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

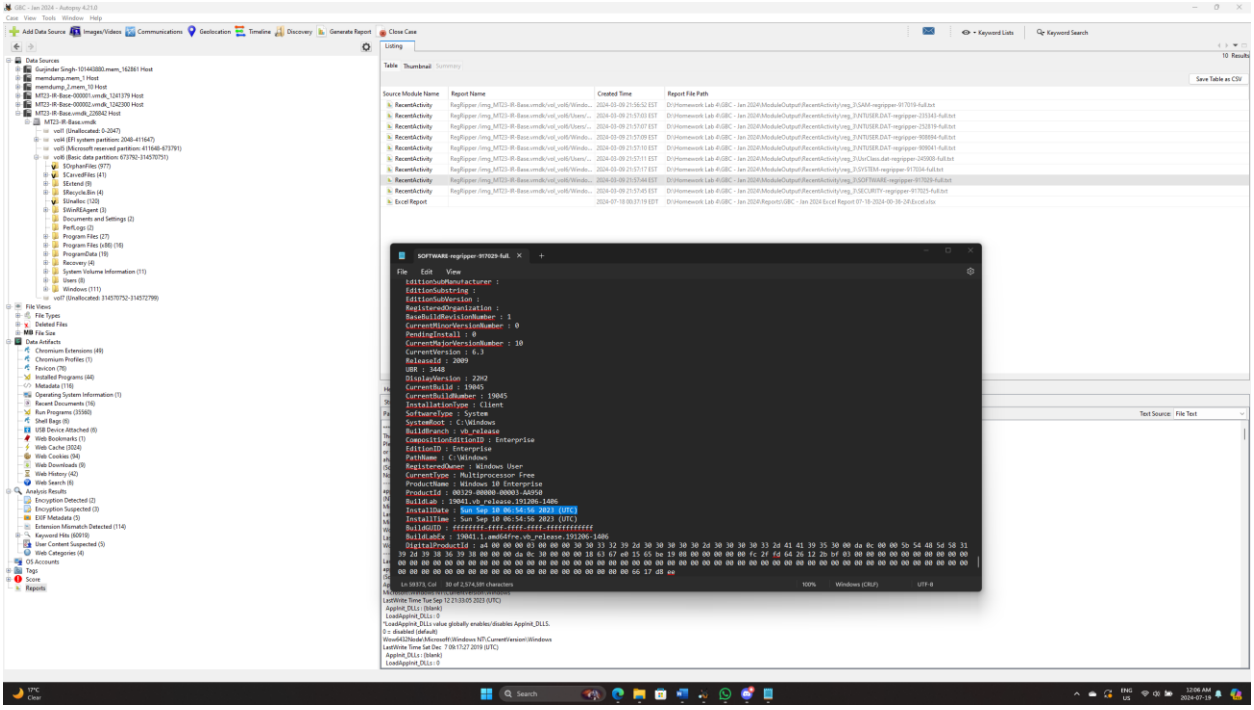
Lab Objective:

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.

