GD0-100$^{Q\&As}$

Certification Exam For ENCE North America

Pass Guidance Software GD0-100 Exam with 100% Guarantee

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

https://www.passapply.com/gd0-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Guidance Software Official Exam Center

QUESTION 1

You are assigned to assist with the search and seizure of several computers. The magistrate ordered that the computers cannot be seized unless they are found to contain any one of ten previously identified images. You currently have the ten images in JPG format. Using the EnCase methodology, how would you best handle this situation?

A. UseFastBloc or a network/parallel port cable to preview the hard drives. Go to the Gallery view and search for the previously identified images.

B. UseFastBloc or a network/parallel port cable to acquire forensic images of the hard drives, then search the evidence files for the previously identified images.

C. UseFastBloc or a network/parallel port cable to preview the hard drives. Conduct a hash analysis of the files on the hard drives, using a hash library containing the hash values of the previously identified images.

D. Use an EnCase DOS boot disk to conduct a text search for child porn. Use an EnCase DOS boot disk to conduct a text search for child porn?

Correct Answer: C

QUESTION 2

Which of the following is found in the FileSignatures.ini configuration file

A. The results of a hash analysis

B. The information contained in the signature table

C. The results of a signature analysis

D. Pointers to an evidence file

Correct Answer: B

QUESTION 3

The signature table data is found in which of the following files?

A. The evidence file

B. The configuration FileSignatures.ini file

C. All of the above

D. The case file

Correct Answer: B

QUESTION 4

In DOS acquisition mode, if a physical drive is detected, but no partition information is displayed, what would be the cause:

A. Both a and b

B. The partition scheme is not recognized by DOS.

C. Neither a or b

D. There are no partitions present.

Correct Answer: A

QUESTION 5

A SCSI drive is pinned as a master when it is:

A. The only drive on the computer.

B. The primary of two drives connected to one cable.

C. Whenever another drive is on the same cable and is pinned as a slave.

D. A SCSI drive is not pinned as a master.

Correct Answer: D

QUESTION 6

The following GREP expression was typed in exactly as shown. Choose the answer(s) that would result. [^a-z] Tom[^a-z]

A. Tomato

B. om RP

C. Toms

D. Stomp

Correct Answer: B

QUESTION 7

This question addresses the EnCase for Windows search process. If a target word is within a logical file, and it begins in cluster 10 and ends in cluster 15 (the word is fragmented), the search:

A. Will not find it unlessile slack is checked on the search dialog box.

B. Will find it because EnCase performs a logical search.

C. Will not find it because EnCase performs a physical search only.

D. Will not find it because the letters of the keyword are not contiguous.

Correct Answer: B

QUESTION 8

During the power-up sequence, which of the following happens first?

A. The boot sector is located on the hard drive.

B. Theower On Self-Test.? 7KH ? RZHU2Q6HOI7HVW

C. The floppy drive is checked for a diskette.

D. The BIOS on an add-in card is executed.

Correct Answer: B

QUESTION 9

If cases are worked on a lab drive in a secure room, without any cleaning of the contents of the drive, which of the following areas would be of most concern?

A. There is no concern

B. Cross-contamination

C. Chain-of-custody

D. Storage

Correct Answer: B

QUESTION 10

A suspect typed a file on his computer and saved it to a floppy diskette. The filename was MyNote.txt. You receive the floppy and the suspect computer. The suspect denies that the floppy disk belongs to him. You search the suspect computer and locate only the suspect? computer. The suspect denies that the floppy disk belongs to him. You search the suspect? computer and locate only the filename within a .LNK file. The .LNK file is located in the folder C:\Windows \Recent. How you would use the .LNK file to establish a connection between the file on the floppy diskette and the suspect computer? connection between the file on the floppy diskette and the suspect? computer?

A. Both a and b

B. The dates and time of the file found in the .LNK file, at file offset 28

C. The full path of the file, found in the .LNK file

D. The file signature found in the .LNK file

Correct Answer: A

QUESTION 11

Which of the following items could contain digital evidence?

A. Credit card readers

B. Personal assistant devices

C. Cellular phones

D. Digital cameras

Correct Answer: ABCD

QUESTION 12

Will EnCase allow a user to write data into an acquired evidence file

A. Yes, but only bookmarks.

B. Yes, but only to resize the partitions.

C. No. Data cannot be added to the evidence file after the acquisition is made.

D. Yes, but only case information.

E. No, unless the user established a writing privilege when the evidence was acquired.

Correct Answer: C

QUESTION 13

In Windows 98 and ME, Internet based e-mail, such as Hotmail, will most likely be recovered in the ______________________ folder.

A. C:\Windows\Online\Applications\email

B. C:\Windows\Temporary Internet files

C. C:\Windows\History\Email

D. C:\Windows\Temp

Correct Answer: B

QUESTION 14

Assume that MyNote.txt has been deleted. The FAT file system directory entry for that file has been overwritten. The data for MyNote.txt is now:

A. Overwritten

B. Allocated

C. Cross-linked

D. Unallocated

Correct Answer: D

QUESTION 15

Which of the following directories contain the information that is found on a Windows 98 Desktop?

A. C:\Program files\Programs\Desktop

B. C:\Desktop

C. C:\Startup\Desktop\Items

D. C:\Windows\Desktop

Correct Answer: D