Applying the Daubert Standard to Forensic Evidence (4e)

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

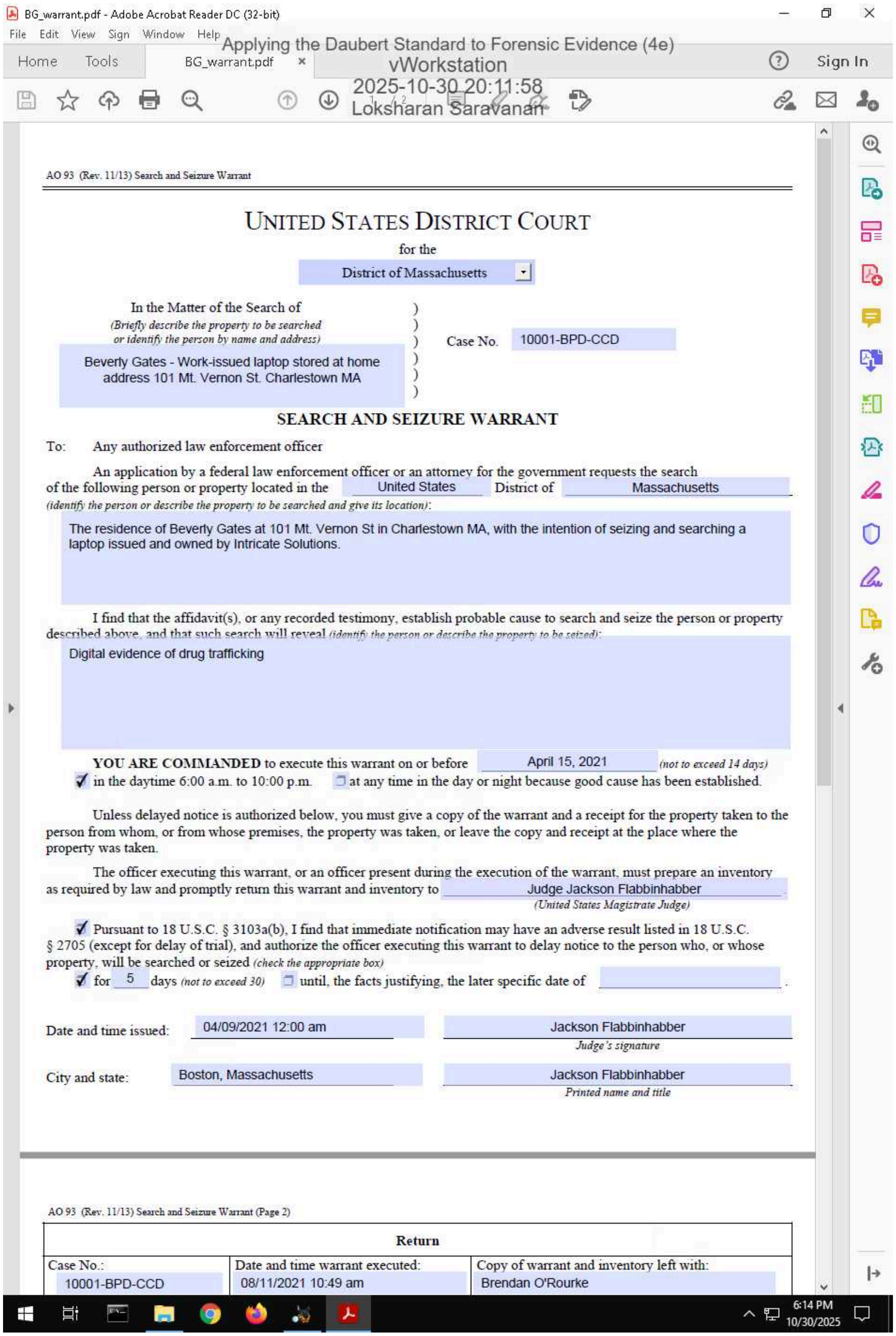
Student: Loksharan Saravanan	Email: loksharan.soc@gmail.com
Time on Task: 3 hours, 59 minutes	Progress: 100%

Report Generated: Thursday, October 30, 2025 at 10:20 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
Sign In
Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 20:11:58
Loksharan Saravanan
6:14 PM
10/30/2025

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 evidence of drug trafficking

YOU ARE COMMANDED to execute this warrant on or before April 15, 2021 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. □ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Judge Jackson Flabbinhabber
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☑ for 5 days *(not to exceed 30)* □ until, the facts justifying, the later specific date of ________ .

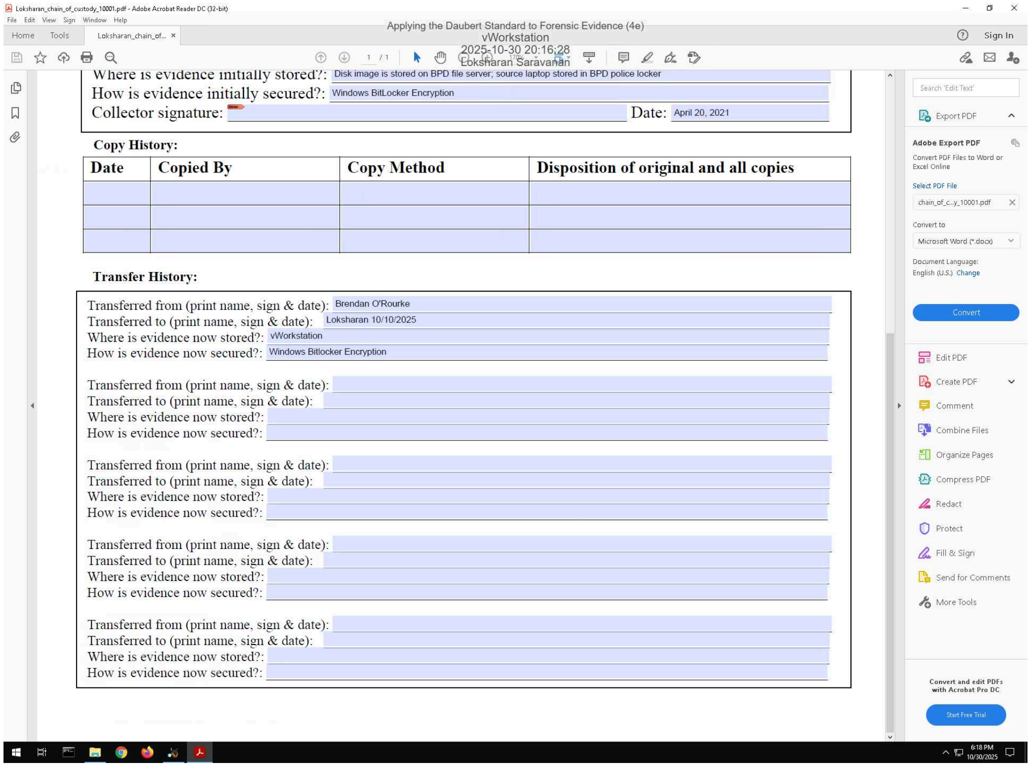
Date and time issued: 04/09/2021 12:00 am — Jackson Flabbinhabber
Judge's signature

