LAB FINAL EXAMINATION

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

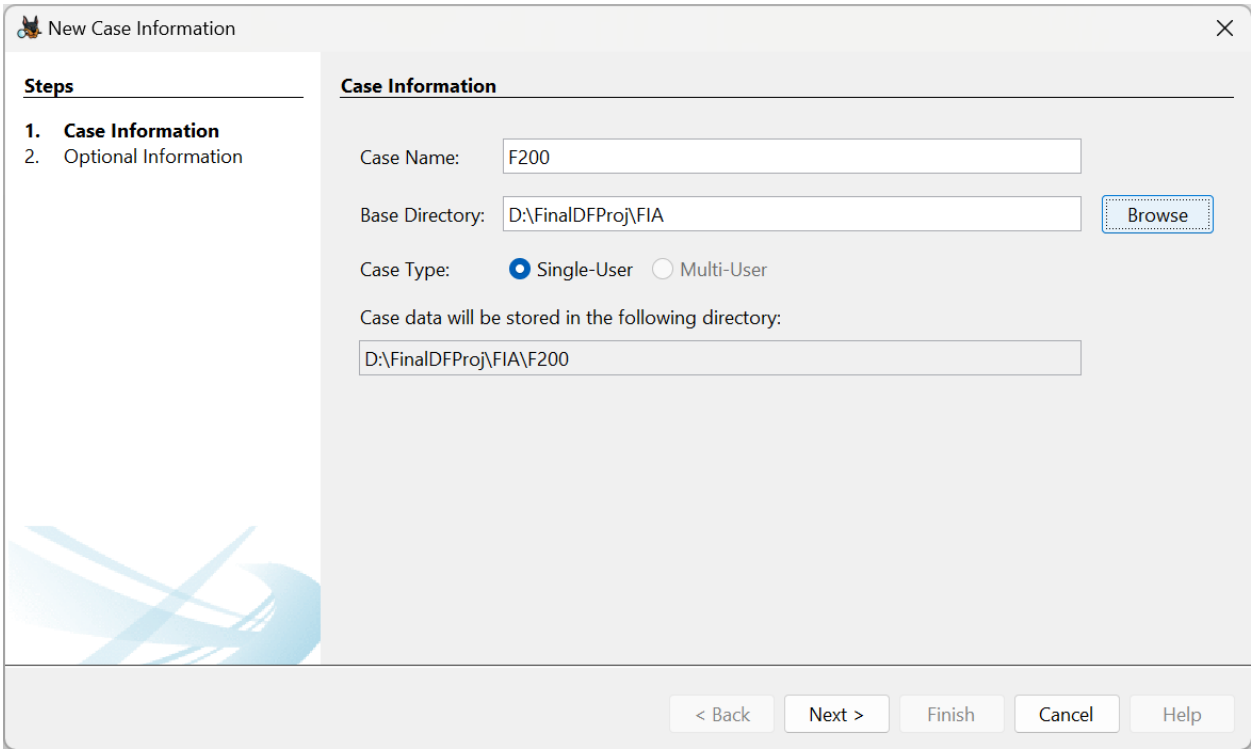
MAY 15, 2024

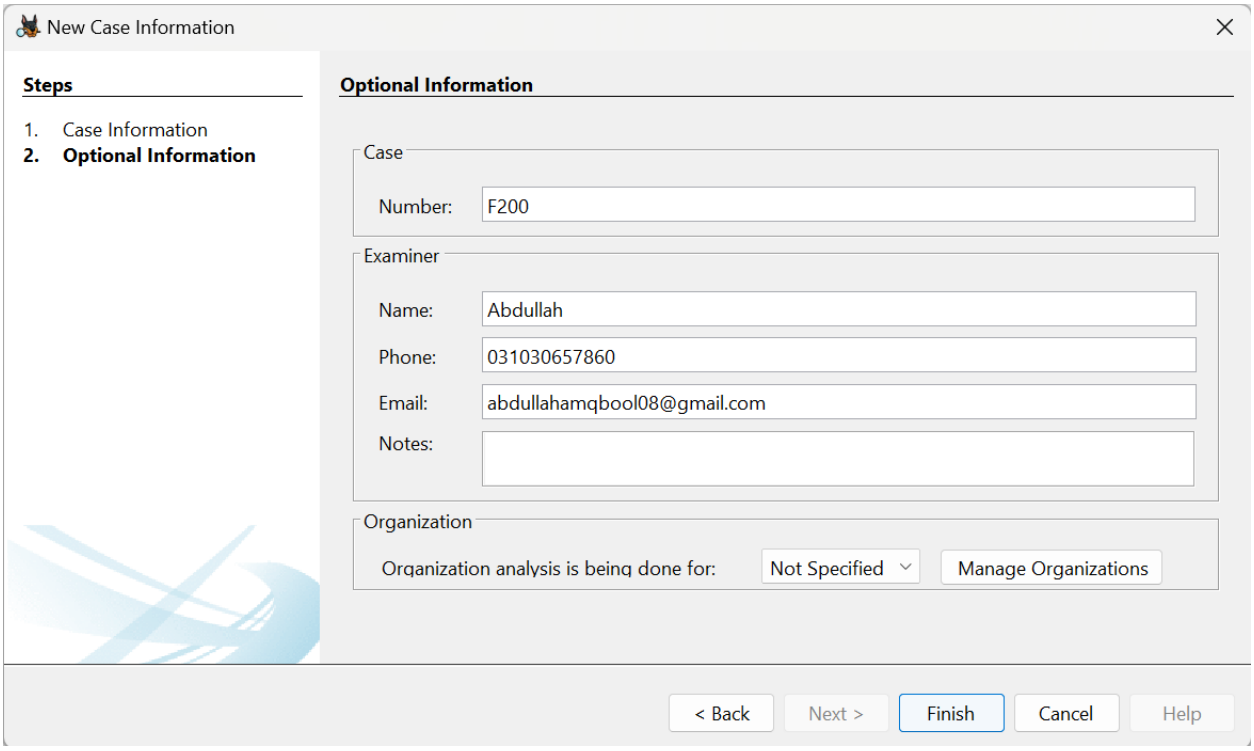
COMSATS UNIVERSITY
ISLAMABAD

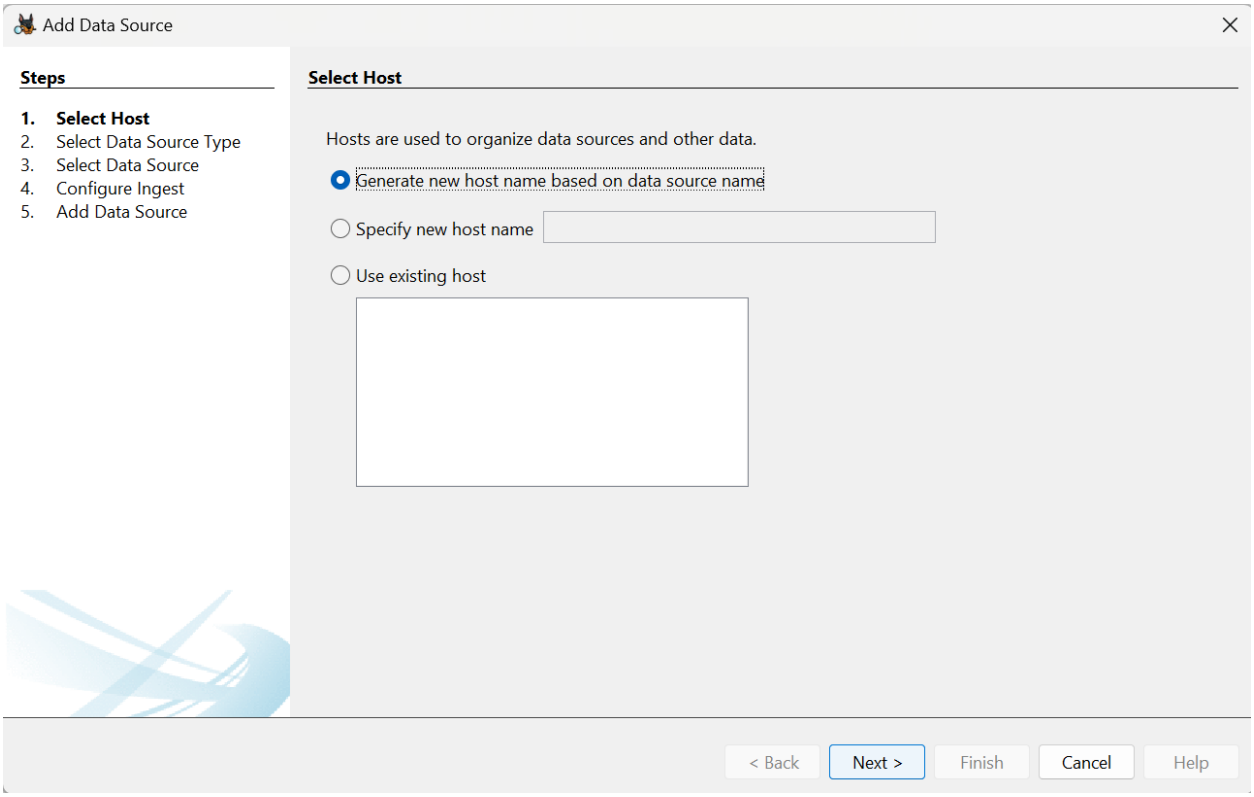
Contents

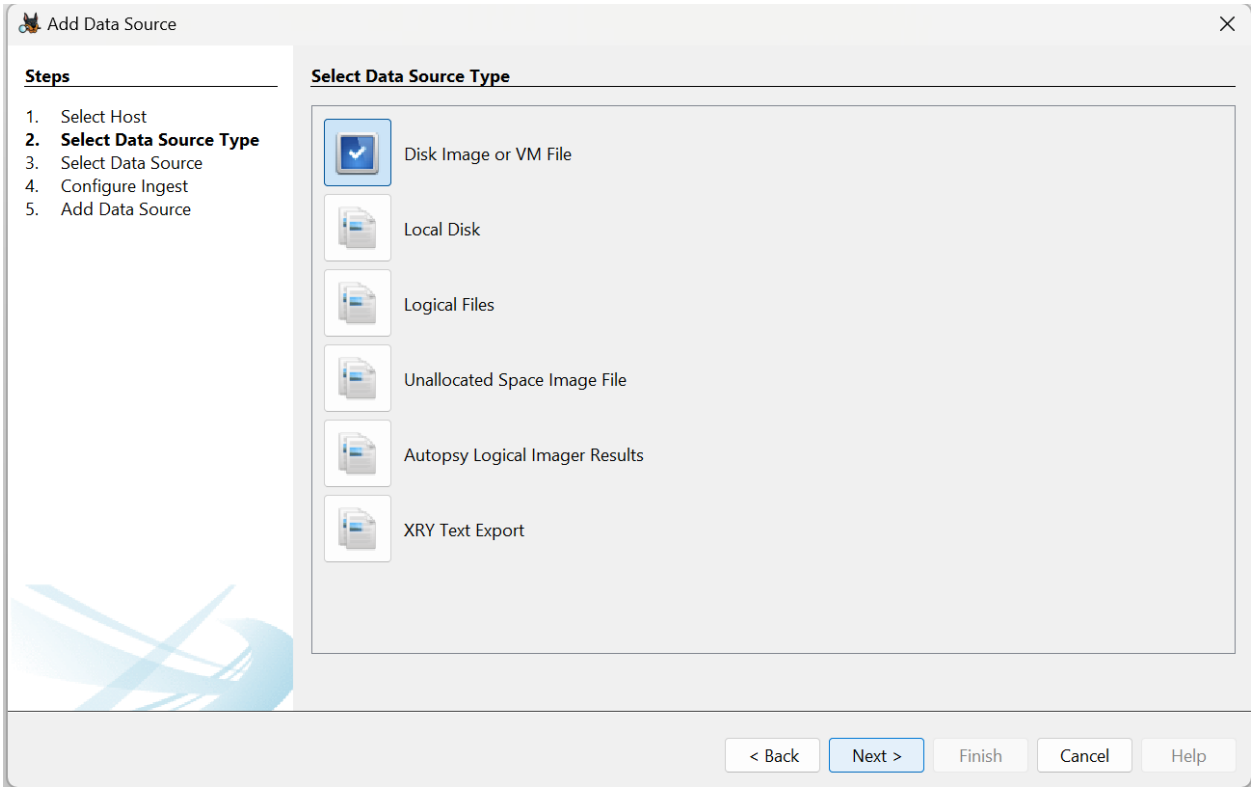
1. Examining a Forensic Image with Autopsy:

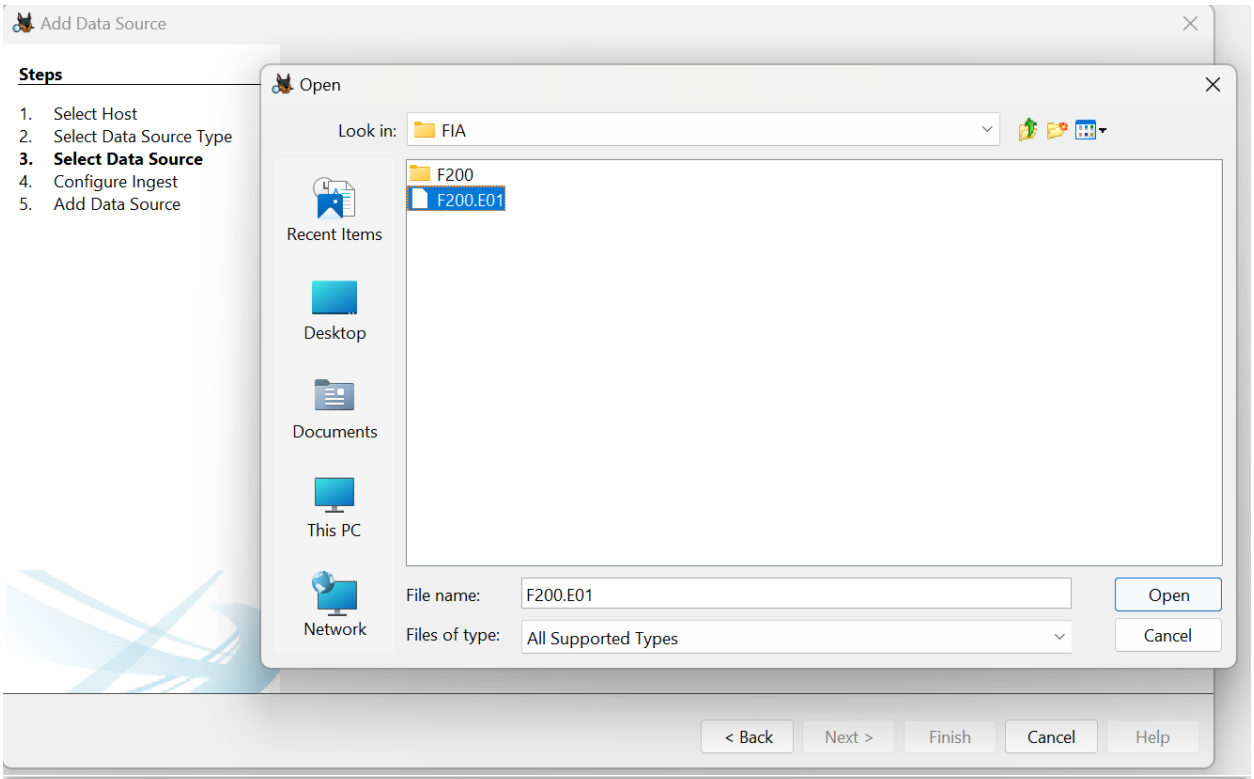
CREATING A CASE:

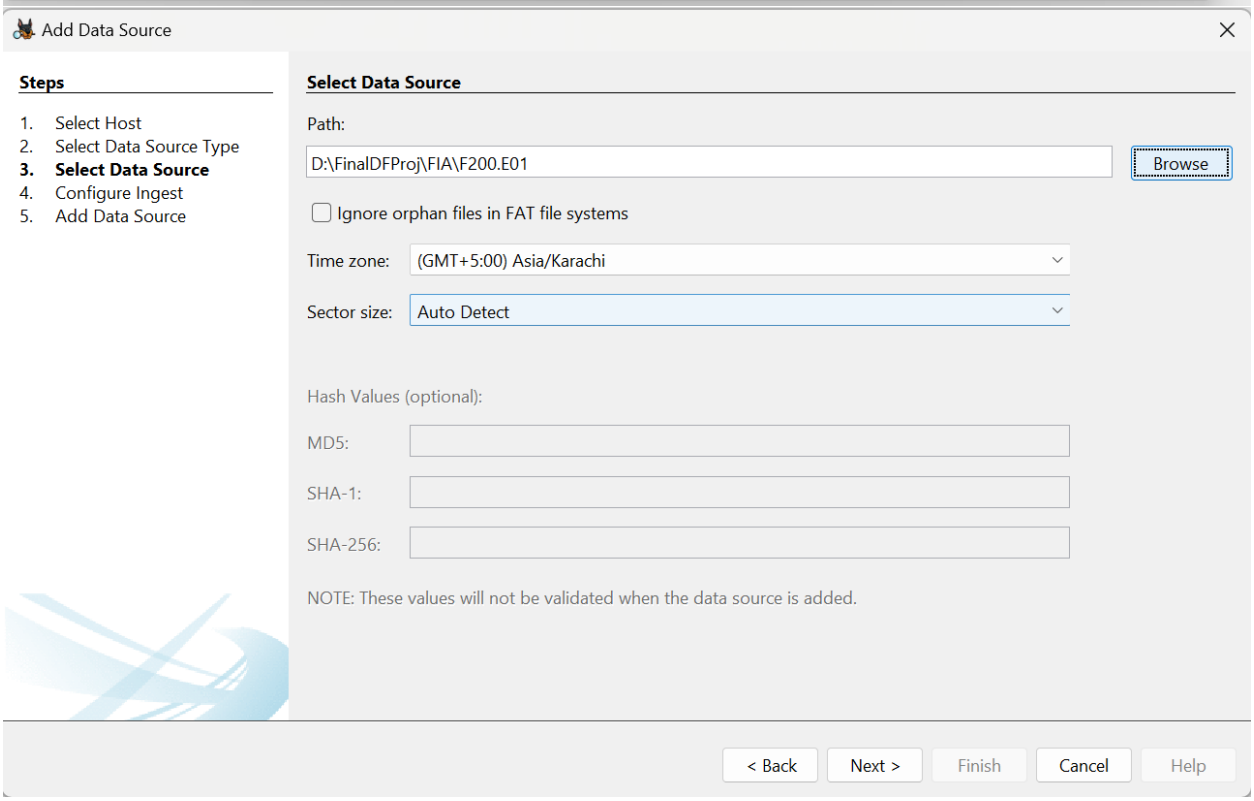


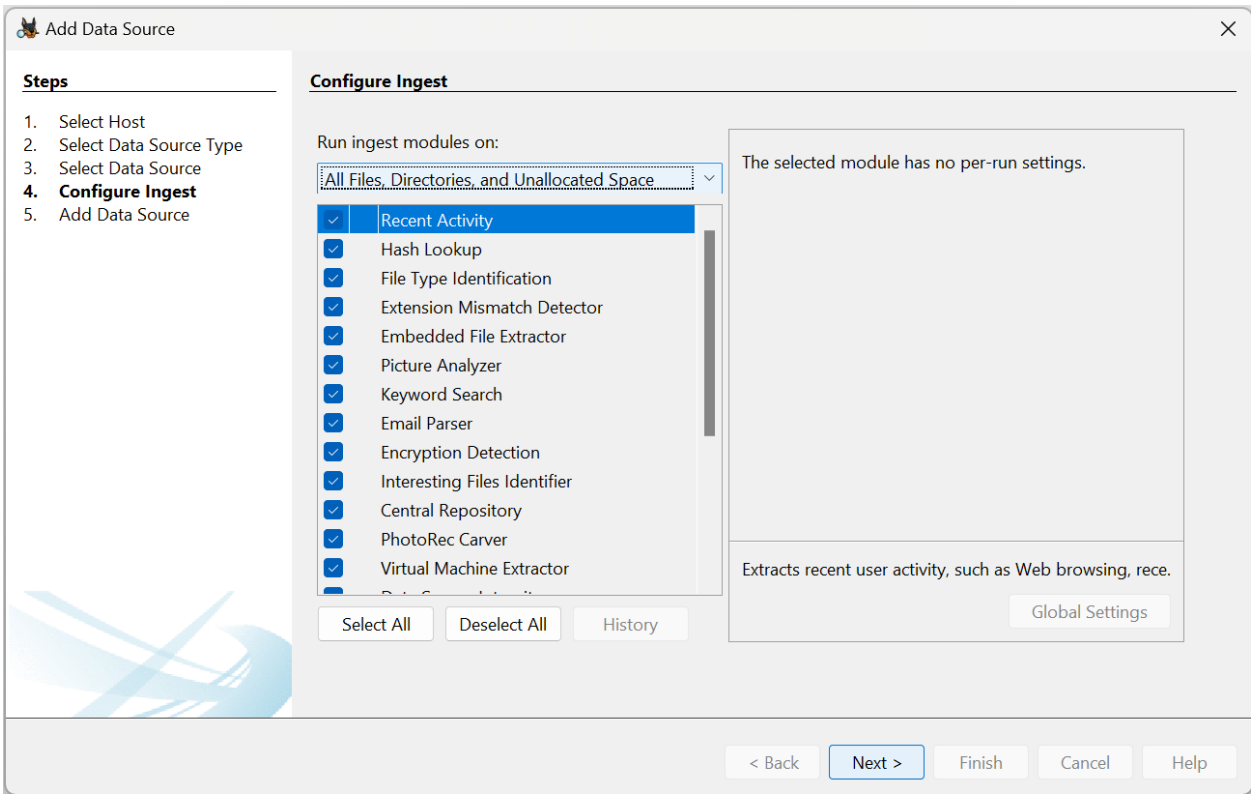



Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

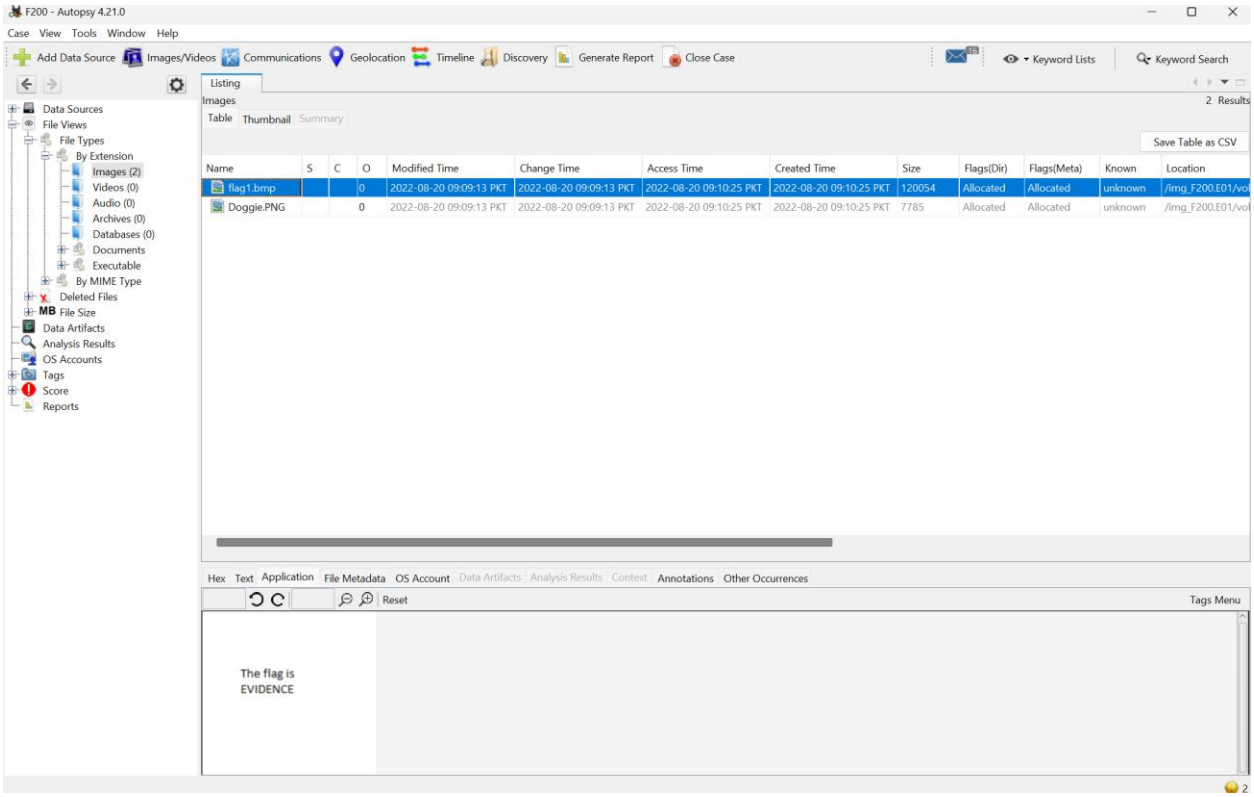

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Open
Look in: FIA
F200
F200.E01
Recent Items
Desktop
Documents
This PC
Network
File name: F200.E01
Files of type: All Supported Types
Open
Cancel
< Back
Next >
Finish
Cancel
Help

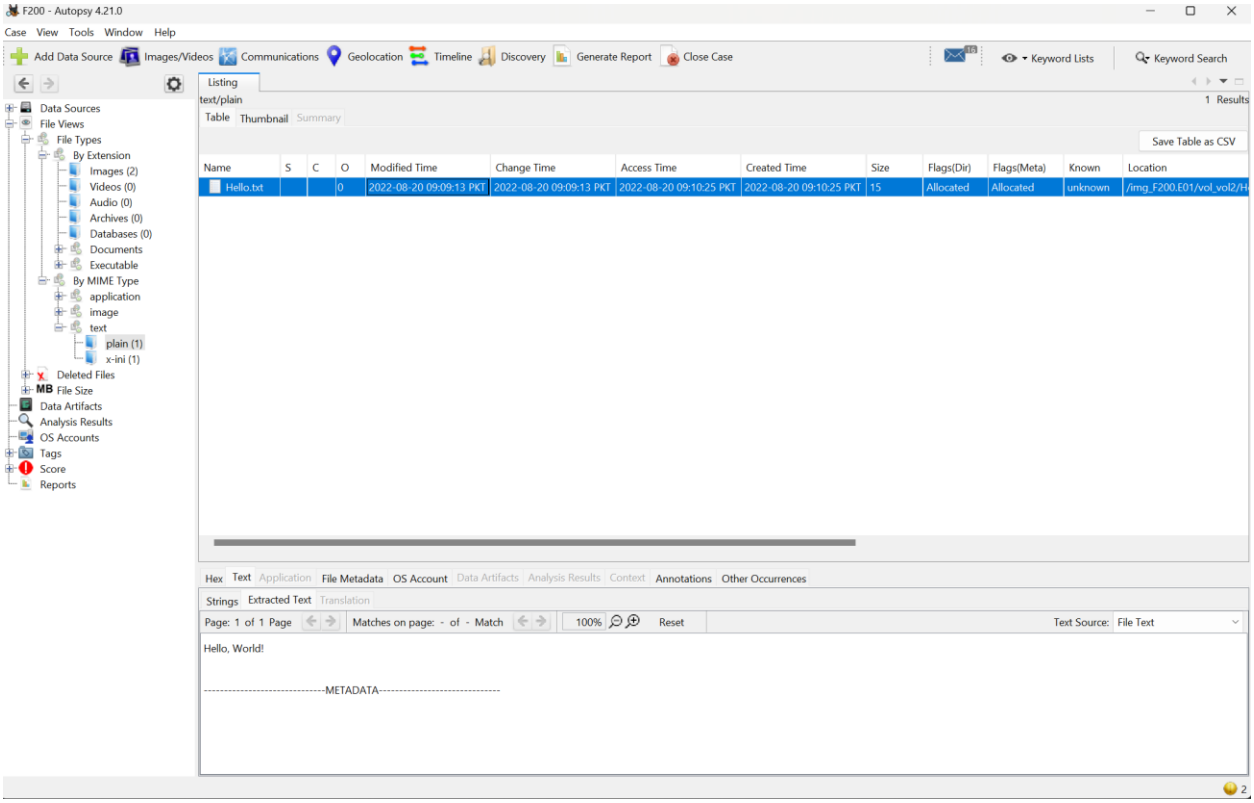

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
D:\FinalDFProj\FIA\F200.E01
Browse
Ignore orphan files in FAT file systems
Time zone: (GMT+5:00) Asia/Karachi
Sector size: Auto Detect
Hash Values (optional):
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:



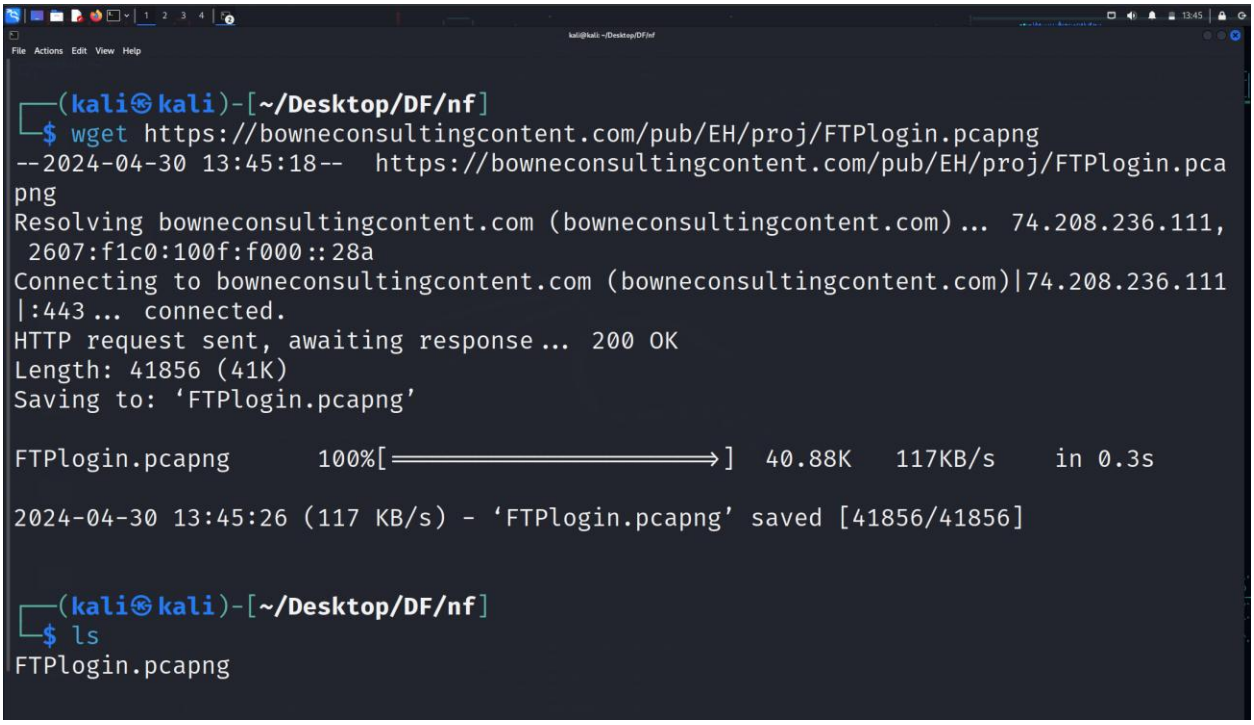
HELLO WORLD FINDING:

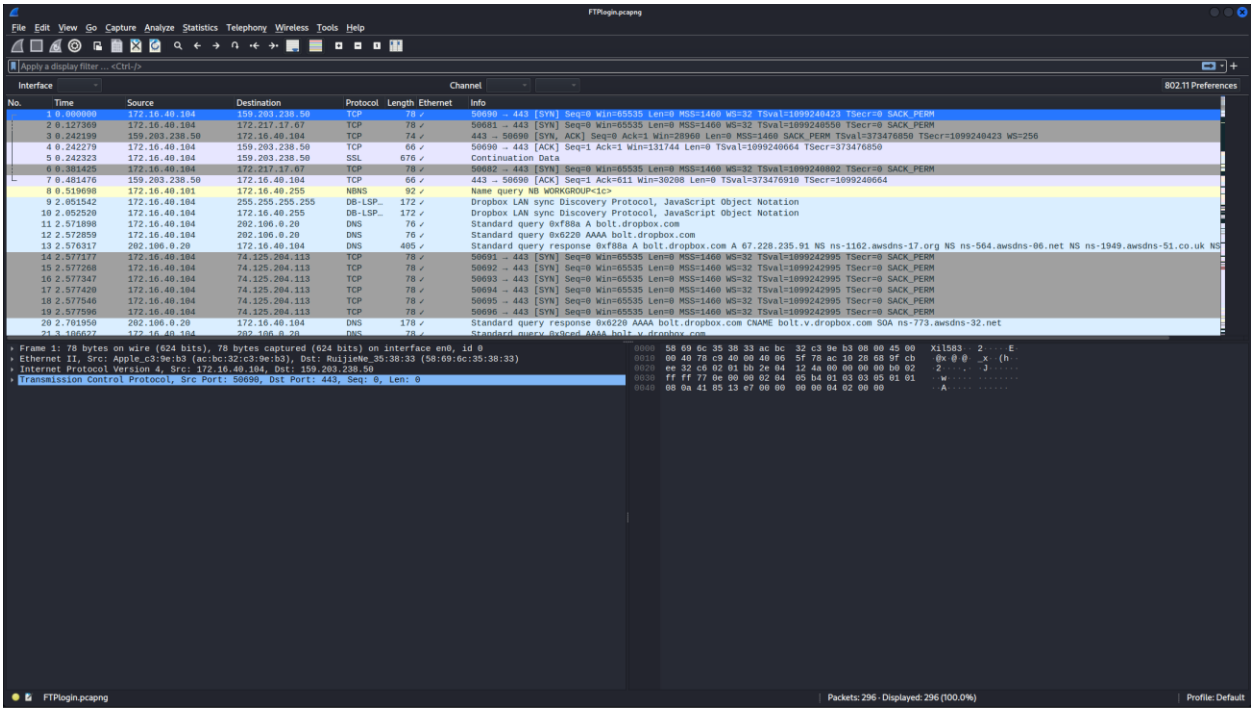


2. Network Forensic using Wireshark.

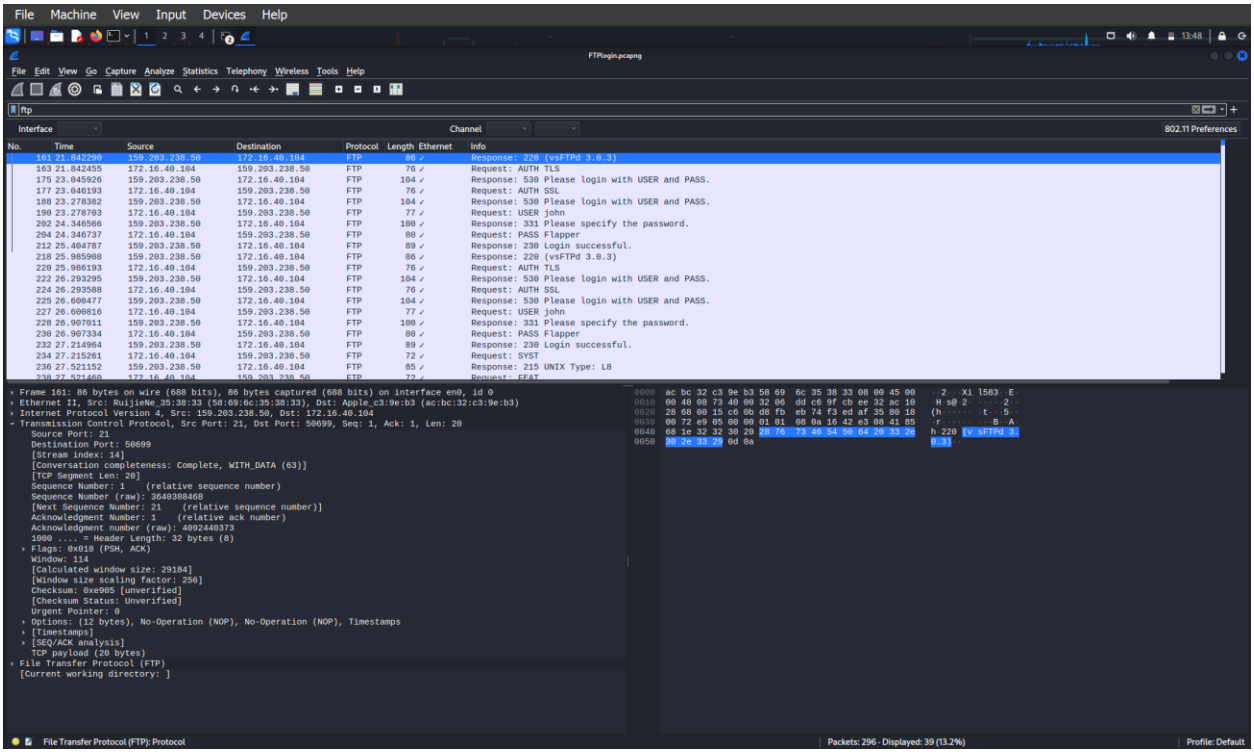
EXAMINING LAYERS 1-4

FTP LOGIN FILE DOWNLOAD:



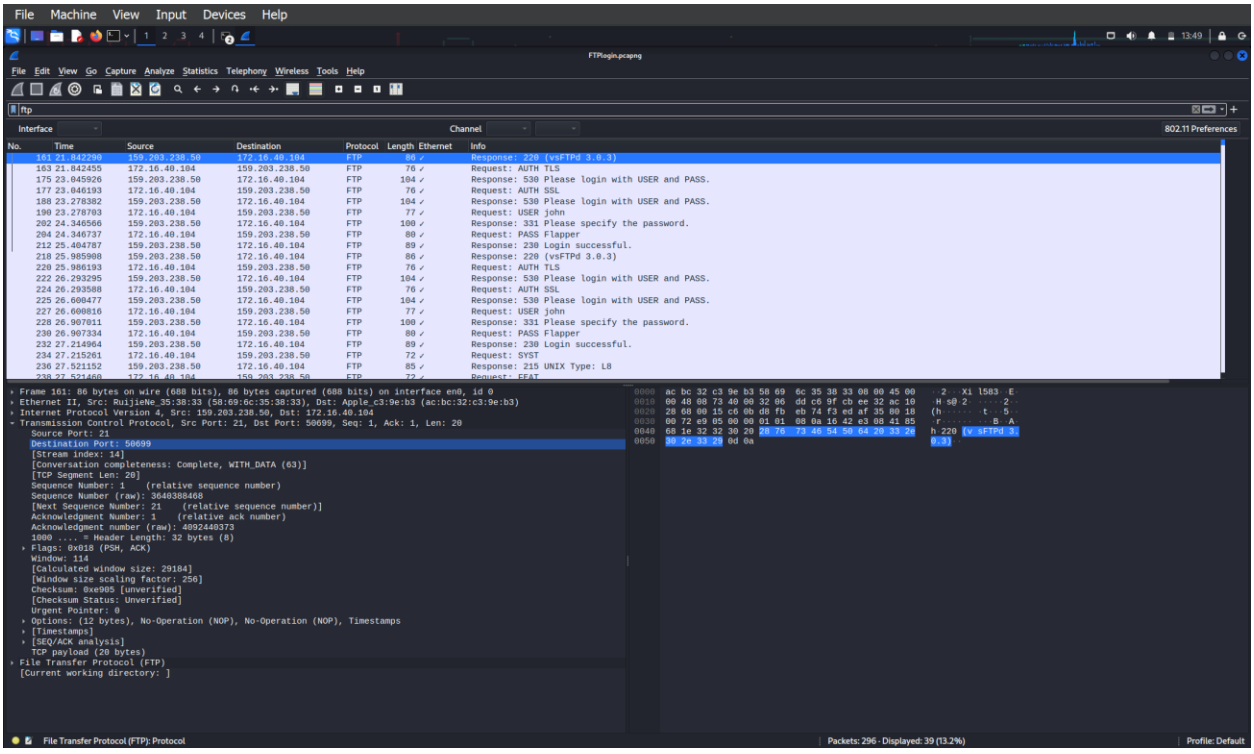


FTP FILE FILTER:

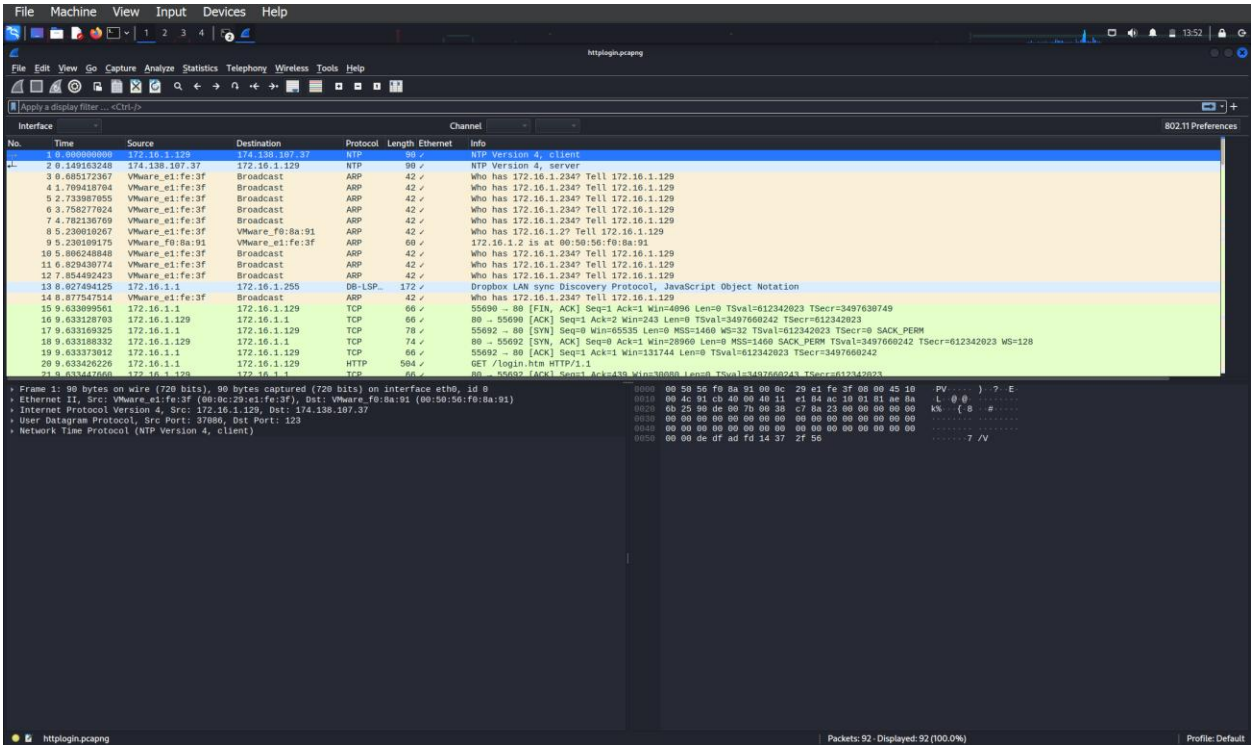


JOHN PASSWORD:

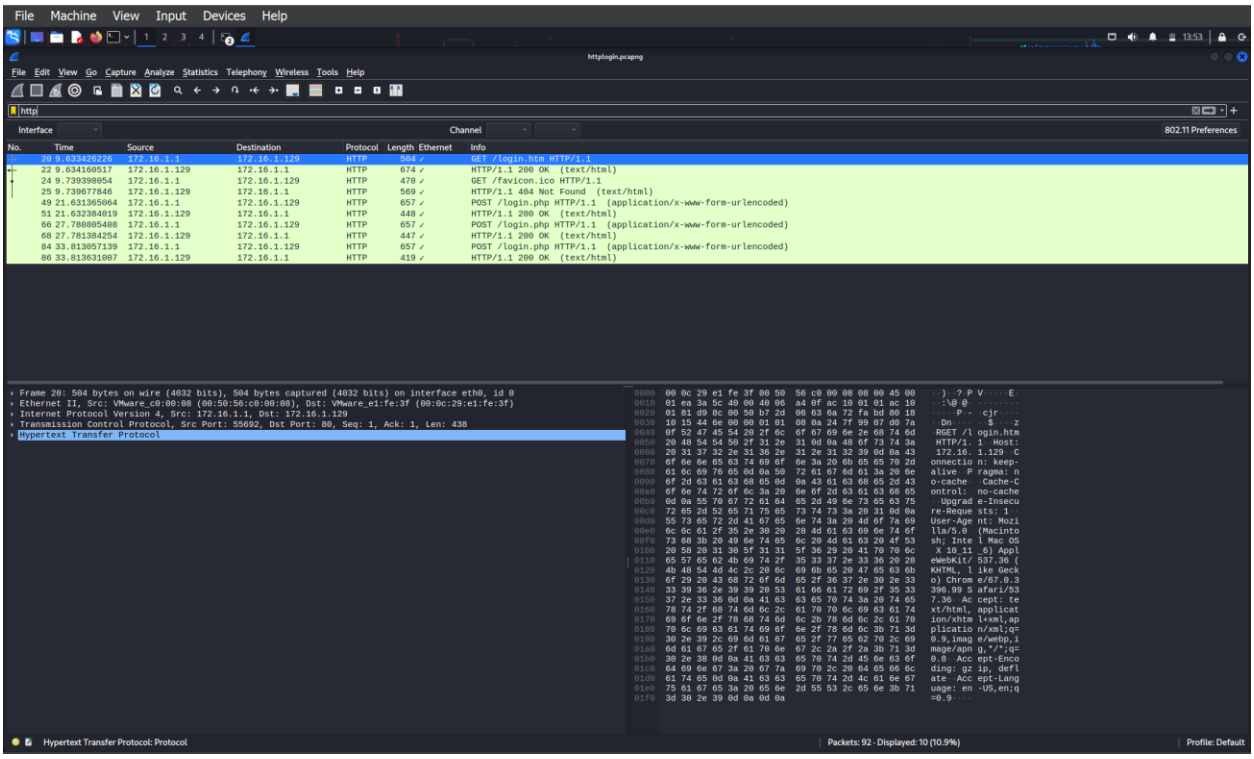
PASS



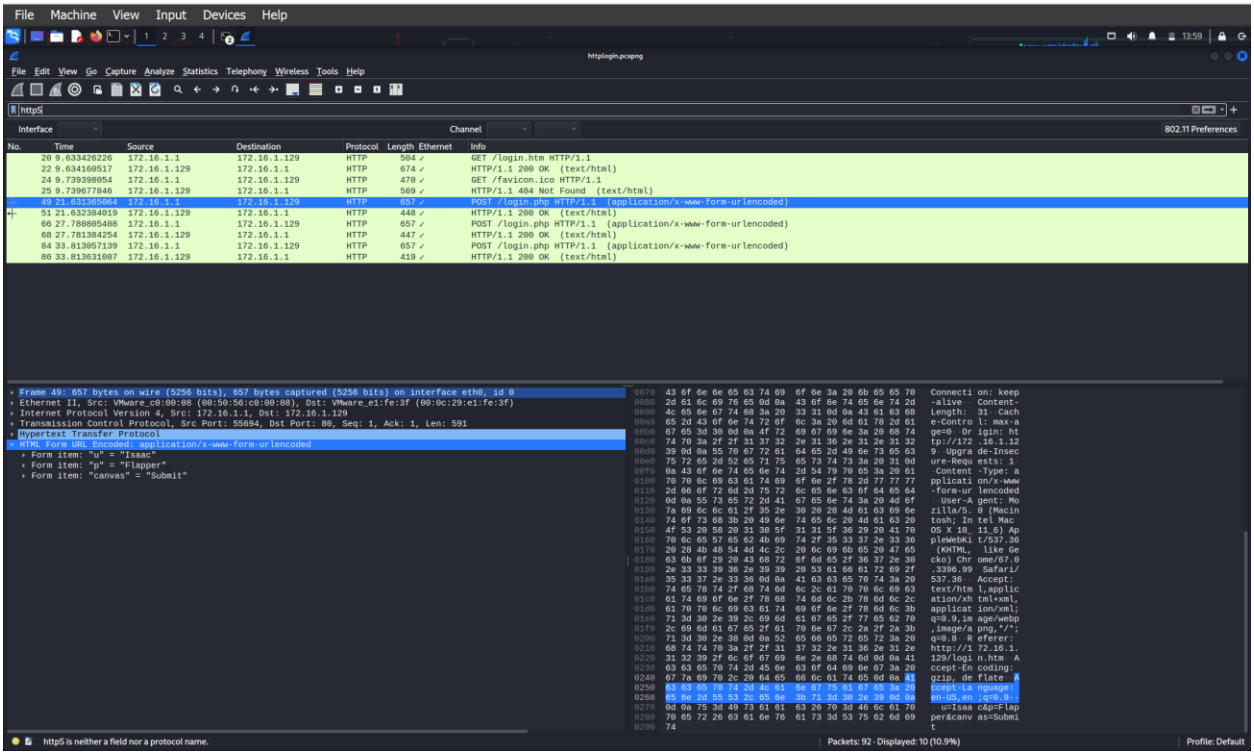
FINDING HTTP PASSWORD:



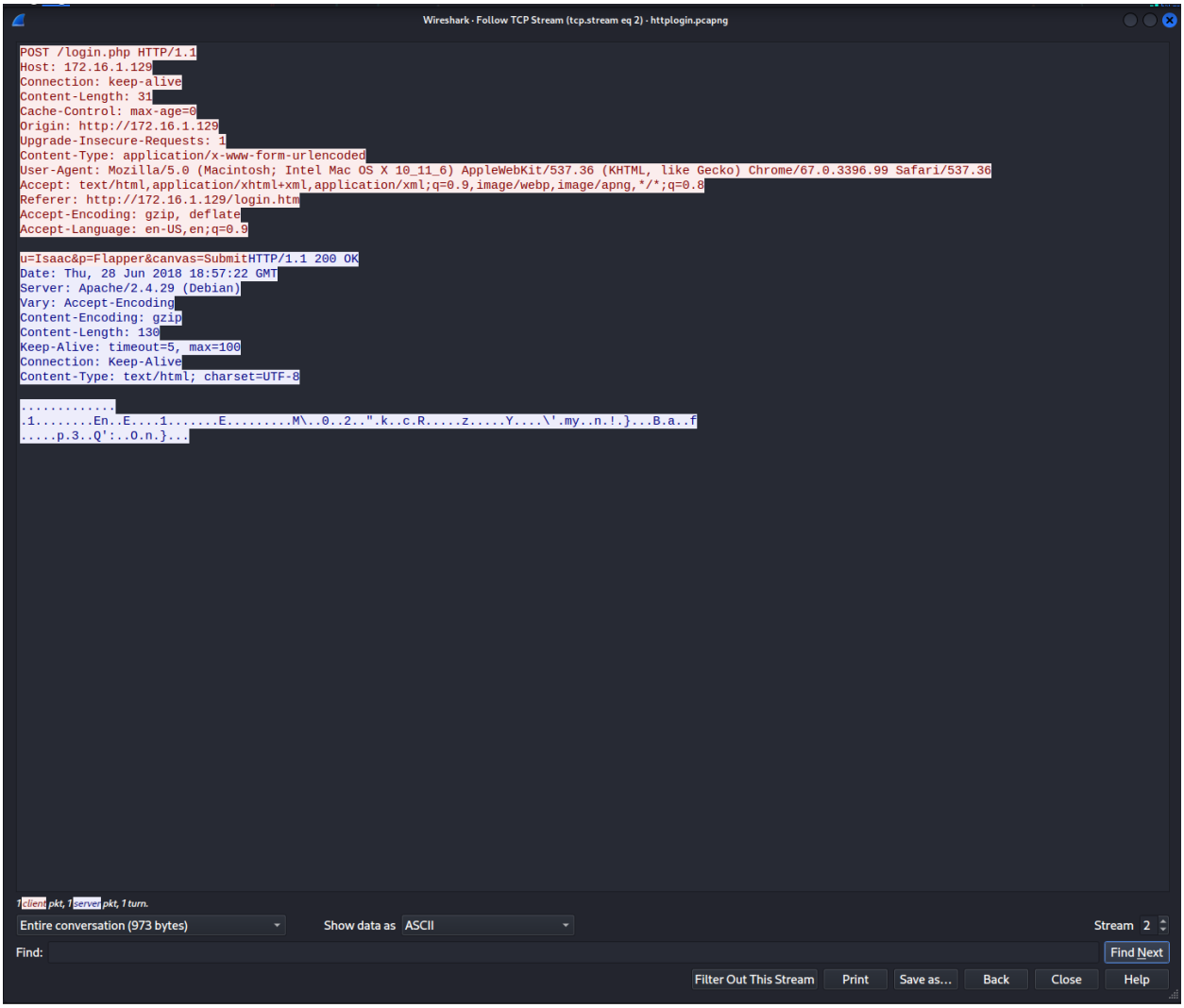
HTTP PACKET FILTER:



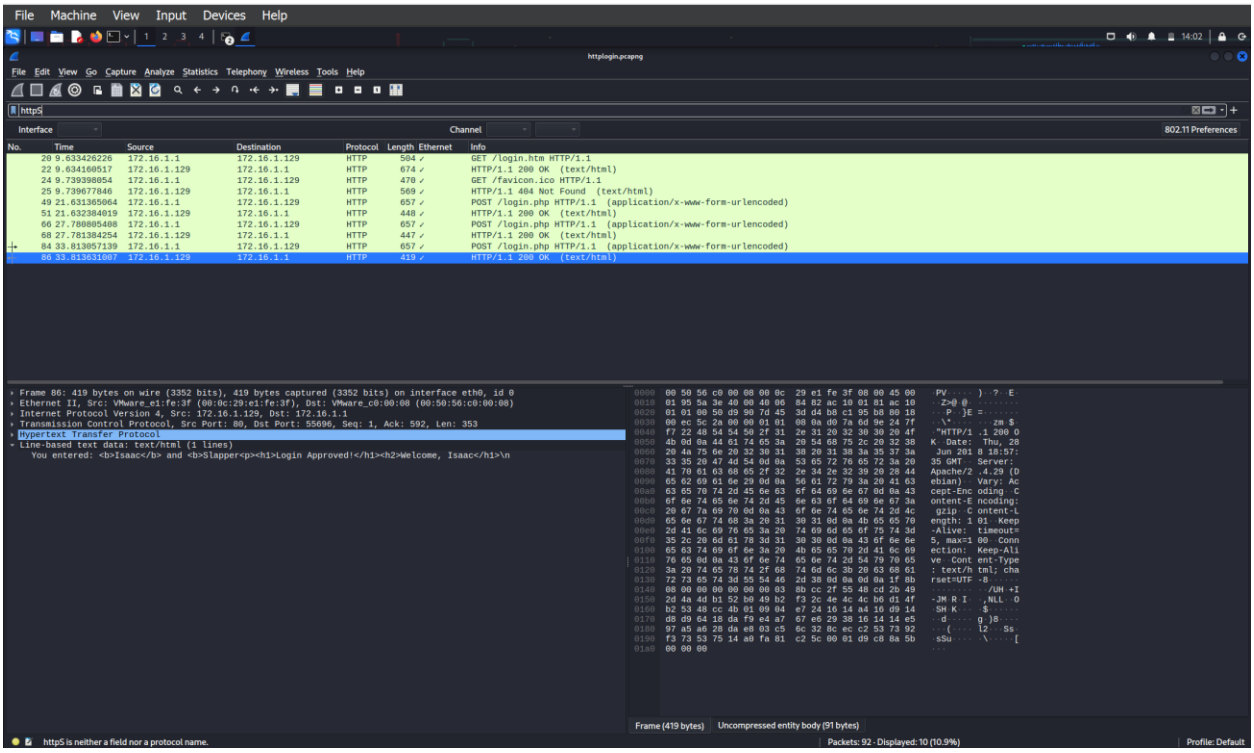
USERNAME ISAAC AND FLAPPER:



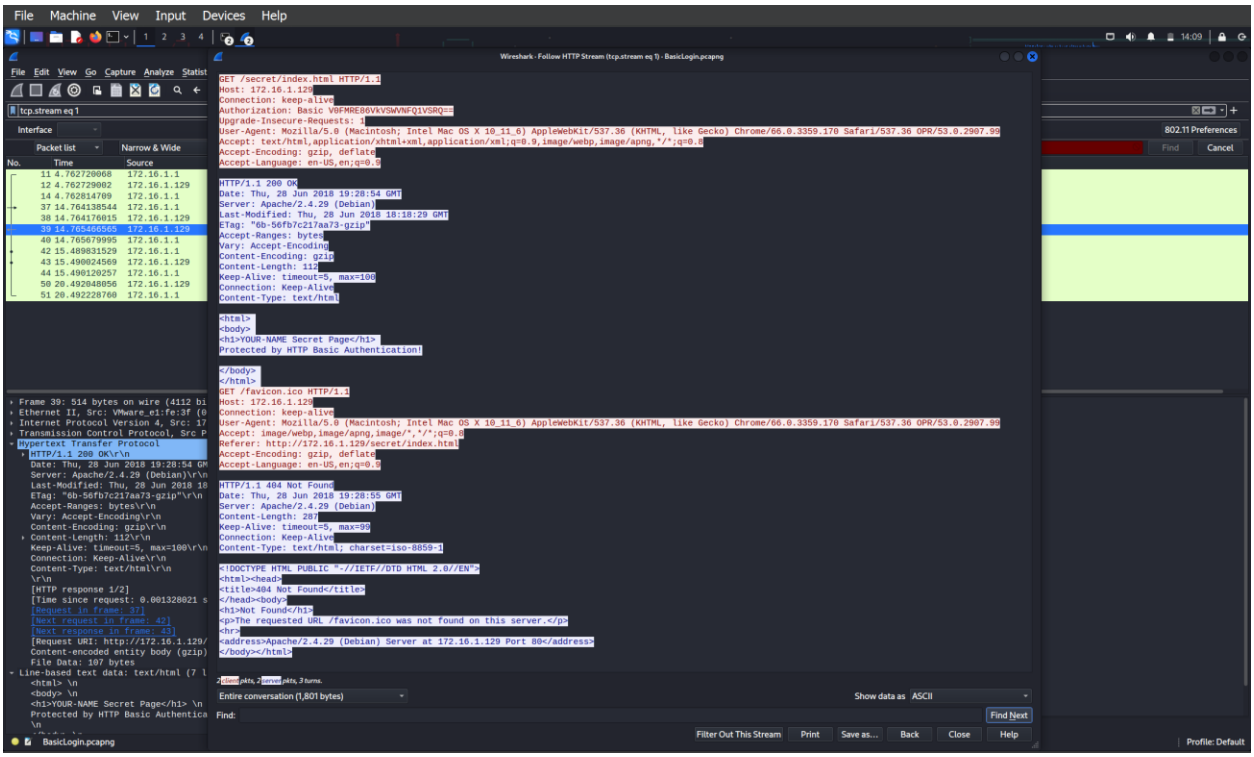
FOLLOWING TCP STREAM:



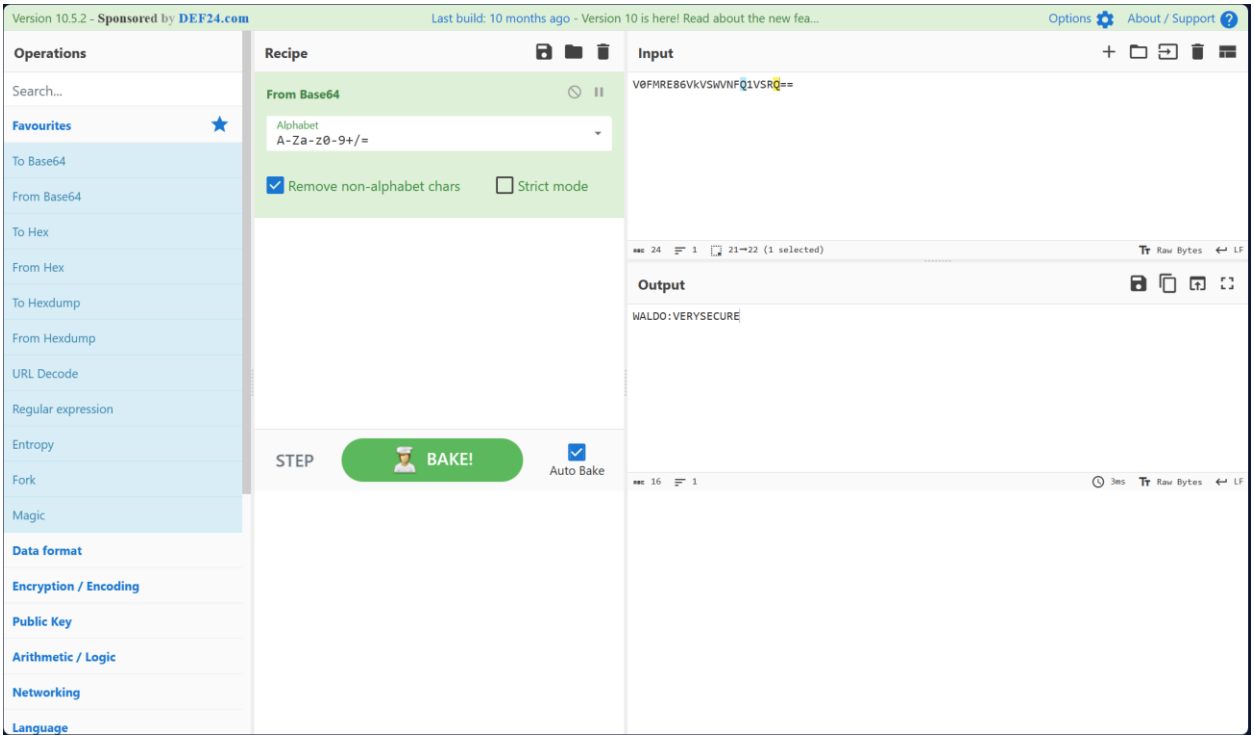
ISAAC PASSWORD “SLAPPER”:



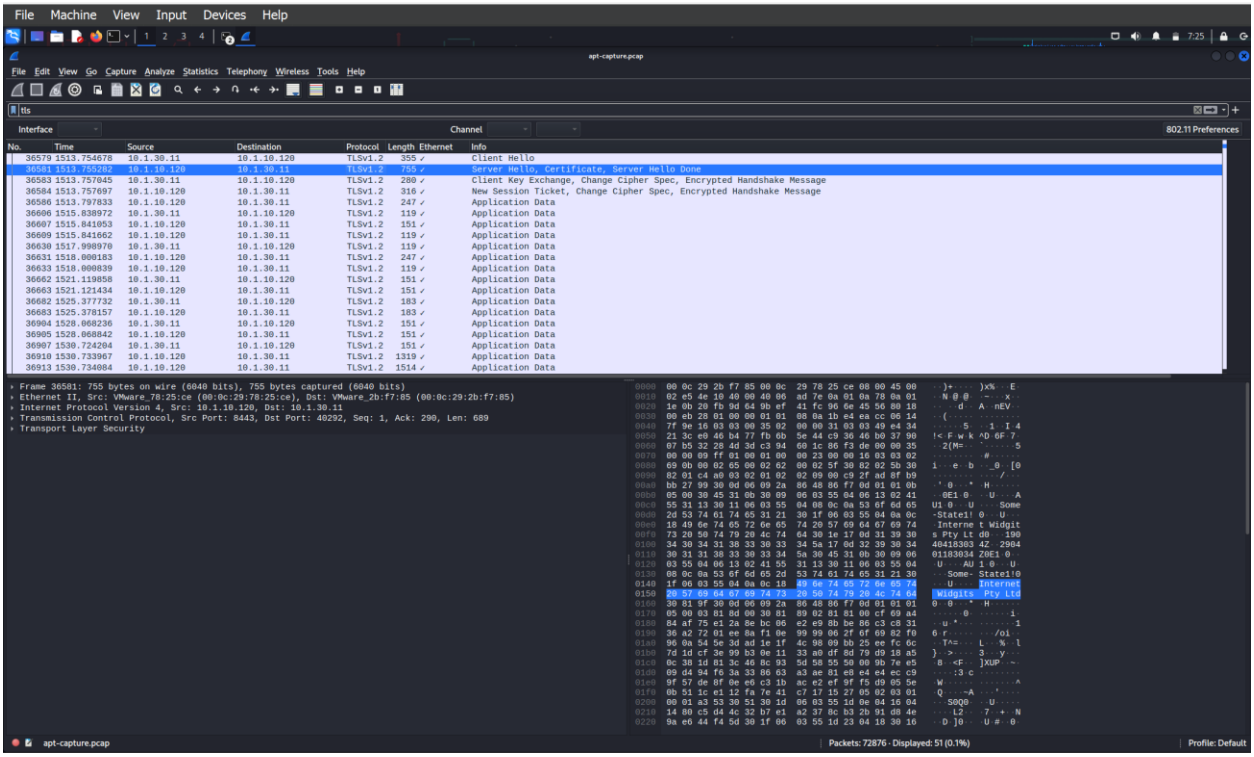
HTTP BASIC AUTHENTICATION:



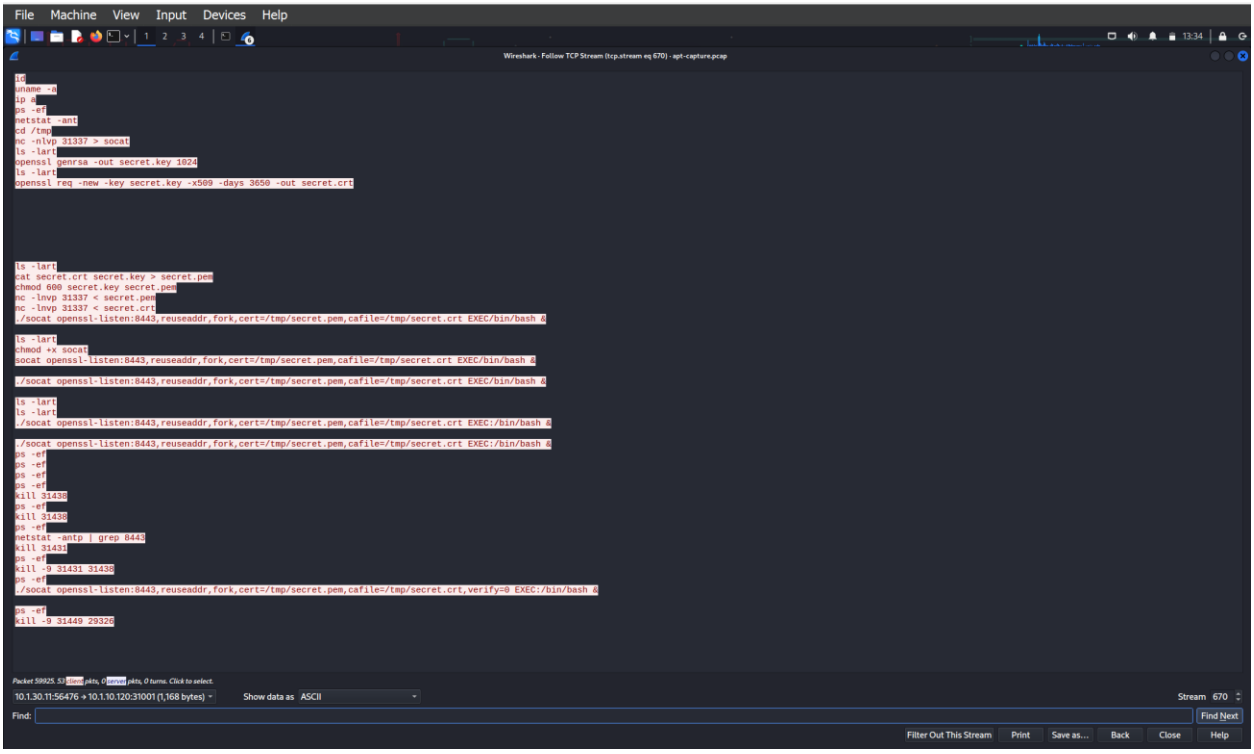
WALDO PASSWORD:



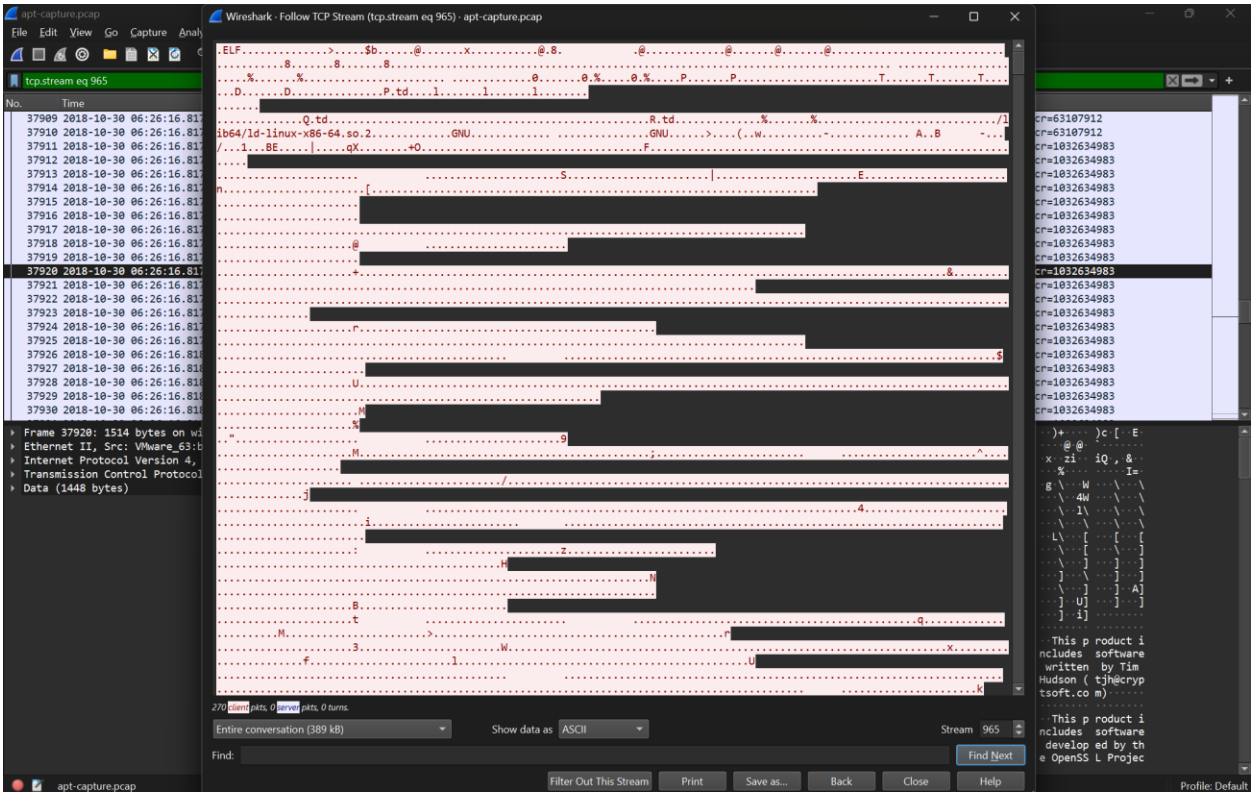
APT CAPTURE:

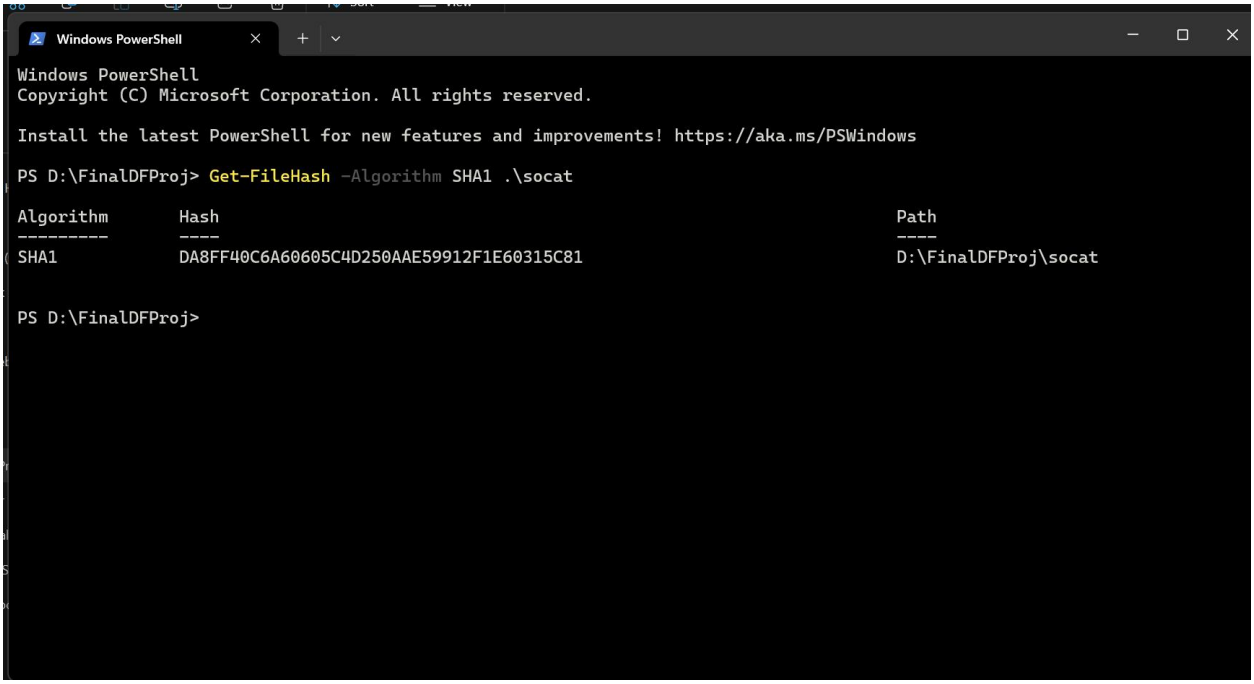


ENCRYPTED TRANSMISSION (TLS) + TOOL (SOCAT):

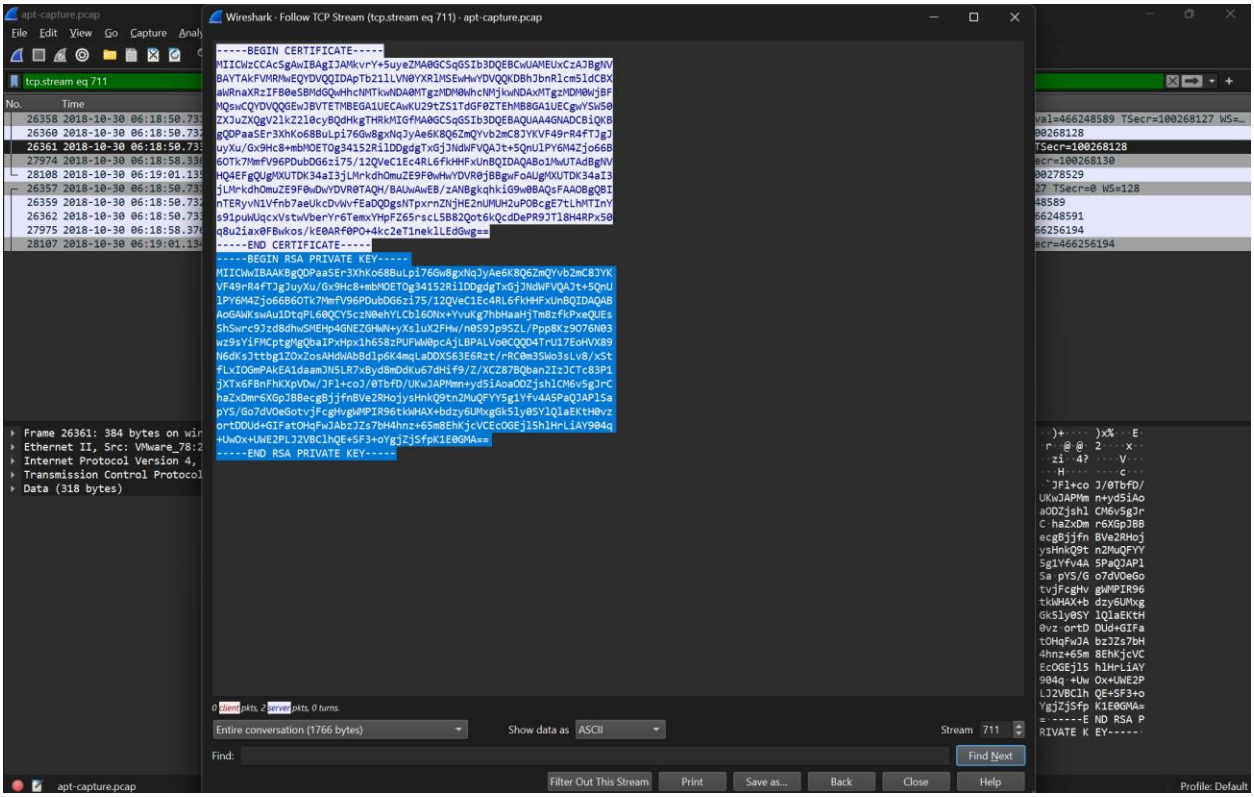


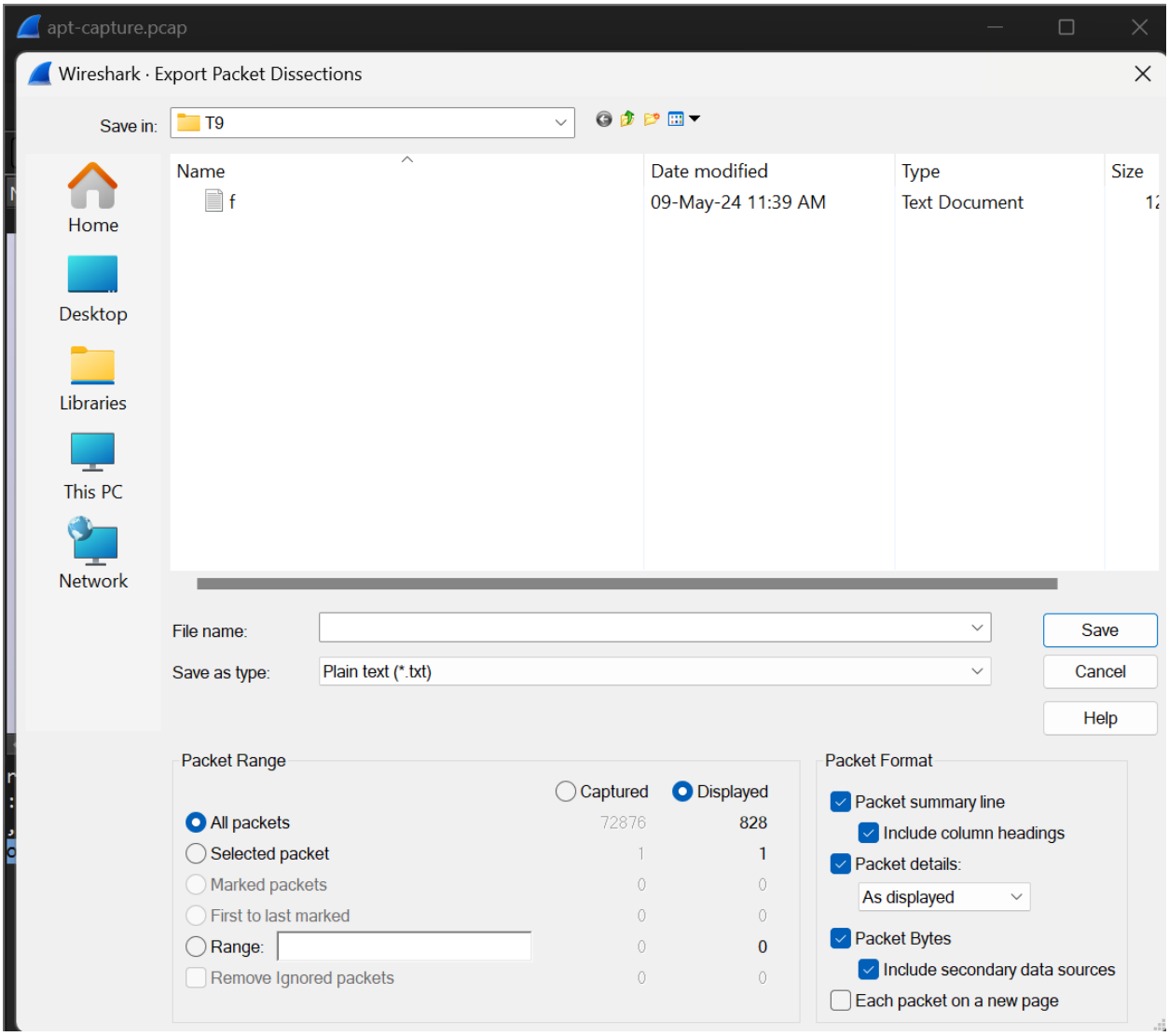
HASH OF TOOL:



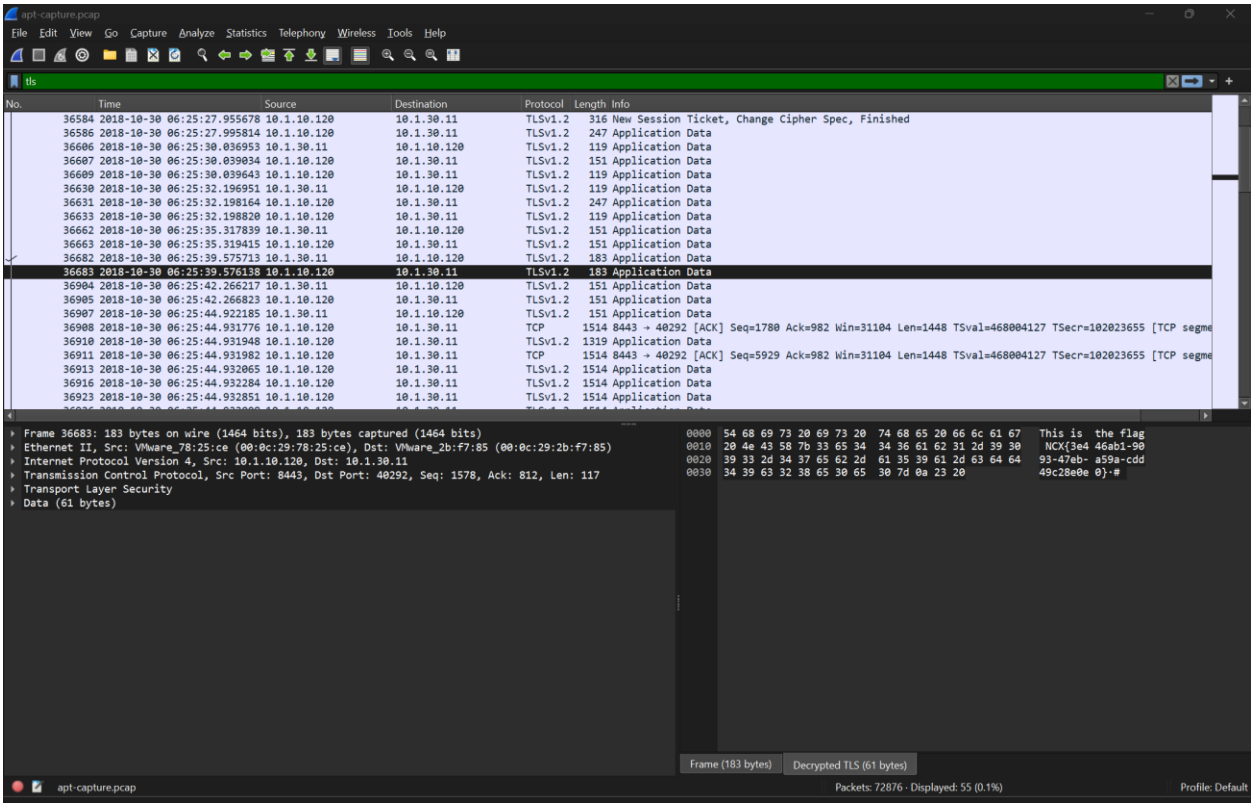

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\FinalDFProj> Get-FileHash -Algorithm SHA1 .\socat
Algorithm Hash Path
SHA1 DA8FF40C6A60605C4D250AAE59912F1E60315C81 D:\FinalDFProj\socat
PS D:\FinalDFProj>

