312-49V10$^{Q\&As}$

ECCouncil Computer Hacking Forensic Investigator (V10)

QUESTION 1

Which of the following hives in Windows registry contain configuration information related to the application type that is used to open various files on the system?

A. HKEY_CURRENT_CONFIG

B. HKEY_CLASSES_ROOT

C. HKEY_CURRENT_USER

D. HKEY_LOCAL MACHINE

Correct Answer: B

Reference: https://what-when-how.com/windows-forensic-analysis/registry-analysis-windows-forensicanalysis-part-1/#:~:text=Each%20of%20these%20hives%20plays,the%20function%20of%20the%20system.andtext=The%20HKEY_CURRENT_CONFIG%20hive%20contains%20the,various%20files%20on%20the%20system

QUESTION 2

When reviewing web logs, you see an entry for esource not found?in the HTTP status code field. What is the actual error code that you wouldWhen reviewing web logs, you see an entry for ?esource not found?in the HTTP status code field. What is the actual error code that you would see in the log for esource not found?see in the log for ?esource not found?

A. 202

B. 404

C. 606

D. 999

Correct Answer: B

QUESTION 3

Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

A. TestDisk for Windows

B. R-Studio

C. Windows Password Recovery Bootdisk

D. Passware Kit Forensic

Correct Answer: D

QUESTION 4

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

A. The X509 Address

B. The SMTP reply Address

C. The E-mail Header

D. The Host Domain Name

Correct Answer: C

QUESTION 5

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

A. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum

B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file

C. A simple DOS copy will not include deleted files, file slack and other information

D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector

Correct Answer: C