



# USE AUTOPSY TO INVESTIGATE A SYSTEM

This document demonstrates the use of Autopsy to see the contents of a disk image file and investigate it.

Jordan Patterson

## Table of Contents

Lab Objective:.....	2
When was the OS built? .....	2
Who are the admin users?.....	3
What profile preferences can you find for the users? Name the file and preferences. ....	5
What applications were installed in 2023? .....	6
Name the files over 1GB in size and their locations.....	7
Device ID of virtual mouse .....	9
What was downloaded?.....	10
Where is consent? .....	12

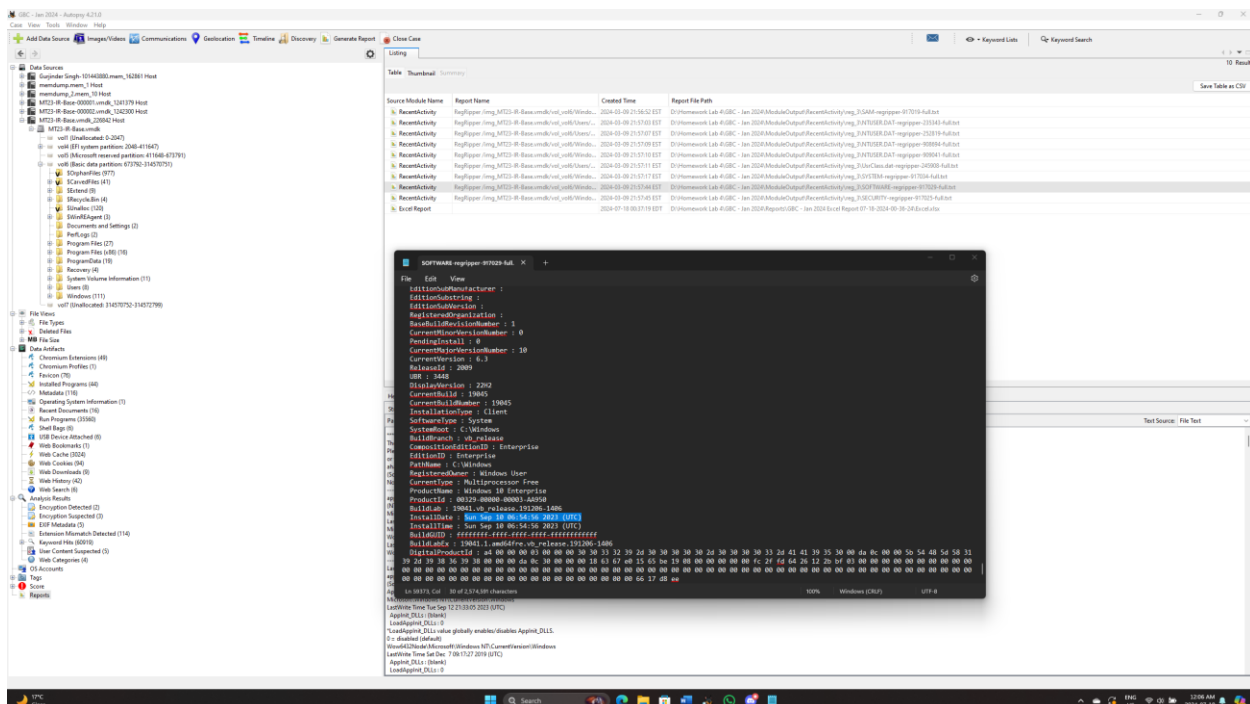
## Lab Objective:

Use Autopsy to open the provided Autopsy case and answer the following questions.

1. When was the OS built?
2. Who are the admin users?
3. What profile preferences can you find for the users? Name the file and preferences.
4. What applications were installed in 2023?
5. Name the files over 1GB in size and their locations
6. Device ID of virtual mouse
7. What was downloaded?
8. Where is consent?

