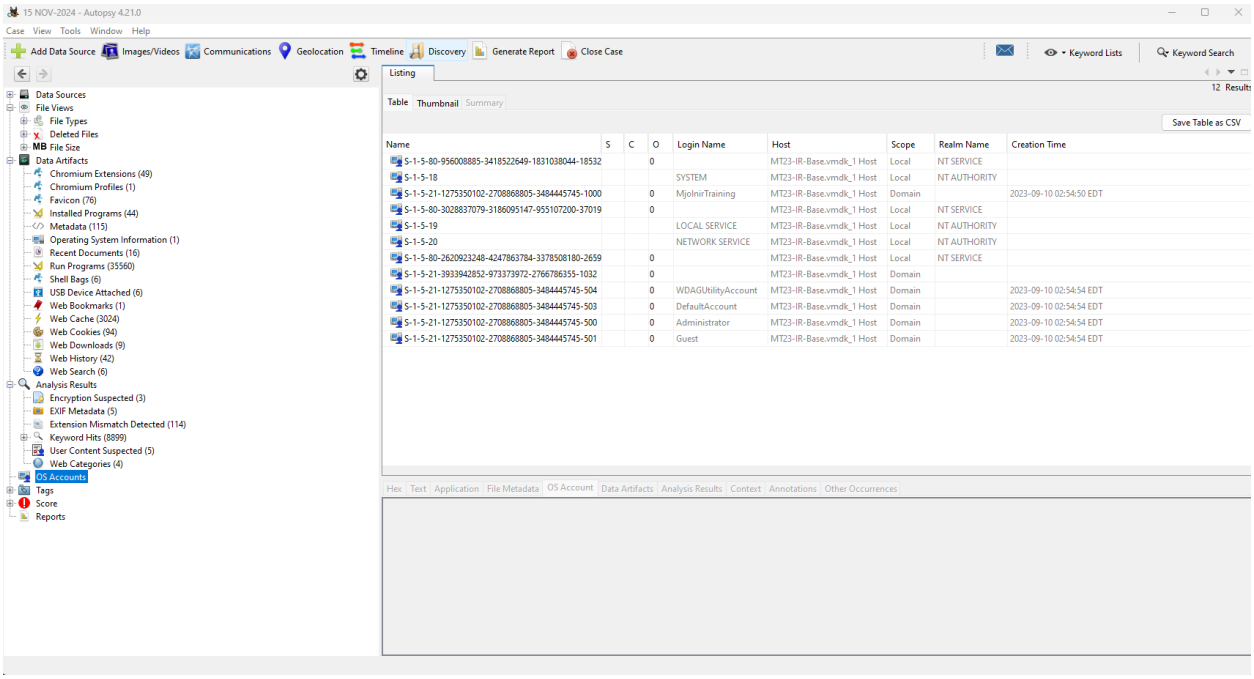
MOHAMAD ALMASR 101167438

DIGITAL FORENSICS&INCID. RESP - COMP 4071

