**Lab 05 Report: Analyzing Images to Identify Suspicious or Modified Files (E3)**

**Course Information**

● **Course Name and Number**:

● **Student Name**: Jennifer

● **Instructor Name**:

● **Lab Due Date**:

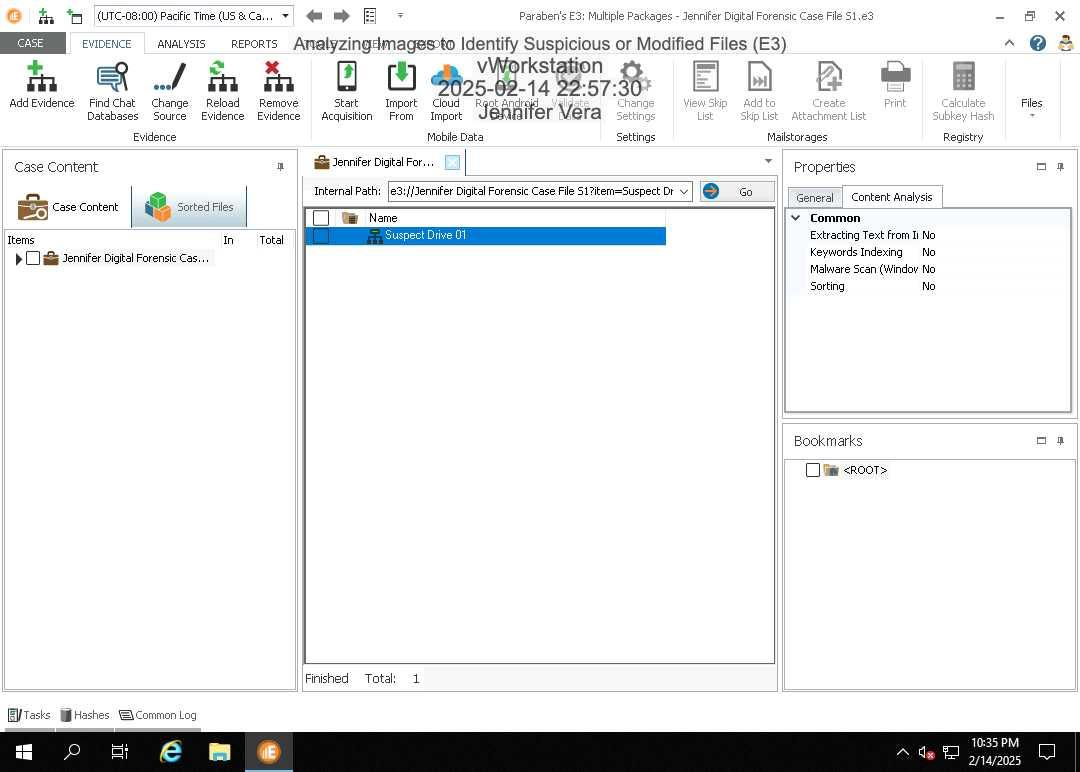
**Introduction**

1. Why might it be important to confiscate and identify the websites and kinds of images found on a suspect’s computer?