## When was the OS built?

My first thought was to check the Registry for this information. Because I did not have the original .VMDK associated with this autopsy file, I could not extract the registry and simply view it. Luckily Autopsy generated a report under the reports tab where I was able to open the SOFTWARE regripper report and view its contents. The report was 84 pages in autopsy so to make it easier to search I opened it in notepad. In the report I found that the OS was built on **Sun Sep 10 06:54:56 2023 (UTC)**



# Who are the admin users?

I started by going to the “OS Accounts” tab of Autopsy. This revealed a mix of service, default, and user created accounts. 12 in total. I went through each account and found that the service accounts, while possibly performing administrative windows functions did not have passwords and could not be logged into like regular user accounts. This left me with 5 other accounts to investigate.

MjolnirTraining: This account was active and had been used 12 times.

WDAGUtilityAccount: This account was Disabled and had never been used.

DefaultAccount: This account was Disabled and had never been used.

Administrator: This account was Disabled and had never been used.

Guest: This account was Disabled and had never been used.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
SYSTEM	0	0	0	SYSTEM	MT23-08-Base.vmdk_22642	Local	NT SERVICE	
MjolnirTraining	0	0	0	MjolnirTraining	MT23-08-Base.vmdk_22642	Host	Domain	2023-09-10 02:54:54 EDT
LOCAL SERVICE	0	0	0	LOCAL SERVICE	MT23-08-Base.vmdk_22642	Host	Local	
NETWORK SERVICE	0	0	0	NETWORK SERVICE	MT23-08-Base.vmdk_22642	Host	Local	
WDAGUtilityAccount	0	0	0	WDAGUtilityAccount	MT23-08-Base.vmdk_22642	Host	Domain	2023-09-10 02:54:54 EDT
DefaultAccount	0	0	0	DefaultAccount	MT23-08-Base.vmdk_22642	Host	Domain	2023-09-10 02:54:54 EDT
Administrator	0	0	0	Administrator	MT23-08-Base.vmdk_22642	Host	Domain	2023-09-10 02:54:54 EDT
Guest	0	0	0	Guest	MT23-08-Base.vmdk_22642	Host	Domain	2023-09-10 02:54:54 EDT

**Basic Properties**

Account: Administrator

Full Name: S-1-5-21-127520102-276888805-348440740-500

Address: 2023-09-10 02:54:54 EDT

Type: 128881

**MjolnirTraining: 22642 Host Details**

Login Count: 0

Description: Built-in account for administering the computer/domain

Password Settings: Password does not expire

Account Settings: Account Disabled

Flag: Normal user account

**Realm Properties**

Name: Unknown

Address: S-1-5-21-127520102-276888805-348440740

Scope: Domain

Confidence: Known

At this stage I was still unsure as to which accounts may be in the Administrators group, so I once again turned to the registry by using the Reports tab of Autopsy. This time I opened the SAM (security Account Manager) regripper report.

As seen in the screenshot above, these SID's correspond to **MjolnirTraining and Administrator**. This group membership makes these two accounts admin users, although the Administrator account is disabled.



# What profile preferences can you find for the users? Name the file and preferences.

The file containing user preferences is named **NTUSER.DAT** and can be found in the user folder of each user. For example, for MjolnirTraining the file would be located at C:\Users\MjolnirTraining\NTUSER.DAT.

This file contains preferences related to power settings, network connections, application settings, and other customizations such as the cursor size, font size, etc.