HOMEWORK LAB 4

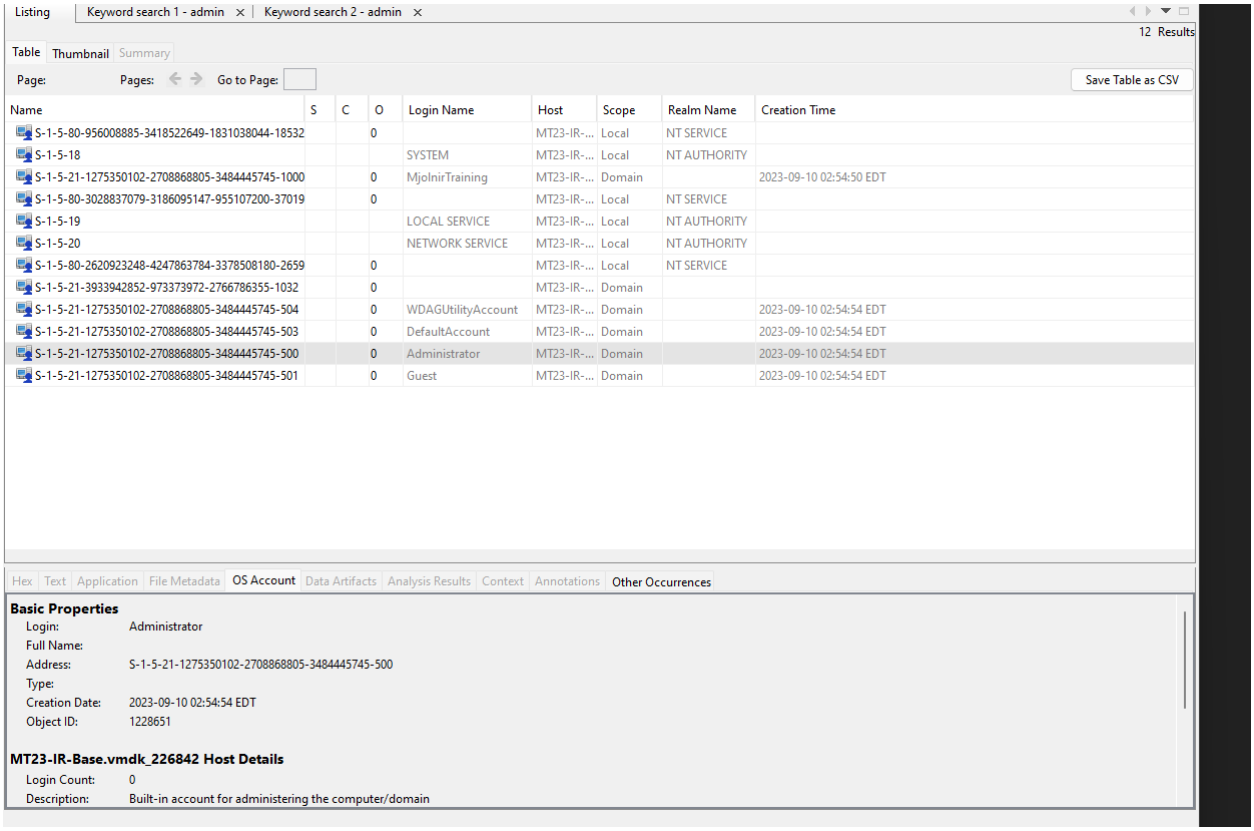
1. When was the OS built?



