FORENSICS AND INVESTIGATION PRACTICAL ASSIGNMENT

PHILOMENA KYALO BSCS/020J/2020

KALUTU DANIEL BSCS/050J/2020

CHEMWA LEWIS BSCS/038J/2020

1. Mobile Device Forensics

1. Introduction

Objective: The objective of this forensic analysis was to investigate the contents of the Downloads folder from an Android device for potential evidence.

Scope: The analysis focused on the Downloads folder from a Redmi 9A device.

2. Acquisition Process

Environment Setup

- **Tools Used:** Autopsy, ADB (Android Debug Bridge)
- **Device:** Redmi 9A, running [Android version]
- **Computer:** HP laptop

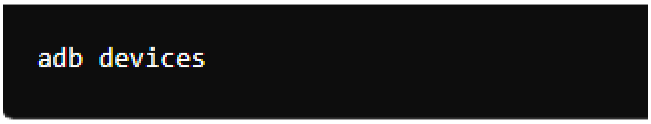
Steps Taken

Enabling USB Debugging:

1. Enabled Developer Options on the Android device.
2. Enabled USB Debugging in Developer Options.

Connecting Device:

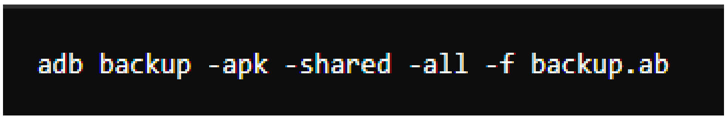
1. Connected the Android device to the computer using a USB cable.
2. Verified the connection using the command:



```
adb devices
```

Creating a Logical Backup:

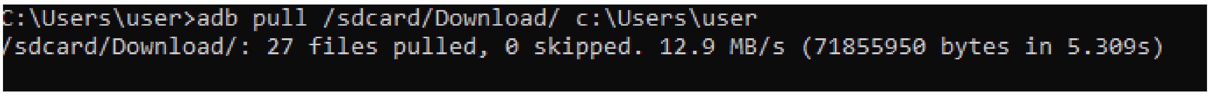
1. Ran the ADB backup command to create a full backup:



```
adb backup -apk -shared -all -f backup.ab
```

Copy the Downloads Folder:

- Use the following command to copy the Downloads folder from your Android device to your computer:



```
C:\Users\user>adb pull /sdcard/Download/ c:\Users\user
/sdcard/Download/: 27 files pulled, 0 skipped. 12.9 MB/s (71855950 bytes in 5.309s)
```

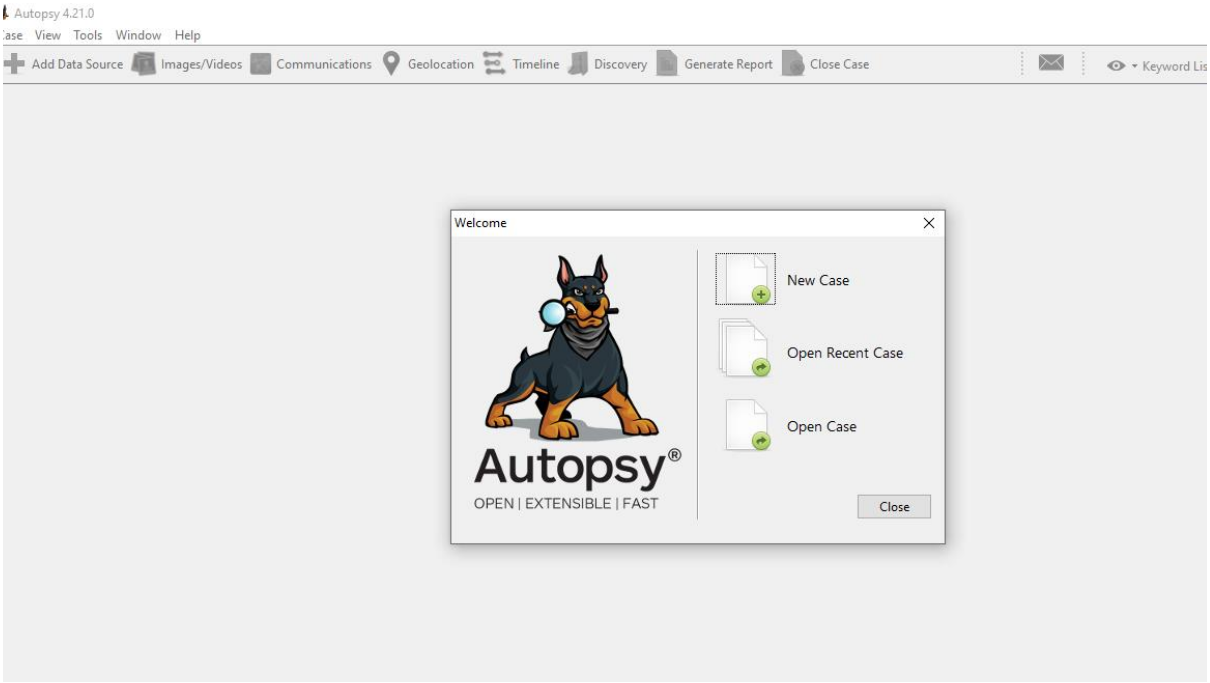
3. Analysis Process

Tools Used

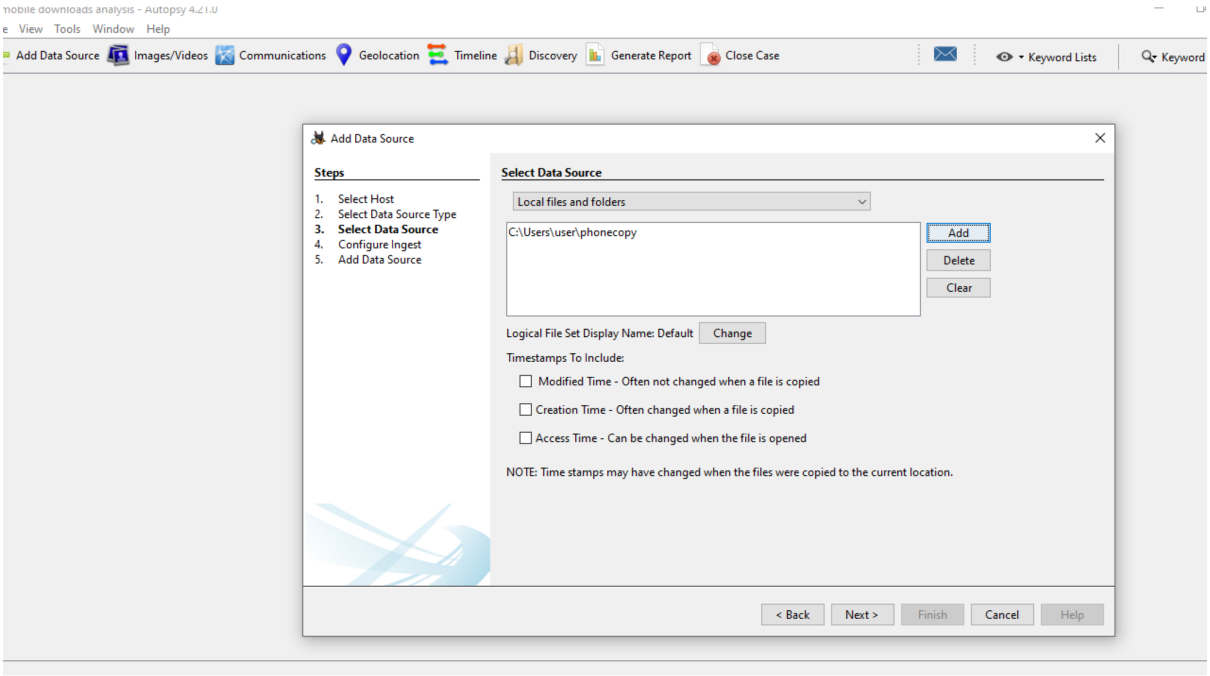
- Autopsy

Adding Data Source to Autopsy

1. Created a new case in Autopsy.



2. Added the extracted Downloads folder as a logical files data source.



Local files and folders

C:\Users\user\phonecopy

Logical File Set Display Name: Default

Timestamps To Include:

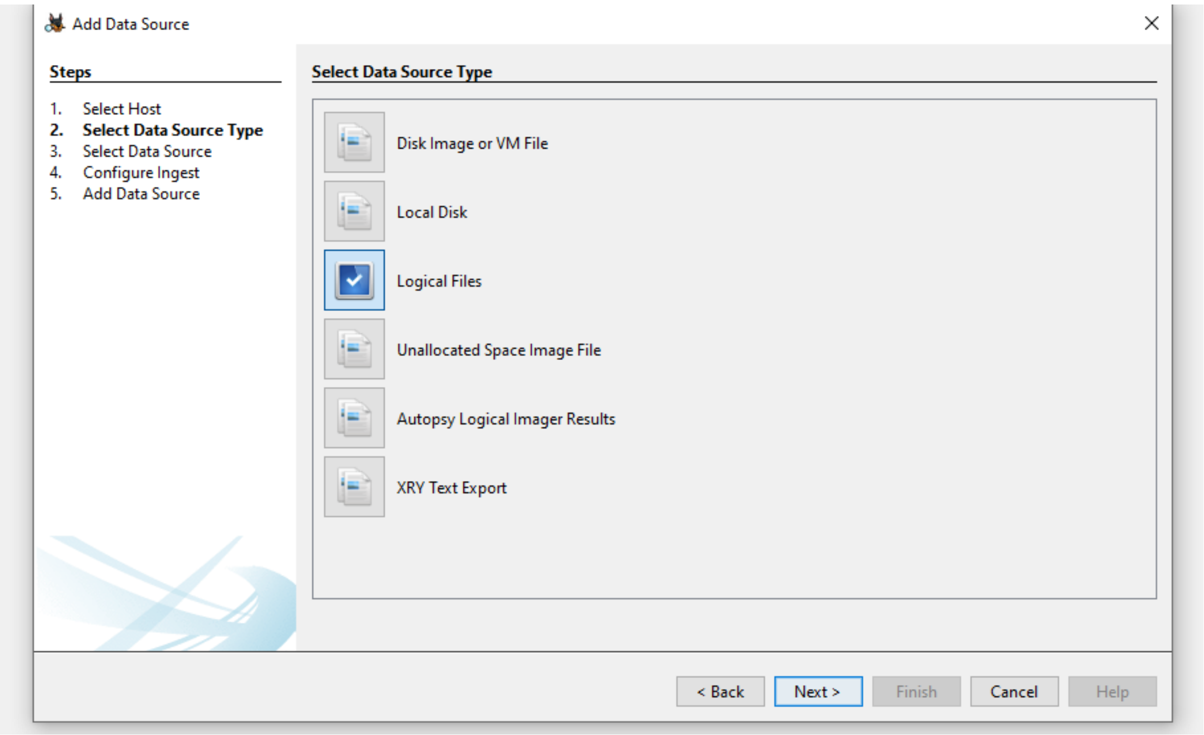
☐ Modified Time - Often not changed when a file is copied

☐ 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.

3. Specify the data source type



Add Data Source

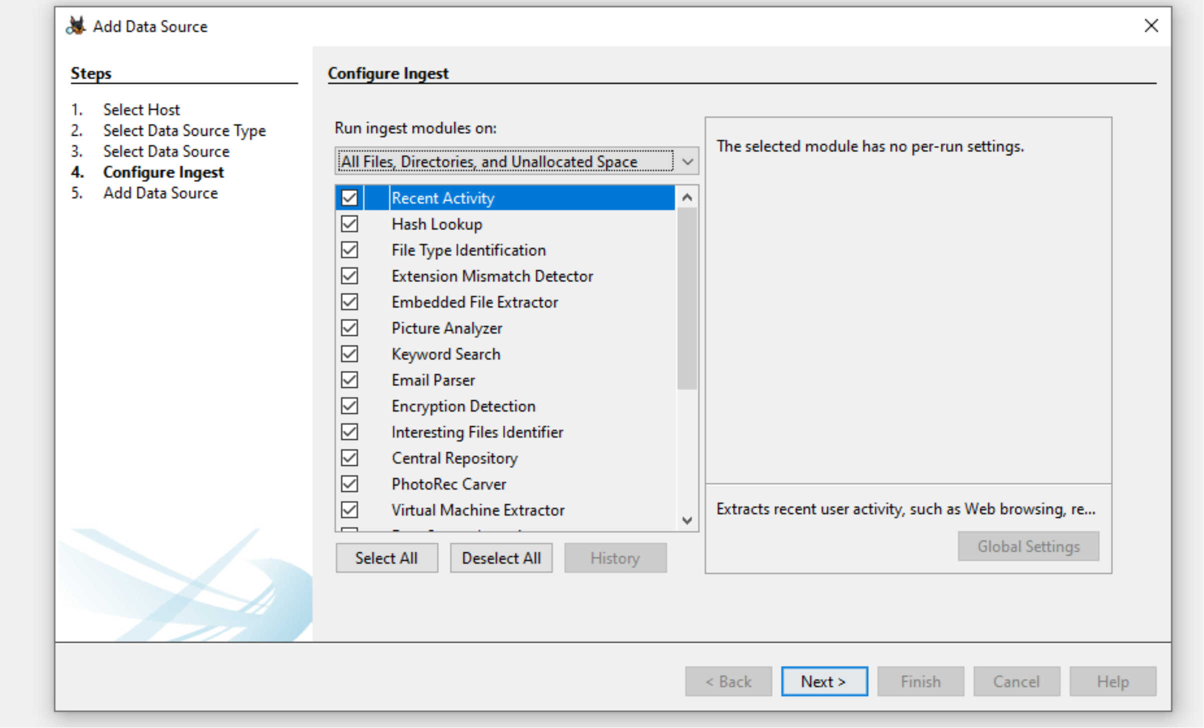
Steps

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

4. Configure the ingest modules



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:

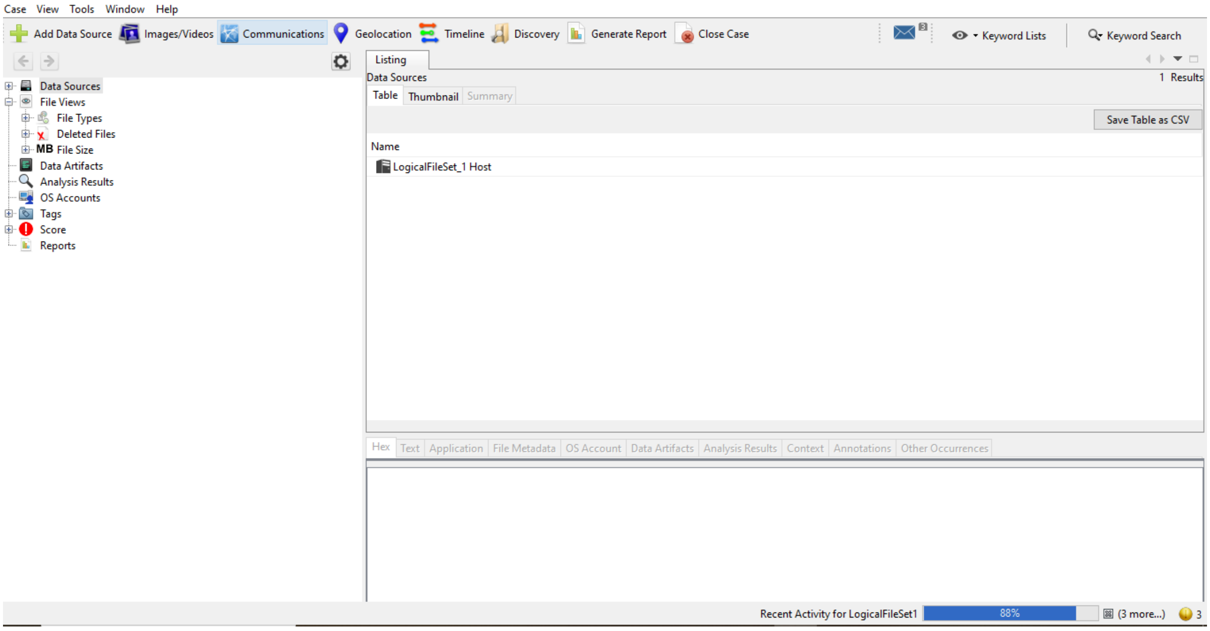
All Files, Directories, and Unallocated Space

☑ 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

The selected module has no per-run settings.

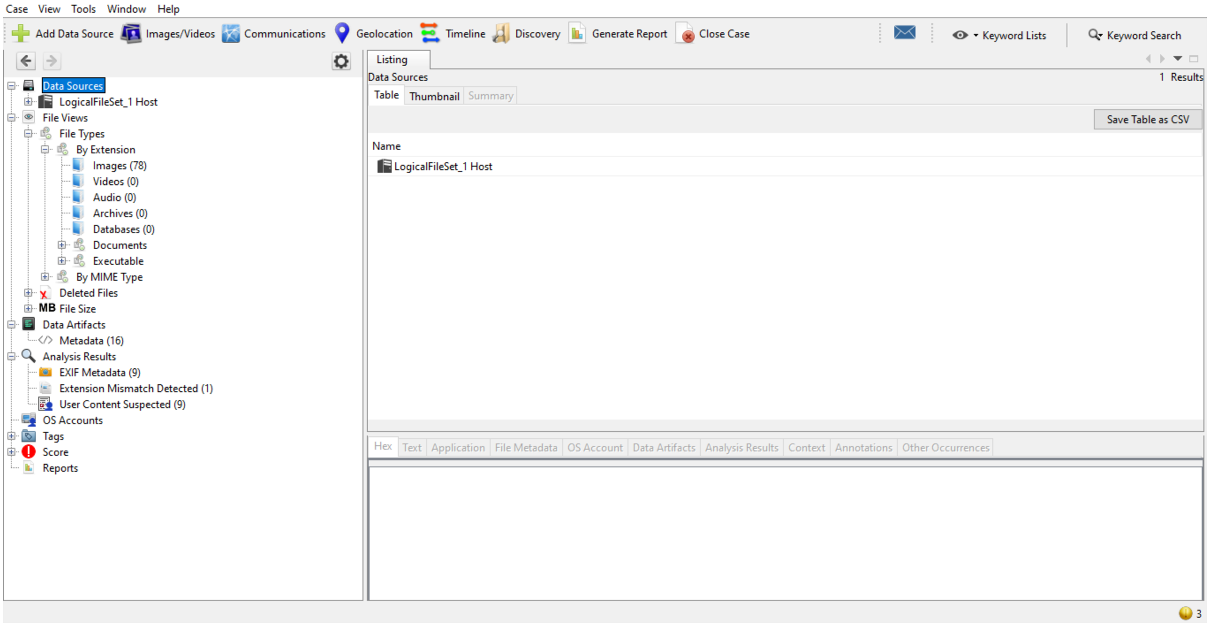
Extracts recent user activity, such as Web browsing, re...

5. Click on finish and then wait for analysis to start.

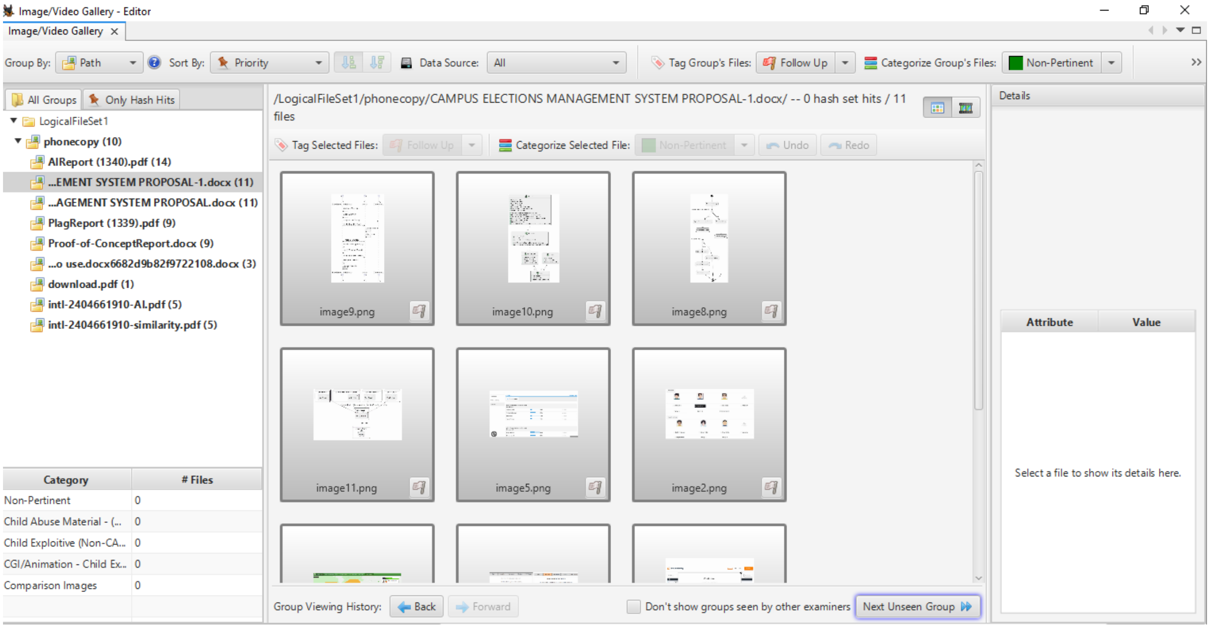


Findings

Immediately after the analysis, here are the findings.



Images and videos found



Group By: Path · Sort By: Priority · Data Source: All · Tag Group's Files: Follow Up · Categorize Group's Files: Non-Pertinent

- LogicalFileSet1
  - phonecopy (10)
    - AIReport (1340).pdf (14)
    - ...EMENT SYSTEM PROPOSAL-1.docx (11)
    - ...AGEMENT SYSTEM PROPOSAL.docx (11)
    - PlagReport (1339).pdf (9)
    - Proof-of-ConceptReport.docx (9)
    - ...o use.docx6682d9b82f9722108.docx (3)
    - download.pdf (1)
    - intl-2404661910-AI.pdf (5)
    - intl-2404661910-similarity.pdf (5)

/LogicalFileSet1/phonecopy/CAMPUS ELECTIONS MANAGEMENT SYSTEM PROPOSAL-1.docx/ -- 0 hash set hits / 11 files

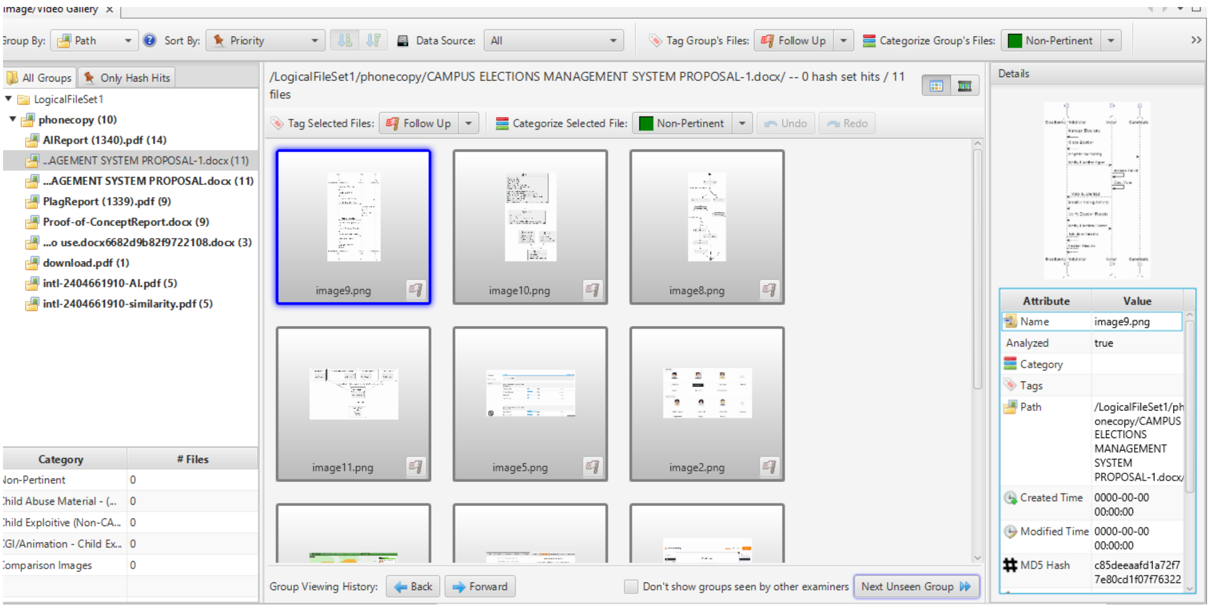
Category	# Files
Non-Pertinent	0
Child Abuse Material - (...	0
Child Exploitive (Non-CA...	0
CGI/Animation - Child Ex...	0
Comparison Images	0

Attribute	Value

Select a file to show its details here.

