Lab 01 Report (CIS 104)

Applying the Daubert Standard to Forensic Evidence

Student Name: Jennifer Vera

Overview

In this lab. you act as a forensic specialist assisting the lead forensics investigator at the Cyber Crimes Division (CCD) for the Fremont Police Department. You were given a hard drive image taken from a seized computer suspected of containing stolen credit card numbers. You reviewed the search warrant and completed the Chain of Custody form that accompanied the evidence drive. You prepared the contents of the seized hard drive using a variety of forensic tools as evidence in accordance with the Daubert standard. You used FIX Imager to create hashes for key evidence files. You then validated the hash code using EnCase Imager and P2 Commander, two common forensic analysis tools.

Essay Questions & Answers from Section 1

⦁ Why is the unallocated space of a Windows system so important to a forensic investigator?

It could have missing or deleted files.

⦁ From where were the badnotesl.txt and badnotes2.txt files recovered?

INFO2 files.

⦁ What is the INF02 file used for?

Contains the original file name and location of deleted files that are now stored as Dcx in the Recycler.

⦁ How do you generate a hash file in FTK Imager?

Select export file hash list from the context menu.

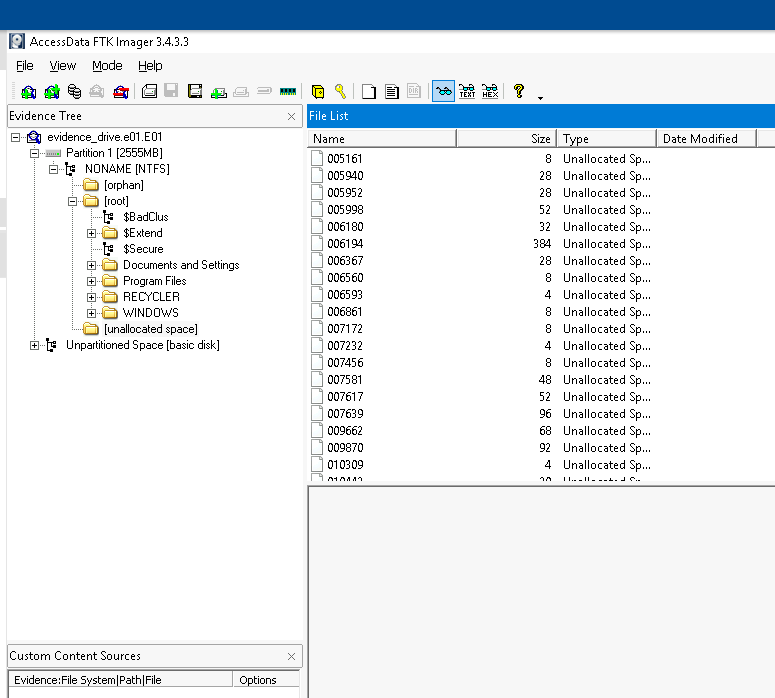
⦁ What was the MD5 hash value in 043458.csv. the deleted e-mail file? FFE0BDB5A41AB189AD31164D5B7D0D67