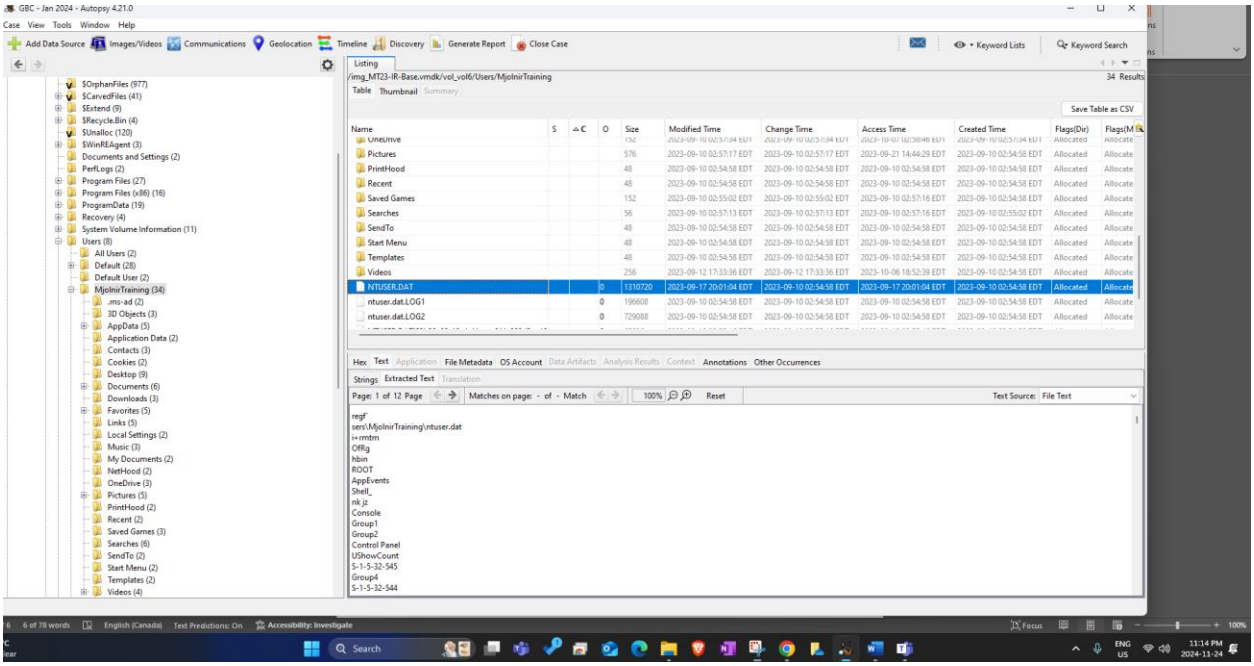
10/09/2023

MOHAMAD ALMASR 101167438

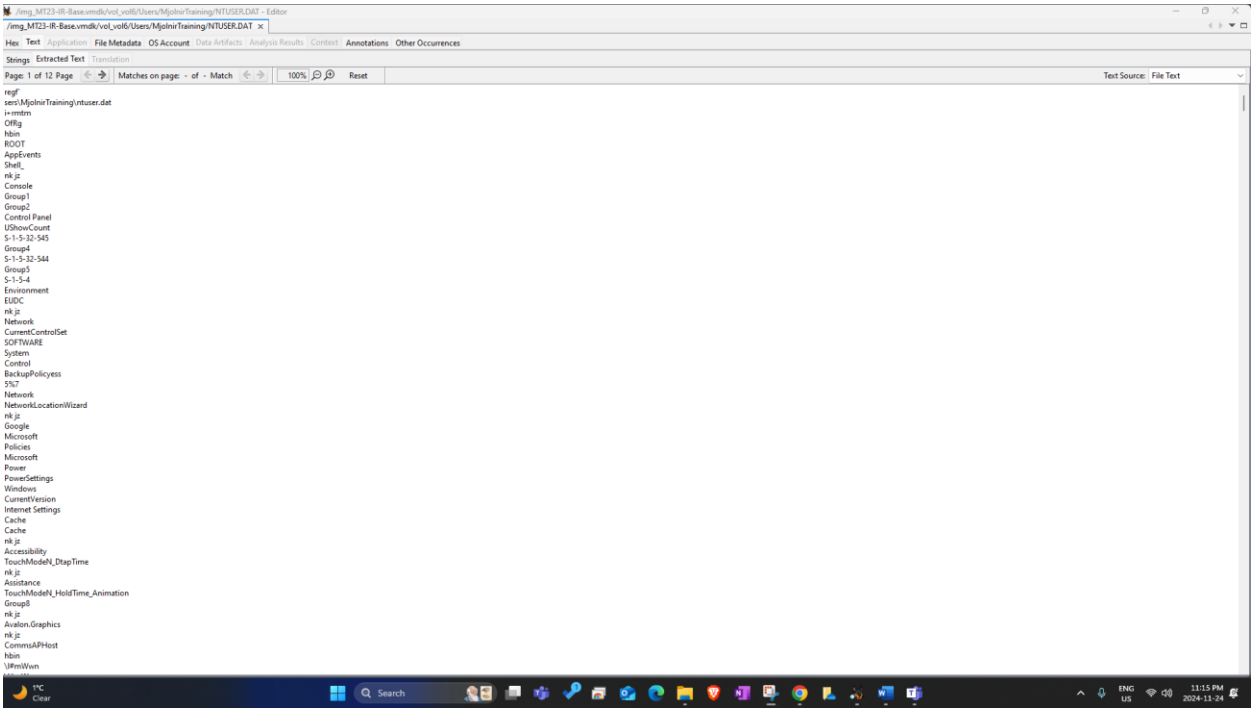
2. Who are the admin users?



