

Exam : **Guidance Software GD0-100**

Title : **Certification Exam For
ENCE North America**

Version : **Demo**

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

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

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

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: 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: 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: B

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

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

Answer: 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: 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: 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: B