A closer analysis to one of the images (Image 9.png)

On the bottom right are the image details



Group By: Path · Sort By: Priority · Data Source: All · Tag Group's Files: Follow Up · Categorize Group's Files: Non-Pertinent

Tag Selected Files: Follow Up · Categorize Selected File: Non-Pertinent

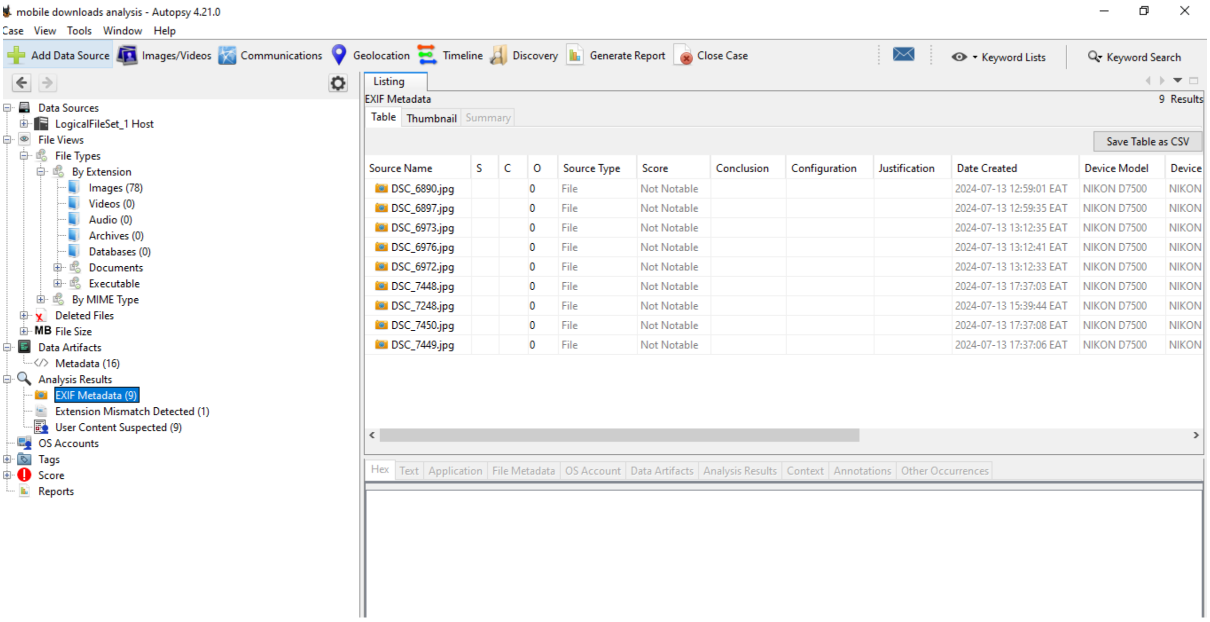
- LogicalFileSet1
  - phonecopy (10)
    - AIReport (1340).pdf (14)
    - ..AGEMENT SYSTEM PROPOSAL-1.docx (11)
    - ...AGEMENT SYSTEM PROPOSAL.docx (11)
    - PlagReport (1339).pdf (9)
    - Proof-of-ConceptReport.docx (9)
    - ...o use.docx6682d9b82f9722108.docx (3)
    - download.pdf (1)
    - intl-2404661910-AI.pdf (5)
    - intl-2404661910-similarity.pdf (5)

/LogicalFileSet1/phonecopy/CAMPUS ELECTIONS MANAGEMENT SYSTEM PROPOSAL-1.docx/ -- 0 hash set hits / 11 files

Category	# Files
Ion-Pertinent	0
hild Abuse Material - (...	0
hild Exploitive (Non-CA...	0
GI/Animation - Child Ex...	0
omparison Images	0

Attribute	Value
Name	image9.png
Analyzed	true
Category	
Tags	
Path	/LogicalFileSet1/phonecopy/CAMPUS ELECTIONS MANAGEMENT SYSTEM PROPOSAL-1.docx/
Created Time	0000-00-00 00:00:00
Modified Time	0000-00-00 00:00:00
MD5 Hash	c85deeaafd1a72f77e80cd1f07f76322

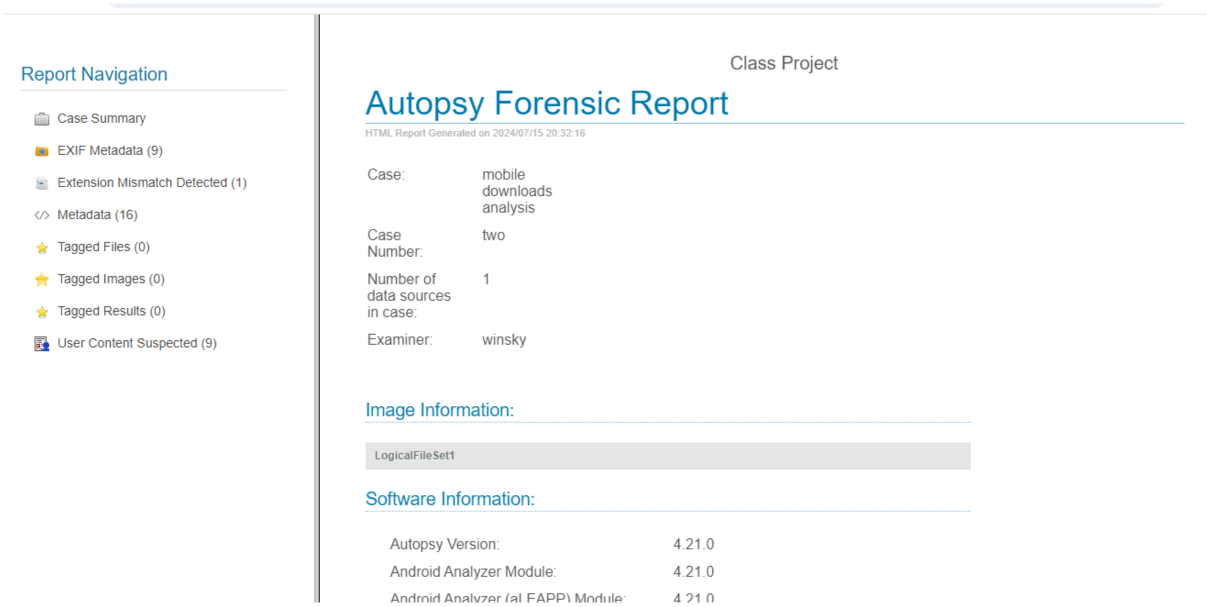
Further analysis



EXIF Metadata 9 Results

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	Device Model	Device
DSC_6890.jpg			0	File	Not Notable				2024-07-13 12:59:01 EAT	NIKON D7500	NIKON
DSC_6897.jpg			0	File	Not Notable				2024-07-13 12:59:35 EAT	NIKON D7500	NIKON
DSC_6973.jpg			0	File	Not Notable				2024-07-13 13:12:35 EAT	NIKON D7500	NIKON
DSC_6976.jpg			0	File	Not Notable				2024-07-13 13:12:41 EAT	NIKON D7500	NIKON
DSC_6972.jpg			0	File	Not Notable				2024-07-13 13:12:33 EAT	NIKON D7500	NIKON
DSC_7448.jpg			0	File	Not Notable				2024-07-13 17:37:03 EAT	NIKON D7500	NIKON
DSC_7248.jpg			0	File	Not Notable				2024-07-13 15:39:44 EAT	NIKON D7500	NIKON
DSC_7450.jpg			0	File	Not Notable				2024-07-13 17:37:08 EAT	NIKON D7500	NIKON
DSC_7449.jpg			0	File	Not Notable				2024-07-13 17:37:06 EAT	NIKON D7500	NIKON

The full details of the forensic report are in the html report generated.



Class Project

Autopsy Forensic Report

HTML Report Generated on 2024/07/15 20:32:16

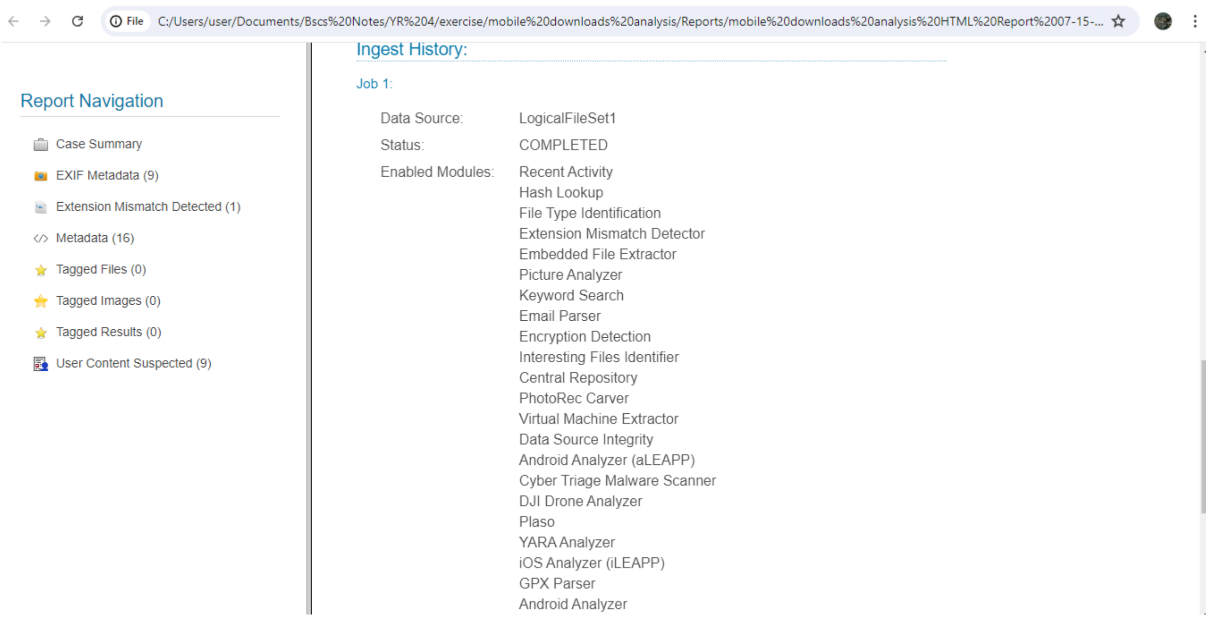
Case:	mobile downloads analysis
Case Number:	two
Number of data sources in case:	1
Examiner:	winsky

Image Information:

LogicalFileSet1

Software Information:

Autopsy Version:	4.21.0
Android Analyzer Module:	4.21.0
Android Analyzer (aLEAPP) Module:	4.21.0



C:/Users/user/Documents/Bscs%20Notes/YR%204/exercise/mobile%20downloads%20analysis/Reports/mobile%20downloads%20analysis%20HTML%20Report%2007-15-...

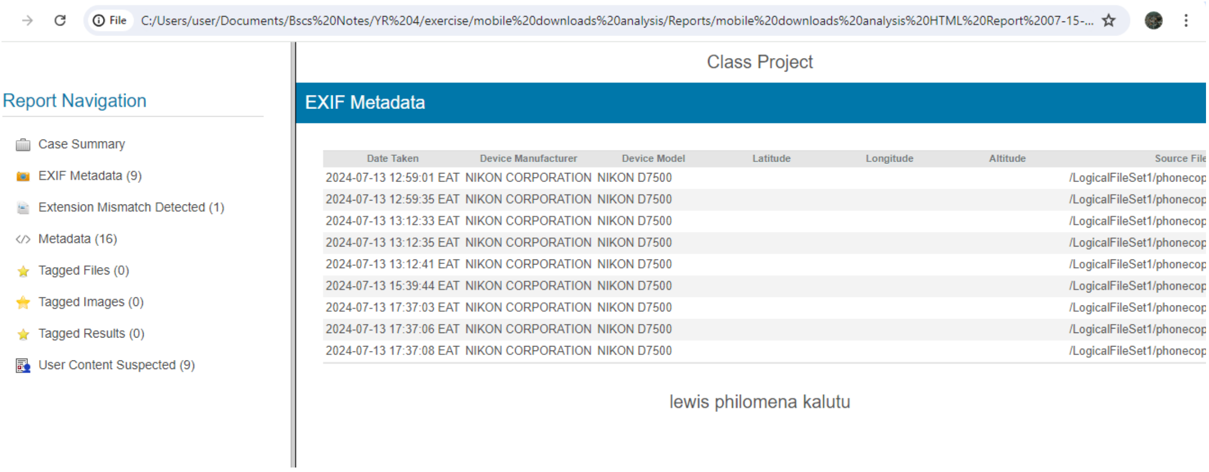
Report Navigation

- Case Summary
- EXIF Metadata (9)
- Extension Mismatch Detected (1)
- Metadata (16)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (9)

Ingest History:

Job 1:

Data Source:	LogicalFileSet1
Status:	COMPLETED
Enabled Modules:	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 Data Source Integrity Android Analyzer (aLEAPP) Cyber Triage Malware Scanner DJI Drone Analyzer Plaso YARA Analyzer iOS Analyzer (iLEAPP) GPX Parser Android Analyzer



C:/Users/user/Documents/Bscs%20Notes/YR%204/exercise/mobile%20downloads%20analysis/Reports/mobile%20downloads%20analysis%20HTML%20Report%2007-15-...