The screenshot displays a forensic analysis interface. On the left, a file tree shows the directory structure of a drive, with 'NTUSER.DAT' highlighted under the 'Users' folder. The main pane shows a detailed list of files and folders. The file 'NTUSER.DAT' is selected, and its details are shown in the right pane. The file is located at 'C:\Users\MjolnirTraining\NTUSER.DAT' and has a size of 1,187,000 bytes. The file is marked as 'Allocated' and 'Known'. The interface also includes a search bar at the top and a bottom status bar.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(DI)	Flags(MI)	Known	Location	MFT Hash
Current Folder				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-10-07 06:10:52 EDT	2019-12-07 04:03:44 EST	56	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Application Data				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Cookies				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Local Settings				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
My Documents				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Network				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Recent				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
SentTo				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Start Menu				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Templates				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	48	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
NTUSER.DAT				2023-09-17 20:01:04 EDT	2023-09-17 20:01:04 EDT	2023-09-17 20:01:04 EDT	2023-09-17 20:01:04 EDT	1,187,000	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	44047403002711141056C66b0c...
NTUSER.DAT.LOG1				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	1,969,000	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	44047403002711141056C66b0c...
NTUSER.DAT\3b3b3b3b-1644-11ea-af11-00155d000000				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-17 20:01:04 EDT	2023-09-10 12:54:58 EDT	5,042,000	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	362236032009143546c0e013af794d...
NTUSER.DAT\3b3b3b3b-1644-11ea-af11-00155d000000				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	5,042,000	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	362236032009143546c0e013af794d...
3D Objects				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	152	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Contexts				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	152	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Documents				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	56	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Links				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	480	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Music				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	152	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Saved Games				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	152	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
Templates				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-17 20:01:04 EDT	2023-09-10 12:54:58 EDT	392	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	
NTUSER.DAT\3b3b3b3b-1644-11ea-af11-00155d000000				2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	2023-09-10 12:54:58 EDT	693,000	Allocated	Allocated	unknown	\\jing.MT23-R-Basic\mnt\vol_005\Users\MjolnirTraining\...	3647779760d0c1d4e4770d0d0c1d4e4...

# What applications were installed in 2023?

To determine which applications were installed in 2023 I navigated to “Installed Programs” under Autopsy’s Data Artifacts tab. I then sorted the applications by date. The Programs installed in 2023 are the following:

