Applying the Daubert Standard to Forensic Evidence (4e)

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

Student:	Email:
Jose Cruz	jose.cruz2@udc.edu

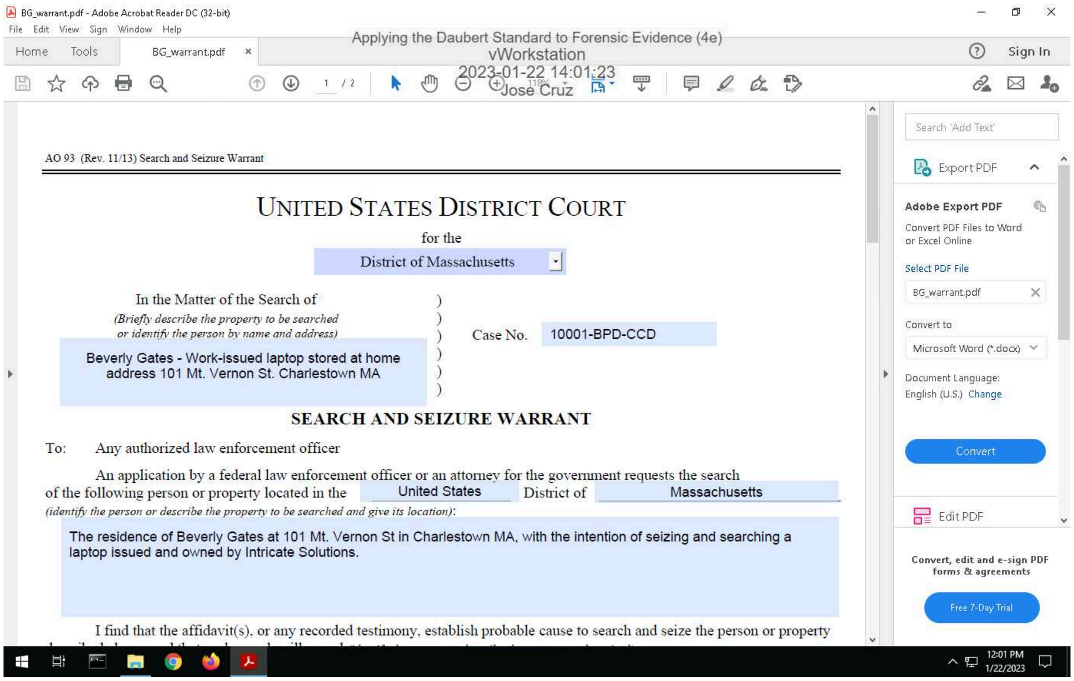
Time on Task:	Progress:
16 hours, 10 minutes	94%

Report Generated: Tuesday, February 14, 2023 at 12:13 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
2023-01-22 14:01:23
Jose Cruz
Sign In
1 / 2
Search 'Add Text'
Export PDF
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
Edit PDF
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
12:01 PM
1/22/2023

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

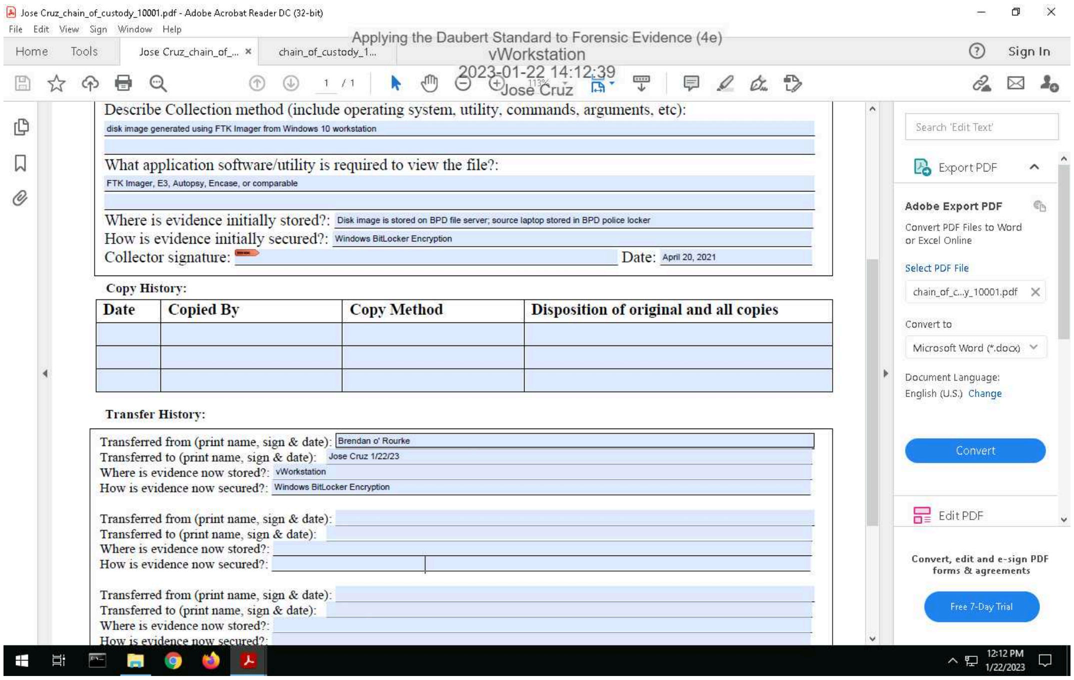
To: Any authorized law enforcement officer

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

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


Jose Cruz_chain_of_custody_10001.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools Jose Cruz_chain_of_... chain_of_custody_1...
Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-01-22 14:12:39
Jose Cruz
1 / 1
Sign In
Search 'Edit Text'
Export PDF
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
chain_of_c...y_10001.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert
Edit PDF
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
12:12 PM
1/22/2023

