

Applying the Daubert Standard to Forensic Evidence (4e)

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

Student:

Alexis Cherpes

Email:

cherpea@ferris.edu

Time on Task:

2 hours, 33 minutes

Progress:

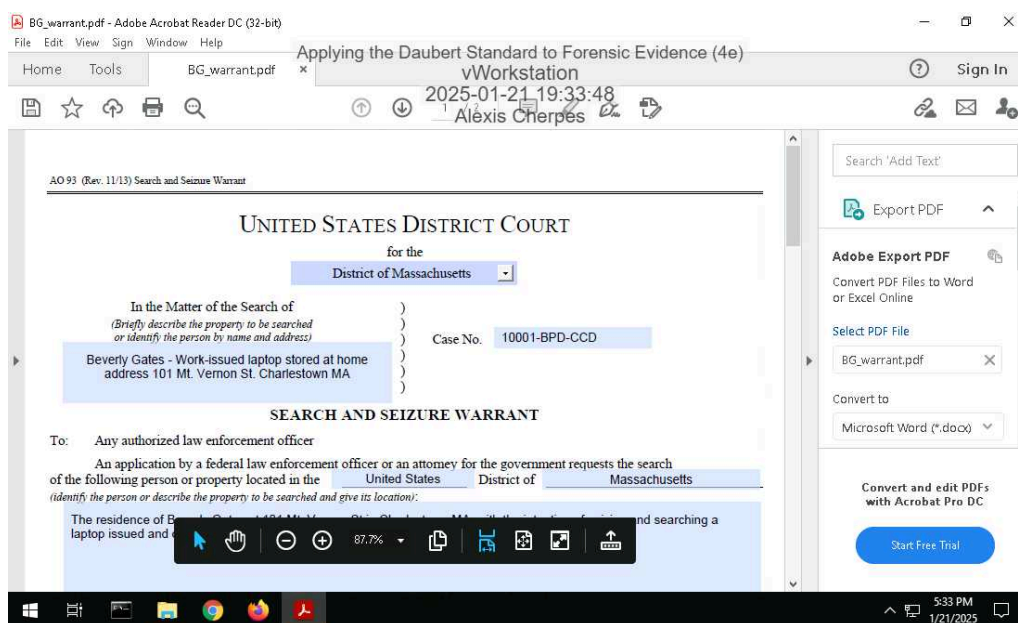
100%

Report Generated: Thursday, May 22, 2025 at 4:46 PM

Section 1: Hands-On Demonstration

Part 1: Complete Chain of Custody Procedures

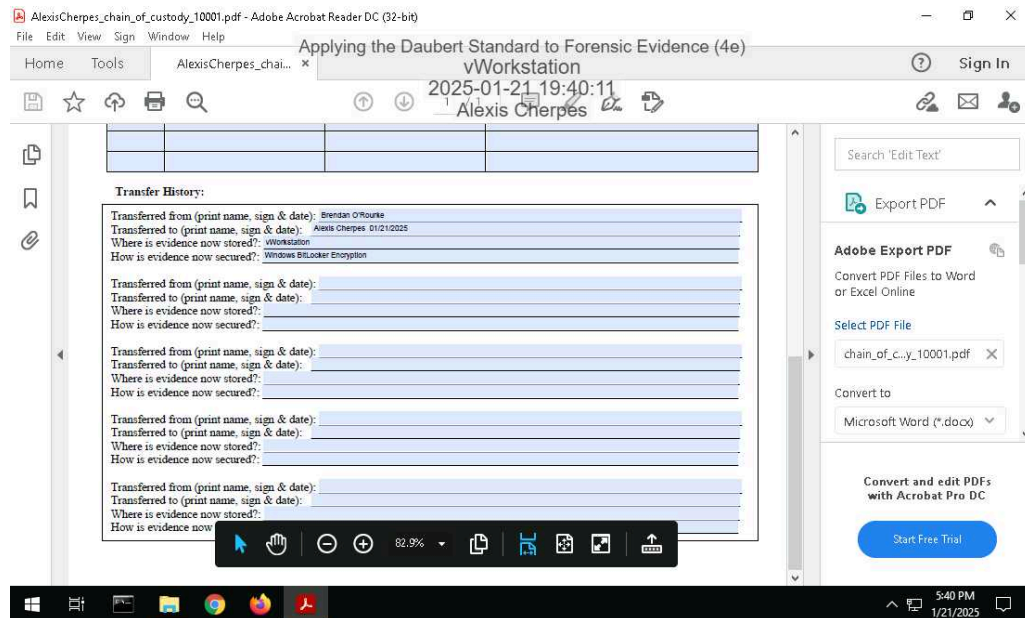
7. Make a screen capture showing the contents of the search warrant in Adobe Reader.