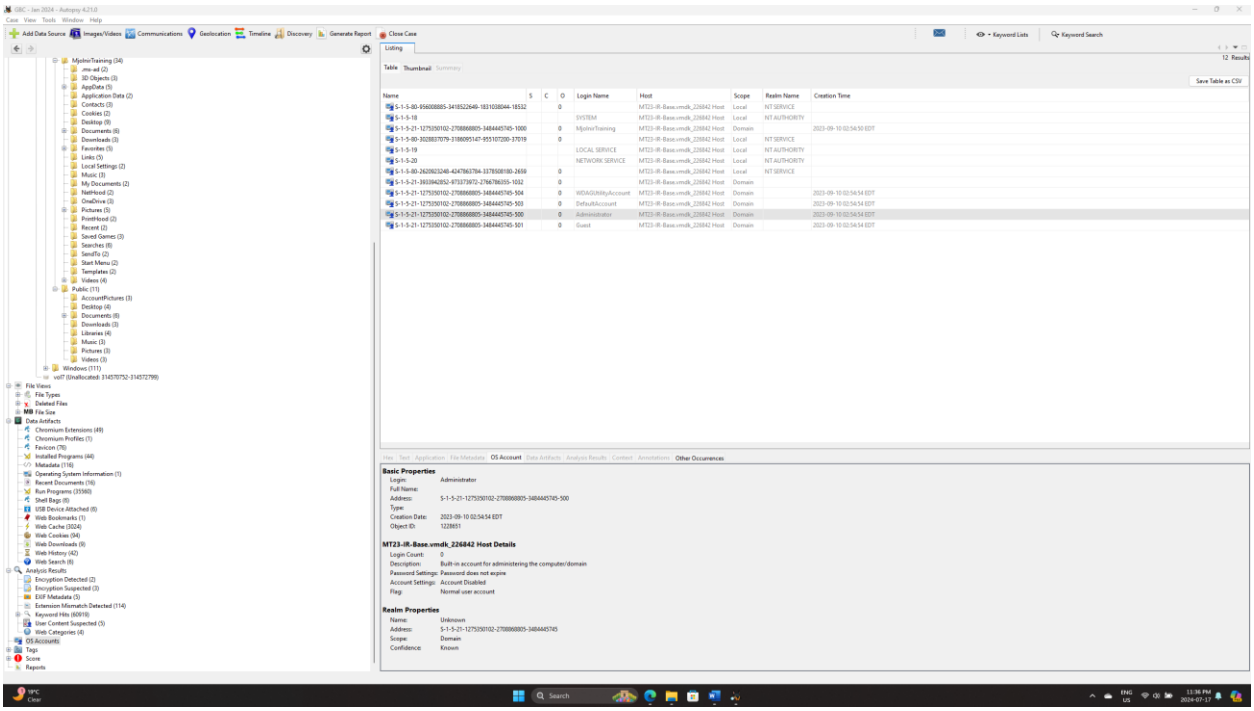
MjolnirTraining: This account was active and had been used 12 times.

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.

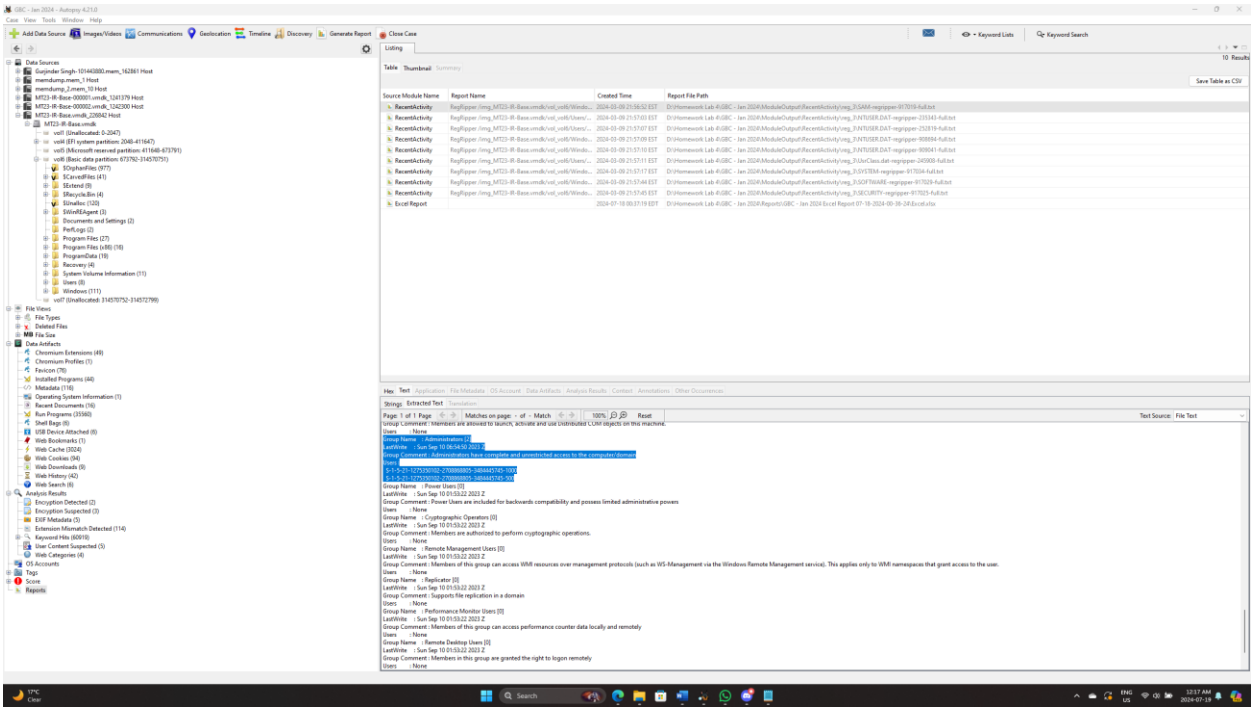
Guest: This account was Disabled and had never been used.



