

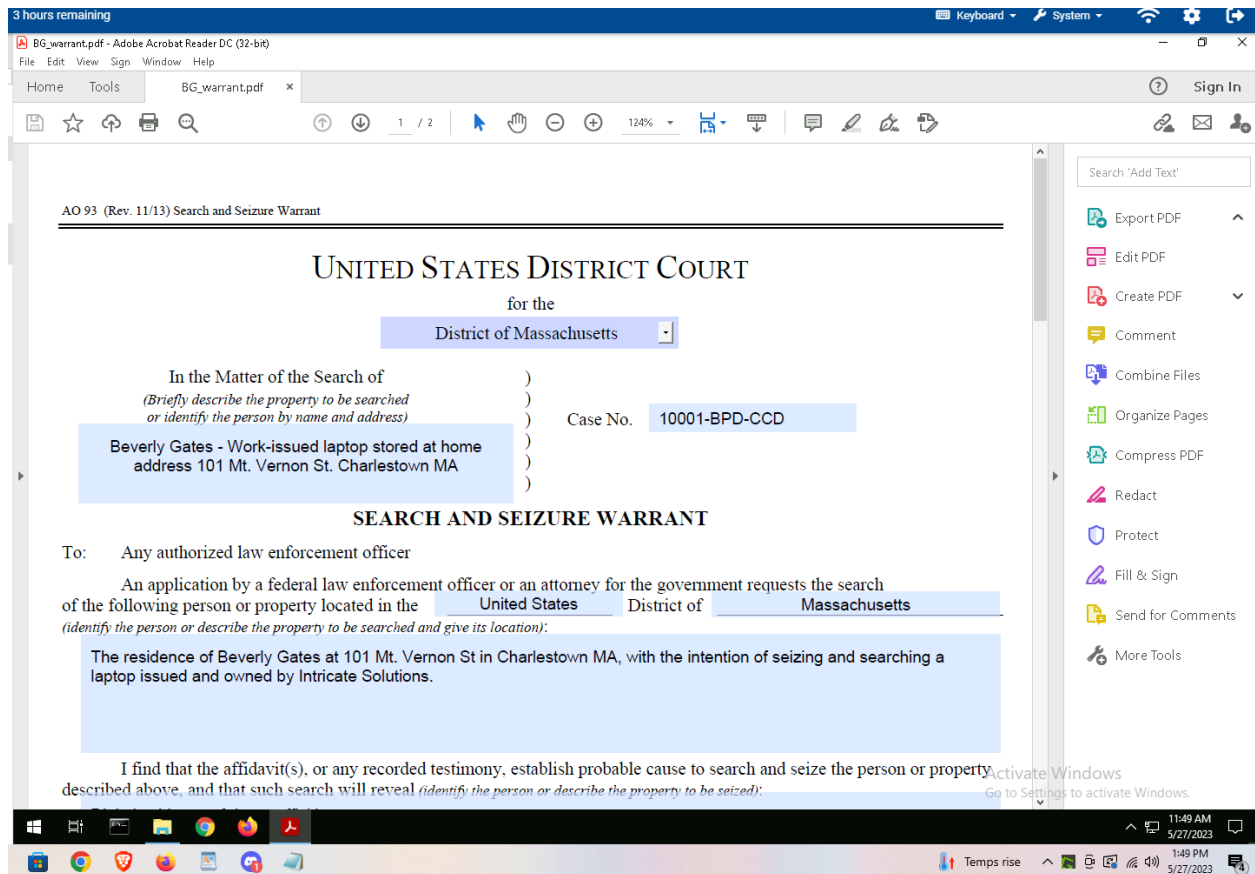
James Tourtellotte

ITN 276 - Computer Forensics

Lab 1 - Applying the Daubert Standard to Forensic Evidence

5/27/2023

Screencap 1:



ScreenCap 2:

JamesTourtellotte_chain_of_custody_10001.pdf - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools JamesTourtellotte_c...

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

Create PDF

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

Activate Windows

Go to Settings to activate Windows.