*Confiscating and identifying websites and images helps aid the investigation.*

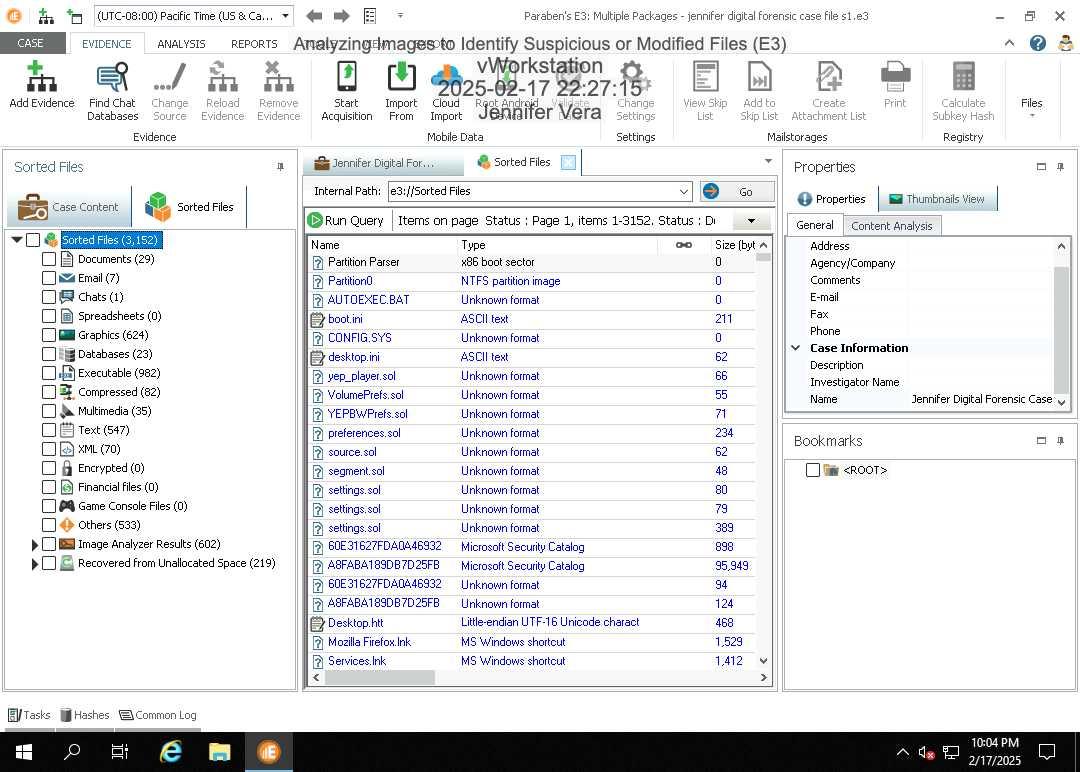
**Section 1: Hands-On Demonstration**

**Part 1: Create a New Case File**

1. Provide a screen capture showing the Suspect Drive 01 evidence loaded in E3.

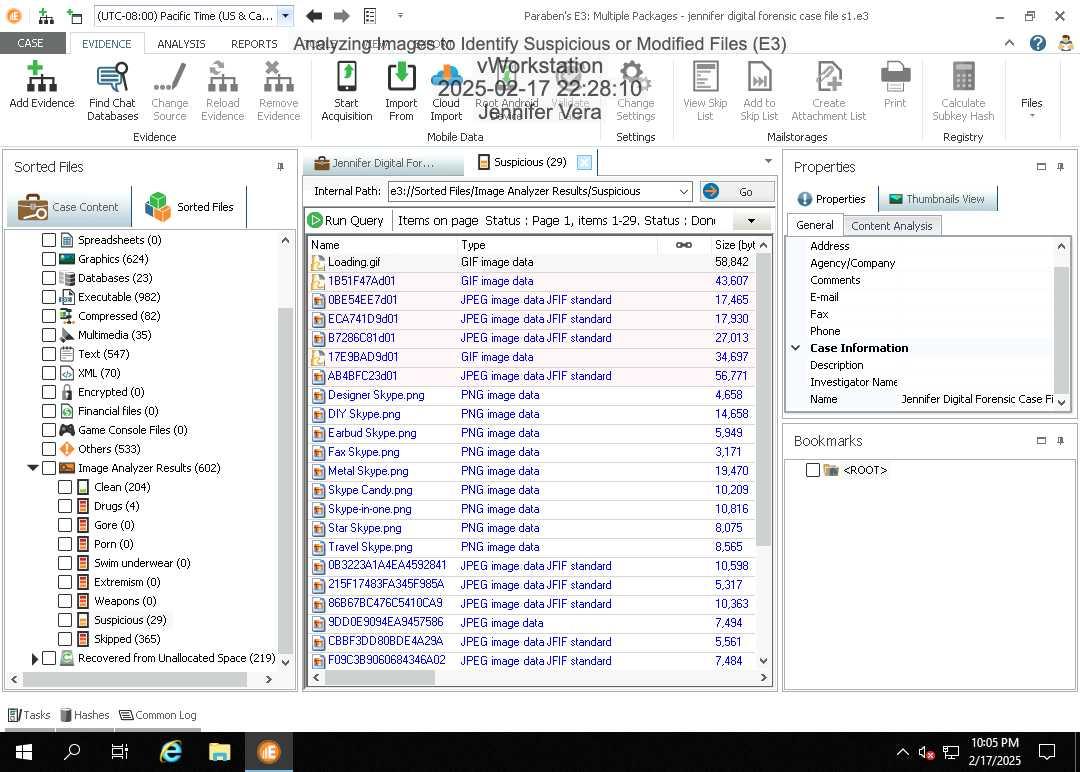
**Part 2: Use the Image Analyzer to Identify Suspicious Files**