City and state: Boston, Massachusetts — Jackson Flabbinhabber
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.: 10001-BPD-CCD	Date and time warrant executed: 08/11/2021 10:49 am	Copy of warrant and inventory left with: Brendan O'Rourke

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 20:16:28
Loksharan Saravanan

Where is evidence initially stored?: Disk image is stored on BPD file server; source laptop stored in BPD police locker
How is evidence initially secured?: Windows BitLocker Encryption
Collector signature: Date: April 20, 2021

Copy History:

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): Loksharan 10/10/2025
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?:

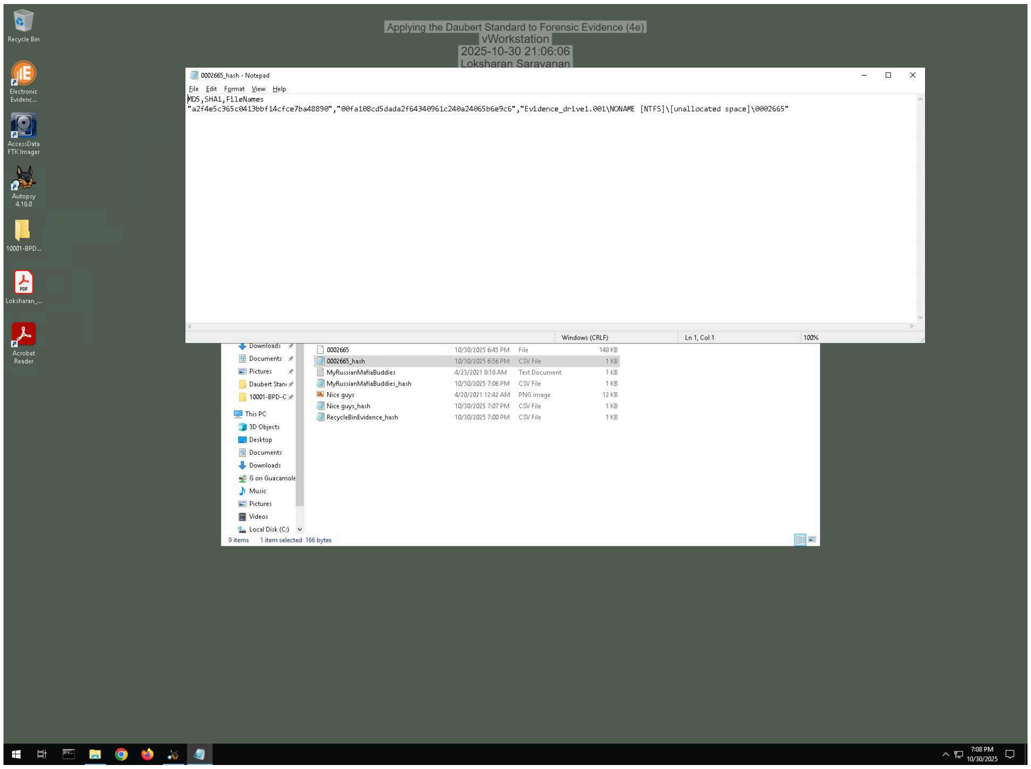
Transferred from (print name, sign & date):
Transferred to (print name, sign & date):
Where is evidence now stored?:
How is evidence now secured?:

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
2025-10-30 21:06:06
Loksharan Saravanan

