**Lab 1.1 Review Questions**

1. **Why is osf an important forensics tool?**

It can be used to help digital forensics investigators locate potential evidence.

1. **OSForensics can search for which of the following types?**

Email, Graphics, Deleted files, registry files

1. **What’s a file hash?**

A hexadecimal value obtained mathematically from a file.

1. **Which of the following statements is true?**

File hashes can verify that the chain of custody has been maintained.

1. **OSForensics uses hash sets for what purpose?**

Hash sets are used to identify known file hashes used by OSs and applications.

**Lab 1.2 Review Questions**

1. **FTK Imager can be used to search all the following except what?**

Encrypted files

1. **FTK Imager is used primarily to produce which of the following?**

Hard disk image that can be analyzed by forensics software.

1. **Why do forensics investigators work with bit-stream images?**

An image file can be examined without damaging the original evidence.

1. **FTK Imager can detect and view encrypted files.**

False

1. **Bit-stream imaging is the process of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

Duplicating data on storage devices for forensic analysis.

**Lab 1.3 Review Questions**

1. **ProDiscover can be used to search all the following file systems except?**

HFS+

1. **The Exif format contains information on which of the following? (Choose all that apply.)**

The shutter speed,Data and time a photo was taken,The camera model.

1. **ProDiscover can search digital devices for which of the following? (Choose all that apply.)**

RAID data, Linux files,UNIX files

1. **ProDiscover isn't capable of producing file hash values.**

False

1. **Which of the following statements is correct?**

ProDiscover can't decrypt any encrypted files.

**Lab 1.4 Review Questions**

1. **The Windows Registry is responsible for which of the following?**

Booting into the Windows environment

1. **The Registry contains valuable forensics information, such as which of the following? (Choose all that apply.)**

Account usernames and hashed passwords, When files were created and deleted

1. **Registry Viewer can recover forensics information, such as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, that can't be viewed in Windows Registry Editor.**

A history of Web sites visited.

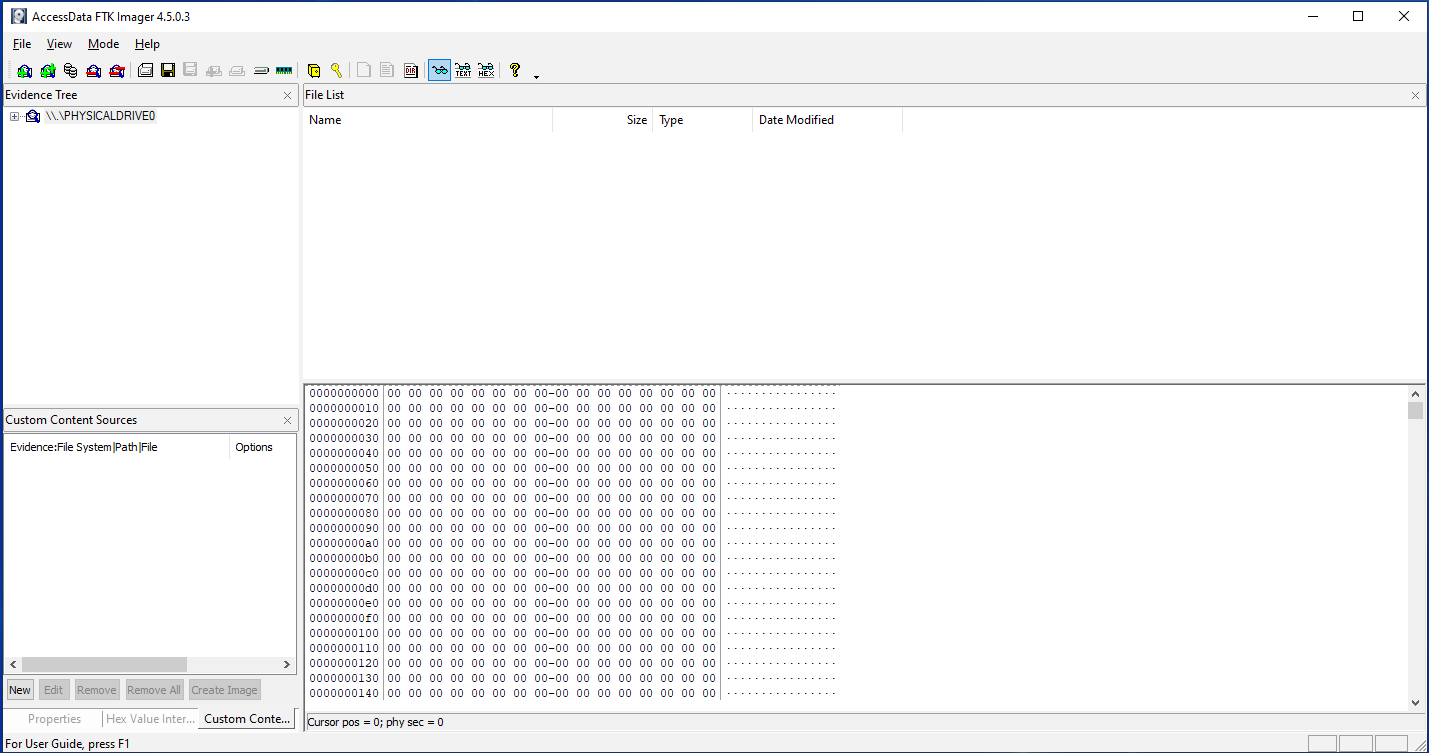
1. **Which of the following statements is true?**

