Review: Quiz 02 - Data Recovery and Data Carving (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

1. To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software? *

- ○ Computer Forensics Tools and Validation Committee (CFTVC)
- ○ Association of Computer Forensics Software Manufactures (ACFSM)
- ◉ National Institute of Standards and Technology (NIST) ✓
- ○ Society for Valid Forensics Tools and Testing (SVFTT)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

2. Alice has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Alice secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events? *

- ○ Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
- ◉ Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence ✓
- ○ Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
- ○ Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

3. You are assigned to work in the computer forensics lab of a state police agency. While working on a high-profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab? *

- (●) Make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab ✓
- ( ) Make an MD5 hash of the evidence and compare it to the standard database developed by NIST
- ( ) There is no reason to worry about this possible claim because state labs are certified
- ( ) Sign a statement attesting that the evidence is the same as it was when it entered the lab

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

4. When examining a file with a **Hex Editor**, what space does the file header occupy? *

- ( ) The last several bytes of the file
- (●) The first several bytes of the file ✓
- ( ) None, file headers are contained in the FAT
- ( ) One byte at the beginning of the file

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

5. When you carve an image, recovering the image depends on which of the following skills? *

- (●) Recognizing the pattern of the header content ✓
- ( ) Recovering the image from a tape backup
- ( ) Recognizing the pattern of a corrupt file
- ( ) All the choices are incorrect

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

6. When searching through **file headers** for picture file formats, what should be searched to find a JPEG file in hexadecimal format? *

- (●) FF D8 FF E0 00 10 ✓
- ( ) FF FF FF FF FF FF
- ( ) FF 00 FF 00 FF 00
- ( ) EF 00 EF 00 EF 00

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

7. One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension? *

- ( ) the File Allocation Table
- (●) the file header ✓
- ( ) the file footer
- ( ) the sector map

✗ **Incorrect** 0/0.5 Points

0 / 0.5 pts
Auto-graded

8. You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to the sensitivity of the case. How would you permanently erase the data on the hard disk? *

- (●) Throw the hard disk into the fire
- ( ) Run the powerful magnets over the hard disk
- ( ) Format the hard disk multiple times using a low-level disk utility
- ( ) Overwrite the contents of the hard disk with Junk data ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

9. A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file? *

- ○ Raster image
- ◉ Vector image ✓
- ○ Metafile image
- ○ Catalog image

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

10. A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? *

- ◉ Image the disk and try to recover deleted files ✓
- ○ Seek the help of co-workers who are eyewitnesses
- ○ Check the Windows registry for connection data (you may or may not recover)
- ○ Approach the websites for evidence

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

11. In General, Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data. *

- ○ Network Forensics
- ○ Data Recovery
- ○ Disaster Recovery
- ◉ Computer Forensics ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

12. While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte **5h**. What does this indicate on the computer? *

- ○ The files have been marked as hidden
- ◉ Te files have been marked for deletion ✓
- ○ The files are corrupt and cannot be recovered
- ○ The files have been marked as read-only

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

13. Alice has encountered a system crash and has lost vital data stored on the hard drive of his windows computer. He has no cloud storage or backup hard drives. He wants to recover all that data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Alice's purpose? *

- ○ Colasoft's Capsa
- ◉ Recuva ✓
- ○ Cain & Abel
- ○ Xplico

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

14. In Windows XP, when a user deletes a file or folder, the system stores the complete path including the original filename is a special hidden file called "**INFO2**" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you ___? *

- ○ Undo the last action performed on the system
- ○ Reboot Windows
- ◉ Use a recovery tool to undelete the file ✓
- ○ Download the file from Microsoft website

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

15. Alice is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files? *

- (●) ff d8 ff ✓
- ( ) 25 50 44 46
- ( ) d0 0f 11 e0
- ( ) 50 41 03 04

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

16. The offset in a hexadecimal code is ____ *

- ( ) the last byte after the colon
- (●) the 0x at the beginning of the code ✓
- ( ) the 0x at the end of the code
- ( ) the first byte after the colon

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

17. What does the **-s** parameter in the **xxd** command do? *

- ( ) Print a summary of available commands and exit
- ( ) Skip printing after writing len octets
- (●) Skip the lines that the user specifies while printing the hexdump of the file ✓
- ( ) Show version string

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

18. You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a simple backup copy of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a simple backup copy will not provide deleted files or recover file fragments.
What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings? *

- (●) Bit-stream Copy ✓
- ( ) Robust Copy
- ( ) Full back up Copy
- ( ) Incremental Backup Copy

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

19. The following tools allow you to recover deleted files on Linux. (Choose all that apply) *

- [ ] WinHex
- [x] Foremost ✓
- [ ] Recuva
- [x] PhotoRec ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

20. On a Linux operating system, which of the following commands can be used to modify the image creation time value in the header section from **2020** to **2024**? *

- ( ) echo "<address>: 3230 3330" | xxd -r - <filename.jpg>
- (●) echo "<address>: 3230 3234" | xxd -r - <filename.jpg> ✓
- ( ) echo "<address>: 3234 3234" | xxd -r - <filename.jpg>
- ( ) echo "<address>: 3230 3230" | xxd -r - <filename.jpg>