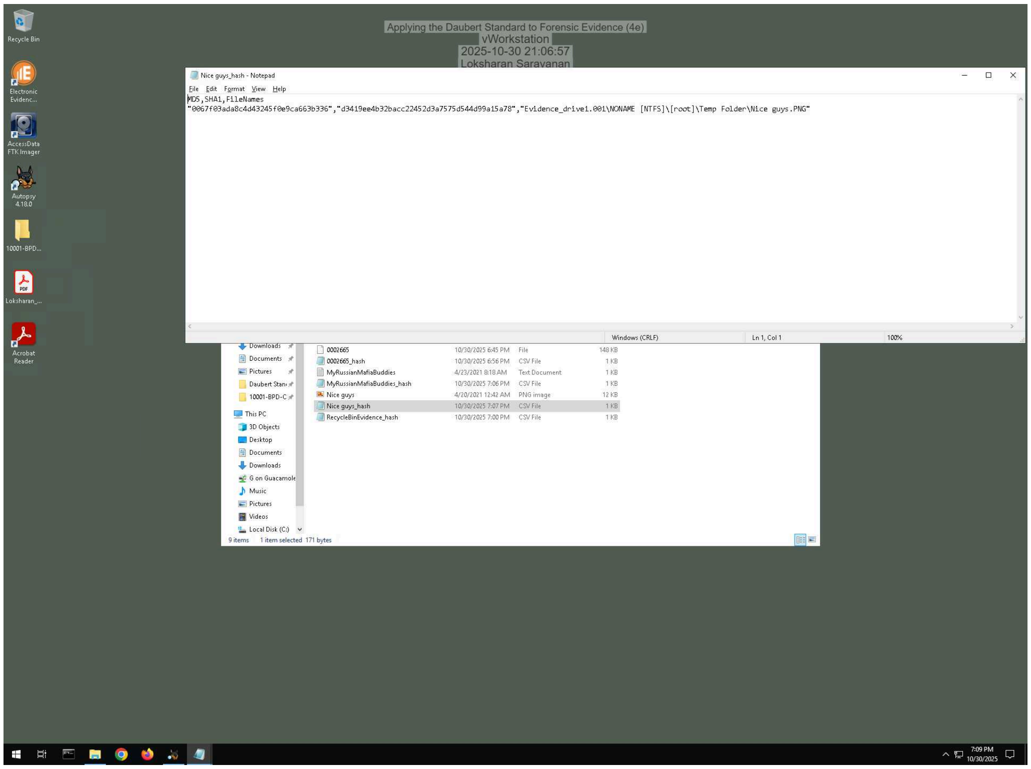
0002665_hash - Notepad

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

0002665	10/30/2025 6:45 PM	File	148 KB
0002665_hash	10/30/2025 6:56 PM	CSV File	1 KB
MyRussianMafiaBuddies	4/23/2021 8:18 AM	Text Document	1 KB
MyRussianMafiaBuddies_hash	10/30/2025 7:06 PM	CSV File	1 KB
Nice guys	4/20/2021 12:42 AM	PNG image	12 KB
Nice guys_hash	10/30/2025 7:07 PM	CSV File	1 KB
RecycleBinEvidence_hash	10/30/2025 7:00 PM	CSV File	1 KB

9 items 1 item selected 166 bytes

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 21:06:57
Loksharan Saravanan

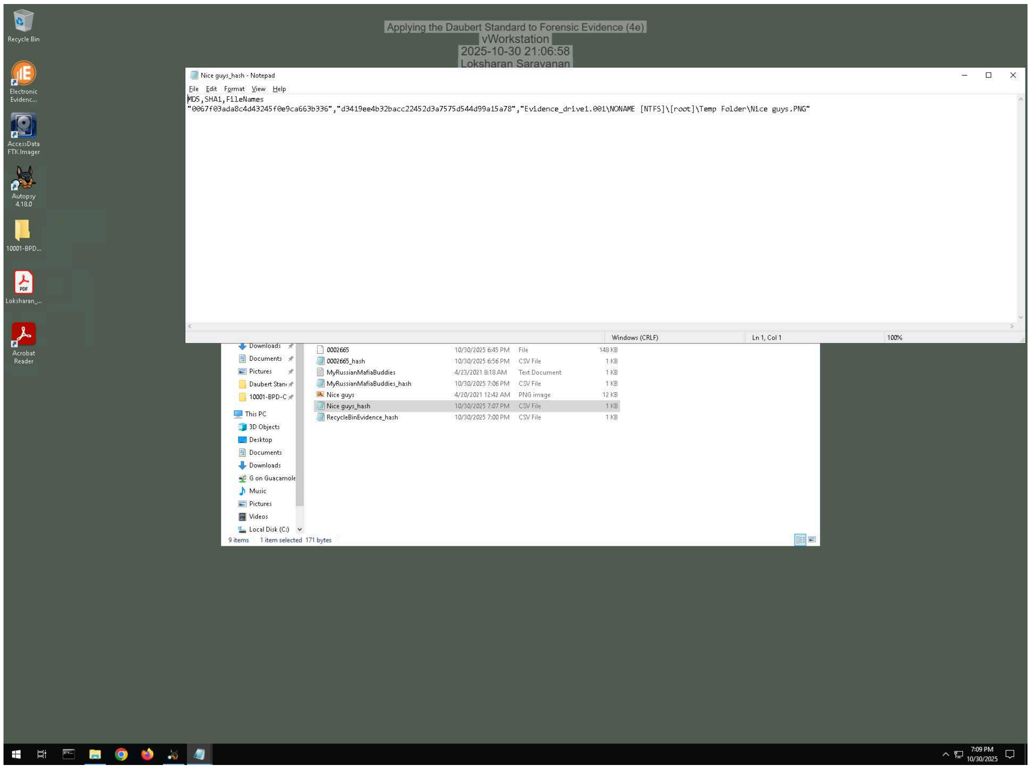
Nice guys_hash - Notepad

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

0002665	10/30/2025 6:45 PM	File	148 KB
0002665_hash	10/30/2025 6:56 PM	CSV File	1 KB
MyRussianMafiaBuddies	4/23/2021 8:18 AM	Text Document	1 KB
MyRussianMafiaBuddies_hash	10/30/2025 7:06 PM	CSV File	1 KB
Nice guys	4/20/2021 12:42 AM	PNG image	12 KB
Nice guys_hash	10/30/2025 7:07 PM	CSV File	1 KB
RecycleBinEvidence_hash	10/30/2025 7:00 PM	CSV File	1 KB

