EDUSUM

#1 Online Certification Guide

312-49

CHFI

A Success Guide to Prepare-
EC-Council Computer Hacking Forensic Investigator

edusum.com

Table of Contents

Introduction to 312-49 Exam on EC-Council Computer Hacking Forensic Investigator

Use this quick start guide to collect all the information about EC-Council CHFI (312-49) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the 312-49 EC-Council Computer Hacking Forensic Investigator exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual EC-Council CHFI v9 certification exam.

The EC-Council CHFI certification is mainly targeted to those candidates who want to build their career in Cyber Security domain. The EC-Council Computer Hacking Forensic Investigator (CHFI) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of EC-Council CHFI v9.

EC-Council 312-49 Certification Details:

Exam Name	EC-Council Computer Hacking Forensic Investigator (CHFI)
Exam Code	312-49
Exam Price	$500 (USD)
Duration	240 min
Number of Questions	150
Passing Score	70%
Books / Training	Courseware
Schedule Exam	Pearson VUE
Sample Questions	EC-Council CHFI Sample Questions
Practice Exam	**EC-Council 312-49 Certification Practice Exam**

EC-Council 312-49 Exam Syllabus:

Topic
- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti-Forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Investigative Reports

312-49 Sample Questions:

01. Syslog is a client/server protocol standard for forwarding log messages across an IP network. Syslog uses _____to transfer log messages in a clear text format.
a) TCP
b) FTP
c) SMTP
d) POP

02. What is the First Step required in preparing a computer for forensics investigation?
a) Do not turn the computer off or on, run any programs, or attempt to access data on a computer
b) Secure any relevant media
c) Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
d) Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

03. A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:
a) Take permission from all employees of the organization for investigation
b) Harden organization network security
c) Create an image backup of the original evidence without tampering with potential evidence
d) Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

04. File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?
a) The last letter of a file name is replaced by a hex byte code E5h
b) The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
c) Corresponding clusters in FAT are marked as used
d) The computer looks at the clusters occupied by that file and does not avails space to store a new file

05. BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?
a) Header
b) The RGBQUAD array
c) Information header
d) Image data

06. When collecting evidence from the RAM, where do you look for data?
a) Swap file
b) SAM file
c) Data file
d) Log file

07. Depending upon the Jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?
a) 18 USC 7029
b) 18 USC 7030
c) 18 USC 7361
d) 18 USC 7371

08. LBA (Logical Block Address) addresses data by allotting a _____to each sector of the hard disk.
a) Sequential number
b) Index number
c) Operating system number
d) Sector number

09. How do you define Technical Steganography?
a) Steganography that uses physical or chemical means to hide the existence of a message
b) Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways
c) Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways
d) Steganography that utilizes visual symbols or signs to hide secret messages

10. Which is not a part of environmental conditions of a forensics lab?
a) Large dimensions of the room
b) Good cooling system to overcome excess heat generated by the work station
c) Allocation of workstations as per the room dimensions
d) Open windows facing the public road

Answers to 312-49 Exam Questions:

Question: 01 Answer: a	Question: 02 Answer: a	Question: 03 Answer: c	Question: 04 Answer: b	Question: 05 Answer: b
Question: 06 Answer: a	Question: 07 Answer: b	Question: 08 Answer: a	Question: 09 Answer: a	Question: 10 Answer: d

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com