

LAB FINAL EXAMINATION

BY:
ABDULLAH (FA22-BCT-004)
SUBMITTED TO:
MR. MUSTAFA KHATTAK



MAY 15, 2024
COMSATS UNIVERSITY
ISLAMABAD

Contents

1.	Examining a Forensic Image with Autopsy:	2
2.	Network Forensic using Wireshark.	7
3.	Rhino Hunt with Autopsy:	19
4.	Rhino Hunt with Wireshark	26
5.	Memory Analysis with Autopsy.....	33
6.	Memory Forensics of LastPass and Keeper.....	40
7.	Capturing and examining the registry	49
8.	Examining a window disk image.	55
9.	Email Forensics:.....	63
10.	Android Studio Emulator.....	68
11.	Rooting Android Studio's Emulator AND 14.....	77
12.	Forensic Acquisition from Android	82
13.	Android Analysis with Autopsy	90
15.	iPhone Analysis with Autopsy.....	95
16.	Windows and Linux Machines	101
17.	Velociraptor Server on Linux.....	103
18.	Investigating a PUP with Velociraptor.....	112
19.	Investigating a Bot with Velociraptor	118
20.	Investigating a Two-Stage RAT with Velociraptor	129

1. Examining a Forensic Image with Autopsy:

CREATING A CASE:

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: F200

Base Directory: D:\FinalDFProj\FIA

Case Type: Single-User Multi-User

Case data will be stored in the following directory:
D:\FinalDFProj\FIA\F200

< Back Help

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number: F200

Examiner

Name: Abdullah

Phone: 031030657860

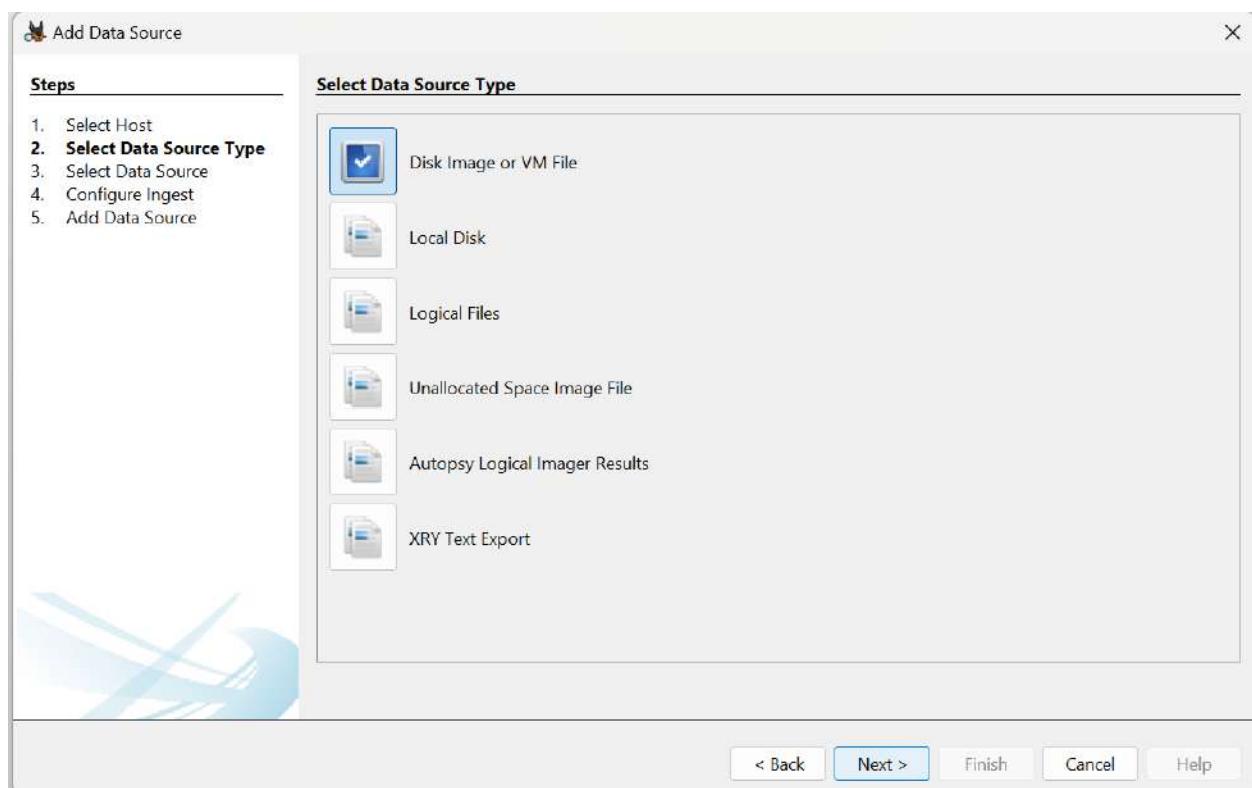
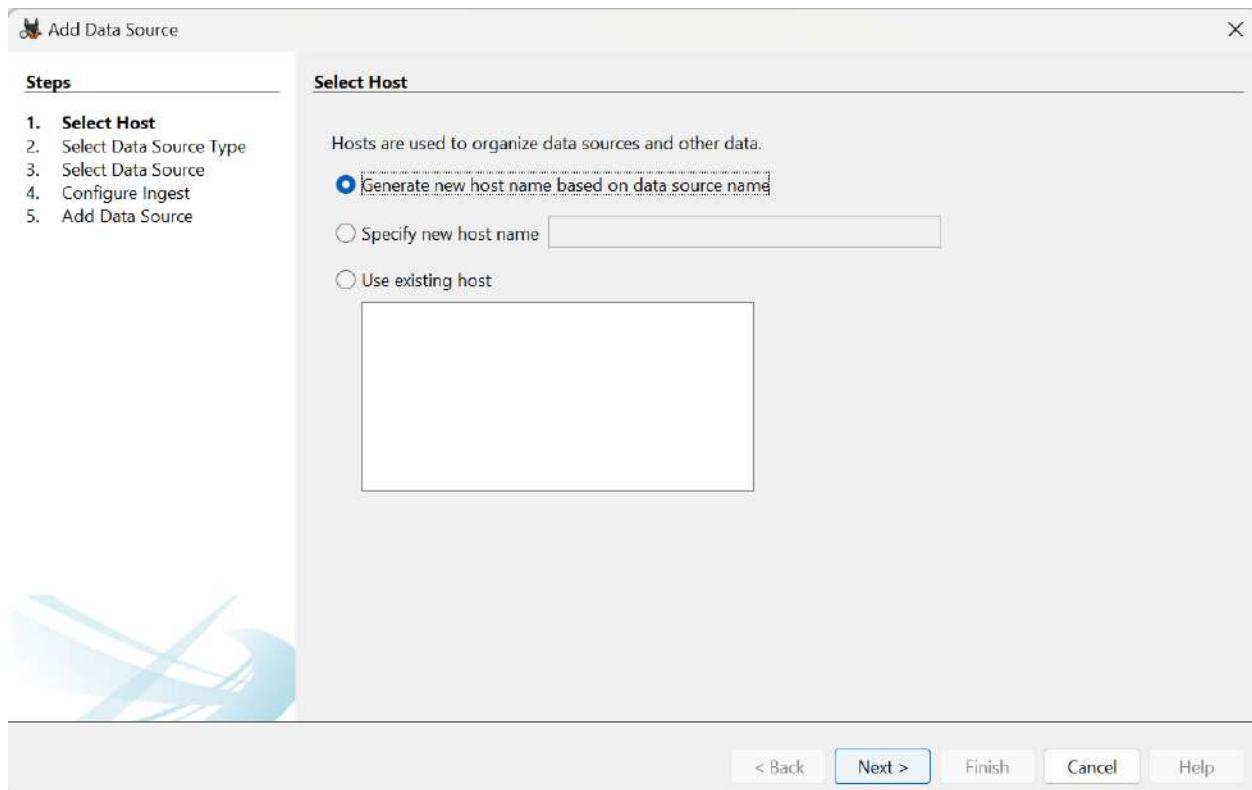
Email: abdullahamqbool08@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

< Back Help



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
- 3. Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: D:\FinalDFProj\FIA\F200.E01

Ignore orphan files in FAT file systems

Time zone: (GMT+5:00) Asia/Karachi

Sector size: Auto Detect

Hash Values (optional):

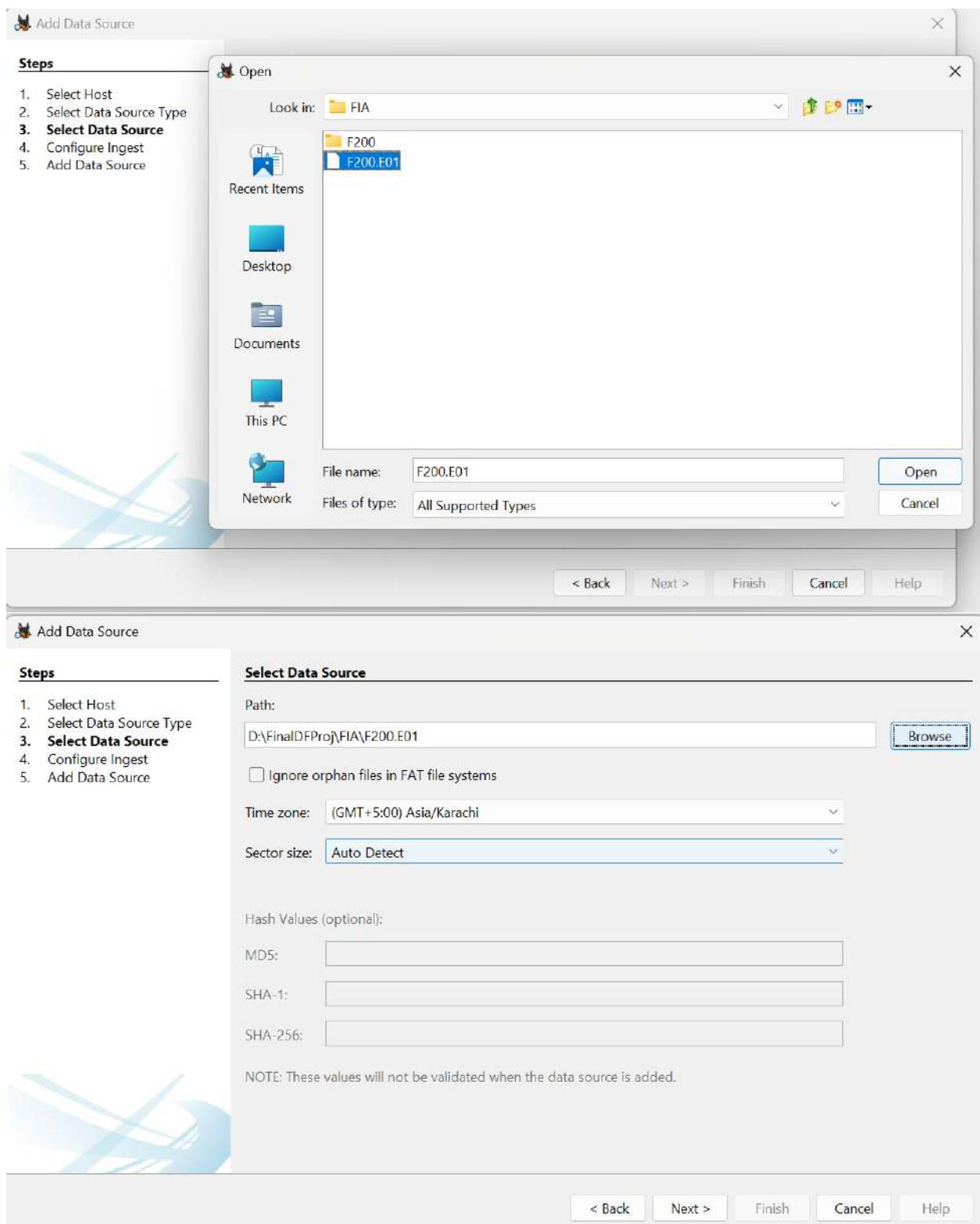
MD5:

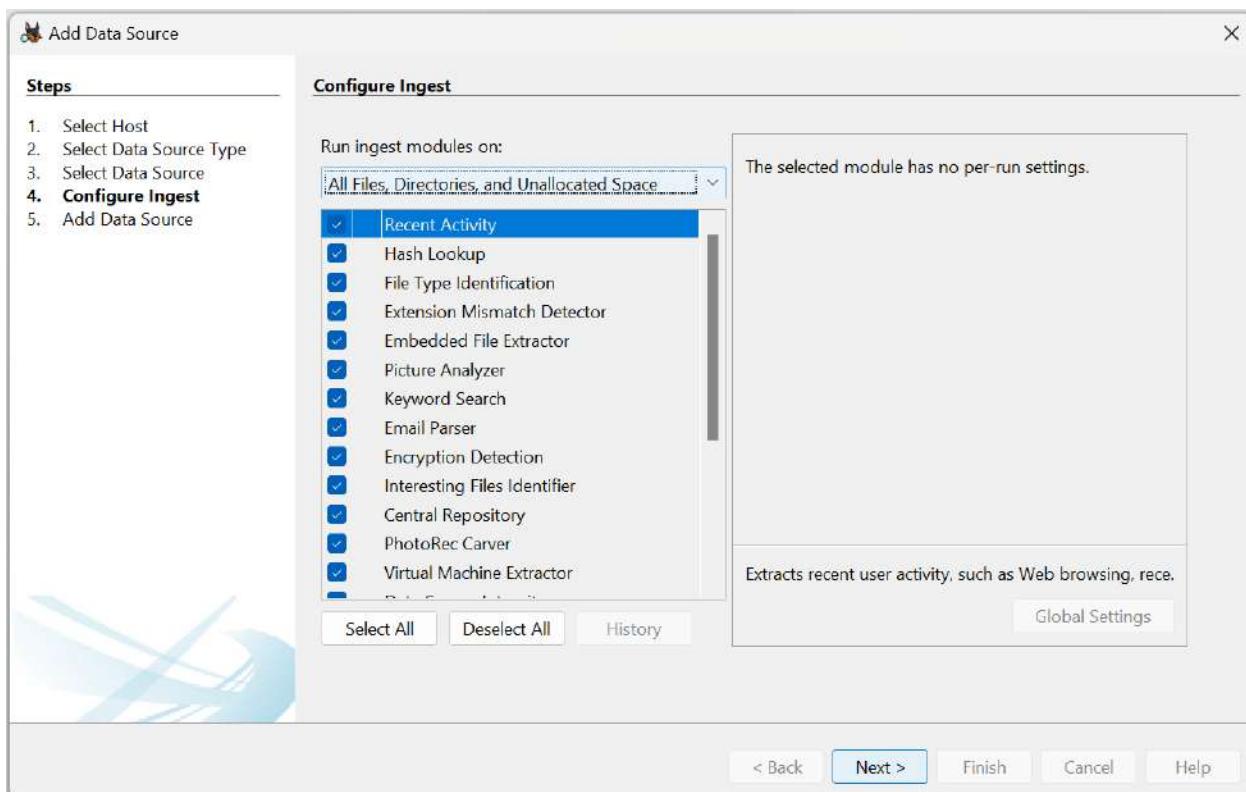
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help





FLAG 1 FINDING:

The screenshot shows the main workspace of the F200 - Autopsy 4.21.0 interface. On the left, the navigation pane includes 'Data Sources', 'File Views', 'File Types' (with 'Images (2)' selected), 'By Extension', 'By MIME Type', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The central area displays a table titled 'Listing' with two entries: 'Flag1.bmp' and 'Doggie.PNG'. The table columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The 'Flag1.bmp' entry has a size of 120054, is Allocated, and is located at '/img_F200_E01/vol'. The bottom panel shows a detailed view of the 'Flag1.bmp' file, with the text 'The flag is EVIDENCE' visible.

HELLO WORLD FINDING:

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar contains navigation links such as Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, MB File Size, Data Artifacts, Analysis Results, OS Accounts, Tags, Score, and Reports. The main area displays a search results table for 'HelloWorld'. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. One entry is listed: HelloWorld, with details: S: 0, O: 0, Modified Time: 2022-08-20 09:09:13 PCT, Change Time: 2022-08-20 09:09:13 PCT, Access Time: 2022-08-20 09:10:25 PCT, Created Time: 2022-08-20 09:10:25 PCT, Size: 15, Flags(Dir): Allocated, Flags(Meta): Allocated, Known: Unknown, Location: /img/F100/E01/vol_vol2/h. Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The Text tab is selected, showing the content "Hello, World!". There are also tabs for Strings, Extracted Text, and Translation. At the bottom, there are buttons for Page: 1 of 1 Page, Matches on page: - of - Match, 100%, and Reset.

2. Network Forensic using Wireshark.

EXAMINING LAYERS 1-4

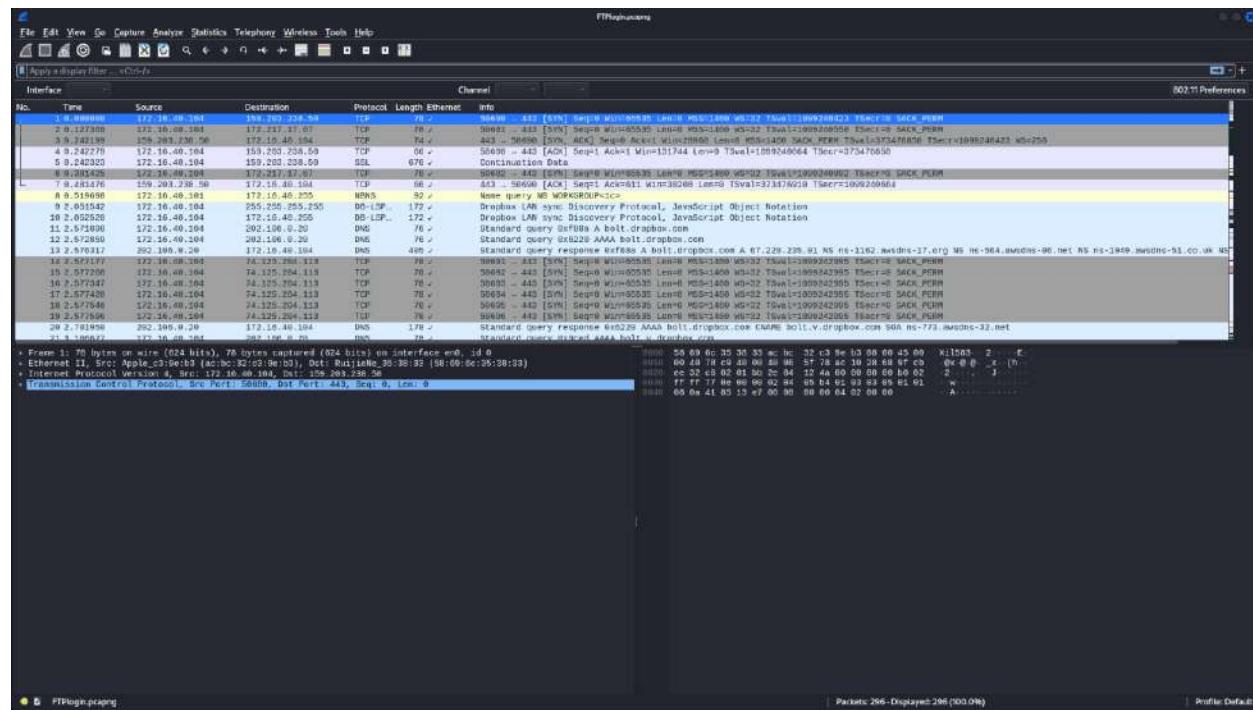
FTP LOGIN FILE DOWNLOAD:

```
(kali㉿kali)-[~/Desktop/DF/nf]
$ wget https://bowneconsultingcontent.com/pub/EH/proj/FTPLogin.pcapng
--2024-04-30 13:45:18-- https://bowneconsultingcontent.com/pub/EH/proj/FTPLogin.pcapng
Resolving bowneconsultingcontent.com (bowneconsultingcontent.com) ... 74.208.236.111,
2607:f1c0:100f:f000::28a
Connecting to bowneconsultingcontent.com (bowneconsultingcontent.com)|74.208.236.111|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 41856 (41K)
Saving to: 'FTPLogin.pcapng'

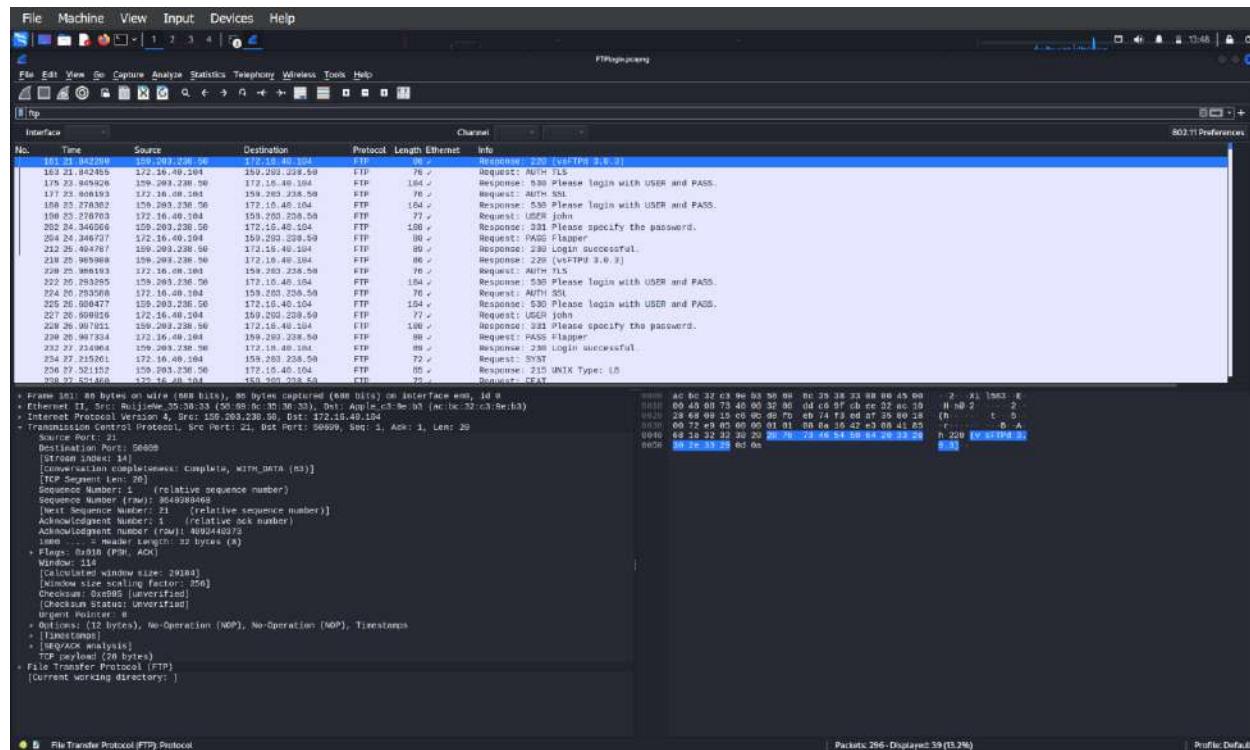
FTPLogin.pcapng      100%[=====] 40.88K   117KB/s    in 0.3s

2024-04-30 13:45:26 (117 KB/s) - 'FTPLogin.pcapng' saved [41856/41856]

(kali㉿kali)-[~/Desktop/DF/nf]
$ ls
FTPLogin.pcapng
```

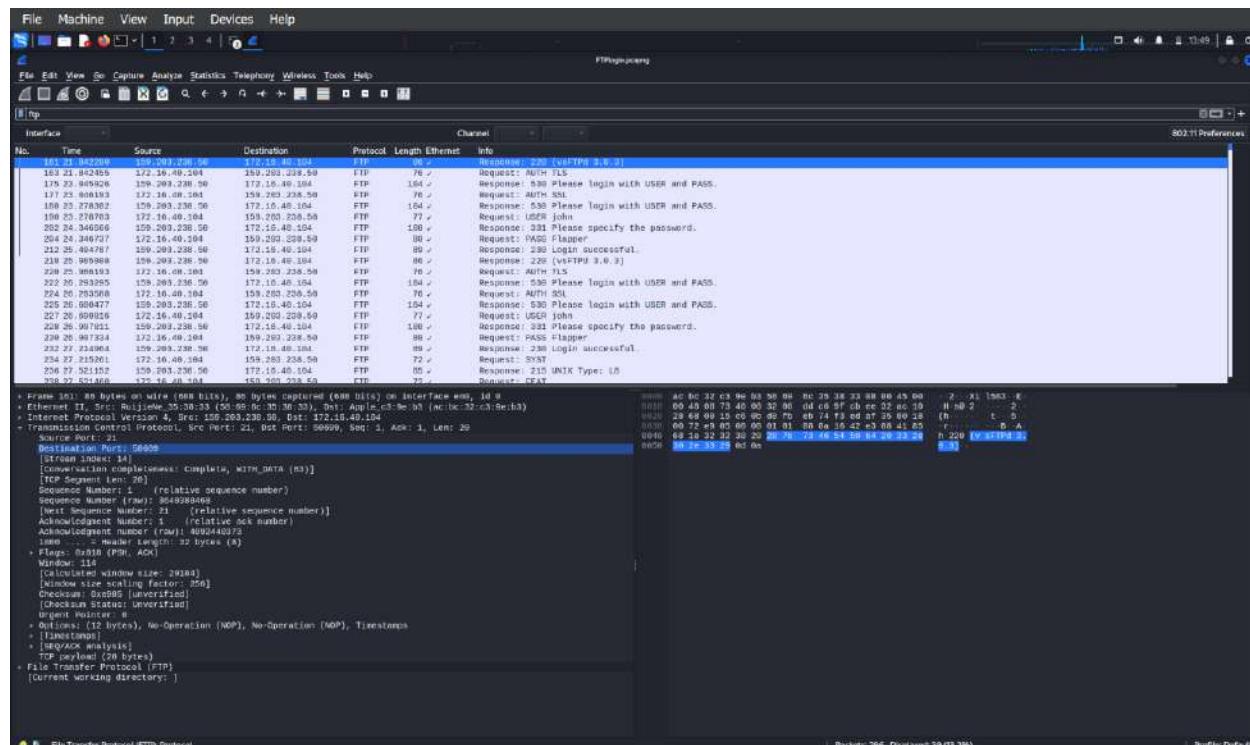


FTP FILE FILTER:

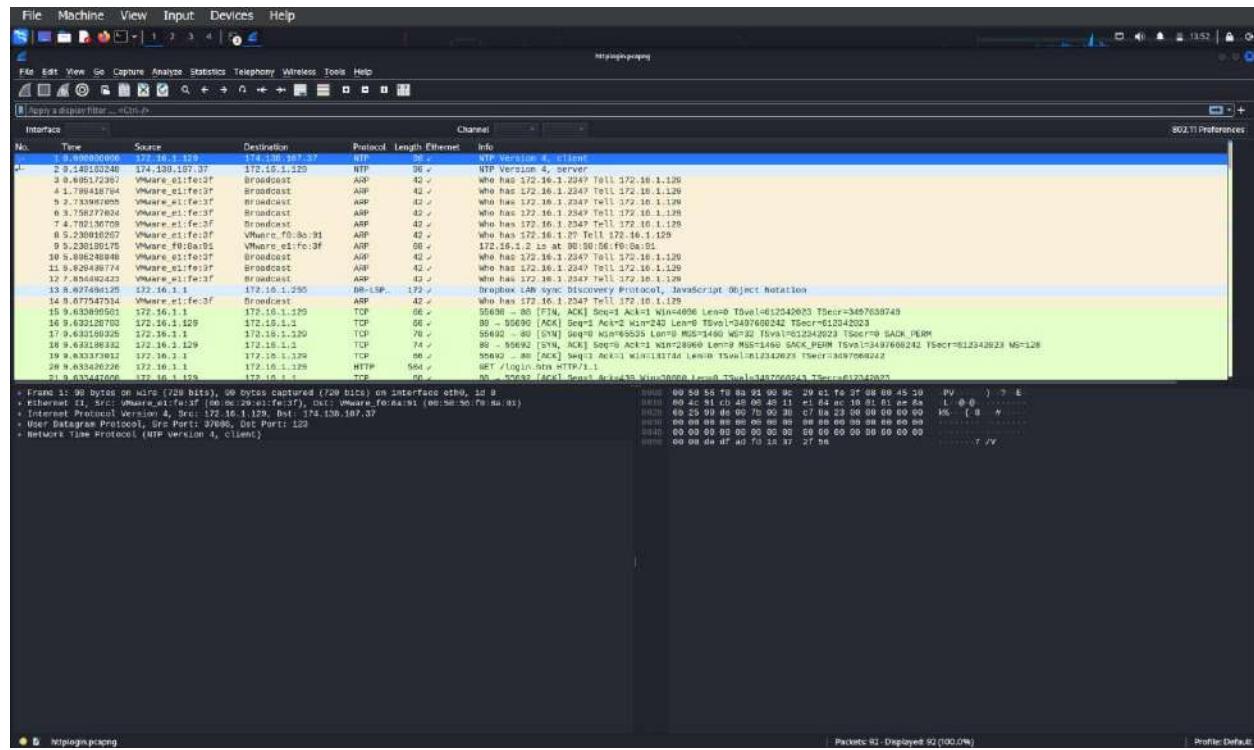


JOHN PASSWORD:

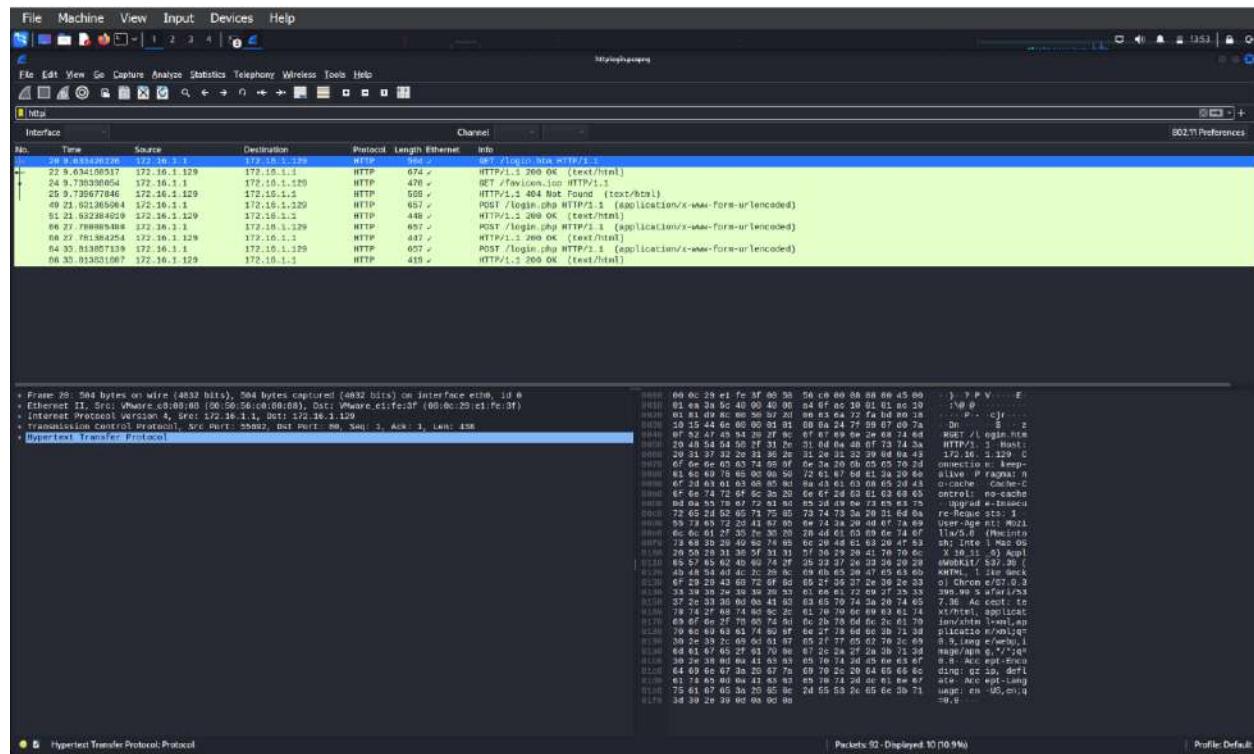
PASS



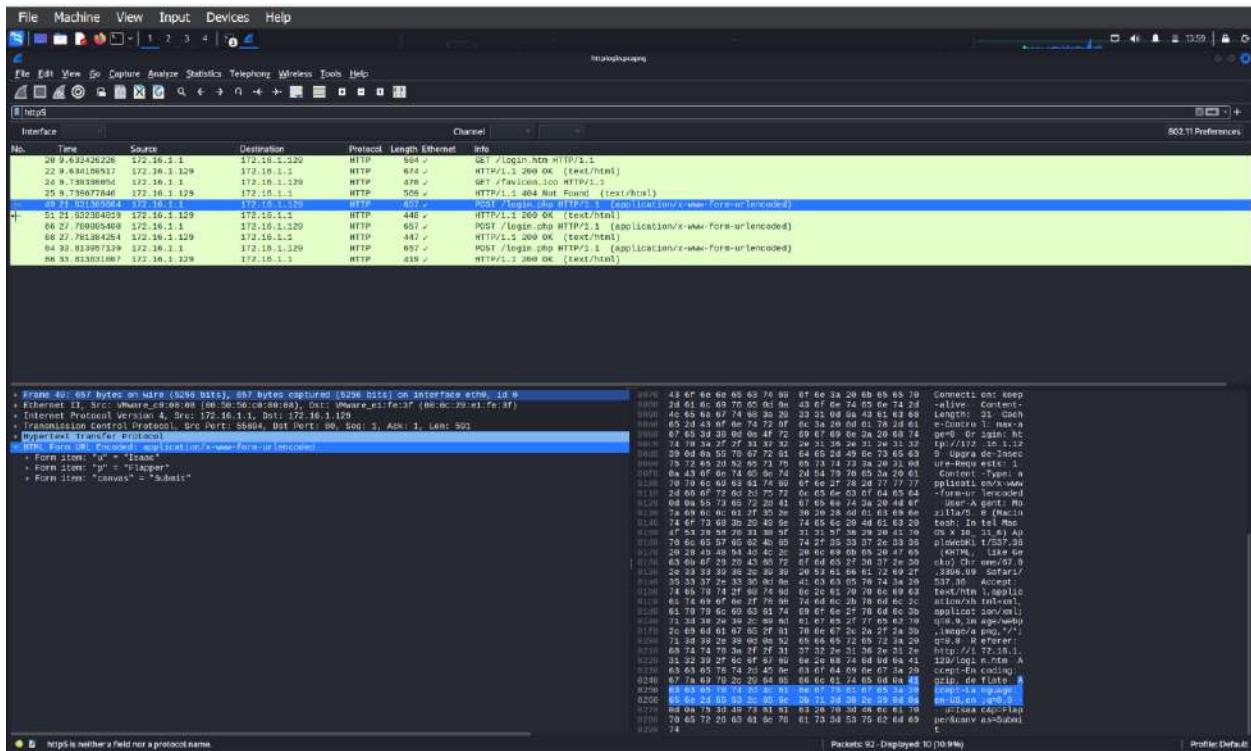
FINDING HTTP PASSWORD:



HTTP PACKET FILTER:



USERNAME ISAAC AND FLAPPER:



FOLLOWING TCP STREAM:

The screenshot shows a Wireshark window titled "Wireshark - Follow TCP Stream (tcp.stream eq 2) - httplogin.pcapng". The main pane displays a single TCP stream (Stream 2) with the following details:

- Request Headers:**

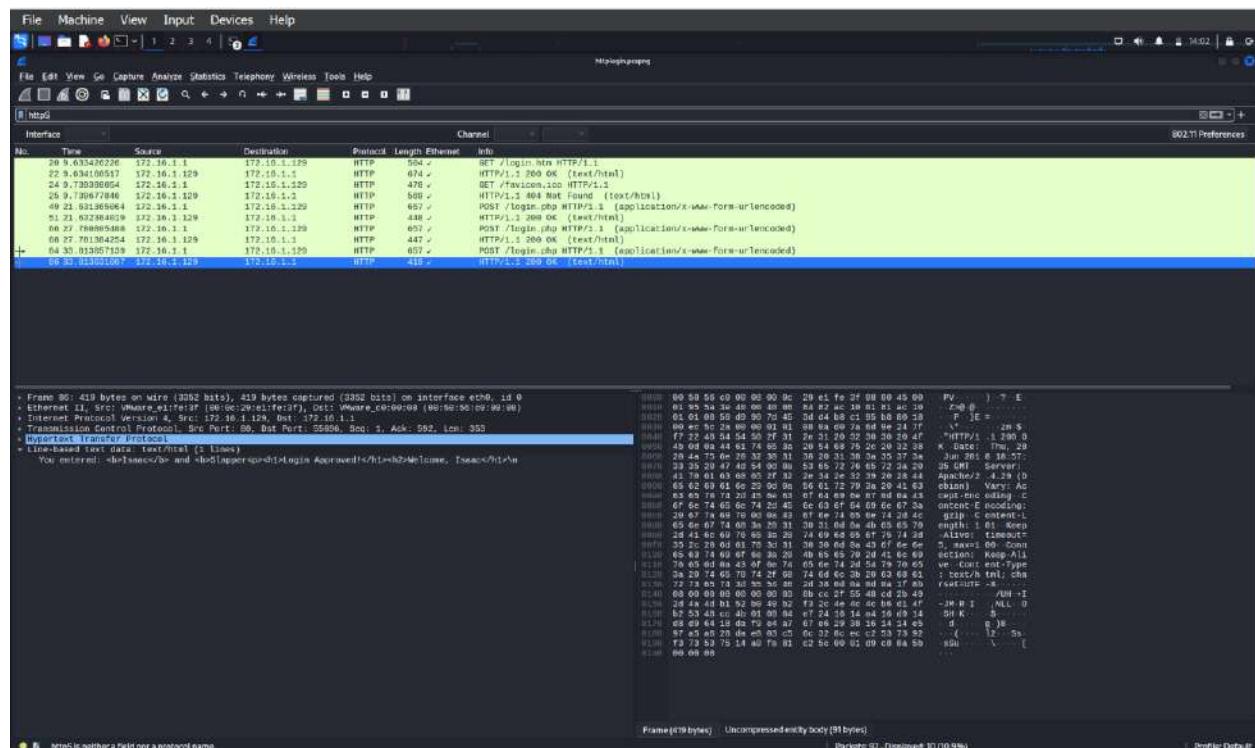
```
POST /login.php HTTP/1.1
Host: 172.16.1.129
Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=6
Origin: http://172.16.1.129
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://172.16.1.129/login.htm
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```
- Response Headers:**

```
HTTP/1.1 200 OK
Date: Thu, 28 Jun 2018 18:57:22 GMT
Server: Apache/2.4.29 (Debian)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 130
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```
- Data:**

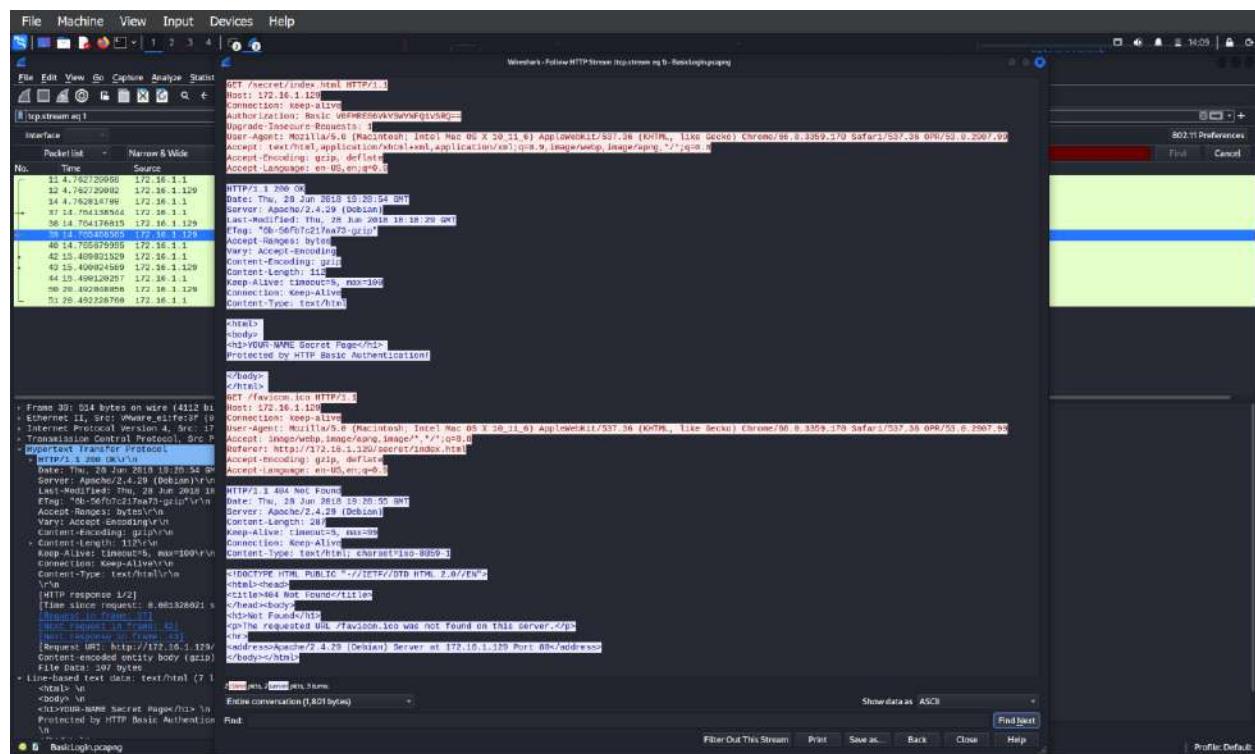
```
.....En.E...1.....E.....M\..0..2..".k..c.R....z....Y...N'.my..n.!}...B.a..f
....p.3..Q'..0.n}...  
.....
```

The bottom status bar indicates "1 client pkt, 1 server pkt, 7 turn." and "Entire conversation (973 bytes)". The interface also includes buttons for "Find Next", "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help".

ISAAC PASSWORD “SLAPPER”:



HTTP BASIC AUTHENTICATION:



WALDO PASSWORD:

The screenshot shows the DEF24.com web application. On the left, there's a sidebar with various tools like Operations, Favourites, and Networking. The main area has tabs for Recipe, Input, and Output. In the Recipe tab, it says "From Base64" and shows the input "V0FMREB6VkvVSvNfQ1v5RQ==". Below that, there's a dropdown for "Alphabet" set to "A-Za-z0-9+=", a checked checkbox for "Remove non-alphabet chars", and an unchecked checkbox for "Strict mode". A large green button labeled "BAKE!" with a chef icon is centered. The Output tab shows the result "WALDO:VERYSECURE". At the bottom, there are tabs for Hex, Raw Bytes, and LF.

APT CAPTURE:

This screenshot shows a Wireshark capture window. The top menu bar includes File, Machine, View, Input, Devices, Help, and a toolbar with icons for file operations. The main pane displays a list of network frames. The first frame is selected, showing details for a "Server Hello" message. The packet list shows several frames related to a TLS session, including Client Key Exchange, Change Cipher Spec, and Encrypted Handshake Message frames. The details and bytes panes show the raw hex and ASCII data for these frames. The bottom status bar indicates "Packets: 72876 - Displayed: 51 (0.7%)".


```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\FinalDFProj> Get-FileHash -Algorithm SHA1 .\socat

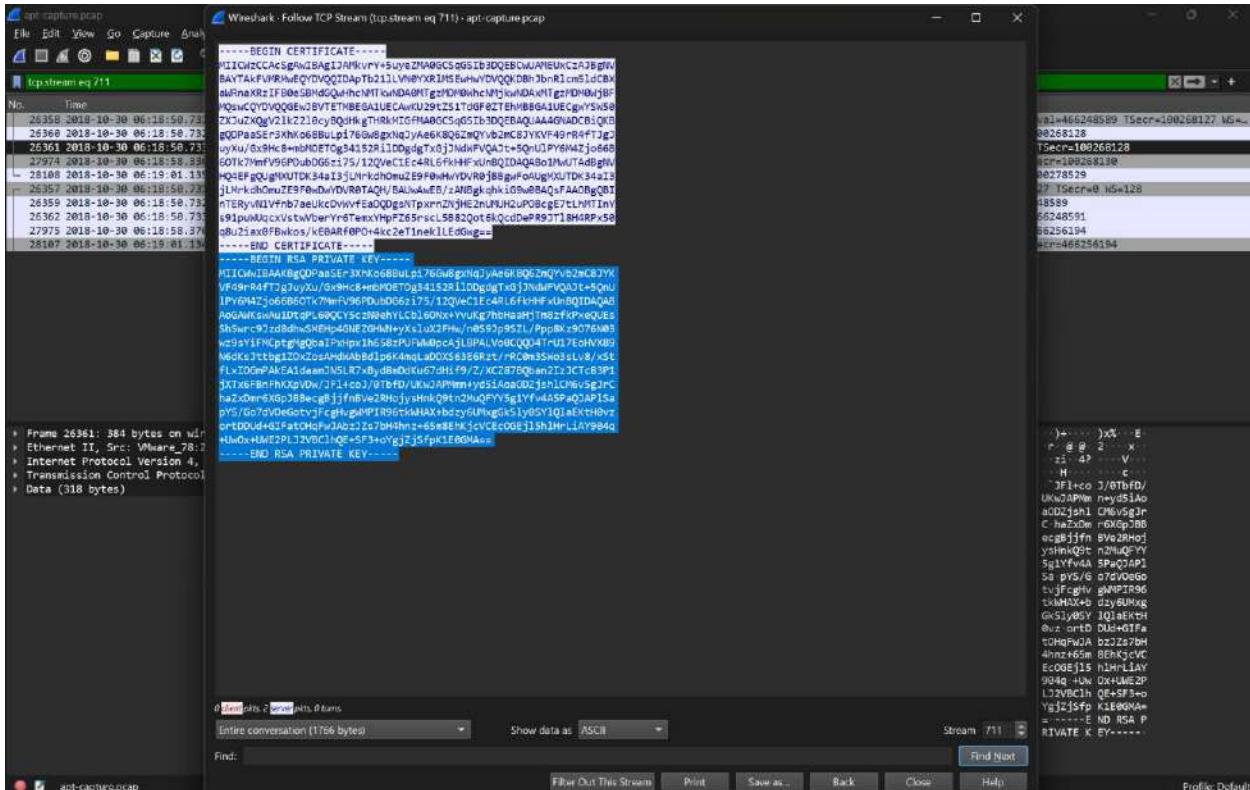
Algorithm      Hash
----          ---
SHA1          DA8FF40C6A60605C4D250AAE59912F1E60315C81

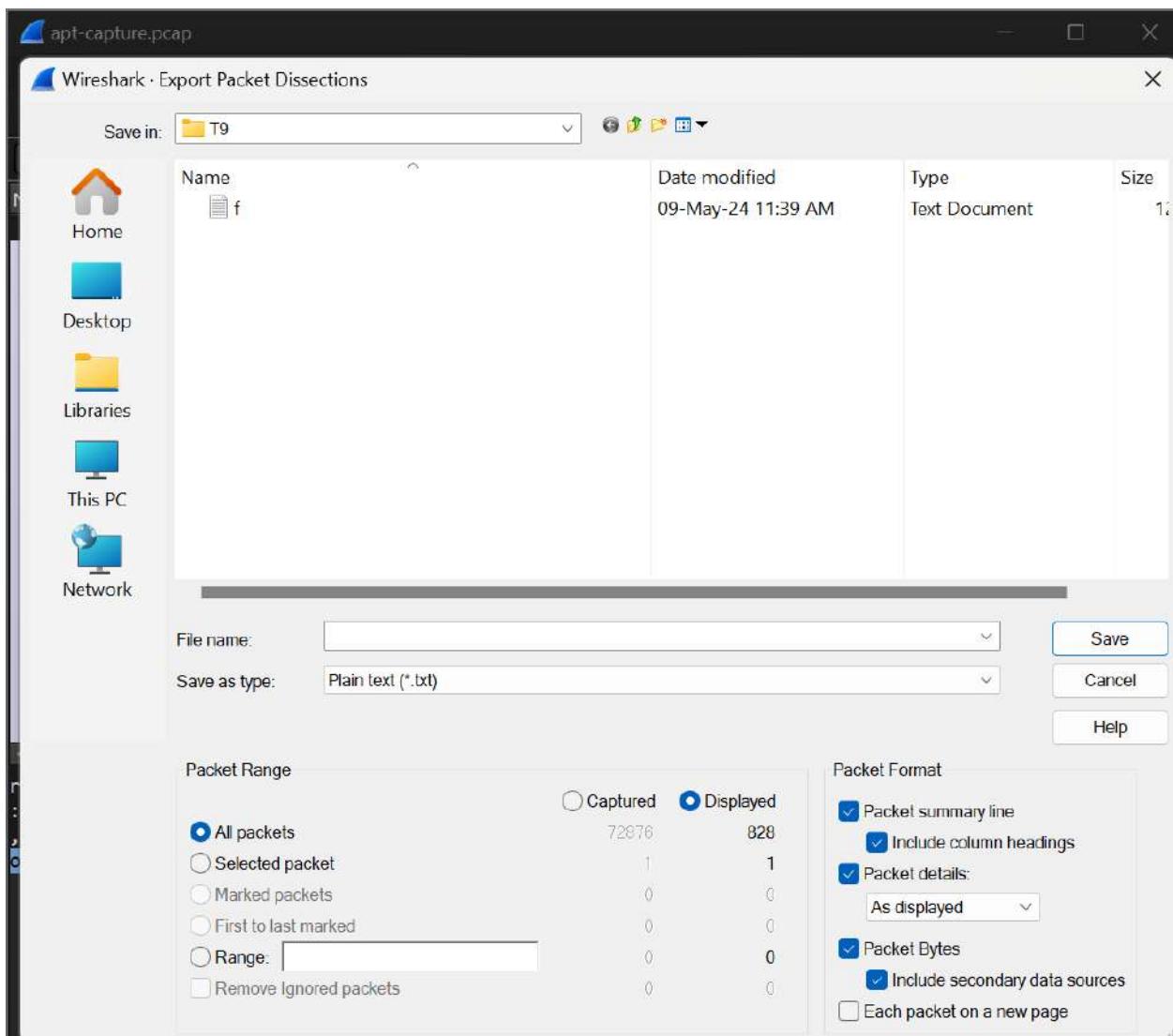
Path
----          D:\FinalDFProj\socat

PS D:\FinalDFProj>

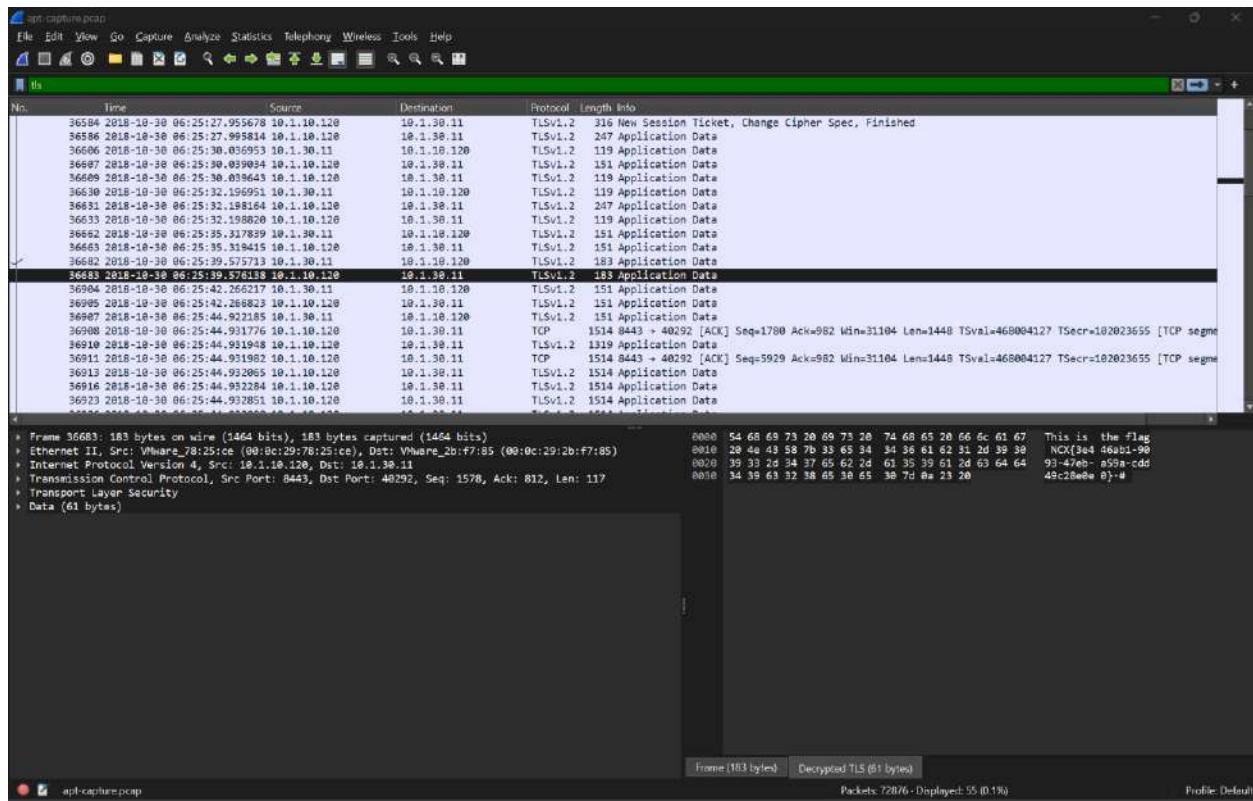
```

DECRYPT:

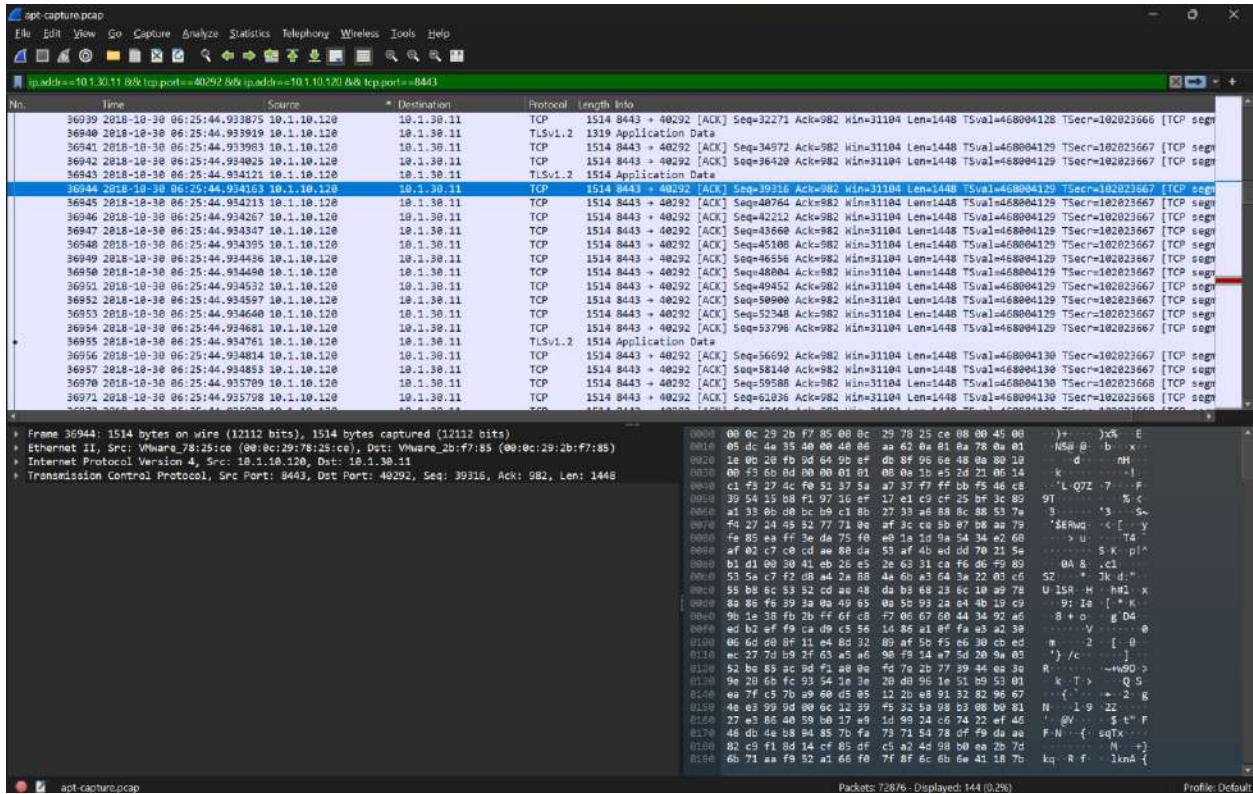




PORT KNOCKING:



EXPLOITATION:



3. Rhino Hunt with Autopsy:

VERIFYING HASH VALUES:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\user\Downloads> Get-FileHash -Algorithm MD5 .\case1.zip

Algorithm      Hash
-----        -----
MD5           6A80946A0FE694C12683A91019D6D2EF

