**Lab 5: Analyzing Images to Identify Suspicious or Modified Files (E3)**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

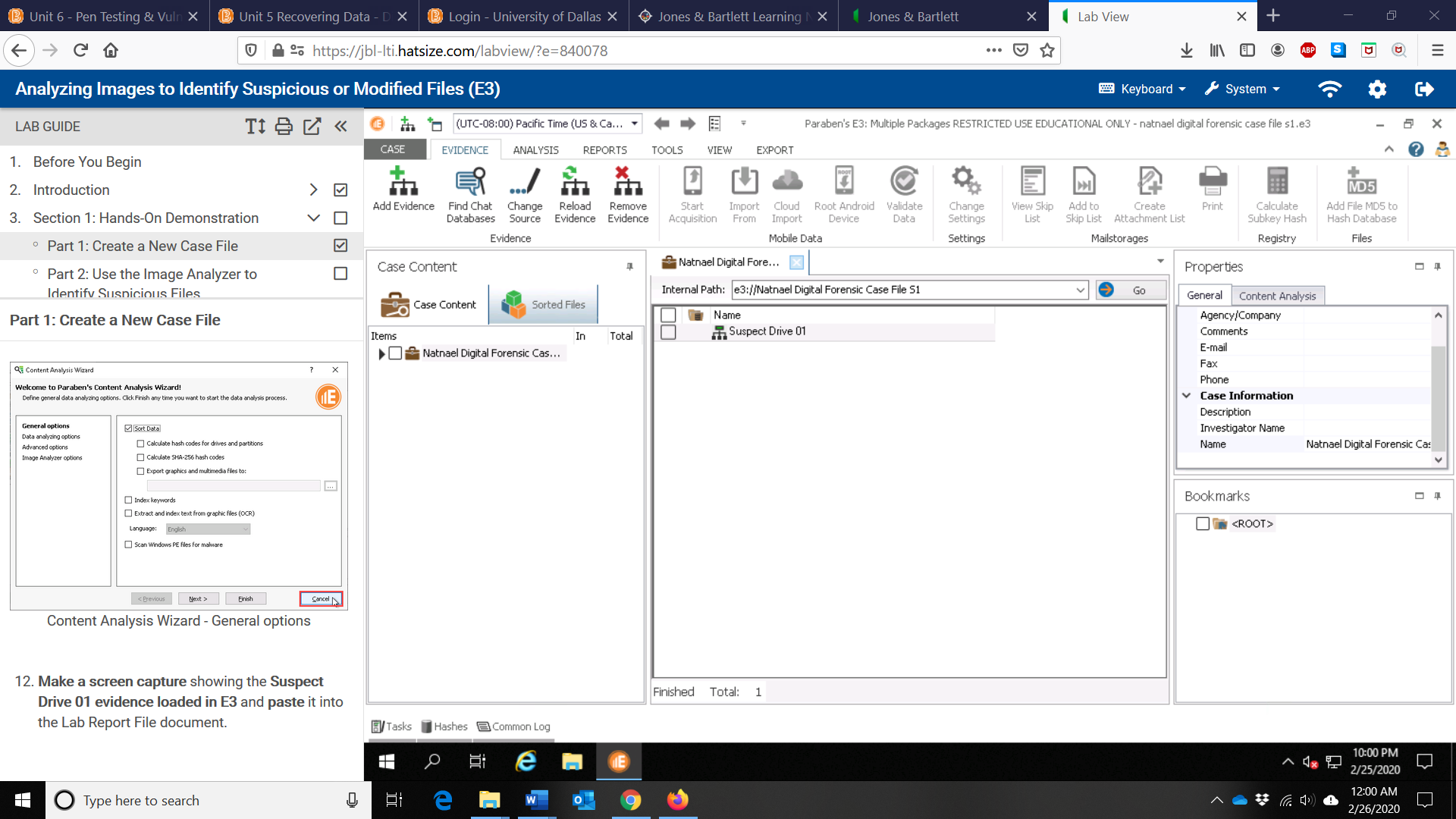
Spring 2020

Presented to Dr. Renita Murimi

**Section 1**

**Part 1**

1. Make a screen capture showing the Suspect Drive 01 evidence loaded in E3 and paste it into your Labe Report File document.