1. Record the total number of sorted files. 3152

2. Provide a screen capture showing the expanded list of categories under Sorted Files. 3. Document the number of files in each of the following categories:

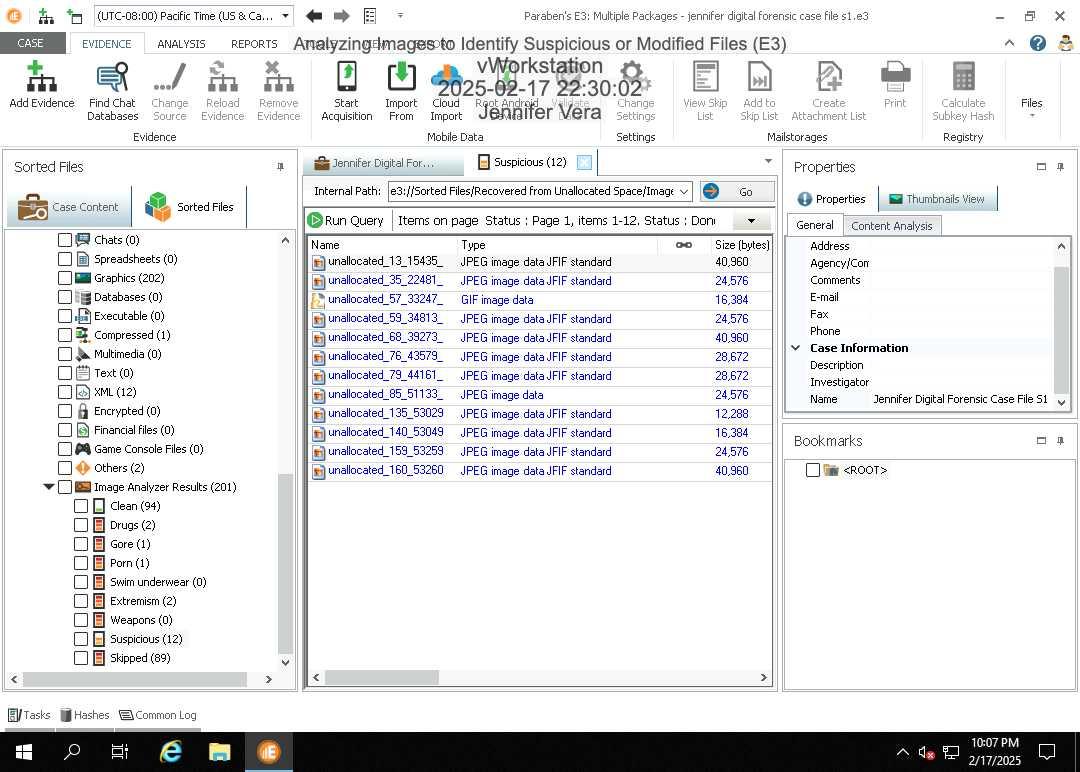
○ Clean: 204

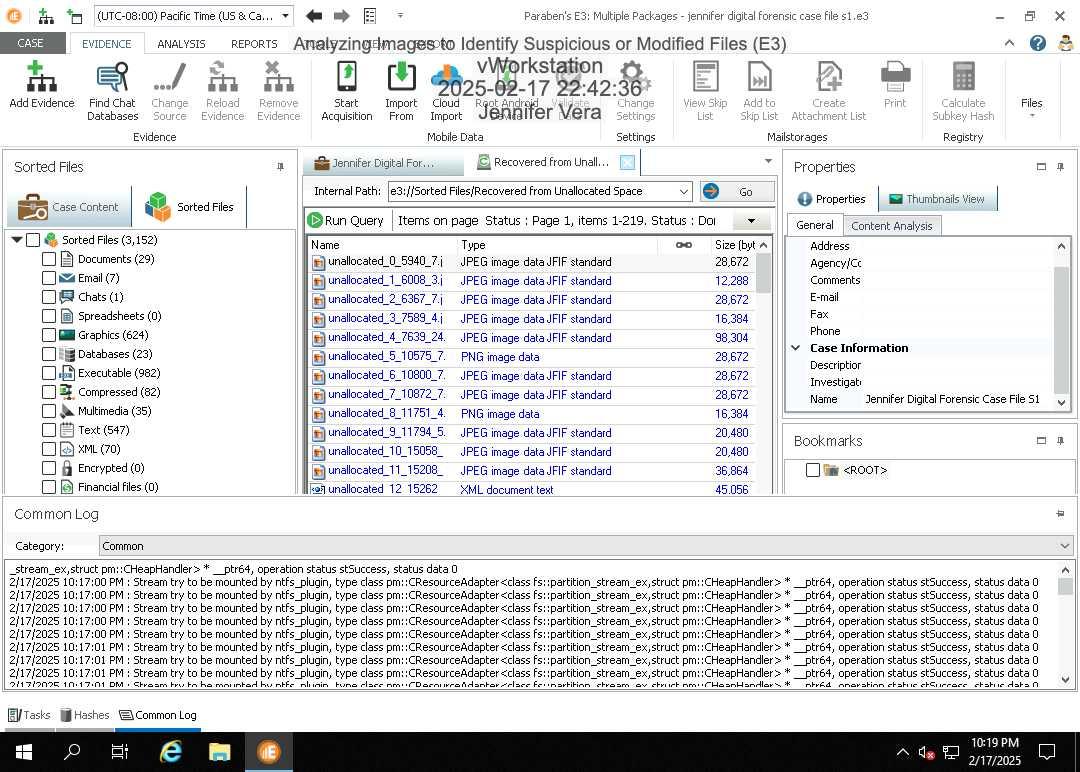
○ Suspicious: 29

