Vendor: Guidance Software

Exam Code:GD0-100

Exam Name: Certification Exam For ENCE North America

Version: Demo

QUESTION 1

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 2

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\Start menu\Documents

C. C:\Windows\Documents

D. C:\Windows\Recent

Correct Answer: D

QUESTION 3

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 4

Which of the following selections is NOT found in the case file

A. External viewers

B. Pointers to evidence files

C. Signature analysis results

D. Search results

Correct Answer: A

QUESTION 5

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

A. Pre-POST

B. After POST

C. During POST

D. None of the above.

Correct Answer: C

QUESTION 6

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

A. The cluster is unallocated

B. The cluster is the end of a file

C. The cluster is allocated

D. The cluster is marked bad

Correct Answer: A

QUESTION 7

A case file can contain ____ hard drive images?

A. 5

B. 1

C. any number of

D. 10

Correct Answer: C

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

A hash set would most accurately be described as:

A. A group of hash libraries organized by category.

B. A group of hash values that can be added to the hash library.

C. A table of file headers and extensions.

D. Botha and b.

Correct Answer: B

QUESTION 10

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

A. It is zeroed out.

B. The first character of the directory entry is marked with a hex 00.

C. It is wiped from the directory.

D. The first character of the directory entry is marked with a hex E5.

Correct Answer: D

QUESTION 11

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 12

What information should be obtained from the BIOS during computer forensic investigations?

A. The video caching information

B. The date and time

C. The port assigned to the serial port

D. The boot sequence

Correct Answer: BD