TestkingPDF

Try before you buy

Download a free sample of any of our exam questions and answers

Download Demo

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Quality and Value

TestkingPDF Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our TestkingPDF testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

TestkingPDF offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.testkingpdf.com

Valid test online & stable pass king & latest PDF dumps

Exam : GD0-100

Title : Certification Exam For ENCE North America

Vendors : Guidance Software

Version : DEMO

NO.1 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

NO.2 ROM is an acronym for:
A. Read Open Memory
B. Random Open Memory
C. Read Only Memory
D. Relative Open Memory
Answer: C

NO.3 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

NO.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. False
B. True
Answer:

NO.5 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

NO.6 In Unicode, one printed character is composed of ____ bytes of data.
A. 8

B. 4
C. 2
D. 1
Answer: C

NO.7 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

NO.8 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

NO.9 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

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

NO.11 The following GREP expression was typed in exactly as shown. Choose the answer(s)
that would result. Jan 1 st , 2?0?00
A. Jan 1st , 1900
B. Jan 1st , 2100
C. Jan 1st , 2001

D. Jan 1st , 2000
Answer: D

NO.12 The following GREP expression was typed in exactly as shown. Choose the answer(s)
that would result. Bob@[a-z]+.com
A. Bob@New zealand.com
B. Bob@My-Email.com
C. Bob@America.com
D. Bob@a-z.com
Answer: C

NO.13 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

NO.14 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

NO.15 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

NO.16 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

NO.17 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

NO.18 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

NO.19 The default export folder remains the same for all cases.
A. True
B. False
Answer:

NO.20 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