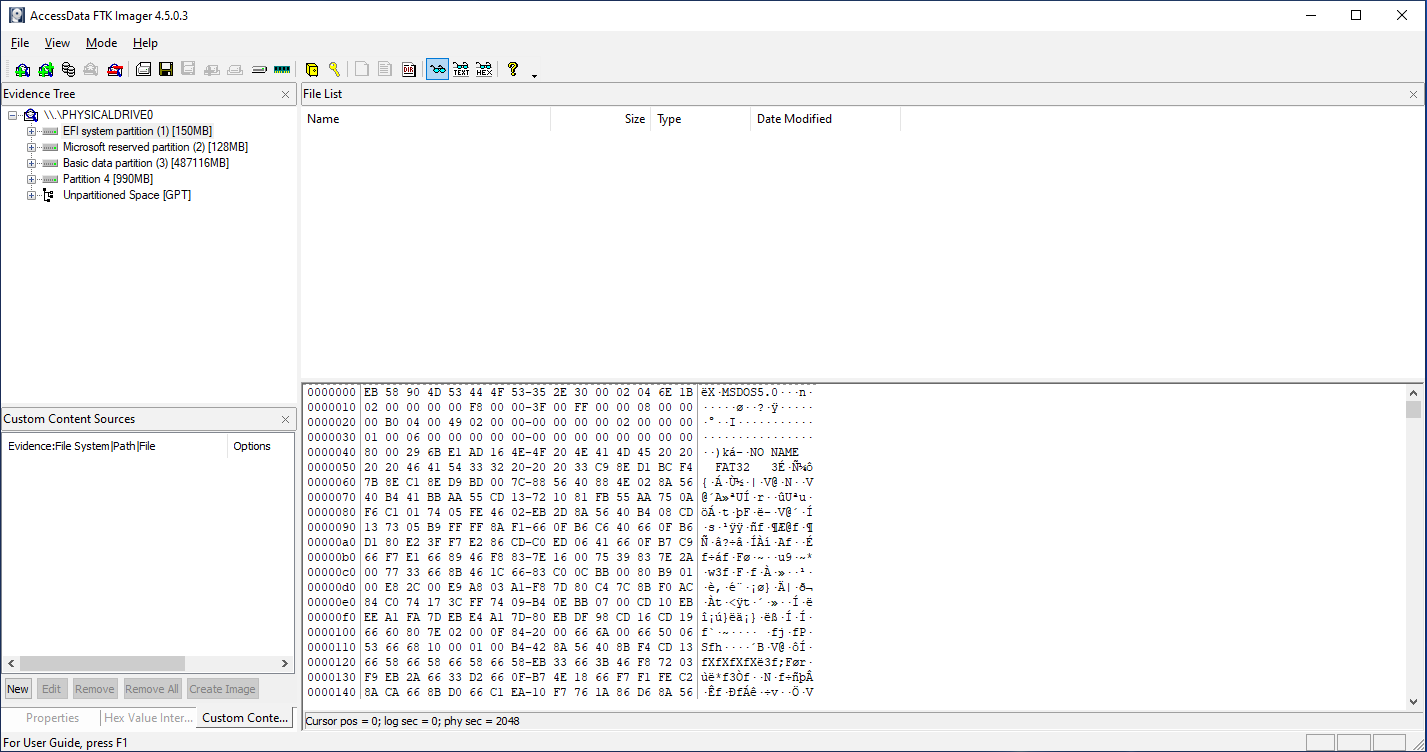
The Registry contains information on the Windows environment.

