ACCENTREX GLOBAL

EC-Council
Building A Culture Of Security

D|FE
Digital Forensics Essentials

Digital Forensics Essentials

Begin Your Cybersecurity Journey with Hands-On, Technical Foundational Skills in Digital Forensics

No IT / Cybersecurity Experience Required

Video Lessons • Hands-on Labs • CTF Challenges • Proctored Exam

EC-COUNCIL ESSENTIALS SERIES

Cybersecurity is very complex and broad; it has many areas of specialty. And sometimes, determining your area of specialization and developing right foundational skills becomes a significant challenge.

Essential series is a hands-on, immersive program to help learners gain solid technical foundational skills in various cybersecurity areas while ensuring the program is highly affordable. Designed and created to develop a new breed of technically abled professionals right at the start of their cybersecurity careers. Essential Series course methodology is designed for school students, fresh graduates, career switchers, starters, and IT / Technology teams with little or no experience in IT / Cybersecurity. This cybersecurity essentials certification enables students and IT teams to learn the different tenets of cybersecurity, allowing them to determine their area of interest/specialization for themselves, while developing diverse skill set in essential different domains. Gain skills for your first CTF competition with this Essentials Series Course. The final module of lab capstone project features a simulated CTF to test your skills in a controlled environment. Use live virtual machines, real software, and networks to solve real-world challenges as a hacker or defender.

EC-Council Essentials Series covers 8 essential skills like: Ethical hacking, Network defense, Digital Forensics, Cloud security, IoT Security, SOC, threat intelligence and DevSecOps.

What Is EC-Council Digital Forensics Essentials?

Digital Forensics Essentials helps learners increase their competency and expertise in digital forensics and information security skills, thereby adding value to their workplace and employer.

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-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

DFE-certified learners have an assured means of formal recognition to add to their resumes and show off their expertise and skills to prospective employers.

This improves their prospects for employment advancement, higher salaries, and greater job satisfaction. If you are looking to learn advance in Digital Forensics click here: Digital Forensics Certification (Computer Hacking Forensics Investigator C|HFI)

Digital Forensics Essentials Program Information

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

Labs

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

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

Lab

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

Module 04: Data Acquisition and Duplication

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

Lab Exercise

- 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

Module 05: 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 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

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 07: 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 08: 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 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

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

Lab Exercise

- Investigating a Suspicious Email

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

Lab Exercise

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

What Skills You'll Learn

- 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

Who Is It For

- 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.

Training & Exam

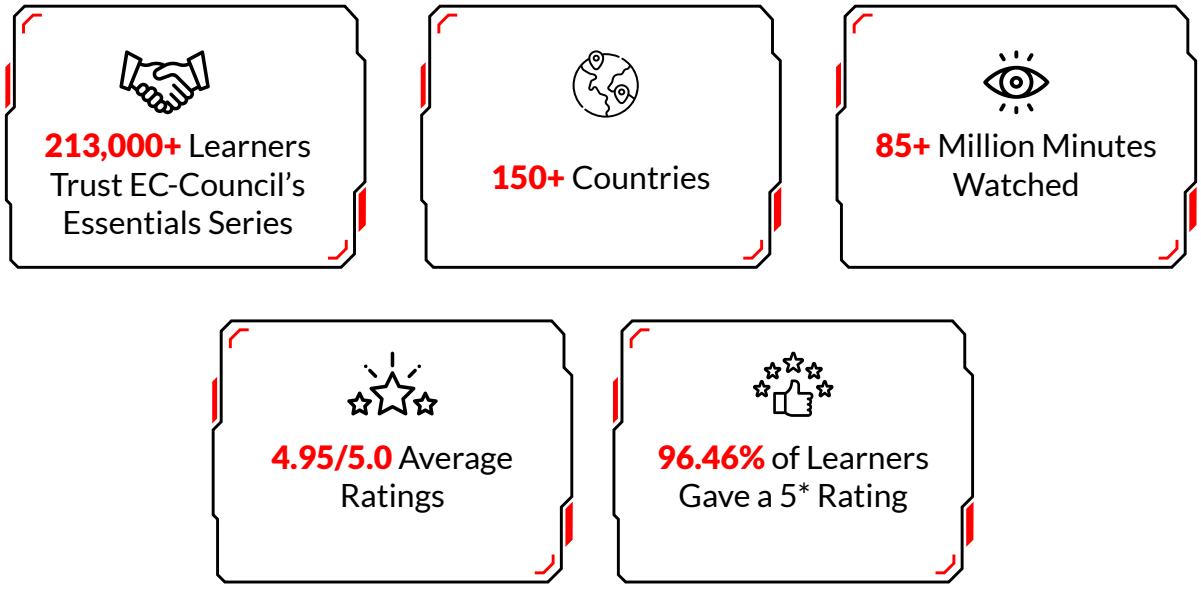
Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.
Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:
- Exam Code: 112-53
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choicew

Key Features

- 11+ Hours of Premium Self-Paced Video Training
- 11 Lab Activities in a Simulated Lab Environment
- 750+ pages of ecourseware
- Capstone Projects with Real-World CTF Challenges
- Year-Long Access to Courseware and 6-Months of Access to labs
- Proctored Exam Voucher with One-Year Validity
- Increase Your Value in the Job Market to Advance Your Career.
- Globally Recognized EC-Council's Certificate

Why EC-Council's Essentials Series is the Most Popular and Fastest Growing Beginner Level Training Program for Career Starters and Career Changers



Why Do Professionals, Students, Career Starters and Changers Worldwide Choose the EC-Council's Essentials Certification?