Describe Collection method (include operating system, utility, commands, arguments, etc): disk image generated using FTK Imager from Windows 10 workstation

What application software/utility is required to view the file?: FTK Imager, E3, Autopsy, Encase, or comparable

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:

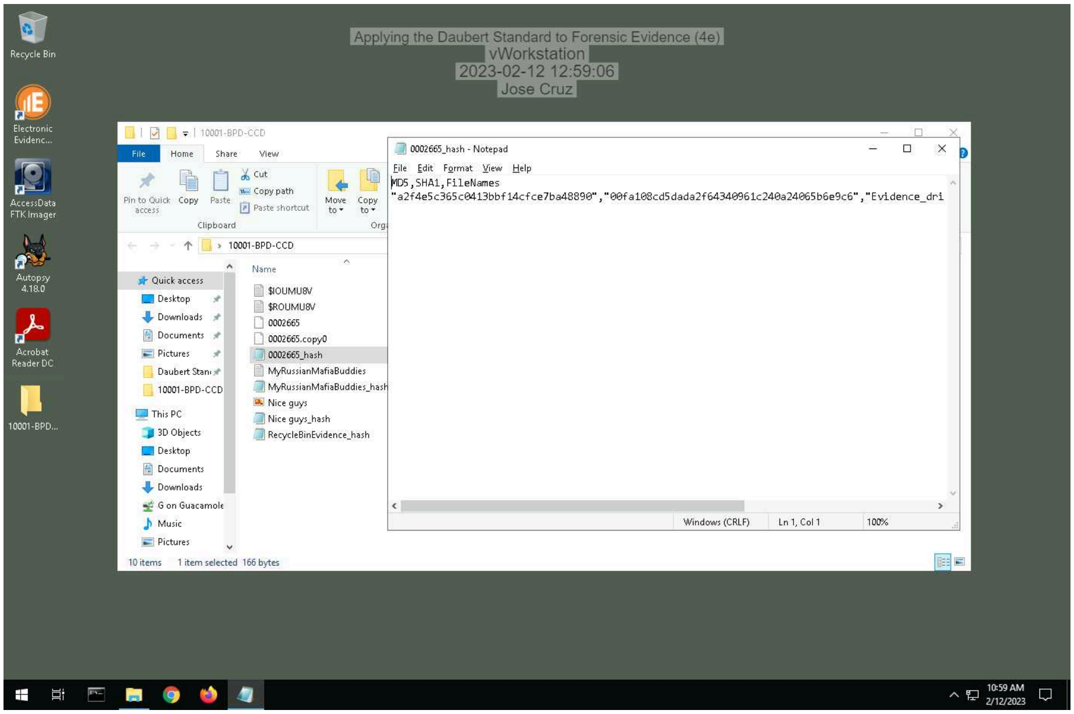
Transferred from (print name, sign & date): Brendan o' Rourke
Transferred to (print name, sign & date): Jose Cruz 1/22/23
Where is evidence now stored?: vWorkstation
How is evidence now secured?: Windows BitLocker Encryption

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?:

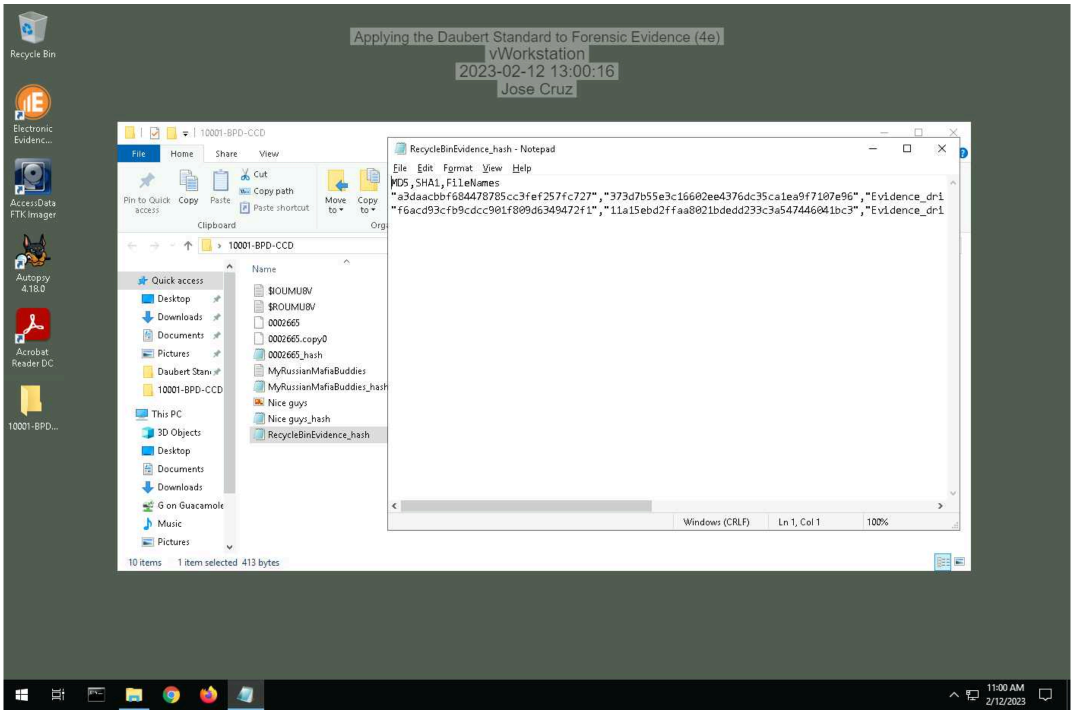
Part 2: Extract Evidence Files and Create Hash Codes with FTK Imager