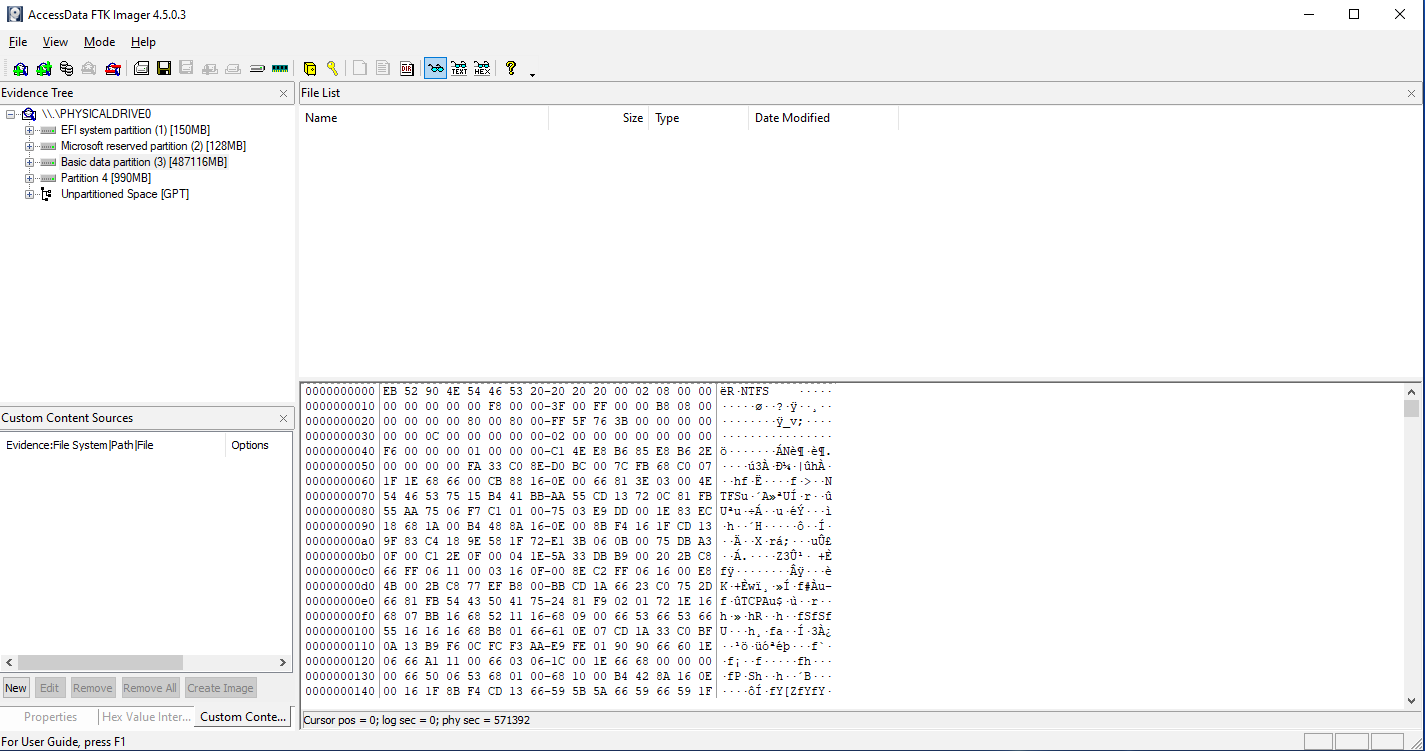
1. **The Registry is composed of \_\_\_\_\_\_\_\_\_\_\_ hives containing system data.**

