Certification Exam for EnCE Outside North America

1. A FAT directory has as a logical size of:

A. One cluster

B. 0 bytes

C. 128 bytes

D. 64 bytes

Answer(s): B

---

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(s): C

---

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

☐ A. HFS

- [ ] B. FAT
- [ ] C. NTFS
- [ ] D. EXT3

Answer(s): A B C D

---

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

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

Answer(s): C

---

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(s): C

---

6. 4 bits allows what number of possibilities?

A. 16

B. 2

C. 4

D. 8

Answer(s): A

---

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 the ecovered 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 the dd 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(s): D

---

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(s): C

---

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(s): C

---

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(s): C

---

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(s): A

---

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

A. 8

B. 4

C. 2

D. 1

Answer(s): C

---

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(s): C

---

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(s): C

---

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(s): D

---

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(s): D

---

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(s): C

---

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. Both a 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(s): A

---

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 by EnCase.

D. Copied to the EnCase specified temp folder and opened by an associated program.

Answer(s): D

---

20. RAM is an acronym for:

A. Random Addressable Memory

B. Relative Addressable Memory

C. Relative Address Memory

D. Random Access Memory

Answer(s): D
