

# Applying the Daubert Standard to Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

Student:

Vishal Singh Bhardvaj

Email:

Time on Task:

2 hours, 50 minutes

Progress:

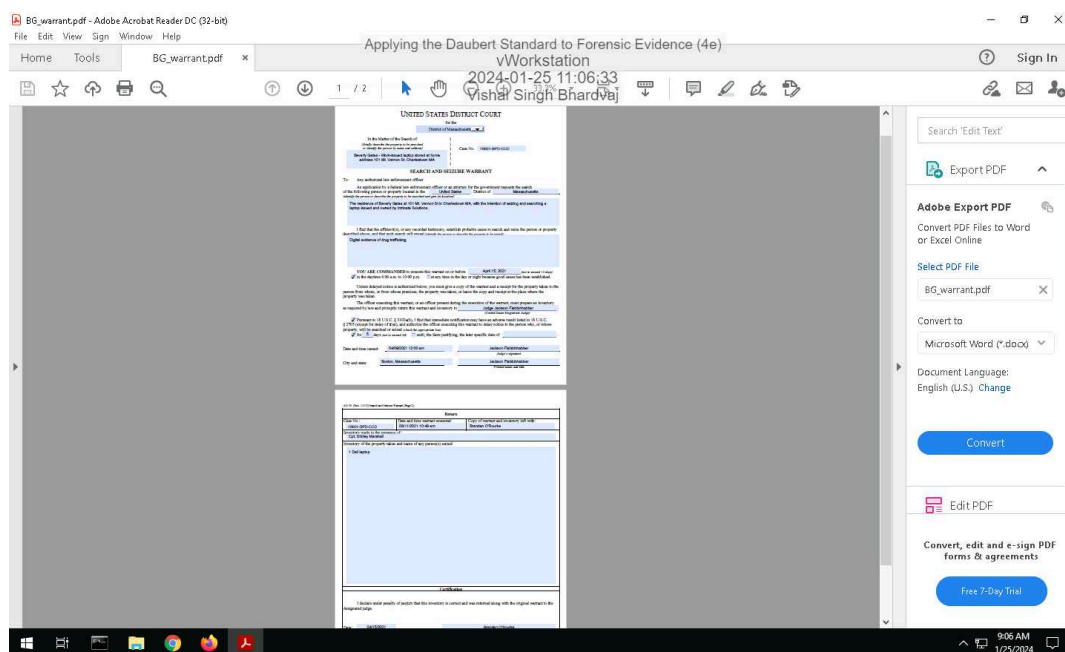
100%

Report Generated: Thursday, January 25, 2024 at 1:53 PM

## Section 1: Hands-On Demonstration

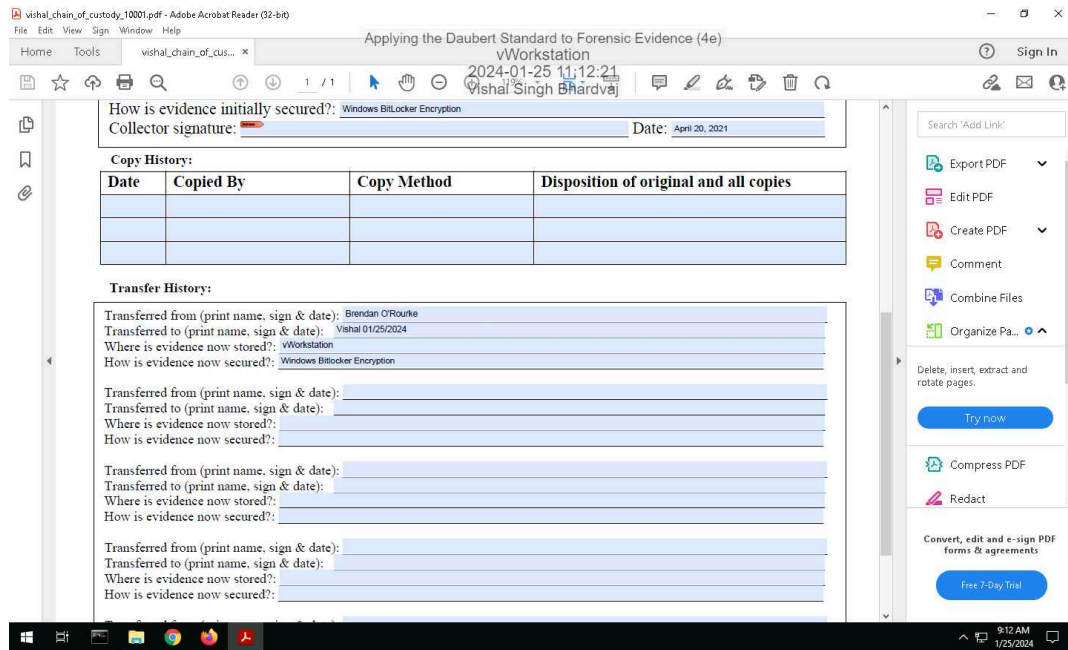
### Part 1: Complete Chain of Custody Procedures

