Lab 5: Analyzing Images to Identify Suspicious or Modified Files

2: Applied Learning

Part 1: Create a new Case File

1. We begin by launching the E3 application and loading it with the image drive.

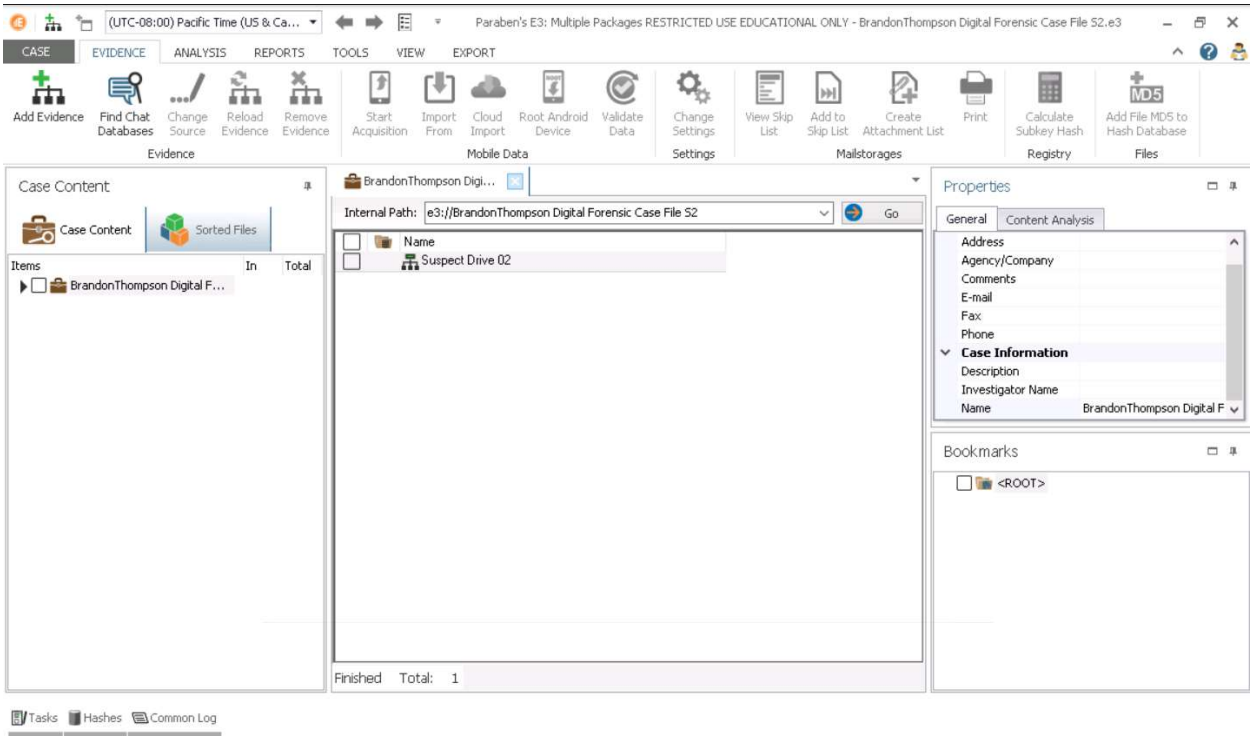

Figure 1 shows the loaded image drive to E3.

