Which of the following is not a step in the digital forensics investigative process?

- Detect

Out of the items listed, what is the most volatile from an evidence collection perspective?

- Process tables

What is the name of the security principle that "holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence."

- Locard’s Exchange Principle

What are the total number of sectors contained within the hard drive shown below?

- 976,773,168

Which RFC specifies the best practices for digital evidence collection and storage?

- RFC 3227

A forensic investigator determines that malicious code has been found on a system. Using the NIST incident reporting method, what category should this attack be reported under?

- CAT 3

Why are disk images and files hashed during a forensics investigation?

- To ensure that no modification of the data occurs during analysis or during transport

What is the maximum partition size for each of the following file systems?
FAT16 → 2 GiB
FAT32 → 8 TiB
NTFS → 256 TiB
FAT12 → 16 MiB

Which Solid State Drive interface is shown below?

- Serial Advanced Technology Attachment

What are the steps used during the digital forensics investigate process?

- Identify - Preserve - Collect - Examine - Analyze - Present

What are the layers of the file system abstraction model discussed in class?

- Disk, Partition, File System, Data Unit, Metadata, File Name

Which of the following is not a capability of the NTFS file system?
- File scripting

Your team has been provided with a wide variety of removal media to analyze and part of the analysis process is to determine where each device was produced. Where was the following CD manufactured?
- Olyphant, USA

Explain the importance of chain of custody during a forensics investigation.
- To ensure proper control of electronic evidence to ensure data integrity

Based on the File Allocation Table shown below, how many files are stored on the partition?
- 3