CDFE - Certified Digital Forensics Examiner

Course Overview

This course will teach students about examining digital forensics. Topics covered include investigative theory, digital acquisition & analysis tools, forensic examination protocols, processing techniques, specialized artifact recovery, mobile forensics, and more.

Module 1 - Computer Forensics Incidents 23m

Computer Forensics Incidents
Where are We?
Overview
Section 1: Origins of digital forensic science
The Legal System
The Legal System
The Legal System
The Legal System
Section 2: Differences between criminal and civil incidents
Criminal Incidents
Criminal Incidents
Criminal Incidents
Criminal Incidents
Criminal Incidents
Criminal Incidents
Criminal Incidents
Civil Incidents
Civil Incidents
Civil Incidents
Section 3: Types of computer fraud incidents
Computer Fraud
Computer Fraud
Computer Fraud
Computer Fraud
Section 4: Internal and external threats
Internal Threats
Internal Threats
External Threats
External Threats
External Threats
External Threats
Section 5: Investigative challenges
Investigative Challenges
Investigative Challenges
Investigative Challenges
Common Frame of Reference
Media Volume
Review

Module 2 - Incident Handling 36m

Incident Handling
Overview
Section 1: What is an Incident?
Incident Handling Defined
What is a Security Event?
Common Security Events of Interest
What is a Security Incident?
What is an Incident Response Plan?
When does the Plan get Initiated?
Common Goals of Incident Response Management
Section 2: Incident Handling Steps
Incident Handling Steps
Phase 1: Preparation
Goal
Be Prepared
The Incident Response Plan
Incident Handling
Incident Response Plan
Incident Response Plan
Incident Response Plan
Roles of the Incident Response Team
Incident Response Team Makeup
Challenges of building an IRT
Incident Response Training and Awareness
Jump Kit
Jump Kit
Prepare Your Sites and Systems
Prepare Your Sites and Systems
Prepare Your Sites and Systems
Prepare Your Sites and Systems
Prepare Your Sites and Systems
Prepare Your Sites and Systems
Phase 2: Identification and Initial Response
Goal
Identification of an Incident
Basic Incident Response Steps
Proper Evidence Handling
Phase 3: Containment
Goal
Containment
Onsite Response
Secure the Area
Conduct Research
Make Recommendations
Establish Intervals
Capture Digital Evidence
Change Passwords
Phase 4: Eradication
Goal

Determine Cause
Defend Against Follow-on Attacks
More Defenses
Analyze Threat and Vulnerability
Restore System(s) to Operation
Phase 5: Recovery
Goal
Report Findings
Restore System
Verify
Decide
Monitor Systems
Phase 6: Follow-up
Goal
Follow-up Report
Follow-up Report
Review

Module 3 - Computer Forensic Investigative Theory 19m

Computer Forensic Investigative Theory
Overview
Section 1: Investigation Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Section 2: Investigative Concepts
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Section 3: BEA & EFA
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory
Computer Forensic Investigative Theory

McAfee Geotagging
Review

Module 4 - Investigative Process 34m

Investigative Process
Overview
Section 1: Investigation Prerequisites
Prior to the Investigation
Forensics Workstation
Building Your Team of Investigators
Who is involved in Computer Forensics?
Who is involved in Computer Forensics?
Approval Authority and Authorization
Risk Assessment
Forensic Investigation Toolkit
Section 2: Investigation Process
Investigating Computer Crimes
Investigation Methodology
Preparing for an Investigation
Preparing for an Investigation (cont.)
Preparing for an Investigation (cont.)
Search Warrant
Forensic Photography
Preliminary Information
First Responder
Collecting Physical Evidence
Collecting Electronic Evidence
Collecting Electronic Evidence
Collecting Electronic Evidence (cont.)
Guideline for Acquiring Electronic Evidence
Securing the Evidence
Managing the Evidence
Chain of Custody
Duplicate the Data
Verify the Integrity of the Image
Recover Last Data
Data Analysis
Data Analysis Tools
Assessing the Evidence
Assessing the Case
Assessing the Case (cont.)
Location Assessment
Best Practices
Documentation
Gathering and Organizing Information
Writing the Report
Writing the Report (cont.)
Expert Witness
Closing the Case
Review