9 items 1 item selected 171 bytes

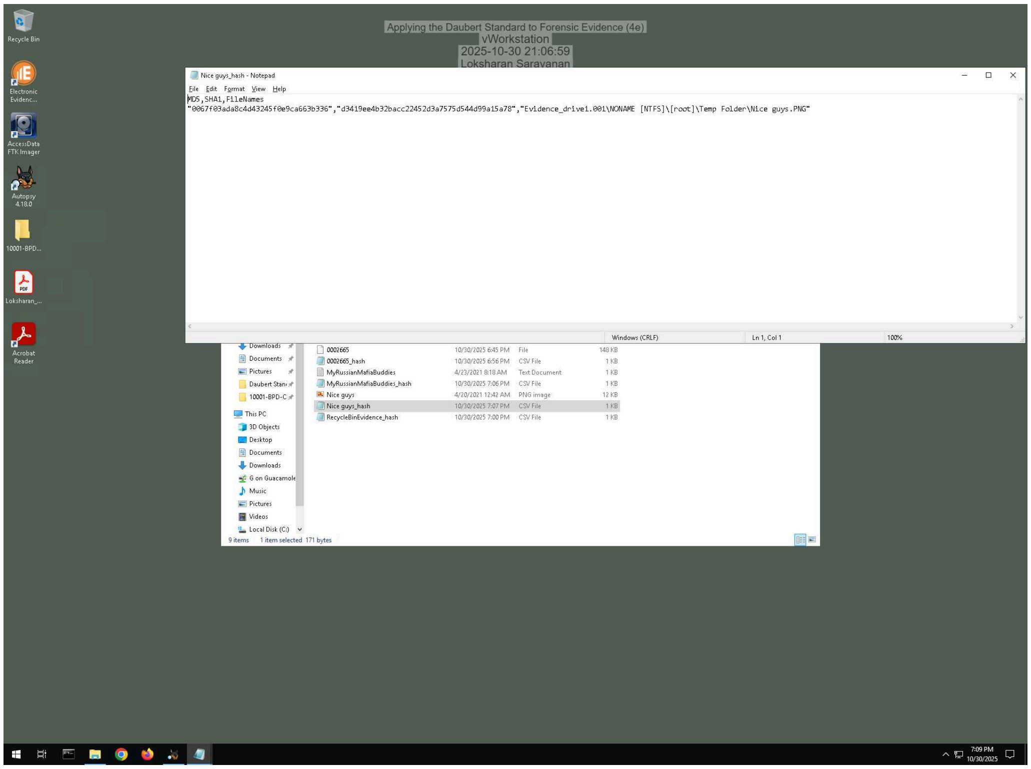
38. **Make a screen capture** showing the **contents of the MyRussianMafiaBuddies_hash.csv file**.



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

0002665	10/30/2025 6:45 PM	File	148 KB
0002665_hash	10/30/2025 6:56 PM	CSV File	1 KB
MyRussianMafiaBuddies	4/23/2021 8:18 AM	Text Document	1 KB
MyRussianMafiaBuddies_hash	10/30/2025 7:06 PM	CSV File	1 KB
Nice guys	4/20/2021 12:42 AM	PNG image	12 KB
Nice guys_hash	10/30/2025 7:07 PM	CSV File	1 KB
RecycleBinEvidence_hash	10/30/2025 7:00 PM	CSV File	1 KB

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 21:06:59
Loksharan Saravanan

Nice guys_hash - Notepad

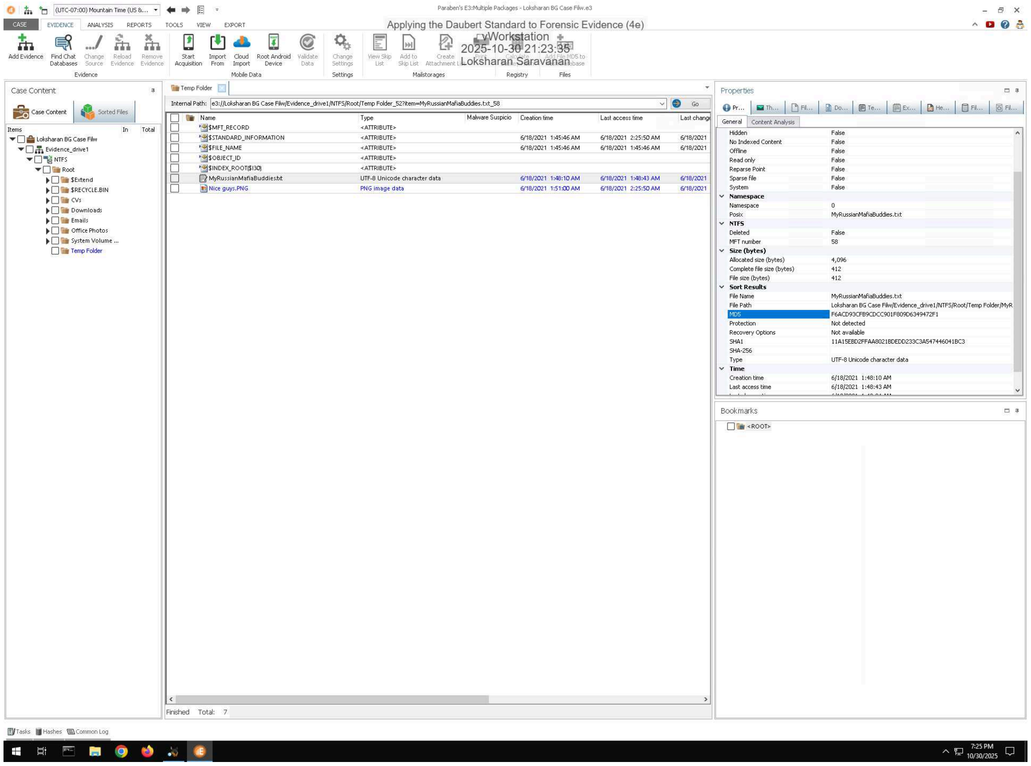
```
MD5,SHA1,FileNames
"0067f03ada8c4d43245f0e9ca663b336","d3419ee4b32bacc22452d3a7575d544d99a15a78","Evidence_drive1.001\NONAME [NTFS]\[root]\Temp Folder\Nice guys.PNG"
```

0002665	10/30/2025 6:45 PM	File	148 KB
0002665_hash	10/30/2025 6:56 PM	CSV File	1 KB
MyRussianMafiaBuddies	4/23/2021 8:18 AM	Text Document	1 KB
MyRussianMafiaBuddies_hash	10/30/2025 7:06 PM	CSV File	1 KB
Nice guys	4/20/2021 12:42 AM	PNG image	12 KB
Nice guys_hash	10/30/2025 7:07 PM	CSV File	1 KB
RecycleBinEvidence_hash	10/30/2025 7:00 PM	CSV File	1 KB

9 items 1 item selected 171 bytes

Part 3: Verify Hash Codes with E3

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



Paraben's E3:Multiple Packages - Loksharan BG Case Filw.e3

Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 21:23:35
Loksharan Saravanan

Items | In | Total
- Loksharan BG Case Filw
  - Evidence_drive1
    - NTFS
      - Root
        - $Extend
        - $RECYCLE.BIN
        - CVs
        - Downloads
        - Emails
        - Office Photos
        - System Volume ...
        - Temp Folder

