Applying the Daubert Standard to Forensic Evidence (4e)

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

Student:	Email:
Karan Atul Vora	kxv230021@utdallas.edu

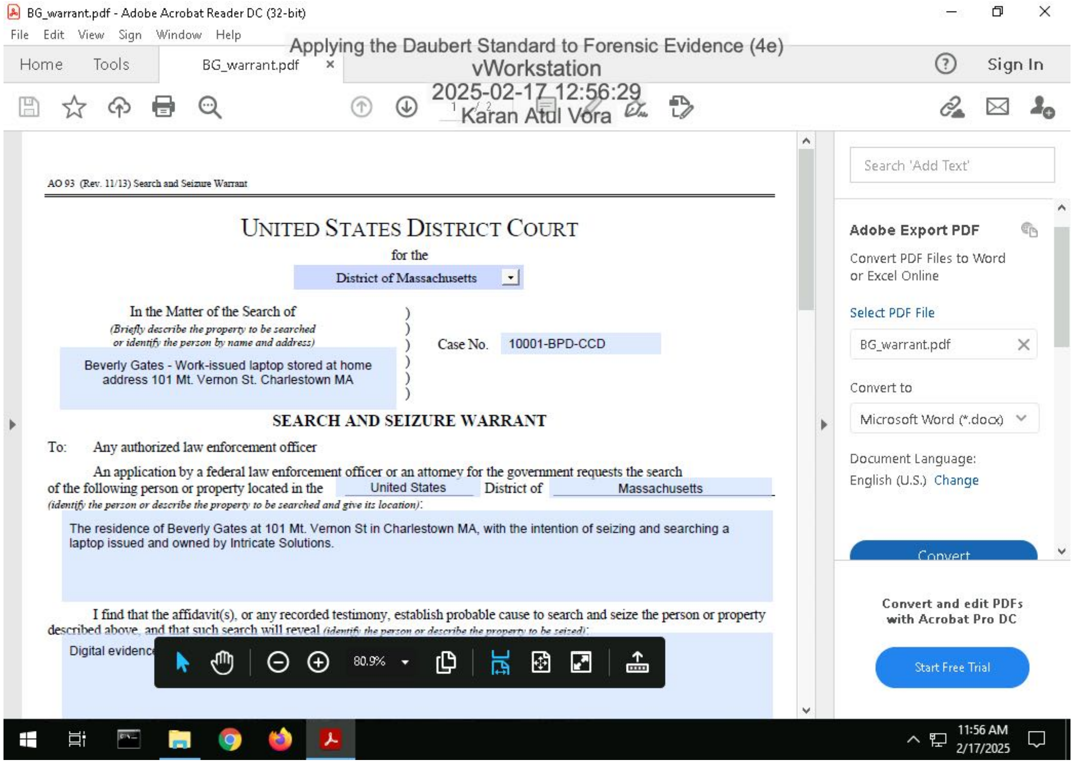
Time on Task:	Progress:
3 hours, 15 minutes	100%

Report Generated: Monday, February 24, 2025 at 4:32 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**.



BG_warrant.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools BG_warrant.pdf
Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 12:56:29
Karan Atul Vora
Sign In
Search 'Add Text'
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
BG_warrant.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert
Convert and edit PDFs with Acrobat Pro DC
Start Free Trial
80.9%
11:56 AM
2/17/2025

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Beverly Gates - Work-issued laptop stored at home address 101 Mt. Vernon St. Charlestown MA

Case No. 10001-BPD-CCD

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

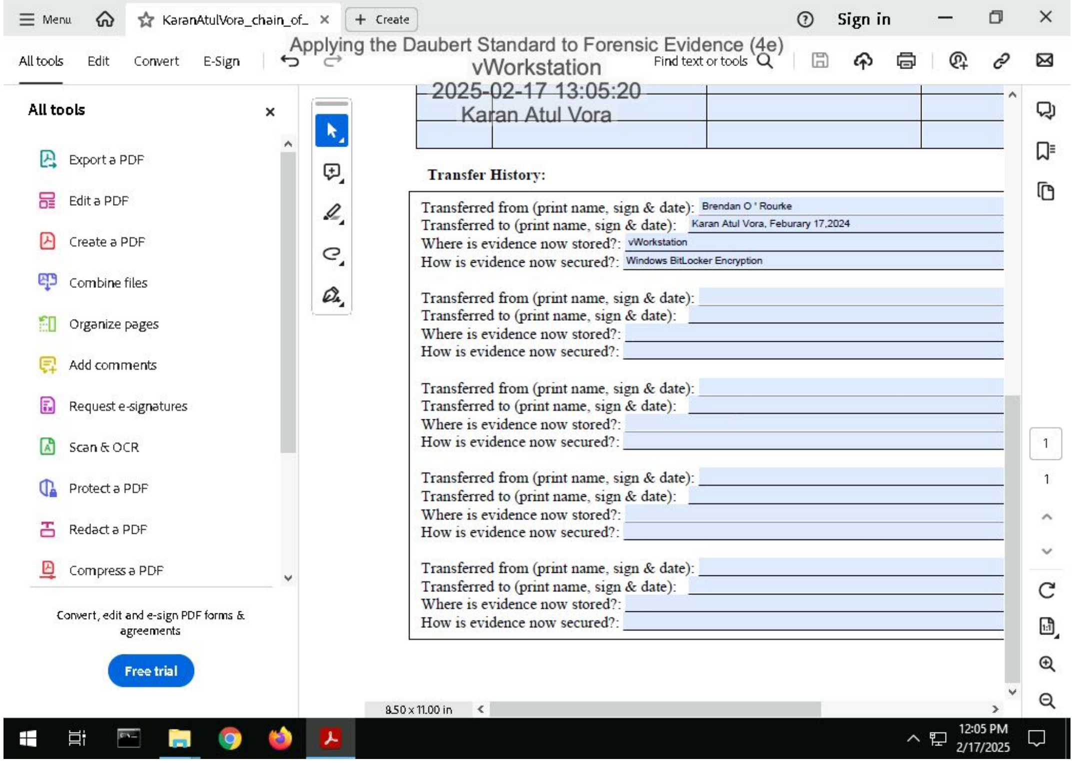
An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the United States District of Massachusetts *(identify the person or describe the property to be searched and give its location)*:

The residence of Beverly Gates at 101 Mt. Vernon St in Charlestown MA, with the intention of seizing and searching a laptop issued and owned by Intricate Solutions.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Digital evidenc

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 13:05:20
Karan Atul Vora

Transfer History:

Transferred from (print name, sign & date): Brendan O ' Rourke
Transferred to (print name, sign & date): Karan Atul Vora, Feburary 17,2024
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?:

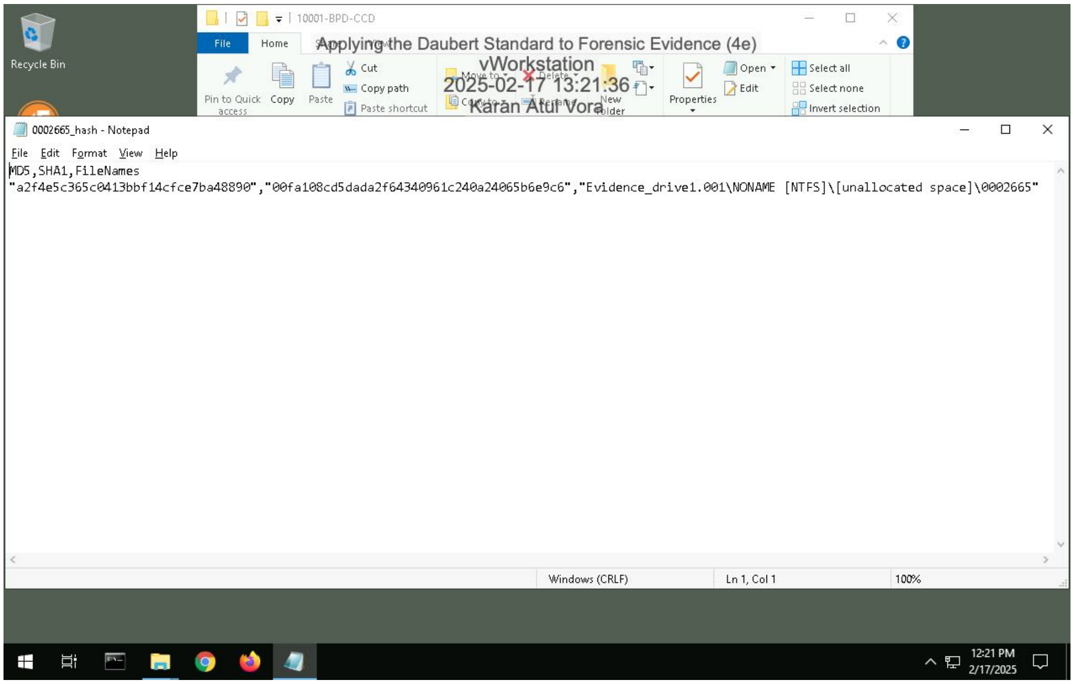
Transferred from (print name, sign & date):
Transferred to (print name, sign & date):
Where is evidence now stored?:
How is evidence now secured?:

Transferred from (print name, sign & date):
Transferred to (print name, sign & date):
Where is evidence now stored?:
How is evidence now secured?:

Transferred from (print name, sign & date):
Transferred to (print name, sign & date):
Where is evidence now stored?:
How is evidence now secured?:

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

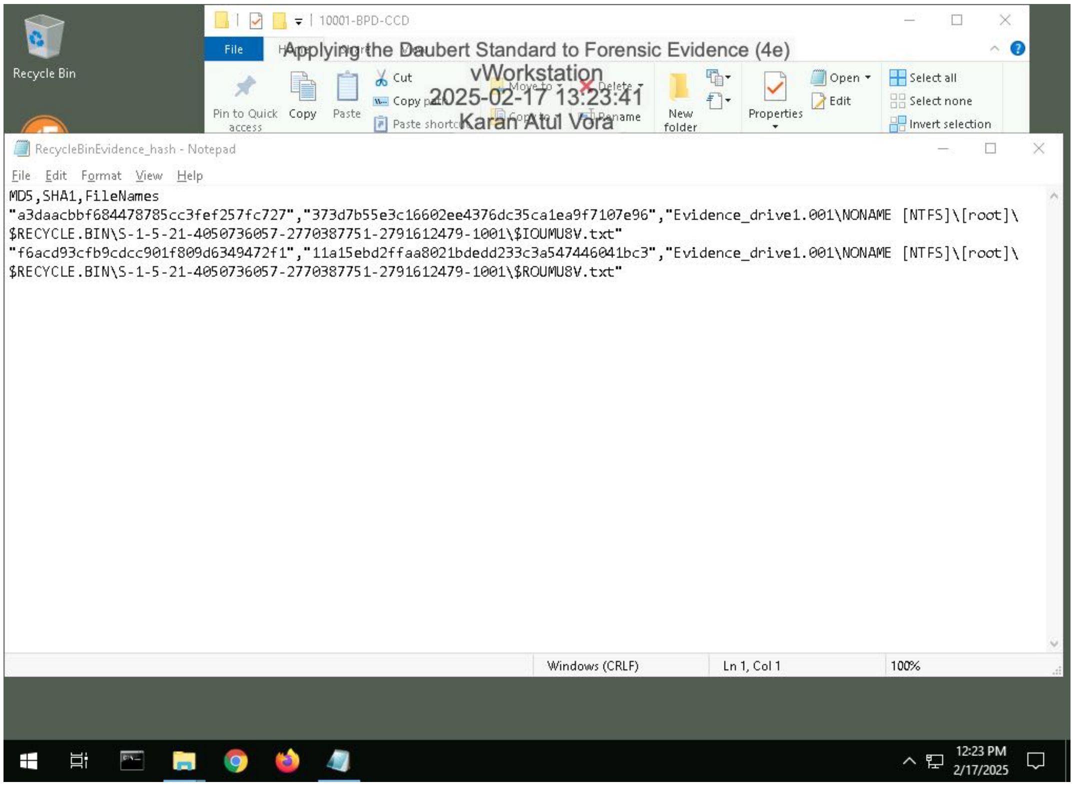
34. **Make a screen capture** showing the **contents of the 0002665_hash.csv file**.



