

Applying the Daubert Standard to Forensic Evidence (4e)

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

Student:

Jake Simpson

Email:

jaksimps@iu.edu

Time on Task:

1 hour, 26 minutes

Progress:

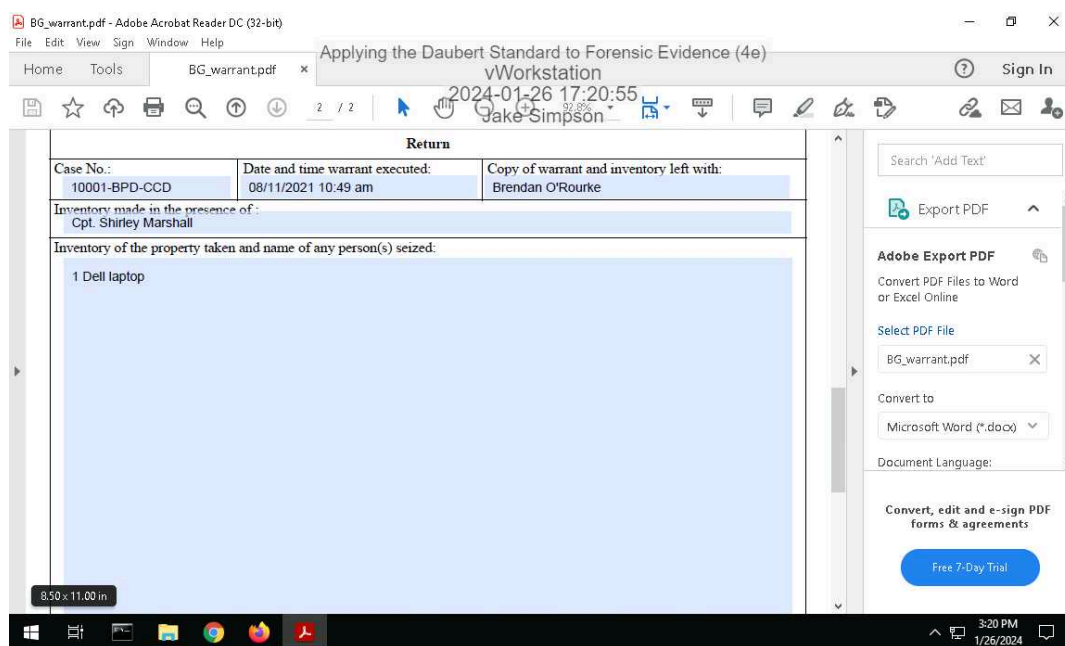
100%

Report Generated: Friday, January 26, 2024 at 6:39 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.

The screenshot shows the Adobe Acrobat Reader interface with a document titled "JakeSimpson_chain_of_custody_10001.pdf". The form is titled "Applying the Daubert Standard to Forensic Evidence (4e)" and includes a "vWorkstation" watermark. The form is filled out with the following information:

- How is evidence initially secured?: Windows BitLocker Encryption
- Collector signature: [Redacted] Date: April 20, 2021
- Copy History table:

Date	Copied By	Copy Method	Disposition of original and all copies

- Transfer History:

Transferred from (print name, sign & date):	Brendan O'Rourke
Transferred to (print name, sign & date):	Jake Simpson 01/25/2024
Where is evidence now stored?:	vWorkstation
How is evidence now secured?:	Windows BitLocker Encryption
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?:	
How is evidence now secured?:	
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?:	
How is evidence now secured?:	
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?:	
How is evidence now secured?:	

The right sidebar shows the "Export PDF" panel with options to convert the PDF to Word or Excel Online. The document language is set to English.

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.

