Certification Exam For ENCE North America

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(s): B

---

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(s): C

---

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(s): A

---

4. 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(s): C

---

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(s): A

---

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(s): B

---

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

A. 8

B. 4

C. 2

D. 1

Answer(s): C

---

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(s): A

---

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(s): B

---

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(s): B

---

11. The default export folder remains the same for all cases.

A. True

B. False

C. Answer not available.

Answer(s): C

---

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(s): B

---

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(s): B

---

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(s): C

---

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(s): C

---

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(s): B

---

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

☐ A. NTFS

☐ B. EXT3

☐ C. FAT

☐ D. HFS

Answer(s): A B C D

---

18. ROM is an acronym for:

A. Read Open Memory

B. Random Open Memory

C. Read Only Memory

D. Relative Open Memory

Answer(s): C

---

19. 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

C. Answer not available.

Answer(s): C

---

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

A. True

B. False

C. Answer not available.

Answer(s): C