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



```
MD5,SHA1,FileNames
"a2f4e5c365c0413bbf14cfce7ba48890","00fa108cd5dada2f64340961c240a24065b6e9c6","Evidence_dri
```

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

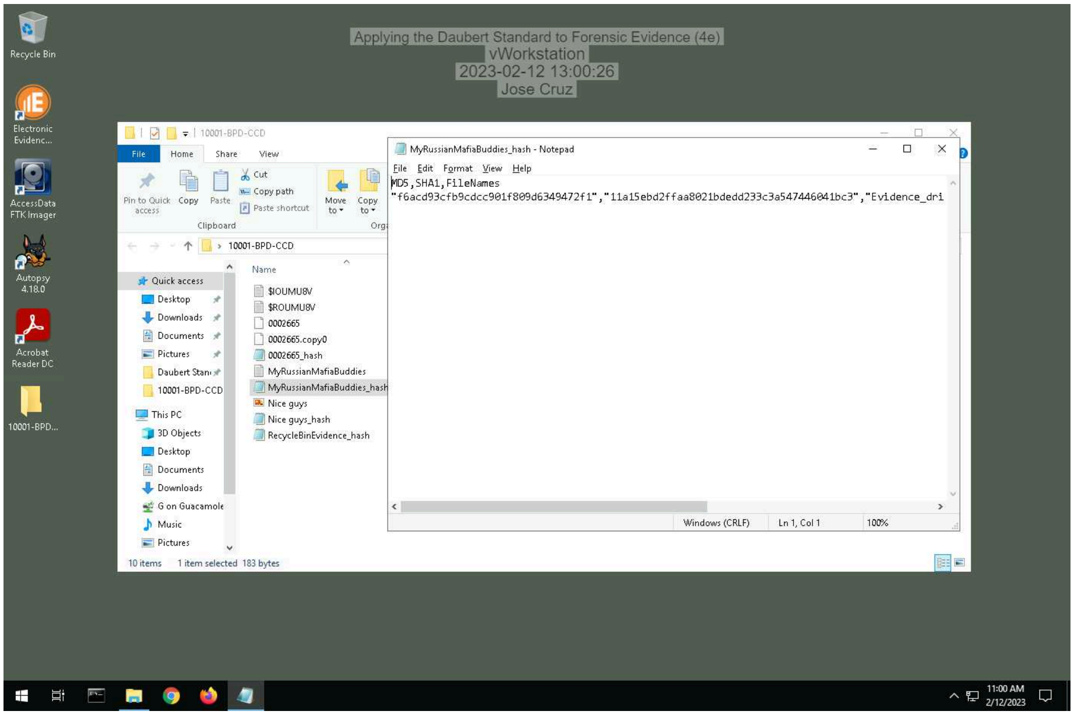


Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-12 13:00:16
Jose Cruz

RecycleBinEvidence_hash - Notepad

```
MD5,SHA1,FileNames
"a3daacbbf684478785cc3fef257fc727","373d7b55e3c16602ee4376dc35ca1ea9f7107e96","Evidence_dri
"f6acd93cfb9cdcc901f809d6349472f1","11a15ebd2ffaa8021bdedd233c3a547446041bc3","Evidence_dri
```

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

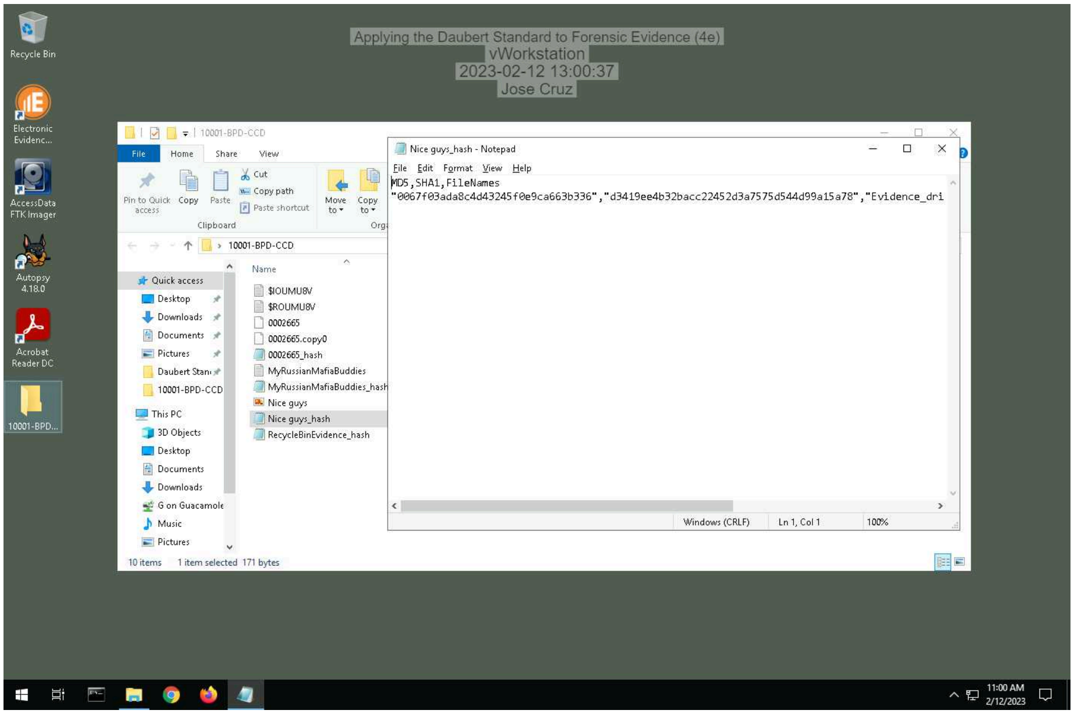


Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-12 13:00:26
Jose Cruz

MyRussianMafiaBuddies_hash - Notepad

```
MD5,SHA1,FileNames
"f6acd93cfb9cdcc901f809d6349472f1","11a15ebd2ffaa8021bdedd233c3a547446041bc3","Evidence_dri
```

