EC-Council Digital Forensics Essentials (DFE)

Category: Networking & Security | **Vendor:** EC-Council

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course will introduce learners to Computer Forensics Fundamentals as well as the Computer Forensics Investigation Process. Plan to learn about Dark Web, Windows, Linux, Malware Forensics, and so much more! The interactive labs component of this course ensures that learners receive the hands-on, practical experience required for a future in digital forensics. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versusmachine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

About This Course

This course will introduce learners to Computer Forensics Fundamentals as well as the Computer Forensics Investigation Process. Plan to learn about Dark Web, Windows, Linux, Malware Forensics, and so much more! The interactive labs component of this course ensures that learners receive the hands-on, practical experience required for a future in digital forensics. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versusmachine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

Who Should Attend

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- High school students who want to get an early start on their cybersecurity careers and master the fundamentals of security online.
- College or university students interested in preparing for a cybersecurity career and aiding their IT education.
- Working professionals who want to get into the cybersecurity field and don’t know where to start their education journey.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Key issues plaguing the computer forensics Different types of digital evidence Computer forensic investigation process and its phases Different types of disk drives and file systems Data acquisition methods and data acquisition methodology Anti-forensics techniques and countermeasures Volatile and non-volatile information gathering from Windows, Linux, and Mac Systems Network forensics fundamentals, event correlation, and network traffic investigation Web server logs and web applications forensics Dark web forensics Email crime investigation Malware forensics fundamentals and different types of malware analysis

Detailed Course Outline

Module 01: Computer Forensics Fundamentals

- Fundamentals of Computer Forensics
- Digital Evidence
- Forensic Readiness
- Roles and Responsibilities of a Forensic Investigator
- Legal Compliance in Computer Forensics

Module 02: Computer Forensics Investigation Process

- Forensic Investigation Process and its Importance
- Forensic Investigation Process – Pre-Investigation Phase
- Forensic Investigation Process – Investigation Phase
- Forensic Investigation Process - Post investigation Phase

Module 03: Understanding Hard Disks and File Systems

- Different Types of Disk Drives and their Characteristics
- Logical Structure of a Disk
- Booting Process of Windows, Linux, and Mac Operating Systems
- File Systems of Windows, Linux, and Mac Operating Systems
- File System Examination

Module 04: Data Acquisition and Duplication

- Data Acquisition Fundamentals
- Types of Data Acquisition
- Data Acquisition Format
- Data Acquisition Methodology

Module 05: Defeating Anti-forensics Techniques

- Anti-Forensics and its Techniques
- Anti-Forensics Countermeasures

Module 06: Windows Forensics

- Volatile and Non-Volatile Information
- Windows Memory and Registry Analysis
- Cache, Cookie, and History Recorded in Web Browsers
- Windows Files and Metadata

Module 07: Linux and Mac Forensics

- Volatile and Non-Volatile Data in Linux
- Analyze Filesystem Images Using The Sleuth Kit
- Memory Forensics
- Mac Forensics

Module 08: Network Forensics

- Network Forensics Fundamentals
- Event Correlation Concepts and Types
- Identify Indicators of Compromise (IoCs) from Network Logs
- Investigate Network Traffic

Module 09: Investigating Web Attacks

- Web Application Forensics
- IIS and Apache Web Server Logs
- Investigating Web Attacks on Windows-based Servers
- Detect and Investigate Attacks on Web Applications

Module 10: Dark Web Forensics

- Dark Web
- Dark Web Forensics
- Tor Browser Forensics

Module 11: Investigating Email Crimes

- Email Basics
- Email Crime Investigation and its Steps

Module 12: Malware Forensics

- Malware, its Components and Distribution Methods
- Malware Forensics Fundamentals and Recognize Types of Malware Analysis
- Static Malware Analysis
- Analyze Suspicious Word Documents
- Dynamic Malware Analysis
- System Behavior Analysis
- Network Behavior Analysis

Frequently Asked Questions

Q: What delivery options are available for EC-Council Digital Forensics Essentials (DFE)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day EC-Council Digital Forensics Essentials (DFE) course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council Digital Forensics Essentials (DFE) training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council Digital Forensics Essentials (DFE)?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council Digital Forensics Essentials (DFE). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for EC-Council Digital Forensics Essentials (DFE)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council Digital Forensics Essentials (DFE) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)