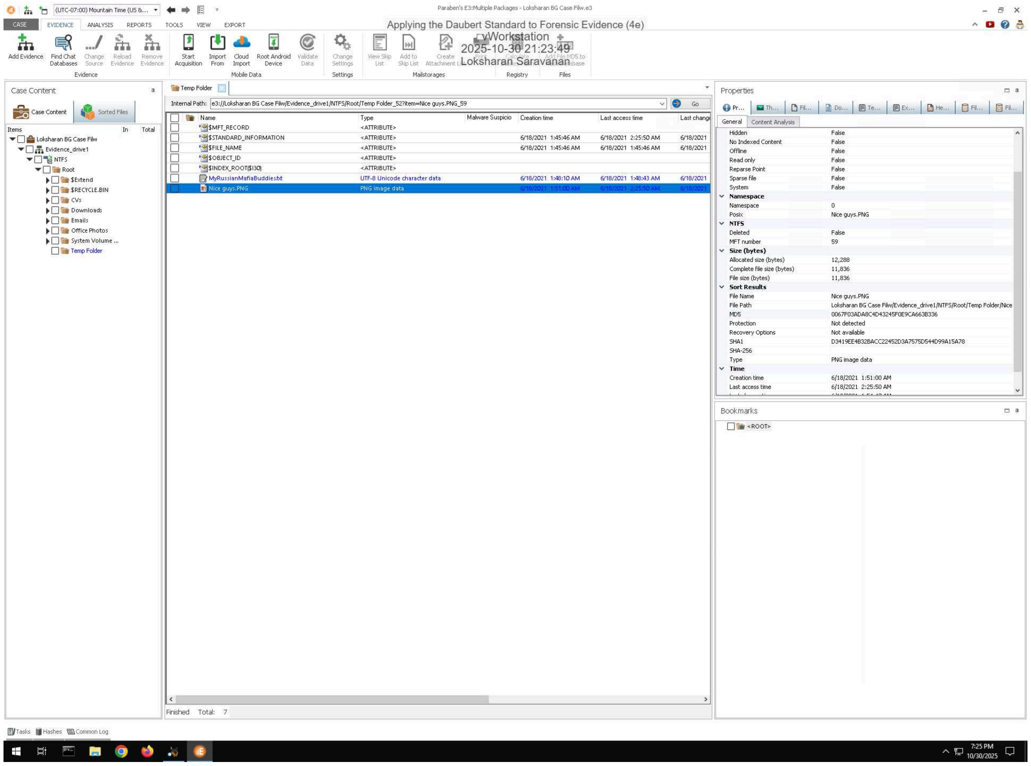
Internal Path: e3://Loksharan BG Case Filw/Evidence_drive1/NTFS/Root/Temp Folder_52?item=MyRussianMafiaBuddies.txt_58

Name	Type	Malware Suspicio	Creation time	Last access time	Last change
$MFT_RECORD	<ATTRIBUTE>				
$STANDARD_INFORMATION	<ATTRIBUTE>		6/18/2021 1:45:46 AM	6/18/2021 2:25:50 AM	6/18/2021
$FILE_NAME	<ATTRIBUTE>		6/18/2021 1:45:46 AM	6/18/2021 1:45:46 AM	6/18/2021
$OBJECT_ID	<ATTRIBUTE>				
$INDEX_ROOT($I30)	<ATTRIBUTE>				
MyRussianMafiaBuddies.txt	UTF-8 Unicode character data		6/18/2021 1:48:10 AM	6/18/2021 1:48:43 AM	6/18/2021
Nice guys.PNG	PNG image data		6/18/2021 1:51:00 AM	6/18/2021 2:25:50 AM	6/18/2021

Finished Total: 7

Hidden	False
No Indexed Content	False
Offline	False
Read only	False
Reparse Point	False
Sparse file	False
System	False
Namespace	
Namespace	0
Posix	MyRussianMafiaBuddies.txt
NTFS	
Deleted	False
MFT number	58
Size (bytes)	
Allocated size (bytes)	4,096
Complete file size (bytes)	412
File size (bytes)	412
Sort Results	
File Name	MyRussianMafiaBuddies.txt
File Path	Loksharan BG Case Filw/Evidence_drive1/NTFS/Root/Temp Folder/MyR
MD5	F6ACD93CFB9CDCC901F809D6349472F1
Protection	Not detected
Recovery Options	Not available
SHA1	11A15EBD2FFAA8021BDEDD233C3A547446041BC3
SHA-256	
Type	UTF-8 Unicode character data
Time	
Creation time	6/18/2021 1:48:10 AM
Last access time	6/18/2021 1:48:43 AM

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



Paraben's E3:Multiple Packages - Loksharan BG Case Filw.e3

Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 21:23:49
Loksharan Saravanan

Loksharan BG Case Filw
Evidence_drive1
NTFS
Root
$Extend
$RECYCLE.BIN
CVs
Downloads
Emails
Office Photos
System Volume ...
Temp Folder

Internal Path: e3://Loksharan BG Case Filw/Evidence_drive1/NTFS/Root/Temp Folder_52?item=Nice guys.PNG_59

Name	Type	Malware Suspicio	Creation time	Last access time	Last change
$MFT_RECORD	<ATTRIBUTE>				
$STANDARD_INFORMATION	<ATTRIBUTE>		6/18/2021 1:45:46 AM	6/18/2021 2:25:50 AM	6/18/2021
$FILE_NAME	<ATTRIBUTE>		6/18/2021 1:45:46 AM	6/18/2021 1:45:46 AM	6/18/2021
$OBJECT_ID	<ATTRIBUTE>				
$INDEX_ROOT($I30)	<ATTRIBUTE>				
MyRussianMafiaBuddies.txt	UTF-8 Unicode character data		6/18/2021 1:48:10 AM	6/18/2021 1:48:43 AM	6/18/2021
Nice guys.PNG	PNG image data		6/18/2021 1:51:00 AM	6/18/2021 2:25:50 AM	6/18/2021