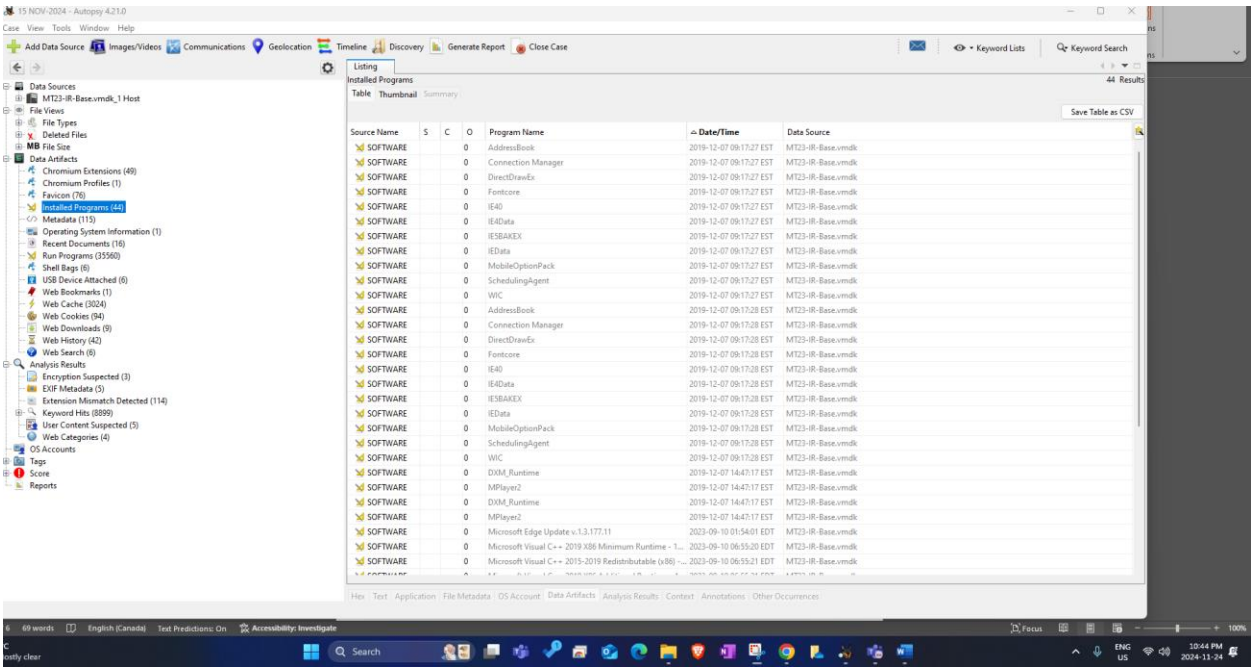
3. What profile preferences can you find for the users? Name the file and preferences.



MOHAMAD ALMASR 101167438



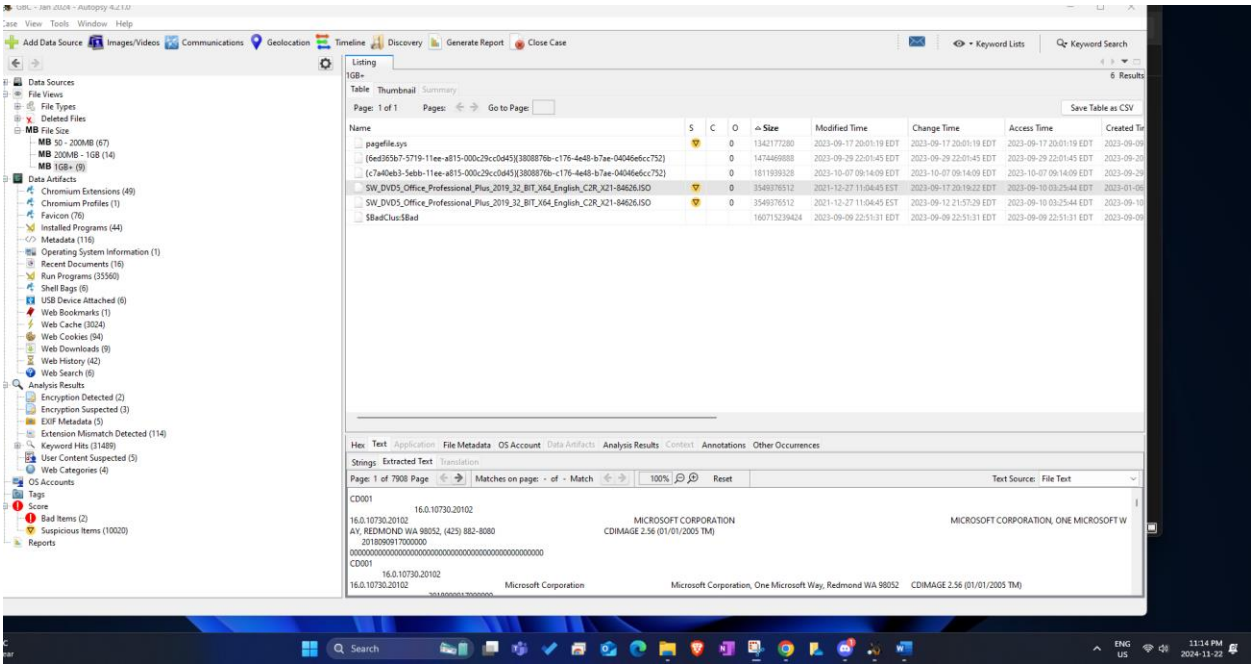
4. What applications were installed in 2021