The screenshot shows a Notepad window titled "0002665_hash - Notepad" with the following content:

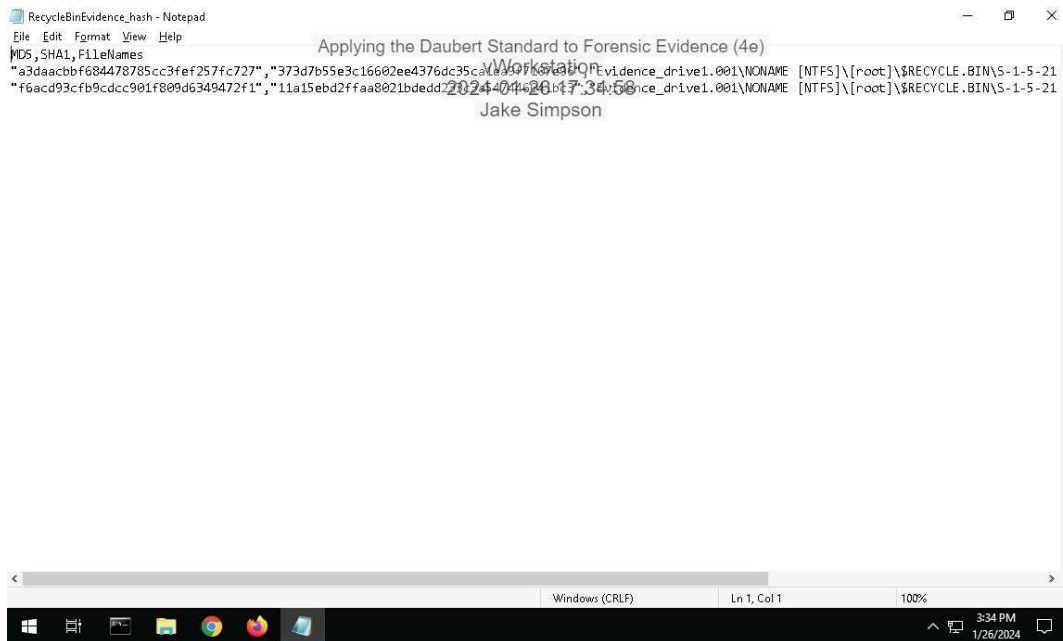
```
MD5,SHA1,FileNames
"a2f4e5c365c0413bbf14cfce7ba48890", "00fa108cd5dada2f64340961c24d4\Workstation\Evidence_drive1.001\NONAME [NTFS]\[unallocated space]\0002665"
```

The Notepad window is overlaid on the Adobe Acrobat Reader window, which is still visible in the background.

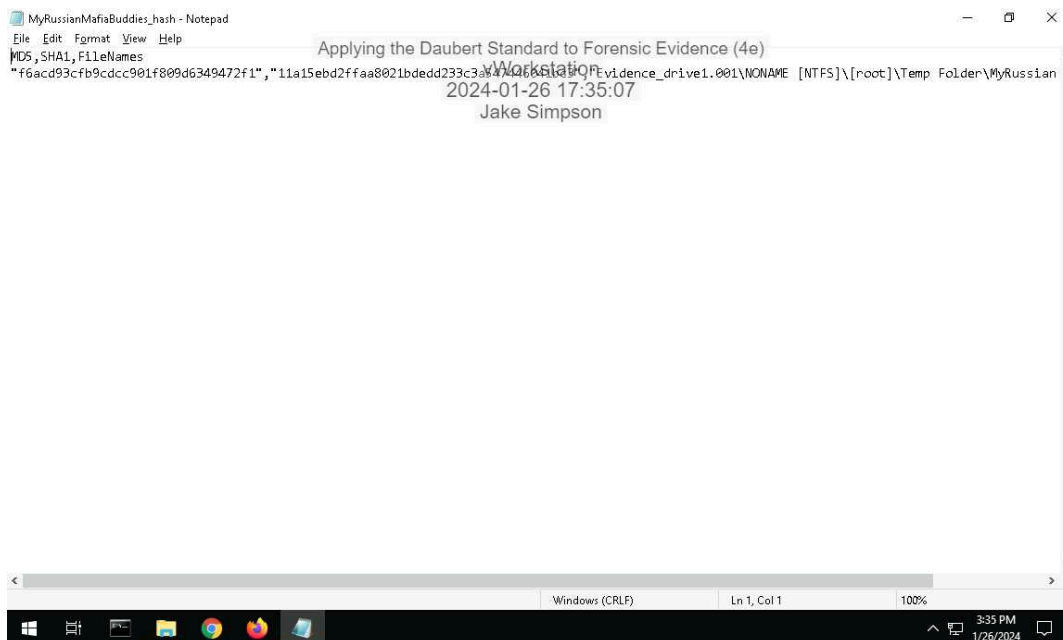
Applying the Daubert Standard to Forensic Evidence (4e)