Applying the Daubert Standard to Forensic Evidence (4e)

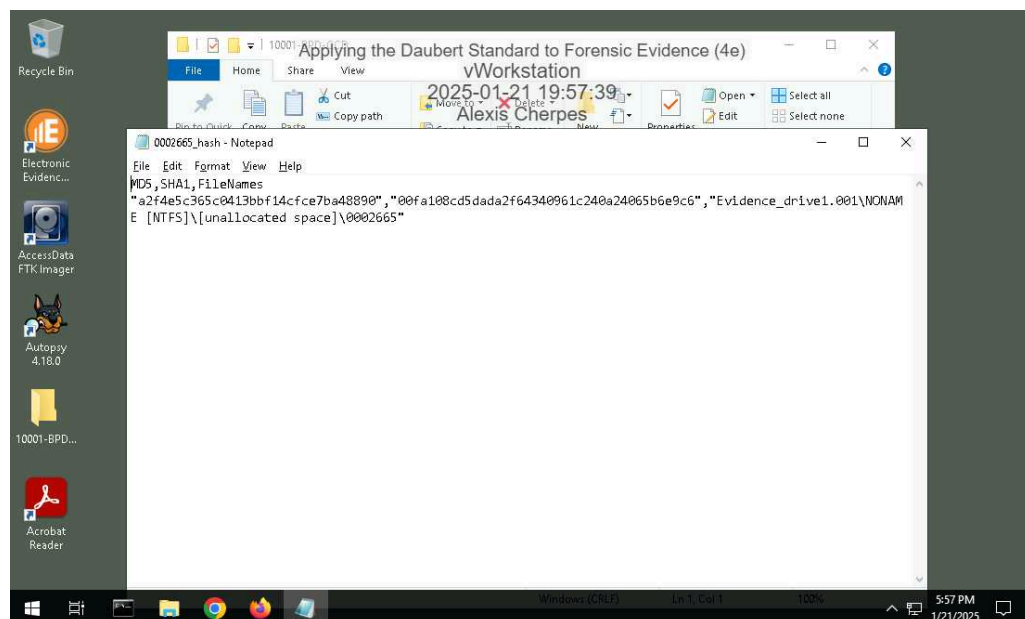
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

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

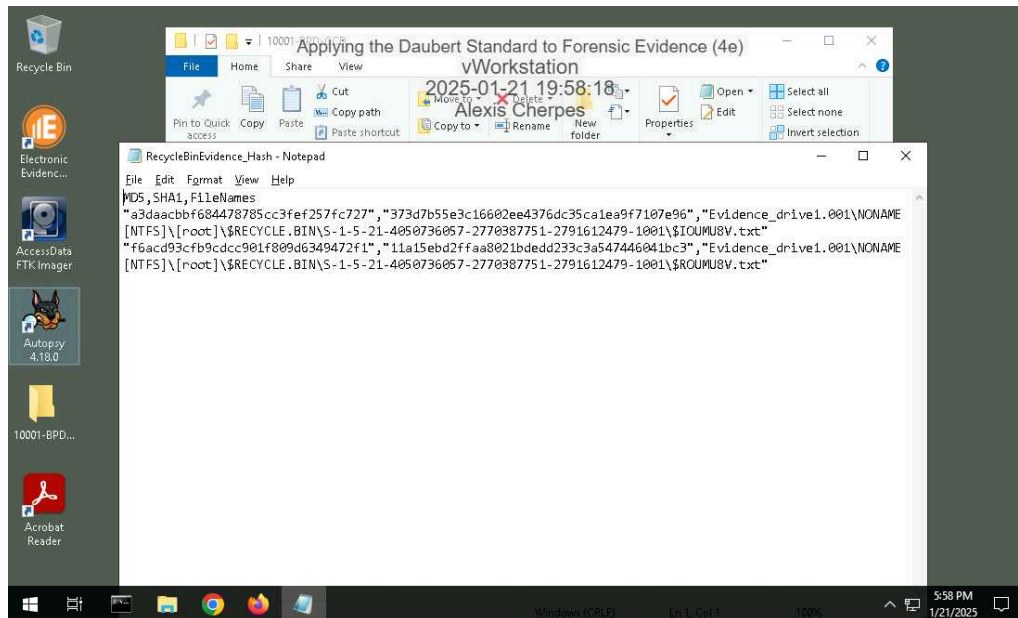
34. Make a screen capture showing the contents of the 0002665_hash.csv file.



