EC-COUNCIL 312-49v11 Computer Hacking Forensic Investigator (CHFI-v11) Exam Questions Get Excellent Scores

DOWNLOAD the newest PrepPDF 312-49v11 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=13-b1JlasHG_tAYKW8ZJiXNqSVG-_59gj

Annual test syllabus is essential to predicate the real 312-49v11 questions. So you must have a whole understanding of the test syllabus. After all, you do not know the 312-49v11 exam clearly. It must be difficult for you to prepare the 312-49v11 exam. Then our 312-49v11 Study Materials can give you some guidance for our professional experts have done all of these above matters for you by collecting the most accurate questions and answers. And you can have a easy time to study with them.

EC-COUNCIL 312-49v11 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Acquisition and Duplication: This domain addresses live and dead acquisition techniques, eDiscovery methodologies, data acquisition formats, validation procedures, write protection, and forensic image preparation for examination.
Topic 2	• Computer Forensics Investigation Process: This domain addresses the structured investigation phases including first response procedures, lab setup, evidence preservation, data acquisition, case analysis, documentation, reporting, and expert witness testimony.
Topic 3	• Linux and Mac Forensics: This domain addresses forensic methodologies for Linux and macOS systems including data collection, memory forensics, log analysis, APFS examination, and platform-specific investigation tools.
Topic 4	• Windows Forensics: This domain covers Windows-specific investigation techniques including volatile and non-volatile data collection, memory and registry analysis, web browser forensics, metadata examination, and analysis of Windows artifacts like ShellBags, LNK files, and event logs.

Topic 5	• Investigating Web Attacks: This domain covers web application forensics including IIS and Apache log analysis, OWASP Top 10 risks, and investigation of attacks like XSS, SQL injection, path traversal, command injection, and brute-force attempts.
Topic 6	• Cloud Forensics: This domain covers cloud platform forensics (AWS, Azure, Google Cloud) including data storage, logging, forensic acquisition of virtual machines, and investigation of cloud security incidents.
Topic 7	• Understanding Hard Disks and File Systems: This domain covers storage media characteristics, disk logical structures, operating system boot processes (Windows, Linux, macOS), file systems analysis, encoding standards, and examination of common file formats.
Topic 8	• IoT Forensics: This domain addresses IoT device investigation including architecture, OWASP IoT threats, forensic processes, wearable and smart device analysis, hardware-level techniques (JTAG, chip-off), and drone data extraction.
Topic 9	• Defeating Anti-Forensics Techniques: This domain teaches methods to overcome evidence hiding techniques including data recovery, file carving, partition recovery, password cracking, steganography detection, encryption handling, and program unpacking.
Topic 10	• Computer Forensics in Today's World: This domain covers fundamentals of computer forensics including cybercrime types, investigation procedures, digital evidence handling, forensic readiness, investigator roles and responsibilities, industry standards, and legal compliance requirements.
Topic 11	• Malware Forensics: This domain addresses malware investigation including controlled lab setup, static analysis, system and network behavior analysis, suspicious document examination, and ransomware investigation techniques.

New EC-COUNCIL 312-49v11 Test Review & 312-49v11 Study Guide Pdf

Why don't you begin to act? The first step is to pass 312-49v11 exam. Time will wait for no one. Only if you pass the exam can you get a better promotion. And if you want to pass it more efficiently, we must be the best partner for you. Because we are professional 312-49v11 Questions torrent provider, we are worth trusting; because we make great efforts, we do better. Here are some reasons to choose us.

EC-COUNCIL Computer Hacking Forensic Investigator (CHFI-v11) Sample Questions (Q401-Q406):

NEW QUESTION # 401
During a ransomware triage in a Microsoft Azure environment, forensic analysts are instructed to preserve evidence from a compromised azure-ubuntu virtual machine by creating a snapshot of its OS disk through the Azure portal. Which of the following sequences accurately completes this task?