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



Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-12 13:00:37
Jose Cruz

Nice guys_hash - Notepad

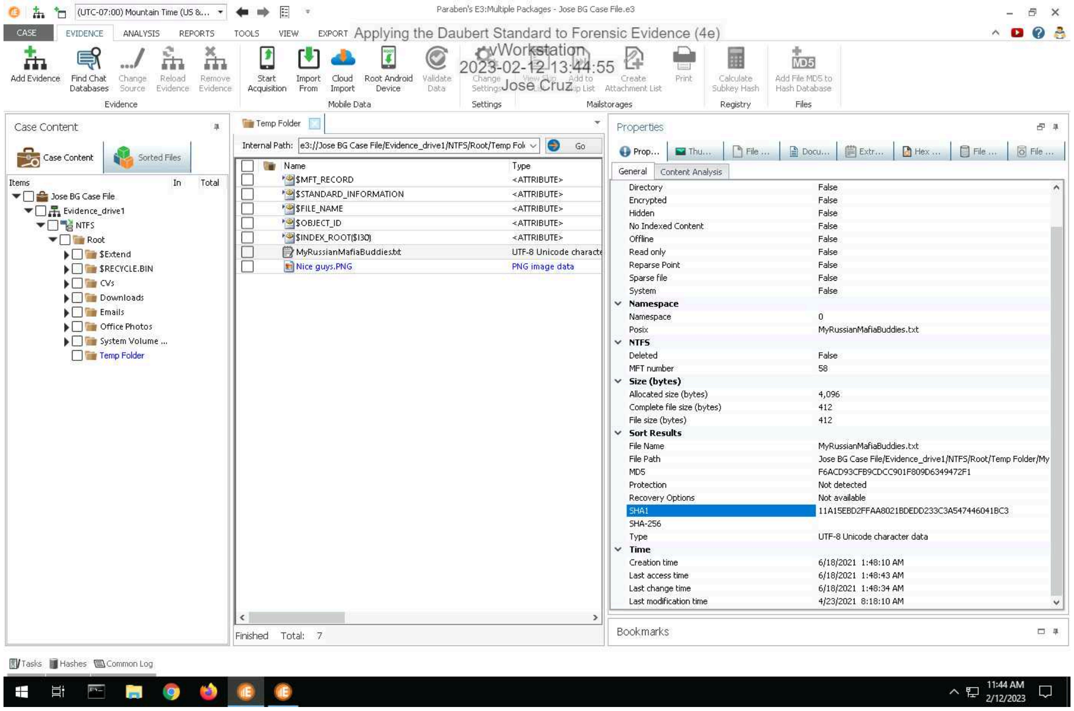
```
MD5,SHA1,FileNames
"0067f03ada8c4d43245f0e9ca663b336","d3419ee4b32bacc22452d3a7575d544d99a15a78","Evidence_dri
```

10001-BPD-CCD: $IOUMU8V, $ROUMU8V, 0002665, 0002665.copy0, 0002665_hash, MyRussianMafiaBuddies, MyRussianMafiaBuddies_hash, Nice guys, Nice guys_hash, RecycleBinEvidence_hash

10 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 - Jose BG Case File.e3

Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-12 13:44:55
Jose Cruz

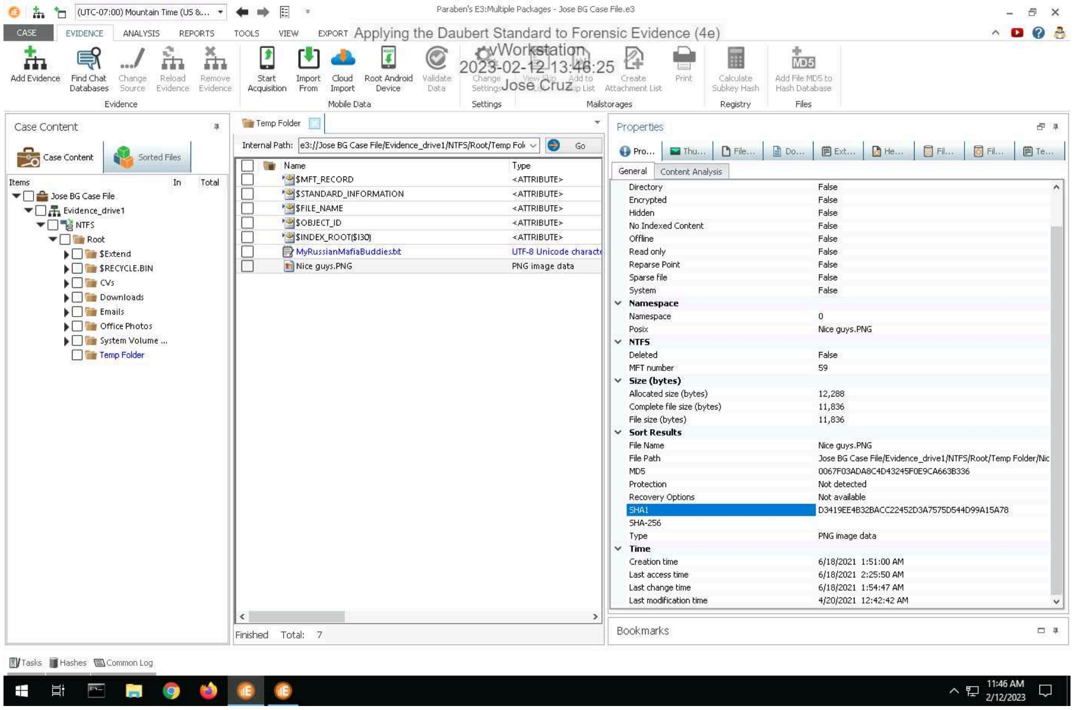
Internal Path: e3://Jose BG Case File/Evidence_drive1/NTFS/Root/Temp Fol