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.

In this report I found that there were two SID's that were members of the Administrators group, S-1-5-21-1275350102-2708868805-3484445745-1000 and S-1-5-21-1275350102-2708868805-3484445745-500.

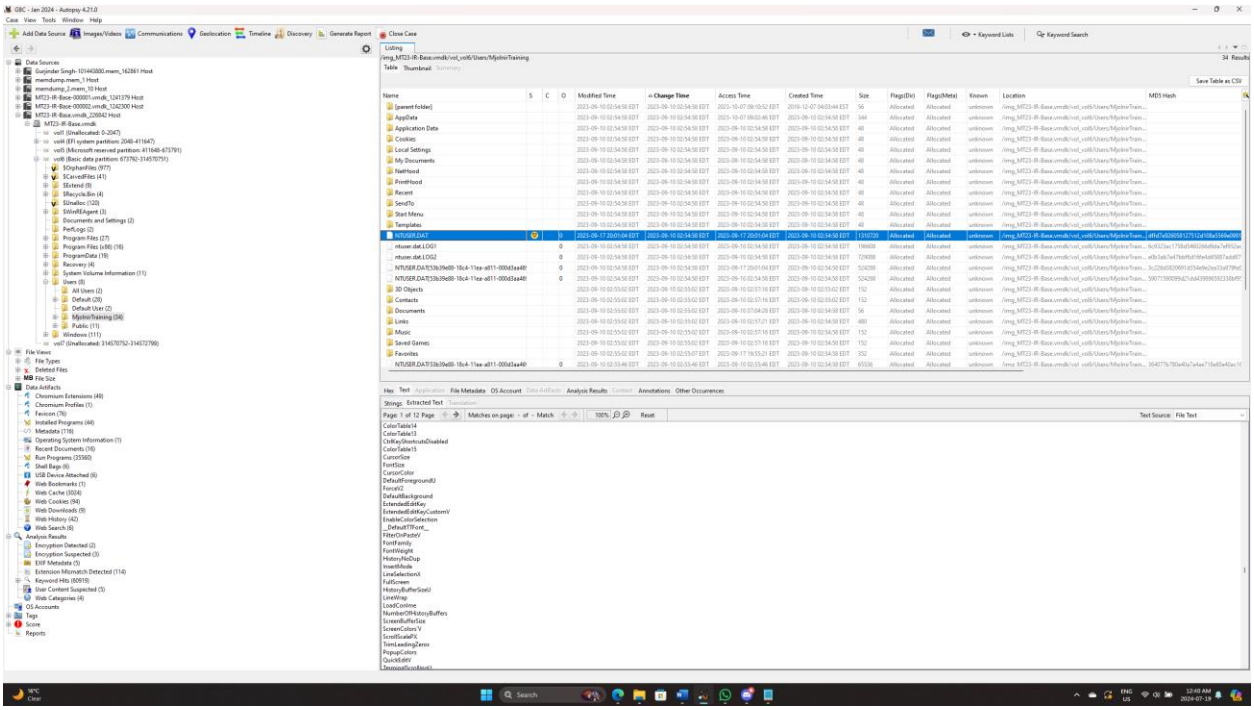
As seen in the screenshot above, these SID's correspond to **MjolnirTraining and Administrator**. This group membership makes these two accounts admin users, although the Administrator account is disabled.



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.