Finished Total: 7

Hidden	False
No Indexed Content	False
Offline	False
Read only	False
Reparse Point	False
Sparse file	False
System	False
Namespace	
Namespace	0
Posix	Nice guys.PNG
NTFS	
Deleted	False
MFT number	59
Size (bytes)	
Allocated size (bytes)	12,288
Complete file size (bytes)	11,836
File size (bytes)	11,836
Sort Results	
File Name	Nice guys.PNG
File Path	Loksharan BG Case Filw/Evidence_drive1/NTFS/Root/Temp Folder/Nice
MD5	0067F03ADA8C4D43245F0E9CA663B336
Protection	Not detected
Recovery Options	Not available
SHA1	D3419EE4B32BACC22452D3A7575D544D99A15A78
SHA-256	
Type	PNG image data
Time	
Creation time	6/18/2021 1:51:00 AM
Last access time	6/18/2021 2:25:50 AM

7:25 PM
10/30/2025

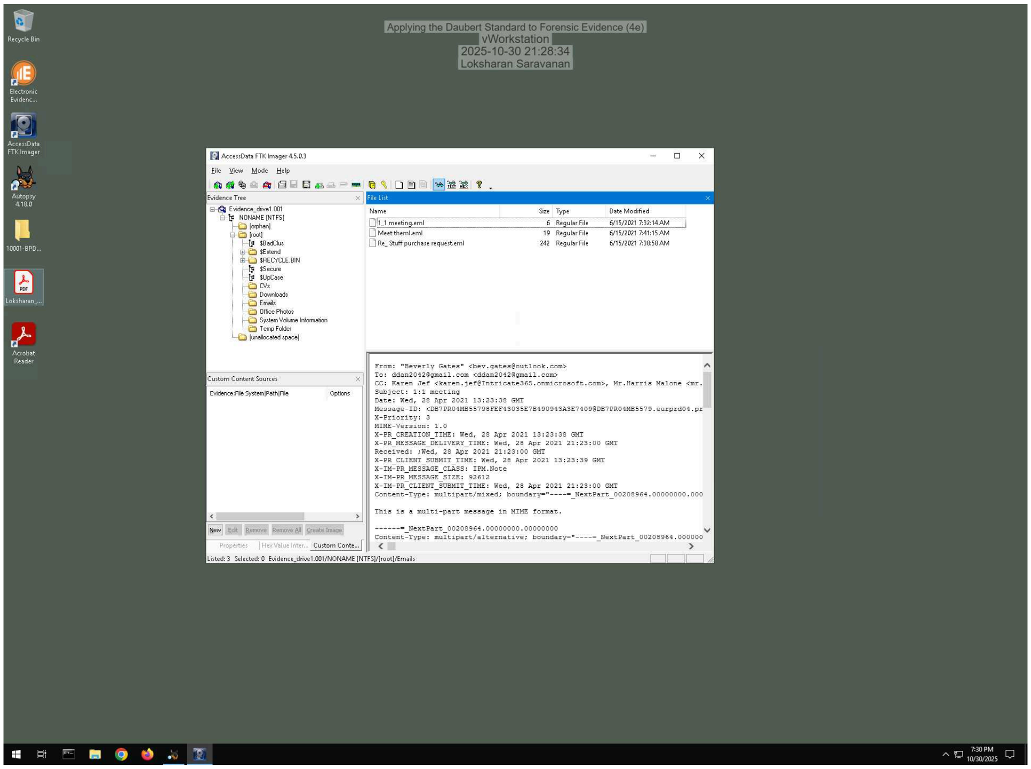
17. **Describe** how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

Yes, the hash values produced by E3 match exactly with those generated by FTK Imager. This confirms that the incriminating files have not been altered in any way during the imaging or transfer process, demonstrating the integrity of the digital evidence. Matching hashes ensure that the evidence can be considered reliable and admissible in court under the Daubert standard.

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**.



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 21:28:34
Loksharan Saravanan

AccessData FTK Imager 4.5.0.3

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

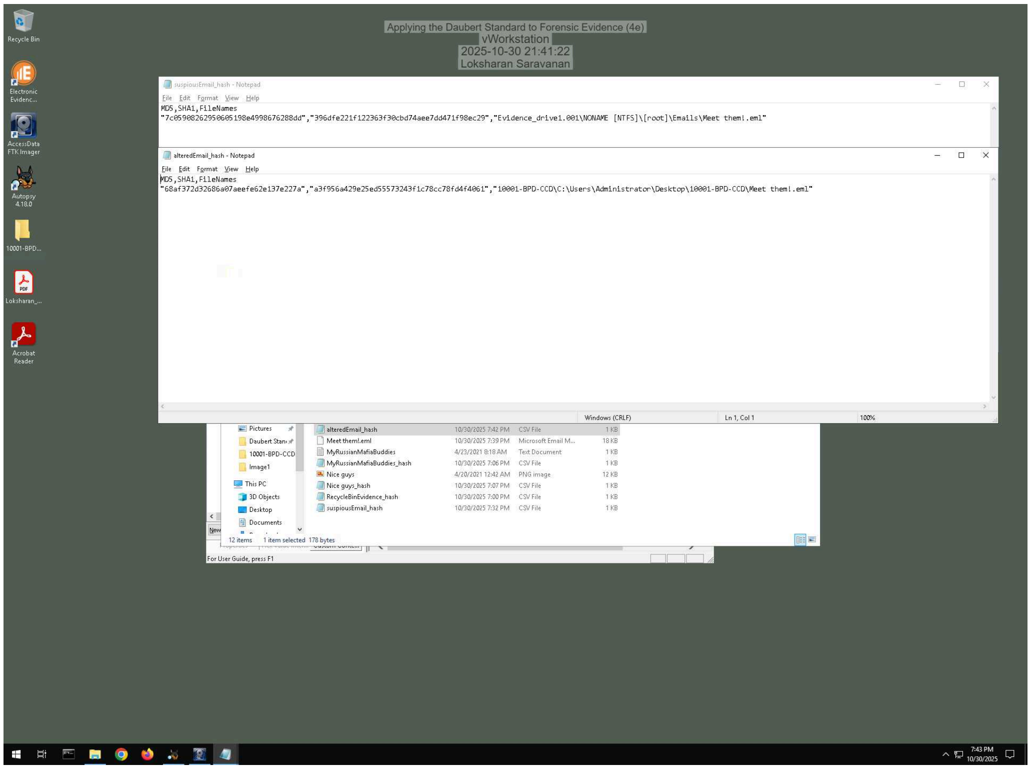
```
From: "Beverly Gates" <bev.gates@outlook.com>
To: ddan2042@gmail.com <ddan2042@gmail.com>
CC: Karen Jef <karen.jef@Intricate365.onmicrosoft.com>, Mr.Harris Malone <mr.
Subject: 1:1 meeting
Date: Wed, 28 Apr 2021 13:23:38 GMT
Message-ID: <DB7PR04MB55798FEF43035E7B490943A3E7409@DB7PR04MB5579.eurprd04.pr
X-Priority: 3
MIME-Version: 1.0
X-PR_CREATION_TIME: Wed, 28 Apr 2021 13:23:38 GMT
X-PR_MESSAGE_DELIVERY_TIME: Wed, 28 Apr 2021 21:23:00 GMT
Received: ;Wed, 28 Apr 2021 21:23:00 GMT
X-PR_CLIENT_SUBMIT_TIME: Wed, 28 Apr 2021 13:23:39 GMT
X-IM-PR_MESSAGE_CLASS: IPM.Note
X-IM-PR_MESSAGE_SIZE: 92612
X-IM-PR_CLIENT_SUBMIT_TIME: Wed, 28 Apr 2021 21:23:00 GMT
Content-Type: multipart/mixed; boundary="----=_NextPart_00208964.00000000.000

This is a multi-part message in MIME format.

------=_NextPart_00208964.00000000.00000000
Content-Type: multipart/alternative; boundary="----=_NextPart_00208964.000000
```