Gene (USA)
Strong Cybersecurity Foundation.
★★★★★

It has given me a solid foundation in the basics of cybersecurity. I now have a better understanding of the different types of cyberattacks, the tools and techniques that attackers use, and the ways to protect myself and my organization from these attacks.

Taylor Cooper (USA)
Career Advancement through Ethical Hacking.
★★★★★

This has helped me enhance my knowledge and skills in tech. I will be able to showcase my knowledge by certifying myself as an ethical hacker and adding it to my resume, which will give me an opportunity to advance in my career and opt for higher-paying roles.

Deeptankshu (USA)
Top Notched Cyber Investigation Skills.
★★★★★

It helped by teaching me how to collect data and evidence to solve crimes and prevent wrongdoers in the Cyber realm. As a Security and Intelligence major, I want to be well-versed in the Cyber realm as well as other realms.

Samuel Tetteh (USA)
Strong Foundation for Digital Forensics
★★★★★

After completing this course, I had the foundation I needed. It assisted me in completing my MS Cybersecurity course in digital forensics, which expanded my knowledge even further. This foundation is perfect for a start in Digital forensics.

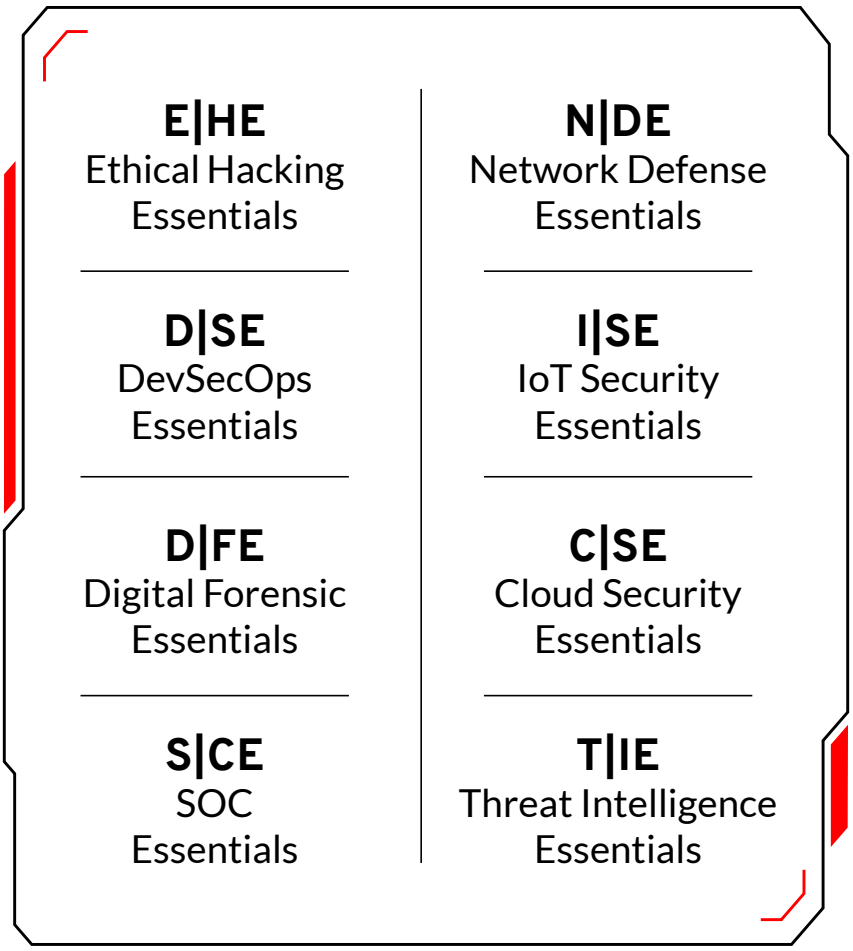
Brian (USA)
Rebuilding Network Defense Knowledge.
★★★★★

This course helped rebuild my baseline knowledge of network defense, which I required before progressing toward more advanced studies in the field.

Nicolas Ntibaziyaremye (USA)
Practical Learning for Career Growth.
★★★★★

The course is project-based. This allows me to apply what I learn in the lectures to real-world problems. I have learned a lot from this course, and I am confident that it will help me in my career.

Learn Foundational Cybersecurity Skills with EC-Council's 8 Essential Series



About EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defence, Intelligence Community, NATO, and over 2,000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 countries. They have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programs, we are dedicated to equipping over 2,30,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs, including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANAB 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies that influence the entire profession.

Founded in 2001, EC-Council employs over 400 individuals worldwide with ten global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at www.eccouncil.org

Digital Forensics Essentials

www.eccouncil.org

ACCENTREX GLOBAL