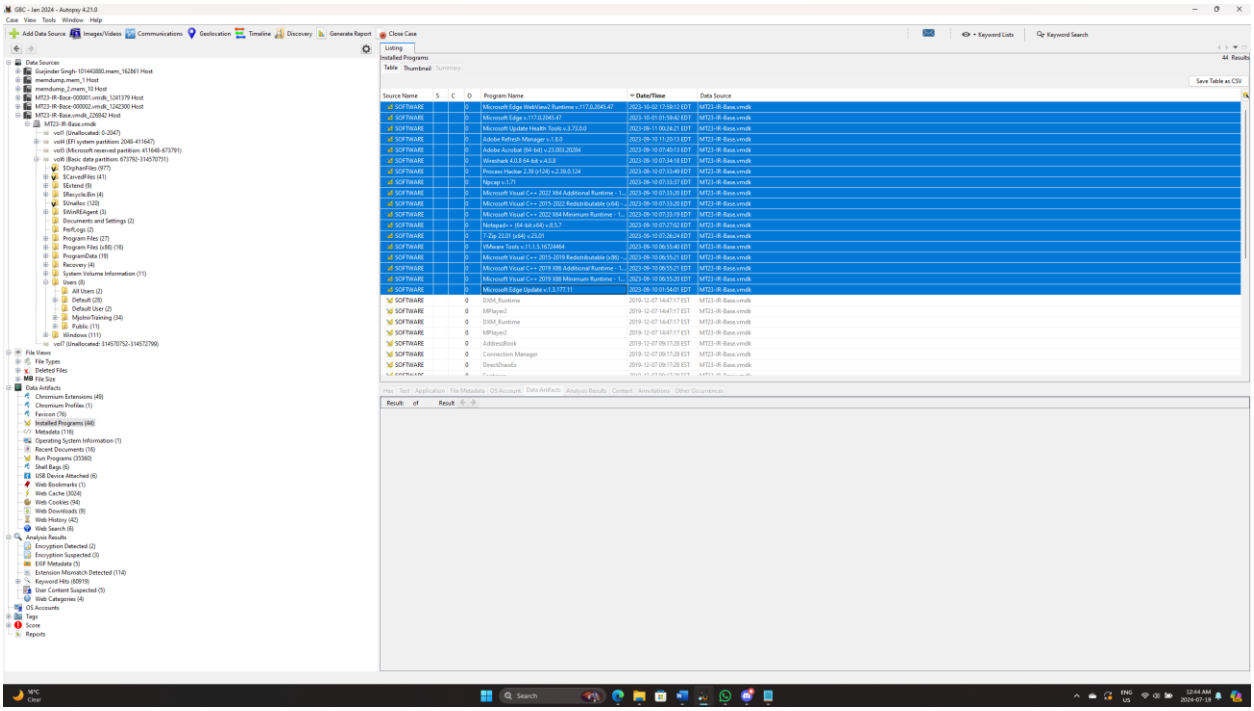
This file contains preferences related to power settings, network connections, application settings, and other customizations such as the cursor size, font size, etc.



What applications were installed in 2023?

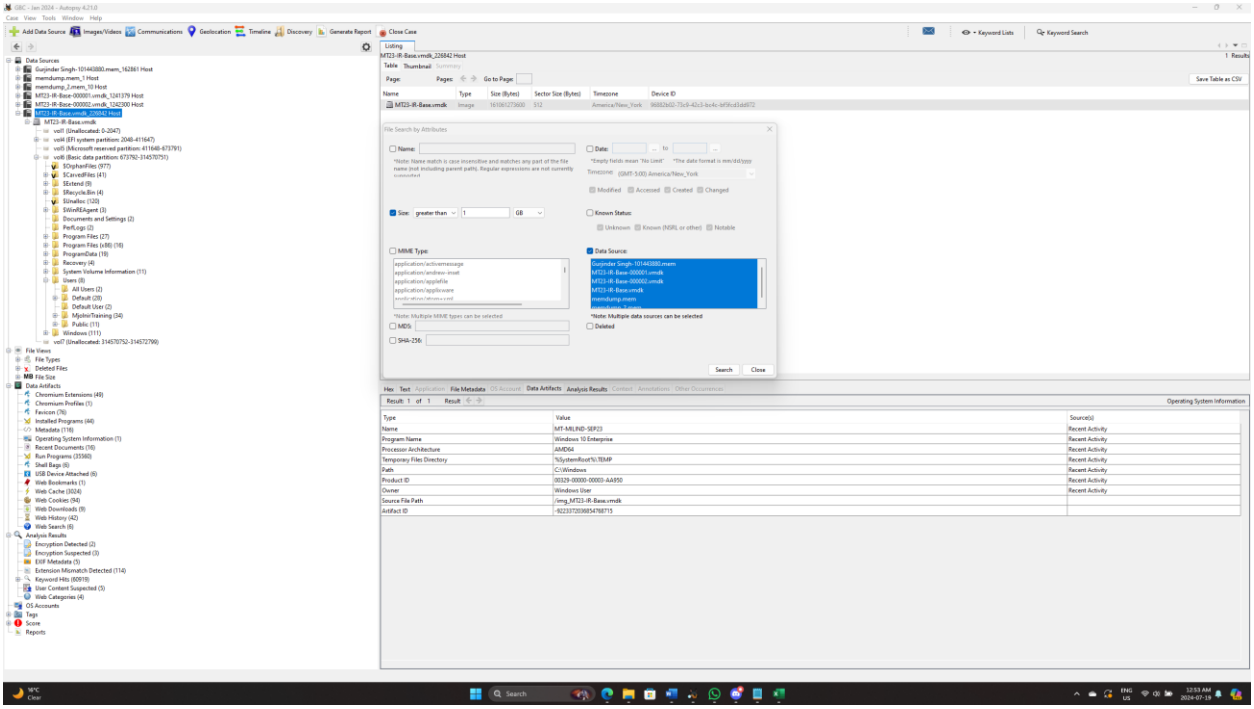
To determine which applications were installed in 2023 I navigated to “Installed Programs” under Autopsy’s Data Artifacts tab. I then sorted the applications by date. The Programs installed in 2023 are the following:

