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 : GD0-110

Title : Certification Exam for EnCE Outside North America

Vendors : Guidance Software

Version : DEMO

NO.1 Which of the following is commonly used to encode e-mail attachments?
A. JPEG
B. GIF
C. EMF
D. Base64
Answer: D

NO.2 Which of the following directories contain the information that is found on a Windows 98 Desktop?
A. C:\Windows\Desktop
B. C:\Desktop
C. C:\Program files\Programs\Desktop
D. C:\Startup\Desktop\Items
Answer:A

NO.3 A hard drive was imaged using EnCase. The original drive was placed into evidence. The restore
feature was used to make a copy of the original hard drive. EnCase verifies the restored copy using:
A. An MD5 hash
B. A 32 bit CRC
C. A running log
D. Nothing. Restored volumes are not verified.
Answer:A

NO.4 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. Programs that are associated with EnCase to open specific file types.
C. Any program that is loaded on the lab hard drive.
D. Any program that will work with EnCase.
Answer: B

NO.5 Within EnCase, clicking on ave?on the toolbar affects what file(s)? Within EnCase, clicking on ?ave?on
the toolbar affects what file(s)?
A. The open case file

B. The configuration .ini files
C. The evidence files
D. All of the above
Answer:A

NO.6 How many partitions can be found in the boot partition table found at the beginning of the drive?
A. 2
B. 4
C. 6
D. 8
Answer: B

NO.7 Which of the following would most likely be an add-in card?
A. A motherboard
B. The board that connects to the power supply
C. A video card that is connected to the motherboard in the AGP slot
D. Anything plugged into socket 7
Answer: C

NO.8 A hard drive has 8 sectors per cluster. File Mystuff.doc has a logical file size of 13,000 bytes. How
many clusters will be used by Mystuff.doc?
A. 1
B. 2
C. 3
D. 4
Answer: D

NO.9 You are assigned to assist with the search and seizure of several computers. The magistrate ordered
that the computers cannot be seized unless they are found to contain any one of ten previously identified
images. You currently have the ten images in JPG format. Using the EnCase methodology, how would
you best handle this situation?
A. Use an EnCase DOS boot disk to conduct a text search for hild porn? Use an EnCase DOS boot disk

to conduct a text search for ?hild porn?
B. Use FastBloc or a network/parallel port cable to acquire forensic images of the hard drives, then search
the evidence files for the previously identified images.
C. Use FastBloc or a network/parallel port cable to preview the hard drives. Go to the Gallery view and
search for the previously identified images.
D. Use FastBloc or a network/parallel port cable to preview the hard drives. Conduct a hash analysis of
the files on the hard drives, using a hash library containing the hash values of the previously identified
images.
Answer: D

NO.10 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 1 st , 1900
B. Jan 1 st , 2000
C. Jan 1 st , 2001
D. Jan 1 st , 2100
Answer: B

NO.11 The following keyword was typed in exactly as shown. Choose the answer(s) that would be found. All
search criteria have default settings. Tom
A. Tomorrow
B. Tom
C. Stomp
D. TomJ@hotmail.com
Answer: ABCD

NO.12 The FAT in the File Allocation Table file system keeps track of:
A. File fragmentation
B. Every addressable cluster on the partition
C. Clusters marked as bad
D. All of the above.
Answer: D

NO.13 A sector on a hard drive contains how many bytes?
A. 512
B. 1024
C. 2048
D. 4096
Answer:A

NO.14 A file extension and signature can be manually added by:
A. Using the new set feature under hash sets.
B. Using the new file signature feature under file signatures.
C. Using the new library feature under hash libraries.
D. Right-clicking on a file and selecting dd.? 5LJKWFOLFNLQJRQDILOHDQGVHOHFWLQJ ? GG
Answer: B

NO.15 When a document is printed using EMF in Windows, what file(s) are generated in the spooling
process?
A. The .SPL file
B. The .SHD file
C. Both a and b
D. Neither a or b
Answer: C

NO.16 The end of a logical file to the end of the cluster that the file ends in is called:
A. Unallocated space
B. Allocated space
C. Available space
D. Slack
Answer: D

NO.17 The EnCase default export folder is:
A. A global setting that can be changed.
B. A case-specific setting that can be changed.
C. A global setting that cannot be changed.
D. A case-specific setting that cannot be changed.
Answer: B

NO.18 When can an evidence file containing a NTFS partition be logically restored to a FAT 32 partition?
A. When the FAT 32 is the same size or bigger.
B. When the FAT 32 has the same number of sectors / clusters.
C. Never
D. Both a and b
Answer: C

NO.19 In DOS and Windows, how many bytes are in one FAT directory entry?
A. 8
B. 16
C. 32
D. 64
E. Variable
Answer: C

NO.20 The EnCase methodology dictates that _____ be created prior to acquiring evidence.
A. an .E01 file on the lab drive
B. a unique directory on the lab drive for case management
C. a text file for notes
D. All of the above
Answer: B