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 13:21:36
Karan Atul Vora

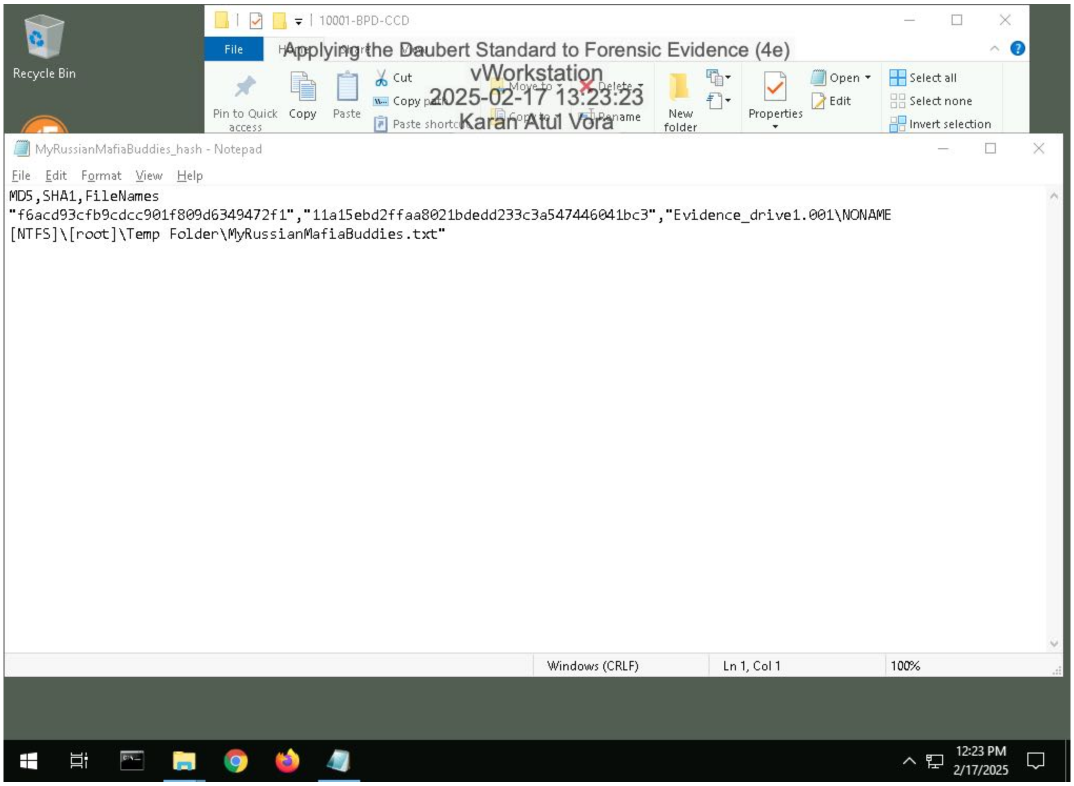
```
MD5,SHA1,FileNames
"a2f4e5c365c0413bbf14cfce7ba48890","00fa108cd5dada2f64340961c240a24065b6e9c6","Evidence_drive1.001\NONAME [NTFS]\[unallocated space]\0002665"
```

