

## Passed EC-Council EC1-349 Exam Today - Free Download EC1-349 Dumps

Vendor: EC-Council Exam Code: EC1-349 Exam Name: Computer Hacking Forensic Investigator Exam QUESTION 1 Which of the following statements does not support the case assessment? A. Review the case investigator's request for service B. Identify the legal authority for the forensic examination request C. Do not document the chain of custody D. Discuss whether other forensic processes need to be performed on the evidence Answer: C QUESTION 2 Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it? A. War driving B. Rogue access points C. MAC spoofing D. Client mis-association Answer: D QUESTION 3 File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows? 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 Answer: B QUESTION 4 What is cold boot (hard boot)? A. It is the process of starting a computer from a powered-down or off state B. It is the process of restarting a computer that is already turned on through the operating system C. It is the process of shutting down a computer from a powered-on or on state D. It is the process of restarting a computer that is already in sleep mode Answer: A QUESTION 5 When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you \_\_\_\_\_. A. Restart Windows B. Kill the running processes in Windows task manager C. Run the antivirus tool on the system D. Run the anti-spyware tool on the system Answer: A QUESTION 6 WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2? A. RC4-CCMP B. RC4-TKIP C. AES-CCMP D. AES-TKIP Answer: C QUESTION 7 The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data. A. True B. False Answer: B QUESTION 8 What is a bit-stream copy? A. Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk B. A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition C. A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition D. Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk Answer: A QUESTION 9 System software password cracking is defined as cracking the operating system and all other utilities that enable a computer to function A. True B. False Answer: A QUESTION 10 Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication? A. Substitution techniques B. Transform domain techniques C. Cover generation techniques D. Spread spectrum techniques Answer: C QUESTION 11 Ron, a computer forensics expert, Is Investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in on condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations he can use to recover the IMEI number? A. \*#06\*# B. \*#06# C. #06r D. \*1MEI# Answer: B QUESTION 12 Who is responsible for the following tasks? Secure the scene and ensure that it is maintained in a secure state until the Forensic Team advises Make notes about the scene that will eventually be handed over to the Forensic Team A. Non-Laboratory Staff B. System administrators C. Local managers or other non-forensic staff D. Lawyers Answer: A QUESTION 13 A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file? A. Plaintext B. Single pipe character C. Multiple pipe characters D. HTML tags Answer: A QUESTION 14 During the seizure of digital evidence, the suspect can be allowed touch the computer system. A. True B. False Answer: B QUESTION 15 Which of the following password cracking techniques works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password? A. Brute forcing attack B. Hybrid attack C. Syllable attack D. Rule-based attack Answer: B QUESTION 16 Consistency in the investigative report is more important than the exact format in the report to eliminate uncertainty and confusion. A. True B. False Answer: A QUESTION 17 When dealing with the powered-off computers at the crime scene, if the computer is switched off, turn it on A. True B. False Answer: B If you want to pass EC-Council EC1-349 successfully, donot missing to read latest lead2pass EC-Council EC1-349 dumps.If you can master all lead2pass questions you will able to pass 100% guaranteed. <http://www.lead2pass.com/EC1-349.html>