Guidance Software GD0-110

Guidance Software GD0-110 Certification Exam for EnCE Outside North America

Practice Test

Version 1.6

QUESTION NO: 1

A FAT directory has as a logical size of:

A. One cluster
B. 0 bytes
C. 128 bytes
D. 64 bytes

Answer: B

QUESTION NO: 2

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

A. 16
B. 8
C. 32
D. Variable
E. 64

Answer: C

QUESTION NO: 3

EnCase is able to read and examine which of the following file systems?

A. HFS
B. FAT
C. NTFS
D. EXT3

Answer: A,B,C,D

QUESTION NO: 4

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

A. 0000 00 01 FF FF BA
B. FF 0000 00 00 FF BA
C. 04 0000 00 FF FF BA

D. 04 06 0000 00 FF FF BA

Answer: C

QUESTION NO: 5

By default, what color does EnCase use for the contents of a logical file?

A. Red
B. Red on black
C. Black
D. Black on red

Answer: C

QUESTION NO: 6

4 bits allows what number of possibilities?

A. 16
B. 2
C. 4
D. 8

Answer: A

QUESTION NO: 7

A hard drive has been formatted as NTFS and Windows XP was installed. The user used fdisk to remove all partitions from that drive. Nothing else was done. You have imaged the drive and have opened the evidence file with EnCase. What would be the best way to examine this hard drive?

A. EnCase will not see a drive that has been fdisked.
B. Use theecovered Deleted Partitions?feature and then examine the system. Use the ?ecovered Deleted Partitions?feature and then examine the system.
C. Conduct a physical search of the hard drive and bookmark any evidence.
D. Use thedd Partition?feature to rebuild the partition and then examine the system. Use the ?dd Partition?feature to rebuild the partition and then examine the system.

Answer: D

QUESTION NO: 8

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

A. Either the CRC or MD5 hash values must verify.
B. The CRC values must verify.
C. The CRC values and the MD5 hash value both must verify.
D. The MD5 hash value must verify.

Answer: C

QUESTION NO: 9

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

Answer: C

QUESTION NO: 10

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

Answer: C

QUESTION NO: 11

In Windows, the file MyNote.txt is deleted from C Drive and is automatically sent to the ecycle Bin.? The long filename was In Windows, the file MyNote.txt is deleted from C Drive and is automatically sent to the ?ecycle Bin.? The long filename was MyNote.txt and the short filename was MYNOTE.TXT. When viewing the ecycle Bin?with EnCase, how will the long filename and MyNote.txt and the short filename was MYNOTE.TXT. When viewing the ?ecycle Bin?with

EnCase, how will the long filename and short filename appear?

A. MyNote.txt, DC0.txt
B. MyNote.del, DC1.del
C. MyNote.txt, CD0.txt
D. MyNote.del, DC0.del

Answer: A

QUESTION NO: 12

In hexadecimal notation, one byte is represented by _____ character(s).

A. 8
B. 4
C. 2
D. 1

Answer: C

QUESTION NO: 13

Hash libraries are commonly used to:

A. Compare a file header to a file extension.
B. Compare one hash set with another hash set.
C. Identify files that are already known to the user.
D. Verify the evidence file.

Answer: C

QUESTION NO: 14

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

Answer: C

QUESTION NO: 15

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

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

Answer: D

QUESTION NO: 16

If cases are worked on a lab drive in a secure room, without any cleaning of the contents of the drive, which of the following areas would be of most concern?

A. Storage
B. There is no concern
C. Chain-of-custody
D. Cross-contamination

Answer: D

QUESTION NO: 17

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

Answer: C

QUESTION NO: 18

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.

Answer: A

QUESTION NO: 19

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

A. Renamed to JPG_0001.jpg and copied to the default export folder.
B. Copied to the default export folder and opened by an associated program.
C. Opened byEnCase.
D. Copied to theEnCase specified temp folder and opened by an associated program.

Answer: D

QUESTION NO: 20

RAM is an acronym for:

A. Random Addressable Memory
B. Relative Addressable Memory
C. Relative Address Memory
D. Random Access Memory

Answer: D

QUESTION NO: 21

The results of a hash analysis on an evidence file that has been added to a case will be stored in which of the following files?

A. The evidence file
B. The case file
C. The configuration HashAnalysis.ini file
D. All of the above

Answer: B

QUESTION NO: 22

The EnCase default export folder is:

A. A global setting that cannot be changed.
B. A case-specific setting that can be changed.
C. A global setting that can be changed.
D. A case-specific setting that cannot be changed.

Answer: B

QUESTION NO: 23

What are the EnCase configuration .ini files used for?

A. Storing information that will be available toEnCase each time it is opened, regardless of the active case(s).
B. Storing the results of a signature analysis.
C. Storing pointers to acquired evidence.
D. Storing information that is specific to a particular case.

Answer: A

QUESTION NO: 24

A CPU is:

A. A chip that would be considered the brain of a computer, which is installed on a motherboard.
B. A Central Programming Unit.
C. An entire computer box, not including the monitor and other attached peripheral devices.
D. A motherboard with all required devices connected.

Answer: A

QUESTION NO: 25

A case file can contain ____ hard drive images?

A. 1
B. 5
C. 10
D. any number of

Answer: D

QUESTION NO: 26 CORRECT TEXT

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

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 27 CORRECT TEXT

The temporary folder of a case cannot be changed once it has been set.

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 28

In Unicode, one printed character is composed of ____ bytes of data.

A. 1
B. 8
C. 4
D. 2

Answer: D

QUESTION NO: 29

The signature table data is found in which of the following files?

A. The case file
B. All of the above
C. The configuration FileSignatures.ini file
D. The evidence file

Answer: C

QUESTION NO: 30

What does the acronym BIOS stand for?

A. Basic Integrated Operating System
B. BasicInput/Output System
C. BinaryInput/Output System
D. Binary Integrated Operating System

Answer: B

QUESTION NO: 31

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

Answer: B

QUESTION NO: 32 CORRECT TEXT

A restored floppy diskette will have the same hash value as the original diskette.

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 33

This question addresses the EnCase for Windows search process. If a target word is within a logical file, and it begins in cluster 10 and ends in cluster 15 (the word is fragmented), the search:

A. Will find it becauseEnCase performs a logical search.
B. Will not find it unlessile slack?is checked on the search dialog box. Will not find it unless ?ile slack?is checked on the search dialog box.
C. Will not find it becauseEnCase performs a physical search only.
D. Will not find it because the letters of the keyword are not contiguous.