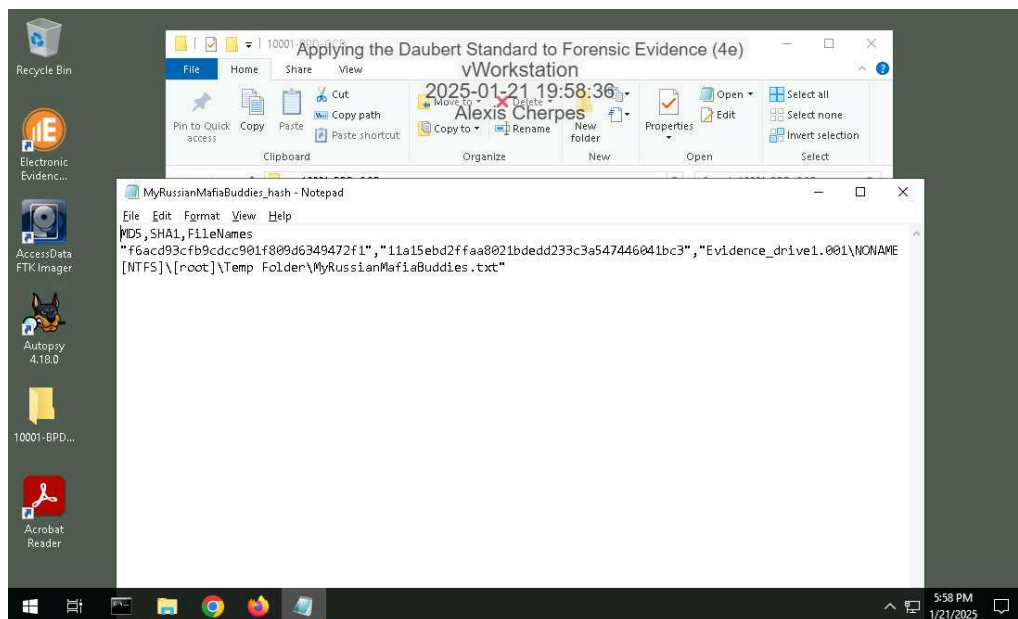
Applying the Daubert Standard to Forensic Evidence (4e)

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

37. Make a screen capture showing the contents of the RecycleBinEvidence_hash.csv file.



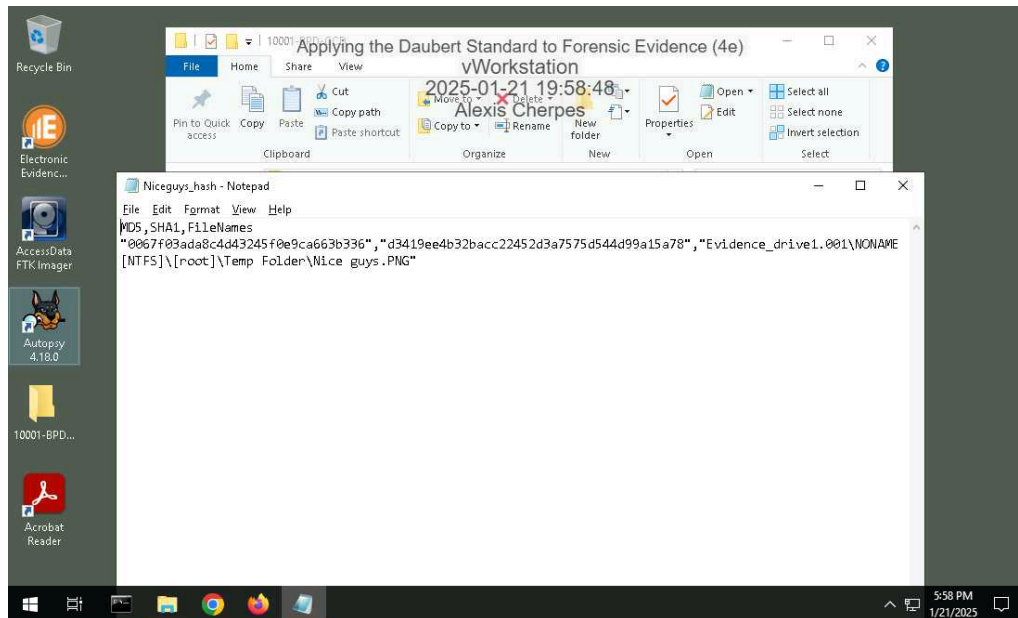
38. Make a screen capture showing the contents of the MyRussianMafiaBuddies_hash.csv file.