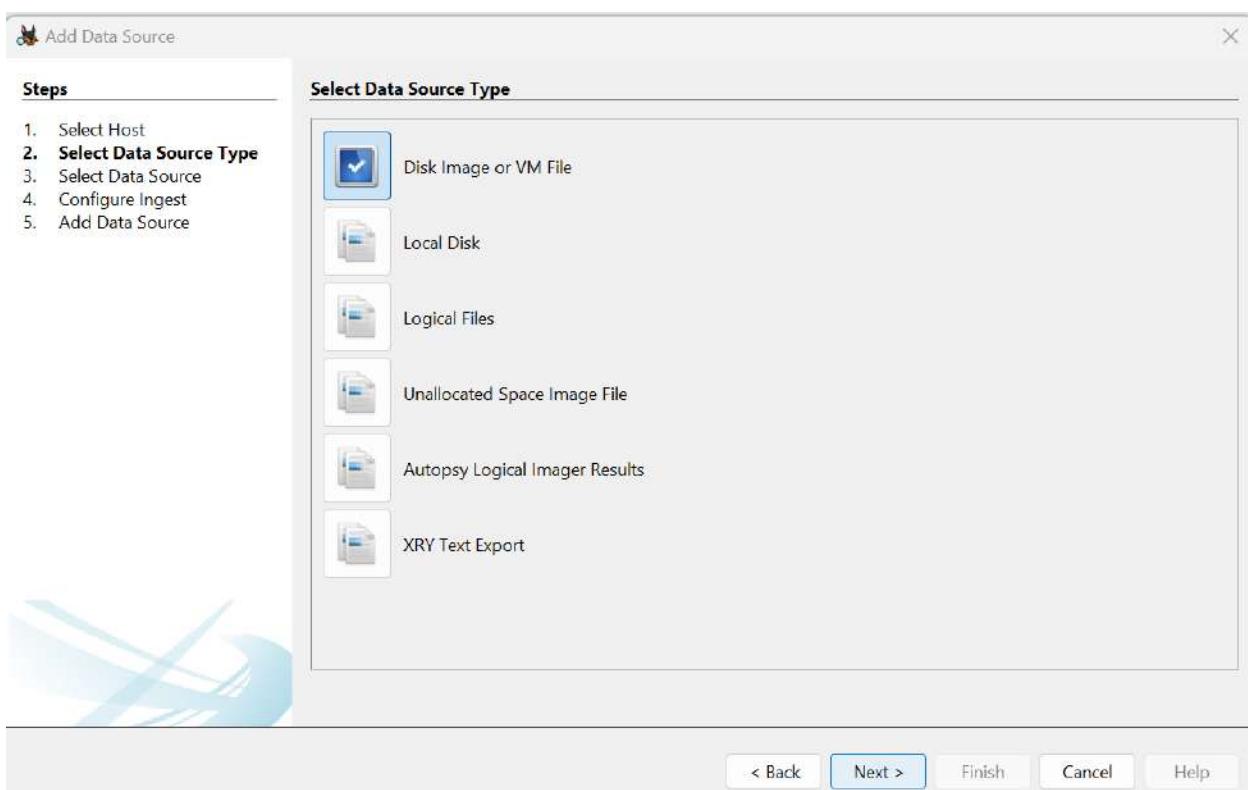
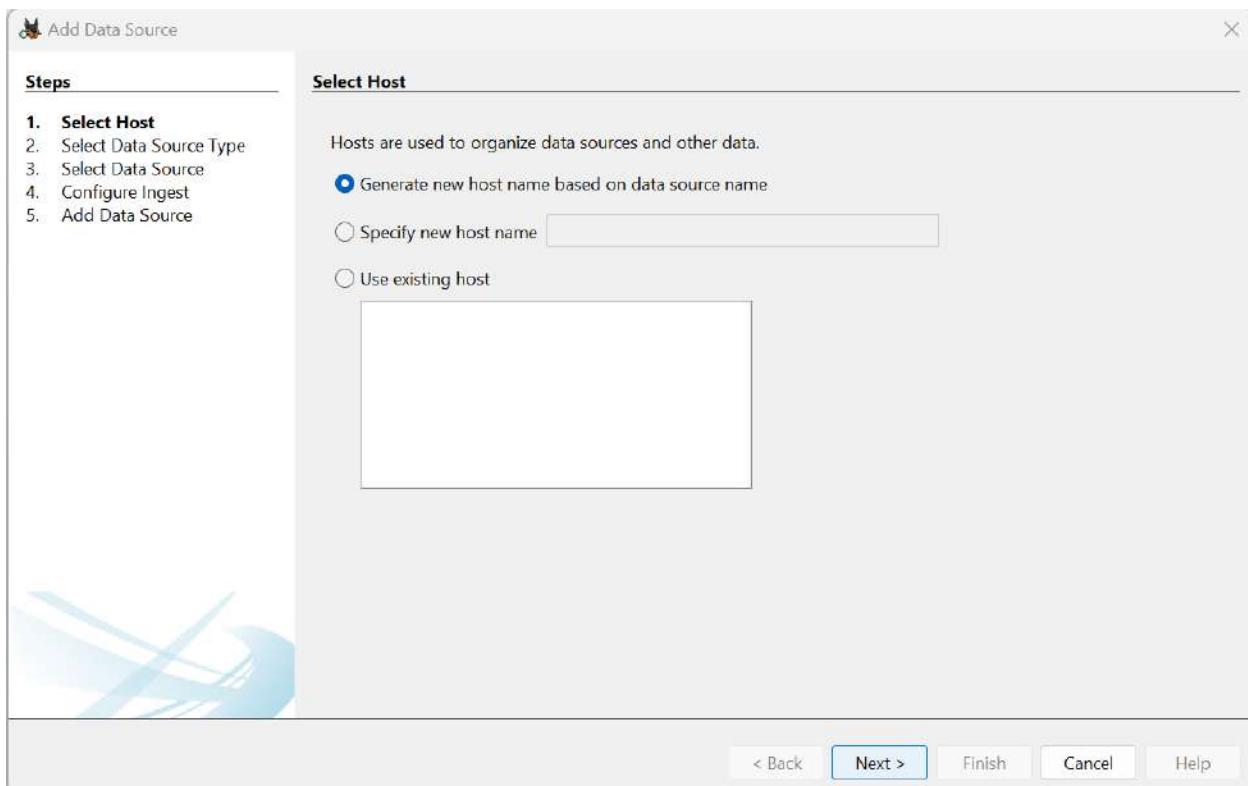
PS C:\Users\user\Downloads> Get-FileHash -Algorithm SHA1 .\case1.zip

Algorithm      Hash
-----        -----
SHA1          A46F502D1EFE90E04905108F947E7ACE7A67BC1D

PS C:\Users\user\Downloads>
```

CREATING AUTOPSY CASE:

The screenshot shows the Autopsy 4.21.0 software interface with the 'New Case Information' dialog open. The dialog is divided into two main sections: 'Case Information' and 'Optional Information'.
Case Information:
- Case Name: F201
- Base Directory: C:\Users\user\Downloads\case1
- Case Type: Single-User (selected)
- Case data will be stored in the following directory: C:\Users\user\Downloads\caser\F201
- Buttons: Back, Next >, Finish, Cancel, Help.
Optional Information:
- Case Number: F201
- Examiner:
 - Name: Abdullah
 - Phone: 031030657860
 - Email: abdullahamqbool08@gmail.com
 - Notes:
- Organization:
 - Organization analysis is being done for: Not Specified
 - Buttons: Back, Next >, Finish, Cancel, Help.



 Add Data Source

Steps

1. Select Host
2. Select Data Source Type
- 3. Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\user\Downloads\case1\RHNIOUSB.dd

Ignore orphan files in FAT file systems

Time zone: (GMT+5:00) Asia/Karachi

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Finish Cancel Help

 Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
- 4. Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

Recent Activity	Hash Lookup	File Type Identification	Extension Mismatch Detector	Embedded File Extractor	Picture Analyzer	Keyword Search	Email Parser	Encryption Detection	Interesting Files Identifier	Central Repository	PhotoRec Carver	Virtual Machine Extractor
<input checked="" type="checkbox"/>												

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rece.

Global Settings

Select All Deselect All History

< Back Finish Cancel Help

ANALYZING DELETED FILES:

Screenshot of Autopsy 4.2.1.0 interface showing deleted files analysis.

File Listing:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
f0000000.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	52998144	Unallocated	Unallocated	unknown
f0103512.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	93814	Unallocated	Unallocated	unknown
f0103704.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415334	Unallocated	Unallocated	unknown
f0104520.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated	Unallocated	unknown
f0105328.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	264600	Unallocated	Unallocated	unknown
f0105848.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6809	Unallocated	Unallocated	unknown
f0105864.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	230665	Unallocated	Unallocated	unknown
f0106320.gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11407	Unallocated	Unallocated	unknown
f0106344.gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4105	Unallocated	Unallocated	unknown
f0106360.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	116793344	Unallocated	Unallocated	unknown
f0334472_She_died_in_February_at_the_age_of_74.c				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	30720	Unallocated	Unallocated	unknown
f0334536.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	264600	Unallocated	Unallocated	unknown
f0335056.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	172546	Unallocated	Unallocated	unknown
f0335404.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1048576	Unallocated	Unallocated	unknown

Image Preview: A close-up photograph of an alligator's head and upper body, resting on green vegetation.

MOTHER AND CHILS FLAG:

Screenshot of Autopsy 4.2.1.0 interface showing deleted files analysis.

File Listing:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0103512.jpg				0000-00-20 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	93814	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R
f0103704.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415334	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R
f0104520.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R
f0105328.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	264600	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R
f0105848.jpg	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6809	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R
f0105864.jpg	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	230665	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R
f0334536.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	264600	Unallocated	Unallocated	unknown	/img_RHINOUSB.d1/\$CarvedFiles/1/R

Image Preview: A photograph of a large white rhinoceros and its calf standing in a muddy watering hole.

SORTING BY FILE TYPE:

Autopsy 4.2.1.0 - Case: [REDACTED] - File Types

File Types (3)

- By Extension
 - Images (7)
 - Videos (0)
 - Audio (0)
 - Archives (0)
 - Databases (0)
 - Documents
 - HTML (0)
 - Office (1)
 - PDF (0)
 - Plain Text (124)
 - Rich Text (0)
 - Executable
 - By MIME Type
 - application
 - image
 - text
- Deleted Files (0)
- All (132)

MB File Size

Data Artifacts (1)

Analysis Results (2)

OS Accounts

Tags

Score

Reports

Listing

Table: Thumbnail | Summary

Type

- application
- image
- text

3 Results

Save Table as CSV

READING DIARY

Autopsy 4.2.1.0 - Case: [REDACTED] - f0334472_She_died_in_February_at_the_age_of_74.c

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loc
f0334472_She_died_in_February_at_the_age_of_74.c	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	30720	Unallocated	Unallocated	unknown	/m

File Metadata

Strings: Extracted Text: Translations:

Page: 1 of 1 Page: 1 of 1 Match: 100% Reset Text Source: File Text

She died in February at the age of 74. In August 2001 it wasn't a decision, since the alternative was regret. It wasn't her fault that I didn't go to the drugstore.. And then getting her to arrange a time with Lynn, so that I can tell her just with me and Tal there.

We were walking from the restaurant to the Irish pub, and who did we run into? Then we had dinner at this really nice restaurant with a patio kind of in Old Town.

Back in March I did a presentation at a research conference held at UC Irvine and presented by the Honors Transfer Council of California.

My mother and I have a unique relationship. Chasing Amy - "whimpers" By all accounts I should have liked this film. Their relationship was a failure! All other IB families are trying to keep their kid in IB, trying to encourage their kid to do good, mine is trying to make me quit. Anyway, this one is someone she was involved with in high school who says he's been trying to find her all these years and finally tracked her down. So seeing how I am scared of pitch black darkness I got up and was trying to see what made the power go out, and my parents got up and joined me with flashlights and candles. I handed in the damn homework, which was really quite stupid for all those who do know how to use the damn computer. He turned back to me, completely sober, completely serious and replied - 'No, I don't dislike you. I'm just scared of you.' I stared at him in disbelief for a moment or two or three - scared of me?

There truly are buckets of phenomenal things to be amazed by, and thankful for.

Stocklos and Andrew were only there for one of the nights I was:

May 15, 2024

HARD DRIVE + EMAIL ADDRESS:

The screenshot shows the Autopsy 4.2.10 forensic analysis interface. The left sidebar displays a tree view of the data source structure, including 'Data Sources' (RHINOUSB.dd_1 Host, RHINOUSB.dd), 'File Views' (File Types, Deleted Files, MB File Size), 'Analysis Results' (Keyword Hits, DS Accounts, Tags, Score, Bad Items, Suspicious Items, Reports), and 'Logs'.

The main area shows a 'Listing' table with two entries:

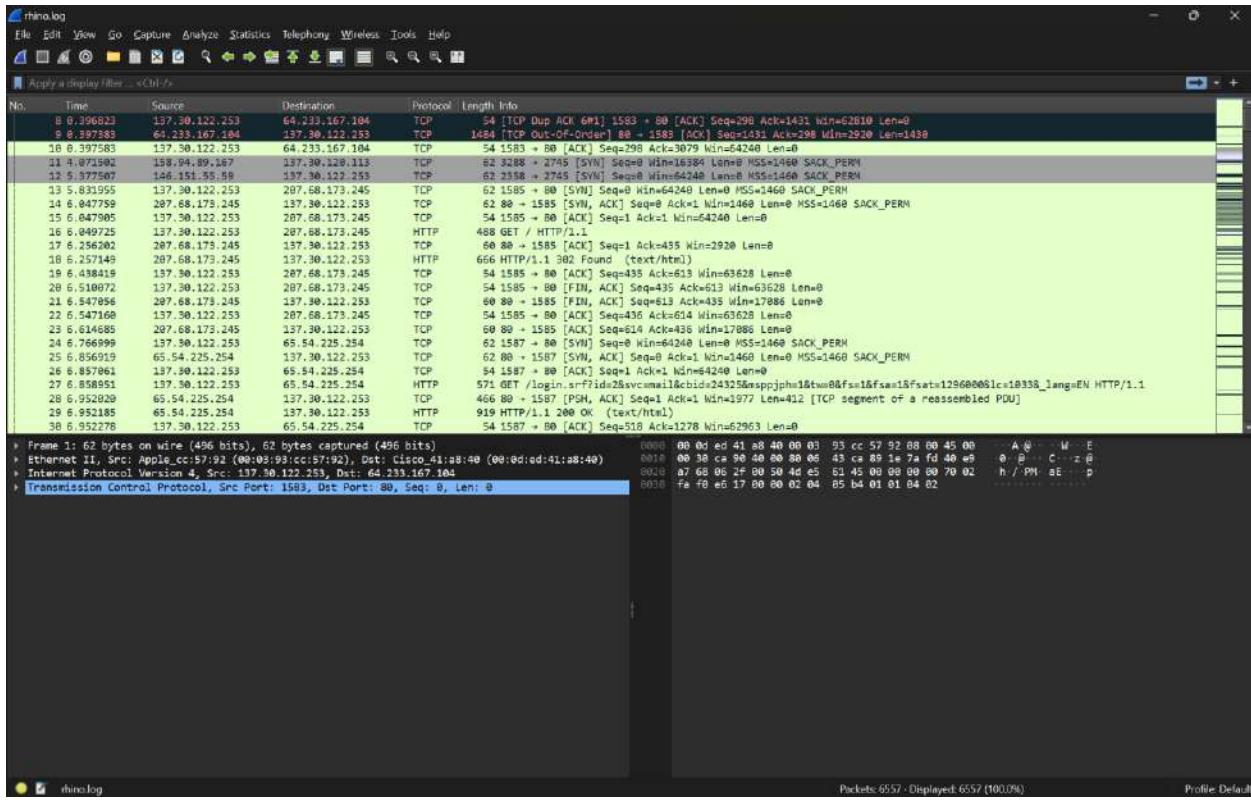
Source Name	S	C	O	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time	Access Time
philip@mit.edu	0			philip@mit.edu	(\w{1} \w{2}-\w{9}\w{1}-\w{1}\w{1}+\w{1}\w{1}+\w{1}\w{1}\w{1}\w{1}\w{1})	[copyright 2000 <philip@mit.edu> \$^".#(7)0144]	0000-00-00 00:00:00	0000-00-00 00:00:00
fo103512.jpg				philip@mit.edu	(\w{1} \w{2}-\w{9}\w{1}-\w{1}\w{1}+\w{1}\w{1}+\w{1}\w{1}\w{1}\w{1}\w{1})	[copyright 2000 <philip@mit.edu> \$^".#(7)0144]	0000-00-00 00:00:00	0000-00-00 00:00:00

Below the table is a 'Text' tab showing extracted text from the file 'fo103512.jpg'. The text content is:

```
3xQ2
39hKOo
[...]
v0Y
C0m
NLE528
rcfS$5
[...]
e$1
F93]
p+g
nA*
(OHF
YK N
n738
XDF
```

4. Rhino Hunt with Wireshark

OPENING RHINO LOG:



FINDING TELNET PACKETS:

Wireshark Log:

No.	Time	Source	Destination	Protocol	Length	Info
641	102.648947	137.30.128.48	137.30.122.253	TELNET	69	Telnet Data ...
642	102.648336	137.30.122.253	137.30.128.48	TELNET	72	Telnet Data ...
644	102.648533	137.30.122.253	137.30.128.48	TELNET	72	Telnet Data ...
646	102.648988	137.30.128.48	137.30.122.253	TELNET	57	Telnet Data ...
647	102.648661	137.30.122.253	137.30.128.48	TELNET	73	Telnet Data ...
649	102.648059	137.30.122.253	137.30.128.48	TELNET	75	Telnet Data ...
650	102.648194	137.30.128.48	137.30.122.253	TELNET	76	Telnet Data ...
652	102.646226	137.30.128.48	137.30.122.253	TELNET	57	Telnet Data ...
653	102.846544	137.30.122.253	137.30.128.48	TELNET	68	Telnet Data ...
655	102.84251	137.30.122.253	137.30.128.48	TELNET	60	Telnet Data ...
656	102.849467	137.30.128.48	137.30.122.253	TELNET	60	Telnet Data ...
657	102.848787	137.30.122.253	137.30.128.48	TELNET	57	Telnet Data ...
1168	106.349725	137.30.122.253	137.30.128.48	TELNET	55	Telnet Data ...
1169	106.359817	137.30.128.48	137.30.122.253	TELNET	60	Telnet Data ...
1170	106.444875	137.30.122.253	137.30.128.48	TELNET	55	Telnet Data ...
1171	106.444437	137.30.128.48	137.30.122.253	TELNET	69	Telnet Data ...
1173	106.594962	137.30.122.253	137.30.128.48	TELNET	55	Telnet Data ...
1174	106.595234	137.30.128.48	137.30.122.253	TELNET	60	Telnet Data ...
1175	106.735722	137.30.122.253	137.30.128.48	TELNET	55	Telnet Data ...
1176	106.736838	137.30.128.48	137.30.122.253	TELNET	60	Telnet Data ...
1177	106.815192	137.30.122.253	137.30.128.48	TELNET	55	Telnet Data ...
1178	106.815566	137.30.128.48	137.30.122.253	TELNET	60	Telnet Data ...
1188	107.077266	137.30.122.253	137.30.128.48	TELNET	55	Telnet Data ...

Frame 641: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
Ethernet II, Src: Oracle [0:19:96] (08:00:20:70:13:96), Dst: Apple [0:19:96] (08:00:39:cc:57:92) (ethernetII)
Internet Protocol Version 4, Src: 137.30.128.48, Dst: 137.30.122.253
Transmission Control Protocol, Src Port: 23, Dst Port: 1653, Seq: 1, Ack: 1, Len: 15
Telnet

Wireshark capture file - 3.114 KB

Telnet Properties

- Name: telnet
- Type: Wireshark capture file (*.pcap)
- Open with: Wireshark
- Location: C:\Users\user\Downloads\case1 (1)
- Size: 3.04 MB (3,187,007 bytes)
- Size on disk: 3.04 MB (3,190,794 bytes)
- Created: Saturday, 4 May, 2024, 11:59:29 PM
- Modified: Saturday, 4 May, 2024, 11:59:29 PM
- Accessed: Today, 4 May, 2024, 11:59:29 PM
- Attributes: Read-only, Hidden

OK Cancel Apply

File Explorer:

case1 (1)

Downloads

case1 (1)

RHINOUSB.dd

telnet

rhino

rhino2

rhino3

Windows (C)

Local Disk (D)

Client

Dark Web

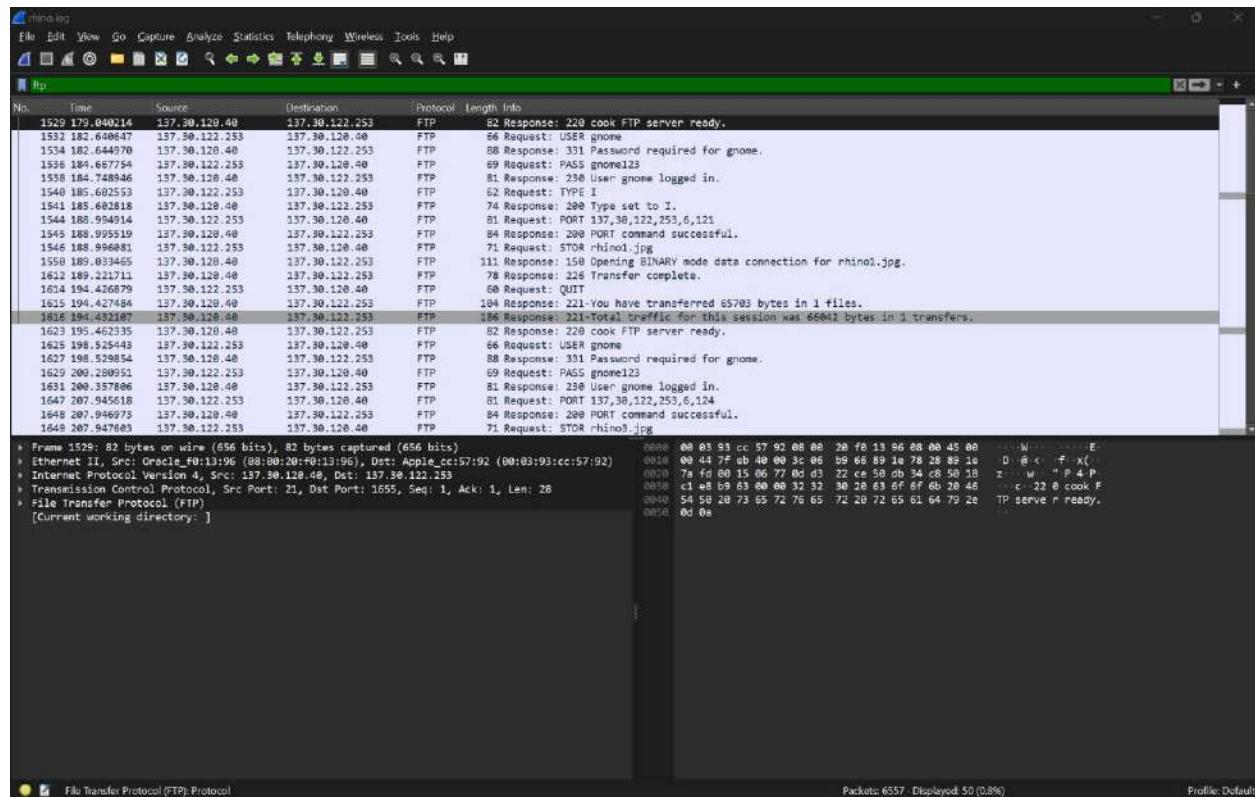
D8

FinalDFProj

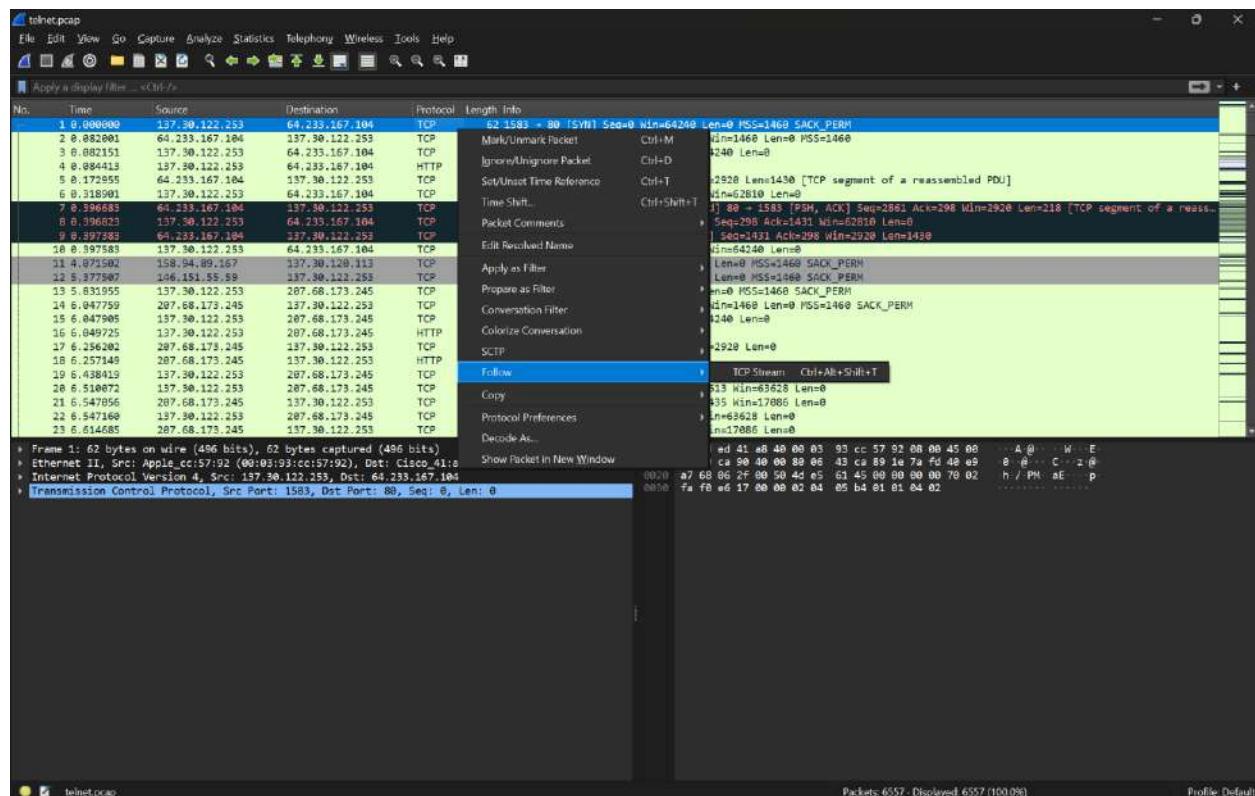
FileScr

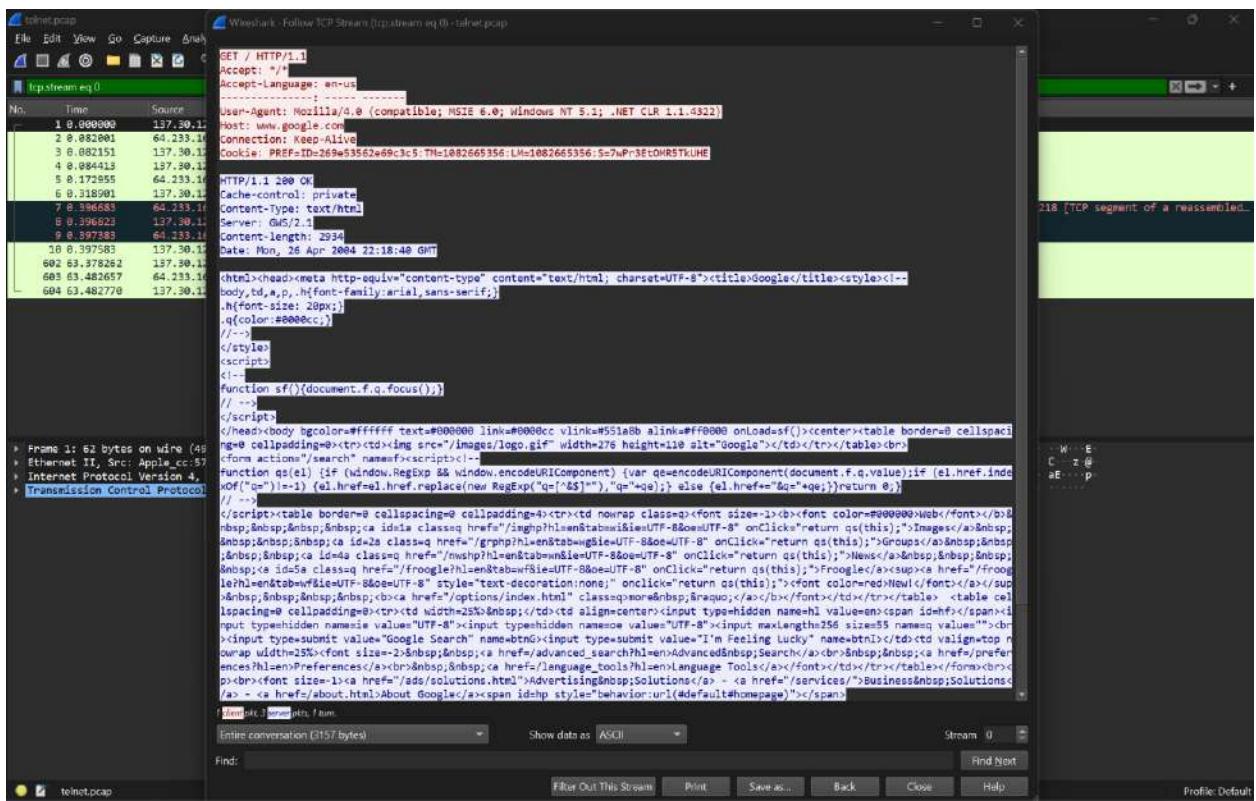
5 items | 1 item selected 3.04 MB |

FINDING FTP PACKETS:



EXAMINING THE TELNET TRAFFIC:





INCORRECT PASSWORD ENTRY:

No.	Date	Time	Source IP	Destination IP	Protocol	Details
1	1860	221.130.944	137.30.128.48	137.30.122.253	FTP	187 Response: 221-Total traffic for this session was 194382 bytes in 2 transfers.
5624	474.150121	137.30.128.48	137.30.122.253	FTP	82 Response: 220 cook FTP server ready.	
5633	477.915226	137.30.122.253	137.30.128.48	FTP	56 Request: USER gnome	
5635	477.919211	137.30.128.48	137.30.122.253	FTP	88 Response: 331 Password required for gnome.	
5637	479.926594	137.30.122.253	137.30.128.48	FTP	69 Request: PASS gnome123	
5639	479.185428	137.30.128.48	137.30.122.253	FTP	81 Response: 230 User gnome logged in.	
5641	481.832819	137.30.122.253	137.30.128.48	FTP	62 Request: TYPE I	

FILENAME:

Wireshark - Follow TCP Stream (tcp.stream eq 318) - telnet.pcap

```
gnome123
cat > JOHNREADME
I tried to hack Golden's account u.but the password was wrong.

--George.ia
.
ls -l
logout
exit
```

135 client pkts, 0 server pkts, 0 turns.

Entire conversation (1637 bytes) Show data as ASCII Stream 318

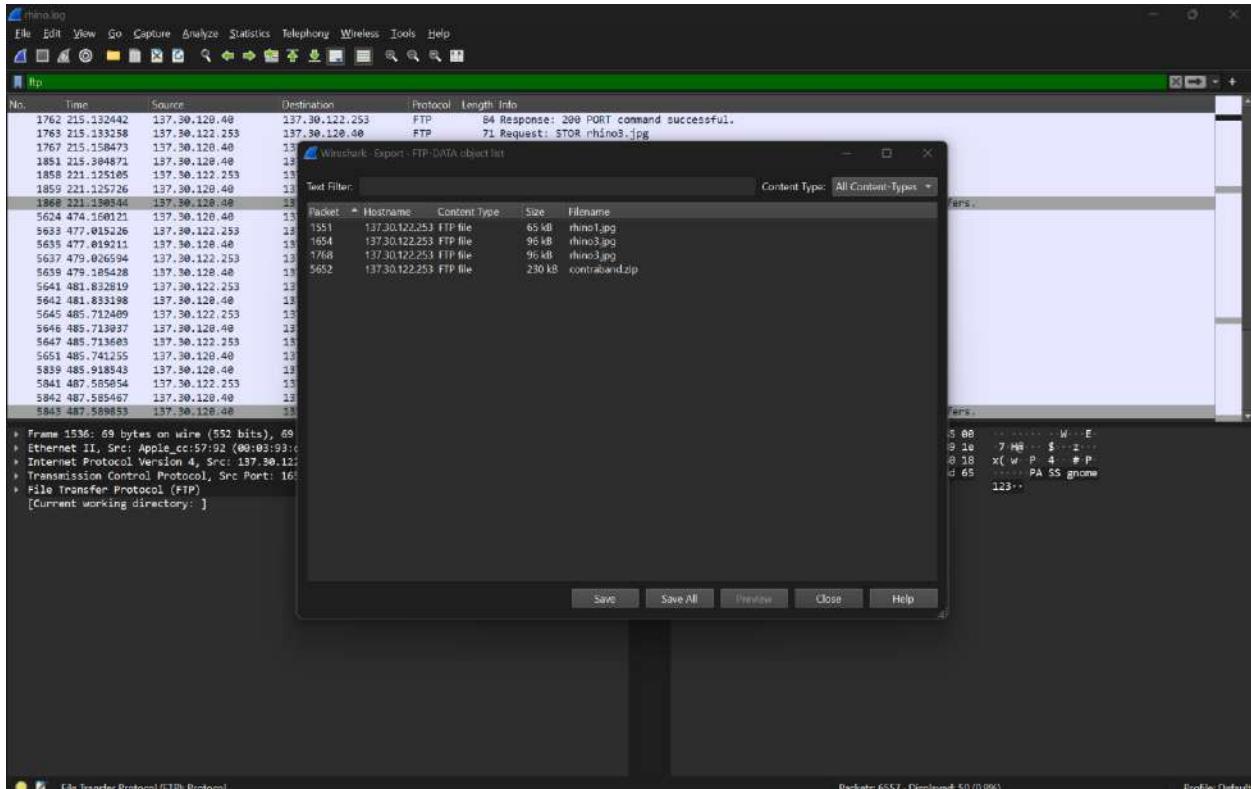
Find: Login Find Next

Filter Out This Stream Print Save as... Back Close Help

FTP FILENAME FINDING:

5647 485.713683	137.30.122.253	137.30.120.40	FTP	75 Request: STOR contraband.zip
5651 485.741255	137.30.120.40	137.30.122.253	FTP	115 Response: 150 Opening BINARY mode data connection for contraband.zip.
5839 485.918843	137.30.120.40	137.30.122.253	FTP	78 Response: 226 Transfer complete.
5841 487.585854	137.30.122.253	137.30.120.40	FTP	60 Request: QUIT
5842 487.585467	137.30.120.40	137.30.122.253	FTP	105 Response: 221-You have transferred 230566 bytes in 1 files.
5845 487.589853	137.30.120.40	137.30.122.253	FTP	187 Response: 221-Total traffic for this session was 290914 bytes in 1 transfers.

EXTRACTING IMAGES FROM THE FTP-DATA TRAFFIC:



EXAMINING HASH-FILE:

```
Windows PowerShell X + ~
PS C:\Users\user\Downloads\case1 (1)> Get-FileHash -Algorithm MD5 rhino1.jpg
Algorithm      Hash
----          ---
MD5          D5A83CDE0131C3A034E5A0D3BD94B3C9
Path
-----
C:\Users\user\Downloads\case1...
```

ZIP PASSWORD CRACKING:

The screenshot shows a web browser window with the URL <https://www.lostmypass.com/jobs/M0c4cm1EVG9lMy9cWEtZD8Lb3Uzdz09/>. The page title is "LostMyPass". The main content area displays a green success message: "Success! Your password is recovered". Below it, a text input field contains the recovered password "monkey". A question "Have we solved your problem?" is followed by two buttons: "Donate" and "Review Us". A note at the bottom states: "We have successfully recovered the password to your file. The password has been automatically verified. However, in rare cases there may be discrepancies due to non-standard encodings and characters. If you have any problems or concerns, please [contact our support team](#)". At the bottom of the page are payment method icons for PayPal, G Pay, VISA, MasterCard, American Express, Discover, Apple Pay, and B.

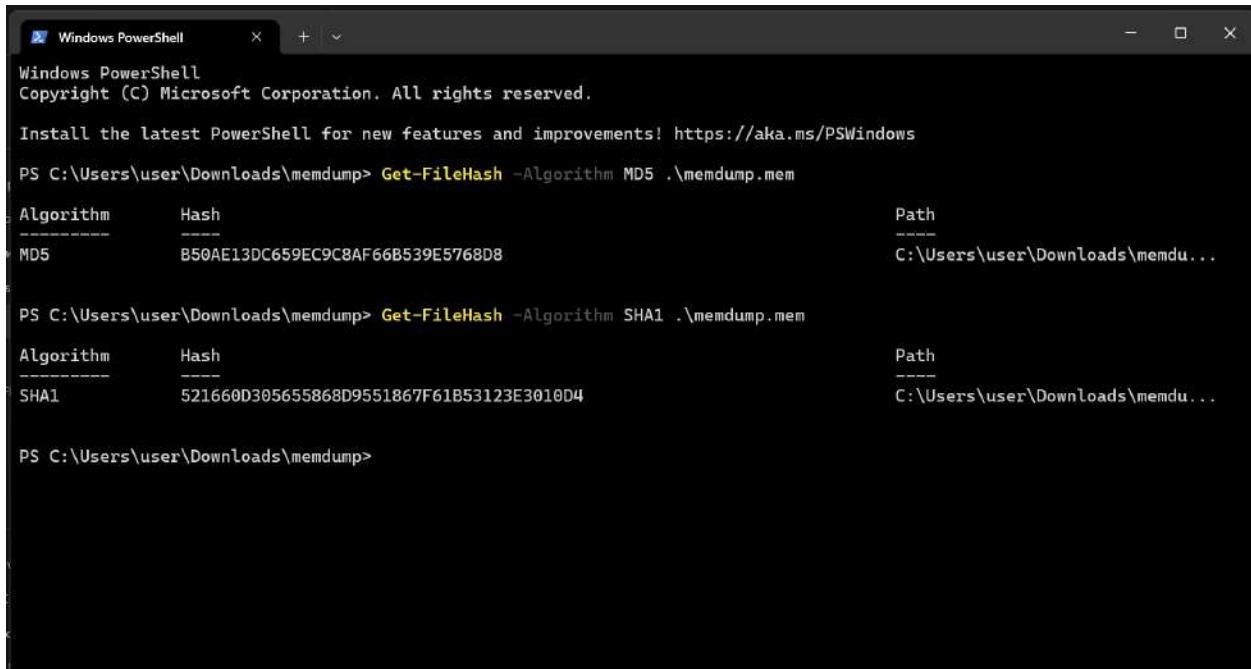
EXAIMING FILE HASH OF RHINO 2:

The screenshot shows a Windows PowerShell window titled "Windows PowerShell". The command run is `Get-FileHash -Algorithm MD5 rhino2.jpg`. The output is a table:

Algorithm	Hash	Path
MD5	ED870202082EA4FD8F5488533A561B35	C:\Users\user\Downloads\case1\contraband\...

5. Memory Analysis with Autopsy

EXAMINING FILE HASH BY TERMINAL:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

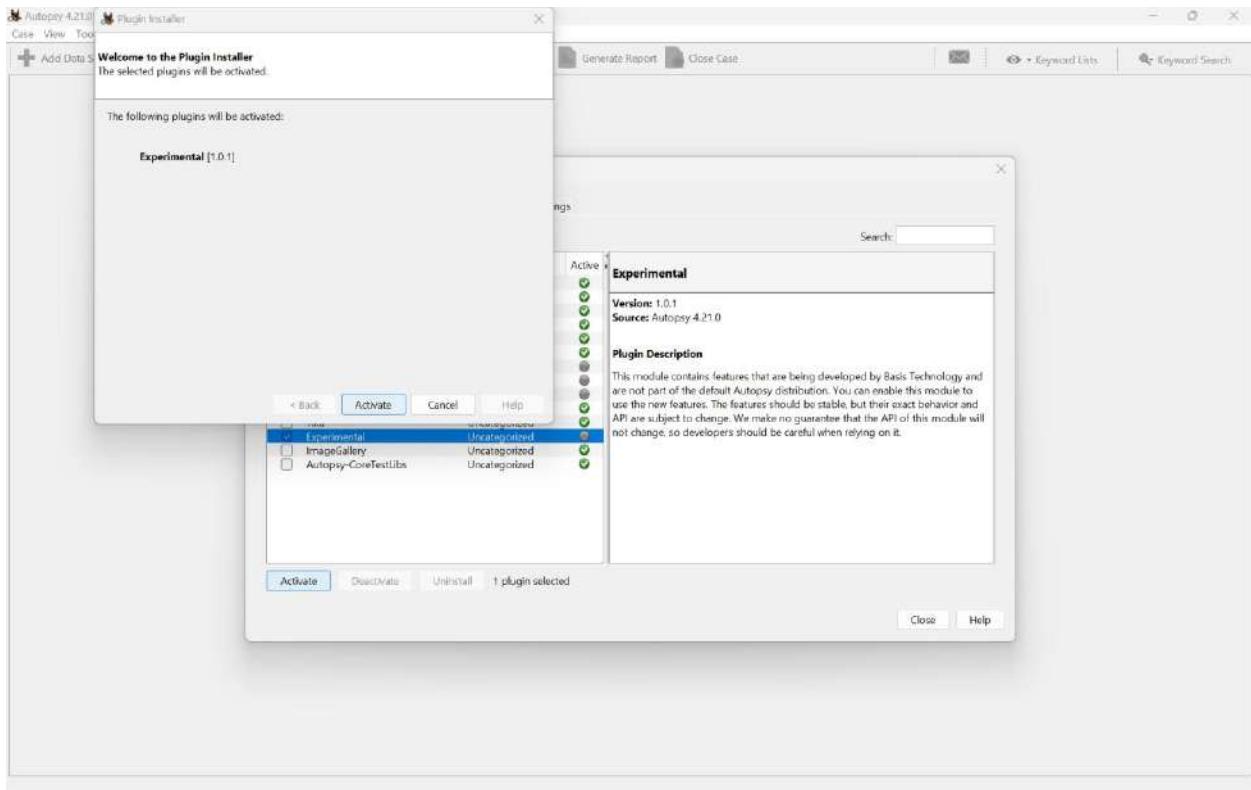
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\user\Downloads\memdump> Get-FileHash -Algorithm MD5 .\memdump.mem
Algorithm      Hash
----          ----
MD5           B50AE13DC659EC9C8AF66B539E5768D8
Path          C:\Users\user\Downloads\memdu...

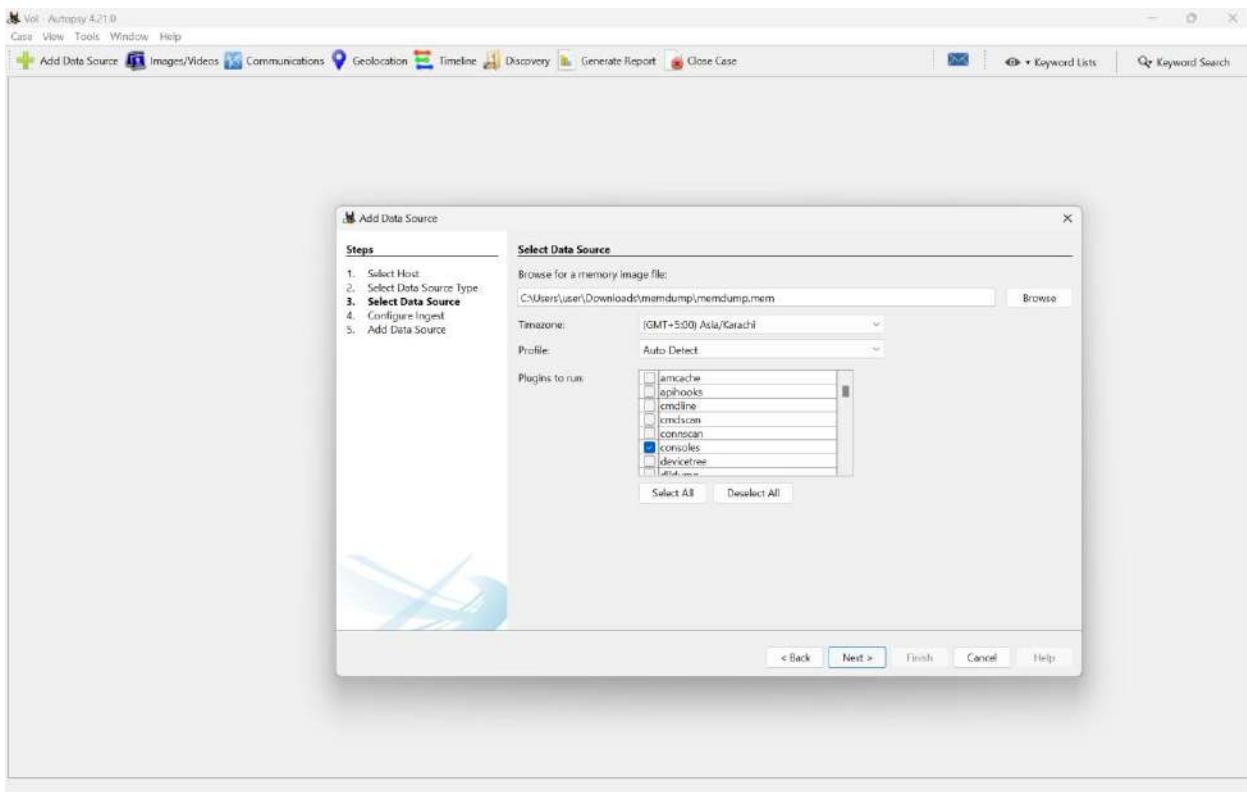
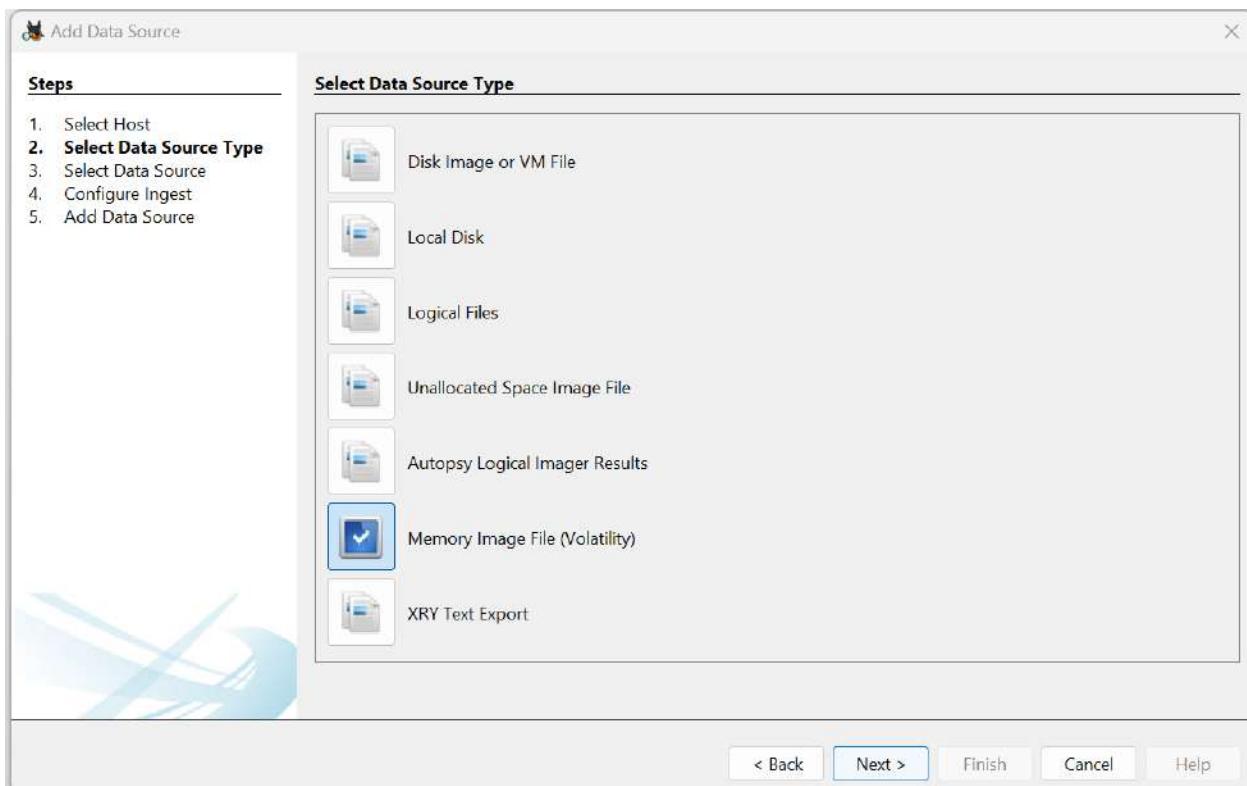
PS C:\Users\user\Downloads\memdump> Get-FileHash -Algorithm SHA1 .\memdump.mem
Algorithm      Hash
----          ----
SHA1          521660D305655868D9551867F61B53123E3010D4
Path          C:\Users\user\Downloads\memdu...

PS C:\Users\user\Downloads\memdump>
```

AUTOPSY PLUGGIN INSTALLATION:



IMPORTING THE MEMORY IMAGE:



DATASOURCES:

The screenshot shows the Vol Autopsy 4.21.0 interface. In the top navigation bar, the 'Data Sources' tab is selected. Below it, the 'ModuleOutput' file is highlighted. The main pane displays a table of file metadata. At the bottom, a detailed view of the 'ModuleOutput' file is shown, including its content and various tabs like Hex, Text, Application, File Metadata, etc.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
consoles	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4440	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
hashdump	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	498	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
imageinfo	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	666	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
lsadump	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	748	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
netcan	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15409	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
pslist	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6950	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
shellbags	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	31142	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
userssist	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12508	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput

CONSOLES SECTION:

The screenshot shows the Vol Autopsy 4.21.0 interface with the 'Consoles' section selected. It displays a list of console entries and their details. Below the list, a text pane shows command history and user creation logs.

```

ConsoleProcess: c:\Windows\system32\cmd.exe Pid: 472
Console: 0x1414:4944 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferSize: 4
OriginalTitle: tasking.ase
Title: 

ConsoleProcess: c:\Windows\system32\cmd.exe Pid: 472
Console: 0x1414:65ec CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferSize: 4

```

```

C:\Users\Administrator>net user YOUR-NAME letmen /add
The command completed successfully.

C:\Users\Administrator>net user waldo Apple123 /add
The command completed successfully.

C:\Users\Administrator>net user YOUR-NAME SuperSecret! /add
The command completed successfully.

```

HASHDUMP SECTION:

The screenshot shows the Volatility 4.21.0 interface with the 'Hashdump' section selected. The central area displays a table of memory dump contents, including columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table lists several files: consoles, hashdump, imageinfo, lsadump, netscan, pslist, shellbags, and userassist. The 'hashdump' file is highlighted. Below the table, a preview pane shows extracted strings from the 'hashdump' file, including administrator, guest, student, probe, walid, and your NAME entries. At the bottom, a 'METADATA' section is visible.

LSADUMP SECTION:

The screenshot shows the Volatility 4.21.0 interface with the 'LSADUMP' section selected. The central area displays a table of memory dump contents, including columns for Name, S, C, D, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table lists the same files as the Hashdump section. The 'lsadump' file is highlighted. Below the table, a preview pane shows extracted strings from the 'lsadump' file, including default password entries like 'DefaultPassword' and 'P@ssw0rd.' and NLSKM values.

NETSCAN SECTION:

The screenshot shows the Autopsy 4.2.1 interface with the 'NetScan' section selected. The left sidebar shows 'Data Sources' with 'memdump.mem_1 Host' expanded, revealing 'memdump.mem' and 'ModuleOutput'. The main pane displays a table of files under 'ModuleOutput' with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. Files listed include consoles, hashdump, imaginfo, lsadump, netscan, plist, shellbags, and userassist. The 'netscan' file is highlighted. Below the table is a hex editor window showing network traffic, specifically a list of listening TCP ports (e.g., 1028, 1508, 1509, 616, 804) and their associated processes (e.g., dnscsvc.exe, ftphaserv.exe, kass.exe, svchost.exe).

PSLIST SECTION:

The screenshot shows the Autopsy 4.2.1 interface with the 'PsList' section selected. The left sidebar shows 'Data Sources' with 'memdump.mem_1 Host' expanded, revealing 'memdump.mem' and 'ModuleOutput'. The main pane displays a table of files under 'ModuleOutput' with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. Files listed include consoles, hashdump, imaginfo, lsadump, netscan, plist, shellbags, and userassist. The 'plist' file is highlighted. Below the table is a hex editor window showing process list data, including entries for svchost.exe processes (e.g., svchost.exe, svchost.exe, svchost.exe, svchost.exe, svchost.exe, svchost.exe) with various process IDs and creation times.

