Certified Network Forensics Examiner (CNFE)

Modality: On Demand

Duration: 19 Hours

About this Course:

In this course students will go through 20+ modules of Network Forensic topics. This course will introduce students to examining network forensics. Topics covered include investigative methodology, physical interception, wireless traffic capture and analysis, malware forensics, and more.

The avaerage salary of Network Forensics Examiner is approx **$99000** per year.

Course Objecives:

Certified Network forensics Examiner students will have knowledge to perfom network forensic examinations. be able to accurately report on their findings, and will be ready to take CNFE Exam

Audience:

- Digital and Network Forensic Examiners
- IS Managers
- Netword Auditors
- IT Managers

Course Outline:

This Course Includes:

- Module 1 - Digital Evidence Concepts
- Module 2 - Network Evidence Challenges
- Module 3 - Network Forensics Investigative Methodology
- Module 4 - Network-Based Evidence
- Module 5 - Network Principles
- Module 6 - Internet Protocol Suite
- Module 7 - Physical Interception
- Module 8 - Traffic Acquisition Software
- Module 9 - Live Acquisition
- Module 10 - Layer 2 Protocol
- Module 11 - Protocol Analysis
- Module 12 - Wireless Access Points
- Module 13 - Wireless Traffic Capture and Analysis
- Module 14 - NIDS/Snort

- Module 15 - Centralized Logging and Syslog
- Module 16 - Investigating Network Devices
- Module 17 - Web Proxies and Encryption
- Module 18 - Network Tunneling
- Module 19 - Malware Forensics
- Module 20 - Network Forensics and Investigating Logs