25: Lab 25 - APPLIED - Performing digital forensics

Security+ (Exam SY0-701)

Congratulations, you passed!

Duration: 1 hour, 35 minutes

confirm the presence of /root/Downloads/1-extend-part/ext-part-test-2.dd *Score: 1*

Select the **Score** button to validate this task:

```
File /root/Downloads/1-extend-part/ext-part-test-2.dd exists
Task complete
```

How many formattable partitions are displayed by fdisk for this drive image? *Score: 1*

- 1
- 3
- 5
- 6

Congratulations, you have answered the question correctly.

What are possible explanations of the unaccounted for sectors from the extended partition? (Select two) *Score: 1*

- [x] Unused space not allocated to a logical drive
- [ ] Bad sectors on the original storage device
- [x] A hidden logical drive
- [ ] The image is not in raw format

Congratulations, you have answered the question correctly.

confirm the presence of /root/Downloads/7-undel-ntfs/7-ntfs-undel.dd *Score: 1*

Select the **Score** button to validate this task:

```
File /root/Downloads/7-undel-ntfs/7-ntfs-undel.dd exists
Task complete
```

What are the names of the recovered files that are in sub-directories? *Score: 1*

- [ ] frag1.dat
- [x] frag3.dat
- [x] mult2.dat
- [ ] sing1.dat

Congratulations, you have answered the question correctly.

confirm the presence of /root/Downloads/11-carve-fat/11-carve-fat.dd *Score: 1*

Select the **Score** button to validate this task:

```
File /root/Downloads/11-carve-fat/11-carve-fat.dd exists
Task complete
```

Which recovered image file includes cats? *Score: 1*

- haxor2.jpg
- paul.jpg
- pumpkin.jpg
- shark.jpg

Congratulations, you have answered the question correctly.

What is the maximum number of primary partitions that can be defined on an MBR drive if logical drives are in use? *Score: 1*

- 1
- 2
- 3
- 4

Congratulations, you have answered the question correctly.

Which of the following are tools from The Sleuth Kit (TSK)? (select all that apply) *Score: 1*

- tsk_recover
- fsstat
- fls
- istat
- mmls

Congratulations, you have answered the question correctly.

What is the forensic process of recovering access to files that are otherwise inaccessible due to corruption, partial data loss (especially headers), deletion, or partition structure damage? *Score: 1*

- Data exfiltration
- File carving
- Acquisition
- Evidence seizure

Congratulations, you have answered the question correctly.

What is an IoC that reveals the presence of a hidden partition? *Score: 1*

- Unused space in an extended partition
- Corrupted MBR
- Use of a GPT header
- Only having 4 primary partitions

Congratulations, you have answered the question correctly.

What is a file system metadata structure that is used to store and organize file object information, such as file size, owner user, group IDs, permissions, and timestamps? *Score: 1*

- partition
- sector
- inode
- MBR

Congratulations, you have answered the question correctly.