Applying the Daubert Standard to Forensic Evidence (4e)

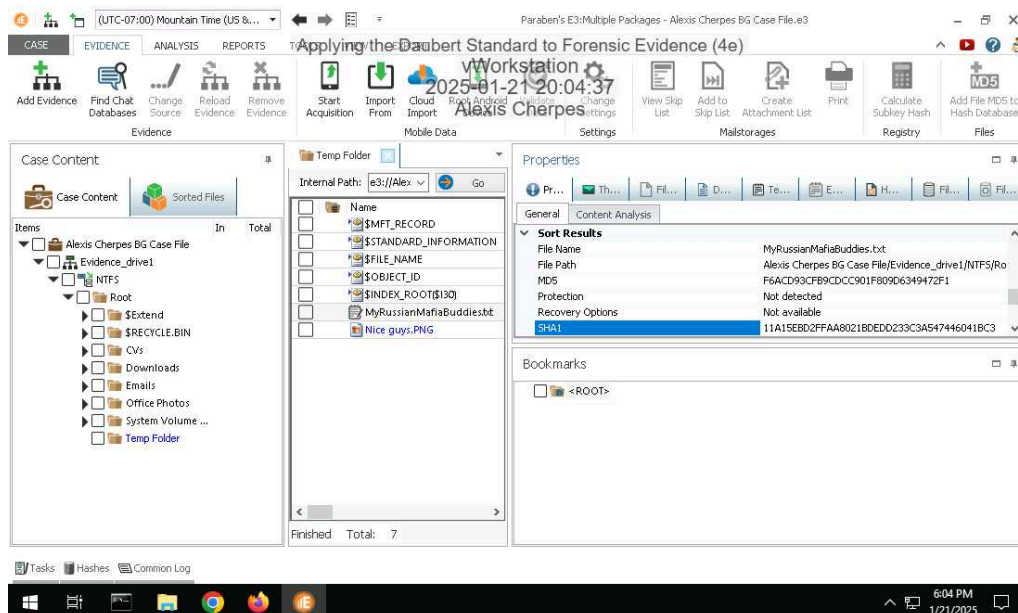
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

39. Make a screen capture showing the contents of the Nice guys_hash.csv file.

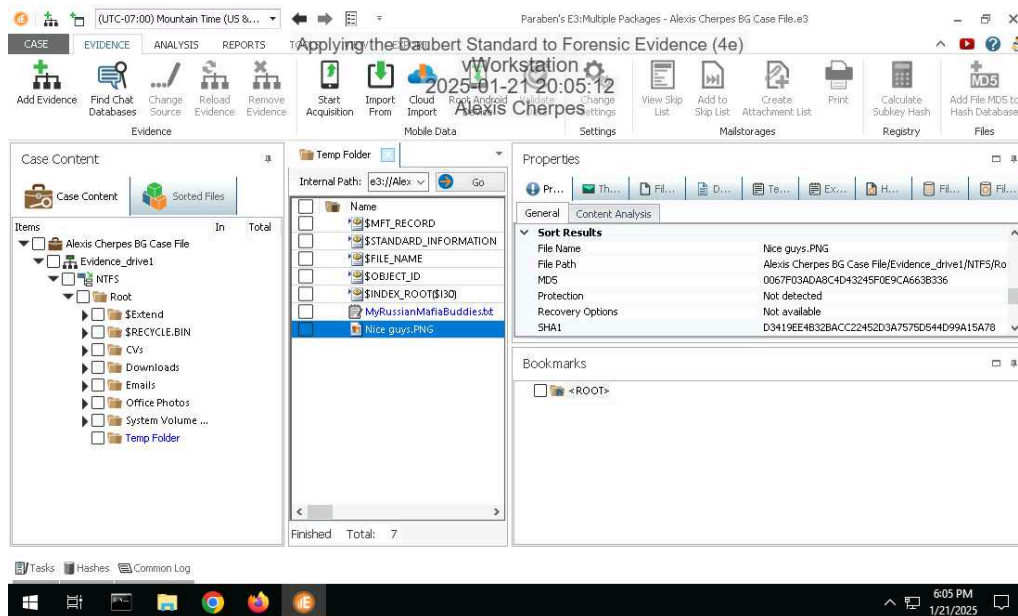


Part 3: Verify Hash Codes with E3

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.



