EDUSUM

#1 Online Certification Guide

EC-COUNCIL 312-49

EC-Council CHFI Certification Questions & Answers

Exam Summary – Syllabus –Questions

312-49

EC-Council Computer Hacking Forensic Investigator (CHFI)

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

Table of Contents:

Know Your 312-49 Certification Well:

The 312-49 is best suitable for candidates who want to gain knowledge in the EC-Council Cyber Security. Before you start your 312-49 preparation you may struggle to get all the crucial materials like 312-49 syllabus, sample questions, study guide.

But don't worry the 312-49 PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the 312-49 syllabus?
- How many questions are there in the 312-49 exam?
- Which Practice test would help me to pass the 312-49 exam at the first attempt?

Passing the 312-49 exam makes you EC-Council Computer Hacking Forensic Investigator (CHFI). Having the certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

EC-Council 312-49 Certification Details:

Exam Name	EC-Council Computer Hacking Forensic Investigator (CHFI)
Exam Code	312-49
Exam Price	$600 (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	- Computer Forensics Objective and Need • Understand computer forensics, and explain the objectives and benefits of computer forensics • Apply the key concepts of Enterprise Theory of Investigation (ETI) - Forensics Readiness • Fuse computer network attack analyses with criminal and counterintelligence investigations and operations - Cyber Crime • Identify elements of the crime • Examine various computer crimes - Web Applications and Webservers Attacks • Understand various types of Web attacks - Email Crimes • Understand various types of email attacks - Network Attacks • Understand various types of network attacks - Forensics and Mobile Devices • Understand mobile based operating systems, their architectures, boot process, password/pin/pattern lock bypass mechanisms - Cyber Crime Investigation • Understand the importance of cybercrime investigation - Computer Forensics Investigation Methodology • Understand the methodology involved in Forensic Investigation - Reporting a Cyber Crime	15%

	• Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc. - Expert Witness • Understand the role of expert witness in computer forensics	
Regulations, Policies and Ethics	- Searching and Seizing Computers with and without a Warrant • Identify legal issues and reports related to computer forensic investigations - Laws and Acts against Email Crimes • Identify legal issues and reports related to computer forensic investigations - Laws pertaining to Log Management • Identify legal issues and reports related to log management - Policies Pertaining to Mobile Forensics • Identify internal BYOD and information security policies of the organization - Laws and Acts against Email Crimes • Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action - General Ethics While Testifying • Identify legal issues and reports related to computer forensic investigations	10%
Digital Evidence	- Digital Evidence • Apply the key concepts of Enterprise Theory of Investigation (ETI) - Types of Digital Evidence • Understand various types and nature of digital evidence - Rules of Evidence • Understand the best evidence rule	20%

	- Electronic Evidence: Types and Collecting Potential Evidence • Secure the electronic device of information source, use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence - Electronic Crime and Digital Evidence Consideration by Crime Category • Electronic Crime and Digital Evidence Consideration by Crime Category - Computer Forensics Lab • Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes HDD SSD, CD/DVD, PDA, mobile phones, GPS, and all tape formats. - Understanding Hard Disks • Perform MAC timeline analysis on a file system - Disk Partitions and Boot Process • Understand the Windows and Macintosh boot process, and handling volatile data - Understanding File Systems • Understand File Systems and help in digital forensic investigations - Windows File Systems • Understanding Windows File Systems and help in digital forensic investigations - Linux File Systems • Understand Linux File Systems and help in digital forensic investigations - Mac OS X File Systems • Understand Mac OS X File Systems and help in digital forensic investigations - RAID Storage System	

	• Understand RAID Storage System and help in digital forensic investigations - File Carving • Understand Carving Process and help in digital forensic investigations - Image Files • Understand Image File Formats - Analyze Logs • Understand Computer Security Logs - Database Forensics • Perform MySQL Forensics • Perform MSSQL Forensics - Email Headers • Perform various steps involved in investigation of Email crimes - Analyzing Email headers • Perform analysis of email headers and gather evidential information - Malware Analysis • Perform static and dynamic malware analysis - Mobile Operating Systems • Understand the hardware and software characteristics of mobile devices • Understand the different precautions to be taken before investigation • Perform various processes involved in mobile forensics	
Procedures and Methodology	- Investigating Computer Crime • Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property • Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated	20%