4. Provide a screen capture showing the list of suspicious files. 

5. Repeat the above steps for the files in the Recovered from Unallocated Space category: ○ Clean: 94

○ Suspicious: 12

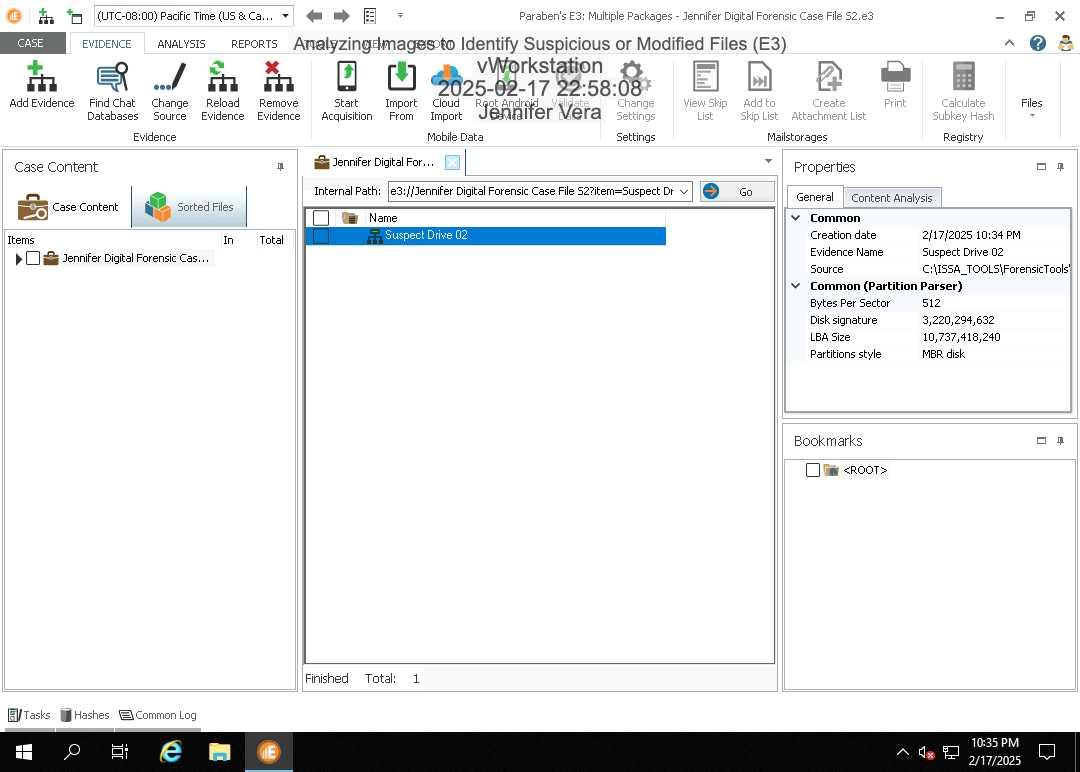
6. Provide a screen capture showing the list of suspicious files from the unallocated space.