SHELLBAGS SECTION:

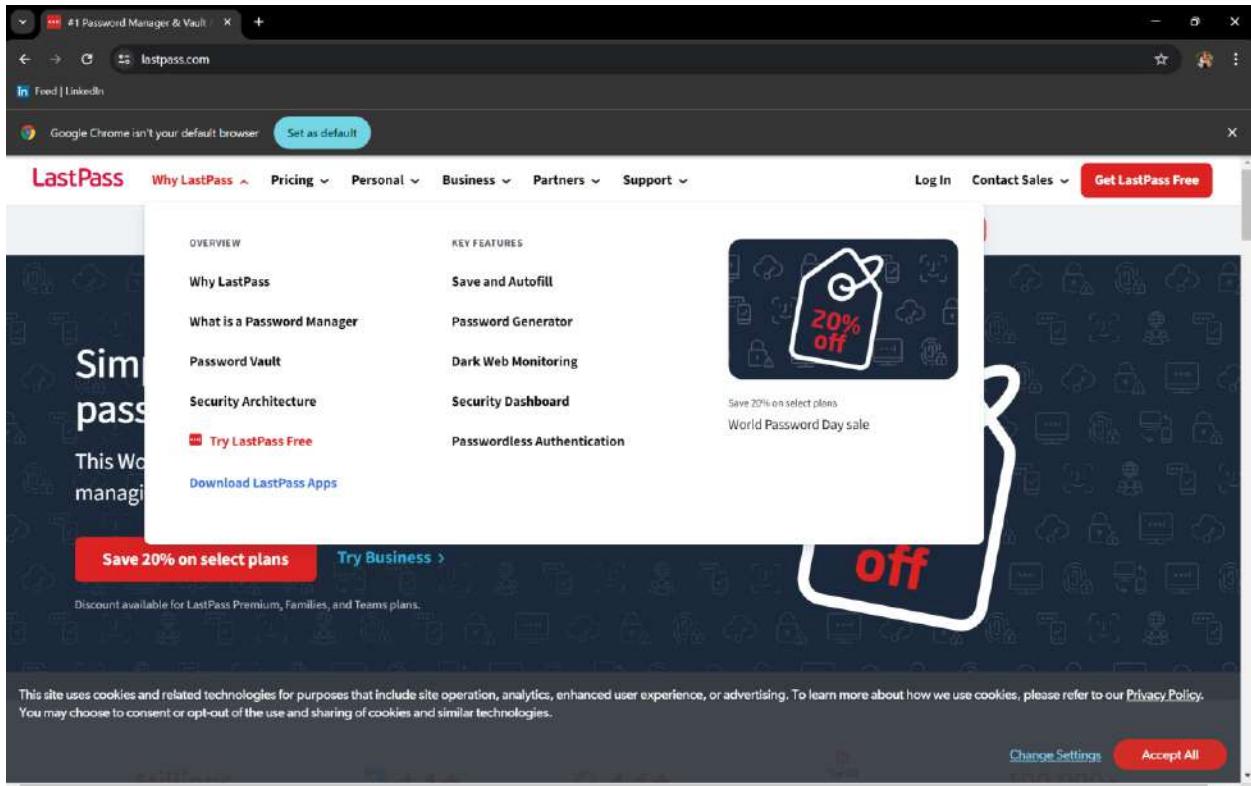
USERASSIST SECTION:

PROBE PASSWORD:

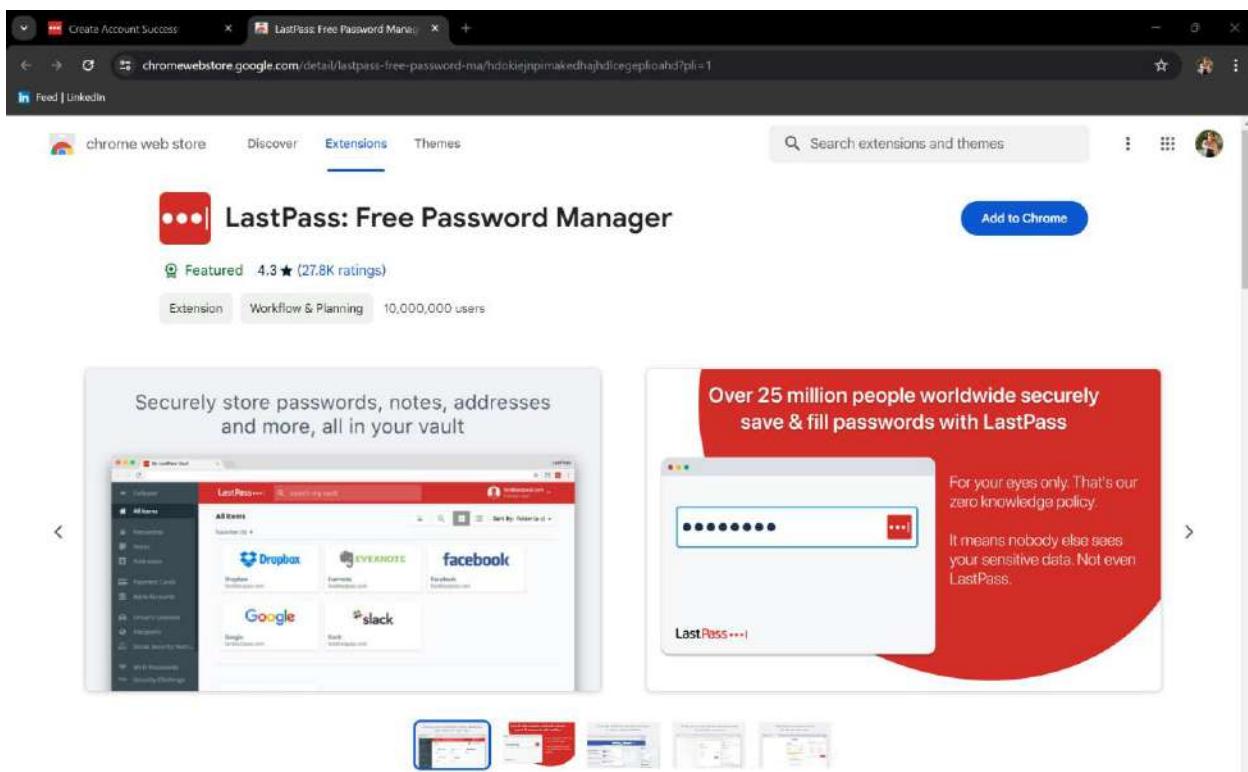
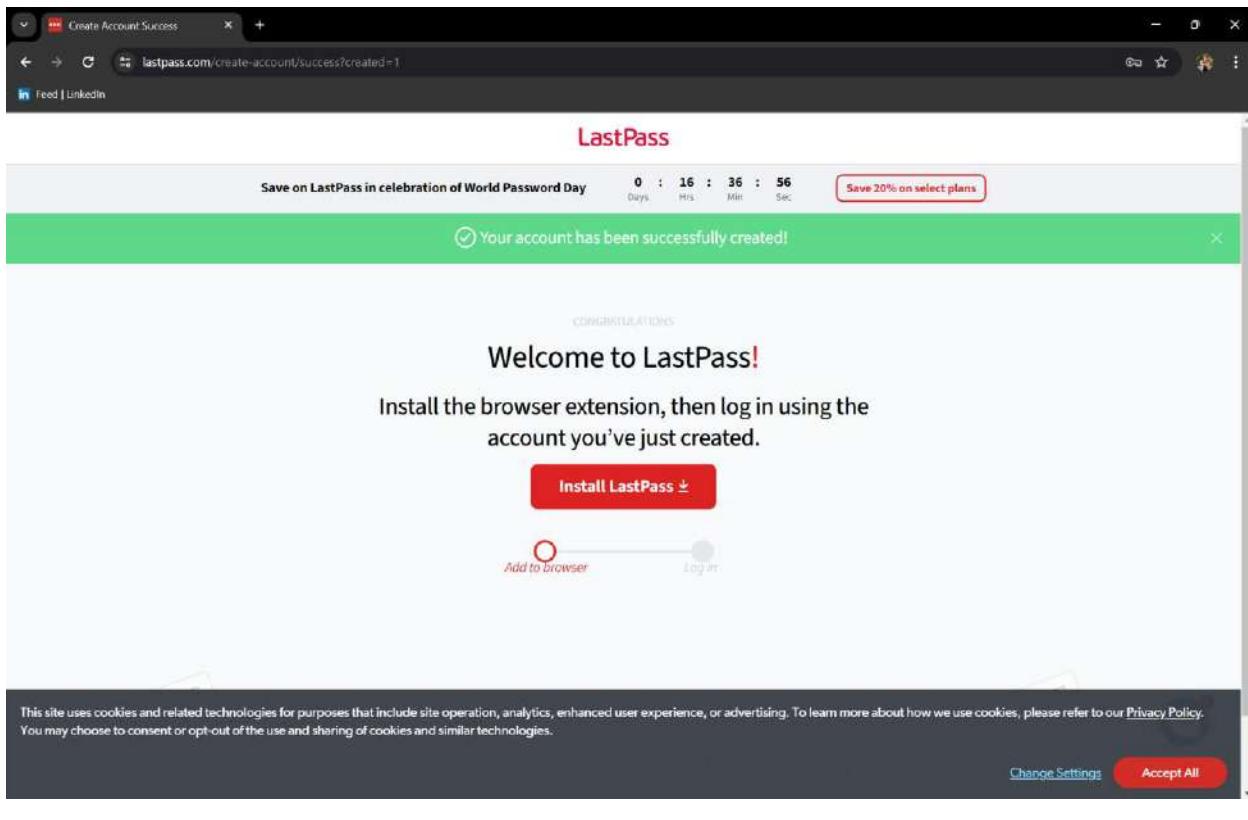
The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with tabs for 'CrackStation', 'Password Hashing Security', 'Defuse Security', and social links for 'Defuse.ca' and 'Twitter'. Below the navigation is the title 'Free Password Hash Cracker'. A text input field contains the password hash 'e19ccf75ee54e06b06a5907af13cef42'. To the right of the input field is a reCAPTCHA verification box with the text 'I'm not a robot' and a checkbox. Below the input field is a table with one row, showing the hash 'e19ccf75ee54e06b06a5907af13cef42' in the 'Hash' column, 'HTLM' in the 'Type' column, and 'Password' in the 'Result' column. A note below the table says 'Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.' At the bottom left, there's a link 'Download CrackStation's Wordlist'. On the left side of the main content area, there's a section titled 'How CrackStation Works' with a detailed explanation of how the service uses pre-computed lookup tables to crack hashes.

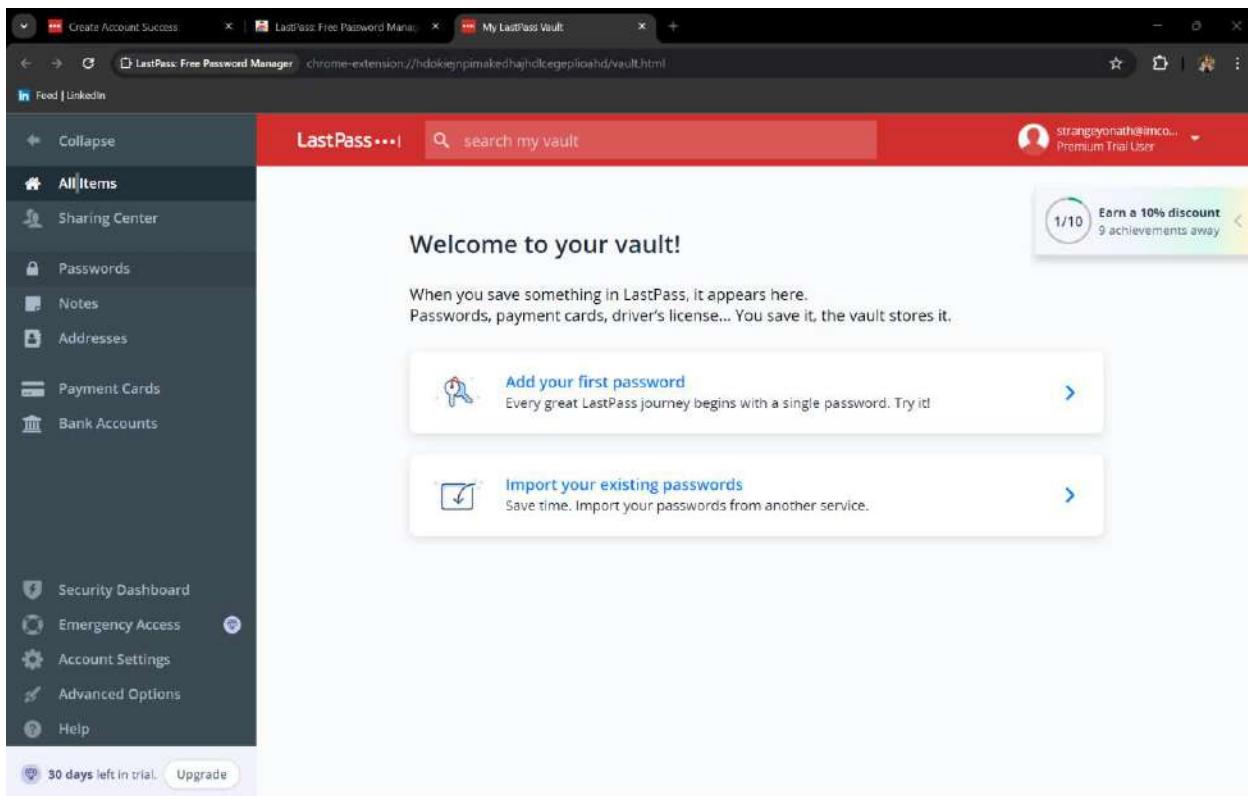
6. Memory Forensics of LastPass and Keeper

LASTPASS OPENED ON CHROME:

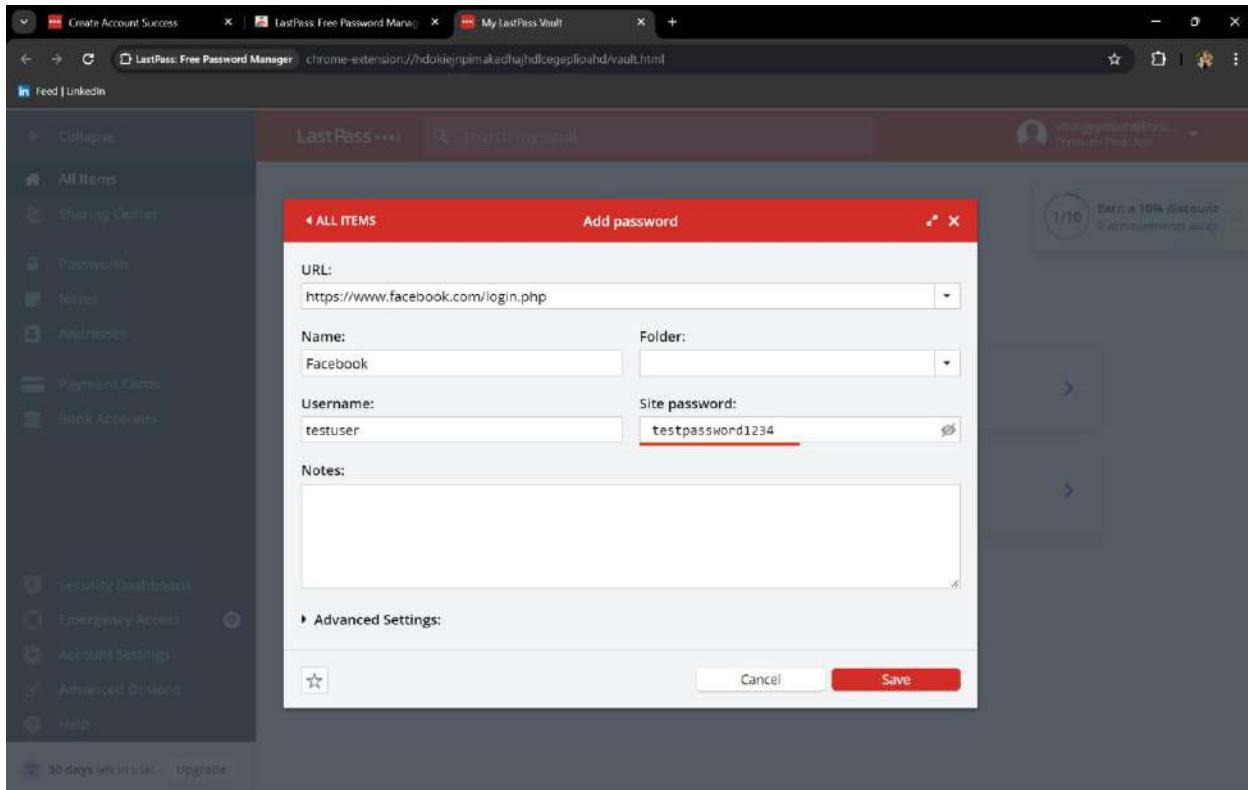


LASTPASS ACCOUNT CREATION





FACEBOOK ACCOUNT CREATION:



PROCESS EXPLORER EXAMINATION:

Process Explorer - Sysinternals: www.sysinternals.com [ABDULLAHM-PC\user]

The screenshot shows the Process Explorer interface with a list of processes. The main table has columns: CPU, Private Bytes, Working Set, PID, Description, and Company Name. A filter bar at the top right says '<Filter by name>'. The process list includes several instances of 'chrome.exe' and 'msedge.exe'. The 'chrome.exe' instances are all from Google LLC, while the 'msedge.exe' instances are from Microsoft Corporation. The 'msedge.exe' instances have a command line path: 'C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe'.

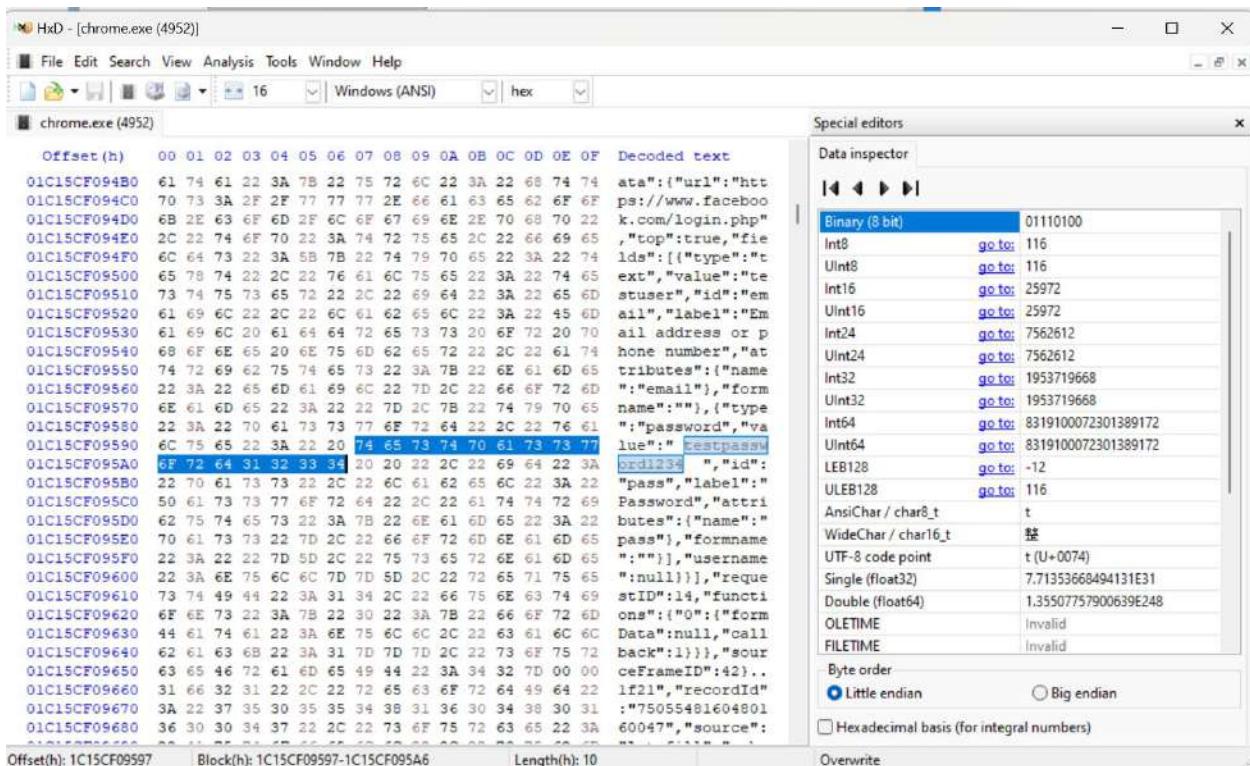
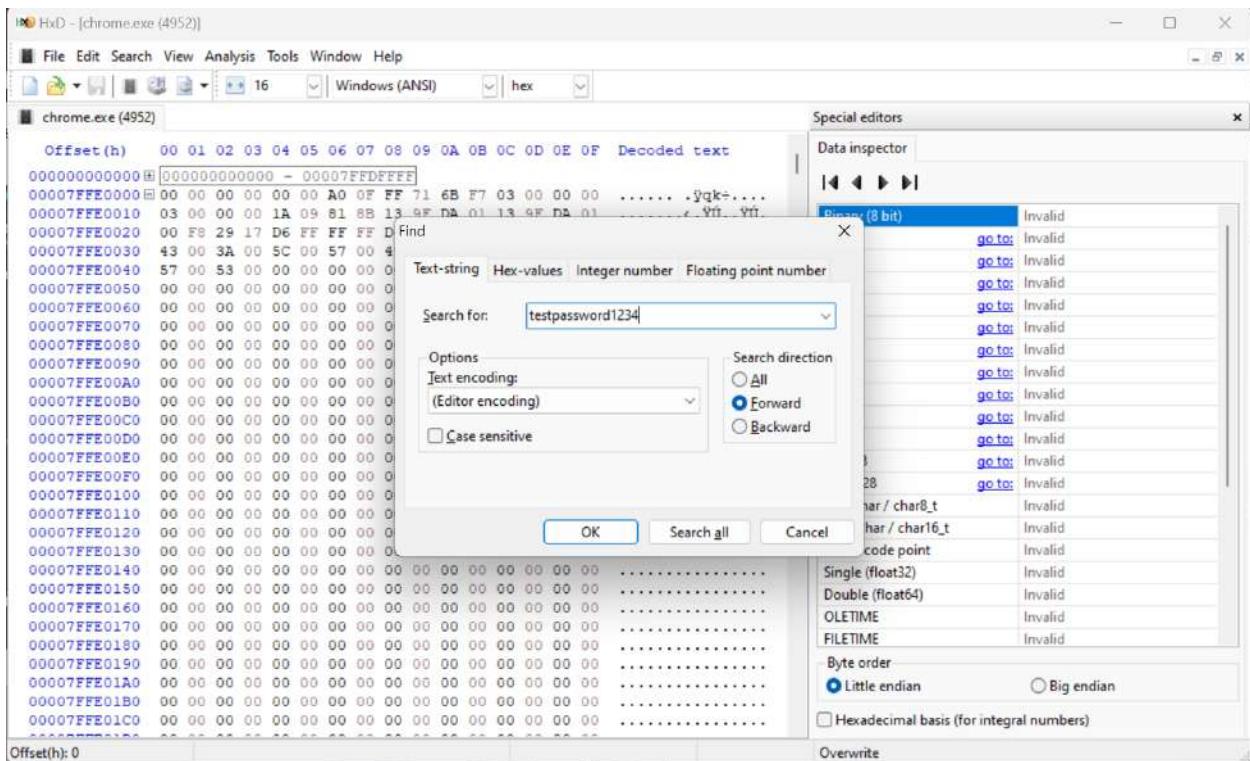
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
ai.exe	< 0.01	22,760 K	19,144 K	15628	Artificial Intelligence (AI) Host...	Microsoft Corporation
alexe	< 0.01	46,368 K	54,780 K	12360	Artificial Intelligence (AI) Host...	Microsoft Corporation
chrome.exe	< 0.01	71,252 K	169,796 K	18368	Google Chrome	Google LLC
		6,700 K	9,060 K	9628	Google Chrome	Google LLC
		215,968 K	231,068 K	18300	Google Chrome	Google LLC
		24,056 K	43,404 K	2920	Google Chrome	Google LLC
		15,740 K	21,904 K	5024	Google Chrome	Google LLC
		64,660 K	114,744 K	8336	Google Chrome	Google LLC
		15,340 K	21,380 K	3132	Google Chrome	Google LLC
		52,900 K	104,252 K	4640	Google Chrome	Google LLC
		29,876 K	62,516 K	14328	Google Chrome	Google LLC
		23,500 K	47,292 K	12380	Google Chrome	Google LLC
		178,284 K	217,460 K	7292	Google Chrome	Google LLC
		36,572 K	71,492 K	11904	Google Chrome	Google LLC
		33,504 K	63,200 K	7852	Google Chrome	Google LLC
		40,428 K	78,100 K	268	Google Chrome	Google LLC
		20,320 K	29,248 K	4952	Google Chrome	Google LLC
		173,280 K	254,488 K	5968	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	22,084 K	44,224 K	7296	Microsoft Edge	Microsoft Corporation
		23,300 K	37,912 K	14736	Microsoft Edge	Microsoft Corporation
		65,924 K	97,368 K	15012	Microsoft Edge	Microsoft Corporation
		72,732 K	103,952 K	15488	Microsoft Edge	Microsoft Corporation
		26,844 K	52,308 K	15792	Microsoft Edge	Microsoft Corporation
		21,132 K	7,656 K	16204	Microsoft Edge	Microsoft Corporation

CPU Usage: 0.00% | Commit Charge: 59.64% | Processes: 241 | Physical Usage: 53.60% |

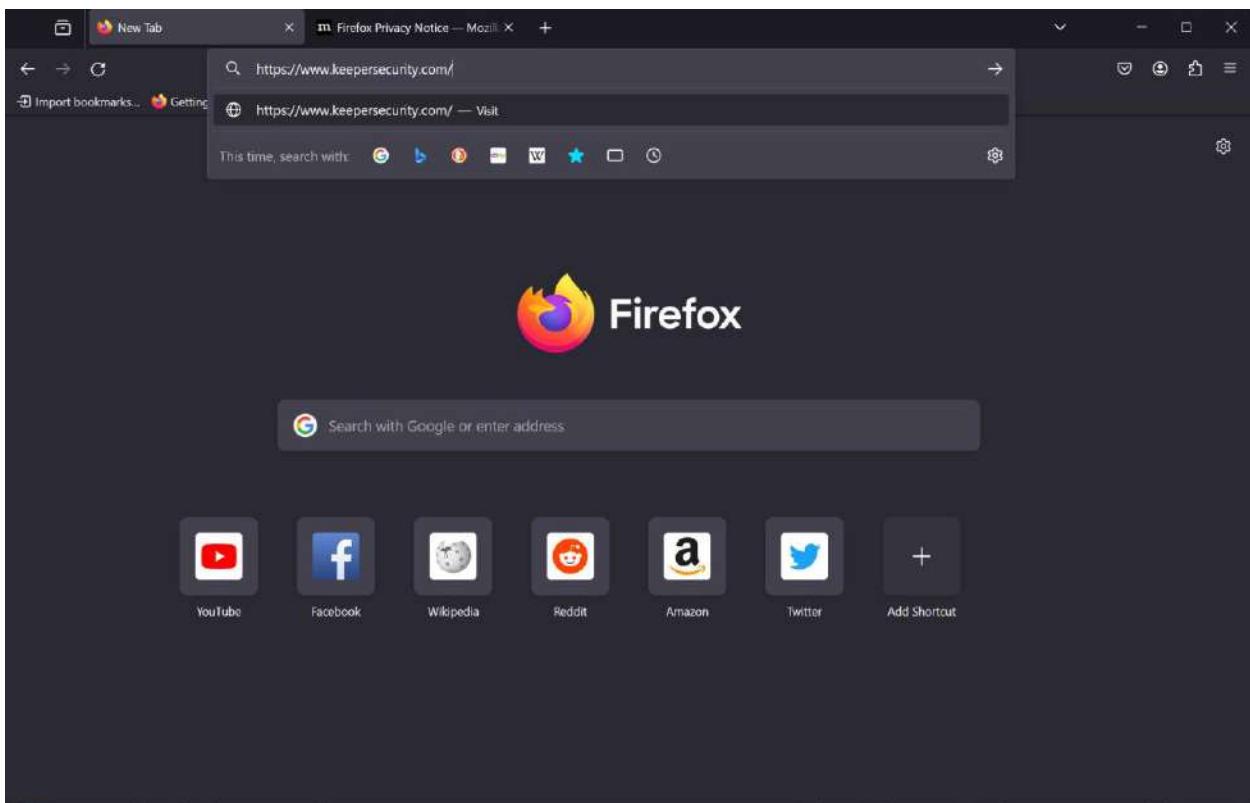
HxD EXAMINATION:

In HxD, click **Search, Find**.
In the "Search for" field, enter **testpa**

The screenshot shows the HxD application interface. At the top, a message box says: "In HxD, click Search, Find. In the 'Search for' field, enter testpa". Below it is the main window with a menu bar: File, Edit, Search, View, Analysis, Tools, Window, Help. A toolbar with icons for file operations is visible. The status bar at the bottom shows "Windows (ANSI)" and "16". The main area displays a list of processes in the "Open main memory" dialog, with "chrome.exe (4952)" selected. To the right, there are two panes: "editors" and "inspector". The "editors" pane shows a list of memory regions, mostly invalid, with some entries like "AnsChar / char8_t" and "WideChar / char16_t". The "Byte order" dropdown is set to "Little endian". The "inspector" pane is partially visible. Below this is the main memory dump window titled "chrome.exe (4952)". It shows memory starting at offset 000000000000, with the first few bytes being 00 00 00 00 - 00007FFDFFFF. The "Decoded text" column shows some readable characters like ".\u0000.\u0000.\u0000.\u0000.". The "Special editors" pane on the right is identical to the one in the search dialog. The status bar at the bottom of this window also shows "Windows (ANSI)" and "16".



TARGET 2: KEEPER



The screenshot shows a Firefox browser window with a dark theme. The address bar displays the URL <https://www.keepersecurity.com/>. Below the address bar is a search bar with the placeholder "Search with Google or enter address". A row of icons for popular websites (YouTube, Facebook, Wikipedia, Reddit, Amazon, Twitter) is visible. The main content area displays the Keeper website's landing page, featuring four service offerings: Business and Enterprise, Public Sector and FedRAMP, MSPs, and Personal and Family. Each offering has a corresponding icon and a brief description. Buttons for "Start Free Trial" or "Contact Sales" are provided for each category.

Start Your Free Trial Today - Ke... https://www.keepersecurity.com/get-keeper.html

KEEPER

Products Pricing Download Use Cases Resources Partners Contact Get a Quote Try It Free Login

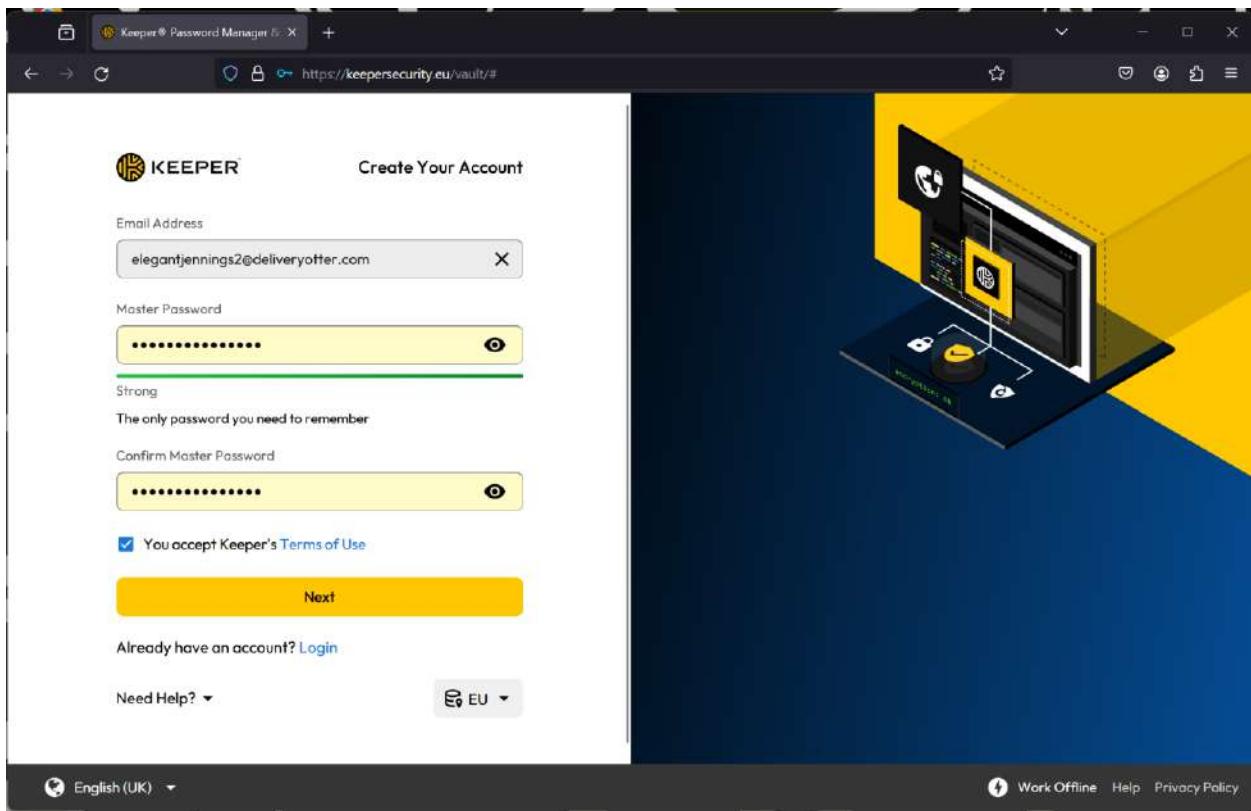
Business and Enterprise
Protect your company from cybercriminals.
[Start Free Trial](#)

Public Sector and FedRAMP
Protect your agency and educational institution from cybercriminals.
[Contact Sales](#)

MSPs
Protect your MSP organisation, your end customers and add new revenue streams.
[Start Free Trial](#)

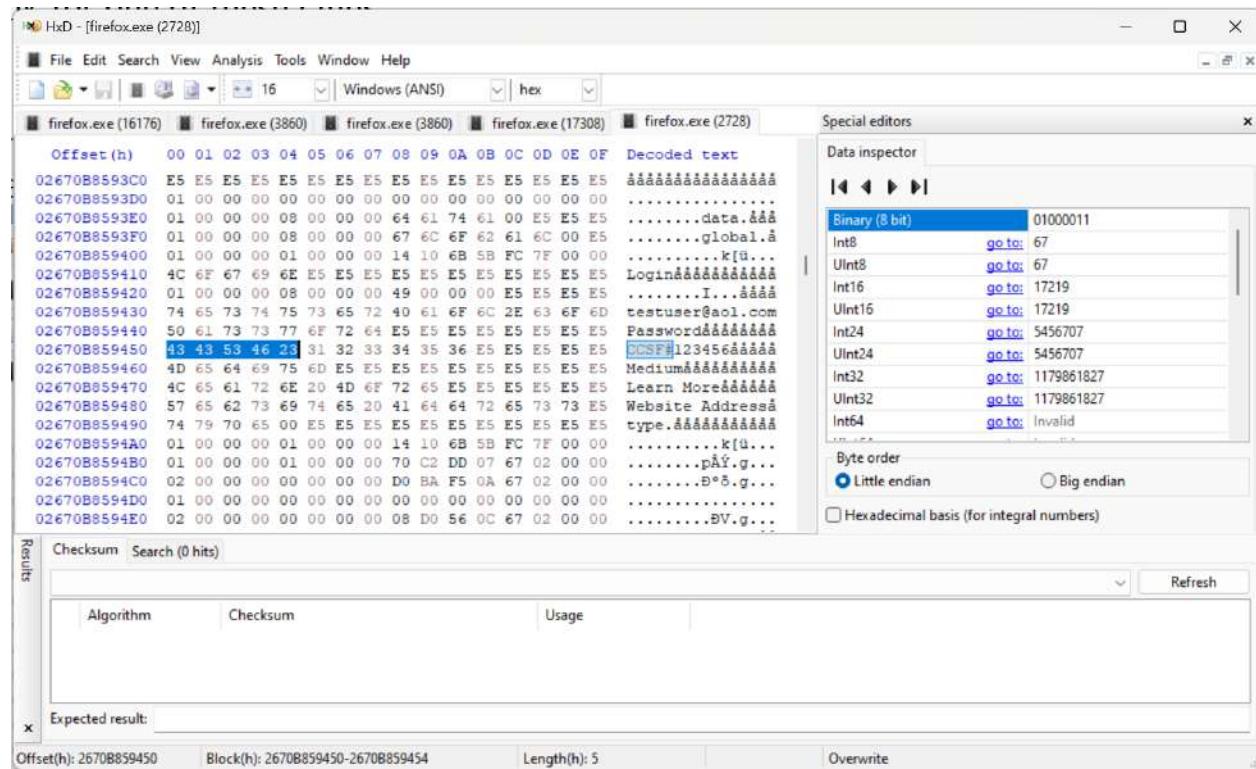
Personal and Family
Protect yourself and your family from cybercriminals.
[Get Protected](#)

Transferring data from www.keepersecurity.com...



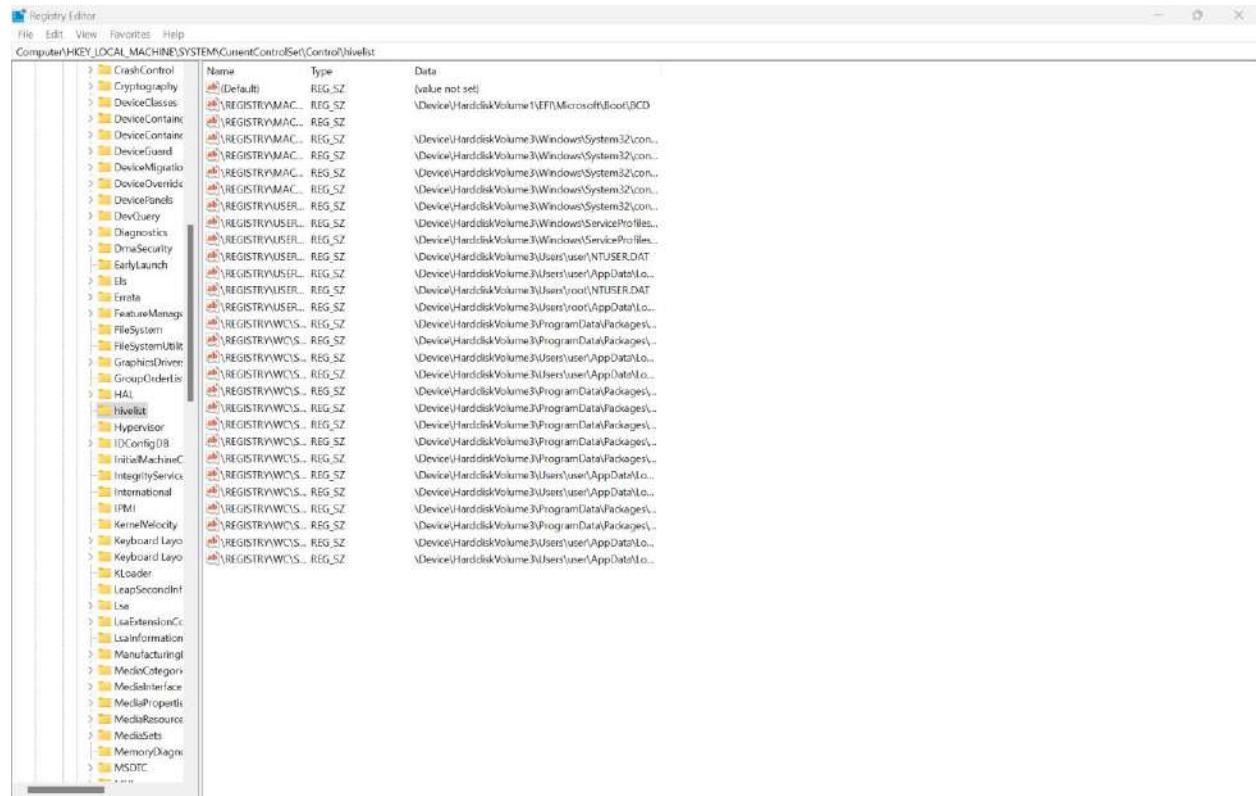
A screenshot of the Keeper Password Manager vault interface. The sidebar on the left shows 'My Vault' selected, along with other options like 'Identity & Payments', 'Security Audit', 'BreachWatch', 'Deleted Items', and 'Secure Add Ons'. The main area displays a 'Protect Your Digital Life with Keeper.' section with icons for 'Records', 'Folders', and 'Sharing'. A modal window is open in the center-right, titled 'Create New', for creating a new 'Login' record. The modal fields include 'Title (Required)' (Facebook), 'Login' (testuser@aol.com), 'Password' (CCSF#123456), and 'Website Address' (https://facebook.com). The bottom of the screen shows a status bar with 'encryption: ON' and navigation links for 'Sync', 'Work Offline', 'Help', and 'Privacy Policy'.

HxD EXAMINING:

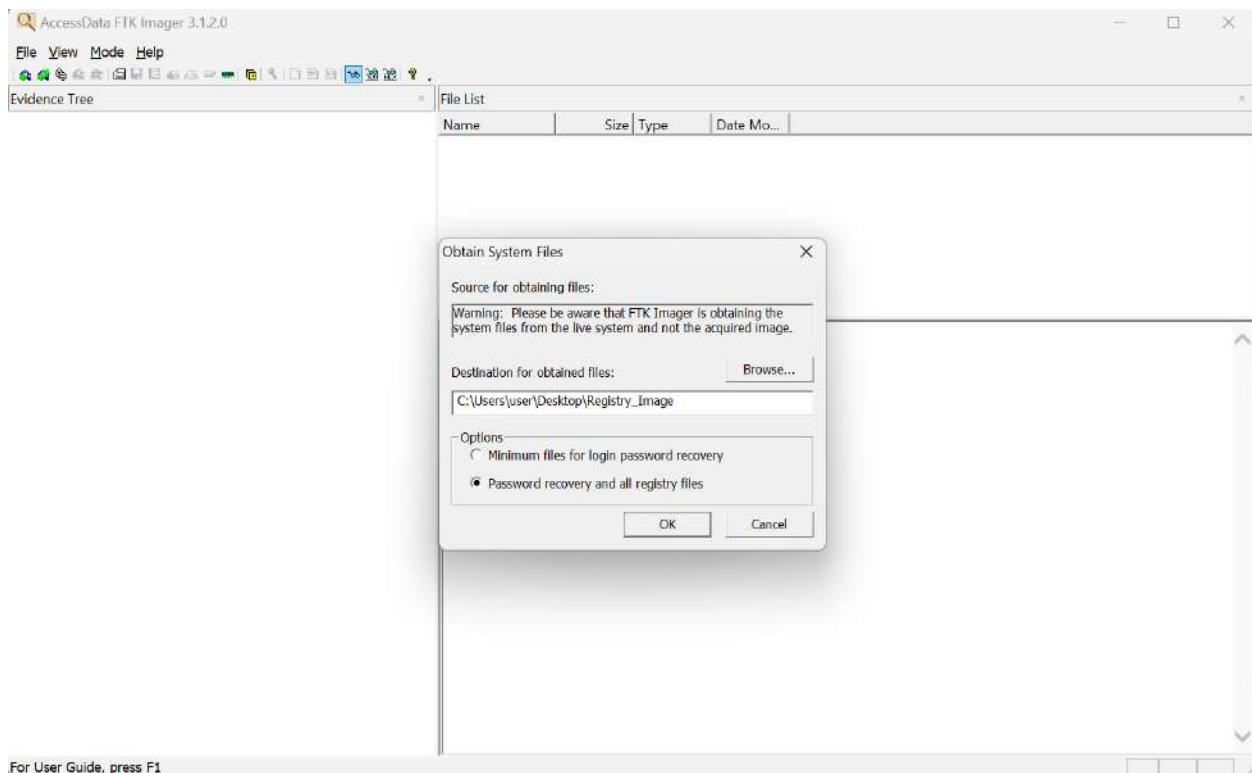


7. Capturing and examining the registry

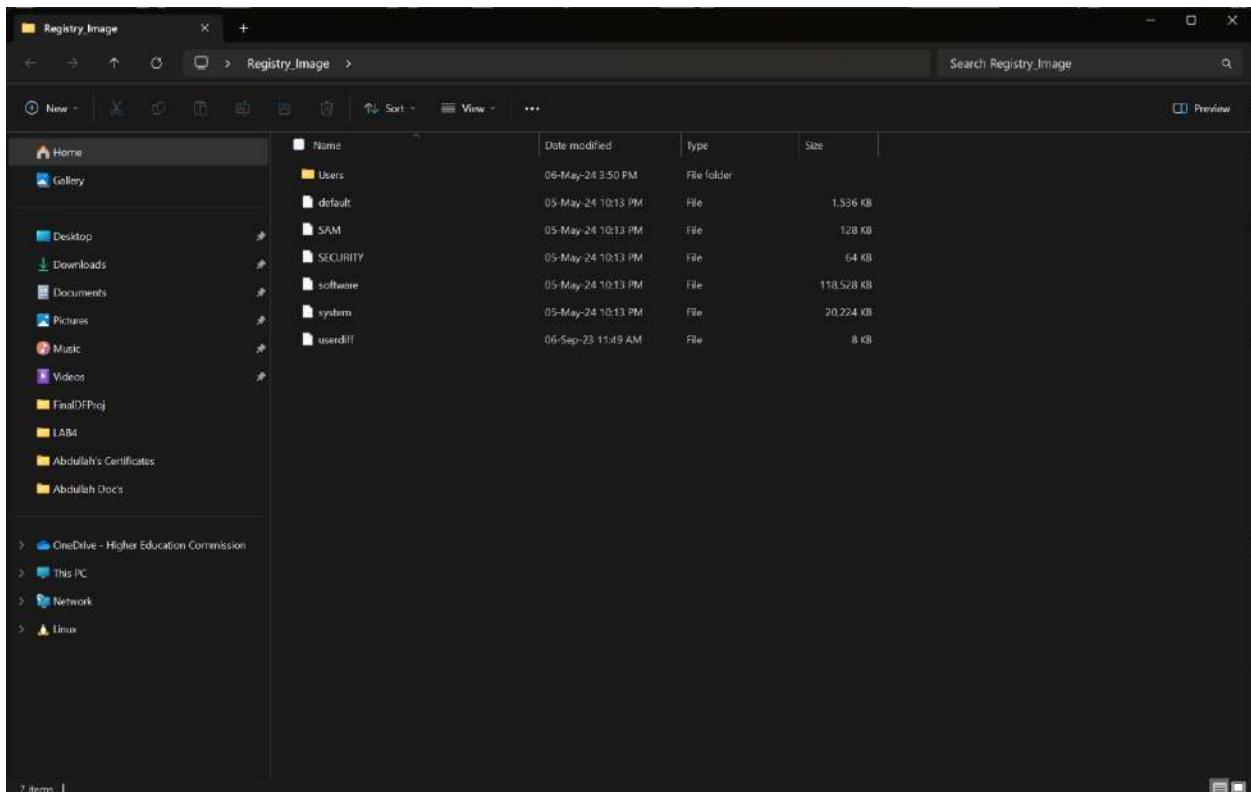
REGISTRY EXAMINATION:



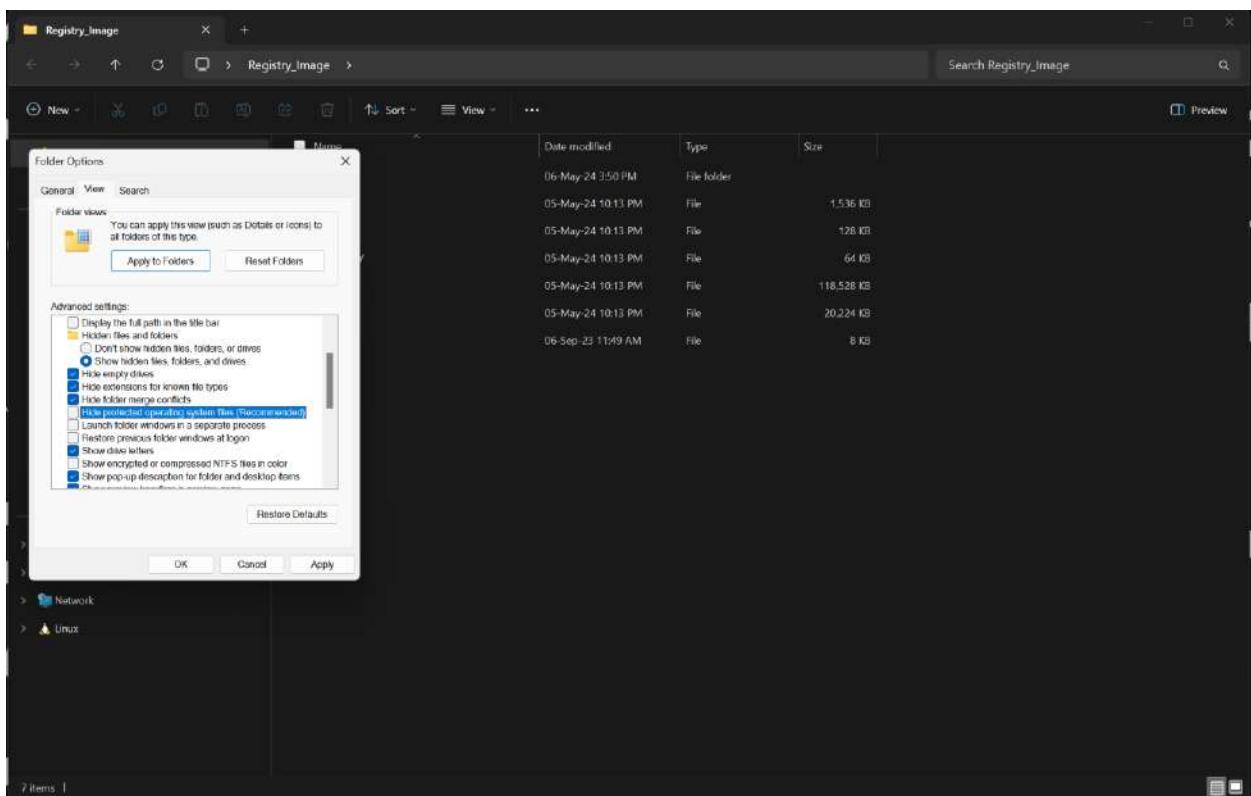
MAKING IMAGE OF REGISTRY:



REGISTRY IMAGE FOLDER AFTER CREATION:



CHECKING FOLDER OPTIONS:



MAKING OF AUTOPSY CASE:

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: Registry

Base Directory: D:\FinalDFProj\T7\

Case Type: Single-User Multi-User

Case data will be stored in the following directory:
D:\FinalDFProj\T7\Registry

< Back **Next >** Finish Cancel Help

CASE INFORMATION:

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 1

Examiner

Name: Abdullah

Phone: 031030657860

Email: abdullahamqbool08@gmail.com

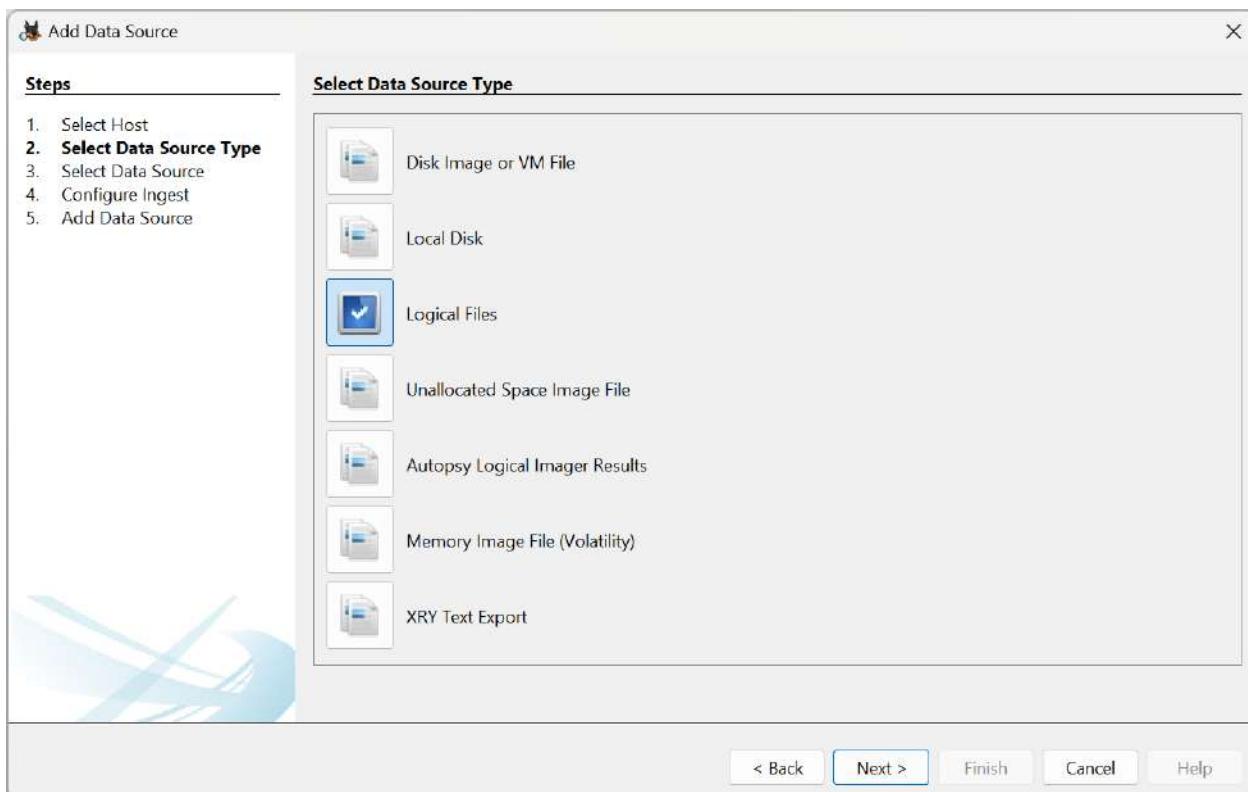
Notes:

Organization

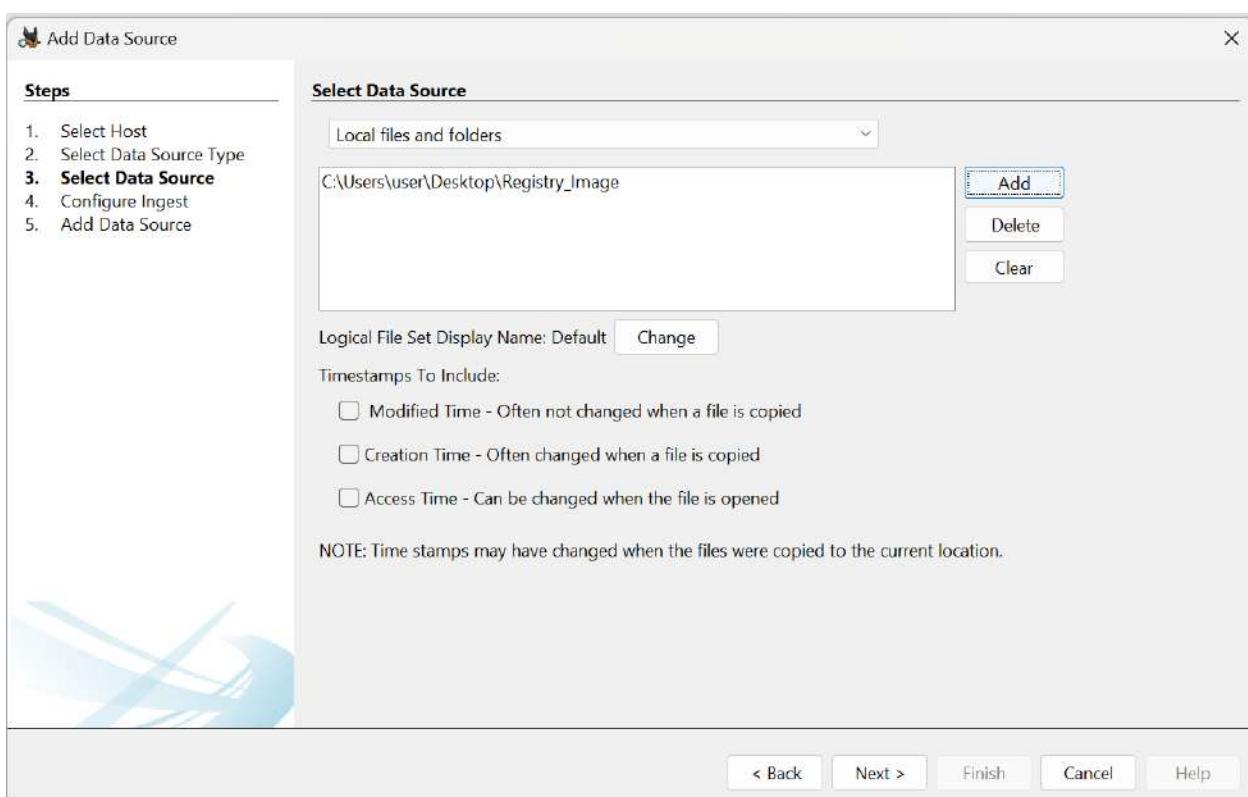
Organization analysis is being done for: Not Specified **Manage Organizations**

< Back **Next >** Finish Cancel Help

SELECTING DATA SOURCE:



DATA SOURCE:



NTUSER.DAT EXAMINATION:

The screenshot shows the Autopsy 4.21.0 interface with the 'Registry' module selected. In the left sidebar, under 'Data Sources', there is a tree view of logical file sets and their contents. The 'LogicalFileSet_1 Host' node has a 'LogicalFileSet1 (1)' child, which further contains a 'Registry_Image (7)' node. This node has a 'Users (8)' folder, which contains several sub-folders like 'All Users (0)', 'Default (1)', 'Default User (0)', 'Public (0)', 'root (3)', and 'user (3)'. Below this, there are sections for 'File Views', 'Data Artifacts', and 'Analysis Results'. The main pane displays a table titled 'Listing /LogicalFileSet1/Registry_Image/Users/user'. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. One row is highlighted for 'NTUSER.DAT'. At the bottom of the main pane, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Text' tab is currently selected, showing a tree view of registry keys under 'ROOT'. The 'Count' key is expanded, showing its sub-values.