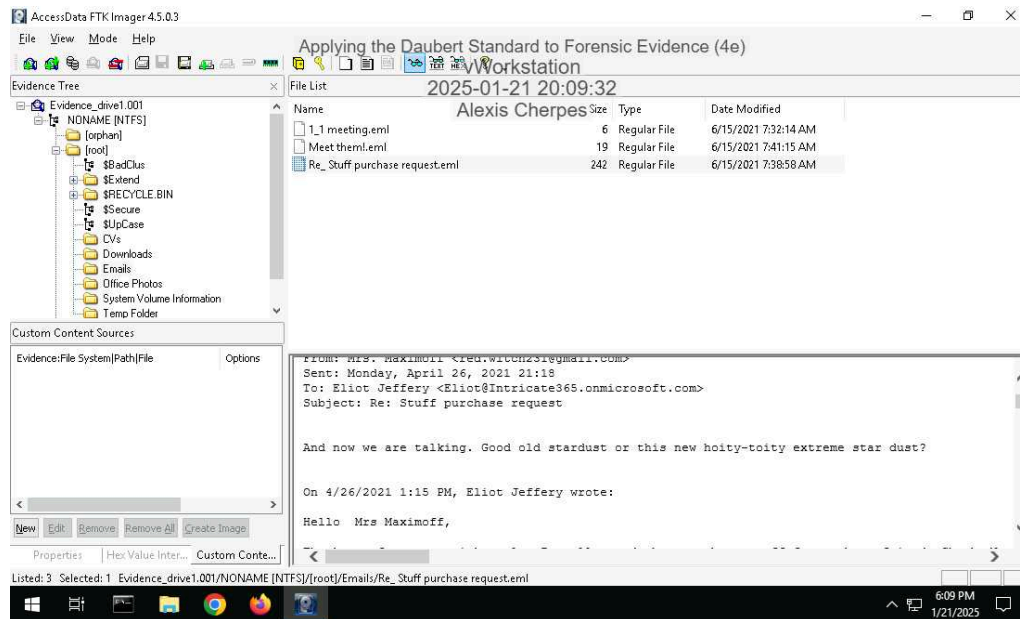
17. **Describe** how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

The hashes produced by E3 are the same as the ones that were produced by FTK.