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



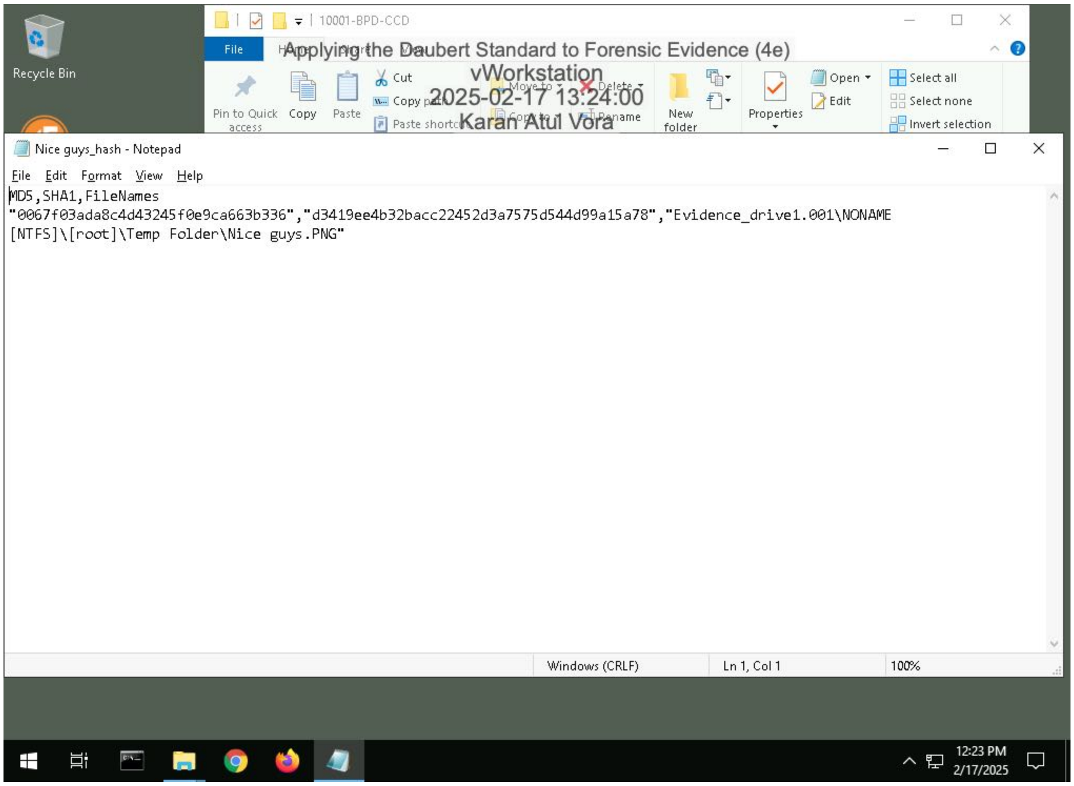
```
MD5,SHA1,FileNames
"a3daacbbf684478785cc3fef257fc727","373d7b55e3c16602ee4376dc35ca1ea9f7107e96","Evidence_drive1.001\NONAME [NTFS]\[root]\
$RECYCLE.BIN\S-1-5-21-4050736057-2770387751-2791612479-1001\$IOUMU8V.txt"
"f6acd93cfb9cdcc901f809d6349472f1","11a15ebd2ffaa8021bdedd233c3a547446041bc3","Evidence_drive1.001\NONAME [NTFS]\[root]\
$RECYCLE.BIN\S-1-5-21-4050736057-2770387751-2791612479-1001\$ROUMU8V.txt"
```

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



```
MD5,SHA1,FileNames
"f6acd93cfb9cdcc901f809d6349472f1","11a15ebd2ffaa8021bdedd233c3a547446041bc3","Evidence_drive1.001\NONAME
[NTFS]\[root]\Temp Folder\MyRussianMafiaBuddies.txt"
```

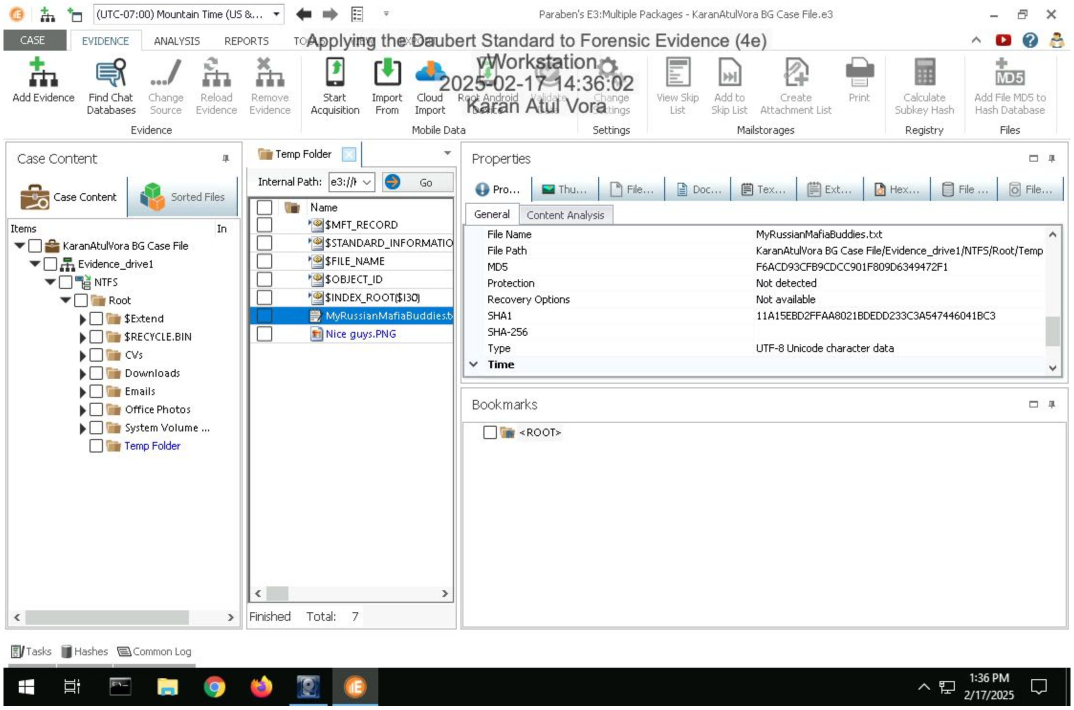
39. **Make a screen capture** showing the **contents of the Nice guys_hash.csv file**.



```
MD5,SHA1,FileNames
"0067f03ada8c4d43245f0e9ca663b336","d3419ee4b32bacc22452d3a7575d544d99a15a78","Evidence_drive1.001\NONAME
[NTFS]\[root]\Temp Folder\Nice guys.PNG"
```