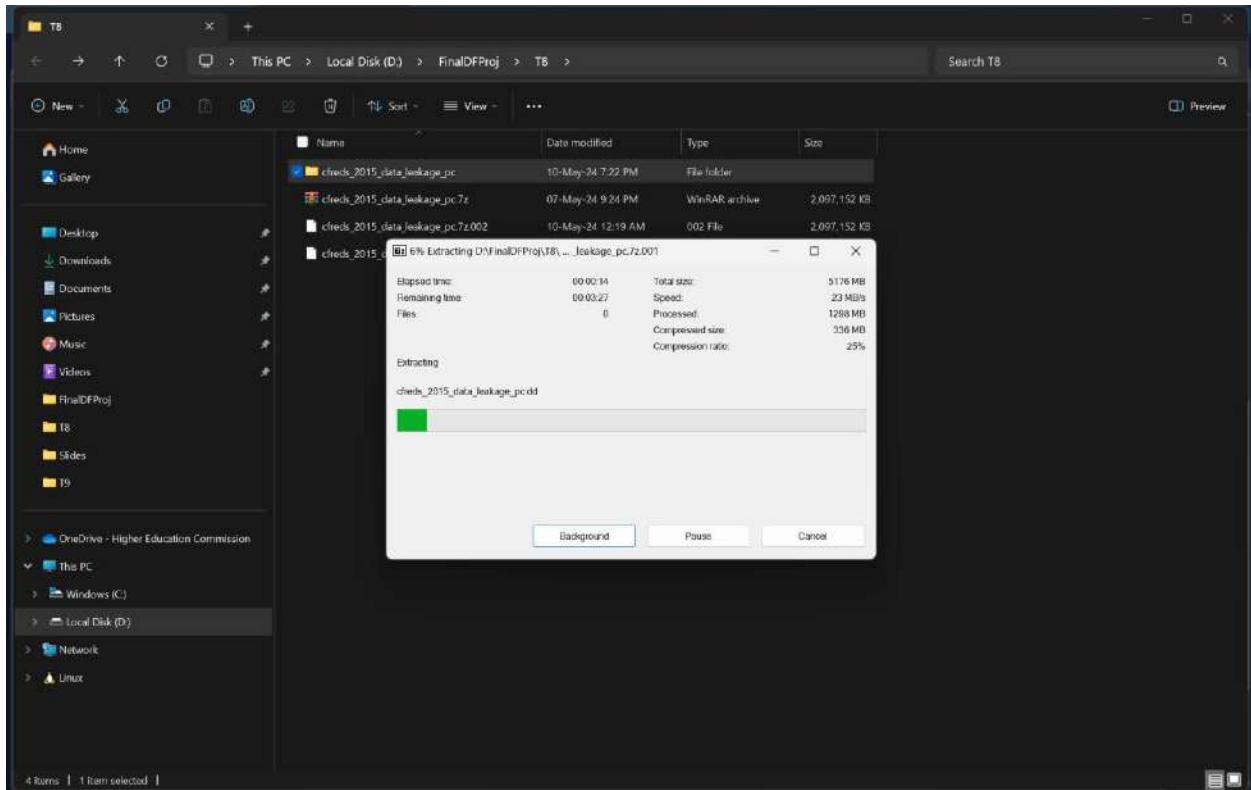
OPENING OF ROT 13:

This screenshot shows the same Autopsy interface as the previous one, but the 'Text' tab in the bottom pane is now active, displaying the contents of the 'Count' registry key. The key's value data is shown in ROT 13 encoding. The values are:

- (B267E3AD-A825-4A09-82B9-FEC22
- (BCB4B33B-4D00-4BF8-B800-D319X
- (CAAA59E3C-4792-41A5-9909-6A6A:
- (CEBFB1SCD-ACE2-4F4F-917B-9926Fz
- Count
 - HRZB_PGYHNPbjag.pgbe
 - HRZB_PGYHNPbjVVA
 - Zpweb.lbsg.lwqbfSrqqcnpxU
 - Zpweb.lbsg.lwqbfPmphyngjt
 - Zpweb.lbsg.lwqbfAbgrmq.8
 - Zpweb.lbsg.lwqbfPyrag.POI
 - Zpweb.lbsg.lwqbfPyrag.POFe_psa1uZoJqfjPsegnanHV
 - Zpweb.lbsg.lwqbfPyrag.POFe_psa1uZoJqfjPsegnanHV

8. Examining a window disk image.

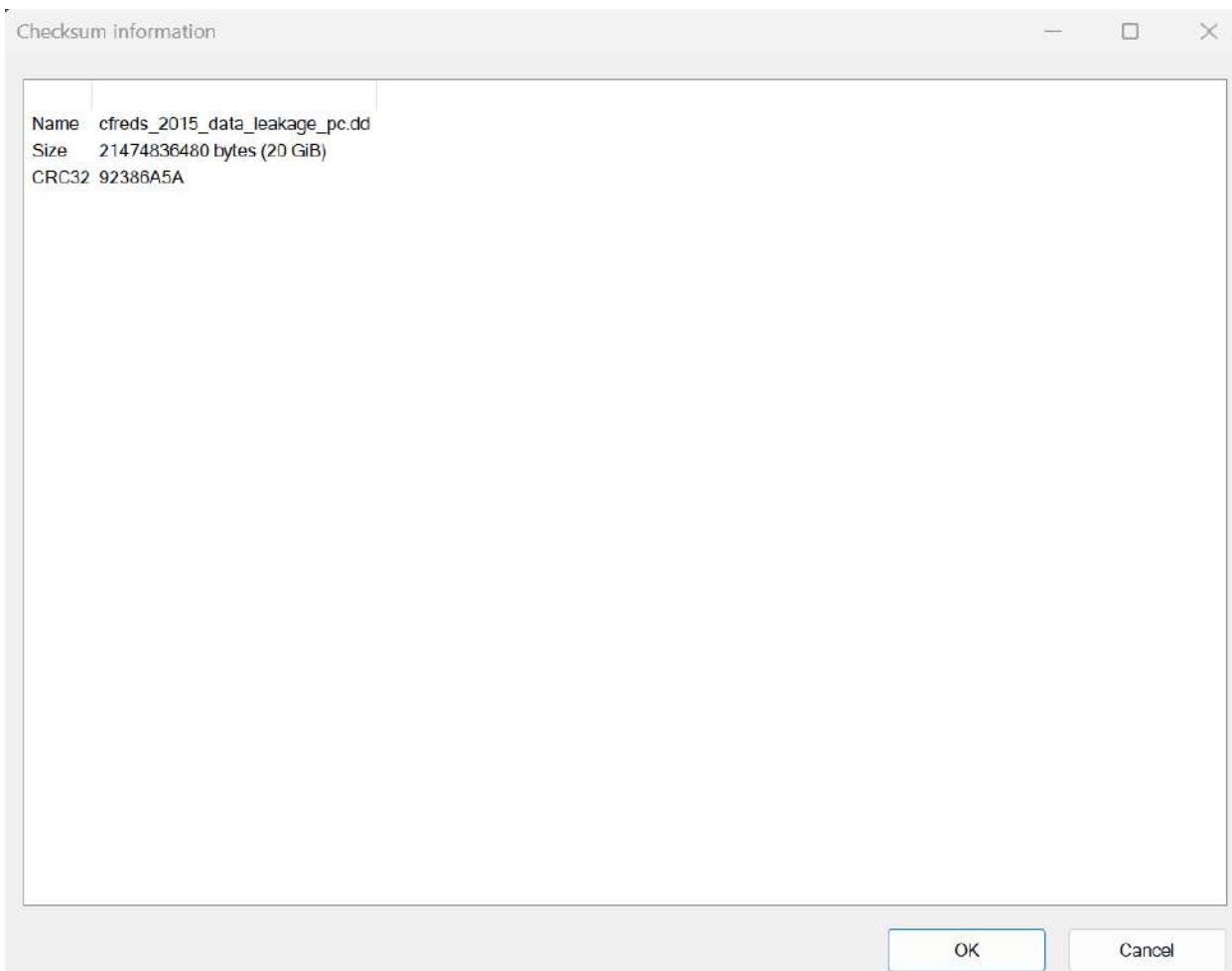
DOWNLOADING EVIDENCE FILE:



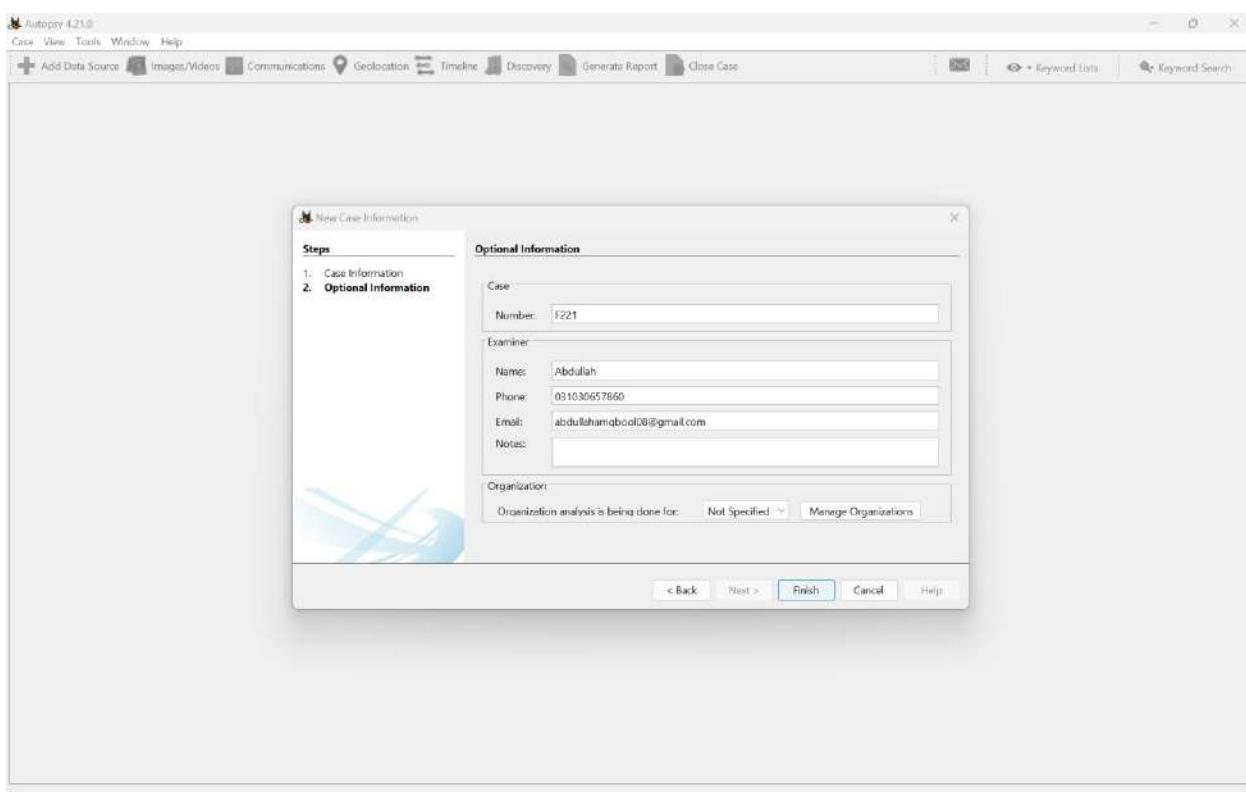
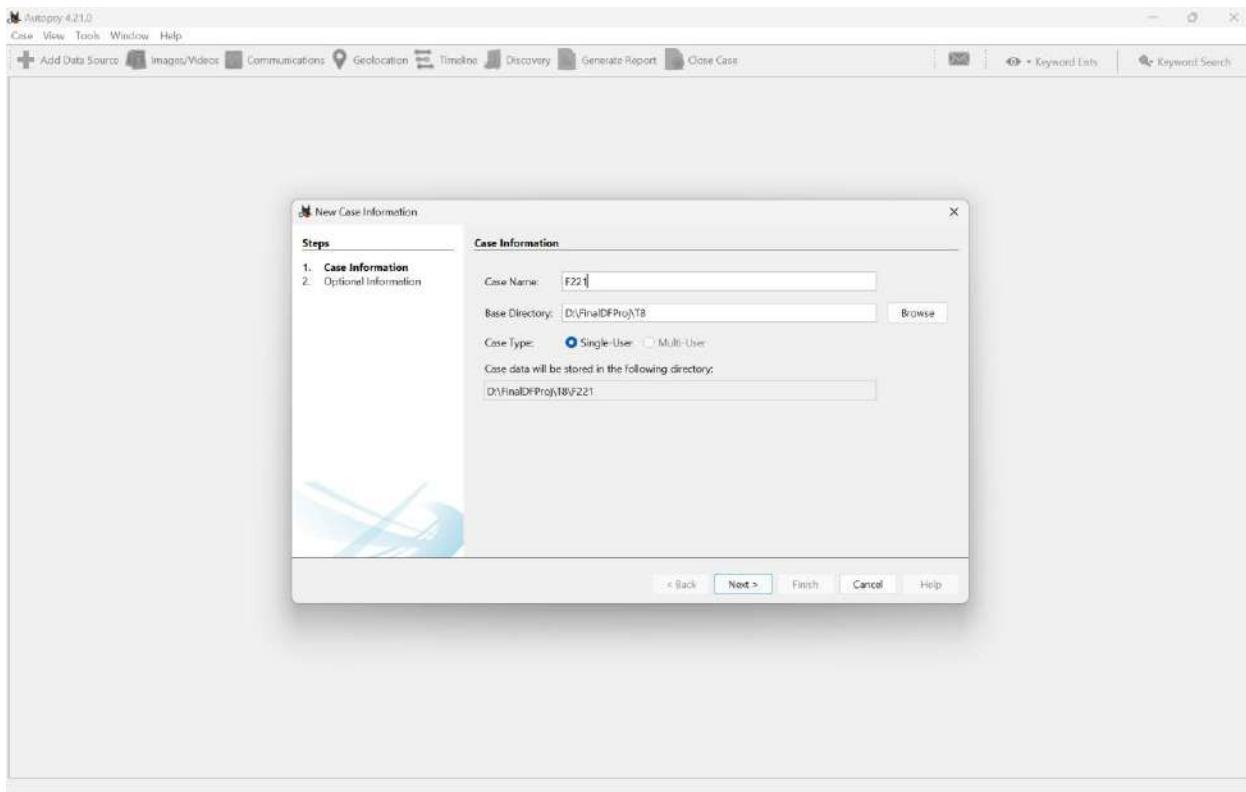
VERIFYING THE HASH:

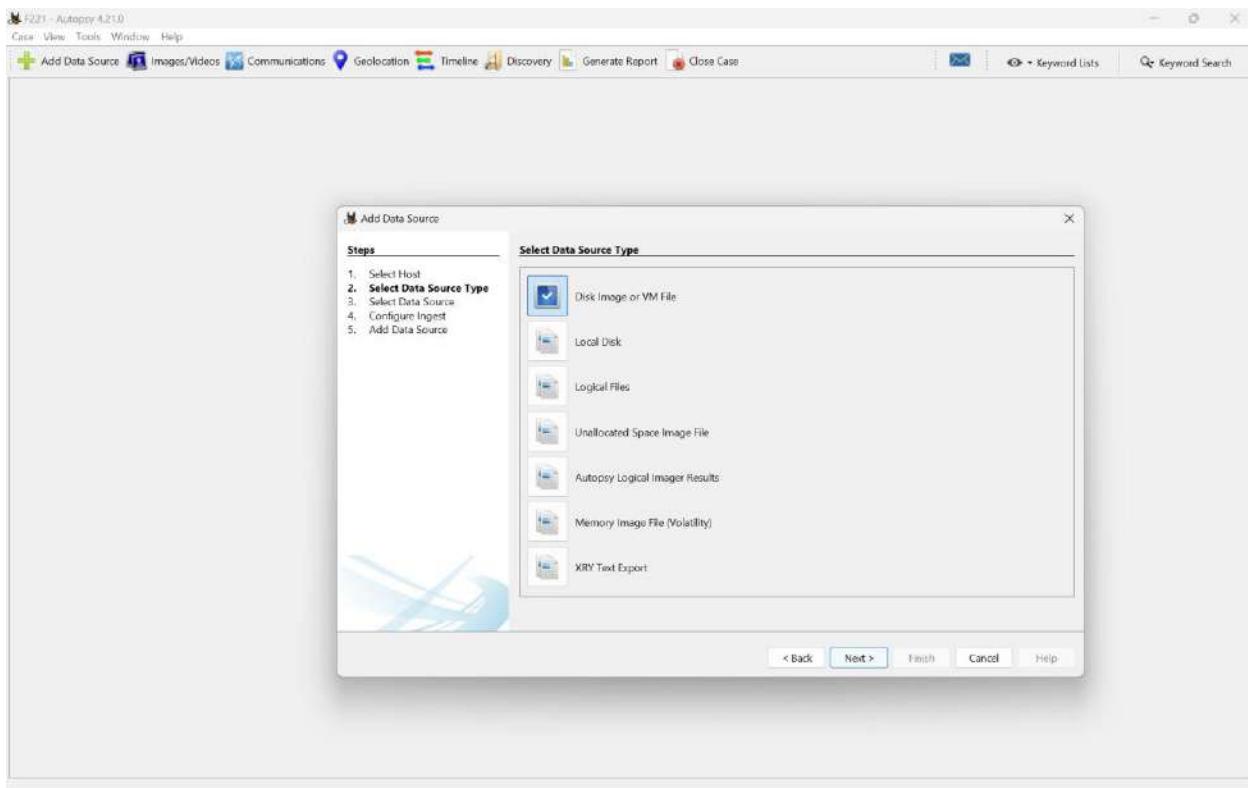
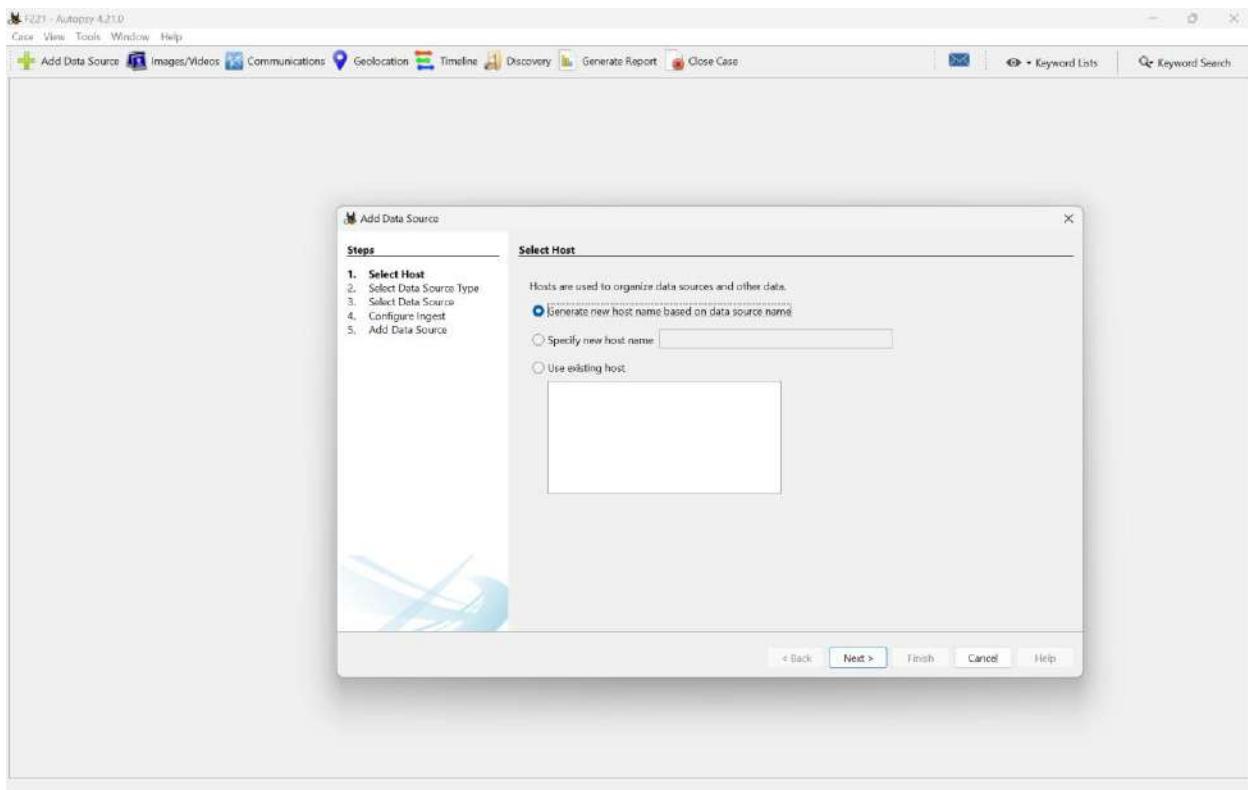
```
PS D:\FinalDFProj\T8\cfreds_2015_data_leakage_pc> Get-FileHash -Algorithm MD5 cfreds_2015_data_leakage_pc.dd
Algorithm      Hash
----          ----
MD5           A49D1254C873808C58E6F1BCD60B5BDE
Path
----          -----
D:\FinalDFProj\T8\cfreds_2015...
```

CRC32 HASH:

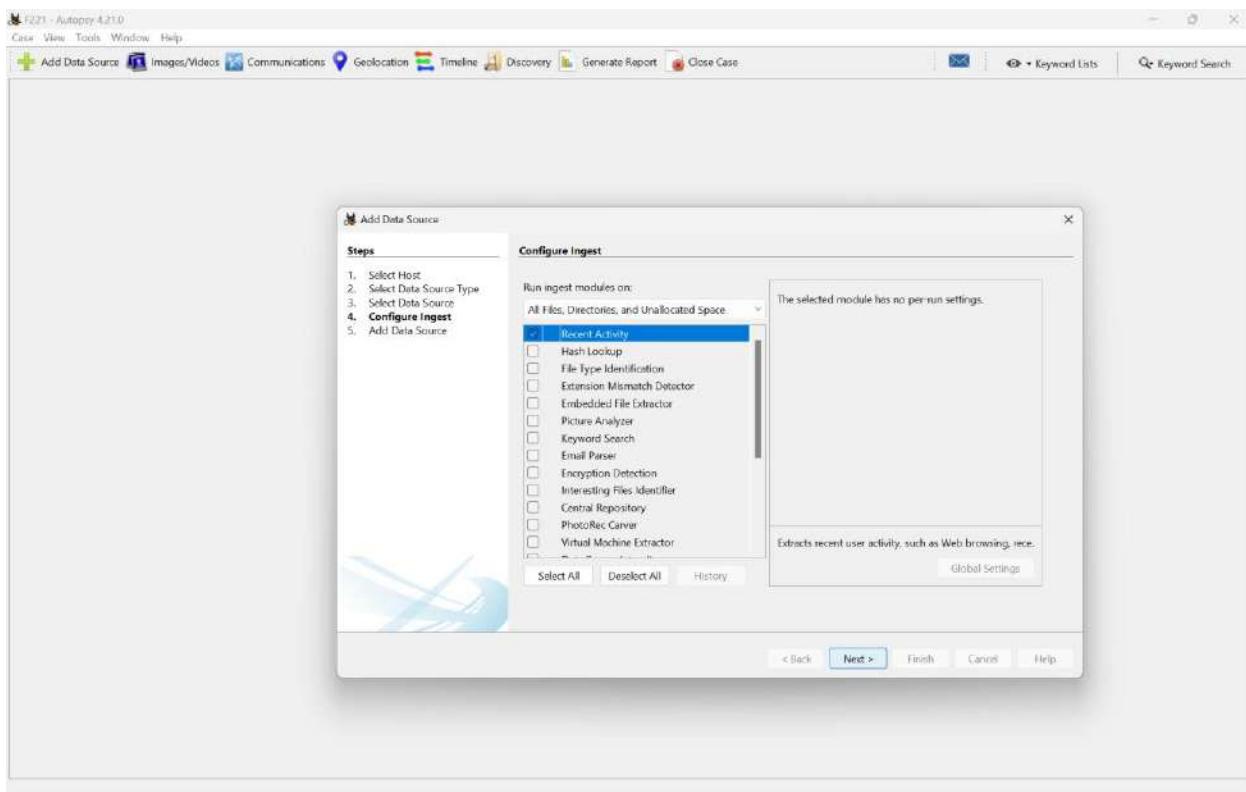
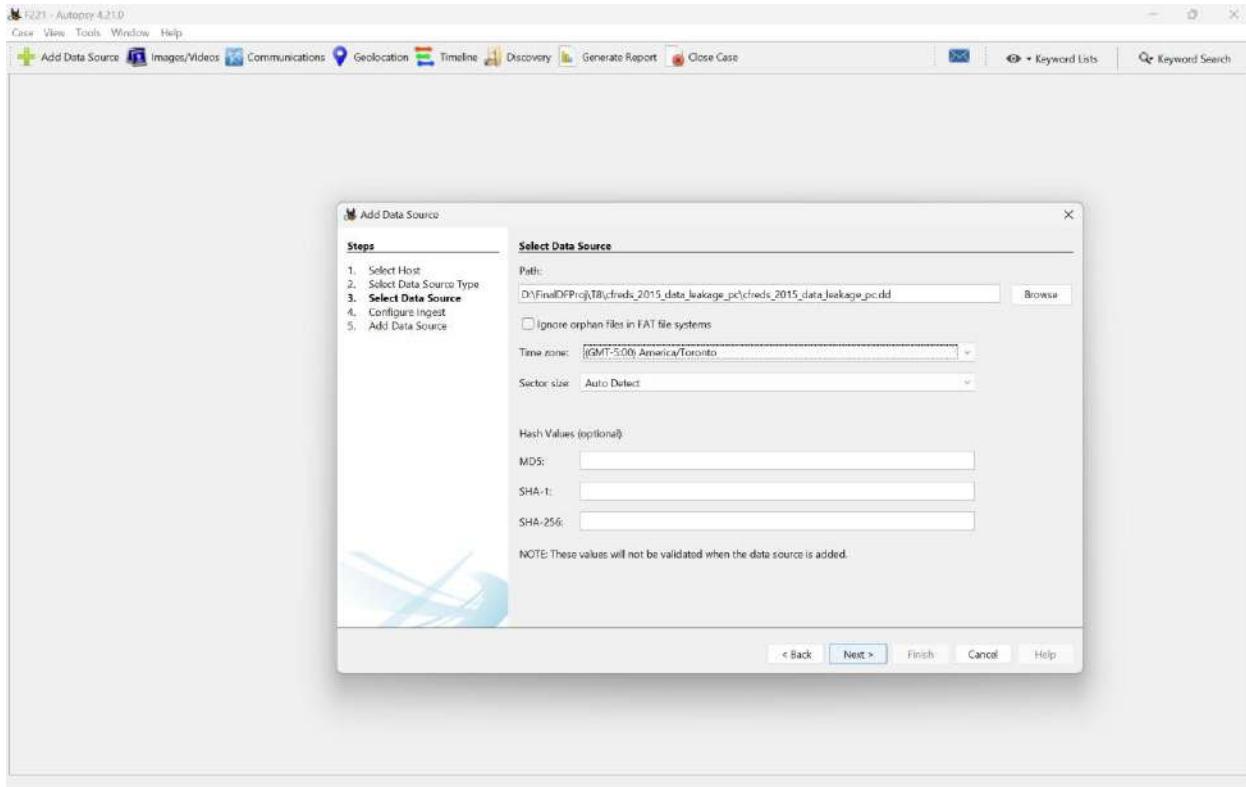


IMPORTING EVIDENCE IMAGE:





SETTING TIME ZONE:



DATA ARTIFACTS:

MOST RECENTLY INSTALLED PROGRAM:

The screenshot shows the Autopsy 4.2.1.0 interface with the 'Installed Programs' section selected. The table displays the following data:

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE	1			DMM_Runtime	2015-03-25 10:15:21 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	1			MPlayer2	2015-03-25 10:15:21 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			iCloud v.0.6.25	2015-03-25 20:01:54 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Bonjour v.3.0.0.10	2015-03-23 20:00:58 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 15:04:14 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 15:03:33 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office 3D-Intl Components 2013 v.15.0.4420.1017	2015-03-22 15:01:46 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Word MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:38 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Outlook MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:37 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office OSM UX MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:34 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office Proofing [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:32 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office Proofing Tools 2013 - English v.15.0...	2015-03-22 15:01:31 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Outil de vérification linguistique 2013 de Microsoft Q...	2015-03-22 15:01:30 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Office Proofing Tools 2013 - Español v.15.0...	2015-03-22 15:01:14 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft OneNote MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:13 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Groove MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:12 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft OCF MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:11 PCT	chredd_2015_data_leakage_pcdd
SOFTWARE	0			Microsoft Publisher MUI [English] 2013 v.15.0.4420.1017	2015-03-22 15:01:10 PCT	chredd_2015_data_leakage_pcdd

MOST RECENT DOCUMENT:

F221 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Recent Documents Table Thumbnail Summary

Source Name S C O Path Date Accessed Data Source

Source Name	S	C	O	Path	Date Accessed	Data Source
Resignation_Letter_(laman_informant).psd				C:\Users\laman_informant\Desktop\Resignation_Letter_(laman_...)	2015-03-25 20:28:33 PKT	cfrods, 2015_data_leakage_pcdd
CD Drive (2).lnk				D:\	2015-03-25 02:01:11 PKT	cfrods, 2015_data_leakage_pcdd
Penguins.jpg.lnk				D:\Penguins.jpg	2015-03-25 02:01:10 PKT	cfrods, 2015_data_leakage_pcdd
Tulips.jpg.lnk				D:\Tulips.jpg	2015-03-25 01:47:30 PKT	cfrods, 2015_data_leakage_pcdd
CD Drive.lnk				D:\	2015-03-25 01:47:22 PKT	cfrods, 2015_data_leakage_pcdd
Koala.jpg.lnk				D:\Koala.jpg	2015-03-25 01:47:22 PKT	cfrods, 2015_data_leakage_pcdd
Resignation_Letter_(laman_informant).docx.LNK				C:\Users\laman_informant\Desktop\Resignation_Letter_(laman_...)	2015-03-24 23:48:41 PKT	cfrods, 2015_data_leakage_pcdd
Desktop.LNK				C:\Users\laman_informant\Desktop	2015-03-24 23:48:40 PKT	cfrods, 2015_data_leakage_pcdd
Resignation_Letter_(laman_informant).docx.lnk				C:\Users\laman_informant\Desktop\Resignation_Letter_(laman_...)	2015-03-24 23:48:40 PKT	cfrods, 2015_data_leakage_pcdd
winter_weather.advisory.zip.lnk				D:\winter_weather_advisory.zip	2015-03-24 19:01:23 PKT	cfrods, 2015_data_leakage_pcdd
[secret_project]_final_meeting.pptb.LNK				W:\10.11.11.12\secured_drive\Secret Project Data\final...	2015-03-24 01:27:37 PKT	cfrods, 2015_data_leakage_pcdd
final.lnk				W:\10.11.11.12\secured_drive\Secret Project Data\final...	2015-03-24 01:27:33 PKT	cfrods, 2015_data_leakage_pcdd
[secret_project]_final_meeting.pptb.lnk				W:\10.11.11.12\secured_drive\Secret Project Data\final...	2015-03-24 01:27:33 PKT	cfrods, 2015_data_leakage_pcdd
pacing_decision.lnk				W:\10.11.11.12\SECURED_DRIVE\Secret Project Data\...	2015-03-24 01:26:54 PKT	cfrods, 2015_data_leakage_pcdd
[secret_project]_pricing_decision.xlsx.LNK				W:\10.11.11.12\SECURED_DRIVE\Secret Project Data\...	2015-03-24 01:26:53 PKT	cfrods, 2015_data_leakage_pcdd
[secret_project]_pricing_decision.xlsx.lnk				W:\10.11.11.12\SECURED_DRIVE\Secret Project Data\...	2015-03-24 01:26:53 PKT	cfrods, 2015_data_leakage_pcdd
[secret_project]_design_concept.LNK				E:\RMF\15\Secret Project Data\design\[secret_project].d...	2015-03-23 23:38:23 PKT	cfrods, 2015_data_leakage_pcdd
[secret_project]_design_concept.lnk				E:\RMF\15\Secret Project Data\design\[secret_project].d...	2015-03-23 23:38:21 PKT	cfrods, 2015_data_leakage_pcdd
Templates.LNK				C:\Users\laman_informant\AppData\Roaming\Microsoft\Te...	2015-03-23 23:38:12 PKT	cfrods, 2015_data_leakage_pcdd

Save Table as CSV

Home Test Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

59 TIMES:

F221 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Recent Documents Table Thumbnail Summary

Source Name S C O Program Name Path Date/Time Count Comment

Source Name	S	C	O	Program Name	Path	Date/Time	Count	Comment
SLC-XE-945U\941.pf				MSCORESW.EXE	\WINDOWS\SYSTEM32\MSCORE...	2015-03-25 19:53:15 PKT	8	Prefetch File
WMIADAP.EXE-FBDFOFA2.pf				WMIADAP.EXE	\WINDOWS\SYSTEM32\WIM...	2015-03-25 18:09:47 PKT	11	Prefetch File
OSPPSVC.EXE-E5303C0.pf				OSPPSVC.EXE	\PROGRAM FILES\COMMON FILES\MICROSOFT SHAR...	2015-03-25 20:43:50 PKT	12	Prefetch File
DLLHOST.EXE-FCB71776.pf				DLLHOST.EXE	\WINDOWS\SYSTEMW64	2015-03-25 20:18:02 PKT	14	Prefetch File
DRVINST.EXE-4CB4314A.pf				DRVINST.EXE	\WINDOWS\SYSTEM32	2015-03-25 15:18:10 PKT	14	Prefetch File
IEEXPLORE.EXE-4B6C9213.pf				IEEXPLORE.EXE	\PROGRAM FILES (X86)\INTERNET EXPLORER	2015-03-25 20:23:07 PKT	14	Prefetch File
MSCORSSW.EXE				MSCORSSW.EXE	\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.303...	2015-03-25 19:53:15 PKT	14	Prefetch File
CONHOST.EXE-1F3E9D7E.pf				CONHOST.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:18:36 PKT	16	Prefetch File
WMPNSCFG.EXE-FCD0398F.pf				WMPNSCFG.EXE	\PROGRAM FILES\WINDOWS MEDIA PLAYER	2015-03-25 19:19:50 PKT	20	Prefetch File
CONSENT.EXE-531B09EA.pf				CONSENT.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:18:29 PKT	22	Prefetch File
WMPIPRVE.EXE-162B051C.pf				WMPIPRVE.EXE	\WINDOWS\SYSTEM32\WIM...	2015-03-25 20:15:55 PKT	23	Prefetch File
TASKNG.EXE-4BDE2E89.pf				TASKNG.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:16:00 PKT	25	Prefetch File
AUDIODEG.EXE-BDFD3029.pf				AUDIODEG.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:14:45 PKT	31	Prefetch File
DLLHOST.EXE-766398D2.pf				DLLHOST.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:18:29 PKT	33	Prefetch File
GOOGLEUPDATE.EXE-995715FS.pf				GOOGLEUPDATE.EXE	\PROGRAM FILES (X86)\GOOGLE\UPDATE	2015-03-25 20:16:00 PKT	38	Prefetch File
DLLHOST.EXE-5146FA0D.pf				DLLHOST.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:23:34 PKT	59	Prefetch File
CHROME.EXE-D999B1BA.pf				CHROME.EXE	\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION...	2015-03-25 02:05:38 PKT	71	Prefetch File
SEARCHPROTODCOLHOST.EXE-0CBBACDE.pf				SEARCHPROTODCOLHOST.EXE	\WINDOWS\SYSTEM32	2015-03-25 22:28:34 PKT	76	Prefetch File
SEARCHFILTERHOST.EXE-77482212.pf				SEARCHFILTERHOST.EXE	\WINDOWS\SYSTEM32	2015-03-25 20:28:34 PKT	82	Prefetch File

Save Table as CSV

Hex Test Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 1 Result: 1 of 1 Run Programs

Type Value

Program Name DLLHOST.EXE

Path \WINDOWS\SYSTEM32

Date/Time 2015-03-25 20:28:34 PKT

Count 59

Comment Prefetch File

Source File Path /img_cfrods_2015_data_leakage_pcdd/vol_vb3/Windows/Prefetch/DLLHOST.EXE-5146FA0D.pf

Artifact ID 013327312605A7A07A1

SEARCH:

F221 - Autopsy 4.21.0

File View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

63 Results

Save Table as CSV

Web Search

Table Thumbnail Summary

Source Name	S	C	G	Domain	Text	Program Name	Date Accessed	Data Source
WabCacheV01.dat				google.com	internet explorer 11	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	file sharing and tethering	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	file sharing and tethering	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	Top Stories	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	Top Stories	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	DPR.DRM	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	Forensic Email Investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	what is windows system artifacts	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	Investigation on windows machine	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	windows event logs	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	cd burning method	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	cd burning method in windows	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	external device and forensics	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	external device and forensics	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	anti-forensic tools	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	eraser	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl
WabCacheV01.dat				bing.com	cleaner	Microsoft Edge Analyzer	0000-00-00 00:00:00	efruds_2015_data_leakage_pc.ddl

Hex Text Application Source File Metadata OS Account Data Artifacts Analyse Results Content Annotations Other Occurrences

Result: 296 of 297 Result < > Web Search

Web Search

Term: eraser

Time: 0000-00-00 00:00:00

Domain: bing.com

Program Name: Microsoft Edge Analyzer

9. Email Forensics:

GETTING FILE HASH OF NITROBA.PCAP

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

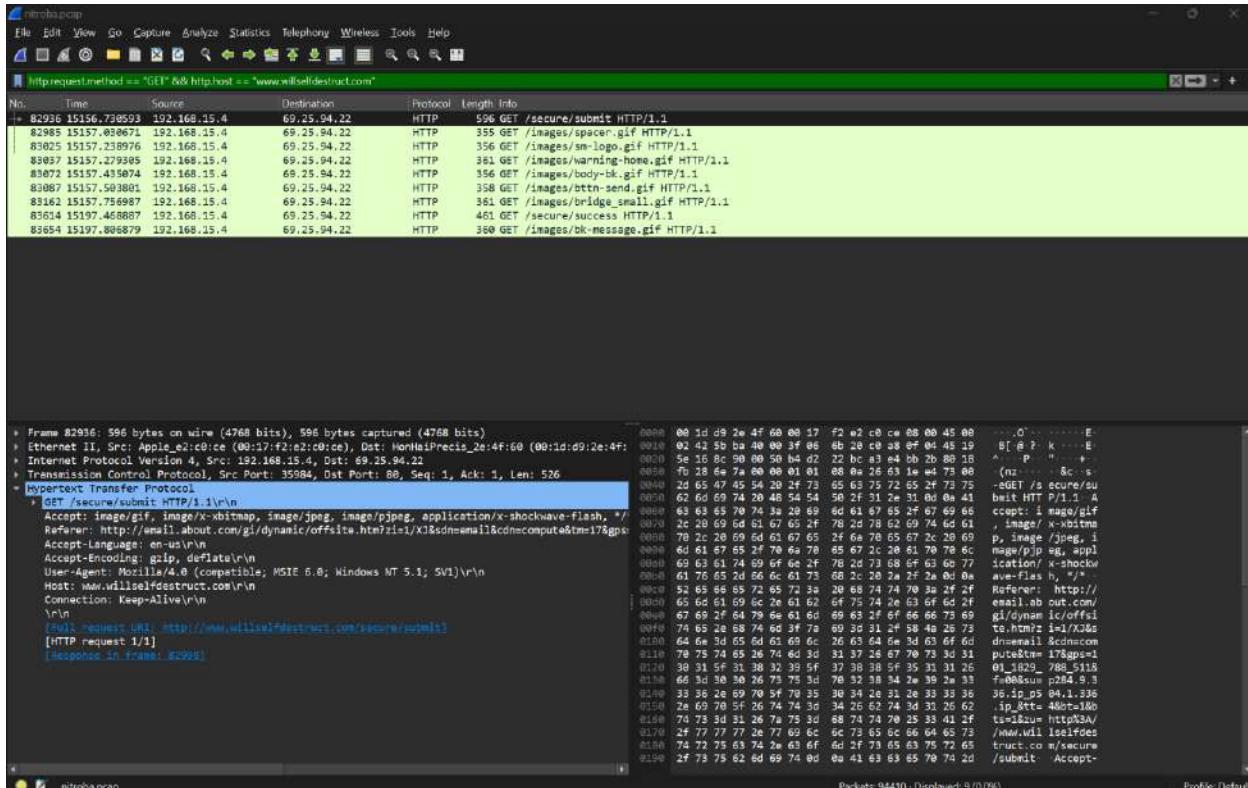
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\FinalDFProj\T9> Get-FileHash -Algorithm MD5 .\nitroba.pcap
Algorithm      Hash                                         Path
----          ----
MD5           9981827F11968773FF815E39F5458EC8             D:\FinalDFProj\T9\nitroba.pcap

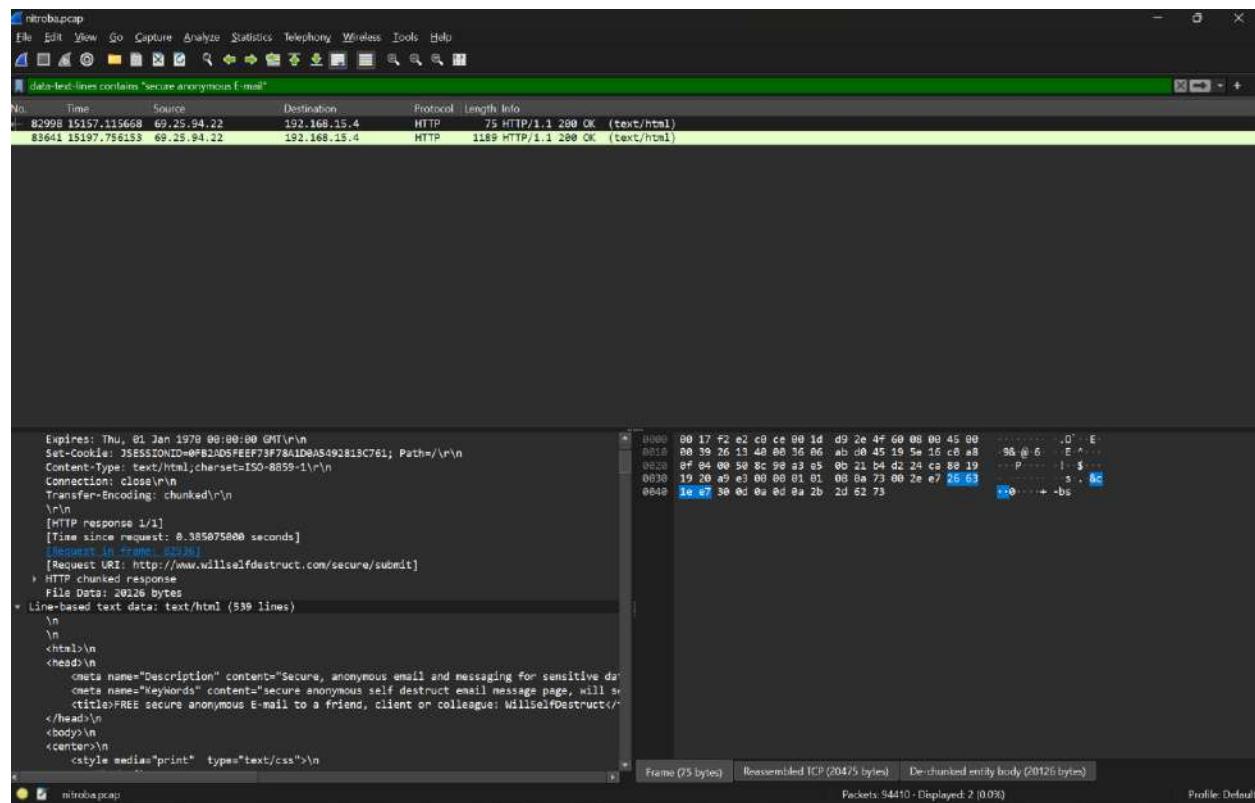
PS D:\FinalDFProj\T9> Get-FileHash -Algorithm SHA1 .\nitroba.pcap
Algorithm      Hash                                         Path
----          ----
SHA1          65656392412ADD15F93F8585197A8998AAEB50A1             D:\FinalDFProj\T9\nitroba.pcap

PS D:\FinalDFProj\T9>
```

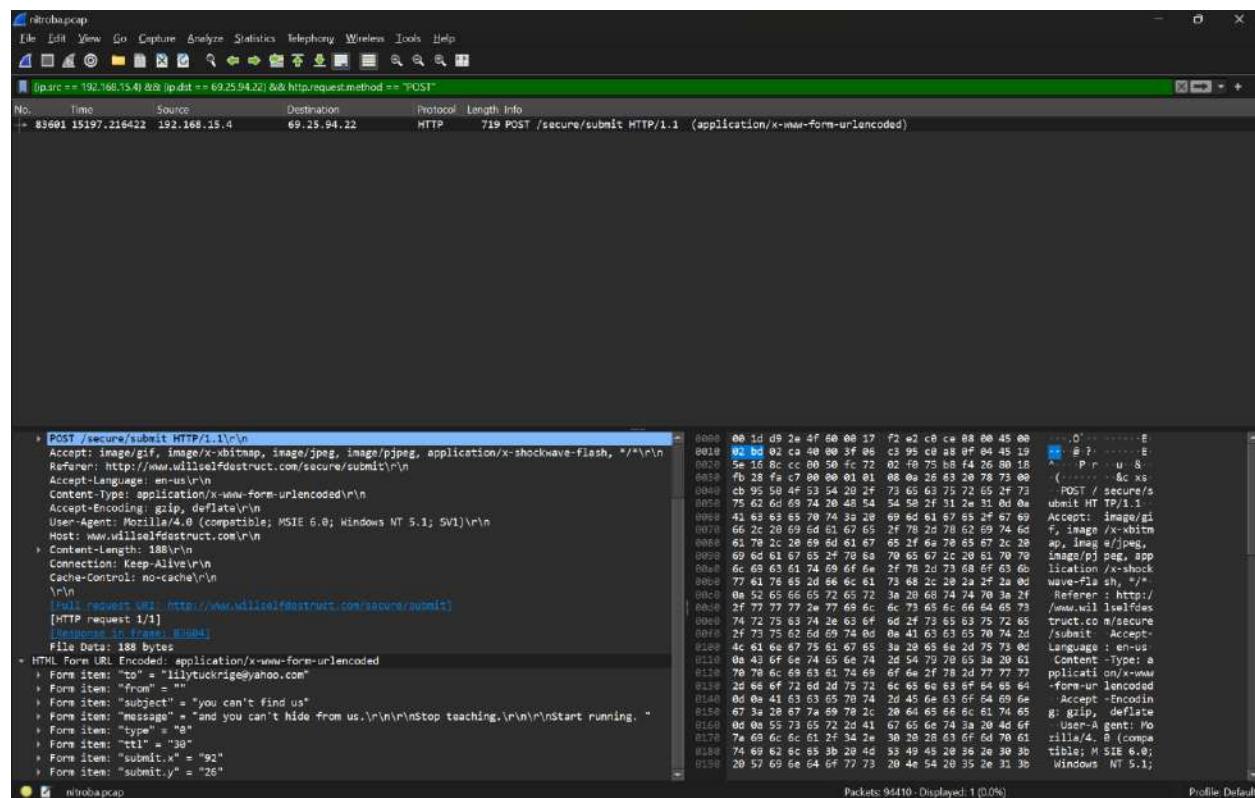
CHECKING THE HOST PACKETS GET:



SECURE ANONYMOUS EMAIL SEARCH:



CHECKING IP SRC:



CHECKING MAC ADDRESSES:

nitrocap

(ip.src == 192.168.15.4) & (ip.dst == 69.25.94.22) & http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
85601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)

```

> Frame 85601: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
> Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHuiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
> Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
> Transmission Control Protocol, Src Port: 36844, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
> Hypertext Transfer Protocol
  POST /secure/submit HTTP/1.1\r\n
    Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
    Referer: http://www.willselfdestruct.com/secure/submit/\r\n
    Accept-Language: en-us\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: www.willselfdestruct.com\r\n
    Content-Length: 188\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    (r/n)
  [Full request URI: http://www.willselfdestruct.com/secure/submit]
  [HTTP request 1/1]
  [Sequence Number: 85601]
  File Data: 188 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "to" = "lillytuckridge@yahoo.com"
    Form item: "from" =
    Form item: "subject" = "you can't find us"

```

Packets: 94410 - Displayed: 1 (0.0%) Profile: Default

nitrocap

withaddr == 00:17:f2:e2:c0:ce

No.	Time	Source	Destination	Protocol	Length	Info
85398	15197.513577	192.168.15.4	TCP	70	[TCP Retransmission]	85396 [FIN, ACK] Seq=563 Win=6492 Len=0 Tsv=1970684949 Tsrec=644030521
85399	15197.516915	192.168.15.4	TCP	79	35965 + 88 [ACK] Seq=543 Ack=563 Win=6535 Tsval=644038527 Tsrec=1970684949	
85400	15197.988118	208.185.127.40	TCP	64	[TCP Retransmission]	35898 [FIN, ACK] Seq=299 Ack=387 Win=6190 Len=0
85401	15197.150911	192.168.15.4	TCP	64	35899 + 88 [ACK] Seq=299 Ack=387 Win=64768 Len=0	
85402	15195.451786	192.168.15.4	TCP	82	36042 + 3283 [SYN] Seq=0 Win=65555 Len=0 NS=1460 NS=2 Tsv=1970684949 Tsrec=0 SACK_PERM	
85403	15196.388296	192.168.15.4	TCP	82	[TCP Retransmission]	36042 + 3283 [SYN, ACK] Seq=563 Win=65555 Len=0 NS=2 Tsv=1970684949 Tsrec=0 SACK_PERM
85404	15197.118251	192.168.15.4	TCP	69	25.94.22	36044 + 88 [SYN] Seq=0 Win=64240 Len=0 NS=1 Tsv=1970684949 Tsrec=0 SACK_PERM
85405	15197.285882	69.25.94.22	TCP	79	88 + 36044 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM	
85406	15197.210545	192.168.15.4	TCP	69	25.94.22	36044 + 88 [ACK] Seq=1 Ack=1 Win=64296 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM
85407	15197.215799	192.168.15.4	TCP	69	22.167.247	36044 + 88 [ACK] Seq=1 Ack=1 Win=64296 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM
85408	15197.216422	192.168.15.4	HTTP	69	25.94.22	719 POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)
85409	15197.223434	192.168.15.4	TCP	79	88 + 35956 [FIN, ACK] Seq=366 Win=6432 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM	
85410	15197.311456	69.25.94.22	TCP	79	88 + 36044 [ACK] Seq=366 Ack=366 Win=6432 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM	
85411	15197.373985	192.168.15.4	TCP	69	25.94.22	36044 + 88 [FIN, ACK] Seq=366 Ack=366 Win=6432 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM
85412	15197.373985	192.168.15.4	TCP	79	88 + 36044 [FIN, ACK] Seq=299 Ack=550 Win=6498 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM	
85413	15197.376297	192.168.15.4	TCP	69	25.94.22	36044 + 88 [ACK] Seq=299 Ack=550 Win=6498 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM
85414	15197.376686	192.168.15.4	TCP	69	25.94.22	36044 + 88 [ACK] Seq=299 Ack=550 Win=6498 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM
85415	15197.377311	192.168.15.4	TCP	69	25.94.22	36044 + 88 [ACK] Seq=299 Ack=550 Win=6498 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM
85416	15197.379749	192.168.15.4	TCP	69	25.94.22	36044 + 88 [SYN] Seq=0 Win=64240 Len=0 NS=1 Tsv=1970684949 Tsrec=0 SACK_PERM
85417	15197.388296	192.168.15.4	TCP	69	22.167.247	36044 + 88 [SYN, ACK] Seq=563 Win=65355 Len=0 NS=2 Tsv=1970684949 Tsrec=0 SACK_PERM
85418	15197.423344	69.25.94.22	TCP	79	88 + 36044 [ACK] Seq=563 Ack=366 Win=6432 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM	
85419	15197.446492	192.168.15.4	TCP	79	88 + 36044 [ACK] Seq=291 Ack=653 Win=6498 Len=0 Tsv=1970684949 Tsrec=0 SACK_PERM	

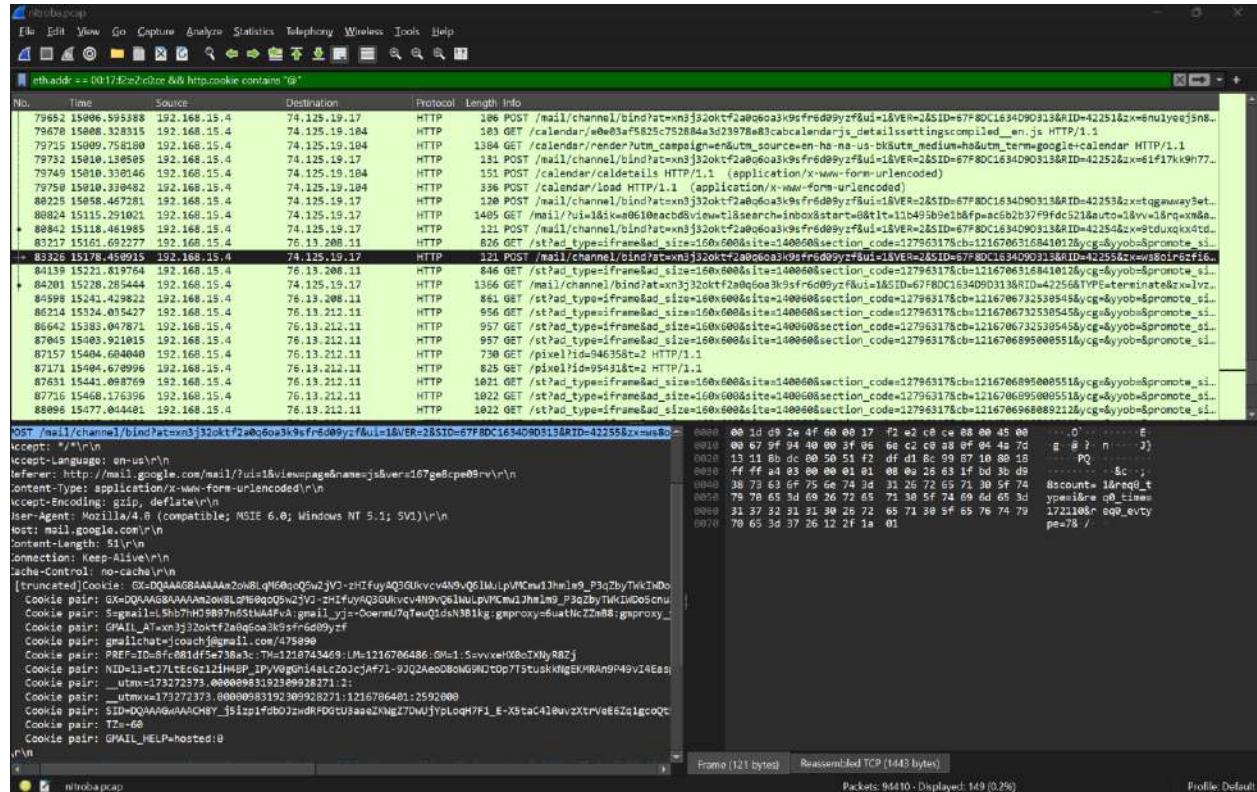
```

> Frame 85601: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
> Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHuiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
> Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
> Transmission Control Protocol, Src Port: 36844, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
> Hypertext Transfer Protocol
  POST /secure/submit HTTP/1.1\r\n
    Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
    Referer: http://www.willselfdestruct.com/secure/submit/\r\n
    Accept-Language: en-us\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: www.willselfdestruct.com\r\n
    Content-Length: 188\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    (r/n)
  [Full request URI: http://www.willselfdestruct.com/secure/submit]
  [HTTP request 1/1]
  [Sequence Number: 85601]
  File Data: 188 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "to" = "lillytuckridge@yahoo.com"
    Form item: "from" =
    Form item: "subject" = "you can't find us"