Police Cyber Crimes Division

Computer Evidence Chain of Custody

Item Number(s): 0000-1
Case: 00001-BPS-CCD

To be completed by initial collector:

Evidence collected by (name): JAMES JAMES
Date/Time collected: 1:30 PM, April 19, 2021
Evidence description:
[Use image taken from seized cell laptop]

Describe Collection method (include operating system, utility, commands, arguments, etc):
[Use image generated using PTK image from Windows 10 workstation]

What application software/utility is required to view the file?:
PTK Image 2.0, Autopsy, Encase, or comparable

Where is evidence initially stored?: [Use image is stored on BPS file server, source laptop stored in BPS police locker]
How is evidence initially secured?: Windows BitLocker Encryption
Collector signature: [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): Brandon O'Rourke
Transferred to (print name, sign & date): James Tourtellotte 5/27/2023
Where is evidence now stored?: [Redacted]
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?:

Windows Taskbar: 71°F Cloudy, 11:52 AM 5/27/2023

Screen Cap 3:

(4e)

Keyboard System

0002665_hash - Notepad

File Edit Format View Help

MD5, SHA1, FileNames

```
"a2f4e5c365c0413bbf14cfc7ba48890", "00fa108cd5dada2f64340961c240a24065b6e9c6", "Evidence_drive1.001\NOMNAME [NTFS]\[unallocated space]\0002665"
```

Windows (CRLF) Ln 1, Col 1

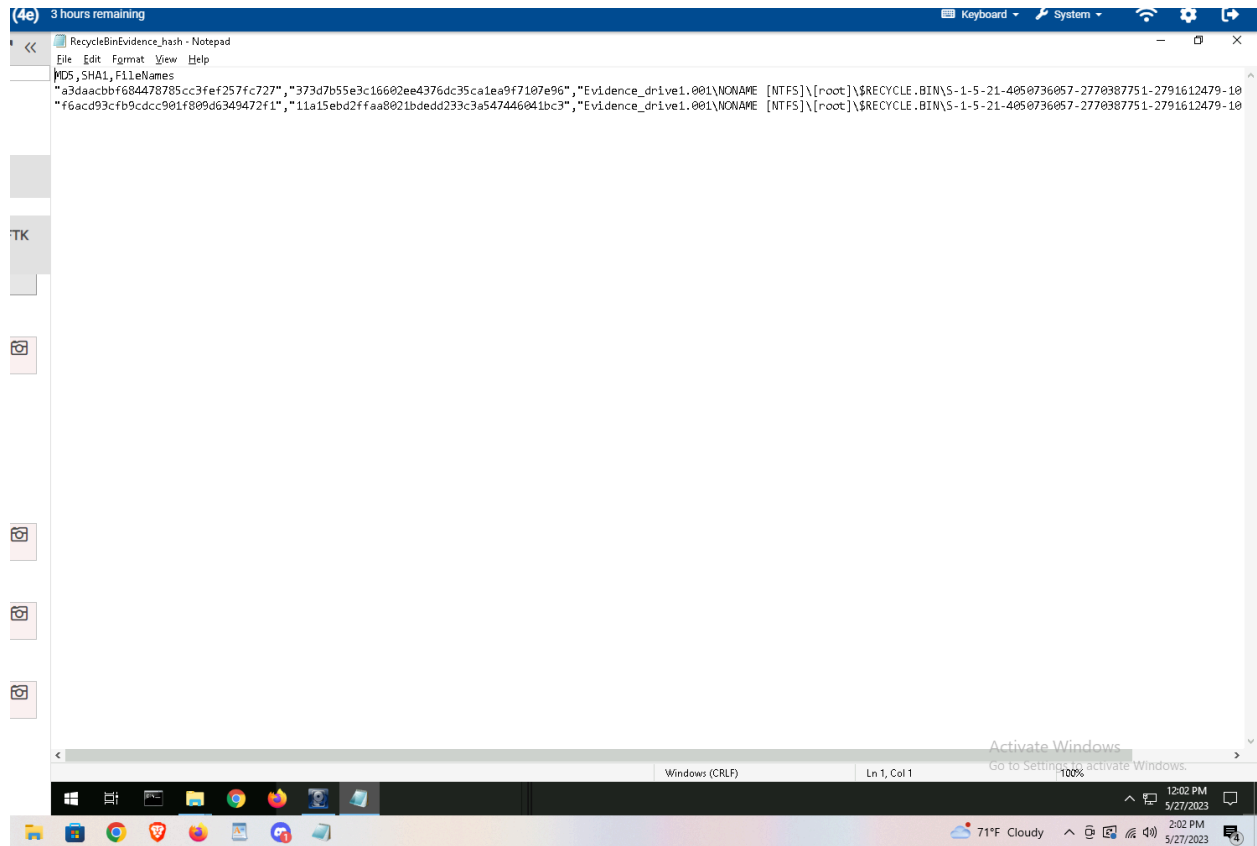
Activate Windows

Go to Settings to activate Windows.

