Dual Certification - TCFI + CHFI v11

Table of Contents

Program Overview

Texial's forensic Investigator program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. This includes establishing the forensics process, lab and evidence handling procedures, as well as the investigation procedures required to validate/triage incidents. This intense hands-on digital forensics program immerses students in over 68 forensic labs, enabling them to work on crafted evidence files and utilize the tools employed by the world's top digital forensics professionals.

Program Features

- 80 hours of instructor-led training
- Accredited training partner of EC-Council
- One year free access to Texial Labs
- Study material by Texial and EC-Council (e-kit)
- 20 current security domains
- Covers 68 forensic labs

Delivery Mode

Offline Real-Time Training
Online Live Training

Eligibility and Prerequisites

- Due to the availability of a plethora of resources to learn these days, there are no such eligibility criteria for learning this Certification Program.
- Any individual with basic Computer Knowledge can opt for this Certification Program.

Target Audience

- Network security officers
- practitioners
- Site administrators
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- IT security specialist, analyst, manager,
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- architect, consultant, or administrator
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- architect, or administrator

Texial.

Key Learning Outcomes

This Digtal Forensic course will help you

- Grasp the fundamentals of cyber forensics and the importance of forensic science in combating cybercrime.
- Understand the types of digital evidence, their sources, and the best practices for preserving and handling digital evidence.
- Learn the step-by-step process of conducting a forensic investigation, from planning and preparation to reporting and presenting findings.
- Gain hands-on experience with various forensic tools and software used in data recovery, analysis, and investigation.
- Understand the techniques for recovering deleted, formatted, or corrupted data from different storage devices.
- Understand the concepts of network forensics, including capturing, recording, and analyzing network traffic.
  Learn how to detect, analyze, and mitigate malware attacks.
- Understand the techniques for investigating email-related crimes, such as phishing, email fraud, and spamming.
- Develop skills to create detailed and accurate forensic reports.
- Understand the importance of incident response and the role of a forensic investigator in the incident response process.
- Learn about the ethical considerations and best practices in forensic investigations.

Certification Alignment

Texial Certified Forensic Investigator is by Texial and Computer Hacking Forensic Investigator is accredited by the EC-Council. We are the registered training provider for this course

About the Exam

CHFI v11

- Number of Questions: 150
- Test Duration: 4 Hours
- Test Format: Multiple Choice
- Test Delivery: ECC EXAM, VUE

TCFI

- Number of questions: 50
- Practical Assesment
- Test Duration: 4 Hours
- Test Format: Multiple Choice Questions and Practical

Course Curriculum

Module 01 - Computer Forensics in Today's World

Unit 01 - Understand the Fundamentals of Computer Forensics
Unit 02 - Understand Cybercrimes and their Investigation Procedures
Unit 03 - Understand Digital Evidence
Unit 04 - Understand Forensic Readiness, Incident Response and the Role of SOC (Security Operations Center) in Computer Forensics
Unit 05 - Identify the Roles and Responsibilities of a Forensic Investigator
Unit 06 - Understand the Challenges Faced in Investigating Cybercrimes

Module 02 - Computer Forensics Investigation Process

Unit 01 - Understand the Forensic Investigation Process and its Importance
Unit 02 - Understand the Pre-investigation Phase
Unit 03 - Understand First Response
Unit 04 - Understand the Investigation Phase
Unit 05 - Understand the Post-investigation Phase

Module 03 - Understanding Hard Disks and File Systems

Unit 01 - Describe Different Types of Disk Drives and their Characteristics
Unit 02 - Explain the Logical Structure of a Disk
Unit 03 - Understand Booting Process of Windows, Linux and Mac Operating Systems
Unit 04 - Understand Various File Systems of Windows, Linux and Mac Operating Systems
Unit 05 - Examine File System Using Autopsy and The Sleuth Kit Tools
Unit 06 - Understand Storage Systems
Unit 07 - Understand Encoding Standards and Hex Editors
Unit 08 - Analyze Popular File Formats Using Hex Editor