Microsoft Edge Update v.1.3.177.11

Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127 v.14.24.28127

Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.24.28127 v.14.24.28127.4

Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127 v.14.24.28127

VMware Tools v.11.1.5.16724464

7-Zip 23.01 (x64) v.23.01

Notepad++ (64-bit x64) v.8.5.7

Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 v.14.36.32532

Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 v.14.36.32532.0

Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 v.14.36.32532

Npcap v.1.71

Process Hacker 2.39 (r124) v.2.39.0.124

Wireshark 4.0.8 64-bit v.4.0.8

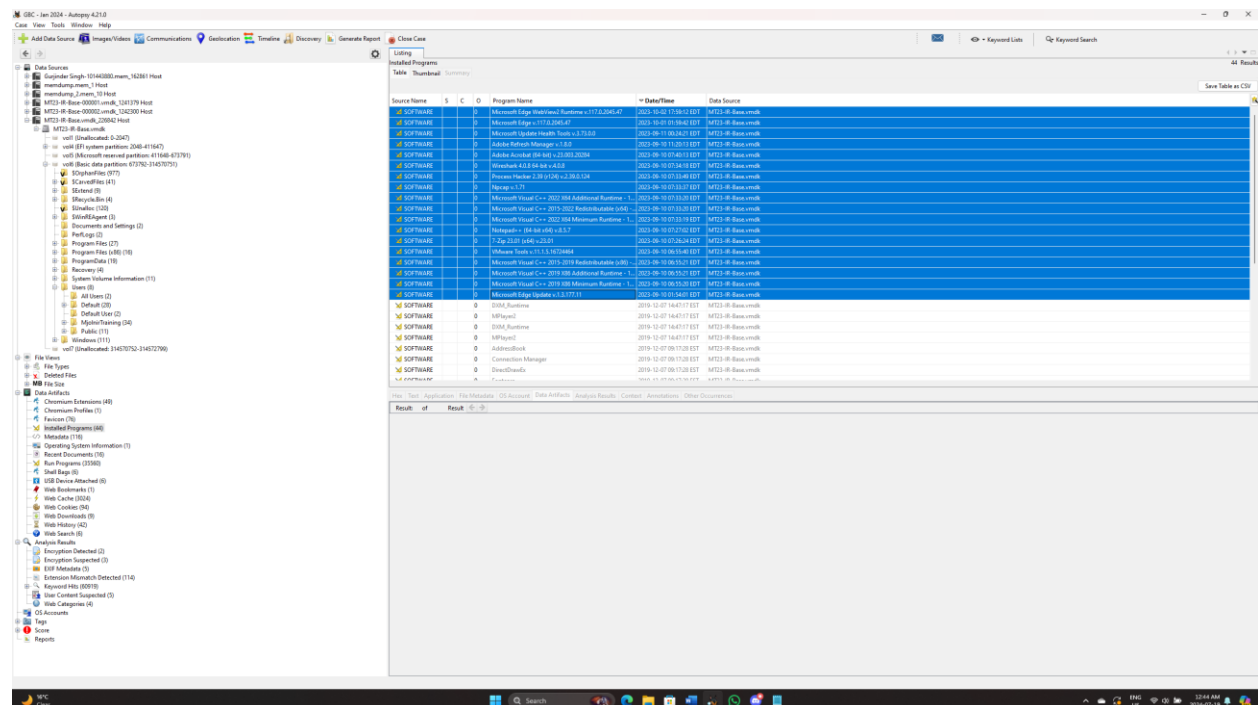
Adobe Acrobat (64-bit) v.23.003.20284

Adobe Refresh Manager v.1.8.0

Microsoft Update Health Tools v.3.73.0.0

Microsoft Edge v.117.0.2045.47

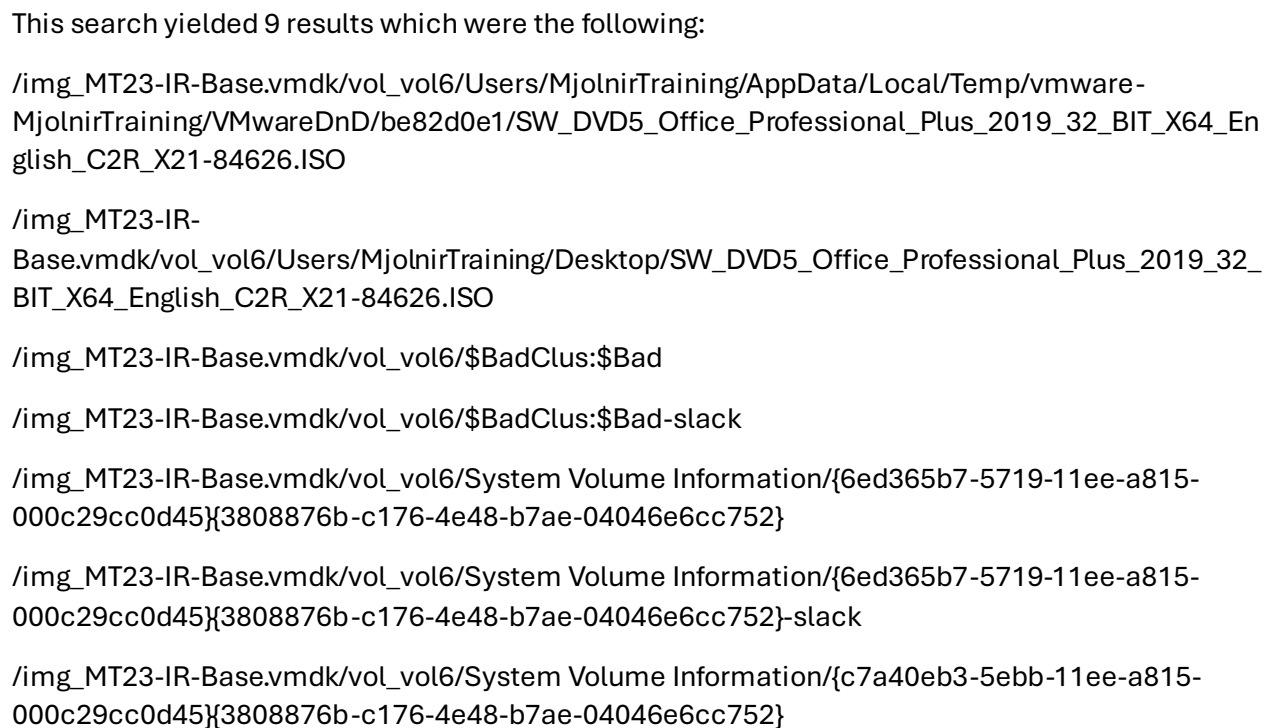
Microsoft Edge WebView2 Runtime v.117.0.2045.47



The screenshot shows the Autopsy 4.21.0 interface with the 'Installed Programs' table selected. The table is sorted by 'Date/Time' in descending order. The left sidebar shows the 'Data Sources' tree with 'Data Artifacts' expanded. The bottom status bar shows the system clock as 12:44 AM on 10/10/23.