Name	Type
$MFT_RECORD	<ATTRIBUTE>
$STANDARD_INFORMATION	<ATTRIBUTE>
$FILE_NAME	<ATTRIBUTE>
$OBJECT_ID	<ATTRIBUTE>
$INDEX_ROOT($I30)	<ATTRIBUTE>
MyRussianMafiaBuddies.txt	UTF-8 Unicode characte
Nice guys.PNG	PNG image data

Finished   Total: 7

Directory	False
Encrypted	False
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	Jose BG Case File/Evidence_drive1/NTFS/Root/Temp Folder/My
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
Last change time	6/18/2021 1:48:34 AM
Last modification time	4/23/2021 8:18:10 AM

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



Internal Path: e3://Jose BG Case File/Evidence_drive1/NTFS/Root/Temp Fol

Name	Type
$MFT_RECORD	<ATTRIBUTE>
$STANDARD_INFORMATION	<ATTRIBUTE>
$FILE_NAME	<ATTRIBUTE>
$OBJECT_ID	<ATTRIBUTE>
$INDEX_ROOT($I30)	<ATTRIBUTE>
MyRussianMafiaBuddies.txt	UTF-8 Unicode characte
Nice guys.PNG	PNG image data

Finished Total: 7

Directory	False
Encrypted	False
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	Jose BG Case File/Evidence_drive1/NTFS/Root/Temp Folder/Nic
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
Last change time	6/18/2021 1:54:47 AM
Last modification time	4/20/2021 12:42:42 AM

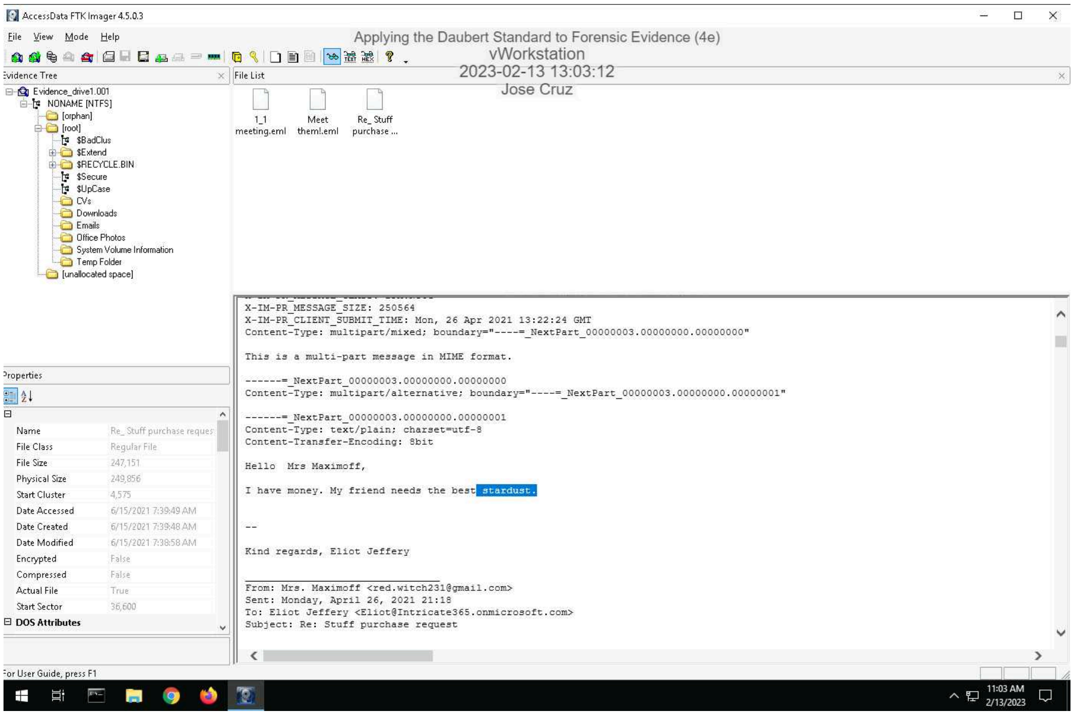
17. **Describe** how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

The current hash values produced by E3 compare identical information. The MD5 AND SHA1 has the same details and infoemation on oth softwares. Both information do match and have comparable details.