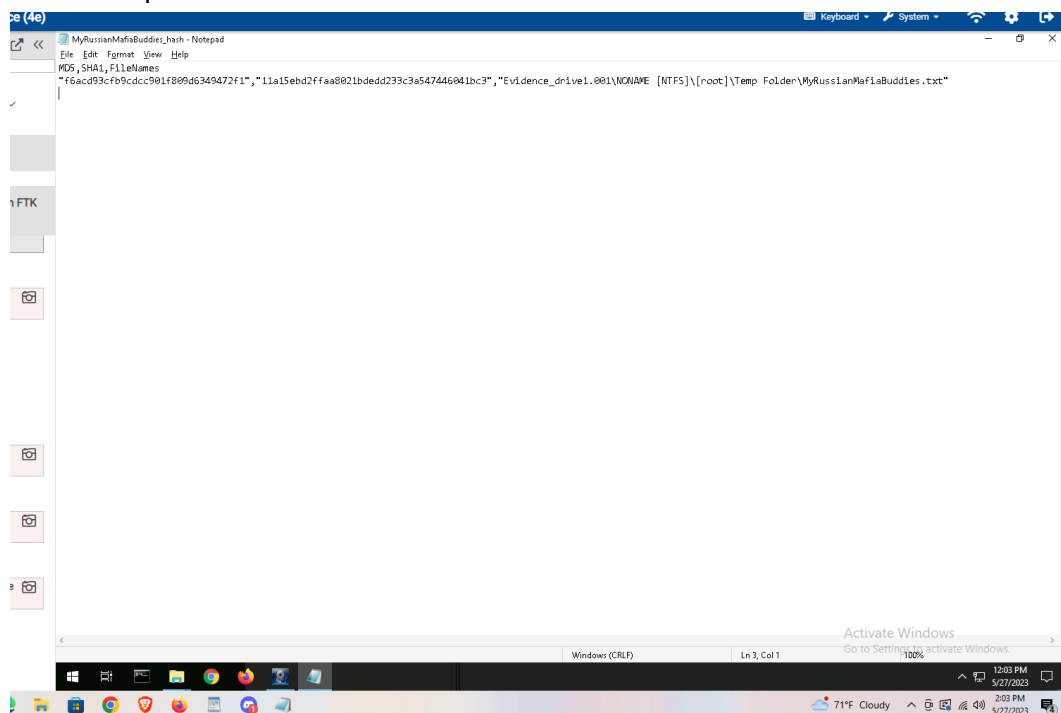
100%

Windows Taskbar: Temps rise, 12:01 PM 5/27/2023