Source Name	S	C	O	Program Name	Date/Time	Data Source
Microsoft Edge (v117.0.2045.47)	0	0	0	Microsoft Edge (v117.0.2045.47)	2023-10-10 12:44:01	Microsoft Edge (v117.0.2045.47)
Microsoft Visual C++ 2019 X86 Minimum Runtime	0	0	0	Microsoft Visual C++ 2019 X86 Minimum Runtime	2023-10-10 12:44:01	Microsoft Visual C++ 2019 X86 Minimum Runtime
Microsoft Visual C++ 2015-2019 Redistributable (x86)	0	0	0	Microsoft Visual C++ 2015-2019 Redistributable (x86)	2023-10-10 12:44:01	Microsoft Visual C++ 2015-2019 Redistributable (x86)
Microsoft Visual C++ 2019 X86 Additional Runtime	0	0	0	Microsoft Visual C++ 2019 X86 Additional Runtime	2023-10-10 12:44:01	Microsoft Visual C++ 2019 X86 Additional Runtime
VMware Tools	0	0	0	VMware Tools	2023-10-10 12:44:01	VMware Tools
7-Zip	0	0	0	7-Zip	2023-10-10 12:44:01	7-Zip
Notepad++	0	0	0	Notepad++	2023-10-10 12:44:01	Notepad++
Microsoft Visual C++ 2022 X64 Minimum Runtime	0	0	0	Microsoft Visual C++ 2022 X64 Minimum Runtime	2023-10-10 12:44:01	Microsoft Visual C++ 2022 X64 Minimum Runtime
Microsoft Visual C++ 2015-2022 Redistributable (x64)	0	0	0	Microsoft Visual C++ 2015-2022 Redistributable (x64)	2023-10-10 12:44:01	Microsoft Visual C++ 2015-2022 Redistributable (x64)
Microsoft Visual C++ 2022 X64 Additional Runtime	0	0	0	Microsoft Visual C++ 2022 X64 Additional Runtime	2023-10-10 12:44:01	Microsoft Visual C++ 2022 X64 Additional Runtime
Npcap	0	0	0	Npcap	2023-10-10 12:44:01	Npcap
Process Hacker	0	0	0	Process Hacker	2023-10-10 12:44:01	Process Hacker
Wireshark	0	0	0	Wireshark	2023-10-10 12:44:01	Wireshark
Adobe Acrobat	0	0	0	Adobe Acrobat	2023-10-10 12:44:01	Adobe Acrobat
Adobe Refresh Manager	0	0	0	Adobe Refresh Manager	2023-10-10 12:44:01	Adobe Refresh Manager
Microsoft Update Health Tools	0	0	0	Microsoft Update Health Tools	2023-10-10 12:44:01	Microsoft Update Health Tools
Microsoft Edge	0	0	0	Microsoft Edge	2023-10-10 12:44:01	Microsoft Edge
Microsoft Edge WebView2 Runtime	0	0	0	Microsoft Edge WebView2 Runtime	2023-10-10 12:44:01	Microsoft Edge WebView2 Runtime

To determine which files were over 1GB in size, I ran a “File Search by Attributes” in Autopsy and set the criteria to show me all files that were greater than 1GB in size and their locations.





```
/img_MT23-IR-Base.vmdk/vol_vol6/System Volume Information/{c7a40eb3-5ebb-11ee-a815-000c29cc0d45}{3808876b-c176-4e48-b7ae-04046e6cc752}-slack
```

/img\_MT23-IR-Base.vmdk/vol\_vol6/pagefile.sys

Office Professional Plus appears twice because it is stored on the desktop of the MjolnirTraining user as well as MjolnirTraining's AppData/Local/Temp folder. There is also a pagefile which is acting as an extension of the systems memory. The remaining 6 files are a little more ambiguous. After some preliminary research it seems they may relate to the disks system volume information or shadow copy's.

[illegible]

# Device ID of virtual mouse

Under Data Artifacts, in the USB Device Attached section of Autopsy there are 3 virtual mice identified, each with their own Device ID.