Module 5 - Digital Acquisition & Analysis Tools 19m

Digital Acquisition & Analysis Tools
Overview
Section 1: Acquisition Procedures
Digital Acquisition
Digital Acquisition
Digital Acquisition
Digital Acquisition
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Section 2: Evidence Authentication
Digital Acquisition Procedures
Digital Acquisition
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Digital Acquisition Procedures
Section 3: Tools
Digital Acquisition Procedures
Digital Forensic Analysis Tools
Digital Forensic Analysis Tools
Digital Forensic Analysis Tools
Digital Forensic Analysis Tools
Review

Module 6 - Disks and Storages 32m

Disks and Storages
Overview
Section 1: Disk OS and FileSystems
Disk Based Operating Systems
Disk Based Operating Systems
Disk Based Operating Systems
Disk Based Operating Systems
Disk Based Operating Systems
OS / File Storage Concepts
OS / File Storage Concepts
OS / File Storage Concepts
OS / File Storage Concepts
OS / File Storage Concepts

OS / File Storage Concepts
Section 2: Spinning Disks Forensics
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
File Carving
Fragmentary Analysis
Section 3: SSD Forensics
Inside SSD
Inside SSD
TRIM
Implications on Forensics
Implications on Forensics
Forensics vs Encryption
Section 4: Files Management
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Disk Storage Concepts
Quick View Plus
Review

Module 7 - Forensic Examination Protocols 18m

Forensic Examination Protocols
Overview
Section 1: Science Applied to Forensics
Forensic Examination Protocols
Forensic Examination Protocols
Forensic Examination Protocols
Forensic Examination Protocols
Forensic Examination Protocols
Section 2: Cardinal Rules & Alpha 5
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination

Section 3: The 20 Basic Steps of Forensics
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Forensic Examination
Review

Module 8 - Digital Evidence Protocols 22m

Digital Evidence Protocols
Overview
Section 1: Digital Evidence Categories
Digital Evidence Concepts
Digital Evidence Concepts
Digital Evidence Concepts
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Digital Evidence Categories
Section 2: Evidence Admissibility
Digital Evidence: Admissibility
Digital Evidence: Admissibility
Digital Evidence: Admissibility
Review

Module 9 - Digital Evidence Presentation 18m

Digital Evidence Presentation
Overview
Section 1: The Best Evidence Rule
Digital Evidence Presentation
Digital Evidence Presentation
Digital Evidence Presentation
Digital Evidence Presentation
Digital Evidence Presentation
Digital Evidence Presentation
Digital Evidence Presentation
Digital Evidence
Digital Evidence
Digital Evidence
Digital Evidence
Digital Evidence
Section 2: Hearsay
Digital Evidence: Hearsay
Digital Evidence: Hearsay
Digital Evidence: Hearsay
Digital Evidence: Hearsay
Section 3: Authenticity and Alteration
Digital Evidence
Digital Evidence
Digital Evidence
Digital Evidence
Digital Evidence
Digital Evidence
Review

Module 10 - Computer Forensic Laboratory Protocols 23m

Computer Forensic Laboratory Protocols
Overview
Overview
Overview
Quality Assurance
Quality Assurance
Standard Operating Procedures
Reports
Peer Review
Who Should Review?
Peer Review
Consistency
Accuracy
Research
Validation
Relevance
Peer Review
Peer Review
Annual Review

Deviation
Deviation
Deviation
Deviation
Lab Intake
Lab Intake
Lab Intake
Tracking
Tracking
Storage
Storage
Discovery
Discovery
Discovery
Discovery
Discovery
Review

Module 11 - Computer Forensic Processing Techniques 29m
Computer Forensic Processing Techniques
Overview
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
National Software Reference Library (NSRL)

Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Computer Forensic Processing Techniques
Review

