University of Roehampton London

Digital Forensics: CMP020N210S

Portfolio 3 – analyzing Forensic Images

STUDENT NAME: Safa Abiasis Bashir Yusuf

STUDENT ID: YUS23603526

BSc. CYBER SECURITY

Table of Contents

Table of Contents

Introduction

This portfolio pertains to the Digital Forensics (CMP020N210S) module and centres on the investigation of a suspected insider attack on a Windows 10 virtual machine (VM). The objective is to identify any indications of malicious activity, understand the events that took place, and evaluate any system damage.

In this investigation, I took on the role of a cybersecurity analyst. I closely analysed the Windows Registry in a forensic image of a virtual machine (VM) using tools like **Autopsy** and **Registry Explorer**. These tools helped me locate crucial data related to software execution, user behaviour, and possible malware activity. The investigation was conducted in line with the UK's **ACPO guidelines**, which ensure that digital evidence is handled correctly and remains admissible in court.

The portfolio consists of three sections. **Component 1** covers the primary registry analysis and provides detailed responses to questions about system events. **Component 2**, also known as the **Wow Factor**, extends the investigation by examining memory and other system files for hidden evidence using advanced tools like **Volatility**. The **executive summary** in Component 3 outlines the key findings, explains the reasoning behind the tools and techniques used, and reflects on the lessons I learned throughout the investigation.

This assignment demonstrates my ability to carry out a real-world digital forensic investigation, apply the appropriate tools, and clearly explain the findings. It also highlights how digital forensics helps organisations understand and respond to security threats.

Investigator Details

Investigator detail	Date of the report	Purpose of the investigation
Safa Abiasis Bashir Yusuf	1th may – 8th may	This investigation's goal is to use digital forensic tools to analyse a Windows 10 virtual machine image for indications of malicious activity and evaluate the results.

1. System Identification and Operating System

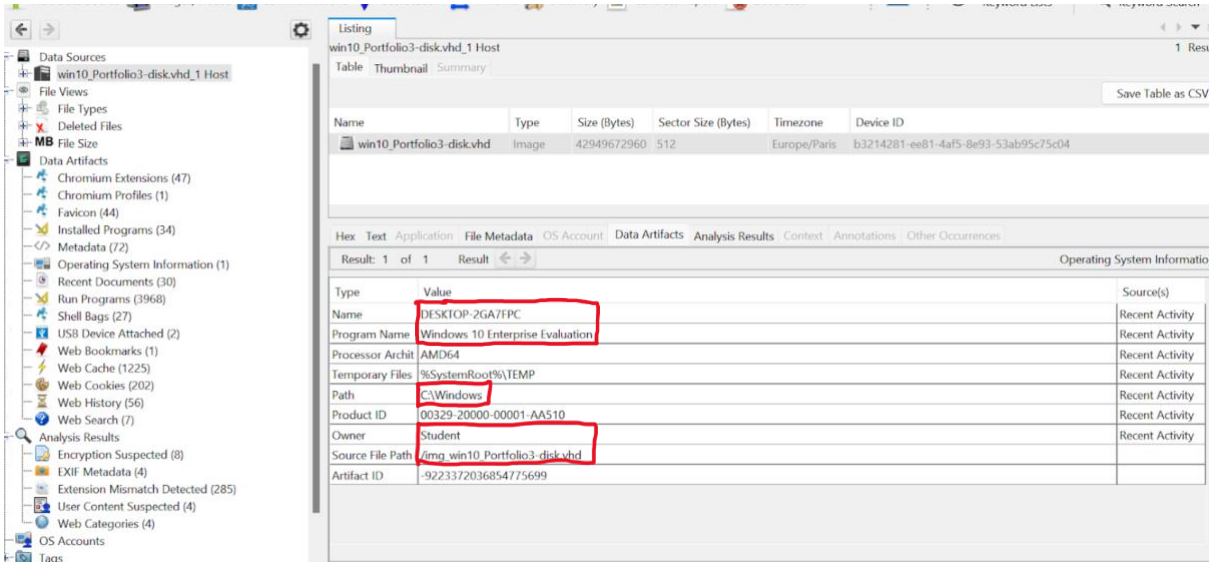
Question: *From which operating system (program name) was the forensic image (win10 Portfolio3-disk.vhd) acquired? What is the computer's name? What is the source file containing this information? What is the Path?*

Answer:

Windows 10 Enterprise Evaluation was the operating system from which the forensic image was taken. The name of the machine is DESKTOP-2GA7FPC. This information was obtained from the **SOFTWARE** registry hive, which can be found at the following path: *C:\Windows\System32\config\SOFTWARE*

I opened the forensic image win10_Portfolio3-disk.vhd in Autopsy to find this data. Under Data Artifacts, I selected Operating System Information from the panel on the left as shown in the screenshot. The results panel displayed the device name, operating system version, source file location, and other system information.

The screenshot below shows us the relevant metadata extracted by Autopsy:



2. Identification of Device Owner of Windows 10

Question: Who is the owner of this device?

Answer:

The Windows 10 device's registered owner is student. This data was retrieved from Autopsy's Operating System Information artefact.

I used Autopsy to open the forensic image win10_Portfolio3-disk.vhd in order to locate this data. I choose Operating System Information after navigating to Data Artefacts in the panel on the left. The Owner field was listed as Student in the results panel on the right, along with other system metadata.

The screenshot below shows the registered owner detail extracted by Autopsy

Name	DESKTOP-2GA7FPC
Program Name	Windows 10 Enterprise Evaluation
Processor Archi	AMD64
Temporary Files	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00329-20000-00001-AA510
Owner	Student
Source File Path	/img_win10_Portfolio3-disk.vhd
Artifact ID	-9223372036854775699

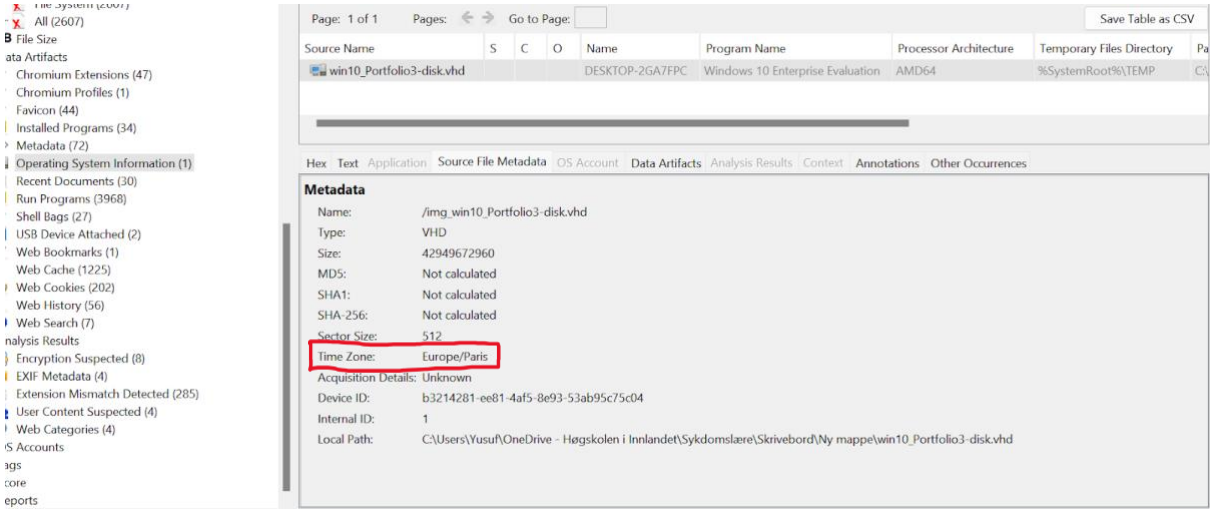
3. System Time zone Settings

Question: what is the time zone settings?

Europe/Paris is the system's time zone setting. This information was found in the Source File Metadata tab of the forensic image **win10_Portfolio3-disk.vhd** using Autopsy.

To locate this information, I opened the image in Autopsy and selected it from the Data Sources section in the left-hand panel. Then, I navigated to the Source File Metadata tab in the main window. In this section, the Time Zone field clearly displayed the value Europe/Paris, along with other metadata such as the device ID, local path, and file size.

The screenshot below confirms the system's time zone setting:



4. Device ID for the Win10_Portfolio3-disk.vhd

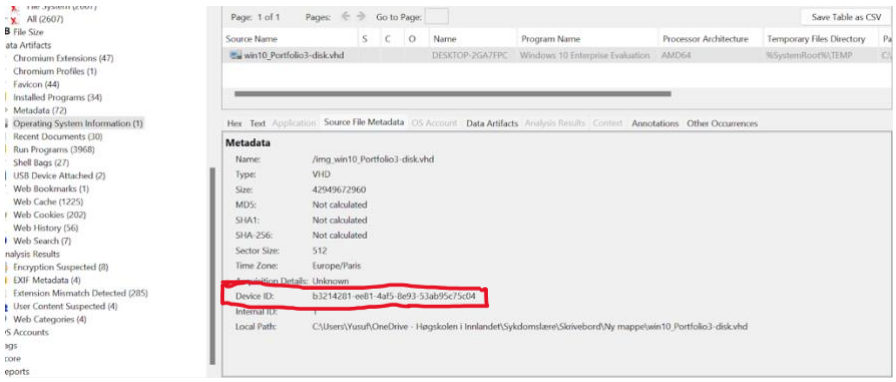
Question: What is the Device ID for the win10_Portfolio3-disk.vhd?

Answer: The Device ID for the forensic image win10_Portfolio3-disk.vhd is:

b3214281-ee81-4af5-8e93-53ab95c75c04

This data was found in the **Source File Metadata** tab of Autopsy. After selecting the image from the **Data Sources** panel on the left, I navigated to the **Source File Metadata** tab in the main viewing area. Other metadata, such as the Time Zone, file size, and local path, were displayed alongside the Device ID.

The screenshot as seen below confirms the Device ID for the forensic image:



5. IP Address and DHCP Network Interface

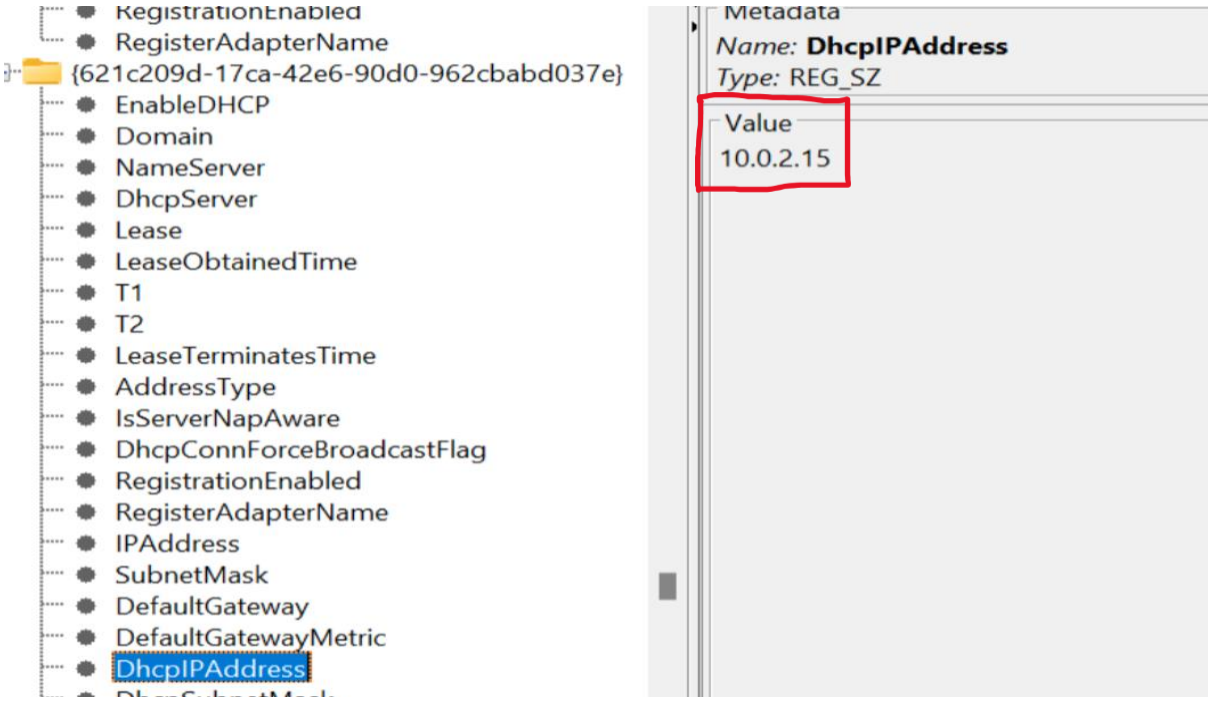
Question: Identify the information of network interface(s) with an IP address assigned by DHCP? What is DHCP IP Address?