Module 04 - Data Acquisition and Duplication

Unit 01 - Understand Data Acquisition Fundamentals
Unit 02 - Understand Data Acquisition Methodology
Unit 03 - Prepare an Image File for Examination

Module 05 - Defeating Anti-Forensics Techniques

Unit 01 - Understand Anti-forensics Techniques

Unit 02 - Discuss Data Deletion and Recycle Bin Forensics

Unit 03 - Illustrate File Carving Techniques & Ways to Recover Evidence from Deleted Partitions

Unit 04 - Explore Password Cracking/Bypassing Techniques

Unit 05 - Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch

Unit 06 - Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption

Unit 07 - Detect Program Packers and Footprint Minimizing Techniques

Unit 08 - Understand Anti-forensics Countermeasures

Module 06 - Windows Forensics

Unit 01 - Collect Volatile and Non-volatile Information

Unit 02 - Perform Windows Memory and Registry Analysis

Unit 03 - Examine the Cache, Cookie and History Recorded in Web Browsers

Unit 04 - Examine Windows Files and Metadata

Unit 05 - Understand ShellBags, LNK Files, and Jump Lists

Unit 06 - Understand Text-based Logs and Windows Event Logs

Module 07 - Linux and Mac Forensics

Unit 01 - Understand Volatile and Non-volatile Data in Linux

Unit 02 - Analyze Filesystem Images Using The Sleuth Kit

Unit 03 - Demonstrate Memory Forensics Using Volatility & PhotoRec

Unit 04 - Understand Mac Forensics

Unit 05 - Hiding Files

Unit 06 - Covering Tracks

Unit 07 - Penetration Testing

Module 08 - Network Forensics

Unit 01 - Understand Network Forensics

Unit 02 - Explain Logging Fundamentals and Network Forensic Readiness

Unit 03 - Summarize Event Correlation Concepts

Unit 04 - Identify Indicators of Compromise (IoCs) from Network Logs

Unit 05 - Investigate Network Traffic

Unit 06 - Perform Incident Detection and Examination with SIEM Tools

Unit 07 - Monitor and Detect Wireless Network Attacks

Module 09 - Investigating Web Attacks

Unit 01 - Understand Web Application Forensics
Unit 02- Understand Internet Information Services (IIS) Logs
Unit 03- Understand Apache Web Server Logs
Unit 04- Understand the Functionality of Intrusion Detection System (IDS)
Unit 05- Understand the Functionality of Web Application Firewall (WAF)
Unit 06- Investigate Web Attacks on Windows-based Servers
Unit 07- Detect and Investigate Various Attacks on Web Applications

Module 10 - Dark Web Forensics

Unit 01 - Understand the Dark Web
Unit 02 - Determine How to Identify the Traces of Tor Browser during Investigation
Unit 03 - Perform Tor Browser Forensics

Module 11 - Database Forensics

Unit 01 - Understand Database Forensics and its Importance
Unit 02 - Determine Data Storage and Database Evidence Repositories in MSSQL Server
Unit 03 - Collect Evidence Files on MSSQL Server
Unit 04 - Perform MSSQL Forensics
Unit 05 - Understand Internal Architecture of MySQL and Structure of Data Directory
Unit 06 - Understand Information Schema and List MySQL Utilities for Performing Forensic Analysis
Unit 07 - Perform MySQL Forensics on WordPress Web Application Database

Module 12 - Cloud Forensics

Unit 01 - Understand the Basic Cloud Computing Concepts
Unit 02- Understand Cloud Forensics
Unit 03- Understand the Fundamentals of Amazon Web Services (AWS)
Unit 04- Determine How to Investigate Security Incidents in AWS
Unit 05- Understand the Fundamentals of Microsoft Azure
Unit 06- Determine How to Investigate Security Incidents in Azure
Unit 07- Understand Forensic Methodologies for Containers and Microservices

Module 13 - Investigating Email Crimes

Unit 01 - Understand Email Basics
Unit 02- Understand Email Crime Investigation and its Steps
Unit 03- U.S. Laws Against Email Crime

