GD0-100Q&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.pass2lead.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

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

QUESTION 1

You are conducting an investigation and have encountered a computer that is running in the field. The operating system is Windows XP. A software program is currently running and is visible on the screen. You should:

A. Navigate through the program and see what the program is all about, then pull the plug.

B. Pull the plug from the back of the computer.

C. Photograph the screen and pull the plug from the back of the computer.

D. Pull the plug from the wall.

Correct Answer: C

QUESTION 2

EnCase can build a hash set of a selected group of files.

A. True

B. False

Correct Answer: A

QUESTION 3

To later verify the contents of an evidence file 7RODWHUYHULI\WKHFRQWHQWVRIDQHYLGHQFHILOH

A. EnCase writes a CRC value for every 64 sectors copied.

B. EnCase writes a CRC value for every 128 sectors copied.

C. EnCase writes an MD5 hash value every 64 sectors copied.

D. EnCase writes an MD5 hash value for every 32 sectors copied.

Correct Answer: A

QUESTION 4

In DOS and Windows, how many bytes are in one FAT directory entry?

A. Variable

B. 32

C. 16

D. 64

E. 8

Correct Answer: B

QUESTION 5

Within EnCase for Windows, the search process is:

A. None of the above

B. both a and b

C. a search of the physical disk in unallocated clusters and other unused disk areas

D. a search of the logical files

Correct Answer: B

QUESTION 6

The first sector on a volume is called the:

A. Master file table

B. Volume boot device

C. Volume boot sector or record

D. Master boot record

Correct Answer: C

QUESTION 7

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

A. 2

B. 3

C. 1

D. 4

Correct Answer: A

QUESTION 8

The following keyword was typed in exactly as shown. Choose the answer(s) that would be found. All search criteria have default settings. Tom

A. Tomorrow

B. TomJ@hotmail.com

C. Tom

D. Stomp

Correct Answer: ABCD

QUESTION 9

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

A. Nothing.

B. It is moved to a special area.

C. It is overwritten with zeroes.

D. The file header is marked with a Sigma so the file is not recognized by the operating system.

Correct Answer: A

QUESTION 10

A signature analysis has been run on a case. The result ?*JPEG ?in the signature column means:

A. The file signature is unknown and the header is a JPEG.

B. The file signature is a JPEG signature and the file extension is incorrect.

C. The file signature is unknown and the file extension is JPEG.

D. None of the above.

Correct Answer: B

QUESTION 11

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 12

When a file is deleted in the FAT file system, what happens to the FAT?

A. The FAT entries for that file are marked as allocated.

B. Nothing.

C. It is deleted as well.

D. The FAT entries for that file are marked as available.

Correct Answer: D

QUESTION 13

When an EnCase user double-clicks on a valid .jpg file, that file is:

A. Copied to the default export folder and opened by an associated program.

B. Renamed to JPG_0001.jpg and copied to the default export folder.

C. Copied to the EnCase specified temp folder and opened by an associated program.

D. Opened by EnCase.

Correct Answer: C

QUESTION 14

For an EnCase evidence file acquired with a hash value to pass verification, which of the following must be true?

A. The MD5 hash value must verify.

B. The CRC values must verify.

C. The CRC values and the MD5 hash value both must verify.

D. Either the CRC or MD5 hash values must verify.

Correct Answer: C

QUESTION 15

You are an investigator and have encountered a computer that is running at the home of a suspect. The computer does

not appear to be a part of a network. The operating system is Windows XP Home. No programs are visibly running. You should:

A. Pull the plug from the back of the computer.

B. Turn it off with the power button.

C. Pull the plug from the wall.

D. Shut it down with the start menu.

Correct Answer: A