EC-COUNCIL 312-49

EC-Council CHFI Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

312-49

EC-Council Computer Hacking Forensic Investigator (CHFI)

150 Questions Exam – 70% Cut Score – Duration of 240 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the 312-49 Certification 2

EC-Council 312-49 CHFI Certification Details: 2

312-49 Syllabus: 2

Broaden Your Knowledge with EC-Council 312-49 Sample Questions: 21

Avail the Study Guide to Pass EC-Council 312-49 CHFI Exam: 25

Career Benefits: 25

Discover More about the 312-49 Certification

Are you interested in passing the EC-Council 312-49 exam? First discover, who benefits from the 312-49 certification. The 312-49 is suitable for a candidate if he wants to learn about Cyber Security. Passing the 312-49 exam earns you the EC-Council Computer Hacking Forensic Investigator (CHFI) title.

While preparing for the 312-49 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 312-49 PDF contains some of the most valuable preparation tips and the details and instant access to useful **312-49 study materials just at one click.**

EC-Council 312-49 CHFI Certification Details:

Exam Name	EC-Council Computer Hacking Forensic Investigator (CHFI)
Exam Code	312-49
Exam Price	$650 (USD)
Duration	240 mins
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**

312-49 Syllabus:

Topic	Details	Weights
Forensic Science	- Understand different types of cybercrimes and list various forensic investigations challenges • Types of Computer Crimes • Impact of Cybercrimes at Organizational Level	18%

Topic	Details	Weights
	• Cyber Crime Investigation • Challenges Cyber Crimes Present for Investigators • Network Attacks • Indicators of Compromise (IOC) • Web Application Threats • Challenges in Web Application Forensics • Indications of a Web Attack • What is Anti-Forensics? • Anti-Forensics Techniques - Understand the fundamentals of computer forensics and determine the roles and responsibilities of forensic investigators • Understanding Computer Forensics • Need for Computer Forensics • Why and When Do You Use Computer Forensics? • Forensic Readiness • Forensic Readiness and Business Continuity • Forensics Readiness Planning • Incident Response • Computer Forensics as part of Incident Response Plan • Overview of Incident Response Process Flow • Role of SOC in Computer Forensics • Need for Forensic Investigator • Roles and Responsibilities of Forensics Investigator • What makes a Good Computer Forensics Investigator? • Code of Ethics	

Topic	Details	Weights
	• Accessing Computer Forensics Resources • Other Factors That Influence Forensic Investigations • Introduction to Web Application Forensics • Introduction to Network Forensics • Postmortem and Real-Time Analys - Understand data acquisition concepts and rules • Understanding Data Acquisition • Live Acquisition • Order of Volatility • Dead Acquisition • Rules of Thumb for Data Acquisition • Types of Data Acquisition • Determine the Data Acquisition Format - Understand the fundamental concepts and working of databases, cloud computing, Emails, IOT, Malware (file and fileless), and dark web • Understanding Dark Web • TOR Relays • How TOR Browser works • TOR Bridge Node • Internal architecture of MySQL • Structure of data directory • Introduction to Cloud Computing • Types of Cloud Computing Services • Cloud Deployment Models • Cloud Computing Threats • Cloud Computing Attacks	

Topic	Details	Weights
	• Introduction to an email system • Components involved in email communication • How email communication works • Understanding parts of an email message • Introduction to Malware • Components of Malware • Common Techniques Attackers Use to Distribute Malware across Web • Introduction to Fileless Malware • Infection Chain of Fileless Malware • How Fileless Attack Works via Memory Exploits • How Fileless Attack Happens Via Websites • How Fileless Attack Happens Via Documents • What is IoT? • IoT Architecture • IoT Security Problems • OWASP Top 10 Vulnerabilities • IoT Threats • IoT Attack Surface Areas	
Regulations, Policies and Ethics	- Understand rules and regulations pertaining to search & seizure of the evidence, and evidence examination • Rules of Evidence • Best Evidence Rule • Federal Rules of Evidence • Scientific Working Group on Digital Evidence (SWGDE) • ACPO Principles of Digital Evidence • Seeking Consent	15%

