration detection via VPN in corporate network

Module 7: Remote Access Forensics in Cloud and BYOD

- Investigating VPN usage on mobile and BYOD devices
- VPN and remote access in hybrid cloud environments
- Cloud-native forensic approaches (AWS, Azure)
- Remote access security controls and logging
- VPN client-side artifacts in virtual machines
- **Case Study**: Cloud data leak via VPN-enabled mobile device

Module 8: Forensic Readiness and Reporting

- Building a VPN forensic readiness strategy
- Documentation and evidence preservation
- Legal and compliance considerations
- Reporting tools and templates for investigations
- Cross-team coordination for rapid response
- **Case Study**: Corporate audit following a remote access policy breach

Training Methodology

- Instructor-led live sessions (online or on-premise)
- Hands-on labs using real forensic tools (Wireshark, Autopsy, Splunk)
- Real-world scenarios and simulations
- Group exercises and live walkthroughs
- Capstone project and certification exam
- Post-training knowledge assessment

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100

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

Register Online Now

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