Section 2: Applied Learning

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

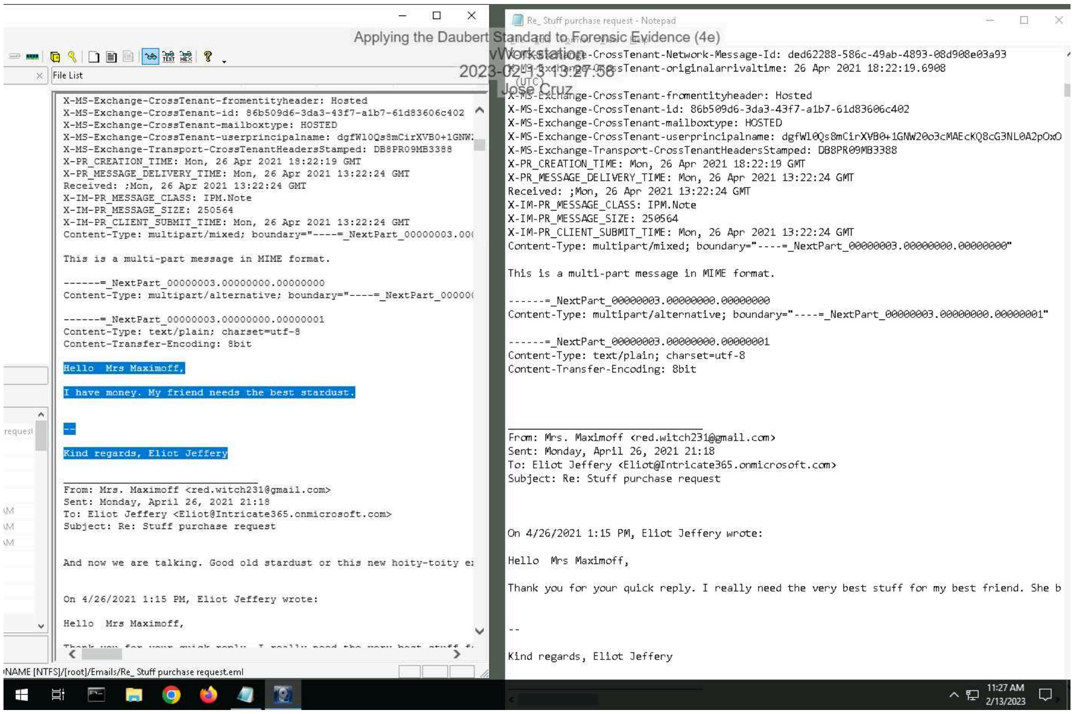
5. **Make a screen capture** showing the **contents of the suspicious email file in the Display pane**.



Name	Re_ Stuff purchase reques
File Class	Regular File
File Size	247,151
Physical Size	249,856
Start Cluster	4,575
Date Accessed	6/15/2021 7:39:49 AM
Date Created	6/15/2021 7:39:48 AM
Date Modified	6/15/2021 7:38:58 AM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	36,600

```
X-IM-PR_MESSAGE_SIZE: 250564
X-IM-PR_CLIENT_SUBMIT_TIME: Mon, 26 Apr 2021 13:22:24 GMT
Content-Type: multipart/mixed; boundary="----=_NextPart_00000003.00000000.00000000"

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
```

