C)DFE: Certified Digital Forensics Examiner

Course ID #: 7000-776-ZZ-Z
Hours: 35

Course Content

Course Description:

In this course you will cover electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation. Students will be taught the methodology for conducting a computer forensic examination. Students will learn to use forensically sound investigative techniques in order to evaluate the scene, collect and document all relevant information, interview appropriate personnel, maintain chain-of-custody, and write a findings report.

Course Objectives:

Upon successful completion of this course, students will:

- Be able to establish industry-acceptable digital forensics standards with current best practices and policies
- Be prepared to competently take the C)DFE exam

Prerequisites:

- 1 Year experience in computers
- C)SP course

Target Audience:

- Virtualization Admins
- Cloud Security Officers
- CIO
- Virtualization and Cloud Auditors
- Virtualization and Cloud Compliance Officers

Topics:

Module 1 – Computer Forensics Incidents

- Origins of digital forensic science
- Differences between criminal and civil incidents
- Types of computer fraud incidents
- Internal and external threats
- Investigative challenges
- Industry Standards

Module 2 – Computer Forensic Investigative Theory

- Investigative Theory
- Investigative Concepts
- Behavioral evidence analysis (BEA) & Equivocal Forensic Analysis (EFA)

C)DFE: Certified Digital Forensics Examiner

Course ID #: 7000-776-ZZ-Z

Hours: 35

Module 3 – Computer Forensic Investigative Process
- Investigative Prerequisites
- Scene Management
- The digital forensics process
- ISO 27043

Module 4 – Digital Acquisition and Analysis Tools
- Acquisition Procedures
- Computer forensics field triage process model (CFFTPM)
- Acquisition Authentication
- Forensic Tools

Module 5 – Disks and Storages
- Disk OS and Filesystems
- Spinning Disks Forensics
- SSD Forensics
- Files Management
- Handling Damaged Drives

Module 6 – Live Acquisitions
- Live Acquisition
- Apple Acquisition
- Linux/UNIX Acquisition

Module 7 – Windows Forensics
- Windows Event Viewer Overview
- EVTX and EVT Logs
- Logs Analysis to Identify Breaches and Attacks

Module 8 - Linux Forensics
- Linux Artifacts
  - File System Structure
  - Basic Identifiers
  - Common Log Files

Module 9 – MAC Forensics
- OSX Artifacts
  - File System Structure
  - Core Storage
  - Default Apps
  - Other Artifacts

Module 10 – Forensic Examination Protocols
- Science Applied to Forensics
- Cardinal Rules
- Alpha 5
- The 20 Basic Steps of Forensics
- Scientific Working Group on Digital Evidence (SWGDE) Standard
- International Organization on Computer Evidence (IOCE) Standard

Module 11 – Digital Evidence Protocols
- Digital Evidence Categories
- Evidence Admissibility

Module 12 – Digital Evidence Presentation
- The Best Evidence Rule
- Hearsay
- Authenticity and Alteration

Module 13 – Computer Forensic Laboratory Protocols
- Forensics Lab Standard Operating Procedures
  - Quality Assurance
  - Quality Control
  - Peer Review
  - Annual Review
  - Deviations
  - Lab Intake

C)DFE: Certified Digital Forensics Examiner

Course ID #: 7000-776-ZZ-Z

Hours: 35

Module 14 – Specialized Artifact Recovery
- Forensics Workstation Prep
- Windows Components with Investigative Interest
- Files Containing Historical Information
- Web Forensics

Module 15 – eDiscovery and ESI
- Electronically Stored Information Rules
  - Legal System
  - Disclosure
  - Rule 37
  - eDiscovery Tools

Module 16 – Mobile Forensics
- Cellular Network
- Forensic Process
- Tools
- Paraben Forensics

Module 17 – Incident Handling
- What is an Incident?
- Incident Handling Steps
  - Preparation
  - Identification and Initial Response
  - Containment
  - Eradication
  - Recovery
  - Follow-up

Module 18 – Digital Forensics Reporting
- Report Sections and Content

Labs:

Lab 1 – Chain of Custody
Lab 2 – Identify Seized Evidences
Lab 3 – Devices Acquisition
Lab 4 – Memory Acquisition
Lab 5 – Prepare the Case Evidence
Lab 6 – Investigate the Acquired Evidence
Lab 7 – Prepare the Case Evidence
Lab 8 – Windows Event Logs Analysis
Lab 9 – Linux Primary Info Retrieval
Lab 10 – Investigate OSX Evidence
Lab 11 – Finding Clues
Lab 12 – Construct the Case Events
Lab 13 -Evidence found from a Seized Android Device
Lab 14 – Incident Response

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535