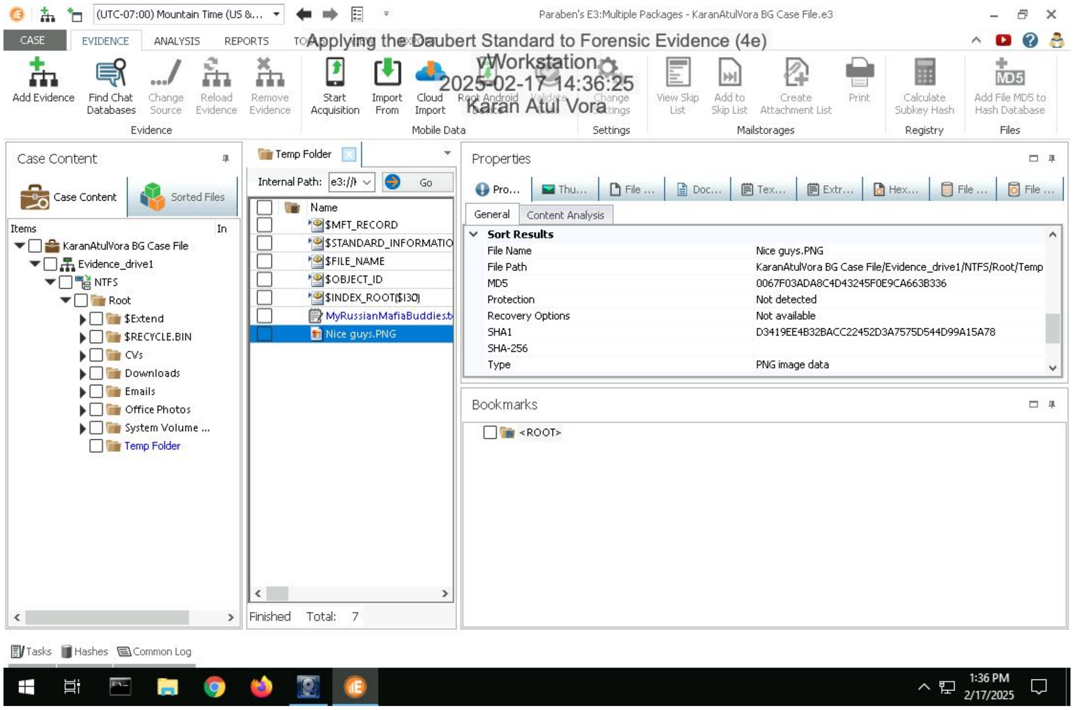
Part 3: Verify Hash Codes with E3

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



File Name	MyRussianMafiaBuddies.txt
File Path	KaranAtulVora BG Case File/Evidence_drive1/NTFS/Root/Temp
MD5	F6ACD93CFB9CDCC901F809D6349472F1
Protection	Not detected
Recovery Options	Not available
SHA1	11A15EBD2FFAA8021BDEDD233C3A547446041BC3
SHA-256	
Type	UTF-8 Unicode character data
Time	

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



Sort Results	
File Name	Nice guys.PNG
File Path	KaranAtulVora BG Case File/Evidence_drive1/NTFS/Root/Temp
MD5	0067F03ADA8C4D43245F0E9CA663B336
Protection	Not detected
Recovery Options	Not available
SHA1	D3419EE4B32BACC22452D3A7575D544D99A15A78
SHA-256	
Type	PNG image data

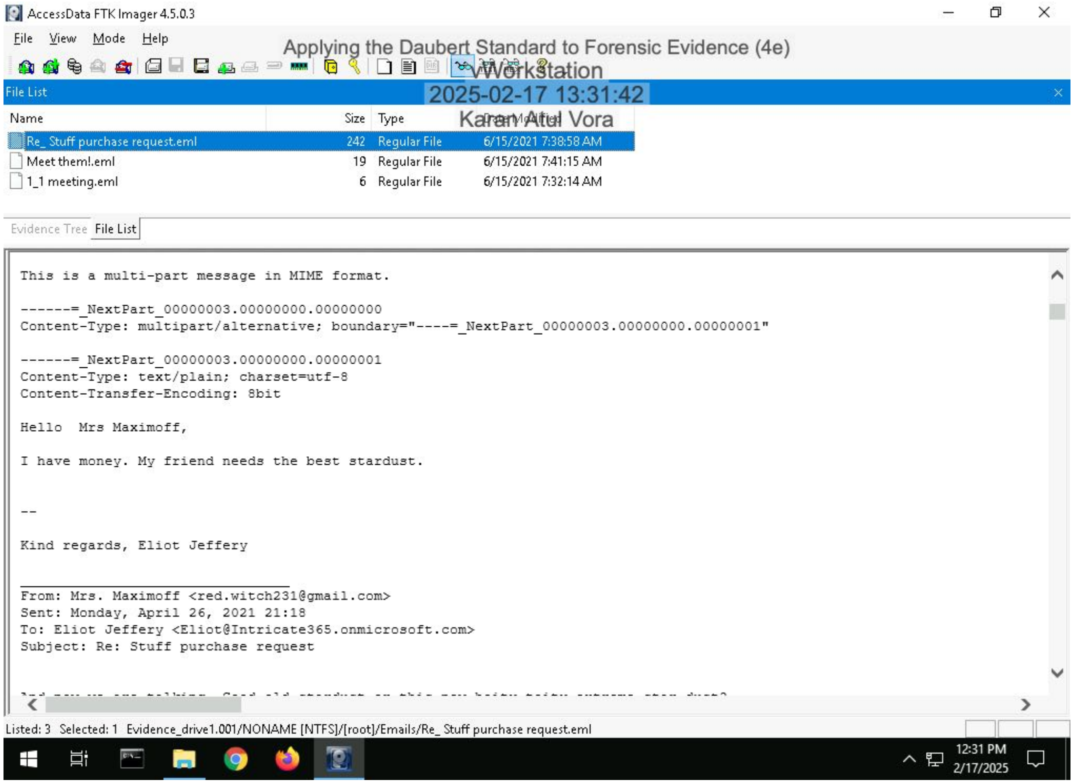
17. **Describe** how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