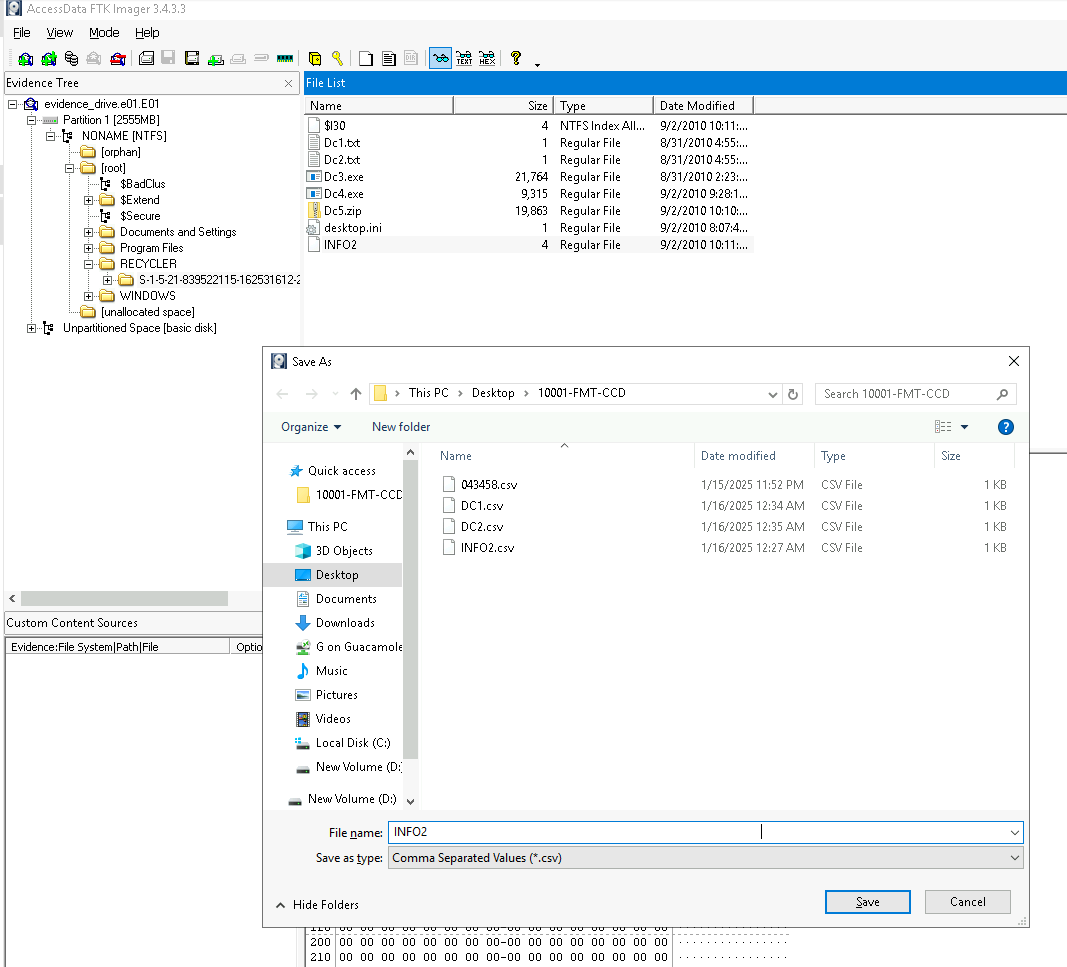
⦁ What is the Daubert standard?