Topic	Details	Weights
	• Obtaining Witness Signatures • Obtaining Warrant for Search and Seizure • Searches Without a Warrant • Initial Search of the Scene • Preserving Evidence • Chain of Custody • Sanitize the Target Media • Records of Regularly Conducted Activity as Evidence • Division of Responsibilities - Understand different laws and legal issues that impact forensic investigations • Computer Forensics: Legal Issues • Computer Forensics: Privacy Issues • Computer Forensics and Legal Compliance • Other Laws that May Influence Computer Forensics • U.S. Laws Against Email Crime: CAN-SPAM Act	
Digital Evidence	- Understand the fundamental characteristics and types of digital evidence • Introduction to Digital Evidence • Types of Digital Evidence • Characteristics of Digital Evidence • Role of Digital Evidence • Sources of Potential Evidence • Understanding Hard Disk • Understanding Solid State Drive (SSD) • RAID Storage System • NAS/SAN Storage • Disk Interfaces	17%

Topic	Details	Weights
	• Logical Structure of Disks - Understand the fundamental concepts and working of desktop and mobile Operating Systems • What is the Booting Process? • Essential Windows System Files • Windows Boot Process: BIOS-MBR Method • Windows Boot Process: UEFI-GPT • Macintosh Boot Process • Linux Boot Process • Windows File Systems • Linux File Systems • Mac OS X File Systems • MAC Forensics Data • MAC Log Files • MAC Directories • CD-ROM / DVD File System • Virtual File System (VFS) and Universal Disk Format File System (UDF) • Architectural Layers of Mobile Device Environment • Android Architecture Stack • Android Boot Process • iOS Architecture • iOS Boot Process • Mobile Storage and Evidence Locations • Mobile Phone Evidence Analysis • Data Acquisition Methods • Components of Cellular Network • Different Cellular Networks	

Topic	Details	Weights
	• Cell Site Analysis: Analyzing Service Provider Data • CDR Contents • Subscriber Identity Module (SIM) • Different types of network-based evidence - Understand different types of logs and their importance in forensic investigations • Understanding Events • Types of Logon Events • Event Log File Format • Organization of Event Records • ELF_LOGFILE_HEADER structure • EventLogRecord Structure • Windows 10 Event Logs • Other Audit Events • Evaluating Account Management Events • Log files as evidence • Legal criteria for admissibility of logs as evidence • Guidelines to ensure log file credibility and usability • Ensure log file authenticity • Maintain log file integrity • Implement centralized log management • IIS Web Server Architecture • IIS Logs • Analyzing IIS Logs • Apache Web Server Architecture • Apache Web Server Logs • Apache Access Logs	

Topic	Details	Weights
	• Apache Error Logs - Understand various encoding standards and analyze various file types • Character Encoding Standard: ASCII • Character Encoding Standard: UNICODE • OFFSET • Understanding Hex Editors • Understanding Hexadecimal Notation • Image File Analysis: JPEG • Image File Analysis: BMP • Understanding EXIF data • Hex View of Popular Image File Formats • PDF File Analysis • Word File Analysis • PowerPoint File Analysis • Excel File Analysis • Hex View of Other Popular File Formats - Understand the fundamental working of WAF and MySQL Database • Web Application Firewall (WAF) • Benefits of WAF • Limitations of WAF • Data Storage in SQL Server • Database Evidence Repositories • MySQL Forensics • Viewing the Information Schema • MySQL Utility Programs for Forensic Analysis	
Procedures and Methodology	- Understand Forensic Investigation Process	17%

Topic	Details	Weights
	• Forensic investigation process • Importance of the Forensic investigation process • Setting up a computer forensics lab • Building the investigation team • Understanding the hardware and software requirements of a forensic lab • Validating laboratory software and hardware • Ensuring quality assurance • First response basics • First response by non-forensics staff • First response by system/network administrators • First response by laboratory forensics staff • Documenting the electronic crime scene • Search and seizure • Evidence preservation • Data acquisition • Data analysis • Case analysis • Reporting • Testify as an expert witness • Generating Investigation Report • Mobile Forensics Process • Mobile Forensics Report Template • Sample Mobile Forensic Analysis Worksheet - Understand the methodology to acquire data from different types of evidence • Data Acquisition Methodology	

Topic	Details	Weights
	• Step 1: Determine the Best Data Acquisition Method • Step 2: Select the Data Acquisition Tool • Step 3: Sanitize the Target Media • Step 4: Acquire Volatile Data • Acquire Data From a Hard Disk • Remote Data Acquisition • Step 5: Enable Write Protection on the Evidence Media • Step 6: Acquire Non-Volatile Data • Step 7: Plan for Contingency • Step 8: Validate Data Acquisition Using • Collecting Volatile Information • Collecting Non-Volatile Information • Collecting Volatile Database Data • Collecting Primary Data File and Active Transaction Logs Using SQLCMD • Collecting Primary Data File and Transaction Logs • Collecting Active Transaction Logs Using SQL Server Management Studio • Collecting Database Plan Cache • Collecting Windows Logs • Collecting SQL Server Trace Files • Collecting SQL Server Error Logs - Illustrate Image/Evidence Examination and Event Correlation • Getting an Image Ready for Examination • Viewing an Image on a Windows, Linux and Mac Forensic Workstations • Windows Memory Analysis	