In Autopsy, I looked at the SYSTEM hive to get the DHCP-assigned IP address and navigated to:

ControlSet001 > Services > Tcpip > Parameters > Interfaces

I found the value DhcpIPAddress, which was set to ***10.0.2.15,*** inside the interface key {621c209d-17ca-42e6-90d0-962cbabd037e}. This confirms that the DHCP was used to assign the IP address.

The screenshot below displays the ***DhcpIPAddress*** *value and the corresponding registry key as extracted by Autopsy:*



6. User Accounts Listed in the System

Question: How many user accounts are listed?

Answer:

The system has six user accounts listed.

I examined the OS Accounts area using Autopsy to ascertain this. I went to the following from the left-hand panel:

OS Accounts > Data Artefacts

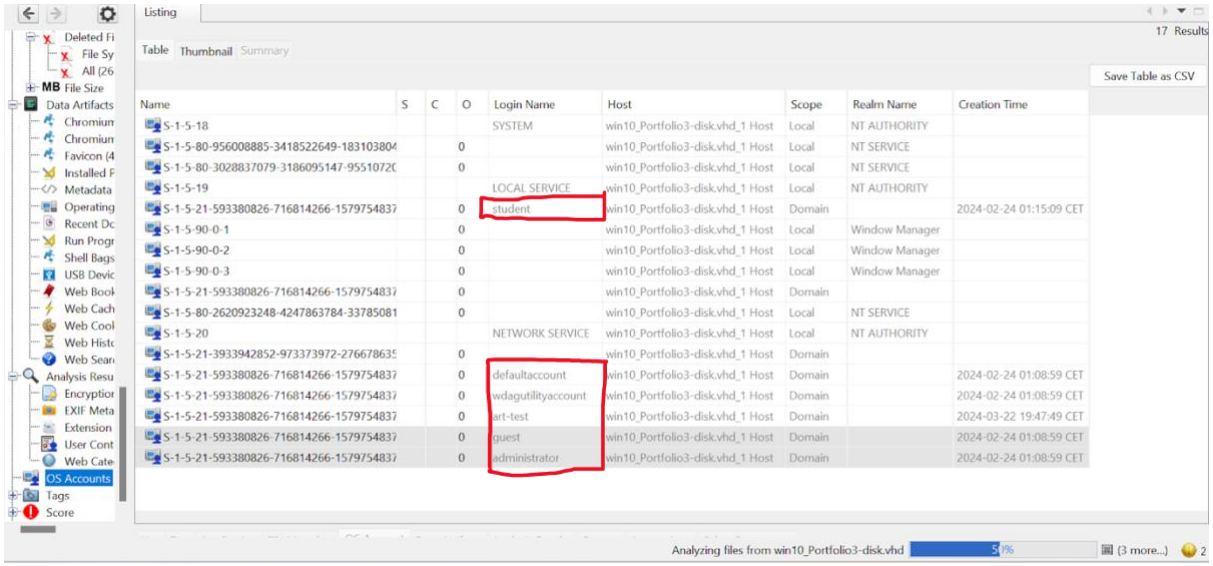
The results panel showed 17 accounts. However, a large number of these are not considered regular user profiles because they are system or service accounts like SYSTEM, LOCAL SERVICE, and NETWORK SERVICE. These accounts are used to manage security contexts or conduct background services and are a part of the Windows operating system.

Only accounts created for interactive use or user-specific procedures are counted for forensic reasons. They consist of:

1. Student
2. Defaultaccount
3. wdagutilityaccount
4. art-test
5. guest
6. administrator

All of these were designed for user-level access, as seen by their unique login names and affiliation with either the domain or the local system.

The screenshot below confirms the listed user accounts as extracted using Autopsy:



7. Last user to login to the PC

Question: Who was the last user to login to the PC?

Answer:

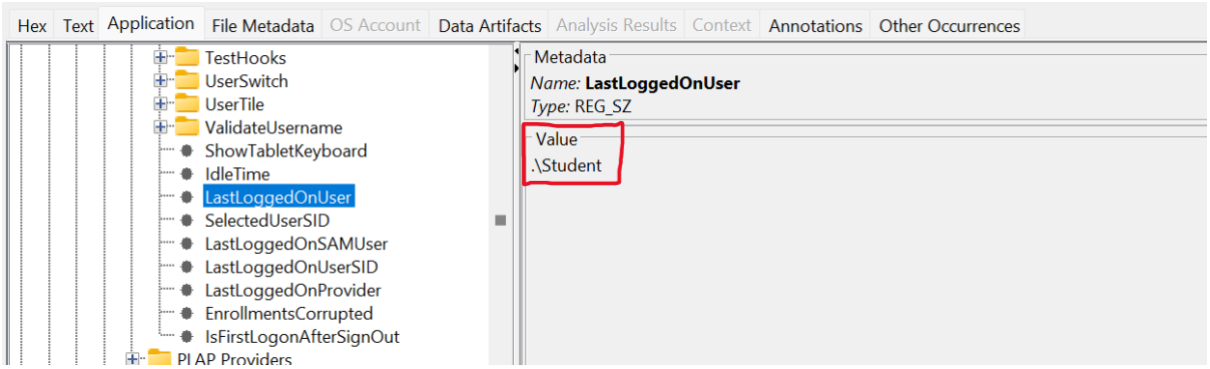
The last user to log in to the system was **Student**.

I used Autopsy's Registry Viewer to analyse the SOFTWARE registry hive in order to discover this information. I went to the registry key listed below:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

I checked the value for ***LastLoggedOnUse*r** under this key, which was set to Student. This shows that the most recent user to log in to the system was the "Student" account.

The LastLoggedOnUser value as extracted by Autopsy is displayed in the screenshot below:



8. Identification of user account with most activity

Question: Identify what is the account name of the user who mostly uses the computer?

Answer:

Student is the user account that uses the computer the most.

I used Autopsy and went to *Data Artifacts* > *OS Accounts* to determine this.

I selected the student account from the list of user accounts. This user has logged in more times than any other account on the system, according to the details panel's Login Count of 41. The fact that this account's Home Directory is C:\Users\Student further confirms that this is the main user profile.

The login count and other account metadata can be confirmed in the screenshot below:

9. The last recorded computer shutdown date/time

Question: Identify when was the last recorded computer shutdown date/time?

Answer:

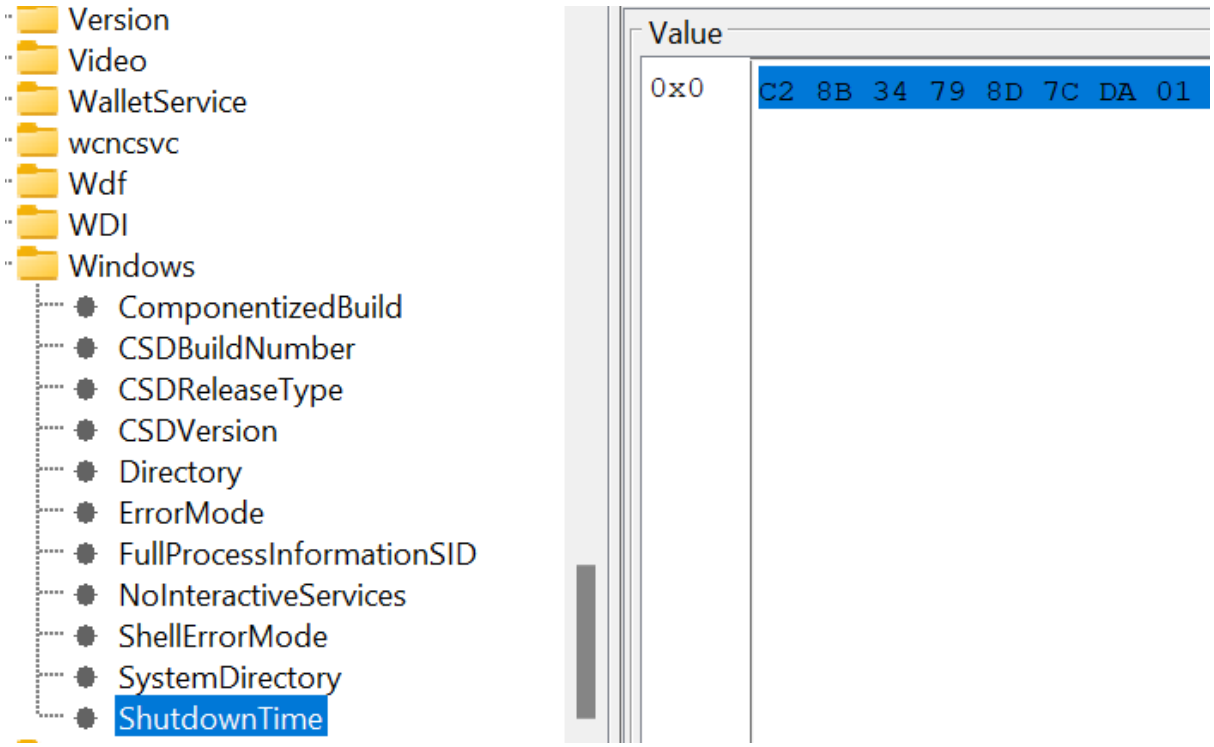
On March 22, 2024, at 19:16:42 (UTC), the system was last known to shut down.