Part 2: Identify Suspicious Files Using Image Analyzer

1. We navigate to the Root Folder to perform a content analysis of the drive.

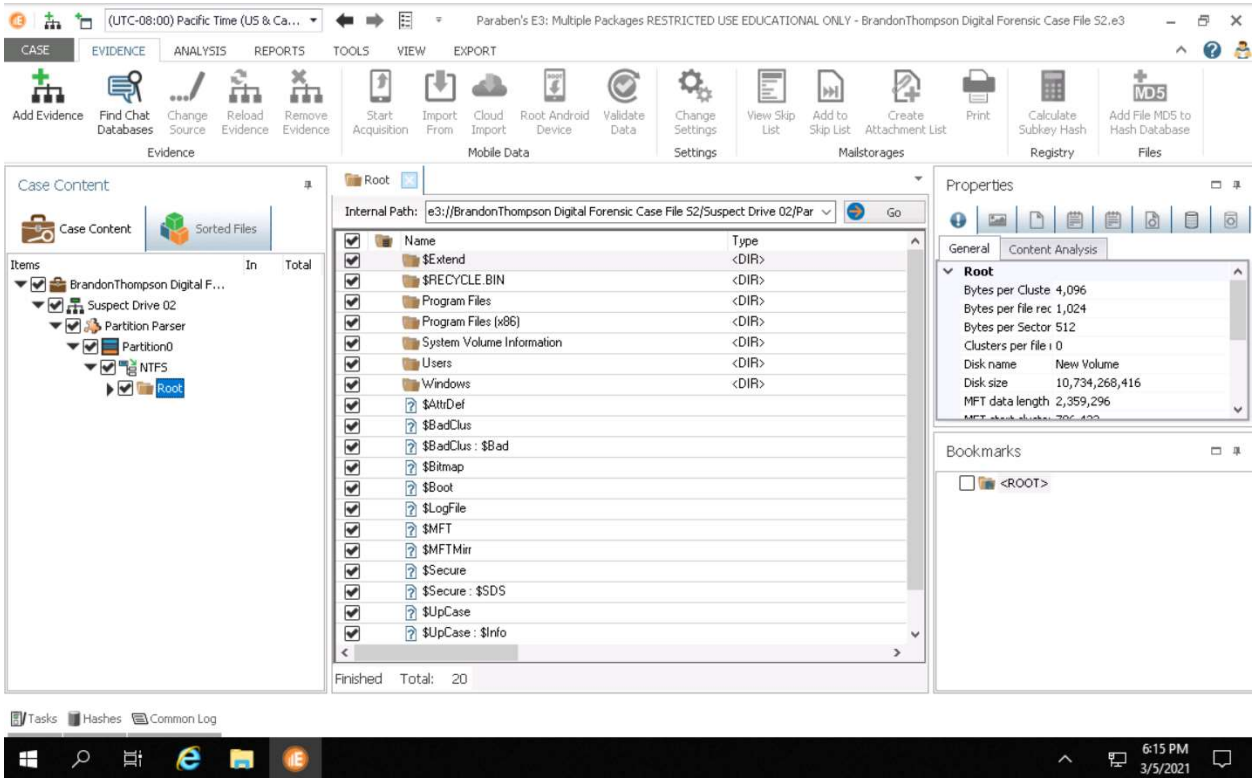

Figure 2 shows the Root file.