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



Name the files over 1GB in size and their locations

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.



This search yielded 9 results which were the following:

/img_MT23-IR-Base.vmdk/vol_vol6/Users/MjolnirTraining/AppData/Local/Temp/vmware-MjolnirTraining/VMwareDnD/be82d0e1/SW_DVD5_Office_Professional_Plus_2019_32_BIT_X64_English_C2R_X21-84626.ISO

/img_MT23-IR-Base.vmdk/vol_vol6/Users/MjolnirTraining/Desktop/SW_DVD5_Office_Professional_Plus_2019_32_BIT_X64_English_C2R_X21-84626.ISO

/img_MT23-IR-Base.vmdk/vol_vol6/$BadClus:$Bad

/img_MT23-IR-Base.vmdk/vol_vol6/$BadClus:$Bad-slack

/img_MT23-IR-Base.vmdk/vol_vol6/System Volume Information/{6ed365b7-5719-11ee-a815-000c29cc0d45}{3808876b-c176-4e48-b7ae-04046e6cc752}

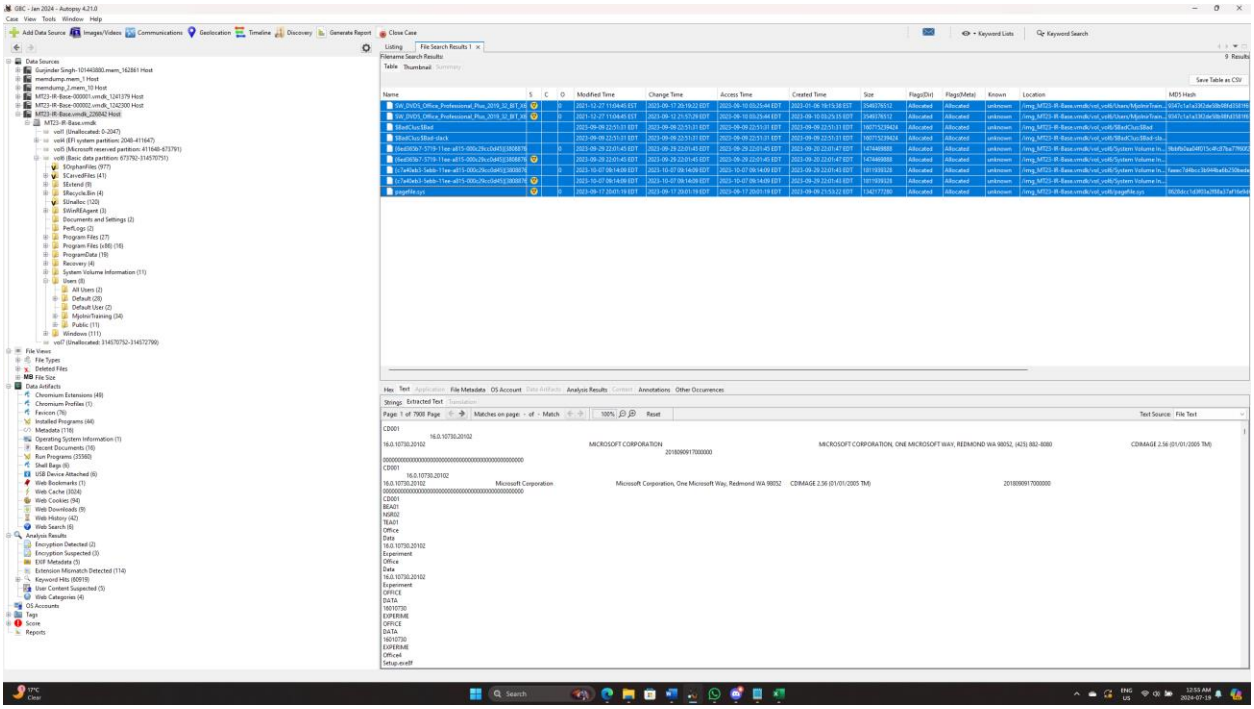
/img_MT23-IR-Base.vmdk/vol_vol6/System Volume Information/{6ed365b7-5719-11ee-a815-000c29cc0d45}{3808876b-c176-4e48-b7ae-04046e6cc752}-slack