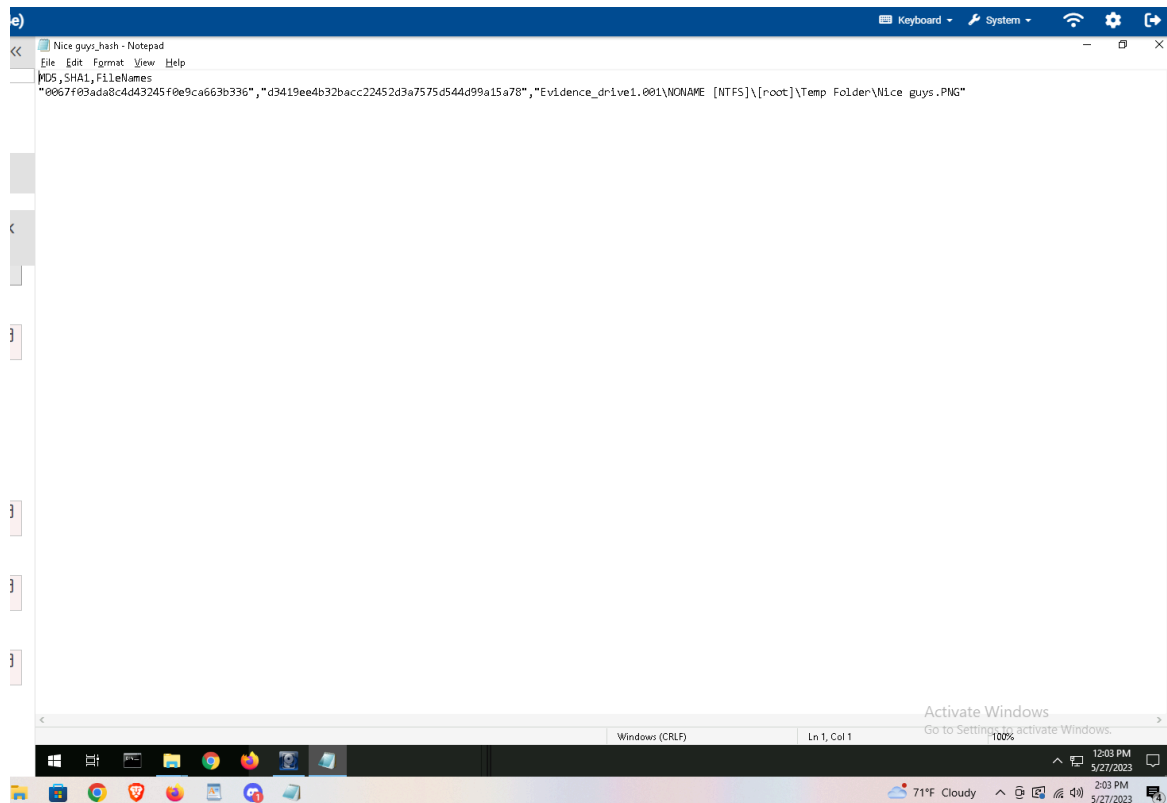
Screen Cap 4:



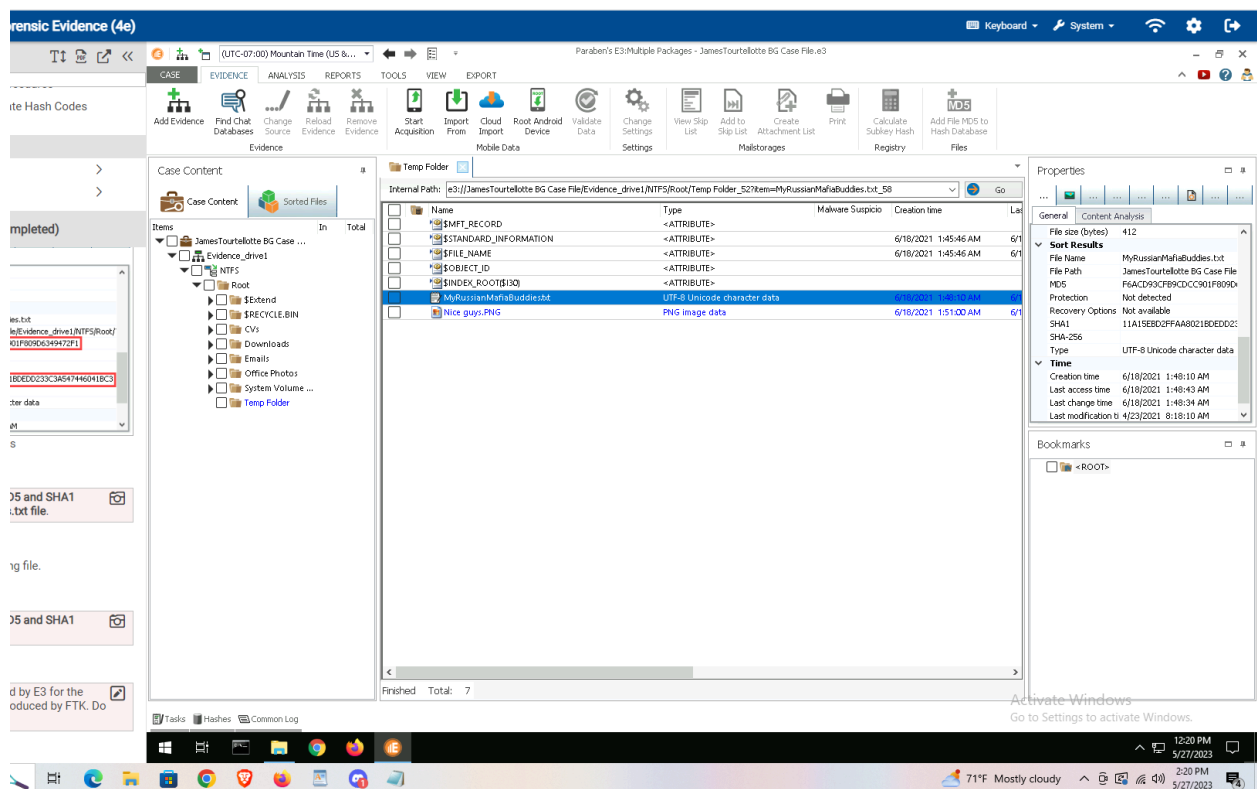
Screen Cap 5:



Screen Cap 6:



Screen Cap 7:



Screen Cap 8:

The screenshot displays the 'Forensic Evidence (4e)' application. The main window shows a file list with columns for Name, Type, Malware Suspicion, Creation time, and Last access time. The selected file is 'Nice guys.PNG', which is a PNG image data file created on 6/18/2021 at 1:46:10 AM. The Properties pane on the right shows details for this file, including its size (11,836 bytes) and SHA1 hash (D3419EE4B32ACC22452D3A7). The left pane shows the file tree structure, including 'Evidence_drive1', 'Root', '\$Extend', '\$RECYCLE.BIN', 'CVs', 'Downloads', 'Emails', 'Office Photos', 'System Volume', and 'Temp Folder'.

Name	Type	Malware Suspicion	Creation time	Last access time
\$EMFT_RECORD	<ATTRIBUTE>			
\$STANDARD_INFORMATION	<ATTRIBUTE>		6/18/2021 1:45:46 AM	6/18/2021 1:45:46 AM
\$FILE_NAME	<ATTRIBUTE>			
\$OBJECT_ID	<ATTRIBUTE>			
\$INDEX_ROOT(\$I30)	<ATTRIBUTE>			
MyRussianMafiaBuddies.txt	UTF-8 Unicode character data		6/18/2021 1:46:10 AM	6/18/2021 1:46:10 AM
Nice guys.PNG	PNG image data		6/18/2021 1:46:10 AM	6/18/2021 1:46:10 AM

Screen Cap 9:

The screenshot displays the 'Forensic Evidence (4e)' application with the 'AccessData FTK Imager 4.5.0.3' window open. The 'Evidence Tree' shows the file 'Re_Staff purchase request.eml' selected. The main window displays the email content, which is a message from Mrs. Maxloff to Eliot Jeffery. The email body text is as follows:

Re_Staff purchase request.eml - Notepad

Kind regards, Eliot Jeffery

From: Mrs. Maxloff <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 standust or this new hoity-toity extreme stan dust?

On 4/26/2021 1:15 PM, Eliot Jeffery wrote:
Hello Mrs Maxloff,
Thank you for your quick reply. I really need the very best stuff for my best friend. She b

Kind regards Eliot Jeffery

Screen Cap 10:

The screenshot displays the Autopsy 4.18.0 interface. The left sidebar shows the 'Data Sources' tree with 'Evidence_drive1.001' expanded, revealing various file types including 'Emails (5)'. The 'Re_ Stuff purchase request.eml (1)' file is selected. The main pane shows a 'Listing' of files, with 'From-the-movie-Stardust.jpg' highlighted. Below the listing, a 'File Metadata' table is visible, showing details for the selected file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(0)
From-the-movie-Stardust.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	169210	Allocate

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
MD5			5b37cf5bae05a7770f9041844bb7cdca				
SHA-256			1f64d992aea2459932b592b802de19404d8fedc069a684e614046405a38dce29				
Hash Lookup Results			UNKNOWN				
Internal ID			130				

Activate Windows
Go to Settings to activate Windows.

1:38 PM
5/27/2023
71°F Cloudy
3:38 PM
5/27/2023

Screen Cap 11:

