

**Norman-Benjamin Consulting**  
**www.norman-benjamin.com**  
Phone: 317.362.7267  
Fax: 317.773.8905  
contact@norman-benjamin.com



## Training Program Information

---

### **Course Outline**

**Note:** EC-Council's fundamental courses are conducted by selected academic partners such as colleges and universities around the world.

#### Module 1: Computer Forensics fundamentals

- Definition of Computer Forensics
- Evolution of Computer Forensics
- Need for Computer Forensics
- Cyber Crime
- Examples of Cyber Crime
- Cyber Crime Investigation Process
- Challenges in Cyber Crime Investigation
- Investigative Agencies : FBI
- Investigative Agencies : National Infrastructure Protection Center
- Reporting Security Breaches To Law Enforcement Agencies In The U.S.A
- Cyber Laws
- Approaches To Formulation Of Cyber Laws
- Some Areas Addressed By Cyber Law
- Important Federal Statutes

#### Module 2: Trademark, copyright and patents

- Trademarks
- Trademark Eligibility and Benefits of Registering It
- Trademark Infringement
- Trademark Search
- Copyright and Copyright Notice
- Investigating Copyright Status of a Particular Work
- How Long Does a Copyright Last?

- U.S Copyright Office
- Doctrine of “Fair Use”
- How are Copyrights Enforced?
- SCO vs. IBM
- Plagiarism
- Turnitin
- Plagiarism Detection Tools

### Module 3: Network and Router Forensics Fundamentals

- Challenges in Network Forensics
- Internal Threat
- External Threat
- Automated Computer Attack
- Sources of Evidence on a Network
- Tool: Ethereal
- What is a Router?
- Functions of a Router
- A Router in an OSI Model
- Types of Router Attacks
- Packet “Mistreating” Attacks
- Routing Table Poisoning
- Router Forensics Vs. Traditional Forensics
- Incident Response & Session Recording
- Investigating Routers
- Accessing the Router
- Router Investigation Steps

### Module 4: Incident Response and Forensics

- What is an Incident?
- How to Identify an Incident?
- Reporting an Incident
- Pointers to Incident Reporting Process
- Procedure for Handling Incidents
- 1. Preparation
- 2. Identification
- 3. Containment

- 4. Eradication
- 5. Recovery (restoring system to its normal mission)
- 6. Follow up
- CSIRT Overview
- Need for CSIRT

## Module 5: Digital Evidence

- Introduction to Digital Evidence
- Rules of Evidence
- Evidence Life Cycle
- Digital Evidence Investigative Process
- Securing Digital Evidence
- Documenting Evidence
- Handling Digital Evidence in a Forensics Lab
- Obtaining a Digital Signature and Analyzing It
- Processing Digital Evidence
- Storing Digital Evidence
- Evidence Retention and Media Storage Requirements
- Forensic Tool: Hex2text
- Forensic Tool: File Date Time Extractor

## Module 6: Understanding Windows, DOS, Linux and Macintosh

## Module 7: Steganography

- Definition of Steganography
- Steganography Vs. Cryptography
- Image Steganography - Overview
- Strides in Steganography
- Steganography - Steps in hiding Information
- Types of Steganography
- Real World Applications of Steganography
- Practical Applications of Steganography
- Unethical use of Steganography

- The Steganography Tree
- Hiding Information In Text Files
- Hiding Information In DNA
- Steganography tool: fort knox
- Steganography tool: Stegowatch

#### Module 8: Analyzing logs

- Importance of Logs in Forensics
- Security Logging
- Application Logs
- Examining Intrusion and Security Events
- Logging in Unix / Linux -Syslog
- Remote Logging with Syslog
- Logging in Windows
- Remote Logging in Windows
- ntsyslog
- Significance of Synchronized Time
- Event Gathering
- EventCombMT
- Writing Scripts
- Event Gathering Tools
- Forensic tool: fwanalog

#### Module 9: E-mail crime and computer forensics

- Understanding Internet Protocols
- Exploring the Roles of the Client and Server in E-mail
- Identifying E-mail Crimes and Violations
- Investigating E-mail Crime and Violation
- Sending E-mail Using Telnet
- Viewing E-mail Headers
- Examining an E-mail Header
- Tracing an E-mail Message
- Using Network Logs Related to E-mail
- Using Specialized E-mail Forensic Tools
- Tool:FINALeMAIL
- Tracing Back
- Tracing Back Web Based E-mail

- Searching E-mail Addresses
- E-mail Search Site
- Tool:eMailTrackerPro

#### Module 10: Introduction to writing investigative reports

- Significance of Investigative Reports
- Report Specifications
- Report Classification
- What to Include in an Investigative Report
- Layout of an Investigative Report
- Writing Report
- Investigative Report Format
- Report and Expert Opinion
- Use of Supporting Material
- Importance of Consistency
- Salient Features of a Good Report

#### Module 11: Computer Forensics as a Profession

- Developing Computer Forensics Resources
- Preparing for Computing Investigations
- Understanding Enforcement Agency Investigations
- Understanding Corporate Investigations
- Maintaining Professional Conduct