DFE – Digital Forensic Essentials (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 11h

Sobre o curso

Spring Deals: Cursos EC-Council com 5% de desconto até 30 de abril

The **Digital Forensics Essentials (DFE)** is an entry-level foundational course to help beginners grasp the facets of digital forensics investigation, its phases, and types. This course covers topics like dark web forensics, Linux, investigating web applications, and more. No IT/Cybersecurity experience required for this course.

Test your skills with CTF-based Capstone Project and validate these newly acquired skills in proctored exams. The DFE course aims to enhance your competency and expertise in digital forensics and information security skills offering 12 comprehensive modules, 11 hours of premium self-paced video training, courseware, and 11 labs.

Key Features:

- 11+ hours of premium self-paced video training
- 11 lab activities in a simulated lab environment
- 750+ pages of eCourseware
- Capstone Project
- Year-long access to courseware and labs
- Globally recognized EC-Council's Certification
- Proctored exam voucher with 1-year validity
- Increase your value in the job market to advance your career

What skills you'll learn:

- Key issues plaguing 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

---

Destinatários

Who is DFE for?

- High School/ College/University students
- Teams and Organizations
- Career Starters
- Working Professionals

Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

Metodologia

Exam Details:

- Exam Code: 112-57
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Programa

- Computer Forensics Fundamentals
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Investigating Web Attacks

- Dark Web Forensics
- Investigating Email Crimes
- Malware Forensics

Computer Forensics Fundamentals

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

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

Labs:

- Performing Hash or HMAC Calculations
- Comparing Hash Values of Files to Check Their Integrity or Viewing Files of Various Formats
- Creating a Disk Image File of a Hard Disk Partition

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

Labs:

- Analyzing File System of a Linux Image
- Recovering Deleted Files from Hard Disks

Data Acquisition and Duplication

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

Labs:

- Creating a dd Image of a System Drive
- Converting Acquired Image File to a Bootable Virtual Machine
- Acquiring RAM from Windows Workstations
- Viewing Contents of Forensic Image File

Defeating Anti-forensics Techniques

- Anti-forensics and its Techniques
- Anti-forensics Countermeasures

Labs:

- SSD File Carving on a Windows File System
- Recovering Data from Lost / Deleted Disk Partition
- Cracking Application Passwords
- Detecting Steganography

Windows Forensics

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

Labs:

- Acquiring Volatile Information from a Live Windows System
- Investigating Forensic Image of Windows RAM
- Examining Web Browser Artifacts
- Extracting Information about Loaded Processes on a Computer

Linux and Mac Forensics

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

Labs:

- Forensic Investigation on a Linux Memory Dump
- Recovering Data from a Linux Memory Dump

Network Forensics

- Network Forensics Fundamentals

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

Labs:

- Identifying and Investigating Various Network Attacks using Wireshark

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

Labs:

- Identifying and Investigating Web Application Attacks Using Splunk

Dark Web Forensics

- Dark Web
- Dark Web Forensics
- Tor Browser Forensics

Labs:

- Detecting TOR Browser on a Machine
- Analyzing RAM Dumps to Retrieve TOR Browser Artifacts

Investigating Email Crimes

- Email Basics
- Email Crime Investigation and its Steps

Lab:

- Investigating a Suspicious Email

Malware Forensics

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

- Network Behavior Analysis

Lab Exercise:

- Performing Static Analysis on a Suspicious File
- Forensic Examination of a Suspicious Microsoft Office Document
- Performing System Behavior Analysis