uCertify

Course Outline

CHFI v8 - Computer Hacking Forensic Investigator

21 May 2020

Lesson

Practice test

Contents

1. Course Objective

Computer forensic practices help to investigate crimes and assaults, system anomalies, or even help system administrators in identifying an issue by characterizing what is ordinary functional specifications and validating system data for uncommon practices. Cyber Security experts with a firm hold on the standards of digital forensics can be seen as members of Incident Handling and Incident Response Teams. Gain hands-on expertise in EC-Council Computer Hacking Forensic Investigator 312-49 V8 exam with Computer Hacking Forensic Investigator course. The course covers all the objectives of the EC Council 312-49 V8 exam and provides competence across a spectrum of skills including computer forensics, digital evidence, steganography, application password crackers, log capturing, event correlation, investigation of various attacks, and much more. The course furnishes a strong learning pattern of key ideas and concepts in the digital forensic domains applicable to the present organizations.

2. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. Quizzes

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

5. Flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.

6. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.

7. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

8. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

9. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assignments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

10. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's

finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 5 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution
    2. Best Virtual Learning Solution
    3. Best Student Assessment Solution
    4. Best Postsecondary Learning Solution
    5. Best Career and Workforce Readiness Solution
    6. Best Instructional Solution in Other Curriculum Areas
    7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform
    2. Best Instructional Solution in Other Curriculum Areas

3. Best Learning Relationship Management Solution

11. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Computer Forensics in Today's World

- Define computer forensics
- Discuss the evolution of computer forensics
- Explain the objectives and benefits of computer forensics
- Discuss forensic readiness planning in detail
- Explain cybercrimes
- Examine various computer crimes
- What is cybercrime investigation?
- Explain the key steps and rules in a forensic investigation

- What is the role of a forensic investigator?
- How to access computer forensics resources
- Describe the role of digital evidence in forensic investigation
- Understanding Corporate Investigations
- Explain the key concepts of Enterprise Theory of Investigation (ETI)
- Discuss various legal issues and reports related to computer forensic investigations

Chapter 2: Computer Forensics Investigation Process

- Provide an overview of the computer crime investigation process
- Describe computer forensics investigation methodology
- Summarize the steps to prepare for a computer forensics investigation
- How to obtain a search warrant
- How to evaluate and secure a scene
- How to collect and secure the evidence in a forensically sound manner
- Explain the different techniques to acquire and analyze the data
- Summarize the importance of evidence and case assessment
- How to prepare the final investigation report
- Testify in the Court as an Expert Witness

- Explain about Computer Forensic Service Providers

Chapter 3: Searching and Seizing Computers

- How to search and seize computers without a warrant
- Discuss the Fourth Amendment's Reasonable Expectation of Privacy
- What is consent and discuss the scope of consent
- Summarize the steps involved in searching and seizing computers with a warrant
- Examine the basic strategies for executing computer searches
- Discuss the Privacy Protection Act
- Describe drafting the warrant and affidavit
- Explain the post-seizure issues
- Describe the Electronic Communications Privacy Act
- What is voluntary disclosure?
- Electronic Surveillance in Communications Networks
- Discuss how content is different from addressing information
- Provide an overview of evidence and authentication

Chapter 4: Digital Evidence

- Define digital evidence and explain its role in case of a computer security incident

- Discuss the characteristics of digital evidence
- What are the various types of digital data?
- What is best evidence rule?
- Discuss federal rules of evidence
- Summarize the international principles for computer evidence
- Discuss about the Scientific Working Group on Digital Evidence (SWGDE)
- What are the considerations for collecting digital evidence from electronic crime scenes?
- Provide an overview of digital evidence examination process and steps involved
- Explain electronic crime and digital evidence consideration by crime category

Chapter 5: First Responder Procedures

- Define electronic evidence
- Who is first responder?
- Provide an overview on how to collect and store electronic evidence
- Describe first responder tool kit and how to create it
- How to get first response from laboratory forensic staff
- Provide an overview on how to collect and secure electronic evidence at the crime scene
- Explain how to conduct preliminary interviews

- How to document electronic crime scene
- Explain how to collect and preserve electronic evidence
- Explain how to package and transport electronic evidence in a forensically sound manner
- How to prepare a report on the crime scene
- Provide a checklist for the first responders
- Discuss the first responder's common mistakes