Topic	Details	Weights
	• Windows Registry Analysis • File System Analysis Using Autopsy • File System Analysis Using The Sleuth Kit (TSK) • Event Correlation • Types of Event Correlation • Prerequisites of Event Correlation • Event Correlation Approaches - Explain Dark Web and Malware Forensics • Dark web forensics • Identifying TOR Browser Artifacts: Command Prompt • Identifying TOR Browser Artifacts: Windows Registry • Identifying TOR Browser Artifacts: Prefetch Files • Introduction to Malware Forensics • Why Analyze Malware? • Malware Analysis Challenges • Identifying and Extracting Malware • Prominence of Setting up a Controlled Malware Analysis Lab • Preparing Testbed for Malware Analysis • Supporting Tools for Malware Analysis • General Rules for Malware Analysis • Documentation Before Analysis • Types of Malware Analysis	
Digital Forensics	- Review Various Anti-Forensic Techniques and Ways to Defeat Them • Anti-Forensics Technique: Data/File Deletion	17%

Topic	Details	Weights
	• What Happens When a File is Deleted in Windows? • Recycle Bin in Windows • File Carving • Anti-Forensics Techniques: Password Protection • Bypassing Passwords on Powered-off Computer • Anti-Forensics Technique: Steganography • Anti-Forensics Technique: Alternate Data Streams • Anti-Forensics Techniques: Trail Obfuscation • Anti-Forensics Technique: Artifact Wiping • Anti-Forensics Technique: Overwriting Data/Metadata • Anti-Forensics Technique: Encryption • Anti-Forensics Technique: Program Packers • Anti-Forensics Techniques that Minimize Footprint • Anti-Forensics Technique: Exploiting Forensics Tools Bugs • Anti-Forensics Technique: Detecting Forensic Tool Activities • Anti-Forensics Countermeasures • Anti-Forensics Tools - Analyze Various Files Associated with Windows and Linux and Android Devices • Windows File Analysis • Metadata Investigation • Windows ShellBags	

Topic	Details	Weights
	• Analyze LNK Files • Analyze Jump Lists • Event logs • File System Analysis using The Sleuth Kit (TSK) • Linux Memory Forensics • APFS File System Analysis: Biskus APFS Capture • Parsing metadata on Spotlight • Logical Acquisition of Android Devices • Physical Acquisition of Android Devices • SQLite Database Extraction • Challenges in Mobile Forensics - Analyze various logs and perform network forensics to investigate network attacks • Analyzing Firewall Logs • Analyzing IDS Logs • Analyzing Honeypot Logs • Analyzing Router Logs • Analyzing DHCP Logs • Why investigate Network Traffic? • Gathering evidence via Sniffers • Sniffing Tool: Tcpdump • Sniffing Tool: Wireshark • Analyze Traffic for TCP SYN flood DOS attack • Analyze Traffic for SYN-FIN flood DOS attack • Analyze traffic for FTP password cracking attempts • Analyze traffic for SMB password cracking attempts	

Topic	Details	Weights
	• Analyze traffic for sniffing attempts • Analyze traffic to detect malware activity • Centralized Logging Using SIEM Solutions • SIEM Solutions: Splunk Enterprise Security (ES) • SIEM Solutions: IBM Security QRadar • Examine Brute-Force Attacks • Examine DoS Attack • Examine Malware Activity • Examine data exfiltration attempts made through FTP • Examine network scanning attempts • Examine ransomware attack • Detect rogue DNS server (DNS hijacking/DNS spoofing) • Wireless network security vulnerabilities • Performing attack and vulnerability monitoring • Detect a rogue access point • Detect access point MAC spoofing attempts • Detect misconfigured access point • Detect honeypot access points • Detect signal jamming attack - Analyze Various Logs and Perform Web Application Forensics to Examine Various Web Based Attacks • Investigating Cross-Site Scripting Attack • Investigating SQL Injection Attack	