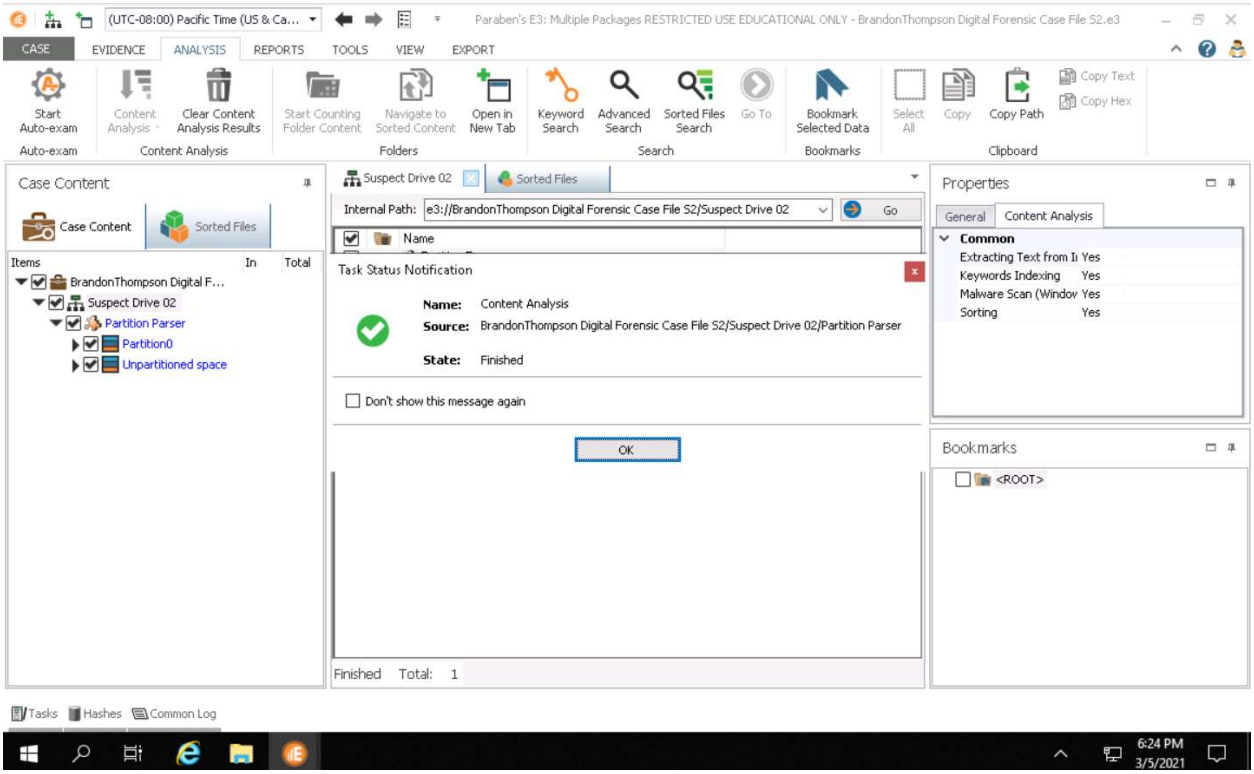

Figure 3 shows the completed analysis.

2. We are including the deleted data under the analysis because it is not actually deleted from the hard drive. Rather, the mapping to the file gets deleted.
3. After performing the content analysis, we check on all of the sorted files. In total, there were 1,663 sorted files.

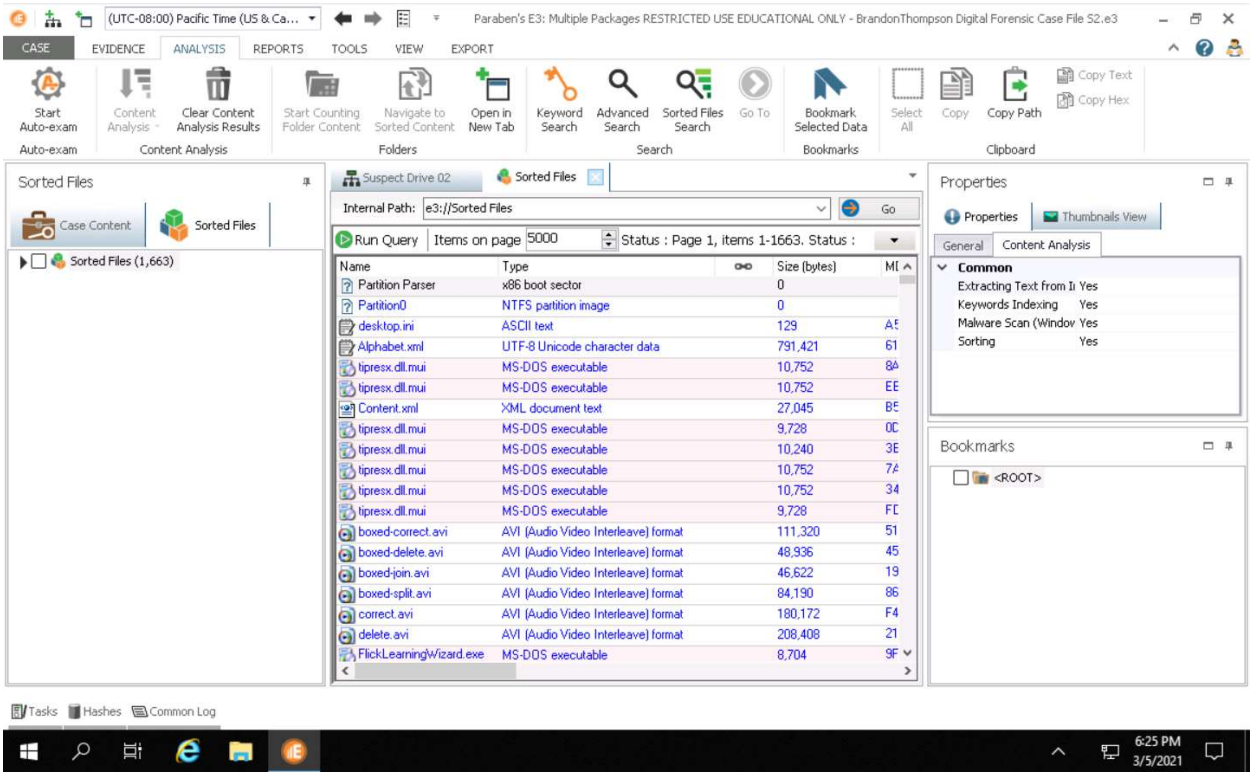

Figure 4 shows the sorted files.

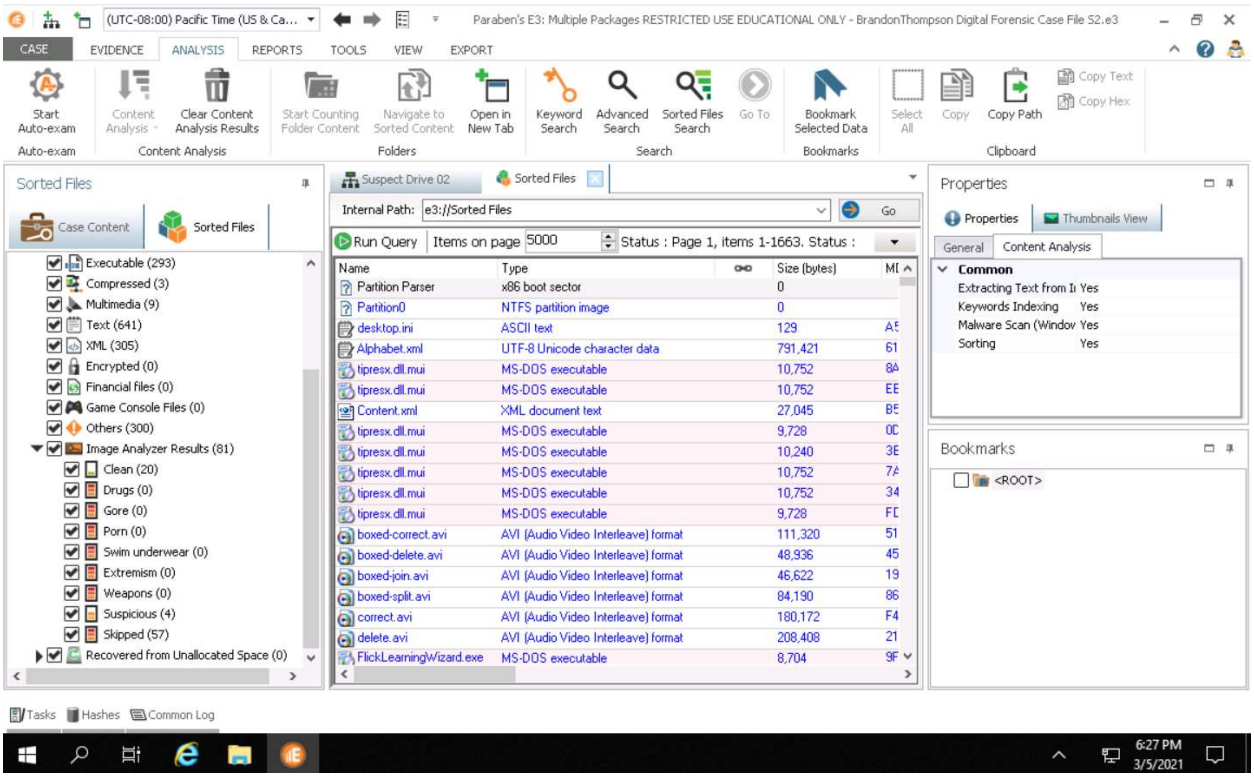

Figure 5 shows the sorted files in their respective folders.

4. In the image analyzer, we observed 20 clean files and 4 suspicious files.

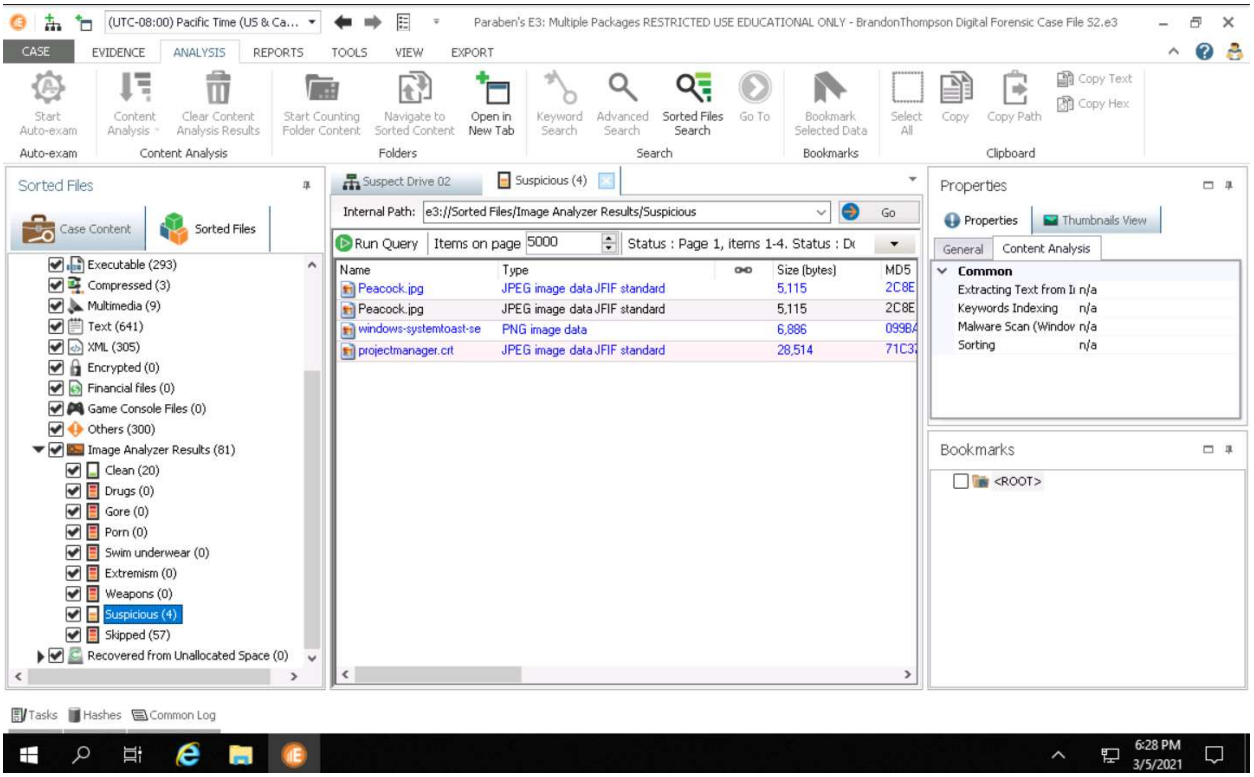

Figure 6 shows the suspicious files.