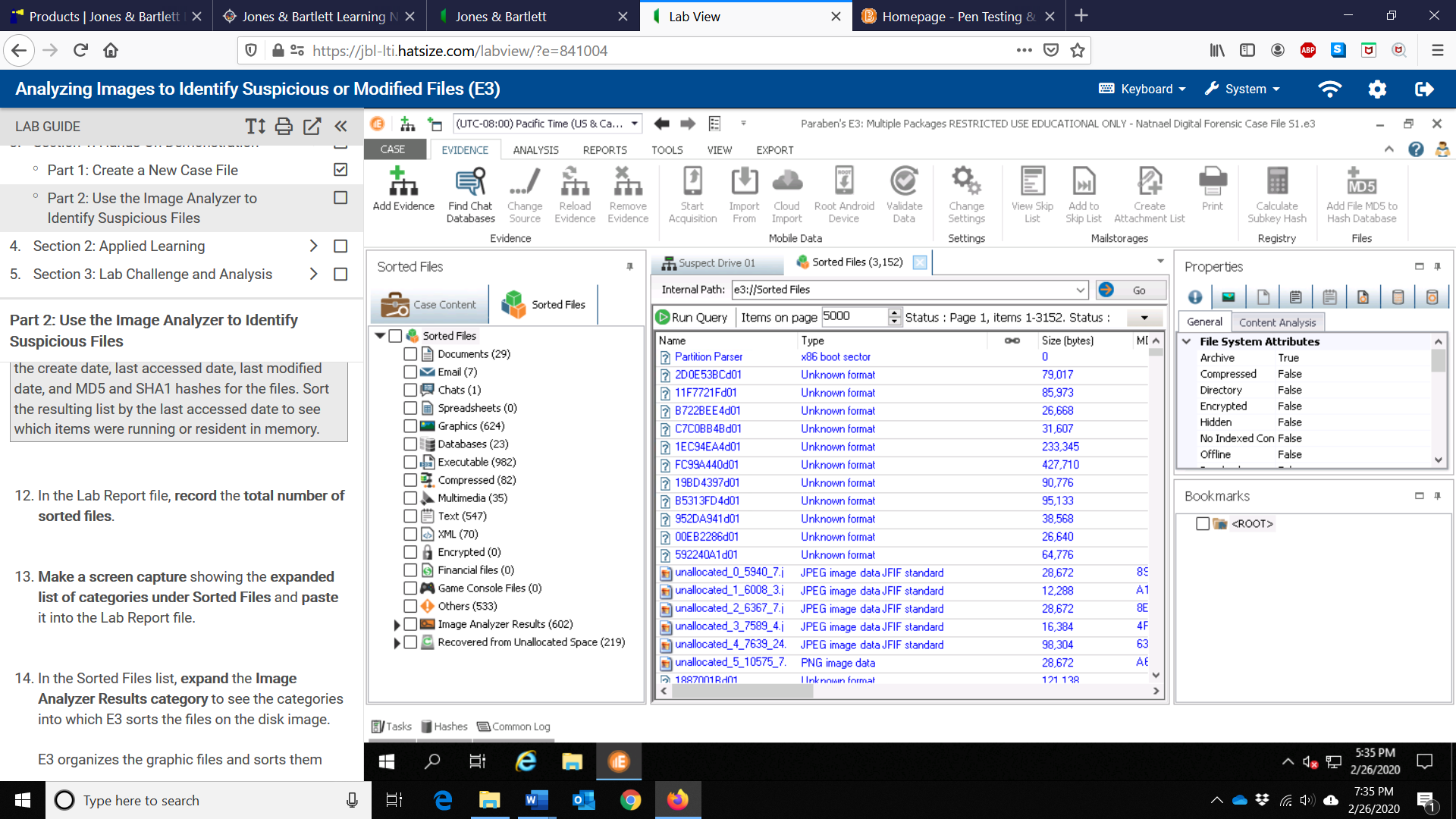


**Part 2**

1. In the Lab Report file, record the total number of sorted files.

3152 files