Both E3 and FTK use the cryptographic hash algorithm to produce hash. If the algorithm is same then the hash do match. i.e. MD5 from E3 matches with MD5 from 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**.

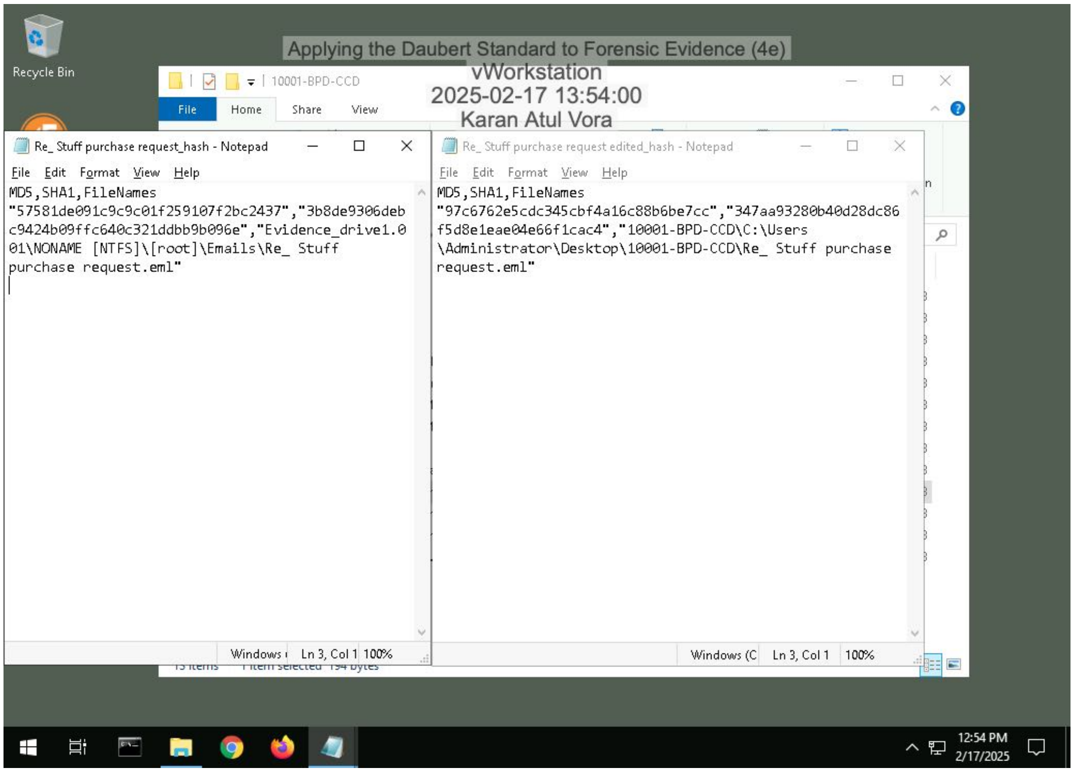


Name	Size	Type	Date Modified
Re_ Stuff purchase request.eml	242	Regular File	6/15/2021 7:38:58 AM
Meet them!.eml	19	Regular File	6/15/2021 7:41:15 AM
1_1 meeting.eml	6	Regular File	6/15/2021 7:32:14 AM

```
This is a multi-part message in MIME format.

------=_NextPart_00000003.00000000.00000000
Content-Type: multipart/alternative; boundary="----=_NextPart_00000003.00000000.00000001"

------=_NextPart_00000003.00000000.00000001
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit

Hello  Mrs Maximoff,

I have money. My friend needs the best stardust.


--

Kind regards, Eliot Jeffery


________________________________
From: Mrs. Maximoff <red.witch231@gmail.com>
Sent: Monday, April 26, 2021 21:18
To: Eliot Jeffery <Eliot@Intricate365.onmicrosoft.com>
Subject: Re: Stuff purchase request
```

Listed: 3 Selected: 1 Evidence_drive1.001/NONAME [NTFS]/[root]/Emails/Re_ Stuff purchase request.eml

