

Lab 4: Creating a Forensic System Case File for Analyzing Forensic Evidence

2: Applied Learning

Part 1: Explore Paraben's E3

1. We begin by launching the E3 application and create a new case file.

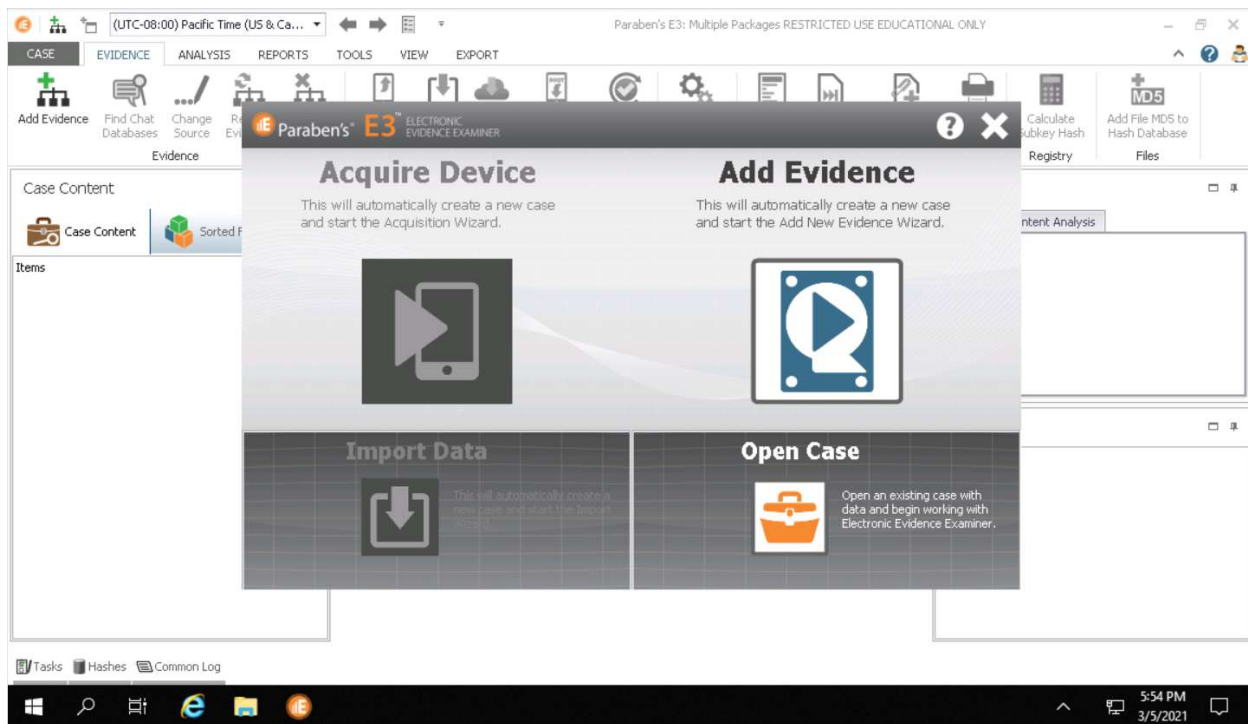


Figure 1 shows the E3 application launch page.