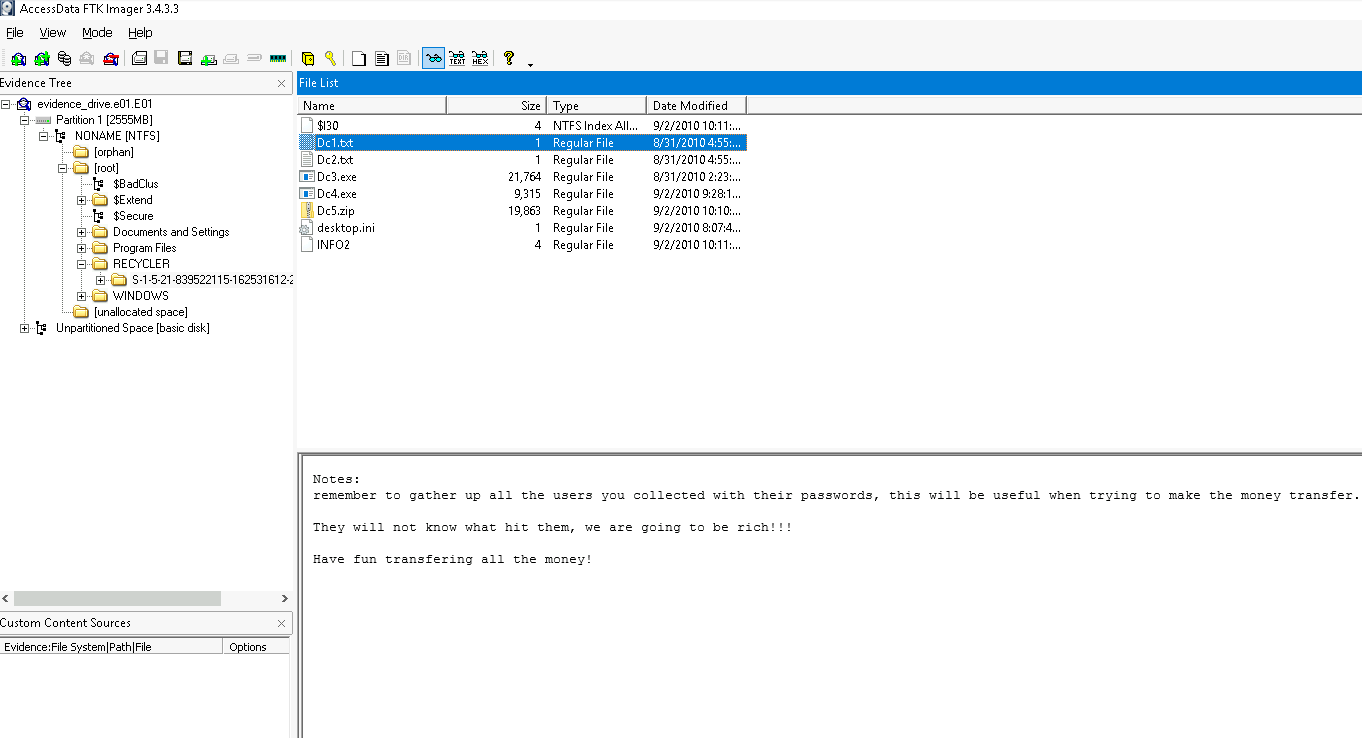
The prosecution must show that evidence files were not tampered with during forensic process.

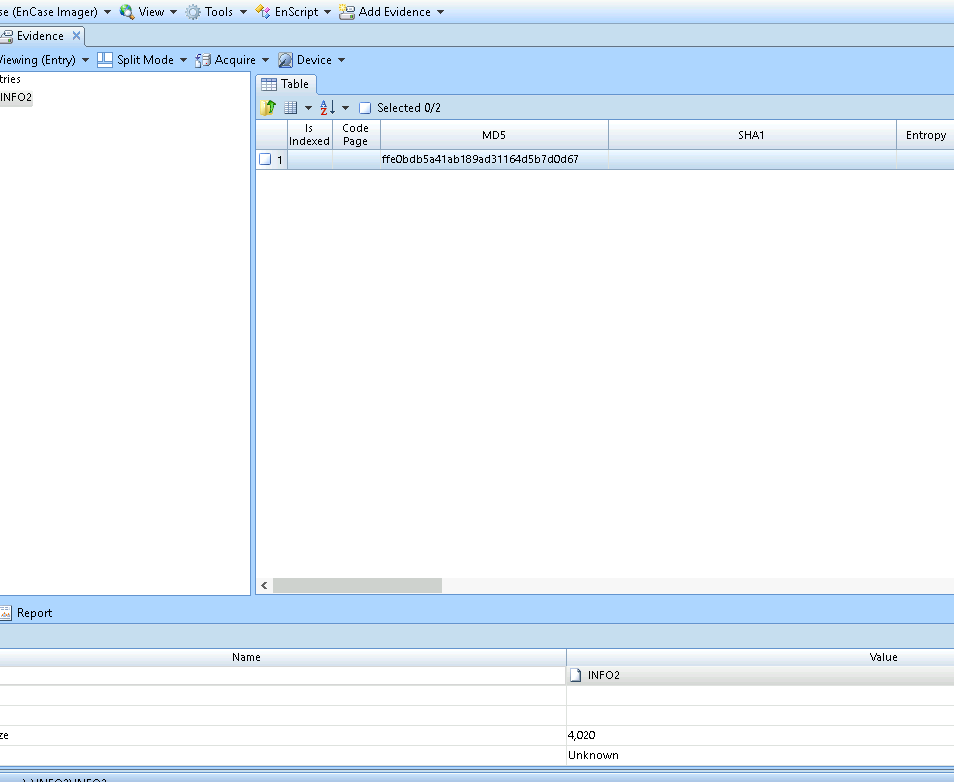
⦁ Why must a forensic investigator be familiar with emerging technologies? Must stay current with technologies