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.

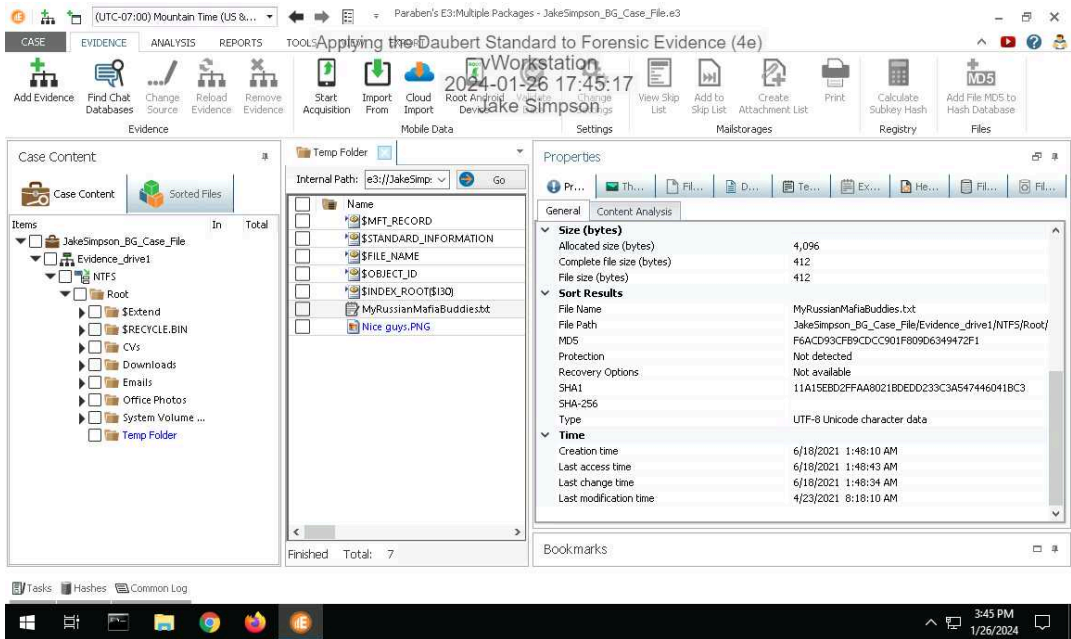


39. Make a screen capture showing the contents of the Nice guys_hash.csv file.

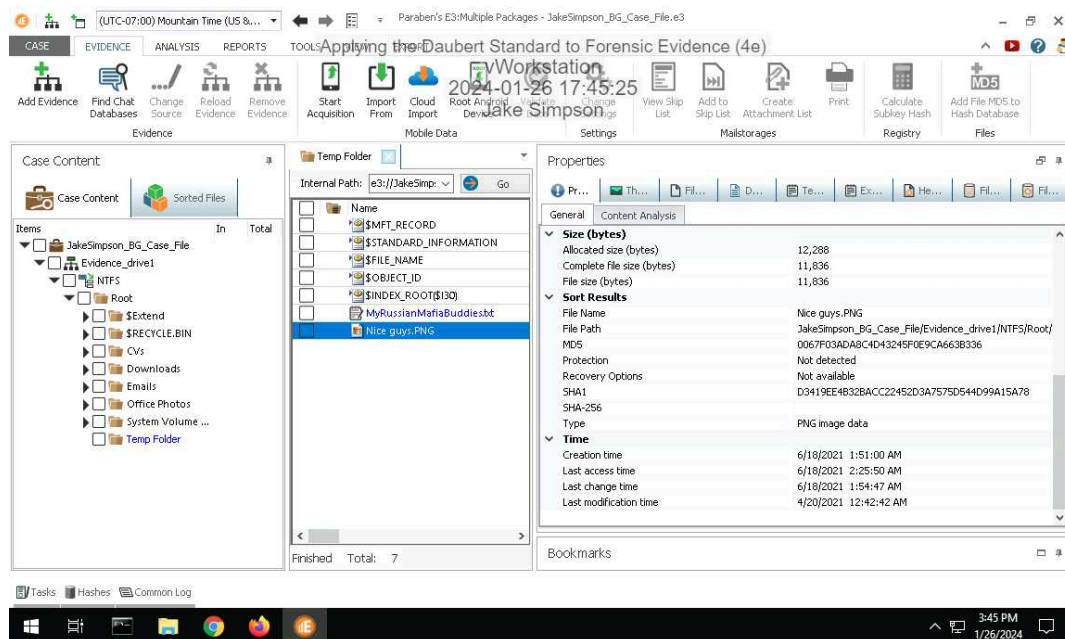


Part 3: Verify Hash Codes with E3

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.



