Training Course on Investigating Encrypted Network Traffic (TLS Inspection)

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 digital landscape, encrypted network traffic is a double-edged sword. While it protects data privacy and integrity, it also offers a hiding place for threat actors and malware. Training Course on Investigating Encrypted Network Traffic (TLS Inspection) equips cybersecurity professionals with the tools and knowledge to analyze encrypted data flows, detect malicious behaviors, and implement TLS decryption techniques without compromising privacy or legal compliance. This course bridges the gap between advanced network security operations and modern cryptographic standards, offering a deep dive into TLS/SSL inspection, network forensics, and intrusion detection in encrypted environments.

With the increasing adoption of TLS 1.3 and the growth of zero-trust architectures, understanding how to inspect encrypted network traffic is essential. This course is designed to provide hands-on experience with tools, frameworks, and real-world case studies to ensure learners are prepared for the evolving threat landscape. Participants will learn to configure and manage TLS visibility solutions, conduct deep packet inspection, and apply AI-driven anomaly detection techniques in encrypted environments—all crucial to cyber threat intelligence and incident response.

Programme Curriculum

Training Course on Investigating Encrypted Network Traffic (TLS Inspection)

Introduction

In today's digital landscape, encrypted network traffic is a double-edged sword. While it protects data privacy and integrity, it also offers a hiding place for threat actors and malware. Training Course on Investigating Encrypted Network Traffic (TLS Inspection) equips cybersecurity professionals with the tools and knowledge to analyze encrypted data flows, detect malicious behaviors, and implement TLS decryption techniques without compromising privacy or legal compliance. This course bridges the gap between advanced network security operations and modern cryptographic standards, offering a deep dive into TLS/SSL inspection, network forensics, and intrusion detection in encrypted environments.

With the increasing adoption of TLS 1.3 and the growth of zero-trust architectures, understanding how to inspect encrypted network traffic is essential. This course is designed to provide hands-on experience with tools, frameworks, and real-world case studies to ensure learners are prepared for the evolving threat landscape. Participants will learn to configure and manage TLS visibility solutions, conduct deep packet inspection, and apply AI-driven anomaly detection techniques in encrypted environments—all crucial to cyber threat intelligence and incident response.

Course Objectives

1. Understand TLS protocol internals and certificate validation mechanisms.
2. Analyze and decrypt encrypted traffic using TLS interception tools.
3. Implement secure and lawful SSL/TLS inspection policies.
4. Detect malware and threats hiding within encrypted streams.
5. Utilize advanced network forensic techniques for encrypted environments.
6. Monitor encrypted traffic in real-time using SIEM and IDS tools.
7. Detect TLS-based command and control (C2) channels.
8. Examine encrypted DNS (DoH/DoT) traffic patterns.
9. Apply AI/ML techniques to detect encrypted traffic anomalies.
10. Understand legal, ethical, and privacy implications of traffic decryption.
11. Design encrypted traffic monitoring in zero-trust networks.
12. Configure inline and passive TLS decryption appliances.
13. Conduct case-based investigations involving encrypted threat vectors.

Target Audiences

1. Cybersecurity Analysts
2. Network Security Engineers
3. Security Operations Center (SOC) Teams
4. Digital Forensics Experts
5. Incident Response Teams
6. Ethical Hackers and Pen Testers
7. Government & Law Enforcement IT Units
8. Compliance & Risk Officers

Course Duration: 5 days

Course Modules

Module 1: Introduction to TLS and Encrypted Traffic

- Overview of SSL/TLS protocols and versions
- The rise of encrypted network traffic in cybersecurity
- TLS 1.3 and its inspection challenges
- Role of certificates and PKI in encryption
- Trends in DoH/DoT encryption
- **Case Study: Analyzing a TLS 1.3 encrypted malware campaign**

Module 2: Legal and Ethical Considerations

- Privacy laws and regulations (GDPR, HIPAA, CCPA)
- Legal frameworks around TLS inspection
- Risk of data exposure and compliance violations
- Ethical boundaries in decrypting user traffic
- Consent and transparency in network monitoring

- **Case Study: TLS decryption audit in a healthcare network**

Module 3: TLS Inspection Architecture & Deployment Models

- Inline vs. passive TLS inspection
- TLS proxies and SSL interception appliances
- Load balancing and failover considerations
- Certificate management and key handling
- Performance impact of inspection on network speed
- **Case Study: Building a scalable TLS visibility solution in an enterprise**

Module 4: Tools and Techniques for TLS Decryption

- Wireshark and Zeek for encrypted traffic analysis
- MITM tools: sslsplit, mitmproxy
- Using decryptable test environments
- TLS fingerprinting with JA3/JA3S
- Decryption using enterprise firewalls
- **Case Study: Investigating a phishing campaign through SSL logs**

Module 5: Detection of Malicious Behavior in Encrypted Traffic

- TLS C2 detection strategies
- Detecting malware beacons in encrypted flows
- Traffic flow analysis without decryption
- Behavior-based detection in encrypted sessions
- Using AI/ML to detect TLS anomalies
- **Case Study: Identifying a ransomware attack hidden in TLS tunnels**

Module 6: Monitoring and Logging Encrypted Traffic

- Integrating TLS logs with SIEM systems
- Real-time encrypted traffic dashboards
- Log retention policies and chain of custody
- Combining NetFlow and TLS inspection data
- Alerting rules and threat hunting playbooks
- **Case Study: SIEM-based detection of exfiltration via HTTPS**

Module 7: Handling Encrypted DNS (DoH/DoT)

- Overview of encrypted DNS protocols
- Blocking vs. monitoring strategies
- DNS fingerprinting for DoH/DoT
- Bypassing DNS encryption in enterprises
- Analyzing encrypted DNS with passive DNS tools
- **Case Study: Data exfiltration via DoH in a corporate network**

Module 8: Future of Encrypted Traffic Monitoring

- The impact of quantum encryption on TLS
- TLS 1.3 session resumption and zero RTT
- Encrypted SNI (ESNI) implications
- Federated learning in encrypted traffic analytics
- Policy development for future TLS standards
- **Case Study: Preparing an organization for TLS 1.4 implementation**

Training Methodology

- Interactive instructor-led sessions and virtual labs
- Hands-on use of open-source and commercial TLS inspection tools
- Case-driven learning with real-world encrypted threat scenarios
- Group-based discussions on legal and ethical issues
- Live packet capture and forensic investigation exercises
- Post-training assessments and certification test

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
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
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

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

Register Online Now

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