DECRYPT:

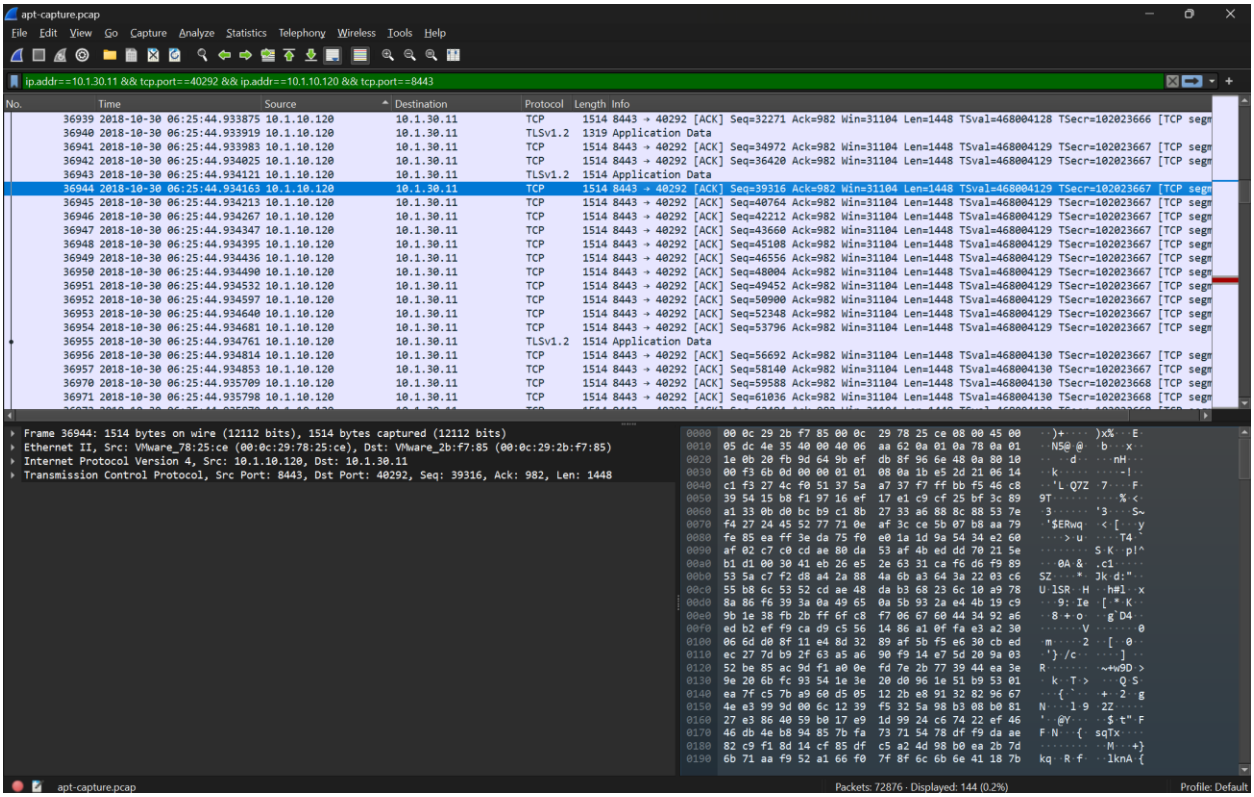

Wireshark · Follow TCP Stream (tcp.stream eq 711) · apt-capture.pcap
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE KEY-----
Entire conversation (1766 bytes)
Show data as ASCII
Stream 711
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


apt-capture.pcap
Wireshark · Export Packet Dissections
Save in:
T9
Home
Desktop
Libraries
This PC
Network
Name
Date modified
Type
Size
f
09-May-24 11:39 AM
Text Document
File name:
Save as type:
Plain text (*.txt)
Save
Cancel
Help
Packet Range
Captured
Displayed
All packets
72876
828
Selected packet
1
1
Marked packets
0
0
First to last marked
0
0
Range:
0
0
Remove Ignored packets
0
0
Packet Format
Packet summary line
Include column headings
Packet details:
As displayed
Packet Bytes
Include secondary data sources
Each packet on a new page

PORT KNOCKING:

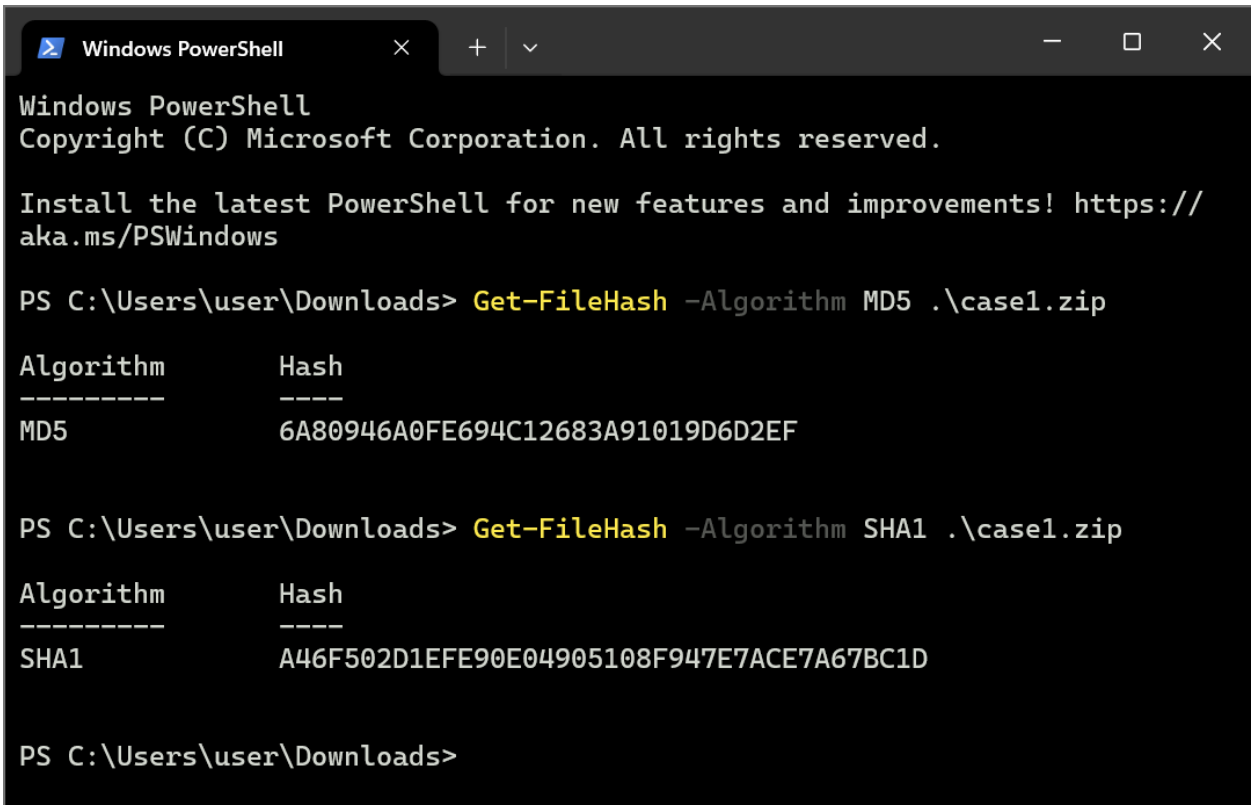


EXPLOITATION:

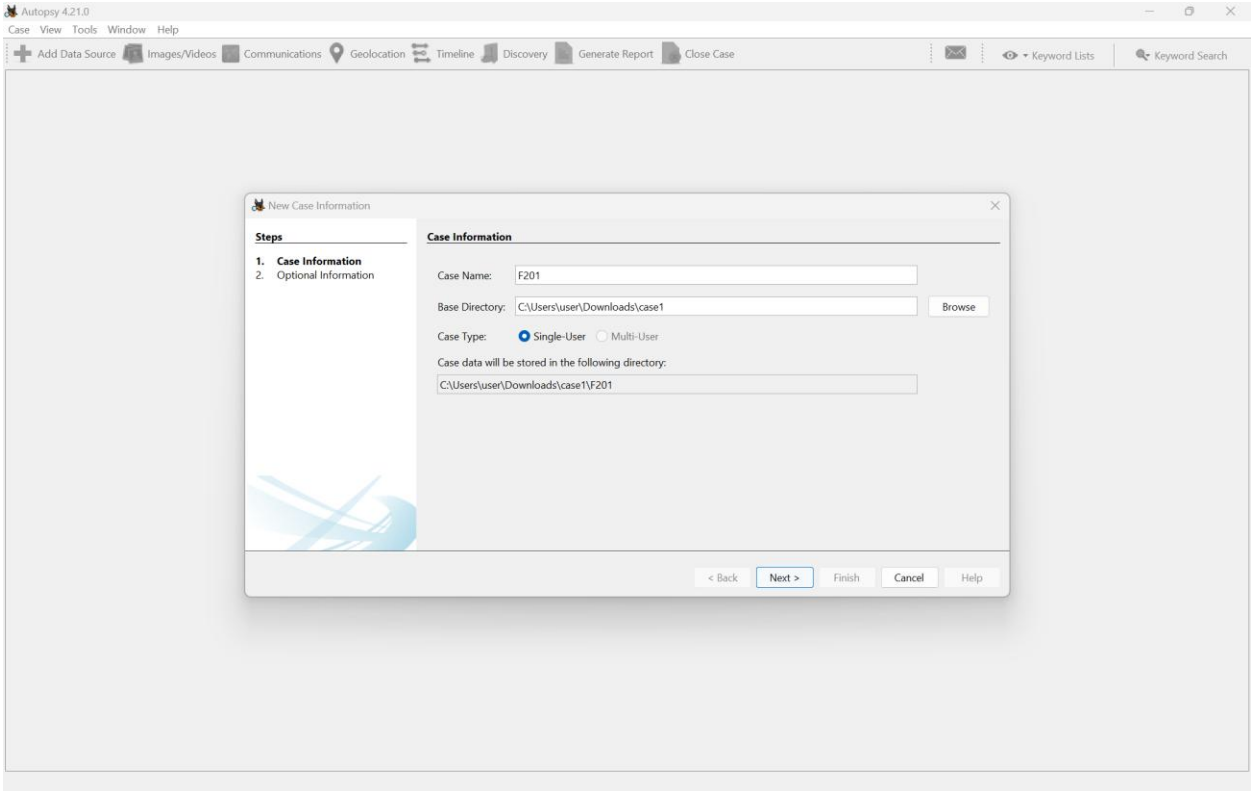


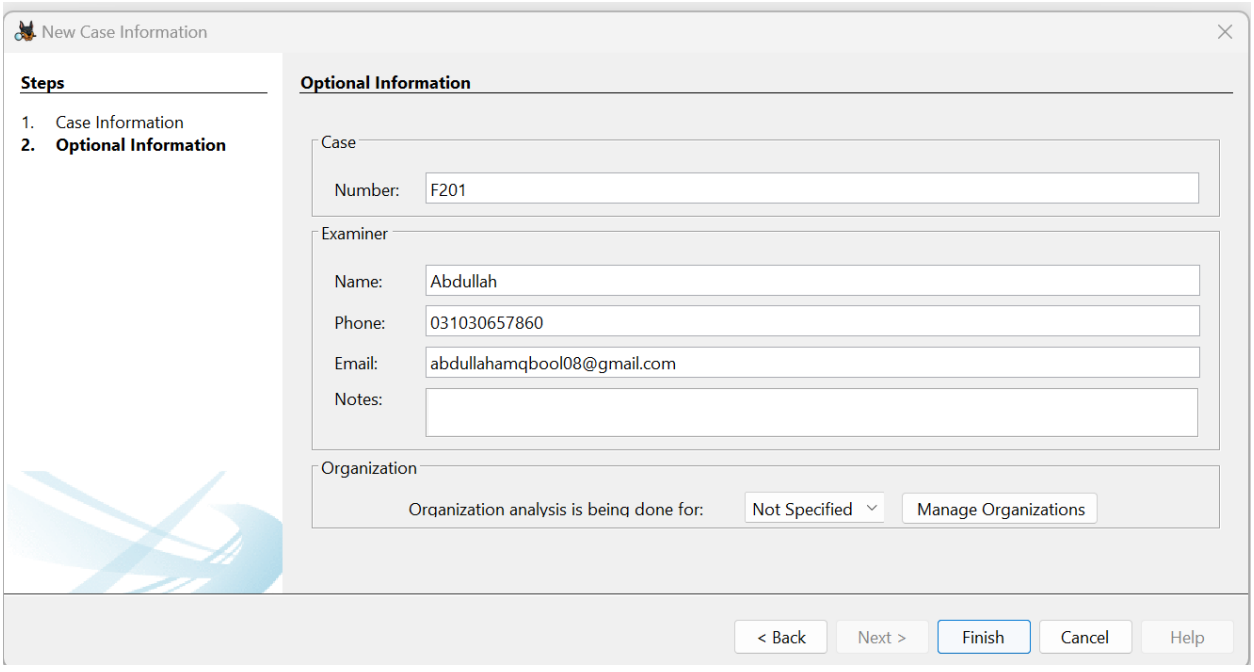
3. Rhino Hunt with Autopsy:

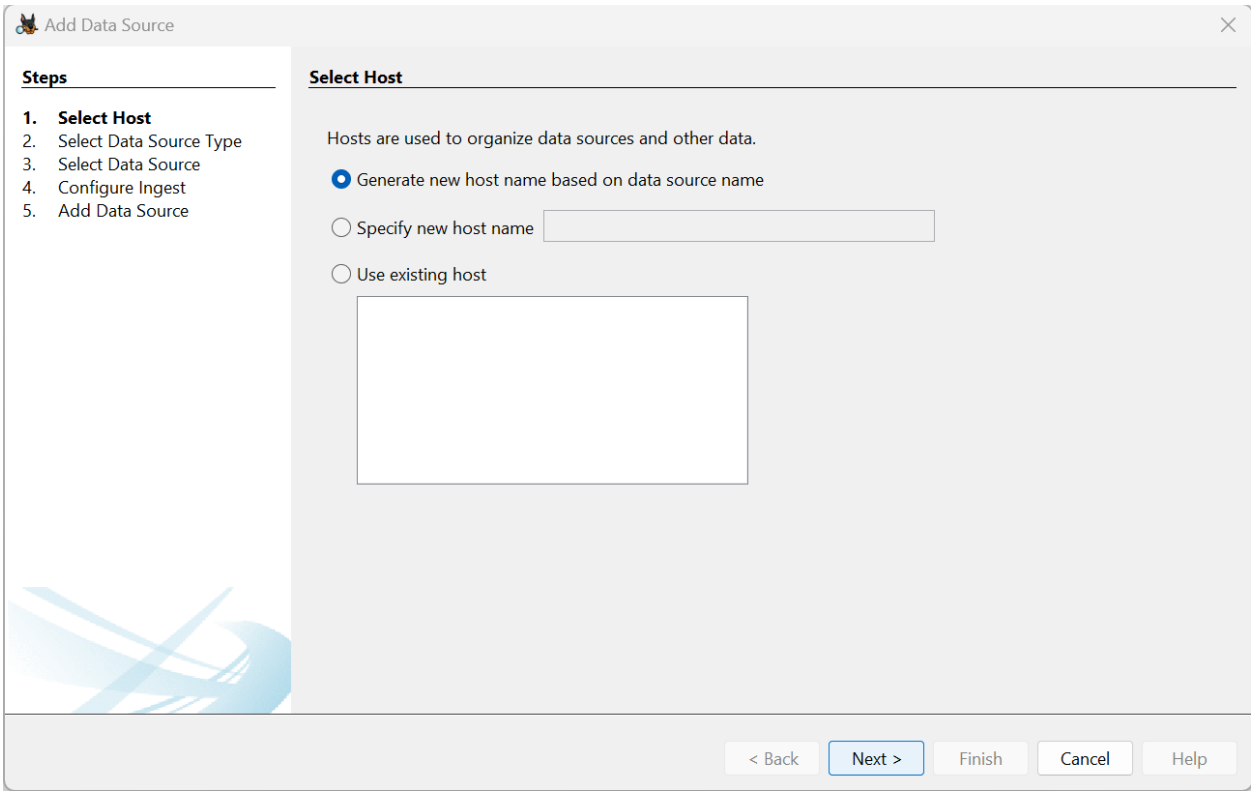
VERIFYING HASH VALUES:

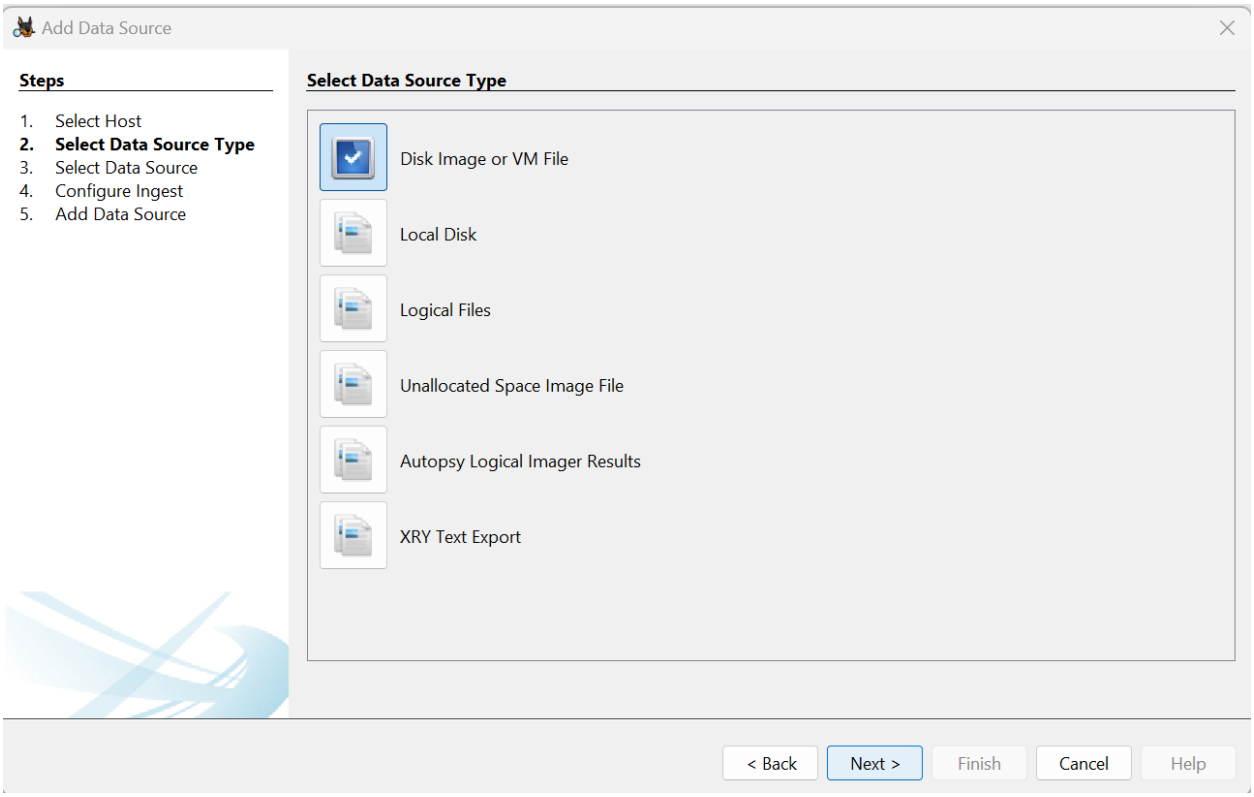


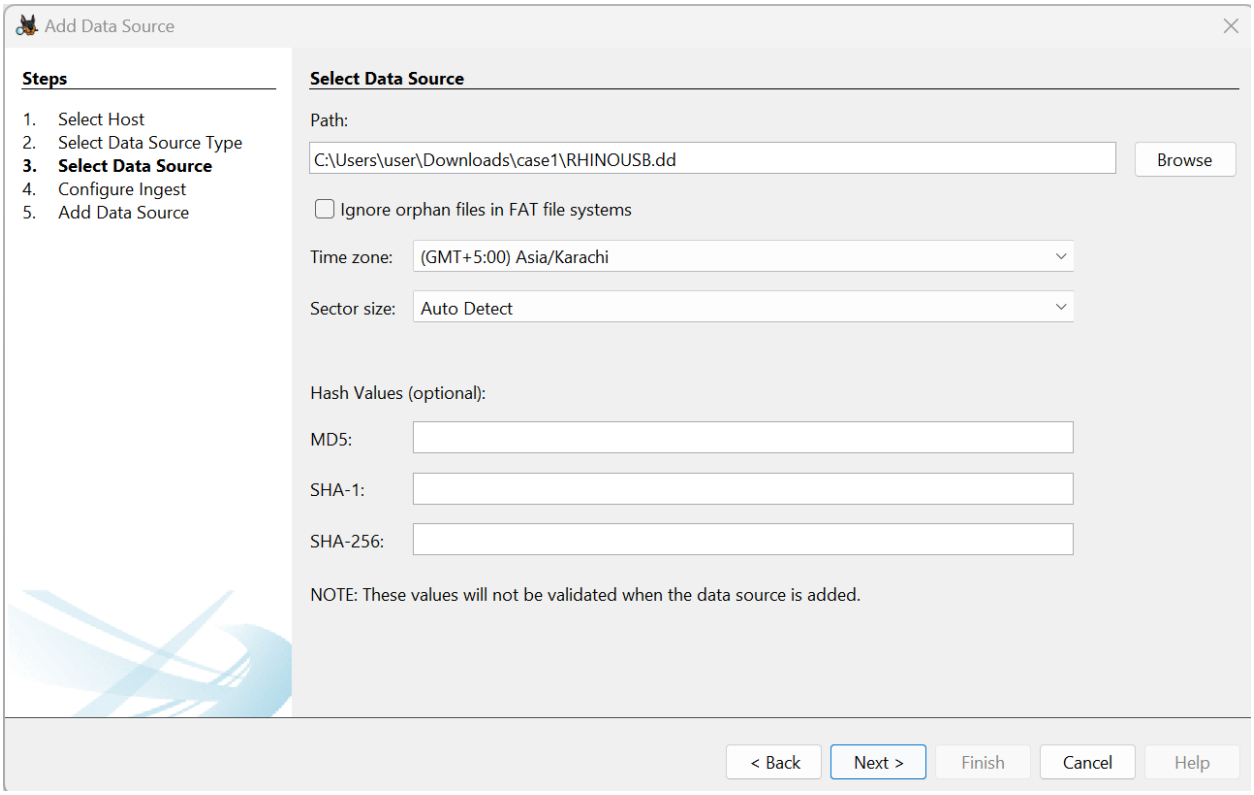
CREATING AUTOPSY CASE:

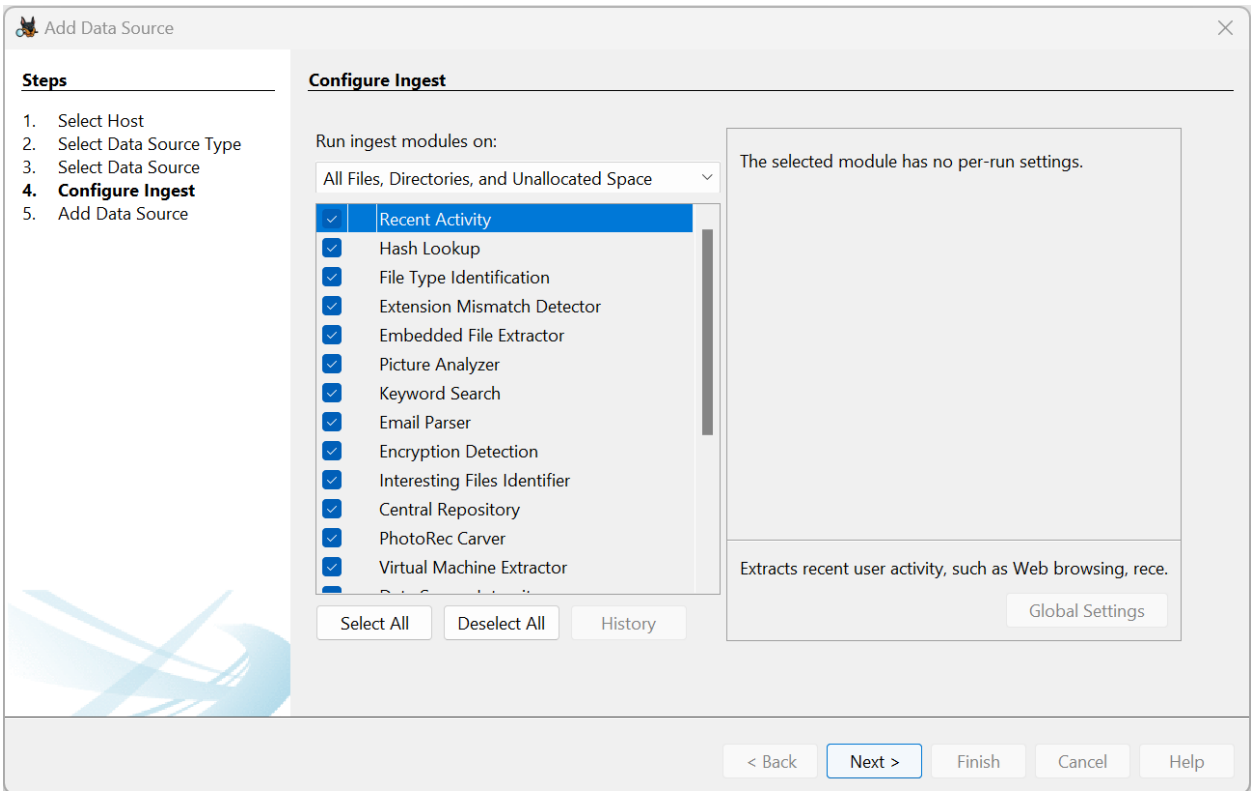




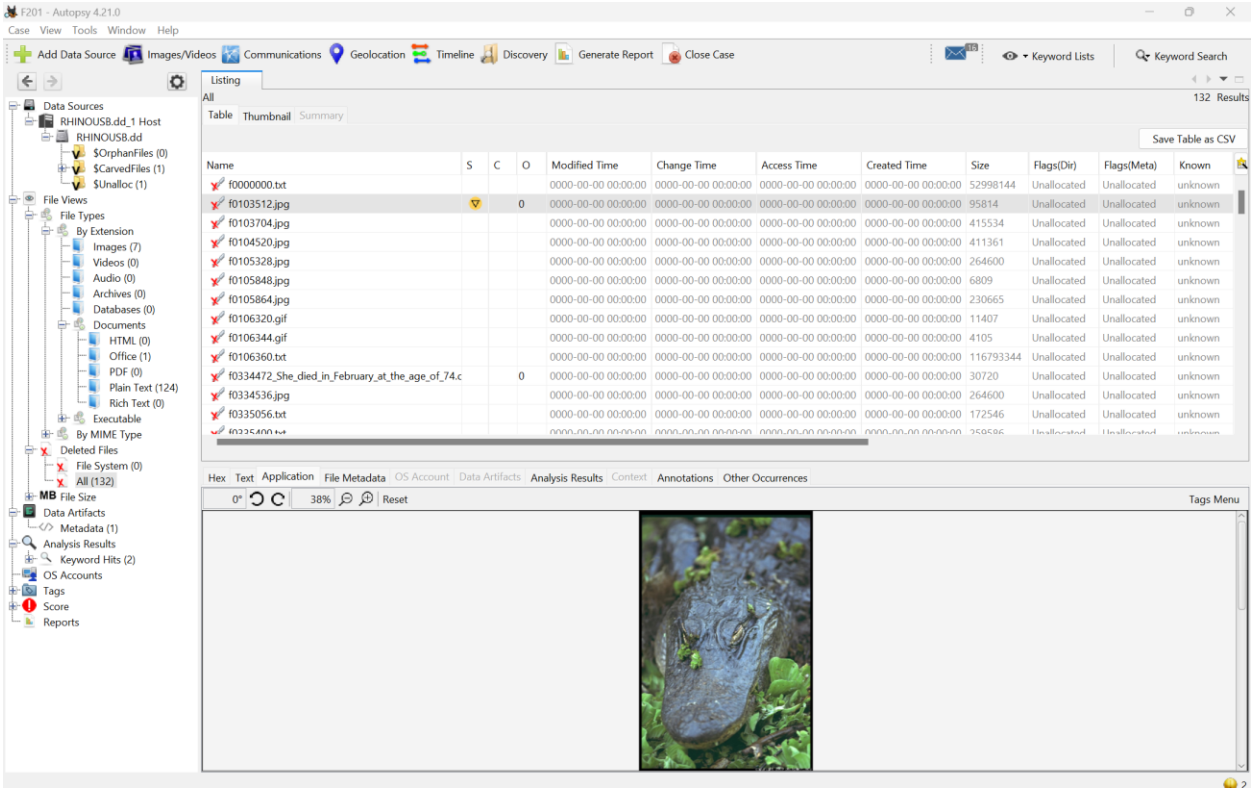

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
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 Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

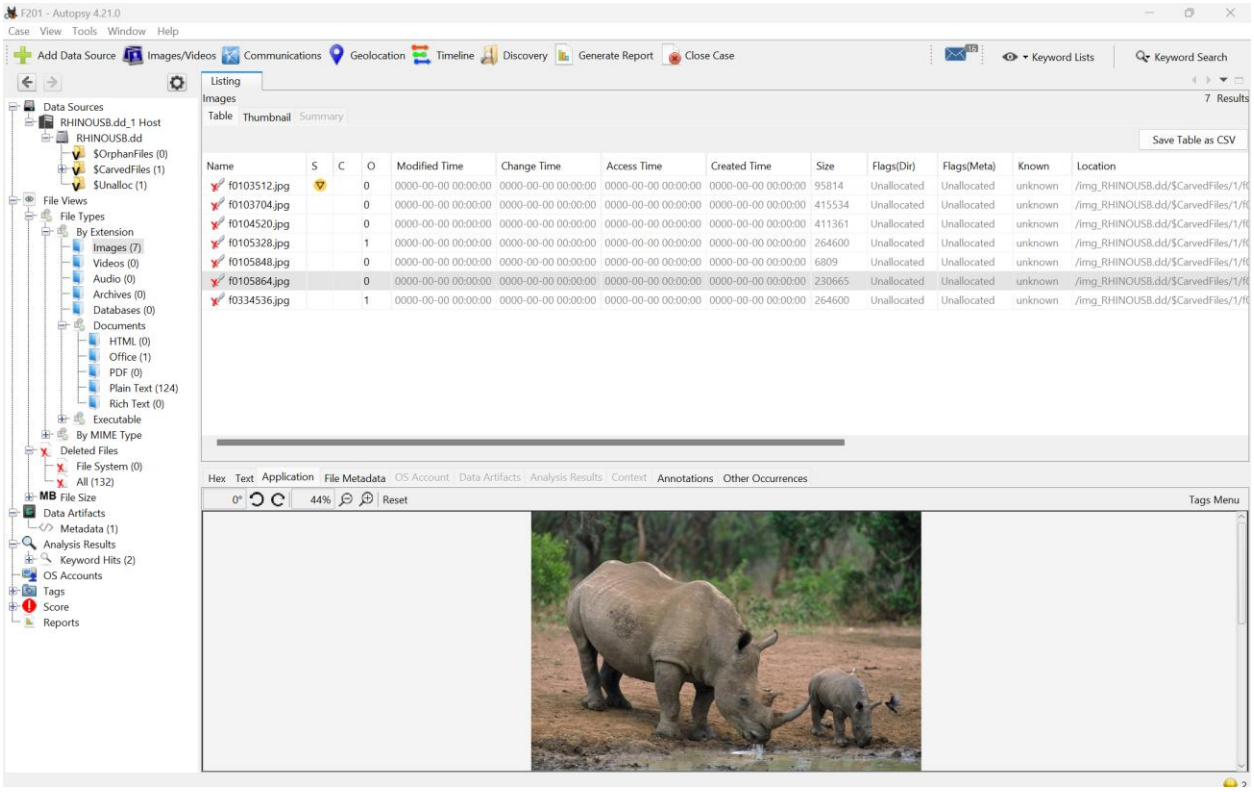

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Users\user\Downloads\case1\RHINOUSB.dd
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+5:00) Asia/Karachi
Sector size:
Auto Detect
Hash 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


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, rece.
Global Settings
< Back
Next >
Finish
Cancel
Help

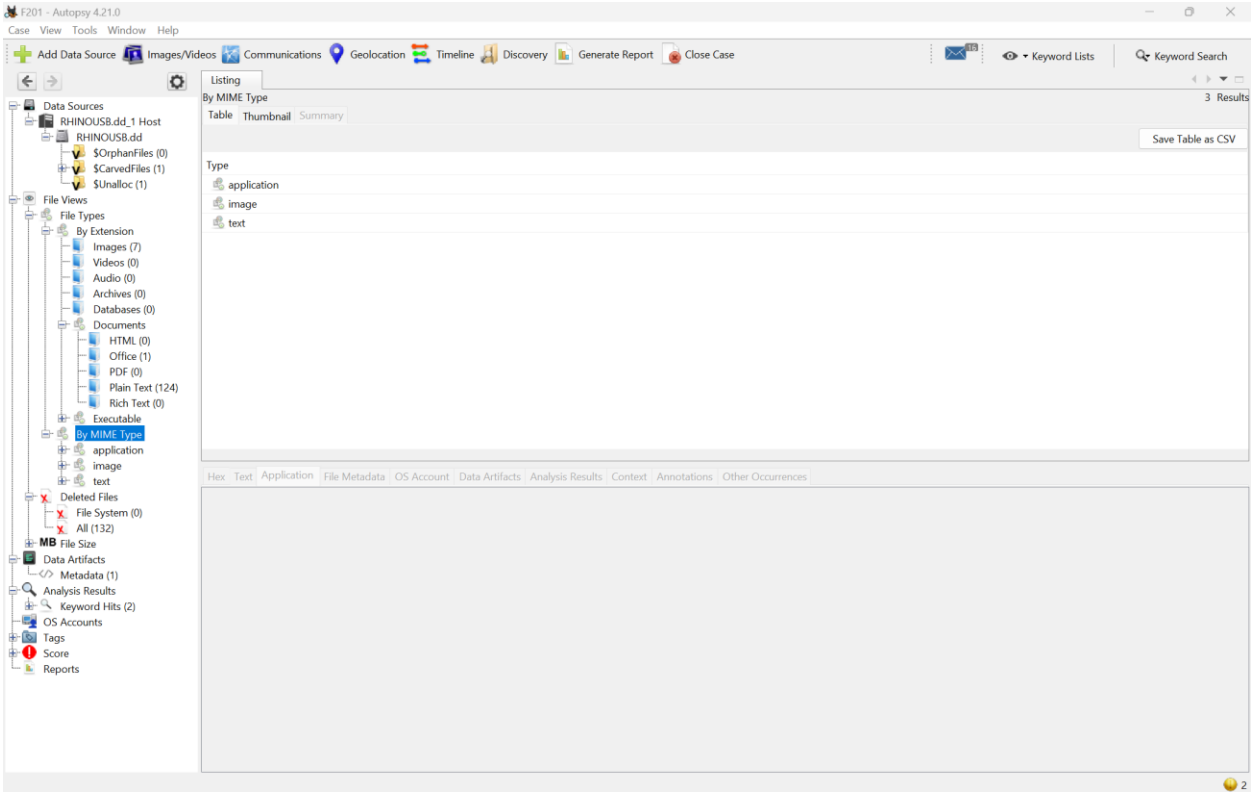
ANALYZING DELETED FILES:



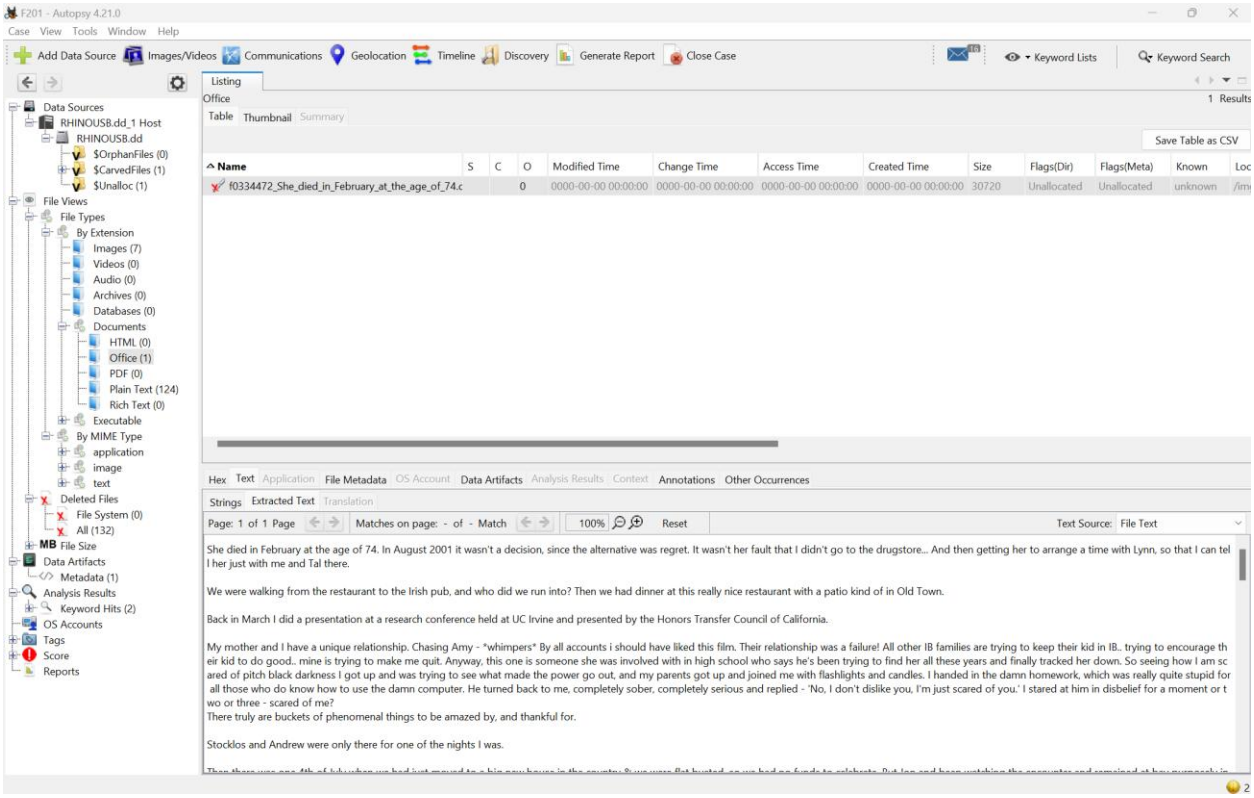
MOTHER AND CHILS FLAG:



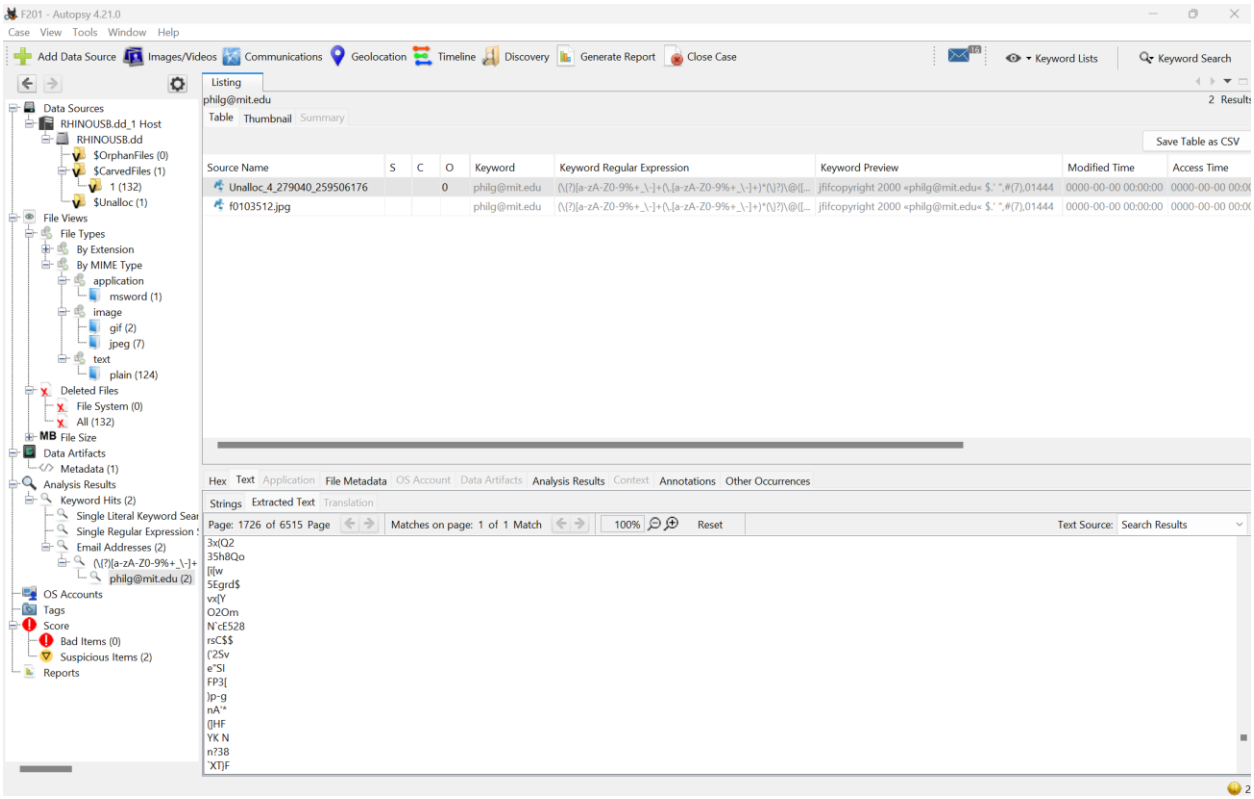
SORTING BY FILE TYPE:



READING DIARY

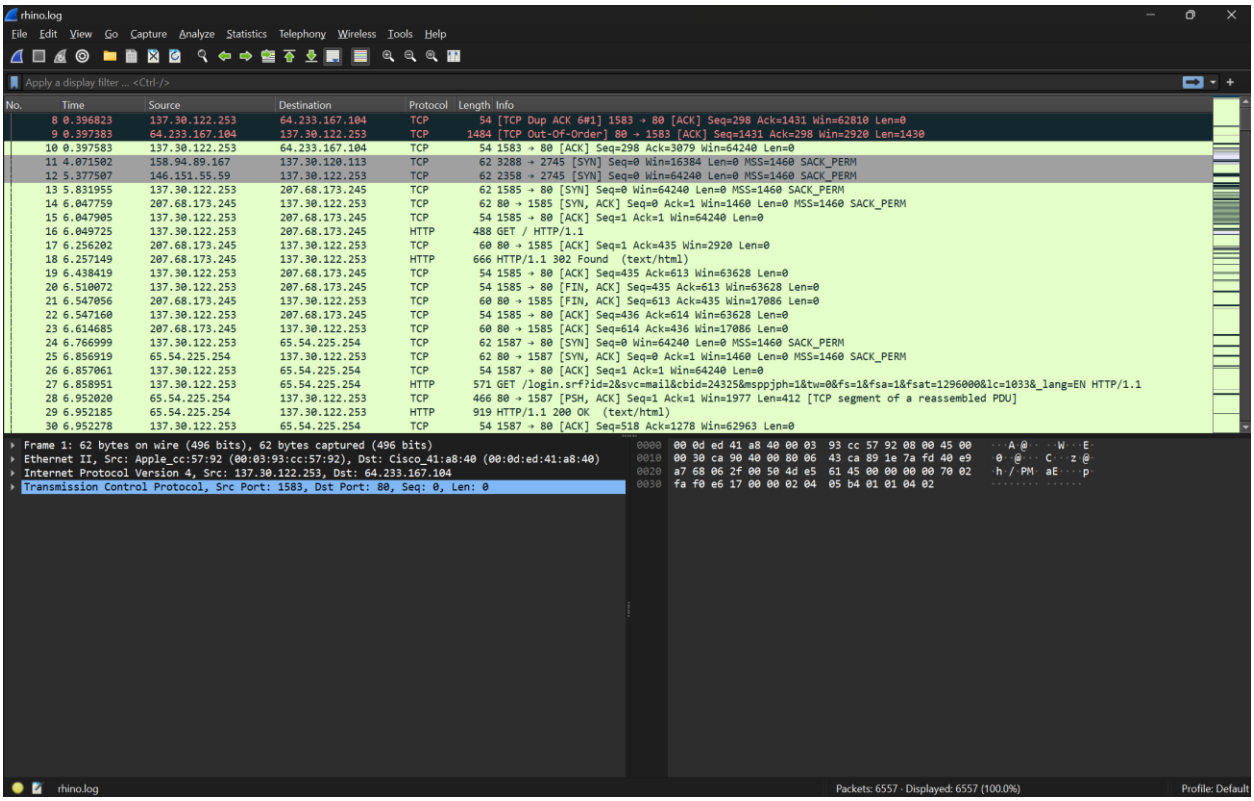


HARD DRIVE + EMAIL ADDRESS:

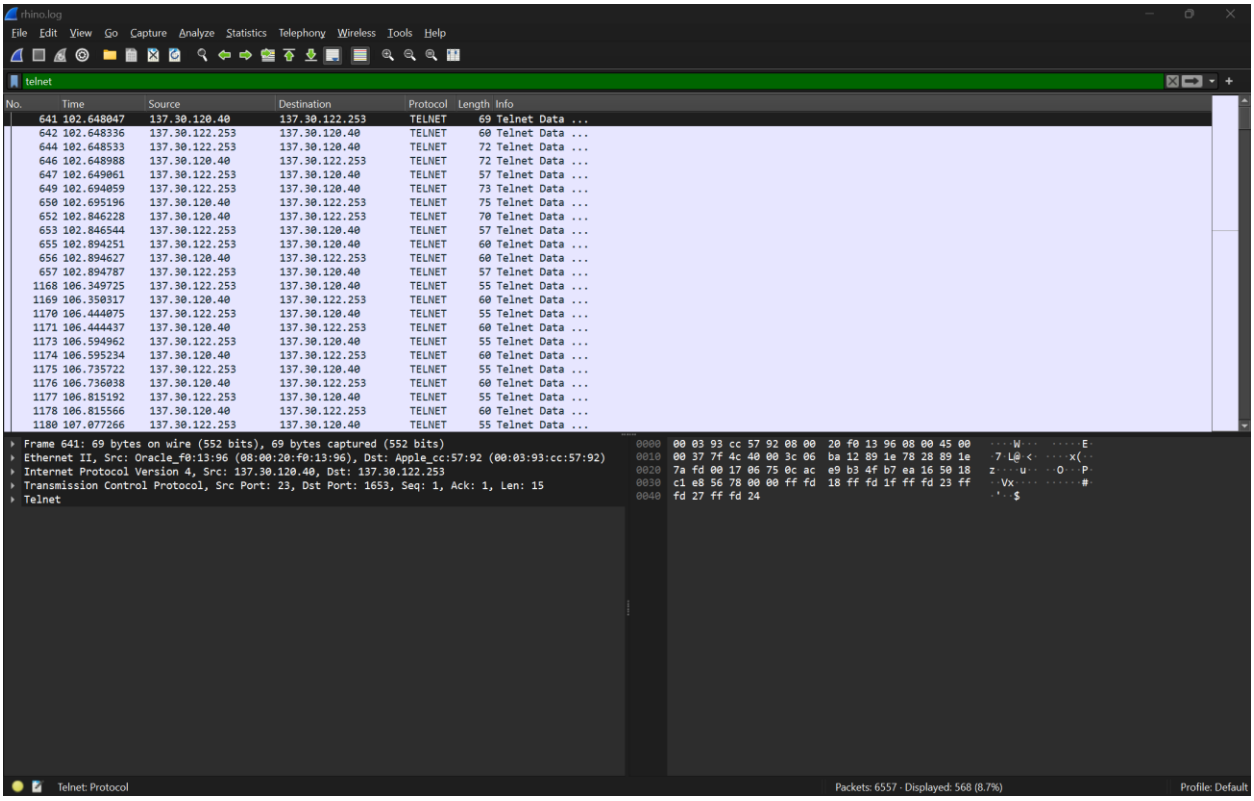


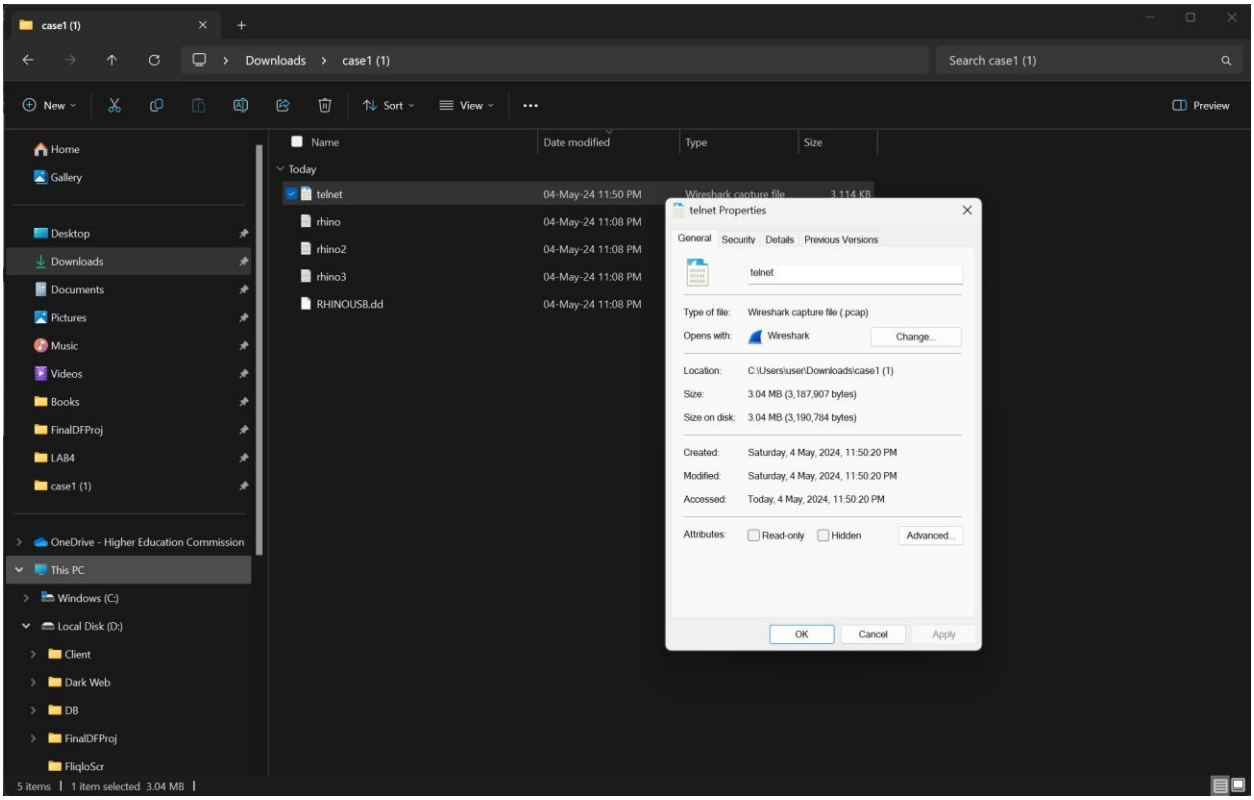
4. Rhino Hunt with Wireshark

OPENING RHINO LOG:

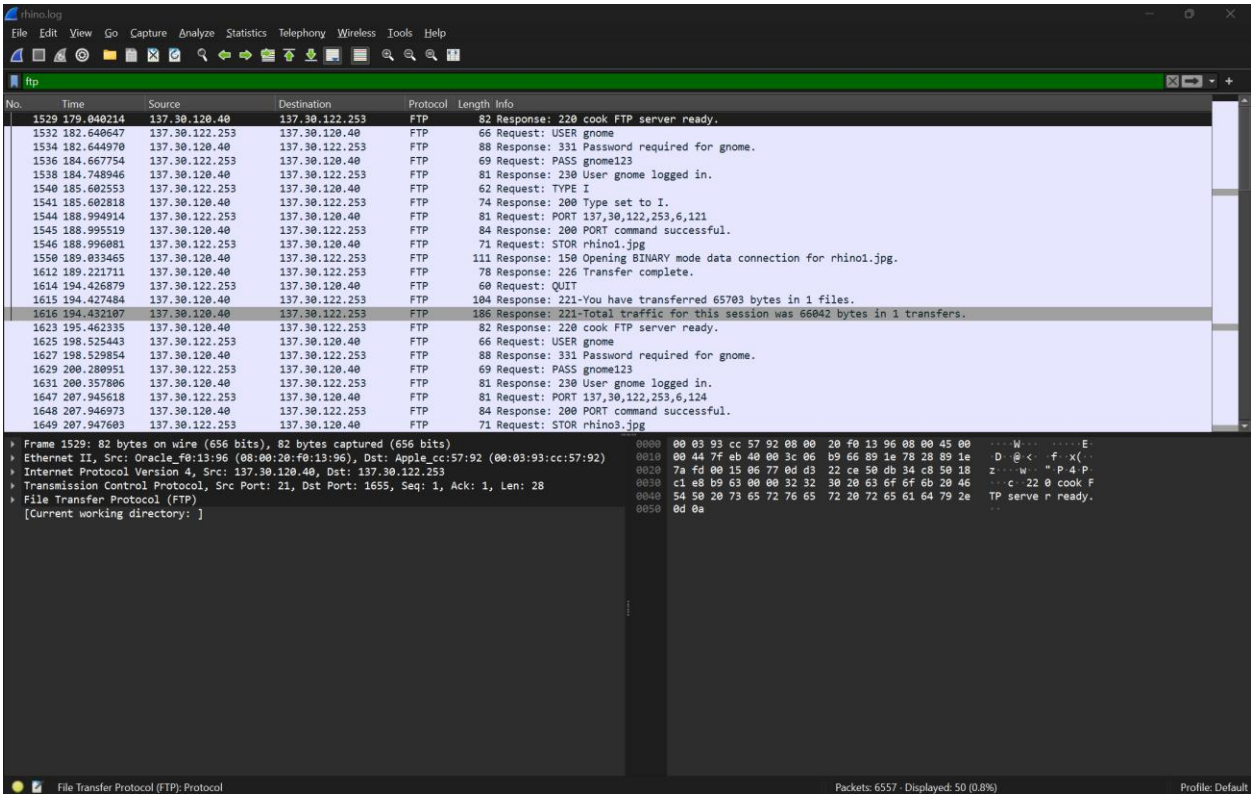


FINDING TELNET PACKETS:

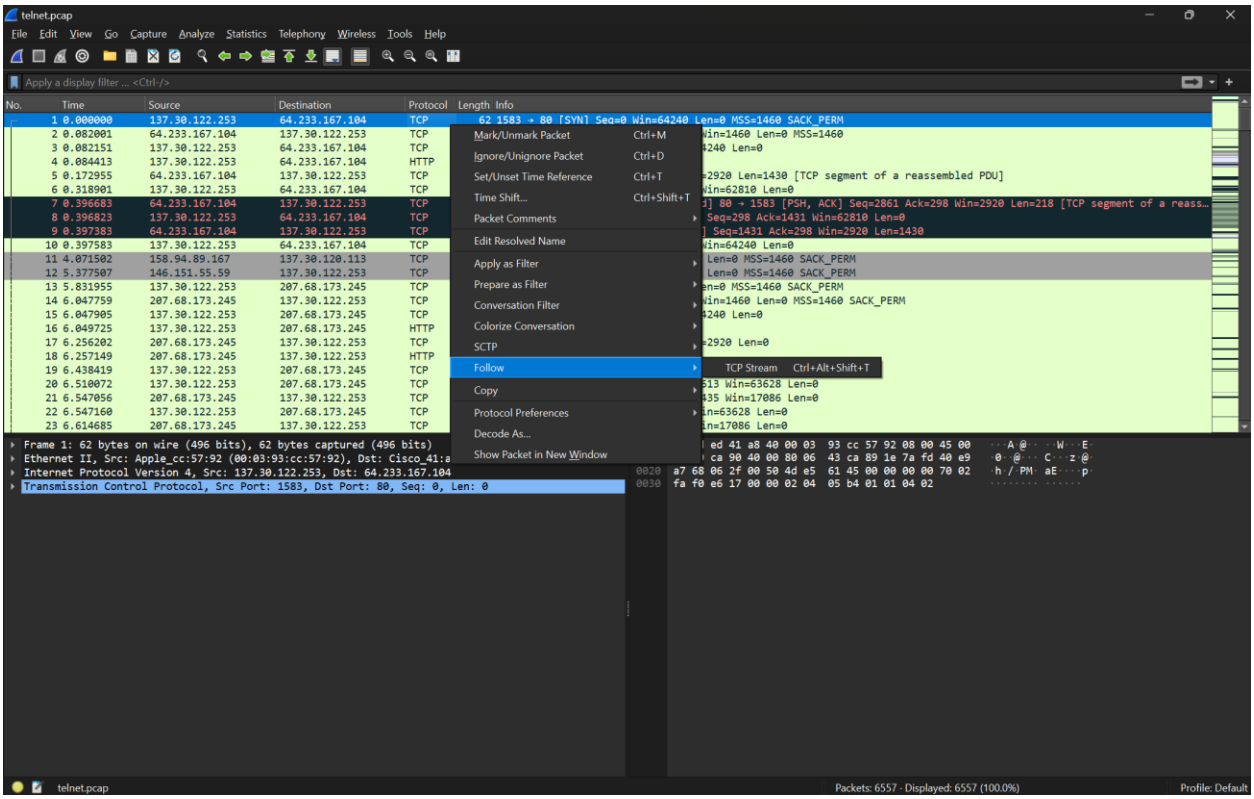


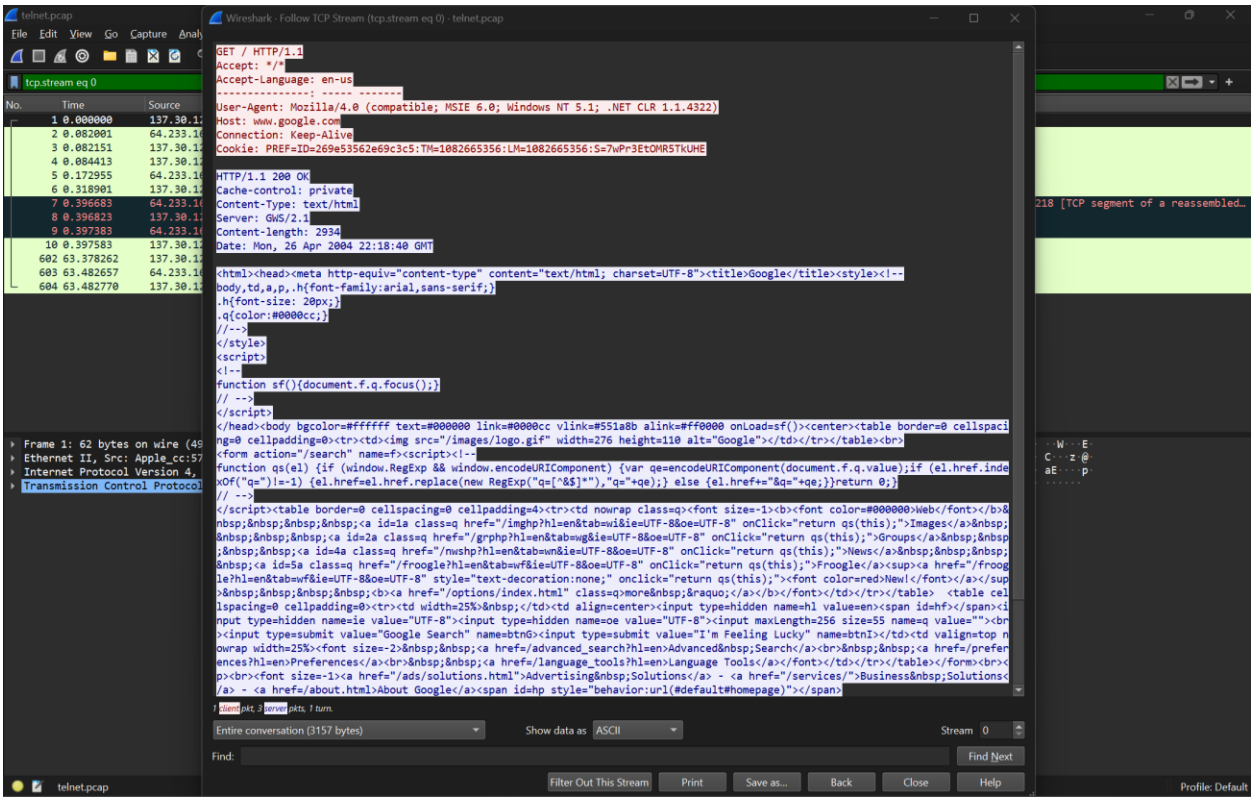


FINDING FTP PACKETS:

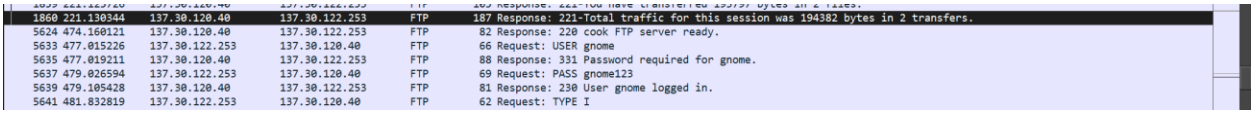


EXAIMINING THE TELNET TRAFFIC:

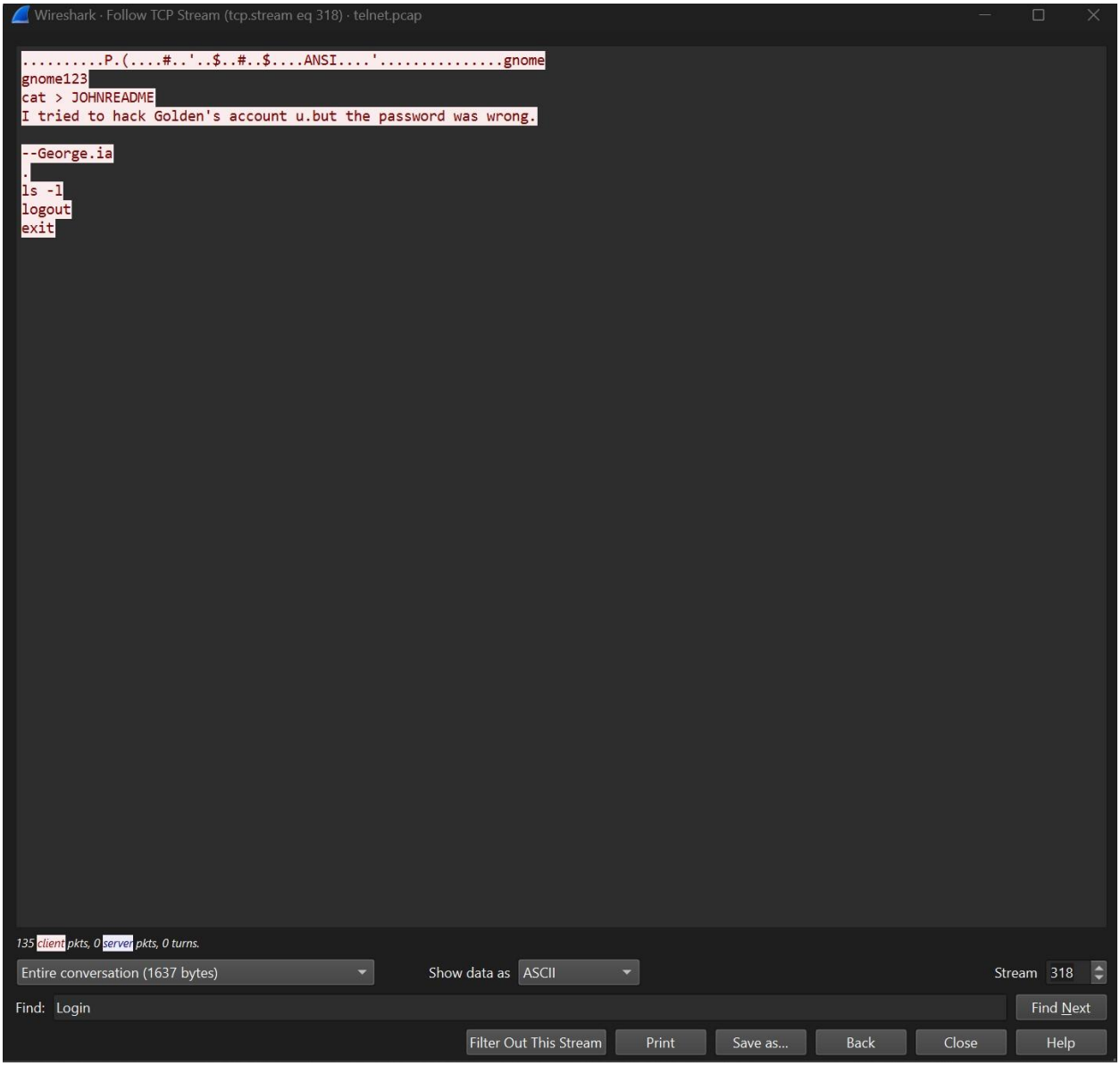




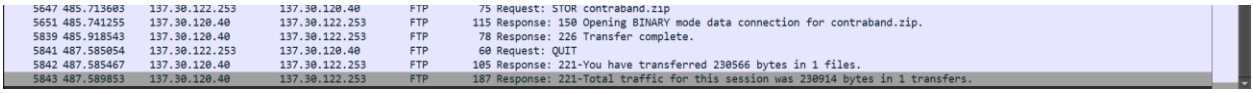
INCORRECT PASSWORD ENTRY:



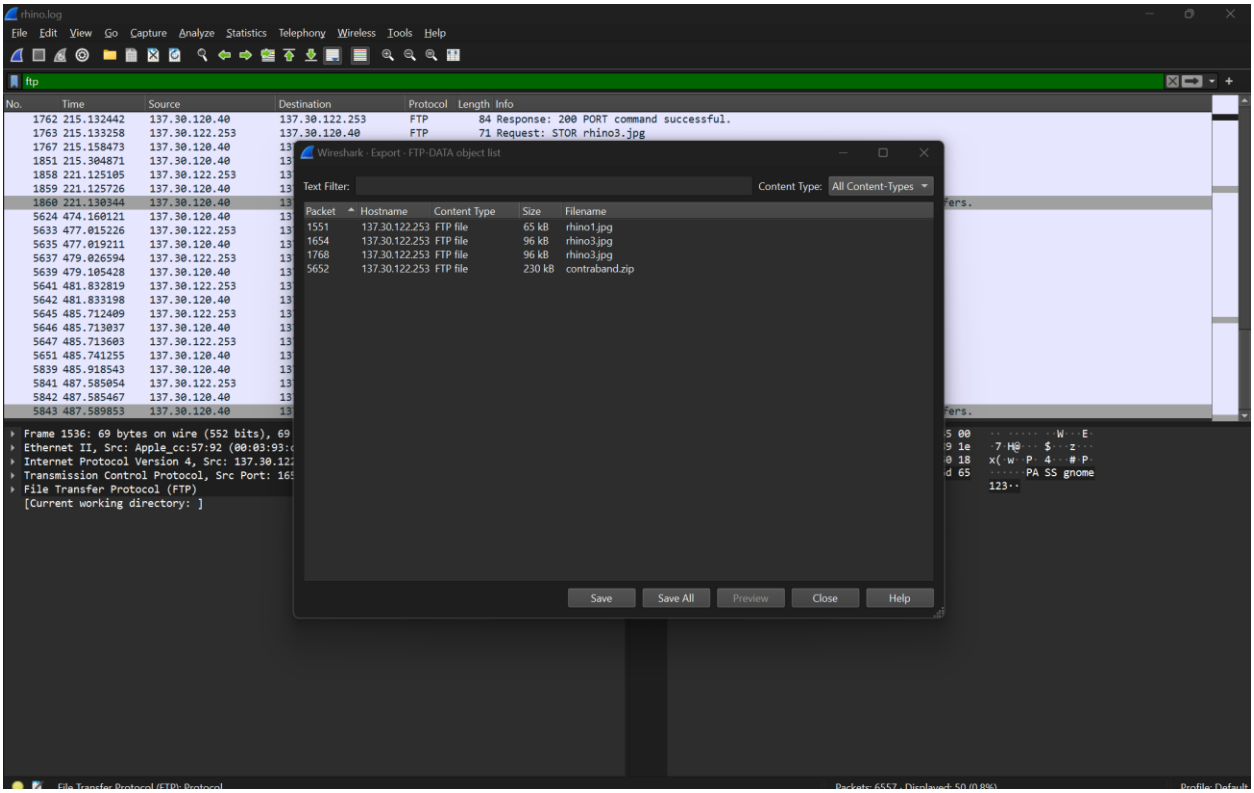
FILENAME:



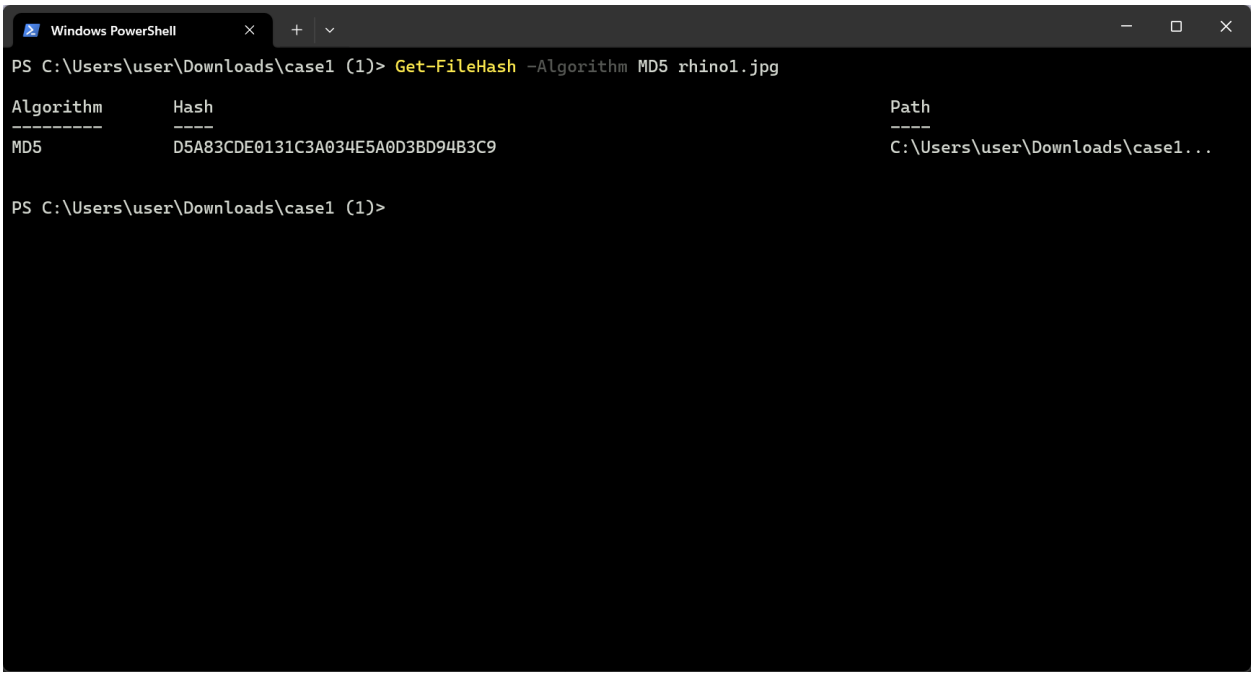
FTP FILENAME FINDING:



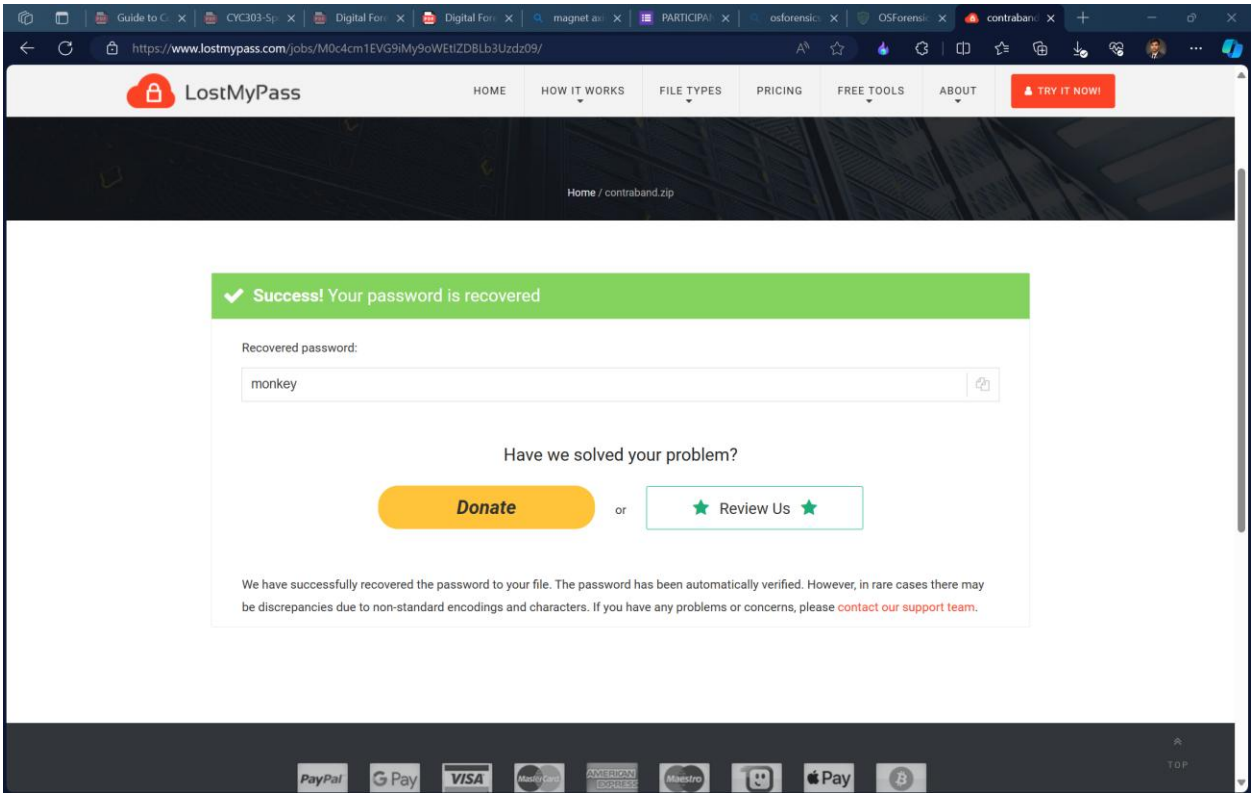
EXTRACTING IMAGES FROM THE FTP-DATA TRAFFIC:



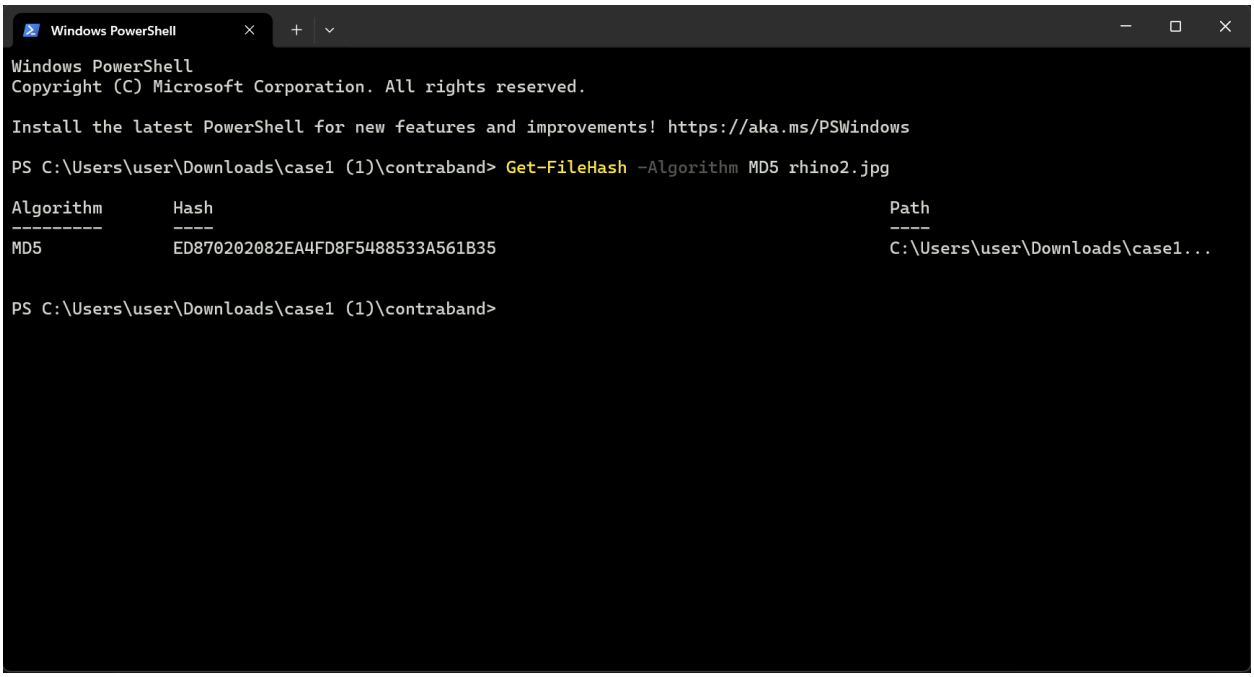
EXAMINING HASH-FILE:



ZIP PASSWORD CRACKING:

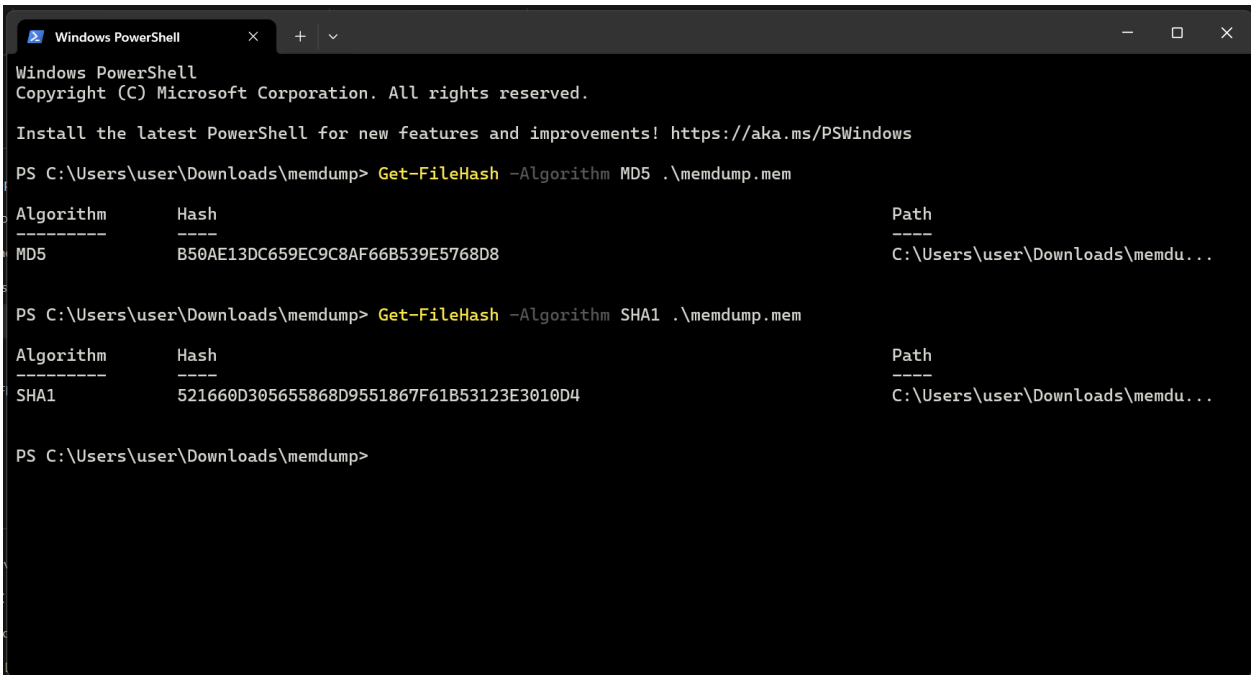


EXAIMING FILE HASH OF RHINO 2:

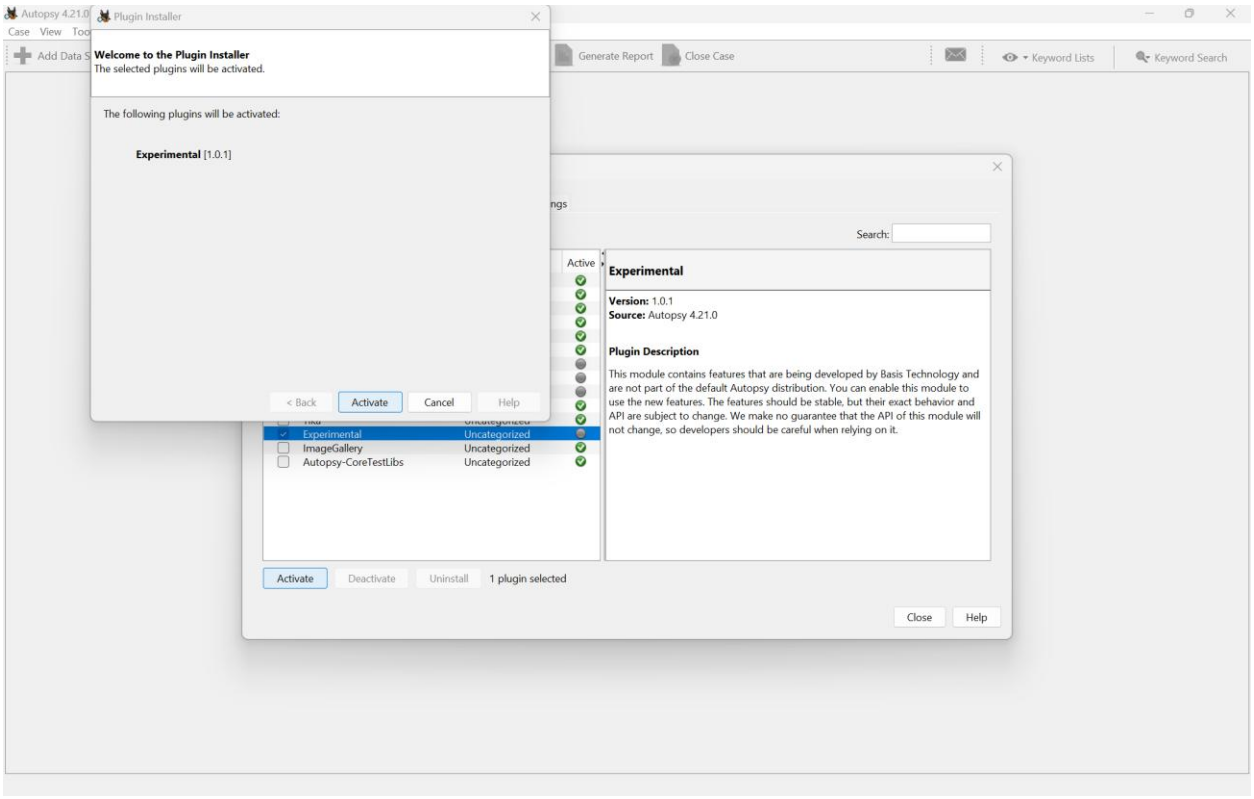


5. Memory Analysis with Autopsy

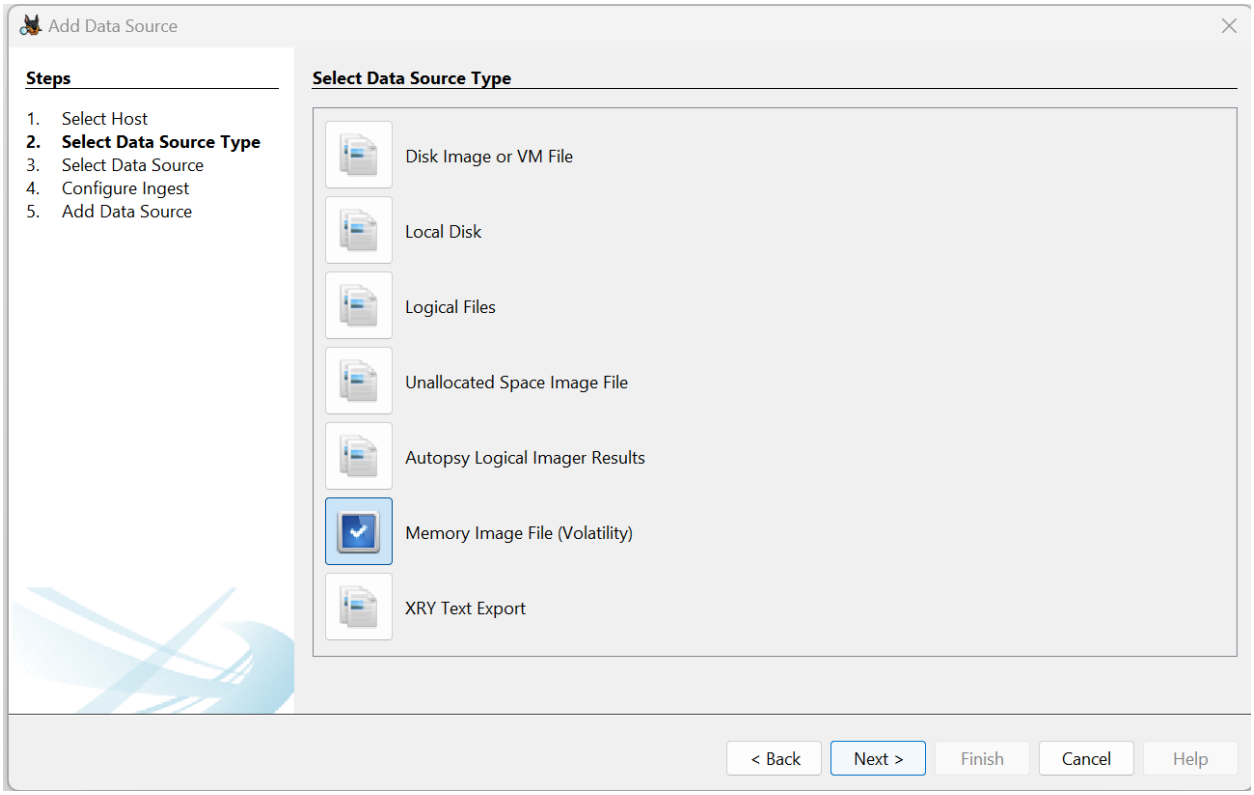
EXAMINING FILE HASH BY TERMINAL:

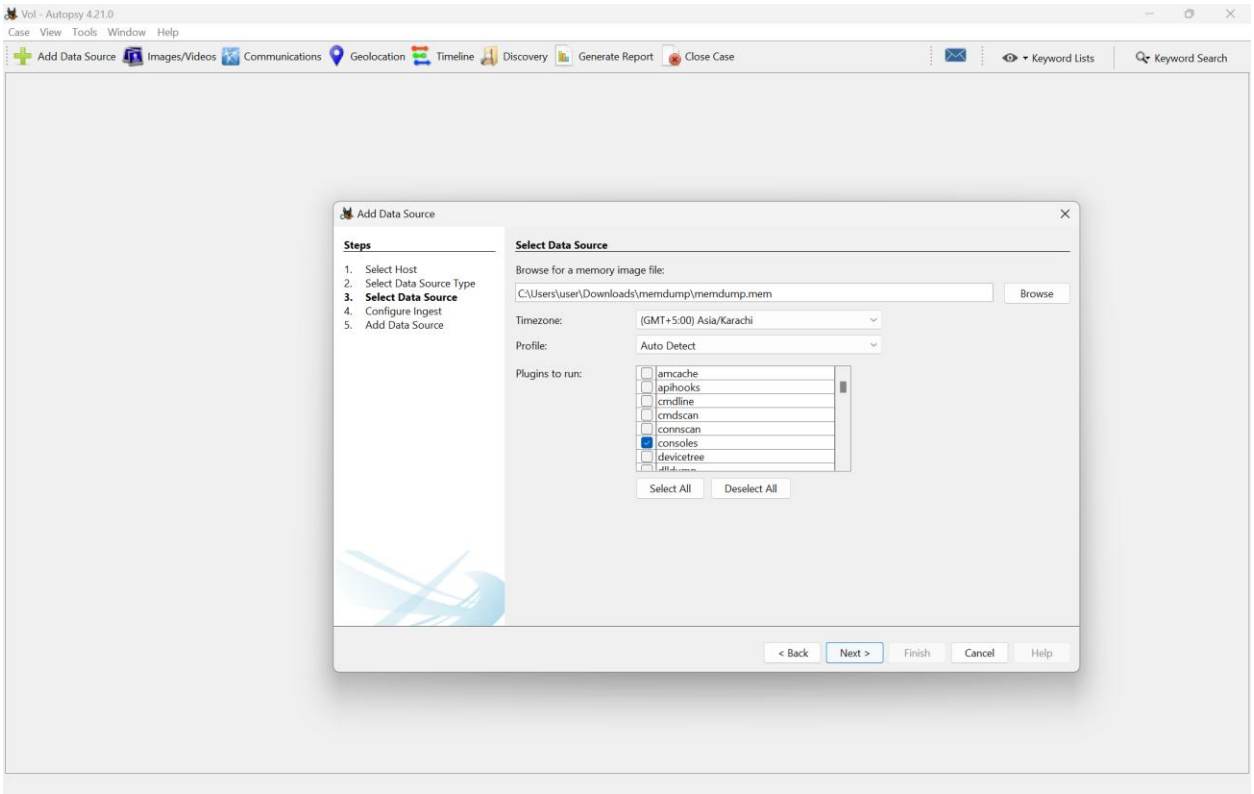


AUTOPSY PLUGGIN INSTALLATION:

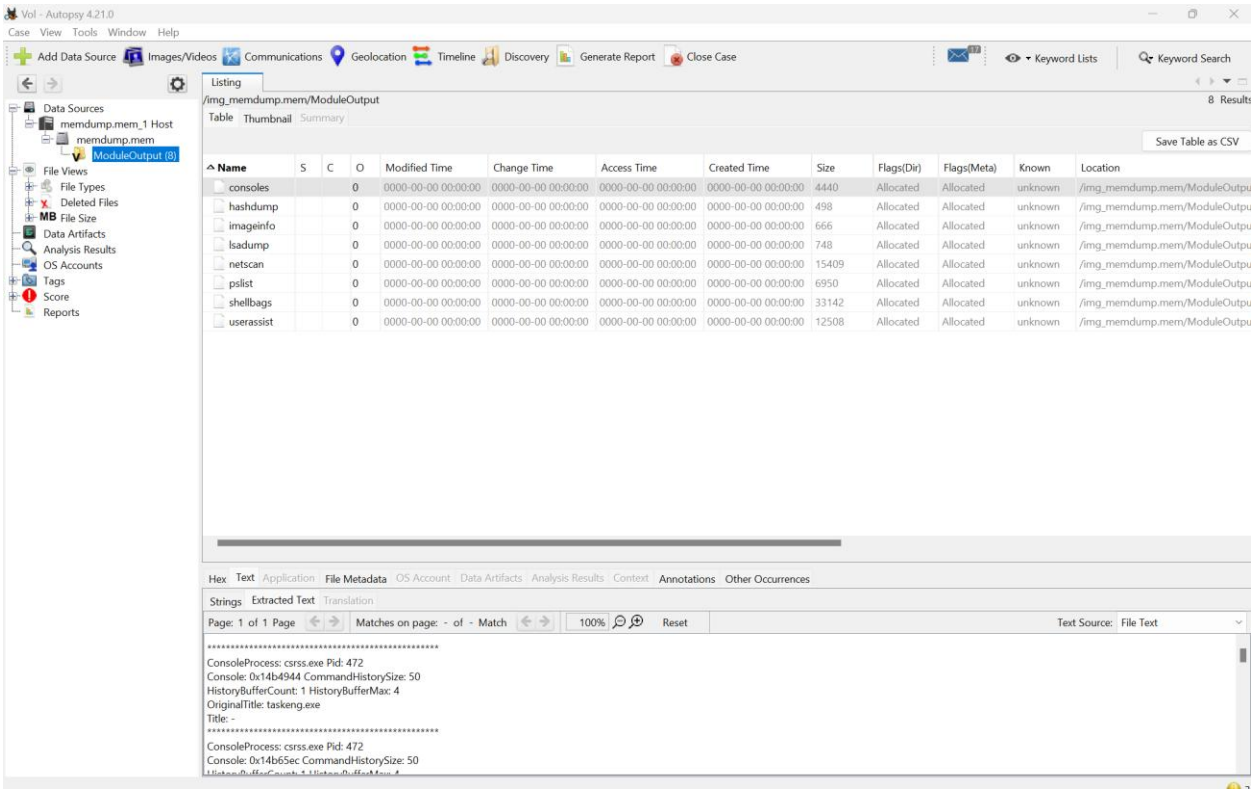


IMPORTING THE MEMORY IMAGE:

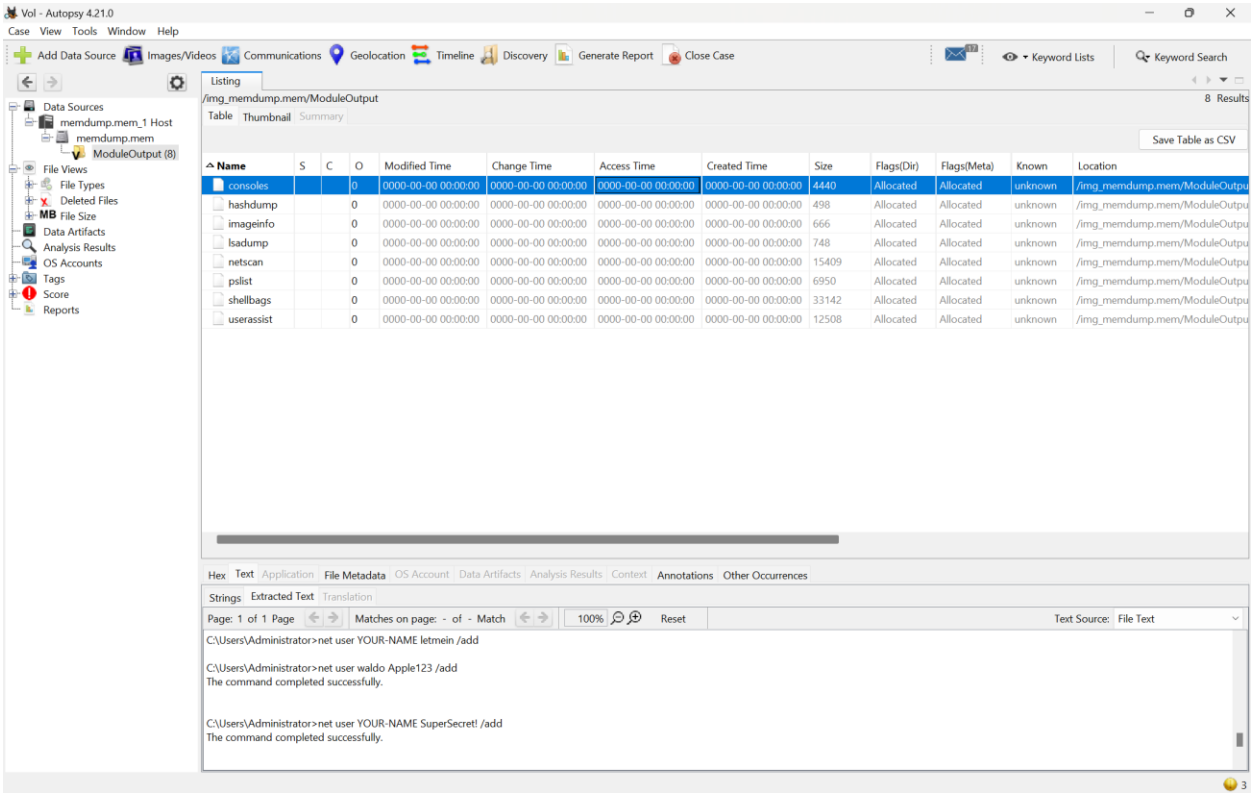




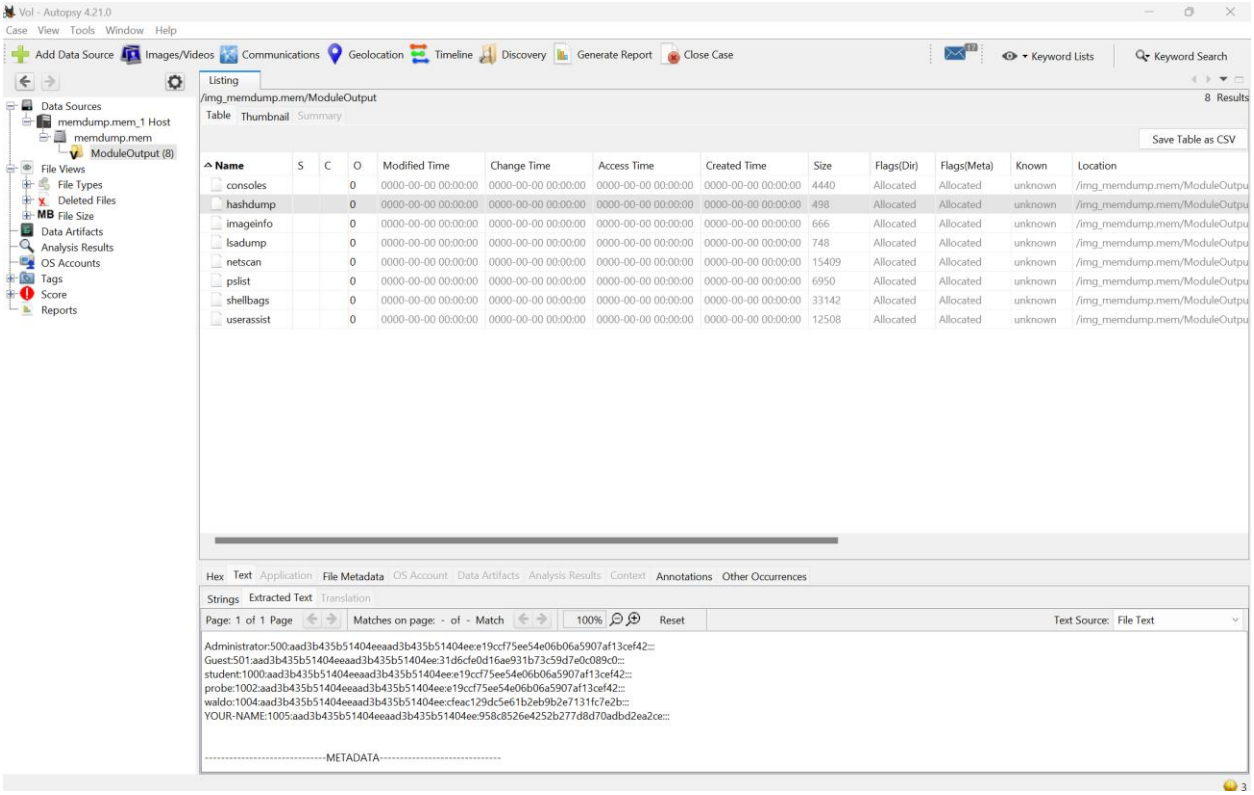
DATASOURCES:



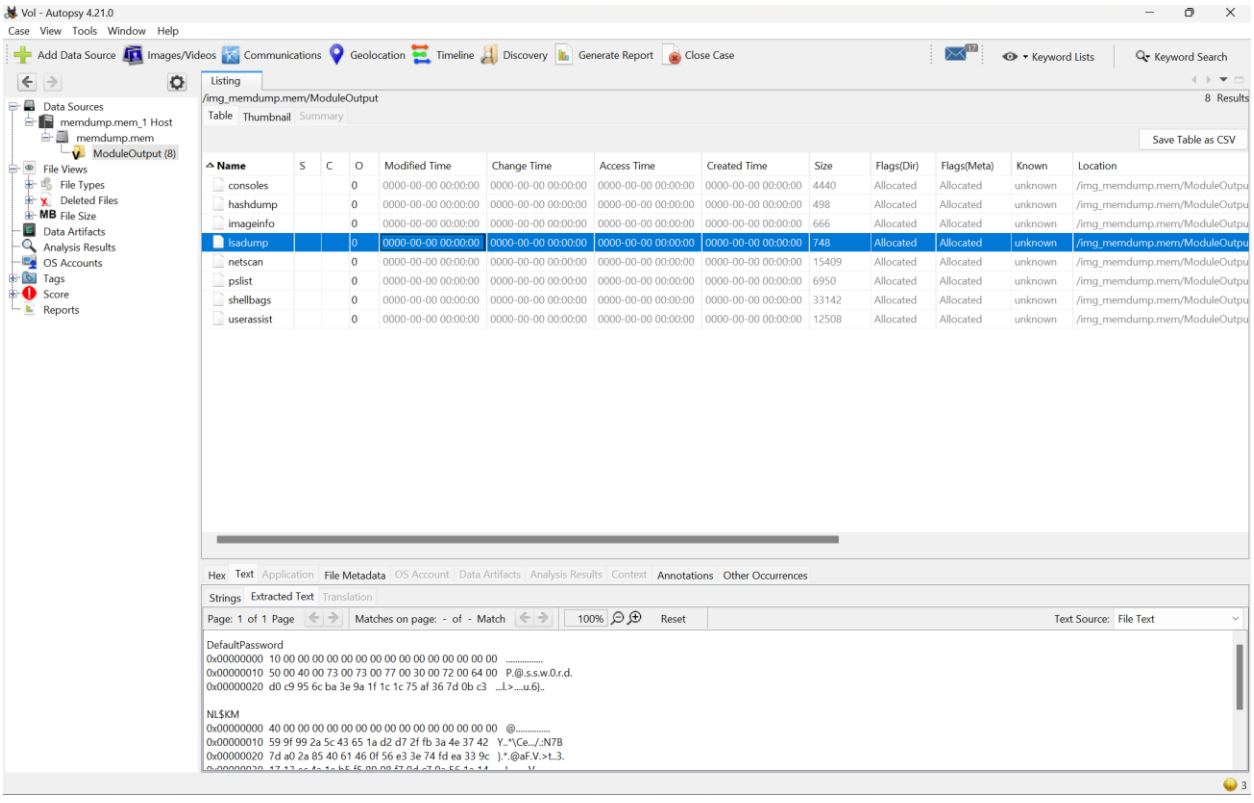
CONSOLES SECTION:



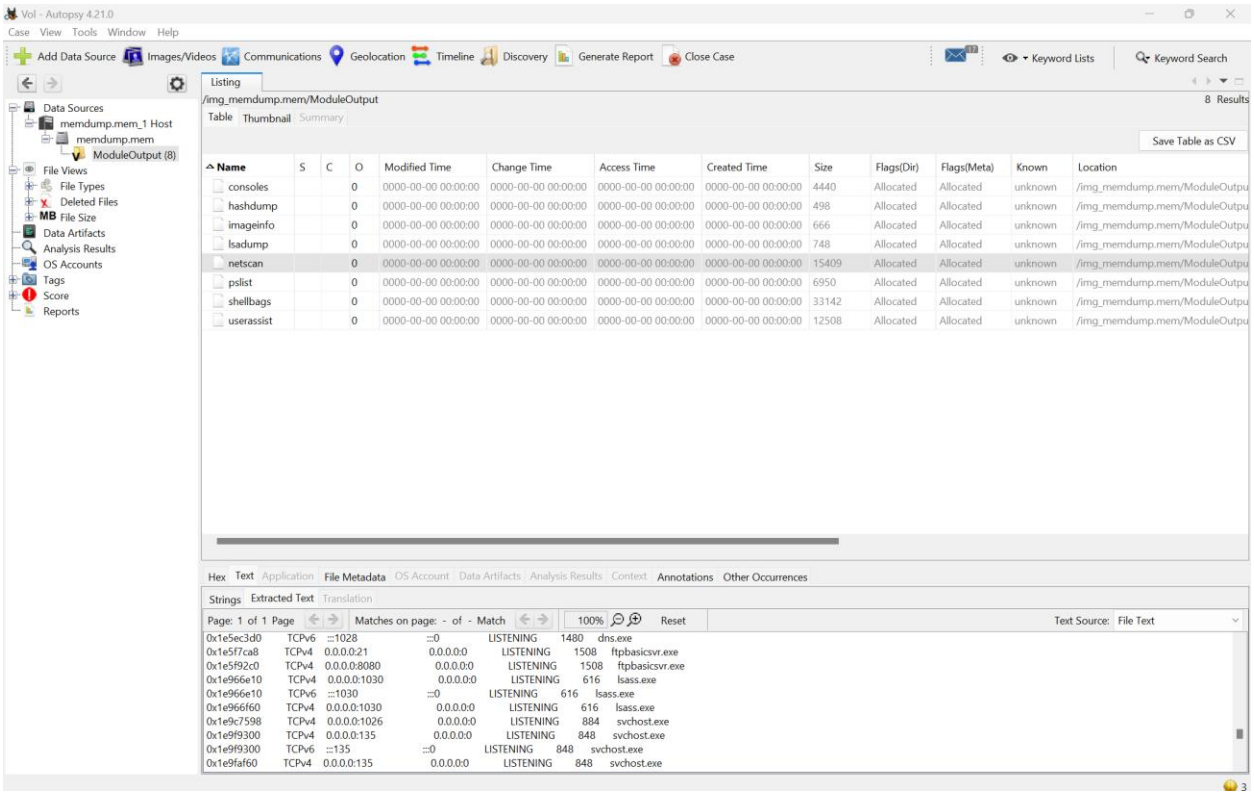
HASHDUMP SECTION:



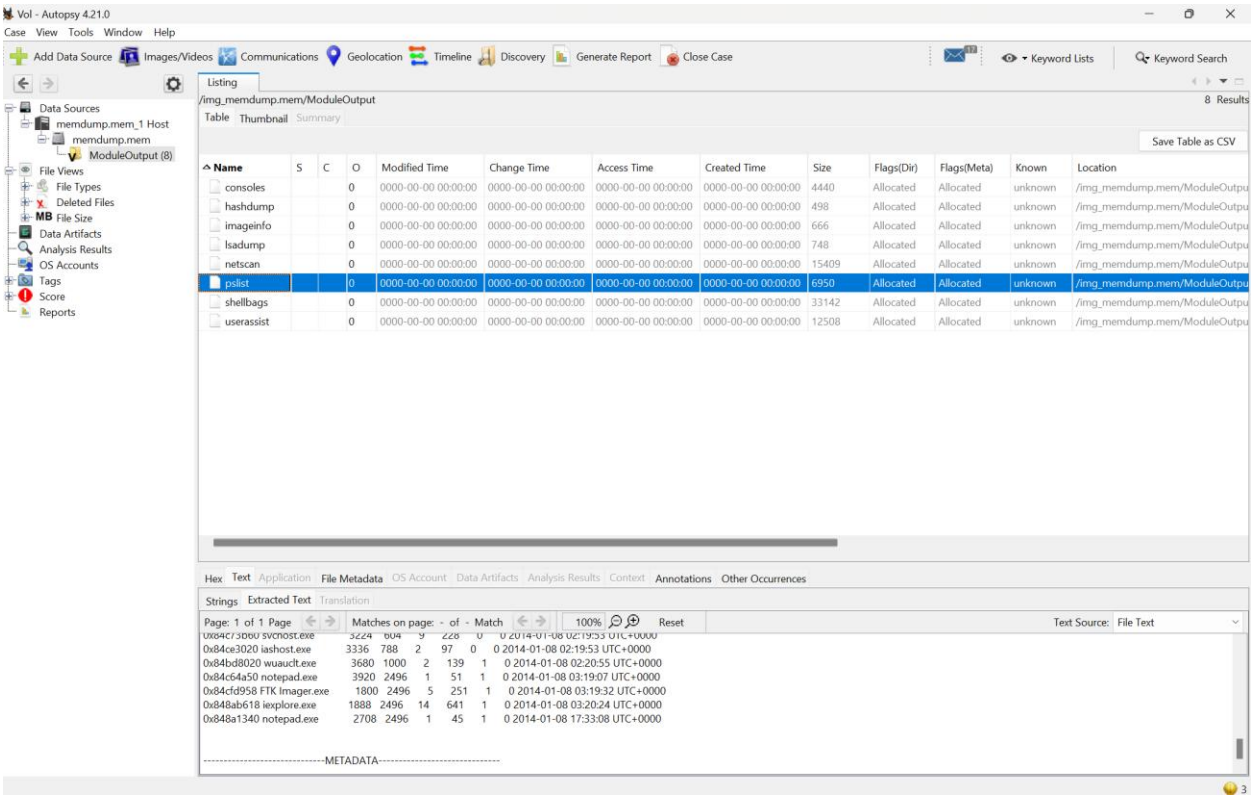
LSADUMP SECTION:



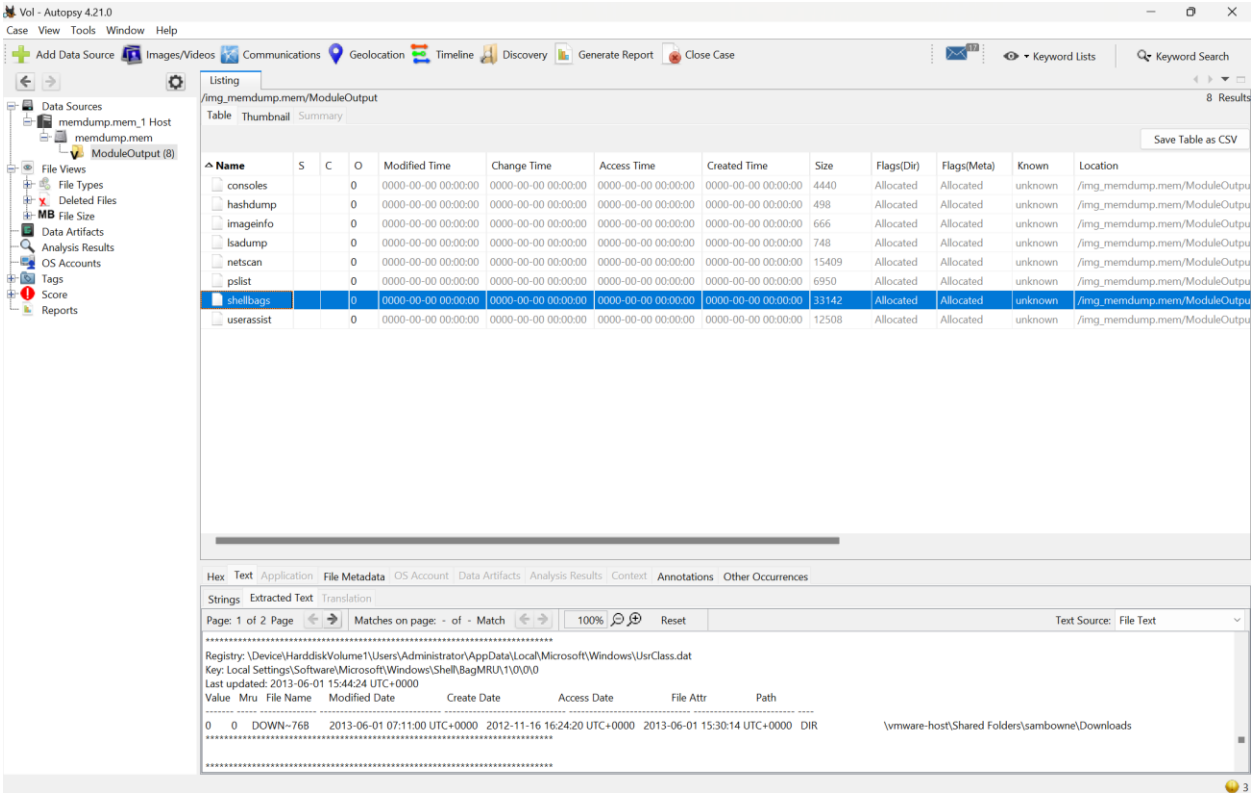
NETSCAN SECTION:



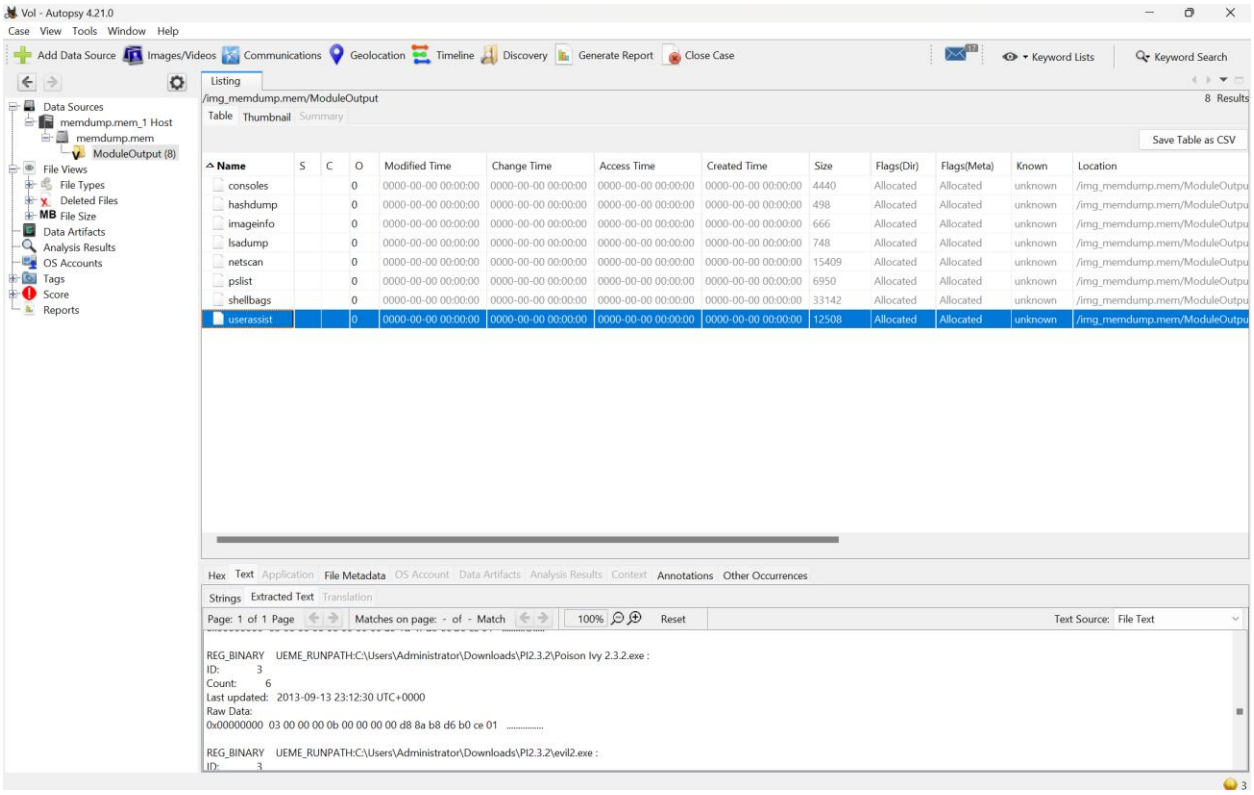
PSLIST SECTION:



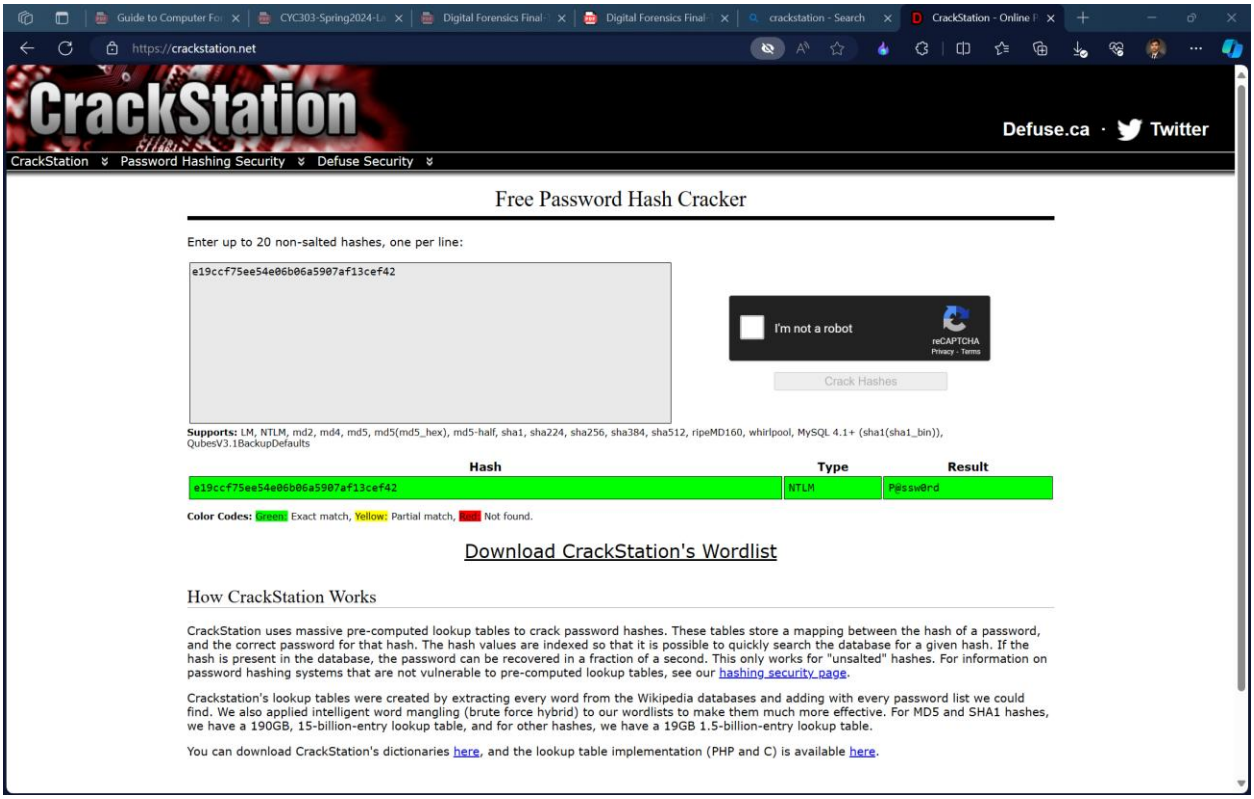
SHELLBAGS SECTION:



USERASSIST SECTION:

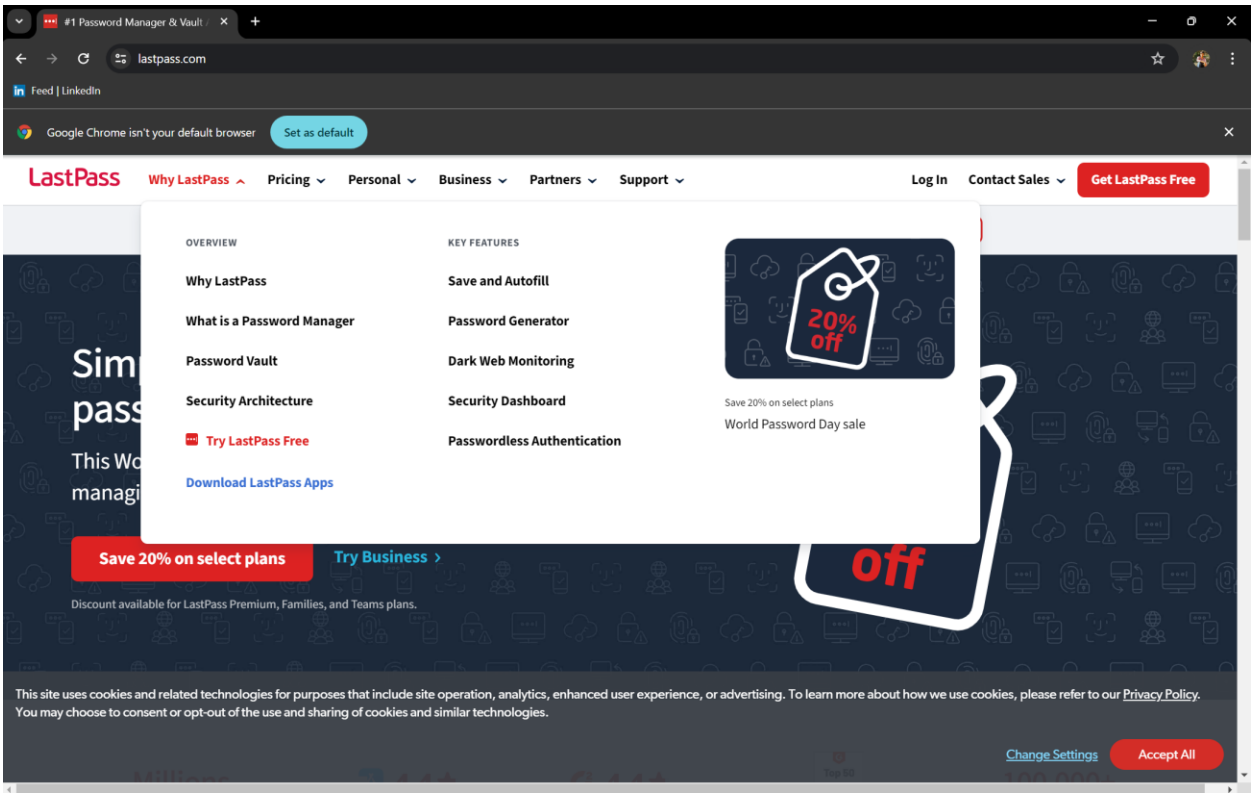


PROBE PASSWORD:

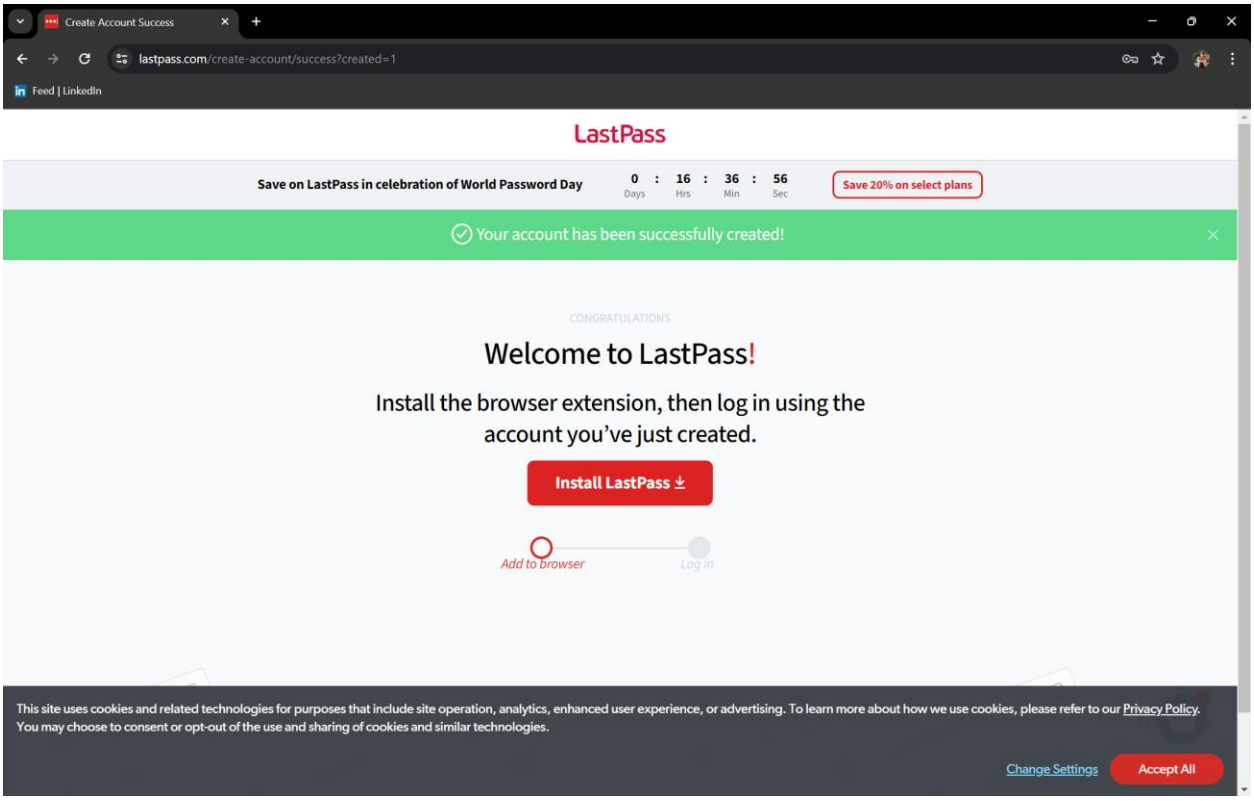


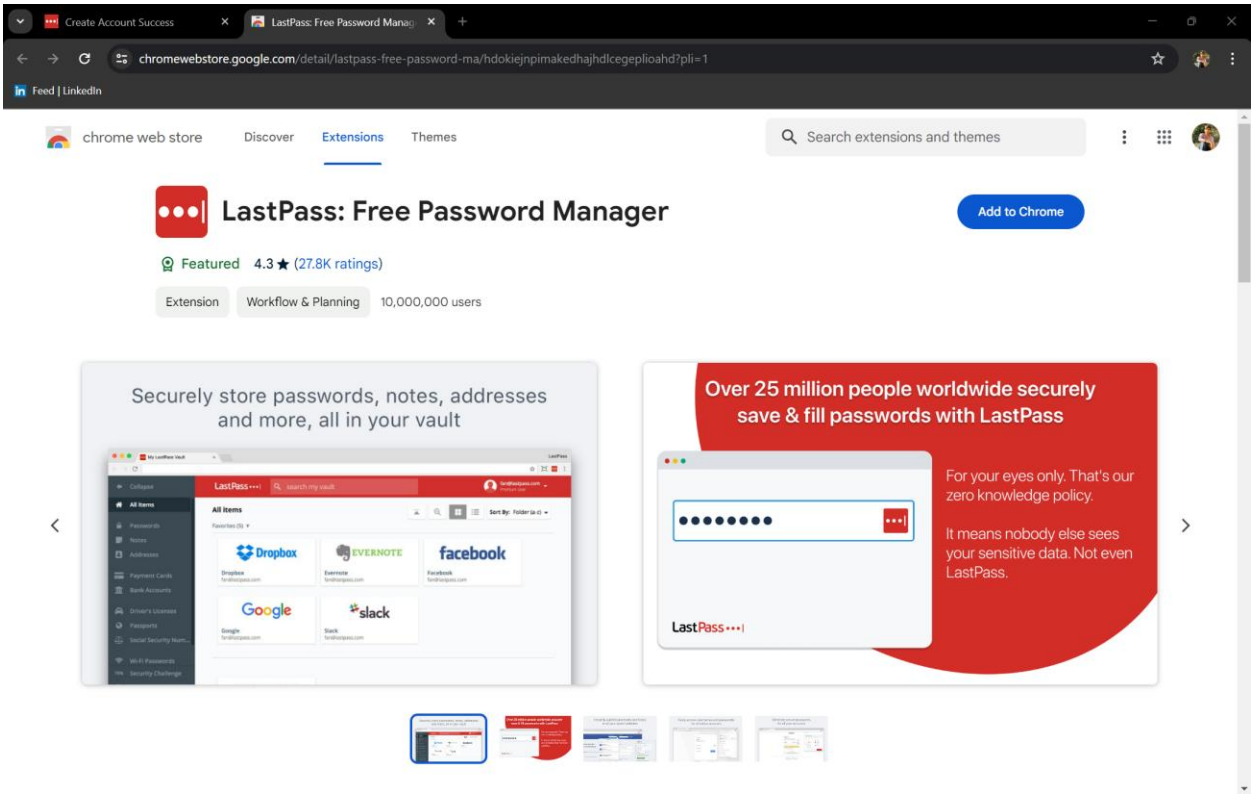
6. Memory Forensics of LastPass and Keeper

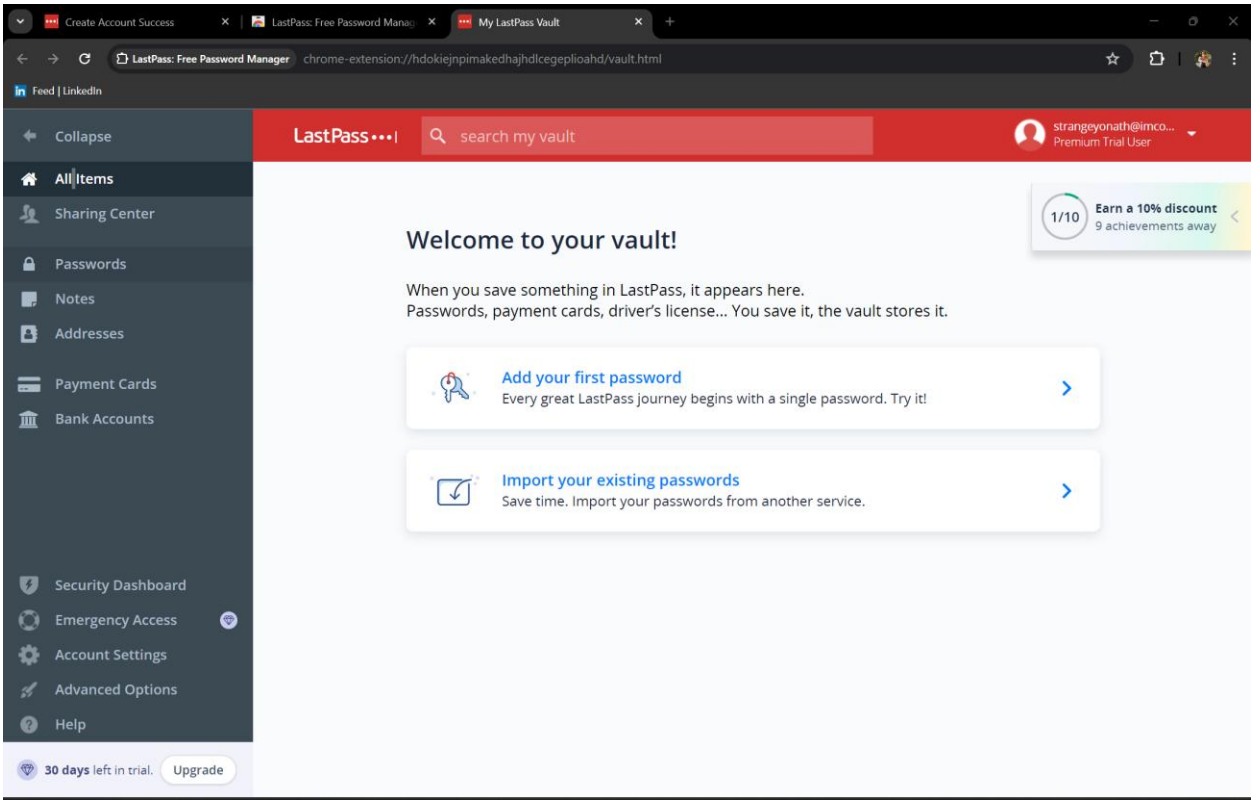
LASTPASS OPENED ON CHROME:



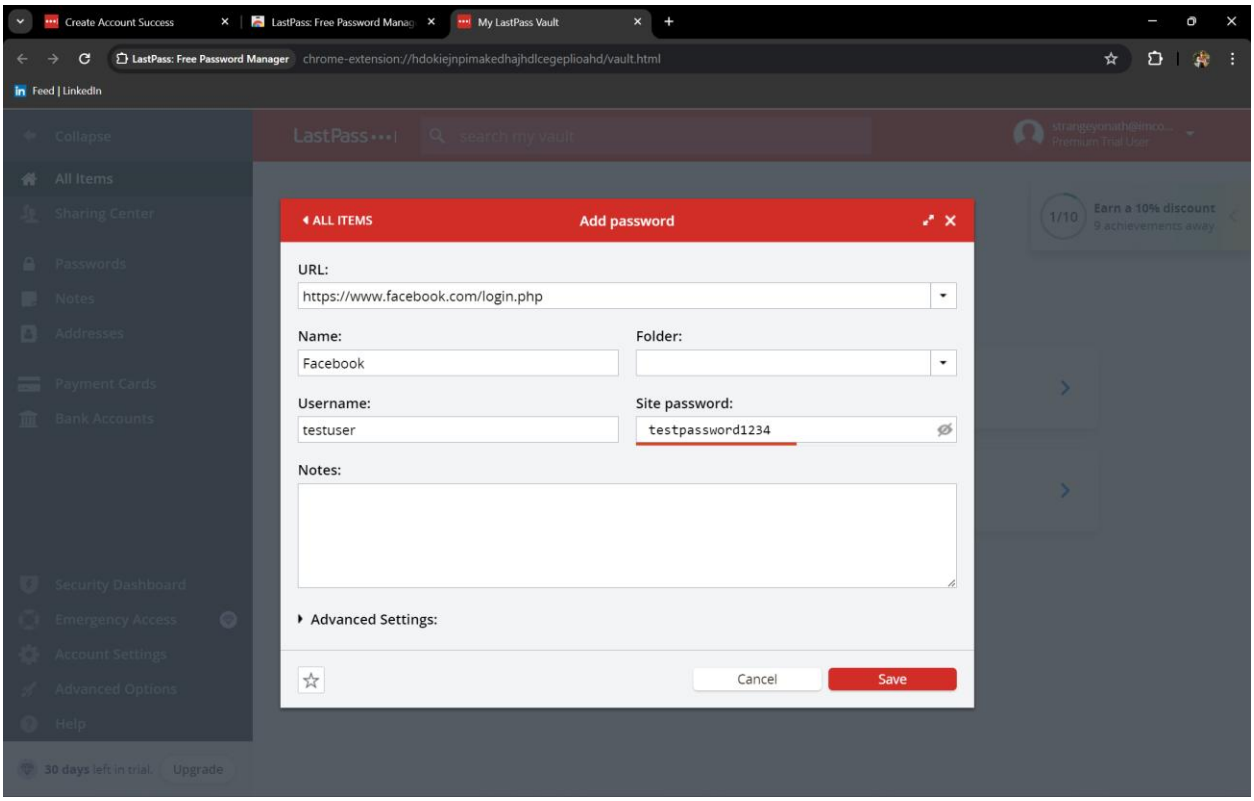
LASTPASS ACCOUNT CREATION



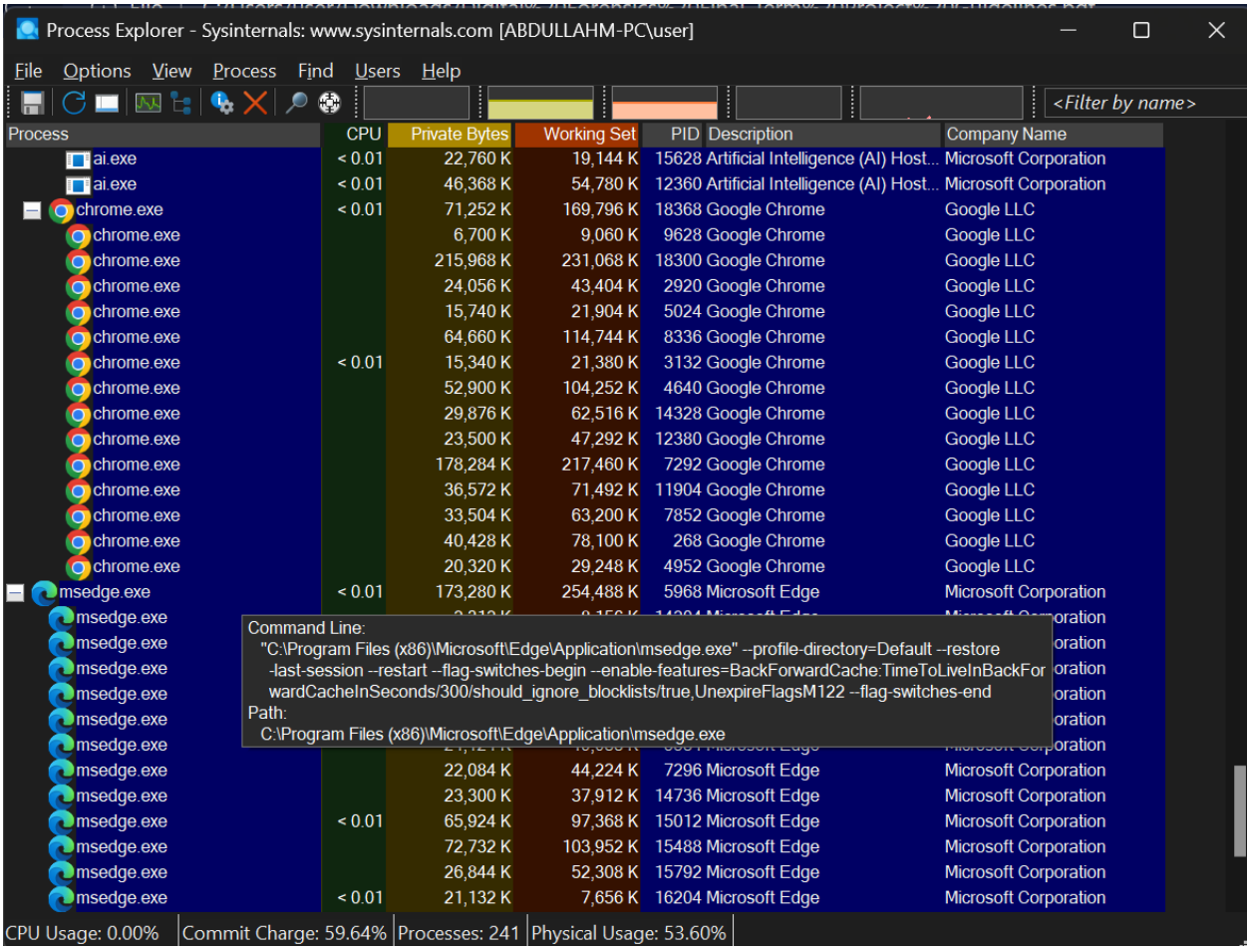




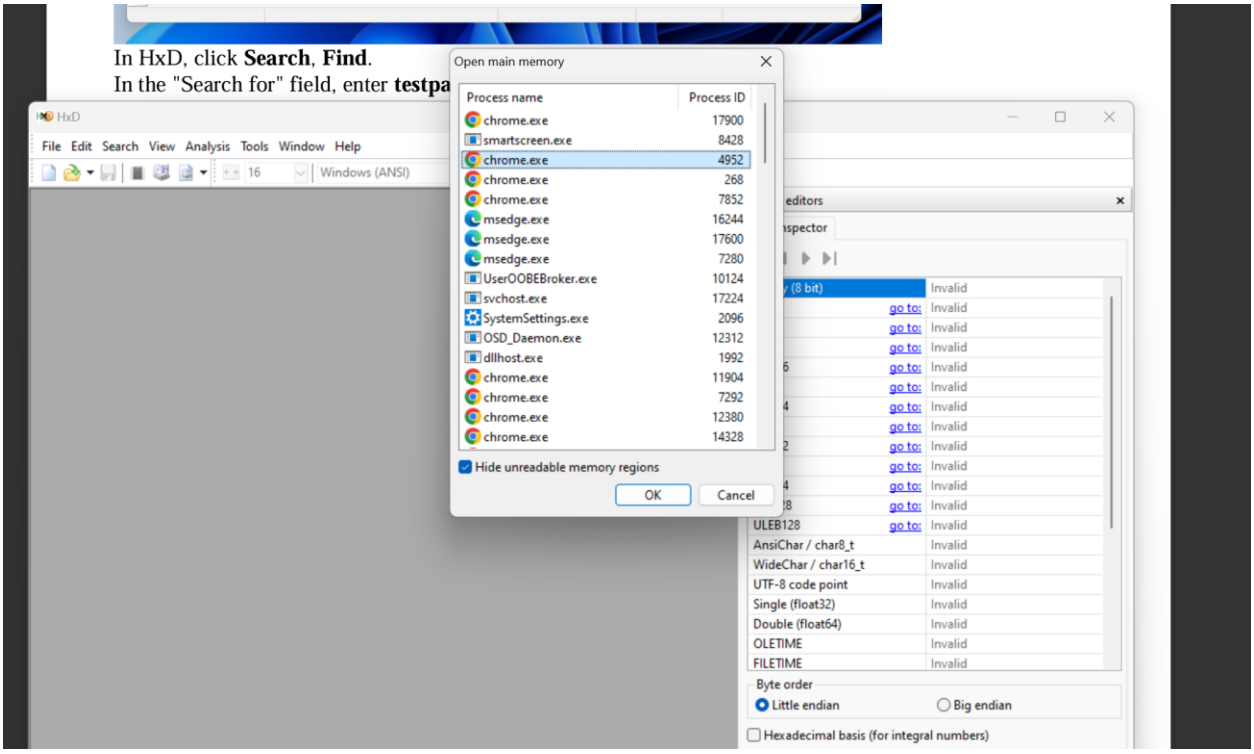
FACEBOOK ACCOUNT CREATION:

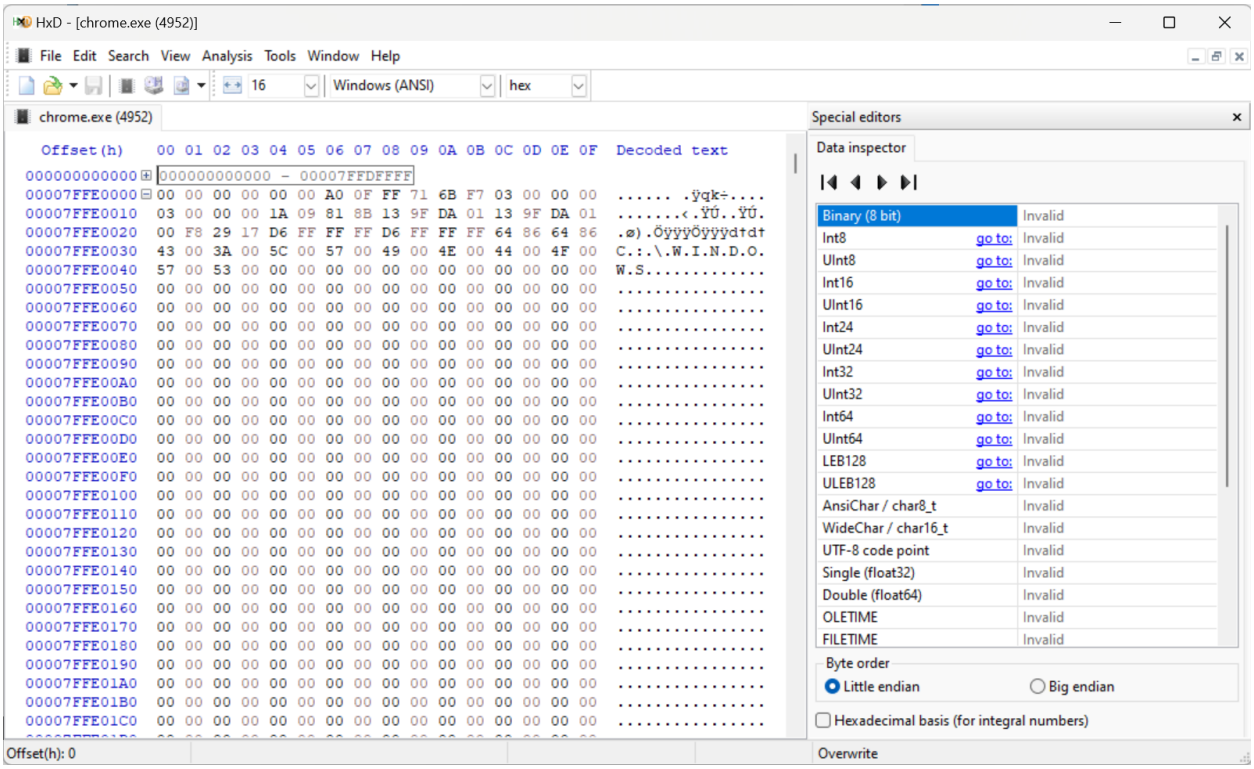


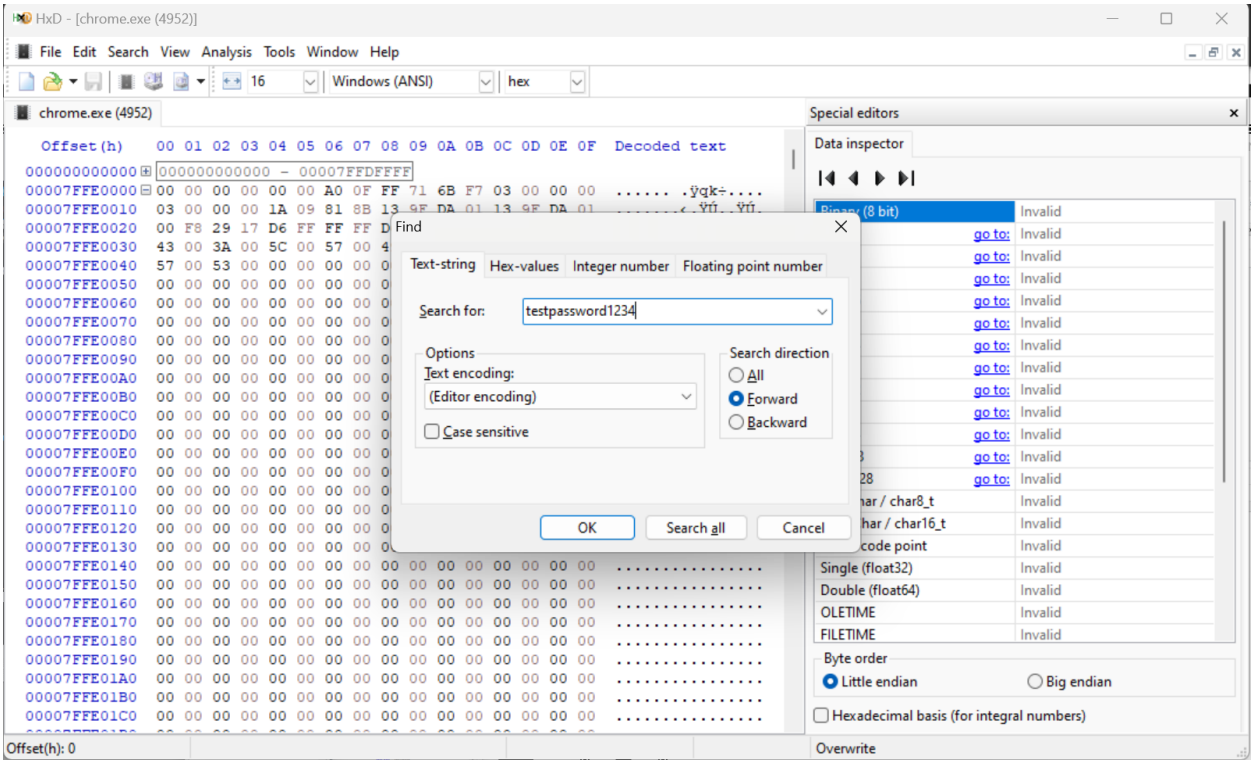
PROCESS EXPLORER EXAMINATION:

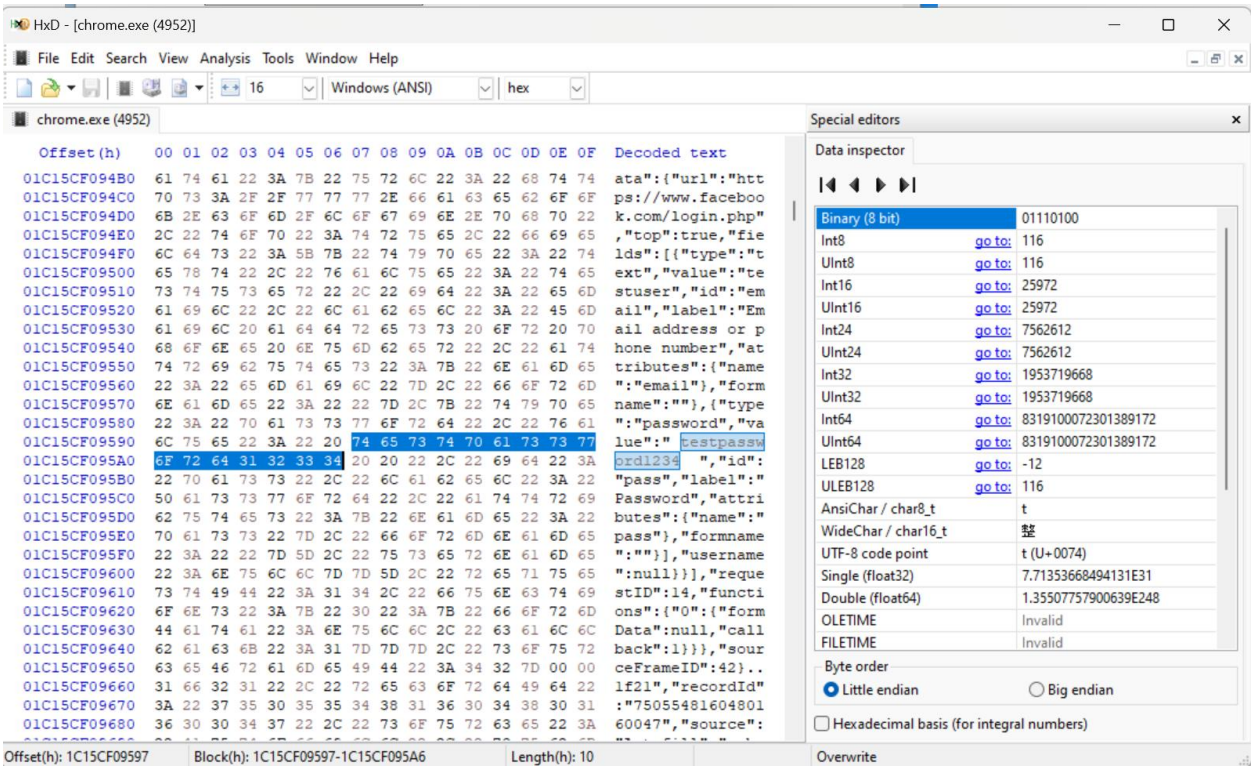


HxD EXAMINATION:

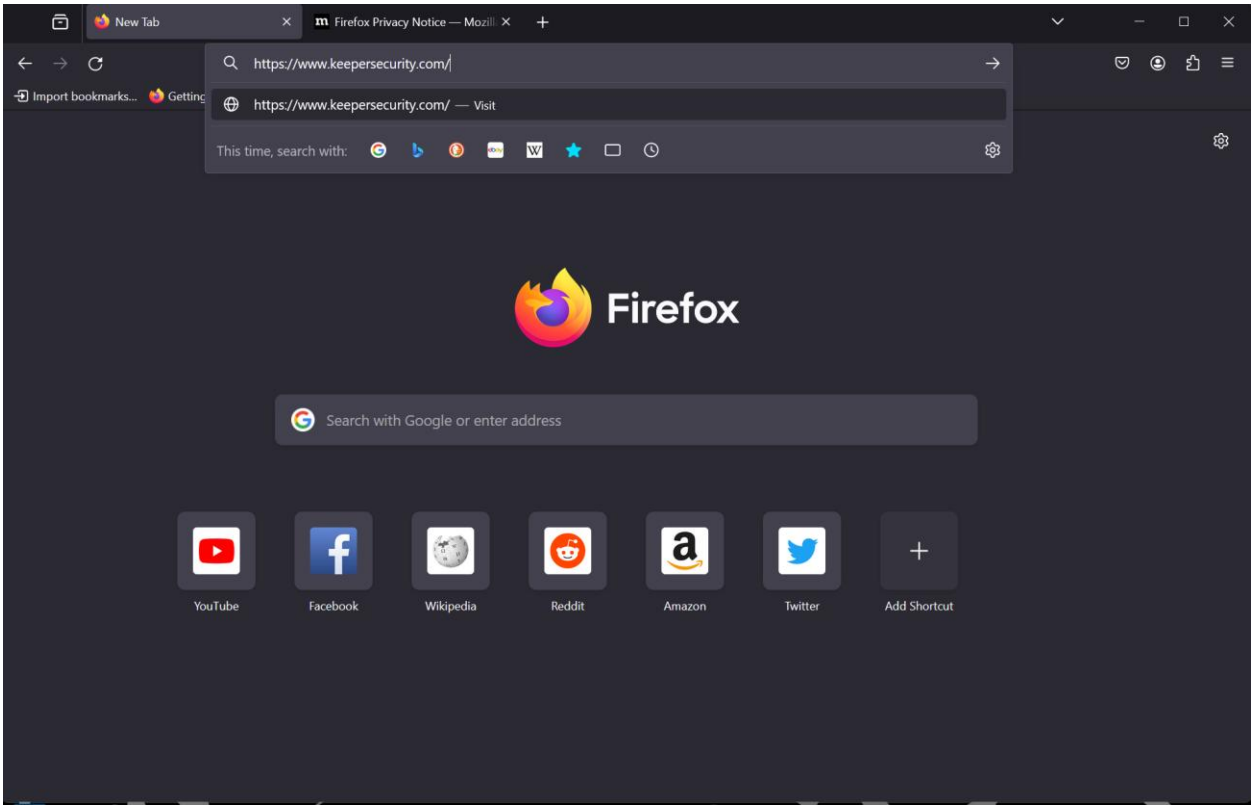


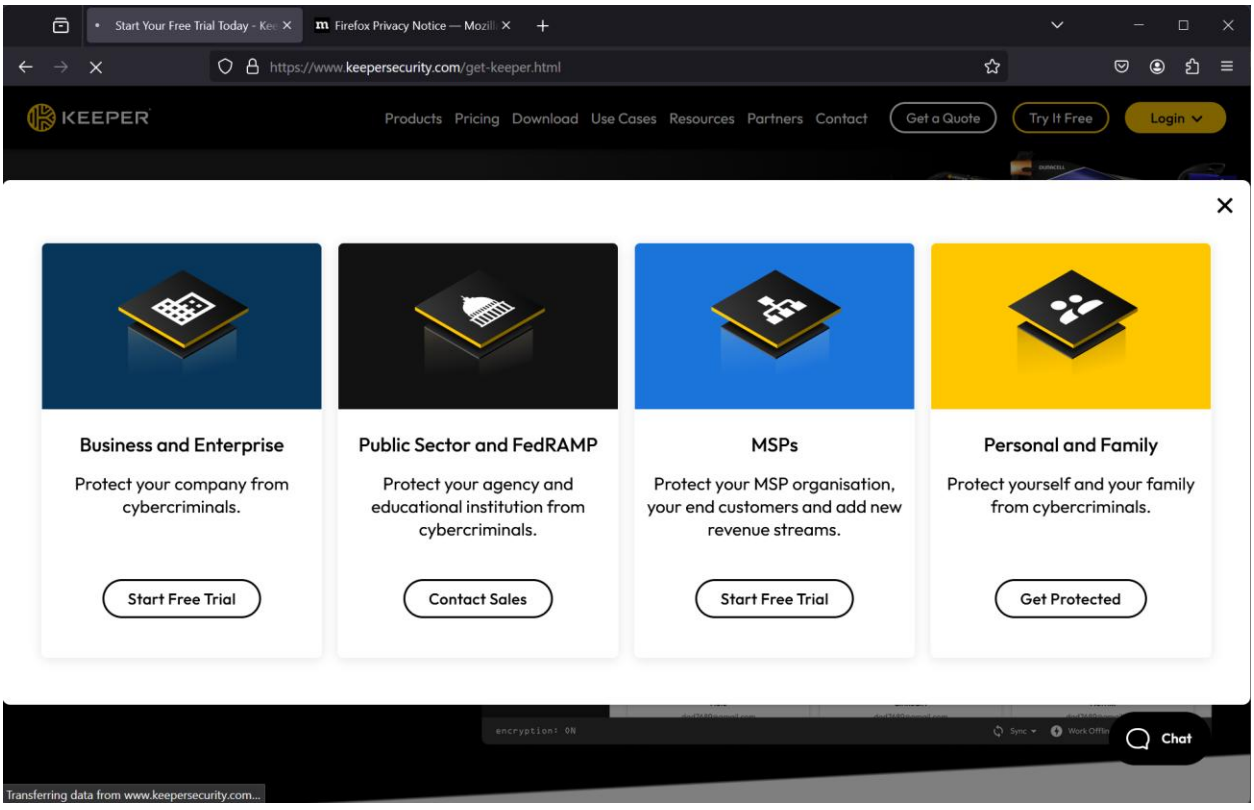


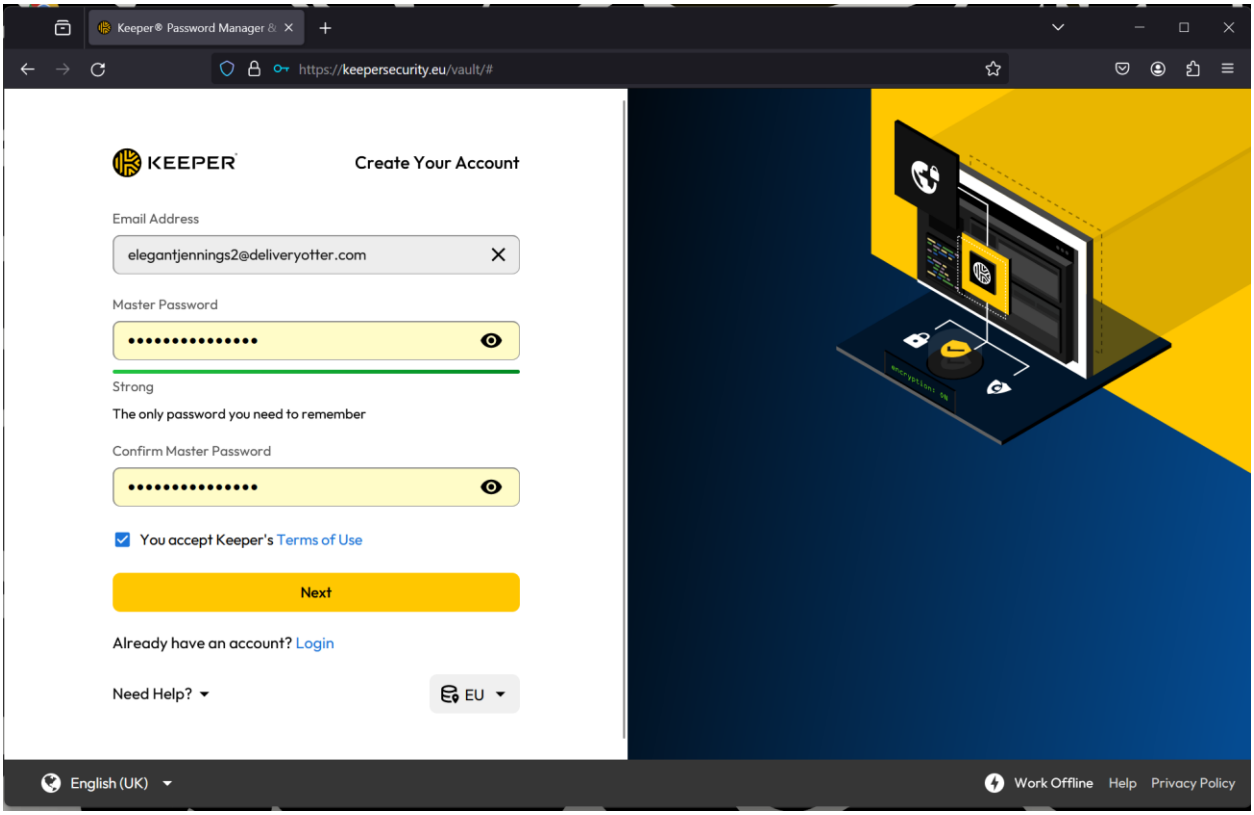

HxD - [chrome.exe (4952)]
File Edit Search View Analysis Tools Window Help
chrome.exe (4952)
Special editors
Data inspector
Find
Text-string
Hex-values
Integer number
Floating point number
Search for:
testpassword1234
Options
Text encoding:
(Editor encoding)
Case sensitive
Search direction
All
Forward
Backward
OK
Search all
Cancel
Offset(h): 0
Overwrite

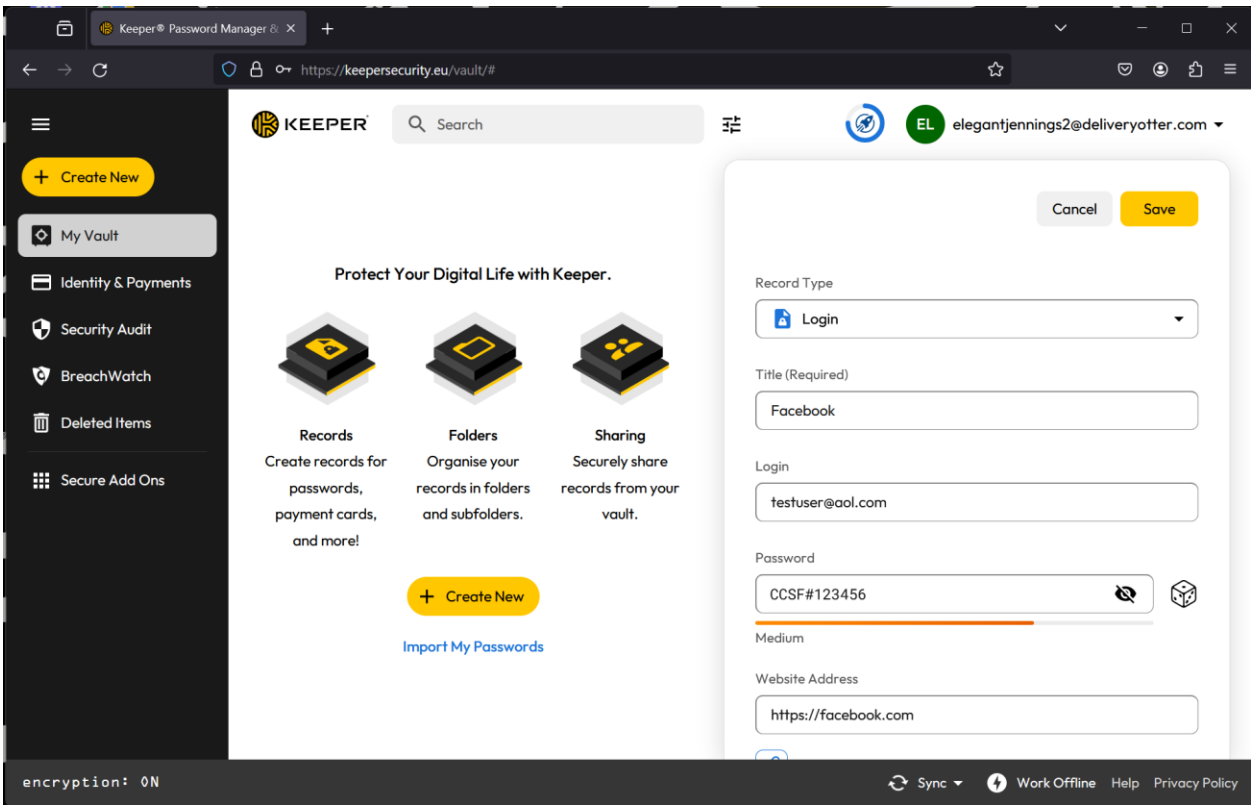

HxD - [chrome.exe (4952)]
File Edit Search View Analysis Tools Window Help
chrome.exe (4952)
Special editors
Data inspector
Offset(h): 1C15CF09597
Block(h): 1C15CF09597-1C15CF095A6
Length(h): 10
Overwrite