Module 14 - Malware Forensics

Unit 01 - Define Malware and Identify the Common Techniques Attackers Use to Spread Malware
Unit 02- Understand Malware Forensics Fundamentals and Recognize Types of Malware Analysis
Unit 03- Understand and Perform Static Analysis of Malware
Unit 04- Analyze Suspicious Word and PDF Documents
Unit 05- Understand Dynamic Malware Analysis Fundamentals and Approaches
Unit 06- Analyze Malware Behavior on System Properties in Real-time
Unit 07- Analyze Malware Behavior on Network in Real-time
Unit 08- Describe Fileless Malware Attacks and How they Happen
Unit 09- Perform Fileless Malware Analysis – Emotet

Module 15 - Mobile Forensics

Unit 01 - Understand the Importance of Mobile Device Forensics
Unit 02 - Illustrate Architectural Layers and Boot Processes of Android and iOS Devices
Unit 03 - Explain the Steps Involved in Mobile Forensics Process
Unit 04 - Investigate Cellular Network Data
Unit 05 - Understand SIM File System and its Data Acquisition Method
Unit 06 - Illustrate Phone Locks and Discuss Rooting of Android and Jailbreaking of iOS Devices
Unit 07 - Perform Logical Acquisition on Android and iOS Devices
Unit 08 - Perform Physical Acquisition on Android and iOS Devices
Unit 09 - Discuss Mobile Forensics Challenges and Prepare Investigation Report

Module 16 - IoT Forensics

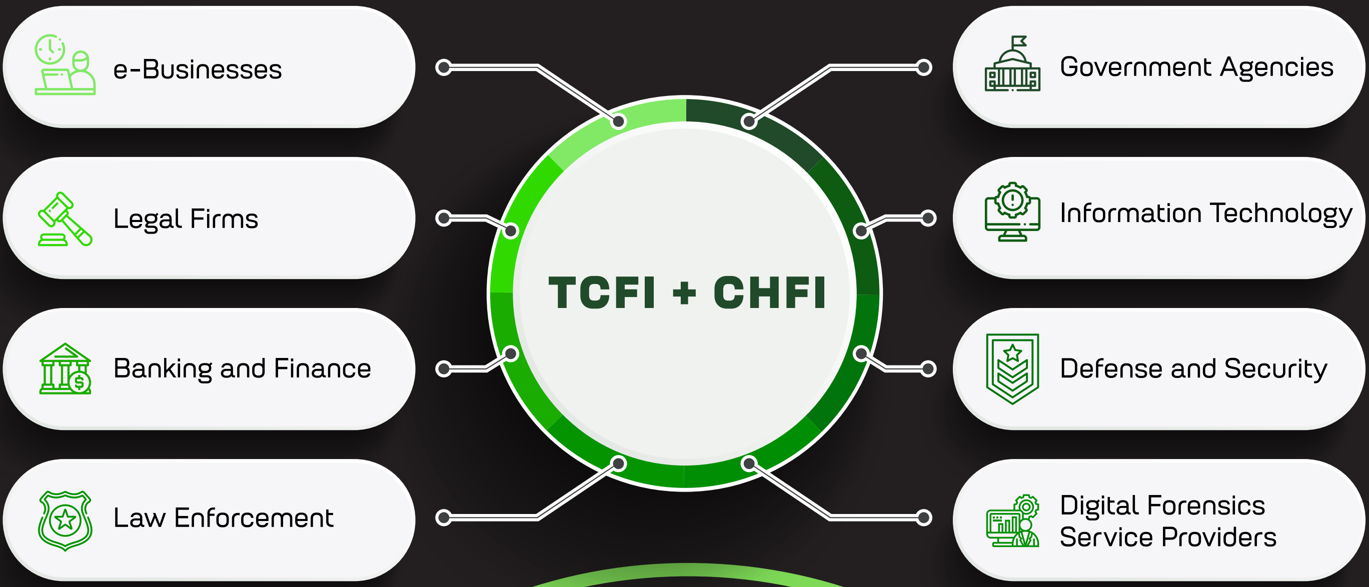
Unit 01 - Understand IoT and IoT Security Problems
Unit 02 - Recognize Different Types of IoT Threats
Unit 03 - Understand IoT Forensics
Unit 04 - Perform Forensics on IoT Devices