5. We then review the common log and observe the timestamp at the bottom.

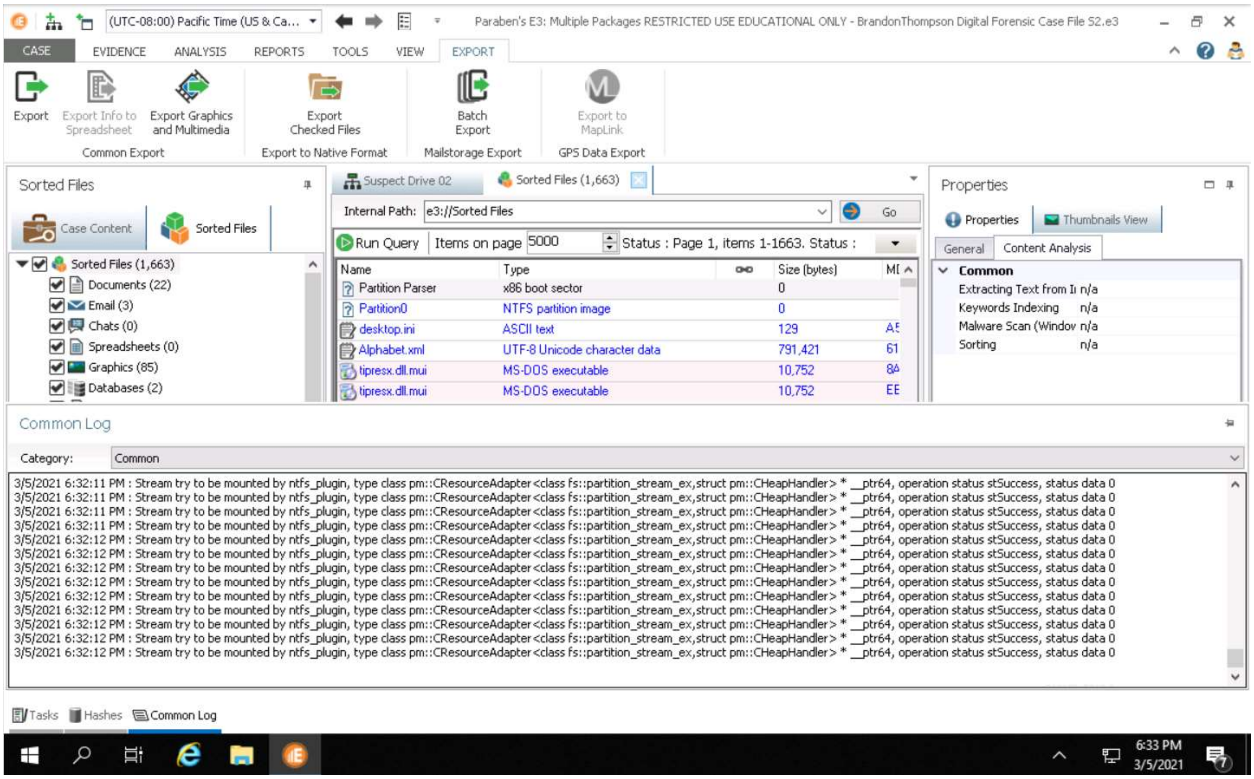

Figure 7 shows the common log and the timestamp.

E3 saved the files into separate containers, based on the sorted files. I expected the files to be saved within one folder.

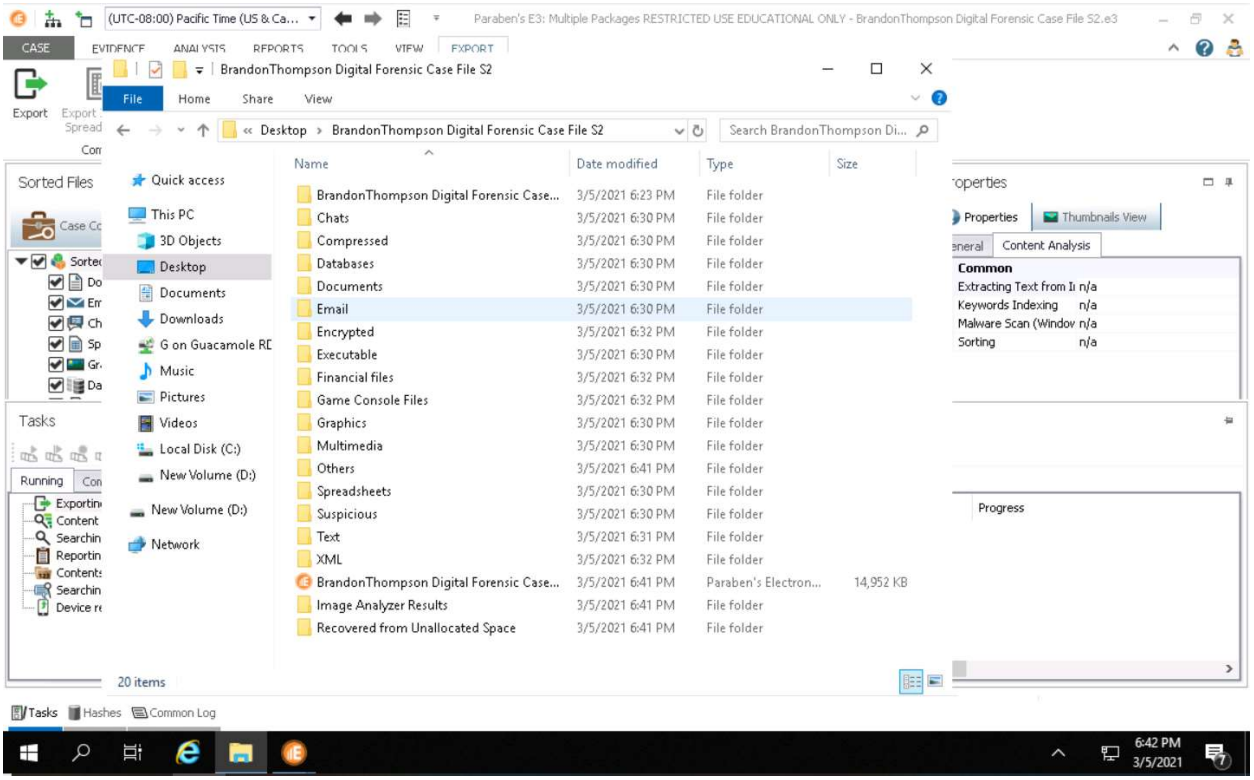

Figure 8 shows the saved sorted files.

In this lab, we went more into depth of using E3. We followed the same steps as in Lab 4 to load our image drive onto the application and create the suspected drive. From there, we navigated to the root folder to perform a content analysis. The content analysis performed an image analysis and sorted the files, ranging from clean to suspicious. Then the common log was observed and we copied the timestamp for it.