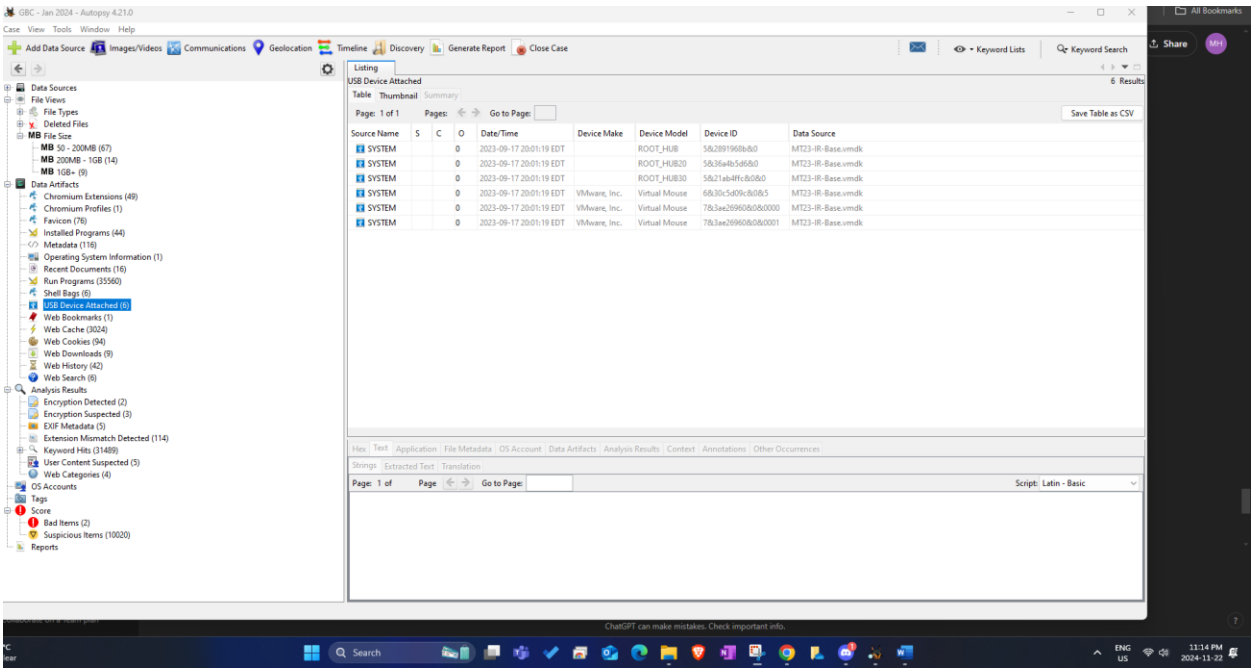
There are no any applications were installed in 2021