Topic	Details	Weights
	• Investigating Directory Traversal Attack • Investigating Command Injection Attack • Investigating Parameter Tampering Attack • Investigating XML External Entity Attack • Investigating Brute Force Attack • Investigating Cookie Poisoning Attack - Perform Forensics on Databases, Dark Web, Emails, Cloud and IoT devices • Database Forensics Using SQL Server Management Studio • Database Forensics Using ApexSQL DBA • Common Scenario for Reference • MySQL Forensics for WordPress Website Database: Scenario 1 • MySQL Forensics for WordPress Website Database: Scenario 2 • Tor Browser Forensics: Memory Acquisition • Collecting Memory Dumps • Memory Dump Analysis: Bulk Extractor • Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Open) • Forensic Analysis of Storage to Acquire the Email Attachments (Tor Browser Open) • Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Closed)	

Topic	Details	Weights
	• Forensic Analysis of Storage to Acquire the Email Attachments (Tor Browser Closed) • Forensic Analysis: Tor Browser Uninstalled • Dark Web Forensics Challenges • Introduction to email crime investigation • Steps to investigate email crimes • Division of Responsibilities • Where Is the Data Stored in Azure? • Logs in Azure • Acquiring A VM in Microsoft Azure • Acquiring A VM Snapshot Using Azure Portal • Acquiring A VM Snapshot Using PowerShell • AWS Forensics • Wearable IoT Device: Smartwatch • IoT Device Forensics: Smart Speaker-Amazon Echo - Perform Static and Dynamic Malware Analysis in a Sandboxed Environment • Malware Analysis: Static • Analyzing Suspicious MS Office Document • Analyzing Suspicious PDF Document • Malware Analysis: Dynamic - Analyze Malware Behavior on System and Network Level, and Analyze Fileless Malware • System Behavior Analysis: Monitoring Registry Artifacts	

Topic	Details	Weights
	• System Behavior Analysis: Monitoring Processes • System Behavior Analysis: Monitoring Windows Services • System Behavior Analysis: Monitoring Startup Programs • System Behavior Analysis: Monitoring Windows Event Logs • System Behavior Analysis: Monitoring API Calls • System Behavior Analysis: Monitoring Device Drivers • System Behavior Analysis: Monitoring Files and Folders • Network Behavior Analysis: Monitoring Network Activities • Network Behavior Analysis: Monitoring Port • Network Behavior Analysis: Monitoring DNS • Fileless Malware Analysis: Emotet • Emotet Malware Analysis • Emotet Malware Analysis: Timeline of the Infection Chain	
Tools/Systems/Programs	• - Identify various tools to investigate Operating Systems including Windows, Linux, Mac, Android and iOS • File System Analysis Tools • File Format Analyzing Tools • Volatile Data Acquisition Tools • Non-Volatile Data Acquisition Tools • Data Acquisition Validation Tools • Tools for Examining Images on Windows • Tools for Examining Images on Linux	16%

Topic	Details	Weights
	• Tools for Examining Images on Mac • Tools for Carving Files on Windows • Tools for Carving Files on Linux • Tools for Carving Files on Mac • Recovering Deleted Partitions: Using R-Studio • Recovering Deleted Partitions: Using EaseUS Data Recovery Wizard • Partition Recovery Tools • Using Rainbow Tables to Crack Hashed Passwords • Password Cracking Using: L0phtCrack and Ophcrack • Password Cracking Using Cain & Abel and RainbowCrack • Password Cracking Using pwdump7 • Password Cracking Tools • Tool to Reset Admin Password • Steganography Detection Tools • Detecting Data Hiding in File System Structures Using OSForensics • ADS Detection Tools • Detecting File Extension Mismatch using Autopsy • Tools to detect Overwritten Data/Metadata • Program Packers Unpacking Tools • USB Device Enumeration using Windows PowerShell • Tools to Collect Volatile Information • Tools to Non-Collect Volatile Information • Tools to perform windows memory and registry analysis	

Topic	Details	Weights
	• Tools to examine the cache, Cookie and history recorded in web browsers • Tools to Examine Windows Files and Metadata • Tools to Examine ShellBags, LNK files and Jump Lists • Tools to Collect Volatile Information on Linux • Tools to Collect Non-Volatile Information on Linux • Linux File system Analysis Tools • Tools to Perform Linux Memory Forensics • APFS File System Analysis • Parsing metadata on Spotlight • MAC Forensic Tools • Network Traffic Investigation Tools • Incident Detection and Examination with SIEM tools • Detect and Investigate Various Attacks on Web Applications by Examining Various Logs • Tools to Identify TOR Artifacts • Tools to Acquire Memory Dumps • Tools to Examine the Memory Dumps • Tools to Perform Static Malware Analysis • Tools to Analyze Suspicious Word and PDF documents • Tools to Perform Static Malware Analysis • Tools to Analyze Malware Behavior on a System • Tools to Analyze Malware Behavior on a Network	