7. Provide a screen capture showing the timestamp at the bottom of the Common Log.

8. Describe how E3 saved the sorted files. How does this compare with your expectations?

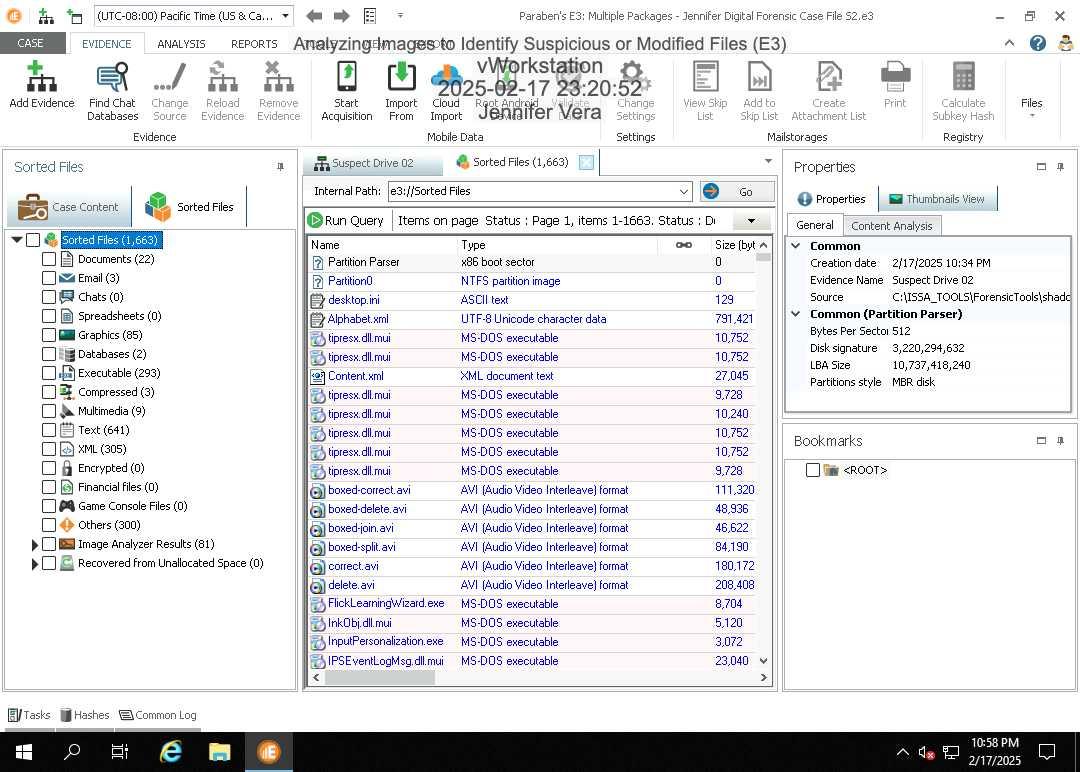