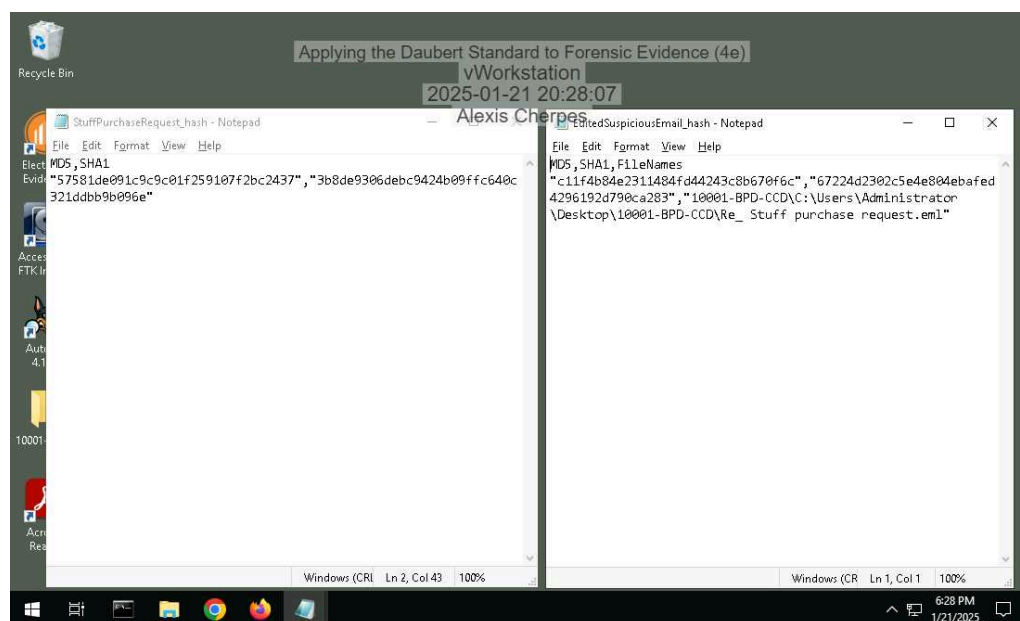
Section 2: Applied Learning

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.

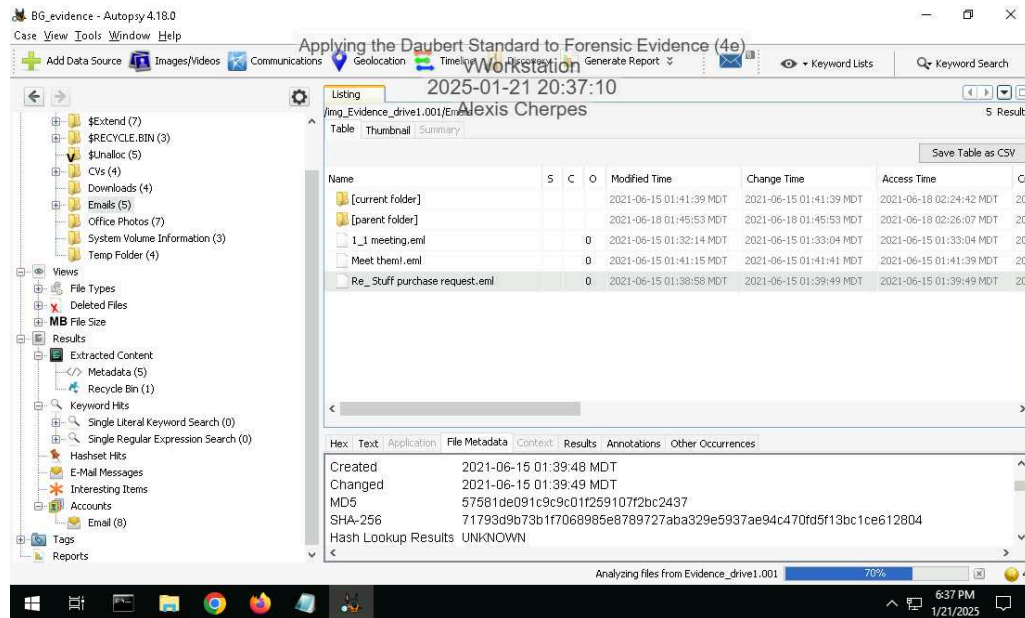


Part 2: Verify Hash Codes with Autopsy

Applying the Daubert Standard to Forensic Evidence (4e)