Report Navigation

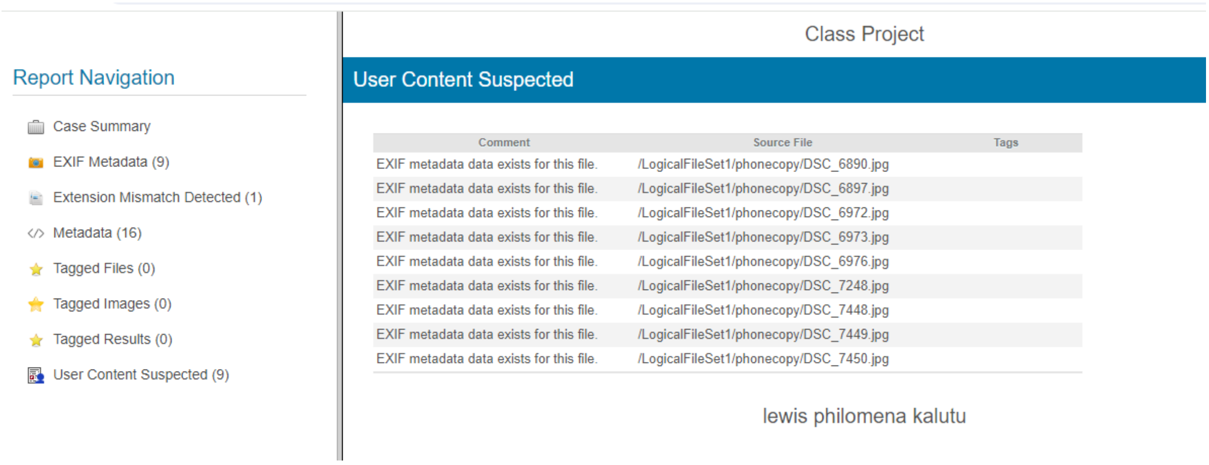
- Case Summary
- EXIF Metadata (9)
- Extension Mismatch Detected (1)
- Metadata (16)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (9)

Class Project

EXIF Metadata

Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File
2024-07-13 12:59:01 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 12:59:35 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 13:12:33 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 13:12:35 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 13:12:41 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 15:39:44 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 17:37:03 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 17:37:06 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop
2024-07-13 17:37:08 EAT	NIKON CORPORATION	NIKON D7500				/LogicalFileSet1/phonecop

lewis philomena kalutu



Report Navigation

- Case Summary
- EXIF Metadata (9)
- Extension Mismatch Detected (1)
- Metadata (16)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (9)

Class Project

User Content Suspected

Comment	Source File	Tags
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_6890.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_6897.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_6972.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_6973.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_6976.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_7248.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_7448.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_7449.jpg	
EXIF metadata data exists for this file.	/LogicalFileSet1/phonecopy/DSC_7450.jpg	

lewis philomena kalutu

The major challenge faced was gaining physical acquisition to the mobile device which requires rooting the device. The risk involved is that rooting the device deletes some of the device's data and it also takes a long time to create a copy of the phone depending on the manufacturer. For Redmi, Xiaomi takes as long as two days before granting full access. Also, majority of the forensic tools are not open source.

2. Network Monitoring Device Forensics Practical Assignment

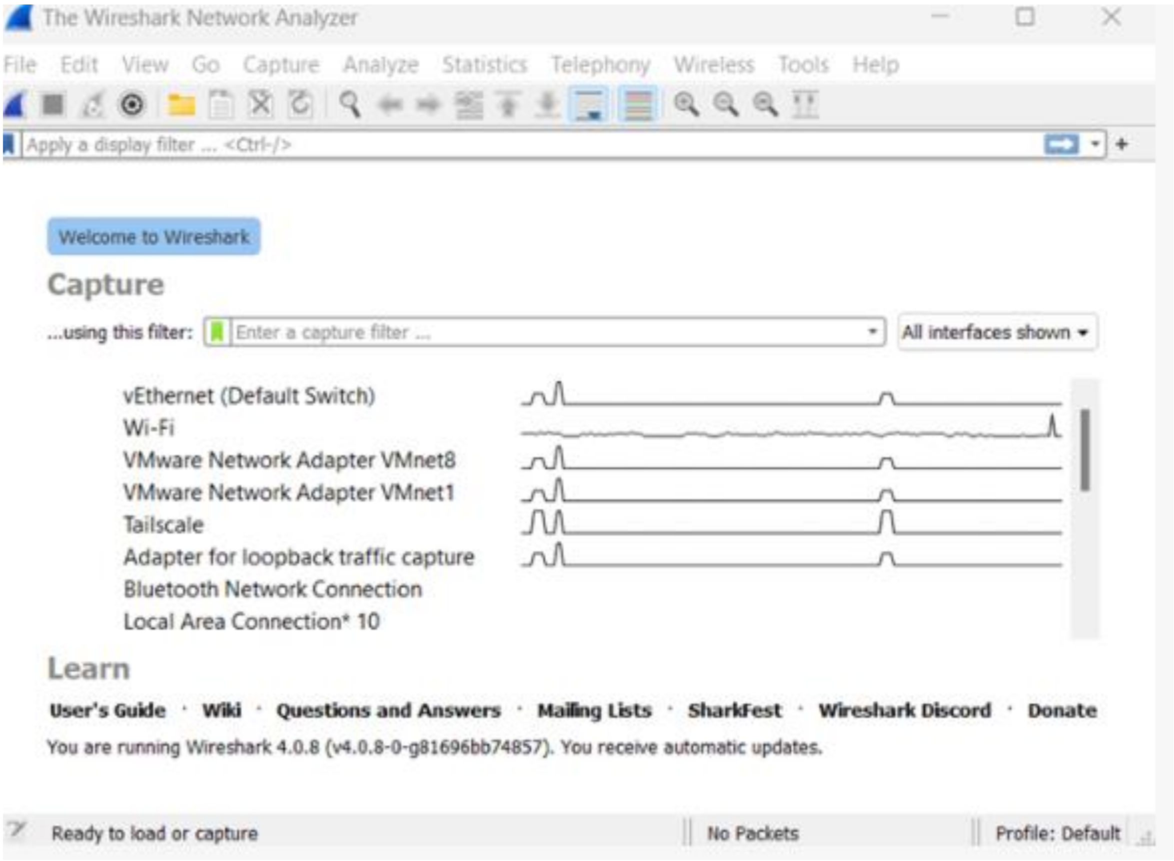
Objective:

To provide practical experience in network monitoring device forensics by performing forensic analysis on a network monitoring device, extracting data, and generating a comprehensive forensic report.

Initial Assessment

I have completed the necessary environment setup as follows:

Installed Forensic Software: Installed essential tools like Wireshark on my laptop.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
vEthernet (Default Switch)
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Tailscale
Adapter for loopback traffic capture
Bluetooth Network Connection
Local Area Connection* 10
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.8 (v4.0.8-0-g81696bb74857). You receive automatic updates.

Ready to load or capture

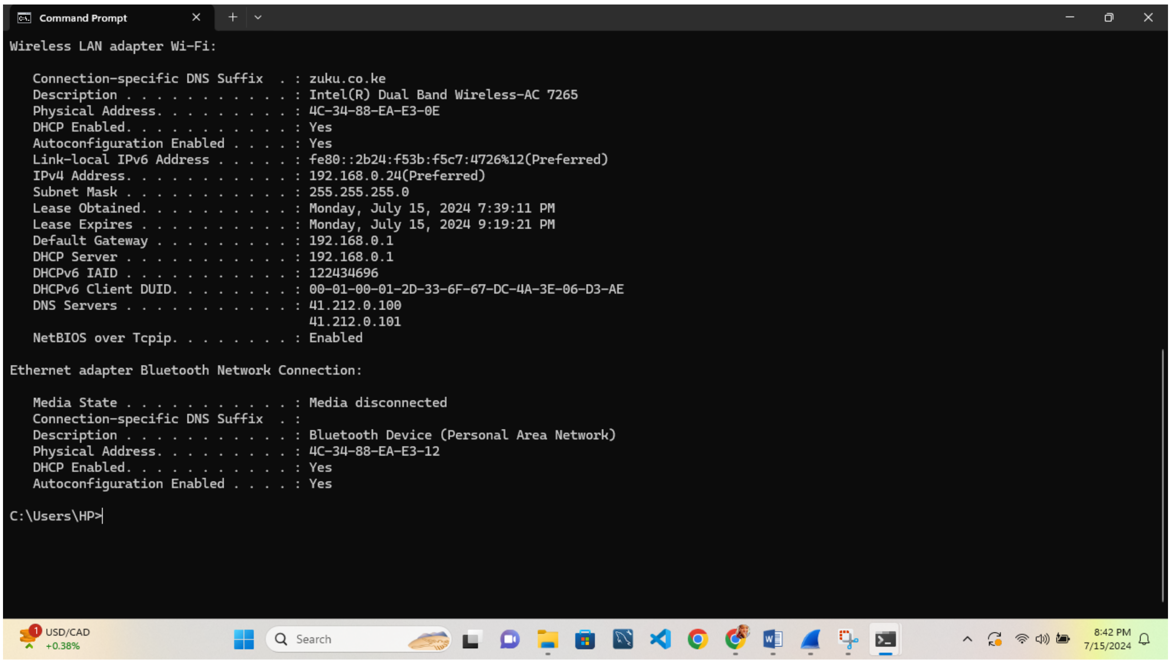
No Packets

Profile: Default

Network Monitoring Device Configuration:

Used the laptop as the network monitoring device.