7. Make a screen capture showing the contents of the search warrant in Adobe Reader.



## Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

14. **Make a screen capture** showing the **completed Chain of Custody form** in Adobe Reader.



## Part 2: Extract Evidence Files and Create Hash Codes with FTK Imager

34. **Make a screen capture** showing the **contents of the 0002665\_hash.csv** file.



# Applying the Daubert Standard to Forensic Evidence (4e)

## Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

37. Make a screen capture showing the contents of the RecycleBinEvidence\_hash.csv file.



```
RecycleBinEvidence_hash - Notepad
File Edit Format View Help
Applying the Daubert Standard to Forensic Evidence (4e)
Workstation\NAME [NTFS]\[root]\$RECYCLE.BIN\S-1-5-21-4060736057-2770307751-2791612479-10
2024-01-25 11:36:49
"f6acd93cfb9c0cc901f809d6349472f1", "11a15ebd2ffaa8021bdedd233c3a547446041bc3", "EvilWin10\NAME [NTFS]\[root]\$RECYCLE.BIN\S-1-5-21-4060736057-2770307751-2791612479-10
2024-01-25 11:36:49
Vishal Singh Bhardvaj
```

38. Make a screen capture showing the contents of the MyRussianMafiaBuddies\_hash.csv file.



```
MyRussianMafiaBuddies_hash - Notepad
File Edit Format View Help
Applying the Daubert Standard to Forensic Evidence (4e)
Workstation\NAME [NTFS]\[root]\Temp Folder\MyRussianMafiaBuddies.txt"
2024-01-25 11:36:49
Vishal Singh Bhardvaj
```

# Applying the Daubert Standard to Forensic Evidence (4e)

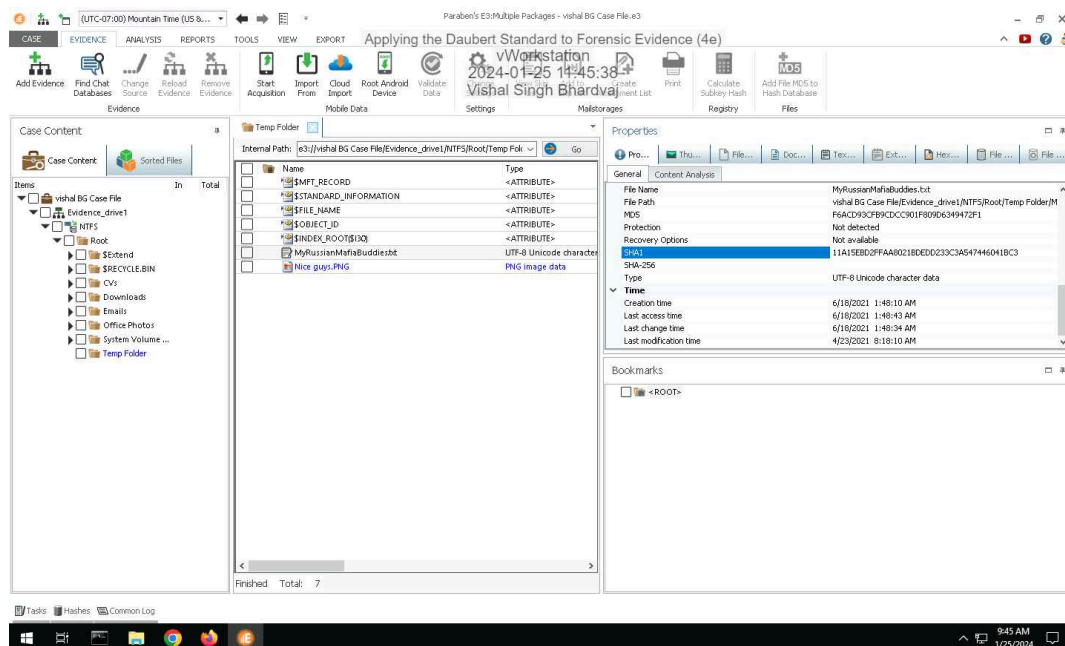
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

