

CFATC COMPUTER FORENSICS CLASS PRE-ASSESSMENT TEST

Please circle "True" or "False" and explain:

1.) If the computer is found on and the date and time are checked, it is not important to check the date and time in the BIOS.

TRUE FALSE WHY: _____

2.) The BIOS is accessed by use of a special boot floppy, CD or USB drive.

TRUE FALSE WHY: _____

3.) To wake a computer that has a screensaver running it is best to use an "Arrow" key on the keyboard.

TRUE FALSE WHY: _____

4.) The data that is stored in the RAM of a computer does not contain information that is useful to an examiner.

TRUE FALSE WHY: _____

5.) When the computer is turned off the information found in RAM will remain.

TRUE FALSE WHY: _____

6.) Storing a hard drive wrapped in plastic bubble wrap and sealed in a plastic bag is recommended.

TRUE FALSE WHY: _____

7.) In a Windows GUI, the "cmd" command will allow you to access a command-line.

TRUE FALSE WHY: _____

8.) In Windows XP, USB devices can be set as "Read-Only".

TRUE FALSE WHY: _____

9.) Using forensic software in a Windows GUI will always protect the device being imaged from inadvertent changes.

TRUE FALSE WHY: _____

10.) It is recommended to only use one automated forensic tool for continuity in court.

TRUE FALSE WHY: _____

11.) If the National Institute of Standards and Technology has validated a tool it should also be validated by the examiner.

TRUE FALSE WHY: _____

12.) It is important to use hash values to verify the integrity of a forensic image.

TRUE FALSE WHY: _____

13.) If a file is sent to the trash and the trash is emptied within a Windows GUI the file can not be recovered.

TRUE FALSE WHY: _____

14.) Searching for file signatures is a common way to recover deleted files.

TRUE FALSE WHY: _____

15.) If a subject runs an evidence-eliminating program on a computer no evidence can will be found.

TRUE FALSE WHY: _____

16.) The Windows registry is an excellent area to examine to find evidence.
TRUE FALSE WHY: _____

17.) If encryption is found running in a computer that is turned on it is ok to remove power and seize the computer.
TRUE FALSE WHY: _____

18.) The "index.dat" file contains the registry settings.
TRUE FALSE WHY: _____

19.) It is possible to recover Internet History that was deleted over a year ago.
TRUE FALSE WHY: _____

20.) If a file has the extension ".jpg" it will always be a picture file.
TRUE FALSE WHY: _____

Student Name: _____

PRINT

DATE: _____

FOR CFATC OFFICE USE ONLY

DATE RECEIVED BY CFATC: _____ BY: _____

SCORE: _____ OUT OF _____