	with cyber intrusion incidents, investigations, and operations - Computer Forensics Investigation Methodology • Write and public Computer Network Defense guidance and reports on incident findings to appropriate constituencies • Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion investigation • Process crime scenes • Track and document Computer Network Defense incidents from initial detection through final resolution • Develop an investigative plan to investigate alleged crime, violation, or suspicious activity using computers and the internet • Identify outside attackers accessing the system from Internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges • Coordinate with intelligence analysts to correlate threat assessment data - Digital Evidence Examination Process • Ensure chain of custody is followed for all digital media acquired (e.g. indications, analysis, and warning standard operating procedure) • Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration • Assist in the gathering and preservation of evidence used in the prosecution of computer crimes • Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures) • Prepare reports to document analysis - Encryption • Decrypt seized data using technical means - First Responder • Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law	

	enforcement agencies, vendors, and public relations professionals) • Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents - First Response Basics • Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation - Roles of First Responder • Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.) • Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems • Perform real-time Computer Network • Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs) • Provide technical assistance on digital evidence matters to appropriate personnel • Conduct interviews and interrogations of victims, witnesses and suspects • Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence • Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.) • Independently conducts large-scale investigations of criminal activities involving complicated computer programs and networks - Data Acquisition and Duplication • Examine recovered data for items of relevance to the issue at hand • Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation	

	• Perform static media analysis • Review forensic images and other data sources for recovery of potentially relevant information • Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration • Identify data of intelligence to evidentiary value to support counterintelligence and criminal investigations • Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise - Defeating Anti-forensics Techniques • Identify Anti-Forensics Techniques • Recover Deleted Files and Partitions • Bypass Windows' and Applications' passwords • Detect steganography and identify the hidden content - Log Management and Event Correlation • Perform command and control functions in response to incidents • Analyze computer generated threats - Network Forensics (Intrusion Detection Systems (IDS)) • Perform Computer Network Defense trend analysis and reporting • Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis - Computer Forensics Reports and Investigative Report Writing • Develop reports which organize and document recovered evidence and forensic processes used • Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies	
Digital Forensics	- Recover Data • Perform file signature analysis, Perform tier 1, 2, and 3 malware analysis	25%

	- File System Analysis • Analyze the file systems contents in FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 - Windows Forensics • Collect Volatile and Non-Volatile Information • Perform Windows registry analysis • Perform Cache, Cookie, and History Analysis • Perform Windows File Analysis • Perform Metadata Investigation • Analyze Windows Event Logs - Linux Forensics • Collect Volatile and Non-Volatile Information • Use various Shell Commands • Examine Linux Log files - MAC Forensics • Examine MAC Forensics Data • Examine MAC Log Files • Analyze MAC Directories - Recovering the Deleted Files and Partitions • Examine MAC Forensics Data • Examine MAC Log Files • Analyze MAC Directories - Steganography and Image File Forensics • Detect steganography • Process images in a forensically sound manner - Steganalysis • Perform steganalysis to recover the data hidden using steganography - Application Password Crackers • Understand various password cracking techniques • crack the password to recover protected information and data	

	- Investigating and Analyzing Logs • Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion • Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion - Investigating Network Traffic • Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts - Investigating Wireless Attacks • Investigate wireless attacks - Web Attack Investigation • Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security - Investigating Email Crime and Violation • Perform various steps involved in investigation of email crimes - Mobile Forensic Process • Perform various processes involved in mobile forensics - Cloud Forensics • Perform investigation on cloud storage services such as Google Drive and Dropbox - Malware Forensics • Understand and perform static and dynamic malware analysis - Defeating Anti-Forensic Techniques • Bypass anti-forensic techniques and access the required resources	