To determine this, I did this by using Autopsy to look at the ShutdownTime value in the Windows Registry's SYSTEM hive. I navigated to:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

The following hexadecimal data was included in the REG_BINARY item that represented the ShutdownTime value:

C2 8B 34 79 8D 7C DA 01



This 64-bit FILETIME value was converted from little-endian to big-endian format, and then to its decimal form:

133556086026570690

I used PowerShell to transform this data into a timestamp that could be read by humans by using the following command:

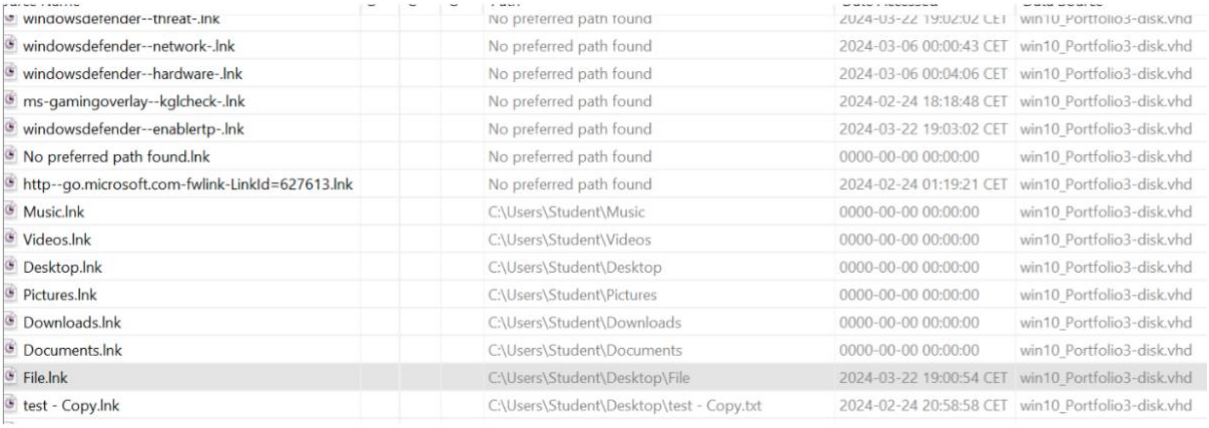
```
PS C:\Users\Yusuf> # Convert the hex to a decimal value:
PS C:\Users\Yusuf> $FileTime = 133556086026570690
PS C:\Users\Yusuf>
PS C:\Users\Yusuf> # Convert to UTC datetime
PS C:\Users\Yusuf> [datetime]::FromFileTimeUtc($FileTime)

fredag 22. mars 2024 19:16:42
```

10. User logged into the device on 22nd March 2024.

Question: Which user was logged into the device on 22nd March 2024.

I used Autopsy to look at.lnk (shortcut) files in the C:\Users\Student\Desktop directory in order to ascertain this. These files are unique to each user profile and contain metadata about recently visited items.

The last accessed timestamps of a number of.lnk files, including File.lnk, were 2024-03-22 19:00:54 CET, which is quite close to the system's most recent shutdown time of 19:16:42 UTC. This clearly shows that the "Student" account was logged in and active at the time.
File paths and timestamps verifying the student account's activity on that day are shown in the screenshot below:



windowsdefender--threat-.lnk	No preferred path found	2024-03-22 19:02:02 CET	win10_Portfolio3-disk.vhd
windowsdefender--network-.lnk	No preferred path found	2024-03-06 00:00:43 CET	win10_Portfolio3-disk.vhd
windowsdefender--hardware-.lnk	No preferred path found	2024-03-06 00:04:06 CET	win10_Portfolio3-disk.vhd
ms-gamingoverlay--kglcheck-.lnk	No preferred path found	2024-02-24 18:18:48 CET	win10_Portfolio3-disk.vhd
windowsdefender--enablertp-.lnk	No preferred path found	2024-03-22 19:03:02 CET	win10_Portfolio3-disk.vhd
No preferred path found.lnk	No preferred path found	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
http--go.microsoft.com-fwlink-LinkId=627613.lnk	No preferred path found	2024-02-24 01:19:21 CET	win10_Portfolio3-disk.vhd
Music.lnk	C:\Users\Student\Music	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
Videos.lnk	C:\Users\Student\Videos	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
Desktop.lnk	C:\Users\Student\Desktop	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
Pictures.lnk	C:\Users\Student\Pictures	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
Downloads.lnk	C:\Users\Student\Downloads	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
Documents.lnk	C:\Users\Student\Documents	0000-00-00 00:00:00	win10_Portfolio3-disk.vhd
File.lnk	C:\Users\Student\Desktop\File	2024-03-22 19:00:54 CET	win10_Portfolio3-disk.vhd
test - Copy.lnk	C:\Users\Student\Desktop\test - Copy.txt	2024-02-24 20:58:58 CET	win10_Portfolio3-disk.vhd

11. User account(s) were created on 22nd March 2024

The user account art-test was created at 19:47:49 CET on March 22, 2024. This data was acquired by utilising Autopsy to examine the SAM registry hive. The creation timestamps for each user account were given under the Operating System Information section.

Only one of the accounts which was art-test, had a creation date that matched with March 22, 2024. The creation dates of all other accounts were earlier, including administrator, student, visitor, and defaultaccount.
The screenshot below is conforming that art test was the only account created on March 22, 2024:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-593380826-716814266-1579754837-10(			0	art-test	win10_Po...	Domain		2024-03-22 19:47:49 CET
S-1-5-21-593380826-716814266-1579754837-10(			0	student	win10_Po...	Domain		2024-02-24 01:15:09 CET
S-1-5-21-593380826-716814266-1579754837-50:			0	defaultaccount	win10_Po...	Domain		2024-02-24 01:08:59 CET
S-1-5-21-593380826-716814266-1579754837-504			0	wdagutilityaccount	win10_Po...	Domain		2024-02-24 01:08:59 CET
S-1-5-21-593380826-716814266-1579754837-501			0	guest	win10_Po...	Domain		2024-02-24 01:08:59 CET
S-1-5-21-593380826-716814266-1579754837-500			0	administrator	win10_Po...	Domain		2024-02-24 01:08:59 CET

12 Registry Explorer: An Analysis of Administrator Group Membership

Question) Investigate user accounts and identify which accounts are administrator group members?

I analysed the forensic image using Autopsy to determine which user accounts are part of the Administrators group. I used Autopsy to extract the SAM registry hive from the forensic image. The location of the file was:

C:\Windows\System32\config\SAM

I then loaded the SAM hive into **Registry Explorer**. Once loaded, I navigated to:

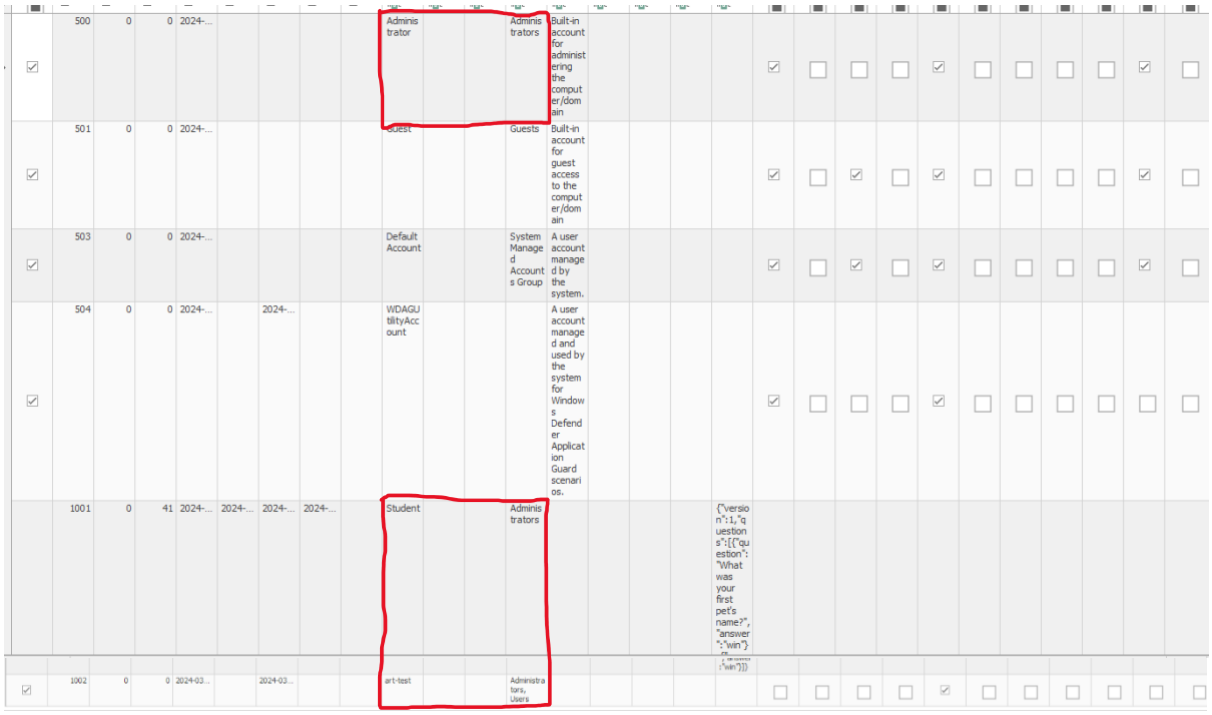
SAM\SAM\Domains\Account\Users

I just clicked on the Users entry, and Registry Explorer showed all the user accounts and their details, saving me the trouble of analysing raw binary data. including their connections with various groups.

Based on this view, the following accounts were listed as members of the Administrators group:

- Student
- Art-test
- Administrator

Screenshot below:



13. Number of files under AtomicRedTeam

Question: How many files are under AtomicRedTeam?

Answer:

I investigated the directory structure of the forensic image found at /img_win10_Portfolio3-disk.vhd/vol_vol3/AtomicRedTeam using Autopsy v4.22.1.

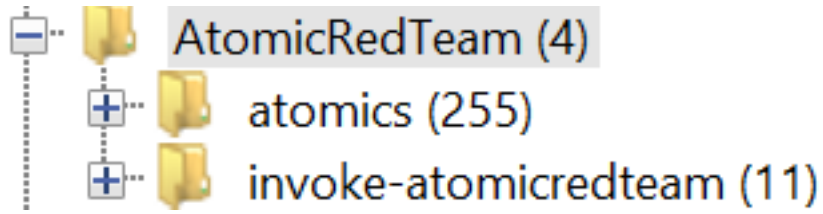
I opened the AtomicRedTeam folder and expanded it from the File Views window on the left. Each subfolder's file counts were displayed directly:

The AtomicRedTeam directory had 266 files in total. This includes:

- **11 files** in the invoke-atomicredteam subfolder
- **255 files** in the atomics subfolder

The total number of files in the AtomicRedTeam directory was determined by adding these numbers.

The directory and file breakdown as seen in Autopsy is shown in the screenshot below:



14 Parent MFT Entry Number for ART-attack.ps1

Question) What is the Parent MFT Entry Number for the file "ART-attack.ps1"?

Answer:

According to the metadata details that Autopsy was able to extract, the file ART-attack.ps1's Parent MFT Entry Number is **102162.**

Screenshot Below:

```
Accessed: 2024-03-22 19:56:40.826244000 (CES)

$FILE_NAME Attribute Values:
Flags: Archive
Name: ART-attack.ps1
Parent MFT Entry: 102162 Sequence: 9
Allocated Size: 4096 Actual Size: 3360
Created: 2024-03-22 19:56:40.826244000 (CES)
File Modified: 2024-03-22 19:56:40.826244000 (CES)
MFT Modified: 2024-03-22 19:56:41.075340400 (CES)
Accessed: 2024-03-22 19:56:40.826244000 (CES)
```

15. BAM User Activity

Question) Open the UserSettings from HKLM\System\ControlSet001\Services\bam . Which executables files did the BAM record for the user (RID 1001). What is the last execution date and time?

Answer:

For the user with RID 1001, 21 executable items were logged by the Background Activity Moderator (BAM) registry entry. The SYSTEM hive file was downloaded using Autopsy, and a registry viewer program was used to analyse and extract this data.