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

/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 extenstion of the systems memory. The remaining 6 files are a little more ambiguous. After some preliminary research it seems the may relate to the disks system volume information or shadow copy's.



Device ID of virtual mouse

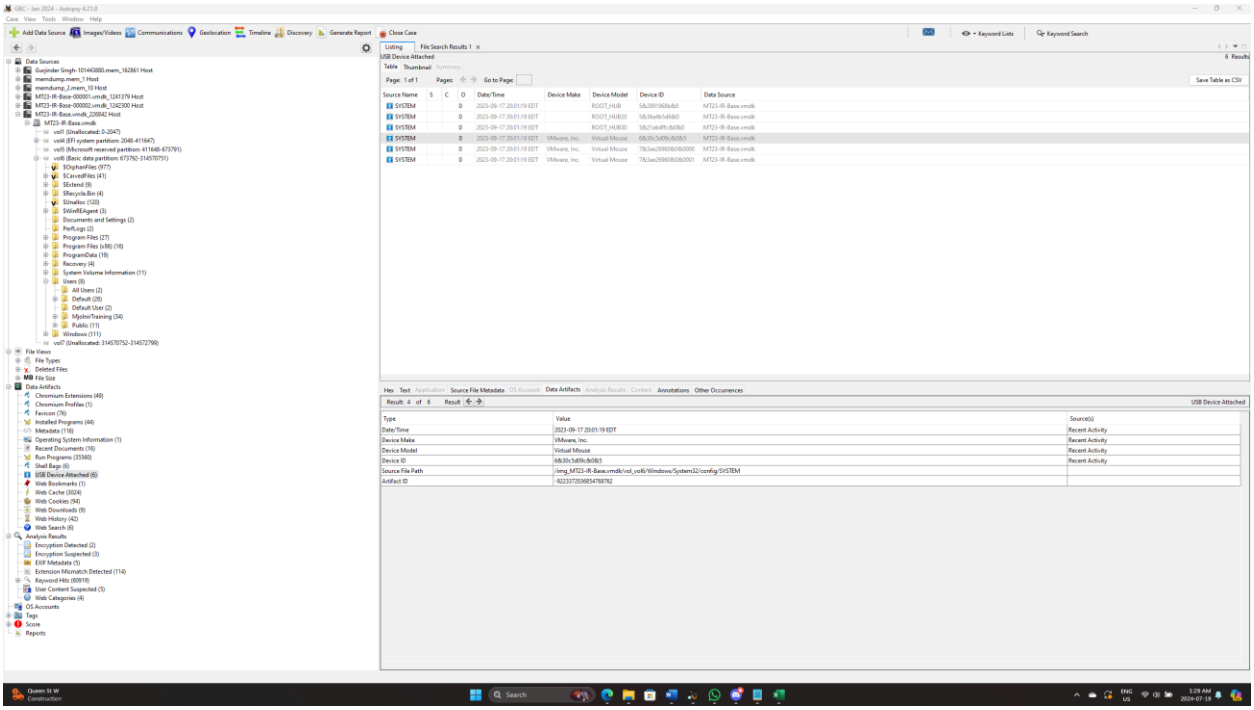
Under Data Artifacts, in the USB Device Attached section of Autopsy there are 3 virtual mice identified, each with their own Device ID.