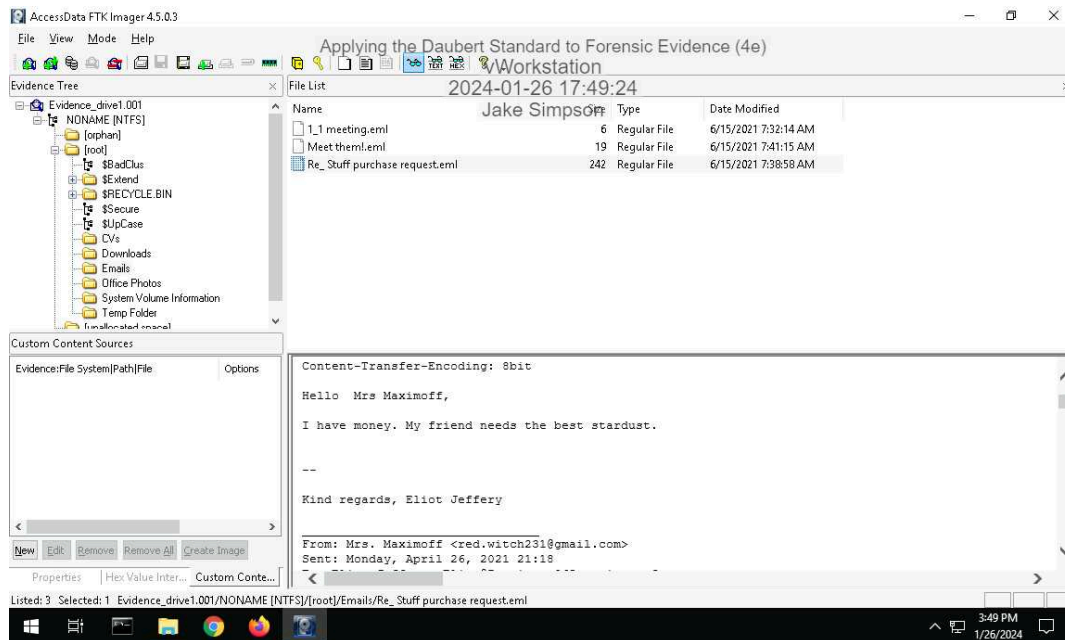
17. Describe how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

Comparing the hash values displayed in E3 and the values we created in FTK we can see that the MD5 and SHA1 values match. This is good news because it shows data integrity that they are the same file.

