Guidance Software GD0-100

GD0-100 Certification Exam For ENCE North America

Practice Test

Version 1.0

QUESTION NO: 1

When an EnCase user double-clicks on a file within EnCase what determines the action that will result? Select all that apply

A. The settings in the case file.
B. The settings in the FileTypes.ini file.
C. The setting in the evidence file.

Answer: B

QUESTION NO: 2

Search results are found in which of the following files? Select all that apply.

A. The evidence file
B. The configuration Searches.ini file
C. The case file

Answer: C

QUESTION NO: 3

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

Answer: A

QUESTION NO: 4 CORRECT TEXT

The following GREP expression was typed in exactly as shown. Choose the

Answer: (s)
Answer: C

QUESTION NO: 5

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.

Answer: A

QUESTION NO: 6

A physical file size is

A. The total size in sectors of an allocated file.
B. The total size of all the clusters used by the file measured in bytes.
C. The total size in bytes of a logical file.
D. The total size of the file including the ram slack in bytes.

Answer: B

QUESTION NO: 7

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

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

Answer: C

QUESTION NO: 8

If cluster number 10 in the FAT contains the number 55, this means

A. That cluster 10 is used and the file continues in cluster number 55.
B. That the file starts in cluster number 55 and continues to cluster number 10.
C. That there is a cross-linked file.
D. The cluster number 55 is the end of an allocated file.

Answer: A

QUESTION NO: 9

How are the results of a signature analysis examined?

A. By sorting on the category column in the Table view. By sorting on the category column in the Table view.
B. By sorting on the signature column in the Table view. By sorting on the signature column in the Table view.
C. By sorting on the hash sets column in the Table view. By sorting on the hash sets column in the Table view.
D. By sorting on the hash library column in the Table view. By sorting on the hash library column in the Table view.

Answer: B

QUESTION NO: 10

The acronym ASCII stands for

A. American Standard Communication Information Index
B. American Standard Code for Information Interchange
C. Accepted Standard Code for Information Interchange
D. Accepted Standard Communication Information Index

Answer: B

QUESTION NO: 11 CORRECT TEXT

The default export folder remains the same for all cases.

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 12

The EnCase default export folder is

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

Answer: B

QUESTION NO: 13

Hash libraries are commonly used to

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

Answer: B

QUESTION NO: 14

Which is the proper formula for determining the size in bytes of a hard drive that uses cylinders (C), heads (H), and sectors (S) geometry?

A. C X H + S
B. C X H X S + 512
C. C X H X S X 512
D. C X H X S

Answer: C

QUESTION NO: 15

Within EnCase, clicking on Save on the toolbar affects what file(s)?

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

Answer: C

QUESTION NO: 16

EnCase uses the _____ to conduct a signature analysis.

A. Both a and b
B. file signature table
C. hash library
D. file Viewers

Answer: B

QUESTION NO: 17

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

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

Answer: A,B,C,D

QUESTION NO: 18

ROM is an acronym for

A. Read Open Memory
B. Random Open Memory
C. Read Only Memory
D. Relative Open Memory

Answer: C

QUESTION NO: 19 CORRECT TEXT

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.

Answer: False
Answer: True
Answer: Pending

QUESTION NO: 20 CORRECT TEXT

A standard Windows 98 boot disk is acceptable for booting a suspect drive.

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 21 CORRECT TEXT

Search terms are case sensitive by default.

Answer: False
Answer: True
Answer: Pending

QUESTION NO: 22 CORRECT TEXT

The following GREP expression was typed in exactly as shown. Choose the

Answer: (s)
Answer: D

QUESTION NO: 23

An evidence file can be moved to another directory without changing the file verification.

A. False
B. True

Answer: B

QUESTION NO: 24

Pressing the power button on a computer that is running could have which of the following results?

A. The computer will instantly shut off.

B. The computer will go into stand-by mode.
C. Nothing will happen.
D. All of the above could happen.
E. The operating system will shut down normally.

Answer: D

QUESTION NO: 25

How does EnCase verify that the evidence file contains an exact copy of the suspect hard drive? How does EnCase verify that the evidence file contains an exact copy of the suspect's hard drive?

A. By means of a CRC value of the suspect hard drive compared to a CRC value of the data stored in the evidence file.By means of a CRC value of the suspect? hard drive compared to a CRC value of the data stored in the evidence file.
B. By means of an MD5 hash of the suspect hard drive compared to an MD5 hash of the data stored in the evidence file.By means of an MD5 hash of the suspect? hard drive compared to an MD5 hash of the data stored in the evidence file.
C. By means of a CRC value of the evidence file itself.
D. By means of an MD5 hash value of the evidence file itself.

Answer: B

QUESTION NO: 26

By default, EnCase will display the data from the end of a logical file, to the end of the cluster, in what color

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

Answer: A

QUESTION NO: 27

A SCSI drive is pinned as a master when it is

A. The only drive on the computer.

B. The primary of two drives connected to one cable.
C. Whenever another drive is on the same cable and is pinned as a slave.
D. A SCSI drive is not pinned as a master.

Answer: D

QUESTION NO: 28 CORRECT TEXT

The following GREP expression was typed in exactly as shown. Choose the

Answer: (s)
Answer: B

QUESTION NO: 29

This QUESTION NO: 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 not find itunlessile slack is checked on the search dialog box.
B. Will find it becauseEnCase performs a logical search.
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.

Answer: B

QUESTION NO: 30

An evidence file was archived onto five CD-Rom disks with the third file segment on disk number three. Can the contents of the third file segment be verified by itself while still on the CD?

A. No. Archived files are compressed and cannot be verified until un-archived.
B. No. All file segments must be put back together.
C. Yes. Any segment of an evidence file can be verified through re-computing and comparing the CRCs, even if it is on a CD.
D. No.EnCase cannot verify files on CDs.

Answer: C

QUESTION NO: 31 CORRECT TEXT

The case file should be archived with the evidence files at the termination of a case.

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 32

A signature analysis has been run on a case. The result "Bad Signature " means

A. The file signature is known and does not match a known file header.
B. The file signature is known and the file extension is known.
C. The file signature is known and does not match a known file extension.
D. The file signature is unknown and the file extension is known.

Answer: D

QUESTION NO: 33 CORRECT TEXT

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

Answer: True
Answer: False
Answer: Pending

QUESTION NO: 34

When can an evidence file containing a NTFS partition be logically restored to a FAT 32 partition?

A. Never
B. When the FAT 32 has the same number of sectors / clusters.
C. When the FAT 32 is the same size or bigger.
D. Both a and b

Answer: A

QUESTION NO: 35