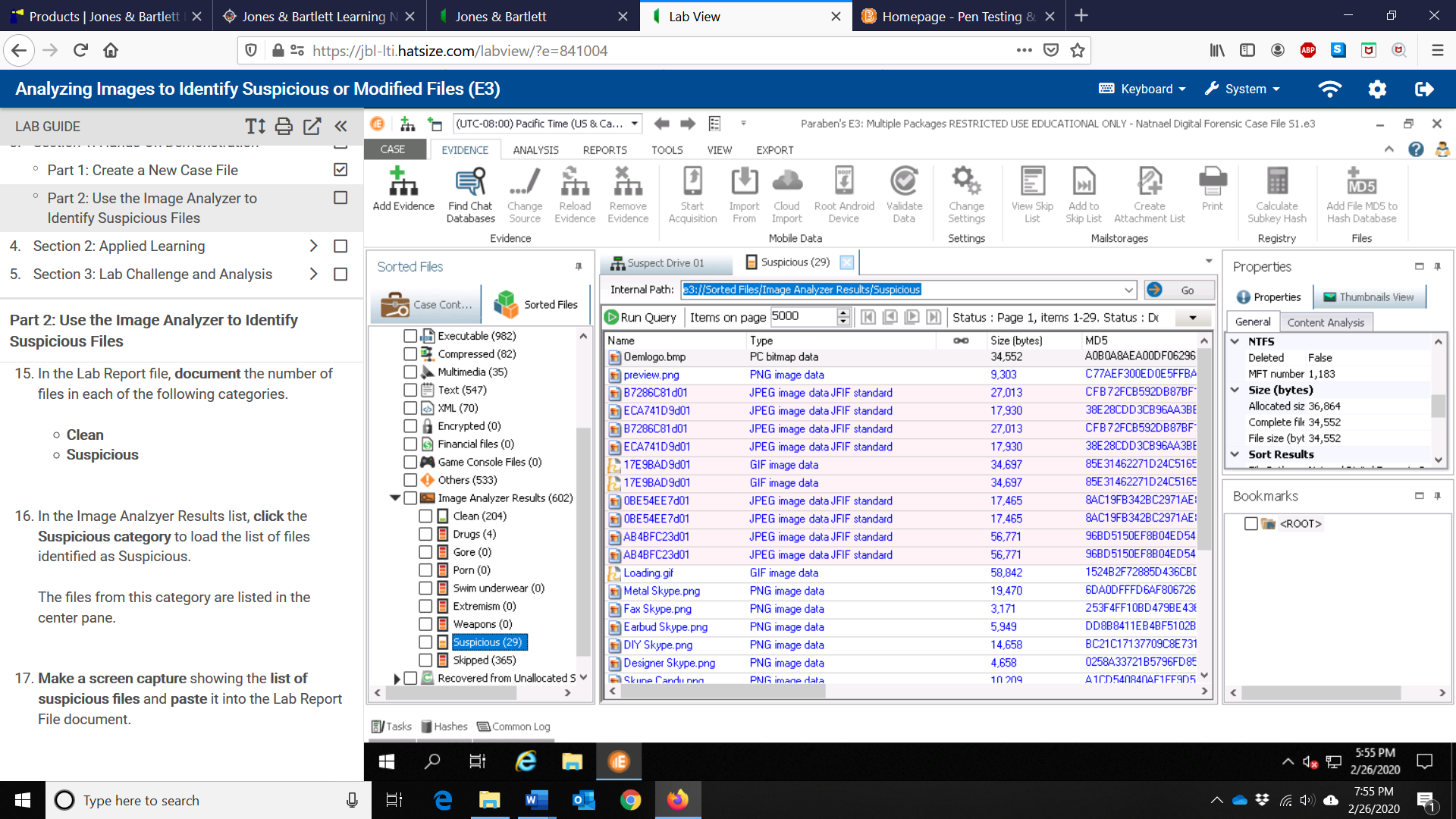
1. Make a screen capture showing the expanded list of categories under Sorted Files and paste it into the Lab Report file.