**Section 2: Applied Learning**

**Part 1: Create a New Case File**

1. Provide a screen capture showing the Suspect Drive 02 evidence loaded in E3. 

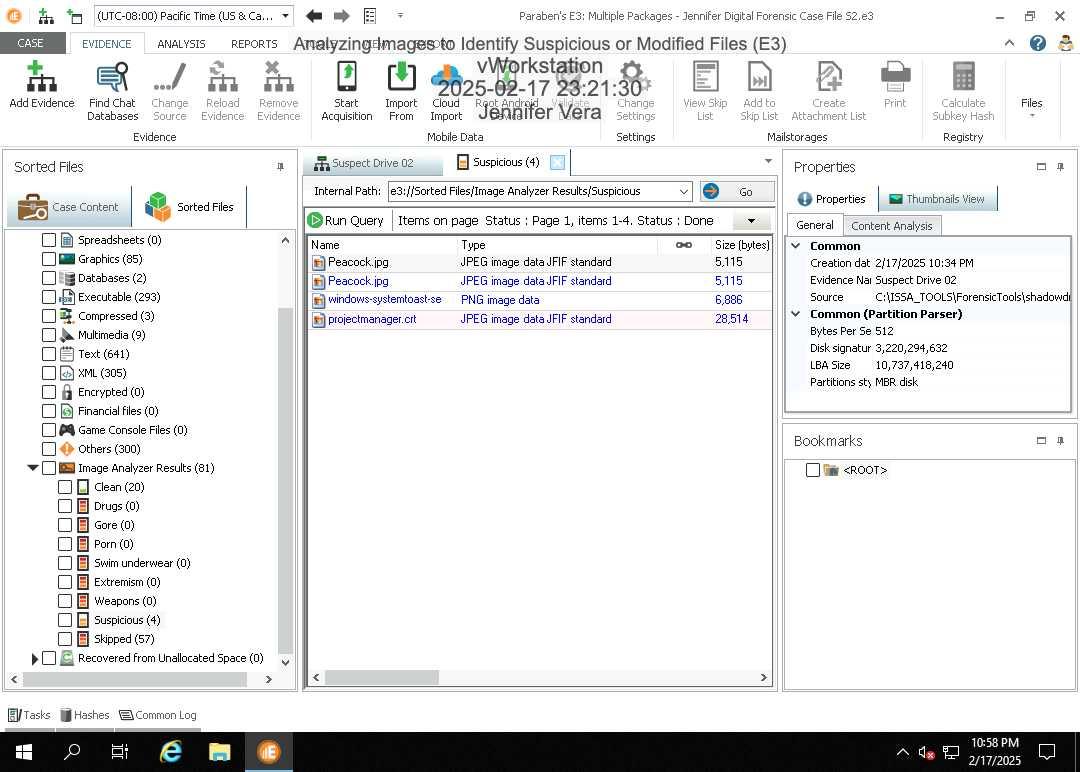
**Part 2: Use the Image Analyzer to Identify Suspicious Files**