Topic	Details	Weights
	• Tools to Perform Logical Acquisition on Android and iOS devices • Tools to Perform Physical Acquisition on Android and iOS devices - Determine the various tools to investigate MSSQL, MySQL, Azure, AWS, Emails and IoT devices • Tools to Collect and Examine the Evidence Files on MSSQL Server • Tools to Collect and Examine the Evidence Files on MySQL Server • Investigating Microsoft Azure • Investigating AWS • Tools to Acquire Email Data • Tools to Acquire Deleted Emails • Tools to Perform Forensics on IoT devices	

Broaden Your Knowledge with EC-Council 312-49 Sample Questions:

Question: 1

Mike is a Computer Forensic Investigator. He got a task from an organization to investigate a forensic case. When Mike reached the organization to investigate the place, he found that the computer at the crime scene was switched off.

In this scenario, what do you think Mike should do?

a) He should turn on the computer
b) He should leave the computer off
c) He should turn on the computer and extract the data
d) He should turn on the computer and should start analyzing it

Answer: b

Question: 2

The process of examining acquired evidence is cyclical in nature and reflected in the relationship among the four panes of the EnCase interface.

Which of the following pane represents a structured view of all gathered evidence in a Windows-like folder hierarchy?

a) Tree Pane
b) Table Pane
c) View Pane
d) Filter Pane

Answer: a

Question: 3

During live response, you can retrieve and analyze much of the information in the Registry, and the complete data during post-mortem investigation.

Which of this registry Hive contains configuration information relating to which application is used to open various files on the system?

a) HKEY_USERS
b) HKEY_CURRENT_USER
c) HKEY_CLASSES_ROOT
d) HKEY_CURRENT_CONFIG

Answer: c

Question: 4

The file content of evidence files can be viewed using the View Pane. The View pane provides several tabs to view file content.

Which of this tab provides native views of formats supported by Oracle outside in technology?

a) Text tab
b) Hex tab
c) Doc tab
d) Picture tab

Answer: c

Question: 5

Which of the following is a legal document that demonstrates the progression of evidence as it travels from original evidence location to the forensic laboratory?

a) Chain of Custody
b) Origin of Custody
c) Evidence Document
d) Evidence Examine

Answer: a

Question: 6

Which of this attack technique is the combination of both a brute-force attack and a dictionary attack to crack a password?

a) Hybrid Attack
b) Rule-based Attack
c) Syllable Attack
d) Fusion Attack

Answer: c

Question: 7

Which type of digital data stores a document file on a computer when it is deleted and helps in the process of retrieving the file until that file space is reused?

a) Metadata
b) Residual Data
c) Archival Data
d) Transient Data

Answer: b

Question: 8

Which one of the following is the smallest allocation unit of a hard disk, which contains a set of tracks and sectors ranging from 2 to 32, or more, depending on the formatting scheme?

a) Sector
b) Cluster
c) Track
d) 4Platter

Answer: b

Question: 9

Source Processor automates and streamlines common investigative tasks that collect, analyze, and report on evidence. Which of this source processor module obtains drives and memory from a target machine?

a) Personal Information Module
b) Internet Artifacts Module
c) Acquisition Module
d) File Processor Module

Answer: c

Question: 10

Redundant Array of Inexpensive Disks (RAID) is a technology that uses multiple smaller disks simultaneously which functions as a single large volume.

In which RAID level disk mirroring is done?

a) RAID Level 3
b) RAID Level 0
c) RAID Level 1
d) RAID Level 5

Answer: c

Avail the Study Guide to Pass EC-Council 312-49 CHFI Exam:

- Find out about the 312-49 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **312-49 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the 312-49 training. Joining the EC-Council provided training for 312-49 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **312-49 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 312-49 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the 312-49 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the 312-49 Certification

EduSum.Com is here with all the necessary details regarding the 312-49 exam. We provide authentic practice tests for the 312-49 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **312-49 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the EC-Council Computer Hacking Forensic Investigator (CHFI).

Start Online Practice of 312-49 Exam by visiting URL
https://www.edusum.com/ec-council/312-49-ec-council-computer-hacking-forensic-investigator