The ID's are:

6&30c5d09c&0&5

7&3ae26960&0&0000

7&3ae26960&0&0001

The screenshot displays the Autopsy 4.21.0 interface. On the left, the 'Data Sources' pane shows a tree view of the file system, including folders like 'System', 'Users', and 'Windows'. The 'Data Artifacts' pane on the right is expanded to 'USB Device Attached', showing a table of artifacts. The table has columns for 'Type', 'Date/Time', 'Device Name', 'Device Model', 'Device ID', and 'Data Source'. Three entries are listed, all of type 'Virtual Mouse' and dated '2023-09-17 20:01:19 EDT'. The Device IDs are '6&30c5d09c&0&5', '7&3ae26960&0&0000', and '7&3ae26960&0&0001'. Below the table, the 'Details' pane shows the 'Source File Path' for the selected artifact: 'C:\Users\user\AppData\Local\Microsoft\Windows\UsbDfs\6&30c5d09c&0&5'.

Type	Date/Time	Device Name	Device Model	Device ID	Data Source
Virtual Mouse	2023-09-17 20:01:19 EDT	ROOT\HUB	58391983A0	6&30c5d09c&0&5	MT23-R-Basic-mouse
Virtual Mouse	2023-09-17 20:01:19 EDT	ROOT\HUB	58391983A0	7&3ae26960&0&0000	MT23-R-Basic-mouse
Virtual Mouse	2023-09-17 20:01:19 EDT	Microsoft, Inc.	683C5495A003	7&3ae26960&0&0001	MT23-R-Basic-mouse

File Path	Source File Path
C:\Users\user\AppData\Local\Microsoft\Windows\UsbDfs\6&30c5d09c&0&5	C:\Users\user\AppData\Local\Microsoft\Windows\UsbDfs\6&30c5d09c&0&5

# What was downloaded?

To find the download items I went into Autopsy's Web Downloads section under Data Artifacts, there were 9 results. Notepad++, Process Hacker, and FTK Imager each show up twice on this list either with a different source URL or download location.

The items that were downloaded were:

## Notepad++

File name: npp.8.5.7.Installer.x64.exe

Source URL: <https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.5.7/npp.8.5.7.Installer.x64.exe>

## Notepad++

File name: npp.8.5.7.Installer.x64.exe

Source URL: [https://objects.githubusercontent.com/github-production-release-asset-2e65be/33014811/186dac6d-40eb-4f23-a13f-c186cab20dc4?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230910%2Fus-east-1%2Fs3%2Faws4\\_request&X-Amz-Date=20230910T072605Z&X-Amz-Expires=300&X-Amz-Signature=d88e30421e3bfd20052ca1fa96eec2da8fe92f70ead2c840e385bfe4ef3bcb79&X-Amz-SignedHeaders=host&actor\\_id=0&key\\_id=0&repo\\_id=33014811&response-content-disposition=attachment%3B%20filename%3Dnpp.8.5.7.Installer.x64.exe&response-content-type=application%2Foctet-stream](https://objects.githubusercontent.com/github-production-release-asset-2e65be/33014811/186dac6d-40eb-4f23-a13f-c186cab20dc4?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230910%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230910T072605Z&X-Amz-Expires=300&X-Amz-Signature=d88e30421e3bfd20052ca1fa96eec2da8fe92f70ead2c840e385bfe4ef3bcb79&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=33014811&response-content-disposition=attachment%3B%20filename%3Dnpp.8.5.7.Installer.x64.exe&response-content-type=application%2Foctet-stream)

## Process Hacker

File name: processhacker-2.39-setup.exe

Source URL: [https://downloads.sourceforge.net/project/processhacker/processhacker2/processhacker-2.39-setup.exe?ts=gAAAAABk\\_XDc1PaaW5XTD07woulqRtOLxjJi8wzH6GGv9fRCKvN9IC1izrTELMz\\_Jm2CL4\\_AjMQ0PcUp985qYEKLa1gp2fNkkg%3D%3D&use\\_mirror=cfhcable&r=https%3A%2F%2Fprocesshacker.sourceforge.io%2F](https://downloads.sourceforge.net/project/processhacker/processhacker2/processhacker-2.39-setup.exe?ts=gAAAAABk_XDc1PaaW5XTD07woulqRtOLxjJi8wzH6GGv9fRCKvN9IC1izrTELMz_Jm2CL4_AjMQ0PcUp985qYEKLa1gp2fNkkg%3D%3D&use_mirror=cfhcable&r=https%3A%2F%2Fprocesshacker.sourceforge.io%2F)