39. Make a screen capture showing the contents of the Nice guys\_hash.csv file.

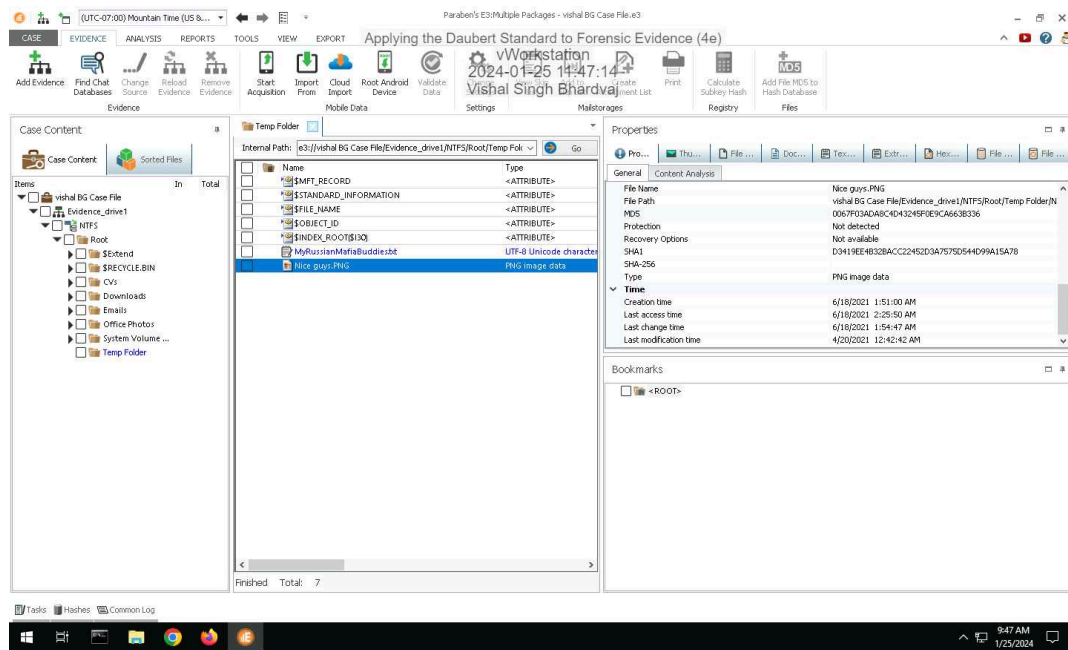


## Part 3: Verify Hash Codes with E3

14. Make a screen capture showing the MD5 and SHA1 values for the MyRussianMafiaBuddies.txt file.



### 16. Make a screen capture showing the MD5 and SHA1 values for the Nice Guys.png file.



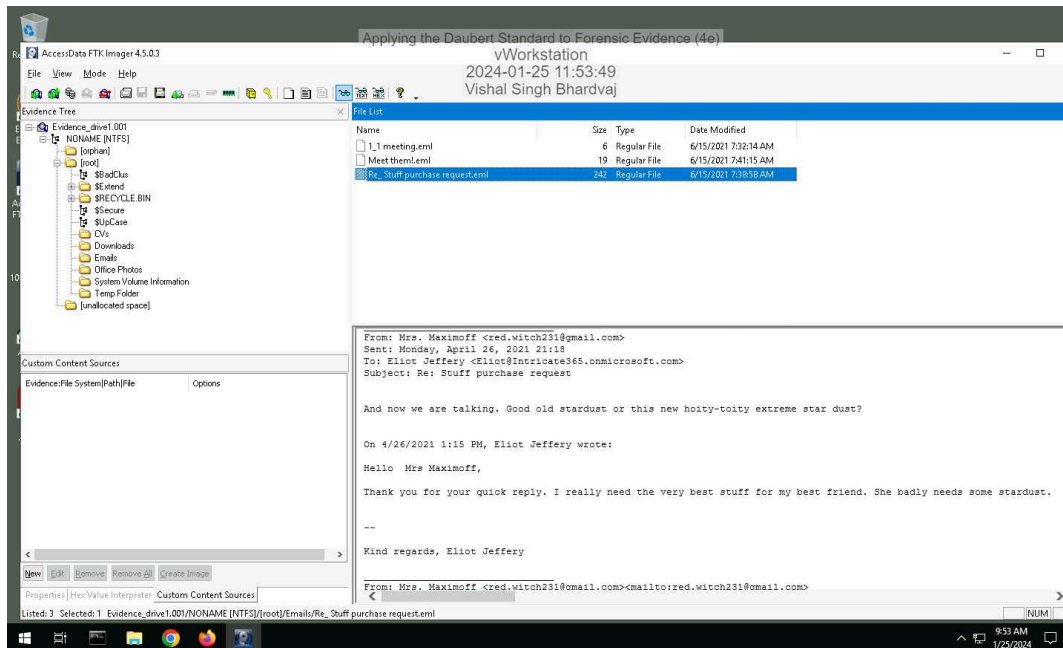
### 17. Describe how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

Hash value generated by FTK and E3 are exactly the same for each file.