- A. Install Azure CLI on a remote forensic workstation, run az login, execute the az vm show command with storageProfile.osDisk.name to view the source disk ID, then run the az snapshot create command with the required parameters
- B. Locate the azure-ubuntu OS disk from the Production-group and click on it, click on Create Snapshot, click on Review plus Create, then click on Create
- C. Stop the azure-ubuntu VM, locate the azure-ubuntu OS disk from the Production-group and click on it, click on Create Snapshot, on the Create Snapshot page give a desired name for the OS snapshot, select the snapshot type as read-only, select a storage type, then click on Review plus Create
- D. Create a snapshot of the OS disk of the suspect VM, copy the snapshot to a storage account under a different resource group, delete the snapshot from the source resource group, and create a backup copy, then mount the snapshot onto the forensic workstation

Answer: C

Explanation:
The correct answer is D because it describes the Azure portal workflow for creating a forensic-style snapshot of the OS disk while preserving the source in a read-only state. Microsoft's Azure documentation explains that a snapshot can be created from a managed disk, and choosing a read-only style is the appropriate preservation-oriented approach for evidentiary handling. Option C is incomplete because it skips the important configuration details that define the snapshot properly, including naming, snapshot characteristics, and storage selection. Option B uses Azure CLI rather than the Azure portal, while the question explicitly asks for the portal-based sequence. Option A adds unnecessary and potentially misleading steps that are not part of the basic snapshot creation task. CHFI v11 includes cloud forensics, Azure evidence acquisition, and VM snapshot acquisition using Azure Portal and PowerShell, so candidates are expected to identify the correct, defensible preservation workflow. Since the scenario focuses on portal-based preservation of a compromised VM's OS disk, the sequence that includes creating a read-only snapshot from the disk in the portal is the best answer.

NEW QUESTION # 402
Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN- DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

- A. WIN-DTRAl83202Xrelay-bin.index
- B. WIN-DTRAI83202Xslow.log
- C. WIN-DTRAI83202X-bin.nnnnnn
- D. relay-log.info

Answer: B

NEW QUESTION # 403
Andie, a network administrator, suspects unusual network services running on a windows system.
Which of the following commands should he use to verify unusual network services started on a Windows system?

- A. lusrmgr
- B. net serv
- C. netmgr
- D. net start

Answer: D

NEW QUESTION # 404
Edward, an experienced CHFI professional, was conducting an investigation into potential intellectual property theft at a major corporation. The company had identified the suspected system, and Edward was tasked with collecting data. Given the high-stakes nature of the investigation, Edward needed to ensure that the collected data was forensically sound, maintained its integrity, and could withstand scrutiny in a court of law. To accomplish this, which rule of thumb for data acquisition should Edward adhere to?

- A. Edward should focus on non-volatile data as it remains consistent.
- B. Edward should avoid making changes to the original data.
- C. Edward should opt for live data acquisition, irrespective of the system state.
- D. Edward should rely on network based acquisition as it is less intrusive.

Answer: B

Explanation:
Option B is the best answer because one of the most fundamental forensic acquisition principles is to avoid changing the original evidence . CHFI v11 emphasizes preserving evidence , best practices for handling digital evidence , data acquisition methodology , and maintaining evidence integrity so the results remain defensible in legal or disciplinary proceedings. That principle applies regardless of device type, operating system, or case category.
This rule of thumb is broader and more important than the other options because the correct acquisition approach depends on the system state and circumstances. Live acquisition is not always appropriate.
Focusing only on non-volatile data may cause investigators to miss valuable volatile evidence. Network- based acquisition is not universally the least intrusive or the best approach. What remains constant is the duty to minimize alteration of the original source.

By preserving the original data and performing analysis on properly acquired copies, the investigator protects the integrity, repeatability, and admissibility of the evidence. Therefore, the most accurate CHFI-aligned rule of thumb is that Edward should avoid making changes to the original data during acquisition.

NEW QUESTION # 405
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

- A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
- B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule
- D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList

Answer: D

NEW QUESTION # 406
.....