In the BAM list, the most recent entry was:

- **Executable:** Microsoft.LockApp_cw5n1h2txyewy
- **Execution Time: 2024-03-22 19:54:10 CET**

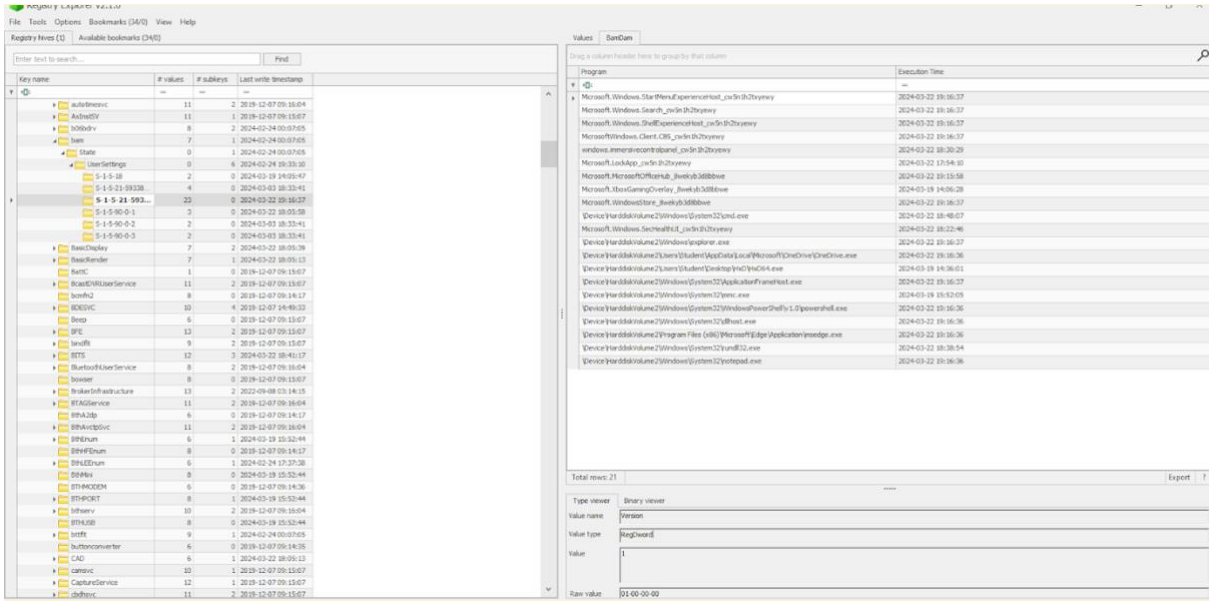
A clear timeline of activity is established by confirming that the user's final execution event happened shortly before the system shutdown.

How it was found:

I used Autopsy to export the SYSTEM hive, then I opened it using a forensic registry analysis application and went to the registry location as follows:

HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-<SID>-1001

The BAM key in the right-hand panel showed a list of the executables that this user has executed, together with the timestamps for each execution. The use of Microsoft.LockApp was last documented on March 22, 2024, at 19:54:10.
The list of executables and the corresponding execution timings are verified in the screenshot below:



16. When T1055.exe and T1036.003.exe was created

Question) When wasT1055.exe and T1036.003.exe was created?

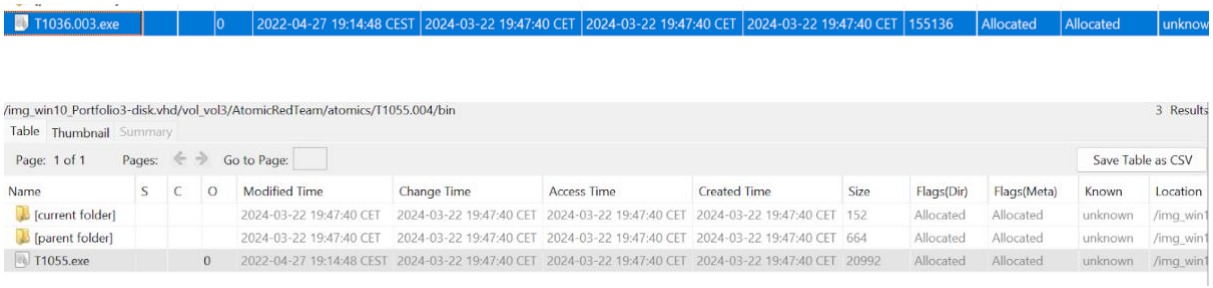
Answer:

I used Autopsy v4.22.1 to look at the metadata of the files T1055.exe and T1036.003.exe in the NTFS file system in order to determine when they were created.

File Name	Created Time	Location
T1055.exe	2024-03-22 19:47:40 CET	vol3\AtomicRedTeam\atomics\T1055.004\bin
T1036.003.exe	2024-03-22 19:47:40 CET	vol3\AtomicRedTeam\atomics\T1036.003\bin

The metadata from the NTFS file system, which is trustworthy for this kind of analysis, was used to get the file creation times. File creation timestamps are not stored in the Windows Registry, therefore using Autopsy to examine metadata is a valid and reliable forensic technique.

The screenshot below confirms the metadata details for both files, and showing creation times for T1036.003.exe and T1055.exe:



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
T1036.003.exe			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	155136	Allocated	Allocated	unknow	

/img_win10_Portfolio3-disk.vhd/vol_vol3/AtomicRedTeam/atomics/T1055.004/bin — 3 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	152	Allocated	Allocated	unknown	/img_win1
[parent folder]				2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	664	Allocated	Allocated	unknown	/img_win1
T1055.exe			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	20992	Allocated	Allocated	unknown	/img_win1

17. number of files that was executed on 22nd March 2024?

Question: How many .exe file was executed on 22nd March 2024?

Answer:

11 executable (.exe) files were executed on the system on March 22, 2024.

How it was found:

I used Autopsy to extract the SYSTEM hive from the disk image, then analysed it with Eric Zimmerman's Registry Explorer. Once the hive was loaded, I navigated to:

\SYSTEM: ControlSet001\Services\bam\State\UserSettings\S-1-5-21-593380826-716814266-1579754837-1001

From there, I then went through each entry's execution timestamp. I was able to identify 11 different.exe files that were executed on **2024-03-22** by filtering for data that had that date.

These included procedures like:

- explorer.exe
- cmd.exe
- msedge.exe
- powershell.exe
- notepad.exe
- And several other

This execution data is important for timeline reconstruction and helps correlate user behaviour or potential malicious activity during the system's final hours. The screenshot below confirms the executable names and execution times:

Program	Execution Time
Microsoft.WindowsStore_8wekyb3d8bbwe	2024-03-22 19:16:37
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2024-03-22 19:16:37
Microsoft.Windows.Search_cw5n1h2txyewy	2024-03-22 19:16:37
Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy	2024-03-22 19:16:37
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2024-03-22 19:16:37
\Device\HarddiskVolume2\Windows\explorer.exe	2024-03-22 19:16:37
MicrosoftWindows.Client.CBS_cw5n1h2txyewy	2024-03-22 19:16:37
\Device\HarddiskVolume2\Users\Student\AppData\Local\Microsoft\OneDrive\OneDrive.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Windows\System32\dllhost.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Windows\System32\notepad.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2024-03-22 19:16:36
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	2024-03-22 19:15:58
\Device\HarddiskVolume2\Windows\System32\cmd.exe	2024-03-22 18:48:07
\Device\HarddiskVolume2\Windows\System32\rundll32.exe	2024-03-22 18:38:54
windows.immersivecontrolpanel_cw5n1h2txyewy	2024-03-22 18:30:29
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy	2024-03-22 18:22:46
Microsoft.LockApp_cw5n1h2txyewy	2024-03-22 17:54:10
\Device\HarddiskVolume2\Windows\System32\mmc.exe	2024-03-19 15:52:05
\Device\HarddiskVolume2\Users\Student\Desktop\HxD\HxD64.exe	2024-03-19 14:36:01
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	2024-03-19 14:06:28

18. Numbers of .dll file was created on *22nd March 2024?*

Question) How many .dll file was created on 22nd March 2024?

Answer:

I used Autopsy to find the number of.dll files produced on March 22, 2024. To filter by Extension → Executable →.dll, I went to the File Views area. I opened the CSV table that I had exported in Excel.
For the date 22.03.2024, I added a custom filter to the Created Time column in Excel. The entire number of.dll files was six complete pages, but only those generated on that particular date were of interest. The final filtered count revealed that on March 22, 2024, 148.dll files were created.

19. Number of Batch (.bat) Files Created on 22nd March 2024

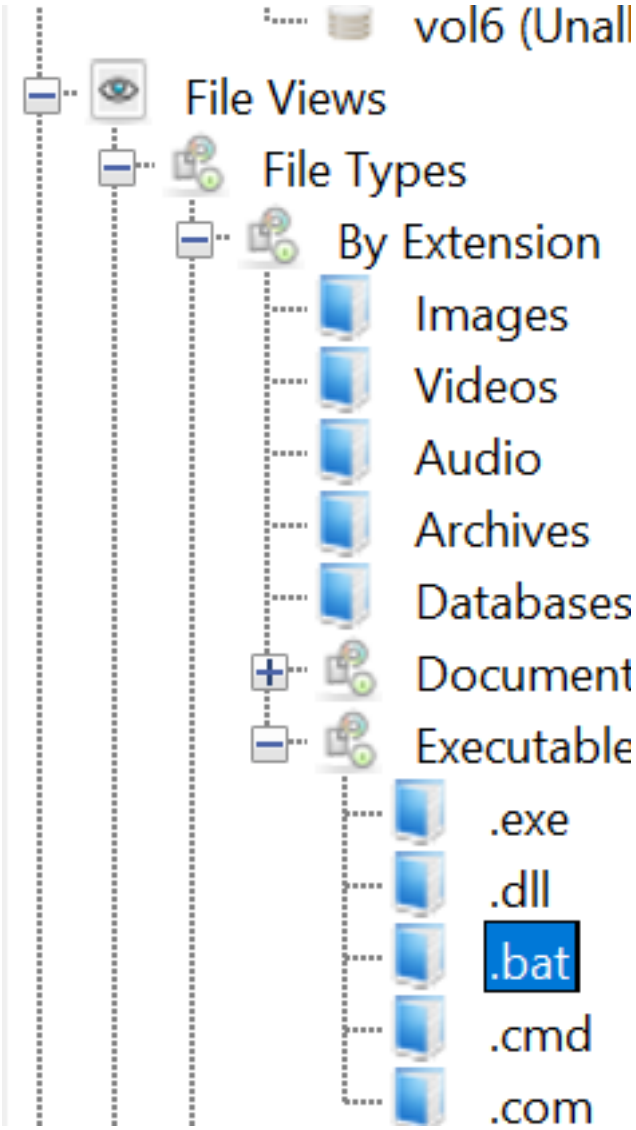
Question: How many .bat files were created on 22nd March 2024?