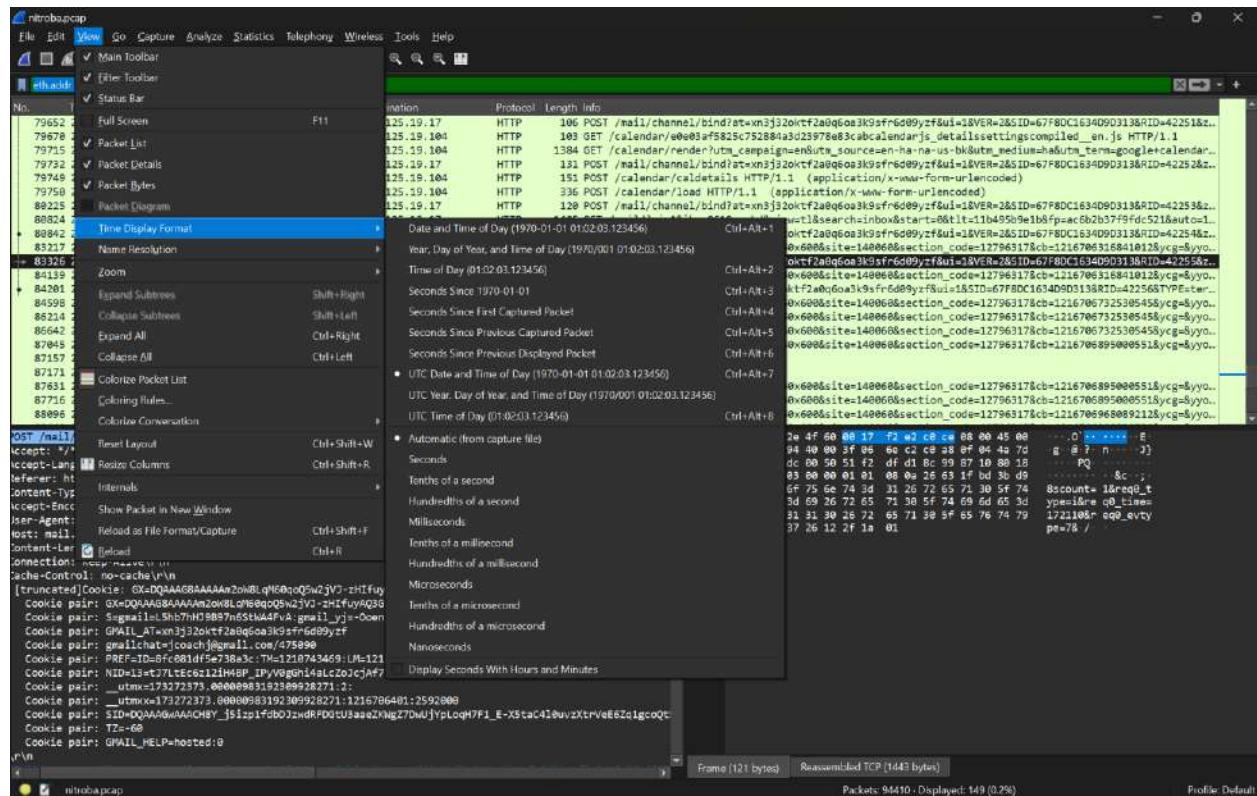
```

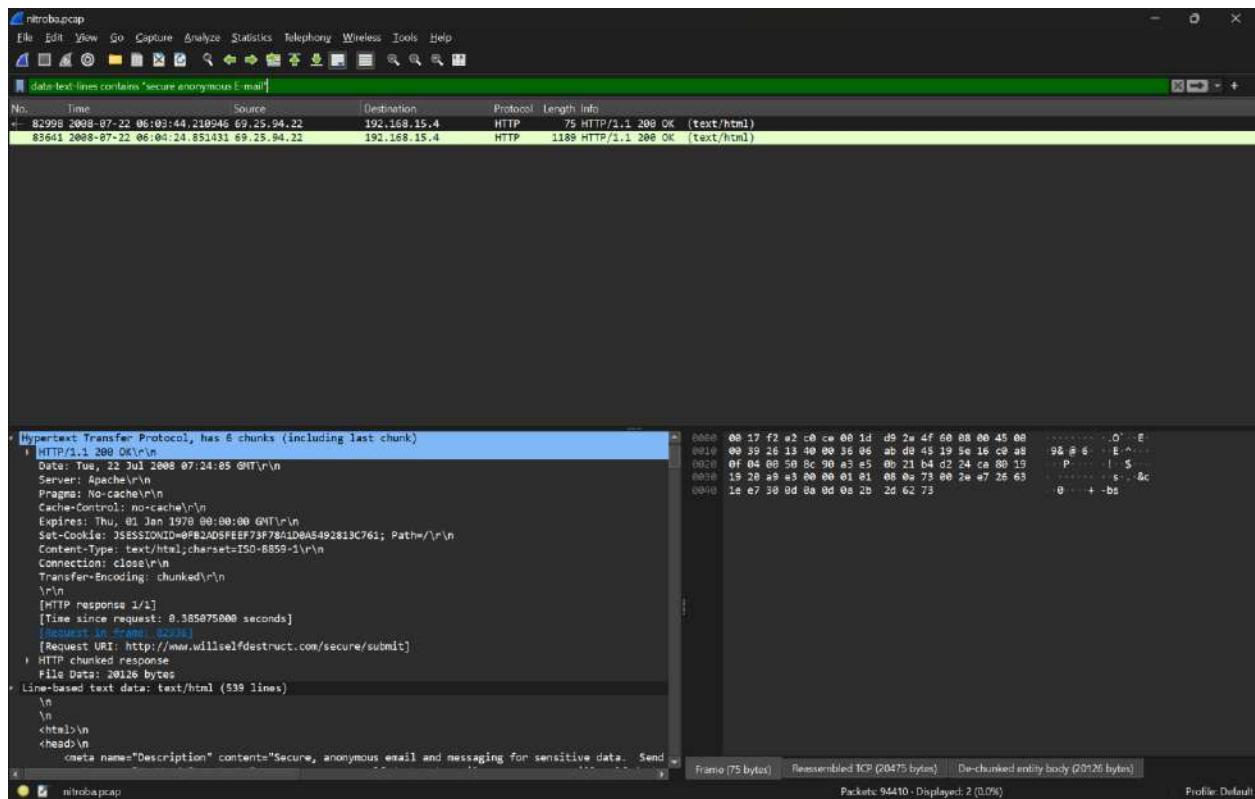
Packets: 94410 - Displayed: 7346 (77.6%) Profile: Default

CHECKING EMAIL THROUGH REGEX:



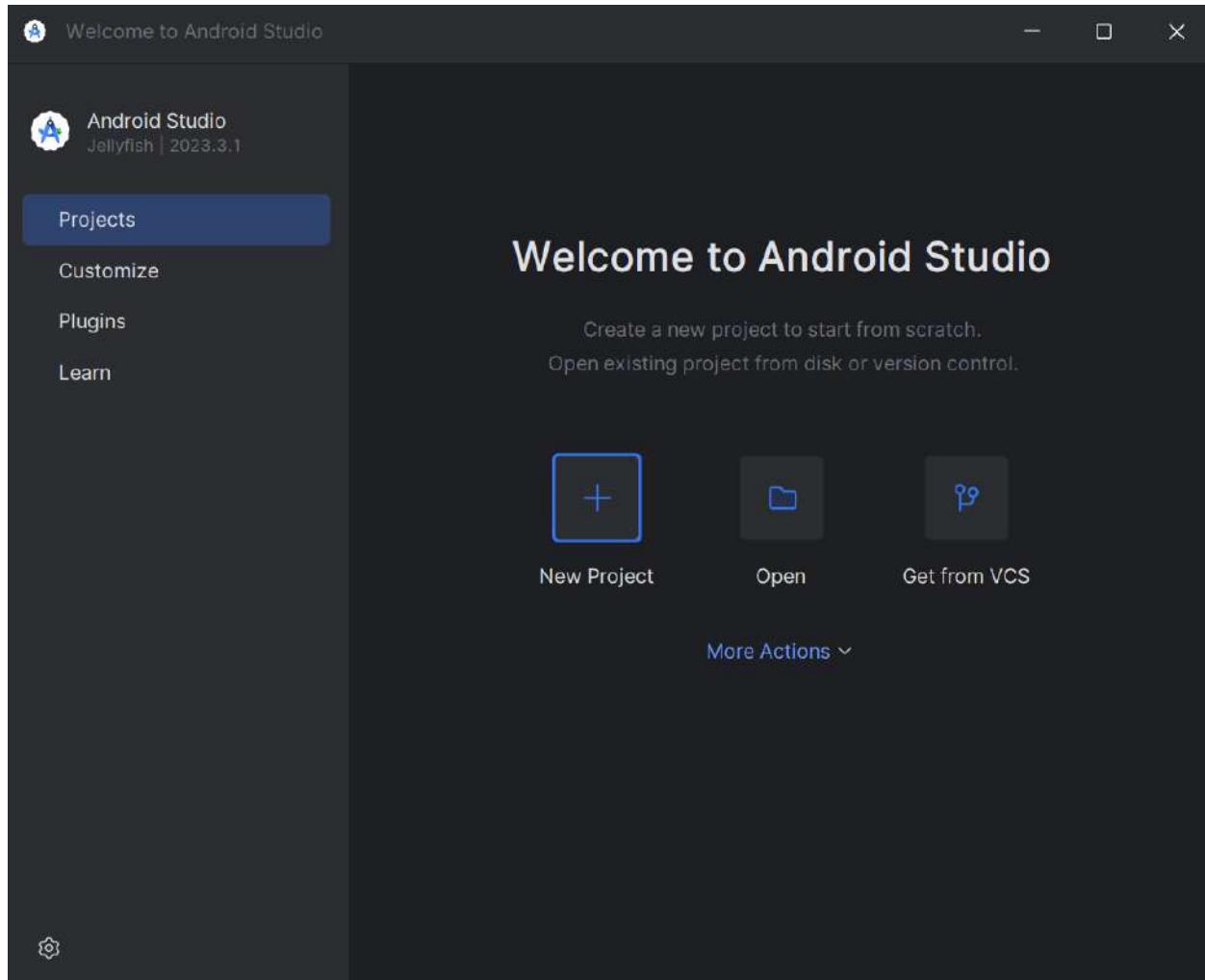
CHECKING TIME OF PACKET:



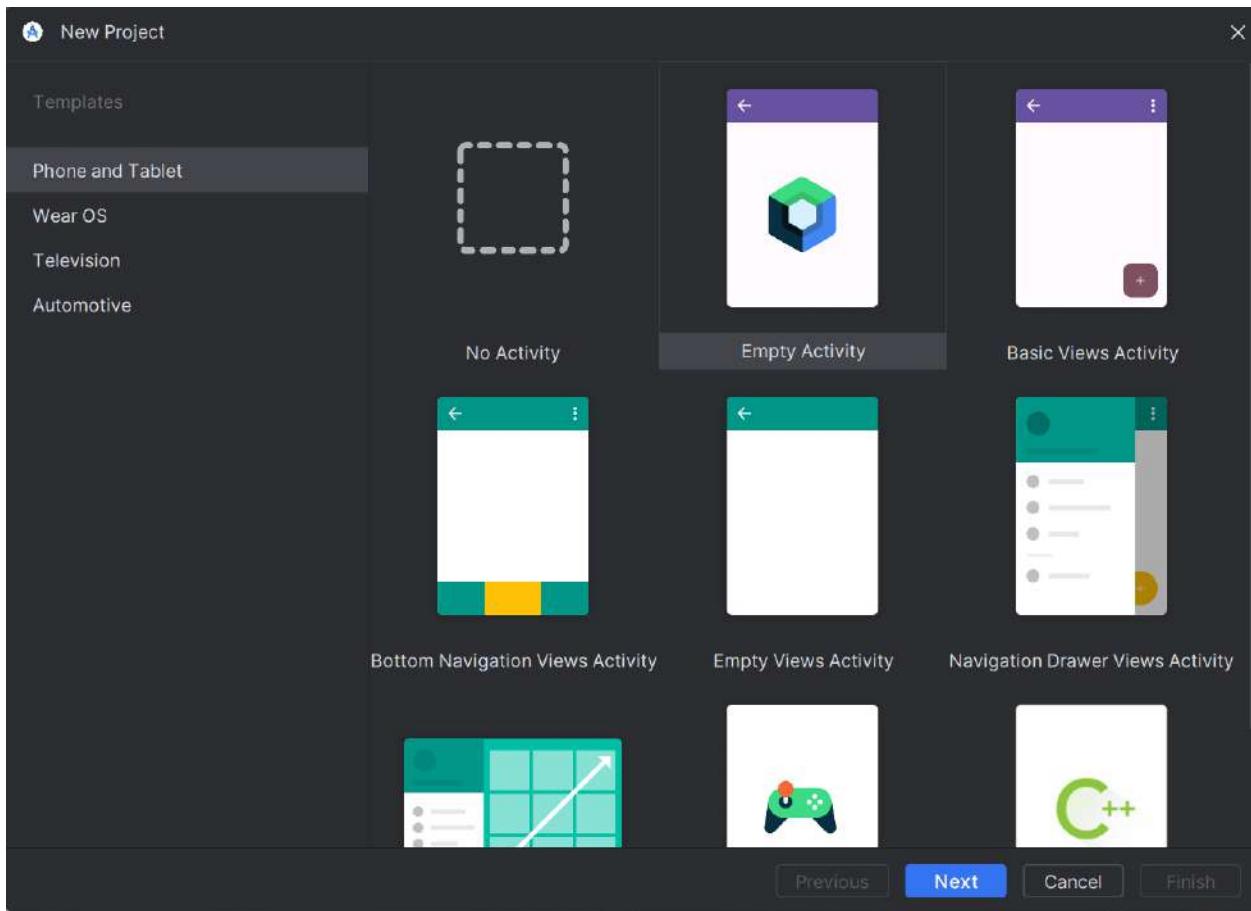


10. Android Studio Emulator

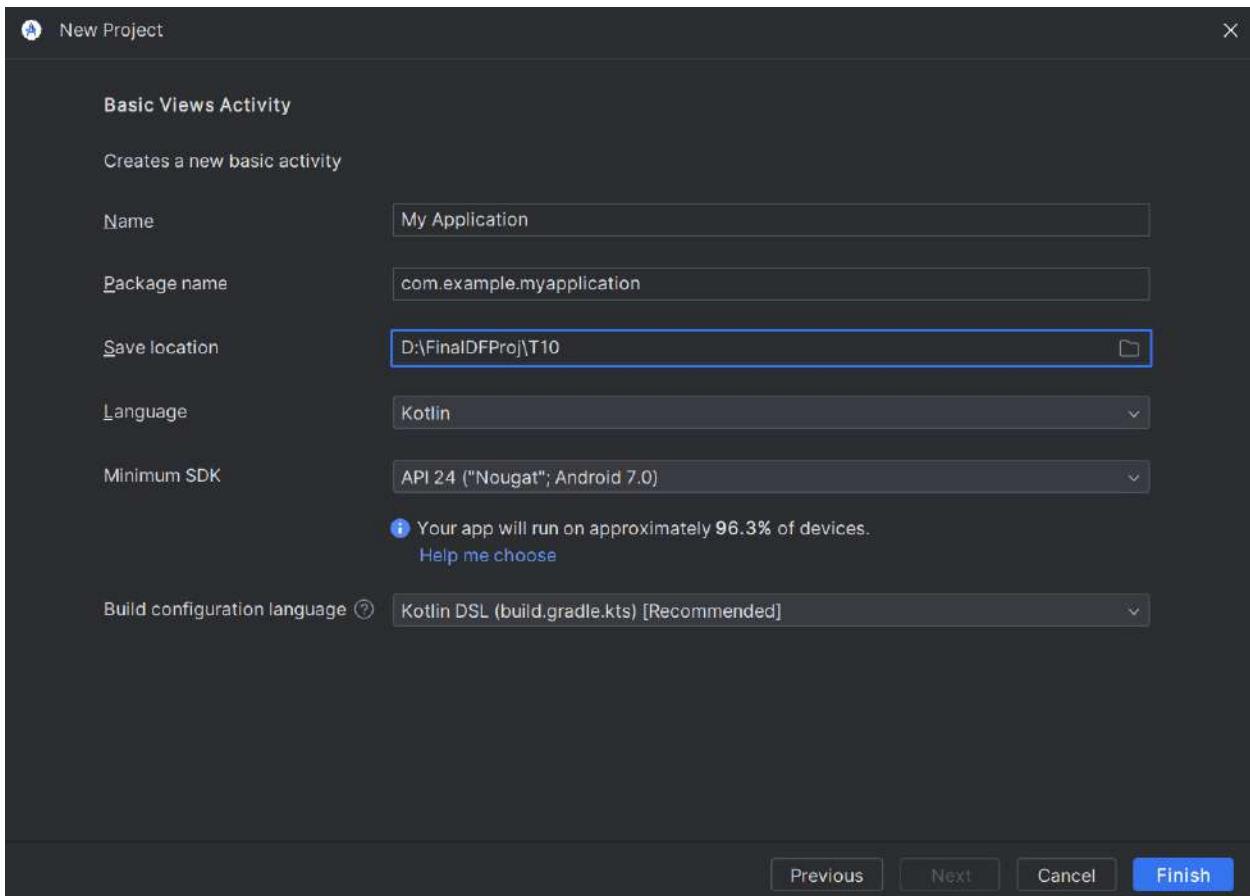
OPENING ANDROID STUDIO:



OPENING BASIC ACTIVITY VIEWS:



CREATING CASE:

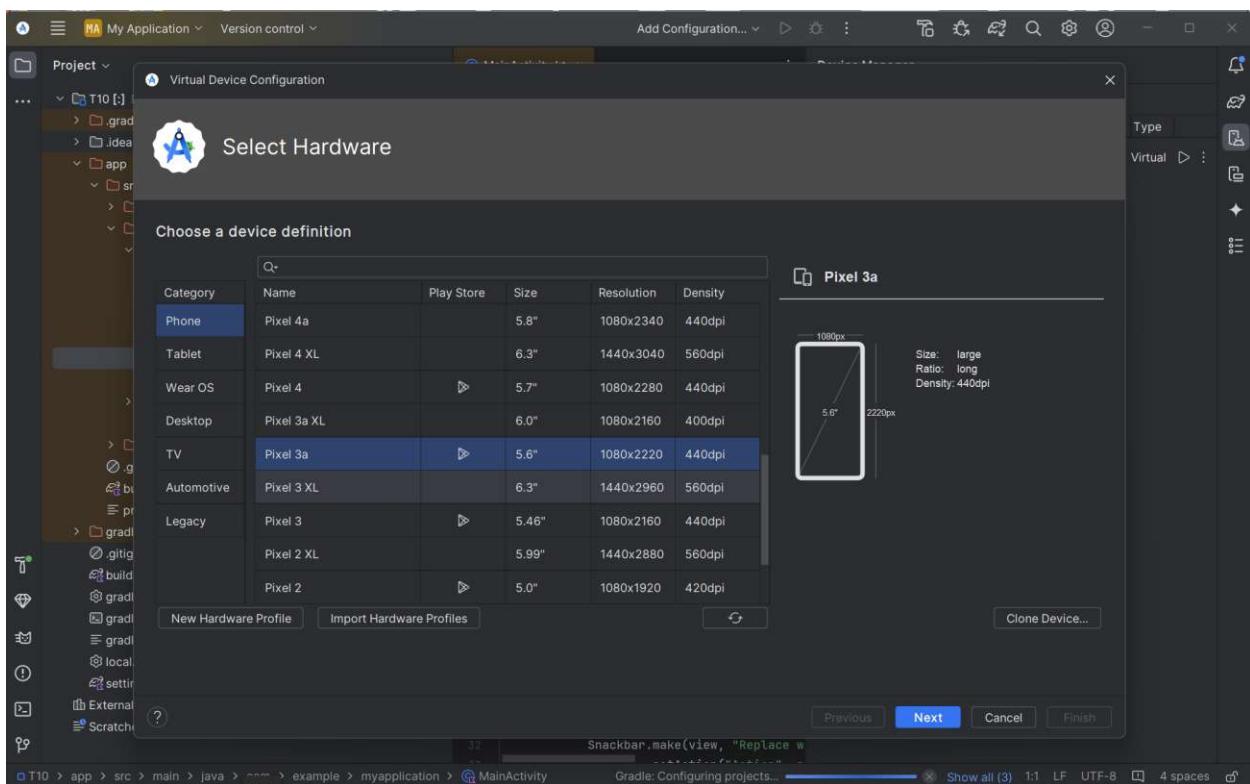


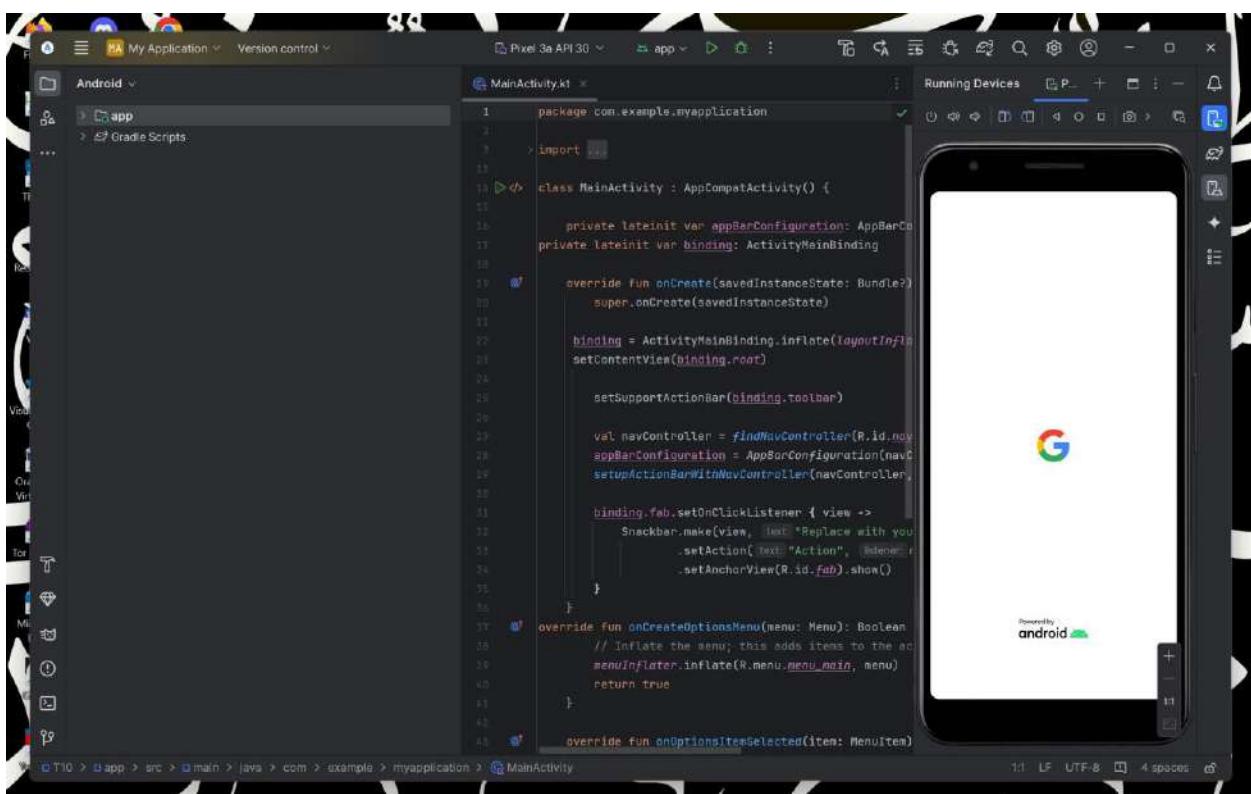
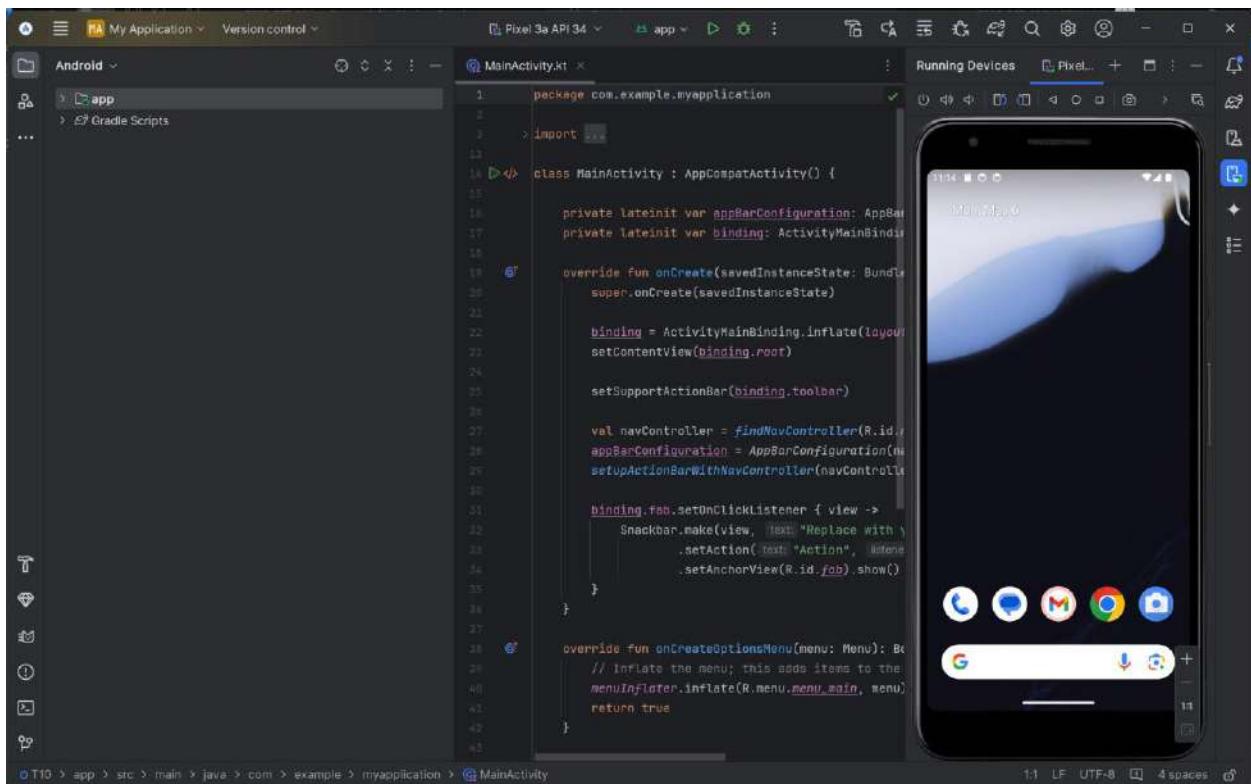
OPENING PHONE:

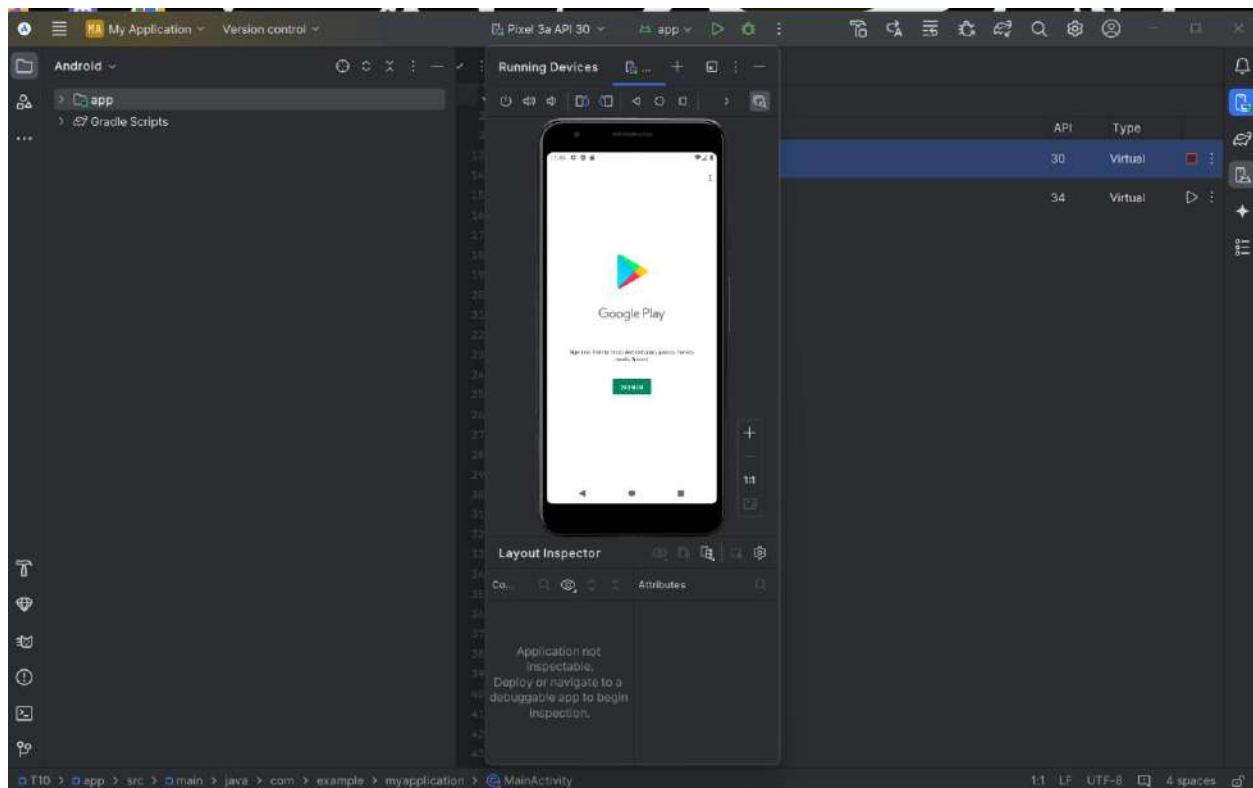
The screenshot shows the Android Studio interface. On the left is the Project Navigational Bar, which includes the gradle folder, idea folder, app folder (containing src, androidTest, main, and test), .gitignore, build.gradle.kts, gradle.properties, gradlew, gradlew.bat, local.properties, settings.gradle.kts, External Libraries, and Scratches and Consoles. The main area is the Device Manager, showing a Pixel 3a API 34 device. The code editor displays the MainActivity.kt file, which contains Java code for an AppCompatActivity. The status bar at the bottom indicates Gradle Building.

```

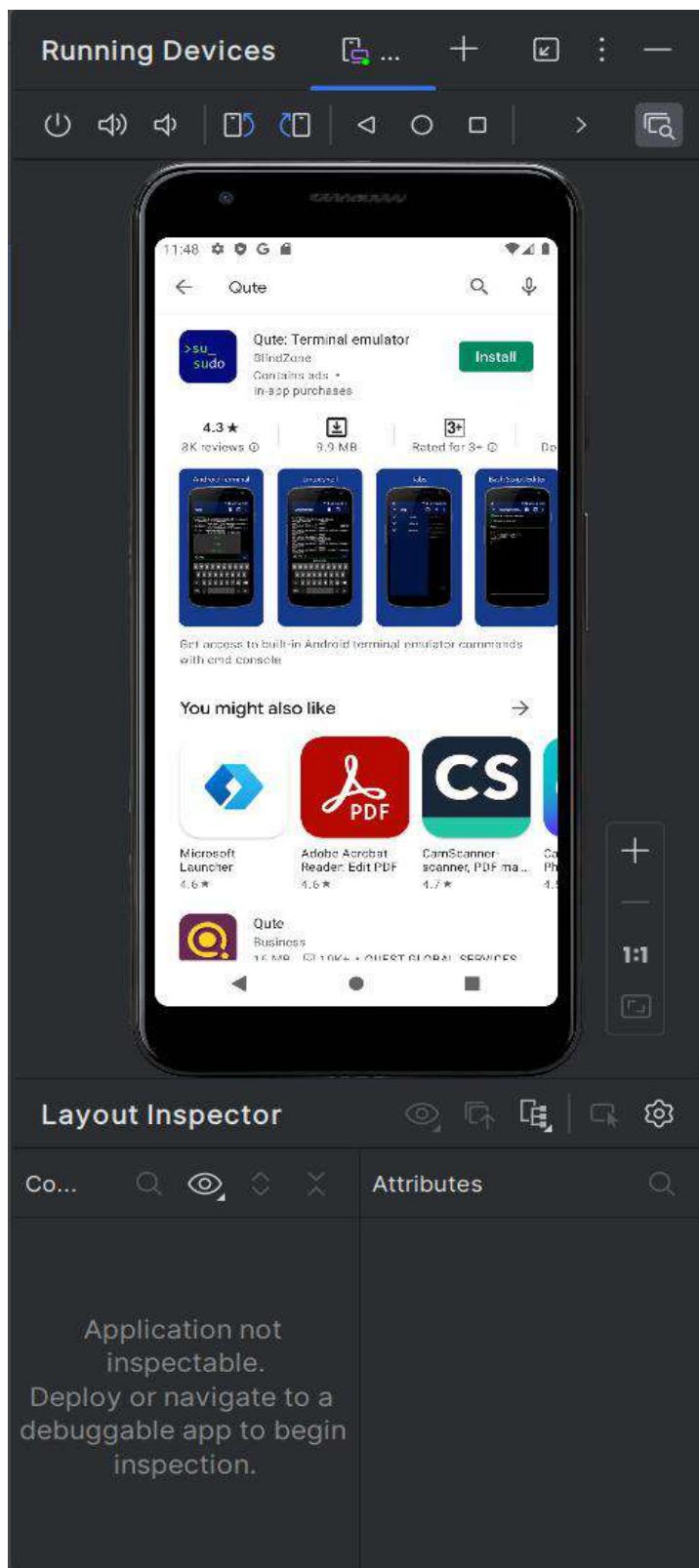
1 package com.example.myapplication
2 import android.os.Bundle
3 import com.google.android.material.snackbar.Snackbar
4 import androidx.appcompat.app.AppCompatActivity
5 import androidx.navigation.findNavController
6 import androidx.navigation.ui.AppBarConfiguration
7 import androidx.navigation.ui.navigateUp
8 import androidx.navigation.ui.setupActionBarWithNavController
9 import android.view.Menu
10 import android.view.MenuItem
11 import com.example.myapplication.databinding.ActivityMainBinding
12
13 class MainActivity : AppCompatActivity() {
14
15     private lateinit var appBarConfiguration: AppBarConfiguration
16     private lateinit var binding: ActivityMainBinding
17
18     override fun onCreate(savedInstanceState: Bundle?) {
19         super.onCreate(savedInstanceState)
20
21         binding = ActivityMainBinding.inflate(layoutInflater)
22         setContentView(binding.root)
23
24         setSupportActionBar(binding.toolbar)
25
26         val navController = findNavController()
27         appBarConfiguration = AppBarConfiguration(navController.graph)
28         setupActionBarWithNavController(navController, appBarConfiguration)
29
30         binding.fab.setOnClickListener { view ->
31             Snackbar.make(view, "Replace with your own action", Snackbar.LENGTH_LONG)
32             .show()
33     }
34 }
35
36 
```



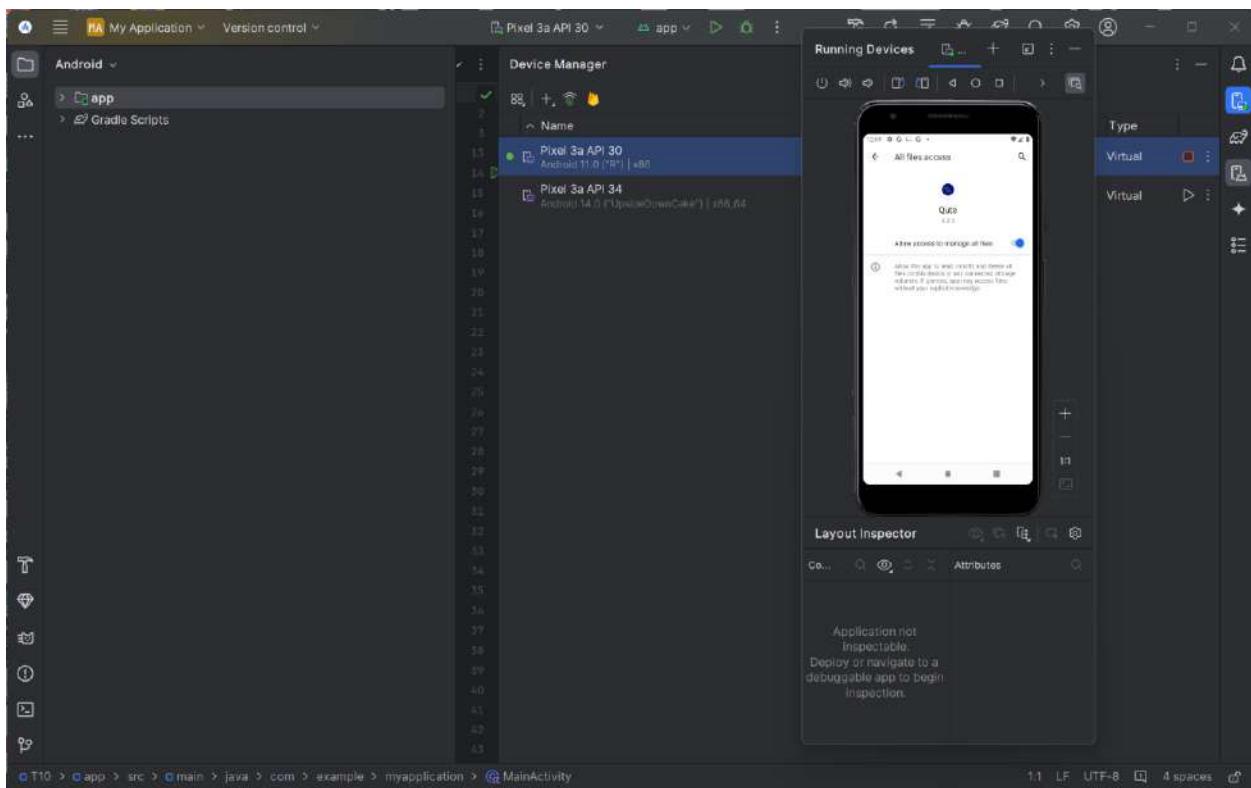




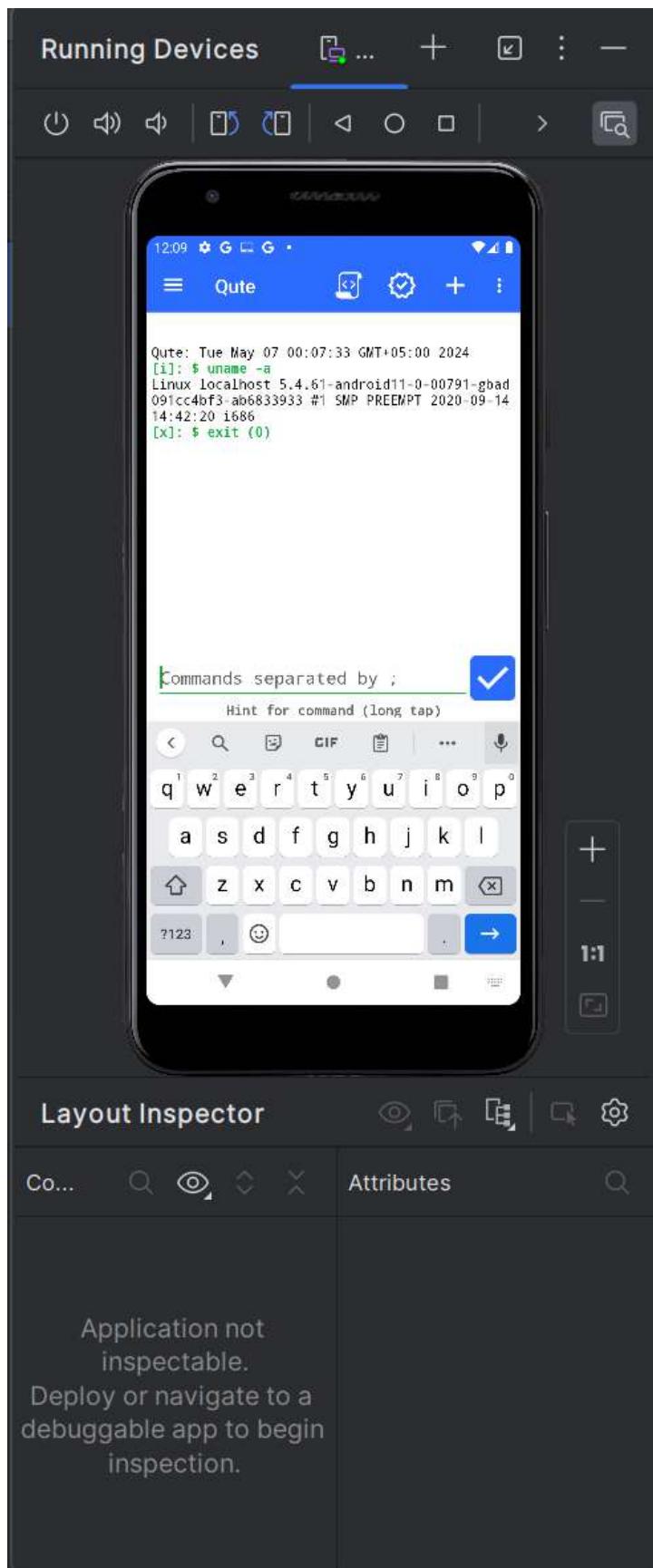
DOWNLOADING QUTE EMULATOR APP:



GRANTING ALL FILE ACCESS



RUNNING COMMAND:



11. Rooting Android Studio's Emulator AND 14

STARTING ADB:

```

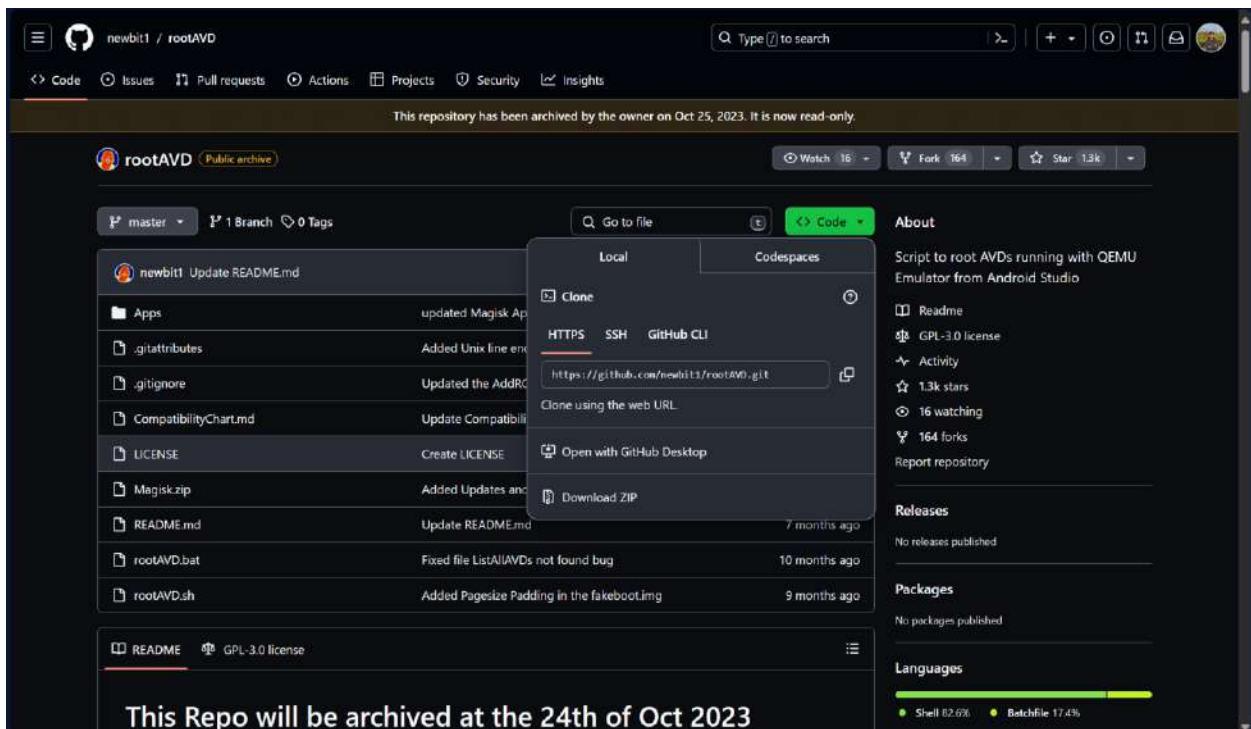
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

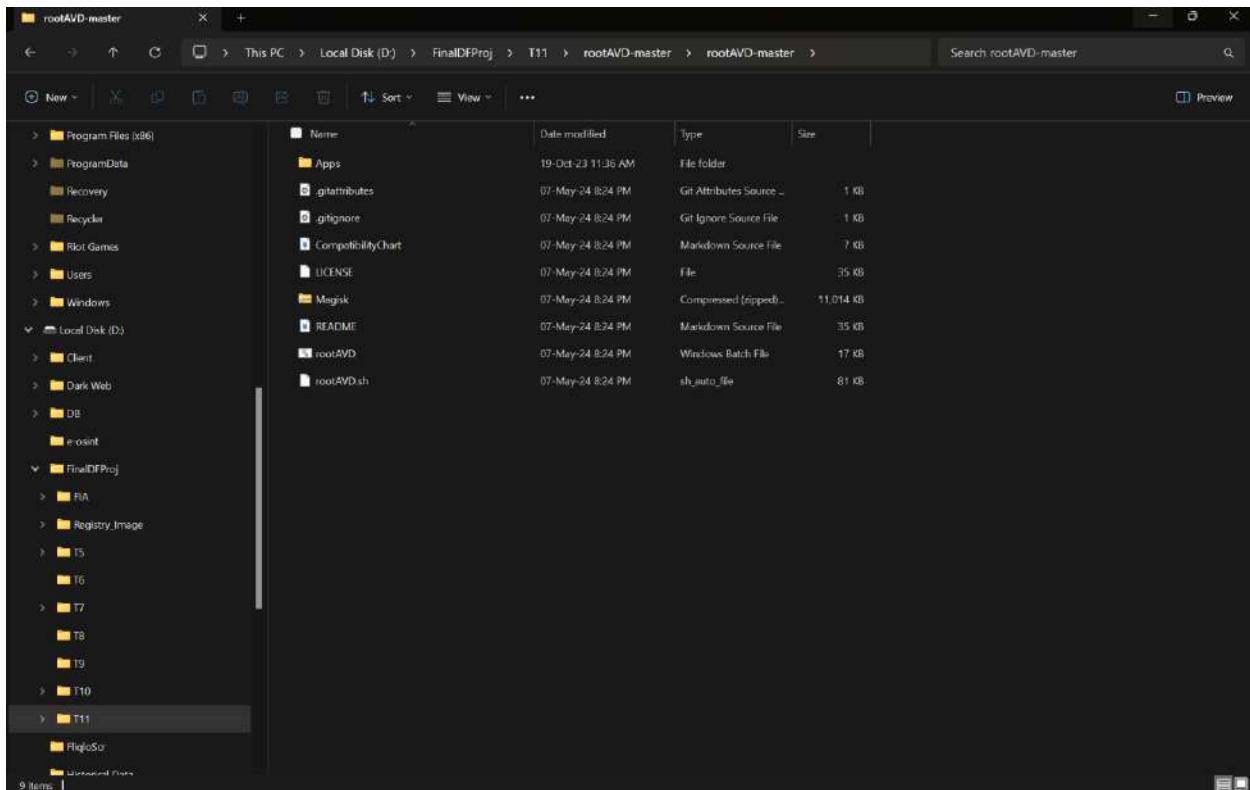
C:\Users\user>adb devices
List of devices attached
emulator-5554    device

C:\Users\user>adb shell
generic_x86_arm:/ $ ps
USER      PID  PPID   VSZ   RSS WCHAN          ADDR S NAME
shell     3916  1809 12916 2936 __ia32_co+        0 S sh
shell     3921  3916 12584 3492 0                 0 R ps
generic_x86_arm:/ $ |

```

DOWNLOADING rootAVD FOR ROOTING:





rootAVD COMMAND:

```
C:\Windows\System32\cmd.exe + ~

C:\Users\user\Downloads\rootAVD-master>rootAVD.bat ListAllAVDs
rootAVD A Script to root AVD by NewBit XDA

Usage: rootAVD [DIR/ramdisk.img] [OPTIONS] | [EXTRA ARGUMENTS]
or:      rootAVD [ARGUMENTS]

Arguments:
  ListAllAVDs          Lists Command Examples for ALL installed AVDs
  InstallApps          Just install all APKs placed in the Apps folder

Main operation mode:
  DIR                  a path to an AVD system-image
                       - must always be the 1st Argument after rootAVD

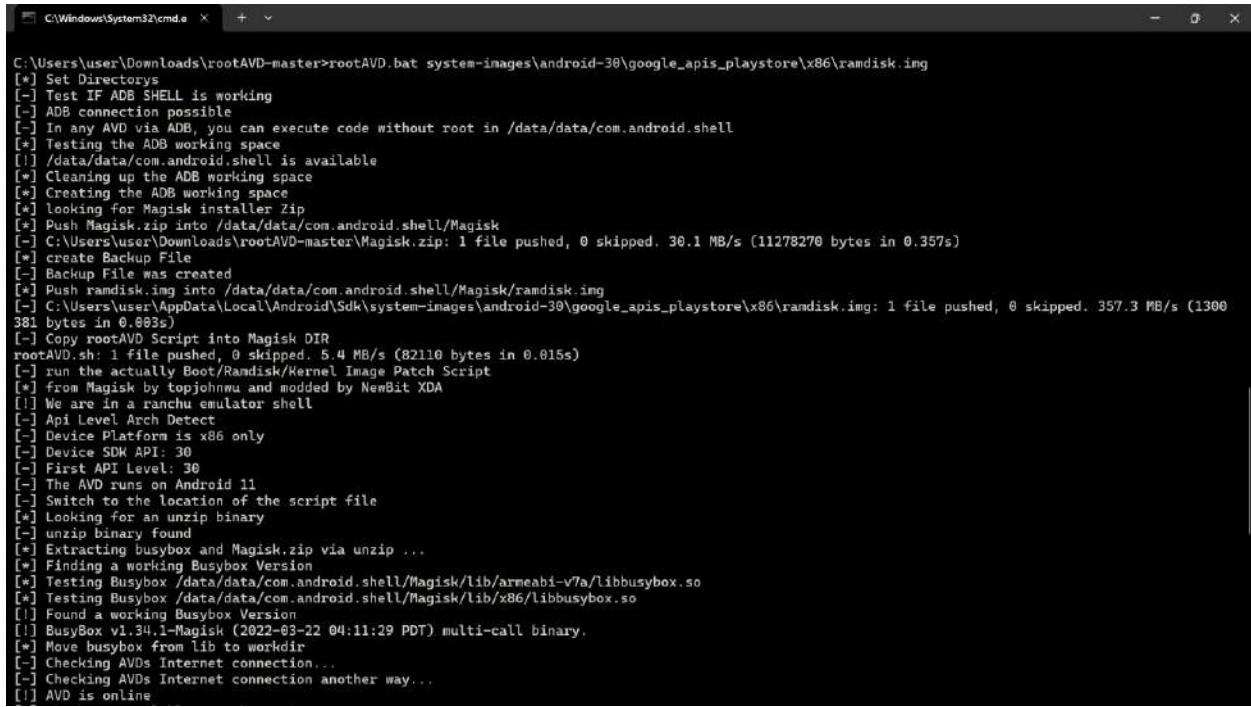
ADB Path | Ramdisk DIR| ANDROID_HOME:
  [M]ac/Darwin:        export PATH=~/.Library/Android/sdk/platform-tools:$PATH
                       export PATH=$ANDROID_HOME/platform-tools:$PATH
                       system-images/Android-$API/google_apis_playstore/x86_64/
  [L]inux:             export PATH=~/.Android/Sdk/platform-tools:$PATH
                       export PATH=$ANDROID_HOME/platform-tools:$PATH
                       system-images/android-$API/google_apis_playstore/x86_64/
  [W]indows:           set PATH=%LOCALAPPDATA%\Android\Sdk\platform-tools;%PATH%
                       system-images\android-$API\google_apis_playstore\x86_64\
  ANDROID_HOME:        By default, the script uses %LOCALAPPDATA%, to set its Android Home
                       directory, search for AVD system-images and ADB binaries. This behaviour
                       can be overwritten by setting the ANDROID_HOME variable.
                       e.g. set ANDROID_HOME=%USERPROFILE%\Downloads\sdk
  $API:                25,29,30,31,32,33,34,UpsideDownCake,etc.

Options:
  restore              restore all existing .backup files, but doesn't delete them
                       - the AVD doesn't need to be running
                       - no other Argument after will be processed

  InstallKernelModules    install custom build kernel and its modules into ramdisk.img
                       - kernel (bzImage) and its modules (initramfs.img) are inside rootAVD
                       - both files will be deleted after installation

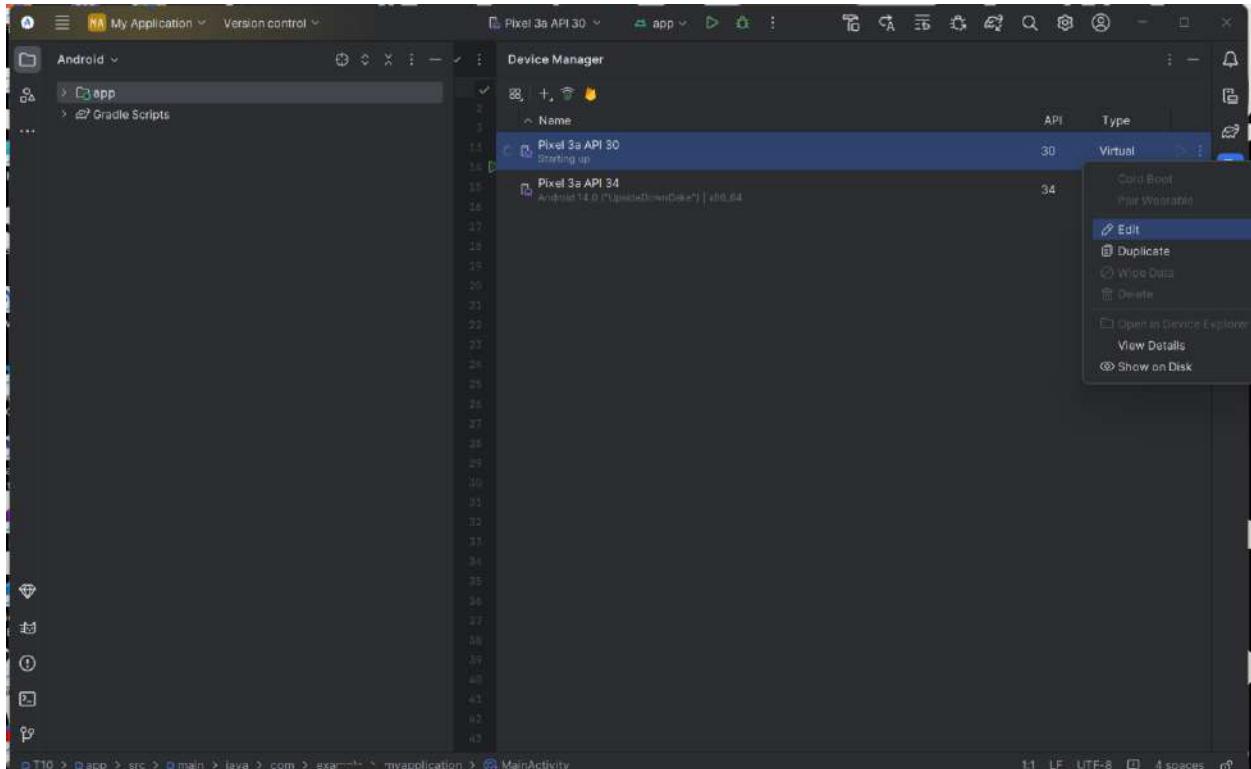
  InstallPrebuiltKernelModules download and install an AOSP prebuilt kernel and its modules into ramdisk.img
                       - similar to InstallKernelModules, but the AVD needs to be online
```

ACQUIRING RAMDISK IMAGE OF DEVICE:

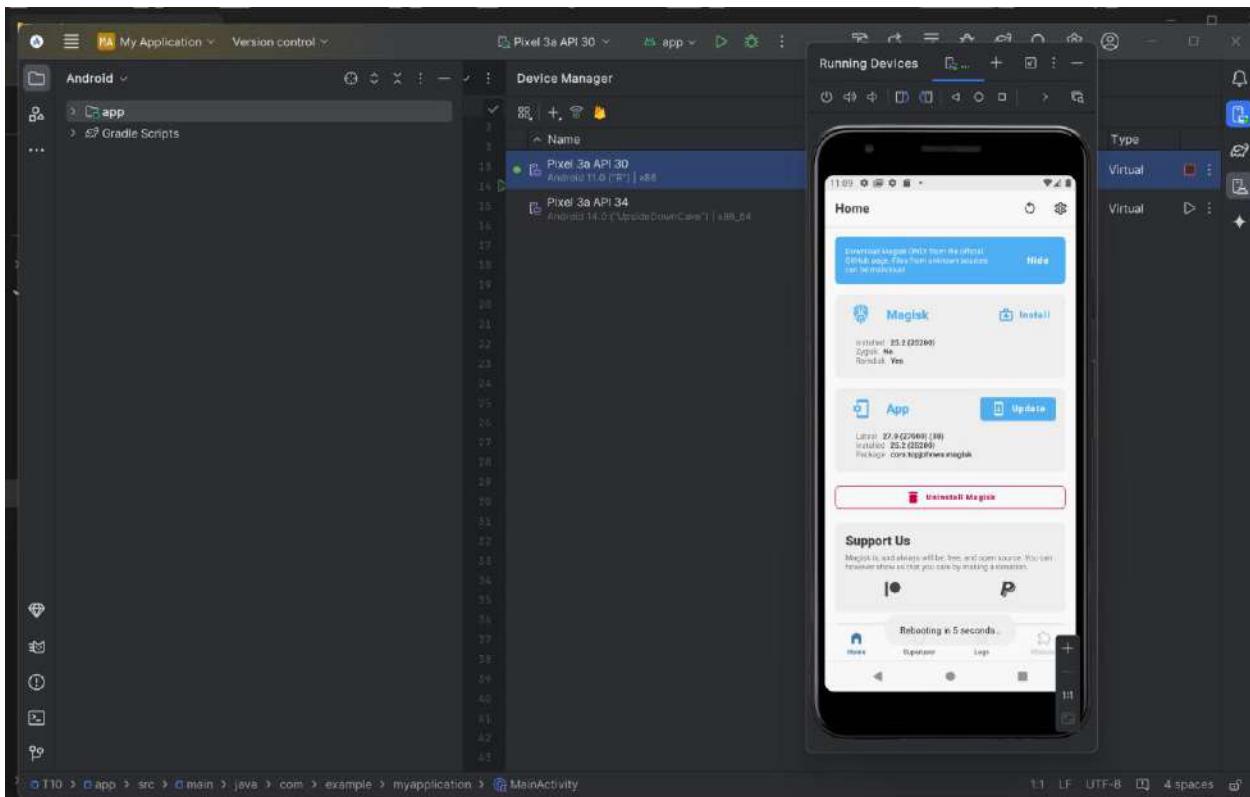