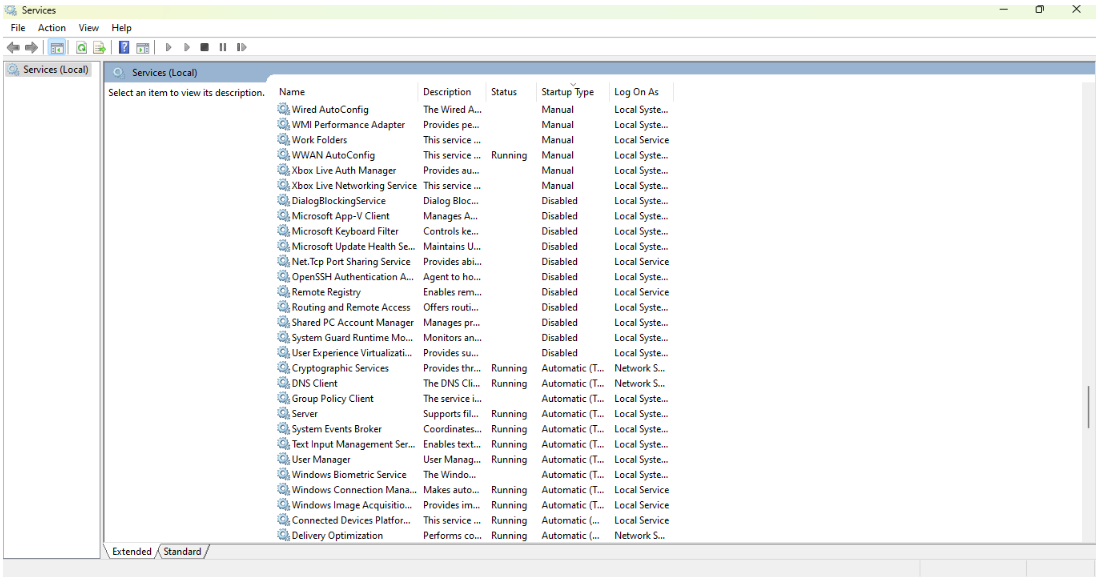
Verified network settings using the ipconfig command to confirm the correct configuration of IP address, subnet mask, default gateway, and DNS servers.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : zuku.co.ke
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Physical Address. . . . . . . . . : 4C-34-88-EA-E3-0E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2b24:f53b:f5c7:4726%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.24(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, July 15, 2024 7:39:11 PM
   Lease Expires . . . . . . . . . . : Monday, July 15, 2024 9:19:21 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 122434696
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-33-6F-67-DC-4A-3E-06-D3-AE
   DNS Servers . . . . . . . . . . . : 41.212.0.100
                                       41.212.0.101
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 4C-34-88-EA-E3-12
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\HP>
```

Secure and Isolated Environment:

Created a secure and isolated setup by disconnecting from external networks, disabling unnecessary services, and maintaining only essential connections for forensic analysis.



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Wired AutoConfig	The Wired A...		Manual	Local Syste...
WMI Performance Adapter	Provides pe...		Manual	Local Syste...
Work Folders	This service ...		Manual	Local Service
WWAN AutoConfig	This service ...	Running	Manual	Local Syste...
Xbox Live Auth Manager	Provides au...		Manual	Local Syste...
Xbox Live Networking Service	This service ...		Manual	Local Syste...
DialogBlockingService	Dialog Bloc...		Disabled	Local Syste...
Microsoft App-V Client	Manages A...		Disabled	Local Syste...
Microsoft Keyboard Filter	Controls ke...		Disabled	Local Syste...
Microsoft Update Health Se...	Maintains U...		Disabled	Local Syste...
Net.Tcp Port Sharing Service	Provides abi...		Disabled	Local Service
OpenSSH Authentication A...	Agent to ho...		Disabled	Local Syste...
Remote Registry	Enables rem...		Disabled	Local Service
Routing and Remote Access	Offers routi...		Disabled	Local Syste...
Shared PC Account Manager	Manages pr...		Disabled	Local Syste...
System Guard Runtime Mo...	Monitors an...		Disabled	Local Syste...
User Experience Virtualizati...	Provides su...		Disabled	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic (T...	Network S...
DNS Client	The DNS Cli...	Running	Automatic (T...	Network S...
Group Policy Client	The service i...		Automatic (T...	Local Syste...
Server	Supports fil...	Running	Automatic (T...	Local Syste...
System Events Broker	Coordinates...	Running	Automatic (T...	Local Syste...
Text Input Management Ser...	Enables text...	Running	Automatic (T...	Local Syste...
User Manager	User Manag...	Running	Automatic (T...	Local Syste...
Windows Biometric Service	The Windo...		Automatic (T...	Local Syste...
Windows Connection Mana...	Makes auto...	Running	Automatic (T...	Local Service
Windows Image Acquisitio...	Provides im...	Running	Automatic (T...	Local Service
Connected Devices Platfor...	This service ...	Running	Automatic (...	Local Service
Delivery Optimization	Performs co...	Running	Automatic (...	Network S...

Services Running

DHCP Client Service: Running (Service name: Dhcp)

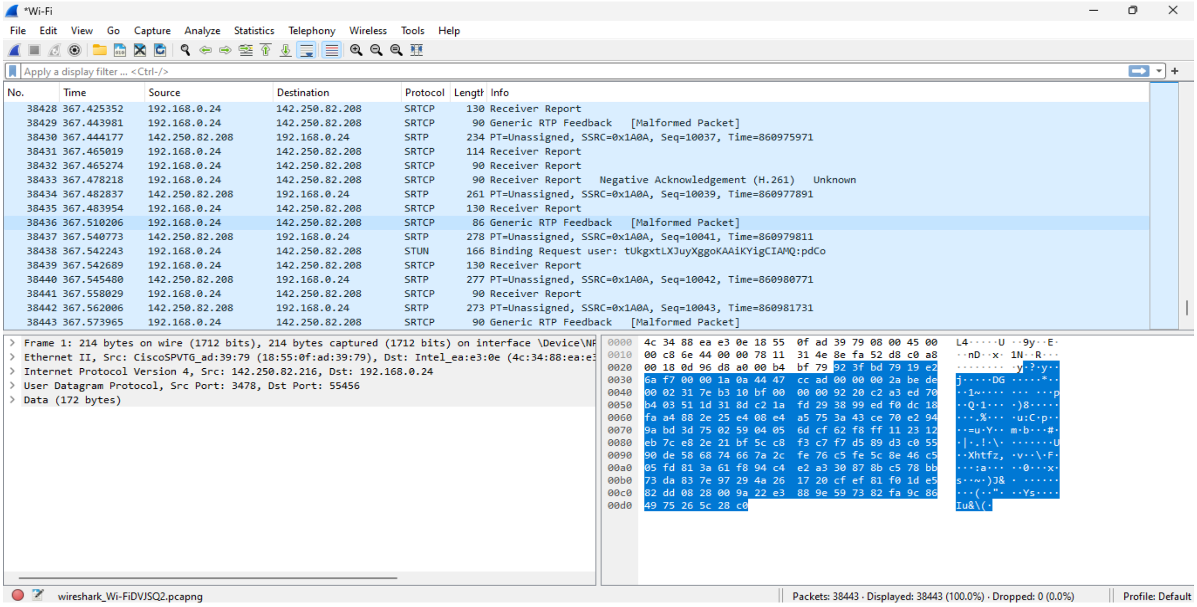
DNS Client Service: Running Service name: Dnscache

NetBIOS over Tcpip: Enabled

Task 2: Data Acquisition

Network Traffic Capture:

Launched Wireshark on the laptop to capture network traffic.
Recorded network activity for 30 minutes (Start Time: 8:10, End Time: 8:40).
Performed various network activities such as visiting websites (YouTube, Google) during the capture period.
Saved the captured traffic file for analysis.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time       Source          Destination     Protocol Length Info
  38428 367.425352 192.168.0.24    142.250.82.208  SRTCP    130 Receiver Report
  38429 367.443981 192.168.0.24    142.250.82.208  SRTCP     90 Generic RTP Feedback   [Malformed Packet]
  38430 367.444177 142.250.82.208  192.168.0.24    SRTP     234 PT=Unassigned, SSRC=0x1A0A, Seq=10037, Time=860975971
  38431 367.465019 192.168.0.24    142.250.82.208  SRTCP    114 Receiver Report
  38432 367.465274 192.168.0.24    142.250.82.208  SRTCP     90 Receiver Report
  38433 367.478218 192.168.0.24    142.250.82.208  SRTCP     90 Receiver Report   Negative Acknowledgement (H.261)   Unknown
  38434 367.482837 142.250.82.208  192.168.0.24    SRTP     261 PT=Unassigned, SSRC=0x1A0A, Seq=10039, Time=860977891
  38435 367.483954 192.168.0.24    142.250.82.208  SRTCP    130 Receiver Report
  38436 367.510206 192.168.0.24    142.250.82.208  SRTCP     86 Generic RTP Feedback   [Malformed Packet]
  38437 367.540773 142.250.82.208  192.168.0.24    SRTP     278 PT=Unassigned, SSRC=0x1A0A, Seq=10041, Time=860979811
  38438 367.542243 192.168.0.24    142.250.82.208  STUN     166 Binding Request user: tUkgxtLXJuyXggoKAAiKYigCIAMQ:pdCo
  38439 367.542689 192.168.0.24    142.250.82.208  SRTCP    130 Receiver Report
  38440 367.545480 142.250.82.208  192.168.0.24    SRTP     277 PT=Unassigned, SSRC=0x1A0A, Seq=10042, Time=860980771
  38441 367.558029 192.168.0.24    142.250.82.208  SRTCP     90 Receiver Report
  38442 367.562006 142.250.82.208  192.168.0.24    SRTP     273 PT=Unassigned, SSRC=0x1A0A, Seq=10043, Time=860981731
  38443 367.573965 192.168.0.24    142.250.82.208  SRTCP     90 Generic RTP Feedback   [Malformed Packet]
```

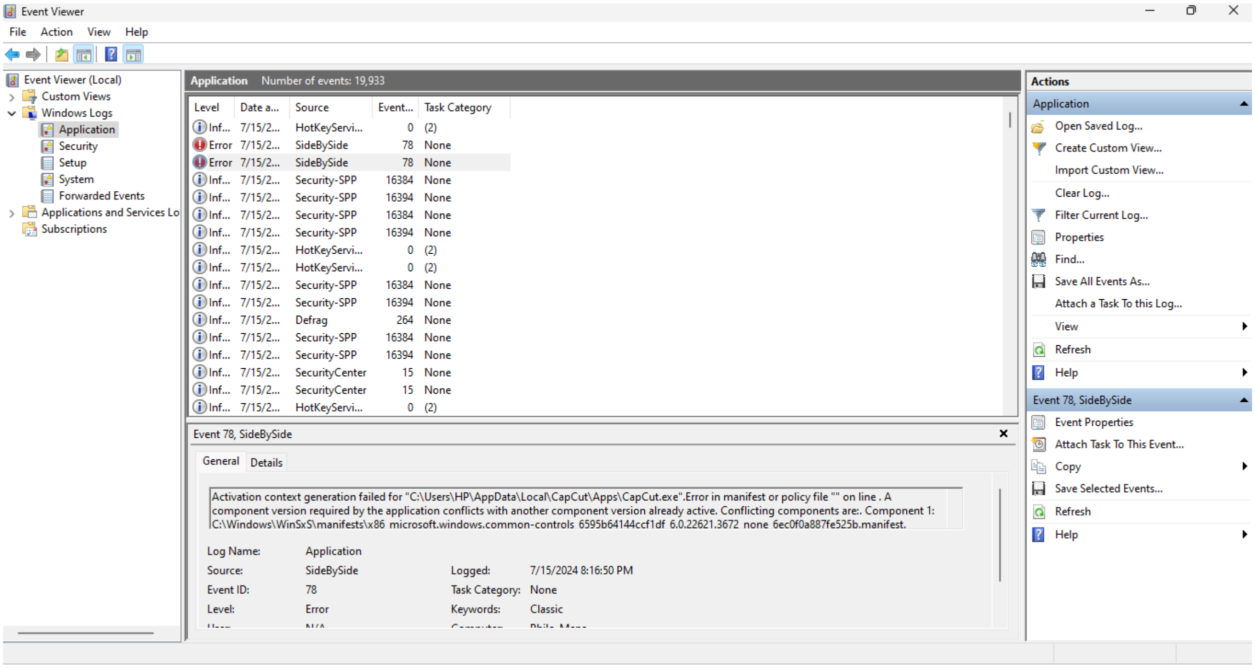
```
> Frame 1: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \Device\NF
> Ethernet II, Src: CiscoSPVTG_ad:39:79 (18:55:0f:ad:39:79), Dst: Intel_ea:e3:0e (4c:34:88:ea:e3
> Internet Protocol Version 4, Src: 142.250.82.216, Dst: 192.168.0.24
> User Datagram Protocol, Src Port: 3478, Dst Port: 55456
> Data (172 bytes)
```

```
0000  4c 34 88 ea e3 0e 18 55  0f ad 39 79 08 00 45 00   L4·····U ··9y··E·
0010  00 c8 6e 44 00 00 78 11  31 4e 8e fa 52 d8 c0 a8   ··nD··x· 1N··R···
0020  00 18 0d 96 d8 a0 00 b4  bf 79 92 3f bd 79 19 e2   ········ ·y·?·y··
0030  6a f7 00 00 1a 0a 44 47  cc ad 00 00 00 2a be de   j·····DG ·····*··
0040  00 02 31 7e b3 10 bf 00  00 00 92 20 c2 a3 ed 70   ··1~···· ··· ···p
0050  b4 03 51 1d 31 8d c2 1a  fd 29 38 99 ed f0 dc 18   ··Q·1··· ·)8·····
0060  fa a4 88 2e 25 e4 08 e4  a5 75 3a 43 ce 70 e2 94   ····.%··· ·u:C·p··
0070  9a bd 3d 75 02 59 04 05  6d cf 62 f8 ff 11 23 12   ··=u·Y·· m·b···#·
0080  eb 7c e8 2e 21 bf 5c c8  f3 c7 f7 d5 89 d3 c0 55   ·|·.!·\· ·······U
0090  90 de 58 68 74 66 7a 2c  fe 76 c5 fe 5c 8e 46 c5   ··Xhtfz, ·v··\·F·
00a0  05 fd 81 3a 61 f8 94 c4  e2 a3 30 87 8b c5 78 bb   ···:a··· ··0···x·
00b0  73 da 83 7e 97 29 4a 26  17 20 cf ef 81 f0 1d e5   s··~·)J& · ······
00c0  82 dd 08 28 00 9a 22 e3  88 9e 59 73 82 fa 9c 86   ···(··"· ··Ys····
00d0  49 75 26 5c 28 c0                                  Iu&\(·
```

wireshark_Wi-FiDVJSQ2.pcapng | Packets: 38443 · Displayed: 38443 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Log File Extraction:

- Accessed Windows Event Viewer to extract relevant log files, including application event logs.
- Saved the log files securely for further analysis.



Application Number of events: 19,933

Level	Date a...	Source	Event...	Task Category
Inf...	7/15/2...	HotKeyServi...	0	(2)
Error	7/15/2...	SideBySide	78	None
Error	7/15/2...	SideBySide	78	None
Inf...	7/15/2...	Security-SPP	16384	None
Inf...	7/15/2...	Security-SPP	16394	None
Inf...	7/15/2...	Security-SPP	16384	None
Inf...	7/15/2...	Security-SPP	16394	None
Inf...	7/15/2...	HotKeyServi...	0	(2)
Inf...	7/15/2...	HotKeyServi...	0	(2)
Inf...	7/15/2...	Security-SPP	16384	None
Inf...	7/15/2...	Security-SPP	16394	None
Inf...	7/15/2...	Defrag	264	None
Inf...	7/15/2...	Security-SPP	16384	None
Inf...	7/15/2...	Security-SPP	16394	None
Inf...	7/15/2...	SecurityCenter	15	None
Inf...	7/15/2...	SecurityCenter	15	None
Inf...	7/15/2...	HotKeyServi...	0	(2)

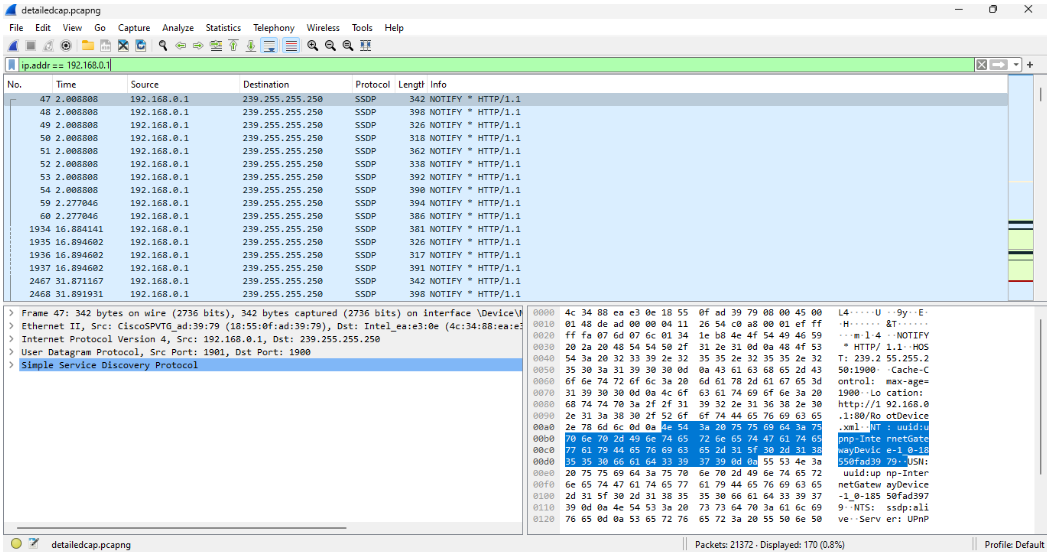
Event 78, SideBySide

```
Activation context generation failed for "C:\Users\HP\AppData\Local\CapCut\Apps\CapCut.exe".Error in manifest or policy file "" on line . A
component version required by the application conflicts with another component version already active. Conflicting components are:. Component 1:
C:\Windows\WinSxS\manifests\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.22621.3672_none_6ec0f0a887fe525b.manifest.
```