Answer:
Using Autopsy 4.22.1**,** I navigated to:

File Views > File Types > By Extension > Executable > .bat

I then looked through each.bat file's Created Time column and filtered for files made on March 22, 2024. On that date, 11.bat files were created, according to this.
These files might be associated with scripting, testing, or possibly harmful system activity. Their introduction on the same day is confirmed by the creation time.
The creation times of the.bat files are displayed in the screenshot below:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
batstartup.bat			1	2022-04-27 19:14:48 CEST	2024-03-22 19:47:41 CET	2024-03-22 19:48:02 CET	2024-03-22 19:48:01 CET	34	Allocated	Allocatec
batstartup.bat			1	2022-04-27 19:14:48 CEST	2024-03-22 19:47:41 CET	2024-03-22 19:48:02 CET	2024-03-22 19:48:01 CET	34	Allocated	Allocatec
batstartup.bat			1	2022-04-27 19:14:48 CEST	2024-03-22 19:47:41 CET	2024-03-22 19:47:41 CET	2024-03-22 19:47:41 CET	34	Allocated	Allocatec
build.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:41 CET	2024-03-22 19:47:41 CET	2024-03-22 19:47:41 CET	64	Allocated	Allocatec
T1548.002.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:41 CET	2024-03-22 19:47:41 CET	2024-03-22 19:47:41 CET	258	Allocated	Allocatec
qakbot.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	243	Allocated	Allocatec
T1036.003_test.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	23	Allocated	Allocatec
Psiphon.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	203	Allocated	Allocatec
T1105.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	739	Allocated	Allocatec
parse_net_users.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	642	Allocated	Allocatec
Discovery.bat			0	2022-04-27 19:14:48 CEST	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	2024-03-22 19:47:40 CET	1806	Allocated	Allocatec



20. Verification of Notepad Usage on 22/03/2024

Question) was notepad opened on 22nd March 2024?

Answer:

Yes, Notepad was opened on 22nd March 2024**.**

I confirmed this by returning to Registry Explorer, where I had imported the SYSTEM file earlier:

C:\Users\Yusuf\Downloads\SYSTEM

I went into Registry Explorer and navigated to:

ControlSet001\Services\bam\State\UserSettings\S-1-5-21-593380826-716814266-1579754837-1001

There, under the **BamDam** view, I found the entry for:

\Device\HarddiskVolume2\Windows\System32\notepad.exe

The given execution time of 2024-03-22 19:16:36 verifies that Notepad was actually used on that day

Program	Execution Time
ABC	=
Microsoft.WindowsStore_8wekyb3d8bbwe	2024-03-22 19:16:37
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2024-03-22 19:16:37
Microsoft.Windows.Search_cw5n1h2txyewy	2024-03-22 19:16:37
Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy	2024-03-22 19:16:37
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2024-03-22 19:16:37
\Device\HarddiskVolume2\Windows\explorer.exe	2024-03-22 19:16:37
MicrosoftWindows.Client.CBS_cw5n1h2txyewy	2024-03-22 19:16:37
\Device\HarddiskVolume2\Users\Student\AppData\Local\Microsoft\OneDrive\OneDrive.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Windows\System32\dllhost.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Windows\System32\notepad.exe	2024-03-22 19:16:36
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2024-03-22 19:16:36
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	2024-03-22 19:15:58
\Device\HarddiskVolume2\Windows\System32\cmd.exe	2024-03-22 18:48:07
\Device\HarddiskVolume2\Windows\System32\rundll32.exe	2024-03-22 18:38:54
windows.immersivecontrolpanel_cw5n1h2txyewy	2024-03-22 18:30:29
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy	2024-03-22 18:22:46
Microsoft.LockApp_cw5n1h2txyewy	2024-03-22 17:54:10
\Device\HarddiskVolume2\Windows\System32\mmc.exe	2024-03-19 15:52:05
\Device\HarddiskVolume2\Users\Student\Desktop\HxD\HxD64.exe	2024-03-19 14:36:01
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	2024-03-19 14:06:28

21. Name of the malicious file accessed on 22nd March 2024

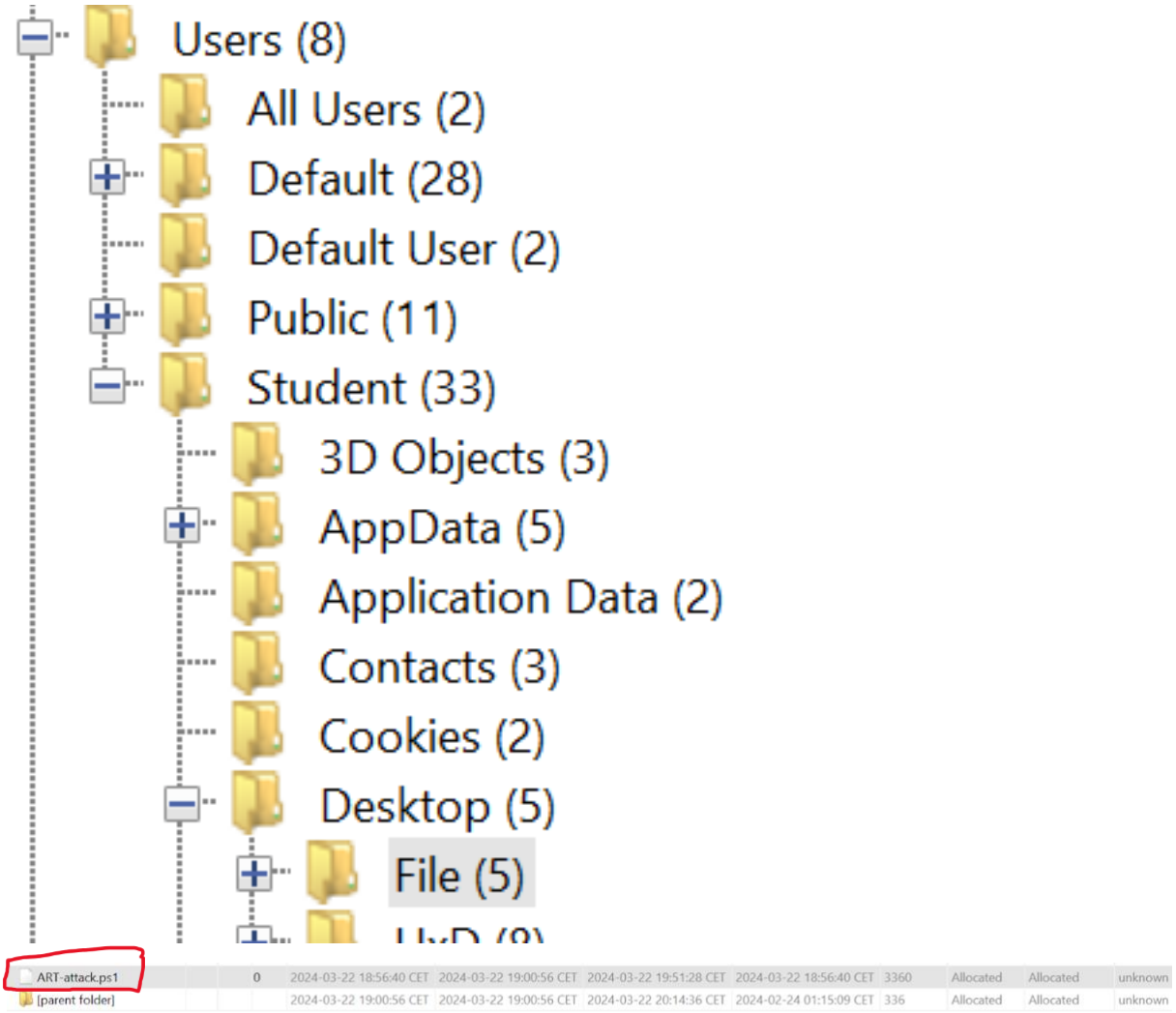
Question: What is the name of the malicious file accessed on 22nd March 2024? by whom and at what time?

Answer:

ART-attack.ps1 is the name of the malicious file that was accessed on March 22, 2024. Using Autopsy, I found it through the directory path ***/vol3/Users/Student/Desktop/File/ART-attack.ps1.*** According to the file information, the user account Student viewed the file on 2024-03-22 at 19:51:28 CET.

This file is a PowerShell script (.ps1), which is frequently used for automated malicious command execution or in attack frameworks. This strongly implies that the file was a

part of illegal or dangerous activities that took place on that day. The screenshots that follow, demonstrate how I accessed this information in Autopsy and show the file's metadata.



22. SYSMON Activity on 22nd March 2024

Question: Is there evidence that the SYSMON program was executed on 22nd March 2024?

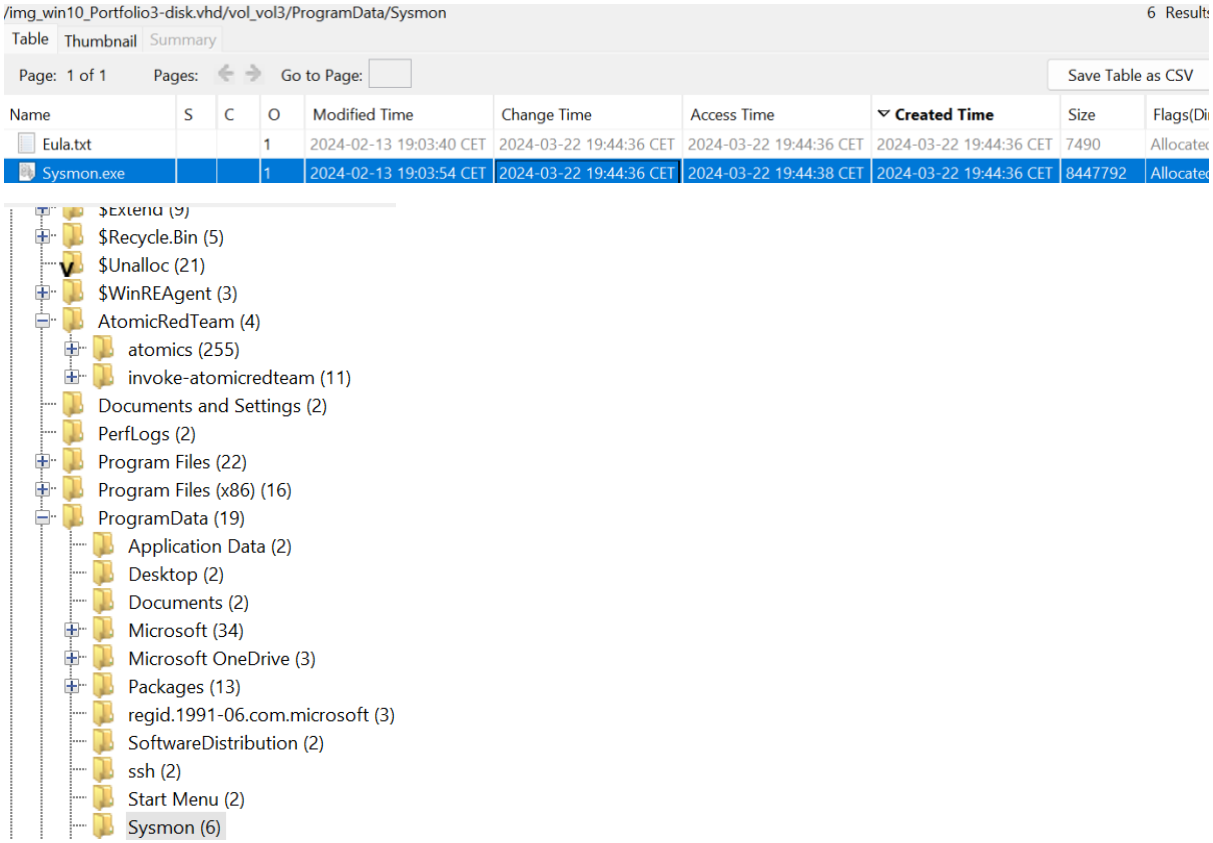
Answer:

Yes, there is proof that on March 22, 2024, Sysmon.exe was accessed. By going to the path **vol3\ProgramData\Sysmon** in Autopsy, I was able to locate

the file.

