Outline- Data Recovery from Windows Computers

Name

Tutor

Institution

Course

Date

**Part I- Essay questions**

**1. Is it necessary for forensic examiners to understand how data is stored by various types of file systems?**

A digital examiner may want to use several files system, which essentially entails the organizational structure of electronic data stored on computer media like thumb drives, floppy, optical, and hard disk. A digital forensic examiner has to be aware of the different file system features essential in data recovery.

**2. When examining evidence media, is it necessary to use the same operating system used on the original?**

In examining evidence media, the digital examiner may want to use a different operating system to understand how the system functioned and was configured. For example, when an investigator is working on a computer intrusion case, it is desirable to use a clone of a compromised system to examine the rootkit.

**3. Is the date-time stamp of various file system objects significant in the analysis of evidentiary media?**

Accurate time is essential in dealing with the computer. During investigations, data-time stamps play a significant role in pointing the time and sequence of events on the computer. Data- timestamps may aid the investigator in visually representing temporal information that helps in recognizing patterns.

**Part II- Scenario**

Understanding how files are stored and erased is an essential piece of digital evidence. During the investigation, evidence is often obtained in the file system. However, other data areas exist where we derive proof, e.g., slack space and unallocated space.