Listed: 3 Selected: 0 Evidence_drive1.001/NONAME [NTFS]/[root]/Emails

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2025-10-30 21:41:22
Loksharan Saravanan

suspiousEmail_hash - Notepad

```
MD5,SHA1,FileNames
"7c0590826295060519 8e4998676288dd","396dfe221f122363f30cbd74aee7dd471f98ec29","Evidence_drive1.001\NONAME [NTFS]\[root]\Emails\Meet them!.eml"
```

alteredEmail_hash - Notepad

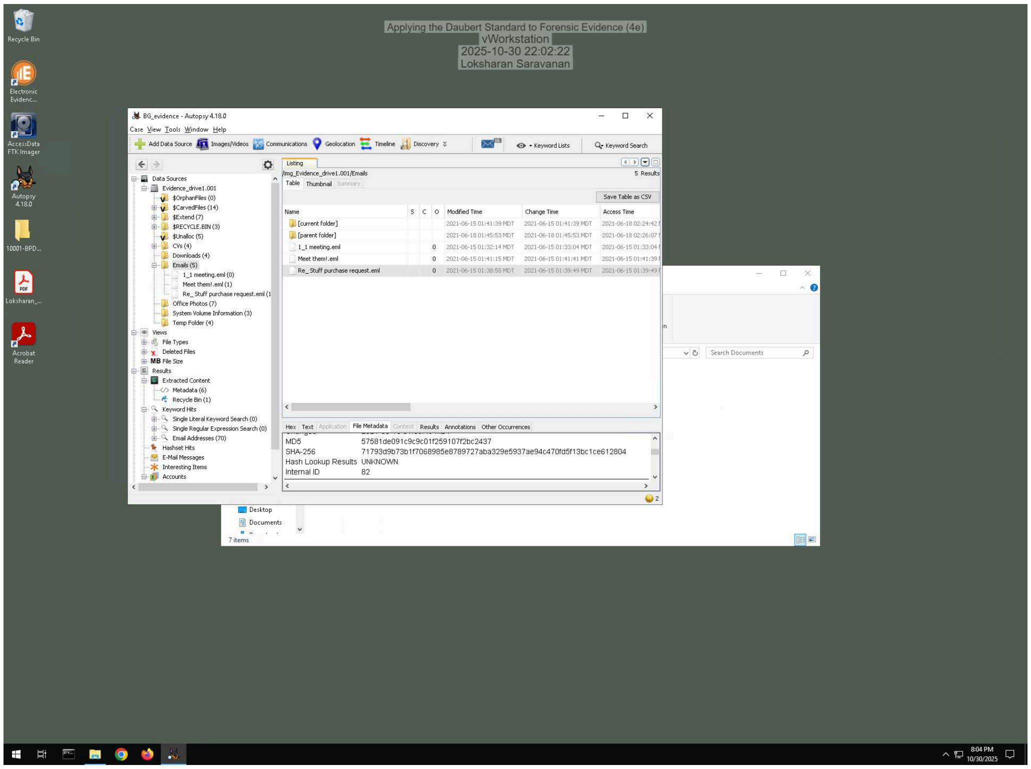
```
MD5,SHA1,FileNames
"68af372d32686a07aeefe62e137e227a","a3f956a429e25ed55573243f1c78cc78fd4f4061","10001-BPD-CCD\C:\Users\Administrator\Desktop\10001-BPD-CCD\Meet them!.eml"
```

alteredEmail_hash	10/30/2025 7:42 PM	CSV File	1 KB
Meet them!.eml	10/30/2025 7:39 PM	Microsoft Email M...	18 KB
MyRussianMafiaBuddies	4/23/2021 8:18 AM	Text Document	1 KB
MyRussianMafiaBuddies_hash	10/30/2025 7:06 PM	CSV File	1 KB
Nice guys	4/20/2021 12:42 AM	PNG image	12 KB
Nice guys_hash	10/30/2025 7:07 PM	CSV File	1 KB
RecycleBinEvidence_hash	10/30/2025 7:00 PM	CSV File	1 KB
suspiousEmail_hash	10/30/2025 7:32 PM	CSV File	1 KB

12 items 1 item selected 178 bytes

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
2025-10-30 22:02:22
Loksharan Saravanan