The ID's are:

6&30c5d09c&0&5

7&3ae26960&0&0000

7&3ae26960&0&0001



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

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

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

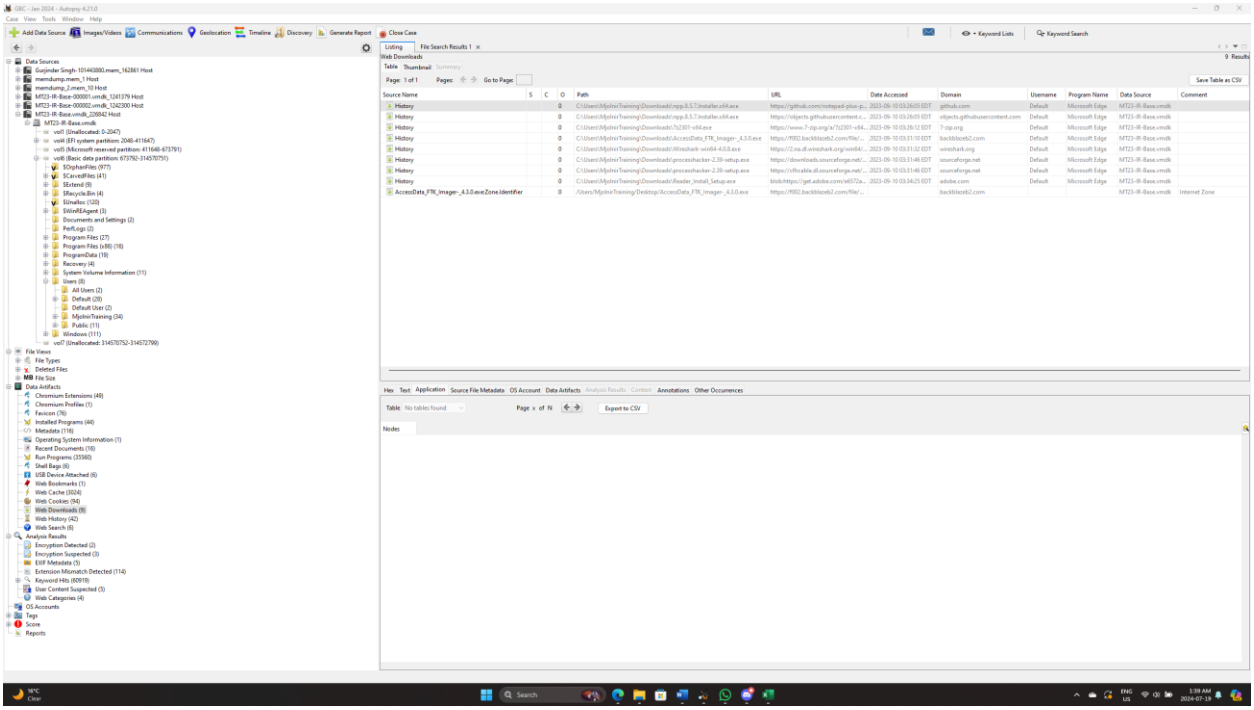
Adobe Reader
File Name: Reader_Install_Setup.exe
Source URL: https://get.adobe.com/e6572a2e-87ec-42d5-9443-de8efc487d47

FTK Imager
File Name: AccessData_FTK_Imager-_4.3.0.exe

Source URL: https://f002.backblazeb2.com/file/mjolnir-share/4n6tools/AccessData_FTK_Imager-_4.3.0.exe

FTK Imager
File Name: AccessData_FTK_Imager-_4.3.0.exe
Source URL: https://f002.backblazeb2.com/file/mjolnir-share/4n6tools/AccessData_FTK_Imager-_4.3.0.exe

7zip
File Name: 7z2301-x64.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.