Vendor: Guidance Software

Exam Code:GD0-110

Exam Name: Certification Exam for EnCE Outside North America

Version: Demo

QUESTION 1

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

A. True

B. False

Correct Answer: A

QUESTION 2

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 an MD5 hash value for every 32 sectors copied.

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

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

Correct Answer: A

QUESTION 3

The Windows 98 Start Menu has a selection called ocuments?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 4

If a floppy diskette is in the drive, the computer will always boot to that drive before any other device. If a floppy diskette is in the drive, the computer will always boot to that drive before any other device.

A. True

B. False

Correct Answer: B

QUESTION 5

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 6

The following GREP expression was typed in exactly as shown. Choose the answer(s) that would result. [^a-z]Tom[^a-z]

A. Tom

B. Toms

C. Tomato

D. Stomp

Correct Answer: A

QUESTION 7

When a drive letter is assigned to a logical volume, that information is temporarily written the volume boot record on the hard drive.

A. True

B. False

Correct Answer: B

QUESTION 8

Searches and bookmarks are stored in the evidence file.

A. True

B. False

Correct Answer: B

QUESTION 9

The following GREP expression was typed in exactly as shown. Choose the answer(s) that would result.
[\x00-\x05]\x00\x00\x00? andgt;?[?[@?[?[?[?[

A. 00 00 00 01 FF FF BA

B. FF 00 00 00 00 FF BA

C. 04 00 00 00 FF FF BA

D. 04 06 00 00 00 FF FF BA

Correct Answer: C

QUESTION 10

A hash library would most accurately be described as:

A. Both a and b.

B. A master table of file headers and extensions.

C. A file containing hash values from one or more selected hash sets.

D. A list of the all the MD5 hash values used to verify the evidence files.

Correct Answer: C

QUESTION 11

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. Pull the plug from the wall.

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

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

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

Correct Answer: B

QUESTION 12

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