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

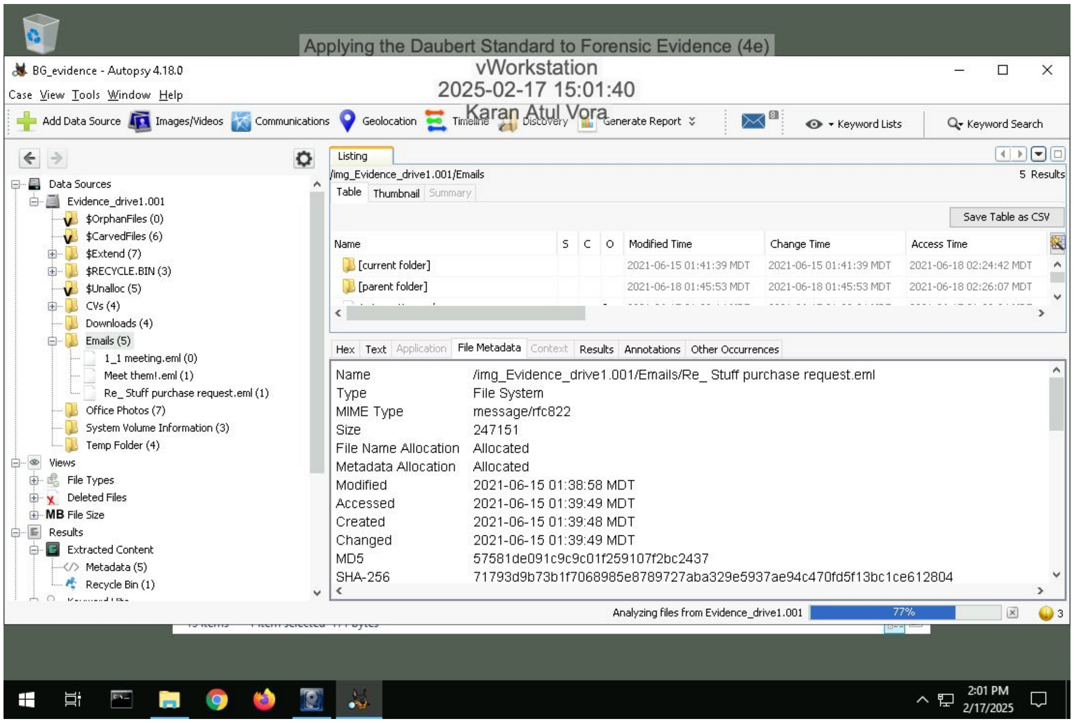

Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 13:54:00
Karan Atul Vora
Recycle Bin
10001-BPD-CCD
File
Home
Share
View
Re_ Stuff purchase request_hash - Notepad
Re_ Stuff purchase request edited_hash - Notepad
File Edit Format View Help
Windows (
Ln 3, Col 1
100%
12:54 PM
2/17/2025

```
MD5,SHA1,FileNames
"57581de091c9c9c01f259107f2bc2437","3b8de9306deb
c9424b09ffc640c321ddbb9b096e","Evidence_drive1.0
01\NONAME [NTFS]\[root]\Emails\Re_ Stuff
purchase request.eml"
```

```
MD5,SHA1,FileNames
"97c6762e5cdc345cbf4a16c88b6be7cc","347aa93280b40d28dc86
f5d8e1eae04e66f1cac4","10001-BPD-CCD\C:\Users
\Administrator\Desktop\10001-BPD-CCD\Re_ Stuff purchase
request.eml"
```

Part 2: Verify Hash Codes with Autopsy

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 15:01:40
Karan Atul Vora

/img_Evidence_drive1.001/Emails
5 Results

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2021-06-15 01:41:39 MDT	2021-06-15 01:41:39 MDT	2021-06-18 02:24:42 MDT
[parent folder]				2021-06-18 01:45:53 MDT	2021-06-18 01:45:53 MDT	2021-06-18 02:26:07 MDT

Name	/img_Evidence_drive1.001/Emails/Re_ Stuff purchase request.eml
Type	File System
MIME Type	message/rfc822
Size	247151
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2021-06-15 01:38:58 MDT
Accessed	2021-06-15 01:39:49 MDT
Created	2021-06-15 01:39:48 MDT
Changed	2021-06-15 01:39:49 MDT
MD5	57581de091c9c9c01f259107f2bc2437
SHA-256	71793d9b73b1f7068985e8789727aba329e5937ae94c470fd5f13bc1ce612804

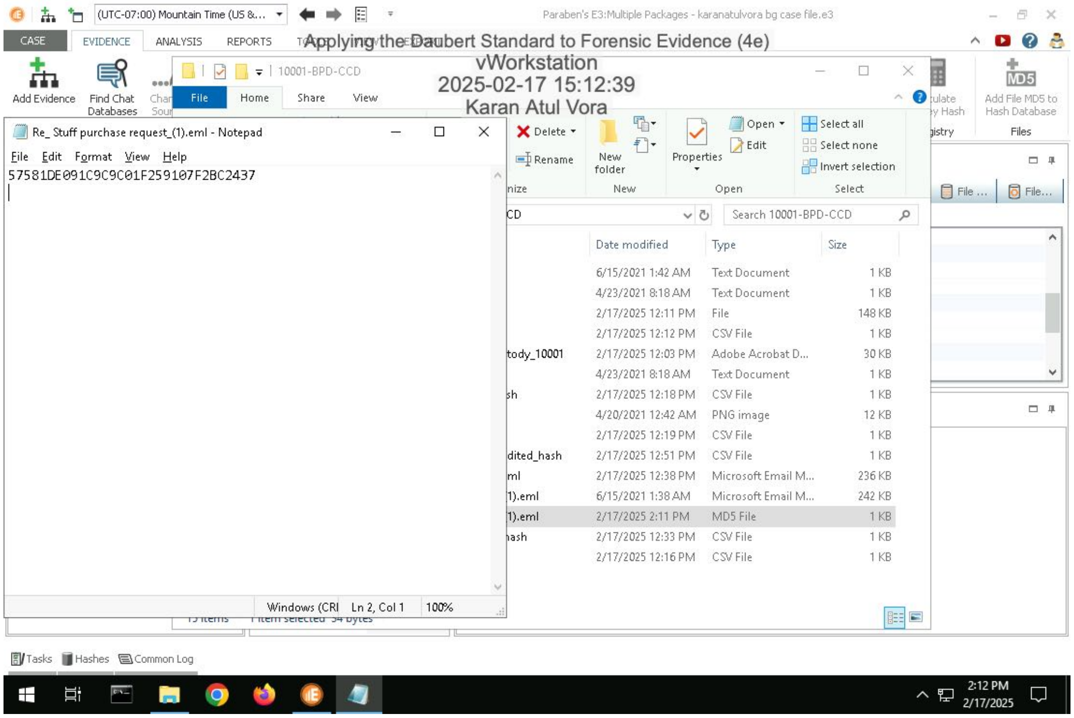
Analyzing files from Evidence_drive1.001 77%