Log Name:	Application		
Source:	SideBySide	Logged:	7/15/2024 8:16:50 PM
Event ID:	78	Task Category:	None
Level:	Error	Keywords:	Classic

Task 3: Data Analysis

Opened the captured network traffic file in Wireshark.
Defined a capture filter to focus on specific IP addresses and ports to capture relevant traffic.
IP Address Filters: Filter packets based on specific IP addresses in this picture, we used (ip.addr == 192.168.0.1)


detailedcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.1

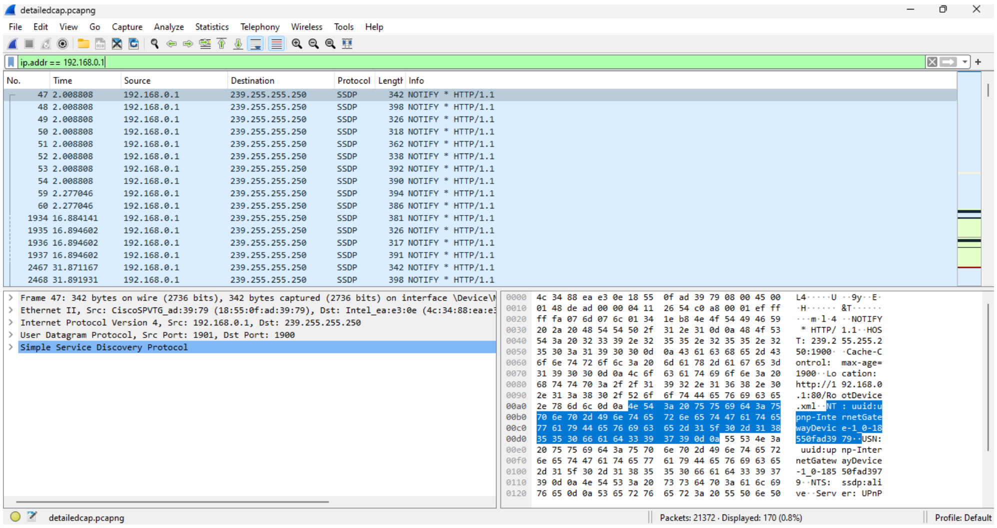
```
No.   Time       Source        Destination       Protocol Length Info
   47 2.008808   192.168.0.1   239.255.255.250   SSDP     342 NOTIFY * HTTP/1.1
   48 2.008808   192.168.0.1   239.255.255.250   SSDP     398 NOTIFY * HTTP/1.1
   49 2.008808   192.168.0.1   239.255.255.250   SSDP     326 NOTIFY * HTTP/1.1
   50 2.008808   192.168.0.1   239.255.255.250   SSDP     318 NOTIFY * HTTP/1.1
   51 2.008808   192.168.0.1   239.255.255.250   SSDP     362 NOTIFY * HTTP/1.1
   52 2.008808   192.168.0.1   239.255.255.250   SSDP     338 NOTIFY * HTTP/1.1
   53 2.008808   192.168.0.1   239.255.255.250   SSDP     392 NOTIFY * HTTP/1.1
   54 2.008808   192.168.0.1   239.255.255.250   SSDP     390 NOTIFY * HTTP/1.1
   59 2.277046   192.168.0.1   239.255.255.250   SSDP     394 NOTIFY * HTTP/1.1
   60 2.277046   192.168.0.1   239.255.255.250   SSDP     386 NOTIFY * HTTP/1.1
 1934 16.884141  192.168.0.1   239.255.255.250   SSDP     381 NOTIFY * HTTP/1.1
 1935 16.894602  192.168.0.1   239.255.255.250   SSDP     326 NOTIFY * HTTP/1.1
 1936 16.894602  192.168.0.1   239.255.255.250   SSDP     317 NOTIFY * HTTP/1.1
 1937 16.894602  192.168.0.1   239.255.255.250   SSDP     391 NOTIFY * HTTP/1.1
 2467 31.871167  192.168.0.1   239.255.255.250   SSDP     342 NOTIFY * HTTP/1.1
 2468 31.891931  192.168.0.1   239.255.255.250   SSDP     398 NOTIFY * HTTP/1.1
```

```
> Frame 47: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\N
> Ethernet II, Src: CiscoSPVTG_ad:39:79 (18:55:0f:ad:39:79), Dst: Intel_ea:e3:0e (4c:34:88:ea:e3
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 1901, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  4c 34 88 ea e3 0e 18 55  0f ad 39 79 08 00 45 00   L4·····U ··9y··E·
0010  01 48 de ad 00 00 04 11  26 54 c0 a8 00 01 ef ff   ·H······ &T······
0020  ff fa 07 6d 07 6c 01 34  1e b8 4e 4f 54 49 46 59   ···m·l·4 ··NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 4f 53    * HTTP/ 1.1··HOS
0040  54 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   T: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 61 63 68 65 2d 43   50:1900· ·Cache-C
0060  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
0070  31 39 30 30 0d 0a 4c 6f  63 61 74 69 6f 6e 3a 20   1900··Lo cation: 
0080  68 74 74 70 3a 2f 2f 31  39 32 2e 31 36 38 2e 30   http://1 92.168.0
0090  2e 31 3a 38 30 2f 52 6f  6f 74 44 65 76 69 63 65   .1:80/Ro otDevice
00a0  2e 78 6d 6c 0d 0a 4e 54  3a 20 75 75 69 64 3a 75   .xml··NT : uuid:u
00b0  70 6e 70 2d 49 6e 74 65  72 6e 65 74 47 61 74 65   pnp-Inte rnetGate
00c0  77 61 79 44 65 76 69 63  65 2d 31 5f 30 2d 31 38   wayDevic e-1_0-18
00d0  35 35 30 66 61 64 33 39  37 39 0d 0a 55 53 4e 3a   550fad39 79··USN:
00e0  20 75 75 69 64 3a 75 70  6e 70 2d 49 6e 74 65 72    uuid:up np-Inter
00f0  6e 65 74 47 61 74 65 77  61 79 44 65 76 69 63 65   netGatew ayDevice
0100  2d 31 5f 30 2d 31 38 35  35 30 66 61 64 33 39 37   -1_0-185 50fad397
0110  39 0d 0a 4e 54 53 3a 20  73 73 64 70 3a 61 6c 69   9··NTS:  ssdp:ali
0120  76 65 0d 0a 53 65 72 76  65 72 3a 20 55 50 6e 50   ve··Serv er: UPnP
```

detailedcap.pcapng | Packets: 21372 · Displayed: 170 (0.8%) | Profile: Default

Port Filters: Filter packets based on specific port numbers.


detailedcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.1

No.	Time	Source	Destination	Protocol	Length	Info
47	2.008808	192.168.0.1	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
48	2.008808	192.168.0.1	239.255.255.250	SSDP	398	NOTIFY * HTTP/1.1
49	2.008808	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
50	2.008808	192.168.0.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
51	2.008808	192.168.0.1	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
52	2.008808	192.168.0.1	239.255.255.250	SSDP	338	NOTIFY * HTTP/1.1
53	2.008808	192.168.0.1	239.255.255.250	SSDP	392	NOTIFY * HTTP/1.1
54	2.008808	192.168.0.1	239.255.255.250	SSDP	390	NOTIFY * HTTP/1.1
59	2.277046	192.168.0.1	239.255.255.250	SSDP	394	NOTIFY * HTTP/1.1
60	2.277046	192.168.0.1	239.255.255.250	SSDP	386	NOTIFY * HTTP/1.1
1934	16.884141	192.168.0.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
1935	16.894602	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
1936	16.894602	192.168.0.1	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
1937	16.894602	192.168.0.1	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
2467	31.871167	192.168.0.1	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
2468	31.891931	192.168.0.1	239.255.255.250	SSDP	398	NOTIFY * HTTP/1.1

```
> Frame 47: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\N
> Ethernet II, Src: CiscoSPVTG_ad:39:79 (18:55:0f:ad:39:79), Dst: Intel_ea:e3:0e (4c:34:88:ea:e3
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 1901, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  4c 34 88 ea e3 0e 18 55  0f ad 39 79 08 00 45 00   L4·····U ··9y··E·
0010  01 48 de ad 00 00 04 11  26 54 c0 a8 00 01 ef ff   ·H······ &T······
0020  ff fa 07 6d 07 6c 01 34  1e b8 4e 4f 54 49 46 59   ···m·l·4 ··NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 4f 53    * HTTP/ 1.1··HOS
0040  54 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   T: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 61 63 68 65 2d 43   50:1900· ·Cache-C
0060  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
0070  31 39 30 30 0d 0a 4c 6f  63 61 74 69 6f 6e 3a 20   1900··Lo cation: 
0080  68 74 74 70 3a 2f 2f 31  39 32 2e 31 36 38 2e 30   http://1 92.168.0
0090  2e 31 3a 38 30 2f 52 6f  6f 74 44 65 76 69 63 65   .1:80/Ro otDevice
00a0  2e 78 6d 6c 0d 0a 4e 54  3a 20 75 75 69 64 3a 75   .xml··NT : uuid:u
00b0  70 6e 70 2d 49 6e 74 65  72 6e 65 74 47 61 74 65   pnp-Inte rnetGate
00c0  77 61 79 44 65 76 69 63  65 2d 31 5f 30 2d 31 38   wayDevic e-1_0-18
00d0  35 35 30 66 61 64 33 39  37 39 0d 0a 55 53 4e 3a   550fad39 79··USN:
00e0  20 75 75 69 64 3a 75 70  6e 70 2d 49 6e 74 65 72    uuid:up np-Inter
00f0  6e 65 74 47 61 74 65 77  61 79 44 65 76 69 63 65   netGatew ayDevice
0100  2d 31 5f 30 2d 31 38 35  35 30 66 61 64 33 39 37   -1_0-185 50fad397
0110  39 0d 0a 4e 54 53 3a 20  73 73 64 70 3a 61 6c 69   9··NTS:  ssdp:ali
0120  76 65 0d 0a 53 65 72 76  65 72 3a 20 55 50 6e 50   ve··Serv er: UPnP
```

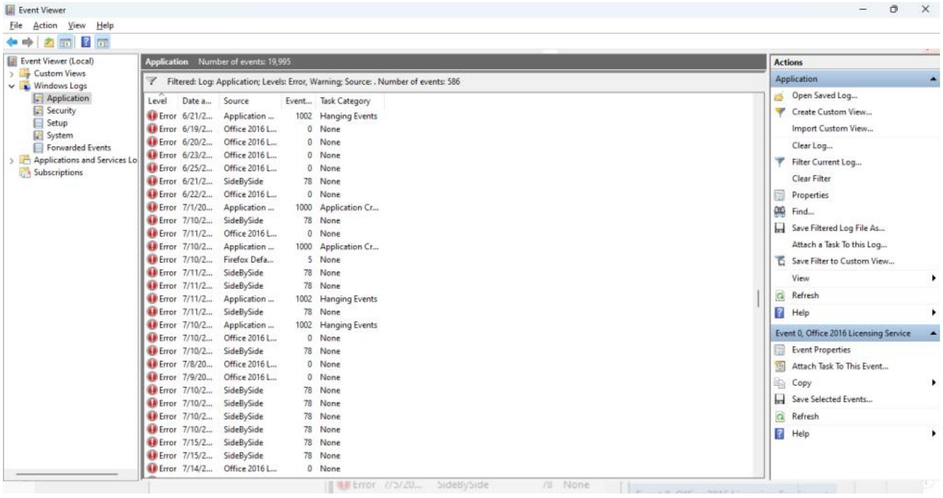
detailedcap.pcapng | Packets: 21372 · Displayed: 170 (0.8%) | Profile: Default

Log Analysis:

Navigate to your saved log file and open it.

Opened the saved application log using Windows Event Viewer.