Section 2: Screen Captures and page 1 captures of reports

Part 2, step 5; contents of the Outlook.eml file in FTK imager: 

Part 2, step 15; hash value of the original Outlook.csv file:

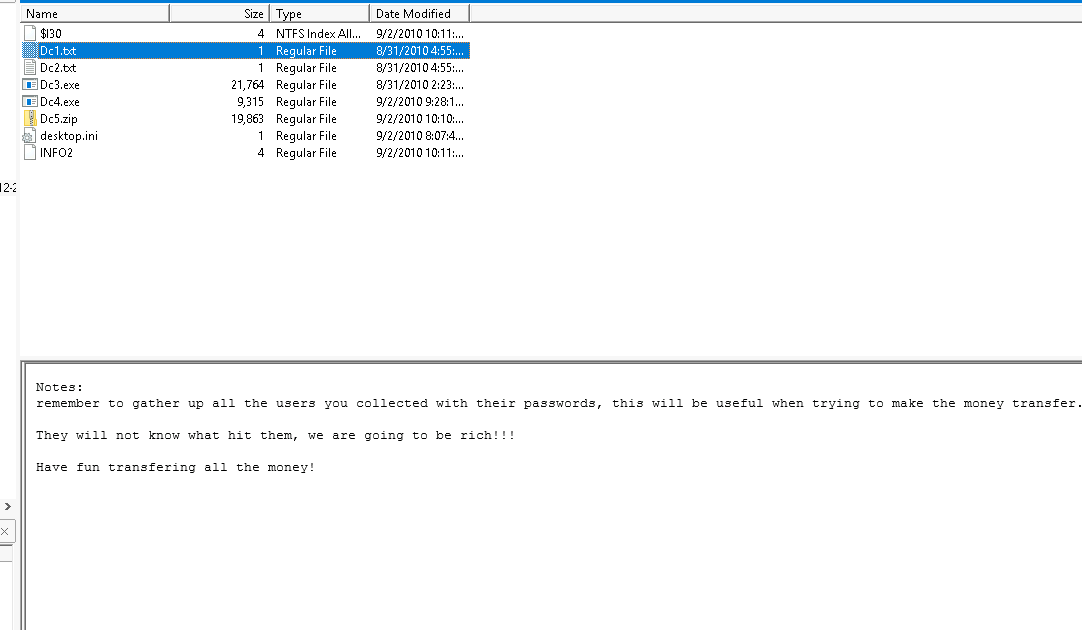
Part 2, step 17; hash value of the Outlook2.csv file:

Part 3, step 14; MD5 field for OutlookEML in Encase Imager:

Part 4, step 8; MD5 field from outlook\_(1).eml.MD5 in P2 Commander: FFE0BDB5A41AB189AD31164D5B7D0D67

Section 1 (Extra Credit): Screen Captures and page 1 captures of reports

Part 2, step 18; contents of the Dc1.txt file:

Part 2, step 18; contents of the Dc2.txt file:

Part 2, step 23; contents of the Desktop folder:

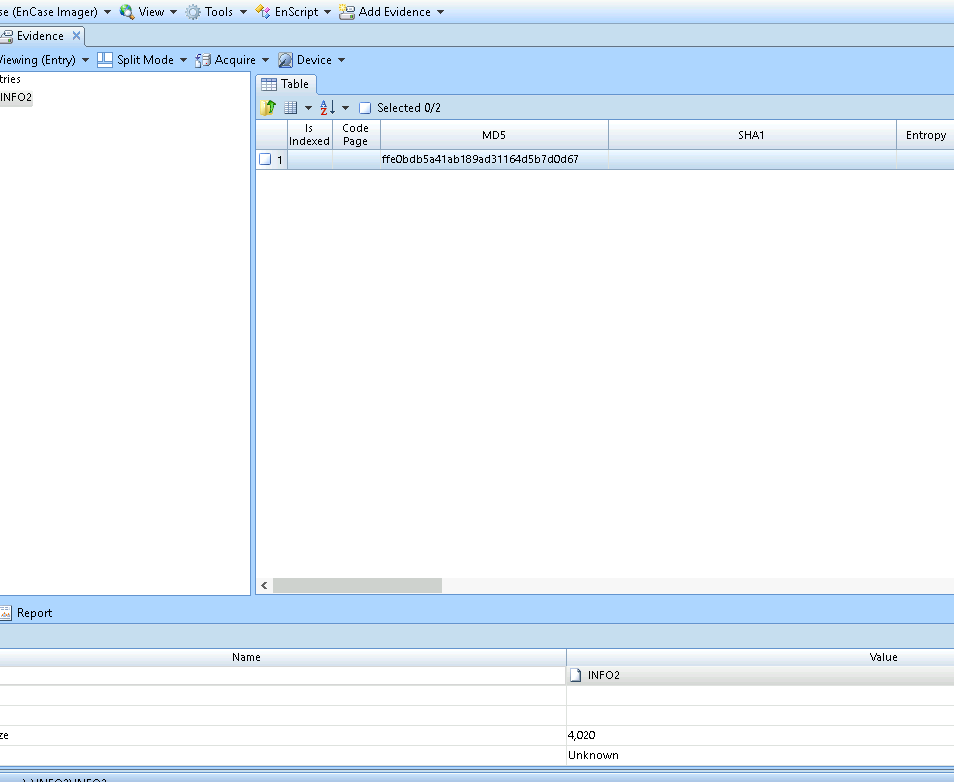
Part 2, step 30; contents of the INFO2.CSV file:

Part 2, step 30; contents of the badnotes1.CSV file:

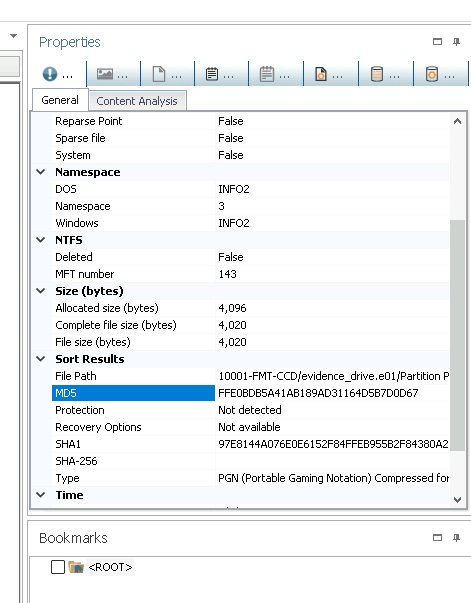
Part 2, step 30; contents of the badnotes2.CSV file:

Part 2, step 30; contents of the Dc1.CSV file:

Part 2, step 30; contents of the Dc2.CSV file:

Part 3, step 13; MD5 field for INFO2 in Encase Imager:

Only the first capture for Part 3, step 13 is required for this report. The others can be ignored

Part 4, step 7; MD5 field for INFO2 in P2 Commander:

Only the first capture for Part 4, step 7 is required for this report. The others can be ignored.

Report: yourname\_S1 \_Chain\_of\_Custody.pdf (capture page 1 only!)