Our Placement Partners

Our graduates embark on remarkable journeys, guided by strong partnerships with leading placement companies. Together, we shape futures, celebrate achievements, and create a thriving ecosystem of opportunity.

cisco
J.P.Morgan
AT&T
IBM
HCL
KPMG
pwc
BOEING
NTT DaTa
tcs TATA CONSULTANCY SERVICES
PayPal
Reliance
PEPSICO
paloalto NETWORKS
accenture
FUJITSU
SGX
Atos
Deloitte.
genpact
HUAWEI
أرامكو السعودية saudi aramco
HSBC
Marriott INTERNATIONAL
QATAR AIRWAYS القطرية
salesforce
gsk
EY
DELL
Microsoft
AIRBUS
L&T Infotech
Capgemini

Industries that prefer CHFI professionals



TCFI + CHFI

- e-Businesses
- Legal Firms
- Banking and Finance
- Law Enforcement
- Government Agencies
- Information Technology
- Defense and Security
- Digital Forensics Service Providers

Texial.

Recent Success Stories

UJJWAL SINH
(PWC INDIA)
Cyber Risk Consultant

VIKSHA A
(KPMG)
Analyst

NIKHIL VITHAL GHORPADE
(ZEROFOX)
Platform Specialist

VIVEK GAONKAR
(QSEAP INFOTECH)
Information Security Consultant

THANMAY A S
(ZEROFOX)
Platform Data Specialis

SAHANA S
(ZEROFOX)
Platform Operation Specialist

ABHAY RS
(ZEROFOX)
Platform Data Specialist

SRI LAKSHMI K N
(ZEROFOX)
Platform Operation Specialist

VISHWATEJ GOLLAR
(GBB)
SOC Analyst - L1

ABHISHEK K K
(ZEROFOX)
Platform Operation Specialist

AMITKUMAR MALIPATIL
(ATOS)
Junior Associate

SRIRAM G
(ZEROFOX)
Platform Data Specialist

ARAVIND M
(ZEROFOX)
Platform Data Specialist

PRAJYOL KUMAR PATEL
(TRINITY MOBILITY)
Cyber Security engineer

SHASHANK VARDHAN
(ZEROFOX)
physical security intelligence

FIRDOSE KHAN
(ZEROFOX)
Platform Operation Specialist

GOKUL P
(ZEROFOX)
Platform Data Specialist

DEVA N
(TRINITY MOBILITY)
Cyber Security engineer

YASHWANTH CM
(ZEROFOX)
Platform Data Specialist

SHREYAS
(QSEAP INFOTECH)
Information Security Consultant

PARTHA SARATHI
(TRINITY MOBILITY)
Cyber Security engineert

SUHAS AREKAL
(ZEROFOX)
Platform Data Specialist

MANMOHAN SARDAR
(QSEAP INFOTECH)
Information Security Consultant

GANESH M
(ZEROFOX)
Platform Operation Specialist

YOUR TURN AWAITS!

JOIN US >

Texial.

About us

Texial Cyber Security is a global leader in information security and cyber forensics. Texial provides state-of-the-art services to keep organizations safe from both external and internal threats. We offer a wide range of cybersecurity needs for individuals and major businesses.

Texial. | www.texial.net

Texial aims to bridge the gap between the availability and necessity of trained and certified security personnel. We provide rigorous training to combat cybercrime effectively.
Texial evaluates digital assets to identify breach possibilities and implements proactive measures. In case of a breach, they help remediate losses and provide detailed reports on cybersecurity measures and causes of the breach.
Texial Cyber Security has a dedicated team of experienced cybersecurity professionals from around the world, delivering world-class solutions to protect information.
If you’re interested in learning more or exploring their courses, you can visit our website: https://texial.net . Feel free to reach out us on +91 9886655699 for any other questions!