Tools/Systems/ Programs	- First Responder Toolkit Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission - Windows Forensic Tools (Helix3 Pro, X-Ways Forensics, Windows Forensic Toolchest (WFT), Autopsy, The Sleuth Kit (TSK), etc.) • Recognize and accurately report forensic artifact indicative of a particular operating system • Perform live forensic analysis (e.g., using Helix in conjunction with LiveView) • Perform dynamic analysis to boot an "image" of a drive (without necessarily having theoriginal drive) to see the intrusion as the user may have seen it, in a native environment • Use data carving techniques (e.g., Autopsy) to extract data for further analysis • Decrypt seized data using technical means - Data Acquisition Software Tools UltraKit Forensic Falcon, etc.) • Perform data acquisition (using UltraKit, Active@ Disk Image, DriveSpy, etc.) - Tools to defeat Anti-Forensics • Use File Recovery Tools (e.g., Recover My Files, EaseUS Data Recovery Wizard, etc.), Partition Recovery Tools (e.g., Active@ Partition Recovery, 7-Data Partition Recovery, Acronis Disk Director Suite, etc.), Rainbow Tables Generating Tools (e.g., rtgen, Winrtgen), Windows Admin Password Resetting Tools (e.g., Active@ Password Changer, Windows Password Recovery Bootdisk, etc.). • Understand the usage of Application Password Cracking Tools (e.g., Passware Kit Forensic, SmartKey Password Recovery Bundle Standard, etc.), Steganography Detection Tools (e.g., Gargoyle Investigator™ Forensic Pro, StegSecret, etc.) - Steganography Tools • Use tools to locate and recover image files - Database Forensics Tools	10%

	• Use tools to perform database forensics (e.g., Database Forensics Using ApexSQL DBA, SQL Server Management Studio, etc.) - Password Cracking Tools • Use tools to recover obstructed evidence - Network Forensics Tools • Use network monitoring tools to capturer real-time traffic spawned by any running malicious code after identifying intrusion via dynamic analysis • Understand the working of wireless forensic tools (e.g., NetStumbler, NetSurveyor, Vistumbler, WirelessMon, Kismet, OmniPeek, CommView for Wi-Fi, Wi-Fi USB Dongle: AirPcap, tcpdump, KisMAC, Aircrack-ng SuiteAirMagnet WiFi Analyzer, MiniStumbler, WiFiFoFum, NetworkManager, KWiFiManager, Aironet Wireless LAN, AirMagnet WiFi Analyzer, Cascade Pilot Personal Edition,Network Observer, Ufasoft Snif, etc.) - Web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools • Understand the working of web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools (e.g., Acunetix Web Vulnerability Scanner, Falcove Web Vulnerability Scanner, Netsparker, N-Stalker Web Application Security Scanner, Sandcat, Wikto, WebWatchBot, OWASP ZAP, dotDefender, IBM AppScan, ServerDefender, Deep Log Analyzer, WebLog Expert, etc.) - Cloud Forensics Tools • Use Cloud Forensics Tools (e.g., UFED Cloud Analyzer, WhatChanged Portable, WebBrowserPassView, etc.) - Malware Forensics Tools • Use Malware Analysis Tools (e.g., VirusTotal, Autoruns for Windows, RegScanner, MJ Registry Watcher, etc.) - Email Forensics Tools • Use email forensic tools (e.g., StellarPhoenix Deleted Email Recovery, Recover My Email, Outlook Express Recovery, Zmeil, Quick Recovery for MS Outlook, Email Detective, Email Trace-Email Tracking, R-Mail, FINALeMAIL, eMailTrackerPro, Paraben's email	

	Examiner, Network Email Examiner by Paraben, DiskInternal's Outlook Express Repair, Abuse.Net, MailDetective Tool, etc.) - Mobile Forensics Software and Hardware Tools • Use mobile forensic software tools (e.g., Oxygen Forensic Suite 2011, MOBILedit! Forensic, BitPim, SIM Analyzer, SIMCon, SIM Card Data Recovery, Memory Card Data Recovery, Device Seizure, Oxygen Phone Manager II, etc.) - Report Writing Tools • Create well formatted computer forensic reports	

EC-Council 312-49 Sample Questions:

Question: 1

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: 2

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: 3

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: 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 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: 6

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) TInternet Artifacts Module
c) Acquisition Module
d) File Processor Module

Answer: c

Question: 7

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: 8

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

Question: 9

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: 10

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

Study Guide to Crack EC-Council 312-49 Exam:

- Getting details of the 312-49 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 312-49 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the EC-Council provided training for 312-49 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 312-49 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 312-49 practice tests is must. Continuous practice will make you an expert in all syllabus areas.