## Process Hacker

File name: processhacker-2.39-setup.exe

Source URL: <https://cfhcable.dl.sourceforge.net/project/processhacker/processhacker2/processhacker-2.39-setup.exe>

## WireShark

File name: Wireshark-win64-4.0.8.exe

Source URL: <https://2.na.dl.wireshark.org/win64/Wireshark-win64-4.0.8.exe>

## Adobe Reader

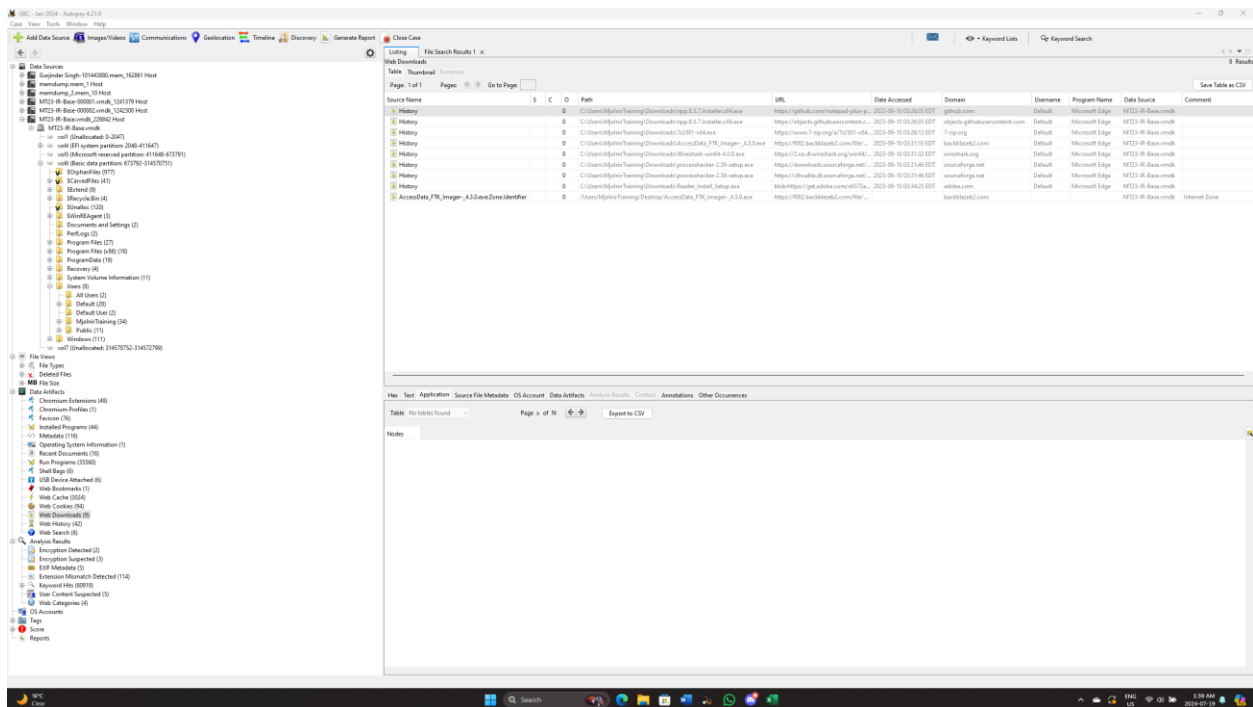
File Name: Reader\_Install\_Setup.exe

Source URL: <https://get.adobe.com/e6572a2e-87ec-42d5-9443-de8efc487d47>

## FTK Imager

File Name: AccessData\_FTK\_Imager-\_4.3.0.exe

Source URL: <https://www.7-zip.org/a/7z2301-x64.exe>



# Where is consent?

Consent.exe can be found in the C:\Windows\System32 folder.

[illegible]