

Network Forensics: Packet Analysis & Log Correlation

12

MODULES

41

TOPICS

LEARNING OBJECTIVES

- Explain digital evidence concepts and investigation methodologies
- Identify sources of network-based evidence in IP internetworking
- Apply active acquisition using network traffic acquisition software
- Analyse network packets, protocols, flows and higher layer traffic
- Interpret statistical flow data from sensors and export protocols
- Assess wireless traffic captures for common attacks and device location
- Evaluate intrusion detection modes and Snort packet logging output
- Correlate event logs and evidence from switches, routers and firewalls

12 Modules, 41 Topics

01

Investigation Strategies

TOPICS

Concepts of Digital Evidence · Challenges Relating to Evidence · Network Forensics Investigation Methodologies

02

Technical Fundamentals

TOPICS

Source of Network Based Evidence · Principals of Internetworking · IP Suite

03

Evidence Acquisition

TOPICS

Network Traffic Acquisition Software · Active Acquisition

04

Network Packet Analysis

TOPICS

Protocol Analysis · Packet Analysis · Flow Analysis · Higher Layer Traffic Analysis

05

Statistical Flow Analysis

TOPICS

Sensor · Flow Record Export Protocol · Collection and Aggregation · Analysis

06

Wireless Network Forensics

TOPICS

Wireless Traffic Capture and Analysis · Common Attacks · Locating Wireless Devices

07

Network Intrusion Detection and Analysis

TOPICS

NIDS/NIPS Functionality · Modes of Detection · Snort and Packet Logging

08

Event Log Aggregation, Correlation and Analysis

TOPICS

Source of Logs · Network Log Architecture · Collecting and Analyzing Evidence

09

Switches, Routers and Firewalls

TOPICS

Switches: Why Investigate Switches? · Content-Addressable Memory Table · Switch Evidence · **Router:** Why Investigate Routers? · Router Evidence · Logging

10

Web Proxies

TOPICS

Web Proxy Functionality · Evidence under Web Proxy · Web Proxy Analysis · Encrypted Web Traffic

11

Network Tunneling

TOPICS

Covert Tunneling · DNS Tunnels · ICMP Tunnel Analysis

12

Malware Forensics

TOPICS

Botnets · Encryption and Obfuscation · Network Behavior of Malware

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

[Visit koenig-solutions.com](https://www.koenig-solutions.com)[✉ info@koenig-solutions.com](mailto:info@koenig-solutions.com)