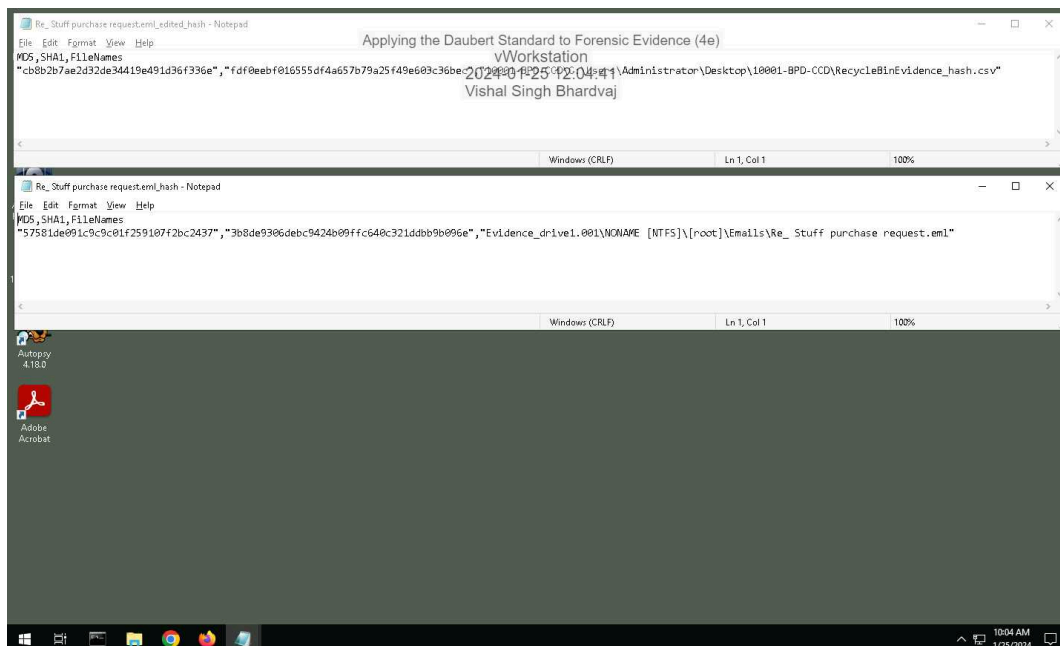
### Section 2: Applied Learning

#### Part 1: Extract Evidence Files and Create Hash Codes with FTK Imager

5. Make a screen capture showing the **contents** of the suspicious email file in the Display pane.

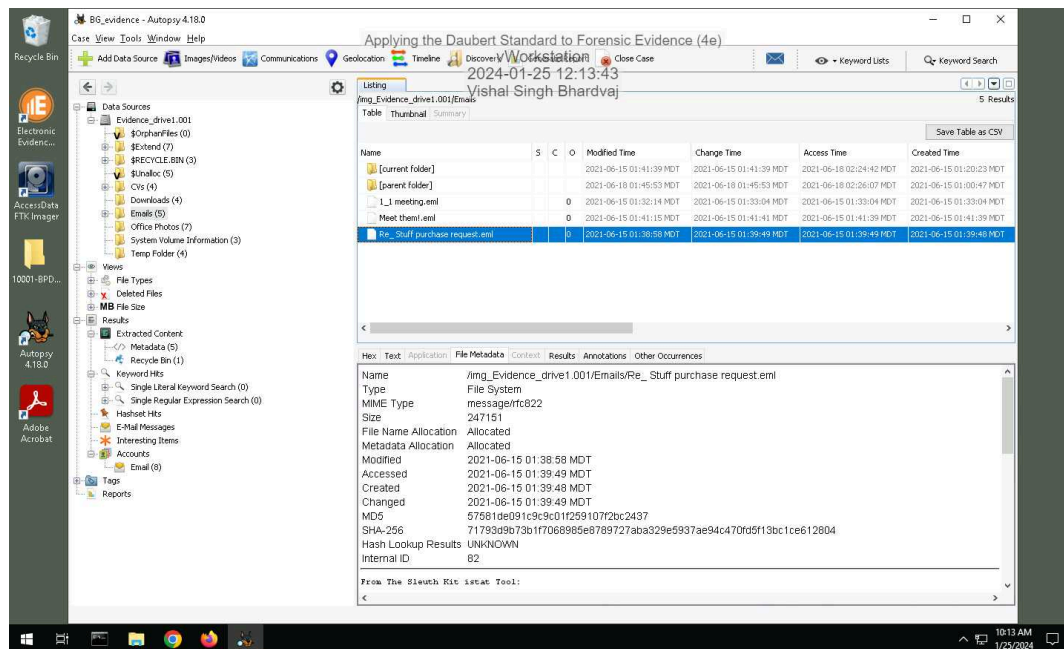


16. Make a screen capture showing the **two** hash values for the suspicious email file.