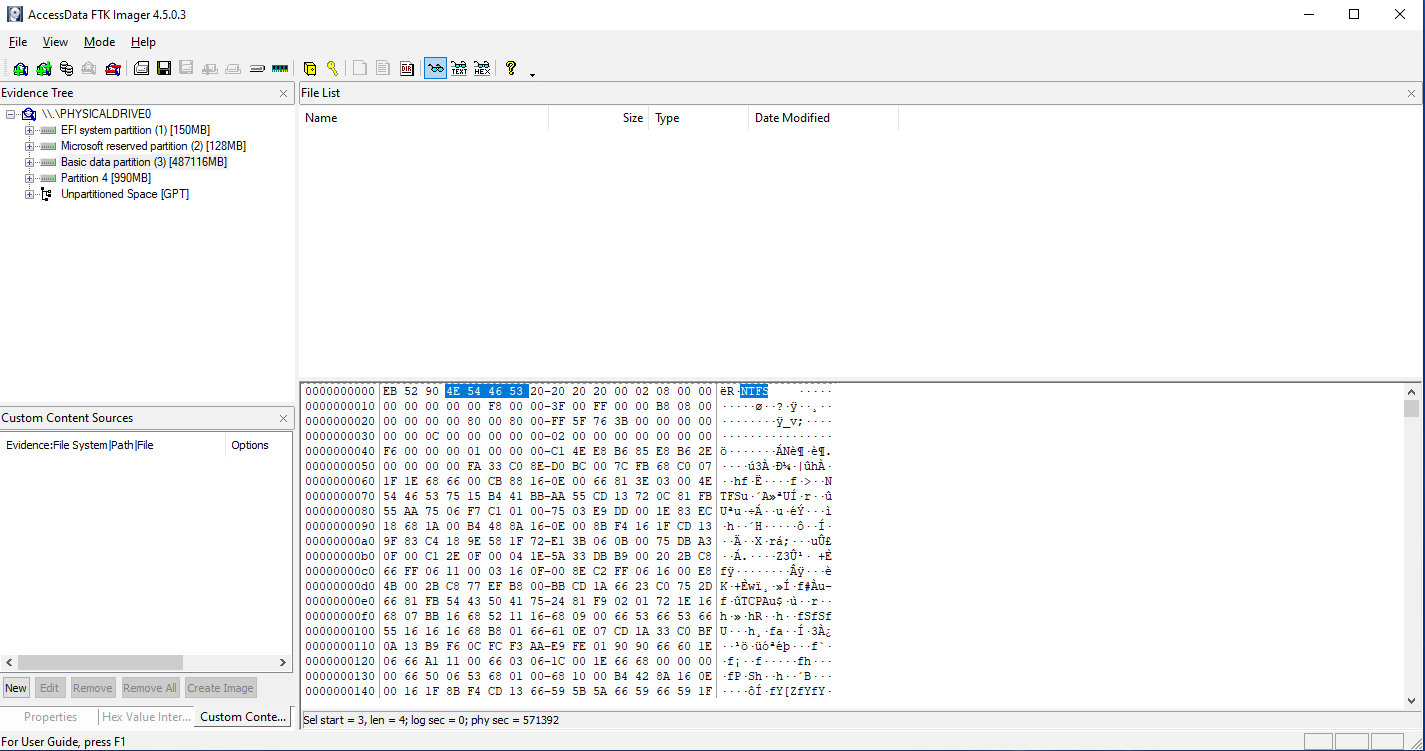
Five

