18: APPLIED LAB: Collecting Forensic Evidence

CySA+ (Exam CS0-003)

Congratulations, you passed!

Duration: 1 hour, 24 minutes

☑ **confirm the presence of /root/Downloads/8-jpeg-search/8-jpeg-search.dd** *Score: 1*

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

```
File /root/Downloads/8-jpeg-search/8-jpeg-search.dd exists
Task complete
```

☑ **confirm the presence of /root/Downloads/file1.jpg** *Score: 1*

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

```
File /root/Downloads/file1.jpg exists
Task complete
```

☒ **confirm the presence of /root/Downloads/file2.jpg** *Score: 0*

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

```
File /root/Downloads/file2.jpg does not exist
Task incomplete
```

☑ **confirm the presence of /root/Downloads/file6.jpg** *Score: 1*

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

```
File /root/Downloads/file6.jpg exists
Task complete
```

☑ **confirm the presence of /root/Downloads/file7.jpg** *Score: 1*

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

```
File /root/Downloads/file7.jpg exists
Task complete
```

☒ **confirm the presence of /root/Downloads/file8.jpg** *Score: 0*

Select the **Score** button to validate this task:
```
File /root/Downloads/file8.jpg does not exist
Task incomplete
```

☑ What is the HEX value that will be present in the header of a JPG graphics file? *Score: 1*

- ○ JFIF
- ◉ FFD8 FFE0
- ○ JPEG
- ○ DEAD B0B5

Congratulations, you have answered the question correctly.

☑ What methods of file recovery can be performed through Autopsy? *Score: 1*

- ☑ Recovering deleted files
- ☑ Discovering files with incorrect extensions
- ☑ Finding files within ZIP archives
- ☐ Restoring data that has been overwritten after being deleted

Congratulations, you have answered the question correctly.

☑ When performing forensic analysis on acquired evidence, what is the most important principle? *Score: 1*

- ○ Save often.
- ○ Use online research tools.
- ○ Export every file.
- ◉ Never modify the original.

Congratulations, you have answered the question correctly.

☑ What is the purpose of viewing evidence files in ASCII or HEX? *Score: 1*

- ○ To confirm the time stamp.
- ○ To determine the base language.
- ◉ To notice words or codes of relevance.
- ○ To find proof of origin or source.

Congratulations, you have answered the question correctly.

☑ What is the typical object imported into Autopsy to be forensically analyzed? *Score: 1*

- Pictures of physical evidence.
- Source drive image file.
- Hash values of files.
- Descriptions of suspicious activities.

Congratulations, you have answered the question correctly.