

## Certified Network Forensic Examiner



The Certified Network Forensic Examiner certification course was originally developed for the U.S. government, and has now been made available to city, county, and state law enforcement agencies. Civilian personnel outside the law enforcement community are also authorized to attend on a case-by-case basis. This comprehensive course brings digital and network forensic core competencies to advanced levels by presenting students with 20 detailed learning objectives and a series of practical lab exercises. Students will be provided with both experiential knowledge and practical skills that simulate real-world scenarios, investigations, and recovery of evidentiary data in systems and networks. With a specific focus on the centralizing and investigating of logging systems and network devices, students will cover topics such as: Network-Based Evidence and Investigative Methodologies; Wireless Traffic Capture and Analysis; and, Web Proxies and Encryption.

Duration: 5 Days

CPE Credits: 40

Course Fee: \$3,500

### Learning Objectives

- |  |   |
|--|---|
| 01) Digital Evidence Concepts                    | 11) Protocol and Flow Analysis                    |
| 02) Network Evidence Challenges                  | 12) Wireless Access Points                        |
| 03) Network Forensic Investigative Methodologies | 13) Wireless Traffic Capture and Analysis         |
| 04) Network-Based Evidence                       | 14) NIDS and NIPS Evidence Acquisition            |
| 05) Network Principles                           | 15) Centralized Logging and Syslog                |
| 06) Internet Protocol Suite                      | 16) Investigating Network Devices                 |
| 07) Physical Interception                        | 17) Web Proxies and Encryption                    |
| 08) Traffic Acquisition Software                 | 18) Network Tunneling                             |
| 09) Principles of Live Acquisition               | 19) Malware Forensics                             |
| 10) IEEE Layer Two Protocol Series               | 20) Investigation, Analysis, and Legality of Logs |

### Hardcopy Training Materials



Course Text / Workbook  
Course Lab Manual  
Supplemental Handout  
Text: Key Security Concepts  
Exam Prep Study Guide  
USB Drives

### Digital Training Materials



Course Text / Workbook  
Course Lab Manual  
Course Video Series  
Exam Prep Study Guide  
Exam Simulator  
CPE Credit Certificate

Certification examination is included in the course fee.



The Certified Network Forensic Examiner course is a component of the career progression track that supports the following Categories, Specialty Areas, and Work Roles as defined by the [National Initiative for Cybersecurity Education \(NICE\) Cybersecurity Workforce Framework](#):

- |   |   |
|---|---|
| Exploitation Analyst<br>(AN-EXP-001)              | Cyber Crime Investigator<br>(IN-INV-001)        |
| Law Enforcement Forensics Analyst<br>(IN-FOR-001) | All Source – Collection Manager<br>(CO-CLO-001) |
| Cyber Intel Planner<br>(CL-OPL-001)               | Cyber Defense Forensics Analyst<br>(IN-FOR-002) |

**Average Yearly Salary:**  
**\$71,000**