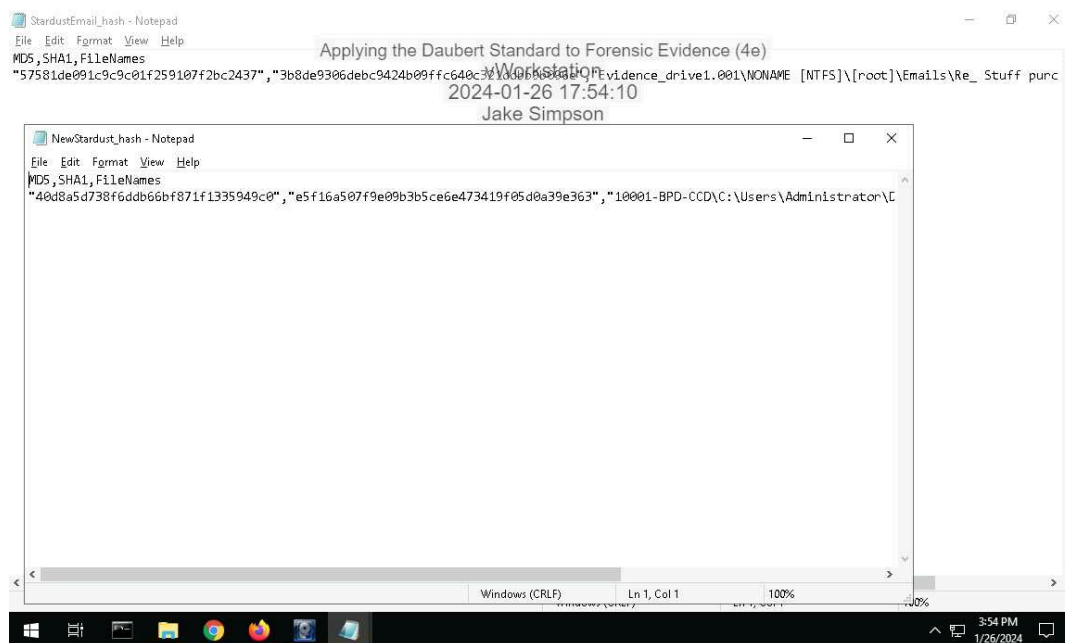
Section 2: Applied Learning

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.

