



EC0-349^{Q&As}

Computer Hacking Forensic Investigator

Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/ec0-349.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

- A. Image the disk and try to recover deleted files
- B. Seek the help of co-workers who are eye-witnesses
- C. Check the Windows registry for connection data (you may or may not recover)
- D. Approach the websites for evidence

Correct Answer: A

QUESTION 2

During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

- A. C:\Program Files\Exchsrvr\servername.log
- B. D:\Exchsrvr\Message Tracking\servername.log
- C. C:\Exchsrvr\Message Tracking\servername.log
- D. C:\Program Files\Microsoft Exchange\srvr\servername.log

Correct Answer: A

QUESTION 3

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.

- A. A Capital X
- B. A Blank Space
- C. The Underscore Symbol
- D. The lowercase Greek Letter Sigma (s)

Correct Answer: D

QUESTION 4



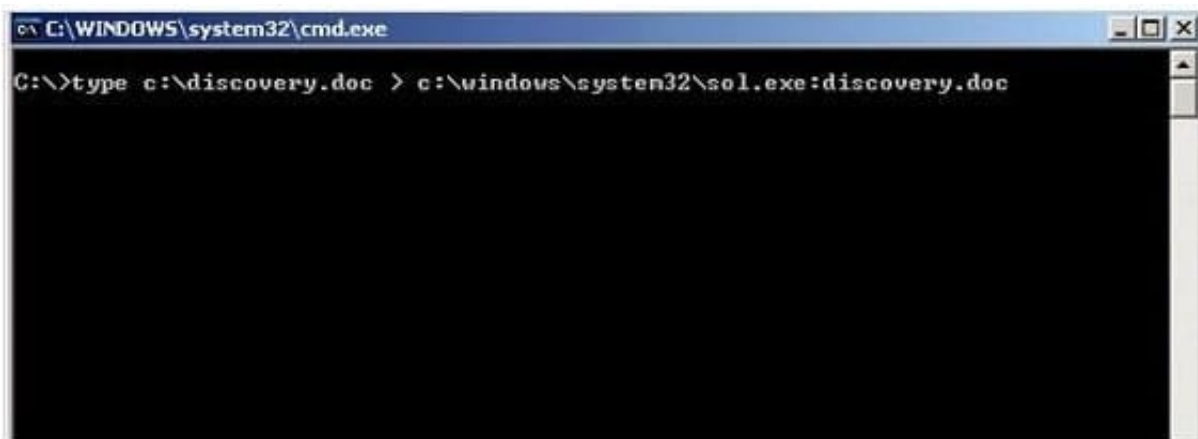
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. False negatives
- B. False positives
- C. True negatives
- D. True positives

Correct Answer: A

QUESTION 5

What feature of Windows is the following command trying to utilize?



```
C:\WINDOWS\system32\cmd.exe
C:\>type c:\discovery.doc > c:\windows\system32\sol.exe:discovery.doc
```

- A. White space
- B. AFS
- C. ADS
- D. Slack file

Correct Answer: C

[EC0-349 PDF Dumps](#)

[EC0-349 VCE Dumps](#)

[EC0-349 Braindumps](#)