Review: Quiz 01 - Data Acquisition (Digital Forensics 152361)

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

1. What will the following Linux command accomplish? **dd if=/dev/mem of=/home/bkcs/mem.bin bs=1024** *

○ Copy the master boot record to a file

○ Copy the contents of the system folder to a file

● Copy the running memory to a file ✓

○ Copy the memory dump file to an image file

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

2. Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish? **dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync** *

● Fill the disk with zeros ✓

○ Low-level format

○ Fill the disk with 4096 zeros

○ Copy files from the master disk to the slave disk on the secondary IDE controller

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

3. Using Linux to carry out a forensics investigation, what would the following command accomplish? **dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror** *

○ Backup a disk to an image file

○ Search for disk errors within an image file

○ Copy a partition to an image file

● Restore a disk from an image file ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

4. What will the following command accomplish? **dcfldd if=/dev/sdb vf=sdb_image.img** *

● Validate the image file with the source ✓

○ Copy a partition to an image file

○ Restore a partition from an image file

○ Copy an image file to a partition

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

5. What will the following command accomplish? **dd if=/dev/xxx of=mbr.backup bs=512 count=1** *

○ Restore the first 512 bytes of the first partition of the hard drive

○ Restore the first 512 bytes of the first partition of the hard drive

○ Restore the master boot record

● Back up the master boot record ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

6. The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block? *

○ 512 bits

● 512 bytes ✓

○ 256 bits

○ 256 bytes

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

7. Alice has acquired data from a hard disk in an open-source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use? *

○ Portable Document Format

○ Raw Format

● Advanced Forensics Format (AFF) ✓

○ Proprietary Format

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

8. Which of the following tools creates a bit-by-bit image of an evidence media? (Choose all that apply) *

□ Recuva

□ FileMerlin

☑ AccessDataFTKImager ✓

☑ TheSleuthKit ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

9. What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images? (Choose all that apply) *

□ mcopy

☑ dcfldd ✓

□ MD5

☑ dd ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

10. You are contracted to work as a computer forensics investigator for a regional bank that has four **30 TB** storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network? *

○ create a compressed copy of the file with DoubleSpace

○ create a sparse data copy of a folder or file

● make a bit-stream disk-to-image file ✓

○ make a bit-stream disk-to-disk file

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

11. Alice needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation? *

○ Static Acquisition

● Sparse or Logical Acquisition ✓

○ Bit-stream disk-to-disk Acquisition

○ Bit-by-bit Acquisition

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

12. Which of the following tools is not a data acquisition hardware tool? *

○ UltraKit

○ Atola Insight Forensic

● F-Response Imager ✓

○ Triage-Responder

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

13. The SHA1 program is used to? *

○ wipe magnetic media before recycling it

○ make directories on an evidence disk

○ view graphics files on an evidence drive

● verify that a disk is not altered when you examine it ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

14. In which implementation of **RAID** will the image of a Hardware RAID volume be different from the image taken separately from the disks? *

○ RAID 0

○ RAID 1

● It will always be different ✓

○ The images will always be identical because data is mirrored for redundancy

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

15. When should an SHA1 hash check be performed when processing evidence? *

○ After the evidence examination has been completed

○ On an hourly basis during the evidence examination

● Before and after evidence examination ✓

○ Before the evidence examination has been completed

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

16. Raw data acquisition format creates ________ of a data set or suspect drive. *

○ Segmented image files

● Simple sequential flat files ✓

○ Compressed image files

○ Segmented files

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

17. When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to? *

○ Automate Collection from image files

○ Avoiding copying data from the boot partition

○ Acquire data from host-protected area on a disk

● Prevent Contamination to the evidence drive ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

18. How many **bytes** is the fixed-length MD5 algorithm checksum of a critical system file? *

○ 128

○ 64

○ 32

● 16 ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

19. Which of the following tools enables data acquisition and duplication? (Choose all that apply) *

□ Colasoft's Capsa

☑ DriveSpy ✓

□ Wireshark

☑ FTK Imager ✓

✓ **Correct** 1/1 Points

1 / 1 pt
Auto-graded

20. Alice, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Alice takes pictures and tags all computer and peripheral equipment found in the house. Alice packs all the items found in his van and takes them back to his lab for further examination. At his lab, Bob, his assistant, helps him with the investigation. Since Bob is still in training, Alice supervises all of his work very carefully. Bob is not quite sure about the procedures to copy all the data off the computer and peripheral devices. **What is the minimum number of data acquisition tools** should Bob use when creating copies of the evidence for the investigation? *

● Two ✓

○ One

○ Three

○ Four