TARGET 2: KEEPER

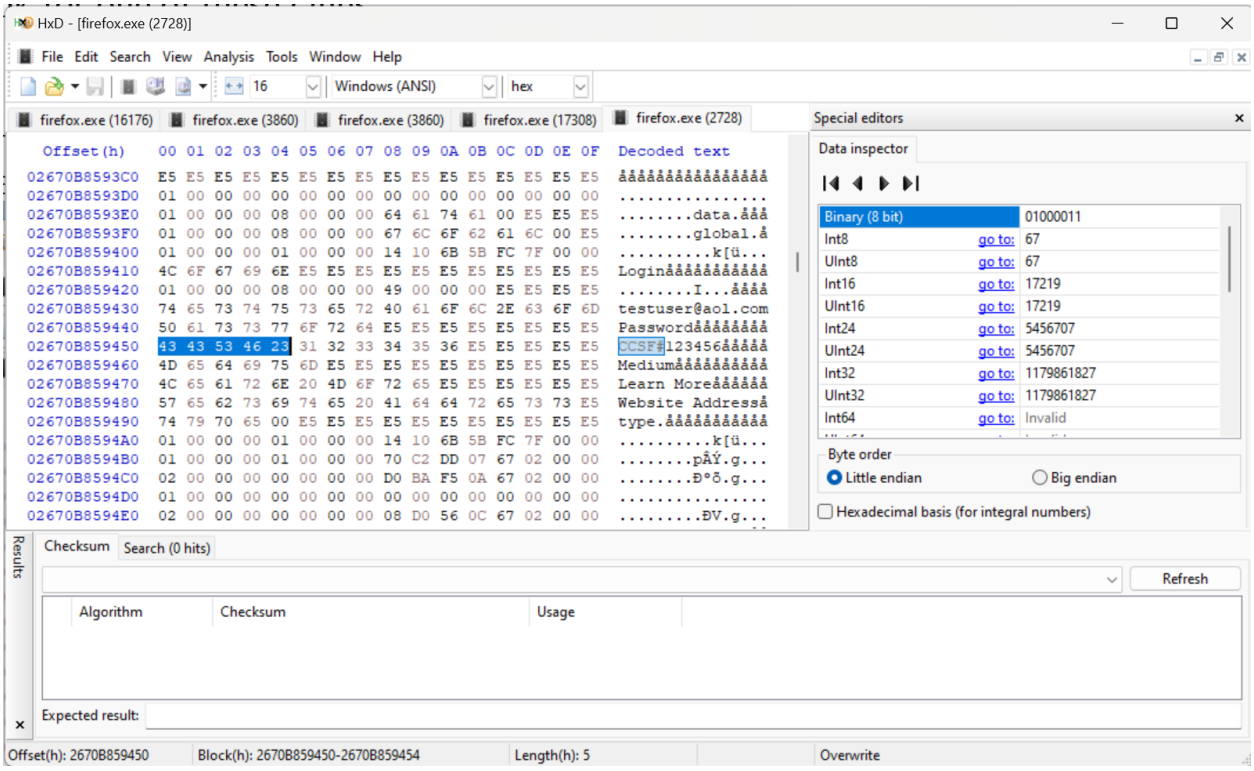





Keeper® Password Manager
https://keepersecurity.eu/vault/#
KEEPER
Create Your Account
Email Address
elegantjennings2@deliveryotter.com
Master Password
Strong
The only password you need to remember
Confirm Master Password
You accept Keeper's Terms of Use
Next
Already have an account? Login
Need Help?
EU
English (UK)
Work Offline
Help
Privacy Policy

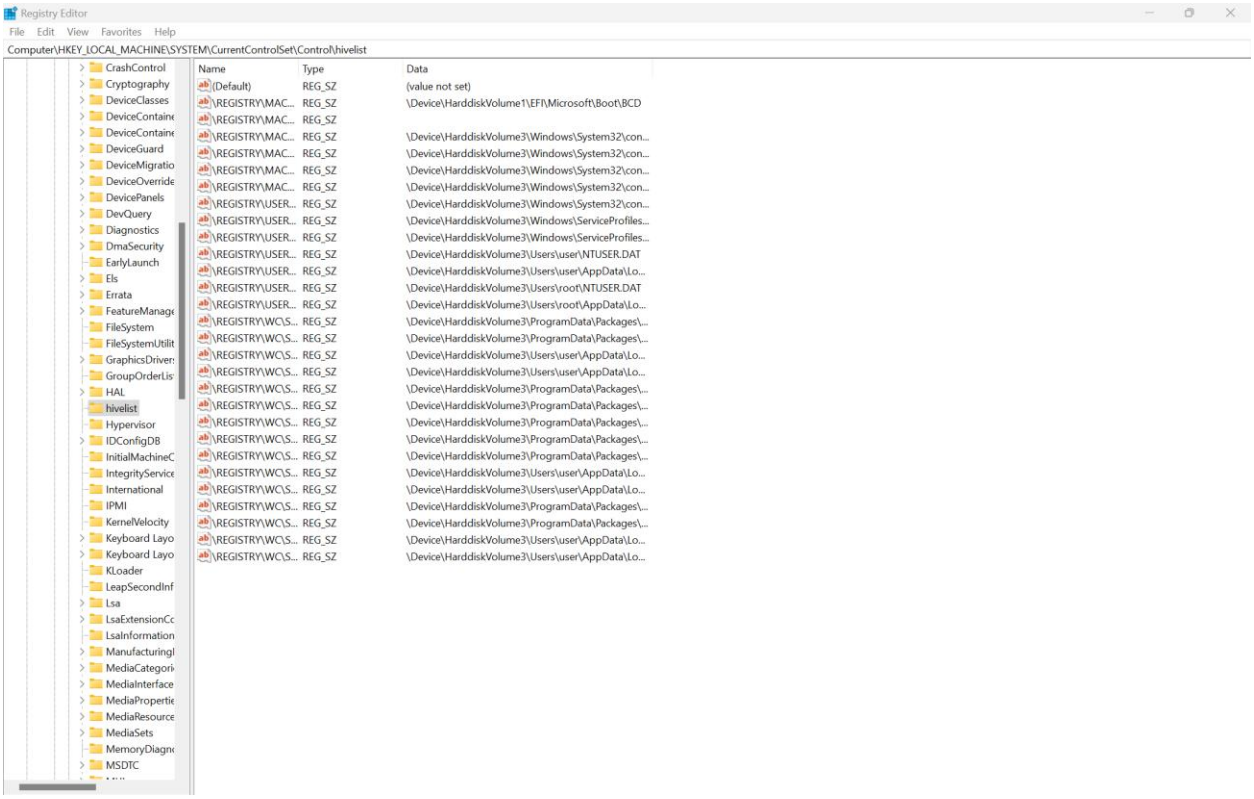

Keeper® Password Manager
https://keepersecurity.eu/vault/#
KEEPER
Search
EL
elegantjennings2@deliveryotter.com
Create New
My Vault
Identity & Payments
Security Audit
BreachWatch
Deleted Items
Secure Add Ons
Protect Your Digital Life with Keeper.
Records
Create records for passwords, payment cards, and more!
Folders
Organise your records in folders and subfolders.
Sharing
Securely share records from your vault.
Create New
Import My Passwords
Cancel
Save
Record Type
Login
Title (Required)
Facebook
Login
testuser@aol.com
Password
CCSF#123456
Medium
Website Address
https://facebook.com
encryption: ON
Sync
Work Offline
Help
Privacy Policy

HxD EXAMINING:

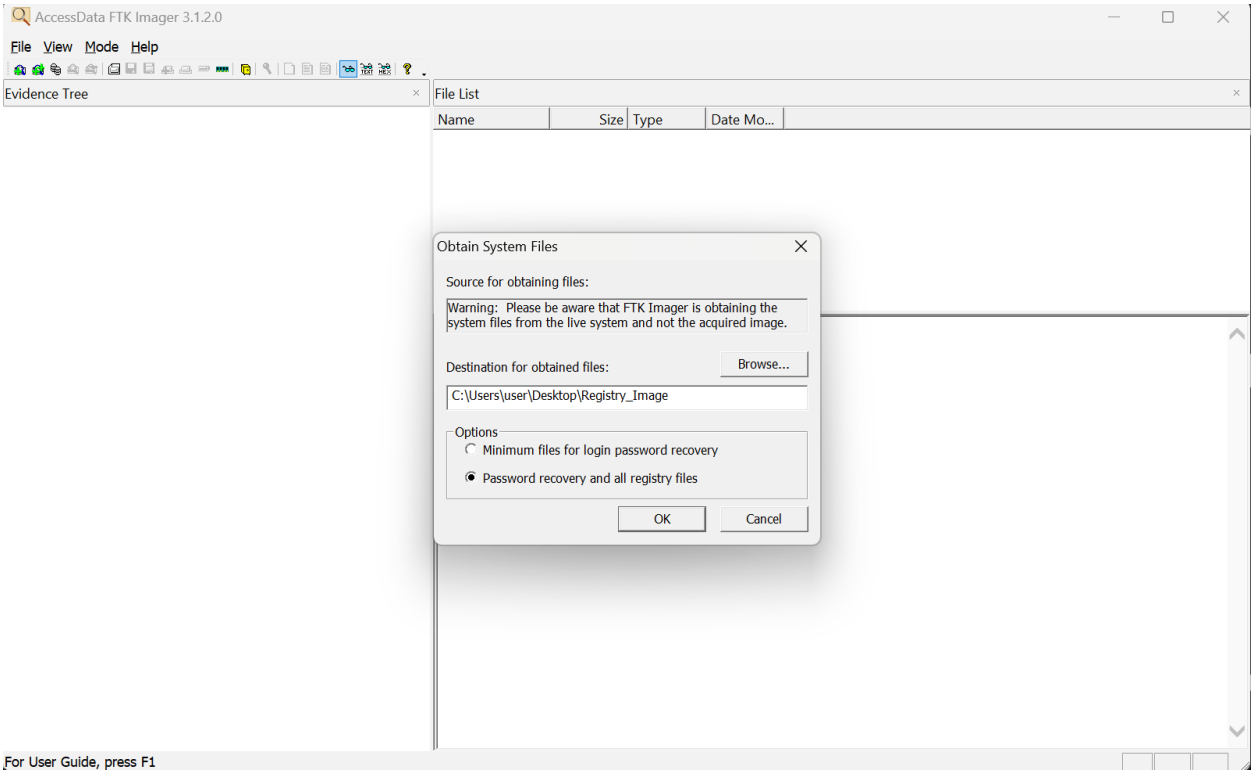


7. Capturing and examining the registry

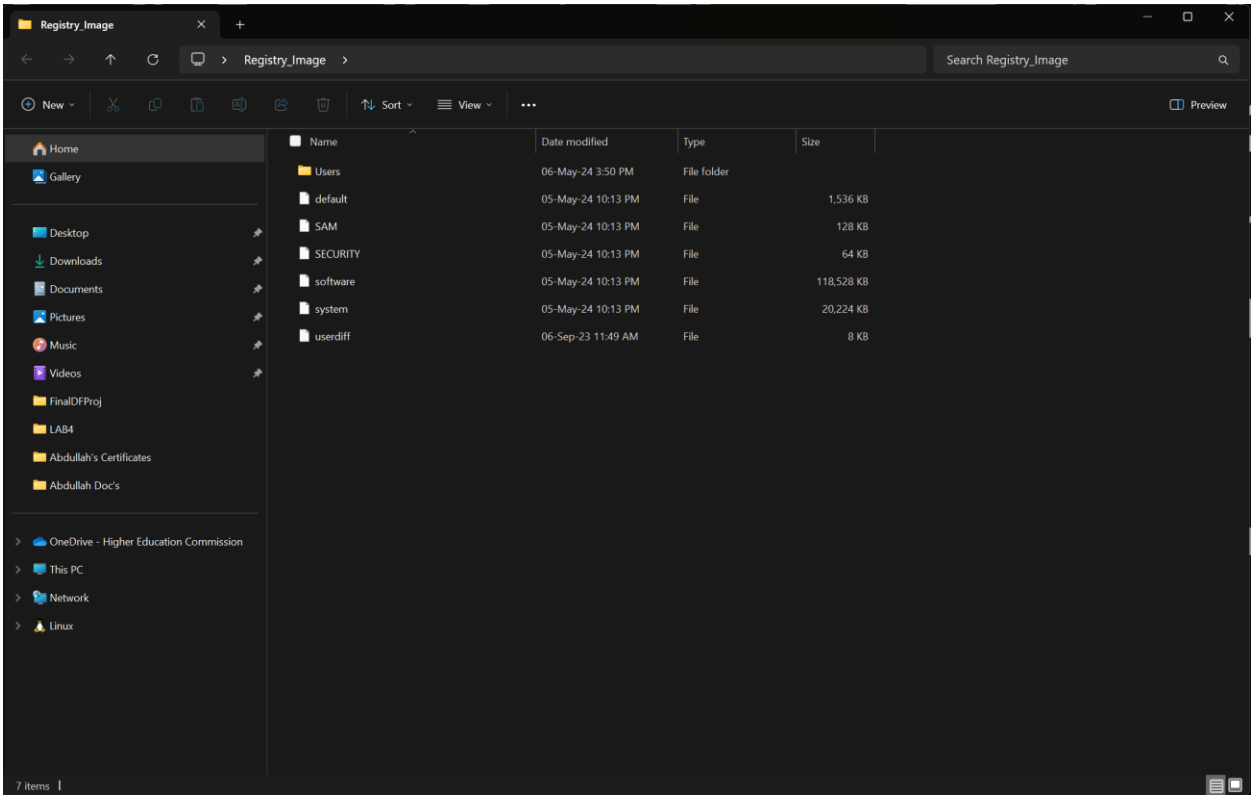
REGISTRY EXAMINATION:



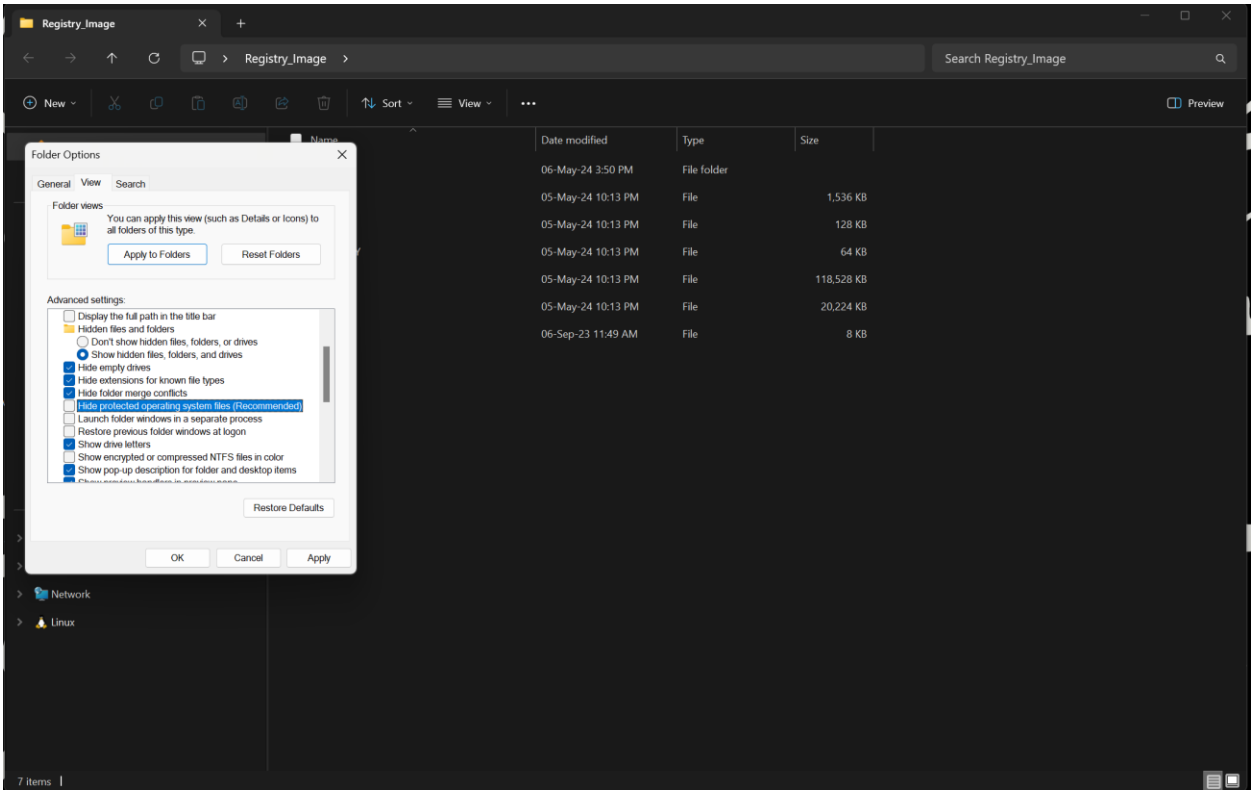
MAKING IMAGE OF REGISTRY:



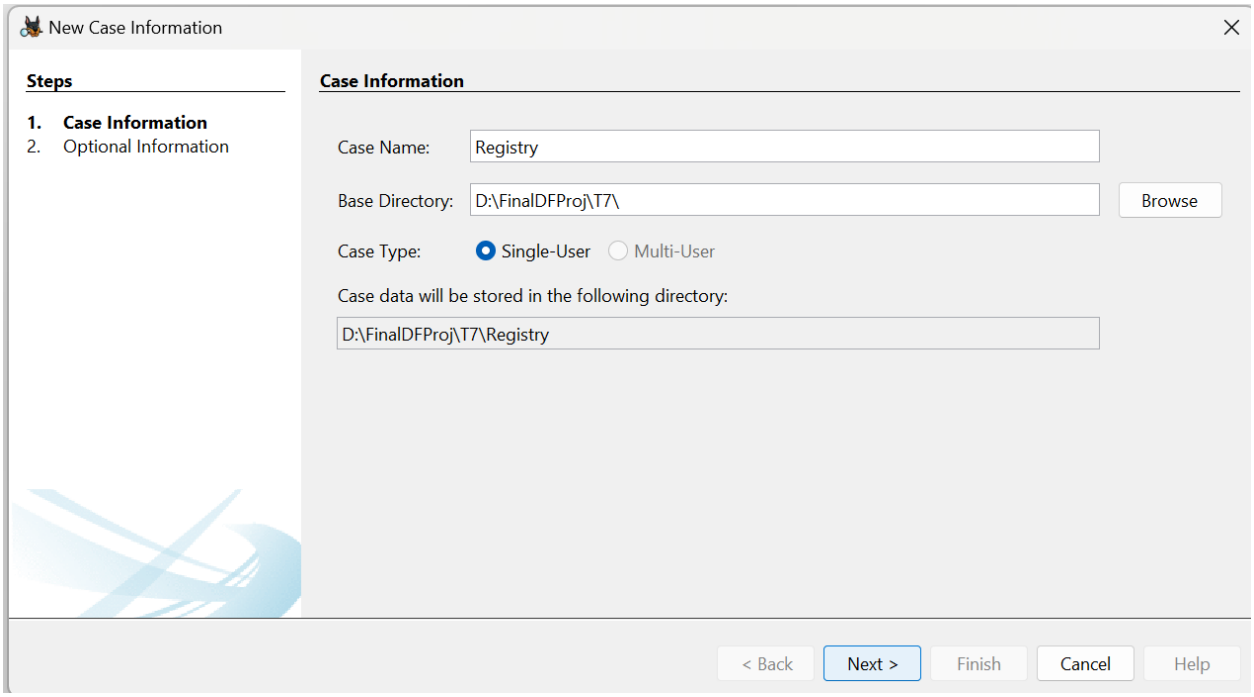
REGISTRY IMAGE FOLDER AFTER CREATION:



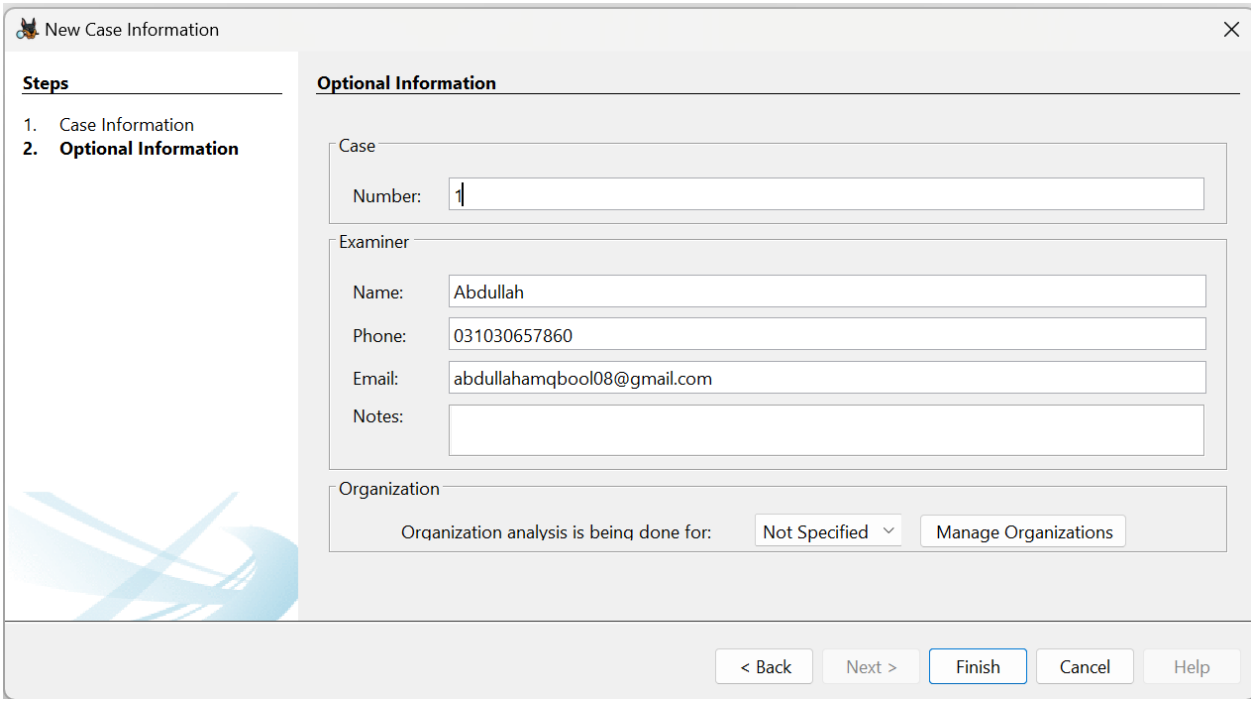
CHECKING FOLDER OPTIONS:



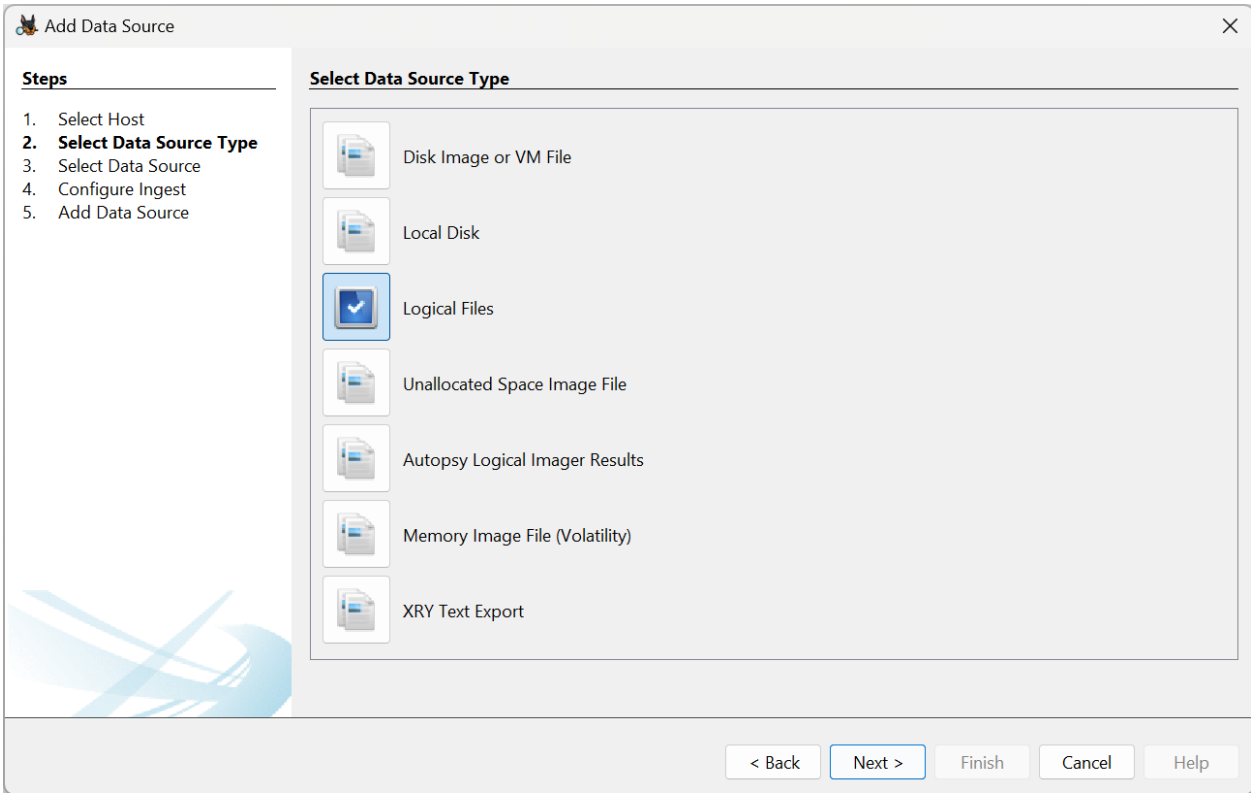
MAKING OF AUTOPSY CASE:



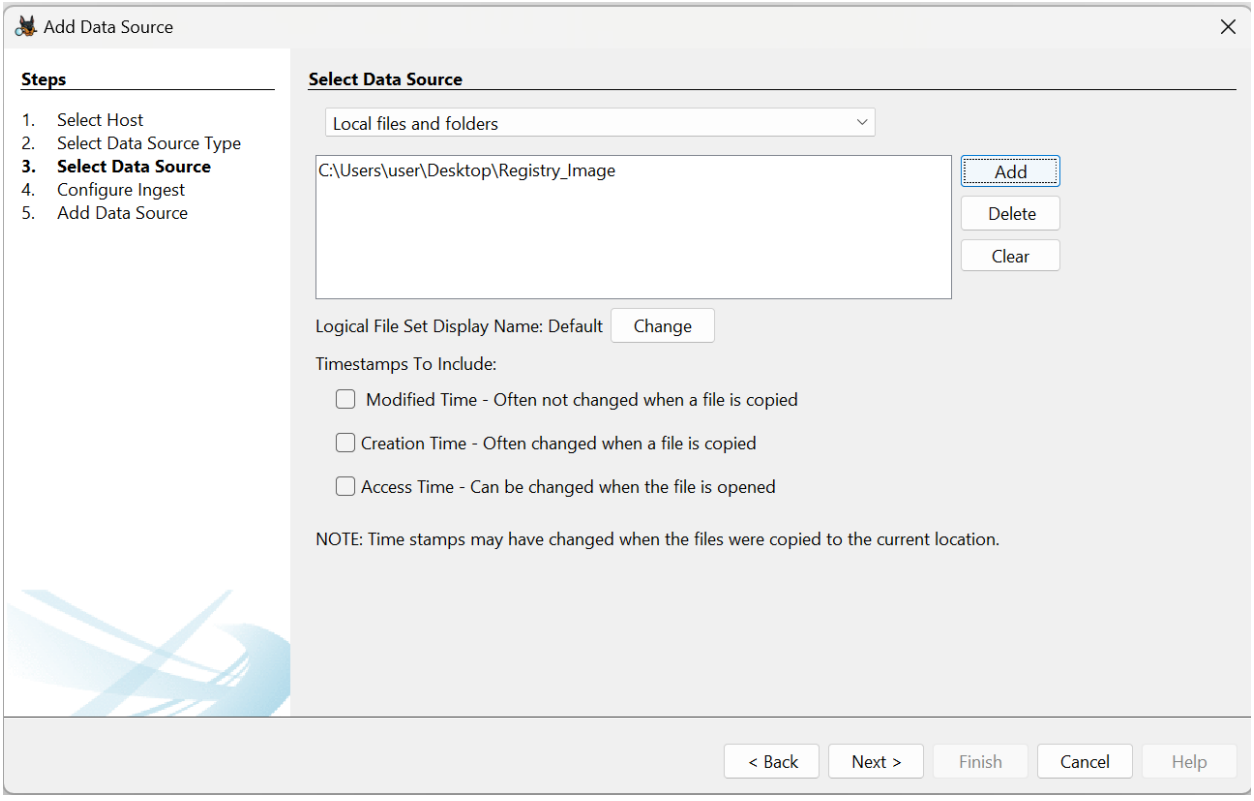
CASE INFORMATION:



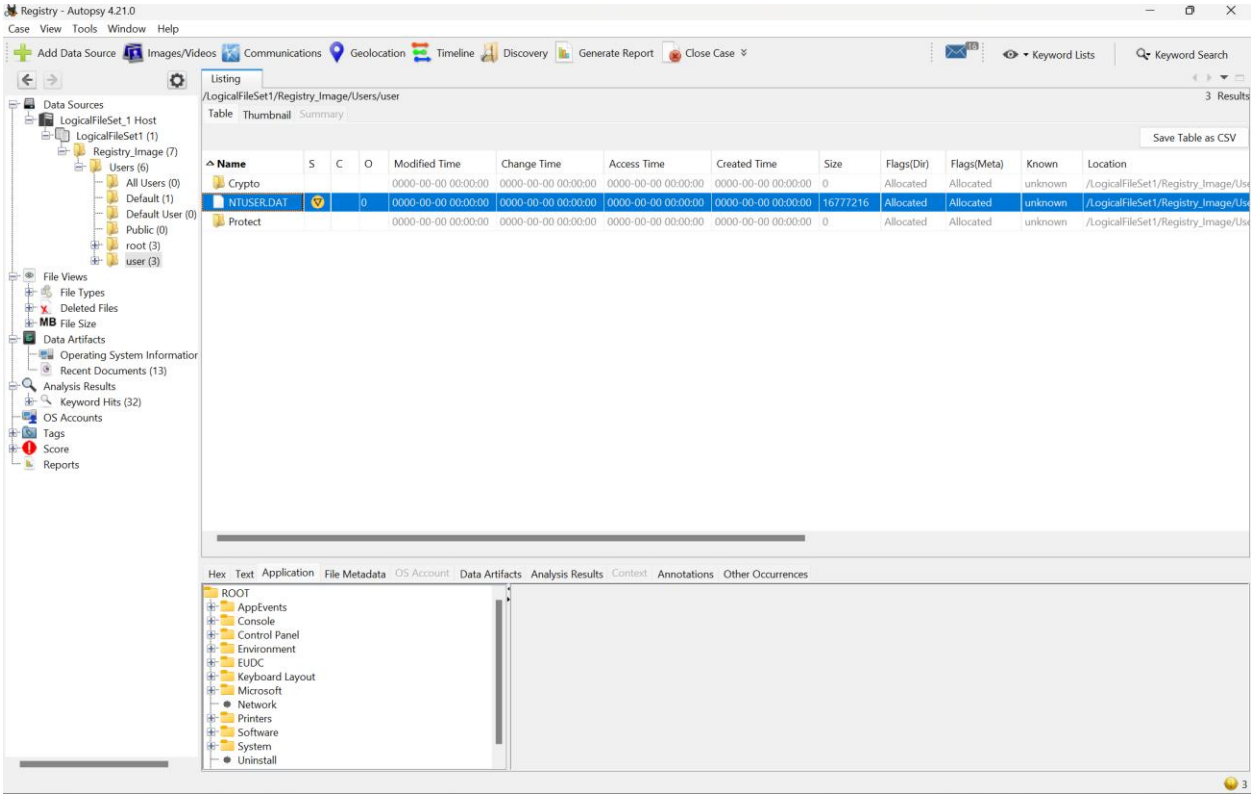
SELECTING DATA SOURCE:



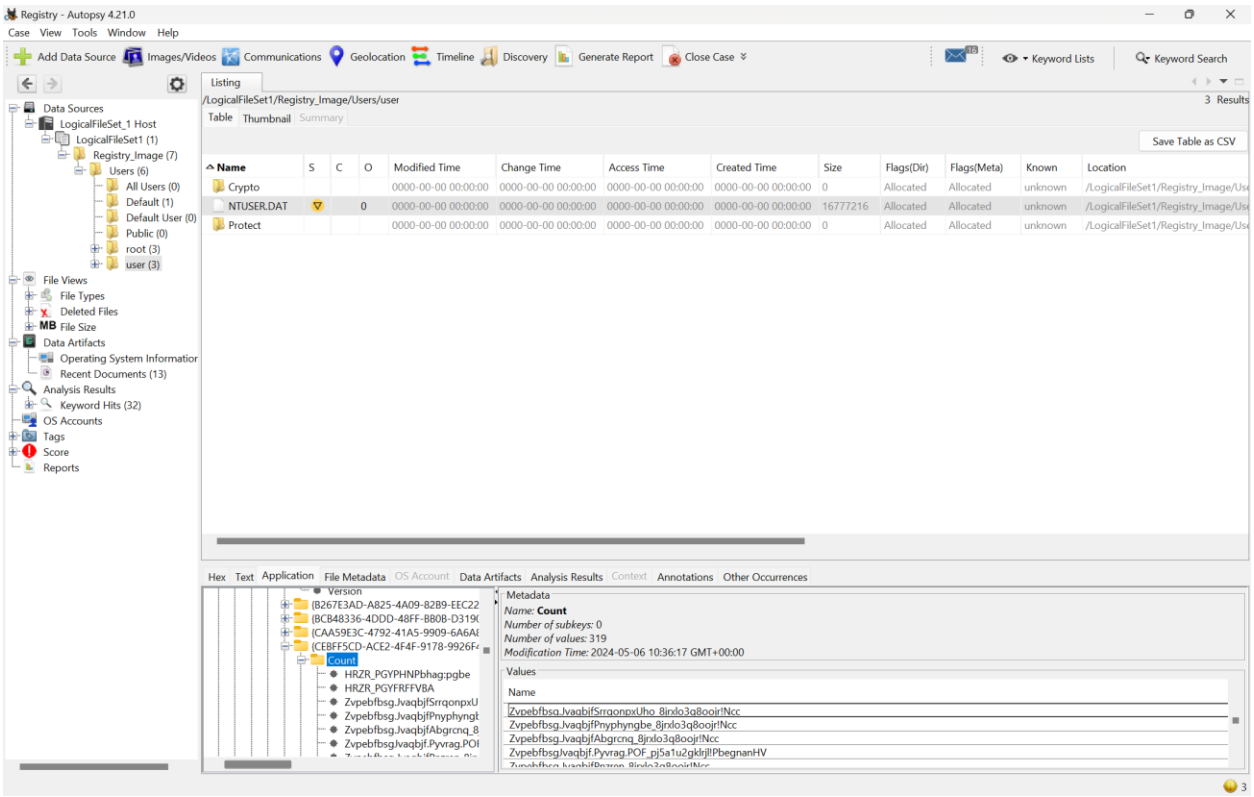
DATA SOURCE:



NTUSER.DAT EXAMINATION:

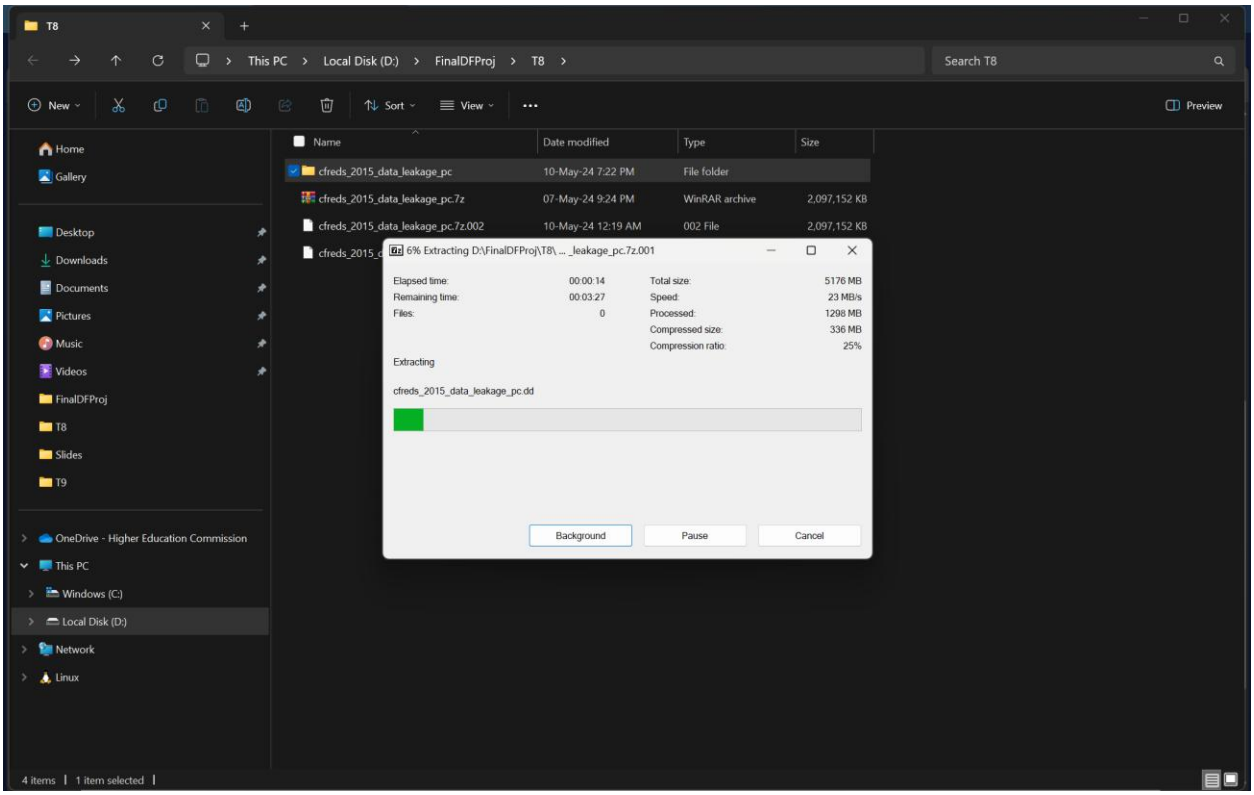


OPENING OF ROT 13:



8. Examining a window disk image.

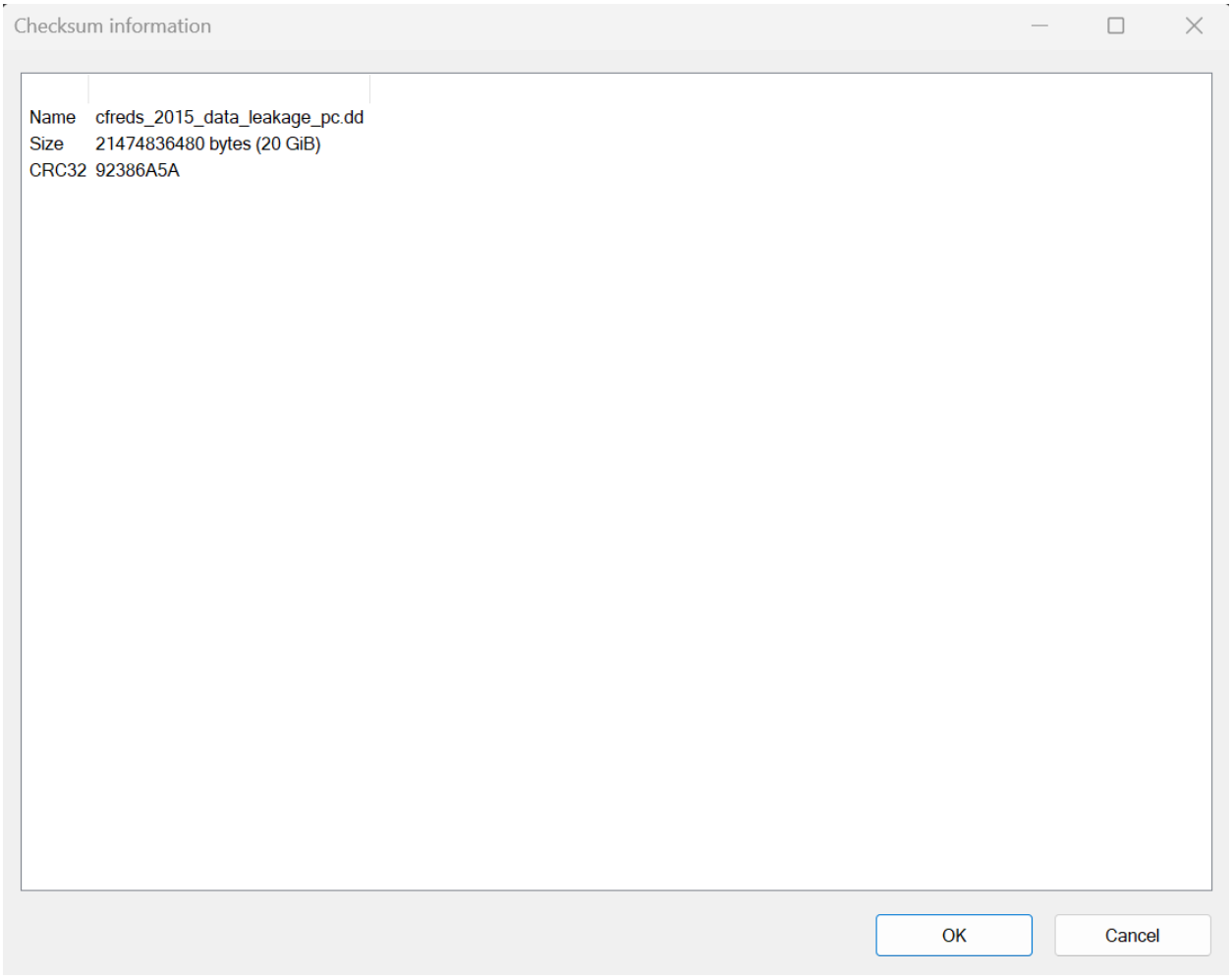
DOWNLOADING EVIDENCE FILE:



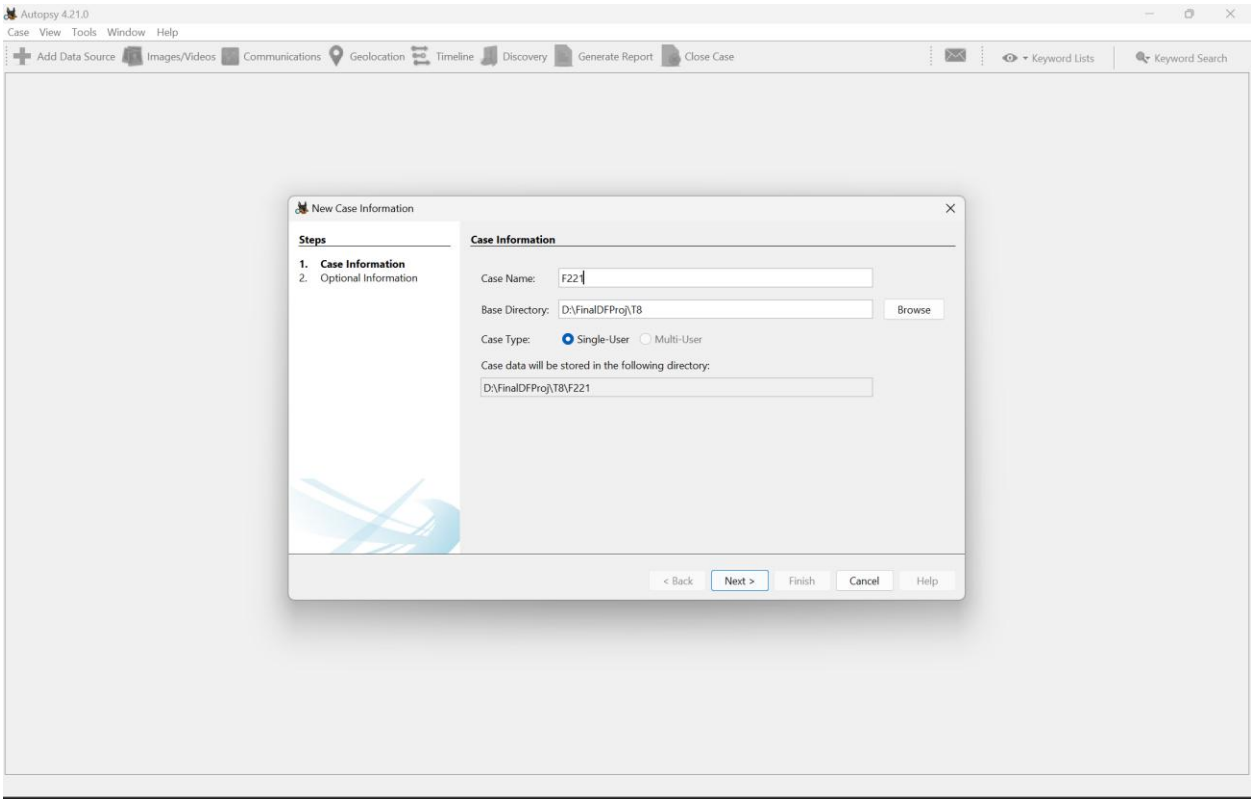
VERIFYING THE HASH:

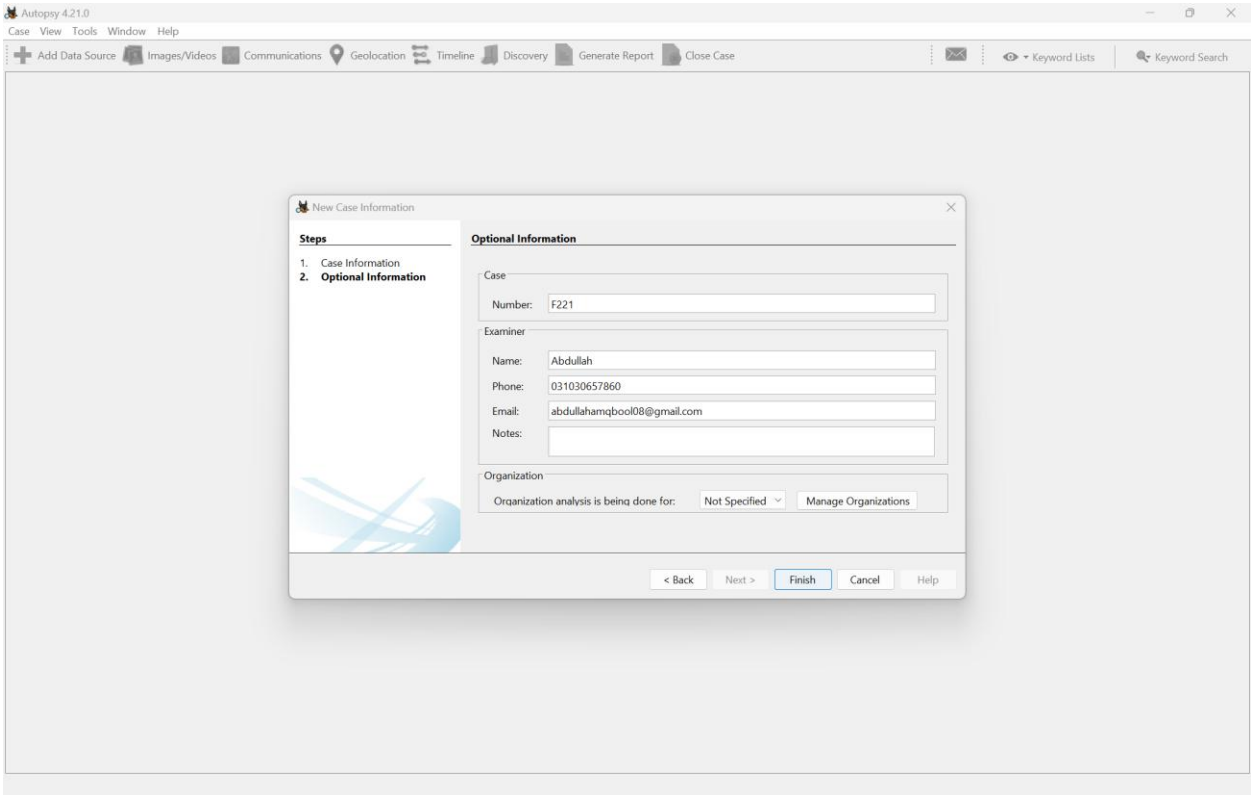
```
PS D:\FinalDFProj\T8\cfreds_2015_data_leakage_pc> Get-FileHash -Algorithm MD5 cfreds_2015_data_leakage_pc.dd

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             A49D1254C873808C58E6F1BCD60B5BDE                                       D:\FinalDFProj\T8\cfreds_2015...

PS D:\FinalDFProj\T8\cfreds_2015_data_leakage_pc>
```

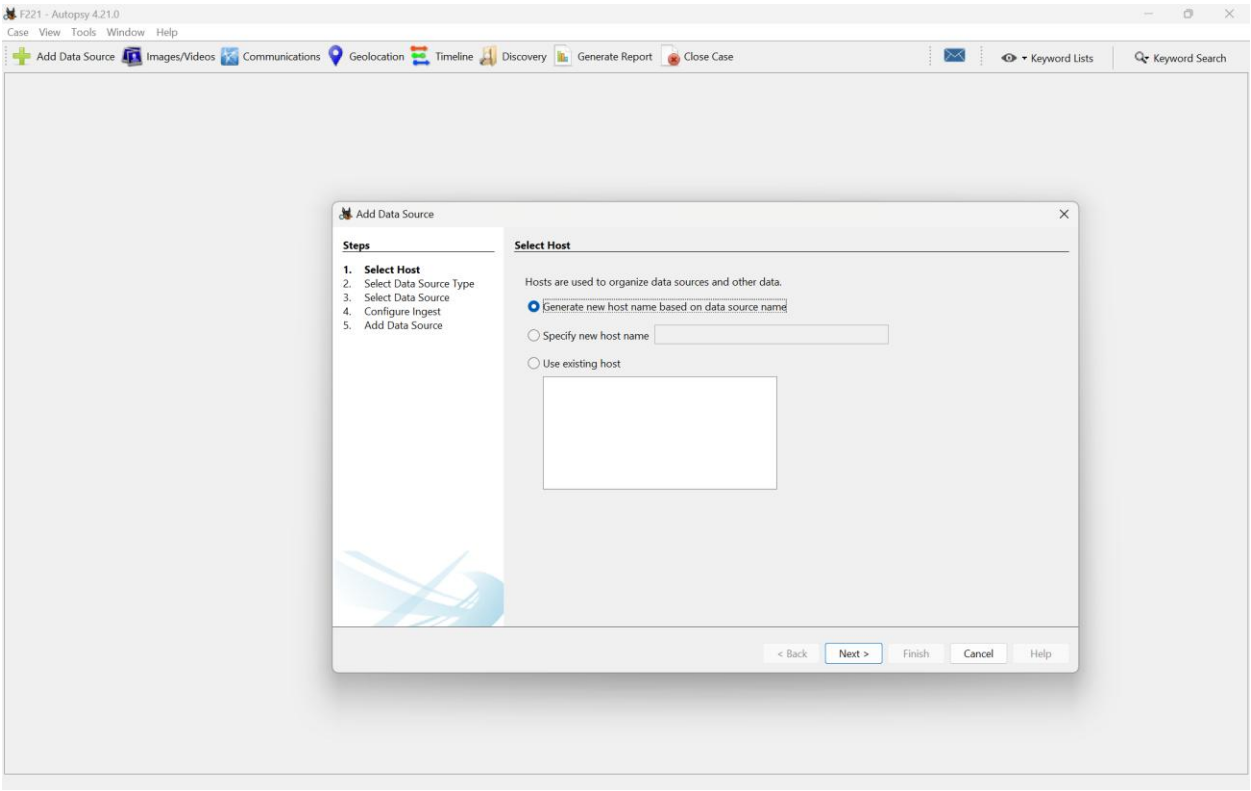
CRC32 HASH:

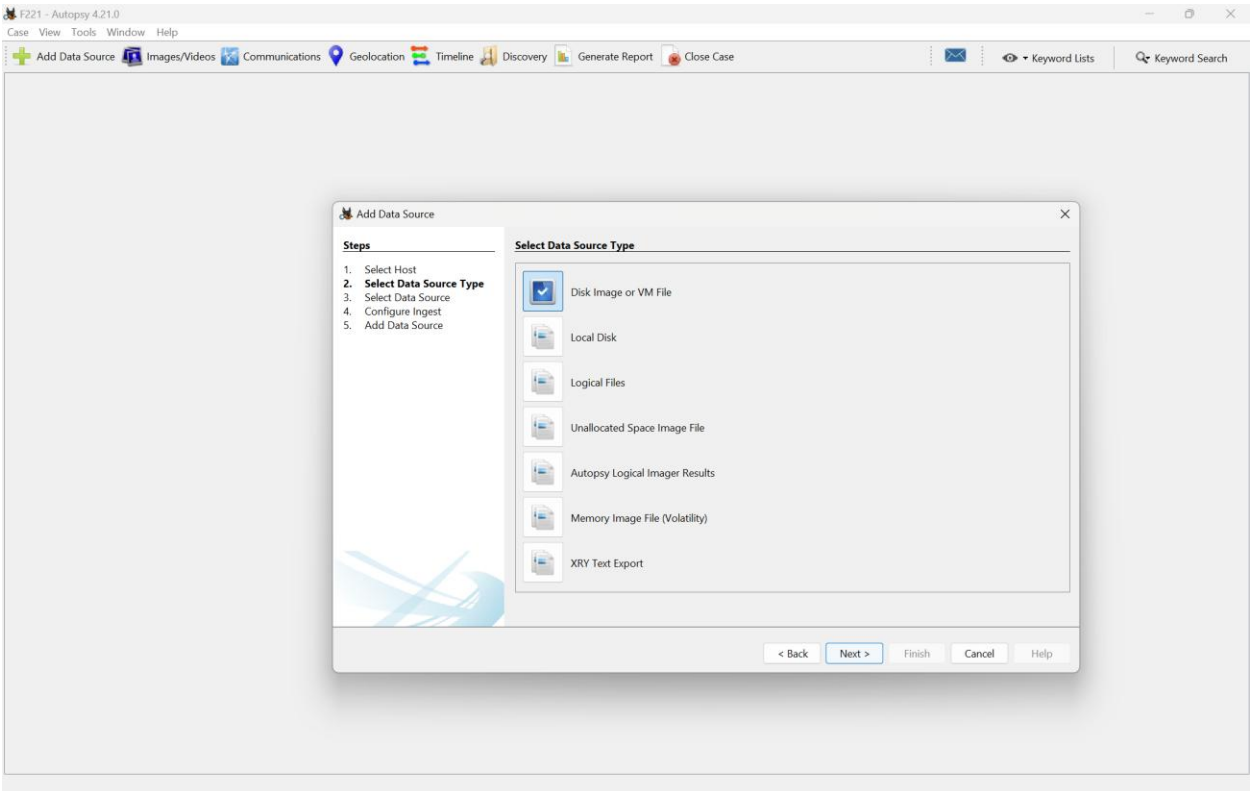

Checksum information
Name cfreds_2015_data_leakage_pc.dd
Size 21474836480 bytes (20 GiB)
CRC32 92386A5A
OK
Cancel

IMPORTING EVIDENCE IMAGE:

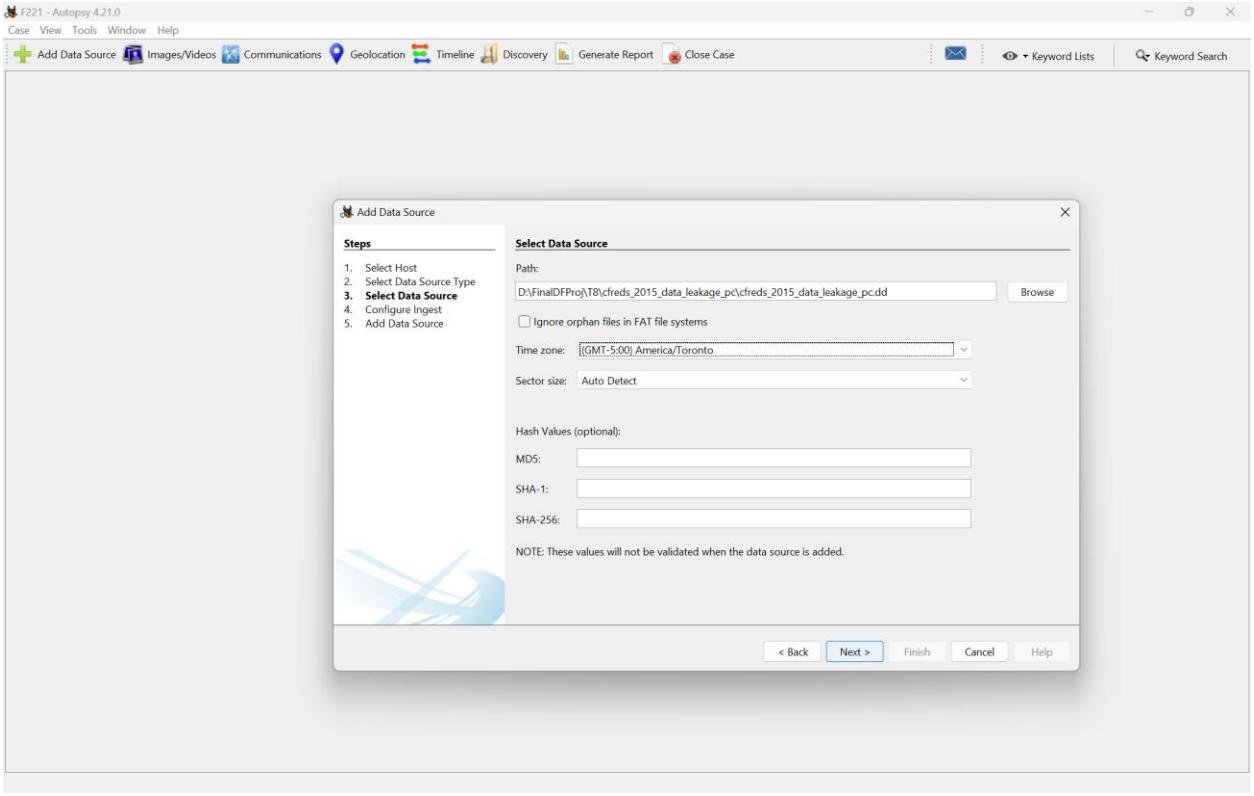


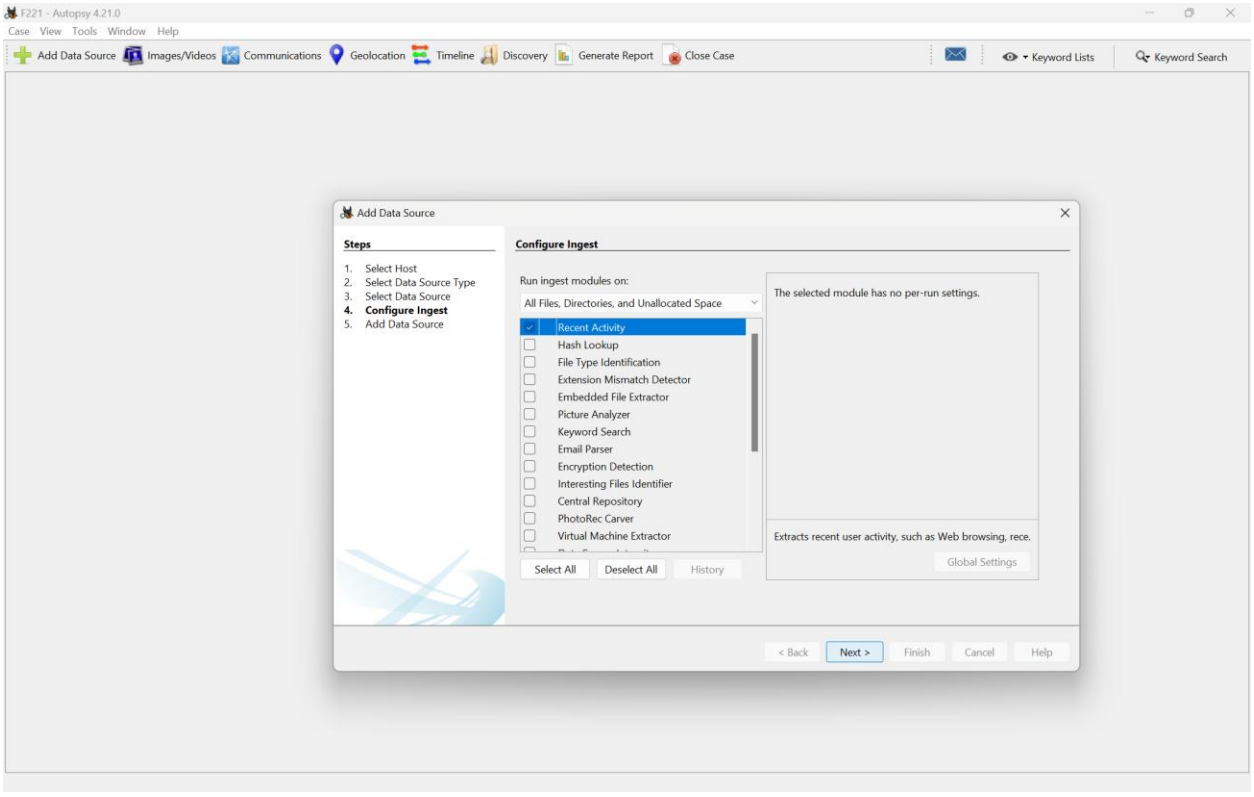



F221 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help


F221 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
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 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
Next >
Finish
Cancel
Help

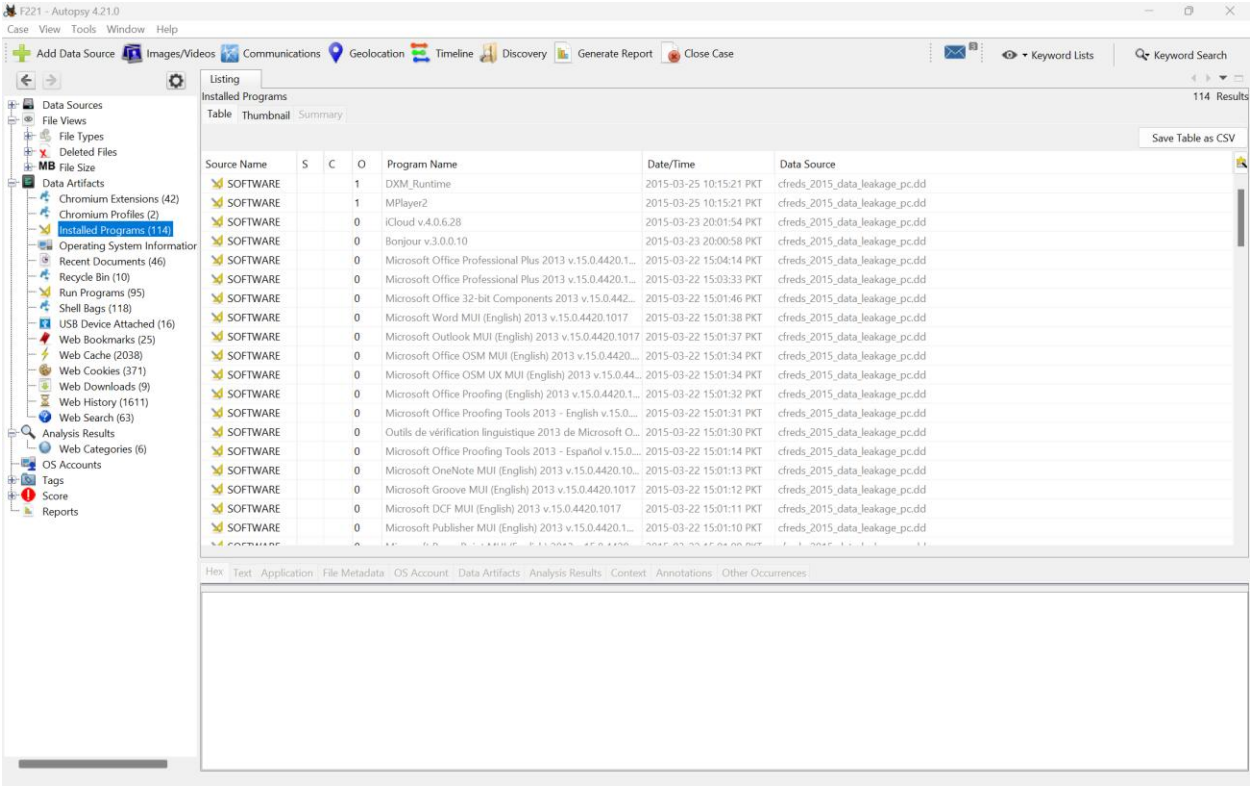
SETTING TIME ZONE:



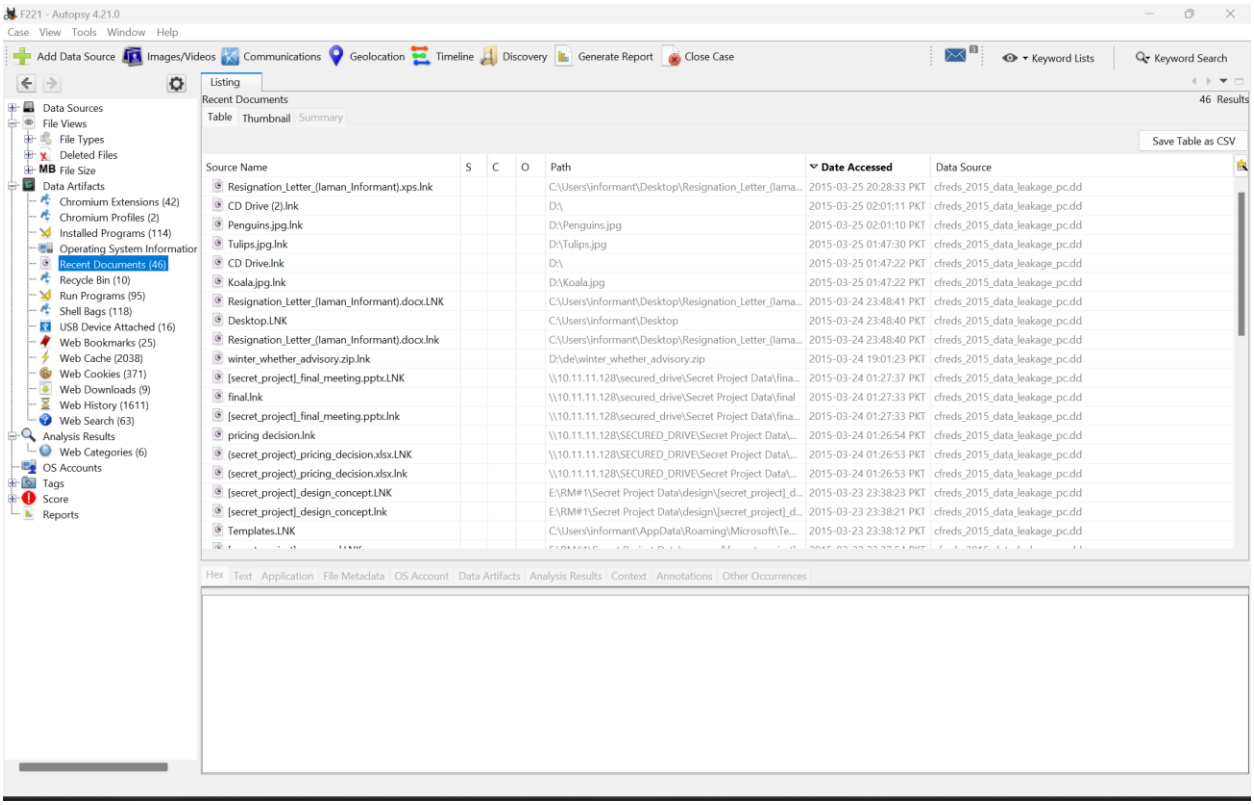


DATA ARTIFICATS:

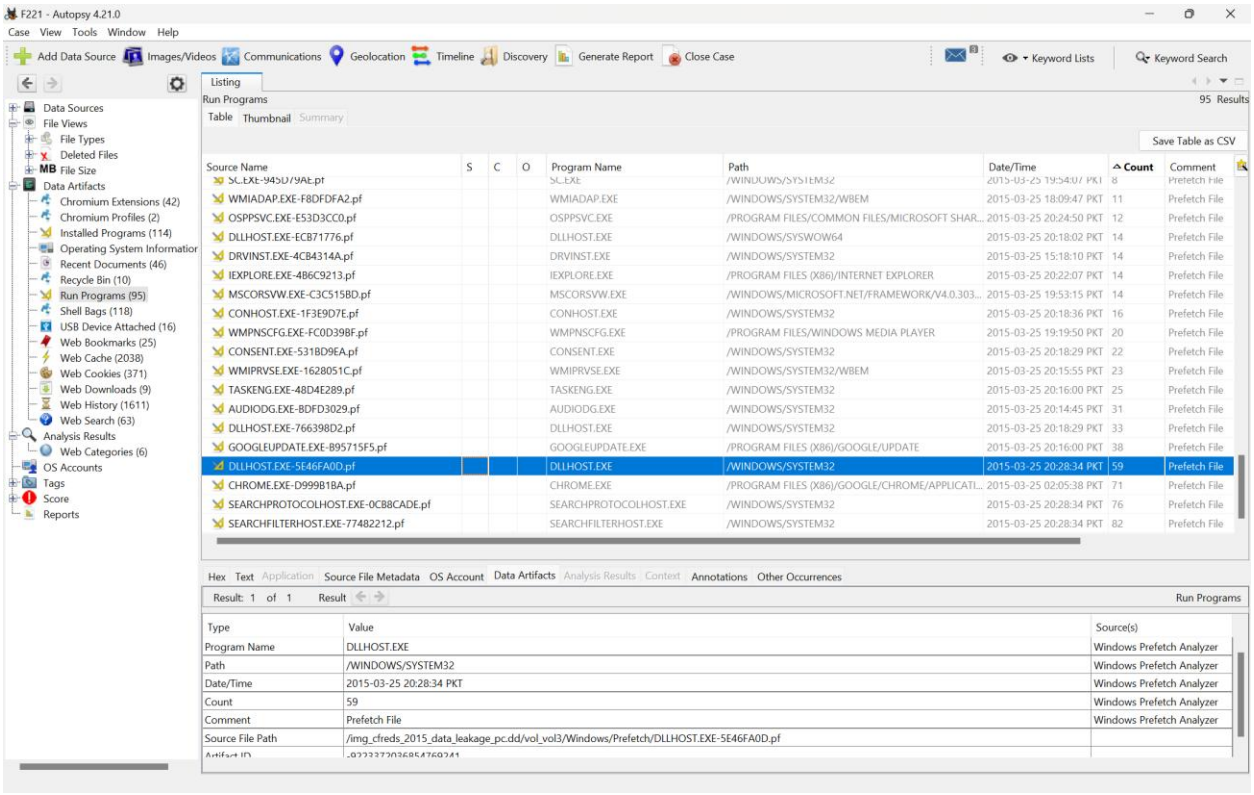
MOST RECENTLY INSTALLED PROGRAM:



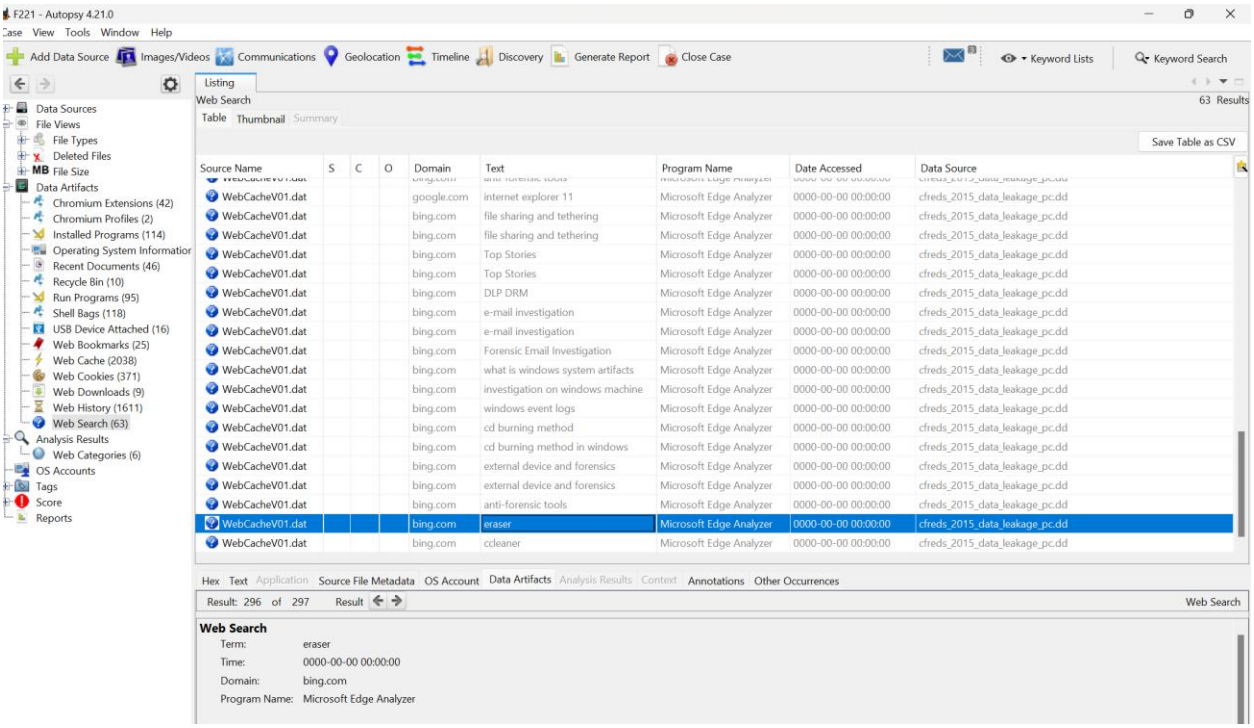
MOST RECENT DOCUMENT:


F221 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Recent Documents
46 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Path Date Accessed Data Source
Resignation_Letter_(laman_Informant).xps.lnk C:\Users\informant\Desktop\Resignation_Letter_(lama... 2015-03-25 20:28:33 PKT cfreds_2015_data_leakage_pc.dd
CD Drive (2).lnk D:\ 2015-03-25 02:01:11 PKT cfreds_2015_data_leakage_pc.dd
Penguins.jpg.lnk D:\Penguins.jpg 2015-03-25 02:01:10 PKT cfreds_2015_data_leakage_pc.dd
Tulips.jpg.lnk D:\Tulips.jpg 2015-03-25 01:47:30 PKT cfreds_2015_data_leakage_pc.dd
CD Drive.lnk D:\ 2015-03-25 01:47:22 PKT cfreds_2015_data_leakage_pc.dd
Koala.jpg.lnk D:\Koala.jpg 2015-03-25 01:47:22 PKT cfreds_2015_data_leakage_pc.dd
Resignation_Letter_(laman_Informant).docx.LNK C:\Users\informant\Desktop\Resignation_Letter_(lama... 2015-03-24 23:48:41 PKT cfreds_2015_data_leakage_pc.dd
Desktop.LNK C:\Users\informant\Desktop 2015-03-24 23:48:40 PKT cfreds_2015_data_leakage_pc.dd
Resignation_Letter_(laman_Informant).docx.lnk C:\Users\informant\Desktop\Resignation_Letter_(lama... 2015-03-24 23:48:40 PKT cfreds_2015_data_leakage_pc.dd
winter_whether_advisory.zip.lnk D:\de\winter_whether_advisory.zip 2015-03-24 19:01:23 PKT cfreds_2015_data_leakage_pc.dd
[secret_project]_final_meeting.pptx.LNK \\10.11.11.128\secured_drive\Secret Project Data\fina... 2015-03-24 01:27:37 PKT cfreds_2015_data_leakage_pc.dd
final.lnk \\10.11.11.128\secured_drive\Secret Project Data\final 2015-03-24 01:27:33 PKT cfreds_2015_data_leakage_pc.dd
[secret_project]_final_meeting.pptx.lnk \\10.11.11.128\secured_drive\Secret Project Data\fina... 2015-03-24 01:27:33 PKT cfreds_2015_data_leakage_pc.dd
pricing decision.lnk \\10.11.11.128\SECURED_DRIVE\Secret Project Data\... 2015-03-24 01:26:54 PKT cfreds_2015_data_leakage_pc.dd
(secret_project)_pricing_decision.xlsx.LNK \\10.11.11.128\SECURED_DRIVE\Secret Project Data\... 2015-03-24 01:26:53 PKT cfreds_2015_data_leakage_pc.dd
(secret_project)_pricing_decision.xlsx.lnk \\10.11.11.128\SECURED_DRIVE\Secret Project Data\... 2015-03-24 01:26:53 PKT cfreds_2015_data_leakage_pc.dd
[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_pc.dd
[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_pc.dd
Templates.LNK C:\Users\informant\AppData\Roaming\Microsoft\Te... 2015-03-23 23:38:12 PKT cfreds_2015_data_leakage_pc.dd
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (42)
Chromium Profiles (2)
Installed Programs (114)
Operating System Information
Recent Documents (46)
Recycle Bin (10)
Run Programs (95)
Shell Bags (118)
USB Device Attached (16)
Web Bookmarks (25)
Web Cache (2038)
Web Cookies (371)
Web Downloads (9)
Web History (1611)
Web Search (63)
Analysis Results
Web Categories (6)
OS Accounts
Tags
Score
Reports

59 TIMES:

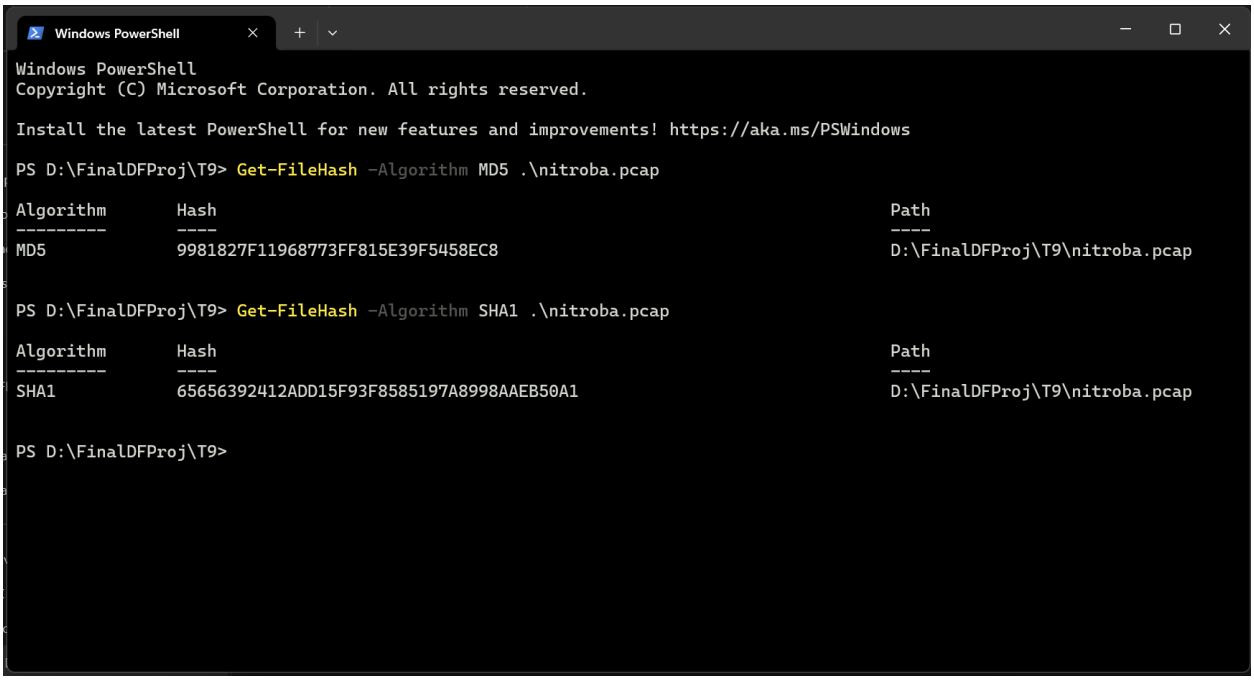

F221 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Run Programs
95 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Program Name Path Date/Time Count Comment
WMIADAP.EXE-F8DFDFA2.pf WMIADAP.EXE /WINDOWS/SYSTEM32/WBEM 2015-03-25 18:09:47 PKT 11 Prefetch File
OSPPSVC.EXE-E53D3CC0.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/SYSWOW64 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/FRAMEWORK/V4.0.303... 2015-03-25 19:53:15 PKT 14 Prefetch File
CONHOST.EXE-1F3E9D7E.pf CONHOST.EXE /WINDOWS/SYSTEM32 2015-03-25 20:18:36 PKT 16 Prefetch File
WMPNSCFG.EXE-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
WMIPRVSE.EXE-1628051C.pf WMIPRVSE.EXE /WINDOWS/SYSTEM32/WBEM 2015-03-25 20:15:55 PKT 23 Prefetch File
TASKENG.EXE-48D4E289.pf TASKENG.EXE /WINDOWS/SYSTEM32 2015-03-25 20:16:00 PKT 25 Prefetch File
AUDIODG.EXE-BDFD3029.pf AUDIODG.EXE /WINDOWS/SYSTEM32 2015-03-25 20:14:45 PKT 31 Prefetch File
DLLHOST.EXE-766398D2.pf DLLHOST.EXE /WINDOWS/SYSTEM32 2015-03-25 20:18:29 PKT 33 Prefetch File
GOOGLEUPDATE.EXE-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-D999B1BA.pf CHROME.EXE /PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICATI... 2015-03-25 02:05:38 PKT 71 Prefetch File
SEARCHPROTOCOLHOST.EXE-0CB8CADE.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
Run Programs
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_cfreds_2015_data_leakage_pc.dd/vol_vol3/Windows/Prefetch/DLLHOST.EXE-5E46FA0D.pf
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (42)
Chromium Profiles (2)
Installed Programs (114)
Operating System Information
Recent Documents (46)
Recycle Bin (10)
Run Programs (95)
Shell Bags (118)
USB Device Attached (16)
Web Bookmarks (25)
Web Cache (2038)
Web Cookies (371)
Web Downloads (9)
Web History (1611)
Web Search (63)
Analysis Results
Web Categories (6)
OS Accounts
Tags
Score
Reports

SEARCH:

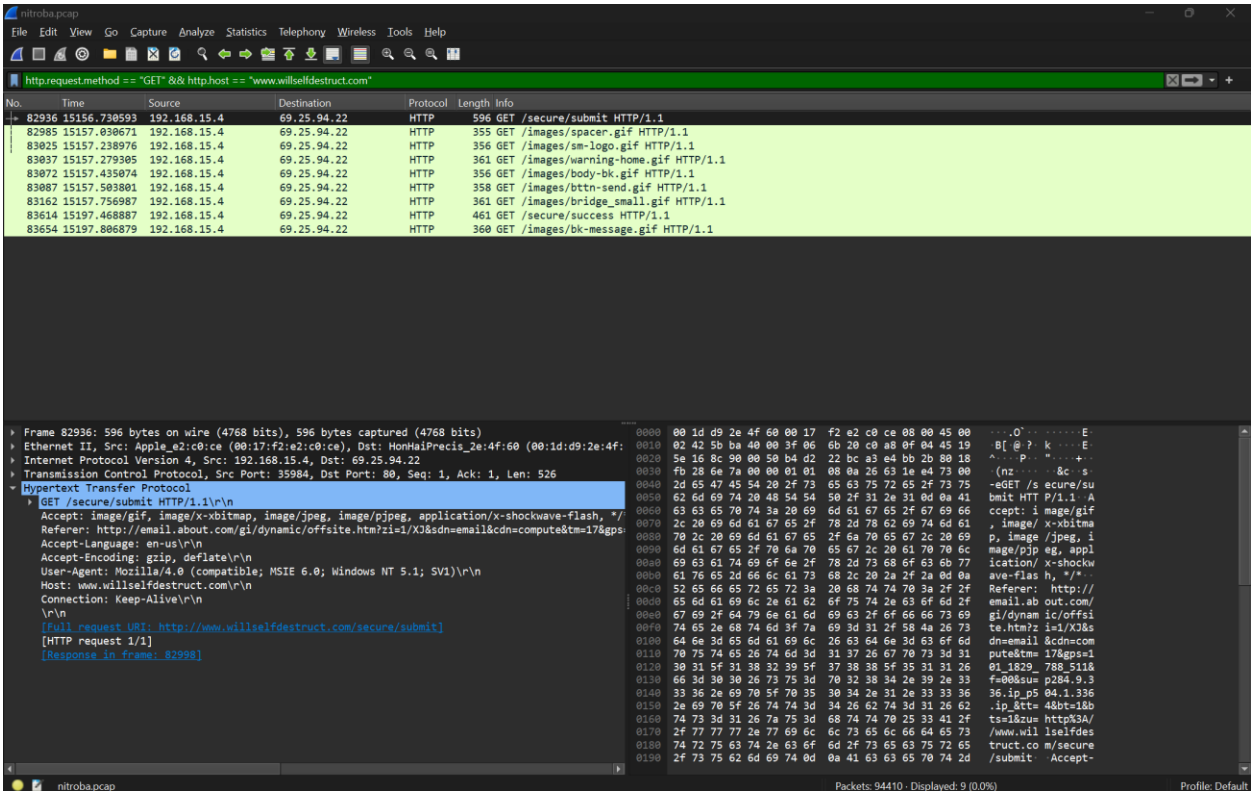

F221 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (42)
Chromium Profiles (2)
Installed Programs (114)
Operating System Informatior
Recent Documents (46)
Recycle Bin (10)
Run Programs (95)
Shell Bags (118)
USB Device Attached (16)
Web Bookmarks (25)
Web Cache (2038)
Web Cookies (371)
Web Downloads (9)
Web History (1611)
Web Search (63)
Analysis Results
Web Categories (6)
OS Accounts
Tags
Score
Reports
Listing
Web Search
63 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Domain
Text
Program Name
Date Accessed
Data Source
WebCacheV01.dat
google.com
internet explorer 11
bing.com
file sharing and tethering
Top Stories
DLP DRM
e-mail investigation
Forensic Email Investigation
what is windows system artifacts
investigation on windows machine
windows event logs
cd burning method
cd burning method in windows
external device and forensics
anti-forensic tools
eraser
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
Web Search
Term: eraser
Time: 0000-00-00 00:00:00
Domain: bing.com
Program Name: Microsoft Edge Analyzer