### Part 2: Verify Hash Codes with Autopsy

#### 11. Make a screen capture showing the MD5 field in the Result Viewer.



#### 12. Describe how the hash value produced by Autopsy compares to the values produced by FTK Imager for the two .eml files.

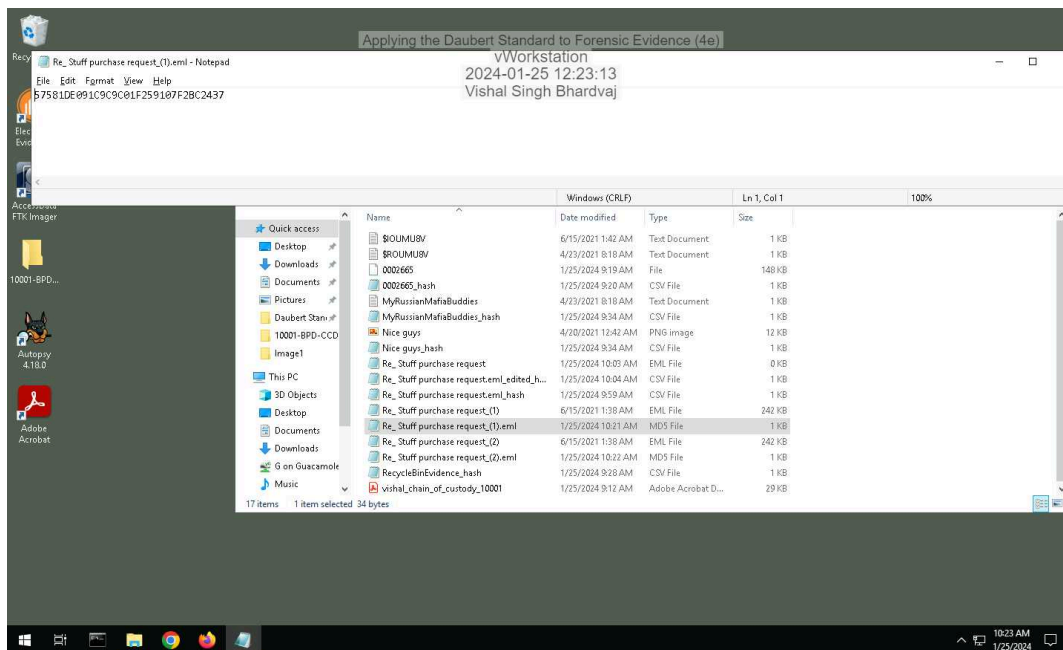
This hash value is same as that of unedited Re\_Stuff Purchase request.eml file but different from edited eml file