According to the information, it was last modified at 19:44:36 CET, created at 19:44:36 CET, and accessed at 19:44:38 CET. Sysmon was active during the event period, as indicated by the access timestamp, which strongly implies that the program was launched or interacted with on that day.

The screenshot below shows that indeed *there is evidence that the SYSMON program was executed on 22nd March 2024*



23. Evidence of the AdFind tool

Question) Is there evidence that the AdFind tool was installed and executed on 22nd March 2024?

Yes, there is clear evidence that the **AdFind tool** was present on the system and accessed on **22nd March 2024**.

During my Autopsy forensic analysis, I ran into a problem where the keyword search feature had failed, making it impossible for me to look up filenames like AdFind.exe directly. To find any tools that could be used on the system, I had to manually search through the directory structure.

During my manual navigation, I found AdFind.exe at the following path:

/vol_vol3/AtomicRedTeam/atomics/T1087.002/src

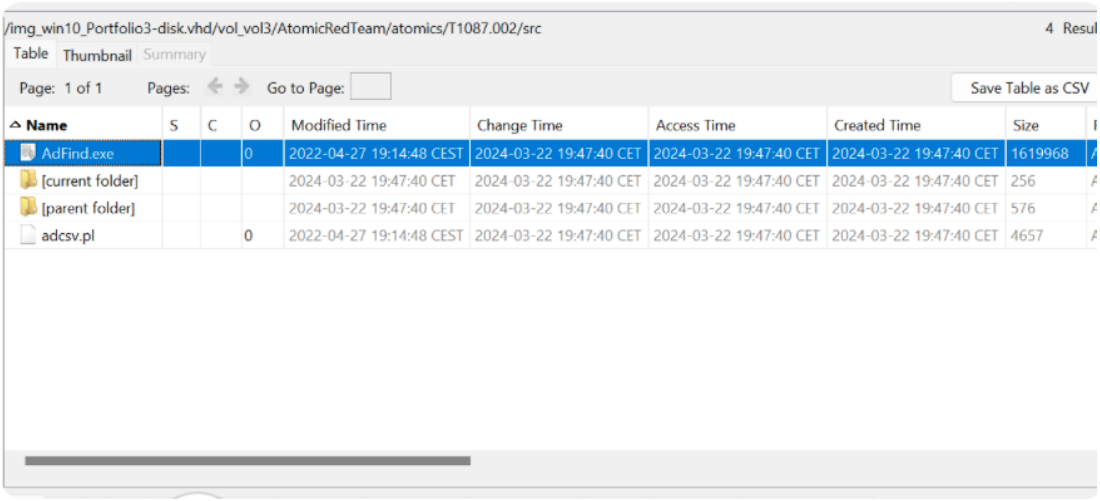
This is a known Active Directory enumeration tool that is frequently used in red teaming or post-exploitation activities. It is a Windows executable (.exe).

Upon reviewing its metadata in Autopsy, I found the following:

- **Created Time**: 2024-03-22 19:47:40 CET
- **Accessed Time**: 2024-03-22 19:47:40 CET
- **Change Time**: 2024-03-22 19:47:40 CET

These timestamps verify that the tool was implemented and most likely used on March 22, 2024, which corresponds to the investigation's date of interest.

Screenshot below:



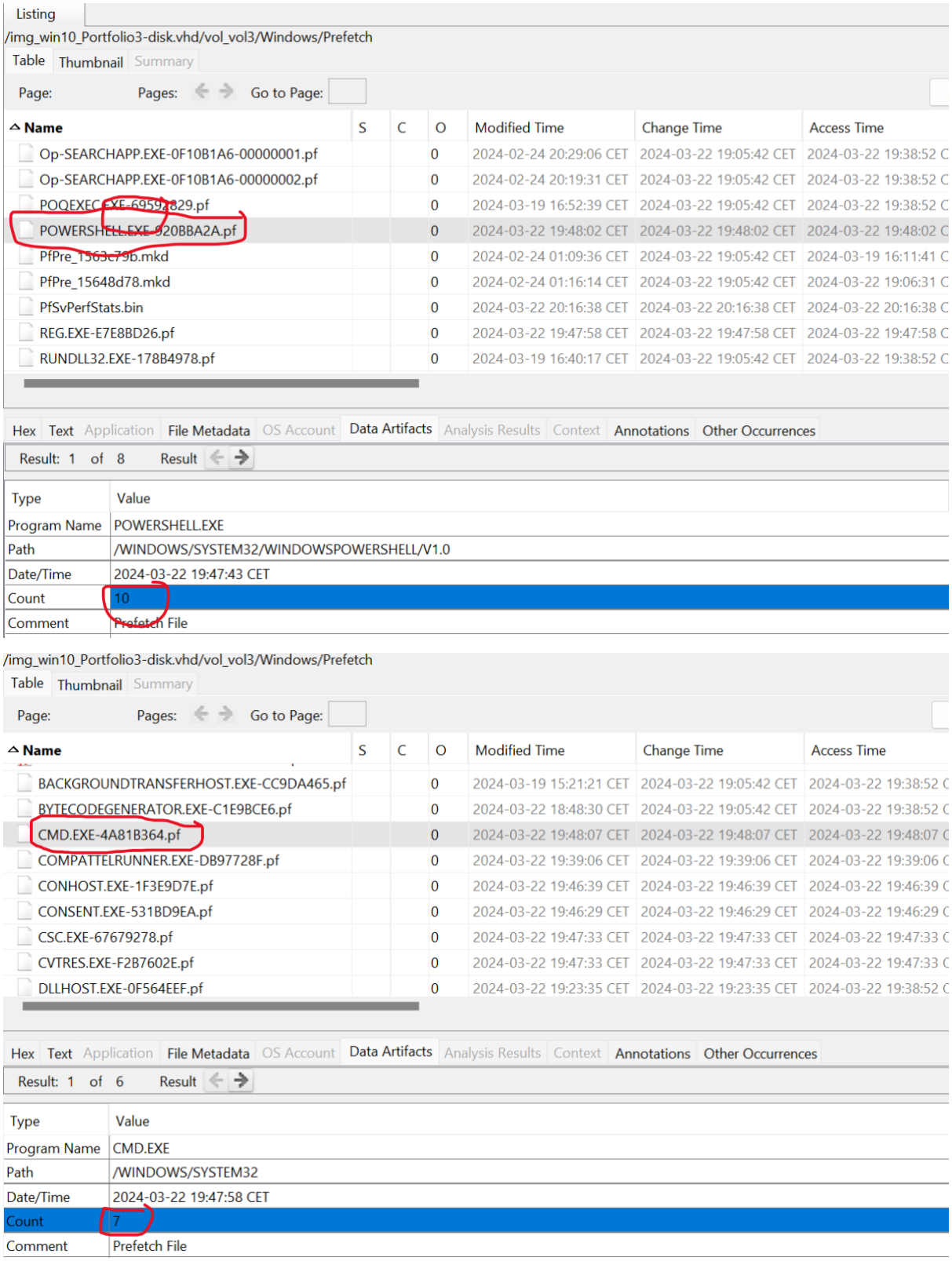
24. Number of times powershell.exe and cmd.exe were executed on 22nd March 2024?

Question) How many times was the command prompt and PowerShell executed on 22nd March 2024

Answer:

Yes, I discovered evidence of how many times PowerShell and Command Prompt were used on March 22, 2024. I used Autopsy to locate the files CMD.EXE-4A81B364.pf and POWERSHELL.EXE-920BBA2A.pf in the vol3\Windows\Prefetchdirectory. Autopsy's metadata view revealed that PowerShell were on the run 10 times, And CMD.EXE were run seven times. Both of them had recorded executions on the timestamps from 2024-03-22, confirming they were used on that date. The execution counts and timestamps, as displayed in Autopsy, are shown in the screenshots below.

.


Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch
Table Thumbnail Summary
Page: Pages: Go to Page:
Name S C O Modified Time Change Time Access Time
Op-SEARCHAPP.EXE-0F10B1A6-00000001.pf 0 2024-02-24 20:29:06 CET 2024-03-22 19:05:42 CET 2024-03-22 19:38:52 C
Op-SEARCHAPP.EXE-0F10B1A6-00000002.pf 0 2024-02-24 20:19:31 CET 2024-03-22 19:05:42 CET 2024-03-22 19:38:52 C
POQEXEC.EXE-69592829.pf 0 2024-03-19 16:52:39 CET 2024-03-22 19:05:42 CET 2024-03-22 19:38:52 C
POWERSHELL.EXE-920BBA2A.pf 0 2024-03-22 19:48:02 CET 2024-03-22 19:48:02 CET 2024-03-22 19:48:02 C
PfPre_1563c79b.mkd 0 2024-02-24 01:09:36 CET 2024-03-22 19:05:42 CET 2024-03-19 16:11:41 C
PfPre_15648d78.mkd 0 2024-02-24 01:16:14 CET 2024-03-22 19:05:42 CET 2024-03-22 19:06:31 C
PfSvPerfStats.bin 0 2024-03-22 20:16:38 CET 2024-03-22 20:16:38 CET 2024-03-22 20:16:38 C
REG.EXE-E7E8BD26.pf 0 2024-03-22 19:47:58 CET 2024-03-22 19:47:58 CET 2024-03-22 19:47:58 C
RUNDLL32.EXE-178B4978.pf 0 2024-03-19 16:40:17 CET 2024-03-22 19:05:42 CET 2024-03-22 19:38:52 C
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Type Value
Program Name POWERSHELL.EXE
Path /WINDOWS/SYSTEM32/WINDOWSPOWERSHELL/V1.0
Date/Time 2024-03-22 19:47:43 CET
Count 10
Comment Prefetch File

/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch
Table Thumbnail Summary
Page: Pages: Go to Page:
Name S C O Modified Time Change Time Access Time
BACKGROUNDTRANSFERHOST.EXE-CC9DA465.pf 0 2024-03-19 15:21:21 CET 2024-03-22 19:05:42 CET 2024-03-22 19:38:52 C
BYTECODEGENERATOR.EXE-C1E9BCE6.pf 0 2024-03-22 18:48:30 CET 2024-03-22 19:05:42 CET 2024-03-22 19:38:52 C
CMD.EXE-4A81B364.pf 0 2024-03-22 19:48:07 CET 2024-03-22 19:48:07 CET 2024-03-22 19:48:07 C
COMPATTELRUNNER.EXE-DB97728F.pf 0 2024-03-22 19:39:06 CET 2024-03-22 19:39:06 CET 2024-03-22 19:39:06 C
CONHOST.EXE-1F3E9D7E.pf 0 2024-03-22 19:46:39 CET 2024-03-22 19:46:39 CET 2024-03-22 19:46:39 C
CONSENT.EXE-531BD9EA.pf 0 2024-03-22 19:46:29 CET 2024-03-22 19:46:29 CET 2024-03-22 19:46:29 C
CSC.EXE-67679278.pf 0 2024-03-22 19:47:33 CET 2024-03-22 19:47:33 CET 2024-03-22 19:47:33 C
CVTRES.EXE-F2B7602E.pf 0 2024-03-22 19:47:33 CET 2024-03-22 19:47:33 CET 2024-03-22 19:47:33 C
DLLHOST.EXE-0F564EEF.pf 0 2024-03-22 19:23:35 CET 2024-03-22 19:23:35 CET 2024-03-22 19:38:52 C
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 6 Result
Type Value
Program Name CMD.EXE
Path /WINDOWS/SYSTEM32
Date/Time 2024-03-22 19:47:58 CET
Count 7
Comment Prefetch File