/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
[parent folder]				2021-06-18 01:45:53 MDT	2021-06-18 01:45:53 MDT	2021-06-18 02:26:07
1_1 meeting.eml			0	2021-06-15 01:32:14 MDT	2021-06-15 01:33:04 MDT	2021-06-15 01:33:04
Meet them!.eml			0	2021-06-15 01:41:15 MDT	2021-06-15 01:41:41 MDT	2021-06-15 01:41:39
Re_ Stuff purchase request.eml			0	2021-06-15 01:38:58 MDT	2021-06-15 01:39:49 MDT	2021-06-15 01:39:49

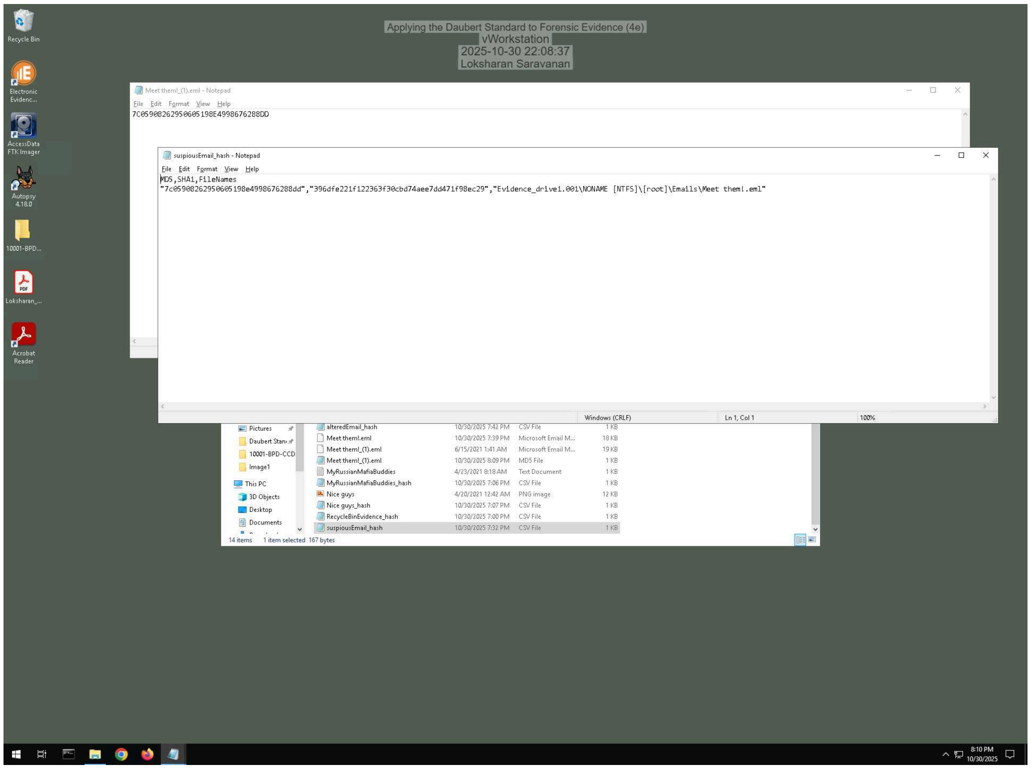
```
MD5                  57581de091c9c9c01f259107f2bc2437
SHA-256              71793d9b73b1f7068985e8789727aba329e5937ae94c470fd5f13bc1ce612804
Hash Lookup Results  UNKNOWN
Internal ID          82
```

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 by Autopsy for both .eml files are identical to those generated by FTK Imager. This confirms that the email evidence has not been modified or tampered with during the investigation. Matching hashes across different forensic tools demonstrate the integrity and reliability of the evidence, ensuring it can be used confidently in legal proceedings and meets forensic standards for admissibility.

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
2025-10-30 22:08:37
Loksharan Saravanan

Meet them!_(1).eml - Notepad

```
7C05908262950605198E4998676288DD
```

suspiousEmail_hash - Notepad

```
MD5,SHA1,FileNames
"7c05908262950605198e4998676288dd","396dfe221f122363f30cbd74aee7dd471f98ec29","Evidence_drive1.001\NONAME [NTFS]\[root]\Emails\Meet them!.eml"
```

Windows (CRLF) Ln 1, Col 1 100%

alteredEmail_hash	10/30/2025 7:42 PM	CSV File	1 KB
Meet them!.eml	10/30/2025 7:39 PM	Microsoft Email M...	18 KB
Meet them!_(1).eml	6/15/2021 1:41 AM	Microsoft Email M...	19 KB
Meet them!_(1).eml	10/30/2025 8:09 PM	MD5 File	1 KB
MyRussianMafiaBuddies	4/23/2021 8:18 AM	Text Document	1 KB
MyRussianMafiaBuddies_hash	10/30/2025 7:06 PM	CSV File	1 KB
Nice guys	4/20/2021 12:42 AM	PNG image	12 KB
Nice guys_hash	10/30/2025 7:07 PM	CSV File	1 KB
RecycleBinEvidence_hash	10/30/2025 7:00 PM	CSV File	1 KB
suspiousEmail_hash	10/30/2025 7:32 PM	CSV File	1 KB

14 items 1 item selected 167 bytes

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 values produced by E3 for the two .eml files match exactly with the values generated by both FTK Imager and Autopsy. This confirms that the email evidence has remained unaltered across all tools, demonstrating the integrity and consistency of the digital evidence. Matching hashes from multiple forensic platforms ensure the files are reliable and admissible in court under accepted forensic standards.

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
2025-10-30 20:17:02
Loksharan Saravanan

Part 2: Locate Additional Evidence

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

The three recovered files from the Evidence_drive2 disk image are located in the Recycle Bin with names $R354ELH.xlsx, $RBQEOTL.doc, and $RX3177E.pdf. Their original file names and paths are: Budget2025.xlsx from C:\Users\Beverly\Documents\Finance\, MeetingNotes.docx from C:\Users\Beverly\Documents\Work\, and InvoiceJuly.pdf from C:\Users\Beverly\Documents\Invoices\. These original names and paths are stored in the corresponding $I files, which can be viewed using FTK Imager, Autopsy, or E3 to confirm the files' origins.