9. Email Forensics:

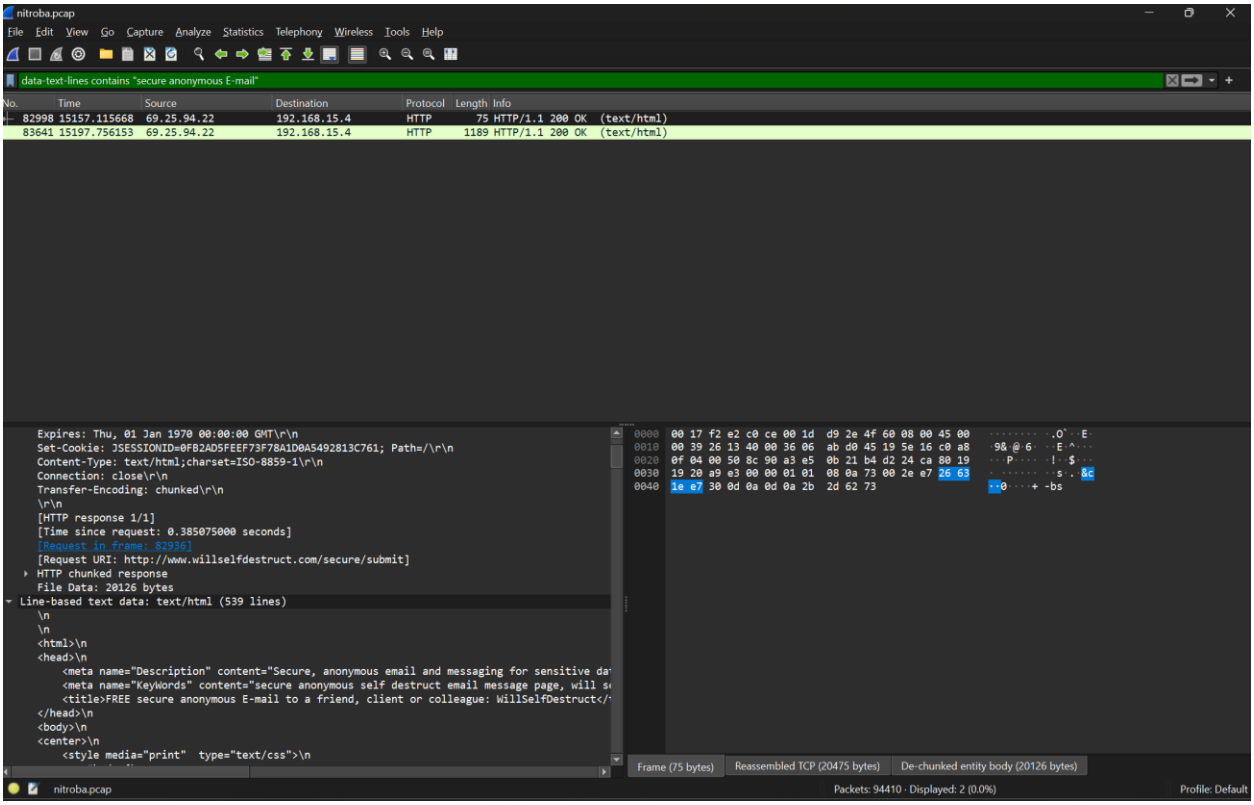
GETTING FILE HASH OF NITROBA.PCAP



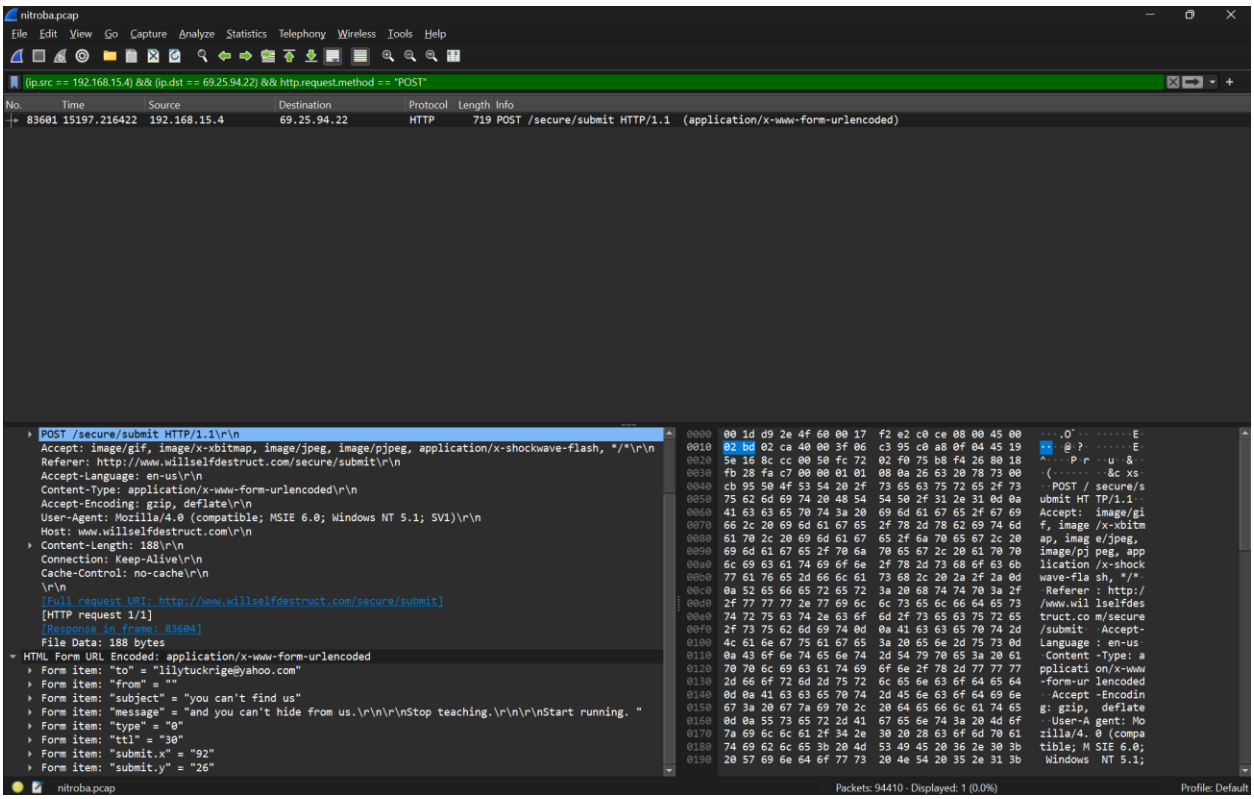
CHECKING THE HOST PACKETS GET:



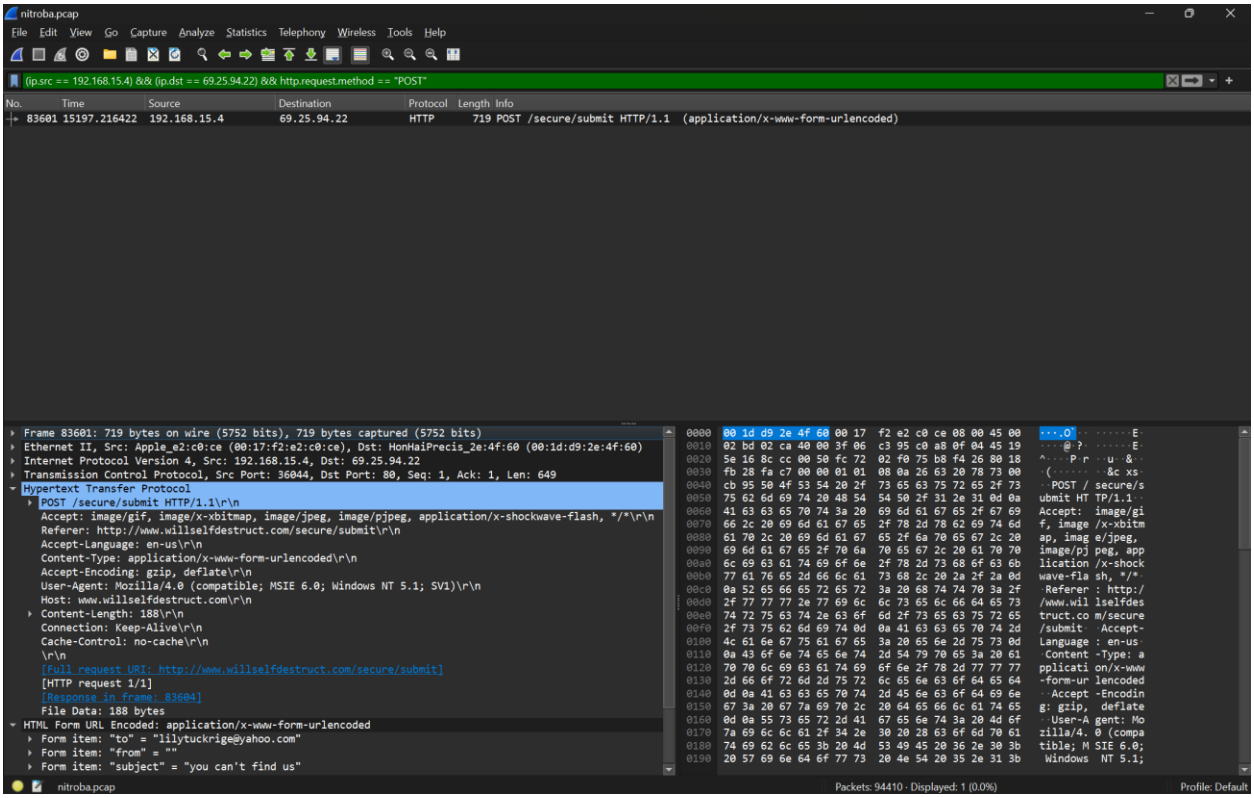
SECURE ANONYMUS EMAIL SEARCH:

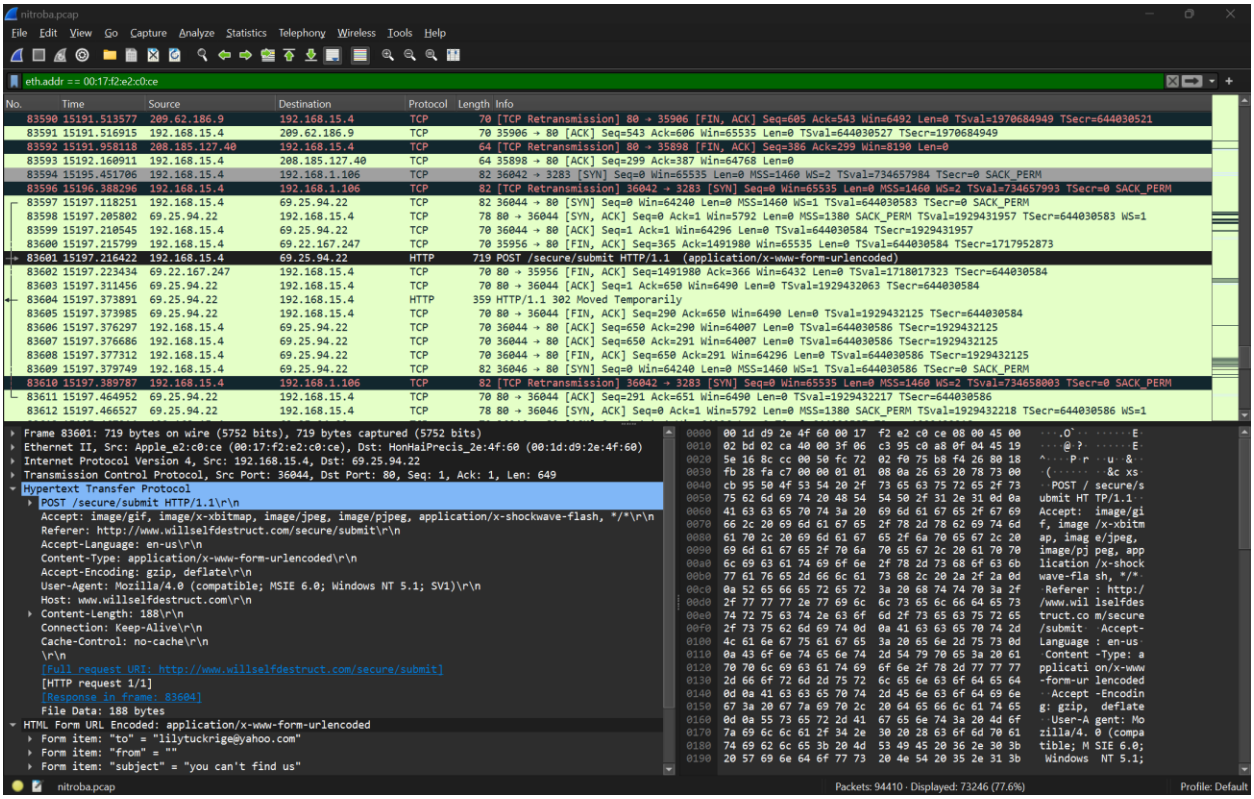


CHECKING IP SRC:

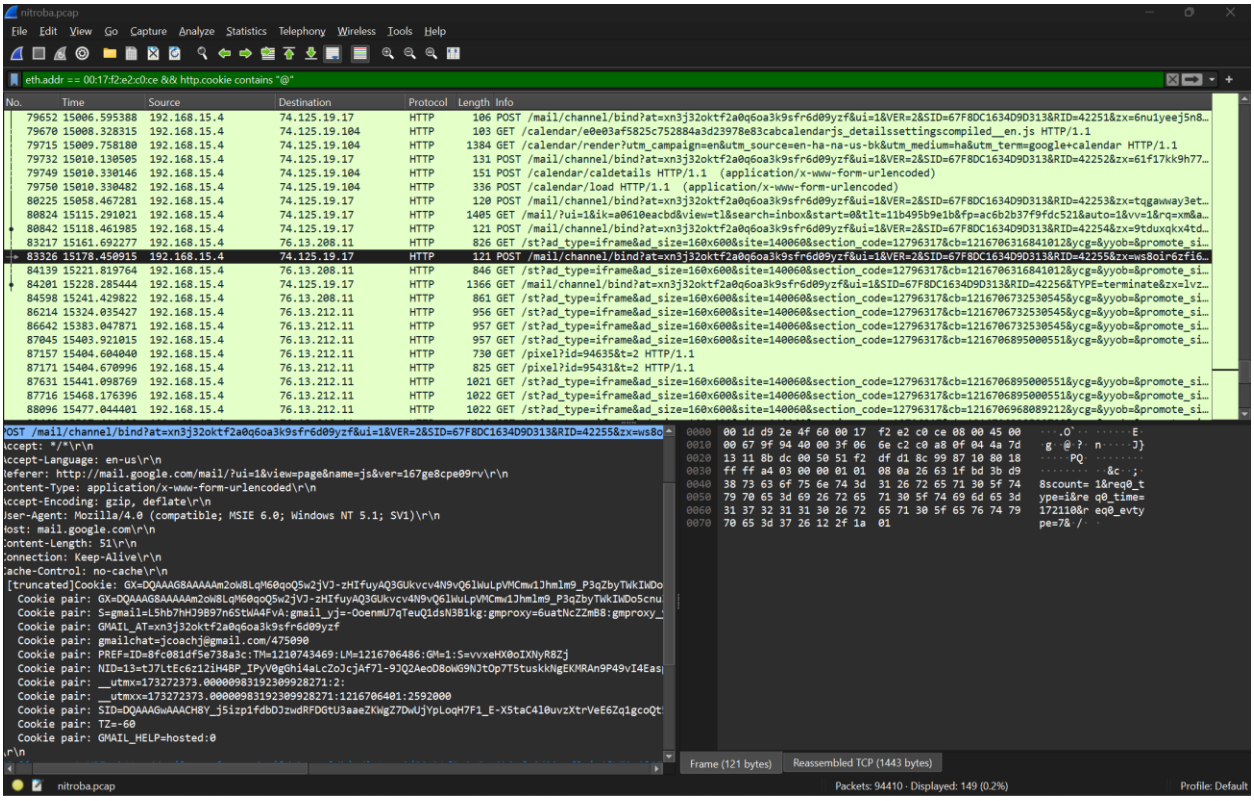


CHECKING MAC ADDRESSES:

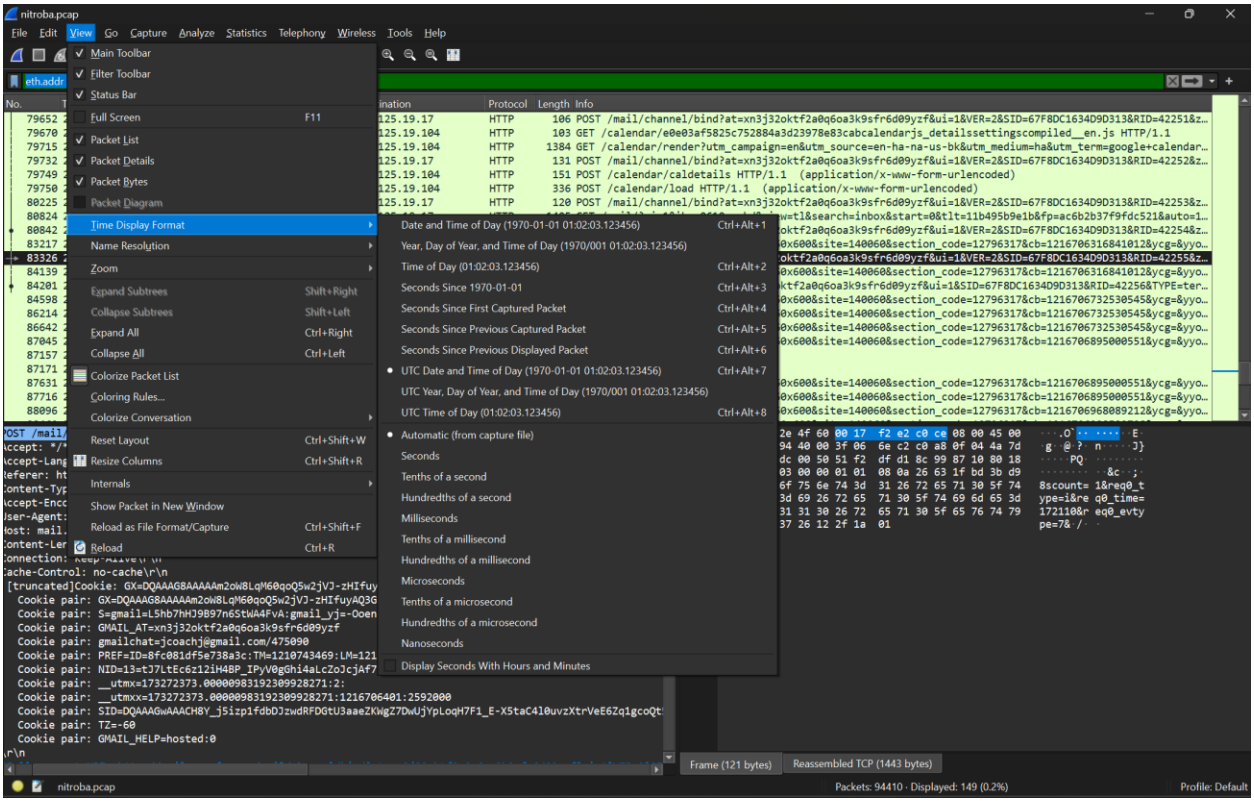


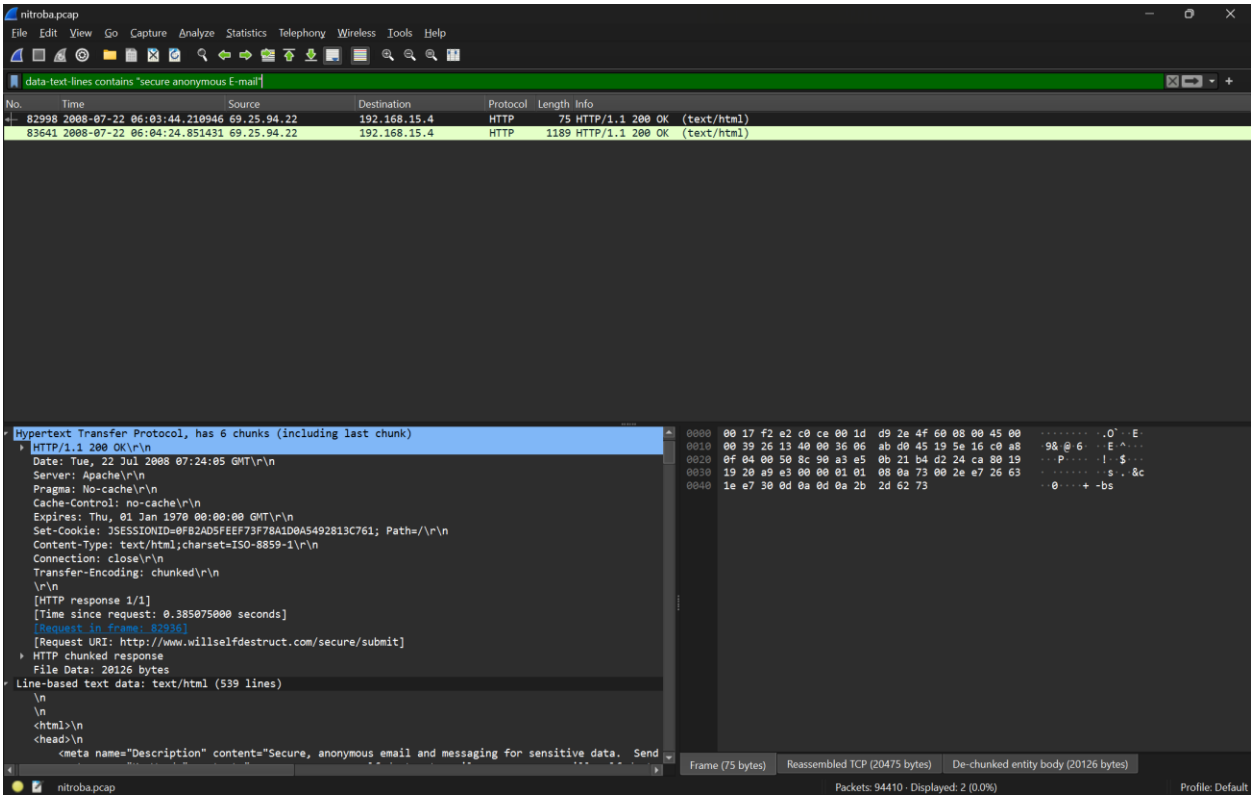


CHECKING EMAIL THROUGH REGEX:



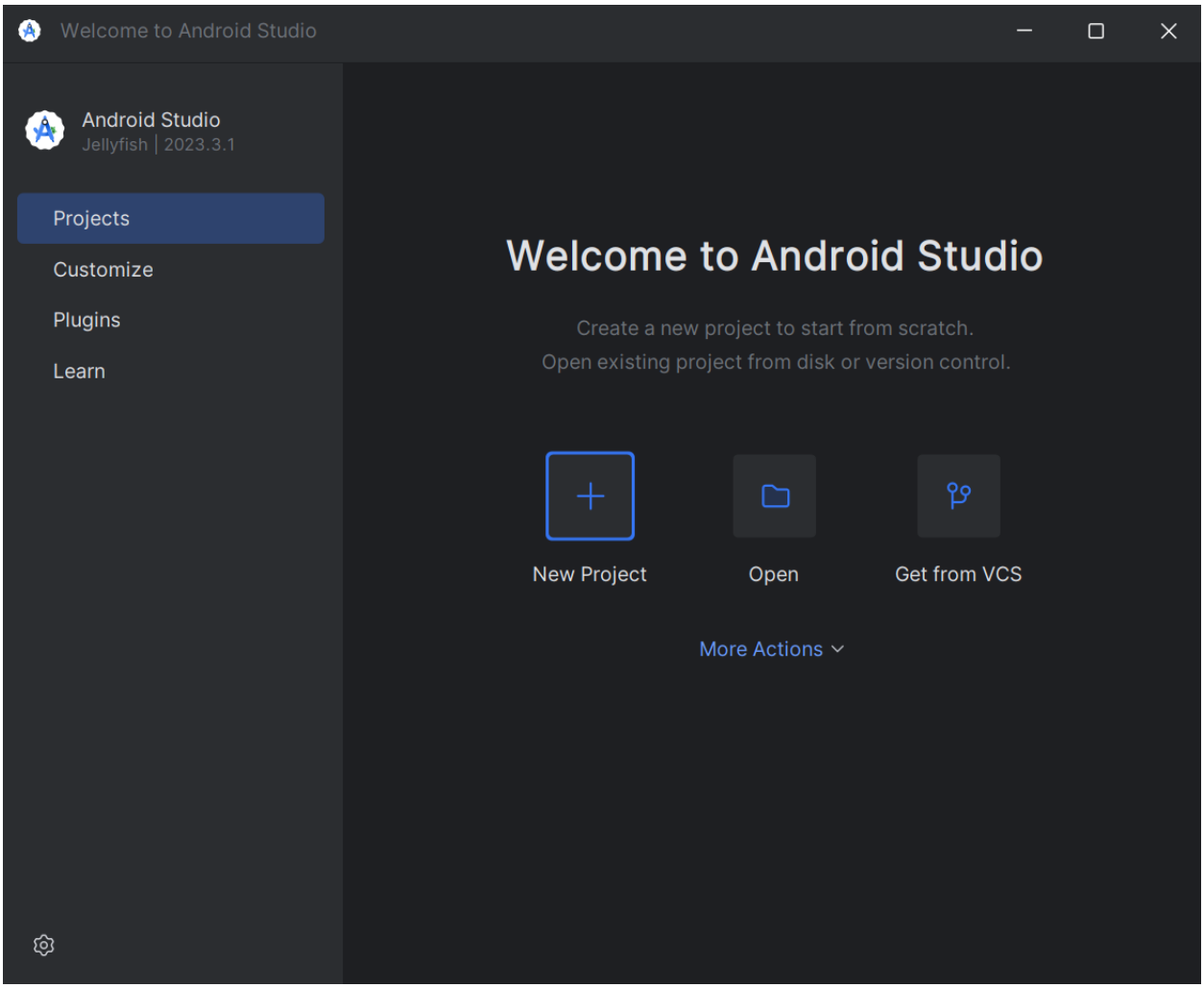
CHECKING TIME OF PACKET:



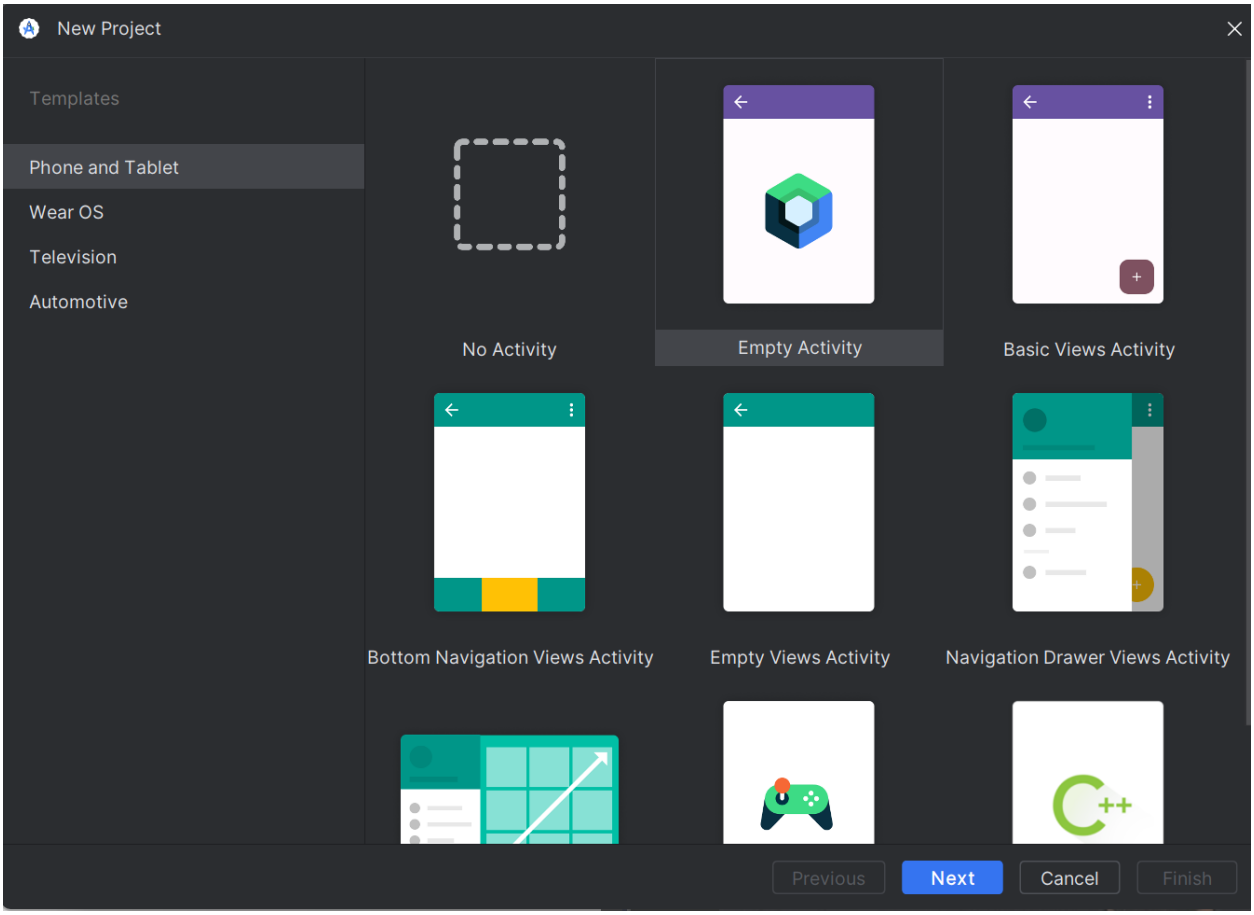

nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
data-text-lines contains "secure anonymous E-mail"
No. Time Source Destination Protocol Length Info
82998 2008-07-22 06:03:44.210946 69.25.94.22 192.168.15.4 HTTP 75 HTTP/1.1 200 OK (text/html)
83641 2008-07-22 06:04:24.851431 69.25.94.22 192.168.15.4 HTTP 1189 HTTP/1.1 200 OK (text/html)
Hypertext Transfer Protocol, has 6 chunks (including last chunk)
HTTP/1.1 200 OK\r\n
Date: Tue, 22 Jul 2008 07:24:05 GMT\r\n
Server: Apache\r\n
Pragma: No-cache\r\n
Cache-Control: no-cache\r\n
Expires: Thu, 01 Jan 1970 00:00:00 GMT\r\n
Set-Cookie: JSESSIONID=0FB2AD5FEEF73F78A1D0A5492813C761; 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: 82936]
[Request URI: http://www.willselfdestruct.com/secure/submit]
HTTP chunked response
File Data: 20126 bytes
Line-based text data: text/html (539 lines)
\n
\n
<html>\n
<head>\n
<meta name="Description" content="Secure, anonymous email and messaging for sensitive data. Send
0000 00 17 f2 e2 c0 ce 00 1d d9 2e 4f 60 08 00 45 00
0010 00 39 26 13 40 00 36 06 ab d0 45 19 5e 16 c0 a8
0020 0f 04 00 50 8c 90 a3 e5 0b 21 b4 d2 24 ca 80 19
0030 19 20 a9 e3 00 00 01 01 08 0a 73 00 2e e7 26 63
0040 1e e7 30 0d 0a 0d 0a 2b 2d 62 73
Frame (75 bytes)
Reassembled TCP (20475 bytes)
De-chunked entity body (20126 bytes)
nitroba.pcap
Packets: 94410 · Displayed: 2 (0.0%)
Profile: Default

10. Android Studio Emulator

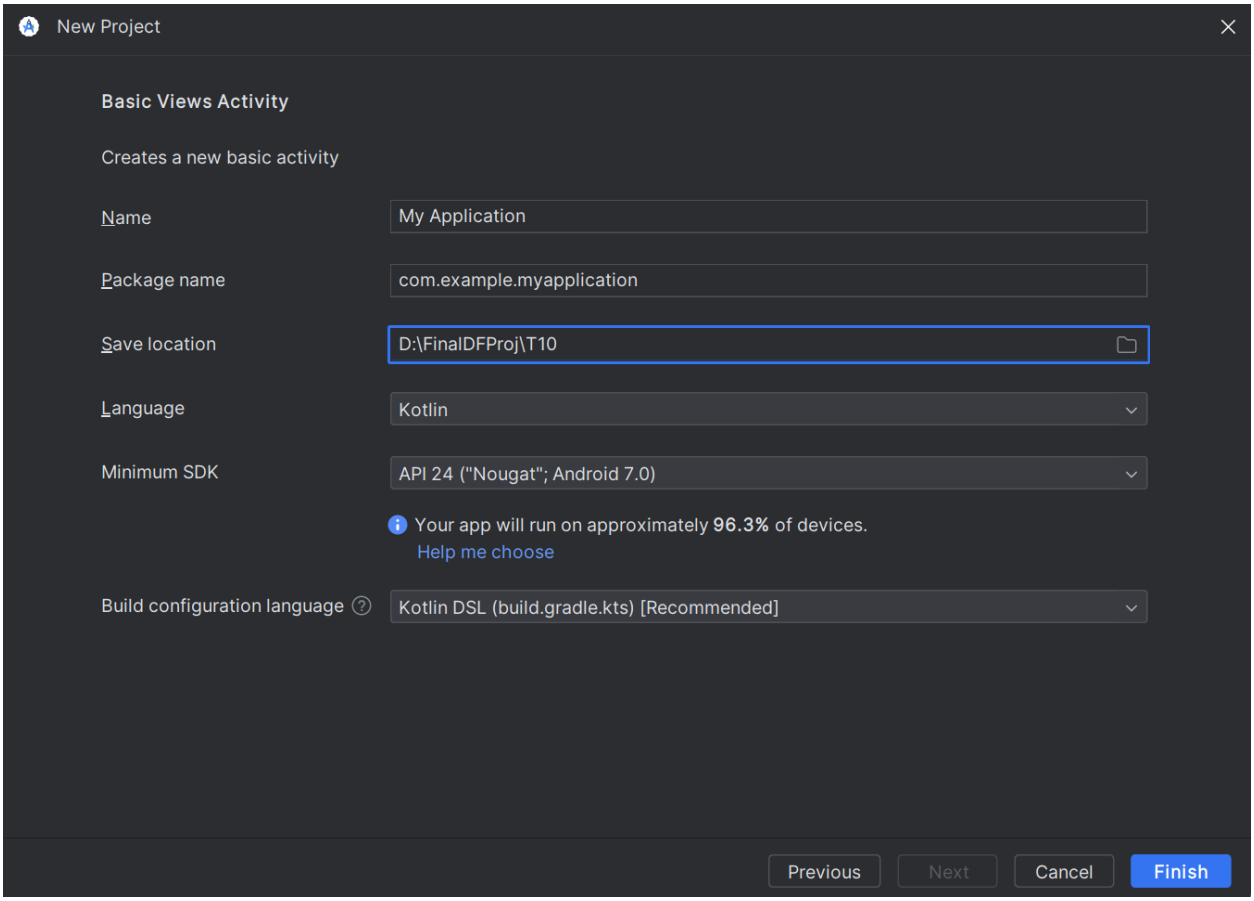
OPENING ANDROID STUDIO:



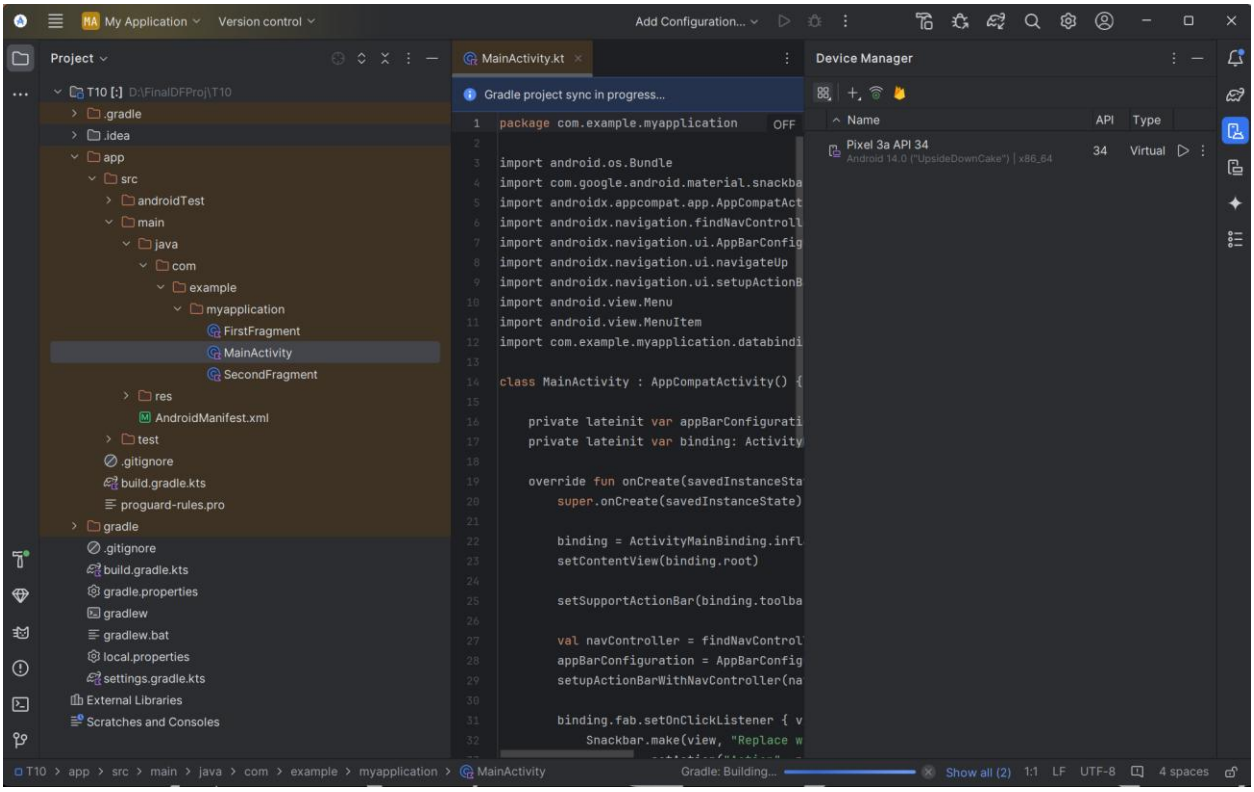
OPENING BASIC ACTIVITY VIEWS:

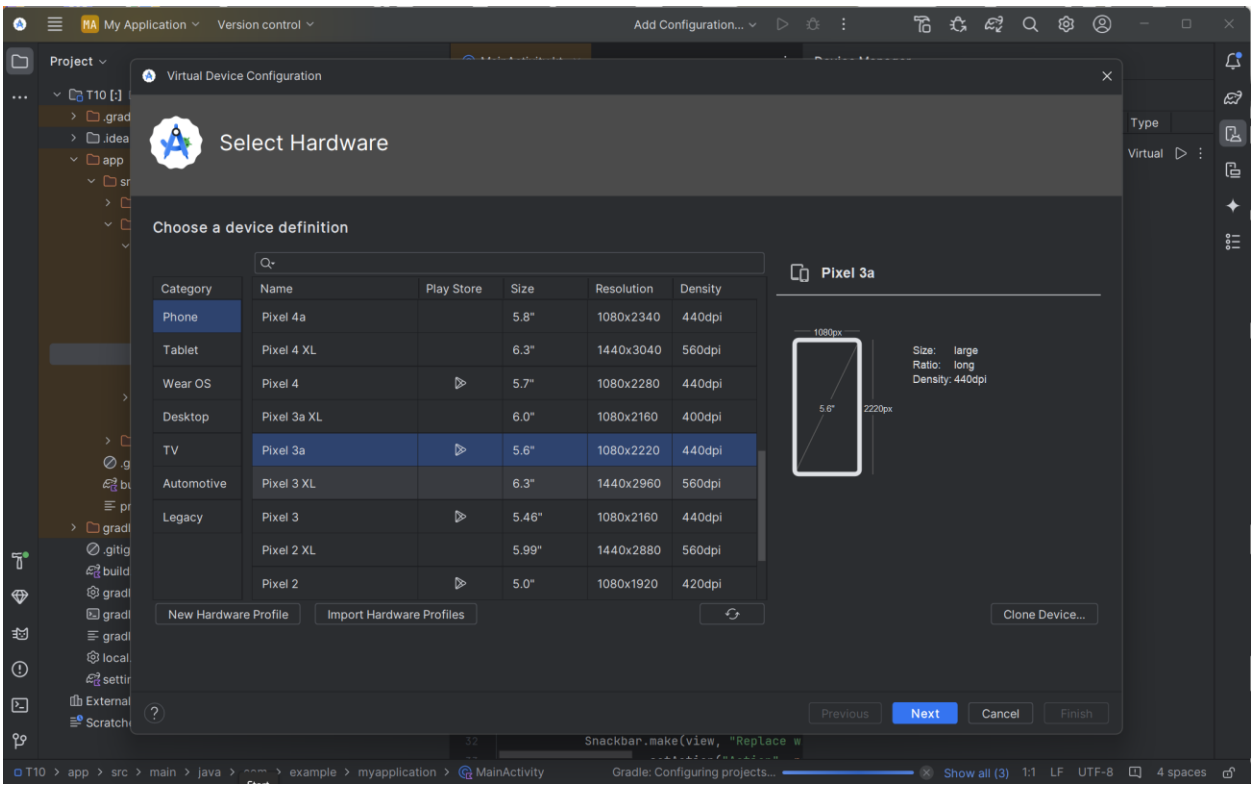


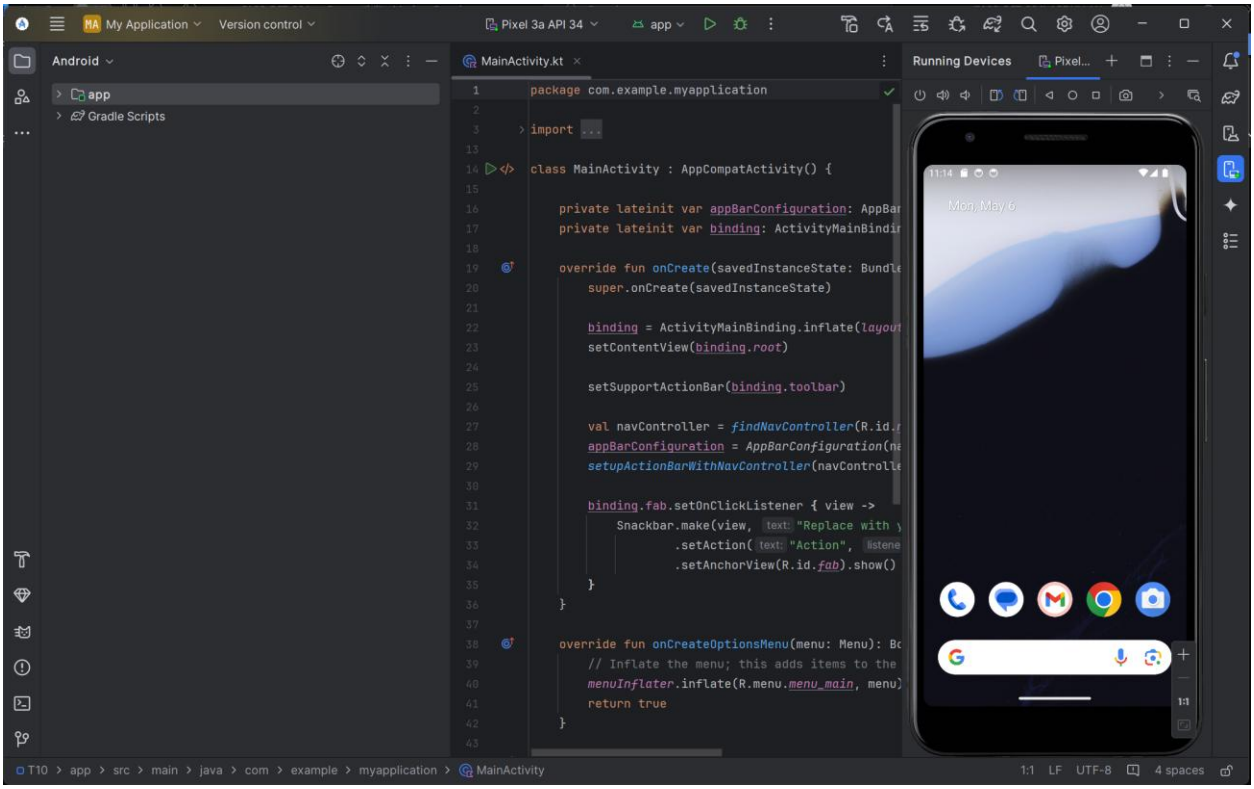
CREATING CASE:

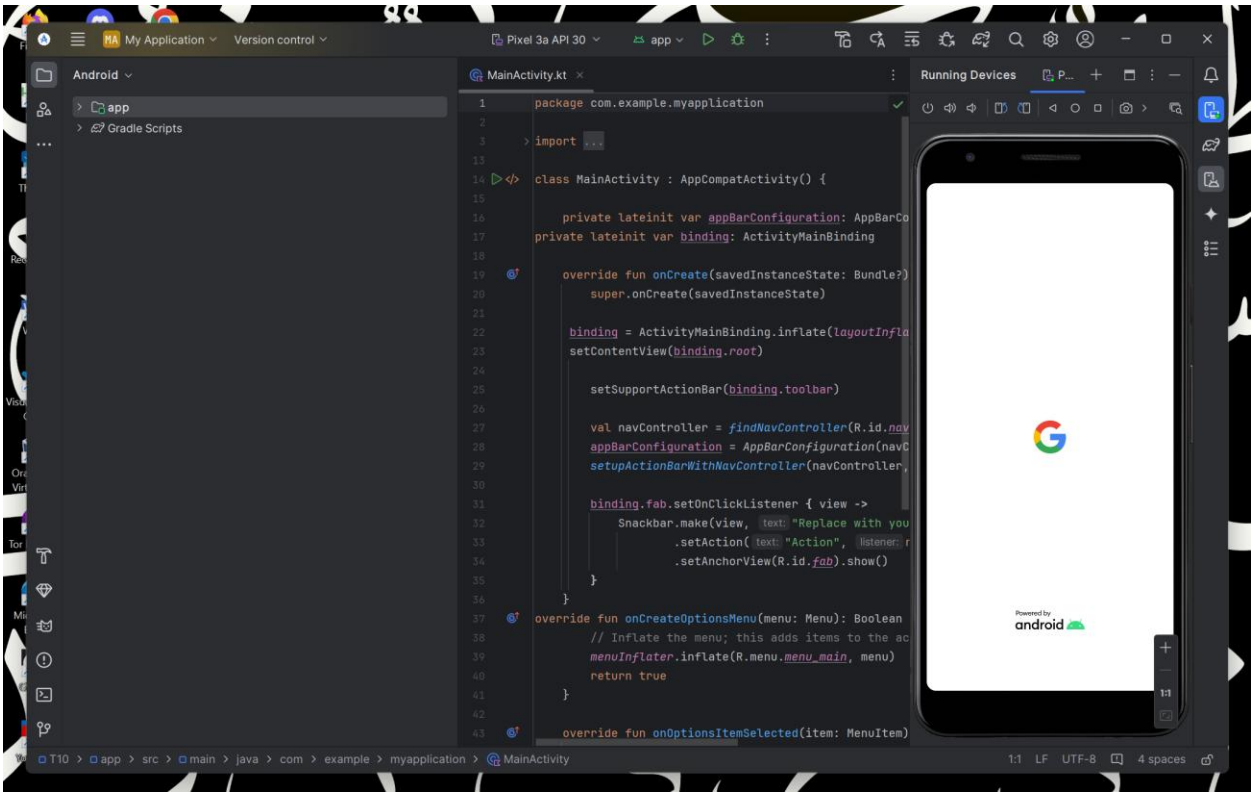


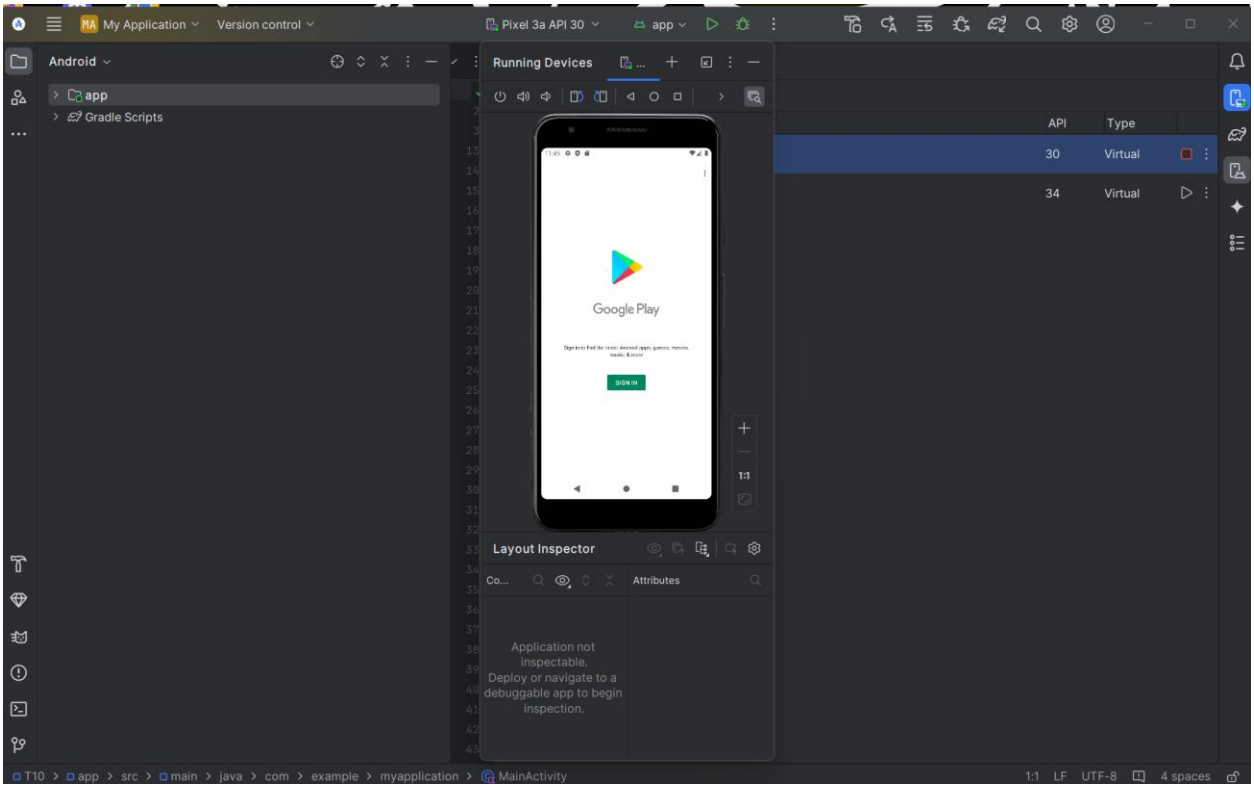
OPENING PHONE:



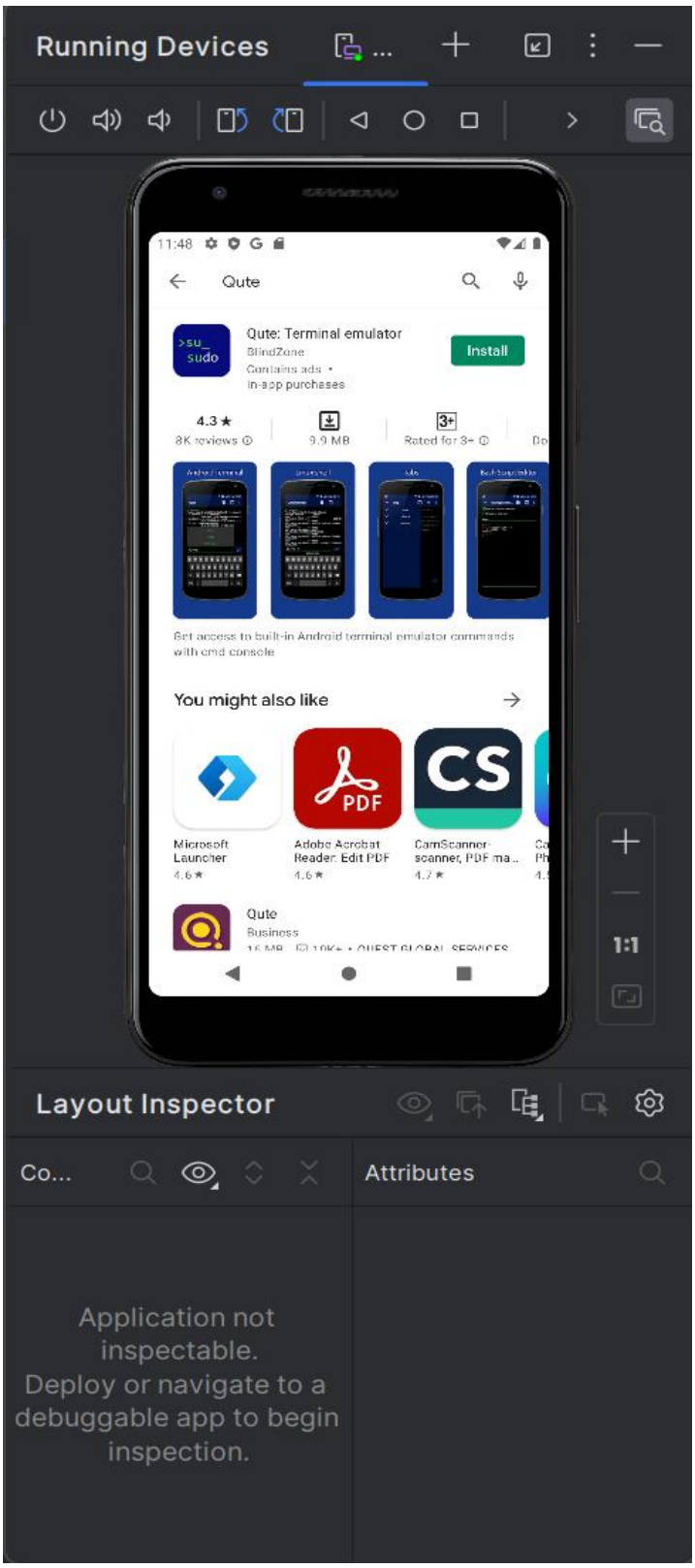



My Application
Version control
Pixel 3a API 34
app
Android
app
Gradle Scripts
MainActivity.kt
Running Devices
package com.example.myapplication
import ...
class MainActivity : AppCompatActivity() {
private lateinit var appBarConfiguration: AppBar
private lateinit var binding: ActivityMainBindi
override fun onCreate(savedInstanceState: Bundl
super.onCreate(savedInstanceState)
binding = ActivityMainBinding.inflate(layou
setContentView(binding.root)
setSupportActionBar(binding.toolbar)
val navController = findNavController(R.id.
appBarConfiguration = AppBarConfiguration(na
setupActionBarWithNavController(navControll
binding.fab.setOnClickListener { view ->
Snackbar.make(view, text: "Replace with
.setAction(text: "Action", listene
.setAnchorView(R.id.fab).show()
}
}
override fun onCreateOptionsMenu(menu: Menu): Bo
// Inflate the menu; this adds items to the
menuInflater.inflate(R.menu.menu_main, menu)
return true
}
T10 > app > src > main > java > com > example > myapplication > MainActivity
1:1 LF UTF-8 4 spaces

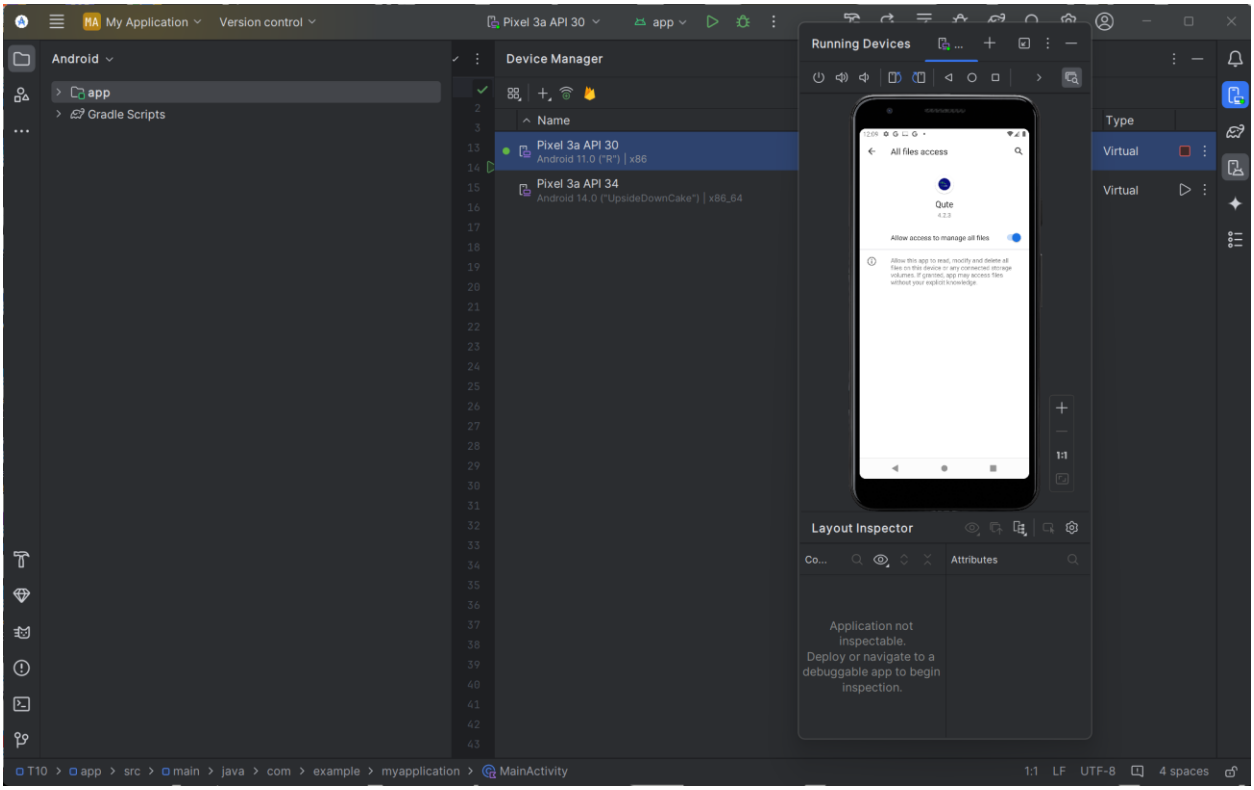

My Application
Version control
Pixel 3a API 30
app
Android
app
Gradle Scripts
MainActivity.kt
Running Devices
package com.example.myapplication
import ...
class MainActivity : AppCompatActivity() {
private lateinit var appBarConfiguration: AppBarCo
private lateinit var binding: ActivityMainBinding
override fun onCreate(savedInstanceState: Bundle?)
super.onCreate(savedInstanceState)
binding = ActivityMainBinding.inflate(layoutInfla
setContentView(binding.root)
setSupportActionBar(binding.toolbar)
val navController = findNavController(R.id.nav
appBarConfiguration = AppBarConfiguration(navC
setupActionBarWithNavController(navController,
binding.fab.setOnClickListener { view ->
Snackbar.make(view, text: "Replace with you
.setAction(text: "Action", listener: r
.setAnchorView(R.id.fab).show()
}
}
override fun onCreateOptionsMenu(menu: Menu): Boolean
// Inflate the menu; this adds items to the ac
menuInflater.inflate(R.menu.menu_main, menu)
return true
}
override fun onOptionsItemSelected(item: MenuItem)
Powered by
android
T10 > app > src > main > java > com > example > myapplication > MainActivity
1:1 LF UTF-8 4 spaces



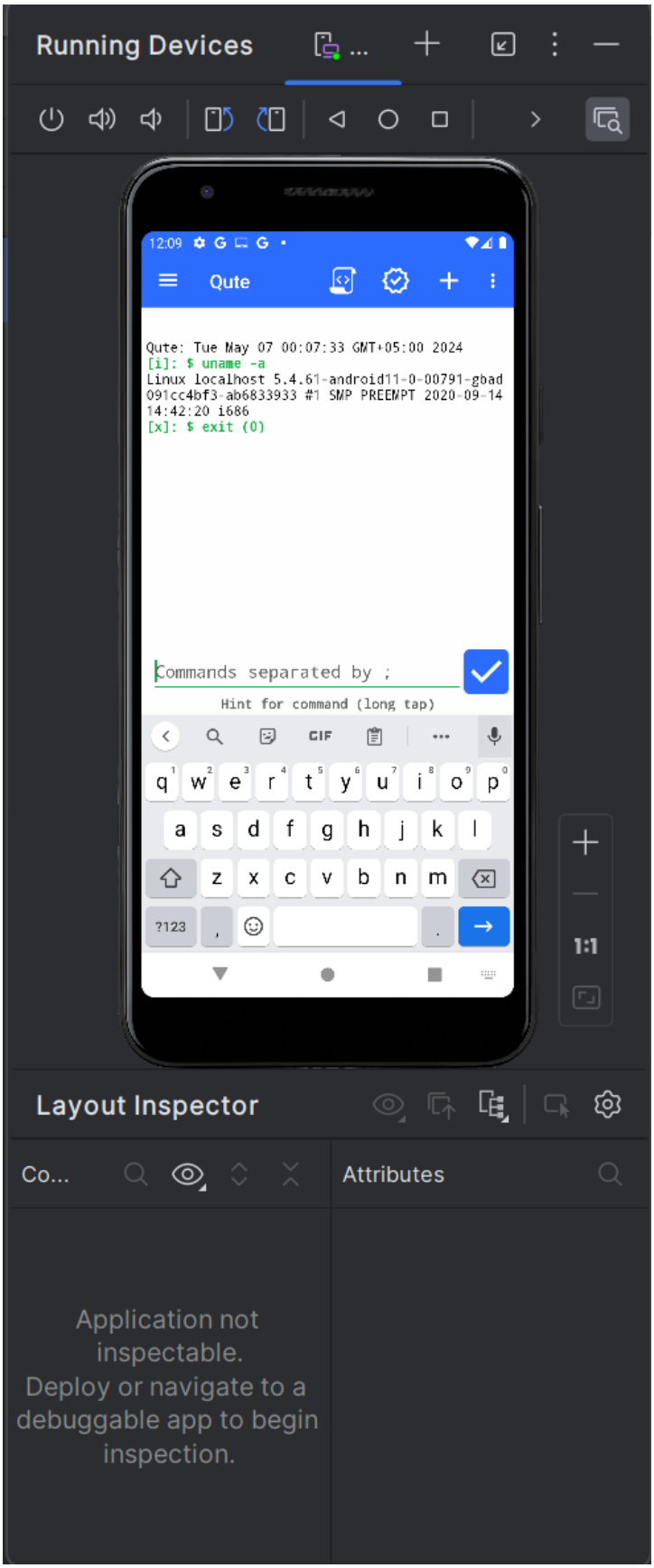
DOWNLOADING QUTE EMULATOR APP:


Running Devices
11:48
Qute
Qute: Terminal emulator
BlindZone
Contains ads •
In-app purchases
Install
4.3 ★
8K reviews
9.9 MB
3+
Rated for 3+
Get access to built-in Android terminal emulator commands with cmd console
You might also like
Microsoft Launcher
Adobe Acrobat Reader: Edit PDF
CamScanner- scanner, PDF ma...
Qute
Business
1:1
Layout Inspector
Co...
Attributes
Application not inspectable.
Deploy or navigate to a debuggable app to begin inspection.

GRANTING ALL FILE ACCESS

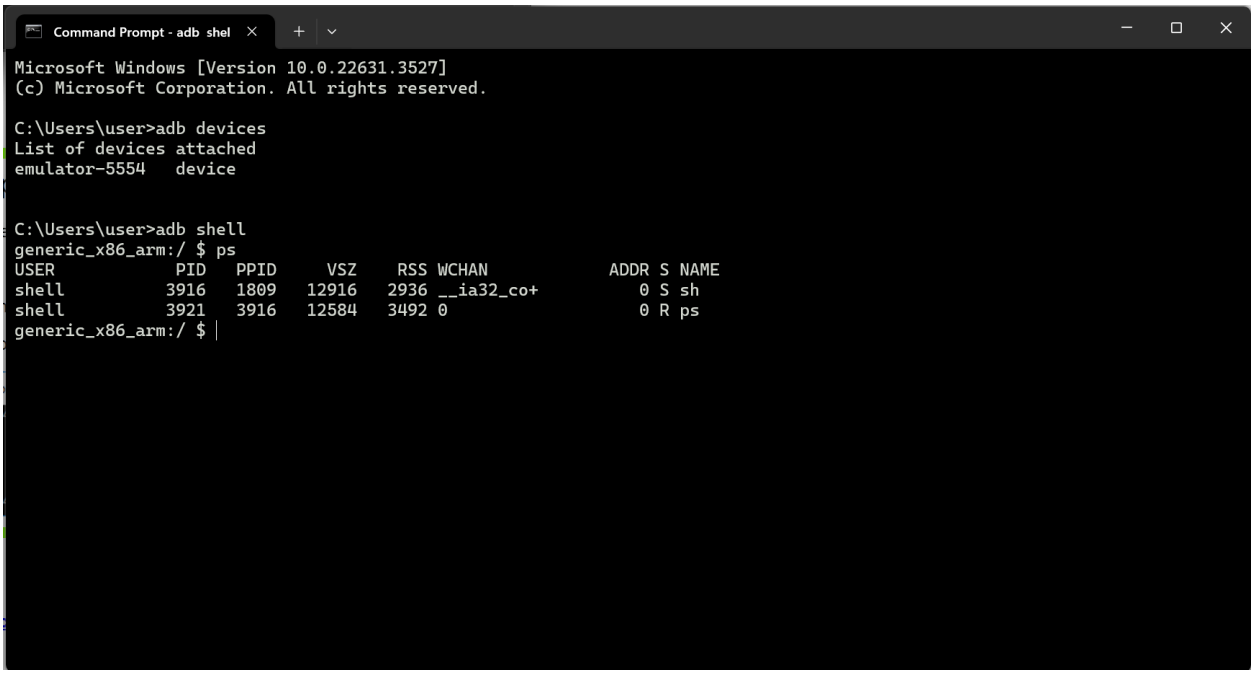


RUNNING COMMAND:

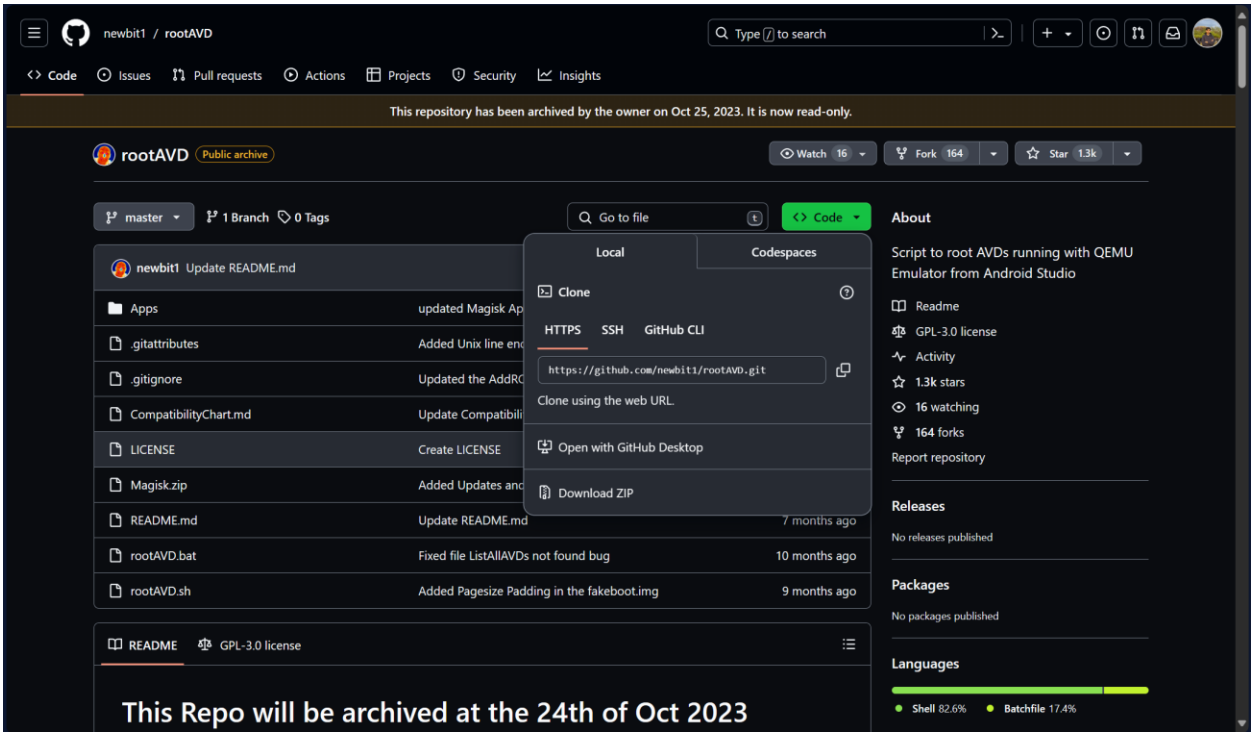

Running Devices
12:09
Qute
Qute: Tue May 07 00:07:33 GMT+05:00 2024
[i]: $ uname -a
Linux localhost 5.4.61-android11-0-00791-gbad
091cc4bf3-ab6833933 #1 SMP PREEMPT 2020-09-14
14:42:20 i686
[x]: $ exit (0)
Commands separated by ;
Hint for command (long tap)
1:1
Layout Inspector
Co...
Attributes
Application not inspectable.
Deploy or navigate to a debuggable app to begin inspection.

