INFOSECTRAIN
Educate. Excel. Empower.

DIFE

Digital Forensics Essentials Training

Course Highlights

16-Hour Instructor-Led Training

Learn from Certified and Experienced DF Professionals

Hands-on Labs with Real-World Forensic Investigations

Forensic Tools: Autopsy, FTK Imager, Volatility, Wireshark

Dark Web, Malware & Anti-Forensics Awareness

Interview Preparation for Digital Forensics & SOC Roles

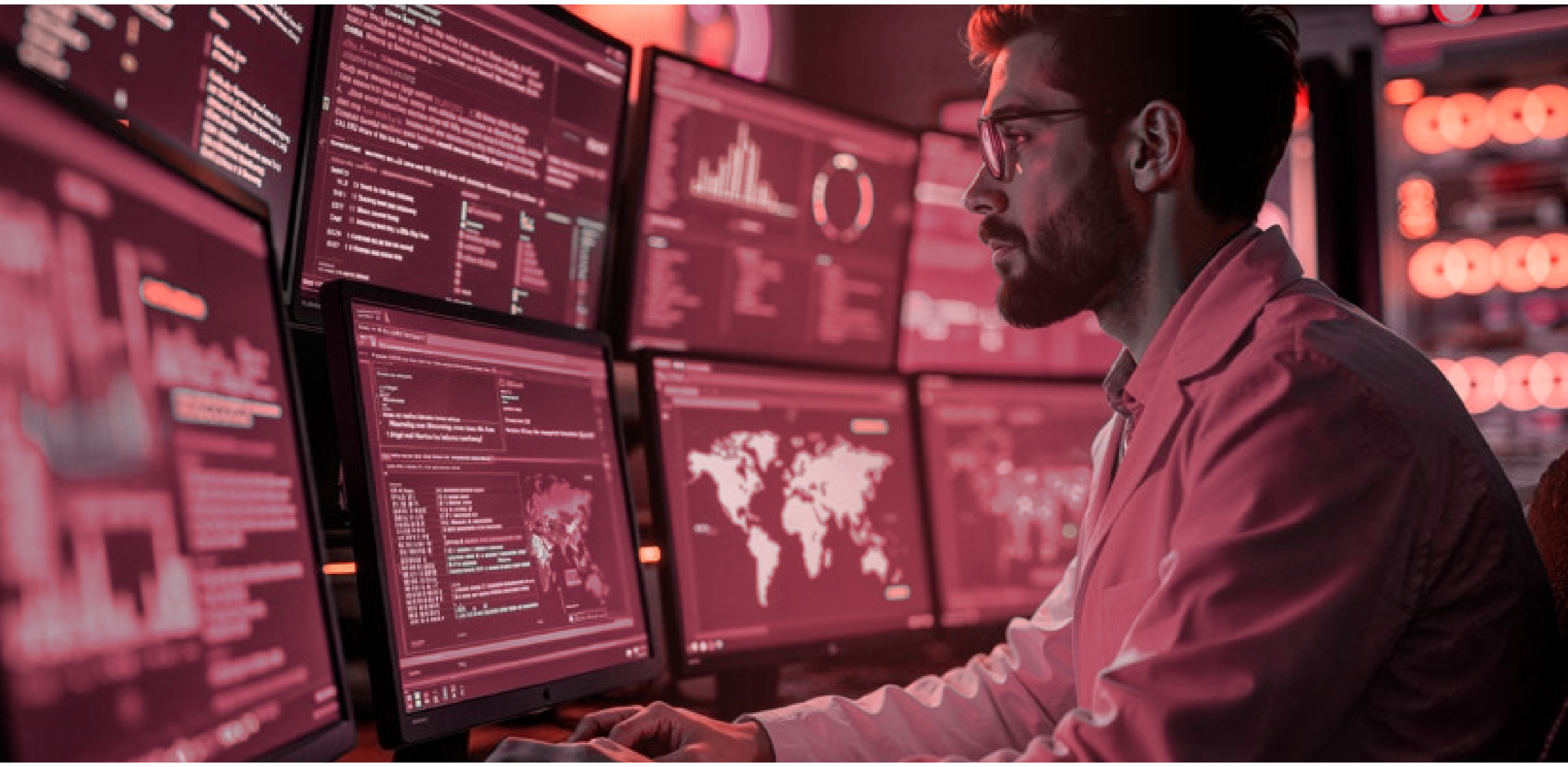
Case Assignments & Evidence Reporting Practice

Post-Training Mentorship & Community Support

Access to Recorded Sessions

About Course

The Digital Forensics Essentials (DFE) Training course by InfosecTrain is designed to help participants develop the investigative mindset required for digital forensics. The program begins with foundational topics such as the investigation process and handling digital evidence (e.g., Computer Forensics Fundamentals and Investigation Process modules). Participants then move into technical deep dives, exploring hard disk and file system analysis, data acquisition and duplication workflows, and anti-forensics countermeasures. From there, the course covers platform-specific investigations (Windows, Linux, and Mac), network and web-attack forensics, dark-web and email-crime investigations, and concludes with malware forensics. The training uses a blend of theory, guided labs, and case-based scenarios to equip participants with the practical skills required to step into DF roles and support real-world investigations.



Course Objectives

This course aims to:

- Build a strong foundation in DFE concepts and investigation workflows
- Develop hands-on forensic analysis and evidence-collection skills
- Train participants to detect, analyze, and document unauthorized activities
- Prepare participants for the EC-Council DFE certification exam

Target Audience

This course is ideal for:

- Students and Beginners aspiring to enter Cybersecurity
- SOC & Security Analysts (Level 1-2)
- IT Professionals exploring a shift into DFIR
- Law Enforcement & Cyber-Crime Professionals
- System Administrators & IT Support Staff
- Anyone interested in Digital Investigations

Pre-Requisites

- Basic understanding of computers and networks

Exam Details

Exam Code	112-57
Exam Duration	120 Minutes
Number of Questions	75
Exam Format	Multiple-choice Questions
Passing Score	70%
Exam Language	English

Course Content

Module 1 Computer Forensics Fundamentals

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

Module 2 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

Module 3 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

Module 4 Data Acquisitions and Duplications

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

Labs:

- Creating Add 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

Module 5 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

Module 6 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

Module 7 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

Module 8 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

Module 9 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

Module 10 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

Module 11 Investigating Email Crimes

- Email Basics
- Email Crime Investigation and its Steps

Labs:

- Investigating a Suspicious Email

Module 12 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

Labs:

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

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on