

Boost Your CHFIv11 Exam Preparation with Eccouncil 312-49v11 Exam Questions

Preparing for the Eccouncil 312-49v11 exam can be challenging if you don't know where to focus. Pass4Future provides the latest Eccouncil 312-49v11 Exam Questions that make understanding digital forensics concepts easier and highlight the areas where you need more practice. By working through these 312-49v11 practice questions, you can reinforce your knowledge, identify weak spots, and gain the confidence to tackle the exam with certainty. Don't leave your success to chance, practice with Pass4Future and take a step closer to becoming a certified Computer Hacking Forensic Investigator(CHFIv11). Here are some Eccouncil 312-49v11 sample questions:

1. A digital forensics investigator is tasked with analyzing a compromised Mac computer recovered from a cybercrime scene. However, upon examination, the investigator discovers that the log messages containing crucial evidence have been tampered with or deleted. Given the tampering or deletion of log messages on the Mac computer, which anti-forensic technique is likely employed to hinder the forensic analysis process in this scenario?

- A. Data encryption
- B. Data obfuscation
- C. Data hiding
- D. Data manipulation

2. A digital forensic investigator is tasked with analyzing an NTFS image file extracted from a pen drive. They leverage The Sleuth Kit (TSK) for this task, specifically utilizing the fsstat command-line tool. By employing fsstat, they delve into the file system's intricate details, such as metadata, inode numbers, and block or cluster information, thereby facilitating a comprehensive examination. How can an investigator use TSK to analyze disk images?

- A. By performing network scans
- B. By conducting manual inspections
- C. By using the plug-in framework
- D. By writing custom code

PASS4FUTURE

3. A forensic investigator is examining a system that has experienced a failure during booting. The investigator discovers that the boot process was interrupted after the BIOS had initialized the system hardware. What is the next step in the boot process that would have occurred had it not failed?

- A. The boot manager would locate the bootable partition and load the MBR.
- B. The kernel would start and load the system's hardware abstraction layer (HAL).
- C. The system would load the ntoskrnl.exe file from the boot partition.
- D. The bootloader would load the operating system's kernel.

4. Nora, a forensic investigator, is examining the Windows Registry of a compromised system as part of her investigation into a potential insider threat. She wants to determine which folders were most recently accessed by the user. After reviewing the Registry, she discovers that a particular Registry key stores information about the folders the user recently accessed, including the folder names and their paths in the file system. Based on her findings, which of the following Registry keys contains this information?

- A. BagMRU key
- B. MRUListEx key
- C. Bags key
- D. NodeSlot value

5. Alex, a system administrator, is tasked with converting an existing EXT2 file system to an EXT3 file system on a Linux machine. The EXT2 file system is currently in use, and Alex needs to enable journaling to convert it to EXT3. Which of the following commands should Alex use to achieve this conversion?

- A. C:>ECHO text_message > myfile.txt:stream1
- B. C:>MORE < myfile.txt:stream1
- C. dd if=mbr.backup of=/dev/xxx bs=512 count=1
- D. # /sbin/tune2fs -j

Visit Now: <https://www.pass4future.com/questions/eccouncil/312-49v11>