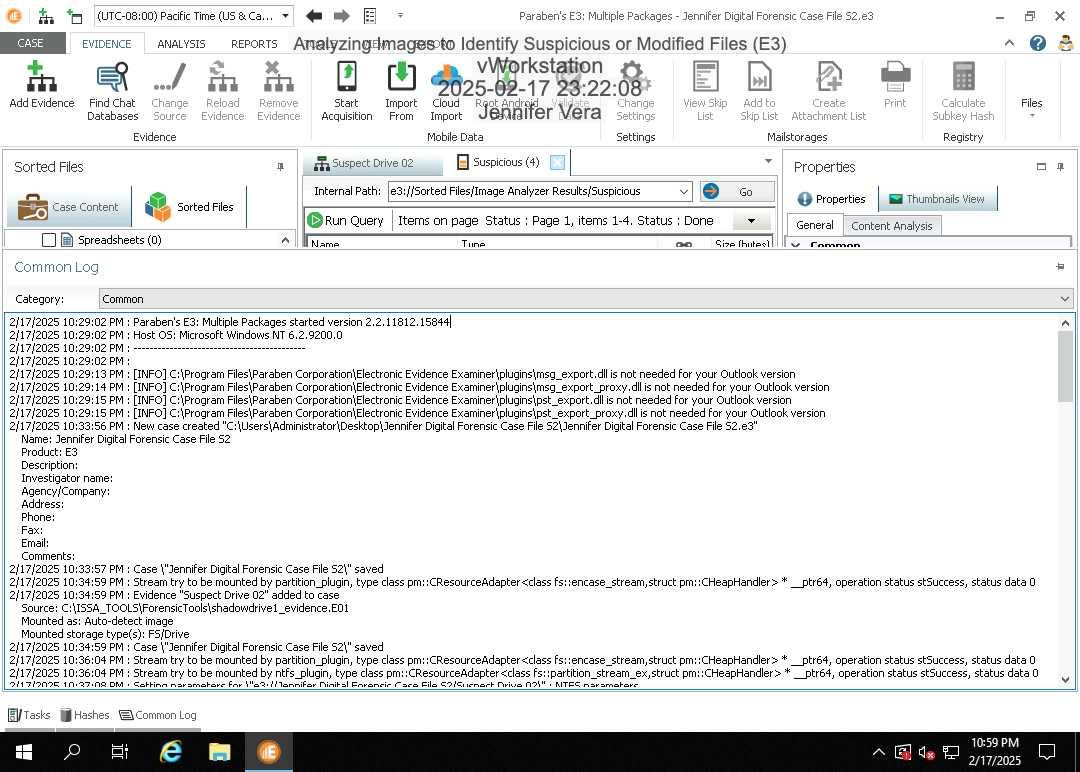
1. Record the total number of sorted files. *1,663*

2. Provide a screen capture showing the expanded list of sorted categories. 3. Document the number of files in each of the following categories:

○ Clean: 20

○ Suspicious: 4

4. Provide a screen capture showing the list of suspicious files. 

5. Provide a screen capture showing the timestamp at the bottom of the Common Log. 

6. Describe how E3 saved the sorted files. How does this compare with your expectations? *E3 organizes files by type documents, images, videos, etc. into folders for easy access. It sorts efficiently but may need some manual input.*