Module 12 - Specialized Artifact Recovery 53m

Specialized Artifact Recovery
Overview
Section 1: Forensics Workstation Prep
Forensics Workstation Prep
Forensics Workstation Prep
Forensics Workstation Prep
Forensics Workstation Prep
Forensics Workstation Prep
Settings For The Nodrivetypeautorun Registry Entry
Prep System Stage
Prep System Stage
Prep System Stage
Section 2: Windows Components with Investigative Interest
Windows Components with Investigative Interest
Types of Dates
File Signatures
File Signatures
File Signatures
File Signatures
Image File Databases
Image File Databases
The Windows OS
Windows Operating Environment
Windows Registry
Windows Registry
Windows Registry Hives
Windows Registry Hives
Windows Registry Hives
Windows Registry Hives
Windows Registry Hives
Windows NT/2000/XP Registry
Windows Vista/Win7, 8, 10 Registry
Windows Alternate Data Streams

Windows Alternate Data Streams
Windows Unique ID Numbers
Windows Unique ID Numbers
Other ID’s
Section 3: Files Containing Historical Information
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Splunk
Historical Files
Historical Files
Event Viewer
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Historical Files
Outlook E-Mail
Outlook E-Mail
Web E-Mail
Section 4: Web Forensics
Web Forensics
Historical Files
IE database location
Mozilla Firefox SQLite database
Google Chrome
Microsoft Edge
Understanding The Database Files
Understanding The Database Files
Investigating SQLite Files
Investigating SQLite Files
Investigating SQLite Files
Tables Relation
Tables Relation
Viewing Visited Websites
Review

Module 13 - Electronic Discovery and Electronically Stored Information 11m

Electronic Discovery and Electronically Stored Information
Overview
eDiscovery
eDiscovery
Discoverable ESI Material
Discoverable ESI Material
eDiscovery Notification
Required Disclosure
eDiscovery Conference
Preserving Information
eDiscovery Liaison
eDiscovery Products
Metadata
What is Metadata?
Data Retention Architecture
“Safe Harbor” Rule 37(f)
eDiscovery Spoliation
Tools for eDiscovery
Review

Module 14 - Mobile Forensics 31m

Mobile Forensics
Overview
Section 1: Cellular Network
Mobile Devices
Types of Cell Networks
What can a criminal do with Cell Phones?
Cell Phone Forensics
Forensics Information in Cell Phones
Subscriber Identity Module (SIM)
Integrated Circuit Card Identification (ICCID)
International Mobile Equipment Identifier (IMEI)
Electronic Seal Number (ESN)
Section 2: Forensic Process
Device Seizure
Device Seizure
Device Seizure
Acquisition
Data Acquisition
Acquire Data from SIM Cards
SIM Cards
Mobile Device Memory
Data Analysis
Reality
Analyze Information
Analyze
Non-Invasive Forensics
Non-Invasive Methods
Invasive Methods

Forensic Methods
Section 3: Tools
Cell Phone Forensic Tools
Device and SIM Card Seizure
Cell Phone Analyzer
Tools
Forensic Card Reader
ForensicSIM Tool
Forensic Challenges
Section 4: Paraben Forensics
Paraben Mobile Field Kit
Paraben Forensics Hardware
Paraben: Power Bank
Paraben: Mobile Field Kit
Paraben: Wireless Stronghold Tent
Paraben: Passport Stronghold Bag
Paraben: Project-a-phone
Paraben: Project-a-phone
Paraben: SIM Card Seizure
Paraben: Sticks
Paraben: P2C-P2 Commander
Review

Module 15 - Digital Forensics Reporting 11m

Digital Forensics Reporting
Overview
Analysis Report
Definition
Computer Sciences
Ten Laws of Good Report Writing
Cover Page
Table of Contents
Examination Report
Background
Request
Summary of Findings
Forensic Examination
Tools
Evidence
Items of Evidence
Analysis
Findings
Conclusion
Exhibits
Signatures
Review

Total Duration: 6h 18m