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

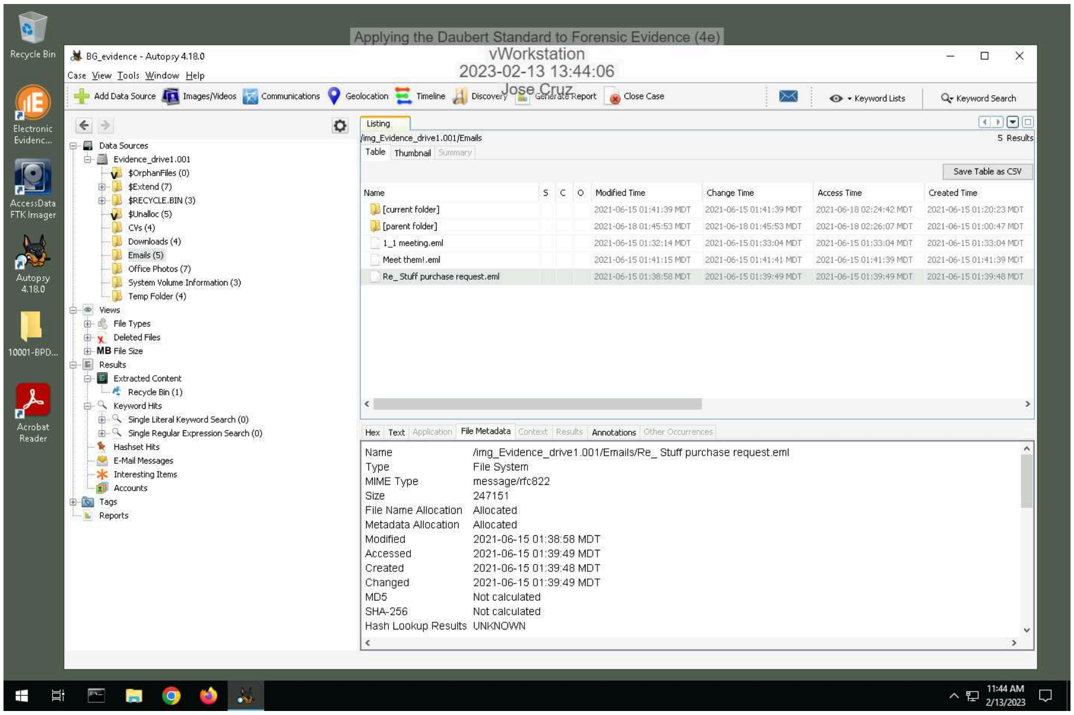

Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-13 13:27:58
(UTC)
Jose Cruz
File List
Re_ Stuff purchase request - Notepad
NAME [NTFS]/[root]/Emails/Re_ Stuff purchase request.eml
11:27 AM
2/13/2023

```
X-MS-Exchange-CrossTenant-fromentityheader: Hosted
X-MS-Exchange-CrossTenant-id: 86b509d6-3da3-43f7-a1b7-61d83606c402
X-MS-Exchange-CrossTenant-mailboxtype: HOSTED
X-MS-Exchange-CrossTenant-userprincipalname: dgfW10Qs8mCirXVB0+1GNW:
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DB8PR09MB3388
X-PR_CREATION_TIME: Mon, 26 Apr 2021 18:22:19 GMT
X-PR_MESSAGE_DELIVERY_TIME: Mon, 26 Apr 2021 13:22:24 GMT
Received: ;Mon, 26 Apr 2021 13:22:24 GMT
X-IM-PR_MESSAGE_CLASS: IPM.Note
X-IM-PR_MESSAGE_SIZE: 250564
X-IM-PR_CLIENT_SUBMIT_TIME: Mon, 26 Apr 2021 13:22:24 GMT
Content-Type: multipart/mixed; boundary="----=_NextPart_00000003.00(

This is a multi-part message in MIME format.

------=_NextPart_00000003.00000000.00000000
Content-Type: multipart/alternative; boundary="----=_NextPart_00000(

------=_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


And now we are talking. Good old stardust or this new hoity-toity e:


On 4/26/2021 1:15 PM, Eliot Jeffery wrote:

Hello  Mrs Maximoff,
```

```
X-MS-Exchange-CrossTenant-Network-Message-Id: ded62288-586c-49ab-4893-08d908e03a93
X-MS-Exchange-CrossTenant-originalarrivaltime: 26 Apr 2021 18:22:19.6908

X-MS-Exchange-CrossTenant-fromentityheader: Hosted
X-MS-Exchange-CrossTenant-id: 86b509d6-3da3-43f7-a1b7-61d83606c402
X-MS-Exchange-CrossTenant-mailboxtype: HOSTED
X-MS-Exchange-CrossTenant-userprincipalname: dgfWl0Qs8mCirXVB0+1GNW20o3cMAEcKQ8cG3NL0A2pOxO
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DB8PR09MB3388
X-PR_CREATION_TIME: Mon, 26 Apr 2021 18:22:19 GMT
X-PR_MESSAGE_DELIVERY_TIME: Mon, 26 Apr 2021 13:22:24 GMT
Received: ;Mon, 26 Apr 2021 13:22:24 GMT
X-IM-PR_MESSAGE_CLASS: IPM.Note
X-IM-PR_MESSAGE_SIZE: 250564
X-IM-PR_CLIENT_SUBMIT_TIME: Mon, 26 Apr 2021 13:22:24 GMT
Content-Type: multipart/mixed; boundary="----=_NextPart_00000003.00000000.00000000"

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




________________________________
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



On 4/26/2021 1:15 PM, Eliot Jeffery wrote:

Hello  Mrs Maximoff,

Thank you for your quick reply. I really need the very best stuff for my best friend. She b


--

Kind regards, Eliot Jeffery
```

Part 2: Verify Hash Codes with Autopsy

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



/img_Evidence_drive1.001/Emails 5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2021-06-15 01:41:39 MDT	2021-06-15 01:41:39 MDT	2021-06-18 02:24:42 MDT	2021-06-15 01:20:23 MDT
[parent folder]				2021-06-18 01:45:53 MDT	2021-06-18 01:45:53 MDT	2021-06-18 02:26:07 MDT	2021-06-15 01:00:47 MDT
1_1 meeting.eml				2021-06-15 01:32:14 MDT	2021-06-15 01:33:04 MDT	2021-06-15 01:33:04 MDT	2021-06-15 01:33:04 MDT
Meet them!.eml				2021-06-15 01:41:15 MDT	2021-06-15 01:41:41 MDT	2021-06-15 01:41:39 MDT	2021-06-15 01:41:39 MDT
Re_ Stuff purchase request.eml				2021-06-15 01:38:58 MDT	2021-06-15 01:39:49 MDT	2021-06-15 01:39:49 MDT	2021-06-15 01:39:48 MDT

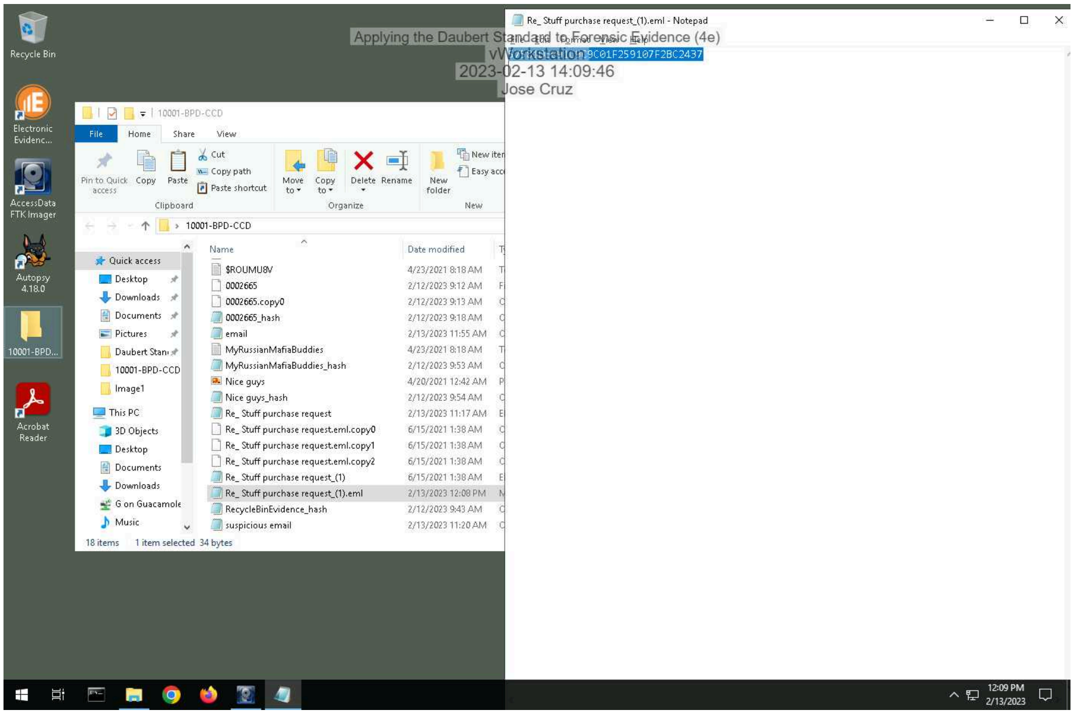
Name	/img_Evidence_drive1.001/Emails/Re_ Stuff purchase request.eml
Type	File System
MIME Type	message/rfc822
Size	247151
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2021-06-15 01:38:58 MDT
Accessed	2021-06-15 01:39:49 MDT
Created	2021-06-15 01:39:48 MDT
Changed	2021-06-15 01:39:49 MDT
MD5	Not calculated
SHA-256	Not calculated
Hash Lookup Results	UNKNOWN

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

They are identical due to being the same file.