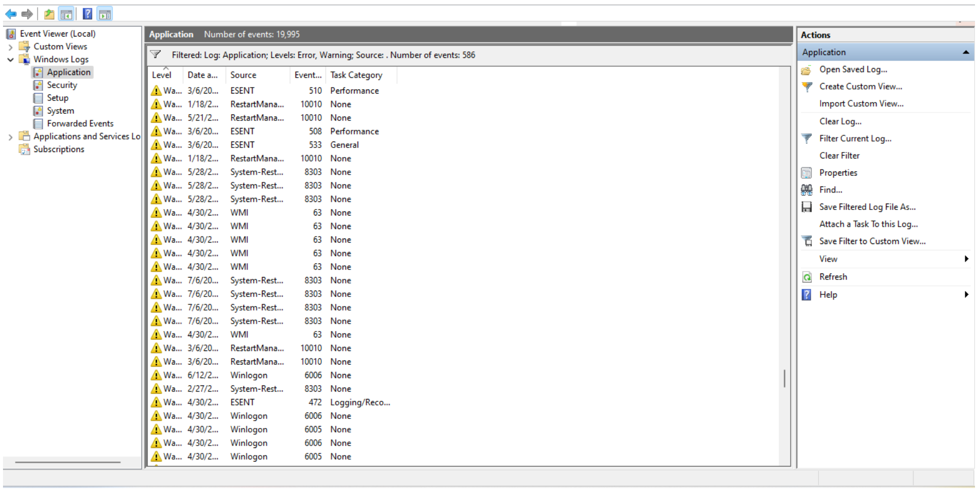
Filtered the log to focus on errors and warnings.



Application Number of events: 19,995

Filtered: Log: Application; Levels: Error, Warning; Source: . Number of events: 586

Level	Date a...	Source	Event...	Task Category
Error	6/21/2...	Application ...	1002	Hanging Events
Error	6/19/2...	Office 2016 L...	0	None
Error	6/20/2...	Office 2016 L...	0	None
Error	6/23/2...	Office 2016 L...	0	None
Error	6/25/2...	Office 2016 L...	0	None
Error	6/21/2...	SideBySide	78	None
Error	6/22/2...	Office 2016 L...	0	None
Error	7/1/20...	Application ...	1000	Application Cr...
Error	7/10/2...	SideBySide	78	None
Error	7/11/2...	Office 2016 L...	0	None
Error	7/10/2...	Application ...	1000	Application Cr...
Error	7/10/2...	Firefox Defa...	5	None
Error	7/11/2...	SideBySide	78	None
Error	7/11/2...	SideBySide	78	None
Error	7/11/2...	Application ...	1002	Hanging Events
Error	7/11/2...	SideBySide	78	None
Error	7/10/2...	Application ...	1002	Hanging Events
Error	7/10/2...	Office 2016 L...	0	None
Error	7/10/2...	SideBySide	78	None
Error	7/8/20...	Office 2016 L...	0	None
Error	7/9/20...	Office 2016 L...	0	None
Error	7/10/2...	SideBySide	78	None
Error	7/10/2...	SideBySide	78	None
Error	7/10/2...	SideBySide	78	None
Error	7/10/2...	SideBySide	78	None
Error	7/15/2...	SideBySide	78	None
Error	7/15/2...	SideBySide	78	None
Error	7/14/2...	Office 2016 L...	0	None



Application Number of events: 19,995

Filtered: Log: Application; Levels: Error, Warning; Source: . Number of events: 586

Level	Date a...	Source	Event...	Task Category
Wa...	3/6/20...	ESENT	510	Performance
Wa...	1/18/2...	RestartMana...	10010	None
Wa...	5/21/2...	RestartMana...	10010	None
Wa...	3/6/20...	ESENT	508	Performance
Wa...	3/6/20...	ESENT	533	General
Wa...	1/18/2...	RestartMana...	10010	None
Wa...	5/28/2...	System-Rest...	8303	None
Wa...	5/28/2...	System-Rest...	8303	None
Wa...	5/28/2...	System-Rest...	8303	None
Wa...	4/30/2...	WMI	63	None
Wa...	4/30/2...	WMI	63	None
Wa...	4/30/2...	WMI	63	None
Wa...	4/30/2...	WMI	63	None
Wa...	4/30/2...	WMI	63	None
Wa...	7/6/20...	System-Rest...	8303	None
Wa...	7/6/20...	System-Rest...	8303	None
Wa...	7/6/20...	System-Rest...	8303	None
Wa...	7/6/20...	System-Rest...	8303	None
Wa...	4/30/2...	WMI	63	None
Wa...	3/6/20...	RestartMana...	10010	None
Wa...	3/6/20...	RestartMana...	10010	None
Wa...	6/12/2...	Winlogon	6006	None
Wa...	2/27/2...	System-Rest...	8303	None
Wa...	4/30/2...	ESENT	472	Logging/Reco...
Wa...	4/30/2...	Winlogon	6006	None
Wa...	4/30/2...	Winlogon	6005	None
Wa...	4/30/2...	Winlogon	6006	None
Wa...	4/30/2...	Winlogon	6005	None

Task 4: Reporting

Introduction

The objective of this assignment was to perform network monitoring device forensics using my laptop as the target device. This report summarizes the findings from the analysis of network traffic, log files, and configuration settings.

Methodology

Steps Taken During Acquisition and Analysis:

Installed Wireshark on my laptop to capture network traffic.

Extracted log files related to firewall and system events.

Reviewed network configuration settings stored on my laptop.

Tools and Techniques Used:

Wireshark for network traffic analysis.

Windows Event Viewer for system log analysis.

Manual inspection of network configuration settings.

Data Extraction and Analysis

Results of Data Extraction:

Captured network traffic using Wireshark for a period of 30 minutes.

Extracted firewall log files from Windows Event Viewer.

Results of Data Analysis:

Identified multiple connections to external IP addresses during the capture period.

Detected several failed login attempts and firewall rule violations in the log files.

Findings and Observations

Screenshots of Important Evidence:

Observed Security Incidents or Vulnerabilities:

3 Forensic Tools to Recover Deleted Files Practical Assignment

Objective:

To gain hands-on experience in using forensic tools to recover deleted files from various storage media, analyze the recovered data, and document findings in a comprehensive report.

Detailed Findings

1. Preparation

Environment Setup: FTK Imager was installed, and a write-blocker was used.

Storage Media Documentation: Type: USB Drive, Capacity: 16GB.

Hash Creation and Verification:

- MD5: 8422ff9ea5239ae65406862967e7bcec
- SHA1: cd3ed33e0e68feecb62203dc9cd8c273f60e21f2

2. Data Acquisition

- Forensic Image Creation: Using FTK Imager.
- Integrity Verification: Hash values matched original.
- Documentation: Screenshots of acquisition process.

3. Data Recovery

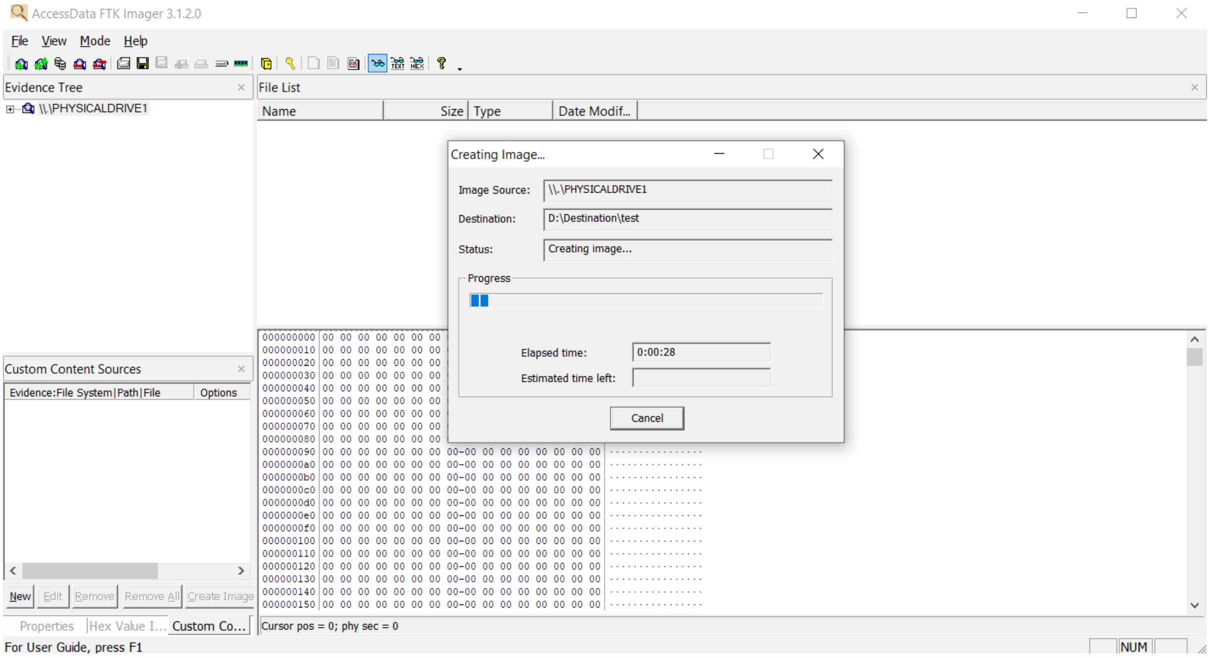
- Image Loading: Forensic image loaded into FTK Imager.
- Unallocated Space Navigation: Identified and recovered deleted files.
- File Recovery: Files recovered and documented.

4. Data Analysis

- File Relevance and Significance Analysis:
  - Documents: Confidential report with proprietary data.
  - Images: Personal photos, no investigation relevance.

Screenshots of Important Evidence:

Create Disk Image:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: D:\Destination\test

Status: Creating image...

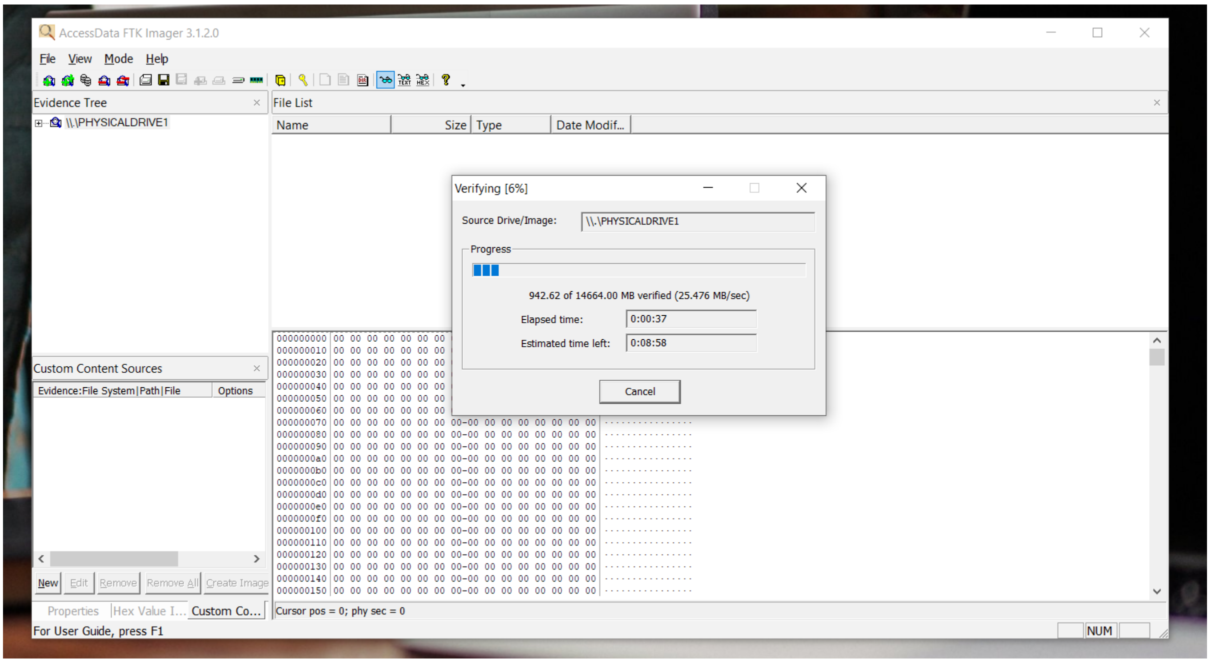
Elapsed time: 0:00:28

Estimated time left:

Cursor pos = 0; phy sec = 0

For User Guide, press F1

Generate Hashing:



Verifying [6%]

Source Drive/Image: \\.\PHYSICALDRIVE1

942.62 of 14664.00 MB verified (25.476 MB/sec)