**Section 3: Challenge and Analysis**

**Part 1: Analysis and Discussion**

1. Why is it important to analyze images in a forensic investigation?

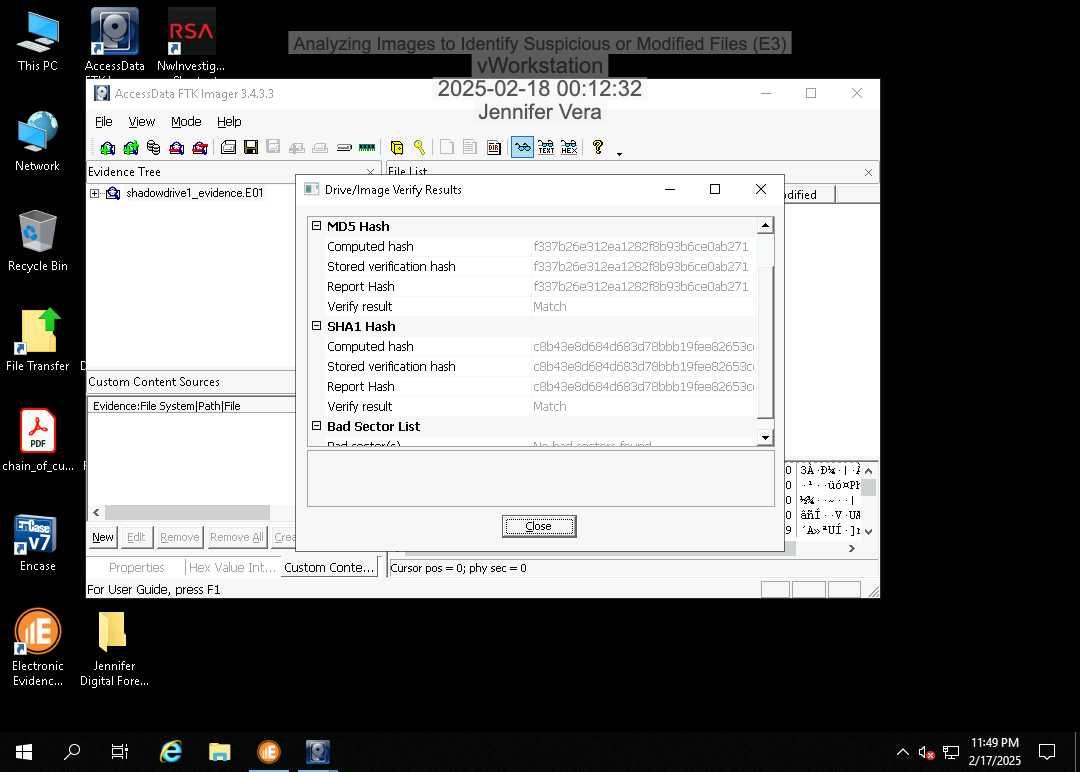
I*t's crucial for finding hidden data for the investigation.*

**Part 2: Tools and Commands**

1. Using E3, search the sorted files in the evidence drive from Section 1 for any files that include the name "foolish." Provide a screen capture showing the results. 

**Part 3: Challenge Exercise**

1. Using any forensic tool available on the vWorkstation desktop, verify the MD5 hash value of the evidence drive used in Section 2

(C:\ISSA\_TOOLS\ForensicTools\shadowdrive1\_evidence.E01). Provide a screen capture of the results. 

**Lab Assessment Questions**

1. Why might it be important to confiscate and identify the websites and kinds of images found on a suspect’s computer? *In order for investigators to access and analyze files.*

2. Explain what the E3 Image Analyzer does and what it looks for.

*It organizes the graphic files and sorts them into different categories based on the suspected content of the image.*

3. How do you decrease the amount of false positives in the Highly Suspect or Suspect categories?

*Manually checking evidence files.*

4. Into what categories does E3’s Sorted Files feature categorize all identified files?

*Provides details such as date, last accessed date, last modified date, MD5, SHA1 hashes for files.*

5. How many files did the Sorted Files feature identify on the evidence drive?

*1,663.*

6. Where would you look to identify a rogue application, malicious spyware application, or keyboard logger application on the target evidence drive?

*Executable category.*

7. Where would you look to identify ZIP files and compressed files that may actually contain embedded malicious software?

*Look within the compressed category.*

8. Where must you also look to examine possible image files on the evidence drive under investigation?

*Unallocated space.*

9. Why is it also important to look under the Graphics folder directly under the Sorted tree as well as the Image Analyzer Results category?

*Sometimes they may not turn up and be sorted.*