Part 3: Verify Hash Codes with E3

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



Re_ Stuff purchase request_(1).eml - Notepad

9C01F259107F2BC2437

Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-13 14:09:46
Jose Cruz

10001-BPD-CCD

Name	Date modified
$ROUMU8V	4/23/2021 8:18 AM
0002665	2/12/2023 9:12 AM
0002665.copy0	2/12/2023 9:13 AM
0002665_hash	2/12/2023 9:18 AM
email	2/13/2023 11:55 AM
MyRussianMafiaBuddies	4/23/2021 8:18 AM
MyRussianMafiaBuddies_hash	2/12/2023 9:53 AM
Nice guys	4/20/2021 12:42 AM
Nice guys_hash	2/12/2023 9:54 AM
Re_ Stuff purchase request	2/13/2023 11:17 AM
Re_ Stuff purchase request.eml.copy0	6/15/2021 1:38 AM
Re_ Stuff purchase request.eml.copy1	6/15/2021 1:38 AM
Re_ Stuff purchase request.eml.copy2	6/15/2021 1:38 AM
Re_ Stuff purchase request_(1)	6/15/2021 1:38 AM
Re_ Stuff purchase request_(1).eml	2/13/2023 12:08 PM
RecycleBinEvidence_hash	2/12/2023 9:43 AM
suspicious email	2/13/2023 11:20 AM

18 items 1 item selected 34 bytes

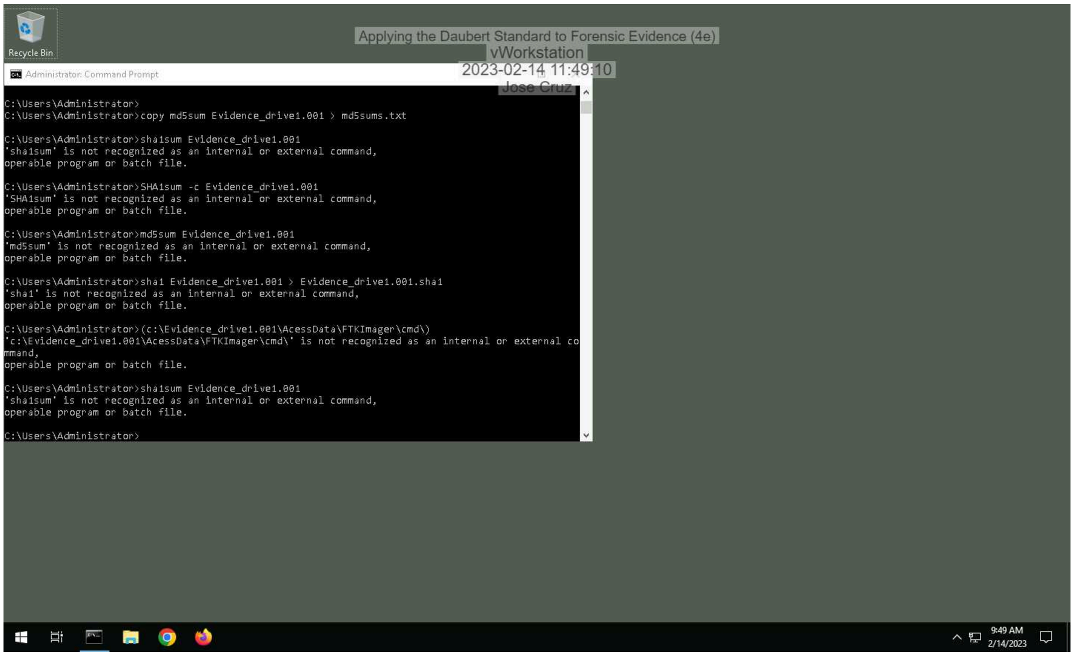
8. **Describe** how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

Seems the hash values change from the apps.

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**.


Recycle Bin
Applying the Daubert Standard to Forensic Evidence (4e)
vWorkstation
2023-02-14 11:49:10
Jose Cruz
Administrator: Command Prompt
9:49 AM
2/14/2023

```
C:\Users\Administrator>
C:\Users\Administrator>copy md5sum Evidence_drive1.001 > md5sums.txt

C:\Users\Administrator>sha1sum Evidence_drive1.001
'sha1sum' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>SHA1sum -c Evidence_drive1.001
'SHA1sum' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>md5sum Evidence_drive1.001
'md5sum' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>sha1 Evidence_drive1.001 > Evidence_drive1.001.sha1
'sha1' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>(c:\Evidence_drive1.001\AcessData\FTKImager\cmd\)
'c:\Evidence_drive1.001\AcessData\FTKImager\cmd\' is not recognized as an internal or external co
mmand,
operable program or batch file.

C:\Users\Administrator>sha1sum Evidence_drive1.001
'sha1sum' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>
```

Part 2: Locate Additional Evidence

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

Incomplete