GD0-110$^{\text{Q\&As}}$

Certification Exam for EnCE Outside North America

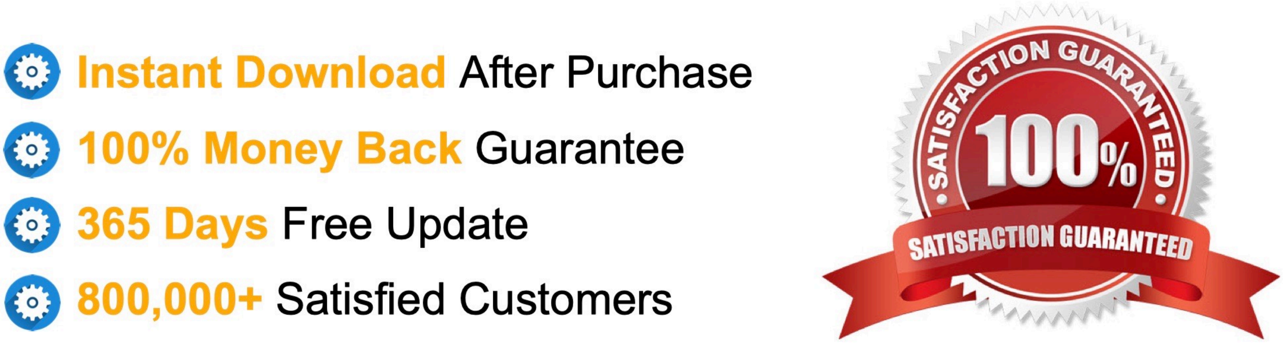
Pass Guidance Software GD0-110 Exam with 100% Guarantee

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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which of the following selections would be used to keep track of a fragmented file in the FAT file system?

A. All of the above

B. The partition table of extents

C. The File Allocation Table

D. The directory entry for the fragmented file

Correct Answer: C

QUESTION 2

Which of the following would be a true statement about the function of the BIOS?

A. The BIOS is responsible for checking and configuring the system after the power is turned on.

B. Botha and c.

C. The BIOS is responsible for swapping out memory pages when RAM fills up.

D. The BIOS integrates compressed executable files with memory addresses for faster execution.

Correct Answer: A

QUESTION 3

In Windows 2000 and XP, which of the following directories contain user personal folders?

A. C:\WINNT\Profiles

B. C:\Documents and Settings

C. C:\Windows\Users

D. C:\Personnel Folders

Correct Answer: B

QUESTION 4

Within EnCase, you highlight a range of data within a file. The length indicator displays the value 30. How many bytes have you actually selected?

A. 15

B. 30

C. 3

D. 60

Correct Answer: B

QUESTION 5

To undelete a file in the FAT file system, EnCase obtains the starting extent from the:

A. Directory entry

B. Operating system

C. File header

D. FAT

Correct Answer: A

QUESTION 6

How does EnCase verify that the case information (Case Number, Evidence Number, Investigator Name, etc) in an evidence file has not been damaged or changed, after the evidence file has been written?

A. The .case file writes a CRC value for the case information and verifies it when the case is opened.

B. EnCase does not verify the case information and case information can be changed by the user as it becomes necessary.

C. EnCase writes a CRC value of the case information and verifies the CRC value when the evidence is added to a case.

D. EnCase writes an MD5 hash value for the entire evidence file, which includes the case information, and verifies the MD5 hash when the evidence is added to a case.

Correct Answer: C

QUESTION 7

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 8

The acronym ASCII stands for:

A. American Standard Communication Information Index

B. Accepted Standard Communication Information Index

C. American Standard Code for Information Interchange

D. Accepted Standard Code for Information Interchange

Correct Answer: C

QUESTION 9

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

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

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

C. The ower On Self-Test.? 7KH ? RZHU2Q6HOI7HVW

D. The floppy drive is checked for a diskette.

Correct Answer: C

QUESTION 10

What files are reconfigured or deleted by EnCase during the creation of an EnCase boot disk?

A. command.com

B. io.sys

C. autoexec.bat

D. drvspace.bin

Correct Answer: ABD

QUESTION 11

Within EnCase for Windows, the search process is:

A. a search of the logical files

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

C. both a and b

D. None of the above

Correct Answer: C

QUESTION 12

Within EnCase, what is purpose of the default export folder?

A. This is the folder used to hold copies of files that are sent to external viewers.

B. This is the folder that will automatically store an evidence file when the acquisition is made in DOS.

C. This is the folder that will be automatically selected when the copy/unerase feature is used.

D. This is the folder that temporarily stores all bookmark and search results.

Correct Answer: C

QUESTION 13

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. Shut it down with the start menu.

C. Pull the plug from the wall.

D. Turn it off with the power button.

Correct Answer: A

QUESTION 14

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 15

In the EnCase environment, the term xternal viewers?is best described as: In the EnCase environment, the term ?xternal viewers?is best described as:

A. Programs that are exported out of an evidence file.

B. Programsthat are associated with EnCase to open specific file types.

C. Any program that will work with EnCase.

D. Any program that is loaded on the lab hard drive.

Correct Answer: B