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

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

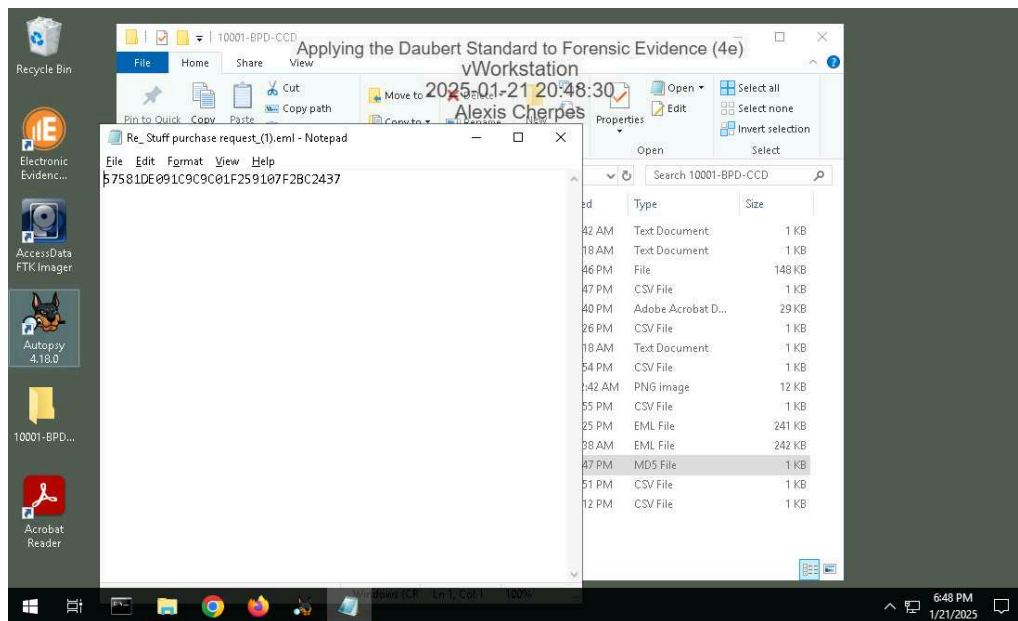


12. Describe how the hash value produced by Autopsy compares to the values produced by FTK Imager for the two .eml files.

They are the same.

Part 3: Verify Hash Codes with E3

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



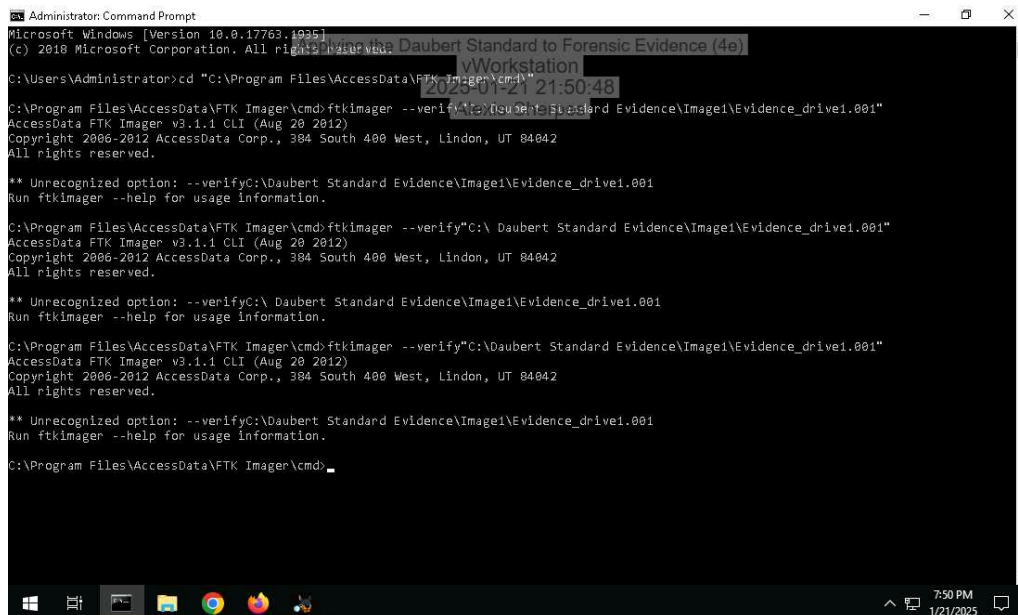
8. Describe how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

They all produced the same hash value but this time it only showed me the MD5 hash value

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.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\AccessData\FTK Imager\cmd"

C:\Program Files\AccessData\FTK Imager\cmd>ftkimager --verify"C:\Daubert Standard Evidence\Image1\Evidence_drive1.001"
AccessData FTK Imager v3.1.1 CLI (Aug 20 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

** Unrecognized option: --verifyC:\Daubert Standard Evidence\Image1\Evidence_drive1.001
Run ftkimager --help for usage information.

C:\Program Files\AccessData\FTK Imager\cmd>ftkimager --verify"C:\ Daubert Standard Evidence\Image1\Evidence_drive1.001"
AccessData FTK Imager v3.1.1 CLI (Aug 20 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

** Unrecognized option: --verifyC:\ Daubert Standard Evidence\Image1\Evidence_drive1.001
Run ftkimager --help for usage information.

C:\Program Files\AccessData\FTK Imager\cmd>ftkimager --verify"C:\Daubert Standard Evidence\Image1\Evidence_drive1.001"
AccessData FTK Imager v3.1.1 CLI (Aug 20 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

** Unrecognized option: --verifyC:\Daubert Standard Evidence\Image1\Evidence_drive1.001
Run ftkimager --help for usage information.

C:\Program Files\AccessData\FTK Imager\cmd>
```

Part 2: Locate Additional Evidence

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