KOENIG
step forward

Digital Forensic : Network Forensics Investigation

Module -1 (Investigation Strategies)

Concepts of Digital Evidence

Challenges Relating to Evidence

Network Forensics Investigation Methodologies

Module -2 (Technical Fundamentals)

Source of Network Based Evidence

Principals of Internetworking

IP Suite

Module - 3(Evidence Acquisition)

Network Traffic Acquisition Software

Active Acquisition

Module - 4 (Network Packet Analysis)

Protocol Analysis

Packet Analysis

Flow Analysis

Higher layer traffic Analysis

Module - 5 (Statistical Flow Analysis)

Sensor

Flow Record Export Protocol

Collection and Aggregation

Analysis

Module - 6 (Wireless Network Forensics)

Wireless traffic capture and analysis

Common Attacks

Locating Wireless Devices

Module - 7 (Network Intrusion Detection and Analysis)

NIDS/NIPS Functionality

Modes of Detection

Snort and packet logging

Module - 8 (Event Log Aggregation, Correlation and Analysis)

Source of Logs

Network Log Architecture

Collecting and Analyzing Evidence

Module - 9 (Switches, Routers and Firewalls)

Switches: Why Investigate Switches?

Content-Addressable Memory Table

Switch Evidence

Router: Why Investigates Routers?

Router Evidence

Logging

Module - 10 (Web Proxies)

Web Proxy Functionality

Evidence under Web Proxy

Web Proxy Analysis

Encrypted Web Traffic

Module - 11 (Network Tunneling)

Covert Tunneling

DNS Tunnels

ICMP Tunnel Analysis

Module - 12 (Malware Forensics)

Botnets

Encryption and Obfuscation

Network Behavior of Malware