MOHAMAD ALMASR 101167438

5. Name the files over 1GB in size and their locations



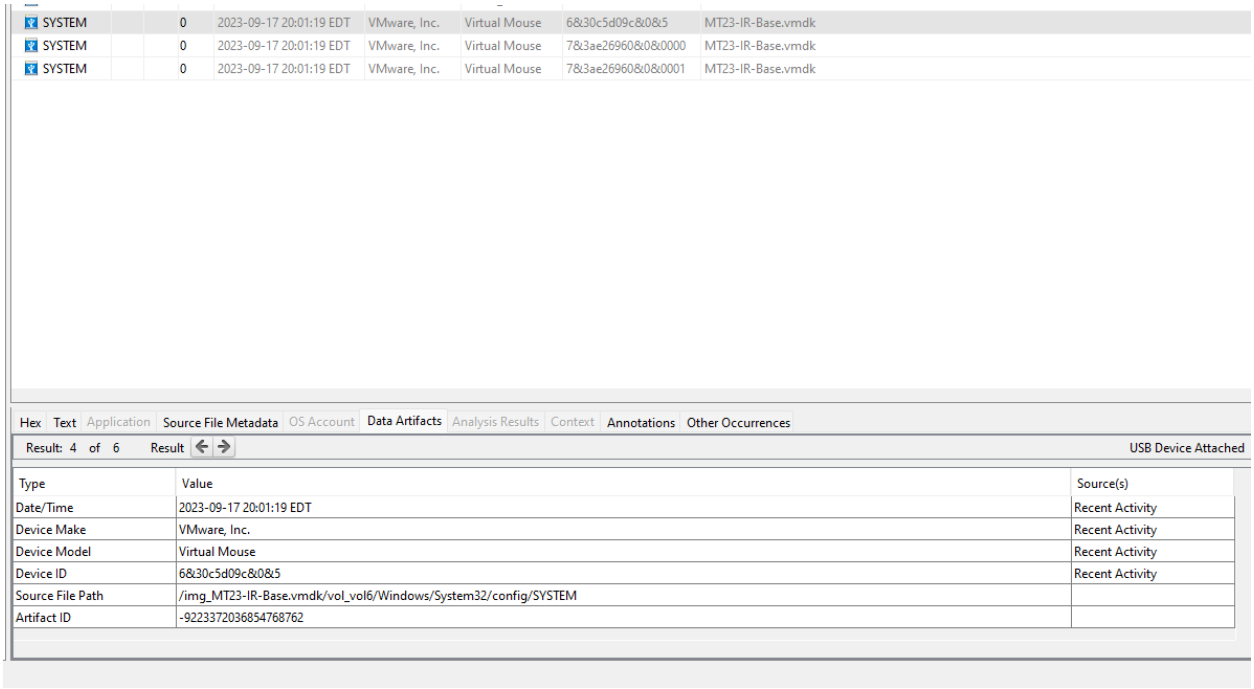
6. Device ID of virtual mouse



1. 6&30c5d09c&0&5

MOHAMAD ALMASR 101167438

2. 7&3ae26960&0&0000
3. 7&3ae26960&0&0001

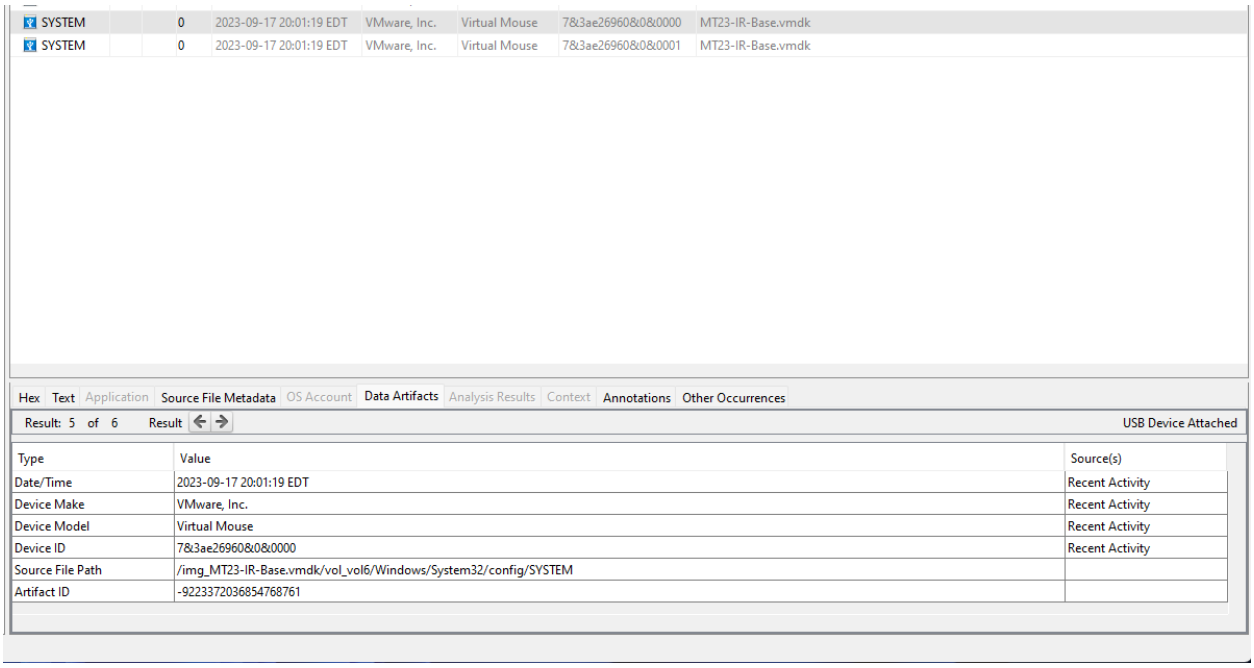


SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	6&30c5d09c&0&5	MT23-IR-Base.vmdk
SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	7&3ae26960&0&0000	MT23-IR-Base.vmdk
SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	7&3ae26960&0&0001	MT23-IR-Base.vmdk

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