2. After attaching the image drive and naming it "Suspect Drive 02," we analyze the contents of the file.

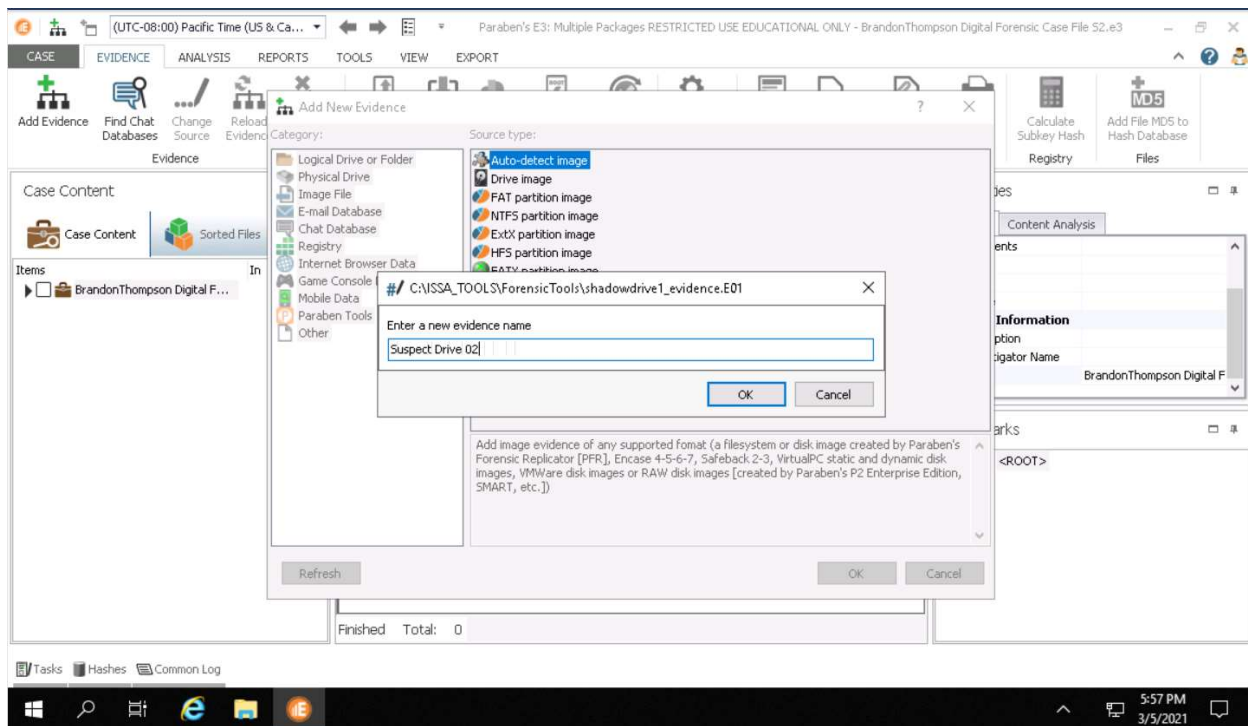


Figure 2 shows the image being added and renamed.

3. We then proceed to the Root file to see the file structure of the evidence.

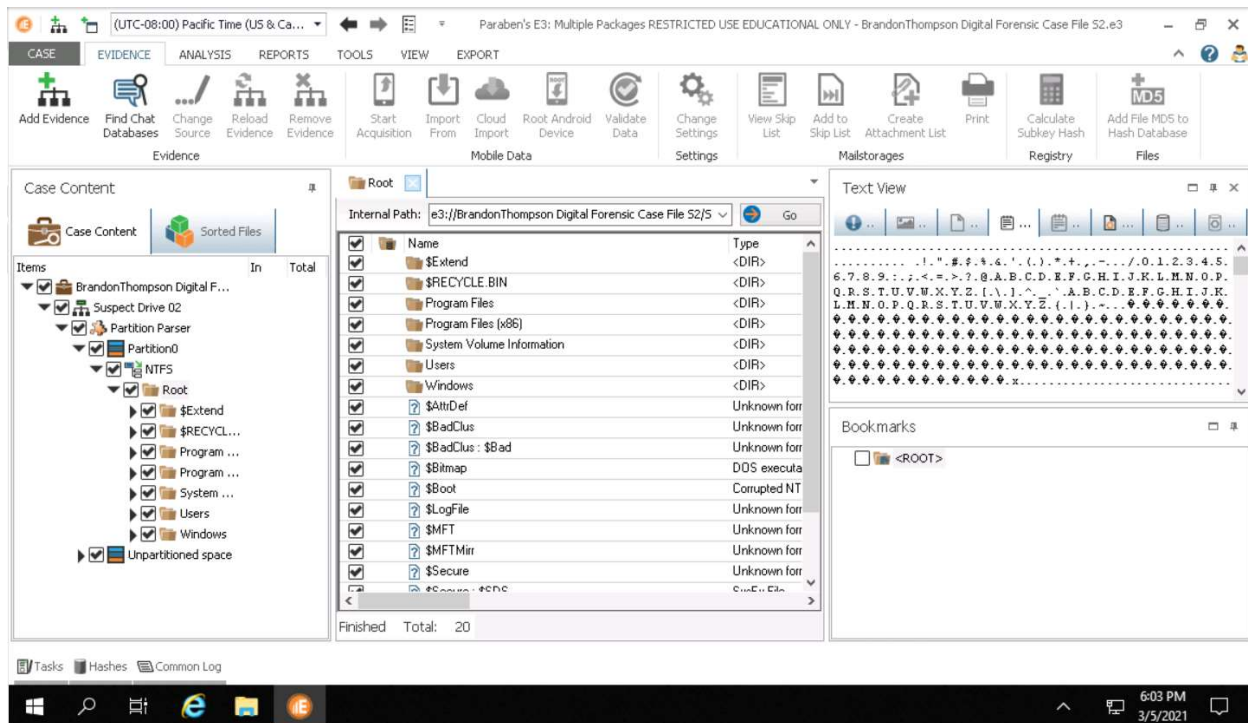


Figure 3 shows the contents of the Root file.

Within the Root folder, we see directories within the computer, such as Program Files and Windows. We also see other types of files that include necessary information, such as the Log File, MFT, and Bitmap.

In this lab, we learned how to use E3 to add evidence and analyze it. Using E3, we were able to view the contents of the image drive, including the contents of the root folder.