### Part 3: Verify Hash Codes with E3

# Applying the Daubert Standard to Forensic Evidence (4e)

## Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

### 7. Make a screen capture showing the MD5 value produced by E3.



### 8. Describe how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

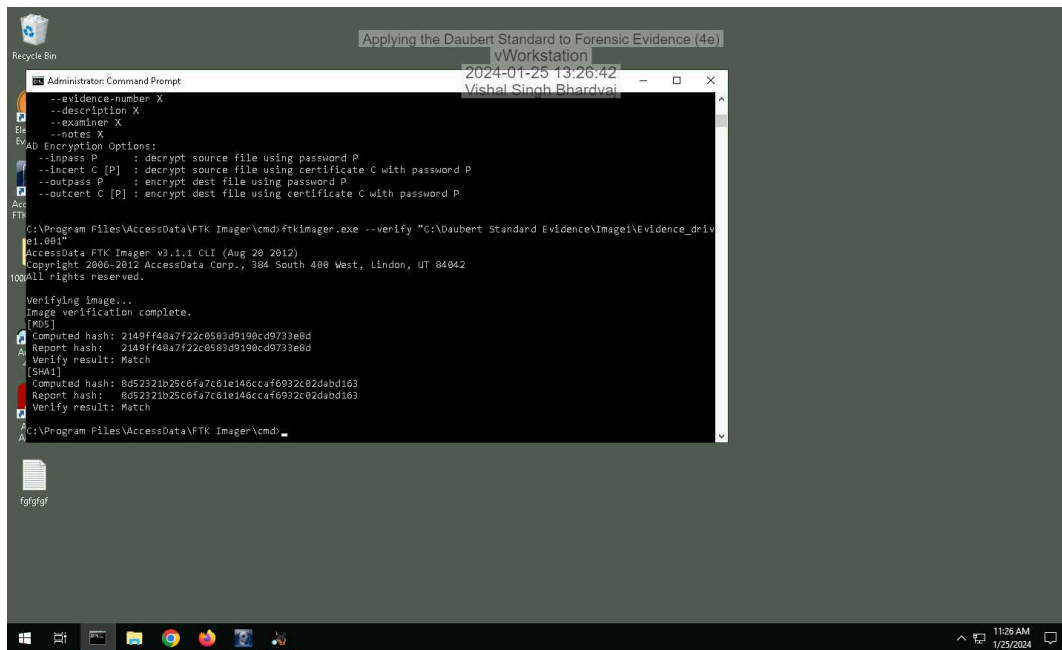
Hash value generated by FTK,E3 and Autopsy are exactly the same except that edited email file hash value is different.



### Section 3: Challenge and Analysis

#### Part 1: Verify Hash Codes on the Command Line

Make a screen capture showing the hash values for the Evidence\_drive1.001 file.



#### Part 2: Locate Additional Evidence

Define the original file names and file paths for each of the three files.

\$R354ELH.xlsx - location- G:\VIP Infor\; file name - 2021DrugSales.xlsx

\$RBQEOTL.doc - location - G:\Students\; file name - manual-testing-fresher-resume-1.doc

\$RX3177E.pdf - location G:\Work Doc\; file name - hr letter for visa.pdf