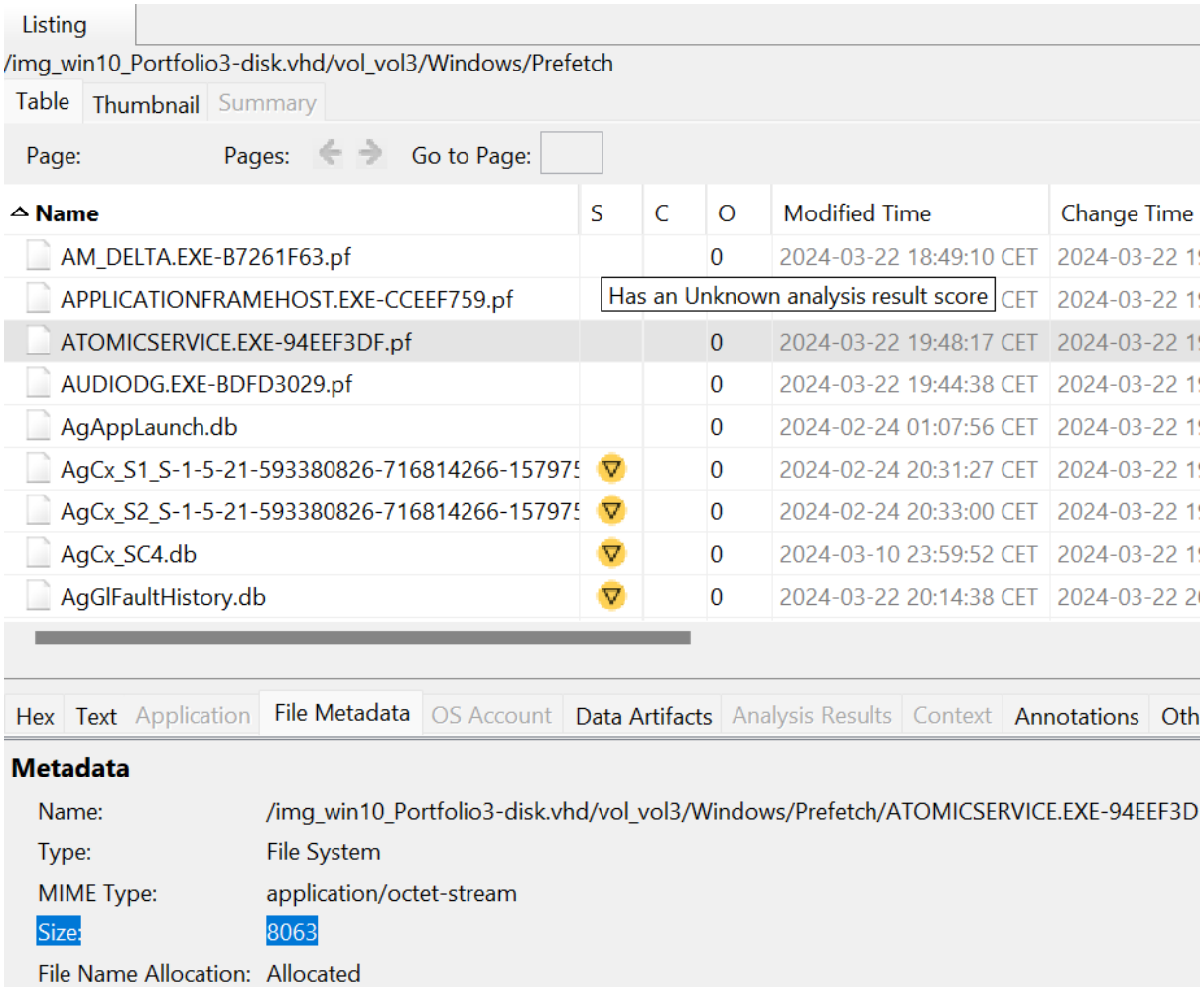
25.Prefetch Analysis: AtomicService.exe's Recorded Size

Question) Open C:\Windows\Prefetch, What size was recorded for AtomicService.exe?

Answer:

I navigated to C:\Windows\Prefetch in autopsy, then I located to the file: ATOMICSERVICE.EXE-94EEF3DF.pf. According to the meta data panel inside of File metadata, the recorded size for ATOMICSERVICE.EXE is **8063 bytes.**

The screenshot following below is confirming the recorded size for ATOMICSERIVICE.EXE



26) Timeline of Suspicious Execution Events via Prefetch

Question: Investigate the C:\Windows\Prefetch path to produce a timeline of suspicious execution events for the following programs:

- POWERSHELL.exe
- cmd.exe
- NET.exe
- REG.exe
- SCHTASKS.exe
- SC.exe
- ATOMICSERVICE.exe
- MAVINJECT.exe
- NOTEPAD.exe

Answer:

I tried using Autopsy to look through the C:\Windows\Prefetch directory, but I could only verify PowerShell, CMD, and Notepad execution data. There were either missing or unreadable prefetch files for NET.exe, REG.exe, SCHTASKS.exe, SC.exe, ATOMICSERVICE.exe, and MAVINJECT.exe.

This could be the result of files being deleted, Prefetch being turned off, or specific circumstances preventing it from generating. I could have extended the analysis if I had had more time.

27. Run Key Path for AtomicService.exe

Question) Investigate the Student NTUSER\Software hive to identify path of the AtomicService.exe file that was added to the run keys?

Answer:

I looked at the NTUSER.DAT hive in the Student user profile in order to determine the path of the AtomicService.exe file added to the Run keys:

/img_win10_Portfolio3-disk.vhd/vol_vol3/Users/Student/NTUSER.DAT

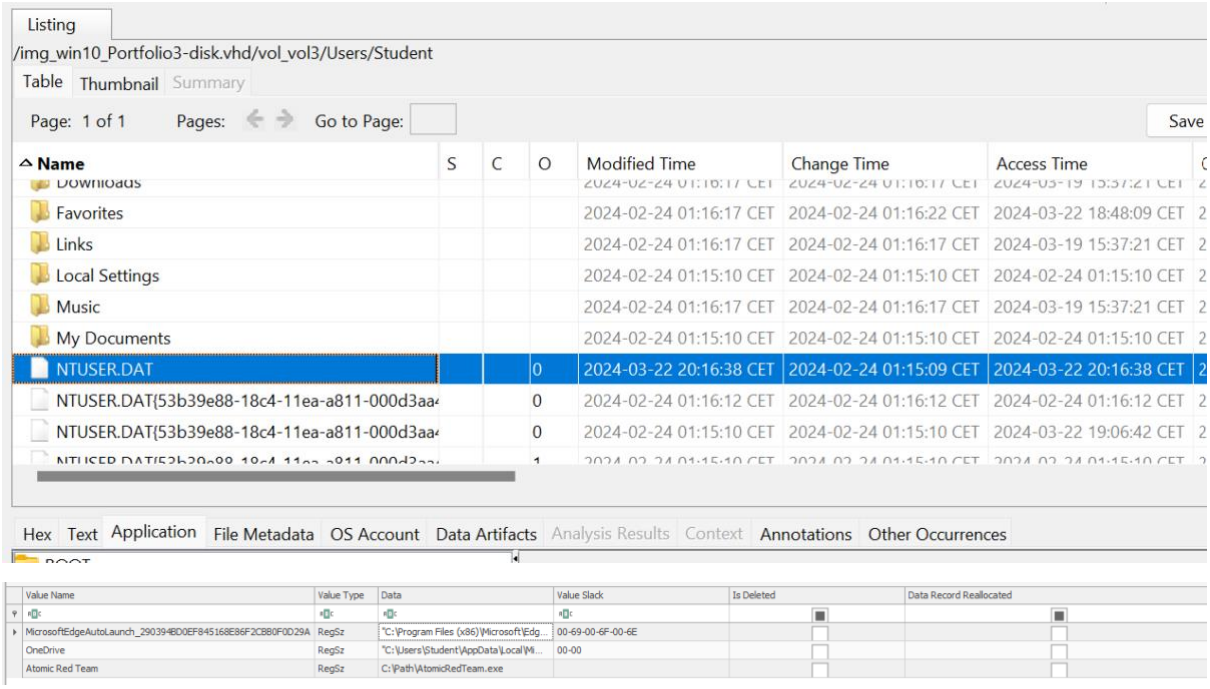
After that I went to the following registry path using Registry Explorer:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run

I discovered an entry with the name Atomic Red Team inside this key, pointing to the executable path:

I C:\Path\AtomicRedTeam.exe

This shows that the AtomicService.exe (also known as Atomic Red Team) was set up to launch automatically from the Windows Run key when the user logged in.



28. Identification of the suspicious script in the StartUp folder

Question) 28. Identify what is the name of the suspicious script in the StartUp folder?

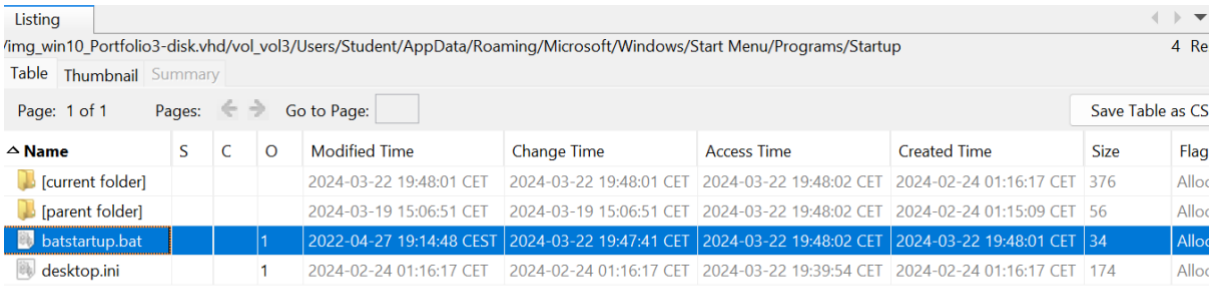
Answer:

Batstartup.bat is the name of the suspicious script located in the StartUp folder.

I used Autopsy to navigate to the following directory in order to find it:

/Users/Student/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup

I discovered batstartup.bat from this folder because of its strange name and the.bat extension, which usually refers to a script intended to run commands at startup.



29. investigation on HKLM\Software hive

Question) Investigate HKLM\Software hive and identify which tasks were scheduled to start at Logon and Startup and how many times they were executed?

Answer:

I used Registry Explorer to look at the SOFTWARE registry hive and see which tasks were set to perform upon logon or startup. I found the following route:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

In this location, I found two scheduled startup entries:

1. **SecurityHealthSystray.exe**

   Path: %windir%\system32\SecurityHealth\Systray.exe
2. **VBoxTray.exe**

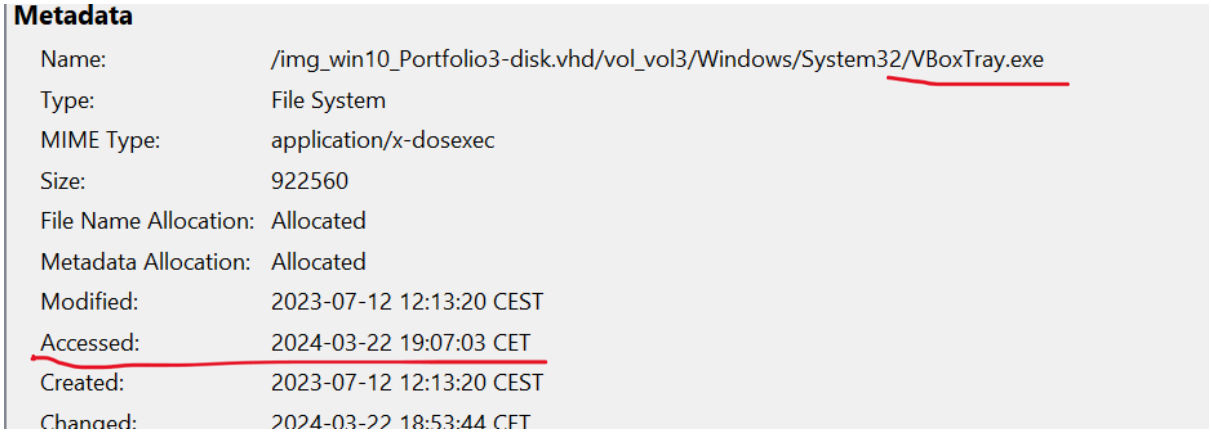
   Path: %SystemRoot%\system32\VBoxTray.exe

The fact that both programs were set up to run automatically upon system startup or user login is confirmed by these entries.

I looked through Autopsy's Windows Prefetch folder to see how many times these programs had run. Nevertheless, neither executable had any.pf files discovered. This can be because the programs don't fulfil the requirements for Prefetch creation, or Prefetch has been cleared or disabled.

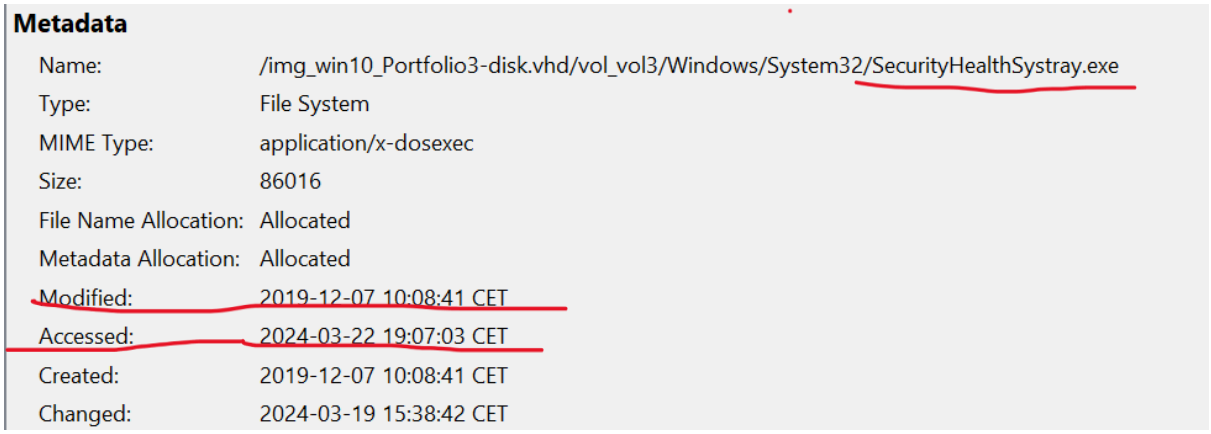
Instead, I used Autopsy to look at the file metadata. The Accessed timestamp of 2024-03-22 19:07:03 CET was displayed in both files, confirming that both programs were accessed and, most likely, run on that day.

In conclusion, the accessed timestamps of SecurityHealthSystray.exe and VBoxTray.exe in the file system metadata show that they were both run on **March 22, 2024**, even though they were both scheduled to start at logon.



Metadata

Name:	/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/System32/VBoxTray.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	922560
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-07-12 12:13:20 CEST
Accessed:	2024-03-22 19:07:03 CET
Created:	2023-07-12 12:13:20 CEST
Changed:	2024-03-22 18:53:44 CET



Metadata

Name:	/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/System32/SecurityHealthSystray.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	86016
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-12-07 10:08:41 CET
Accessed:	2024-03-22 19:07:03 CET
Created:	2019-12-07 10:08:41 CET
Changed:	2024-03-19 15:38:42 CET

Wow Factor - Investigation of Suspicious Script ART-attack.ps1

As part of my extended forensic analysis, I focused on a suspicious PowerShell script named ART-attack.ps1, located at the following path:

/vol3/Users/Student/Desktop/File/ART-attack.ps1

Just minutes before the ultimate system shutdown, on March 22, 2024, at 19:51:28 CET, the user "student" accessed the script. The script's name, file type, location, and the timing of this access immediately raised concerns about malicious activity.

ART-attack.ps1 is not a harmless file, as I confirmed after extracting the script from Autopsy and reviewing its contents. It is a PowerShell script that executes a series of high-risk simulations replicating real-world cyberattacks, automatically installing the Atomic Red Team framework, a widely used attack simulation toolkit. These simulations align with several MITRE ATT&CK techniques, including:

- **Phishing simulation (T1566.001):** downloading a macro-enabled attachment
- **Fileless script execution (T1059.001):** running PowerShell scripts in memory
- **Service creation and manipulation (T1543.003)**
- **Persistence mechanisms (T1547.001, T1053.005):** via registry and scheduled tasks
- **Process injection (T1055.001)**
- **Privilege escalation (T1078.003):** creating a local account with admin rights
- **Anti-forensic activity (T1070.004):** deleting logs or evidence

The student accessed the script just before the system's final shutdown. Using Invoke-AtomicTest, which executes specific Atomic Red Team modules, the techniques mentioned above were replicated. Several aspects of this script are particularly alarming:

- It was run from a regular user’s desktop (a student), not from a red team environment or administrative toolkit.
- The timestamp of execution (19:51:28) corresponds with other suspicious activity: execution of *AdFind.exe*, creation of the *art-test* account, and system logon/shutdown events.
- The script downloads and installs third-party tools, introducing further potential risk to the system.
- It spans multiple stages of the cyber kill chain from initial access to defence evasion, suggesting a deliberate attempt to simulate or carry out a full-scale penetration.

All evidence indicates that the user "student" was not acting in an administrative or conventional capacity. More likely, the user was intentionally initiating attack simulations or performing unauthorised security testing. While it remains unclear whether this was a legitimate red-team exercise or a potential insider attack, the behaviour, timing, and automation of the script strongly suggest hostile intent.

By correlating registry traces, file system metadata, and script analysis, this case demonstrates how a single file can reveal a complex sequence of covert operations. It also highlights the importance of linking user activity to tool usage and execution timing in forensic investigations to uncover suspicious behaviour.

Screenshots Below:

```
#TODO - check if ART framework is already installed

#Install Execution Framework and Atomics Folder

Write-Output "Installing AtomicRedTeam"
Write-Output "================================"
IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);
Install-AtomicRedTeam -RepoOwner bluecapesecurity

Write-Output "Installing AtomicsFolder...this might take a few minutes."
IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicsfolder.ps1' -UseBasicParsing);
Install-AtomicsFolder -Force -Branch 724cb3f50dcdd341815d5d2f34cbf90168017404

# Starting atomics attack simulation

Write-Output "Starting ART attack simulation"
Write-Output "================================"


# initial-access
#

"T1566.001 Atomic Test #1 - Download Macro-Enabled Phishing Attachment"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1566.001/T1566.001.md#atomic-test-1---download-macro-enabled-phishing-attachm
ent
Invoke-AtomicTest T1566.001 -TestNumbers 1

Start-Sleep -s 2
```

```
Start-Sleep -s 2

"T1543.003 Atomic Test #2 - Service Installation CMD"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1543.003/T1543.003.md#atomic-test-2---service-installation-cmd
Invoke-AtomicTest T1543.003 -TestNumbers 2

Start-Sleep -s 2

# defense-evasion

"T1055.001 Atomic Test #1 - Process Injection via mavinject.exe"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1055.001/T1055.001.md#atomic-test-1---process-injection-via-mavinjectexe
Invoke-AtomicTest T1055.001 -TestNumbers 1

Start-Sleep -s 2

"T1070.004 Atomic Test #6 - Delete a single file - Windows PowerShell"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1070.004/T1070.004.md#atomic-test-6---delete-a-single-file---windows-powershell
Invoke-AtomicTest T1070.004 -TestNumbers 6 -GetPrereqs
Invoke-AtomicTest T1070.004 -TestNumbers 6


------------------------------METADATA------------------------------
```

Component 3: Executive Summary

The investigation's main focus was a possible insider attack on a virtual machine (VM) This investigation looked into a suspected insider attack on a Windows 10 virtual machine. The focus was on identifying any signs of malicious activity and understanding what happened in the lead-up to the system shutdown on **March 22, 2024, at 19:51:28 CET**. The most concerning discovery was the execution of a PowerShell script called **ART-attack.ps1**by the user **"student"**, shortly before the system went down.

The script wasn’t harmless, it automatically installed the Atomic Red Team framework and ran simulations that matched real-world cyberattack techniques. These included phishing, persistence, process injection, privilege escalation, and log deletion. What raised further concern was that this activity came from a standard user account, not from a controlled testing or red-team environment.

To investigate this, I used tools like **Autopsy**, **Registry Explorer**, Power shell, and **Volatility**. I examined registry hives, BAM logs, system metadata, and user activity. The evidence clearly showed that the user "student" created new accounts, ran external tools like **AdFind.exe**, and triggered multiple stages of the cyber kill chain, all in a very short time window.

The behaviour, combined with the timing and the nature of the script, strongly suggested that this was either an unauthorised red-team simulation or a deliberate insider attack.

References

- Atomic Red Team. (n.d.) *Atomic Red Team*. Available at: https://github.com/redcanaryco/atomic-red-team (Accessed: 4 May 2025).
- Autopsy. (n.d.) *Autopsy: Digital Forensics Platform*. Available at: https://www.autopsy.com/ (Accessed: 2 May 2025).
- CACI. (n.d.) *What is digital forensics?* Available at: https://www.caci.co.uk/insights/opinions/what-is-digital-forensics/(Accessed: 6 May 2025).
- Eric Zimmerman. (n.d.) *Registry Explorer*. Available at: https://ericzimmerman.github.io/ (Accessed: 3 May 2025).
- Eric Zimmerman. (n.d.) *RegistryPlugins – GitHub Repository*. Available at: https://github.com/EricZimmerman/RegistryPlugins (Accessed: 5 May 2025).
- Joeware. (n.d.) *AdFind Tool*. Available at: https://www.joeware.net/freetools/tools/adfind/ (Accessed: 5 May 2025).
- MITRE. (n.d.) *MITRE ATT&CK Framework*. Available at: https://attack.mitre.org/ (Accessed: 1 May 2025).
- The Volatility Foundation. (n.d.) *The Volatility Framework*. Available at: https://www.volatilityfoundation.org/ (Accessed: 7 May 2025).

- Infosec Institute, 2021. *7 Best Computer Forensics Tools [Updated 2021]*. [online] Available at: https://www.infosecinstitute.com/resources/digital-forensics/7-best-computer-forensics-tools/ [Accessed 6 May 2025].