```
C:\Users\user\Downloads\rootAVD-master>rootAVD.bat system=images\android-30\google_apis_playstore\x86\ramdisk.img
[*] Set Directory
[-] Test IF ADB SHELL is working
[-] ADB connection possible
[-] In any ADB via ADB, you can execute code without root in /data/data/com.android.shell
[*] Testing the ADB working space
[]/data/data/com.android.shell is available
[*] Cleaning up the ADB working space
[*] Creating the ADB working space
[*] Looking for Magisk installer Zip
[*] Push Magisk.zip into /data/data/com.android.shell/Magisk
[-] C:\Users\user\Downloads\rootAVD-master\Magisk.zip: 1 file pushed, 0 skipped. 30.1 MB/s (11278270 bytes in 0.359s)
[*] create Backup File
[-] Backup File was created
[*] Push ramdisk.Img into /data/data/com.android.shell/Magisk/ramdisk.img
[-] C:\Users\user\AppData\Local\Android\Sdk\system-images\android-30\google_apis_playstore\x86\ramdisk.img: 1 file pushed, 0 skipped. 357.3 MB/s (1300381 bytes in 0.083s)
[-] Copy rootAVD Script into Magisk DIR
rootAVD.sh: 1 file pushed, 0 skipped. 5.4 MB/s (82110 bytes in 0.015s)
[-] run the actually Boot/Ramdisk/Kernel Image Patch Script
[*] from Magisk by topjohnwu and modded by NewBit XDA
[] We are in a ranchu emulator shell
[-] Api Level Arch Detect
[-] Device Platform is x86 only
[-] Device SDK API: 30
[-] First API Level: 30
[-] The AVD runs on Android 11
[-] Switch to the location of the script file
[*] Looking for an unzip binary
[-] unzip binary found
[*] Extracting busybox and Magisk.zip via unzip ...
[*] Finding a working Busybox Version
[*] Testing Busybox /data/data/com.android.shell/Magisk/lib/armeabi-v7a/libbusybox.so
[*] Testing Busybox /data/data/com.android.shell/Magisk/lib/x86/libbusybox.so
[] Found a working Busybox Version
[] BusyBox v1.34.1-Magisk (2022-03-22 04:11:29 PDT) multi-call binary.
[*] Move busybox from lib to workdir
[-] Checking AVDs Internet connection...
[-] Checking AVDs Internet connection another way...
[] AVD is online
```

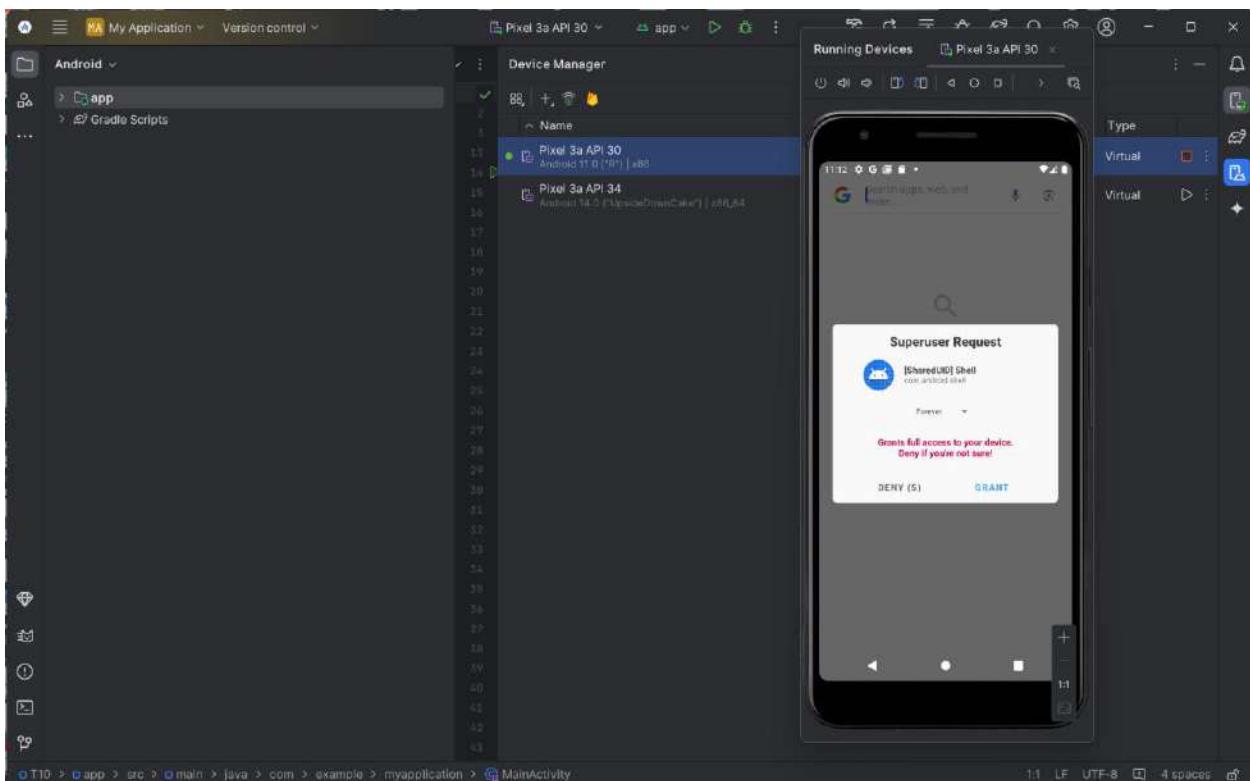
COLD BOOTING OF DEVICE:



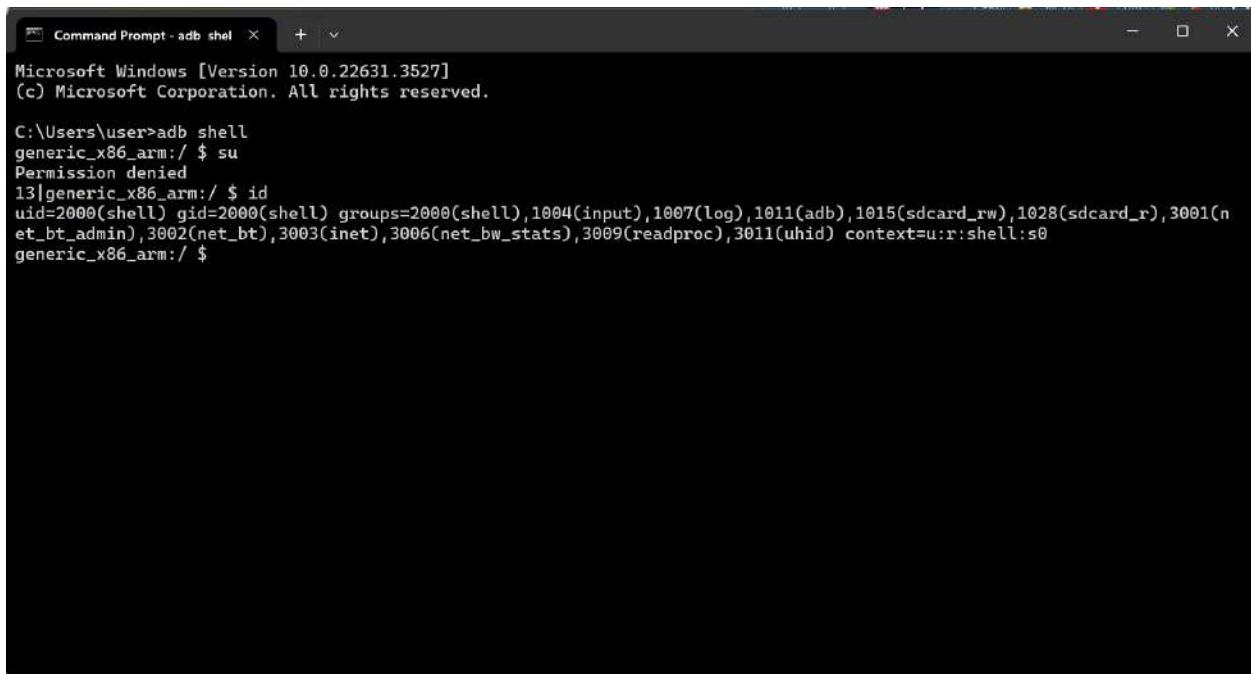
MAGISK SOFTWARE:



SHELL ACCESS GRANT:



FLAG(SHELL):



```
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>adb shell
generic_x86_arm:/ $ su
Permission denied
13|generic_x86_arm:/ $ id
uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(n
et_bt_admin),3002(net_bt),3003/inet),3006/net_bw_stats),3009(readproc),3011(uhid) context=u:r:shell:s0
generic_x86_arm:/ $
```

12. Forensic Acquisition from Android

NCAT STARTING AUTH TOKEN:

The image contains two screenshots of a Windows Command Prompt window titled "Command Prompt - ncirc 127.0.0.1".

The top screenshot shows the initial setup of the ncirc listener command:

```
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

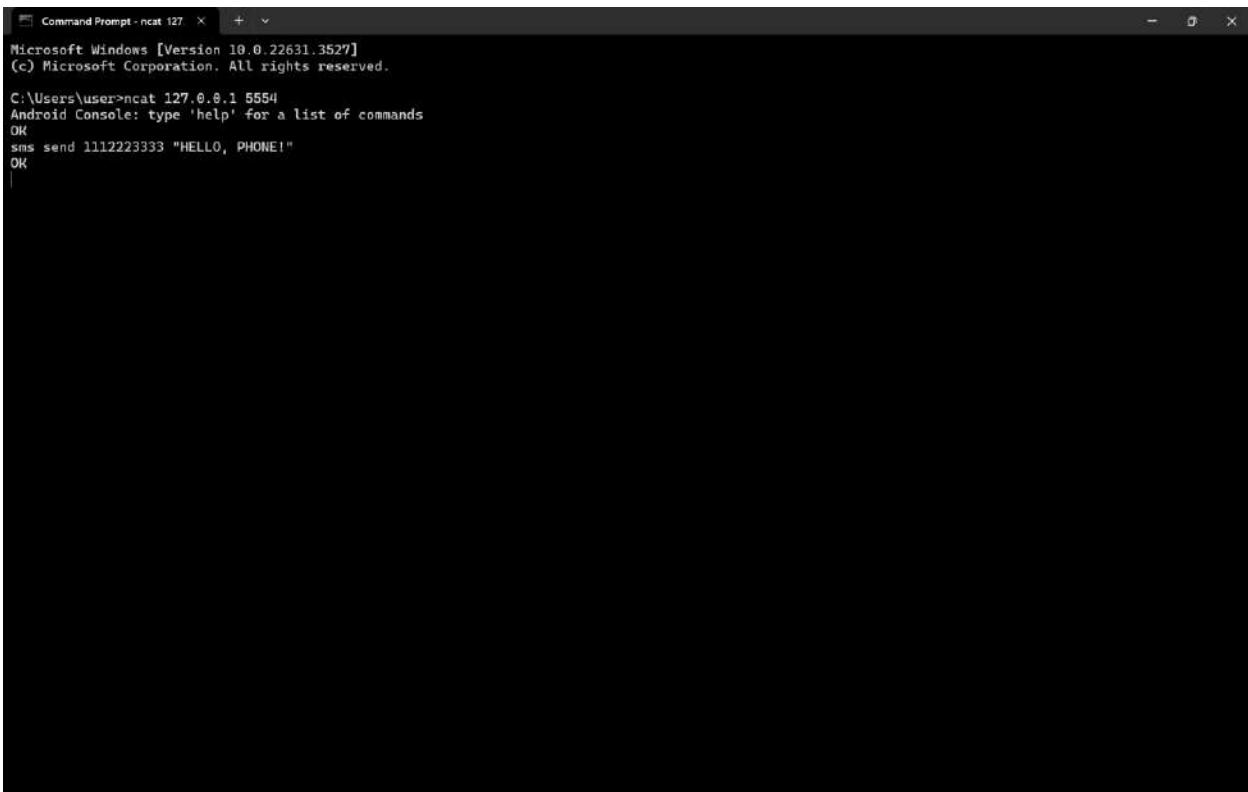
C:\Users\user>ncirc 127.0.0.1 5554
```

The bottom screenshot shows the ncirc listener receiving a connection and prompting for an authentication token:

```
Android Console: Authentication required
Android Console: type 'auth <auth_token>' to authenticate
Android Console: you can find your <auth_token> in
'C:\Users\user\.emulator_console_auth_token'
OK
```

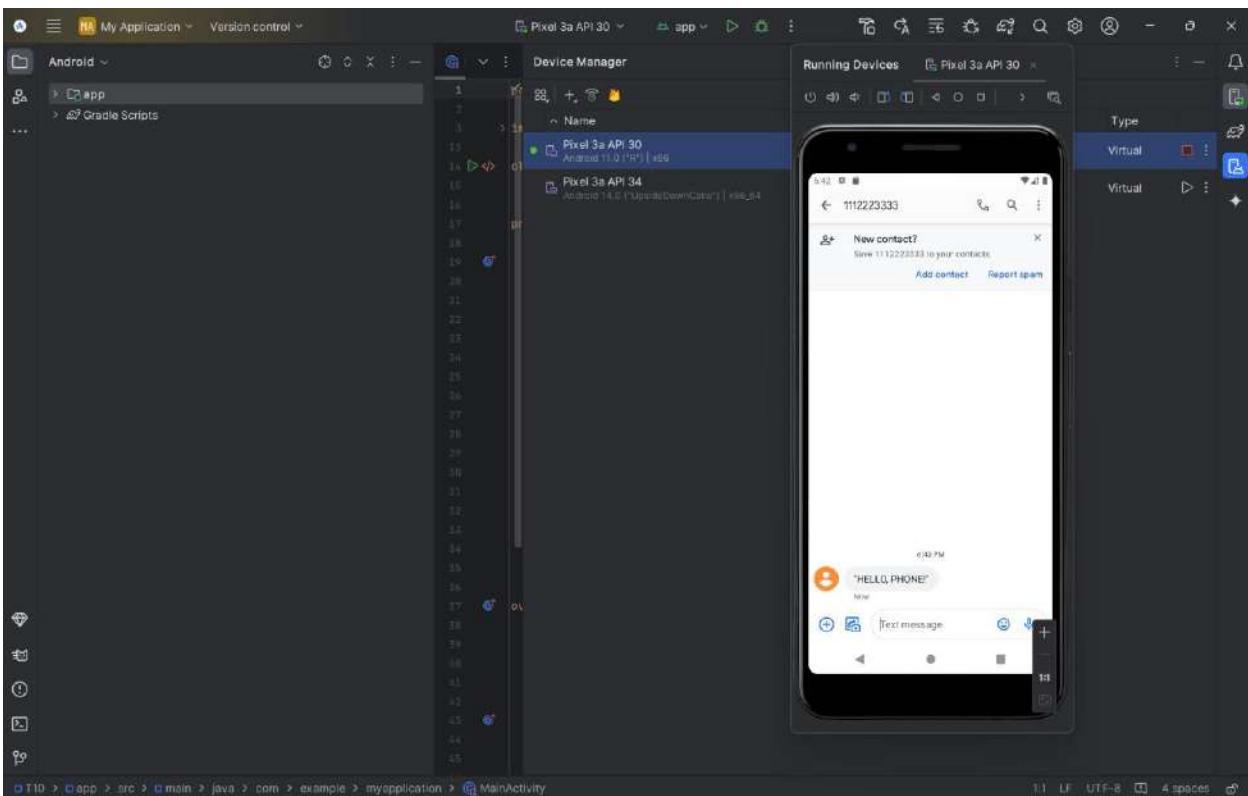
Below the screenshots, the command prompt shows the path ".emulator_console_auth_token" and the token value "kwfv9mmnFU/uUoev" entered.

SENDING MESSAGE TO PHONE:

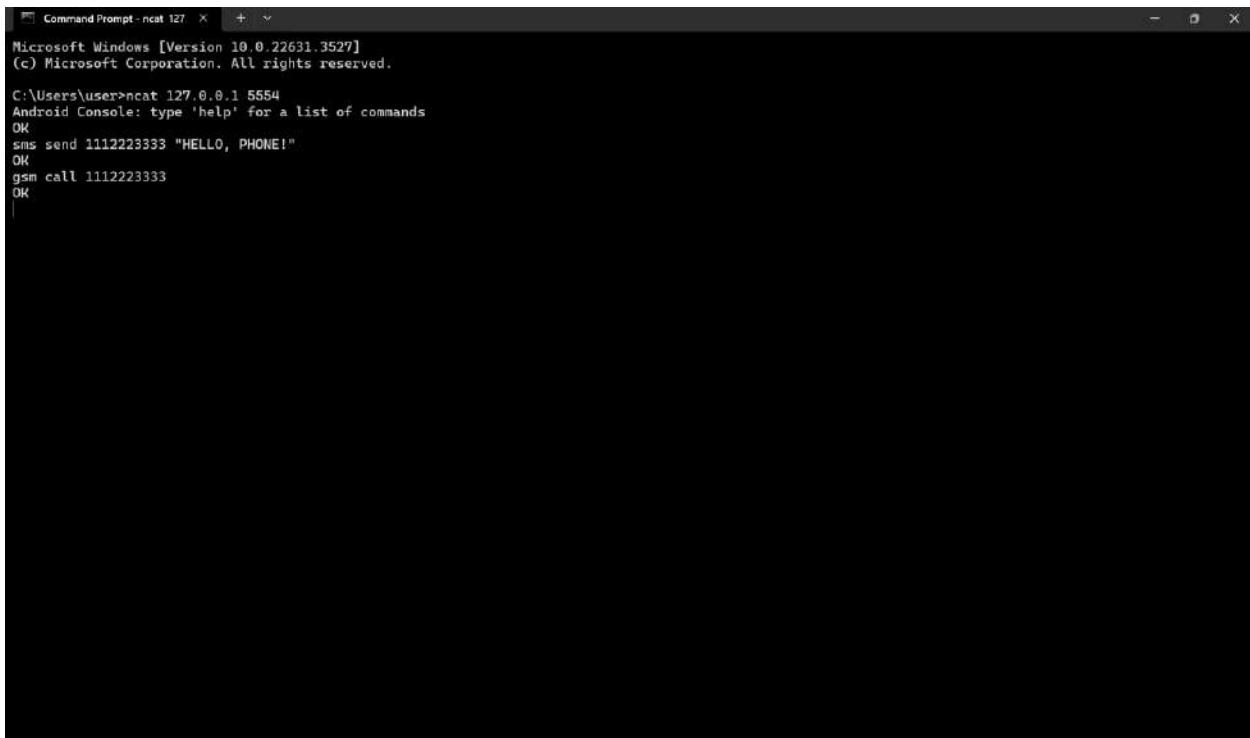


```
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ncat 127.0.0.1 5554
Android Console: type 'help' for a list of commands
OK
sms send 1112223333 "HELLO, PHONE!"
OK
```

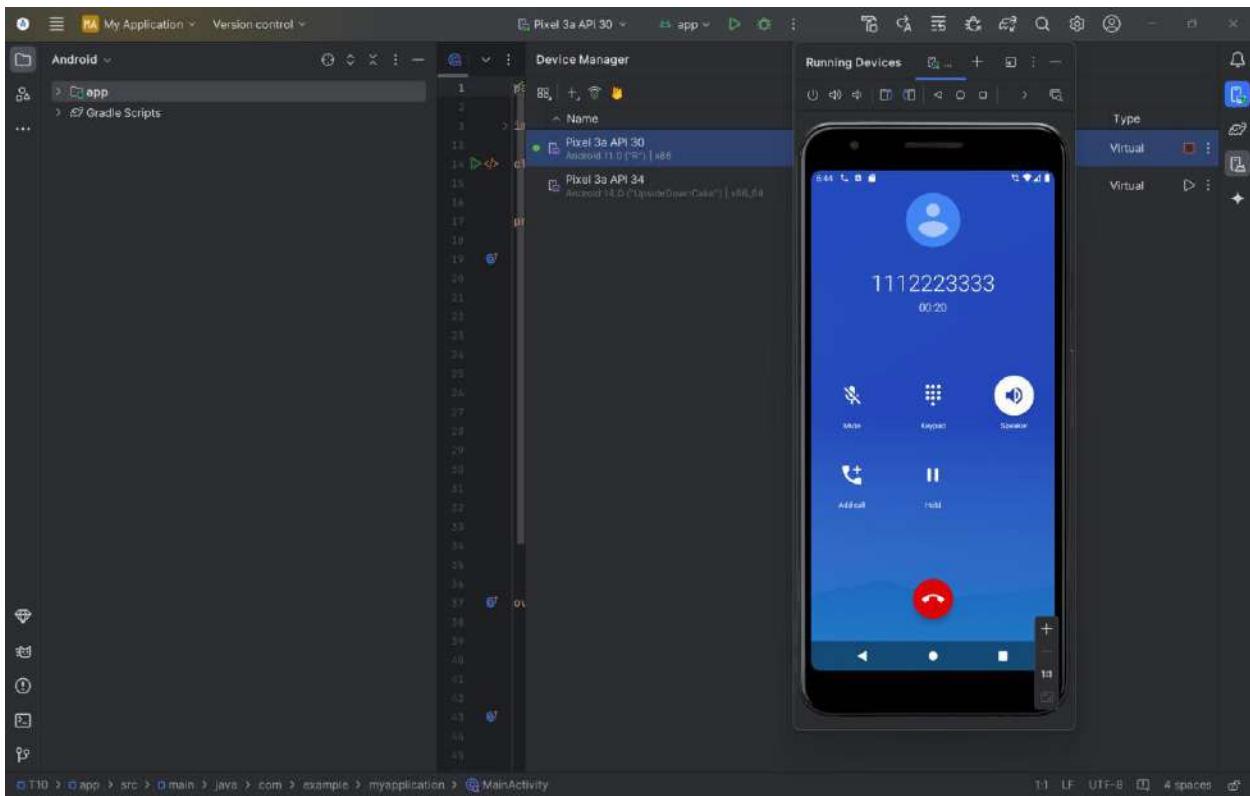


CALLING PHONE:

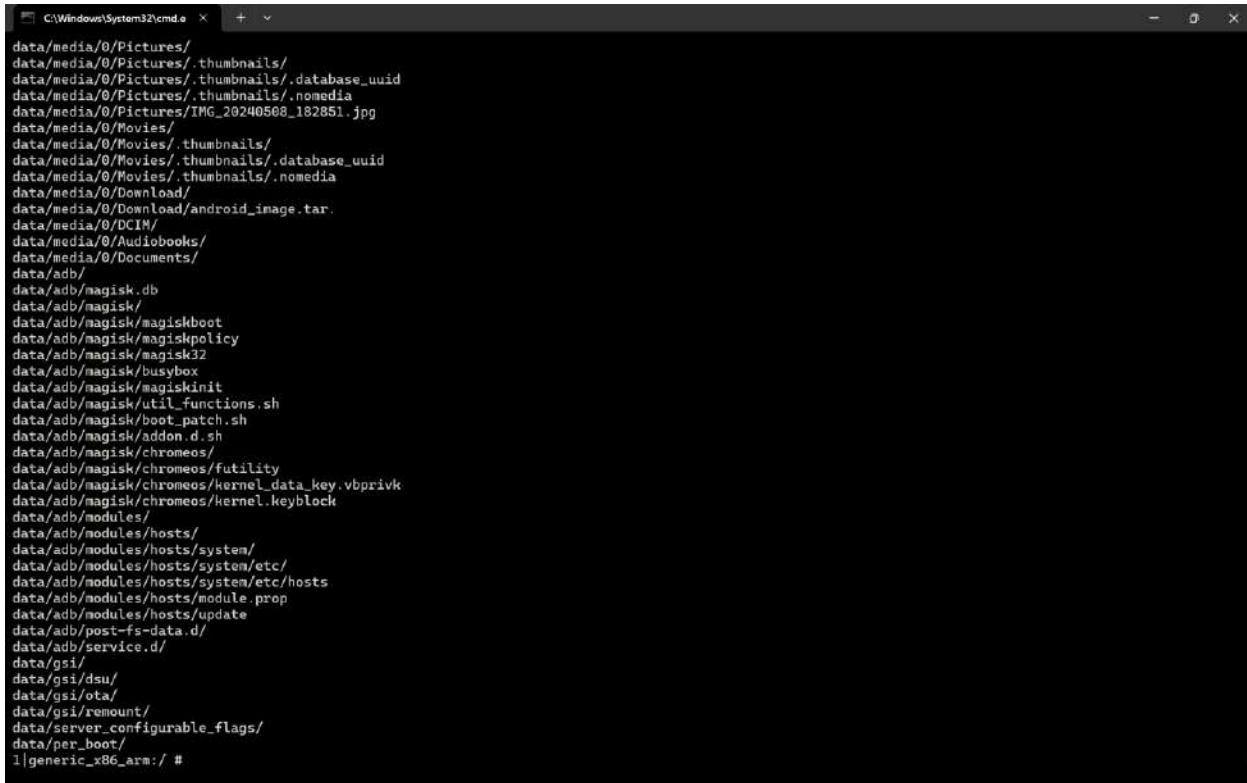


```
Command Prompt - ncat 127.0.0.1 5554
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

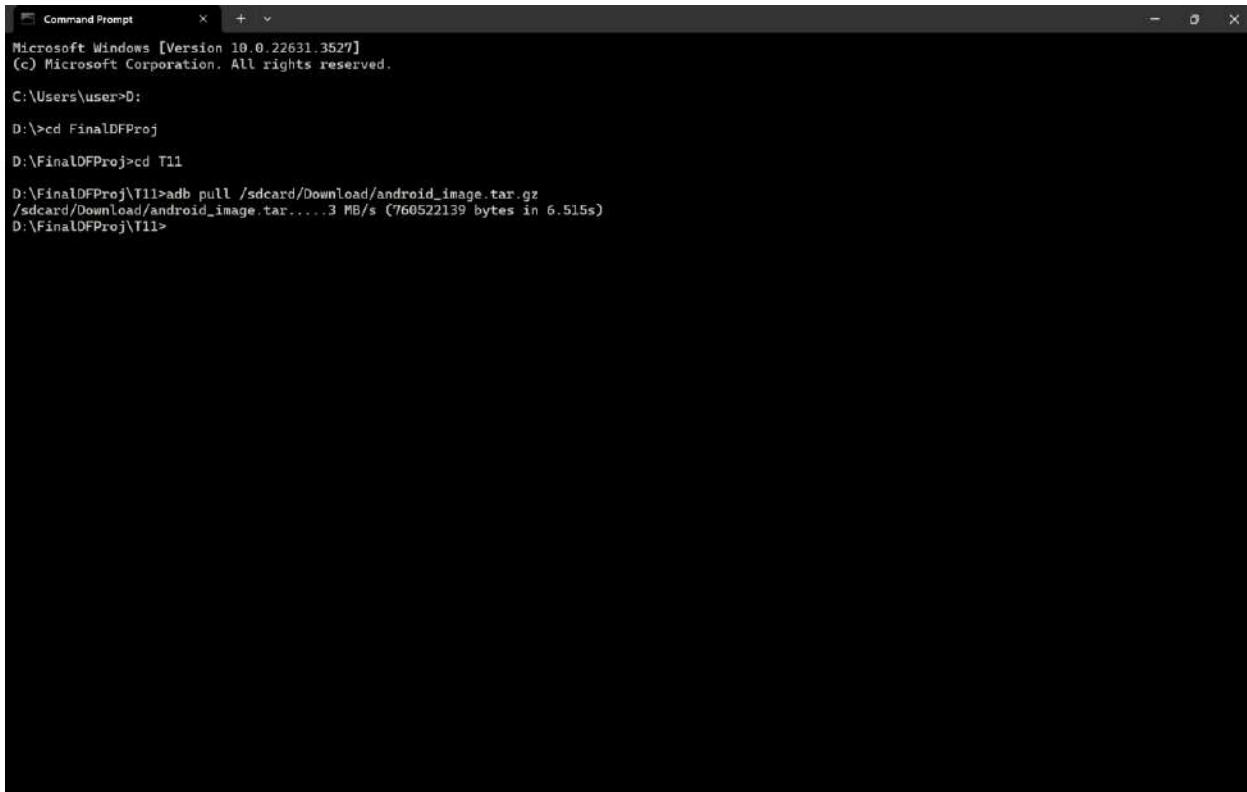
C:\Users\user>ncat 127.0.0.1 5554
Android Console: type 'help' for a list of commands
OK
sms send 1112223333 "HELLO, PHONE!"
OK
gsm call 1112223333
OK
```



ACQUIRING IMAGE:



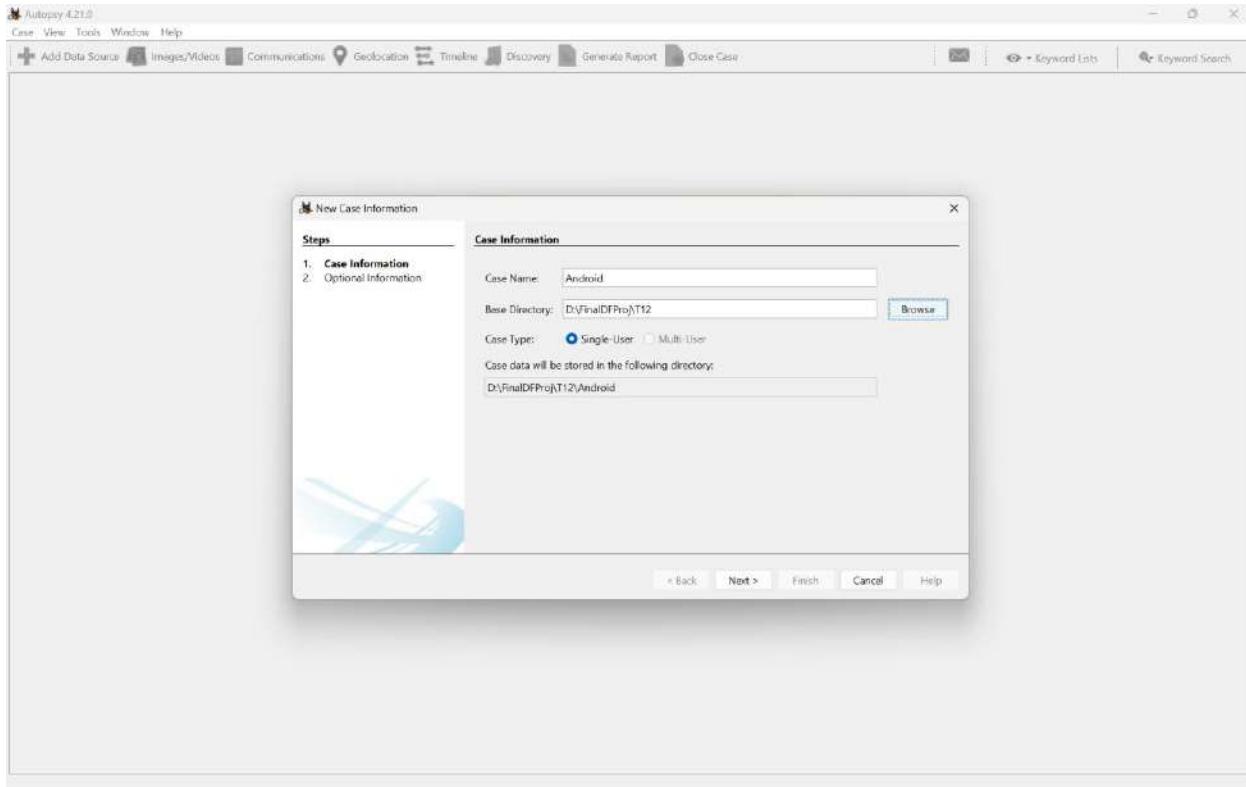
```
C:\Windows\System32\cmd.exe + ~
data/media/0/Pictures/
data/media/0/Pictures/.thumbnails/
data/media/0/Pictures/.thumbnails/.database_uuid
data/media/0/Pictures/.thumbnails/.nomedia
data/media/0/Pictures/IMG_20240508_182851.jpg
data/media/0/Movies/
data/media/0/Movies/.thumbnails/
data/media/0/Movies/.thumbnails/.database_uuid
data/media/0/Movies/.thumbnails/.nomedia
data/media/0/Download/
data/media/0/Download/android_image.tar.
data/media/0/DCIM/
data/media/0/Audiobooks/
data/media/0/Documents/
data/adb/
data/adb/magisk.db
data/adb/magisk/
data/adb/magisk/magiskboot
data/adb/magisk/magiskpolicy
data/adb/magisk/magisk32
data/adb/magisk/busybox
data/adb/magisk/magiskinit
data/adb/magisk/util_functions.sh
data/adb/magisk/boot_patch.sh
data/adb/magisk/addon.d.sh
data/adb/magisk/chromeos/
data/adb/magisk/chromeos/futility
data/adb/magisk/chromeos/kernel_data_key.vbprivk
data/adb/magisk/chromeos/kernel.keyblock
data/adb/modules/
data/adb/modules/hosts/
data/adb/modules/hosts/system/
data/adb/modules/hosts/system/etc/
data/adb/modules/hosts/system/etc/hosts
data/adb/modules/hosts/module.prop
data/adb/modules/hosts/update
data/adb/post-fs-data.d/
data/adb/service.d/
data/gsi/
data/gsi/dsu/
data/gsi/ota/
data/gsi/remount/
data/server_configurable_flags/
data/per_boot/
l|generic_x86_arm:/ #
```



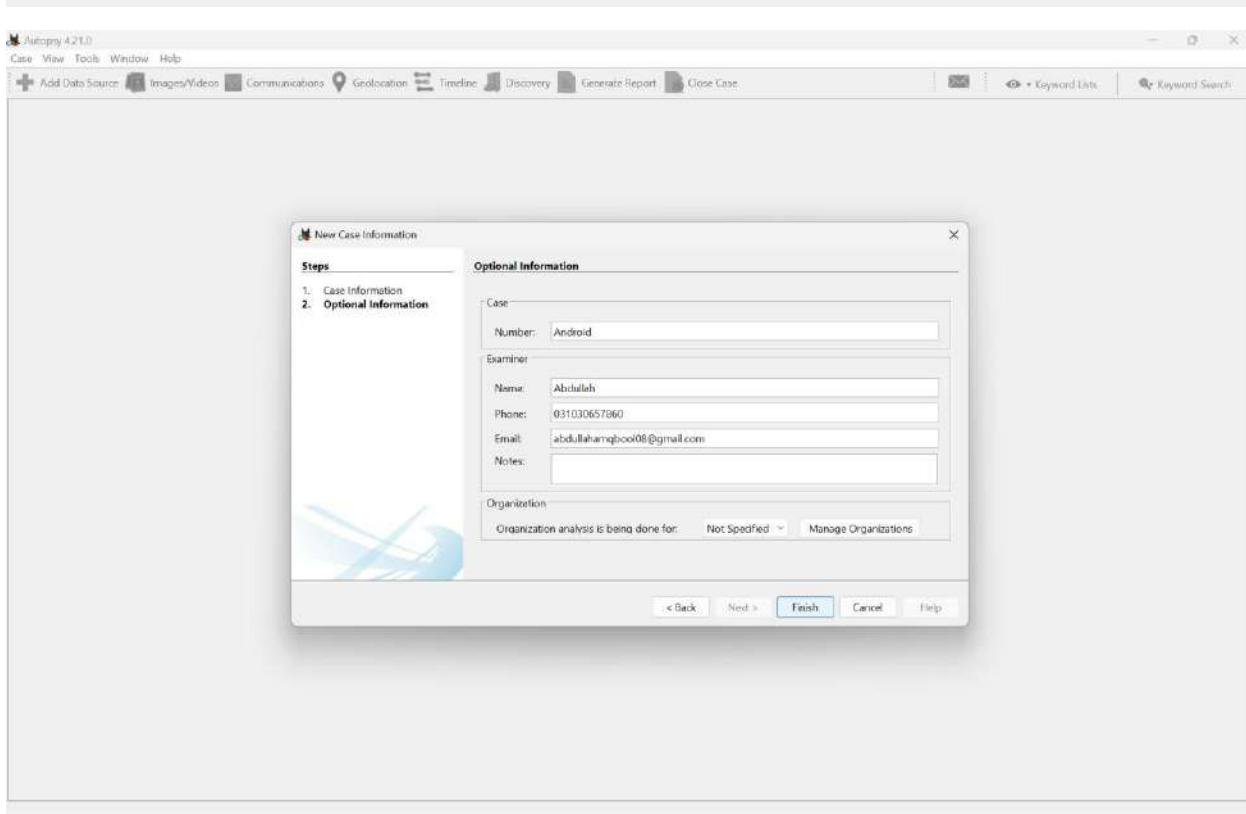
```
Command Prompt + ~
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>D:
D:\>cd FinalDFProj
D:\FinalDFProj>cd T11
D:\FinalDFProj\T11>adb pull /sdcard/Download/android_image.tar.gz
/sdcard/Download/android_image.tar....3 MB/s (760522139 bytes in 6.515s)
D:\FinalDFProj\T11>
```

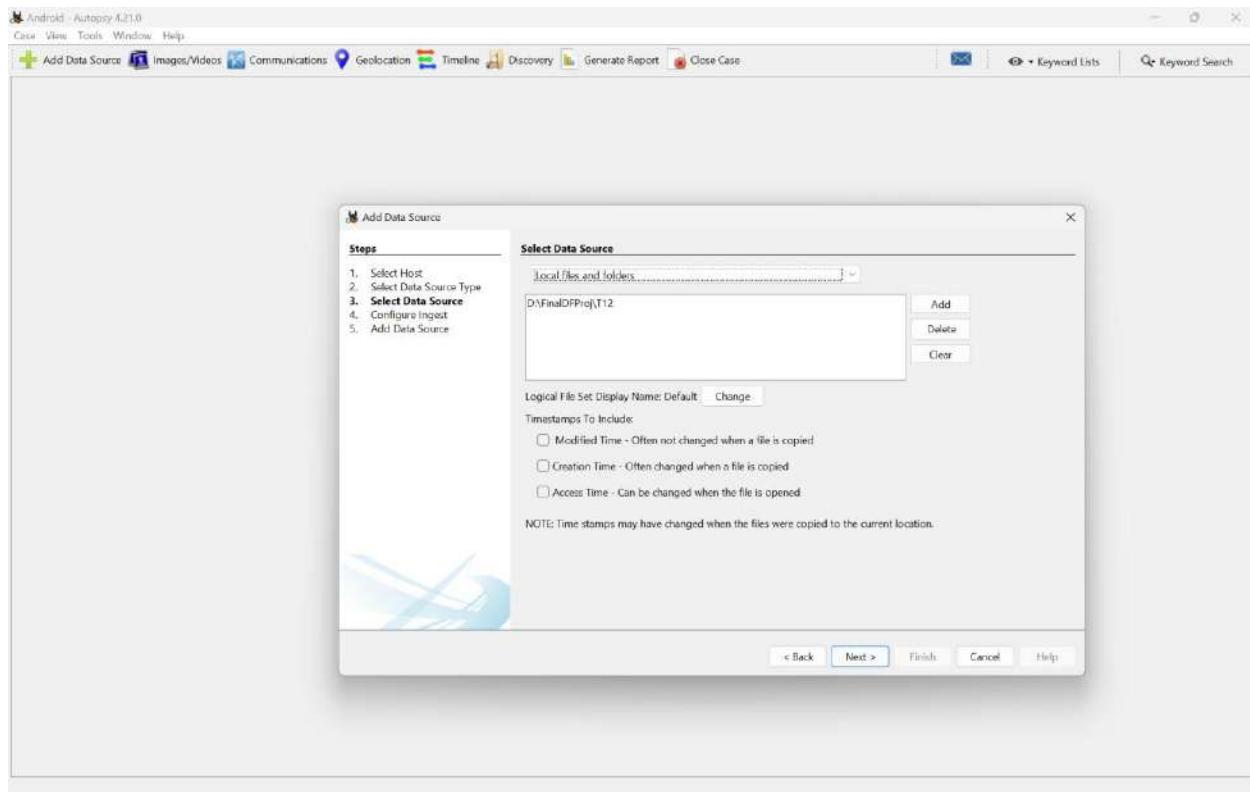
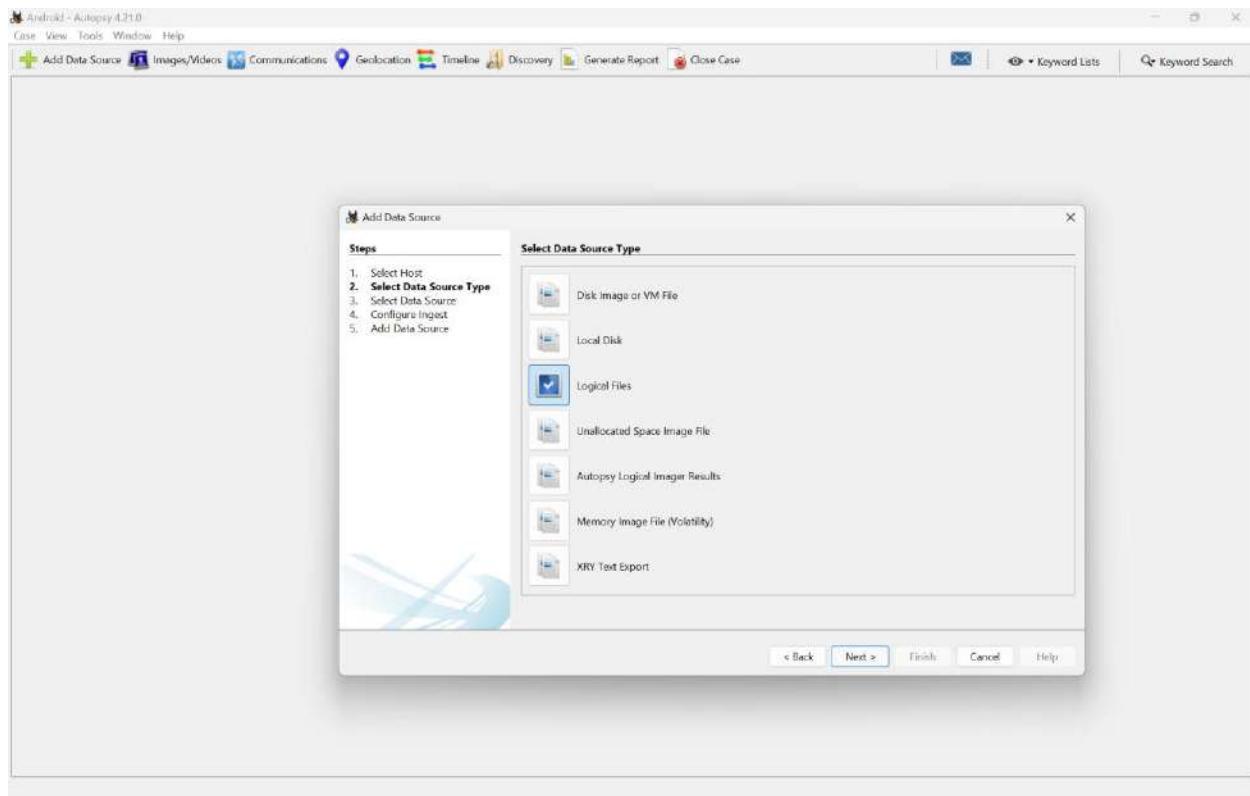
RUNNING AUTOPSY:



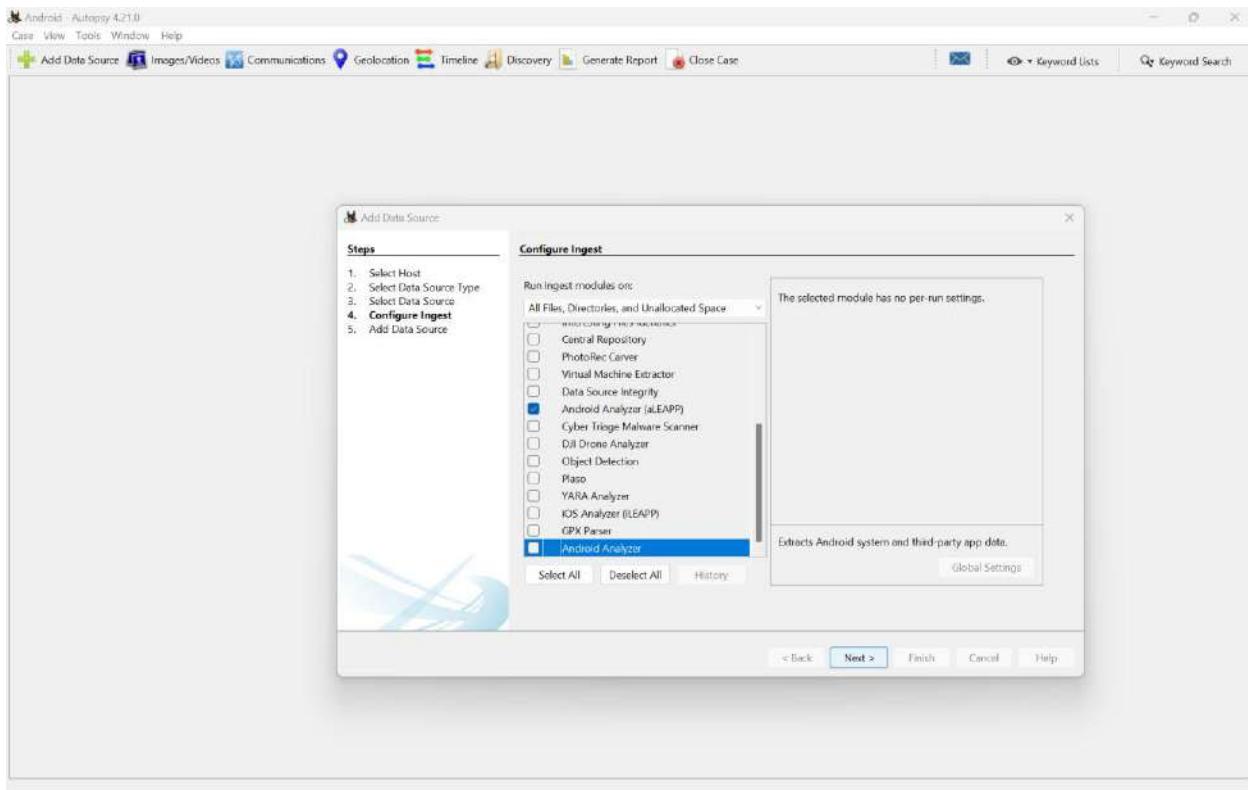
The screenshot shows the Autopsy 4.21.0 interface with the 'New Case Information' dialog box open. The dialog has two tabs: 'Case Information' and 'Optional Information'. The 'Case Information' tab is selected, showing fields for 'Case Name' (Android), 'Base Directory' (D:\FinalDFPro\T12), and 'Case Type' (Single-User). The 'Optional Information' tab is shown below, containing fields for 'Case Number' (Android), 'Examiner' (Name: Abdullah, Phone: 031030657960, Email: abdullahamqbo08@gmail.com), and 'Notes'. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.



The screenshot shows the 'Optional Information' tab of the 'New Case Information' dialog box. It contains fields for 'Case Number' (Android), 'Examiner' (Name: Abdullah, Phone: 031030657960, Email: abdullahamqbo08@gmail.com), and 'Notes'. Below these fields, it says 'Organization analysis is being done for: Not Specified' and has a 'Manage Organizations' button. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.



CHECKBOXING:



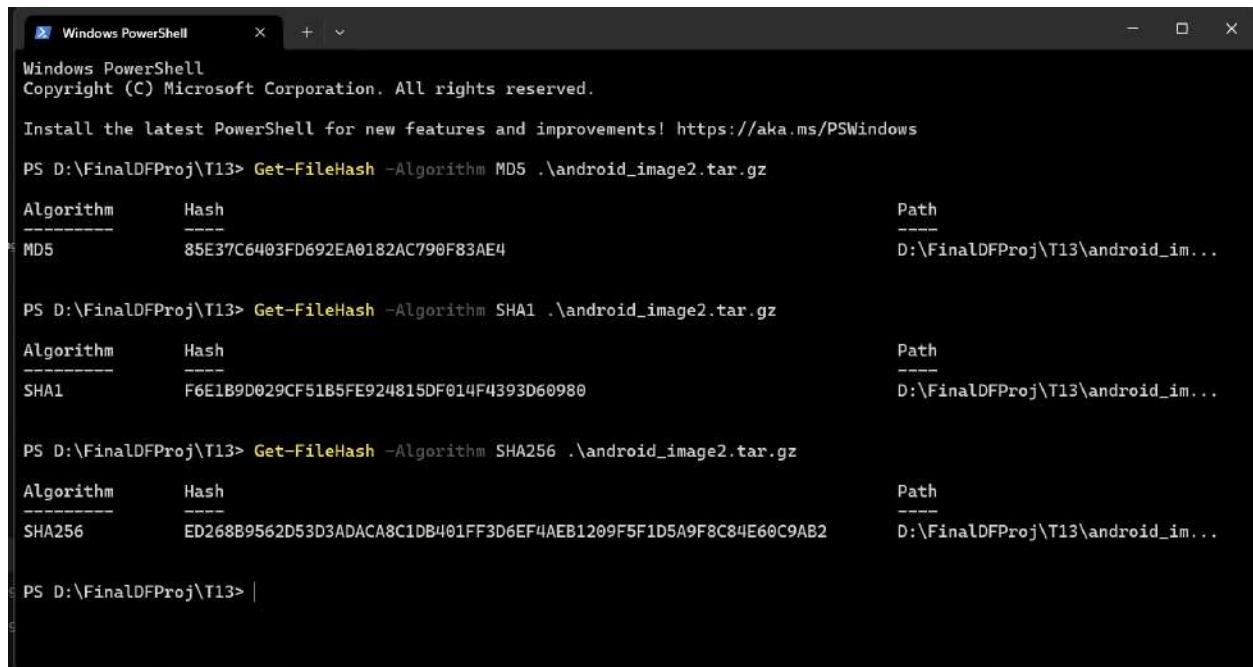
FLAG (MMSSMS.DB):

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar contains a tree view of data sources, including 'Data Sources', 'File Views', 'File Types', 'Defined Files', 'MB File Size', 'Data Artifacts', 'Call Logs (1)', 'Communication Accounts (5)', 'Device (2)', 'Installed Programs (190)', 'Messages (1)', 'Web Accounts (55)', 'Web Search (1)', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main panel displays a table titled 'Listing' with three rows. The columns are 'Source Name', 'S', 'C', 'O', 'Account Type', 'ID', and 'Data Source'. The rows are: 1. LogicalFileSet1, 0, 0, PHONE, +15555215554, LogicalFileSet1. 2. LogicalFileSet1, 0, 0, PHONE, 1112223333, LogicalFileSet1. 3. mmssms.db, 0, 0, PHONE, 1112223333, LogicalFileSet1. Below the table is a navigation bar with links: Host, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences.

Source Name	S	C	O	Account Type	ID	Data Source
LogicalFileSet1	0	0	PHONE	+15555215554	LogicalFileSet1	
LogicalFileSet1	0	0	PHONE	1112223333	LogicalFileSet1	
mmssms.db	0	0	PHONE	1112223333	LogicalFileSet1	

13. Android Analysis with Autopsy

EXAMINING FILE-HASH:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\FinalDFProj\T13> Get-FileHash -Algorithm MD5 .\android_image2.tar.gz

Algorithm      Hash                               Path
----          ----
MD5           85E37C6403FD692EA0182AC790F83AE4   D:\FinalDFProj\T13\android_im...

PS D:\FinalDFProj\T13> Get-FileHash -Algorithm SHA1 .\android_image2.tar.gz

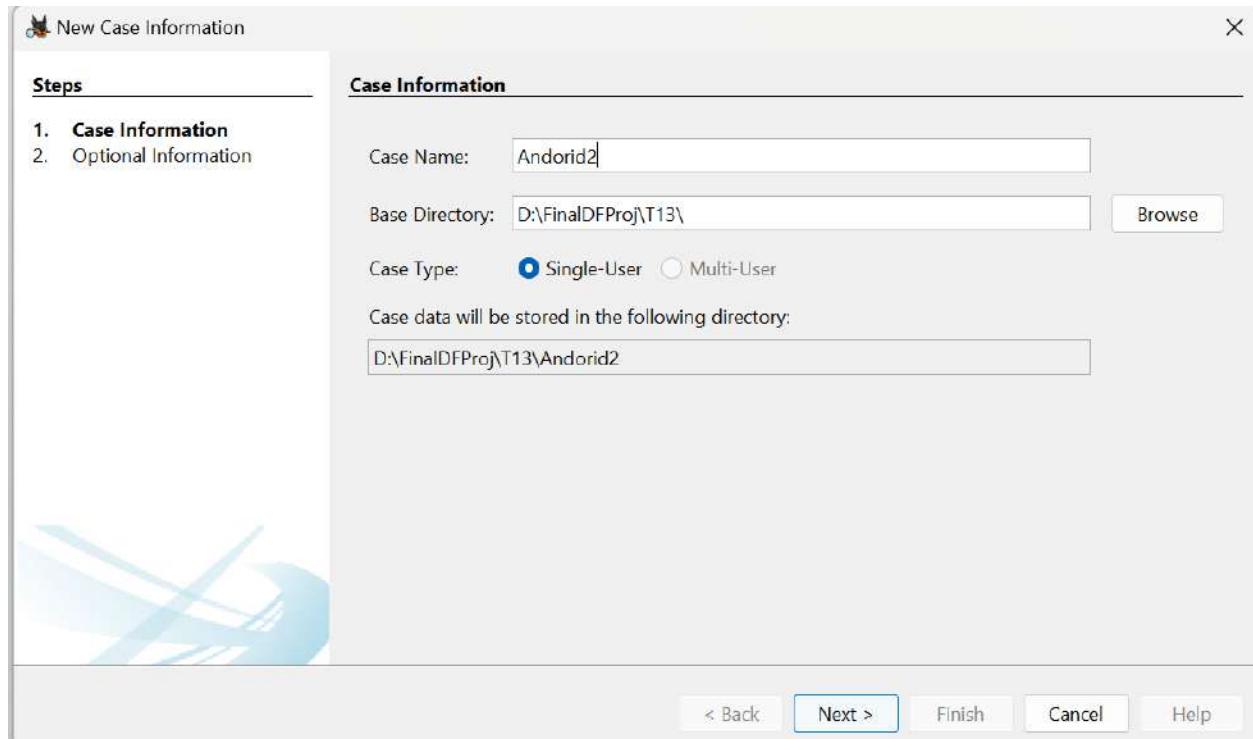
Algorithm      Hash                               Path
----          ----
SHA1          F6E1B9D029CF51B5FE924815DF014F4393D60980   D:\FinalDFProj\T13\android_im...

PS D:\FinalDFProj\T13> Get-FileHash -Algorithm SHA256 .\android_image2.tar.gz

Algorithm      Hash                               Path
----          ----
SHA256         ED268B9562D53D3ADACA8C1DB401FF3D6EF4AEB1209F5F1D5A9F8C84E60C9AB2   D:\FinalDFProj\T13\android_im...

PS D:\FinalDFProj\T13> |
```

RUNNING AUTOPSY:



New Case Information

Steps

- Case Information
- Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for:

< Back

Add Data Source

Steps

- Select Host
- Select Data Source Type**
- Select Data Source
- Configure Ingest
- Add Data Source

Select Data Source Type

Disk Image or VM File

Local Disk

Logical Files

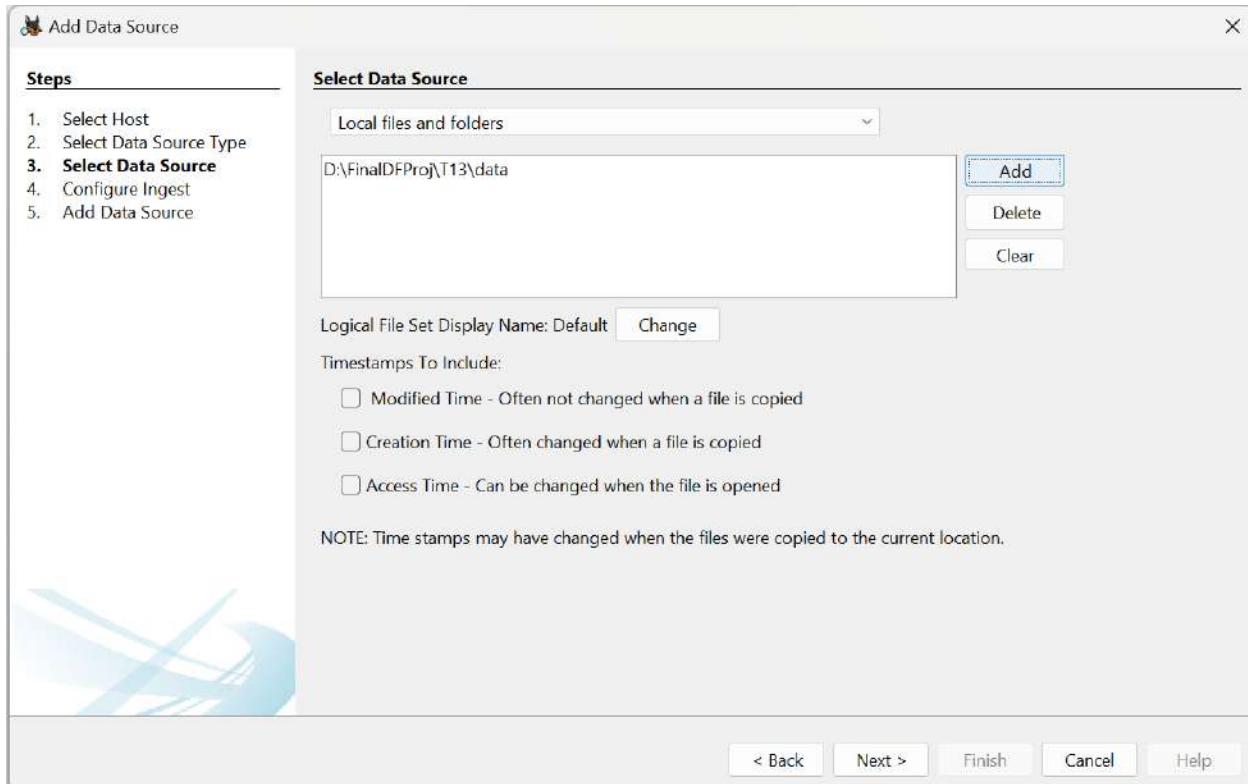
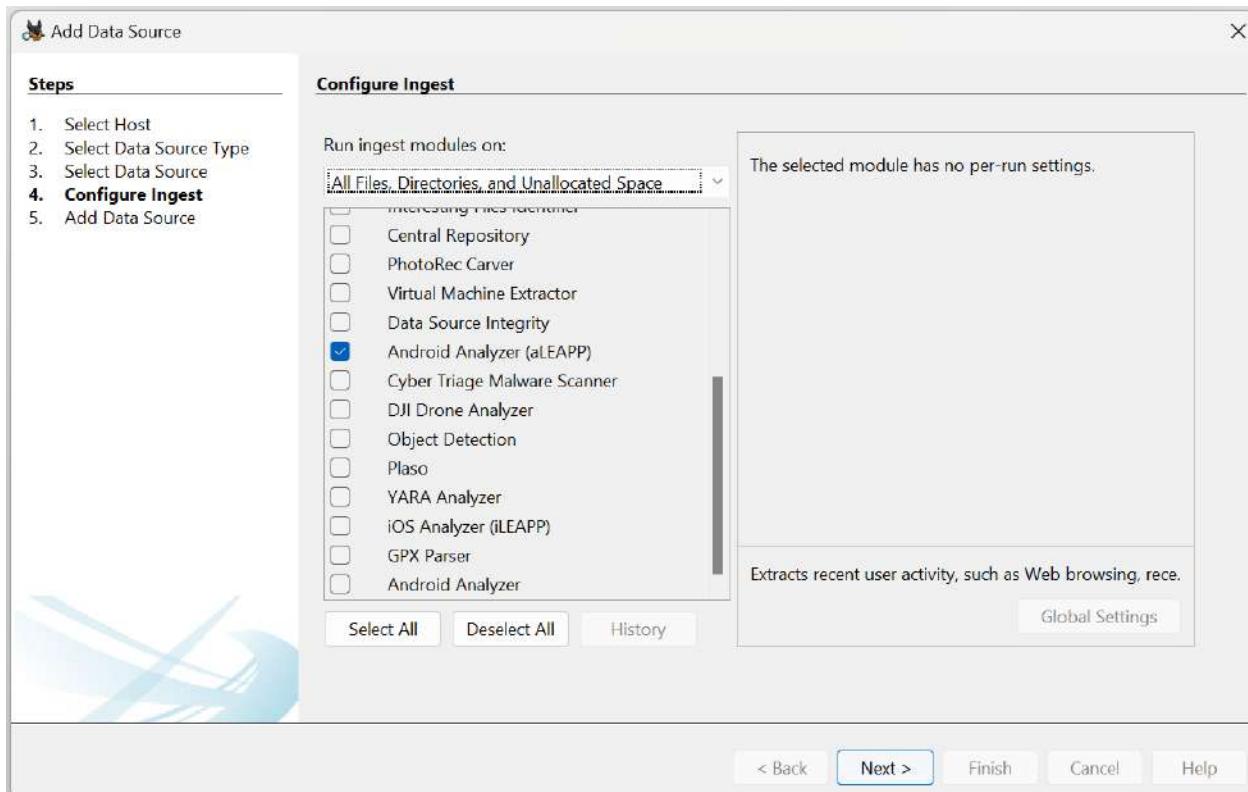
Unallocated Space Image File

Autopsy Logical Imager Results

Memory Image File (Volatility)

XRY Text Export

< Back

**CHECKBOXING:**

EXAMINING OF ARTIFACT:

The screenshot shows the Autopsy 4.21.0 interface with the 'Call Logs' listing selected. The left sidebar contains various data sources like Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, and Communication Accounts (7). The main pane displays a table with columns: Source Name, S, C, O, Start Date/Time, Phone Number, and Data Source. There are two entries: 'LogicalFileSet1' at 02:24:22 PKT with phone number 1112223333 and 'LogicalFileSet1' at 14:56:43 PKT with phone number 7872254076, both from LogicalFileSet1.