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

the hash values produced in Autopsy do match with the hash produced by FTK

Part 3: Verify Hash Codes with E3

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 15:12:39
Karan Atul Vora

Re_ Stuff purchase request_(1).eml - Notepad

```
57581DE091C9C9C01F259107F2BC2437
```

	Date modified	Type	Size
	6/15/2021 1:42 AM	Text Document	1 KB
	4/23/2021 8:18 AM	Text Document	1 KB
	2/17/2025 12:11 PM	File	148 KB
	2/17/2025 12:12 PM	CSV File	1 KB
tody_10001	2/17/2025 12:03 PM	Adobe Acrobat D...	30 KB
	4/23/2021 8:18 AM	Text Document	1 KB
sh	2/17/2025 12:18 PM	CSV File	1 KB
	4/20/2021 12:42 AM	PNG image	12 KB
	2/17/2025 12:19 PM	CSV File	1 KB
dited_hash	2/17/2025 12:51 PM	CSV File	1 KB
ml	2/17/2025 12:38 PM	Microsoft Email M...	236 KB
1).eml	6/15/2021 1:38 AM	Microsoft Email M...	242 KB
1).eml	2/17/2025 2:11 PM	MD5 File	1 KB
hash	2/17/2025 12:33 PM	CSV File	1 KB
	2/17/2025 12:16 PM	CSV File	1 KB

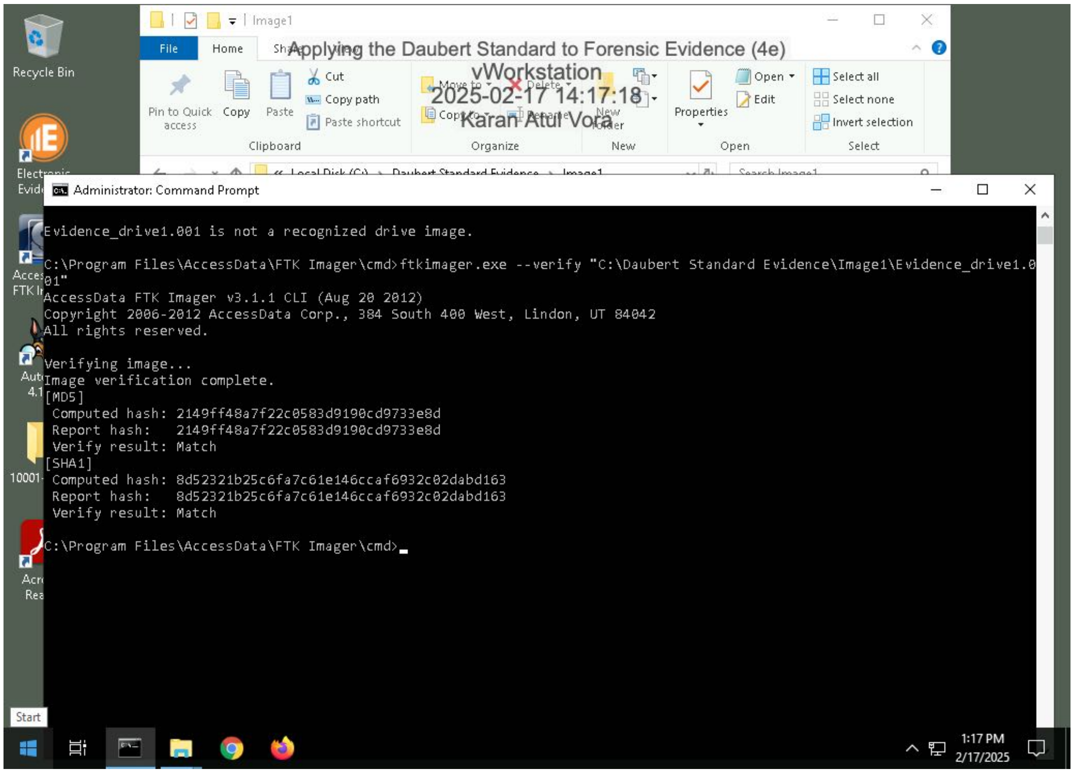
8. **Describe** how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

the hash generated by E3, FTK Imager and Autopsy are same. i.e. they do 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**.



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-02-17 14:17:18
Karan Atul Vora

```
Evidence_drive1.001 is not a recognized drive image.

C:\Program Files\AccessData\FTK Imager\cmd>ftkimager.exe --verify "C:\Daubert Standard Evidence\Image1\Evidence_drive1.0
01"
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

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.

G:\VIP Info21DrugSales.xlsx 2021DrugSales.xlsx **G:\Students\manual-testing-fresher-resume-1.doc** manual-testing-fresher-resume-1 **G:\Work Doc\hr letter for visa.pdf** hr letter for visa