

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.pass2lead.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

The following GREP expression was typed in exactly as shown. Choose the answer(s) that would result. 800[] \-]+555-1212

- A. 800-555 1212
- B. 800.555.1212
- C. 8005551212
- D. (800) 555-1212

Correct Answer: D

QUESTION 2

Which of the following aspects of the EnCase evidence file can be changed during a reacquire of the evidence file?

- A. The investigator name The investigator? name
- B. The acquisition notes
- C. None of the above
- D. The evidence number

Correct Answer: C

QUESTION 3

You are investigating a case of child pornography on a hard drive containing Windows XP. In the : \Documents and Settings\Bad You are investigating a case of child pornography on a hard drive containing Windows XP. In the : \Documents and Settings\Bad Guy\Local Settings\Temporary Internet Files folder you find three images of child pornography. You find no other copies of the images on the suspect hard drive, and you find no other copies of the filenames. What can be deduced from your findings images on the suspect hard drive, and you find no other copies of the filenames. What can be deduced from your findings?

- A. The presence and location of the images is strong evidence of possession.
- B. The presence and location of the images proves the images were intentionally downloaded.
- C. Both a and c
- D. The presence and location of the images is not strong evidence of possession.

Correct Answer: D

QUESTION 4

Before utilizing an analysis technique on computer evidence, the investigator should:

- A. Test the technique on simulated evidence in a controlled environment to confirm that the results are consistent.
- B. Neither a or b.
- C. Be trained in the employment of the technique.
- D. Both a and b.

Correct Answer: D

QUESTION 5

All investigators using EnCase should run tests on the evidence file acquisition and verification process to:

- A. Give more weight to the investigator testimony in court. Give more weight to the investigator? testimony in court.
- B. Further the investigator understanding of the evidence file. Further the investigator? understanding of the evidence file.
- C. All of the above.
- D. Insure that the investigator is using the proper method of acquisition.

Correct Answer: C

QUESTION 6

If cluster #3552 entry in the FAT table contains a value of this would mean:

- A. The cluster is allocated
- B. The cluster is marked bad
- C. The cluster is unallocated
- D. The cluster is the end of a file

Correct Answer: C

QUESTION 7

A personal data assistant was placed in a evidence locker until an examiner has time to examine it. Which of the following areas would require special attention?

- A. Chain-of-custody
- B. Cross-contamination
- C. Storage

D. There is no concern

Correct Answer: C

QUESTION 8

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

- A. No. Data cannot be added to the evidence file after the acquisition is made.
- B. Yes, but only bookmarks.
- C. Yes, but only case information.
- D. No, unless the user established a writing privilege when the evidence was acquired.
- E. Yes, but only to resize the partitions.

Correct Answer: A

QUESTION 9

Which of the following would most likely be an add-in card?

- A. Anything plugged into socket 7
- B. A motherboard
- C. A video card that is connected to the motherboard in the AGP slot
- D. The board that connects to the power supply

Correct Answer: C

QUESTION 10

Search terms are stored in what .ini configuration file?

- A. FileTypes.ini
- B. FileSignatures.ini
- C. TextStyle.ini
- D. Keywords.ini

Correct Answer: D

QUESTION 11

How many copies of the FAT are located on a FAT 32, Windows 98-formatted partition?

- A. 3
- B. 1
- C. 4
- D. 2

Correct Answer: D

QUESTION 12

The Windows 98 Start Menu has a selection called documents which displays a list of recently used files. Which of the following The Windows 98 Start Menu has a selection called documents which displays a list of recently used files. Which of the following folders contain those files?

- A. C:\Windows\History
- B. C:\Windows\Documents
- C. C:\Windows\Start menu\Documents
- D. C:\Windows\Recent

Correct Answer: D

QUESTION 13

A file extension and signature can be manually added by:

- A. Right-clicking on a file and selecting dd.? 5LJKWFOLFNLQJRQDILQHDQGVHOFHLQJ ? GG
- B. Using the new file signature feature under file signatures.
- C. Using the new library feature under hash libraries.
- D. Using the new set feature under hash sets.

Correct Answer: B

QUESTION 14

GREP terms are automatically recognized as GREP by EnCase.

- A. True
- B. False

Correct Answer: B

QUESTION 15

A standard DOS 6.22 boot disk is acceptable for booting a suspect drive.

A. True

B. False

Correct Answer: B

[GD0-110 PDF Dumps](#)

[GD0-110 Practice Test](#)

[GD0-110 Study Guide](#)