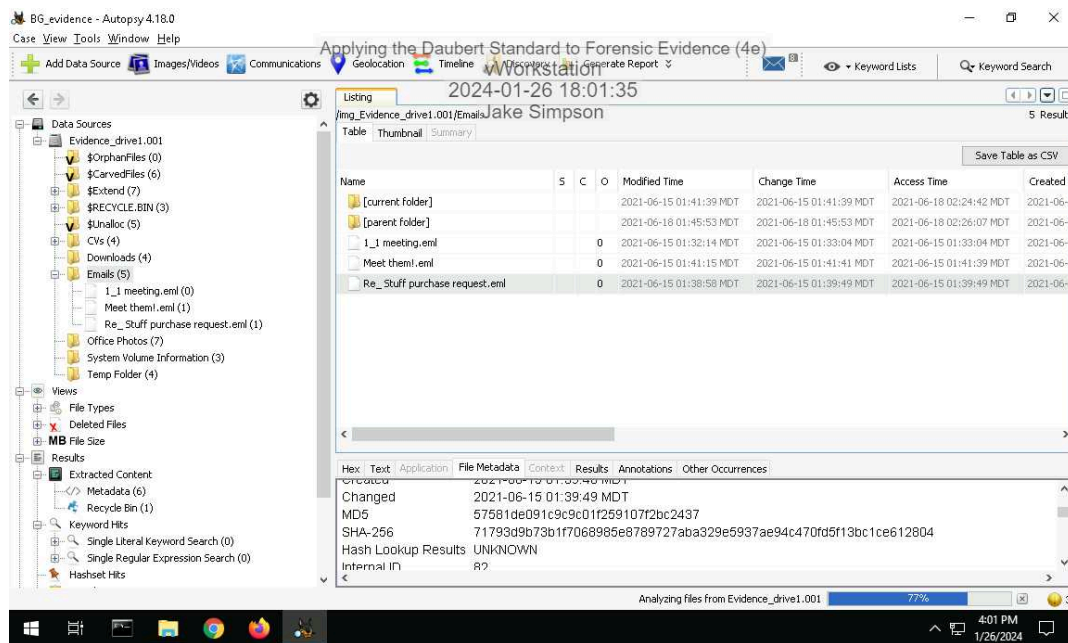


16. Make a screen capture showing the two hash values for the suspicious email file.



Part 2: Verify Hash Codes with Autopsy

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

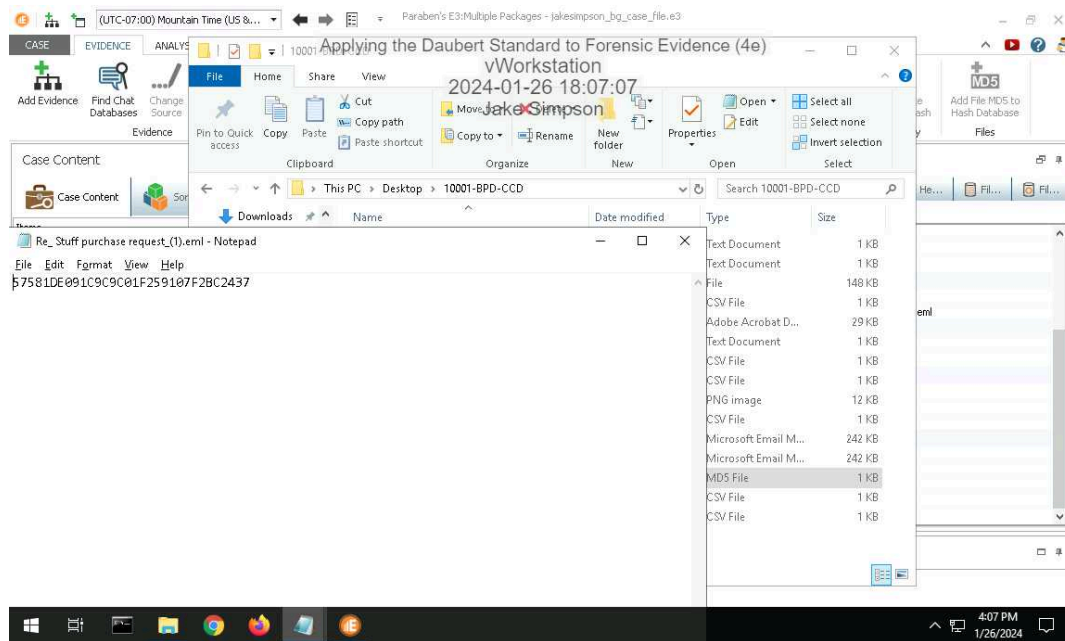


12. Describe how the hash value produced by Autopsy compares to the values produced by FTK Imager for the two .eml files.

The MD5 hash created by Autopsy matches the original hash that was created using FTK. This shows the data integrity of that email as both hashes produced by different tools match. This shows that the data hasn't changed and that they are the same. You can see what happens if there is a change in the data because the hashes won't match much like how the Autopsy hash and the second hash created by FTK after we altered the file don't.