Chapter 6: Computer Forensics Lab

- How to set up a computer forensics lab
- Discuss the investigative services in computer forensics
- What are the basic hardware requirements in a forensics lab?
- List and summarize various hardware forensic
- Discuss the basic software requirements in a forensics lab
- Summarize various software forensic tools

Chapter 7: Understanding Hard Disks and File Systems

- What is a hard disk drive?
- Explain solid-state drive (SSD)

- Provide an overview of physical and logical structure of a hard disk
- Describe the various types of hard disk interfaces
- Examine the components of a hard disk
- What are disk partitions?
- Explain Windows and Macintosh boot process
- What are file systems?
- Explain various types of file systems
- Provide an overview of Windows, Linux, Mac OS X, and Sun Solaris 10 file systems
- Discuss about CD-ROM/DVD File System
- Explain about RAID storage system and RAID levels
- Explain file system analysis using the sleuth

Chapter 8: Windows Forensics

- What is volatile information?
- Explain what is network and process information
- Define non-volatile information
- Describe memory dump
- Parsing Process Memory

- Describe the different techniques for collecting non-volatile information
- Explain various processes involved in forensic investigation of a Windows system
- Provide an overview of IIS, FTP, and system firewall logs
- Discuss the importance of audit events and event logs in Windows forensics
- Explain the static and dynamic event log analysis techniques
- Discuss different Windows password security issues such as password cracking
- How to analyze restore point registry settings
- Provide an overview of cache, cookie, and history analysis
- How to evaluate account management events
- How to search with Event Viewer
- Discuss various forensics tools

Chapter 9: Data Acquisition and Duplication

- Define data acquisition and explain various types of data acquisition systems
- Explain various data acquisition formats and methods
- How to determine a best acquisition method?
- What is contingency planning for image acquisitions?
- Describe static and live data acquisition

- Provide an overview of volatile data collection methodology
- Explain various types of volatile information
- What are the requirements of the disk imaging tool?
- How to validate data acquisitions
- Discuss Linux and Windows validation methods
- How to acquire RAID Disks
- Examine the best practices of acquisition
- List various data acquisition software and hardware tools

Chapter 10: Recovering Deleted Files and Deleted Partitions

- Explain how to recover files in Windows, MAC, Linux, for Windows
- Discuss file recovery tools for Windows, MAC, and Linux
- How to identify creation date, last accessed date of a file, and deleted sub-directories
- Steps to recover the deleted partitions and list partition recovery tools

Chapter 11: Forensics Investigation Using AccessData FTK

- What is Forensic Toolkit (FTK) and discuss its various features
- Explain FTK installation steps
- Discuss about FTK Case Manager

- How to restore an image to a disk?
- Explain the FTK examiner user interface
- How to verify drive image integrity
- Discuss how to mount an image to a drive
- Summarize the steps involved in creating a case
- Discuss the functions of FTK interface tabs
- Explain the steps involved in adding evidence to a case
- How to acquire local live evidence
- Explain the steps involved in acquiring data remotely using remote device management system (RDMS)
- Discuss the steps involved in imaging drives
- How to mount and unmount a device
- Explain the steps involved in conducting an index search and live search
- How to decrypt EFS Files and Folders

Chapter 12: Forensic Investigation Using EnCase

- Provide an overview of EnCase forensic
- Discuss EnCase, its uses, and functionality

- Discuss about EnCase forensic modules
- How to install EnCase forensic
- Explain how to configure EnCase
- Provide an overview of case structure
- What is case management?
- How to add a Device to a Case and how to acquire a Device
- Explain the verification process of evidence files
- What is a source processor?
- Discuss how to analyze and search files
- Describe how to view file content
- Provide an overview on bookmarks
- How to create various types of bookmark?
- Explain how to create a report using the Report tab
- How to export a Report

Chapter 13: Steganography and Image File Forensics

- Summarize steganography and its types
- List the application of steganography

- Discuss various digital steganography techniques
- What is Steganalysis?
- How to detect steganography
- List various steganography detection tools
- Discuss about image file formats
- How to compress data
- How to process forensic image using MATLAB
- Explain how to locate and recover image files
- How to identify unknown file formats
- List picture viewer tools and image file forensic tools

Chapter 14: Application Password Crackers

- What are the terminologies used?
- Explain the functionality of password crackers
- Summarize various types of passwords
- What is a password cracker?
- How does a password cracker work?
- Discuss various password cracking techniques

- List various types of password attacks
- List various system and application software password cracking
- What are default passwords?
- Discuss various password cracking tools

Chapter 15: Log Capturing and Event Correlation

- What are computer security logs?
- Discuss about logon events in Windows
- What are IIS logs?
- How to view the DHCP logs
- What is ODBC logging?
- Explain the legality of using logs
- Explain log management
- Discuss various challenges in log management
- Centralized logging
- Discuss about syslog
- Why Synchronize Computer Times
- What is NTP?