LATEST PROGRAM INSTALLED FLAG:

The screenshot shows the Autopsy 4.21.0 interface with the 'Installed Programs' listing selected. The left sidebar is identical to the previous screenshot. The main pane displays a table with columns: Source Name, S, C, O, Program Name, Comment, Data Source, and Date/Time. The table lists numerous Google Play Store installed applications, such as com.google.android.tts, com.google.android.apps.attachyon, com.google.android.mms, com.google.android.apps.youtube.music, com.google.android.deskclock, com.google.android.webview, com.google.android.apps.messaging, com.android.chrome, com.google.android.apps.photos, com.google.android.videos, com.google.android.apps.usualpaper, com.google.android.gm, com.google.android.apps.docs, com.google.android.inputmethod.latin, com.google.android.youtube, com.google.android.calendar, com.google.android.googlequicksearchbox, com.google.android.gms, and com.u360mobile.usana, all from LogicalFileSet1.

SITE VISTED AT SPECIFIC TIME FLAG:

The screenshot shows the Autopsy 4.21.0 interface with the 'Web History' tab selected. The left sidebar displays various data sources and artifacts. The main pane shows a table of web history entries. A specific row for 'https://www.yahoo.com/' is highlighted in blue.

Source Name	Date Accessed	URL	Title	Comment
LogicalFileSet1	2022-10-08 14:52:39 PKT	https://www.yahoo.com/	Yahoo Mail, Weather, Search, Politics, News, Finance, Sports & Videos	Chrome History
LogicalFileSet1	2022-10-08 14:52:48 PKT	http://kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome History
LogicalFileSet1	2022-10-08 14:52:58 PKT	https://www.kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome History
LogicalFileSet1	2022-10-08 14:52:59 PKT	https://www.yahoo.com/	Yahoo Mail, Weather, Search, Politics, News, Finance, Sports & Videos	Chrome History
LogicalFileSet1	2022-10-08 14:53:08 PKT	https://www.google.com/search?q=hockey+mask&o...	hockey mask - Google Search	Chrome History
LogicalFileSet1	2022-10-08 14:53:18 PKT	https://www.google.com/search?q=hockey+mask&o...	hockey mask - Google Search	Chrome History
LogicalFileSet1	2022-10-08 14:53:20 PKT	https://www.google.com/search?q=fake+blood&clen...	Fake blood - Google Search	Chrome History
LogicalFileSet1	2022-10-08 14:53:23 PKT	http://ccsf.edu/	CCSF Home CCSF	Chrome History
LogicalFileSet1	2022-10-08 14:53:23 PKT	http://www.ccsf.edu/	CCSF Home CCSF	Chrome History
LogicalFileSet1	2022-10-08 14:53:23 PKT	http://www.ccsf.edu/	CCSF Home CCSF	Chrome History
LogicalFileSet1	2022-10-08 14:53:30 PKT	https://samclass.info/	samclass.info: Sam Bowie Class Information	Chrome History
LogicalFileSet1	2022-10-08 14:53:30 PKT	https://amsclass.info/	amsclass.info: Sam Bowie Class Information	Chrome History
LogicalFileSet1	2022-10-08 14:53:39 PKT	http://yahoo.com/	Yahoo Mail, Weather, Search, Politics, News, Finance, Sports & Videos	Chrome History
LogicalFileSet1	2022-10-08 14:52:39 PKT	https://www.yahoo.com/	Yahoo Mail, Weather, Search, Politics, News, Finance, Sports & Videos	Chrome History
LogicalFileSet1	2022-10-08 14:52:48 PKT	http://kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome History
LogicalFileSet1	2022-10-08 14:52:58 PKT	https://www.kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome History
LogicalFileSet1	2022-10-08 14:53:18 PKT	https://www.google.com/search?q=hockey+mask&o...	hockey mask - Google Search	Chrome History
LogicalFileSet1	2022-10-08 14:53:18 PKT	https://www.google.com/search?q=hockey+mask&o...	hockey mask - Google Search	Chrome History
LogicalFileSet1	2022-10-08 14:53:20 PKT	https://www.google.com/search?q=fake+blood&clen...	Fake blood - Google Search	Chrome History
LogicalFileSet1	2022-10-08 14:53:23 PKT	http://ccsf.edu/	CCSF Home CCSF	Chrome History
LogicalFileSet1	2022-10-08 14:53:23 PKT	http://www.ccsf.edu/	CCSF Home CCSF	Chrome History
LogicalFileSet1	2022-10-08 14:53:23 PKT	http://www.ccsf.edu/	CCSF Home CCSF	Chrome History
LogicalFileSet1	2022-10-08 14:53:30 PKT	https://samclass.info/	samclass.info: Sam Bowie Class Information	Chrome History
LogicalFileSet1	2022-10-08 14:53:30 PKT	https://amsclass.info/	amsclass.info: Sam Bowie Class Information	Chrome History
LogicalFileSet1	2022-10-08 14:53:39 PKT	http://yahoo.com/	Yahoo Mail, Weather, Search, Politics, News, Finance, Sports & Videos	Chrome History

Visit Details

- Title: Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos
- Date Accessed: 2022-10-08 14:52:39 PKT
- URL: https://yahoo.com/

Other

- Comment: Chrome History

15. iPhone Analysis with Autopsy

EXAMINING FILE HASH:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\FinalDFProj\T15> Get-FileHash -Algorithm SHA256 '2021 CTF - iOS.zip'

Algorithm      Hash
----          ---
SHA256        BBFBAE3F3B52D3E546EF32DBB80EF8E431199DB1D30AA29AE26D4519D4E03187

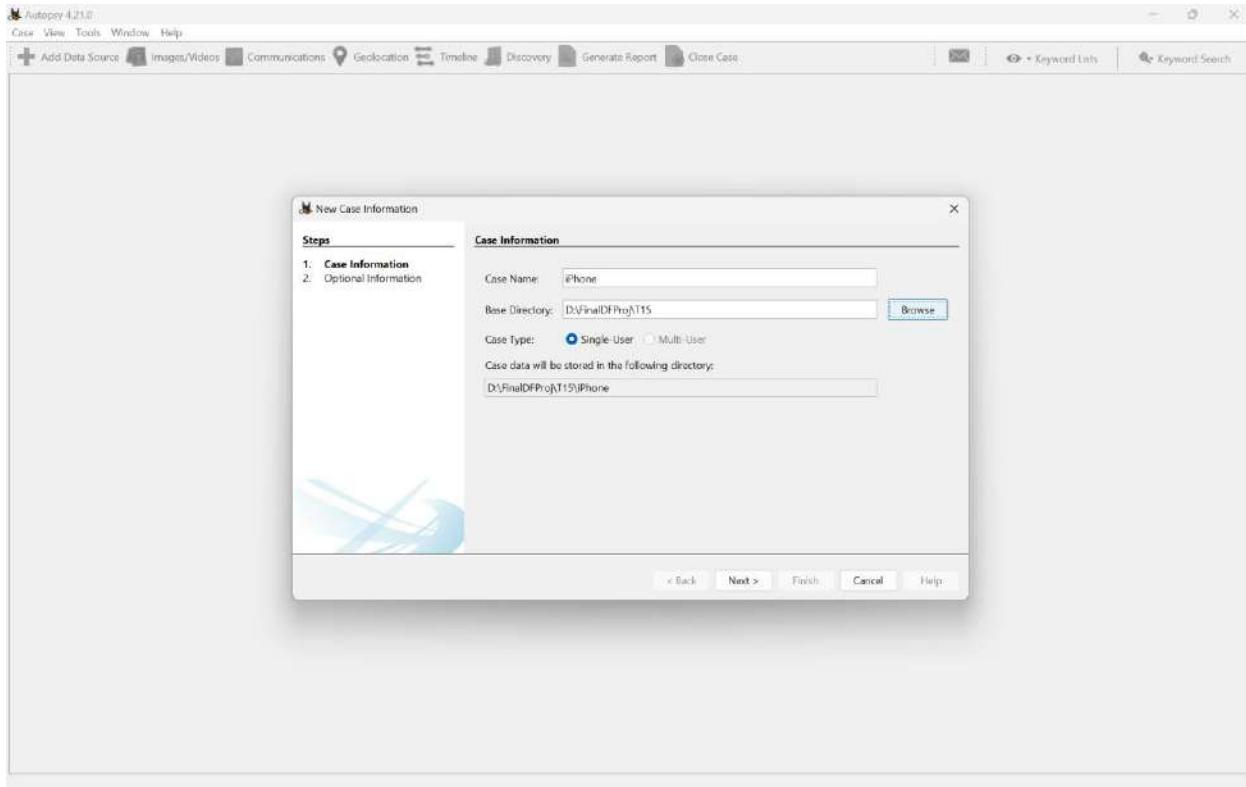
PS D:\FinalDFProj\T15> |
```

Name	Size	Date	Hash	Path
Takeout.zip	350,709,500	2022-07-21 10:02:40Z	0e17253f1022473572ac0e90009c419e6853108d5ca218708d335880154040590	1000104021cc141035c2920c040701158201331621cc00484042302627234
2020 CTF - Windows Memory.zip	1,309,342,281	2022-07-21 16:54:15Z	Bba868f49bd33970a1cc6d7144a63ff8336d83bf5/bfdcce3ba34a771a7d75955	77f169c6fe46c33358938efb80e8c1d700b035d1d676Fd2dc08e5594f3cd808
2020 CTF - Windows.zip	29,307,002,002	2022-07-21 16:59:38Z	None	None
2020 CTF - iOS.zip	12,773,266,329	2022-07-21 19:00:26Z	None	None
2021 CTF - Chromebook.lgz	408,901,035	2022-07-22 04:23:27Z	672111a1ebd876a77a298e5b0e746790b22c83a30d660530827eaab94b32c	e10e3d8f7367314b43e00f90030e022fd19dd27313ec879b3e88811848958
2021 CTF - MacOS.zip	81,139,010,088	2022-07-21 19:51:22Z	None	None
2021 CTF - Takeout.zip	4,446,601	2022-07-22 01:12:39Z	a8431aa87fcf83657fcc5a8bebe394cf39f0a9b2eb42f0bf0ee89adae0eb325	S12693825fb9adce798de65c6d7f495130a392f33aa811d3cc1f720dd8ae1bed
2021 CTF - iOS.zip	5,788,946,761	2022-07-22 01:12:46Z	b1ffac1f3b5243e546ef32dbb8ff8ed31199df1d1ba029a26d4519d4e03187	8e3d1485e060b243b37eccb3779ff2978c47d8ehba7ace83e7290e31f3c93d
2022 CTF - Android-001.tar	9,511,577,600	2022-07-22 05:00:15Z	294843a2795e182462f972053f4e128ecab7900e89135f0fc257403488fc947	a6a8b426d02901749ce374141abc80f4f1123592f80208c93054f36ab5e37c9
2022 CTF - Linux.7z	14,552,740,705	2022-07-22 05:37:37Z	3195b438c82ffdbb21ac807649b3944a67e55fc86c8ff9cfcc28ea3b9415774	bbe9a1b003b41ec2a97f8243c78b509c4cf92e15e3a1013751f84fad0f69ce2d
2022 CTF - Takeout.zip	2,580,041	2022-07-22 01:36:48Z	800e0b74aeb407e1daae9176e17ccf9871d7b645c4ccc3c2e64109373131990c	90fff0585244172817a0d11343946bf00cb293a5db4f43d6d1973690a267b4c
2022 CTF - Windows.zip	37,725,211,173	2022-07-22 01:36:53Z	None	None
2022 CTF - iOS Full File System.zip	4,711,982,945	2022-07-22 04:04:55Z	None	None
README.md	2,933	2022-07-22 12:37:20Z	3326df44761bd0ea0374c5c83f6f817c2fb39870f4c634d82e0c6a560769a15	b9c997413cd033f54754f3b94932006f921df5d00c9e25052b44f0c7a608d1

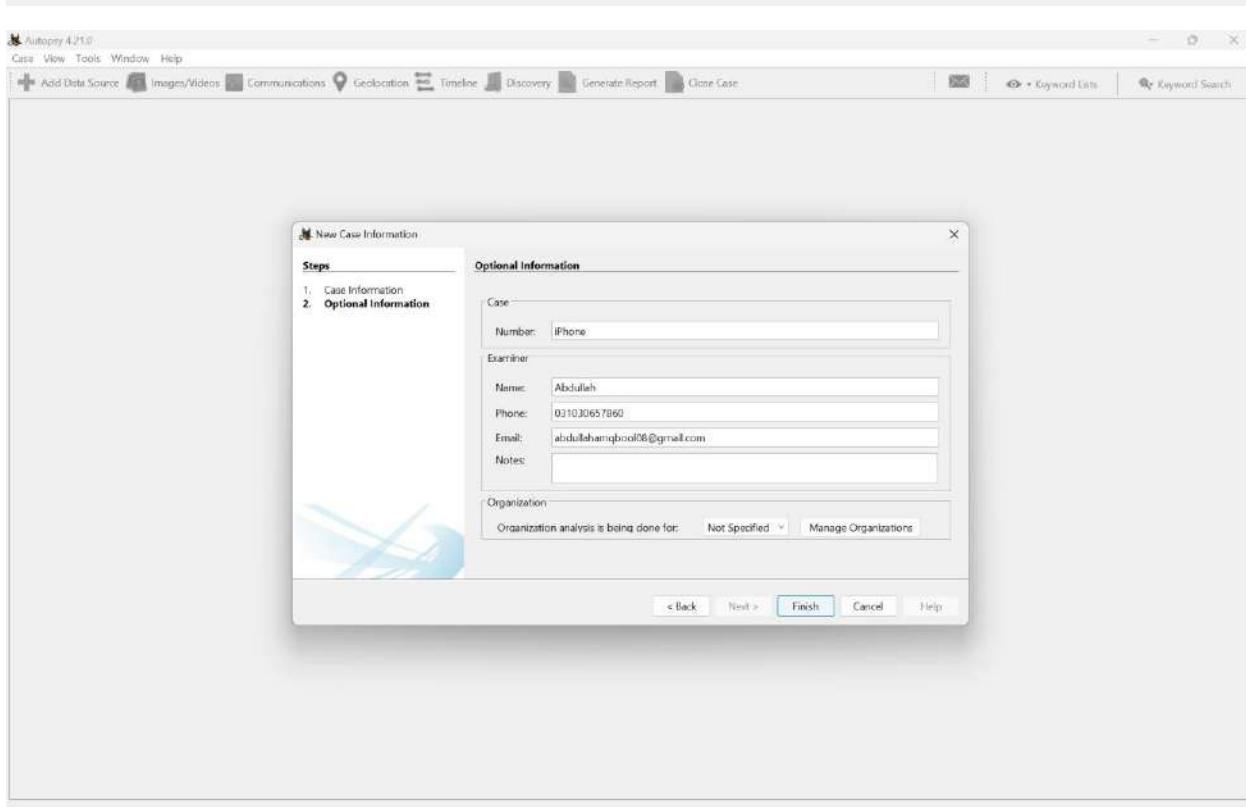
Thanks to Magnet Forensics for providing these CTF images. Full documentation is under development.

Name	Description
------	-------------

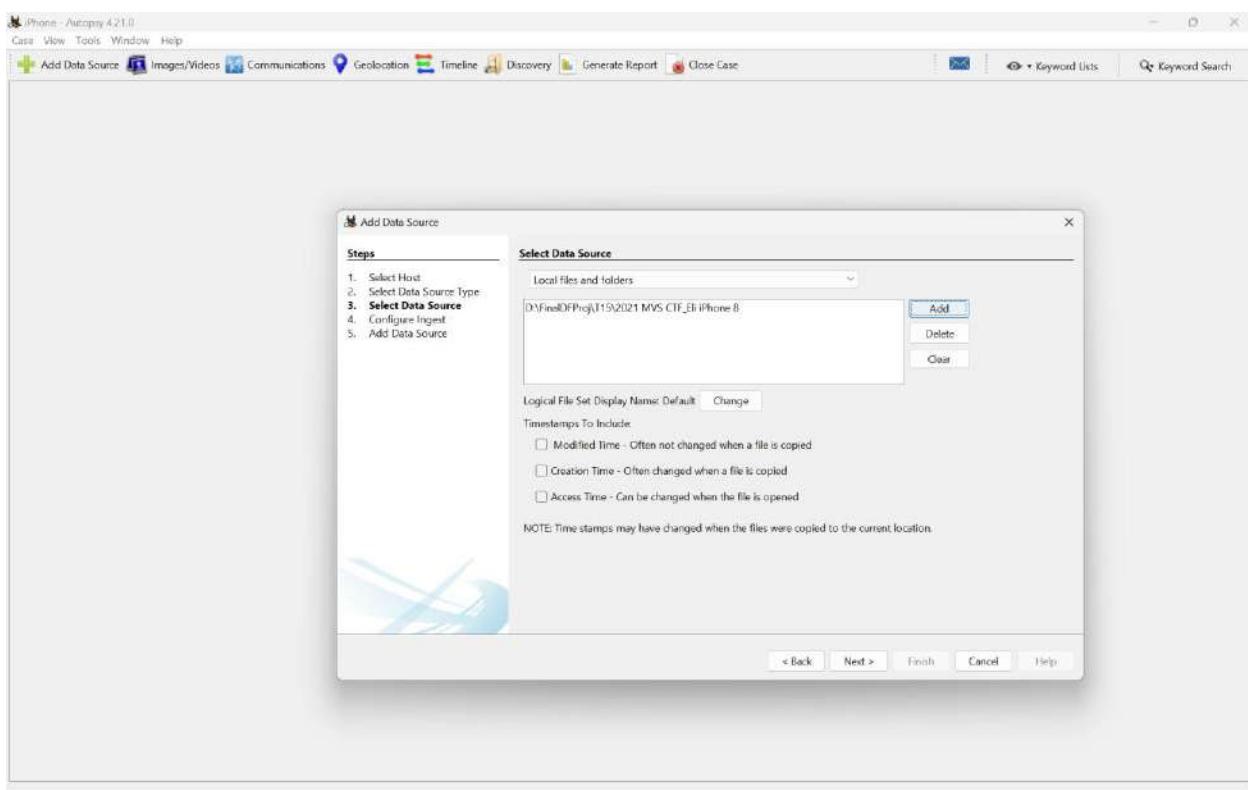
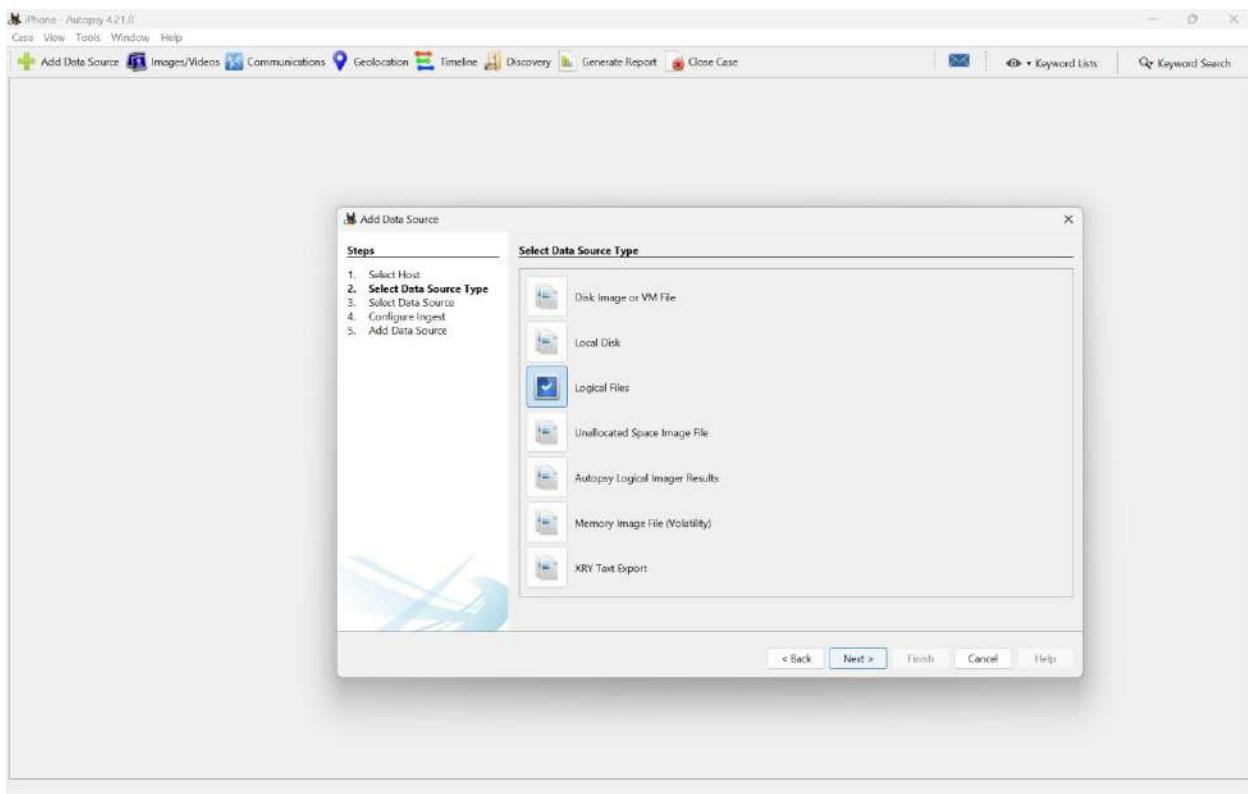
IMPORTING EVIDENCE FILE:



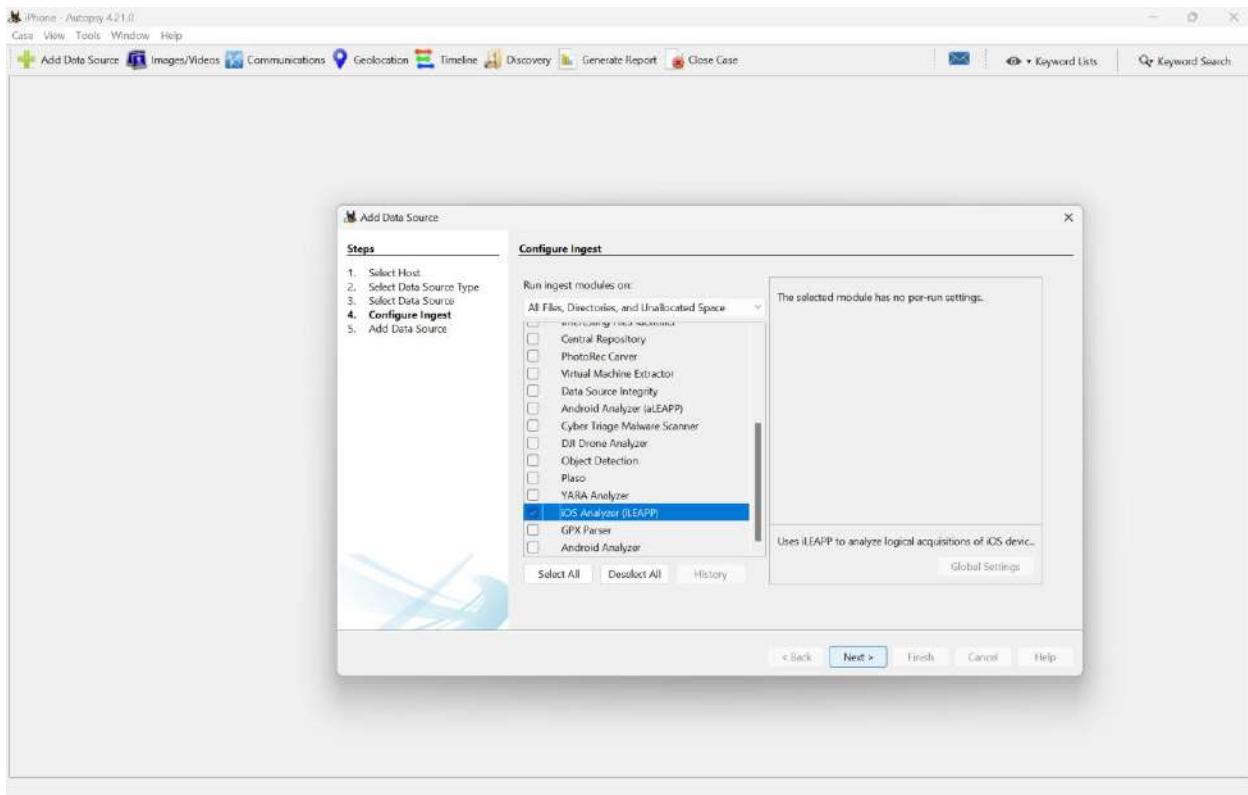
The screenshot shows the Autopsy 4.21.0 interface with the 'New Case Information' dialog box open. The dialog has two tabs: 'Case Information' and 'Optional Information'. The 'Case Information' tab is selected, showing fields for 'Case Name' (iPhone), 'Base Directory' (D:\FinalDFProjT15), 'Case Type' (Single-User selected), and a note about case data storage. The 'Optional Information' tab is also visible, showing fields for 'Case Number' (iPhone), 'Examiner' (Name: Abdullah, Phone: 031030657860, Email: abdullahmqb00@gmail.com), and 'Notes'. Buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.



The screenshot shows the 'Optional Information' tab of the 'New Case Information' dialog box. It contains fields for 'Case Number' (iPhone), 'Examiner' (Name: Abdullah, Phone: 031030657860, Email: abdullahmqb00@gmail.com), and 'Notes'. Below these, there is an 'Organization' section with a dropdown menu for 'Organization analysis it is being done for' (set to 'Not Specified') and a 'Manage Organizations' button. Navigation buttons at the bottom are '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.



CHECKBOXING:



PHONE NUMBER FLAG:

Source Name	S	C	O	Device ID	Device Name	Comment	Data Source	MAC Address
518e8d766f9b3e76db216f3f5fdb6b0604e50/61b.f	0	0	0	5B8GF53D-E321-B975-5294-A935844104F8	Ell's Apple Watch	Bluetooth Paired	LogicalFileSet1	A4BD255E-C3D9-DBD4-E83D-09F07D118243
518e8d766f9b3e76db216f3f5fdb6b0604e50/61b.f	0	0	0	A4BD255E-C3D9-DBD4-E83D-09F07D118243	Ell's Mac mini	Bluetooth Paired	LogicalFileSet1	5D467F8F8A5986
518e8d766f9b3e76db216f3f5fdb6b0604e50/61b.f	0	0	0	5B8GF53D-E321-B975-5294-A935844104F8	Ell's Mac mini	Bluetooth Paired	LogicalFileSet1	5D467F8F8A5986

LATITUDE FLAG:

The screenshot shows the Autopsy 4.21.0 interface with the 'Wireless Networks' analysis results. The left sidebar lists various data sources and artifacts. The main pane displays a table with one entry:

Source Name	S	C	D	Date/Time	SSID	Latitude	Longitude	MAC Address	Comment	Data Source
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	0			2021-03-04 21:42:46 PCT	Guest	44.49025717014438	-73.18488271294526	76:83:x2:ad:e1:3c	Will	LogicalFileSet1

SMS FLAG:

The screenshot shows the Autopsy 4.21.0 interface with the 'Messages' analysis results. The left sidebar lists various data sources and artifacts. The main pane displays a table with multiple entries, showing a series of messages from 'SIGNAL' to a recipient. The table includes columns for Source Name, Date/Time, Text, Thread ID, Comment, and Data Source.

Source Name	Date/Time	Text	Thread ID	Comment	Data Source
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-02-13 17:00:22 PCT	Total Wireless: Please take a Total Wireless survey to ha..._1		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-02-14 19:01:10 PCT	Total Wireless: Did you know you can save 5% EVER..._2		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-02-16 02:57:12 PCT	SIGNAL: Your code is: 191-1160! Tap: sgml://verify/19..._3		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-02-16 03:01:56 PCT	Snapchat code: 248566. Do not share it or use it else..._4		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-02-20 21:12:18 PCT	[TikTok] 5469 is your verification code, valid for 5 minu..._5		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-02-29 19:00:31 PCT	Total Wireless: Get 5% off on your plan EVER month ..._2		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-03-01 15:33:31 PCT	Hey! Call me on Wilks for the most succe... communica..._6		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-03-01 23:01:24 PCT	It'sThe7's right! With Auto-refill, you'll save 5% on ever..._1		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-03-05 19:03:00 PCT	Total Wireless: Upgrade to our \$50 Plan to enjoy 25GB..._1		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-03-07 01:22:13 PCT	Total Wireless: Your Service End Date is in 7 days - refil..._2		SMS - iMessage	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0504e50161b_f	2021-03-14 16:10:25 PCT	Total Wireless: Your Service End Date is in 1 days - refil..._2		SMS - iMessage	LogicalFileSet1

SIGNAL CONTACT:

iPhone - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Program Notifications

Table Thumbnail Summary

Save Table as CSV

29 Results

Source Name	S	C	O	Date/Time	Program Name	Title	Value
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-06 14:51:48 PCT	com.whispersystems.signal	TikTok	Did my dog just speak to me \ud83d\udc56\ud83d\udc48
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-05 23:51:49 PCT	com.whispersystems.signal	TikTok	How to do a middle part tutorial \ud83d\udc56\ud83d\udc44
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-05 19:51:50 PCT	com.whispersystems.signal	TikTok	Anyone can get obsessed with this song \ud83d\udc56
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-05 14:51:56 PCT	com.whispersystems.signal	TikTok	The rumors are from dollar tree!
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 23:52:08 PCT	com.whispersystems.signal	TikTok	Cutting watermelon on a whole new level \ud83d\udc56
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 20:52:09 PCT	com.whispersystems.signal	TikTok	Sugar cut & sexy hair style \ud83d\udc56\ud83d\udc4d
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 15:52:07 PCT	com.whispersystems.signal	TikTok	A whale greeting a human baby \ud83d\udc56\ud83d\udc33
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 18:52:47 PCT	com.whispersystems.signal	TikTok	You have a new message
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 06:05:20 PCT	org.whispersystems.signal	Johnathan Chipp	Reacted \ud83d\udc56\ud83d\udc48 to: "You will be!"
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-07 18:18:50 PCT	com.facebook.Facebook		\ud83d\udc56\ud83d\udc48 Eli, you have 2 new notifications at
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-06 18:53:01 PCT	com.facebook.Facebook		\ud83d\udc56\ud83d\udc48 You have a new friend suggestion.
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-06 02:11:56 PCT	com.facebook.Facebook		\ud83d\udc56\ud83d\udc48 Coleen Fenton posted an update.
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-06 00:45:02 PCT	com.facebook.Facebook		\ud83d\udc56\ud83d\udc48 Coleen Fenton posted an update.
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 19:57:11 PCT	com.facebook.Facebook		Coleen Fenton sent you a message.
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 19:56:44 PCT	com.facebook.Facebook		Coleen Fenton sent you a message.
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 19:09:21 PCT	com.facebook.Facebook		Coleen Fenton sent you a friend request.
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-04 17:50:48 PCT	com.apple.news	Apple News Spotlight	Inside a notorious wedding that spread COVID-19 deaths
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-02-22 22:28:03 PCT	com.apple.news	News Top Stories	The U.S. has surpassed 300,000 COVID-19 deaths
518e8d766f9b3e76db21635fdb60604e50f61b.f				2021-03-07 13:00:17 PCT	di.pentagonal.protocol	Vineyard vines	(LAST Day Limited Edition Easter Styles)

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

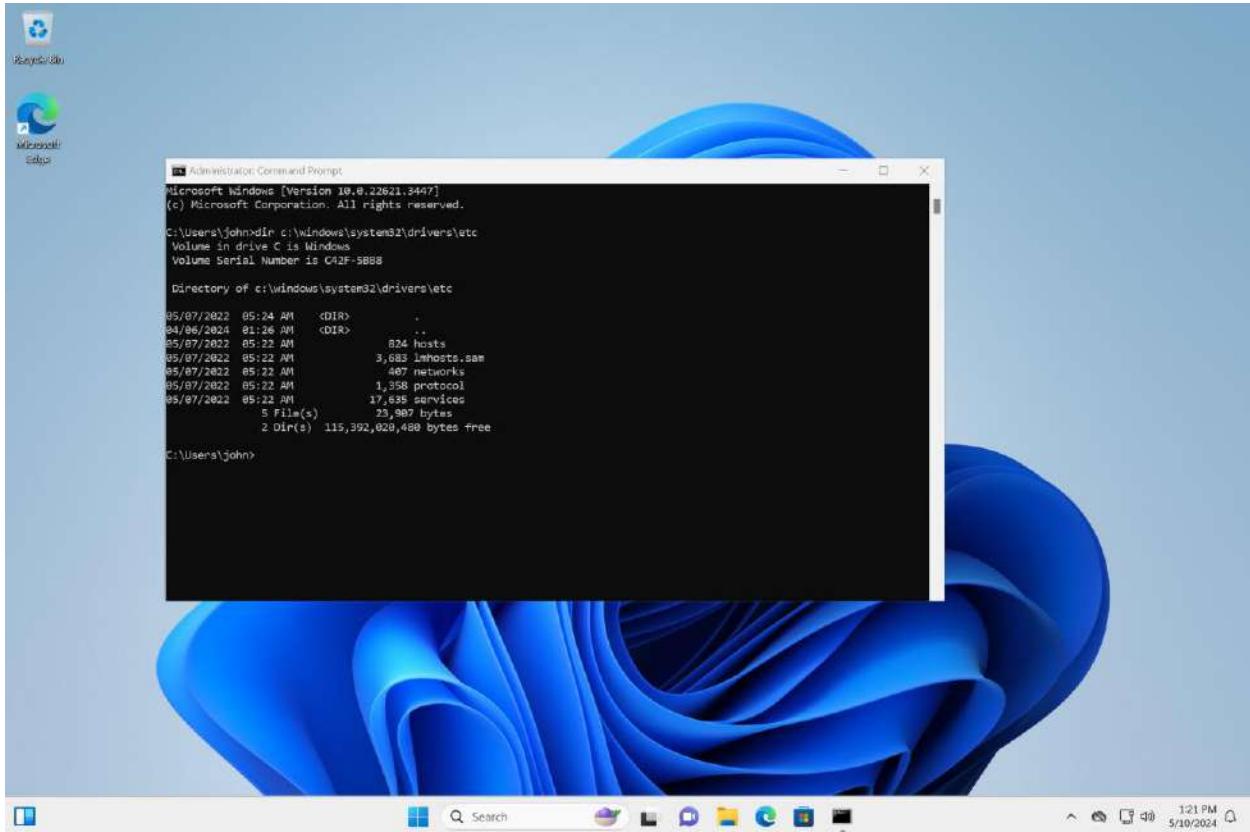
Result: 369 of 393 Result

Program Notifications

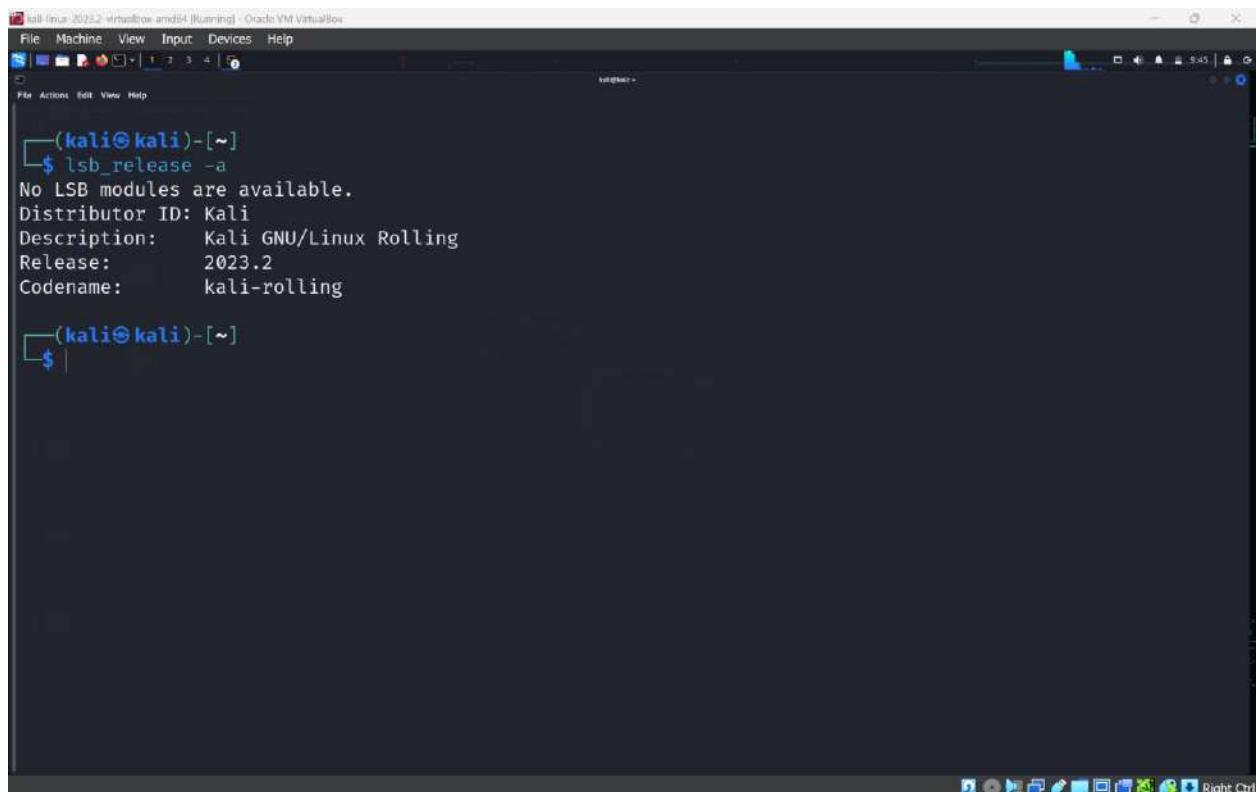
Type	Value	Source(s)
Date/Time	2021-03-04 06:02:00 PCT	iOS Analyzer (LEAPP)
Program Name	org.whispersystems.signal	iOS Analyzer (LEAPP)
Title	Johnathan Chipp	iOS Analyzer (LEAPP)
Value	Reacted \ud83d\udc56\ud83d\udc48 to: "You will be!"	iOS Analyzer (LEAPP)
Comment	iOS Notifications	iOS Analyzer (LEAPP)
Source File Path	/LogFileSett/2021 MVS CTF_Eli iPhone 8/518e8d766f9b3e76db21635fdb60604e50f61b_files/full.zip	
Address XY	0x33337700300C #7C #10	

16.Windows and Linux Machines

WINDOWS FLAG:



LINUX FLAG:



(kali㉿kali)-[~]\$ lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description: Kali GNU/Linux Rolling
Release: 2023.2
Codename: kali-rolling
(kali㉿kali)-[~]\$

17. Velociraptor Server on Linux

FINDING THE LAST VERSION:

The screenshot shows the GitHub releases page for the 'velociraptor' repository. It displays a list of recent commits and a detailed list of assets. The assets section includes files like 'velociraptor-collector' and various binary files for different platforms. The last asset listed is a 'tar.gz' file from March 10.

Asset	Size	Last Updated
velociraptor-collector	78 KB	last week
velociraptor-collector.sig	438 Bytes	last week
velociraptor-v0.72.0-darwin-amd64	61.7 MB	2 weeks ago
velociraptor-v0.72.0-darwin-amd64.sig	438 Bytes	2 weeks ago
velociraptor-v0.72.0-darwin-arm64	59.3 MB	2 weeks ago
velociraptor-v0.72.0-darwin-arm64.sig	438 Bytes	2 weeks ago
velociraptor-v0.72.0-freebsd-amd64	55.1 MB	2 weeks ago
velociraptor-v0.72.0-freebsd-amd64.sig	438 Bytes	2 weeks ago
velociraptor-v0.72.0-linux-amd64	55.6 MB	2 weeks ago
velociraptor-v0.72.0-linux-amd64-musl	55.7 MB	2 weeks ago
Source code (zip)		Mar 10
Source code (tar.gz)		Mar 10

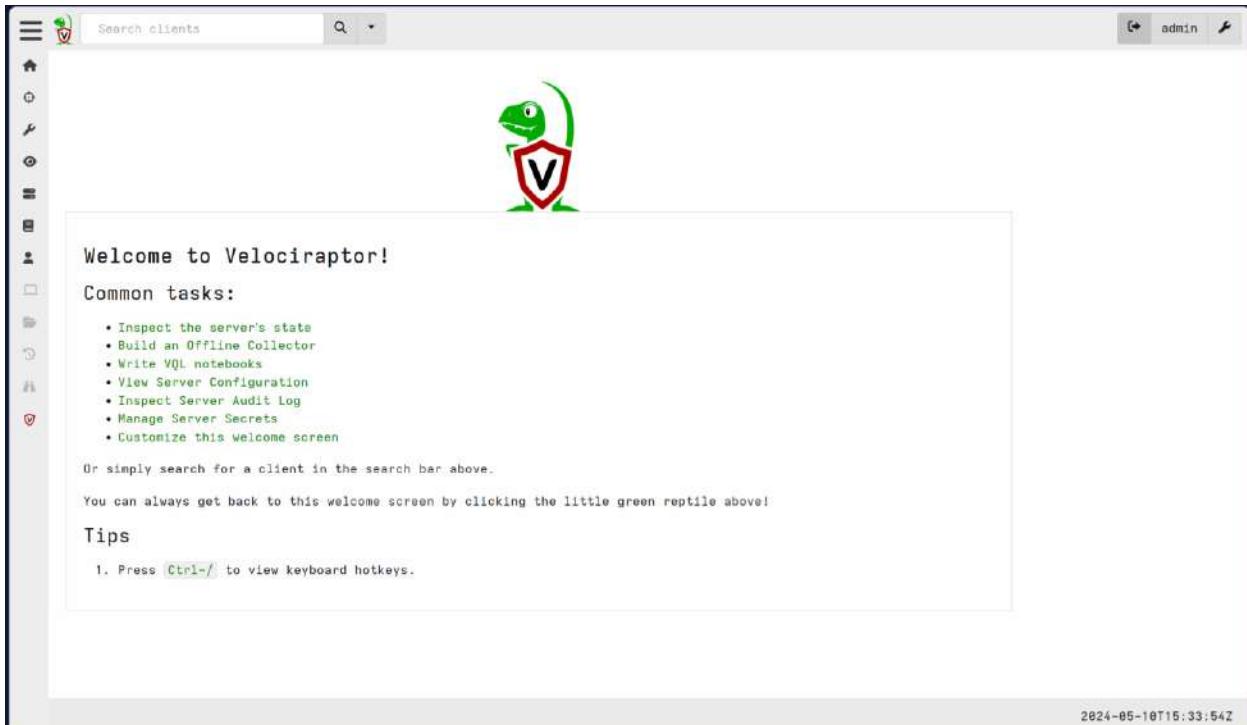
PREPARING THE SERVER:

```
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ chmod +x velociraptor-v0.72.1-linux-amd64 ./velociraptor-v0.72.1-linux-amd64 config generate > velociraptor.config.yaml
chmod: cannot access 'config': No such file or directory
chmod: cannot access 'generate': No such file or directory
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ chmod +x velociraptor-v0.72-rc1-linux-amd64
chmod: cannot access 'velociraptor-v0.72-rc1-linux-amd64': No such file or directory
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ chmod +x velociraptor
chmod: cannot access 'velociraptor': No such file or directory
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ chmod +x velociraptor-v0.72.1-linux-amd64
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ ./velociraptor-v0.72.1-linux-amd64 config generate > velociraptor.config.yaml
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ ip a
19: eth0: <NO-SPEC> mtu 1500 group default qlen 1
    link/ether b0:60:88:8b:63:6f
        inet 169.254.195.226/16 brd 169.254.255.255 scope global dynamic
            valid_lft forever preferred_lft forever
14: eth1: <BROADCAST,MULTICAST,UP> mtu 1500 group default qlen 1
```

```
[INFO] 2024-05-10T15:32:19Z Upgrading tool SysmonBinary {"Tool": {"name": "SysmonBinary", "url": "https://live.sysinternals.com/tools/sysmon64.exe", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool SysmonConfig {"Tool": {"name": "SysmonConfig", "url": "https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool WinPmem {"Tool": {"name": "WinPmem", "url": "https://github.com/Velocidex/WinPmem/releases/download/v4.0.rc1/winpmem_mini_x64_rc2.exe", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool Bulk_Extractor_Binary {"Tool": {"name": "Bulk_Extractor_Binary", "url": "https://github.com/Velocidex/Tools/raw/main/BulkExtractor/bulk_extractor.exe", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool SunburstYARARules {"Tool": {"name": "SunburstYARARules", "url": "https://raw.githubusercontent.com/fireeye/sunburst_countermeasures/main/all-yara.yar"}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool WinPmem64 {"Tool": {"name": "WinPmem64", "github_project": "Velocidex/WinPmem", "github_asset_regex": "winpmem_min_x64_+exe", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool Intezer {"Tool": {"name": "Intezer", "url": "https://analyze.intezer.com/api/scans/download"}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool etl2pcapng {"Tool": {"name": "etl2pcapng", "url": "https://github.com/microsoft/etl2pcapng/releases/download/v1.4.0/etl2pcapng.zip"}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool OSQueryWindows {"Tool": {"name": "OSQueryWindows", "github_project": "Velocidex/OSQuery-Releases", "github_asset_regex": "windows-and64.exe"}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool Autorun_386 {"Tool": {"name": "Autorun_386", "url": "https://live.sysinternals.com/tools/autorunsc.exe", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z Upgrading tool Autorun_amd64 {"Tool": {"name": "Autorun_amd64", "url": "https://live.sysinternals.com/tools/autorunsc64.exe", "serve_locally": true}}
[INFO] 2024-05-10T15:32:19Z CryptoServerManager: Watching for events from Server.Internal.ClientDelete
[INFO] 2024-05-10T15:32:19Z Compiled all artifacts.
[INFO] 2024-05-10T15:32:19Z Throttling connections to 100 QPS
[INFO] 2024-05-10T15:32:19Z Starting gRPC API server on 192.168.56.1:8001

[INFO] 2024-05-10T15:32:19Z Launched Prometheus monitoring server on 192.168.56.1:8003
[INFO] 2024-05-10T15:32:19Z GUI will use the Basic authenticator
[INFO] 2024-05-10T15:32:19Z GUI is ready to handle TLS requests on https://192.168.56.1:8889/
[INFO] 2024-05-10T15:32:19Z Frontend is ready to handle client TLS requests at https://192.168.56.1:8000/
```

VIEWING THE GUI:



SERVER NAME:

The screenshot shows a web-based management interface with two main sections: 'Users' and 'Server version'.

Users section:

name	Roles
admin	administrator

Below the table, there are buttons for sorting and filtering, and a pagination control showing "Showing 1 to 1 of 1".

Server version section:

Version
<pre>v { "name": "velociraptor", "version": "0.72.1", "commit": "26df171", "build_time": "2024-05-08T00:25:45Z", "ci_build_url": "https://github.com/Velocidex/velociraptor/actions/", "compiler": "go1.22.2" }</pre>

Below the table, there are buttons for sorting and filtering, and a pagination control showing "Showing 1 to 1 of 1".

At the bottom right of the interface, the timestamp "2024-05-10T15:34:39Z" is displayed.

WINSCP DOWNLOAD:

The screenshot shows the SourceForge project page for WinSCP. At the top, there's a navigation bar with links for 'For Vendors', 'Help', 'Create', and 'Join'. A search bar is also present. Below the header, there's a banner for 'WinSCP' with the text: 'WinSCP is a free SFTP, SCP, S3, WebDAV, and FTP client for Windows. Brought to you by: martinprikryl'. There are buttons for 'Get Updates', 'Share This', and 'Problems Downloading?'. A note below says 'WinSCP-6.3.3-Setup.exe | Scanned for malware ✓'. To the right, there's a 'Related Business Categories' sidebar with links to 'Communications', 'IT Security', 'IT Management', and 'FTP Clients'. A 'Web Werks' logo is also visible.

AGENT NAME:

The screenshot shows the VelocityX interface for managing agents. The top bar shows the agent name 'ABDULLAHM-PC' and its status as 'Connected'. The main panel displays detailed information about the agent, including:

- Client ID:** C.ca282919b38c0ae1
- Agent Version:** 8.72.1
- Agent Build Time:** 2024-05-08T08:33:32Z
- First Seen At:** 2024-05-11T17:50:23Z
- Last Seen At:** 2024-05-11T17:53:40Z
- Last Seen IP:** 127.0.0.1:53005
- Labels:** (empty)
- Operating System:** windows
- Hostname:** ABDULLAHM-PC
- FQDN:** ABDULLAHM-PC
- Release:** Microsoft Windows 11 Home10.0.22631 Build 22631
- Architecture:** amd64
- MAC Addresses:**
 - b8:b8:27:b0:b0:b0
 - b8:b0:88:8b:63:6c
 - b2:b0:88:8b:63:6b
 - b8:b0:88:8b:63:6b
 - b8:b0:88:8b:63:6f

AGENT NAME:

The screenshot shows the 'Overview' tab of the Agent interface. It displays the following details for the agent 'ABDULLAHM-PC':

Client ID	C.ca282919b38c0ae1
Agent Version	8.72.1
Agent Build Time	2024-05-08T08:33:32Z
First Seen At	2024-05-11T17:59:23Z
Last Seen At	2024-05-11T17:54:05Z
Last Seen IP	127.0.0.1:53005
Labels	(empty)

USING VIRTUAL FILE SYSTEM:

The screenshot shows the 'VFS Drilldown' tab of the Agent interface. The left sidebar lists mounted volumes: 'auto', 'ntfs' (selected), and 'registry'. The main pane displays the contents of the 'C:' drive:

Download	Name	Size	Mode	mtime	ctime
	\.\.\C:	225279Mb	drwxr-xr-x	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z
	\.\.\D:	240871Mb	drwxr-xr-x	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z

Below the table, there are two panes for the 'C:' volume:

- Properties:**

Description	Local Fixed Disk
DeviceID	C:
FreeSpace	13367812096
Size	236223197184
SystemName	ABDULLAHM-PC
VolumeName	Windows
VolumeSerialNumber	CC1CF525
- File List:** This pane is currently empty.

REGISTRY INFORMATION:

The screenshot shows the APTA interface with the 'registry' section selected in the left sidebar. The 'HKEY_CURRENT_USER' key is highlighted. The main pane displays a table of files under this key, with the first five entries shown:

Download	Name	Size	Mode	mtime	ctime
	AppEvents	0	drwxr-xr-x	2023-09-05T19:52:40Z	2023-09-05T19:52:40Z
	Console	0	drwxr-xr-x	2024-01-28T15:14:15Z	2024-01-28T15:14:15Z
	Control Panel	0	drwxr-xr-x	2023-09-05T19:58:44Z	2023-09-05T19:58:44Z
	Environment	0	drwxr-xr-x	2024-05-08T13:21:46Z	2024-05-08T13:21:46Z

The bottom right corner shows the timestamp 2024-05-11T17:56:13Z.

EXPLORING THE FILE SYSTEM:

The screenshot shows the APTA interface with the 'file' section selected in the left sidebar. The 'C:' drive is selected. The main pane displays a table of files and folders under the C:\ drive, with several entries shown:

Download	Name	Size	Mode	mtime	ctime
	NTUSER.DAT{9e1c93ef-4c25-11ee-99ad-9907f6d8b92b}.T	512Kb	-rwxr-xr-x	2023-09-05T19:52:33Z	2023-09-05T19:52:33Z
	.dotnet	0	drwxr-xr-x	2024-04-11T05:51:11Z	2024-04-11T05:51:11Z
	AppData	0	drwxr-xr-x	2022-05-07T05:24:50Z	2023-09-05T19:52:33Z
	Application	0	drwxr-xr-x	2023-09-05T19:55:31Z	2023-09-05T19:55:31Z
	Data	0	drwxr-xr-x	2023-09-05T19:55:31Z	2023-09-05T19:55:31Z

The bottom right corner shows the timestamp 2024-05-11T17:57:56Z.

COLLECTING AN ARTIFACT:

WINDOWS.NETWORK.NETSTATENRICHED:

The screenshot shows the NetworkMiner interface with the following details:

Artifacts Table:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
X	F.C0VR4NQE6OME0	Windows.Network.NetstatEnriched	2024-05-11T18:01:03Z	2024-05-11T18:01:11Z	admin	0 b	0
✓	F.C0VR38306086C	System.VFS.ListDirectory	2024-05-11T17:57:52Z	2024-05-11T17:57:52Z	admin	0 b	32
✓	F.C0VR256HOVKPU	System.VFS.ListDirectory	2024-05-11T17:57:04Z	2024-05-11T17:57:05Z	admin	0 b	8
✓	F.C0VR20H6BPH9C	System.VFS.ListDirectory	2024-05-11T17:56:58Z	2024-05-11T17:56:51Z	admin	0 b	38

Artifact Collection Overview:

- Artifact Names: Windows.Network.NetstatEnriched
- Flow ID: F.C0VR4NQE6OME0
- Creator: admin
- Create Time: 2024-05-11T18:01:03Z
- Start Time: 2024-05-11T18:01:03Z
- Last Active: 2024-05-11T18:01:11Z
- Duration: 8.01 seconds
- State: RUNNING
- Ops/Sec: Unlimited
- CPU Limit: Unlimited
- IOPS Limit: Unlimited
- Timeout: 600 seconds
- Max Rows: 1M rows

Results Panel:

Artifacts with Results
Total Rows: 0
Uploaded Bytes: 0 / 0
Files uploaded: 0
Download Results: Select a download method

2024-05-11T18:01:14Z

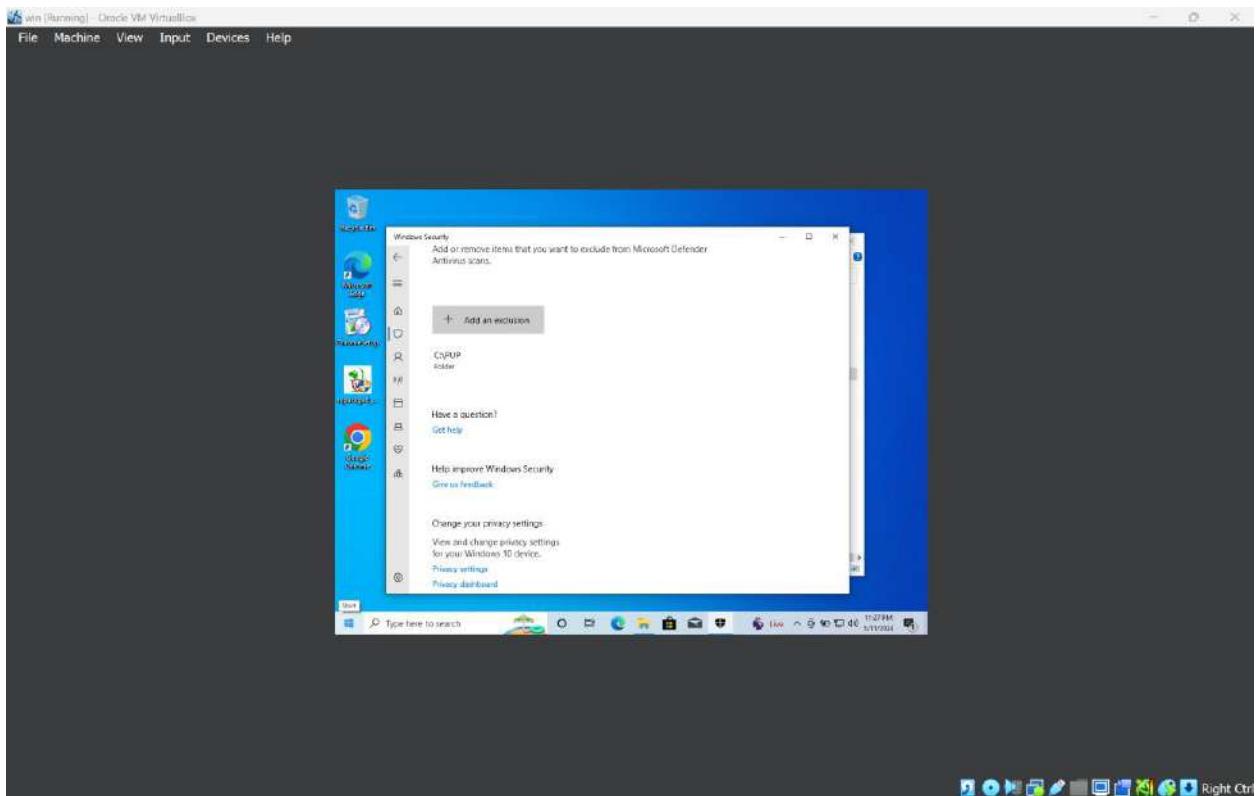
DESTPORT FLAG:

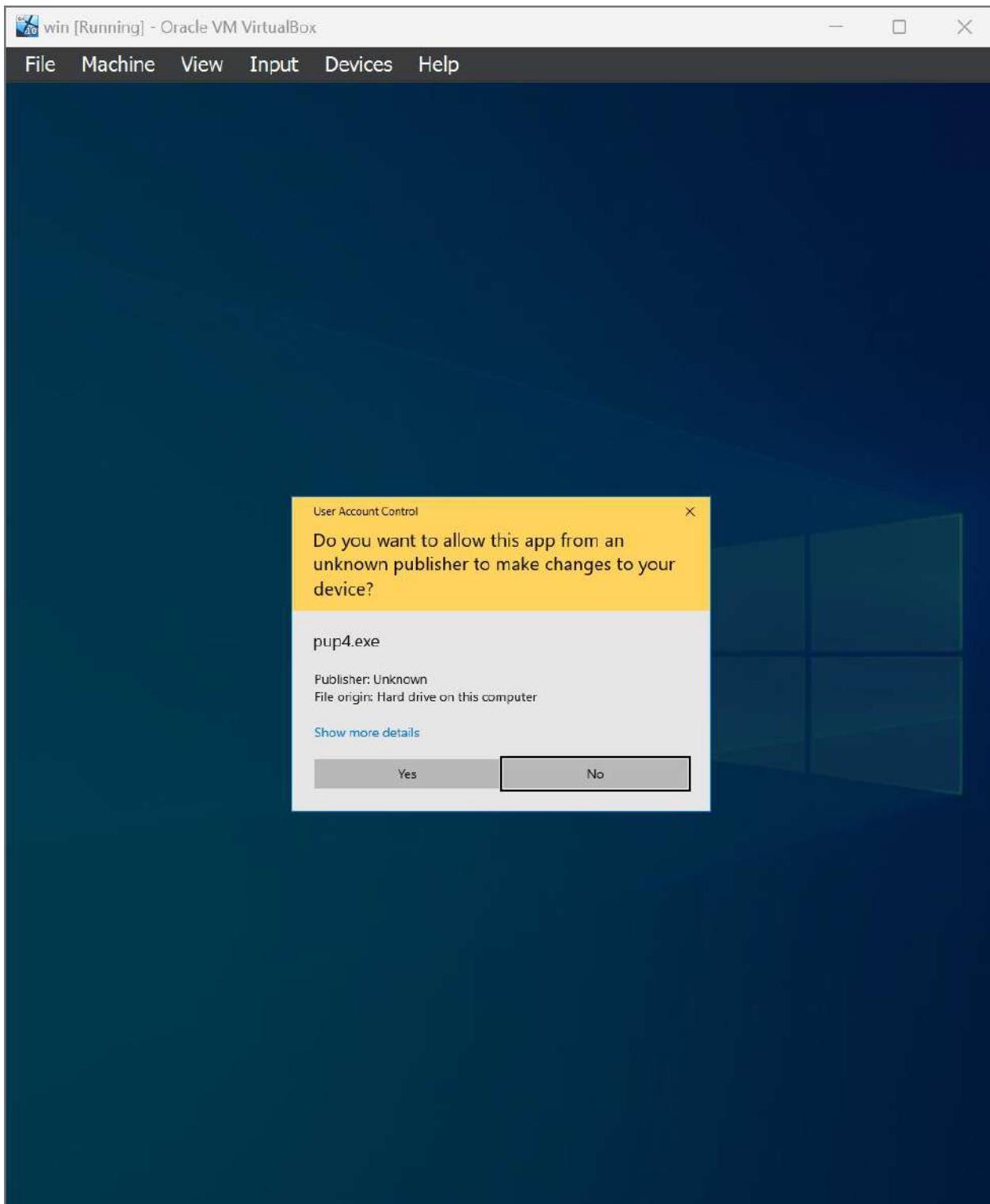
The screenshot shows a NetworkMiner tool window titled "Raw Response JSON". The interface includes a left sidebar with various icons, a central pane for displaying the JSON data, and a right sidebar with a tree view of captured items. The JSON data is displayed in a monospaced font, showing two main objects. The first object has fields like "Authenticode", "Family", "Type", "Status", "SrcIP", "SrcPort", "DestIP", "DestPort", and "Timestamp". The second object contains fields such as "Pid", "Ppid", "Name", "Path", "CommandLine", "Hash", "MD5", "SHA1", and "SHA256". Both objects have "Username" and "Authenticode" fields. The timestamp in the JSON is "2024-05-11T17:45:20Z". The bottom right corner of the window shows the date and time: "2024-05-11T19:04:45Z".