Result: 4 of 6 Result USB Device Attached

Type	Value	Source(s)
Date/Time	2023-09-17 20:01:19 EDT	Recent Activity
Device Make	VMware, Inc.	Recent Activity
Device Model	Virtual Mouse	Recent Activity
Device ID	6&30c5d09c&0&5	Recent Activity
Source File Path	/img_MT23-IR-Base.vmdk/vol_vol6/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854768762	



SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	7&3ae26960&0&0000	MT23-IR-Base.vmdk
SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	7&3ae26960&0&0001	MT23-IR-Base.vmdk

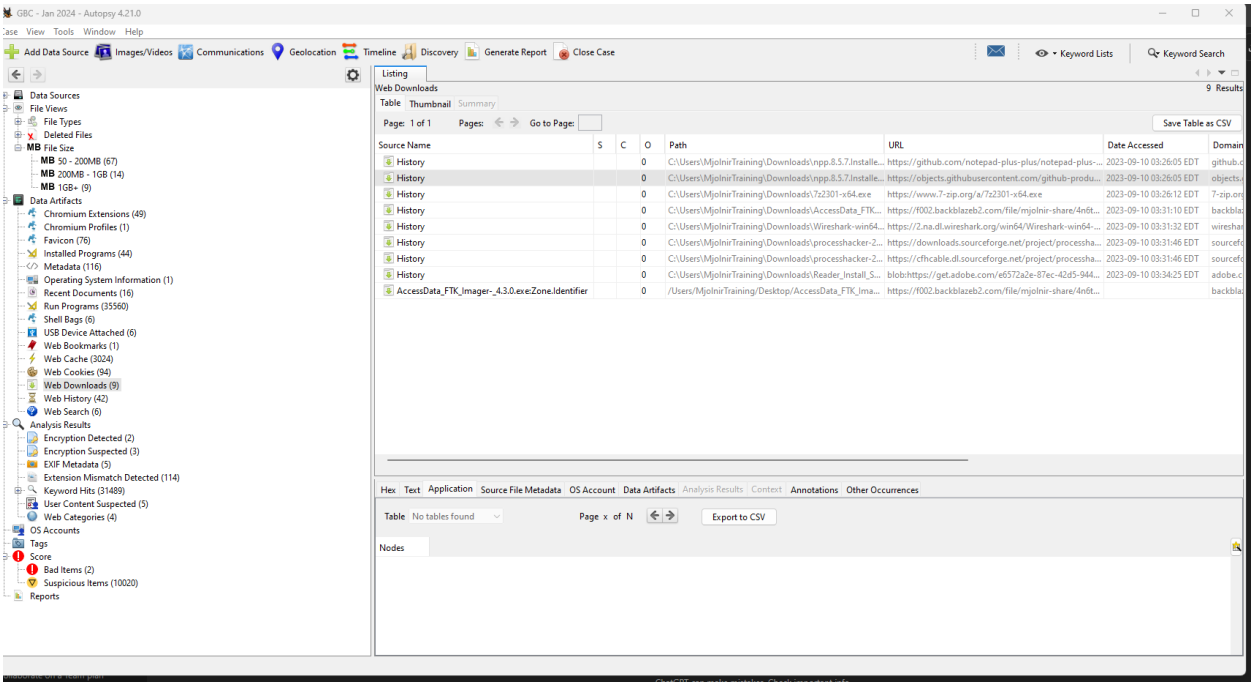
Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