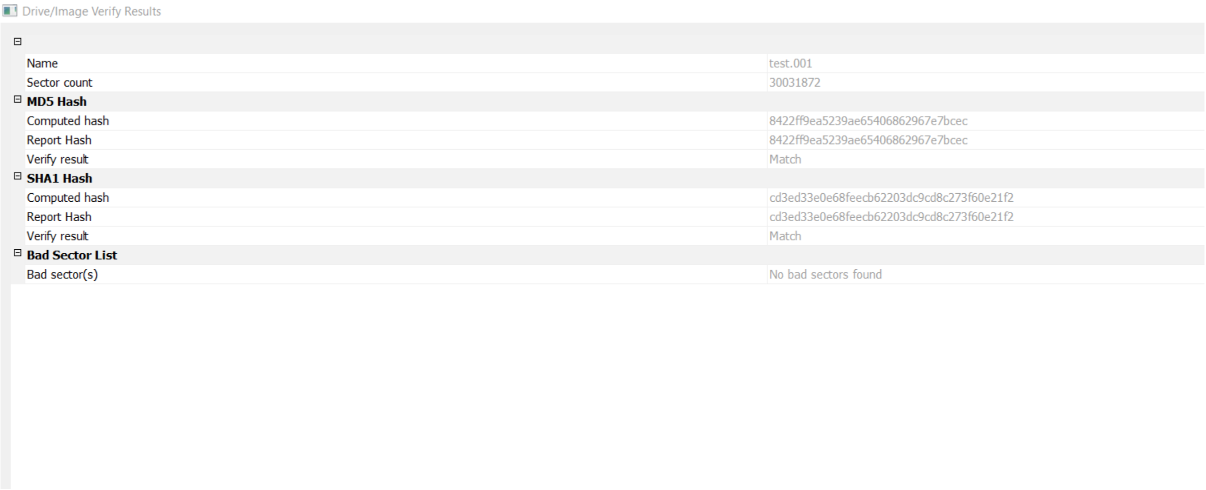
Elapsed time: 0:00:37

Estimated time left: 0:08:58

Cursor pos = 0; phy sec = 0

For User Guide, press F1

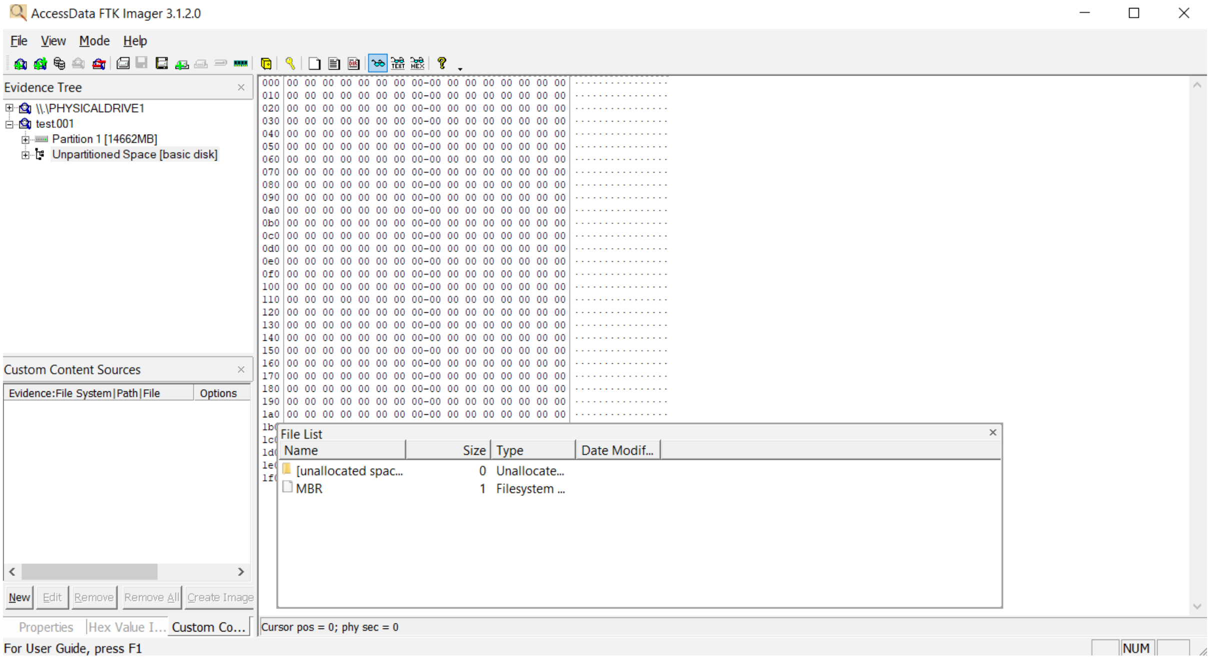
Hash Match:



Drive/Image Verify Results

Name	test.001
Sector count	30031872
MD5 Hash	
Computed hash	8422ff9ea5239ae65406862967e7bcec
Report Hash	8422ff9ea5239ae65406862967e7bcec
Verify result	Match
SHA1 Hash	
Computed hash	cd3ed33e0e68feecb62203dc9cd8c273f60e21f2
Report Hash	cd3ed33e0e68feecb62203dc9cd8c273f60e21f2
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Unallocated Space Navigation



AccessData FTK Imager 3.1.2.0

Evidence Tree

- \\.\PHYSICALDRIVE1
- test.001
  - Partition 1 [14662MB]
  - Unpartitioned Space [basic disk]

```
000 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
1a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
1b
1c
1d
1e
1f
```

File List

Name	Size	Type	Date Modif...
[unallocated spac...	0	Unallocate...	
MBR	1	Filesystem ...	

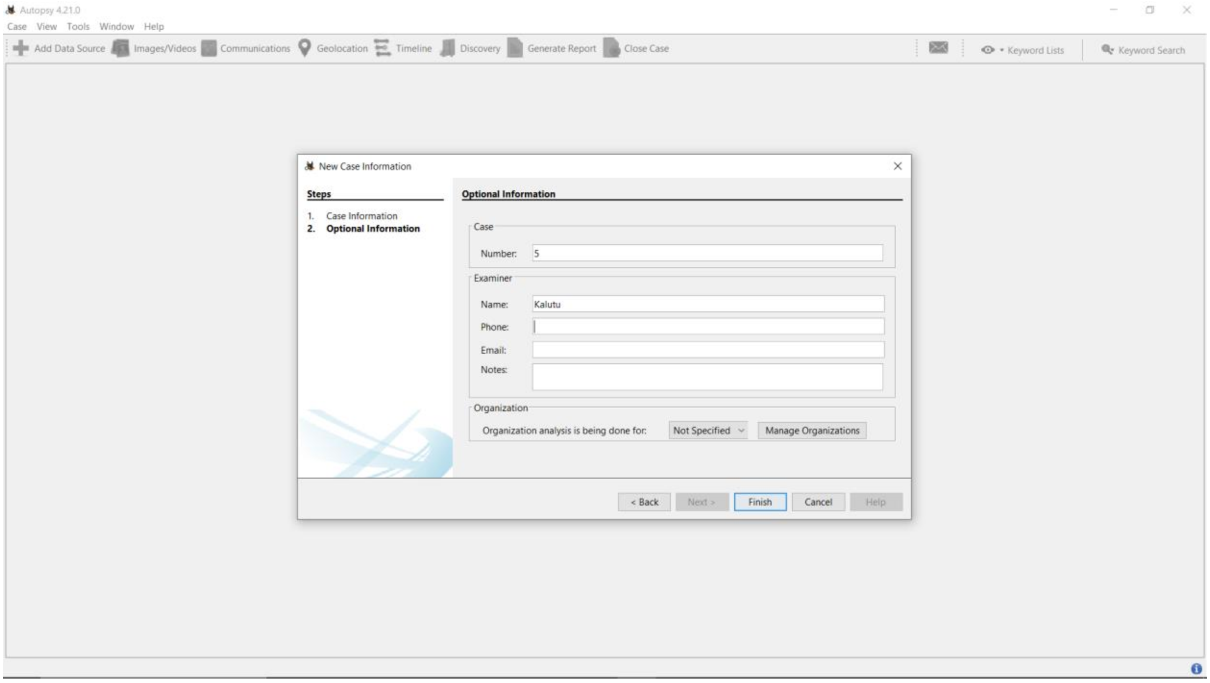
Custom Content Sources

Evidence:File System|Path|File	Options

Cursor pos = 0; phy sec = 0

For User Guide, press F1

Create Case Autopsy



Case

Number: 5

Examiner

Name: Kalutu

Phone:

Email:

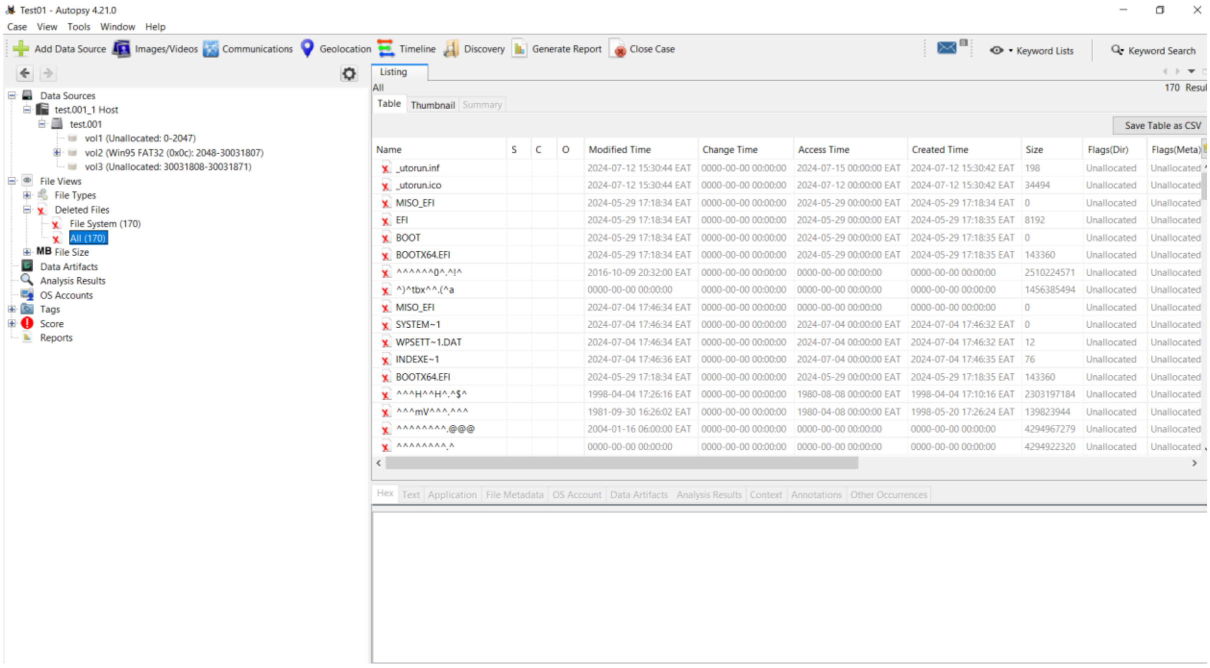
Notes:

Organization

Organization analysis is being done for: Not Specified

Manage Organizations

Recover Deleted Files



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
_utorun.inf				2024-07-12 15:30:44 EAT	0000-00-00 00:00:00	2024-07-15 00:00:00 EAT	2024-07-12 15:30:42 EAT	198	Unallocated	Unallocated
_utorun.ico				2024-07-12 15:30:44 EAT	0000-00-00 00:00:00	2024-07-12 00:00:00 EAT	2024-07-12 15:30:42 EAT	34494	Unallocated	Unallocated
MISO_EFI				2024-05-29 17:18:34 EAT	0000-00-00 00:00:00	2024-05-29 00:00:00 EAT	2024-05-29 17:18:34 EAT	0	Unallocated	Unallocated
EFI				2024-05-29 17:18:34 EAT	0000-00-00 00:00:00	2024-05-29 00:00:00 EAT	2024-05-29 17:18:35 EAT	8192	Unallocated	Unallocated
BOOT				2024-05-29 17:18:34 EAT	0000-00-00 00:00:00	2024-05-29 00:00:00 EAT	2024-05-29 17:18:35 EAT	0	Unallocated	Unallocated
BOOTX64.EFI				2024-05-29 17:18:34 EAT	0000-00-00 00:00:00	2024-05-29 00:00:00 EAT	2024-05-29 17:18:35 EAT	143360	Unallocated	Unallocated
^^^^^^0^.^!^				2016-10-09 20:32:00 EAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2510224571	Unallocated	Unallocated
^)^tbx^^.(^a				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1456385494	Unallocated	Unallocated
MISO_EFI				2024-07-04 17:46:34 EAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated
SYSTEM~1				2024-07-04 17:46:34 EAT	0000-00-00 00:00:00	2024-07-04 00:00:00 EAT	2024-07-04 17:46:32 EAT	0	Unallocated	Unallocated
WPSETT~1.DAT				2024-07-04 17:46:34 EAT	0000-00-00 00:00:00	2024-07-04 00:00:00 EAT	2024-07-04 17:46:32 EAT	12	Unallocated	Unallocated
INDEXE~1				2024-07-04 17:46:36 EAT	0000-00-00 00:00:00	2024-07-04 00:00:00 EAT	2024-07-04 17:46:35 EAT	76	Unallocated	Unallocated
BOOTX64.EFI				2024-05-29 17:18:34 EAT	0000-00-00 00:00:00	2024-05-29 00:00:00 EAT	2024-05-29 17:18:35 EAT	143360	Unallocated	Unallocated
^^^H^^H^.^$^				1998-04-04 17:26:16 EAT	0000-00-00 00:00:00	1980-08-08 00:00:00 EAT	1998-04-04 17:10:16 EAT	2303197184	Unallocated	Unallocated
^^^mV^^^.^^^				1981-09-30 16:26:02 EAT	0000-00-00 00:00:00	1980-04-08 00:00:00 EAT	1998-05-20 17:26:24 EAT	139823944	Unallocated	Unallocated
^^^^^^^^.@@@				2004-01-16 06:00:00 EAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4294967279	Unallocated	Unallocated
^^^^^^^^.^				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4294922320	Unallocated	Unallocated