Objectives:

- Use FTK Imager to navigate a complete XP forensic image.
- Locate and extract "Secret Files" without an extension.
- Use HxD to identify and assign the correct extension for each file.
- Determine if any incriminating evidence exists in these files.

1. Open FTK Imager and use the "Add Evidence Item" option to add the suspect "Vader_Home_Computer.001".
2. Navigate to the folder C:\Documents and Settings\Owner\My Documents\Business\Secret Files.
3. Extract the "Secret Files" folder to your local hard drive.
4. Open HxD and use it to open each secret file in Hex View.
5. Examine the initial bytes at the start of each file to identify the files' signatures. Use the PDF file from Wikipedia as a reference.
6. Record the following for each file.

Filename: file1
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file2
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file3
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file4
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file5
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file6
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file7
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file8
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

Filename: file8
The first four bytes: ___ ___ ___ ___
File type/extension: ____
Rename the file with the correct extension and open it. Describe it._____

7. Did you recover any information that may be useful to this investigation?