

GD0-110^{Q&As}

Certification Exam for EnCE Outside North America

Pass Guidance Software GD0-110 Exam with 100% Guarantee

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

<https://www.leads4pass.com/gd0-110.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

A sector on a floppy disk is the same size as a sector on a NTFS formatted hard drive.

- A. True
- B. False

Correct Answer: A

QUESTION 2

RAM is tested during which phase of the power-up sequence?

- A. None of the above.
- B. During POST
- C. After POST
- D. Pre-POST

Correct Answer: B

QUESTION 3

A case file can contain hard drive images?

- A. 1
- B. 5
- C. 10
- D. any number of

Correct Answer: D

QUESTION 4

A restored floppy diskette will have the same hash value as the original diskette.

- A. True
- B. False

Correct Answer: A

QUESTION 5

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

- A. The case file
- B. All of the above
- C. The configuration FileSignatures.ini file
- D. The evidence file

Correct Answer: C

QUESTION 6

ROM is an acronym for:

- A. Random Open Memory
- B. Read Open Memory
- C. Relative Open Memory
- D. Read Only Memory

Correct Answer: D

QUESTION 7

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. Storage
- B. There is no concern
- C. Chain-of-custody
- D. Cross-contamination

Correct Answer: D

QUESTION 8

When an EnCase user double-clicks on a file within EnCase what determines the action that will result?

- A. The setting in the evidence file.
- B. Both a and b.

- C. The settings in the case file.
- D. The settings in the FileTypes.ini file.

Correct Answer: D

QUESTION 9

When a document is printed using EMF in Windows, what file(s) are generated in the spooling process?

- A. The .SHD file
- B. The .SPL file
- C. Both a and b
- D. Neither a or b

Correct Answer: C

QUESTION 10

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. Use FastBloc or a network/parallel port cable to acquire forensic images of the hard drives, then search the evidence files for the previously identified images.
- B. Use FastBloc or a network/parallel port cable to preview the hard drives. Go to the Gallery view and search for the previously identified images.
- C. Use FastBloc 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 hild porn. Use an EnCase DOS boot disk to conduct a text search for child porn?

Correct Answer: C

QUESTION 11

When a file is deleted in the FAT or NTFS file systems, what happens to the data on the hard drive?

- A. The file header is marked with a Sigma so the file is not recognized by the operating system.
- B. It is moved to a special area.
- C. It is overwritten with zeroes.

D. Nothing.

Correct Answer: D

QUESTION 12

The EnCase signature analysis is used to perform which of the following actions?

- A. Analyzing the relationship of a file signature to its file header. Analyzing the relationship of a file signature to its file header.
- B. Analyzing the relationship of a file signature to a list of hash sets. Analyzing the relationship of a file signature to a list of hash sets.
- C. Analyzing the relationship of a file signature to its computed MD5 hash value. Analyzing the relationship of a file signature to its computed MD5 hash value.

Correct Answer: A

QUESTION 13

How many partitions can be found in the boot partition table found at the beginning of the drive?

- A. 4
- B. 2
- C. 8
- D. 6

Correct Answer: A

QUESTION 14

GREP terms are automatically recognized as GREP by EnCase.

- A. True
- B. False

Correct Answer: B

QUESTION 15

When does the POST operation occur?

- A. When the power button to a computer is turned on.

- B. When SCSI devices are configured.
- C. When Windows starts up.
- D. After a computer begins to boot from a device.

Correct Answer: A

[GD0-110 PDF Dumps](#)

[GD0-110 Study Guide](#)

[GD0-110 Braindumps](#)