```
33     "Authenticode": "",  
32     "Family": "IPv4",  
31     "Type": "TCP",  
30     "Status": "LISTEN",  
29     "SrcIP": "192.168.56.1",  
28     "SrcPort": 8801,  
27     "DestIP": "0.0.0.0",  
26     "DestPort": 0,  
25     "Timestamp": "2024-05-11T17:45:20Z"  
24 },  
23 {  
22     "Pid": 25300,  
21     "Ppid": 22304,  
20     "Name": "velociraptor-v0.72.1-linux-amd64",  
19     "Path": "",  
18     "CommandLine": "",  
17     "Hash": {  
16         "MD5": "d41d8cd98f00b204e9800998ecf8427e",  
15         "SHA1": "da39a3ee5e6b4b0d3255bfe95601890afdb80709",  
14         "SHA256": "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855"  
13     },  
12     "Username": "ABDULLAHM-PC\\user",  
11     "Authenticode": "",  
10     "Family": "IPv4",  
9     "Type": "TCP",  
8     "Status": "ESTAB",  
7     "SrcIP": "192.168.56.1",  
6     "SrcPort": 8801,  
5     "DestIP": "192.168.56.1",  
4     "DestPort": 52828,  
3     "Timestamp": "2024-05-11T17:45:20Z"  
2 },  
1 {}  
300 ]
```

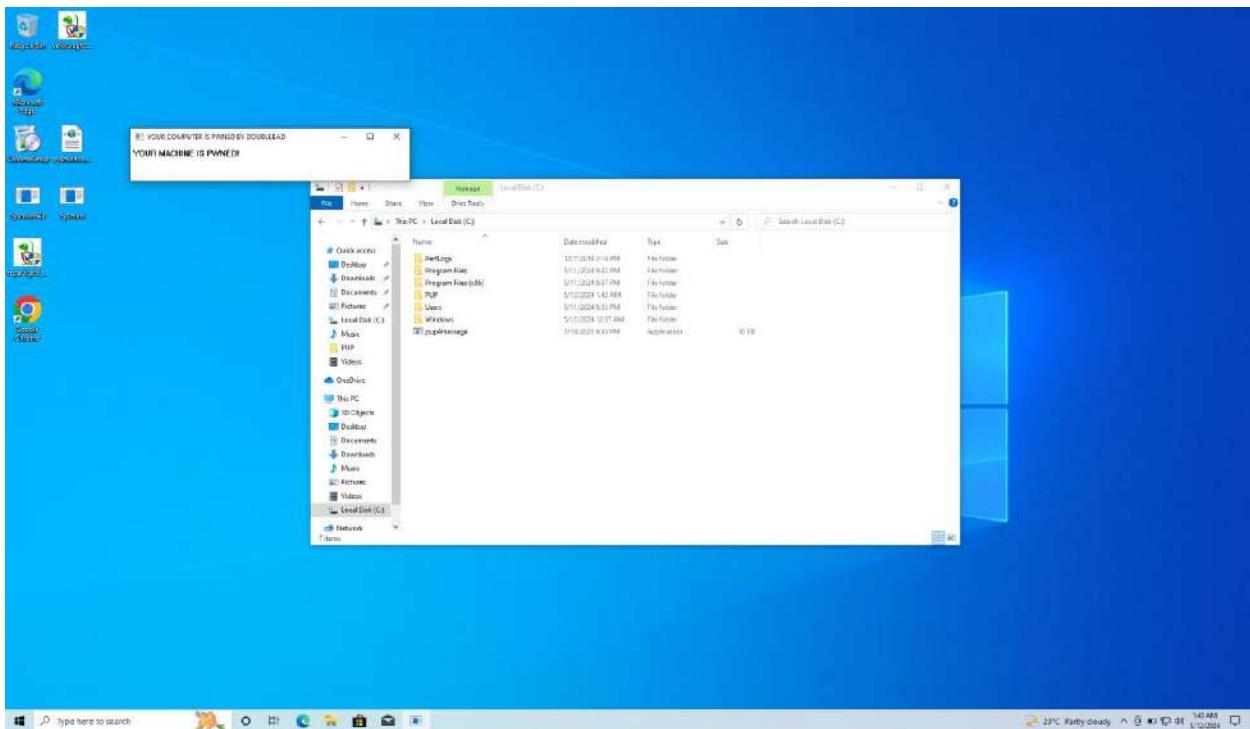
18. Investigating a PUP with Velociraptor

ADDING EXCLUSION:





INFECTING MACHINE:



RUNKEY FLAG:

```

KnownDlls, rpcrt4,enabled,Known DLLs, System-wide, Remote Procedure Call Runtime,(Verified) Microsoft Windows,Microsoft Corporation,c:\KnownDlls,sehost,enabled,Known DLLs, System-wide, Host for SCM/SSDL/LSA Lookup APIs,(Verified) Microsoft Windows,Microsoft Corporation,c:\KnownDlls,Setupapi,enabled,Known DLLs, System-wide, Windows Setup API,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\sysw KnownDlls,SHCORE,enabled,Known DLLs, System-wide, SHCORE,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\sysw KnownDlls,SHLL32,enabled,Known DLLs, System-wide, Windows Shell Common Dll,(Verified) Microsoft Windows,Microsoft Corporation,c:\wind KnownDlls,SHLWAPI,enabled,Known DLLs, System-wide, Shell Light-weight Utility Library,(Verified) Microsoft Windows,Microsoft Corporation,c:\KnownDlls,user32,enabled,Known DLLs, System-wide, Multi-User Windows USER API Client DLL,(Verified) Microsoft Windows,Microsoft Corporation,c:\KnownDlls,WLDAP32,enabled,Known DLLs, System-wide, Win32 LDAP API DLL,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\syswin,enabled,Known DLLs, System-wide, ,,,c:\windows\syswow64\wow64.dll,,wow64.dll, ,,,win,enabled,Known DLLs, System-wide, ,,,c:\windows\syswow64\wow64win.dll,,wow64win.dll, ,,,,
KnownDlls,WS2_32,enabled,Known DLLs, System-wide, Windows Socket 2.0 32-Bit DLL,(Verified) Microsoft Windows,Microsoft Corporation,c:\KnownDlls,logon\Shell, ,,,Logon, System-wide, ,,,,
logon\Shell,explorer.exe,enabled,Logon, System-wide, Windows Explorer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\explorer\shell, ,,,Logon, System-wide, ,,,,
teShell,cmd.exe,enabled,Logon, System-wide, Windows Command Processor,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\syslogon, System-wide, ,,,,
urityHealth,enabled,Logon, System-wide, Windows Security notification icon,(Verified) Microsoft Windows,Microsoft Corporation,c:\windo xTray,enabled,Logon, System-wide, VirtualBox Guest Additions Tray Application,(Verified) Microsoft Windows Hardware Compatibility Pub sion\Run, ,,,Logon, System-wide, ,,,,
sion\Run,PUP4,enabled,Logon, System-wide, ,,,c:\pup4message.exe, ,C:\PUP4message.exe,A53BFC803E217B9D599C7C774970550,DA0935468E6CA8686 tem-wide, ,,,,
Explorer,System-wide,Microsoft (R) HTML Viewer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\mshtml.dll,11. plorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11.0 plorer,System-wide,ActiveX control for streaming video,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\msvidc explorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11. plorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11.0 plorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11. Explorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11.0 plorer,System-wide,Microsoft® InfoTech Storage System Library,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\msvied,Explorer,System-wide,Microsoft (R) HTML Viewer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\mshtml.dll,11. Explorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11.0 ,Explorer,System-wide,Microsoft (R) HTML Viewer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\mshtml.dll,11.0. ,Explorer,System-wide,TBAuth protocol handler,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\tbauth.dll,10.0 plorer,System-wide,ActiveX control for streaming video,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\msvidc1 ,Explorer,System-wide,Microsoft (R) HTML Viewer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\mshtml.dll,11.0. ,enabled,Explorer,System-wide,TBAuth protocol handler,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\tbauth. nts, ,,,Logon, System-wide, ,,,,
nts,Microsoft Windows Media Player,enabled,Logon, System-wide, Microsoft Windows Media Player Setup Utility,(Verified) Microsoft Wind nts,Themes Setup,enabled,Logon, System-wide, Windows Theme API,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\ nts,Microsoft Windows Media Player,enabled,Logon, System-wide, Microsoft Windows Media Player Setup Utility,(Verified) Microsoft Wind nts,Windows Desktop Update,enabled,Logon, System-wide, Windows Shell Common Dll,(Verified) Microsoft Windows,Microsoft Corporation,c:\n nts,Web Platform Customizations,enabled,Logon, System-wide, IE Per-User Initialization Utility,(Verified) Microsoft Windows,Microsoft Corporation,n/a,enabled,Logon, System-wide,Microsoft .NET IE SECURITY REGISTRATION,(Verified) Microsoft Corporation,Microsoft Corporation,c:\pro nts,Google Chrome,enabled,Logon, System-wide, Google Chrome Installer,(Verified) Google LLC,Google LLC,c:\program files\google\chrome\ nts,Microsoft Edge,enabled,Logon, System-wide, Microsoft Edge Installer,(Verified) Microsoft Corporation,Microsoft Corporation,c:\pro lled Components, ,,,Logon, System-wide, ,,,,
lled Components,Microsoft Windows Media Player,enabled,Logon, System-wide, Microsoft Windows Media Player Setup Utility,(Verified) Mi lled Components,Microsoft Windows Media Player,enabled,Logon, System-wide, Microsoft Windows Media Player Setup Utility,(Verified) Mi lled Components,n/a,enabled,Logon, System-wide, Microsoft .NET IE SECURITY REGISTRATION,(Verified) Microsoft Corporation,Microsoft Cor ows\IconServiceLib, ,,,Logon, System-wide, ,,,,
ows\IconServiceLib,IconCodecService.dll,enabled,Logon, System-wide, Converts a PNG part of the icon to a legacy bmp icon,(Verified) Mi r\ShellServiceObjects, ,,,Explorer, System-wide, ,,,,
r\ShellServiceObjects, Published Items Shell Service Object,enabled,Explorer, System-wide, Windows Shell Common Dll,(Verified) Microso r\ShellServiceObjects,Microsoft VolumeControlService Class,enabled,Explorer, System-wide, SCA Volume,(Verified) Microsoft Windows,Micr r\ShellServiceObjects,Windows To Go Shell Service Object,enabled,Explorer, System-wide, Windows To Go Shell Service Object,(Verified) r\ShellServiceObjects," {566296fe-e0e8-475f-ba9c-a31ad31620b1}",enabled,Explorer, System-wide, Device Stage Shell Extension,(Verified) r\ShellServiceObjects,Cloud Cache Invalidator SSO,enabled,Explorer, System-wide, Cloud Data Store,(Verified) Microsoft Windows,Microsoft r\ShellServiceObjects,UnexpectedShutdownReason,enabled,Explorer, System-wide, Systray shell service object,(Verified) Microsoft Windo

```

MD5 OF EXE:

DESKTOP-IECJWJI Connected admin

State	FlowId	Artifacts	Created	Last Active	Creator	File	Size
✓	F_COVTP74013924	Windows.System.Plist	2024-05-11T21:01:16Z	2024-05-11T21:01:16Z	admin	0 b	95
✓	F_COV1LOC285364	Windows.System.Internal.Autorun	2024-05-11T20:52:17Z	2024-05-11T20:54:07Z	admin	0 b	1346
✓	F_COVSNRM2J308	Windows.EventLog.ExchHunter	2024-05-11T20:09:39Z	2024-05-11T20:09:39Z	admin	0 b	0
✓	F_COVSNPMMJHS	Windows.Search.Yara	2024-05-11T19:48:39Z	2024-05-11T19:49:37Z	admin	0 b	0
✓	F_COV12PHY30U	Windows.Search.Yara	2024-05-11T19:39:59Z	2024-05-11T19:40:54Z	admin	0 b	0
✓	F_COV3ST3739PC	Windows.System.DNSCache	2024-05-11T19:35:19Z	2024-05-11T19:35:21Z	admin	0 b	2
✓	F_COVSAF4TII0	Generic Client Data	2024-05-11T19:12:40Z	2024-05-11T19:12:40Z	InteractionsService	0 b	0

Artifact Collection Uploaded Files Requests Results Log Notebook

Windows.System.Plist

Pid	Ppid	TokenElevated	Base	CommandLine	Exe	TokenInfo	Hash	Authenticode	Username	WorkingSetSize
4	0	False	System				✓ { "000": "0d1d8cd8f80902a90a900000980c78c27e", "500": "0a3fa30e6edab40bd32551fe05501898a0d8709", "": "" }			129264
72	4	False	Registry				✓ { "000": "0d1d8cd8f80902a90a900000980c78c27e", "500": "0a3fa30e6edab40bd32551fe05501898a0d8709", "": "" }	NT AUTHORITY\SYSTEM		20848040

2024-05-11T21:02:02Z

YARA:

DESKTOP-IECJWJI 17 seconds ago admin

State	FlowId	Artifacts	Created	Last Active	Creator	File	Size
✓	F_COVTP74013924	Windows.Search.Yara	2024-05-11T21:01:05	2024-05-11T21:01:12Z	admin	0 b	1
✓	F_COVTP74013924	Windows.System.Plist	2024-05-11T21:01:16Z	2024-05-11T21:01:36Z	admin	0 b	95
✓	F_COV1LOC285364	Windows.System.Internal.Autorun	2024-05-11T20:52:11Z	2024-05-11T20:54:07Z	admin	0 b	1346
✓	F_COVSNRM2J308	Windows.EventLog.ExchHunter	2024-05-11T20:09:36Z	2024-05-11T20:09:39Z	admin	0 b	0
✓	F_COVSNPMMJHS	Windows.Search.Yara	2024-05-11T19:48:39Z	2024-05-11T19:49:37Z	admin	0 b	0
✓	F_COV12PHY30U	Windows.Search.Yara	2024-05-11T19:39:59Z	2024-05-11T19:40:54Z	admin	0 b	0
✓	F_COV3ST3739PC	Windows.System.DNSCache	2024-05-11T19:16:36	2024-05-11T19:16:37Z	admin	0 b	3

Artifact Collection Uploaded Files Requests Results Log Notebook

Windows.Search.Yara

Rule	HitOffset	HitContext	FileName	Size	ModTime	Upload
Hit	En44	P V N E D	\ \ \C\ \wpimessage.exe	18248	2024-05-18T18:55:36Z	

10 25 30 50 Showing 1 to 1 of 1

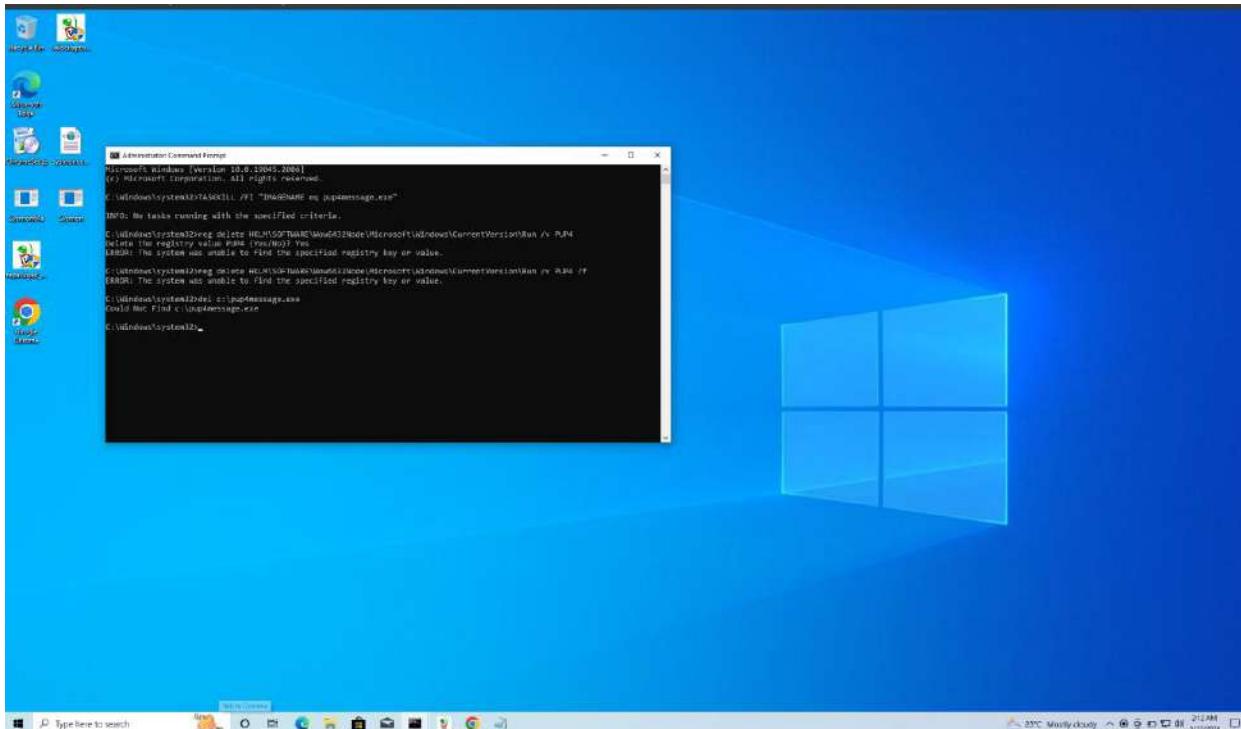
REMEDIATION:



```
DESKTOP-1ECCB83 Connected
PowerShell * del c:\pup4message.exe
del c:\pup4message.exe
Logs
reg delete HKEY\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v pup4 /f
The operation completed successfully.

Logs
taskkill /FI "IMAGENAME eq pup4message.exe"
INFO: No tasks running with the specified criteria.

Logs
```

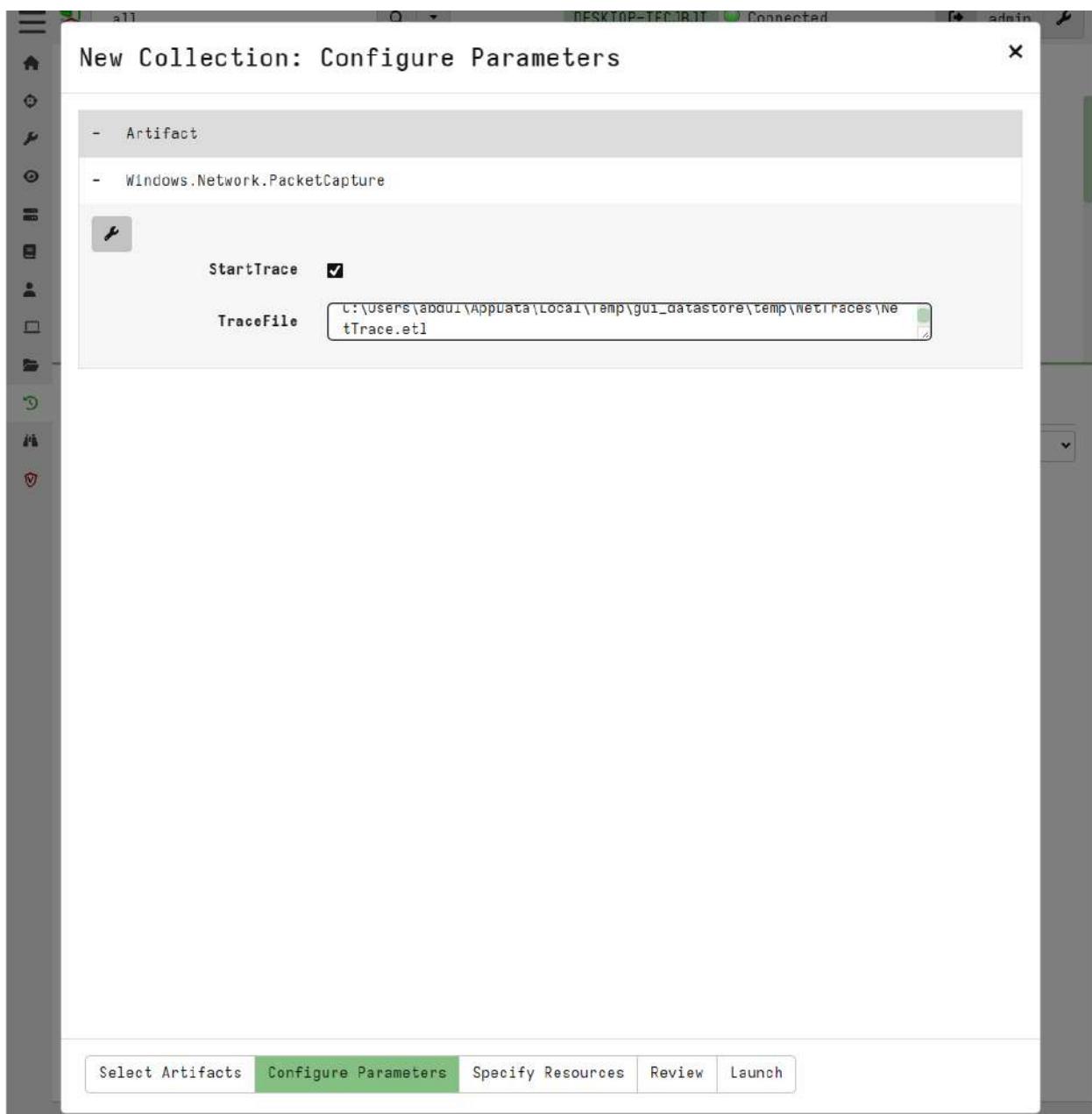


19. Investigating a Bot with Velociraptor

CAPTURING NETWORK TRAFFIC REMOTELY:

The screenshot shows the Velociraptor interface with the following details:

- Header:** Shows the connection status as "Connected" to "DESKTOP-IECJBJI" and the user "admin".
- Table:** A table listing captured artifacts. The columns are: State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows. The table contains four rows of data.
- Artifact Collection:** A tabbed section showing "Results" which is selected. It displays the artifact type as "Windows.Network.PacketCapture".
- File Path:** The file path shown is "C:\Users\abdul\AppData\Local\Temp\gui_datastore\temp\NetTraces\NetTrace.etl".
- Pagination:** Shows "Showing 1 to 1 of 1".
- Timestamp:** The timestamp at the bottom right is "2024-05-12T09:28:16Z".



CAPTURING FILES:

Screenshot of a network analysis tool interface showing captured files and artifacts.

Top Bar:

- Search bar: **all**
- Connected status: **DESKTOP-IECJBJI Connected**
- User: **admin**

Captured Files Table:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP0802236CU4	Windows.Network.PacketCapture	2024-05-12T09:29:44Z	2024-05-12T09:31:20Z	admin	58 Mb	4
✓	F.CP08M0D0FUHE	Windows.Network.PacketCapture	2024-05-12T09:26:57Z	2024-05-12T09:27:14Z	admin	0 b	1
✓	F.COVTSQLQ10U84	Windows.System.PowerShell	2024-05-11T21:08:31Z	2024-05-11T21:08:32Z	admin	0 b	1
✓	F.COVTSCG4RJ6S	Windows.System.PowerShell	2024-05-11T21:08:02Z	2024-05-11T21:08:03Z	admin	0 b	1

Artifact Collection Table:

Timestamp	started	vfs_path	Type	file_size	uploaded_size	Preview
1715506285	2024-05-12 09:31:25.3110634 +0000 UTC	C:\Users\abdul\AppData\Local\Temp\gui_datastore\temp\tmp3578561919.pcapng		29626836	29626836	
1715506292	2024-05-12 09:31:32.2004936 +0000 UTC	C:\Users\abdul\AppData\Local\Temp\gui_datastore\temp\NetTraces\NetTrace.etl		31457280	31457280	

Pagination: Showing 1 to 2 of 2

Timestamp: 2024-05-12T09:32:25Z

CREATING. PCAPNG FILES:

USER-AGENT:

The screenshot shows a Wireshark capture window with the following details:

- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephone, Wireless, Tools, Help.
- Toolbar:** Undo, Redo, Cut, Copy, Paste, Delete, Select, Find, Replace, Filter, Stop, Refresh, Stop Capturing, Stop All, Stop All, Stop All.
- Http requestMethod == "GET"** filter applied.
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info.
- Table Data:** A list of approximately 1000 GET requests from various IP addresses (e.g., 151.139.31.158, 172.24.10.1) to the same destination port (12345). The requests are timestamped between May 12, 2024, and May 13, 2024.
- Severity level: Chat**
- Group: Sequence**
- Request Method: GET**
- Request URI [truncated]: /filestreamingservice/files/225ca989-c169-475b-86af-e2c45c825eca?P1=17155213978P2=4048P3=2&P4=c89..**
- Request URI Path: /filestreamingservice/files/225ca989-c169-475b-86af-e2c45c825eca**
- Request URI Query: P1=17155213978P2=4048P3=2&P4=c89..**
- Request URI Query Parameter: P1=17155213978P2=4048P3=2&P4=c89..**
- Request URI Query Parameter: P2=4048**
- Request URI Query Parameter: P3=2**
- Request URI Query Parameter: P4=c89..**
- Request URI Query Parameter: cachedHostOriginal=1.tlu.d1.delivery.mp.microsoft.com**
- Request Version: HTTP/1.1**
- Connection: Keep-Alive\r\n**
- Accept: */*\r\n**
- Range: bytes=598690524-598736895\r\n**
- User-Agent: Microsoft-Delivery-Optimization/10.0\r\n**
- MS-CV: DgJ0h1/KUkL79688.1.1.55.2.14.3.1.445\r\n**
- Content-Length: 0\r\n**
- Host: 151.139.31.158\r\n**
- \r\n**
- [HTTP request 1/109]**
- [Response 1/109]**
- [Next Request in frame 128]**

DNS CACHE:

```
securityreport 198.199.94.12      A          219      Success      Answer
.samsclass.inf

0
```

BEACONING EXE:

The screenshot shows the NetworkMiner interface with the following details:

Top Bar: Shows "all" selected in the search bar, a connected status for "DESKTOP-IECJBJI", and the user "admin".

Main Table: Displays a list of artifacts found in the session.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP09C9RR5L88	Windows.Search.Yara A	2024-05-12T10:12:55Z	2024-05-12T10:13:48Z	admin	0 b	1
✓	F.CP094V5BENKD	Windows.System.DNSCache 4	2024-05-12T09:57:16Z	2024-05-12T09:57:18Z	admin	0 b	33
✓	F.CP093Q81VQ6I	Windows.System.DNSCache 4	2024-05-12T09:54:49Z	2024-05-12T09:54:51Z	admin	0 b	33
✓	F.CP0802236CU4	Windows.Network.PacketCapture G	2024-05-12T09:29:44Z	2024-05-12T09:31:20Z	admin	58 Mb	4

Artifact Collection Table: Shows a single hit for "Windows.Search.Yara".

Rule	HitOffset	HitContext	FileName	Size	ModTime	Upload
secrep	51471	securityreport	\.\.\C:\PUP\security\securityte st.exe	96256	2021-07-21T15:14:42Z	

Pagination: Shows page 1 of 1.

Timestamp: 2024-05-12T10:14:09Z

SYMON INSTALLATION:

WINDOWS.EVENTLOGS. EVTXHUNTER:

EventTime	Computer	Channel	Provider	EventID	EventRecordID	UserSID	Username	UserData	LogPath
2024-05-12T11:22:02Z	DESKTOP-IECJ0J1	Microsoft-Windows-Sysmon\Operational	Microsoft-Windows-Sysmon	11	2464	S-1-5-18	SYSTEM		C:\Windows\System32\vinet\Logs\Microsoft-Windows-Sysmon\Operational.evtx
2024-05-12T11:22:02Z	DESKTOP-IECJ0J1	Microsoft-Windows-Sysmon\Operational	Microsoft-Windows-Sysmon	11	2465	S-1-5-18	SYSTEM		C:\Windows\System32\vinet\Logs\Microsoft-Windows-Sysmon\Operational.evtx

PARENT COMMND LINE:

SCHEDULED TASKS:

State	FlowID	Artifacts	Created	Last Active	Creator	Mo	Row
✓	F_CPAHF00007C	Windows.System.TaskScheduler	2024-05-12T11:32:16Z	2024-05-12T11:32:27Z	admin	0 h	203
✓	F_CPAHF00007C	Windows.EventLogs.EvtxHunter	2024-05-12T11:28:59Z	2024-05-12T11:29:04Z	admin	0 h	2
✓	F_CPAHF00007C	Windows.EventLogs.EvtxHunter	2024-05-12T11:28:59Z	2024-05-12T11:27:18Z	admin	0 h	0
✓	F_CPAHF00007C	Windows.Search.Yara	2024-05-12T09:52:06Z	2024-05-12T09:52:08Z	admin	0 h	1
✓	F_CPAHF00007C	Windows.System.DNSCache	2024-05-12T09:52:16Z	2024-05-12T09:57:18Z	admin	0 h	33
✓	F_CPAHF00007C	Windows.System.DNSCache	2024-05-12T09:54:49Z	2024-05-12T09:54:51Z	admin	0 h	33
✓	F_CPAHF00007C	Windows.Network.PacketCapture	2024-05-12T09:26:17Z	2024-05-12T09:27:14Z	admin	0 h	4
✓	F_CPAHF00007C	Windows.Network.PacketCapture	2024-05-12T09:26:17Z	2024-05-12T09:27:14Z	admin	0 h	1

HUNTS:

The screenshot shows the 'New Hunt - Configure Hunt' dialog box. The 'Description' field contains 'Detect securitytest beaconer'. The 'Expiry' field shows '19/5/2024 16:34'. The 'Include Condition' dropdown is set to 'Run everywhere'. The 'Exclude Condition' dropdown is also set to 'Run everywhere'. Under 'Orgs', 'All Orgs' is selected. The 'Hunt State' section has an unchecked checkbox for 'Start Hunt Immediately'. Below this, a green bar displays 'Estimated affected clients 1' and a dropdown menu set to 'All known Clients'. At the bottom, there are tabs: 'Configure Hunt' (which is green), 'Select Artifacts', 'Configure Parameters', 'Specify Resources', 'Review', and 'Launch'.

Create Hunt: Configure artifact parameters

Filter artifact parameter

EvtxGlob	%SystemRoot%\System32\Winevt\Logs*.evtx
IocRegex	securitytest
WhitelistRegex	? for suggestions
PathRegex	.
ChannelRegex	.
ProviderRegex	.
IdRegex	.
VSSAnalysisAge	0
DateAfter	12/05/2024 4:31 <input type="checkbox"/> UTC Now
DateBefore	--/--/---- --:-- <input type="checkbox"/> UTC Now

- Windows.System.TaskScheduler

TasksPath	c:/Windows/System32/Tasks/SecurityScript
AlsoUpload	<input type="checkbox"/> If set we also upload the task XML files.
UploadCommands	<input type="checkbox"/> If set we attempt to upload the commands that are mentioned in the scheduled tasks

- Windows.System.DNSCache

Configure Hunt Select Artifacts **Configure Parameters** Specify Resources Review Launch

2024-05-12T11:35:43Z

The screenshot shows the Splunk Hunt interface. A modal dialog box is centered over the main content area, asking "Run this hunt?". Below the dialog, the main page displays a table of hunts. One specific hunt is highlighted, showing its details in the center pane. The hunt has the following parameters:

Artifact Names	Windows.EventLogs.EvtxHunter Windows.System.TaskScheduler Windows.System.DNSCache
Hunt ID	H.CP0AJITP4BS9K
Creator	admin
Creation Time	2024-05-12T11:36:43Z
Expiry Time	2024-05-19T11:34:12Z
State	PAUSED
Ops/Sec	Unlimited
CPU limit	Unlimited
IOPS Limit	Unlimited

The "Parameters" section lists the selected artifacts: Windows.EventLogs.EvtxHunter, IocRegex securitytest, DataAfter 2024-05-12T04:31:00Z, Windows.System.TaskScheduler, TasksPath c:/Windows/System32/Tasks/SecurityScript, and Windows.System.DNSCache.

The "Results" pane indicates 0 scheduled clients and 0 download results. A "Select a download method" dropdown is present.

The bottom right corner of the main pane shows the timestamp 2024-05-12T11:38:12Z.

TASKSCHEDULER /ANALYSIS:

		all	Search	DESKTOP-IECJOBJI Connected		User
				+	Filter	Home
				Save	Print	Logout
State	HuntId	Description	Created	Started	Expires	Scheduled Creator
X	H.CP0AJITP4BS 9K	Detect securitytest beaconer	2024-05-12T11:36:43Z	2024-05-12T11:38:37Z	2024-05-19T11:34:12Z	1 admin
10 25 30 50	Showing 1 to 1 of 1		«	8	»	Goto Page
10 25 30 50	Showing 1 to 4 of 4		«	8	»	Goto Page

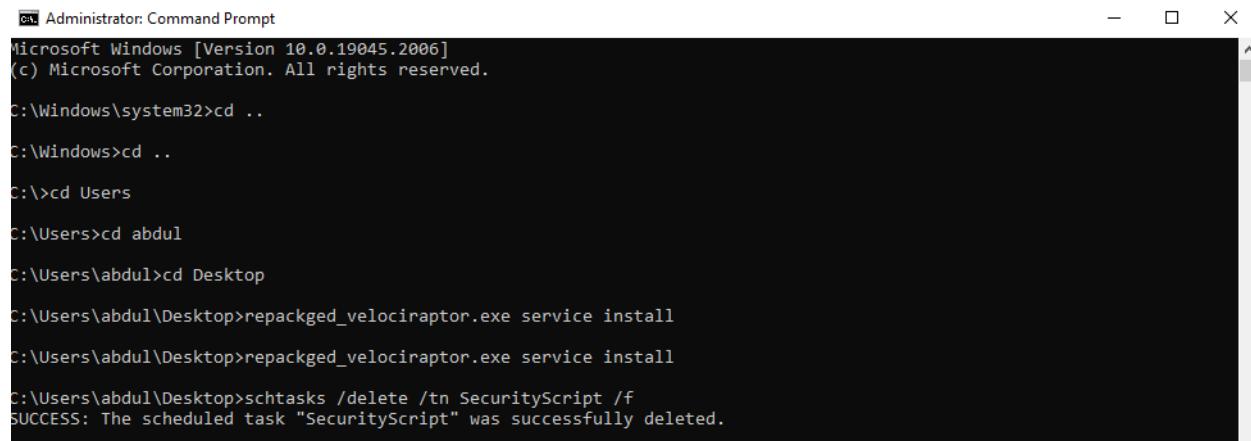
Windows.System.TaskScheduler/Analysis

DSPATH	COMMAND	EXPANDED COMMAND	ARGUMENTS	COMMAND HANDLER	USER ID	
C:\Windows\System32\Tasks\SecurityScript	C:\Users\abdul\Downloads\security\securitytest.exe	C:\Users\abdul\Downloads\sec ds\security\securityt est.exe			DESKTOP-IECJOBJI\abdul	
10 25 30 50	Showing 1 to 1 of 1		«	8	»	Goto Page

Windows.System.DNSCache

NAME	RECORD	RECORD TYPE	TTL	QUERY STATUS	SECTION TYPE	FLOW ID
132.209.58.216.in-	arn09s05-in-f4.1e100.net.	PTR	59099	Success	Answer	F.CP0AJI9K.H
						2024-05-12T11:39:35Z

REMEDIATION:



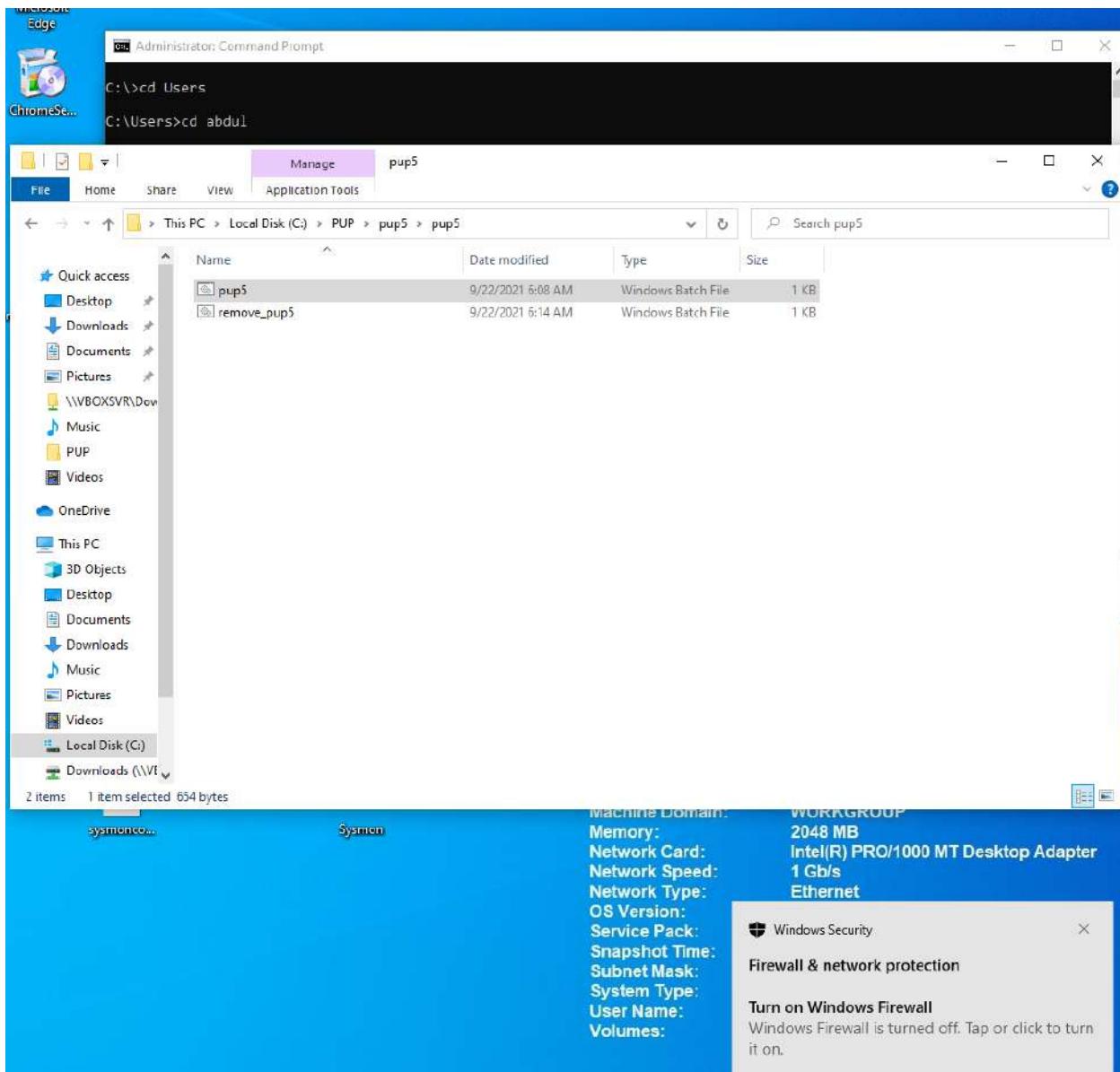
The screenshot shows an Administrator Command Prompt window on a Windows 10 system. The command history is as follows:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
C:\Windows>cd ..
C:\>cd Users
C:\Users>cd abdul
C:\Users\abdul>cd Desktop
C:\Users\abdul\Desktop>repackged_velociraptor.exe service install
C:\Users\abdul\Desktop>repackged_velociraptor.exe service install
C:\Users\abdul\Desktop>schtasks /delete /tn SecurityScript /f
SUCCESS: The scheduled task "SecurityScript" was successfully deleted.
```

20. Investigating a Two-Stage RAT with Velociraptor

INSTALLING RAT:



AUDITING AUTORUNS:

Screenshot of the X-Shell interface showing audit results for Autoruns.

Artifact Collection:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP0AS2JE5GFAC	Windows.Network.Netstat	2024-05-12T11:54:58Z	2024-05-12T11:54:52Z	admin	0 b	112
✓	F.CP0AJITP4BS9K	Windows.EventLogs.EvtxH .H unter Windows.System.TaskSche duler Windows.System.DNSCache	2024-05-12T11:38:37Z	2024-05-12T11:38:52Z	admin	0 b	46
✓	F.CP0AHFS0PKFTQ	Windows.System.TaskSche	2024-05-	2024-05-	admin	0 b	203

Results:

Windows.Network.Netstat

Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr
824	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	135	0.0.0
4	System	IPv4	TCP	LISTEN	10.0.2.15	139	0.0.0
756	shellbind.e xe	IPv4	TCP	LISTEN	0.0.0.0	4444	0.0.0
1860	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5040	0.0.0
6064	velociraptor r-v0.72.1- windows- amd64.exe	IPv4	TCP	LISTEN	127.0.0.1	8000	0.0.0
6064	velociraptor r-v0.72.1- windows- amd64.exe	IPv4	TCP	ESTAB	127.0.0.1	8000	127.0
6064	velociraptor r-v0.72.1- windows- amd64.exe	IPv4	TCP	ESTAB	127.0.0.1	8000	127.0
6064	velociraptor	IPv4	TCP	ESTAB	127.0.0.1	8000	127.0

2024-05-12T11:55:06Z

SHELLBIND.EXE PATH:

```
ption": "Shell Light-weight Utility Library", "Signer": "(Verified) Microsoft Windows", "Compa  
tion": "Multi-User Windows USER API Client DLL", "Signer": "(Verified) Microsoft Windows", "Com  
ption": "Win32 LDAP API DLL", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Co  
": "", "Company": "", "Image Path": "c:\\windows\\syswow64\\wow64.dll", "Version": "", "Launch Stri  
ner": "", "Company": "", "Image Path": "c:\\windows\\syswow64\\wow64win.dll", "Version": "", "Launc  
tion": "Windows Socket 2.0 32-Bit DLL", "Signer": "(Verified) Microsoft Windows", "Company": "Mi  
": "", "Company": "", "Image Path": "", "Version": "", "Launch String": "", "MD5": "", "SHA-1": "", "PESH  
ription": "Windows Explorer", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Co  
, "Company": "", "Image Path": "", "Version": "", "Launch String": "", "MD5": "", "SHA-1": "", "PESHA-1"  
"Windows Command Processor", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Co  
", "Image Path": "", "Version": "", "Launch String": "", "MD5": "", "SHA-1": "", "PESHA-1"  
"Windows Security notification icon", "Signer": "(Verified) Microsoft Windows", "Company": "Microso  
x Guest Additions Tray Application", "Signer": "(Verified) Microsoft Windows Hardware Compati  
r": "", "Company": "", "Image Path": "c:\\shellbind\\shellbind.exe", "Version": "", "Launch String"  
"Path": "", "Version": "", "Launch String": "", "MD5": "", "SHA-1": "", "PESHA-1": "", "PESHA-256": "", "  
ewer", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Image Path  
n32", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Image Path"  
eaming video", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Im  
in32", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Image Path  
n32", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Image Path"  
in32", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Image Path  
Win32", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporation", "Image Pat  
rage System Library", "Signer": "(Verified) Microsoft Windows", "Company": "Microsoft Corporati  
MI Viewer" "Signer": "(Verified) Microsoft Windows" "Company": "Microsoft Corporation" "Image
```

CREATION TIME:

Screenshot of a log viewer application showing a list of artifacts and their details, along with a detailed log entry for a PowerShell session.

Artifacts Table Headers:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
-------	--------	-----------	---------	-------------	---------	----	------

Artifacts Data:

✓	F.CP0AUNGSMBQP6	Windows.System.PowerShe ll	2024-05-11	2024-05-12T12:00:30Z	admin	0 b	1
✓	F.CP0AUAU37957U	Windows.System.PowerShe ll	2024-05-11	2024-05-12T11:59:39Z	admin	0 b	1
✓	F.CP0ASH6UH2I4G	Windows.Sysinternals.Au toruns	2024-05-12T11:55:48Z	2024-05-12T11:56:57Z	admin	0 b	1351
✓	F.CP0AS2JE5GFAC	Windows.Network.Netstat	2024-05-12T11:54:50Z	2024-05-12T11:54:52Z	admin	0 b	112

Log Entry (Stdout):

```
#< CLIXML <Objs Version="1.1.0.1"
  xmlns="http://schemas.microsoft.com/powershell/2004
  /04"><Obj S="progress" RefId="0"><TN RefId="0">
<T>System.Management.Automation.PSCustomObject</T>
<T>System.Object</T></TN><MS><I64
N="SourceId">1</I64><PR N="Record"><AV>Preparing
modules for first use.</AV><AI>0</AI><N1 />
<PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR>
<SD> </SD><PR></PR><Obj><S S="Error">dir : Cannot
find path 'C:\c:\shellbind\shellbind.exe' because
it does not exist._x000D__x000A_</S><S S="Error">At
line:1 char:1_x000D__x000A_</S><S S="Error">+ dir
C:/c/\shellbind\shellbind.exe_x000D__x000A_</S><S
S="Error">+
~~~~~_x000D__x000A_</
S><S S="Error"> + CategoryInfo : ObjectNotFound:
(C:\c:\shellbind\shellbind.exe:String) [Get-
ChildItem], ItemNotFoundException_x000D__x000A_</S><S
S="Error">ption_x000D__x000A_</S><S S="Error"> +
FullyQualifiedErrorId :
PathNotFound,Microsoft.PowerShell.Commands.GetChild
ItemCommand_x000D__x000A_</S><S S="Error">
_x000D__x000A_</S></Obj>
```

Log Footer:

Showing 1 to 1 of 1 Goto Page 8 2024-05-12T12:01:18Z

PREFETCH:

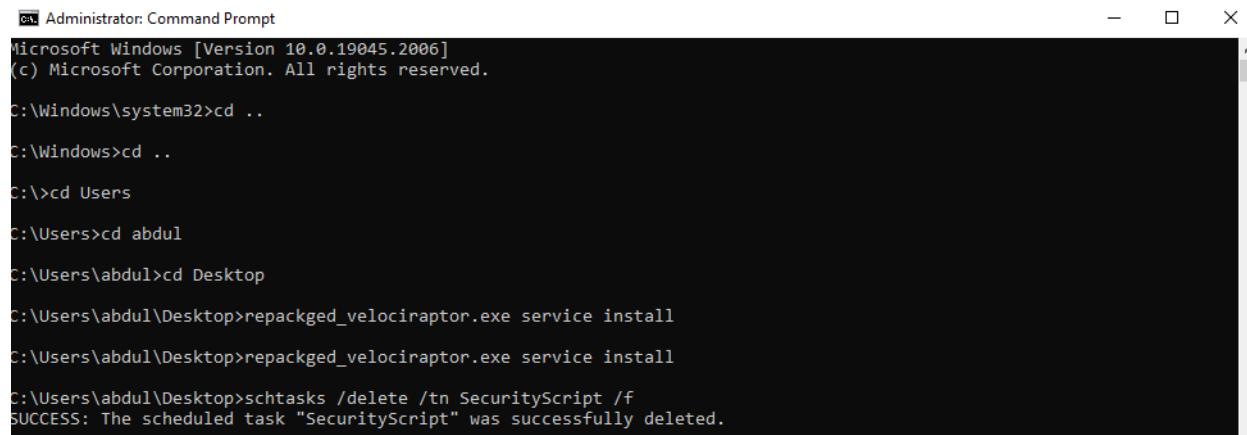
The screenshot shows the Volatility Forensics interface with the following details:

- Header:** DESKTOP-IECJBJI Connected admin
- Toolbar:** Includes icons for file operations like New, Open, Save, Print, etc.
- Table:** Shows a list of Prefetch artifacts with columns: State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP0AVKNEH5QFU	Windows.Forensics.Prefetch	2024-05-12T12:02:26Z	2024-05-12T12:02:30Z	admin	0 b	1
✓	F.CP0AUNGSMBQP6	Windows.System.PowerShell	2024-05-11T12:00:30Z	2024-05-12T12:00:30Z	admin	0 b	1
✓	F.CP0AUUAU37957U	Windows.System.PowerShell	2024-05-11T11:59:39Z	2024-05-12T11:59:41Z	admin	0 b	1
✓	F.CP0ASH6UH2I4G	Windows.Systeminternals.Authoruns	2024-05-12T11:55:48Z	2024-05-12T11:56:57Z	admin	0 b	1351
- Bottom Navigation:** Buttons for Artifact Collection, Uploaded Files, Requests, Results (highlighted), Log, and Notebook.
- Artifact Details:** A large panel below shows the structure of a selected Prefetch artifact (SHELLBIND.EXE) with its properties and last run times.
- Timestamp:** 2024-05-12T12:02:46Z

SYSMON LOGS:

```
0", "ProcessId":424, "Image": "C:\\Windows\\System32\\svchost.exe", "TargetObject": "\\REGISTRY\\Id":424, "Image": "C:\\Windows\\System32\\svchost.exe", "TargetObject": "\\REGISTRY\\A\\{5d4560 reedge.net", "QueryStatus": "0", "QueryResults": "type: 5 fp-vp.ec.azureedge.net;type: 5 cs9. \\Downloads\\7z2301-x64.exe", "User": "DESKTOP-IECJBJI\\abdul"}, "Message": "Process terminated: 24, "Image": "C:\\Windows\\System32\\svchost.exe", "TargetObject": "HKU\\S-1-5-21-2084553860-39 } , "Image": "C:\\Windows\\Explorer.EXE", "TargetObject": "HKU\\S-1-5-21-2084553860-3995606750-26 ational.evtx"} es (x86)\\Google\\GoogleUpdater\\126.0.6462.0\\updater.exe", "FileVersion": "126.0.6462.0", "D -2B02-000000000C00!s!\nProcessId: 2596!s!\nImage: C:\\Program Files (x86)\\Google\\Up 24-05-12T11:48:40Z", "Channel": "Microsoft-Windows-Sysmon/Operational", "EventRecordID": 3672, "Explorer.EXE", "TargetFilename": "C:\\PUP\\pup5\\pup5\\pup5.bat", "CreationUtcTime": "2024-05-1 xplorer.EXE", "TargetFilename": "C:\\PUP\\pup5\\pup5\\remove_pup5.bat", "CreationUtcTime": "202 s (x86)\\Google\\GoogleUpdater\\126.0.6462.0\\updater.exe", "FileVersion": "126.0.6462.0", "De , "ParentProcessGuid": "13299C5D-AC98-6640-2B02-000000000C00", "ParentProcessId": 2596, "ParentI \"--attachment=C:\\Program Files (x86)\\Google\\GoogleUpdater\\updater.log\" --initial-cl \\\Microsoft-Windows-Sysmon%4Operational.evtx"}
```

REMEDIATION:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:>cd Users

C:\Users>cd abdul

C:\Users\abdul>cd Desktop

C:\Users\abdul\Desktop>repackged_velociraptor.exe service install
C:\Users\abdul\Desktop>repackged_velociraptor.exe service install

C:\Users\abdul\Desktop>schtasks /delete /tn SecurityScript /f
SUCCESS: The scheduled task "SecurityScript" was successfully deleted.
```