Part 3: Verify Hash Codes with E3

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



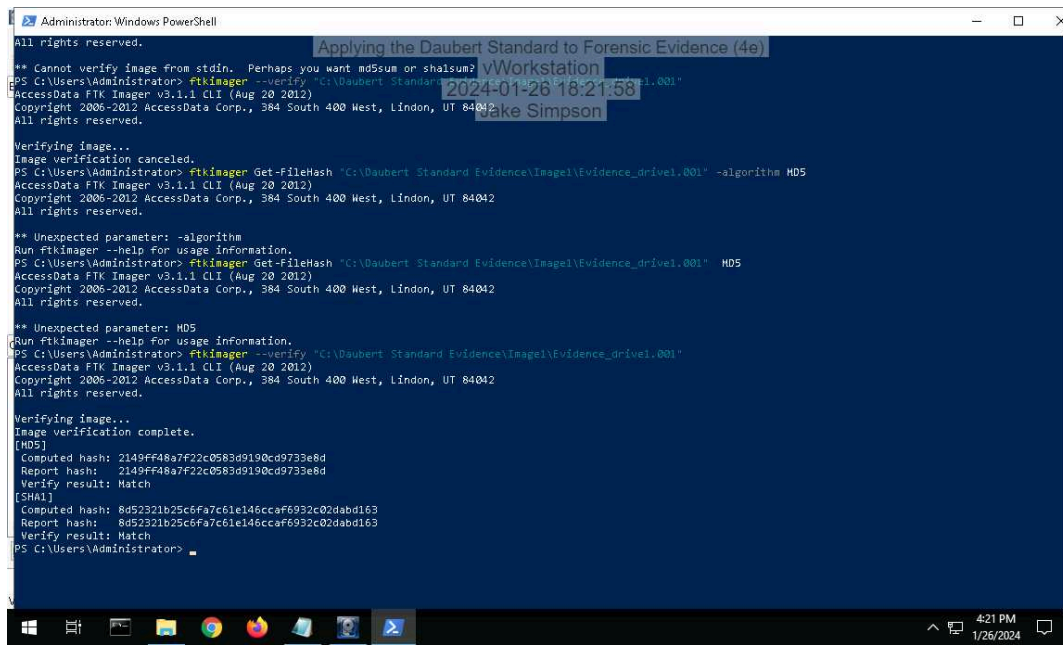
8. Describe how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

The MD5 hash produced by E3 matches the Autopsy MD5 hash and the first FTK hash which makes sense because they are hashing the same file. You can see the altered file's hash is the only one that doesn't match.

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 Windows PowerShell
All rights reserved.

** Cannot verify image from stdin. Perhaps you want md5sum or sha1sum?
PS C:\Users\Administrator> ftkimager --verify "C:\Daubert Standard Evidence\Imagel\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.

Verifying image...
Image verification canceled.
PS C:\Users\Administrator> ftkimager Get-FileHash "C:\Daubert Standard Evidence\Imagel\Evidence_drive1.001" -algorithm MD5
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.

** Unexpected parameter: -algorithm
Run ftkimager --help for usage information.
PS C:\Users\Administrator> ftkimager Get-FileHash "C:\Daubert Standard Evidence\Imagel\Evidence_drive1.001" MD5
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.

** Unexpected parameter: MD5
Run ftkimager --help for usage information.
PS C:\Users\Administrator> ftkimager --verify "C:\Daubert Standard Evidence\Imagel\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.

Verifying image...
Image verification complete.
[MD5]
Computed hash: 2149ff48a7f22c0583d9190cd9733e8d
Report hash: 2149ff48a7f22c0583d9190cd9733e8d
Verify result: Match
[SHA1]
Computed hash: 8d52321b25c6fa7c61e146ccaf6932c02dabd163
Report hash: 8d52321b25c6fa7c61e146ccaf6932c02dabd163
Verify result: Match
PS C:\Users\Administrator>
```

Part 2: Locate Additional Evidence

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

For \$R354ELH.xlsx, it was located at G:\VIP Info\ 2021DrigSales.xlsx

For \$RBQEOTL.doc, it was located at G:\ Students\manual_testing_fresher_resume_1.doc

For \$Fx3177E.pdf, it was located at G:\Work Doc\hr_letter_For_visa.pdf