- List various NIST time servers
- Discuss various event correlation approaches
- List various log capturing and analysis tools

Chapter 16: Network Forensics, Investigating Logs, and Investigating Network Traffic

- Summarize network forensics concepts
- Explain the network forensics analysis mechanism
- What are intrusion detection systems (IDS)?
- Define the terms firewall and honeypot
- Discuss various network vulnerabilities
- Explain various types of network attacks
- Explain the new line injection attack and the timestamp injection attack
- Where to look for evidence
- How to handle logs as evidence
- Explain how to condense a log file
- Why to Investigate Network Traffic
- How to acquire traffic using DNS poisoning techniques
- Explain how to gather from the ARP table

- List various traffic capturing and analysis tools

Chapter 17: Investigating wireless attacks

- Discuss the advantages and disadvantages of wireless networks
- List different components of wireless networks
- What are the various types of wireless networks?
- List various types of wireless standards
- What is MAC filtering?
- What is a Service Set Identifier (SSID)?
- Discuss various types of wireless encryption
- List various types of wireless attacks
- How to investigate wireless attacks
- What are the requirements of a tool design and summarize the best practices for wireless forensics
- List various wireless forensics tools

Chapter 18: Investigating Web Attacks

- What are Web applications?
- Explain Web application architecture

- Why Web servers are compromised
- Provide an overview of Web logs
- What are Internet Information Services (IIS) and Apache Web server Logs?
- Discuss various types of Web attacks
- How to investigate Web attacks?
- Explain the investigation process of Web attacks in Windows-based servers
- Describe how to investigate IIS and Apache logs
- When does Web page defacement occur?
- Discuss various security strategies to Web applications
- List various Web attack detection tools
- Discuss about various tools for locating an IP address

Chapter 19: Tracking E-mails and Investigating E-mail Crimes

- Explain the terms E-mail system, E-mail client, E-mail server, and E-mail message
- Discuss the importance of electronic records management
- Discuss various types of E-mail crimes
- Provide examples of E-mail header
- List Common Headers

- Why to Investigate E-mails
- Discuss the steps involved in investigation of E-mail crimes
- List various E-mail forensics tools
- What are the different laws and acts against E-mail crimes?

Chapter 20: Mobile Forensics

- List different mobile devices
- What are the hardware and software characteristics of mobile devices?
- What is a cellular network?
- Provide an overview of mobile operating systems
- Discuss various types of mobile operating systems
- What a criminal can do with mobiles phones
- Describe various mobile forensic challenges
- Discuss various memory considerations in mobiles
- What are the different precautions to be taken before an investigation?
- Explain the process involved in mobile forensics
- List various mobile forensic hardware and software tools

Chapter 21: Investigative Reports

- Explain the importance of reports and need of an investigative report
- Discuss the salient features of a good report
- Provide computer forensic report template
- How is a report classified
- Provide layout of an investigative report
- What are the guidelines for writing a report?
- Provide an overview of an investigative report format
- How to document a case report
- What are the best practices for investigators?
- How to write a report using FTK and ProDiscover

Chapter 22: Becoming an Expert Witness

- What is an Expert witness?
- Explain the role of an expert witness
- Describe various types of expert witnesses
- What is the scope of expert witness testimony?
- Explain the differences between Technical Witness and Expert Witness

- What are the various steps involved in evidence processing?
- How to prepare a report
- List the rules pertaining to an expert witness' qualification
- How to testify in court
- What are the general ethics while testifying?
- How to testify during direct and cross-examination
- How to find a computer forensic expert

12. Practice Test

uCertify provides full length practice tests. These tests closely follow the exam objectives and are designed to simulate real exam conditions. Each course has a number of test sets consisting of hundreds of items to ensure that learners are prepared for the certification exam.

Here's what you get

100	100
PRE-ASSESSMENTS QUESTIONS	POST-ASSESSMENTS QUESTIONS

Features

Full Remediation

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Learn, Test and Review Mode

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

13. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.