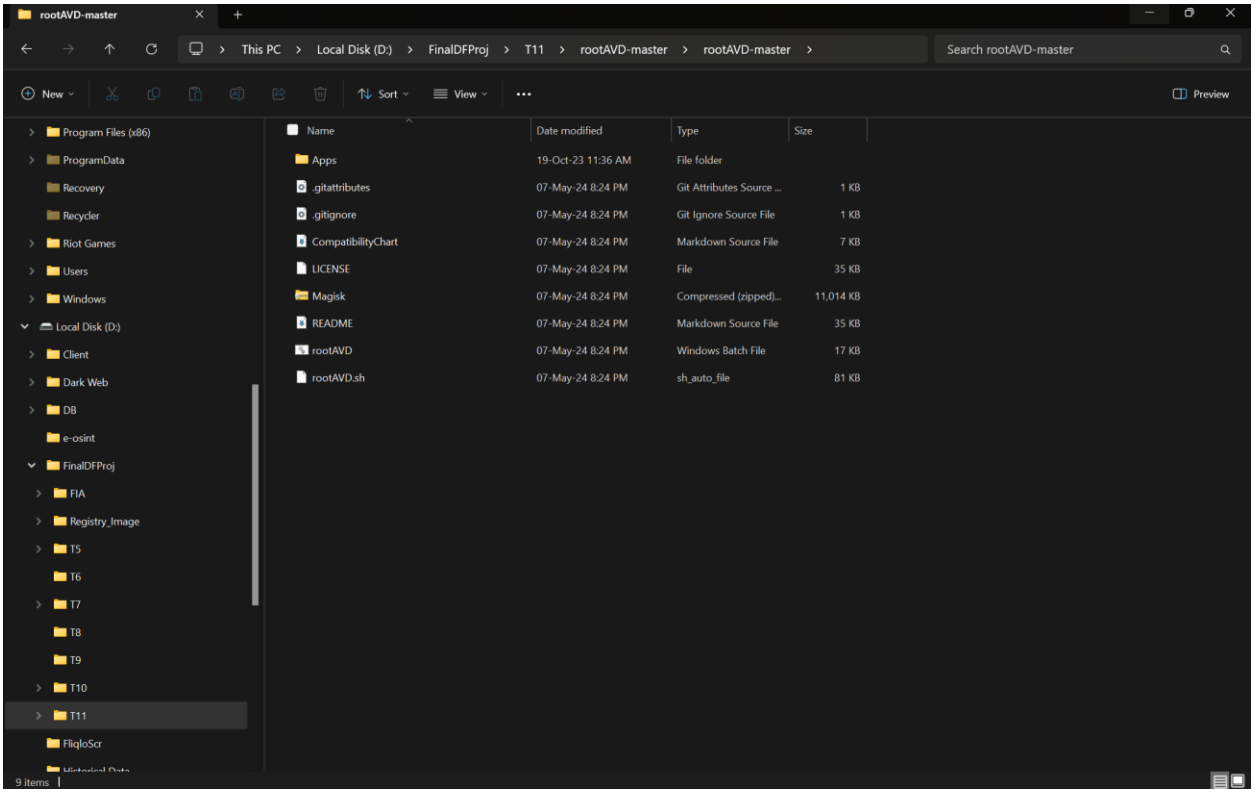
11. Rooting Android Studio's Emulator AND 14

STARTING ADB:

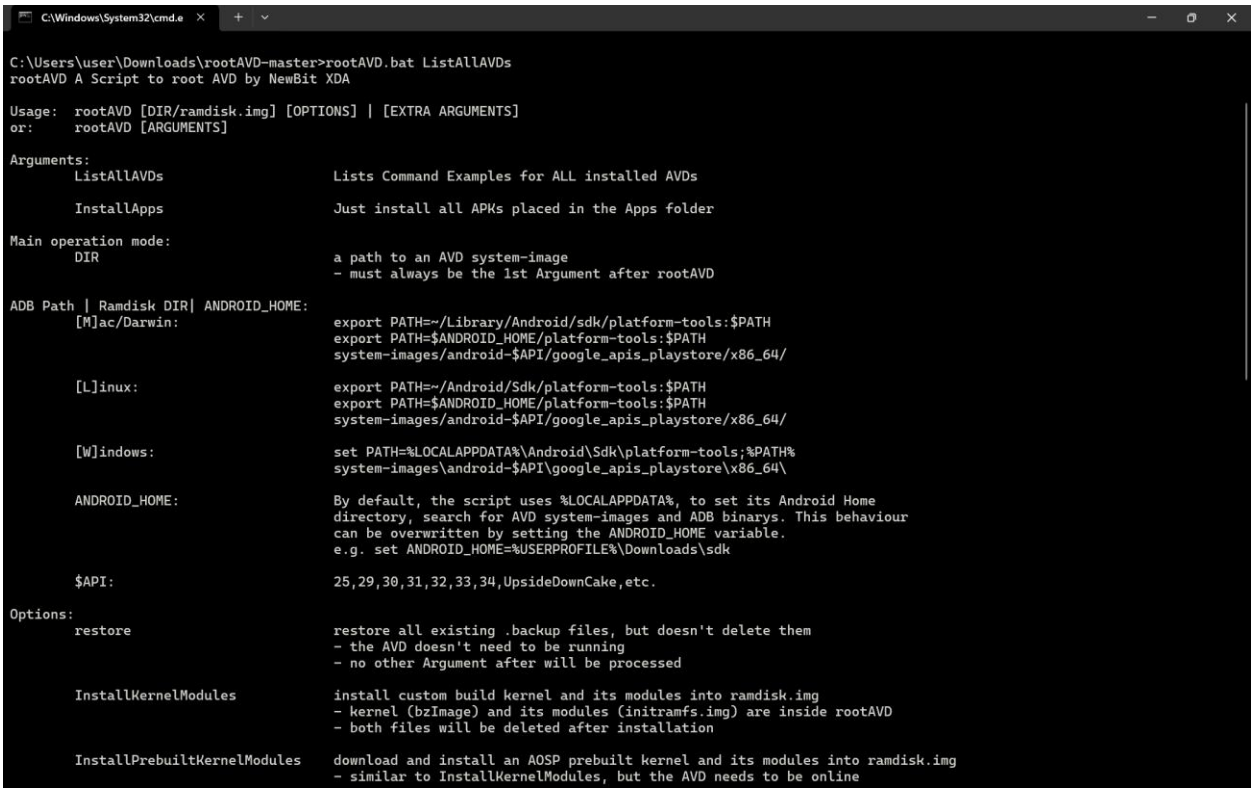


DOWNLOADING rootAVD FOR ROOTING:

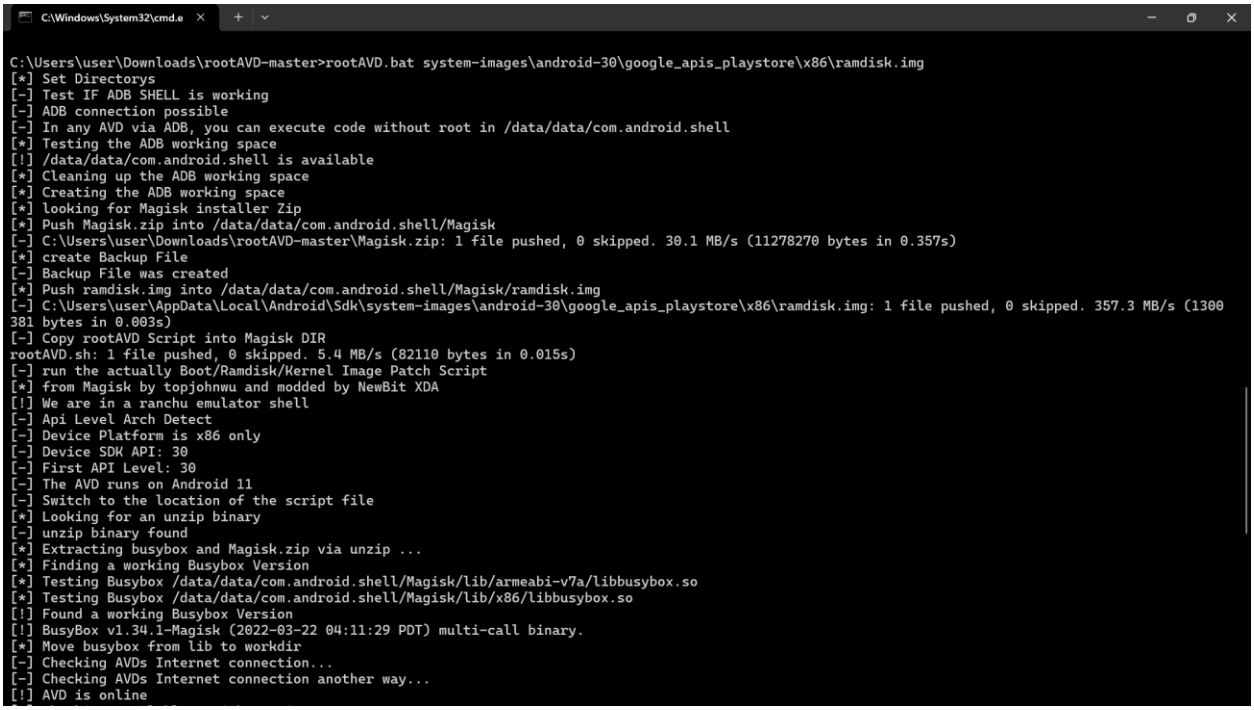




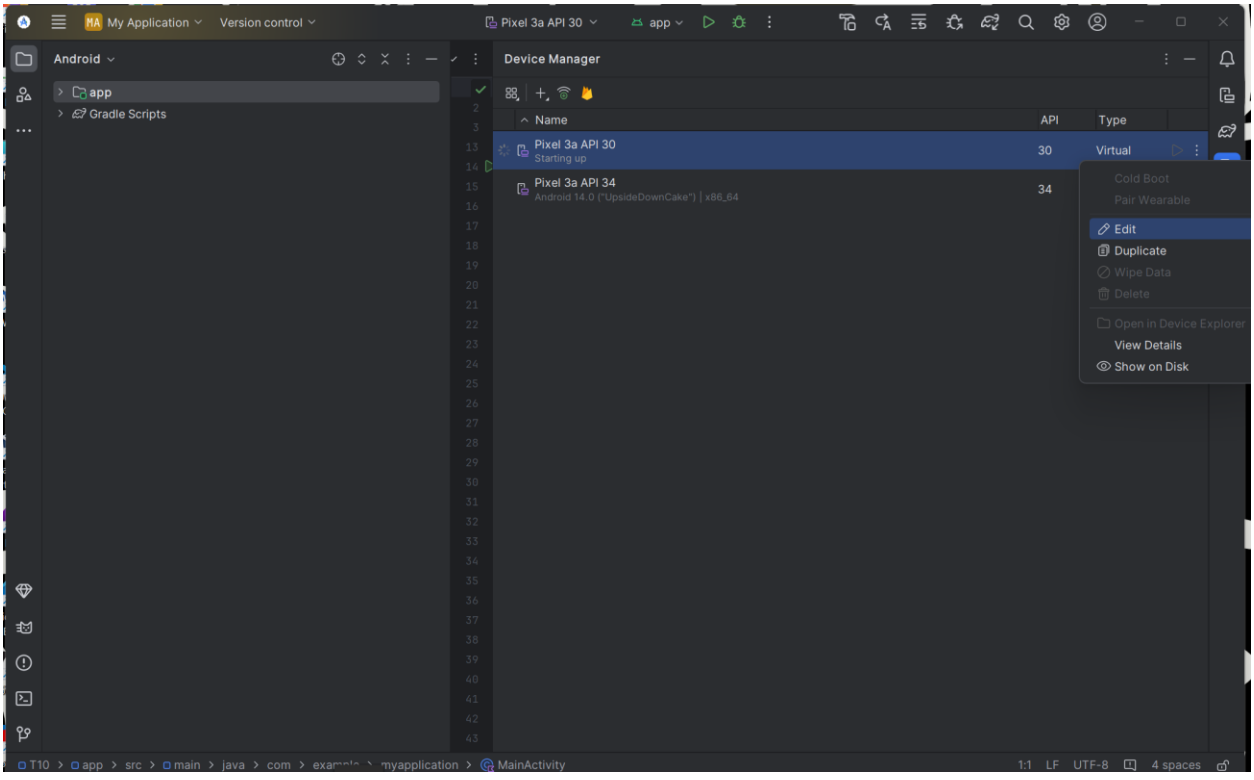
rootAVD COMMAND:



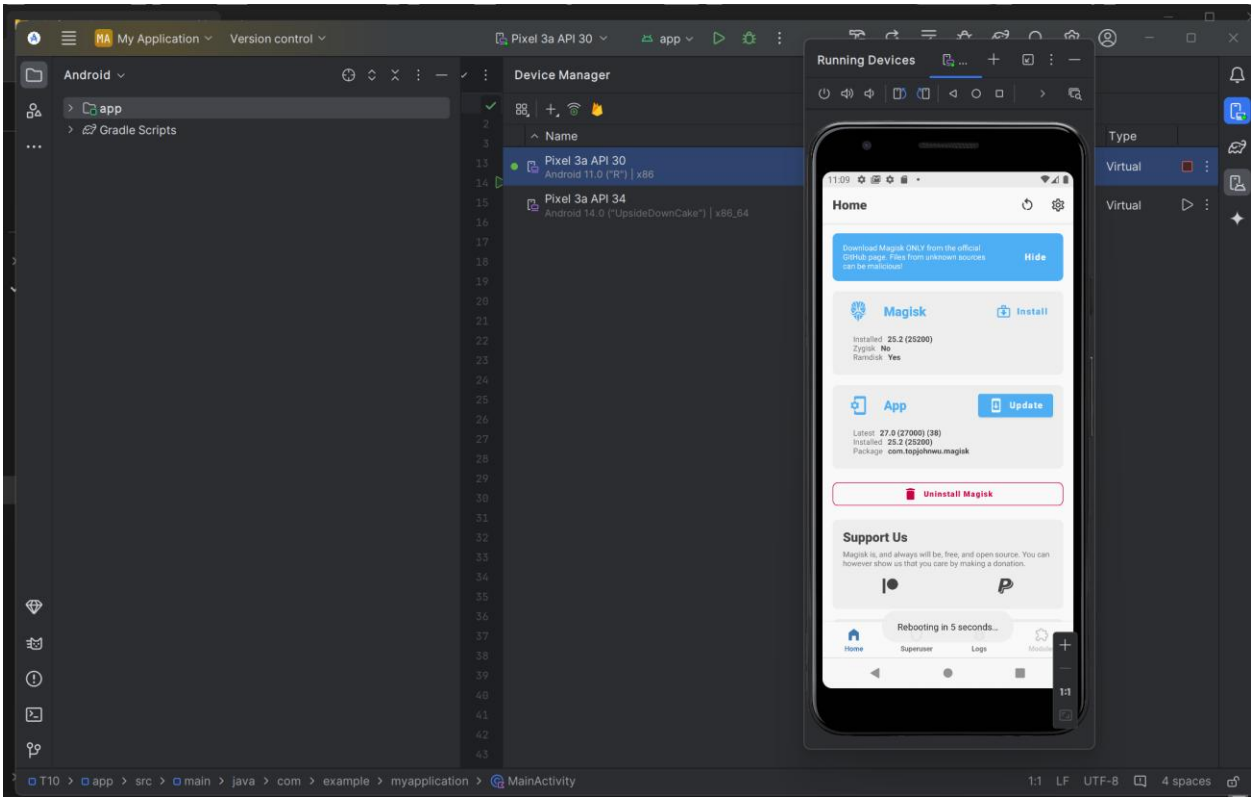
ACQUIRING RAMDISK IMAGE OF DEVICE:



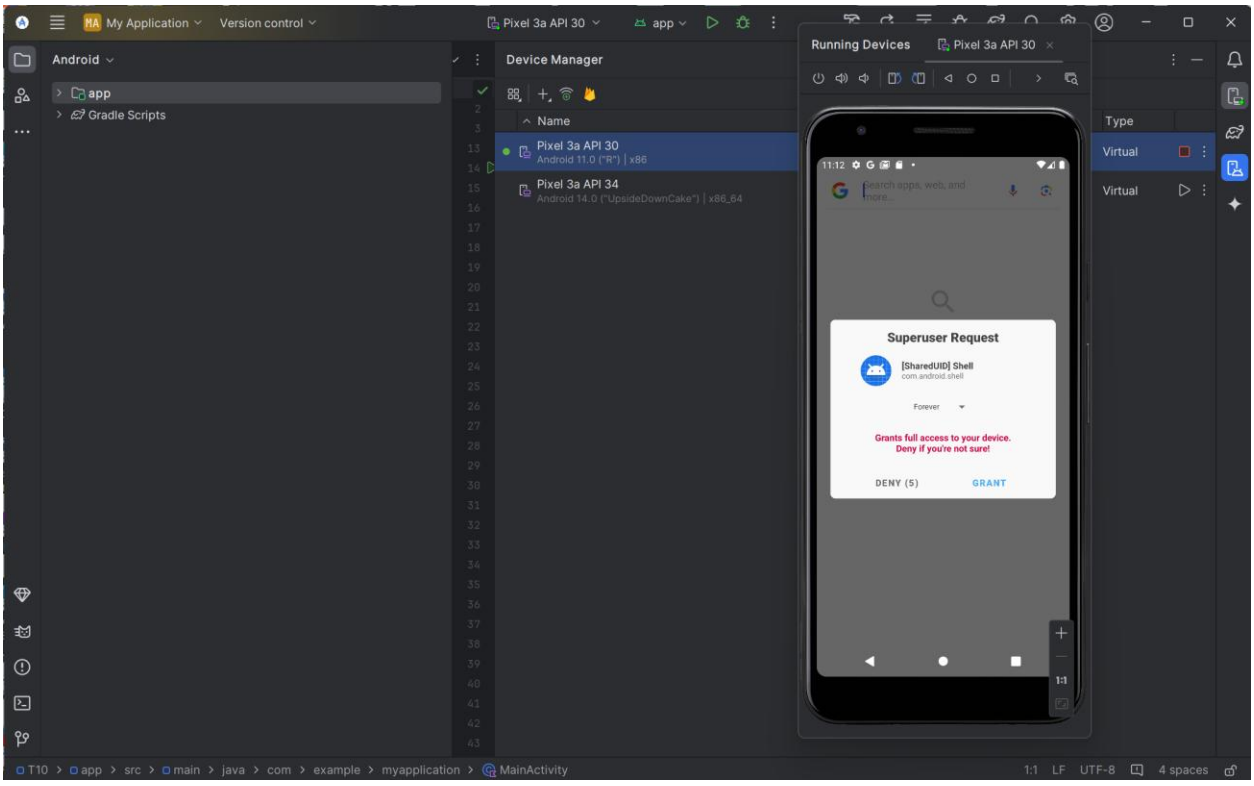
COLD BOOTING OF DEVICE:



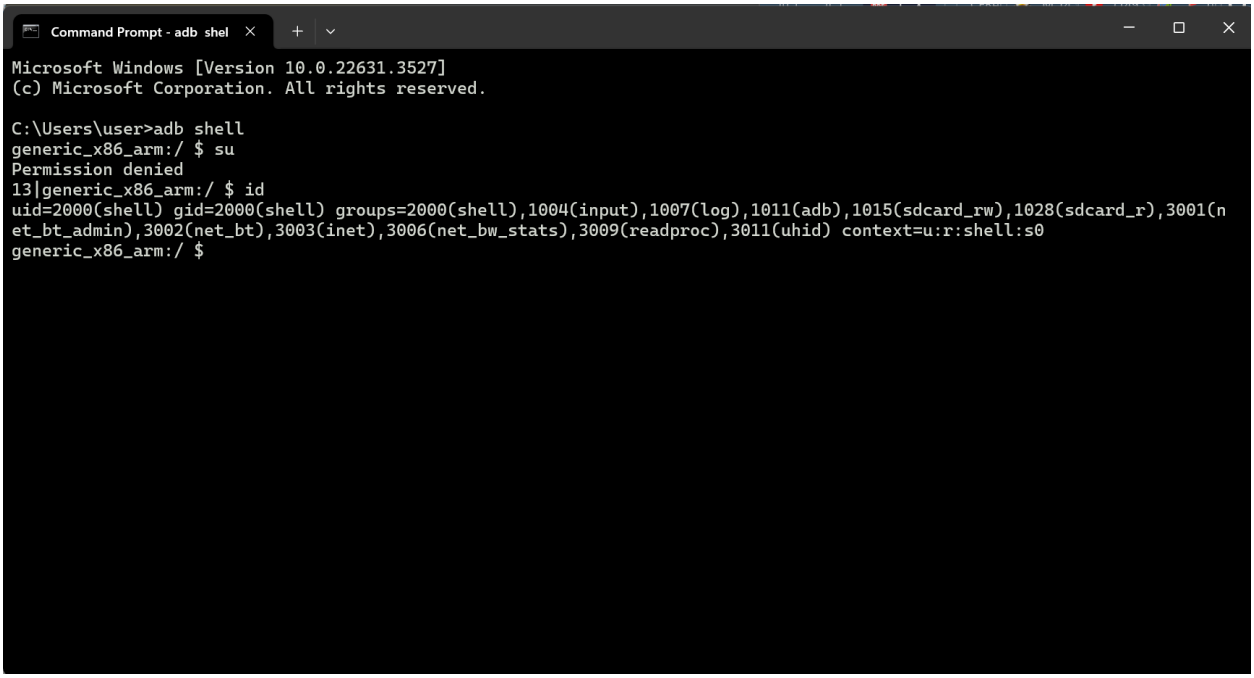
MAGISK SOFTWARE:



SHELL ACCESS GRANT:

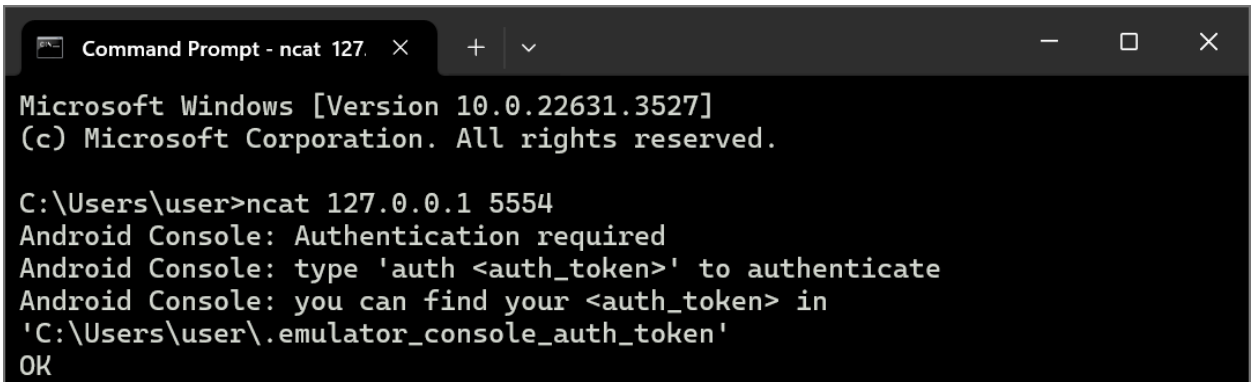


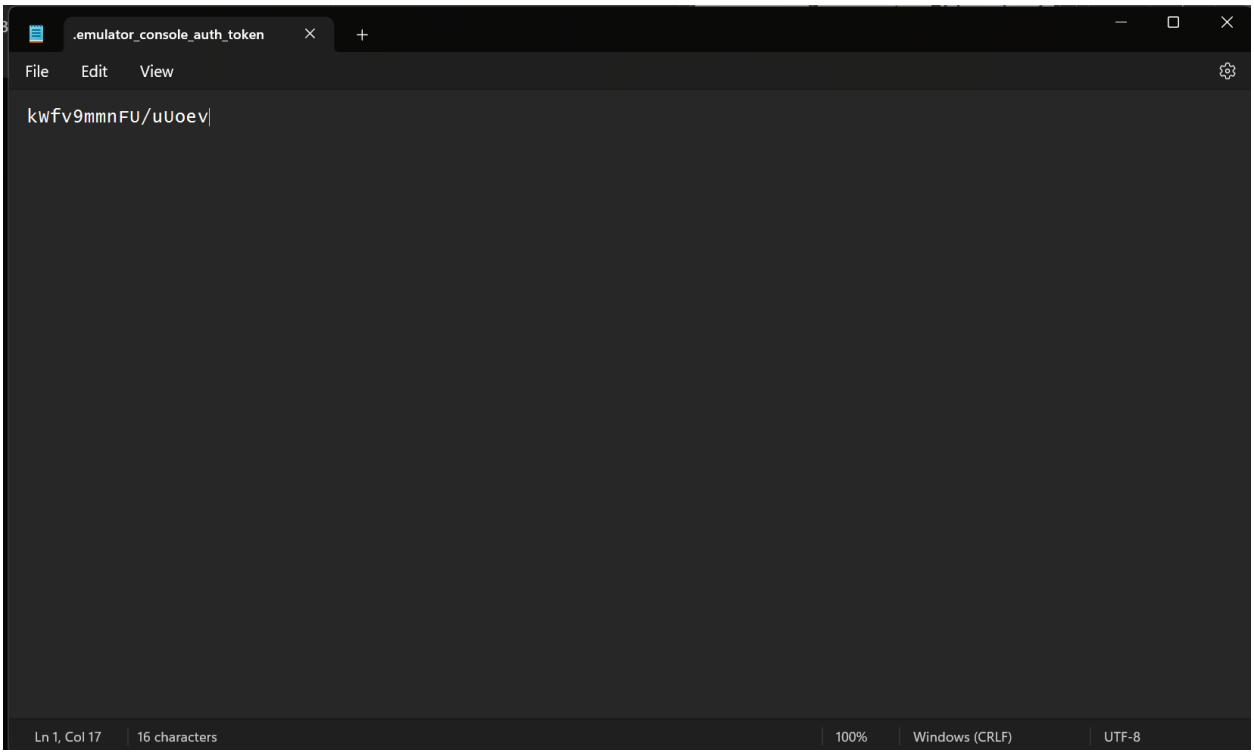
FLAG(SHELL):


Command Prompt - adb shel
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(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc),3011(uhid) context=u:r:shell:s0
generic_x86_arm:/ $

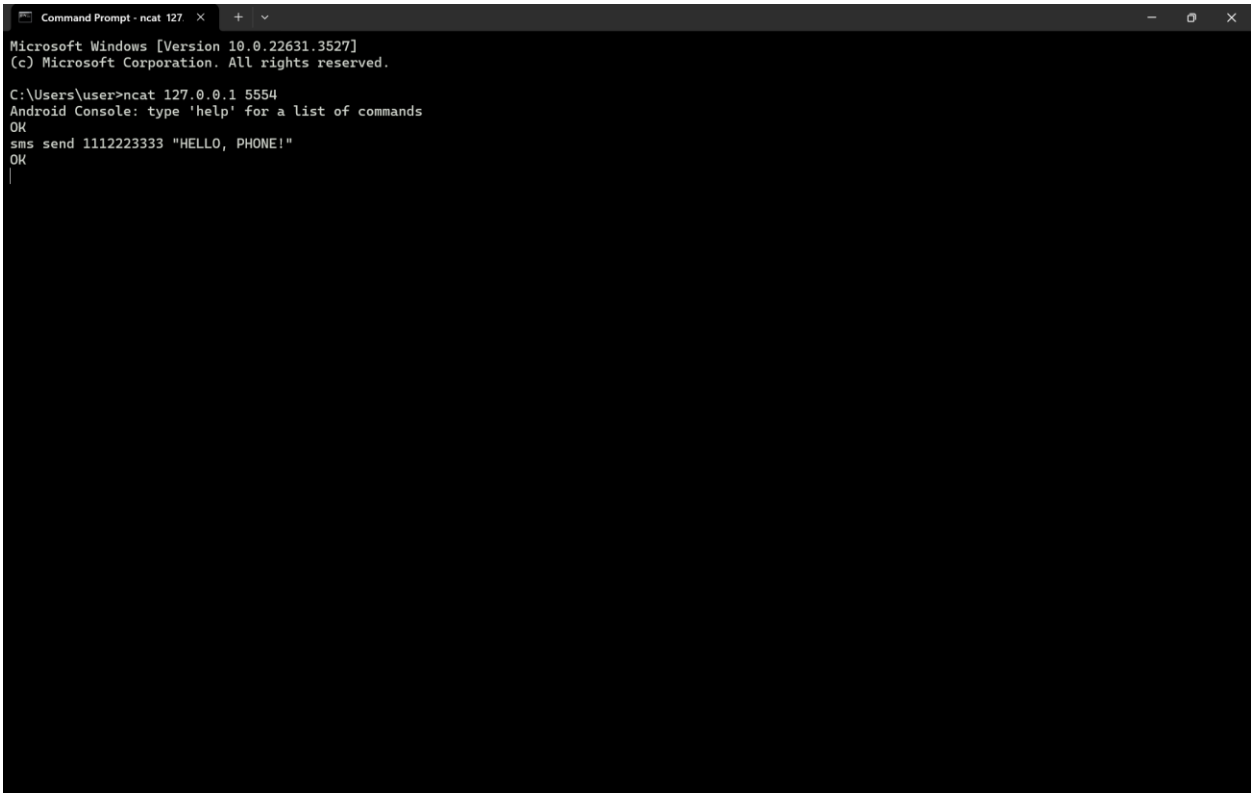
12. Forensic Acquisition from Android

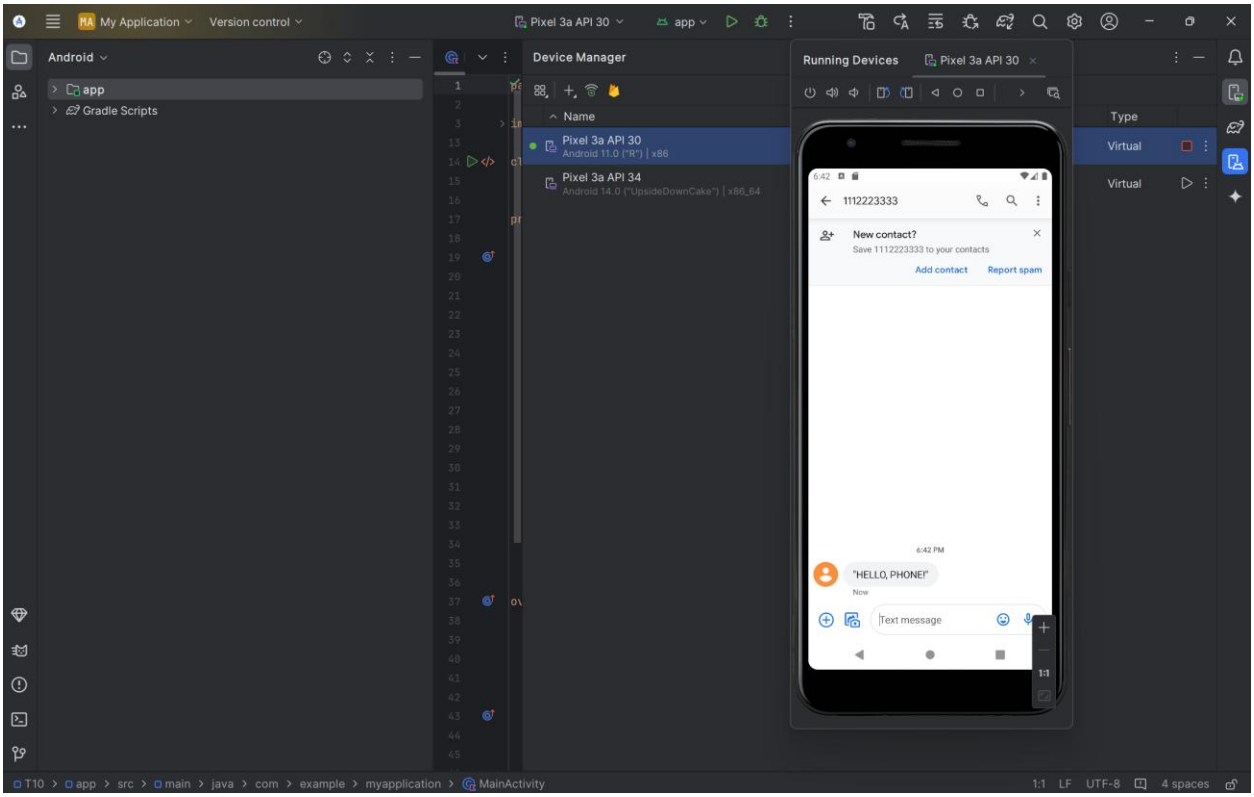
NCAT STARTING AUTH TOKEN:



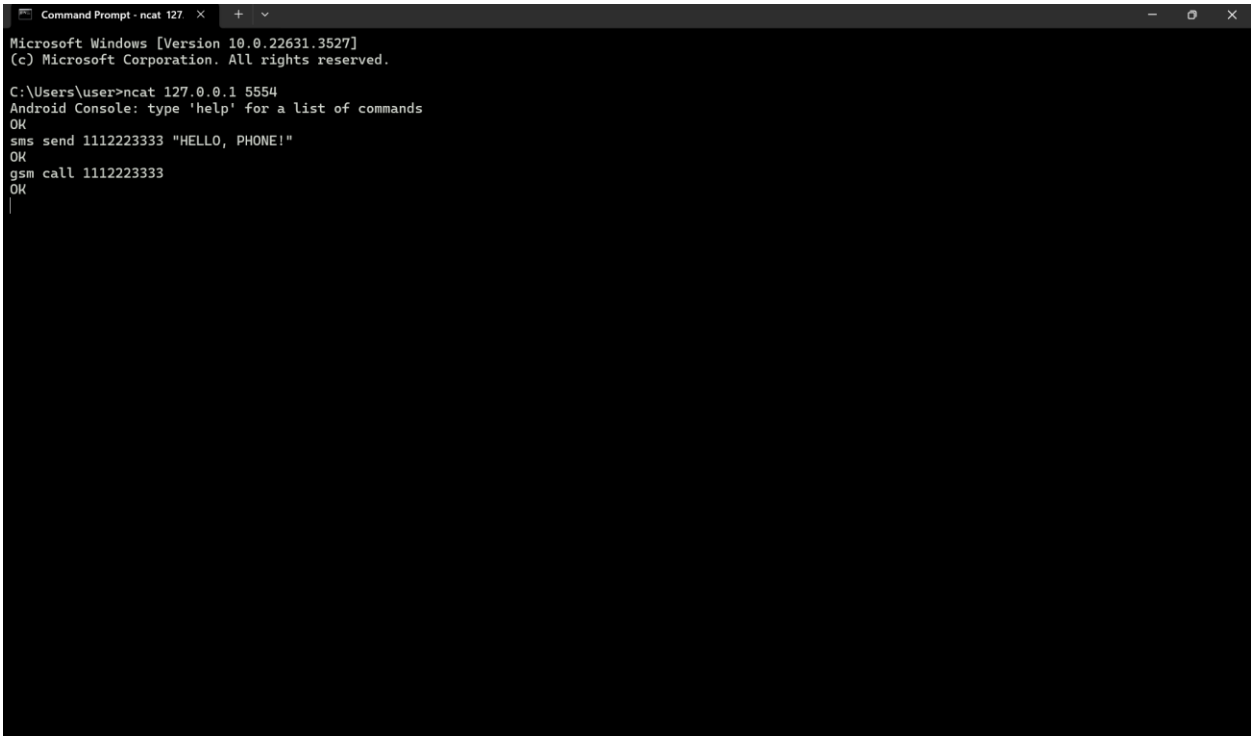


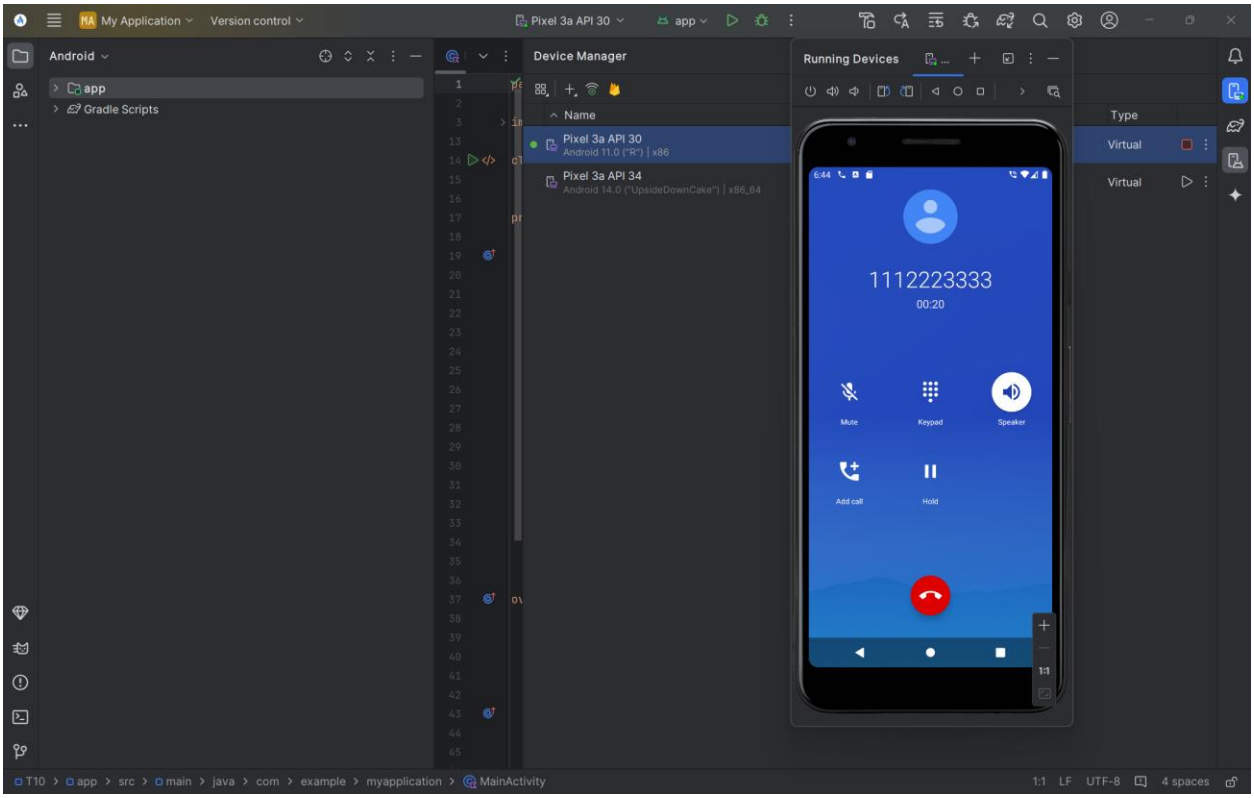
SENDING MESSAGE TO PHONE:



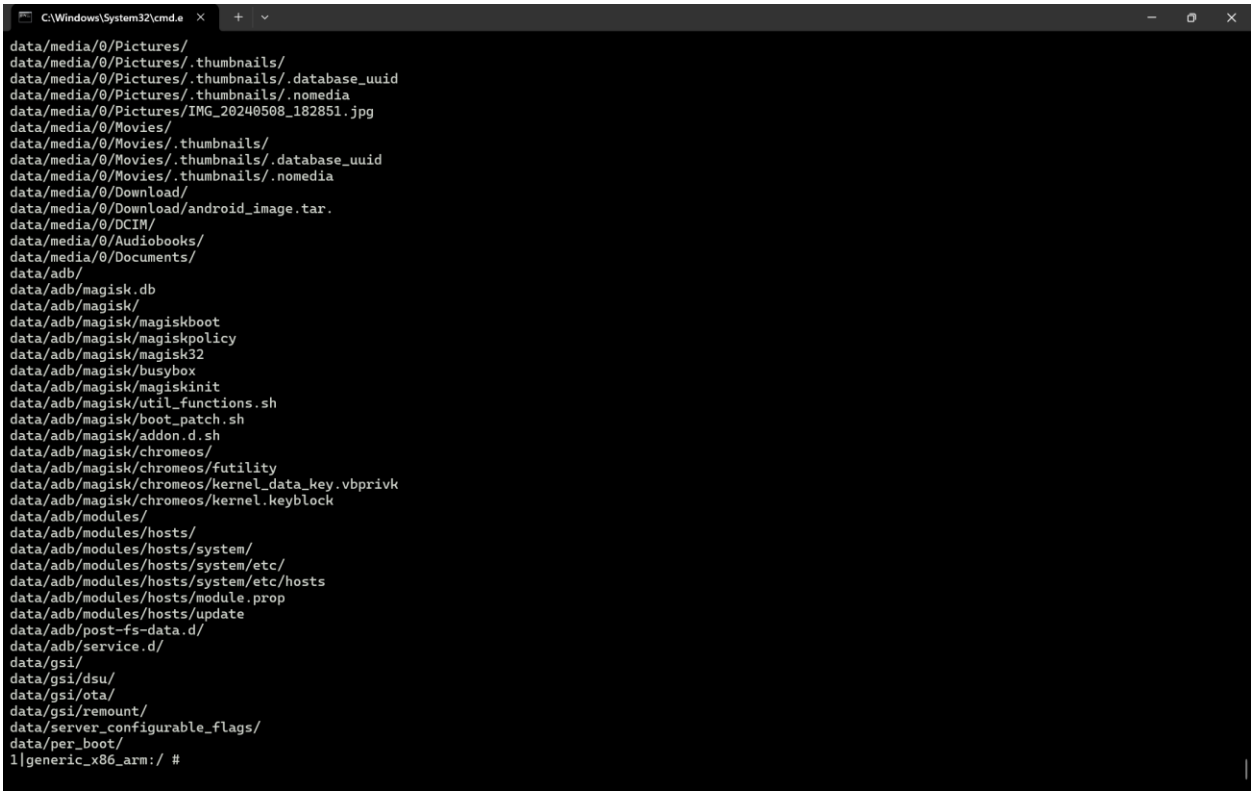


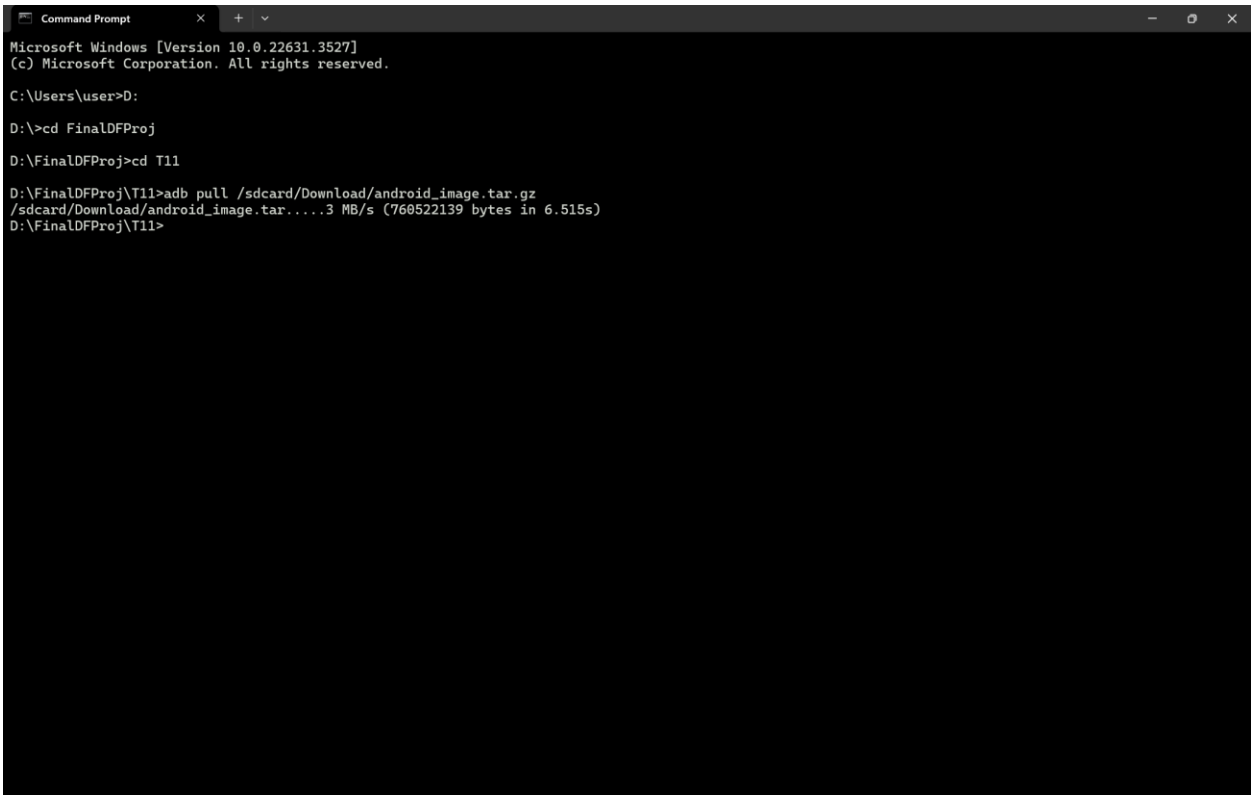
CALLING PHONE:



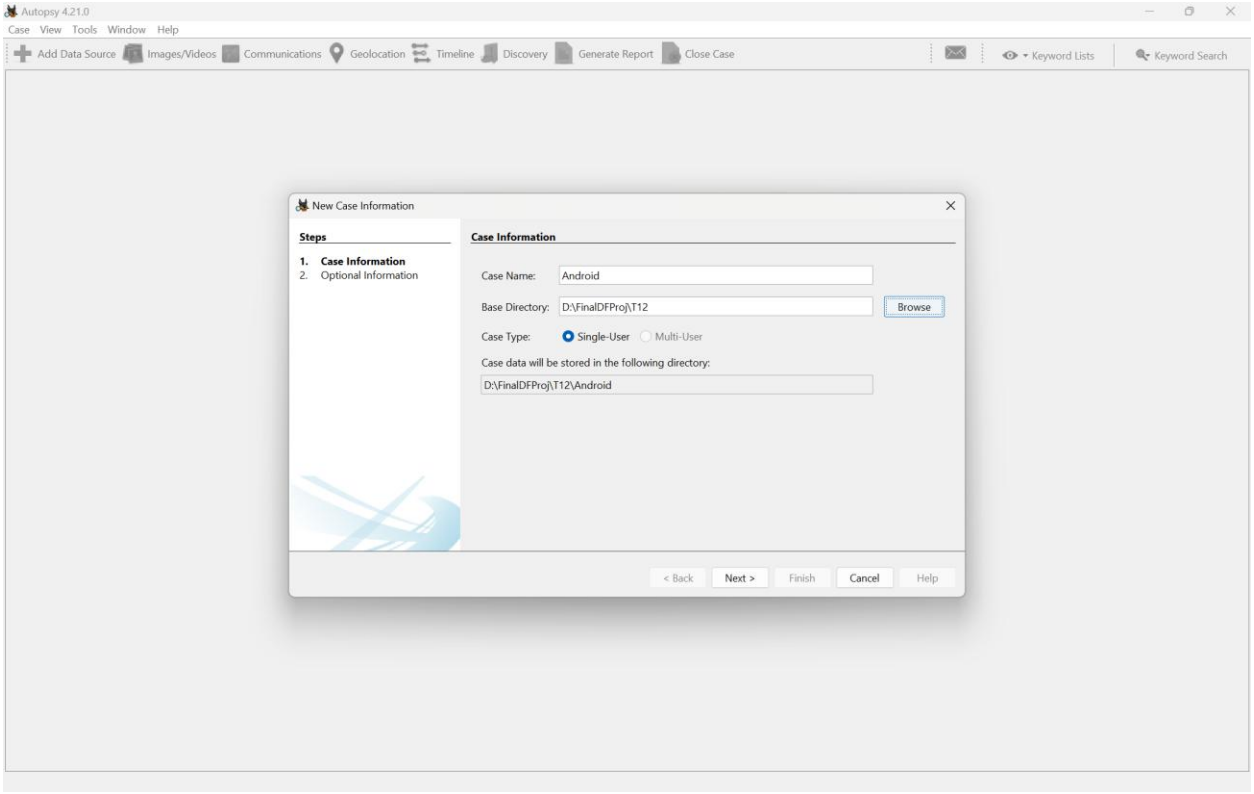


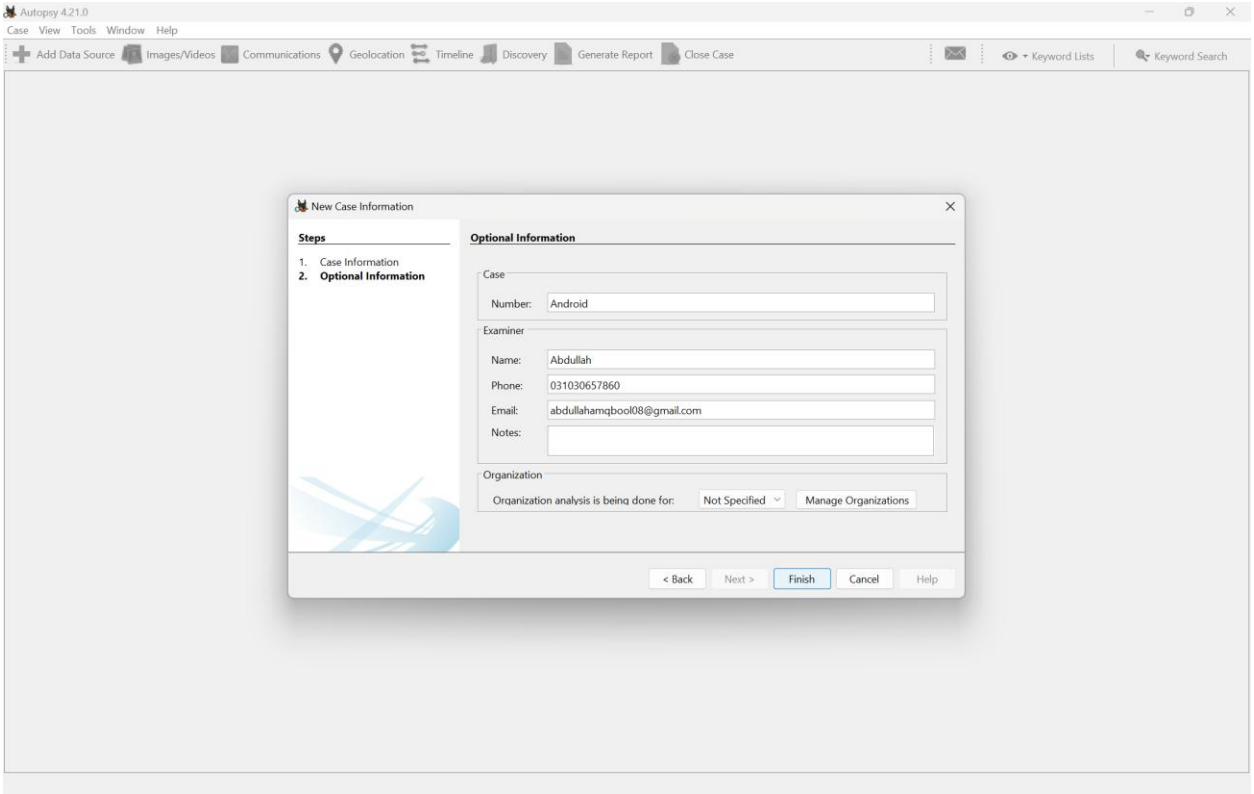
ACQUIRING IMAGE:

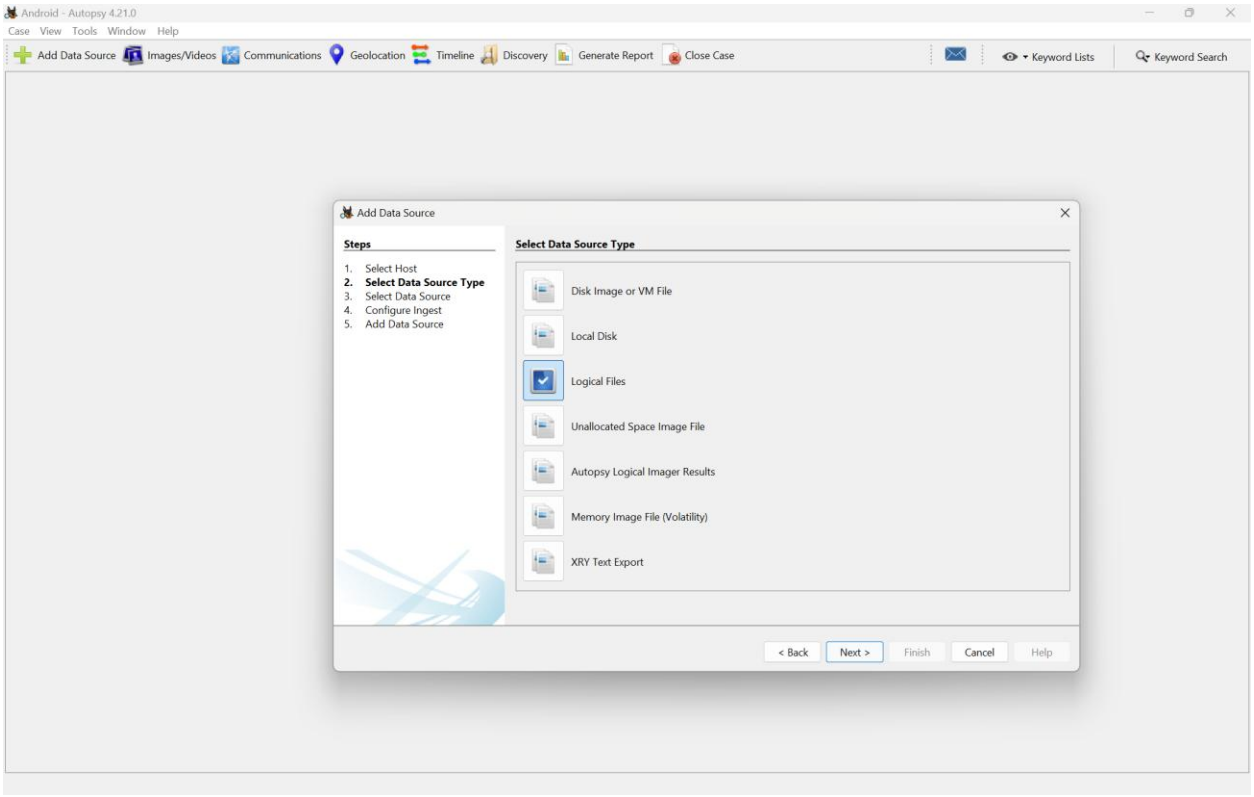


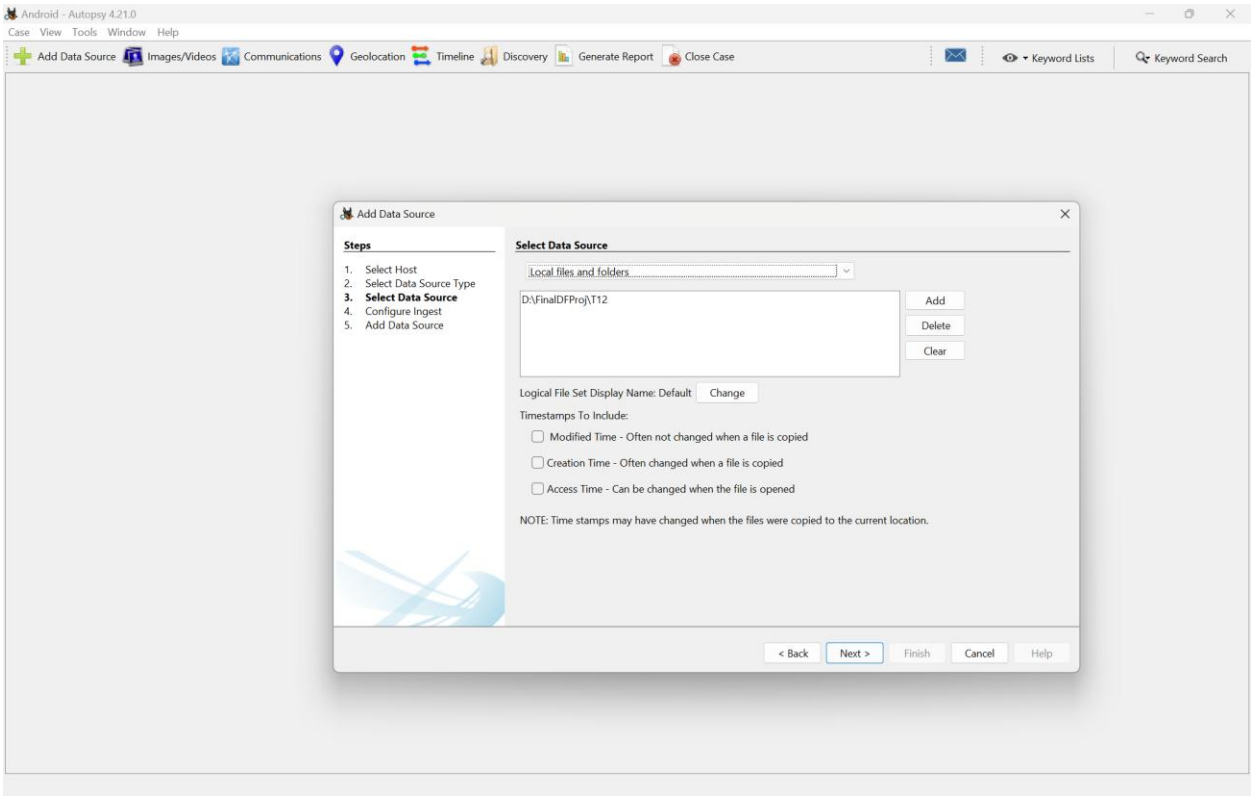


RUNNING AUTOPSY:

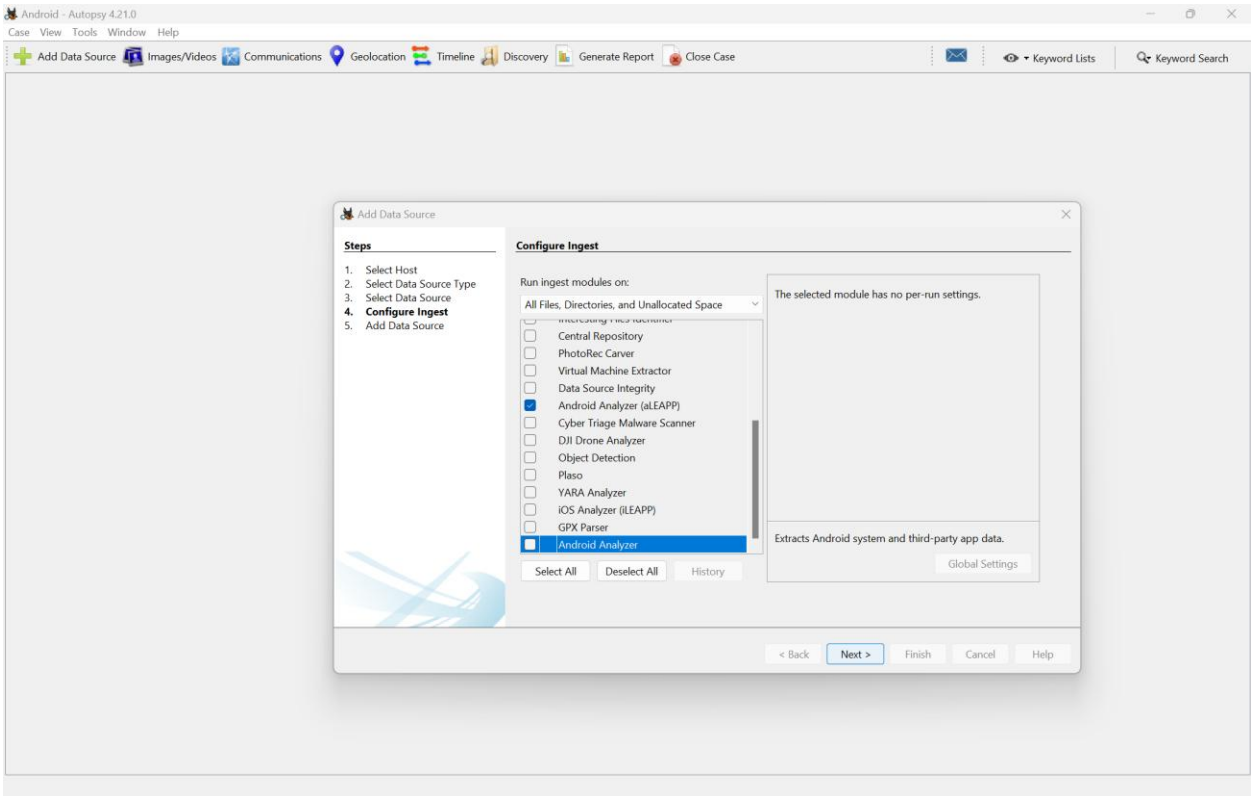




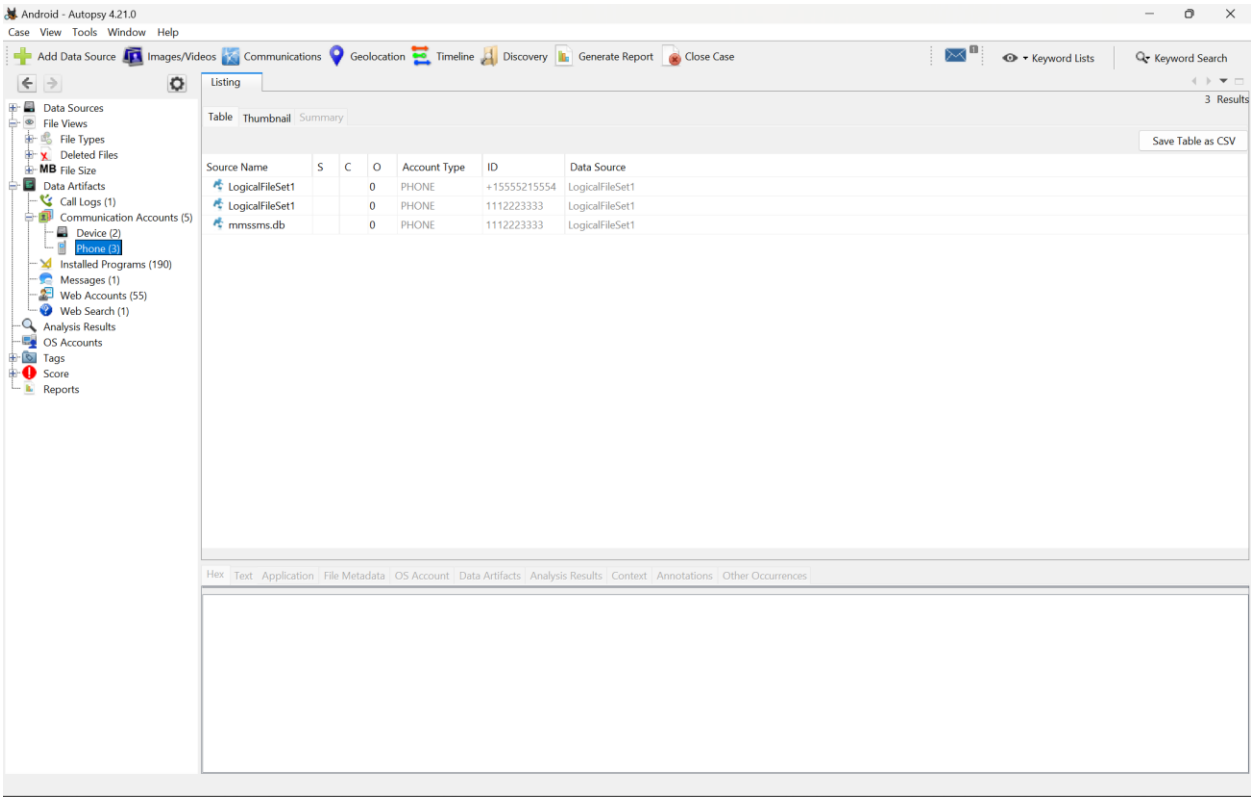

Android - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source 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
Next >
Finish
Cancel
Help


Android - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
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
Local files and folders
D:\FinalDFProj\T12
Add
Delete
Clear
Logical File Set Display Name: Default
Change
Timestamps To Include:
Modified Time - Often not changed when a file is copied
Creation Time - Often changed when a file is copied
Access Time - Can be changed when the file is opened
NOTE: Time stamps may have changed when the files were copied to the current location.
< Back
Next >
Finish
Cancel
Help

CHECKBOXING:

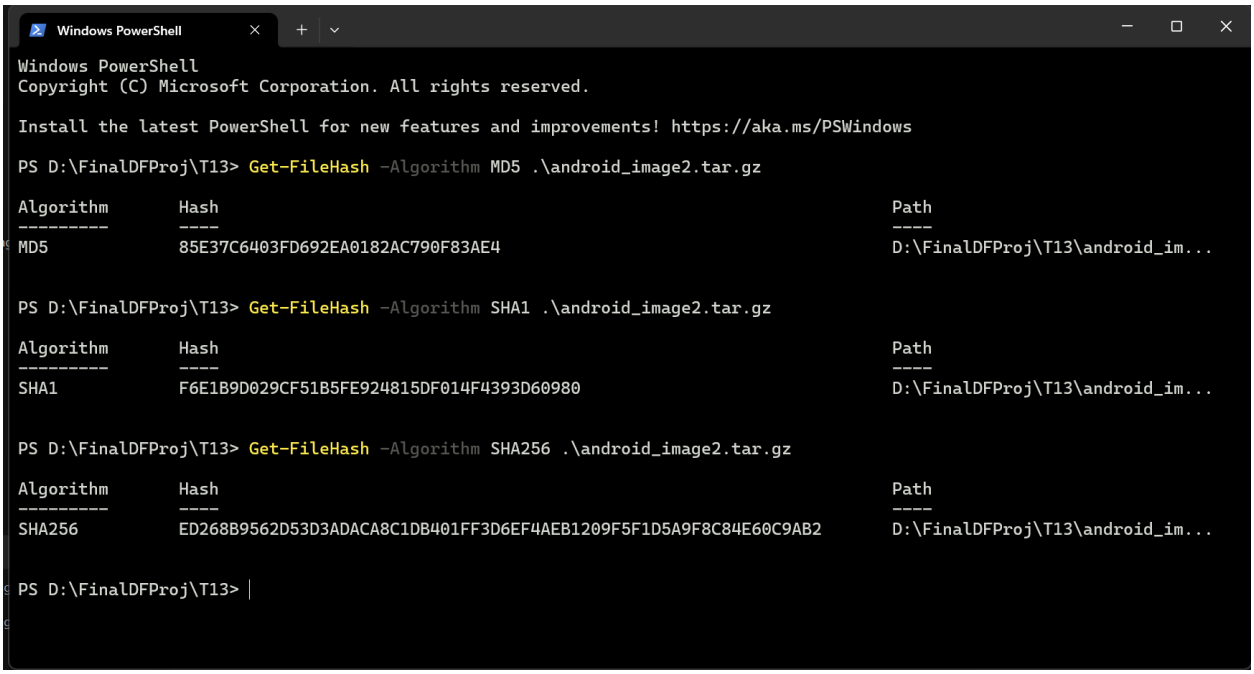


FLAG (MMSSMS.DB):

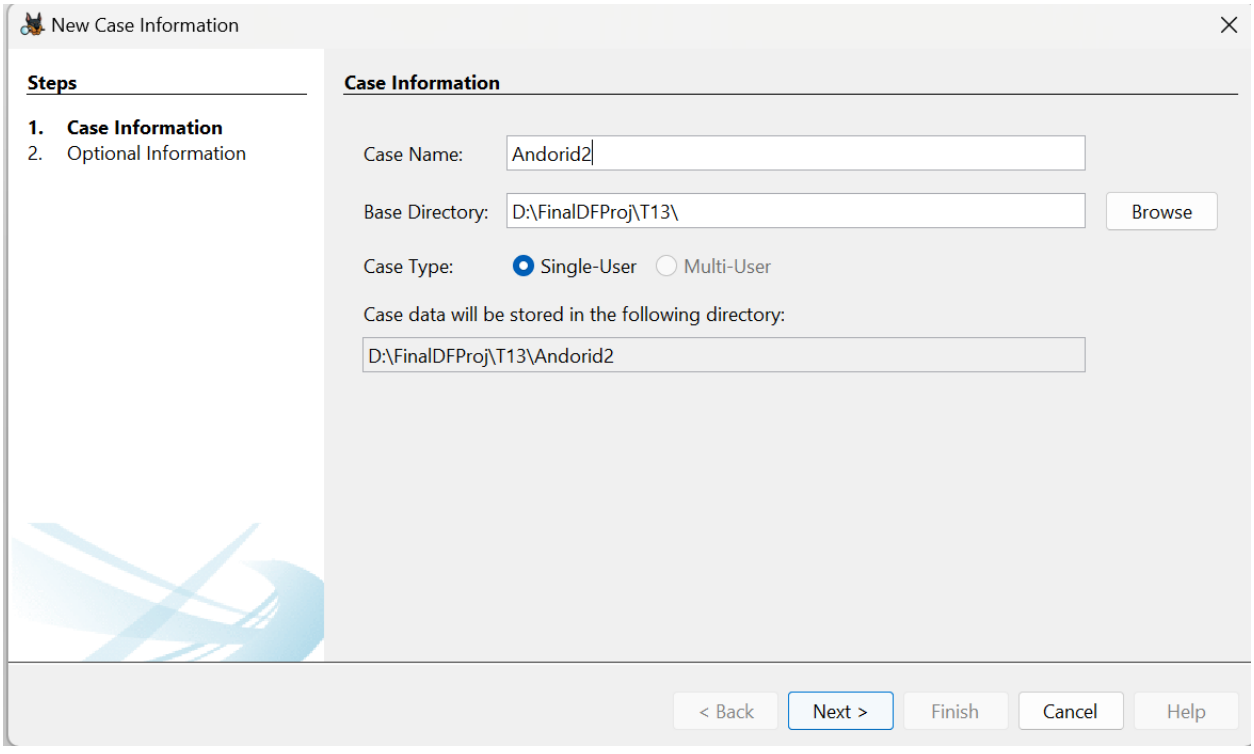


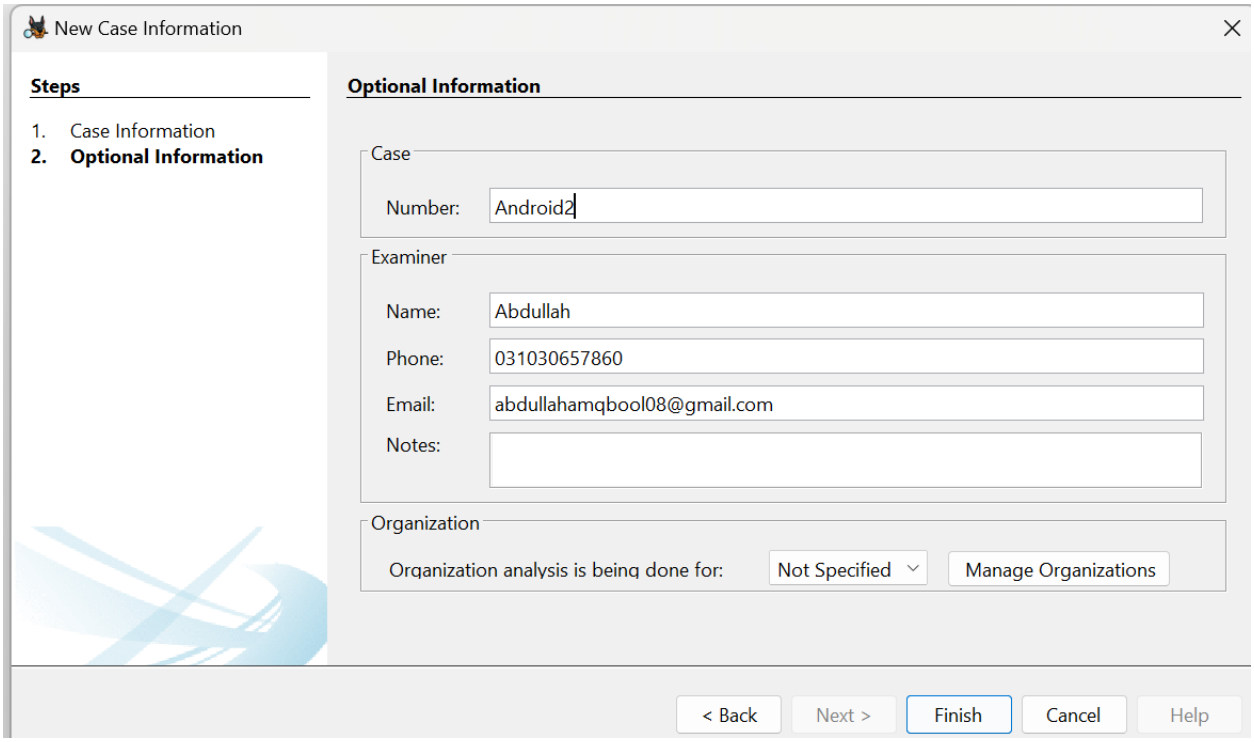
13. Android Analysis with Autopsy

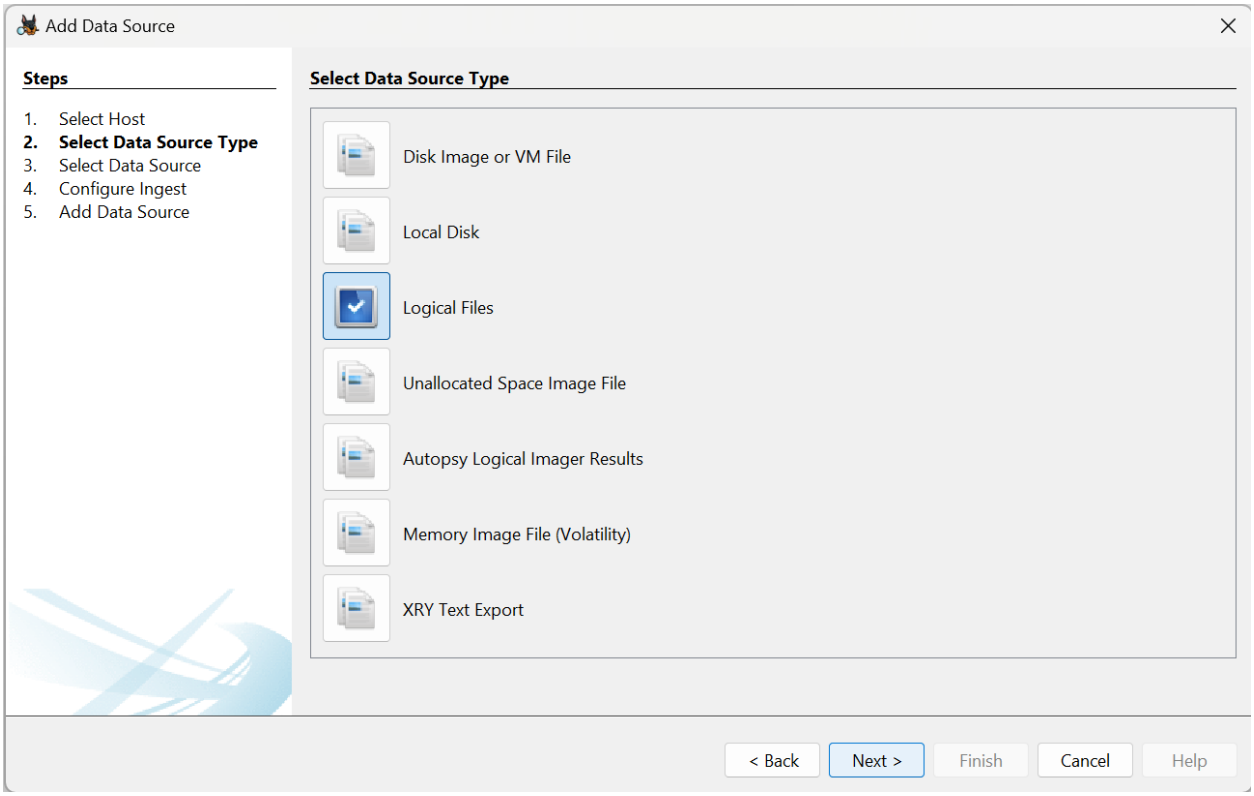
EXAMINING FILE-HASH:

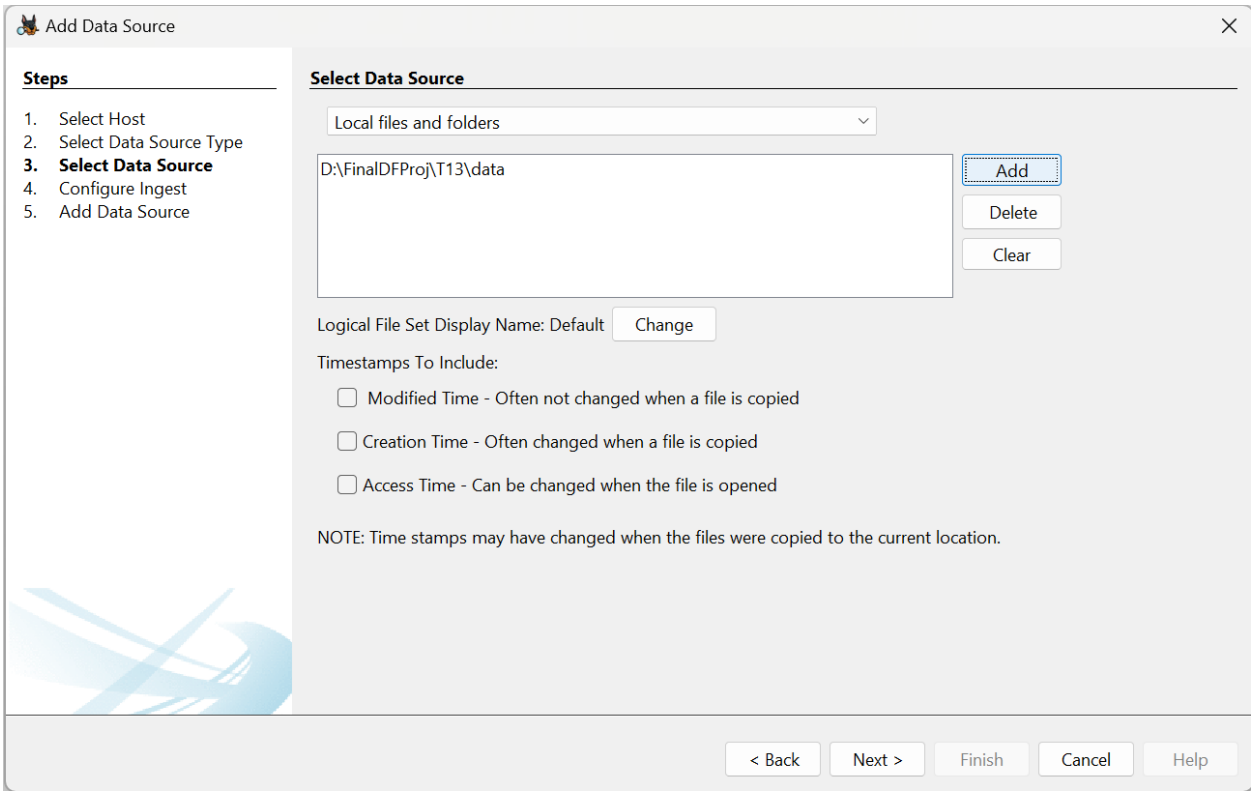


RUNNING AUTOPSY:

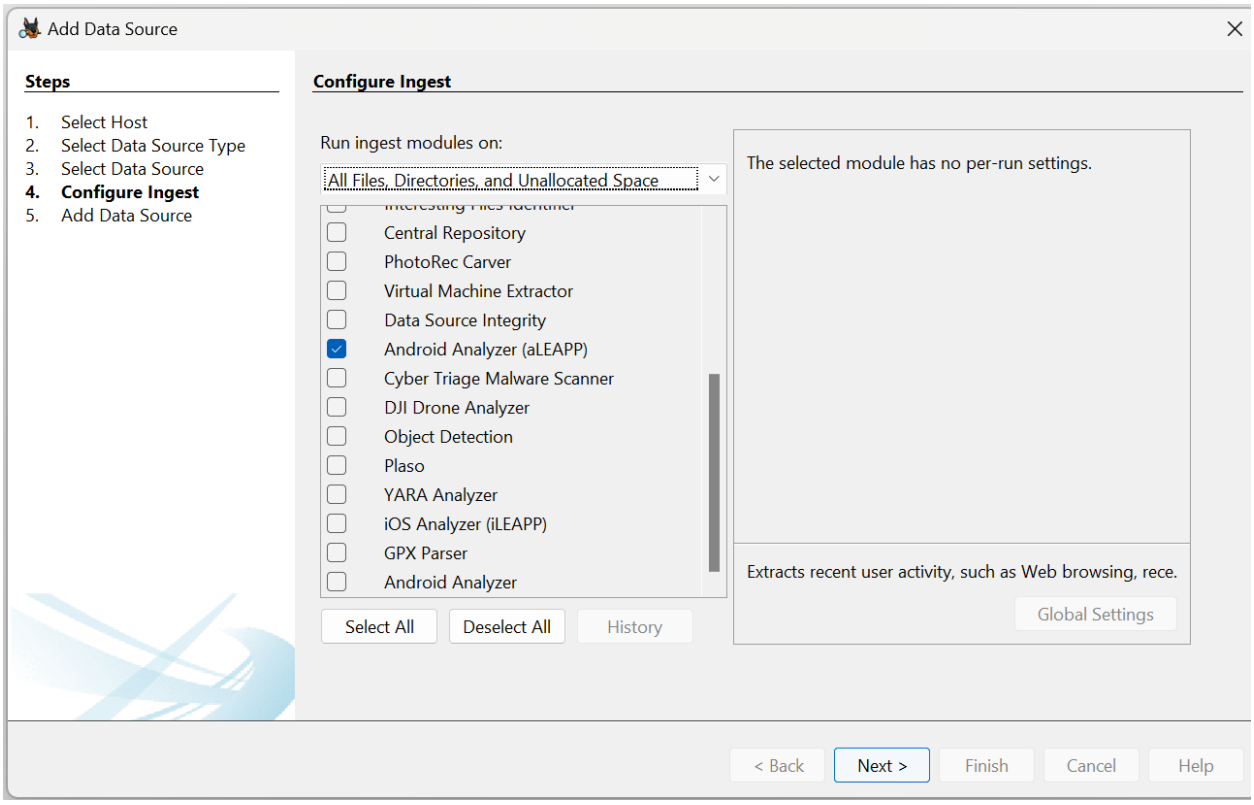



New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: Android2
Examiner
Name: Abdullah
Phone: 031030657860
Email: abdullahamqbool08@gmail.com
Notes:
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

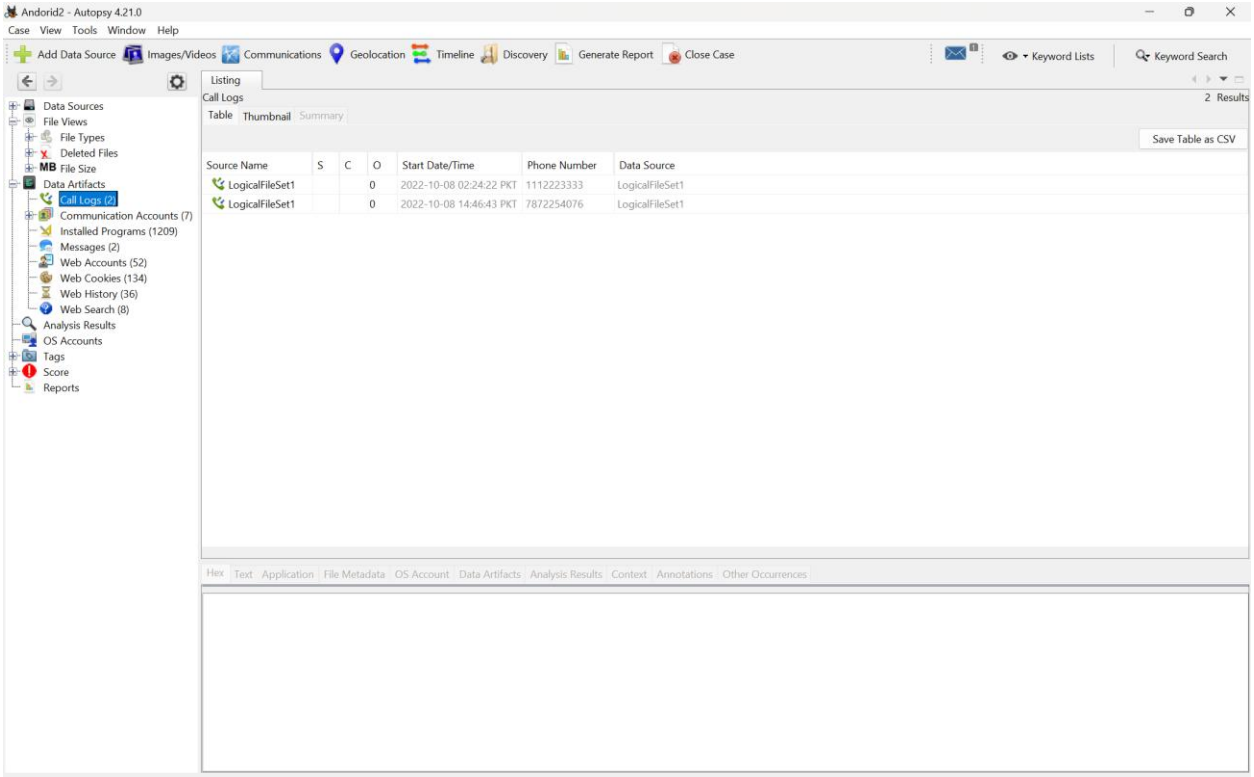

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
Memory Image File (Volatility)
XRY Text Export
< Back
Next >
Finish
Cancel
Help



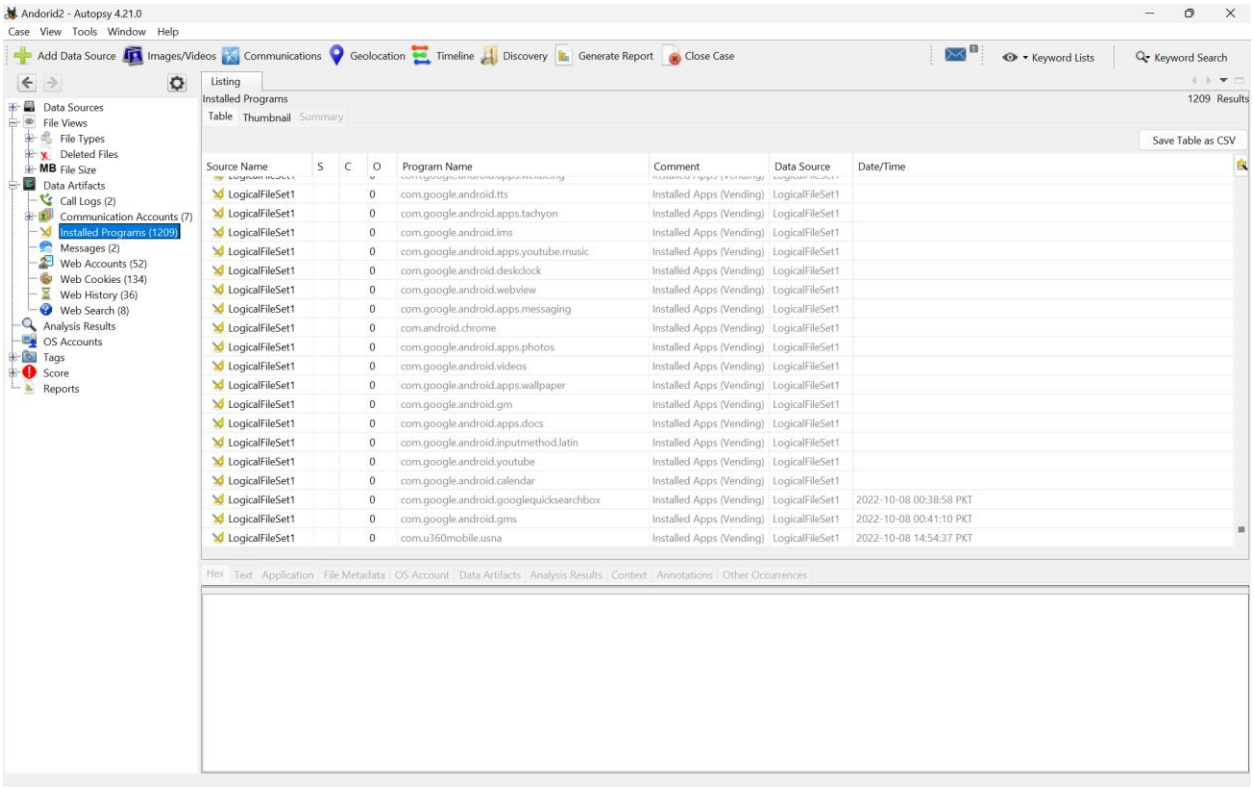
CHECKBOXING:



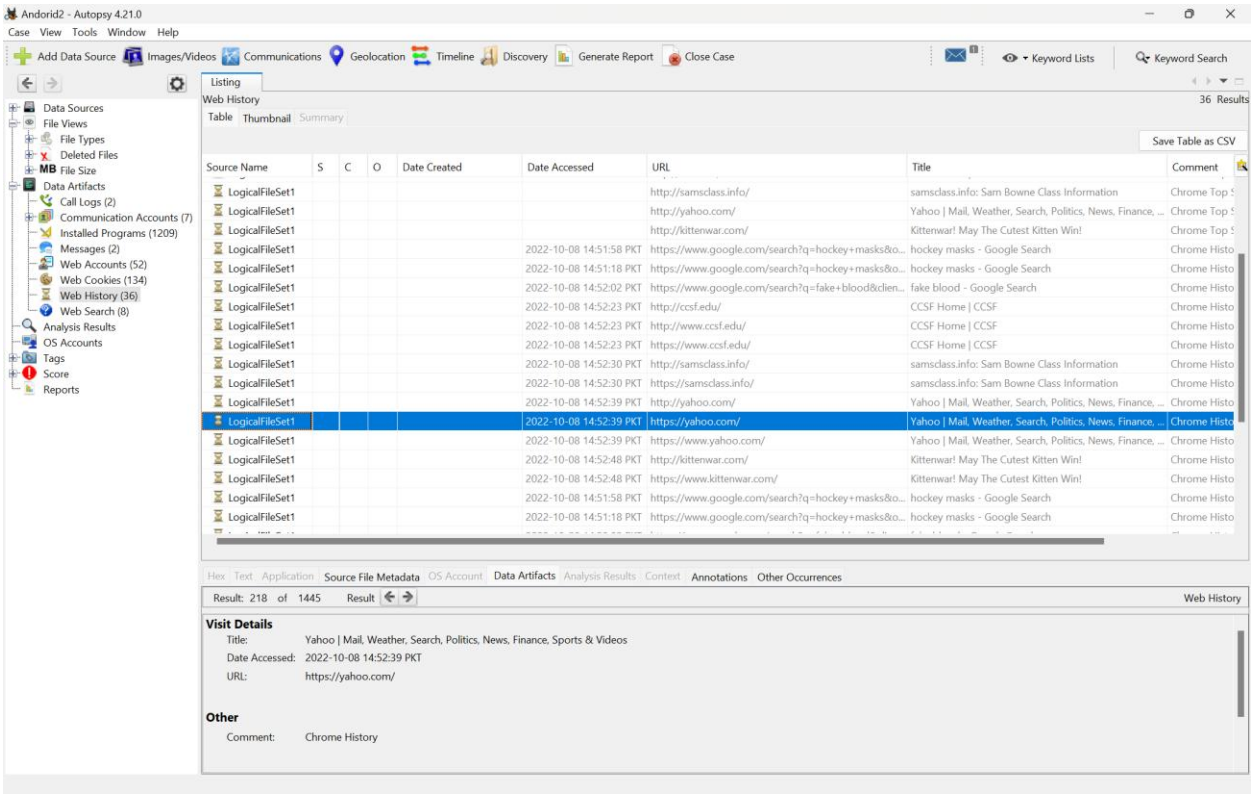
EXAMINING OF ARTIFACT:



LATEST PROGRAM INSTALLED FLAG:

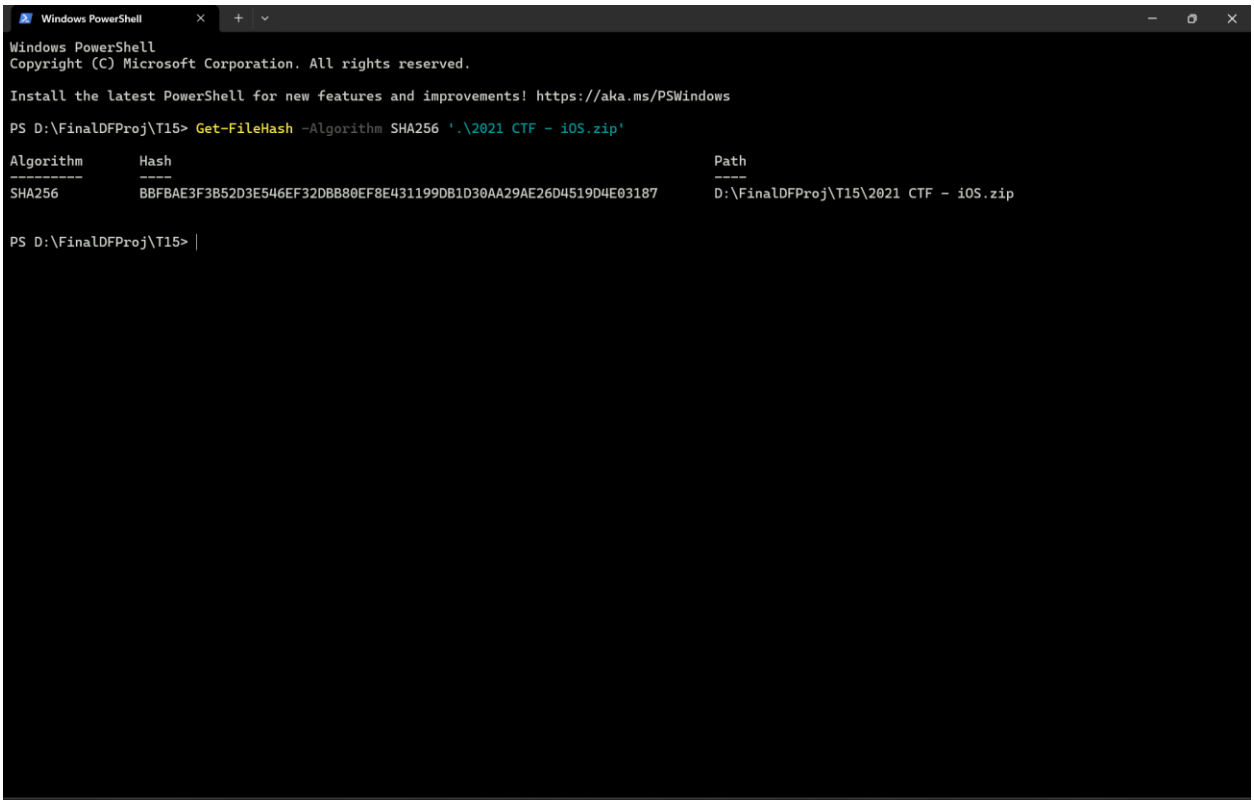


SITE VISTED AT SPECIFIC TIME FLAG:



15. iPhone Analysis with Autopsy

EXAMINING FILE HASH:

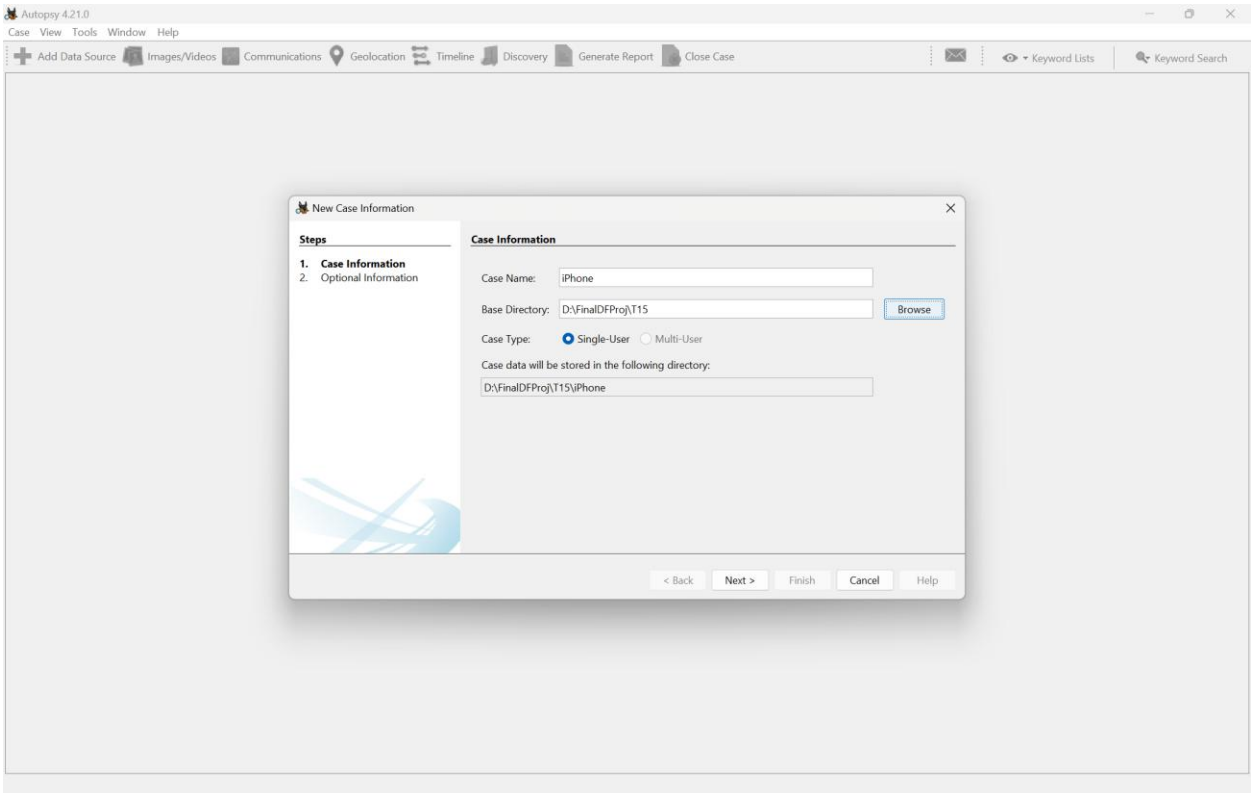


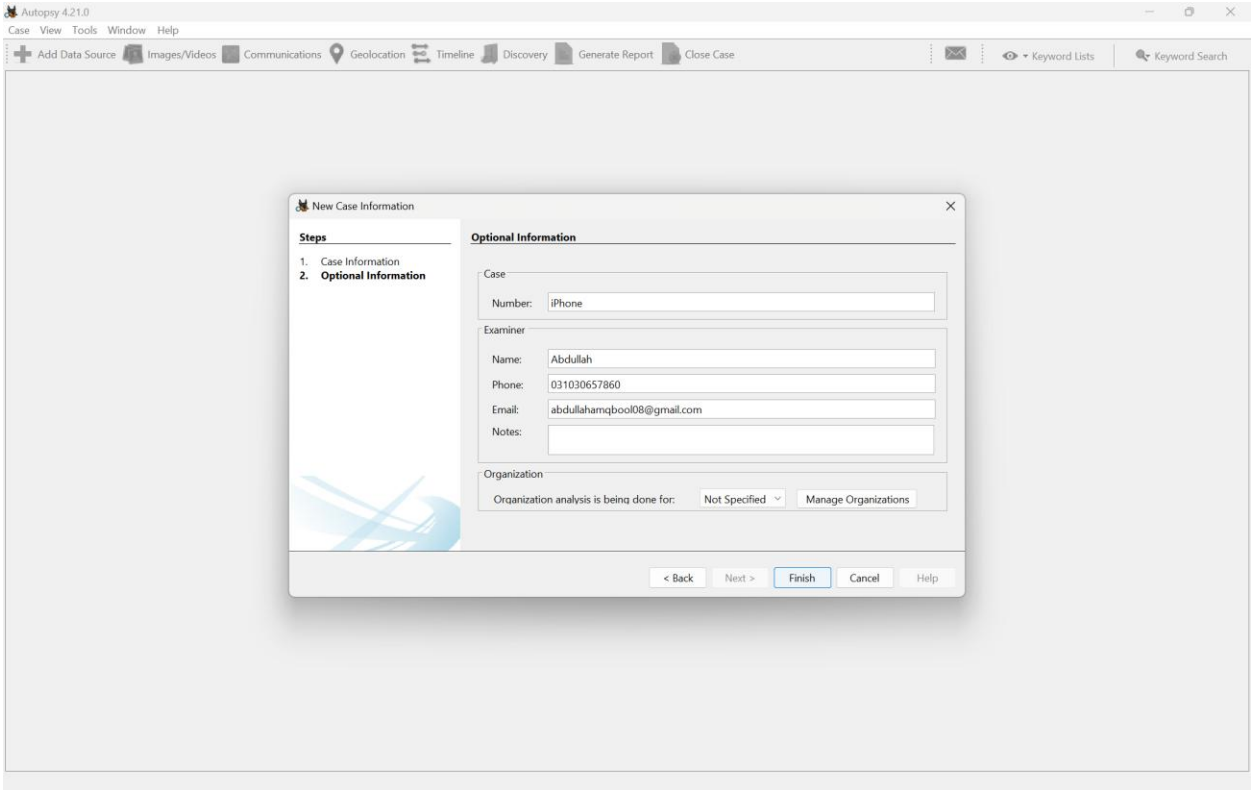
Takeout.zip	350,764,300	2022-07-21 16:52:46Z	8c1f235410a2475d71ac8090de9c4f8e8855fe8aaca3f8706a353dd6184d4d59d	106ef04621c074ce35c259c8407d1ff381df33fe2fcc0a4849406e15e0282f134
2020 CTF - Windows Memory.zip	1,309,342,281	2022-07-21 16:54:15Z	8ba868f49bd33970a1cc6d7144a63f8336d83bf57bfddce3ba34a771a7d75955	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	67211e1aebd876a677a1298e5b08746790b22c83a3ed6605308276aab94b3c2c	e10e3d8f7367314b43ed0bf9003b0422fdf19dd27313ec879b36b88b11848958
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	a84314a87fcf83657fcca58b6b03947f39f049b20b42f0bfeee89adae06b3245	512693825fb9adce798de65c6d7f495130a397f33aa811d3cc1f720dd84e1be4
2021 CTF - iOS.zip	5,788,946,761	2022-07-22 01:12:46Z	bbfbae3f3b52d3e546ef32dbb80ef8e431199db1d30aa29ae26d4519d4e03187	8e3d1e4859ed6b8243b37eccb37799f7978c47d0ebba7ace83e7200e31f3c93d
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	3196b438c82fd9b021acc0704983944aa67e55fc86c8f9cfcfc28ea3b9415774	b8e9a1b003b41ec2a97f8243c78b509c4cf92e15e3a1013753f84fa40f69ce2d
2022 CTF - Takeout.zip	2,580,941	2022-07-22 01:36:48Z	800e0b74aeb407e1daae0176e17ccf6871d7b645c4ccc3c2e641d9373131999c	90ff05852441728l7a48d11343946bf00cb293a5db4df43d6d1973690aa67b4c
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

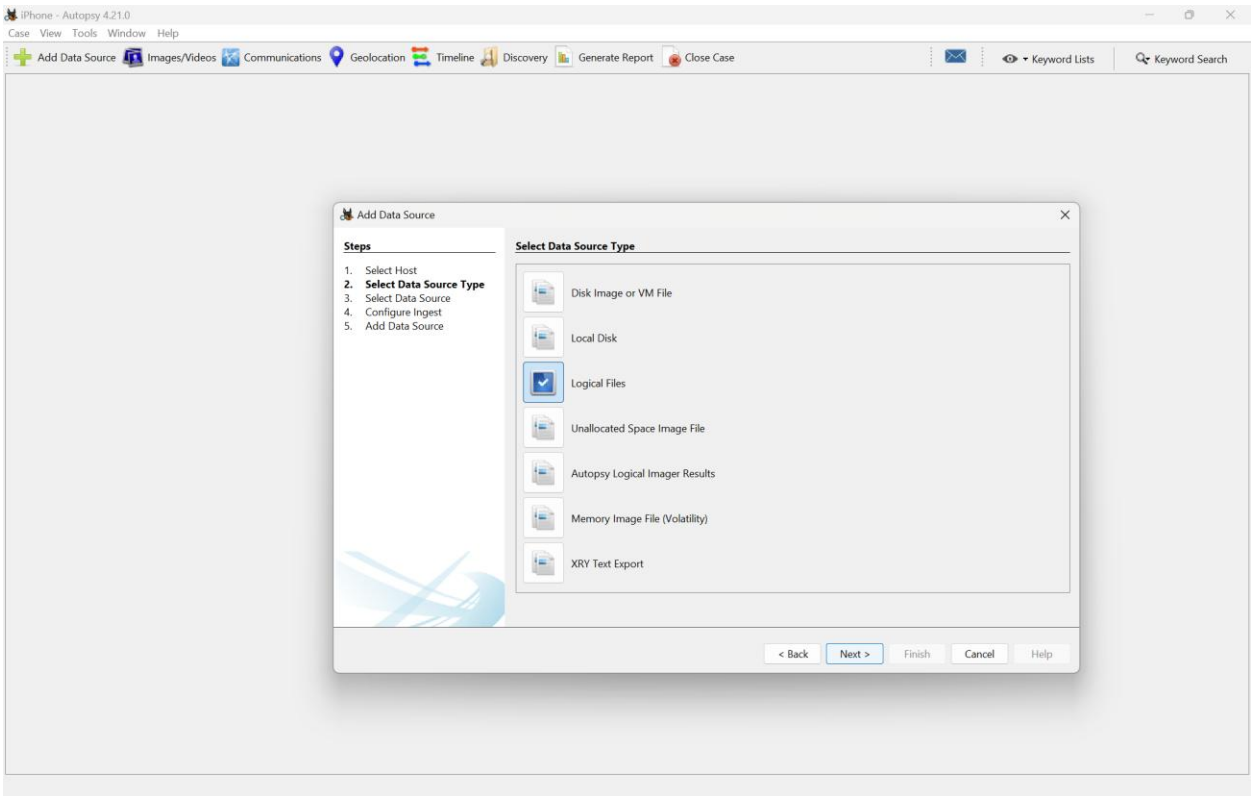
Thanks to Magnet Forensics for providing these CTF images. Full documentation is under development.