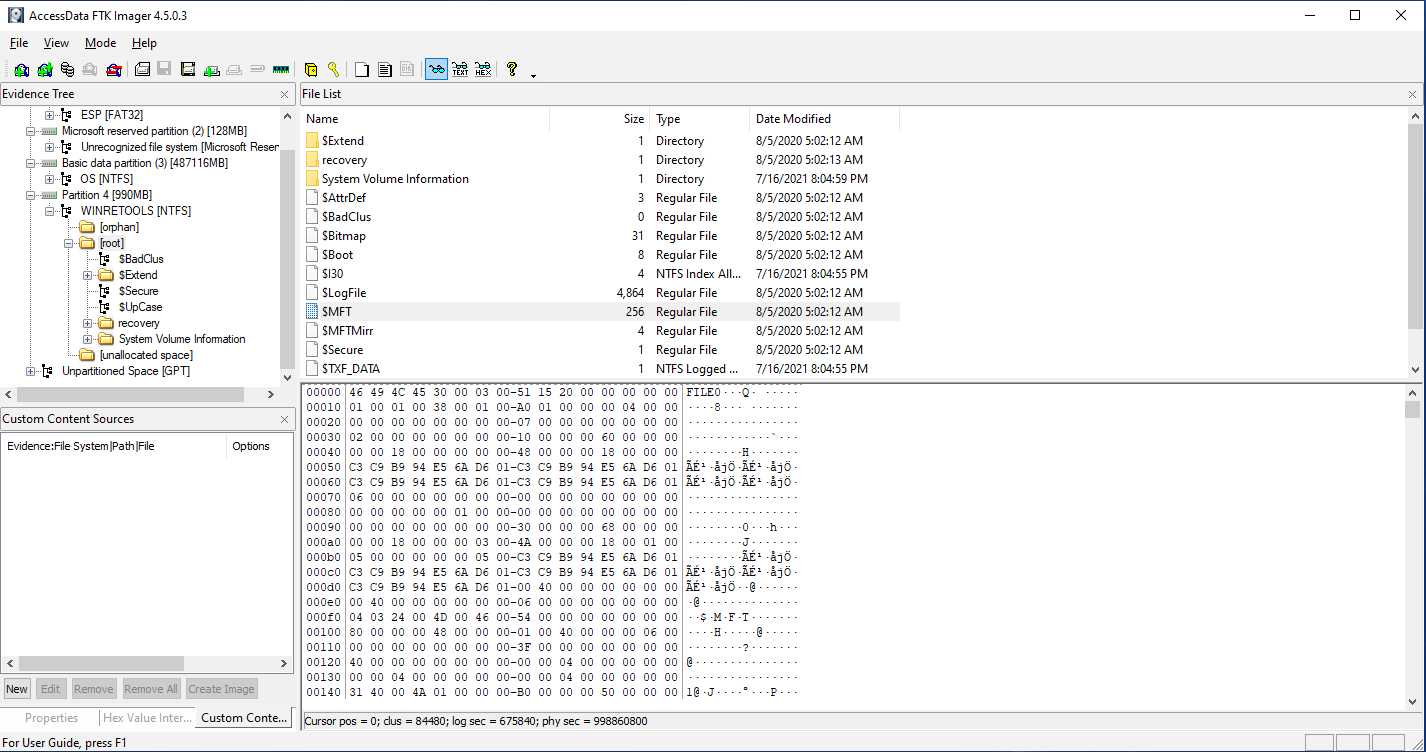
**PART 2**

****

****

****

****

****