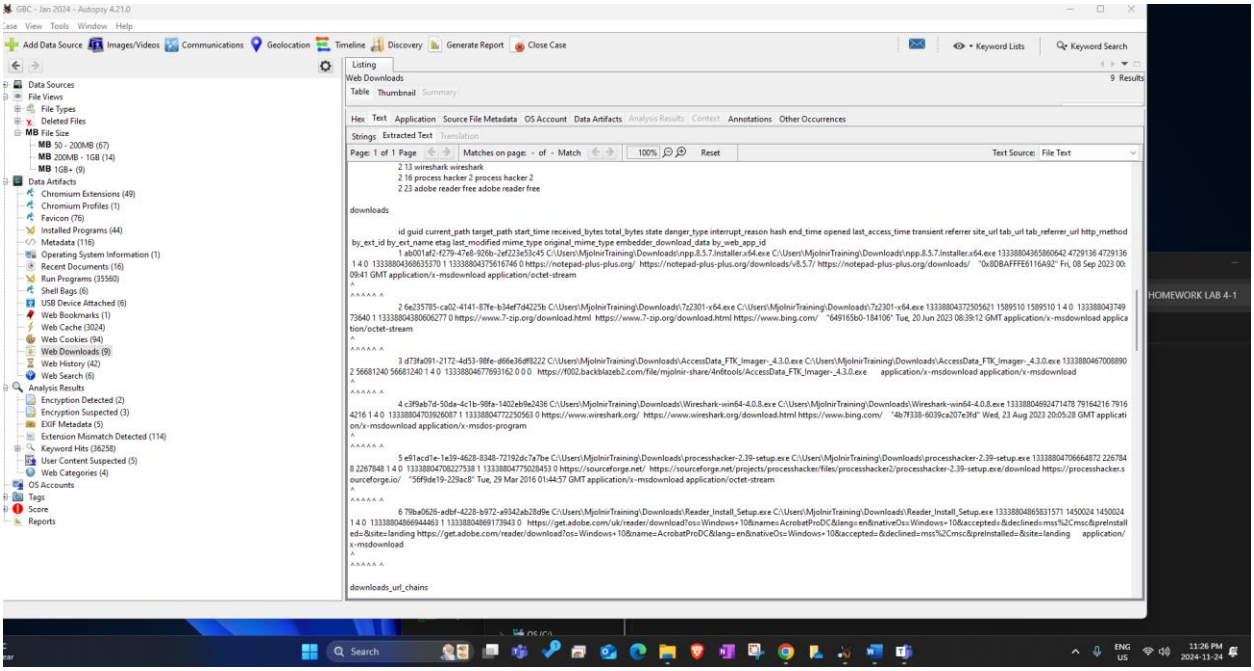
Result: 5 of 6 Result USB Device Attached

Type	Value	Source(s)
Date/Time	2023-09-17 20:01:19 EDT	Recent Activity
Device Make	VMware, Inc.	Recent Activity
Device Model	Virtual Mouse	Recent Activity
Device ID	7&3ae26960&0&0000	Recent Activity
Source File Path	/img_MT23-IR-Base.vmdk/vol_vol6/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854768761	

MOHAMAD ALMASR 101167438

7. What was downloaded?





8. Where is consent?

MOHAMAD ALMASR 101167438