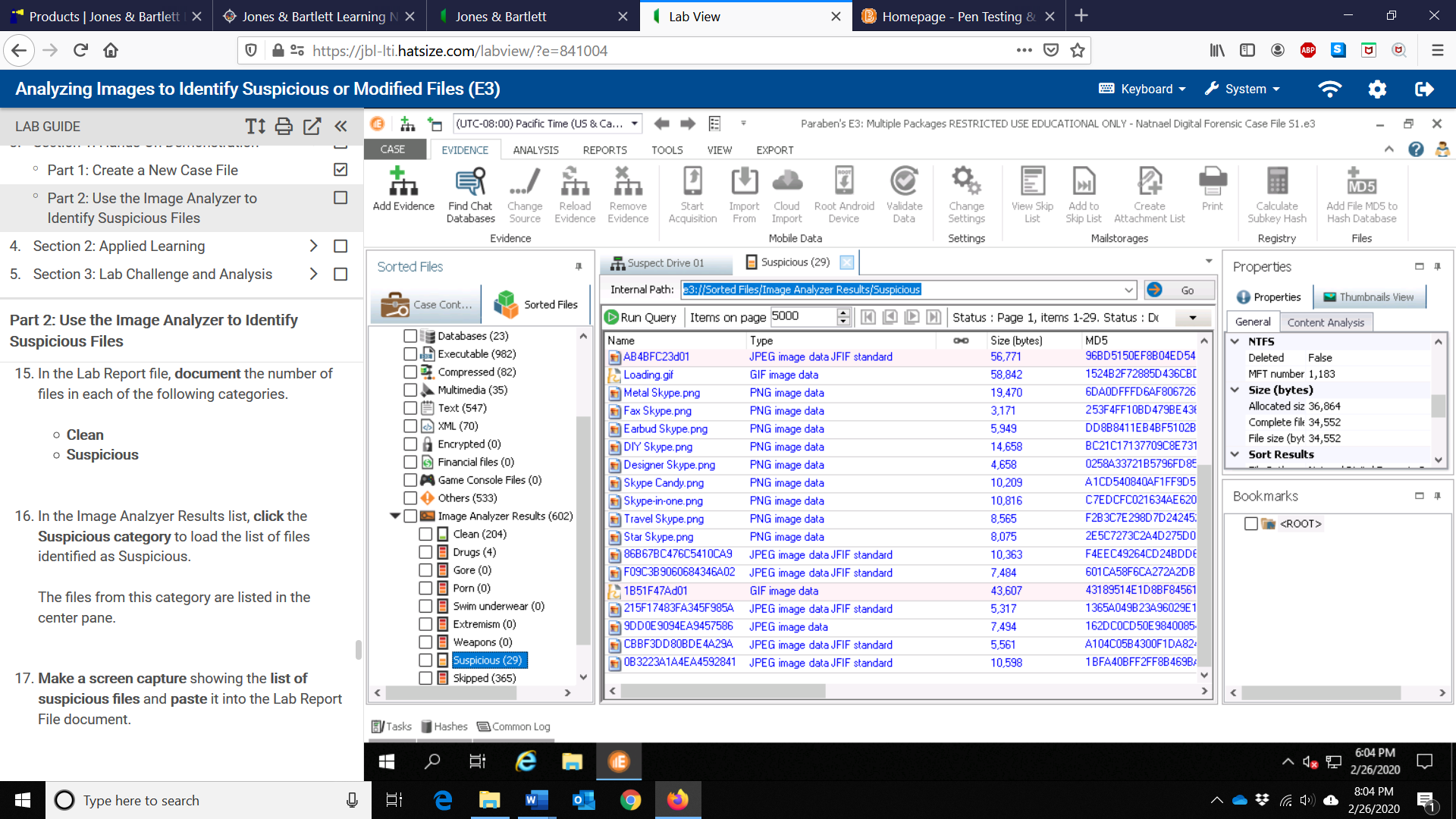


1. In the Lab Report file, document the number of files in each of the following categories.

* Clean: 204 files
* Suspicious: 29 files

1. Make a screen capture showing the list of suspicious files and paste it into the Lab Report File document.

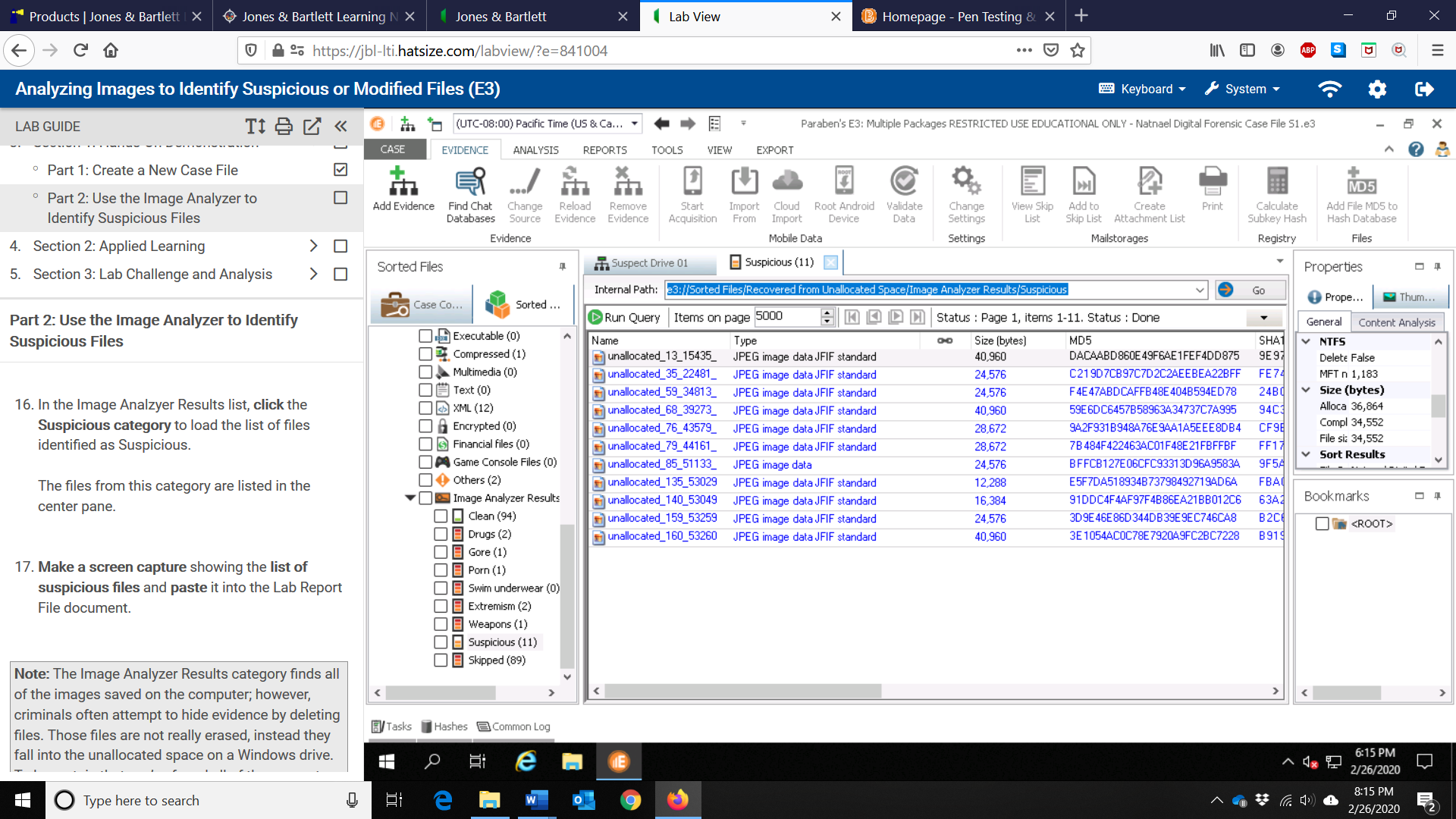




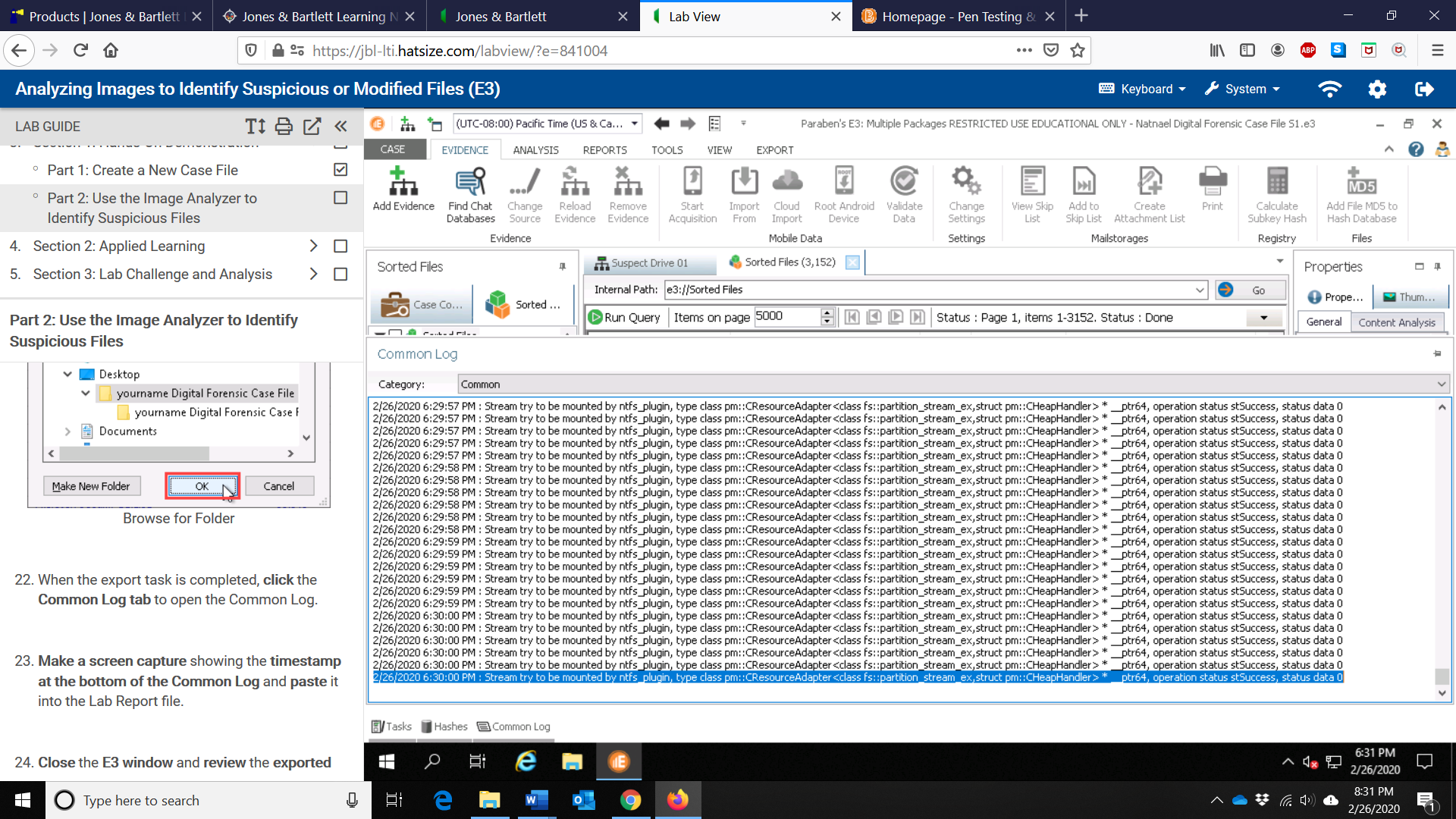
1. In the Lab Report file, document the number of files in each of the following categories from the Recovered from Unallocated Space category.

* Clean: 94 files
* Suspicious: 11 files

1. Make a screen capture showing the list of suspicious files from the unallocated space and paste it into the Lab Report File document.



1. Make a screen capture showing the timestamp at the bottom of the Common Log and paste it into the Lab Report file.



1. In the Lab Report file, describe how E3 saved the sorted files. How does this compare with your expectations?

E3 saved the sorted files in alphabetical order with each of the category files placed in corresponding folders. It saved the sorted files in folders matching the sorted categories. Additionally, E3 saved the sorted files along with the MD5 hash of each corresponding file in the folder. This is how I would have expected E3 to save the sorted files. However, the way the saved sorted files appear is different from the corresponding categories in the E3 GUI. The former is ordered based on alphabetical order while the latter is not.