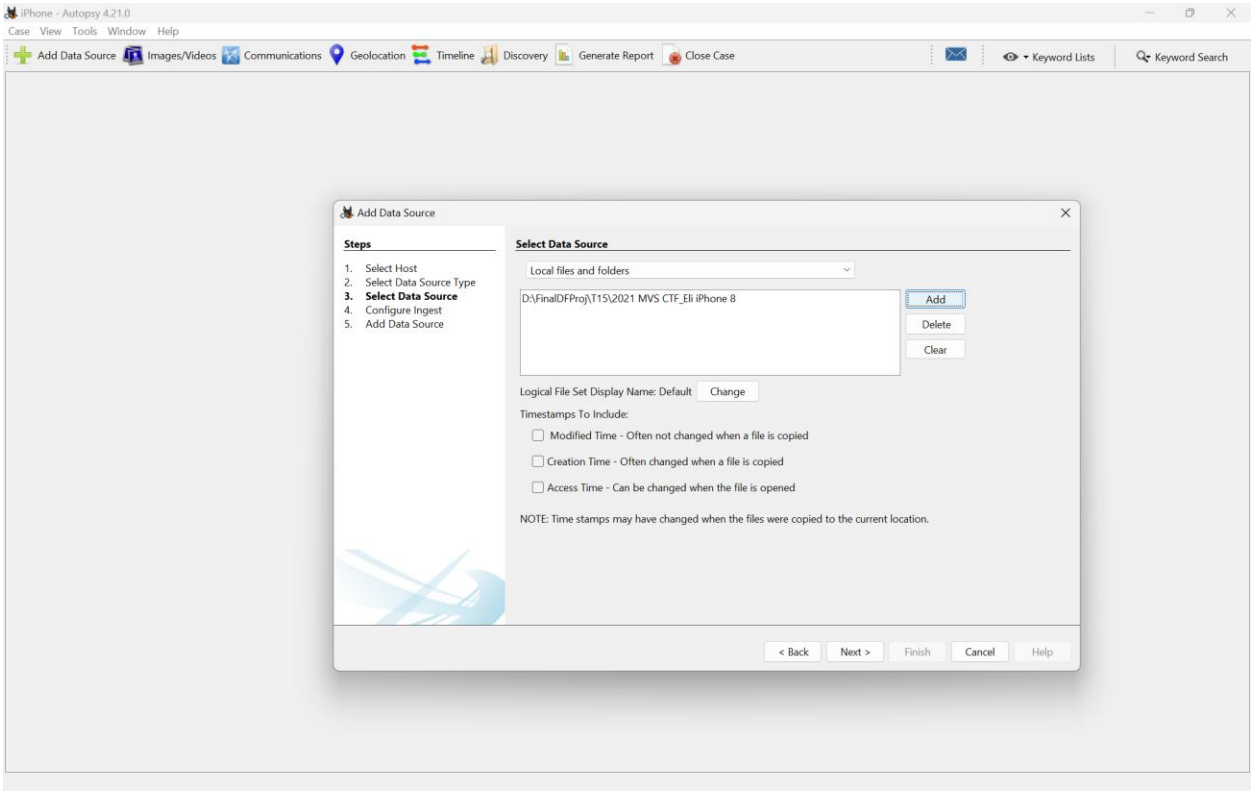
Name	Description

IMORTING EVIDENCE FILE:

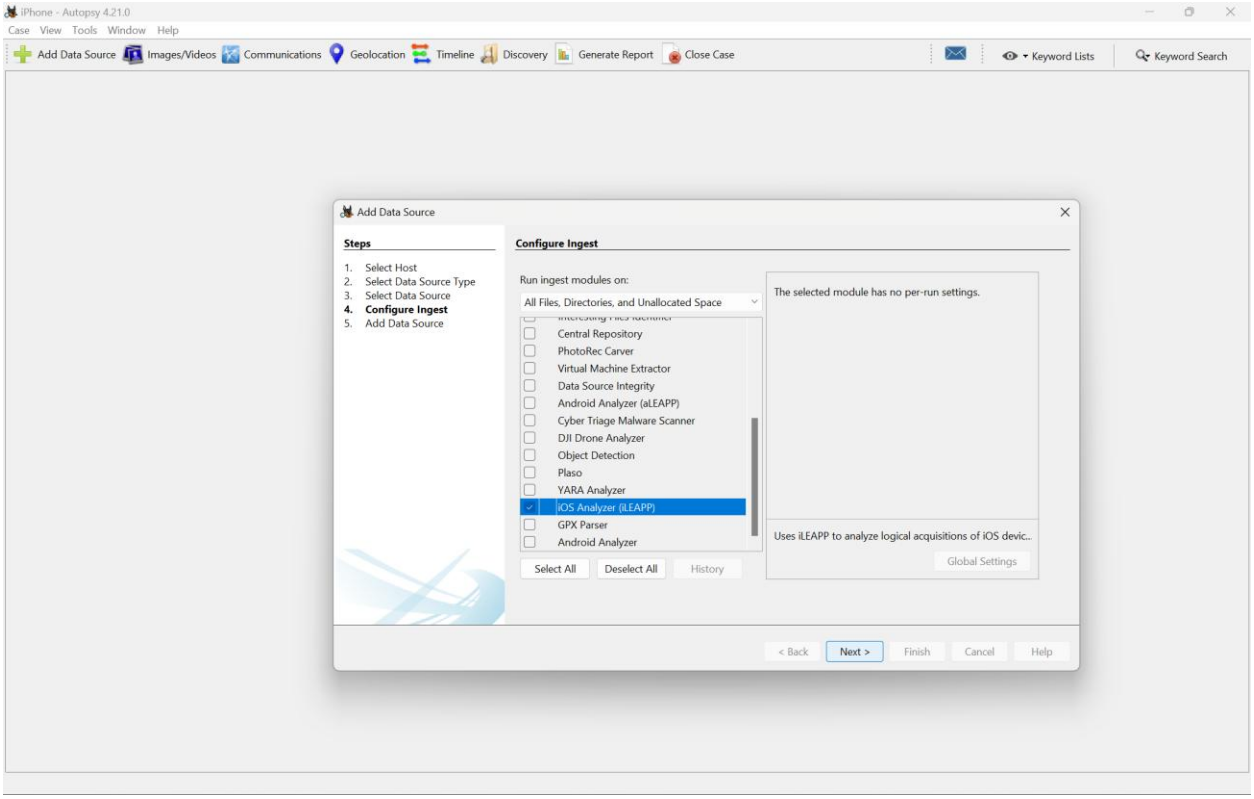




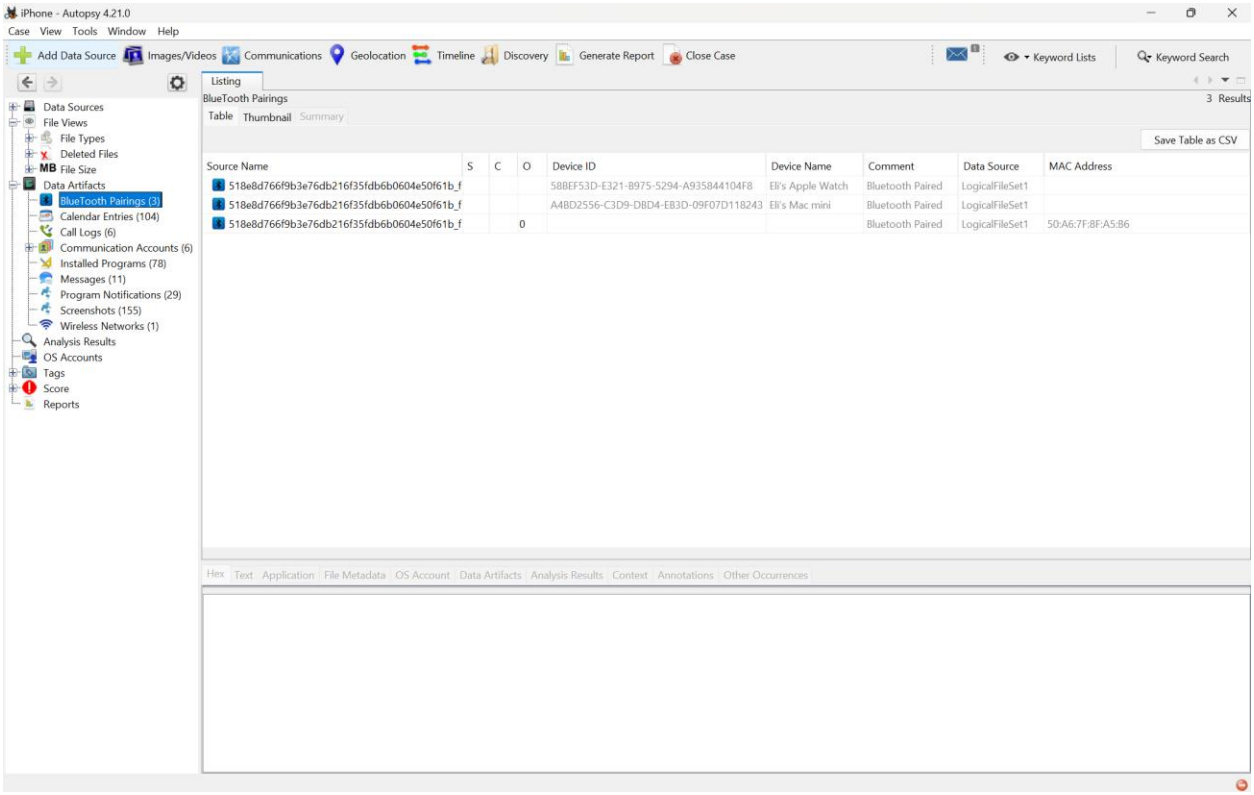

iPhone - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source 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
Next >
Finish
Cancel
Help


iPhone - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
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
Local files and folders
D:\FinalDFProj\T15\2021 MVS CTF_Eli iPhone 8
Add
Delete
Clear
Logical File Set Display Name: Default
Change
Timestamps To Include:
Modified Time - Often not changed when a file is copied
Creation Time - Often changed when a file is copied
Access Time - Can be changed when the file is opened
NOTE: Time stamps may have changed when the files were copied to the current location.
< Back
Next >
Finish
Cancel
Help

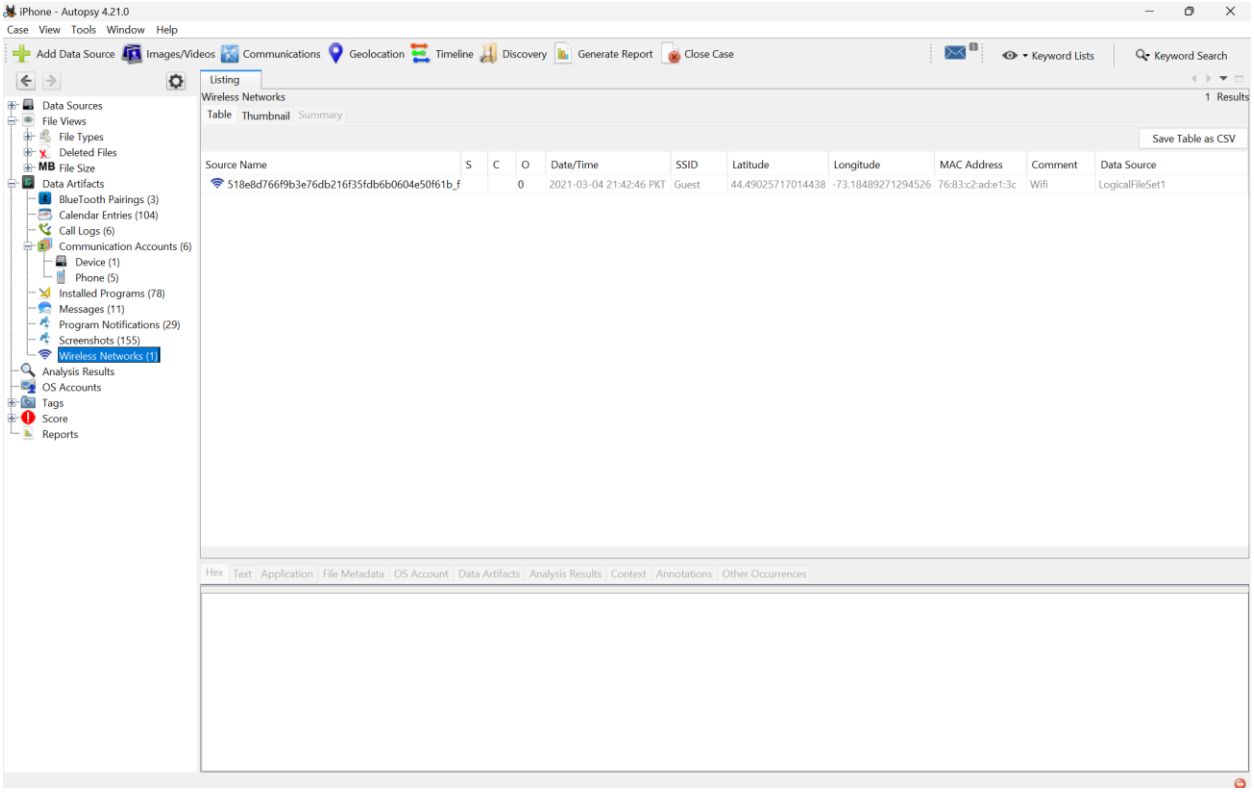
CHECKBOXING:



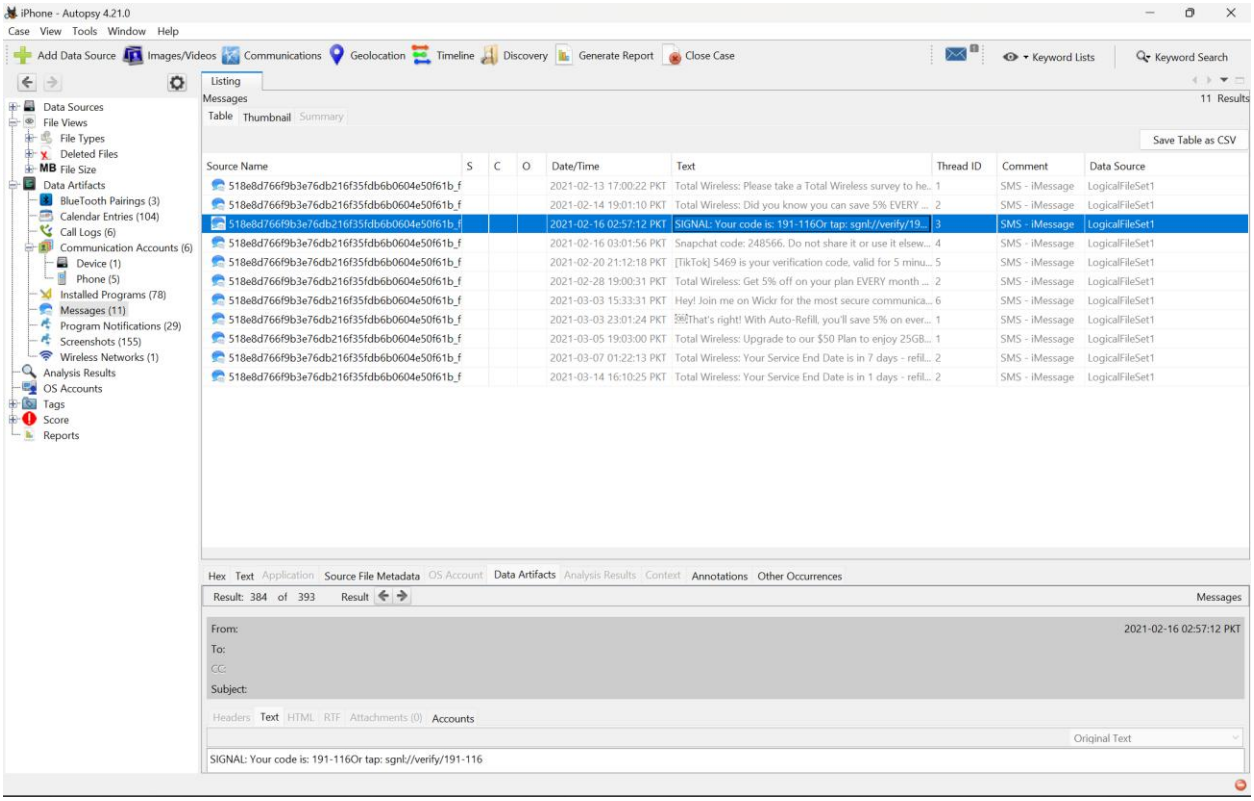
PHONE NUMBER FLAG:



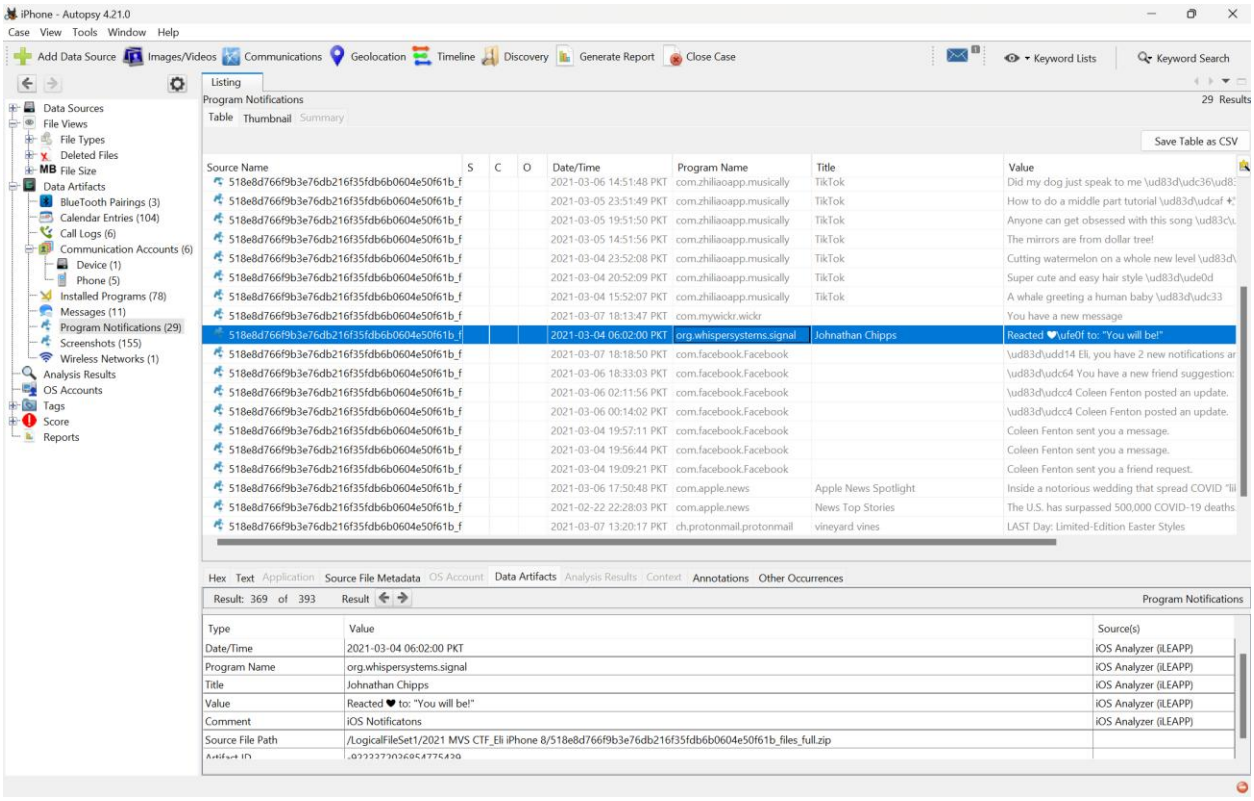
LATITUDE FLAG:



SMS FLAG:

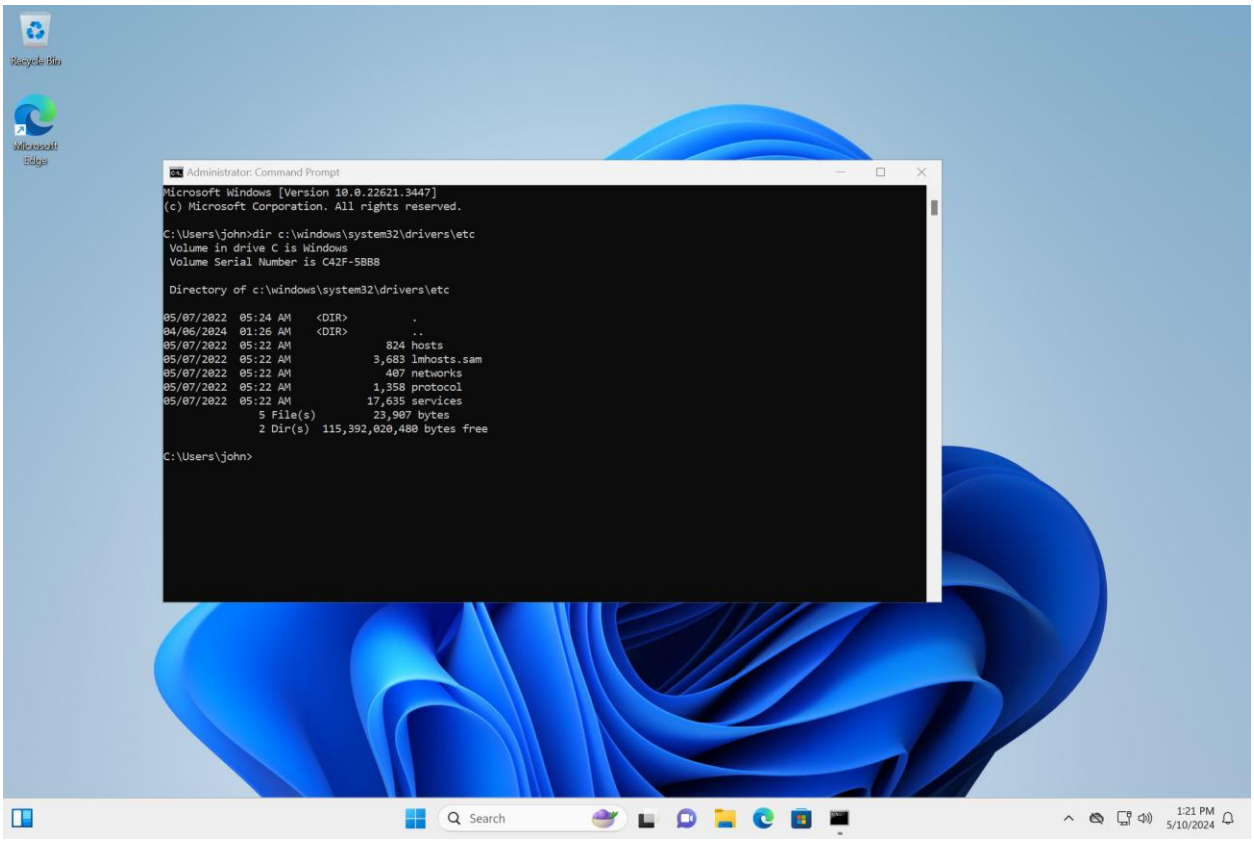


SIGNAL CONTACT:

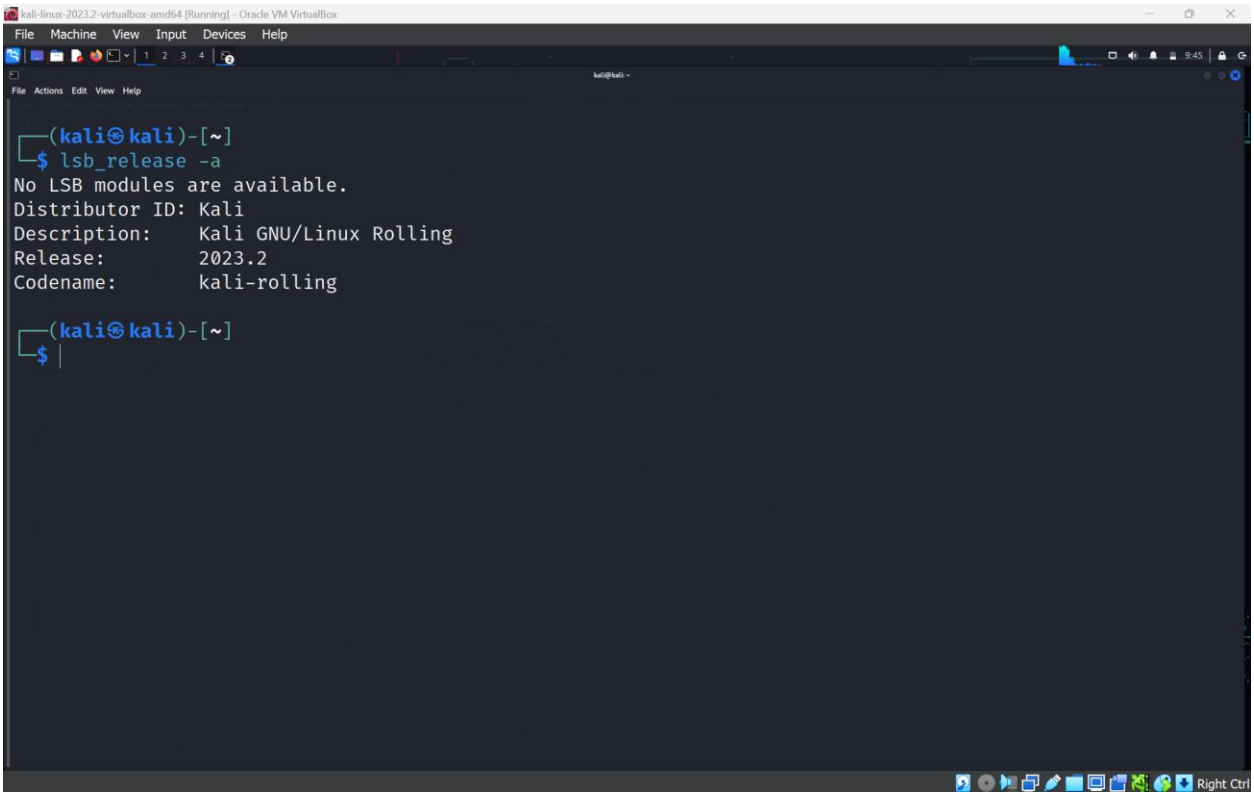


16.Windows and Linux Machines

WINDOWS FLAG:

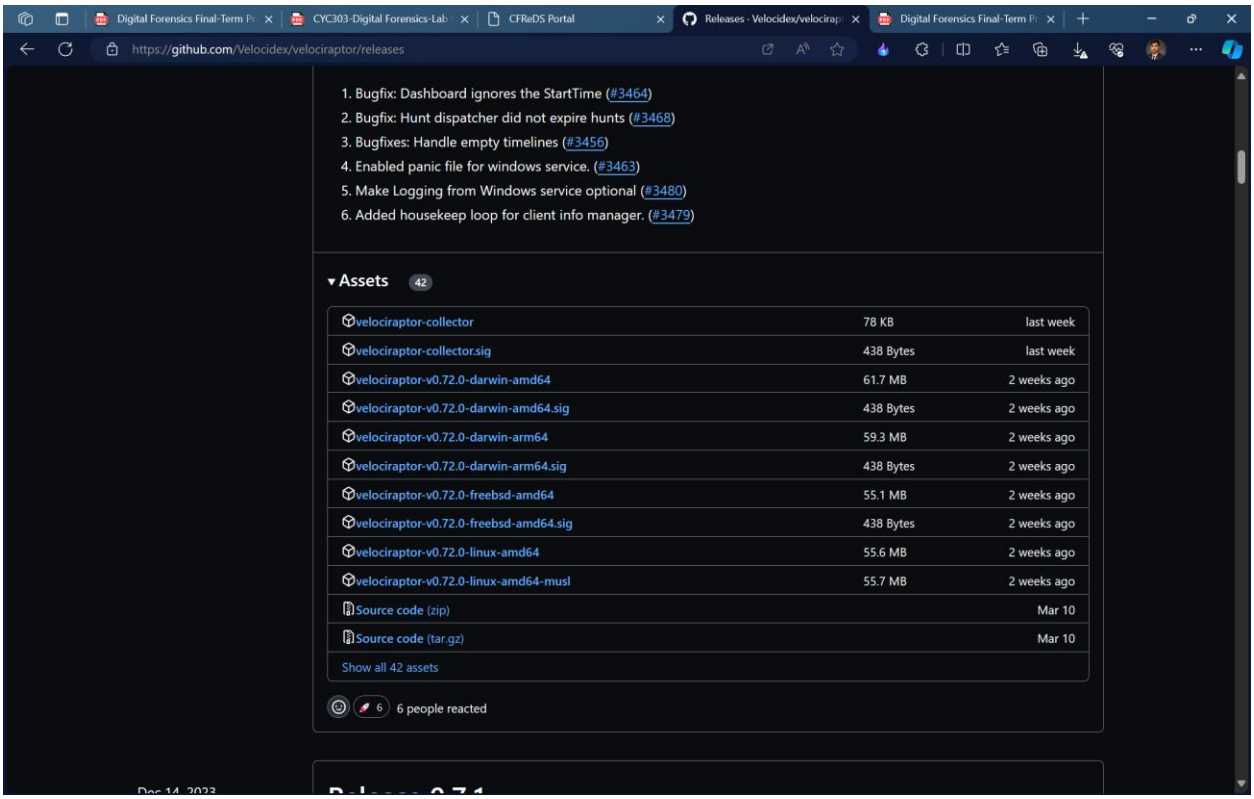


LINUX FLAG:

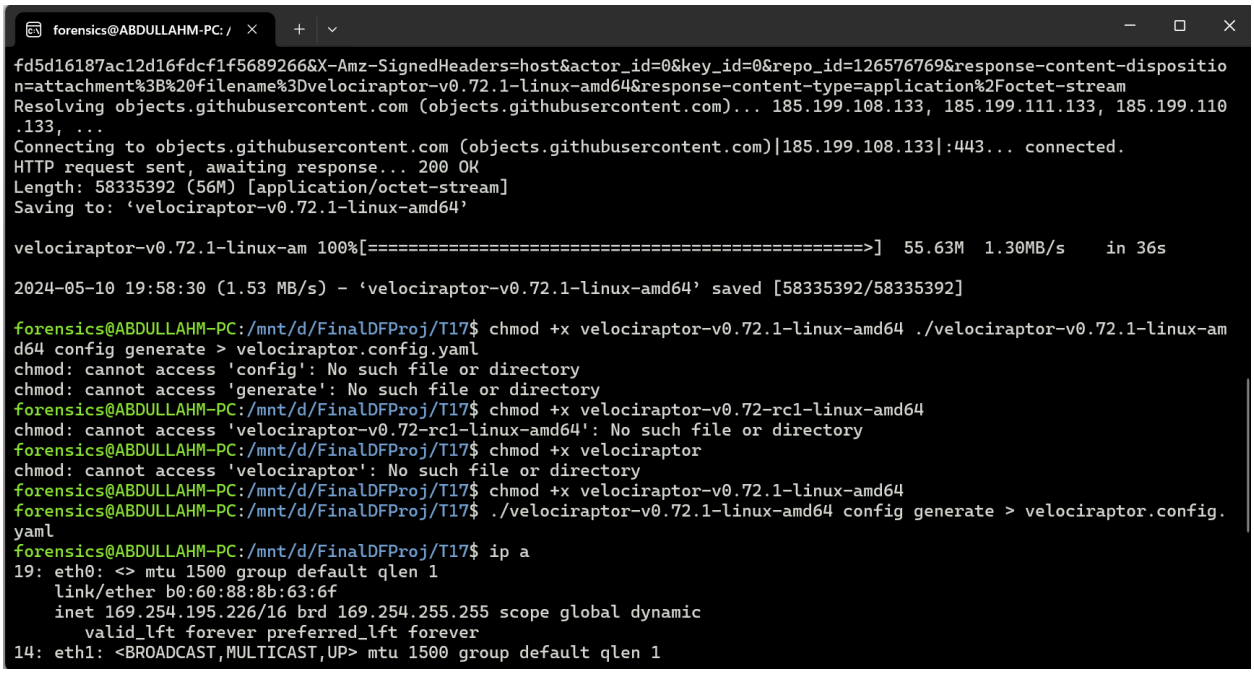

kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description: Kali GNU/Linux Rolling
Release: 2023.2
Codename: kali-rolling
(kali㉿kali)-[~]
$
Right Ctrl

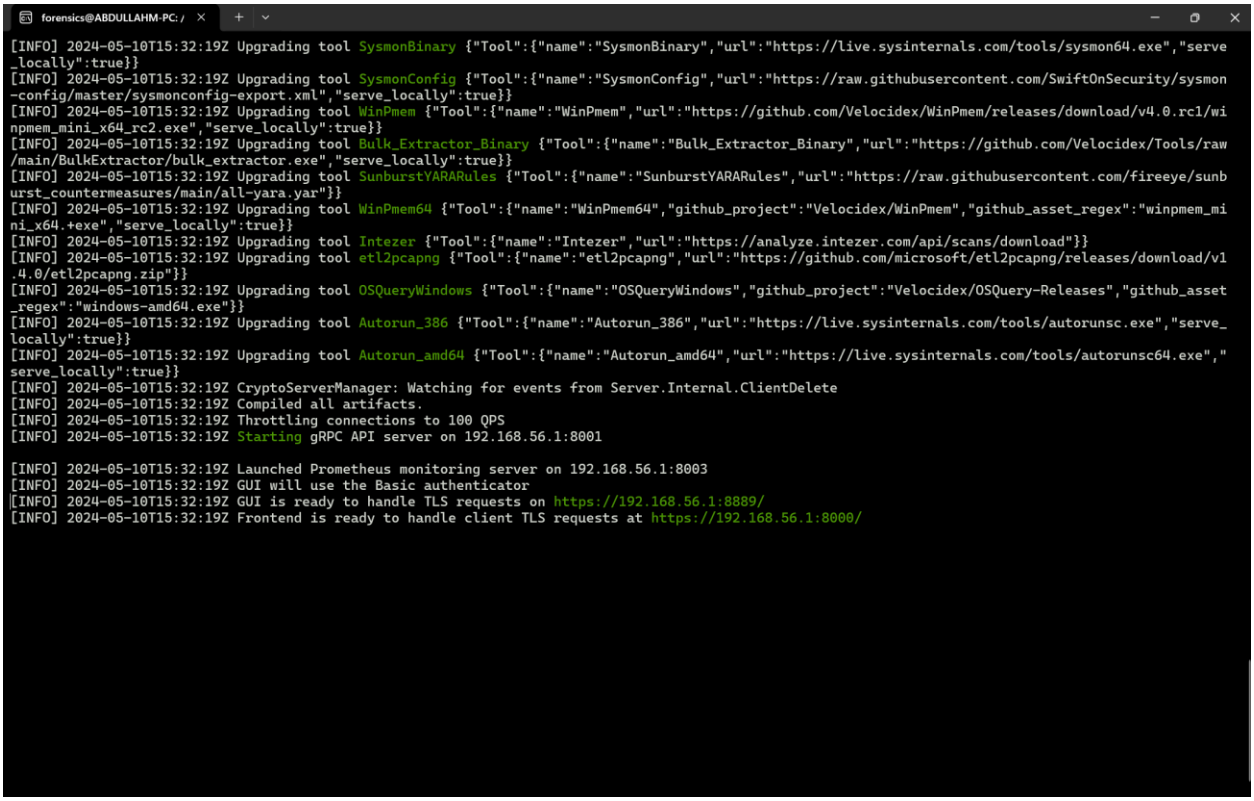
17.Velociraptor Server on Linux

FINDING THE LAST VERSION:

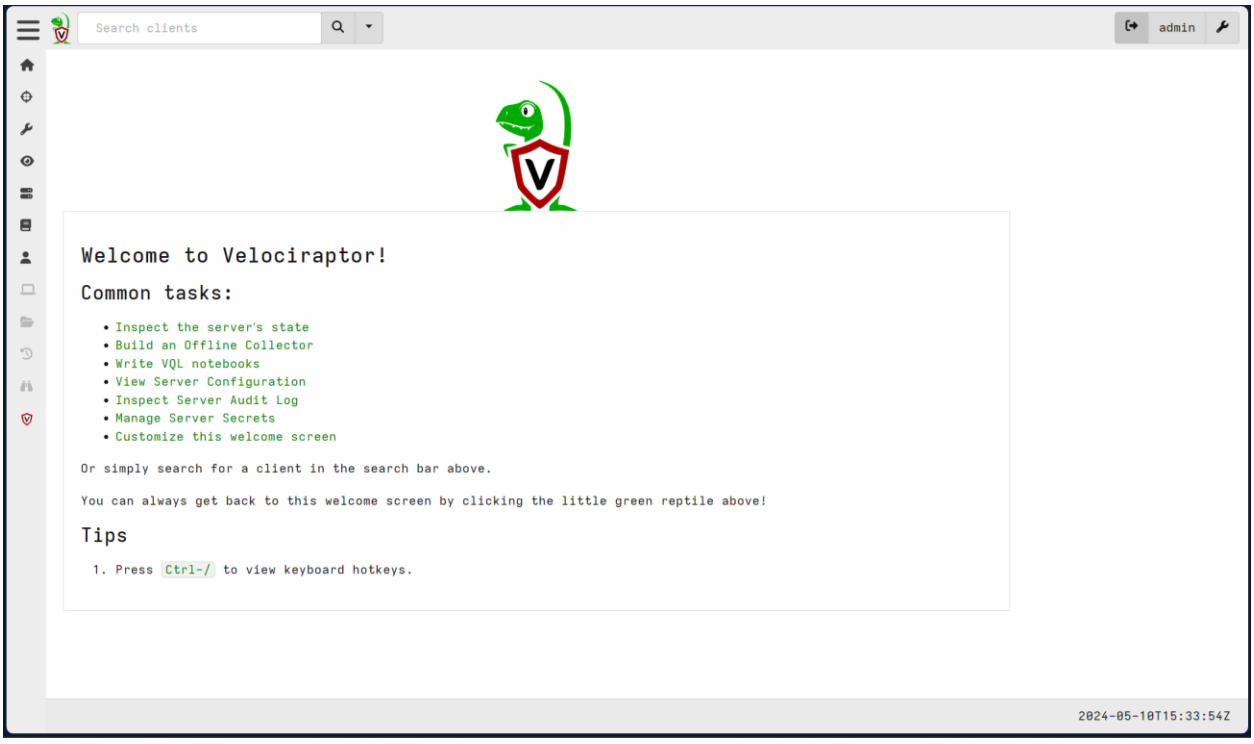


PREPARING THE SERVER:

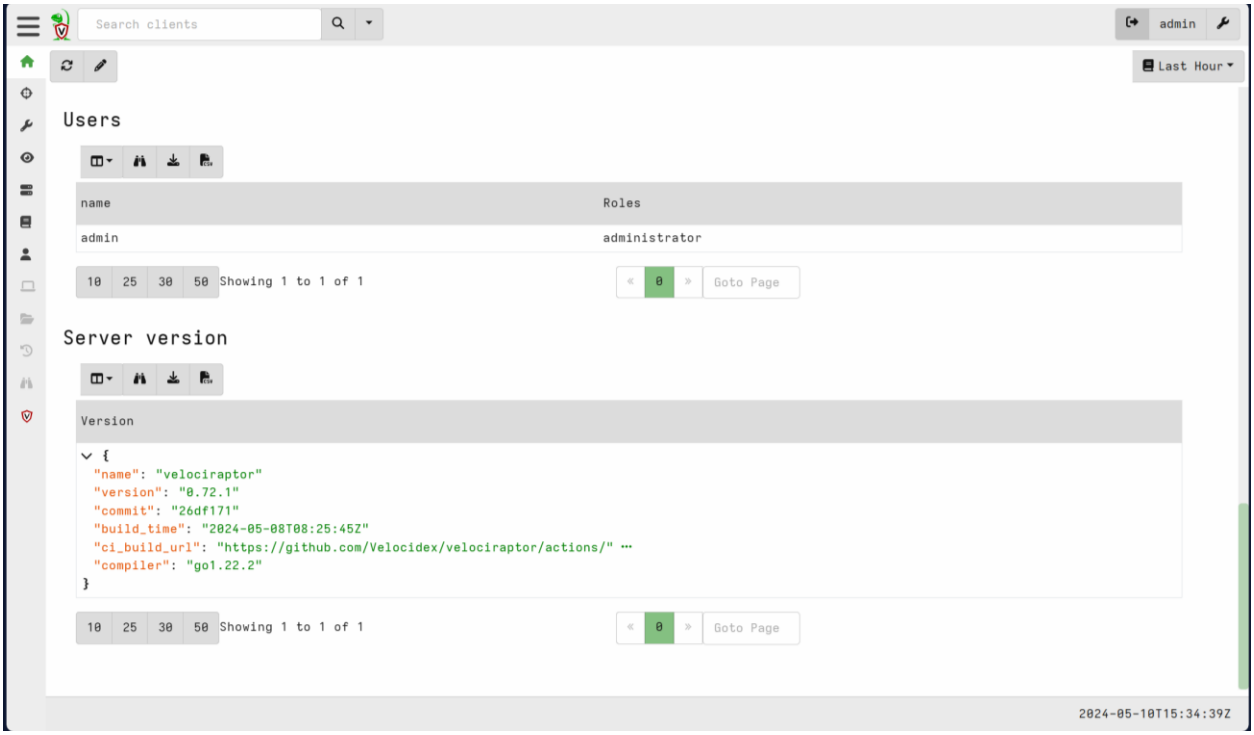




VIEWING THE GUI:

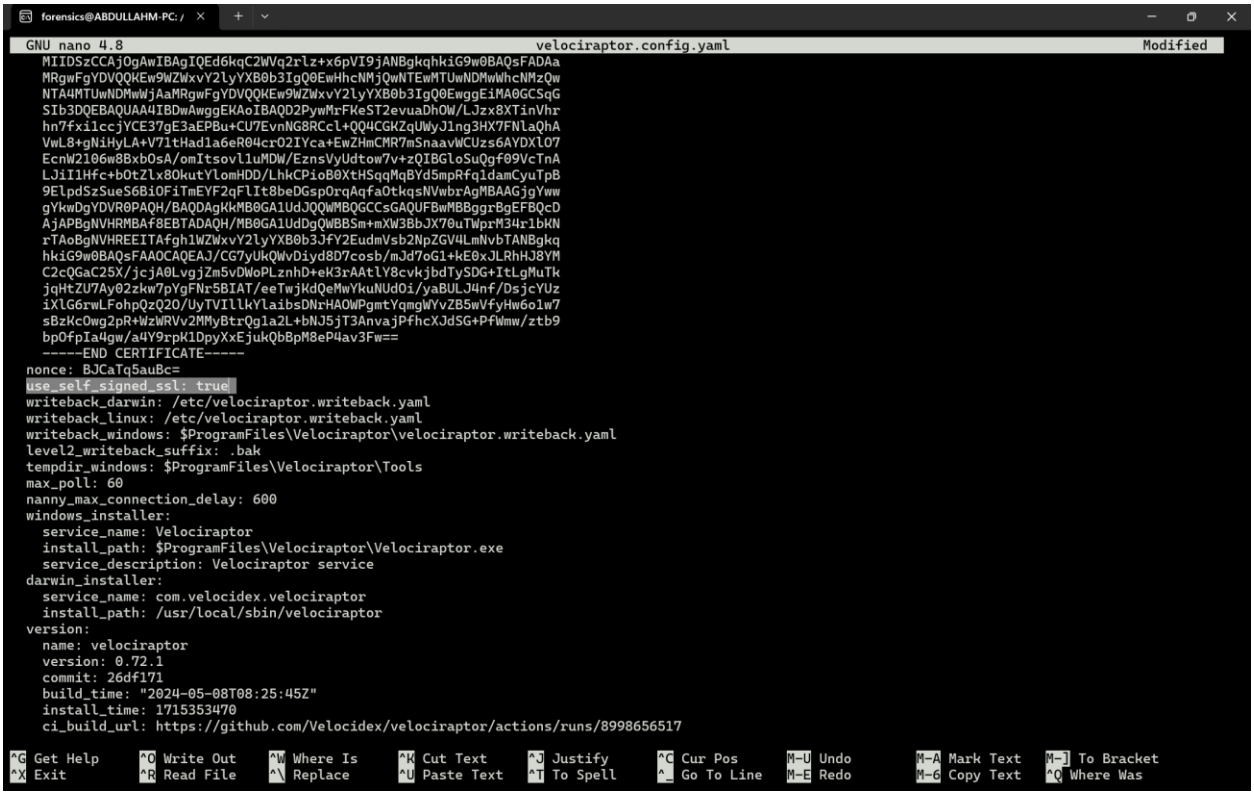


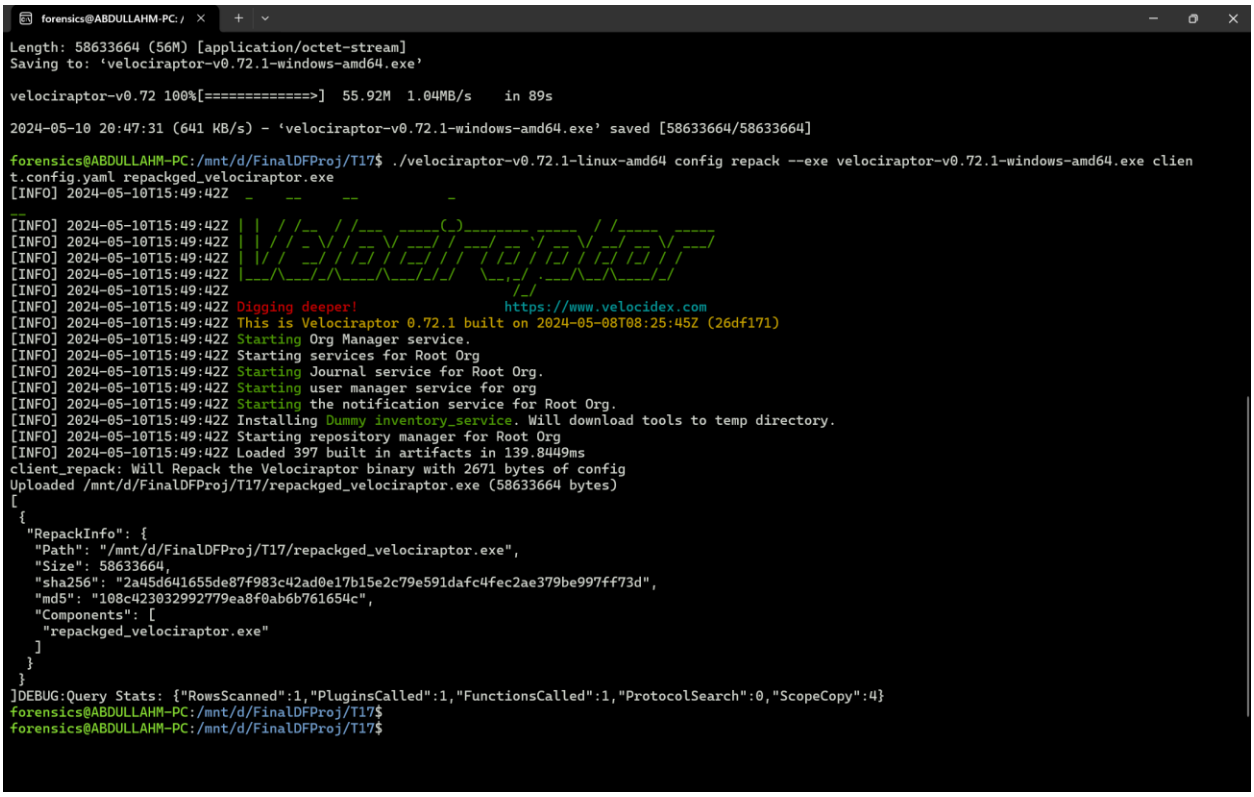
SERVER NAME:


Search clients
admin
Last Hour
Users
name
Roles
admin
administrator
10 25 30 50 Showing 1 to 1 of 1
0
Goto Page
Server version
Version
{
"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"
}
10 25 30 50 Showing 1 to 1 of 1
0
Goto Page
2024-05-10T15:34:39Z

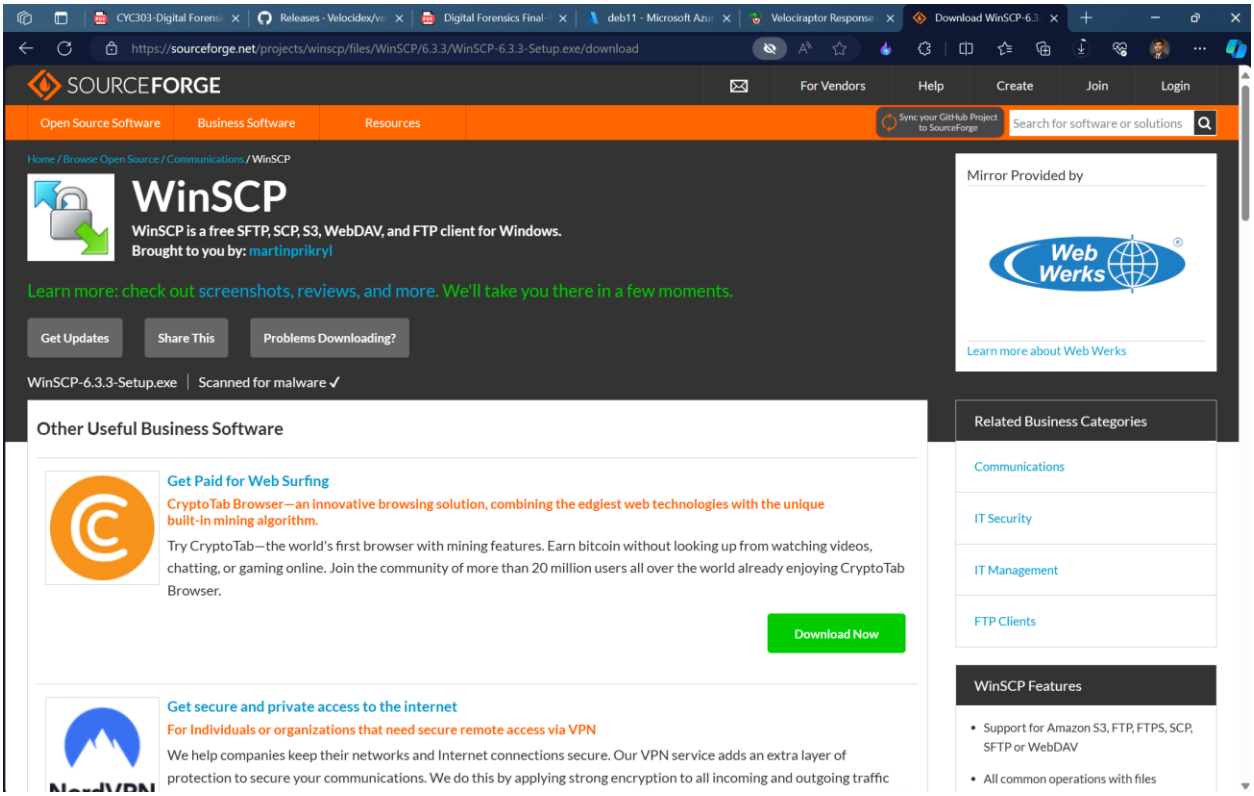
ADDING A WINDOWS CLIENT:

PREPARING A CLIENT CONFIG FILE:

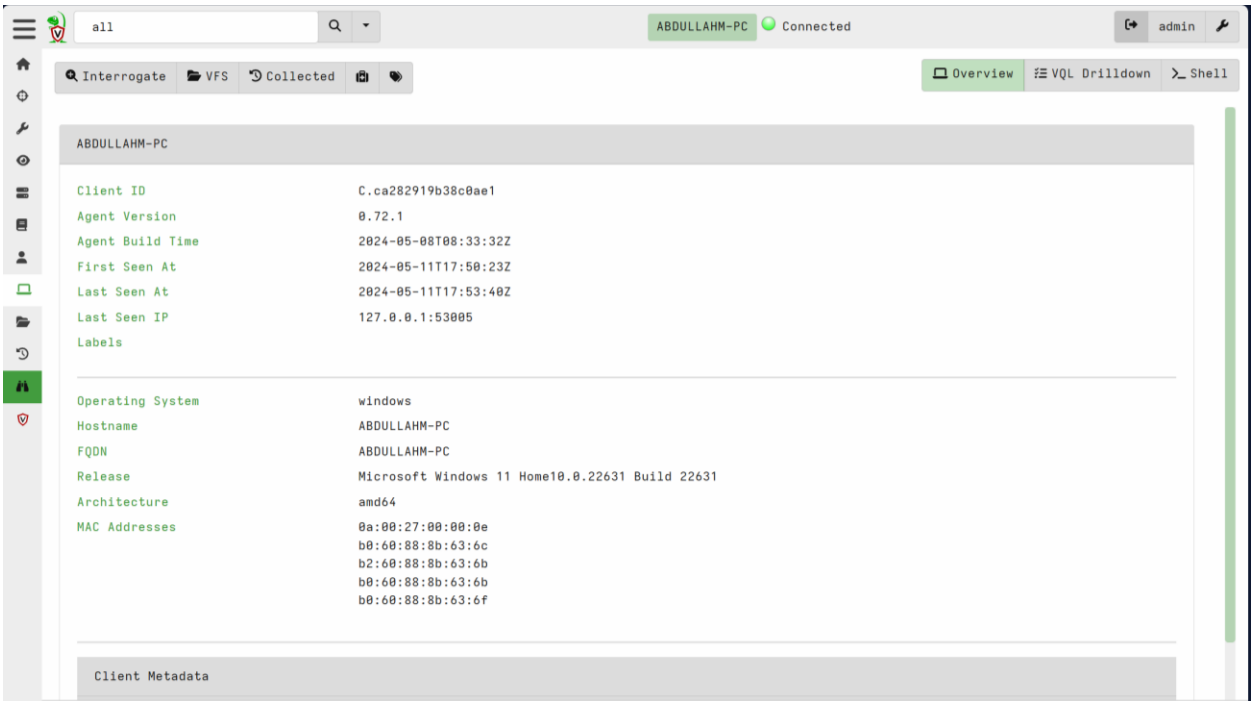




WINSCP DOWNLOAD:

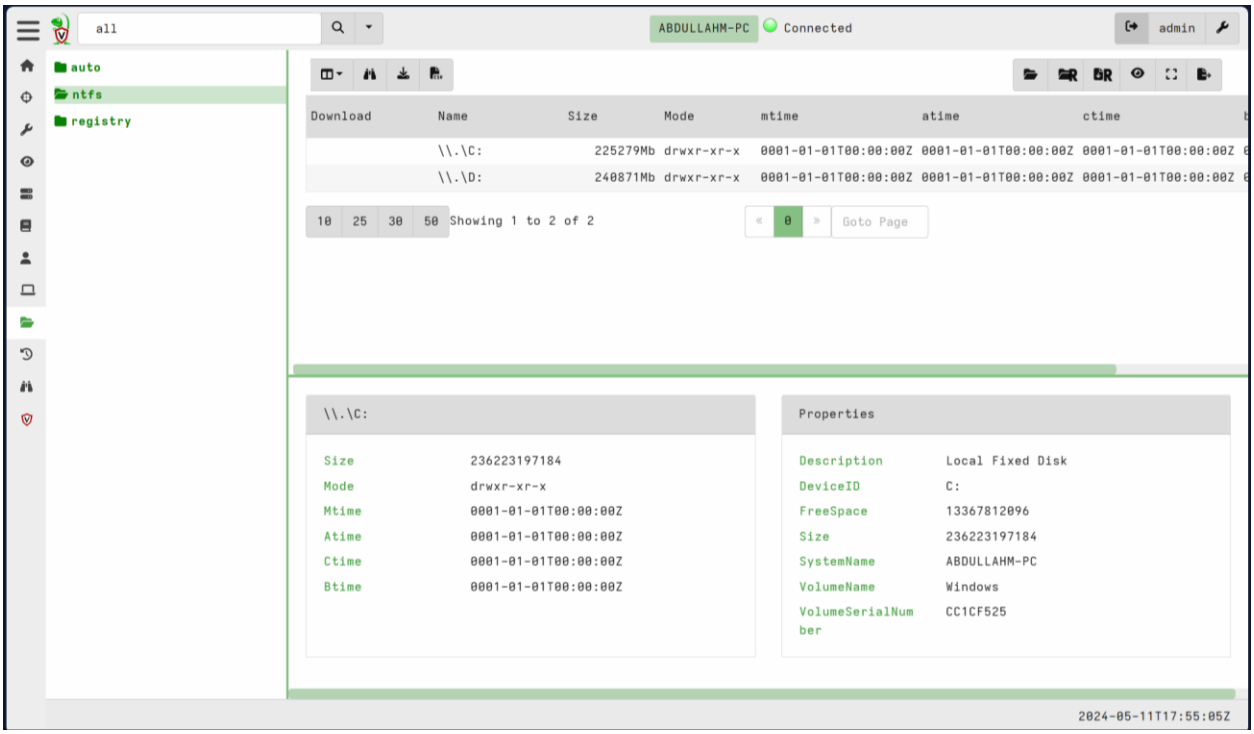


AGENT NAME:

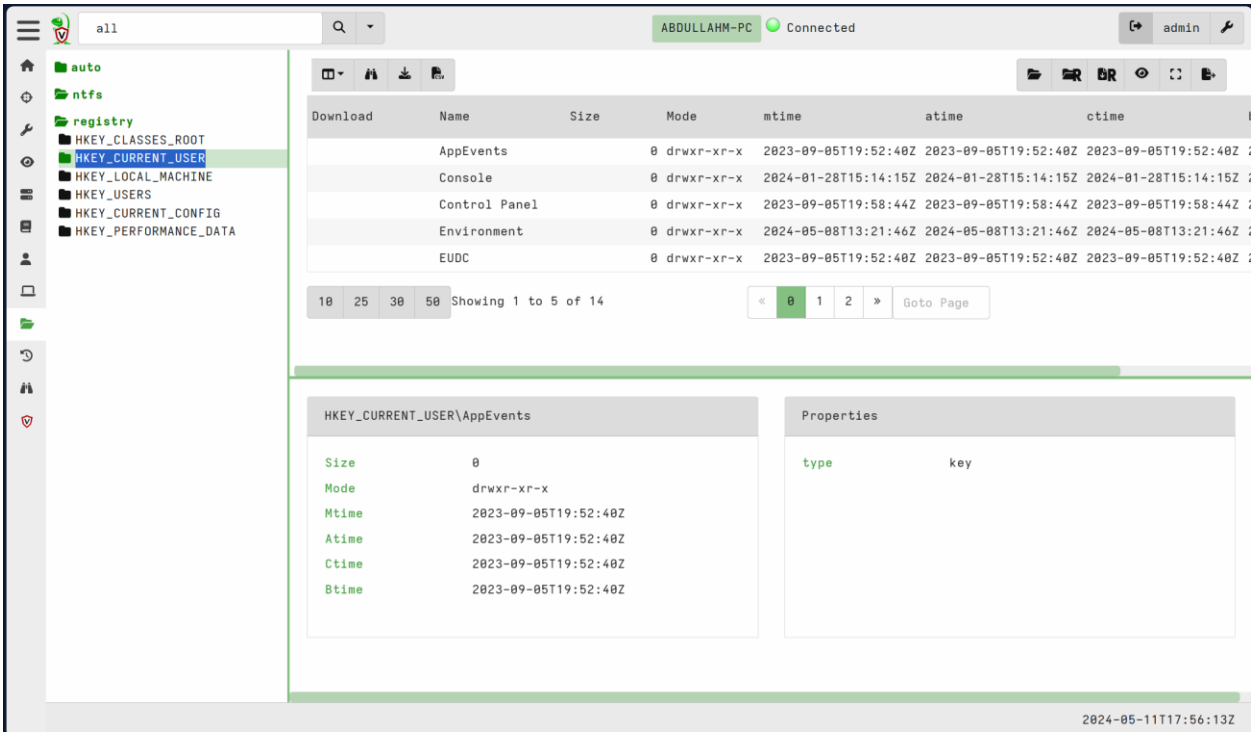


AGENT NAME:

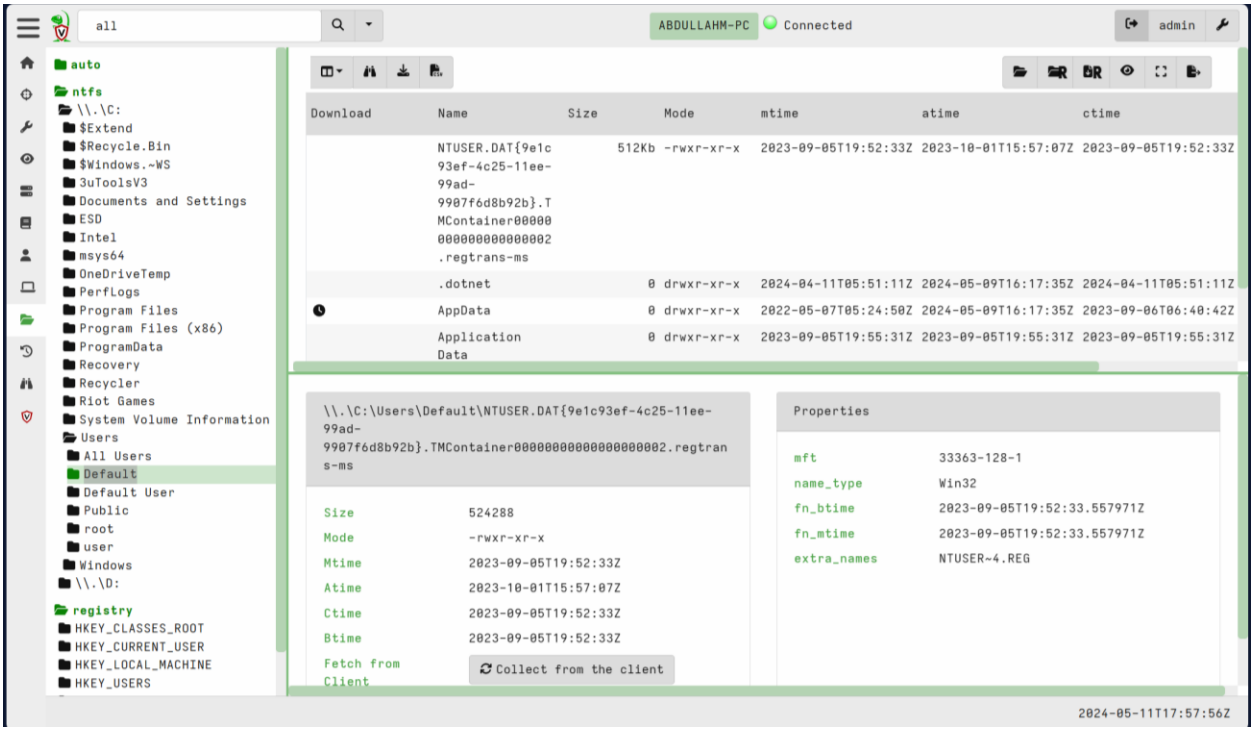
USING VRTUAL FILE SYSTEM:



REGISTRY INFORMATION:

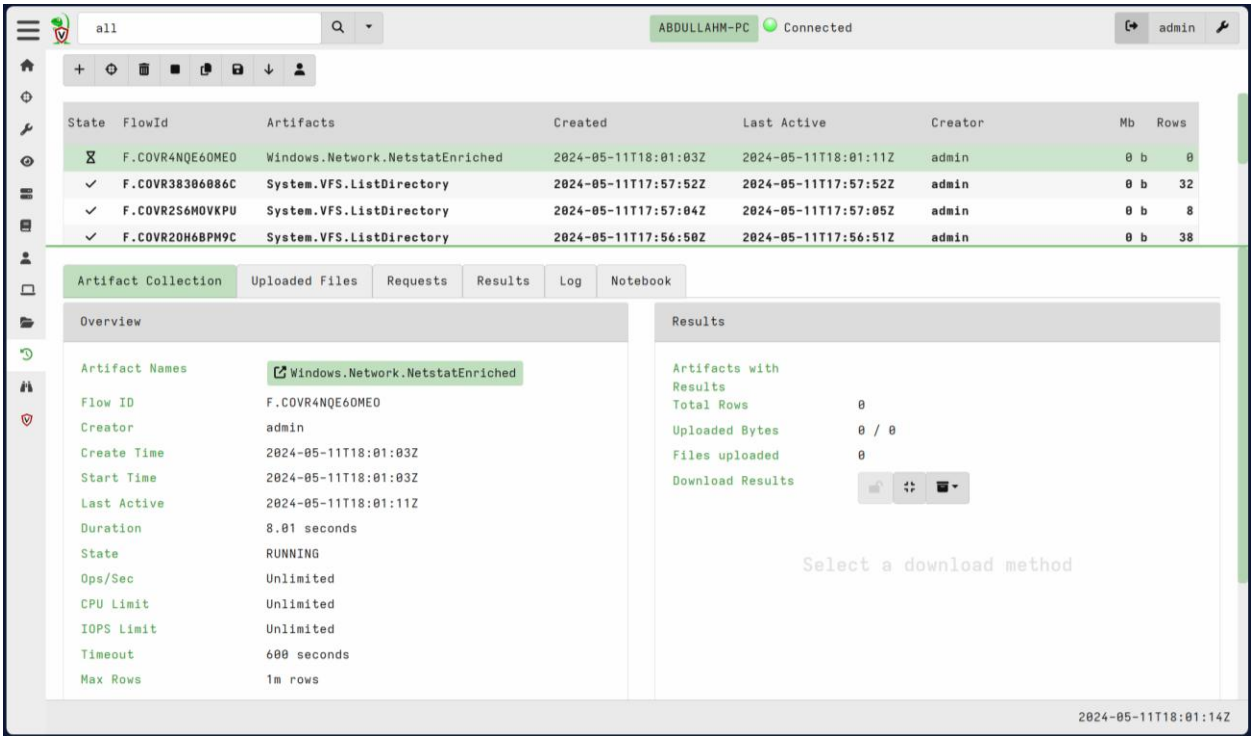


EXPLORING THE FILE SYSTEM:

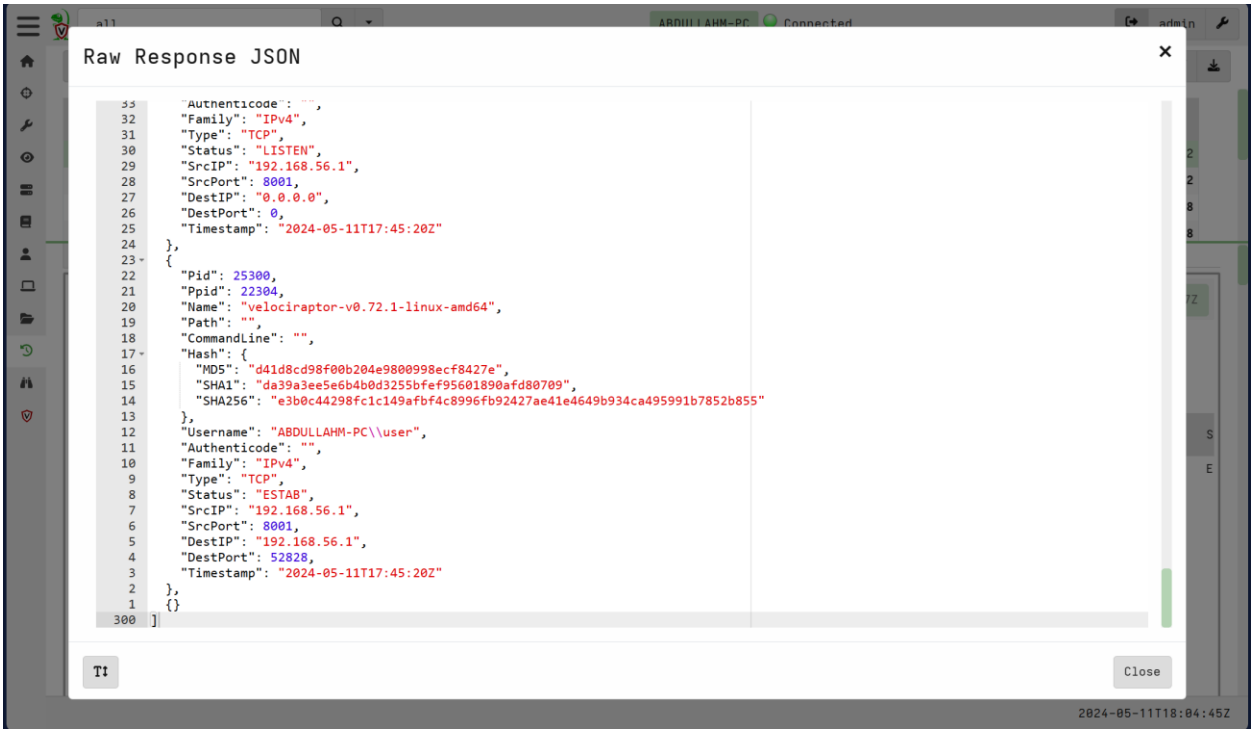


COLLECTING AN ARTIFICAT:

WINDOWS.NETWORK. NETSTATENRICHED:

