BDO CYBER ACADEMY

ICSI INTERNATIONAL CYBERSECURITY INSTITUTE

Course: ICSI | CDFE Digital Forensics, Incident Response and Threat Hunting

In this course, we will discuss what Incident Response and Digital Forensics are, the legal implications they have and how they are structured. We will also perform various exercises on digital forensics tools in order to get a clear understanding of the technicality that digital forensics assumes.

We will study how to capture images of memory, storage, network packets and logs and how to correlate them in order to draw conclusions. Finally, we will look at malware and threat analysis, which are more than ever relevant today.

Audience Profile:

- Anyone who is interested in digital forensics
- System administrators
- Security practitioners
- Incident handlers
- Incident response team members
- Law enforcement officers

Candidate Prerequisites:

Basic familiarity with Windows Operating System.

Duration:

5 Days (40 Hours)

Accreditation:

NCSC Certified Training
MSc Cybersecurity 20 Credits

Exam Details:

Exam Code: CDFE
Type of Questions: Hands-On Multiple Choice
Duration: 2 Hours and 30 minutes
Passing Score: 70%
Exam Voucher Included

Course Outline:

Module 1: Incident Response

Lessons:

- What is Incident Response
- The Incident Response Process Model
- The Role of Digital Forensics
- Why Incident Response is Needed
- The Incident Response Framework
- The CSIRT Response Charter
- The Incident Response Team
- The Incident Response Plan
- Incident Classification
- The Incident Response Playbook
- Escalation Procedures
- Incident Response Capability Maintenance

Review Questions

Module 2: Identification, Authentication and Authorisation

Lessons:

- Digital Forensic Fundamentals
- UK Laws and Regulations
- Digital Forensic Process
- Forensics Lab

Review Questions

Module 3: Collection of Network Evidence

Lessons:

- Collection of Network Evidence
- Preparation
- Evidence from Network Devices
- Collection of Evidence

Review Questions

Module 4: Capturing Evidence from Host Systems

Lessons:

- Capturing Evidence from Host Systems
- Methods for Acquiring Evidence
- Procedures for Collecting Evidence
- Acquiring Memory
- Acquiring Memory Remotely
- Virtual Machines Captures
- Non-Volatile Data

Review Questions

Labs

- Acquiring Memory with FTK Imager
- Acquiring Memory with WinPmem
- Capturing Registry and Logs using FTK Imager

Module 5: Forensic Imaging

Lessons:

- Forensic Imaging
- Forensic Imaging Overview
- Evidence Drive Preparation
- Dead Imaging
- Live Imaging

Review Questions

Labs:

- Drive Wiping with Eraser
- Encrypting a Drive’s Repository Partition with VeraCrypt
- Creating a Forensic Image with a GUI Tool
- Create a Forensic Image with a CLI Tool
- Creating a Live image using FTK Imager Lite
- Forensic Imaging

Module 6: Analysing Network Evidence

Lessons:

- Analysing Network Evidence
- Wireshark

Labs:

- Network Traffic Identification: PING
- Network Traffic Identification: DNS Query
- Network traffic Identification: TCP Three-Way Handshake
- Traffic Analysis: Host Footprinting / File Extractions
- Analysing Network Evidence

Module 7: Analysis of System Memory

Lessons:

- Analysis of System Memory
- Memory Analysis Methodology

Labs:

- Analysis of Memory File Using Volatility
- Analysis of System Memory

Module 8: Analysis of System Storage

Lessons:

- Analysis of System Storage
- Types of System Storage
- File Systems
- Commercial Tools
- Must Have Tools for Incident Responders
- File Carving
- Email Analysis
- Registry Analysis
- Hashing
- Web Browser Analysis
- File Analysis

- Timestamps and Timeline Analysis
- Event Log Analysis
- Shortcut Files and Jump List Analysis
- Prefetch File Analysis
- Thumbnail Caches Analysis
- GREP Searches
- File Recovery
- Recovering Passwords

Labs:

- File Carving
- Email Header Analysis
- Reading Offline Files with Regedit
- Reading Offline Registry Files with Windows Registry Recovery
- Reading Offline Files with RegRipper
- Hashing Folders and Their Contents for Comparison
- Hashing Individual Files for Comparison
- Hashing Evidence Files for Validation
- Analysing Chrome Internet Cache and History
- File Analysis - Microsoft Office Files
- File Analysis - EXIF Data from Graphic Files
- Combining Timestamps for a Timeline
- Examining Event Logs
- Shortcut File Analysis
- Jump List Analysis
- Prefetch File Analysis
- Analysing Thumbs.db from Windows XP
- Analysing Cache Images within Microsoft Files
- GREP Searching Through Log Files
- Mounting a Forensic Image with FTK Imager and Recovering Files
- Recovering Files from Forensic Images with Autopsy
- Recovering Passwords

Module 9: Log Analysis

Lessons:

- Collecting Data from Network Devices
- Collecting Data from Host Machines and Application Protocols
- Log Analysis Tools
- Using SIEM's for Log Analysis

Labs

- Using Log Parser to Analyse Logs
- Analysing Logs with Linux Tools
- Log Analysis with Splunk

Module 10: Creating Forensics Reports

Lessons:

- Creating Forensic Reports
- What Should Be Documented
- Documentation Types
- Sources to Include
- Audience
- Tracking Incidents
- Written Reports

Review Questions

Module 11: Malware Analysis

Lessons:

- Malware Analysis
- Malware Types and Definition
- Malware Analysis Methodology

Labs

- Performing Static Analysis
- Performing Dynamic Analysis

- Malware Analysis

Module 12: Threat Intelligence

Lessons:

- Threat Intelligence
- Threat Intelligence Actor Groups
- Advanced Persistent Threat
- Types of Threat Intelligence
- Threat Intelligence Life Cycle
- Sourcing Threat Intelligence
- Threat Intelligence Platforms
- Threat Intelligence Use Types

Review Questions

Labs:

- Hashing Evidence – Known Bad Hashes