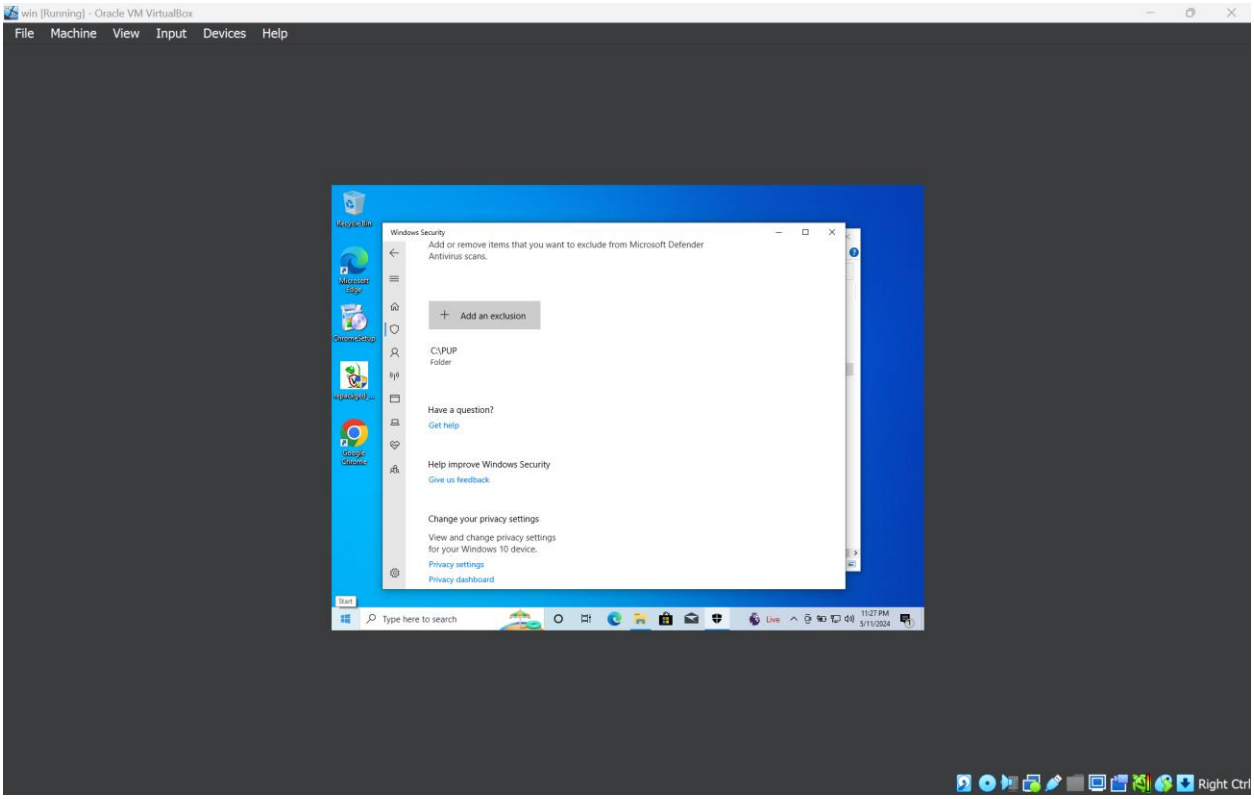


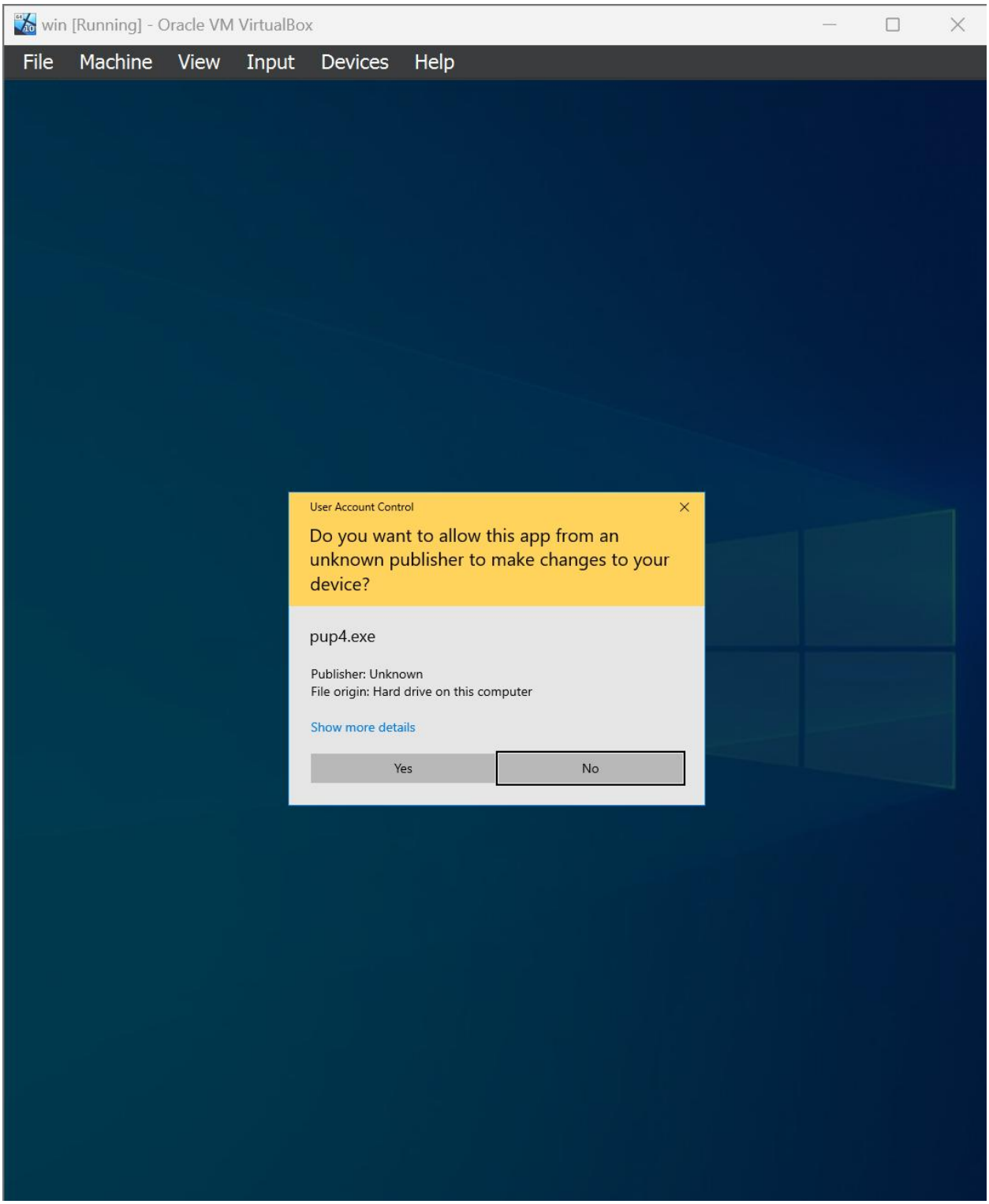
DESTPORT FLAG:


Raw Response JSON
"Authenticode": "",
"Family": "IPv4",
"Type": "TCP",
"Status": "LISTEN",
"SrcIP": "192.168.56.1",
"SrcPort": 8001,
"DestIP": "0.0.0.0",
"DestPort": 0,
"Timestamp": "2024-05-11T17:45:20Z"
},
{
"Pid": 25300,
"Ppid": 22304,
"Name": "velociraptor-v0.72.1-linux-amd64",
"Path": "",
"CommandLine": "",
"Hash": {
"MD5": "d41d8cd98f00b204e9800998ecf8427e",
"SHA1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
"SHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
},
"Username": "ABDULLAHM-PC\\user",
"Authenticode": "",
"Family": "IPv4",
"Type": "TCP",
"Status": "ESTAB",
"SrcIP": "192.168.56.1",
"SrcPort": 8001,
"DestIP": "192.168.56.1",
"DestPort": 52828,
"Timestamp": "2024-05-11T17:45:20Z"
},
{}
]
Close
2024-05-11T18:04:45Z

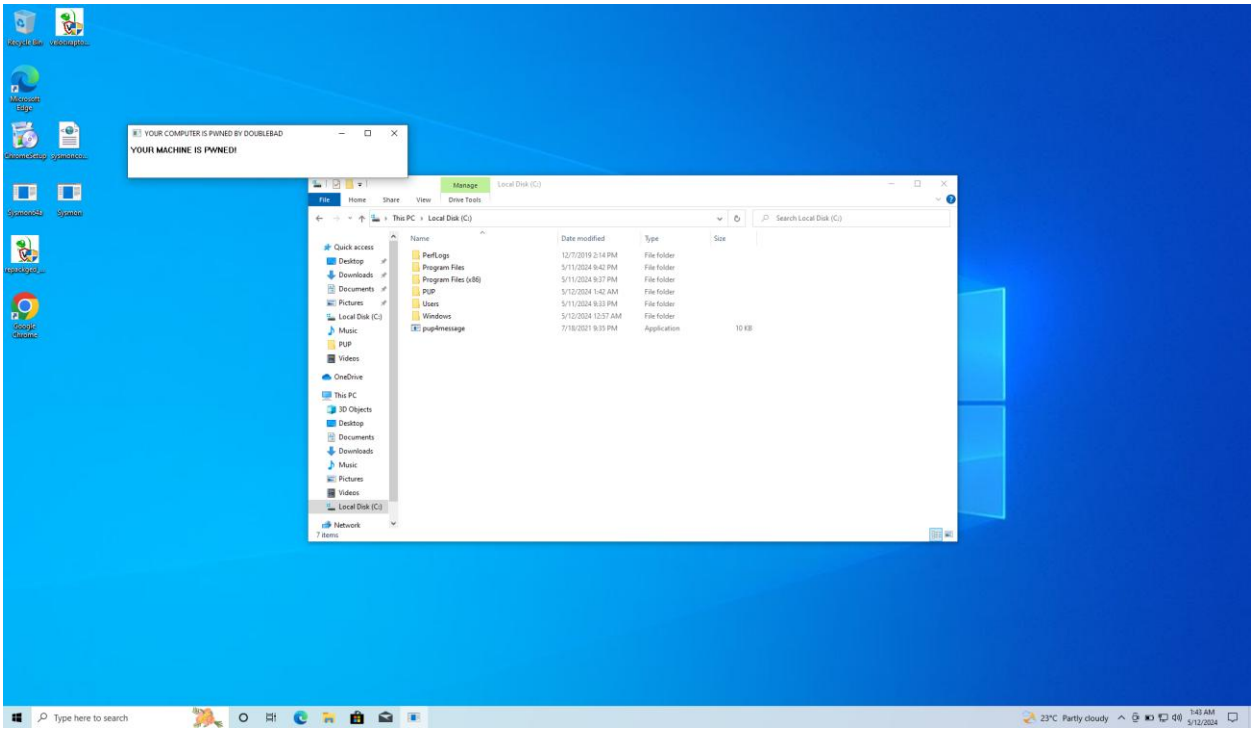
18.Investigating a PUP with Velociraptor

ADDING EXCLUSION:




win [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
pup4.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
No

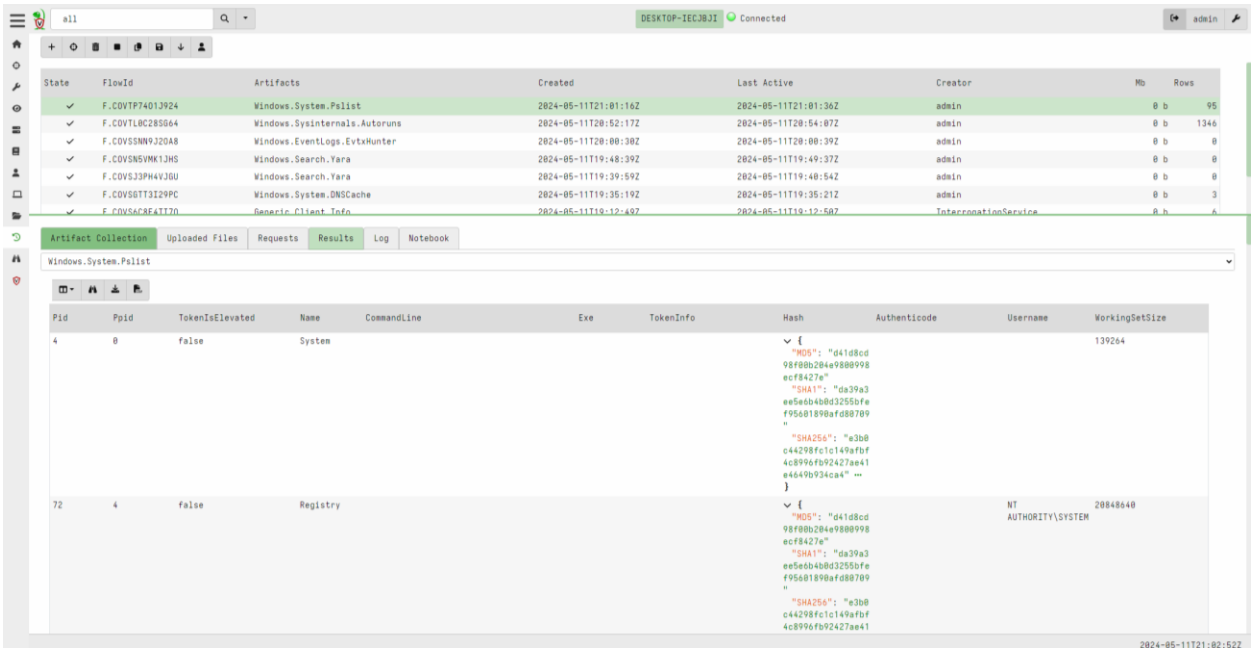
INFECTING MACHINE:



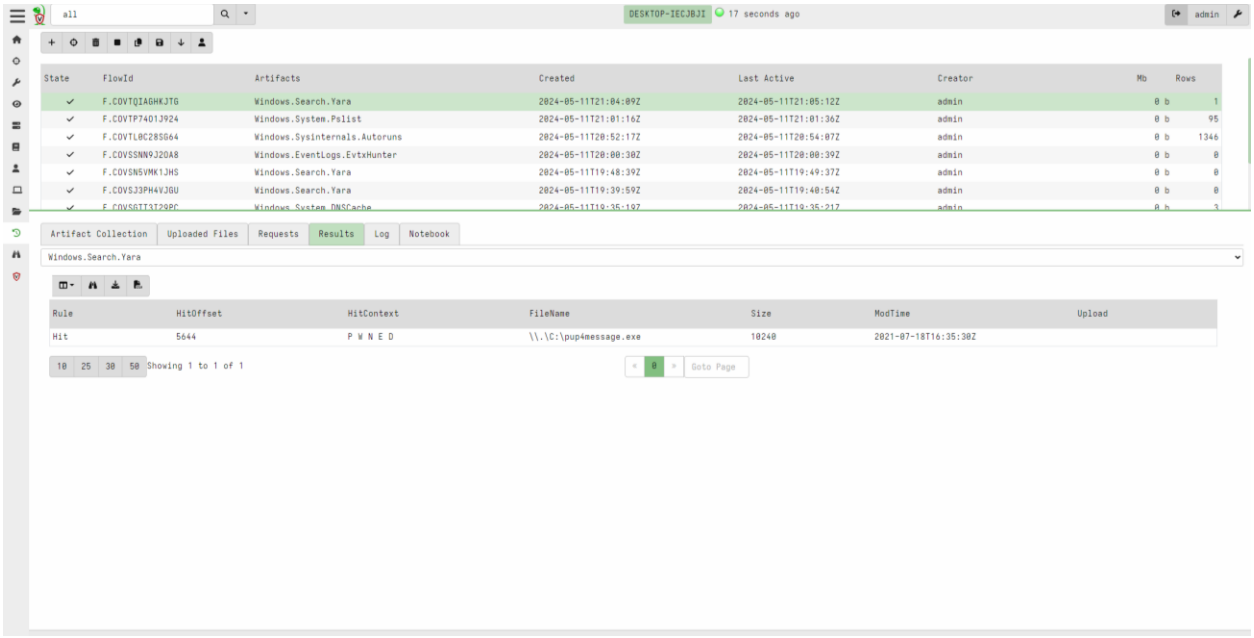
RUNKEY FLAG:

```
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/SDDL/LSA Lookup APIs,(Verified) Microsoft Windows,Microsoft Corporatic
KnownDlls,Setupapi,enabled,Known DLLs,System-wide,Windows Setup API,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\sy
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:\winc
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\sy
,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,,,,,,,,,,,,
ogon\Shell,explorer.exe,enabled,Logon,System-wide,Windows Explorer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\exp
teShell,,,Logon,System-wide,,,,,,,,,,,,
teShell,cmd.exe,enabled,Logon,System-wide,Windows Command Processor,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\sy
ogon,System-wide,,,,,,,,,,,,
urityHealth,enabled,Logon,System-wide,Windows Security notification icon,(Verified) Microsoft Windows,Microsoft Corporation,c:\windc
xTray,enabled,Logon,System-wide,VirtualBox Guest Additions Tray Application,(Verified) Microsoft Windows Hardware Compatibility Publ
sion\Run,,,Logon,System-wide,,,,,,,,,,,,
sion\Run,PUP4,enabled,Logon,System-wide,,,,c:\pup4message.exe,,C:\PUP4message.exe,A53BFCA803E217B9D599C7C774970550,DA0935468E6CA868
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,11.6
plorer,System-wide,ActiveX control for streaming video,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\msvidc
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.
Explorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11
plorer,System-wide,Microsoft® InfoTech Storage System Library,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32
bled,Explorer,System-wide,Microsoft (R) HTML Viewer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\mshtml.dl
Explorer,System-wide,OLE32 Extensions for Win32,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\urlmon.dll,11
,Explorer,System-wide,Microsoft (R) HTML Viewer,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\mshtml.dll,11
Explorer,System-wide,Microsoft Internet Messaging API Resources,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\syster
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\syste
plorer,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,
,enabled,Explorer,System-wide,TBAuth protocol handler,(Verified) Microsoft Windows,Microsoft Corporation,c:\windows\system32\tbauth.
nts,,,Logon,System-wide,,,,,,,,,,,,
nts,Microsoft Windows Media Player,enabled,Logon,System-wide,Microsoft Windows Media Player Setup Utility,(Verified) Microsoft Windc
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 Windc
nts,Windows Desktop Update,enabled,Logon,System-wide,Windows Shell Common Dll,(Verified) Microsoft Windows,Microsoft Corporation,c:\
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:\
nts,Google Chrome,enabled,Logon,System-wide,Google Chrome Installer,(Verified) Google LLC,Google LLC,c:\program files\google\chrome\
nts,Microsoft Edge,enabled,Logon,System-wide,Microsoft Edge Installer,(Verified) Microsoft Corporation,Microsoft Corporation,c:\prog
lled Components,,,Logon,System-wide,,,,,,,,,,,,
lled Components,Microsoft Windows Media Player,enabled,Logon,System-wide,Microsoft Windows Media Player Setup Utility,(Verified) Mic
lled Components,Microsoft Windows Media Player,enabled,Logon,System-wide,Microsoft Windows Media Player Setup Utility,(Verified) Mic
lled Components,n/a,enabled,Logon,System-wide,Microsoft .NET IE SECURITY REGISTRATION,(Verified) Microsoft Corporation,Microsoft Cor
ows\IconServiceLib,,,Logon,System-wide,,,,,,,,,,,,
ows\IconServiceLib,IconCodecService.dll,enabled,Logon,System-wide,Converts a PNG part of the icon to a legacy bmp icon,(Verified) Mi
r\ShellServiceObjects,,,Explorer,System-wide,,,,,,,,,,,,
r\ShellServiceObjects,Published Items Shell Service Object,enabled,Explorer,System-wide,Windows Shell Common Dll,(Verified) Microsof
r\ShellServiceObjects,Microsoft VolumeControlService Class,enabled,Explorer,System-wide,SCA Volume,(Verified) Microsoft Windows,Micr
r\ShellServiceObjects,Windows To Go Shell Service Object,enabled,Explorer,System-wide,Windows To Go Shell Service Object,(Verified)
r\ShellServiceObjects," {566296fe-e0e8-475f-ba9c-a31ad31620b1}",enabled,Explorer,System-wide,Device Stage Shell Extension,(Verified)
r\ShellServiceObjects,Cloud Cache Invalidator SSO,enabled,Explorer,System-wide,Cloud Data Store,(Verified) Microsoft Windows,Microsc
r\ShellServiceObjects,UnexpectedShutdownReason,enabled,Explorer,System-wide,Systray shell service object,(Verified) Microsoft Windov
```

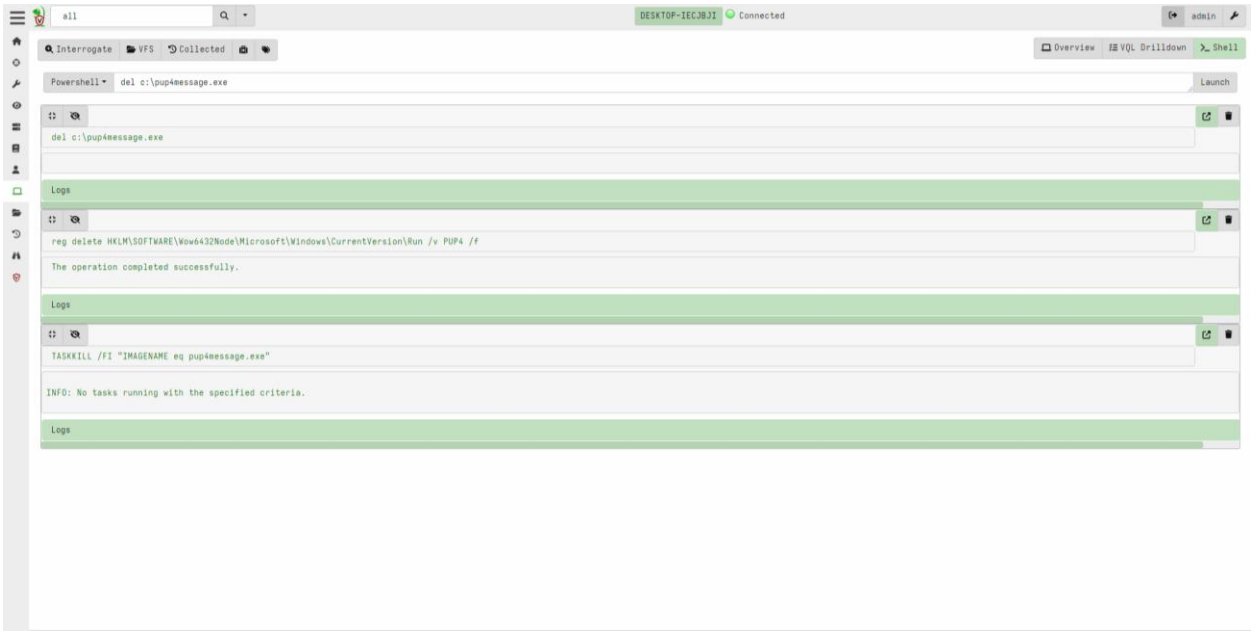
MD5 OF EXE:

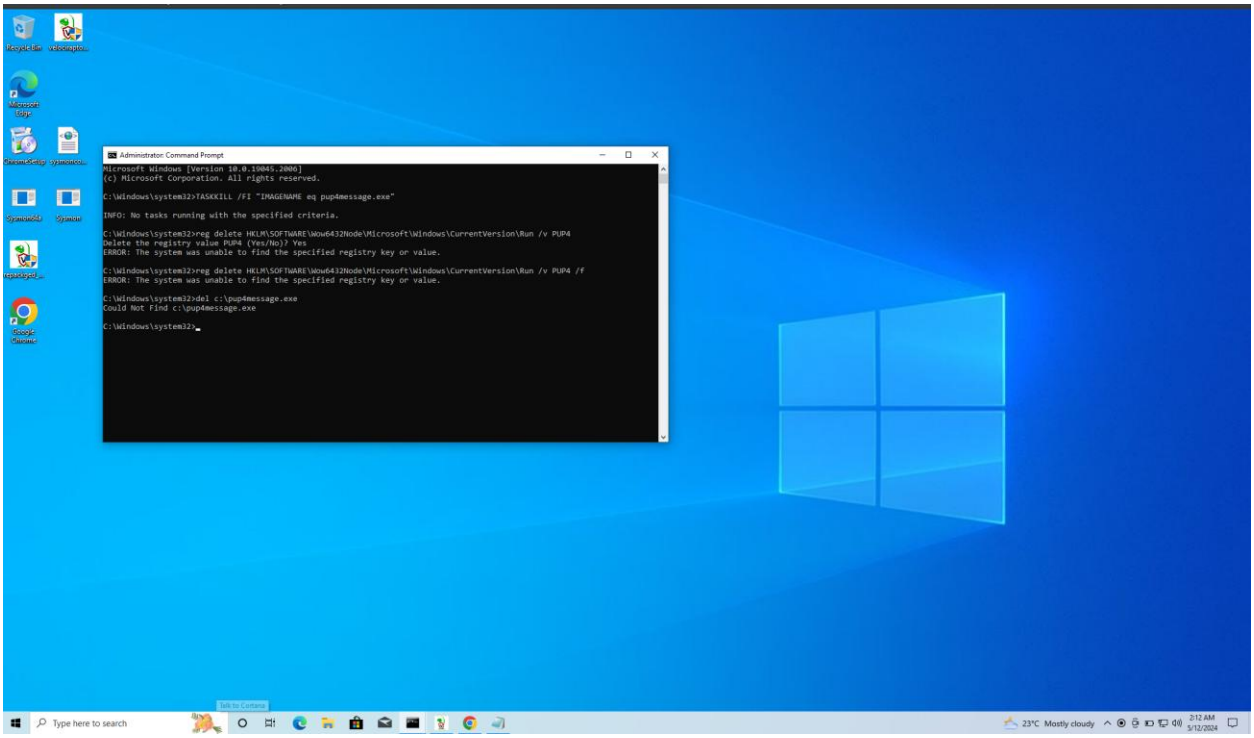


YARA:



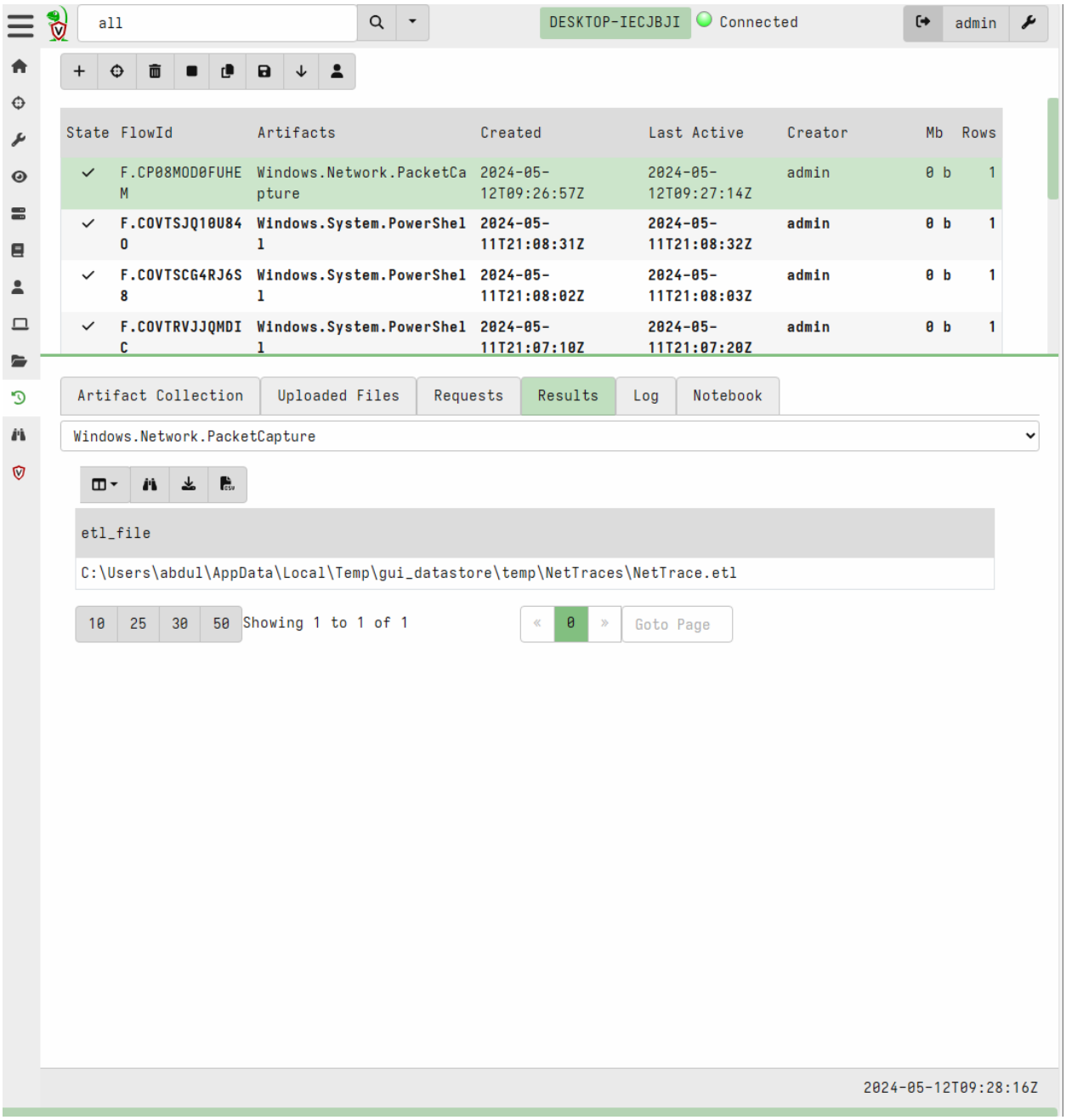
REMEDIATION:

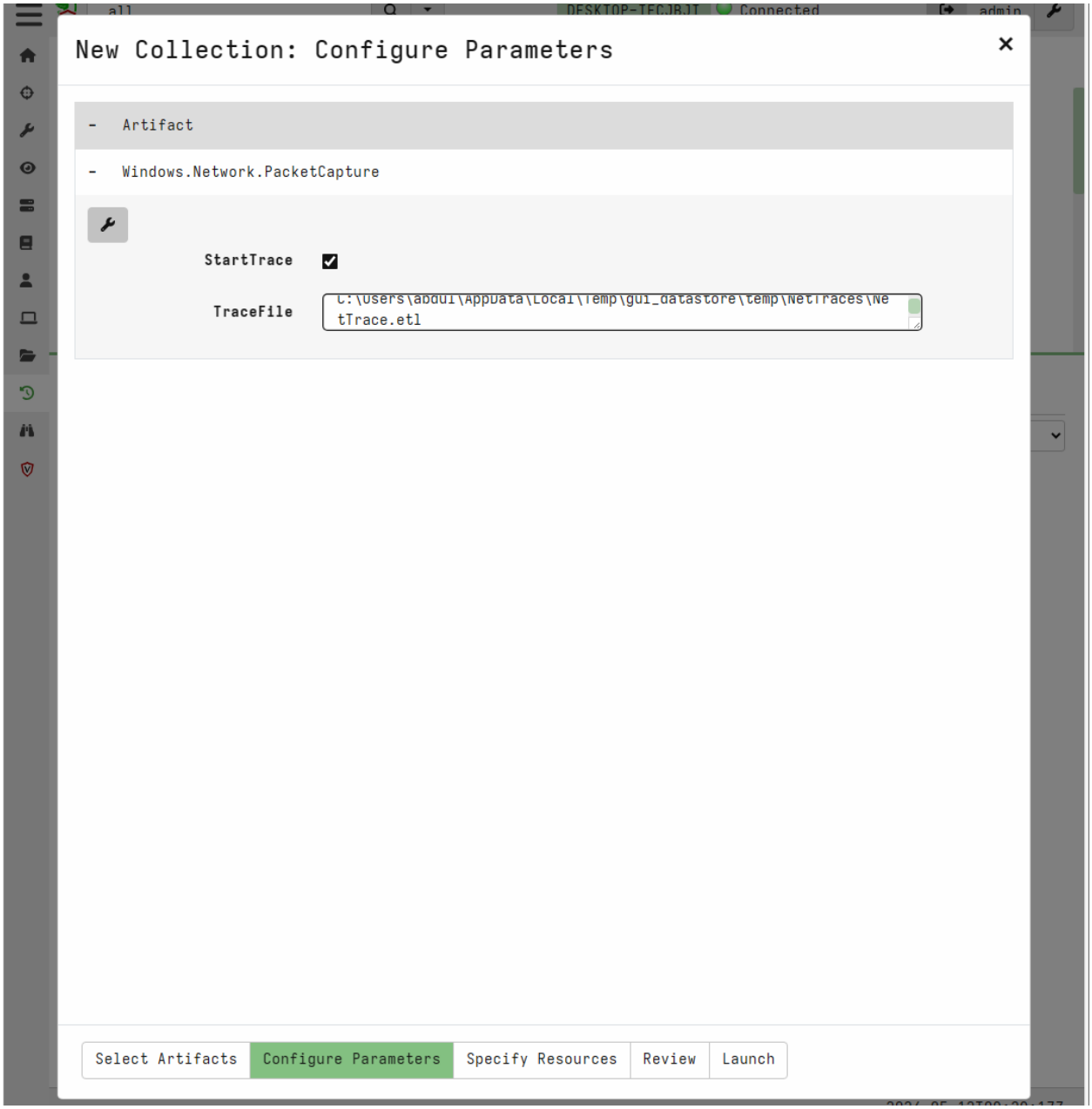




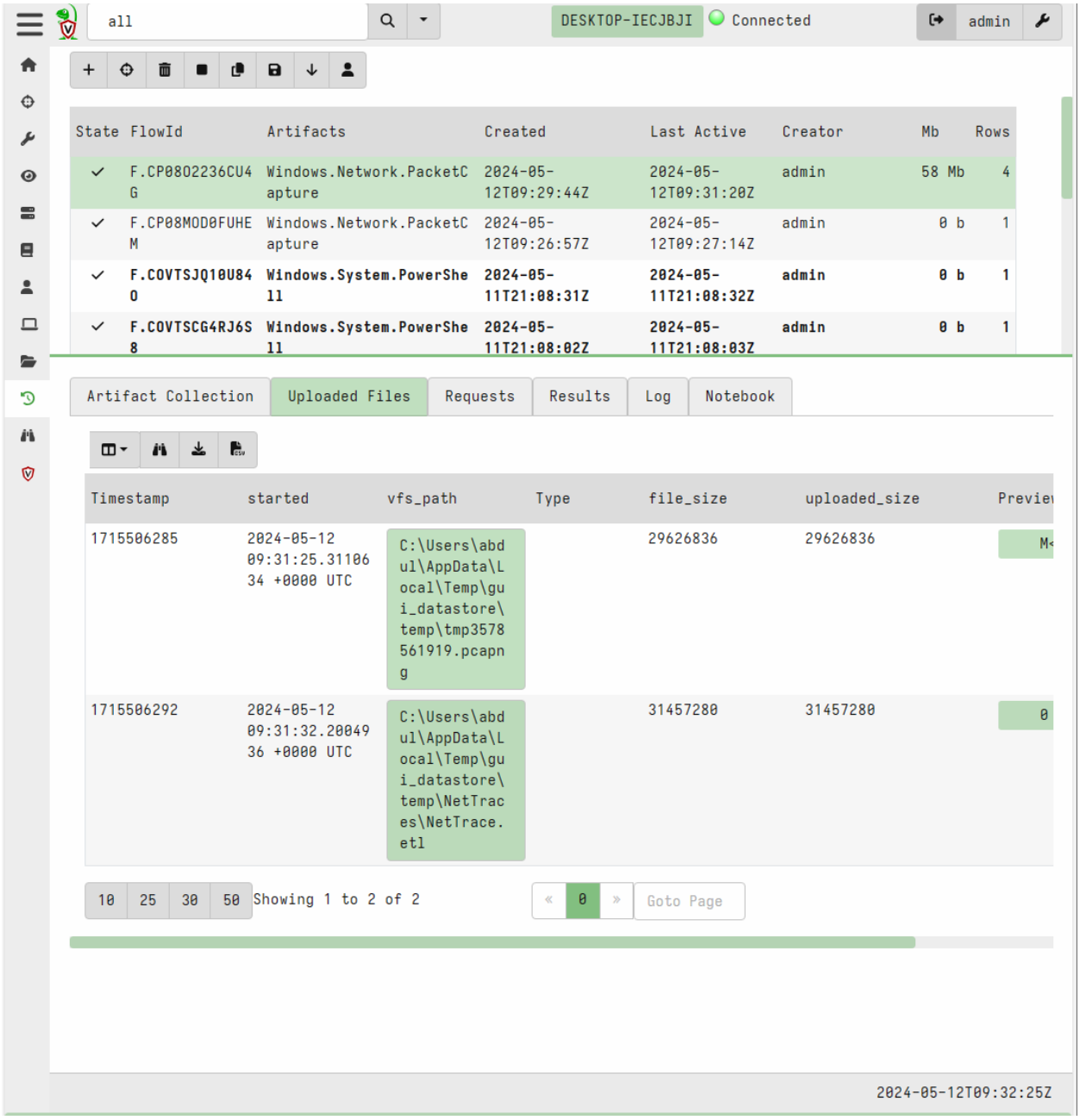
19.Investigating a Bot with Velociraptor

CAPTURING NETWORK TRAFFIC REMOTELY:



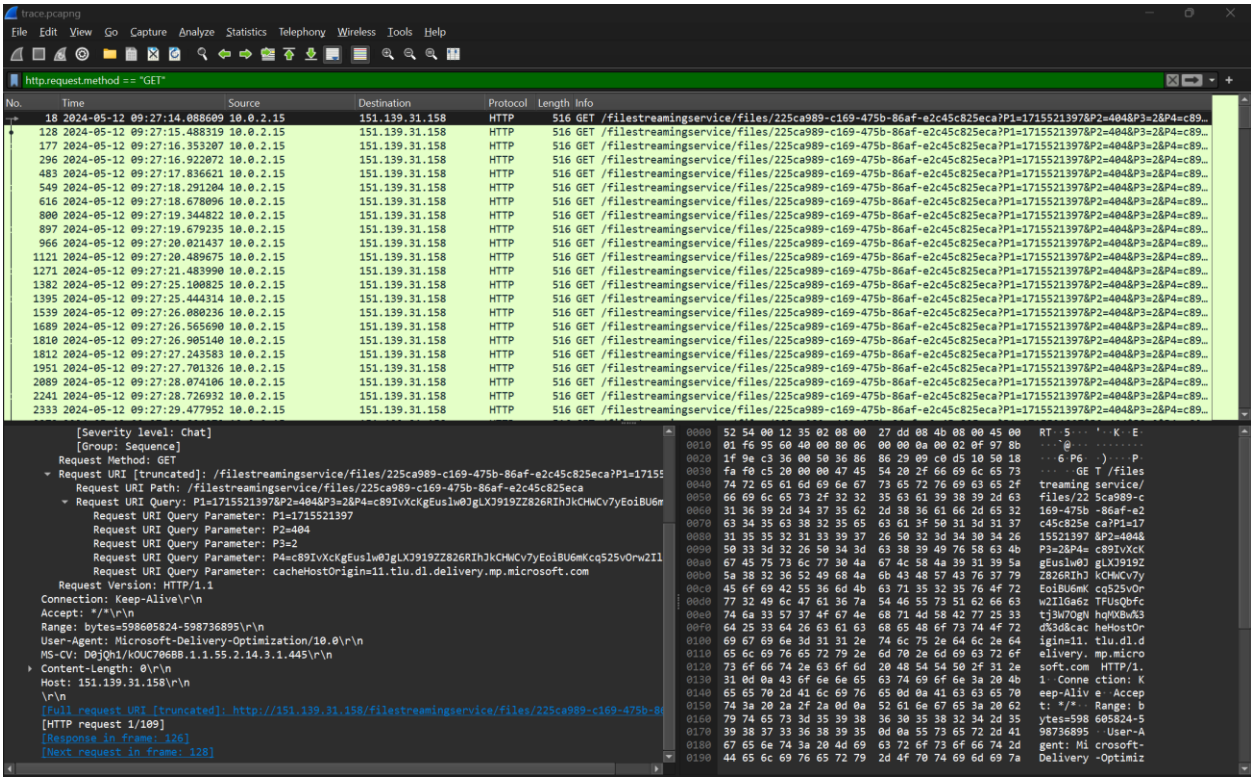

New Collection: Configure Parameters
- Artifact
- Windows.Network.PacketCapture
StartTrace
TraceFile
C:\Users\abdul\AppData\Local\Temp\gui_datastore\temp\NetTraces\NetTrace.etl
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch

CAPTURING FILES:



CREATING. PCAPNG FILES:

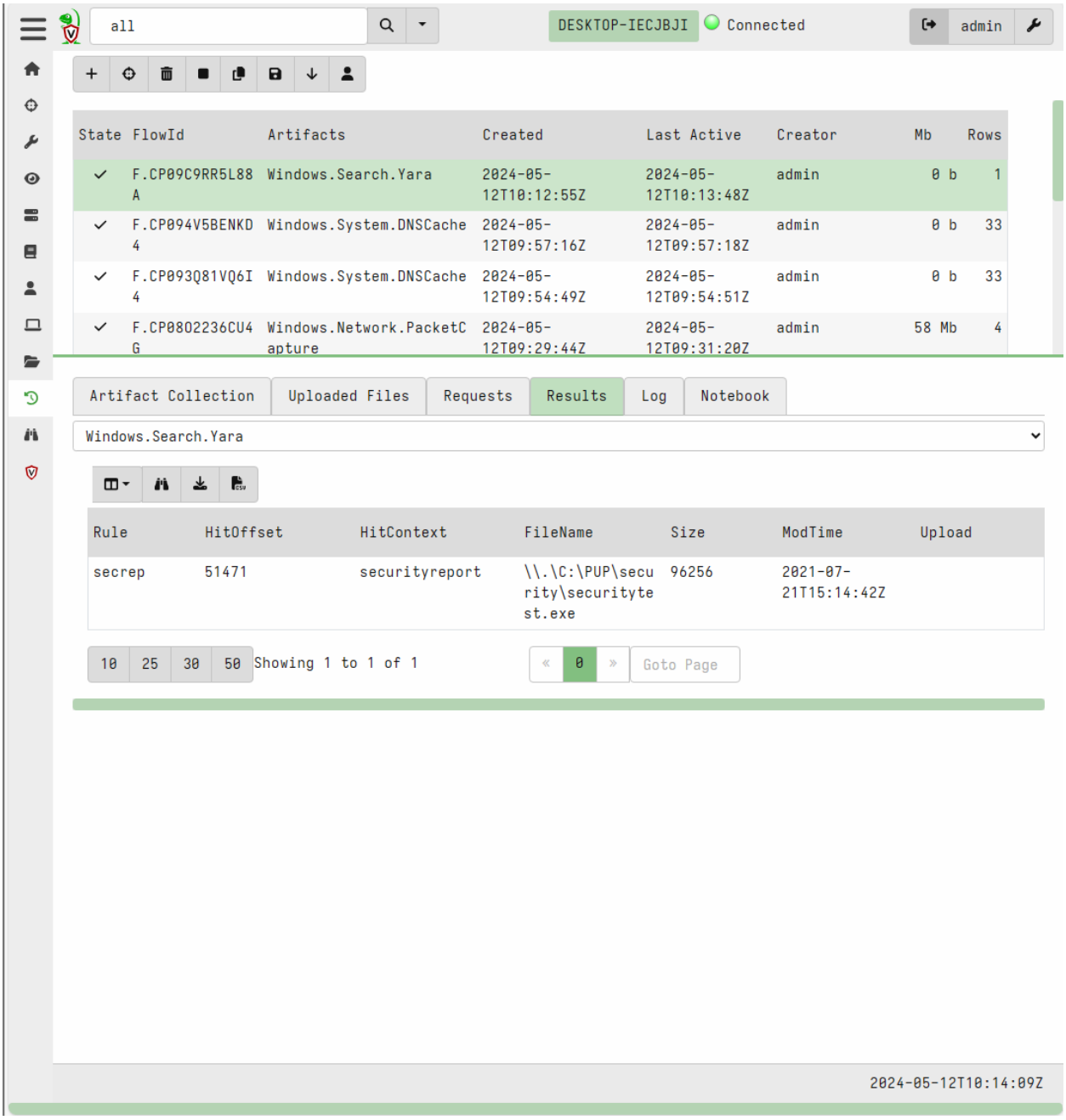
USER-AGENT:



DNS CACHE:

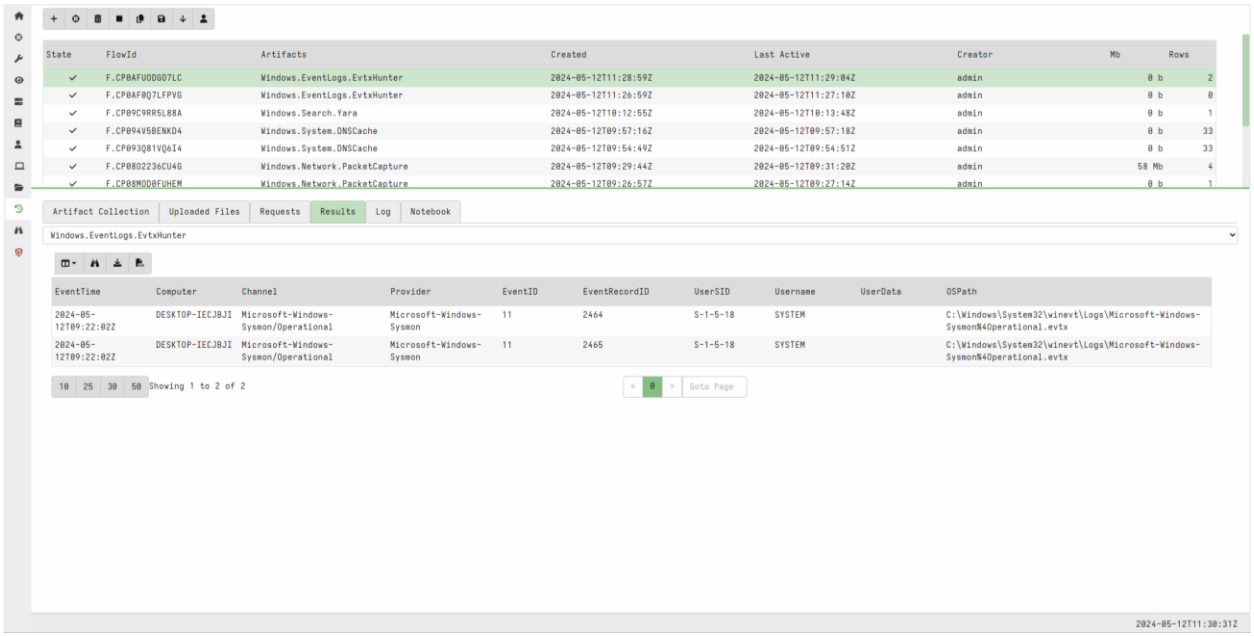
securityreport.samsclass.info	198.199.94.12	A	219	Success	Answer

BEACONING EXE:



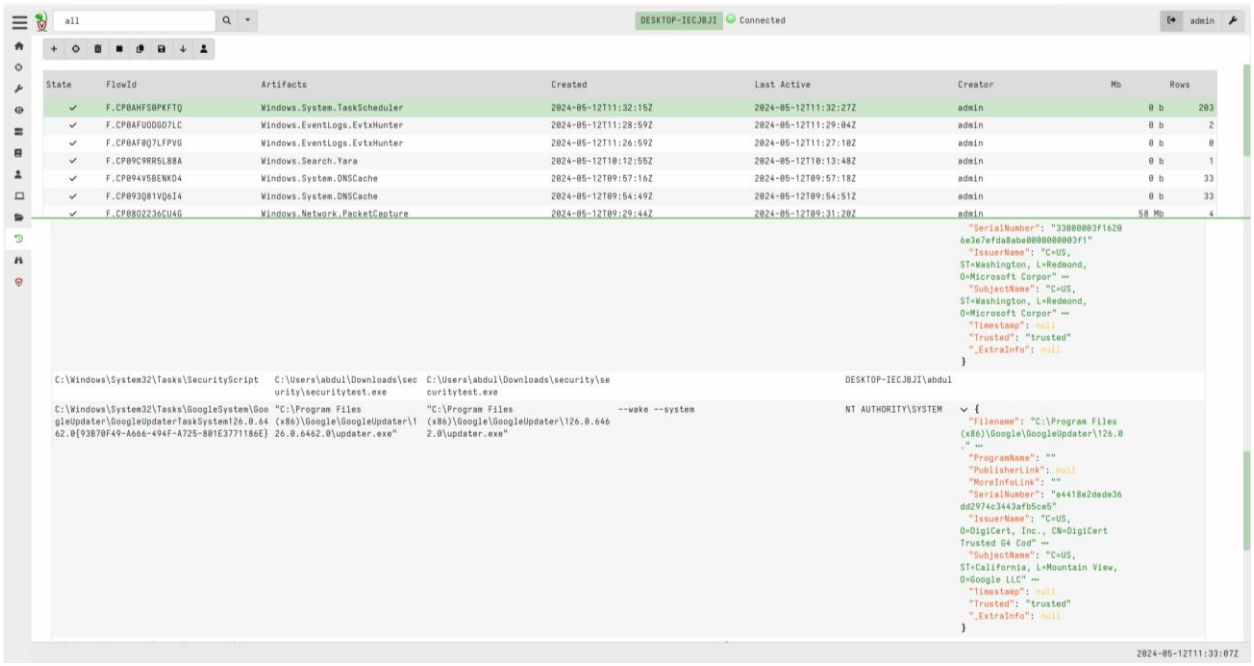
SYSMON INSTALLATION:

WINDOWS.EVENTLOGS. EVTXHUNTER:

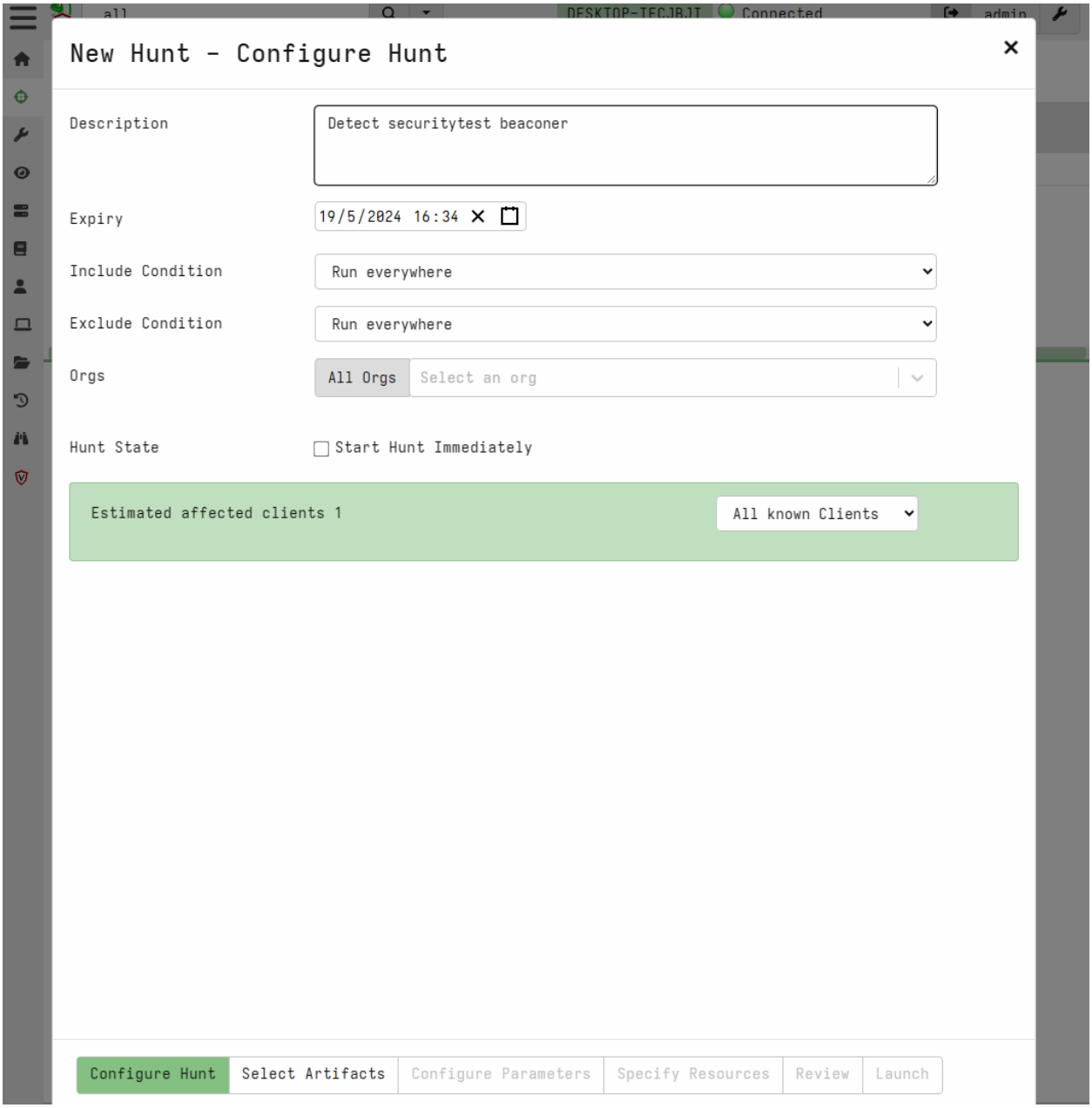


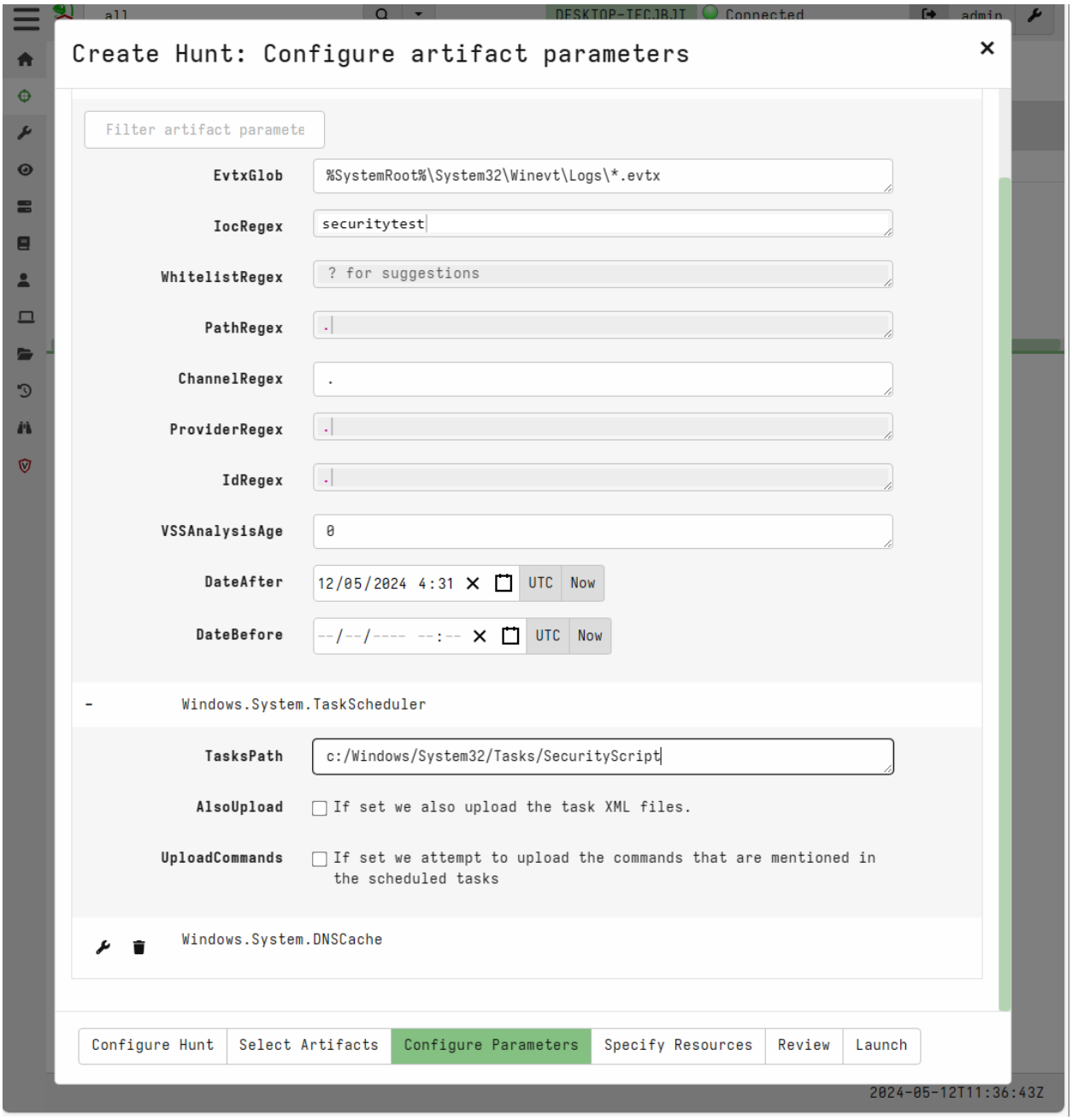
PARENT COMMND LINE:

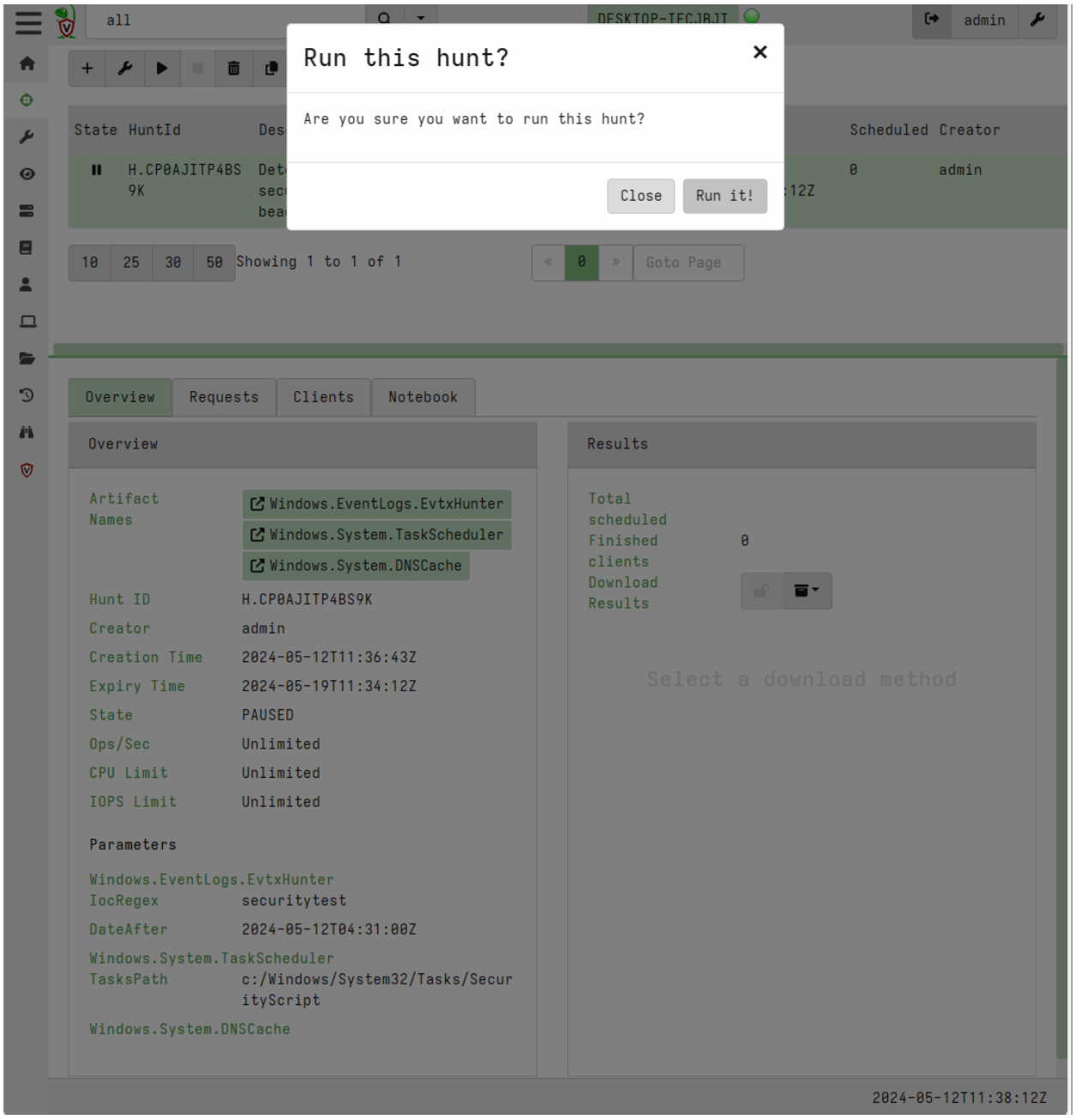
SCHEDULED TASKS:



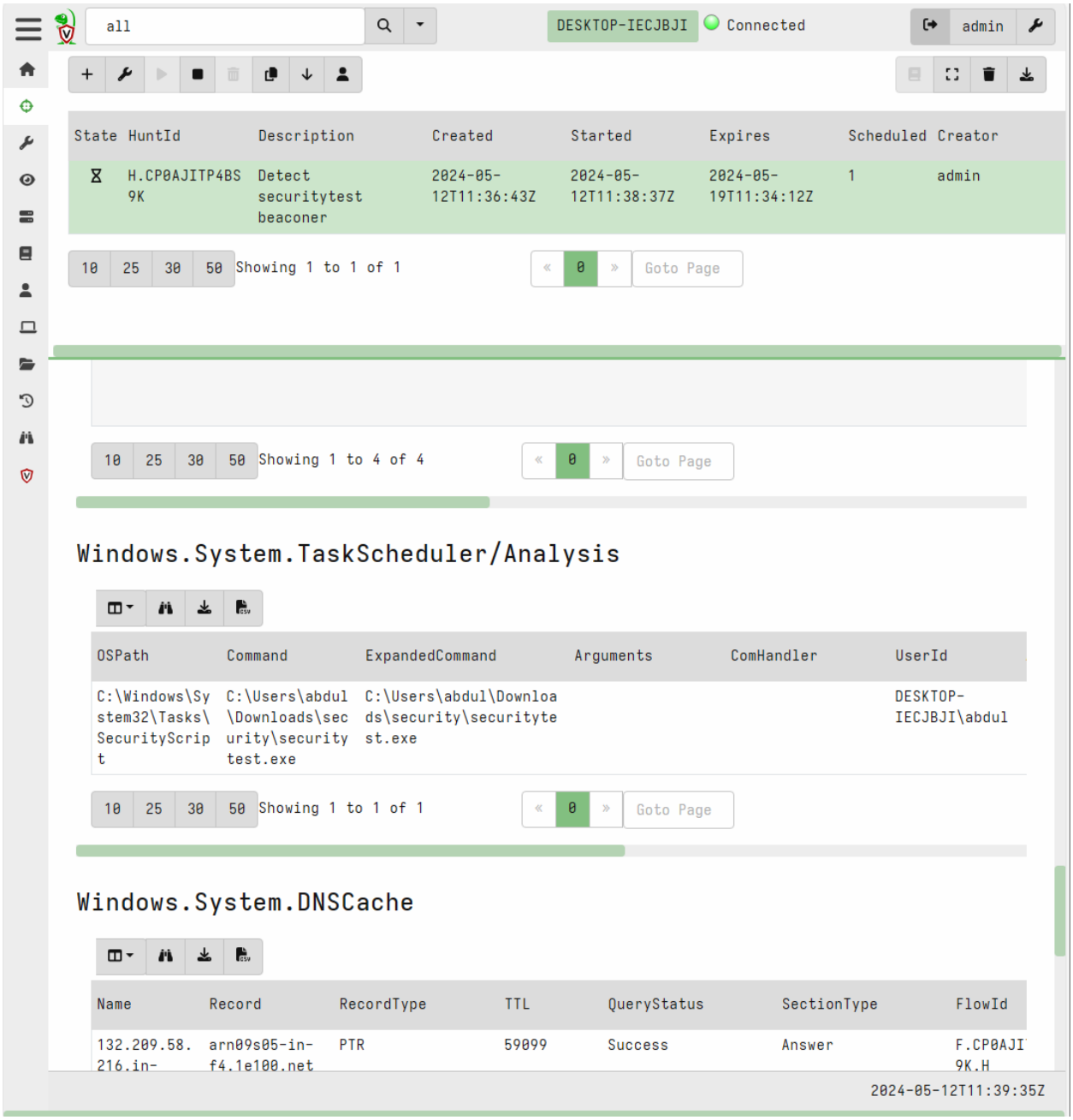
HUNTS:


New Hunt - Configure Hunt
Description
Detect securitytest beaconer
Expiry
19/5/2024 16:34
Include Condition
Run everywhere
Exclude Condition
Run everywhere
Orgs
All Orgs
Select an org
Hunt State
Start Hunt Immediately
Estimated affected clients 1
All known Clients
Configure Hunt
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch

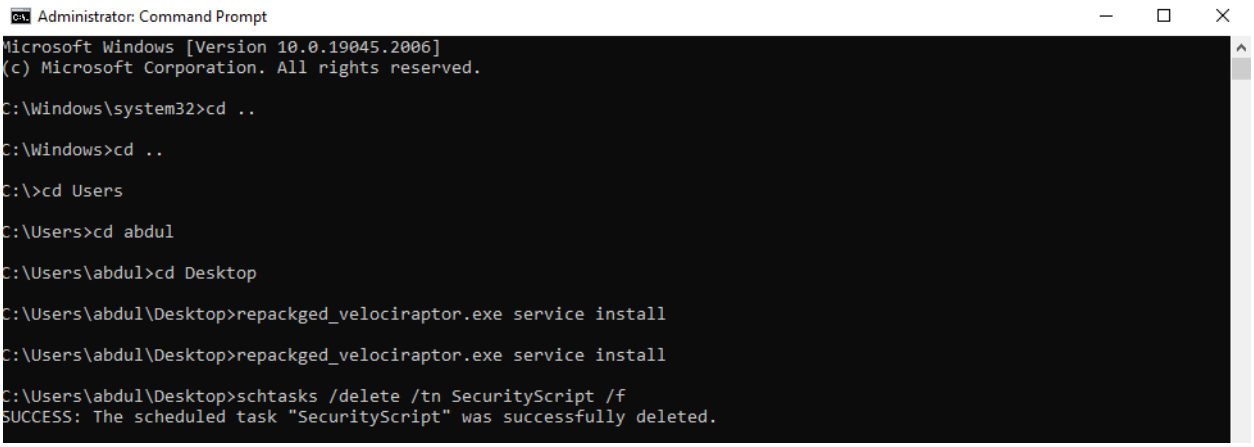

Create Hunt: Configure artifact parameters
Filter artifact paramete
EvtxGlob
%SystemRoot%\System32\Winevt\Logs*.evtx
IocRegex
securitytest
WhitelistRegex
? for suggestions
PathRegex
ChannelRegex
.
ProviderRegex
IdRegex
VSSAnalysisAge
0
DateAfter
12/05/2024 4:31
UTC
Now
DateBefore
--/--/---- --:--
UTC
Now
- Windows.System.TaskScheduler
TasksPath
c:/Windows/System32/Tasks/SecurityScript
AlsoUpload
If set we also upload the task XML files.
UploadCommands
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


all
DESKTOP-IECJBJI
admin
Run this hunt?
Are you sure you want to run this hunt?
Close
Run it!
State HuntId
Scheduled Creator
H.CP0AJITP4BS9K
0 admin
10 25 30 50 Showing 1 to 1 of 1
Goto Page
Overview Requests Clients Notebook
Overview
Artifact Names
Windows.EventLogs.EvtxHunter
Windows.System.TaskScheduler
Windows.System.DNSCache
Hunt ID H.CP0AJITP4BS9K
Creator admin
Creation Time 2024-05-12T11:36:43Z
Expiry Time 2024-05-19T11:34:12Z
State PAUSED
Ops/Sec Unlimited
CPU Limit Unlimited
IOPS Limit Unlimited
Parameters
Windows.EventLogs.EvtxHunter
IocRegex securitytest
DateAfter 2024-05-12T04:31:00Z
Windows.System.TaskScheduler
TasksPath c:/Windows/System32/Tasks/SecurityScript
Windows.System.DNSCache
Results
Total scheduled
Finished clients 0
Download Results
Select a download method
2024-05-12T11:38:12Z

TASKSCHEDULER /ANALYSIS:

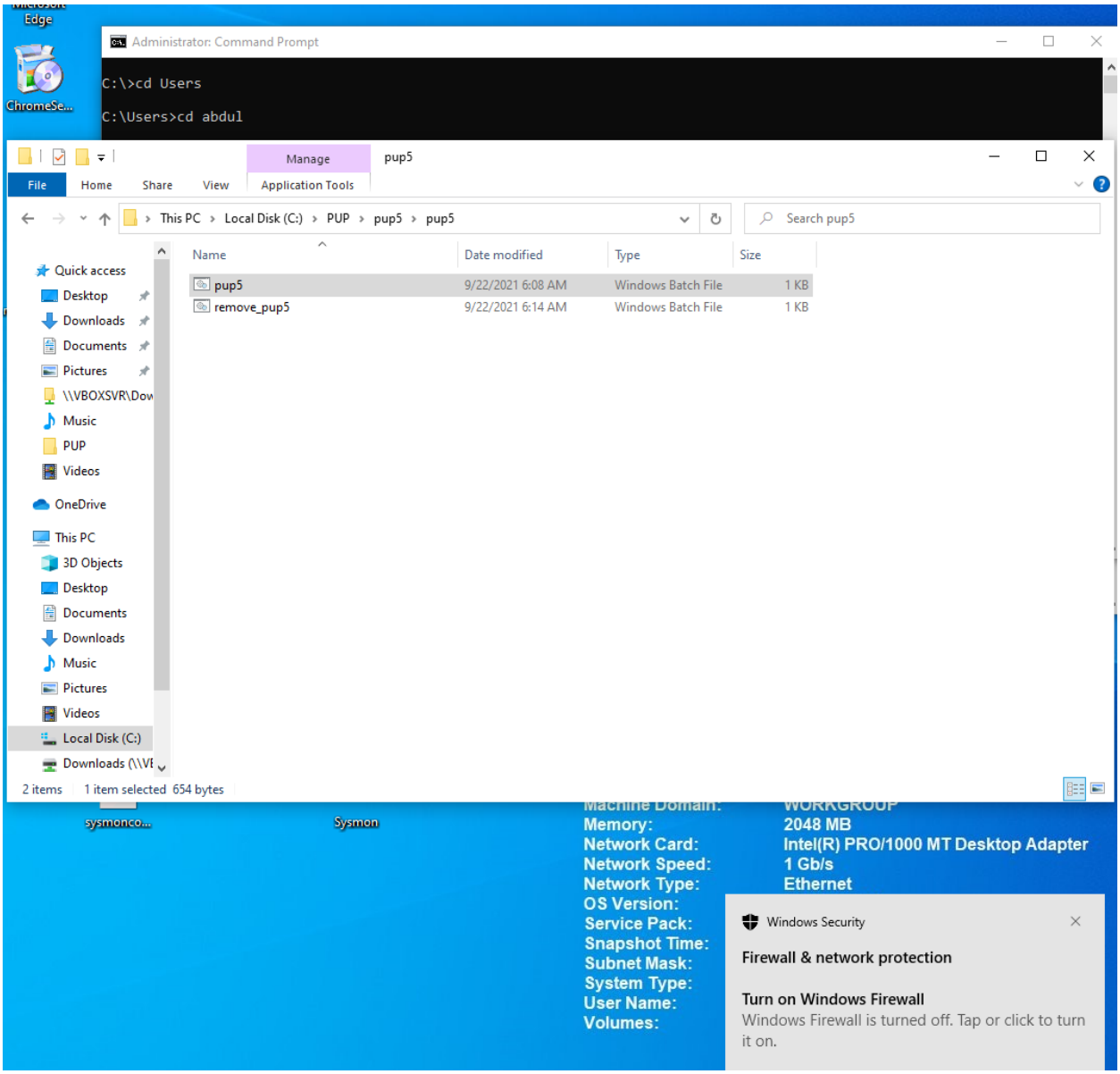


REMEDIATION:

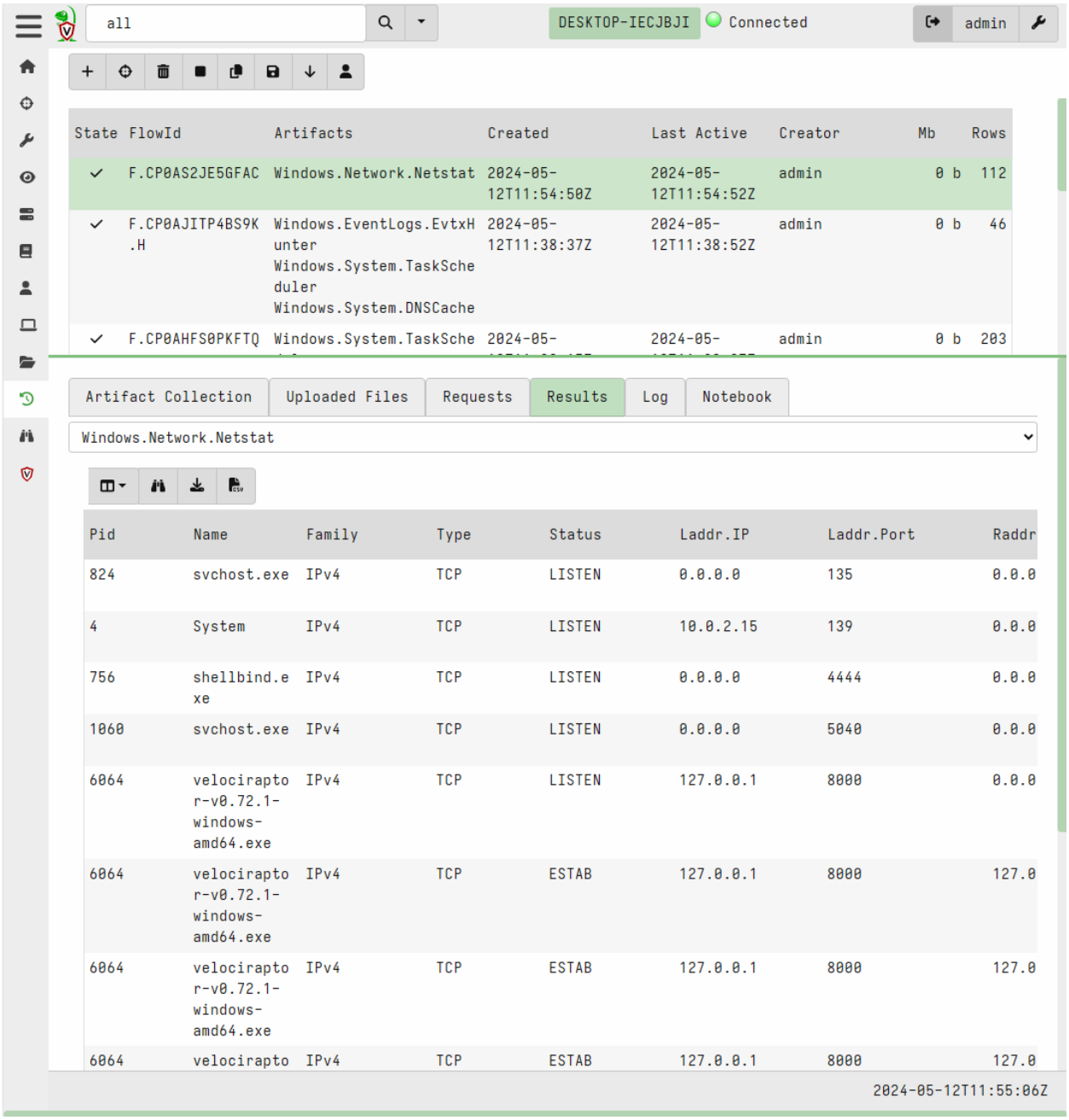


20. Investigating a Two-Stage RAT with Velociraptor

INSTALLING RAT:



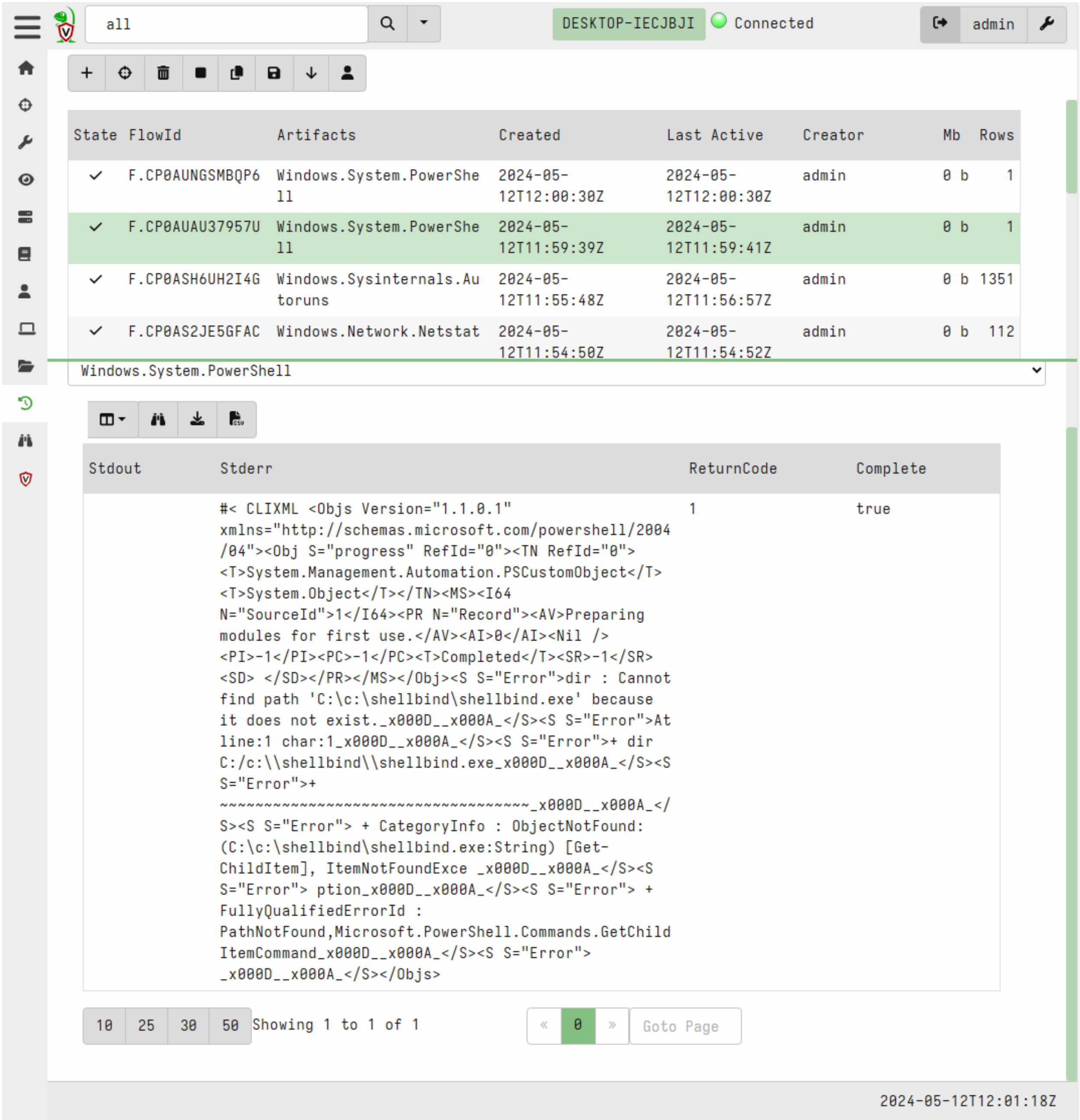
AUDITING AUTORUNS:



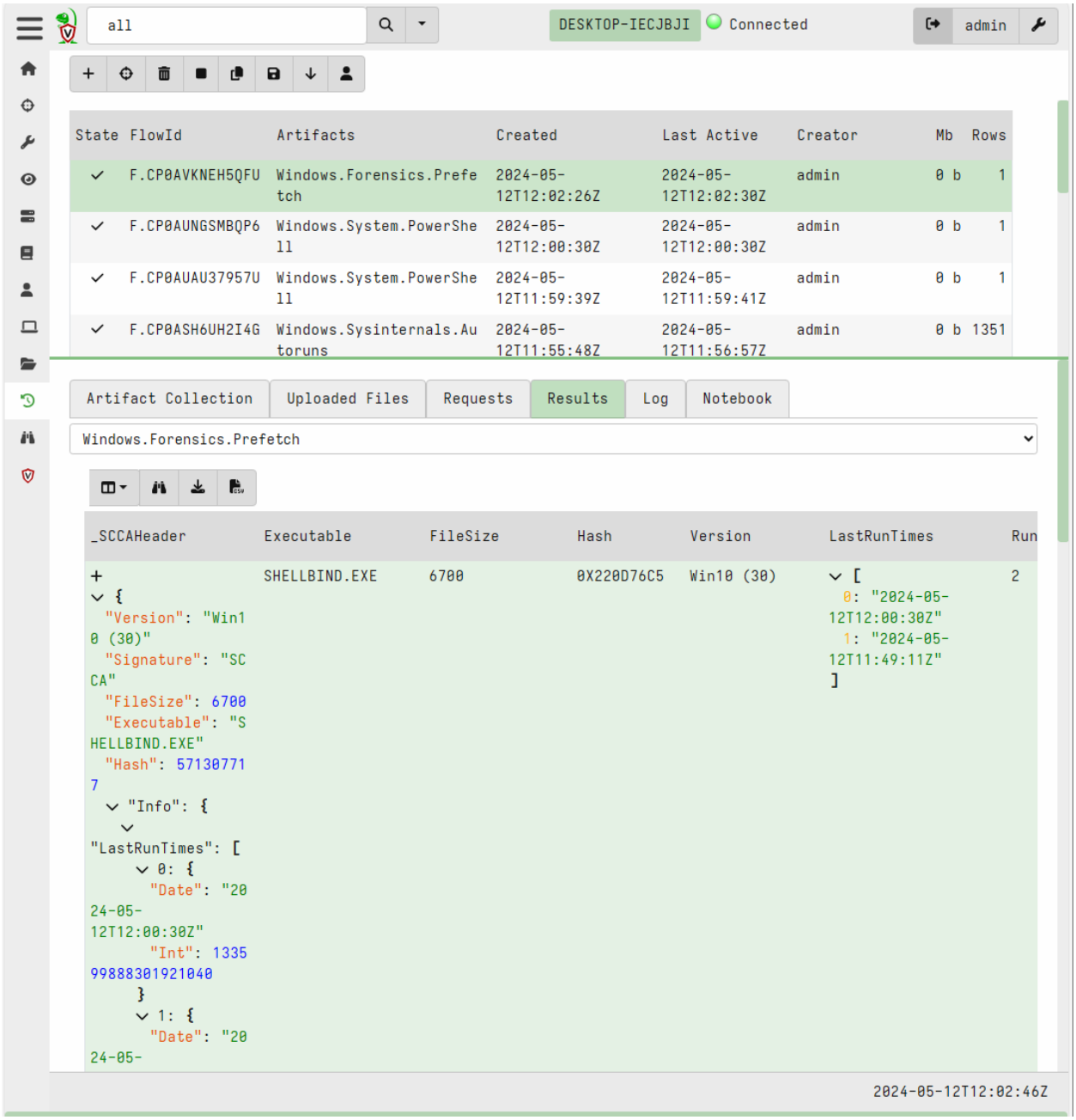
SHELLBIND.EXE PATH:

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":"","PESHA-
dows 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
ML Viewer","Signer":"(Verified) Microsoft Windows","Company":"Microsoft Corporation","Image

CREATION TIME:



PREFETCH:


all
DESKTOP-IECJBJI
Connected
admin
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 2024-05-12T12:00:30Z 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.Autoruns 2024-05-12T11:55:48Z 2024-05-12T11:56:57Z admin 0 b 1351
Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
Windows.Forensics.Prefetch
_SCCAHeader Executable FileSize Hash Version LastRunTimes Run
SHELLBIND.EXE 6700 0X220D76C5 Win10 (30) 2
"Version": "Win10 (30)"
"Signature": "SCCA"
"FileSize": 6700
"Executable": "SHELLBIND.EXE"
"Hash": 571307717
"Info": {
"LastRunTimes": [
0: "2024-05-12T12:00:30Z"
1: "2024-05-12T11:49:11Z"
]
"Date": "2024-05-12T12:00:30Z"
"Int": 133599888301921040
"Date": "2024-05-
2024-05-12T12:02:46Z

SYSMON LOGS:

REMEDIATION: