Digital Forensics: CMP020N210S

Portfolio 3 – Forensic Analysis of an Attack

STUDENT NAME: Sawsan Mounes

STUDENT ID: Mou23620003

BSc. CYBER SECURITY

Table of Contents

Component 1 6

Verification of Evidence Integrity 6

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? 7

Approach 7
Methodology 7
Findings 7
Evidence 8

Who is the owner of this device? 9

Approach 9
Methodology: 9
Findings 9
Evidence : 9

What is the Time zone setting. 10

Approach 10
Methodology: 10
Findings 10
Evidence 11

What is the Device ID for the win10_Portfolio3-disk.vhd? 12

Approach 12

Methodology: 12
Findings: 12
Evidence 13

Identify the information of network interface(s) with an IP address assigned by DHCP? What a is DHCP IP Address? 14

Approach 14
Methodology: 14
Findings 14
Evidence 15

How many user accounts are listed? 16

Approach: 16
Methodology 16
Findings 16
Evidence 17

Who was the last user to log in to the PC? 18

Approach 18
Methodology: 18
Findings 18
Evidence 19

Identify what is the account name of the user who mostly uses the computer? 20

Approach: 20

Methodology: 20
Findings: 20
Evidence 21

Identify when was the last recorded computer shutdown date/time? 22

Approach: 22

Methodology: 22
Findings: 22
Evidence: 23

Which user was logged into the device on 22nd March 2024 24
Approach: 24
Methodology: 24
Findings: 24
Evidence: 25

Which account(s) were created on 22nd March 2024 and at what time? 26
Approach: 26
Methodology: 26
Findings: 26
Evidence: 27

Investigate user accounts and identify which accounts are administrator group members? 28
Approach: 28
Methodology: 28
Findings: 28
Evidence 29

How many files are under AtomicRedTeam? 30
Approach: 30
Methodology: 30
Findings: 30
Evidence 31

What is the Parent MFT Entry Number for the file "ART-attack.ps1"? 32
Approach: 32
Methodology: 32
Tool Used: Autopsy 32
Findings: 32
Evidence 33

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? 34
Approach: 34
Methodology: 34
Findings: 34
Evidence 35

When T1055.exe and T1036.003.exe were created? 37
Approach: 37
Methodology: 37
Findings: 38
Evidence: 38

Was Notepad opened on 22nd March 2024? 40
Approach: 40
Methodology: 40
Findings: 40
Evidence 40

How many .exe file was executed on 22nd March 2024? 41
Approach: 41
Methodology 41
Findings 41

Evidence 41

How many .dll file was created on 22nd March 2024? 42
Approach 42
Methodology 42
Findings 42
Evidence 42

How many .bat file was created on 22nd March 2024? 44
Approach: 44
Methodology: 44
Findings: 44
Evidence: 44

What is the name of the malicious file accessed on 22nd March 2024? by whom and at what time? 45
Approach: 45
Methodology: 45
Findings: 45
Evidence: 46

Is there evidence that the SYSMON program was executed on 22nd March 2024? ... 47
Approach: 47
Methodology: 47
Findings: 47
Evidence : 48

Is there evidence that the AdFind tool was installed and executed on 22nd March 2024? 50
Approach: 50
Methodology: 50
Findings: 51
Evidence: 51

How many times was the command prompt and PowerShell executed on 22nd March 2024? 54
Approach: 54
Methodology: 54
Findings: 54
Evidence: 55

What size was recorded for AtomicService.exe? 57
Approach: 57
Methodology: 57
Findings: 57
Evidence: 58

Investigate C:\Windows\Prefetch path to produce a timeline of suspicious execution events for the following programs: 59
Approach: 59
Methodology: 59
Findings: 60
Evidence: 62

Investigate the Student NTUSER\Software hive to identify path of the AtomicService.exe file that was added to the run keys. 63
Approach: 63
Methodology: 63
Findings: 63
Evidence 63

Identify what is the name of the suspicious script in the StartUp folder? 64
Approach: 64
Methodology: 64
Findings: 64
Evidence: 64

Investigate HKLM\Software hive and identify which tasks were scheduled to start at Logon and Startup and how many times they were executed? 65
Approach: 65
Methodology: 65
Findings: 65
Evidence: 66

Component 2 67

Verification of Evidence Integrity 67

Provide additional evidence by carrying out an investigation of digital forensics artefacts such as log files or memory or file system. For example, analyse win10-Portfolio3-memory.raw using the Volatility tool and provide a timeline of execution events and identifying process owners and SIDs for the relevant programmes. 67
Volatility Plugin Analysis Summary 71

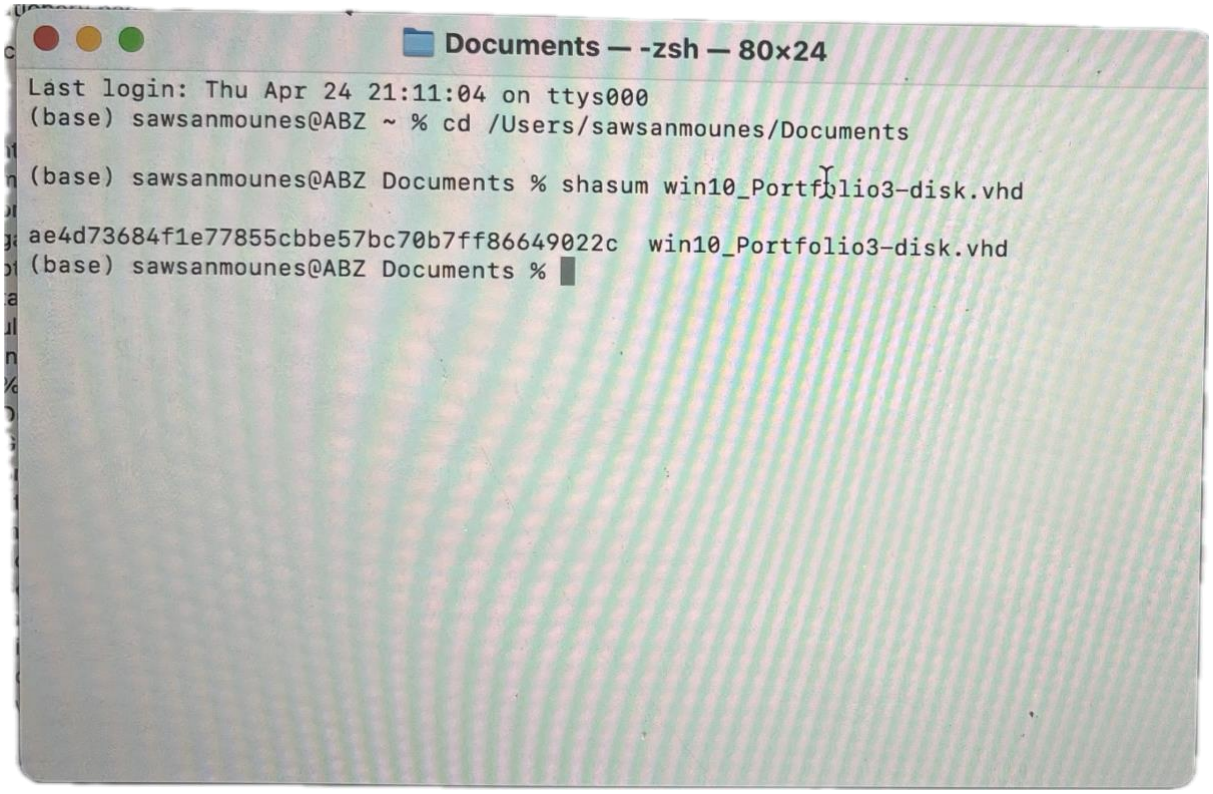
Component 3 76

Executive Summary and Reflection 76
Scope of Analysis and Integrity Validation 76
Analytical Methodology 76
Key Findings 77
Analyst Observation – Possible Network Surveillance 77
Reflection and Learning Experience 78
What I Would Do Differently 78

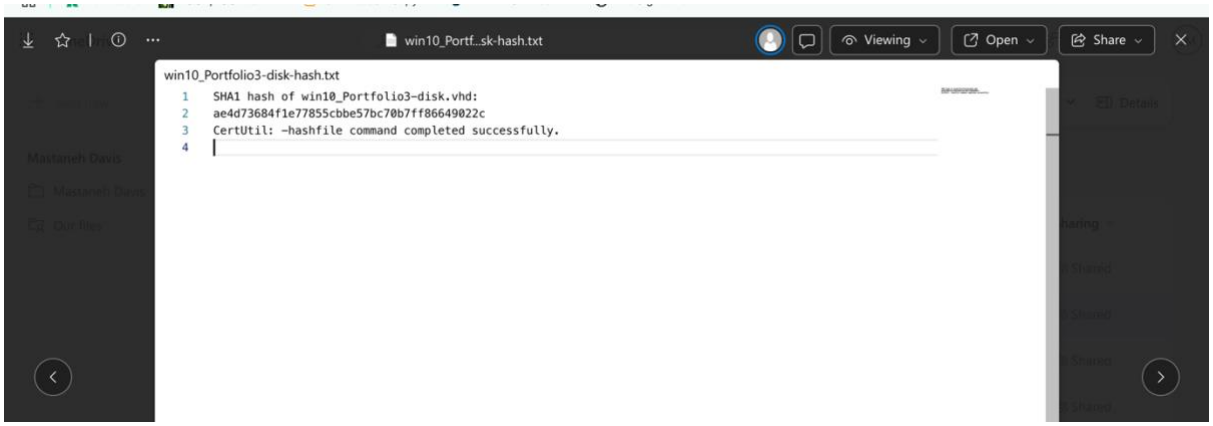
References 79

Component 1

Verification of Evidence Integrity



Verification matched against given hash.



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?

Approach

The forensic image (win10_Portfolio3-disk.vhd) was acquired by our cybersecurity team to investigate potential malicious software activity. Our first step was to identify the operating system because different OS types store forensic evidence differently. Windows uses Registry files, event logs, and Prefetch files, while macOS uses different metadata and logs. Even different versions, like Windows 10 and Windows 7, handle user tracking and security settings differently. Knowing the operating system allowed us to properly locate and analyse the necessary forensic artifacts.

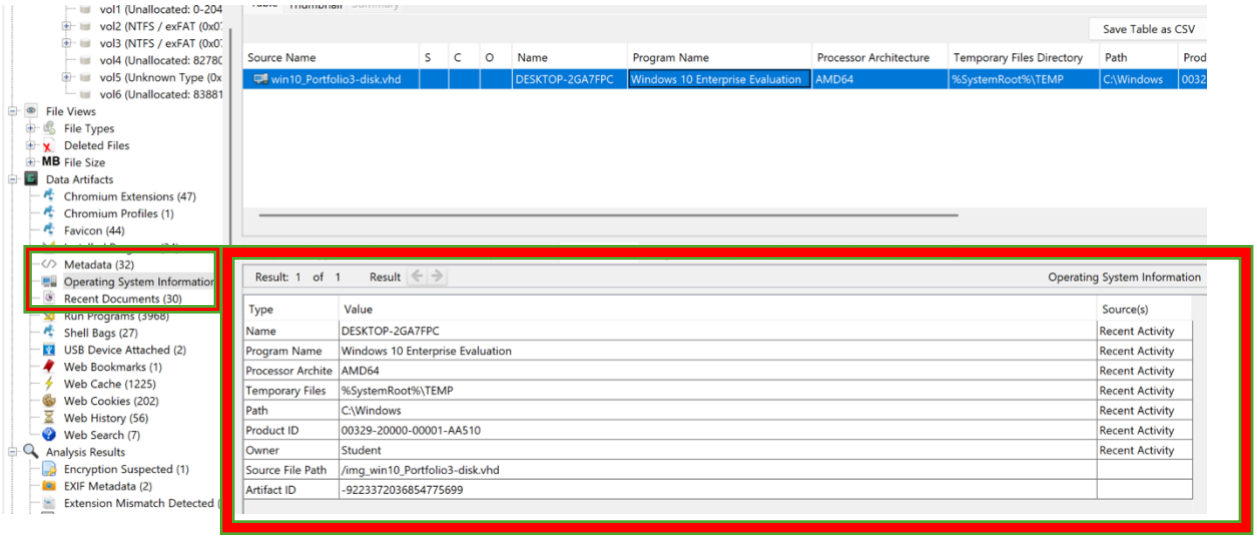
Methodology

Tools: Autopsy
The win10_Portfolio3-disk.vhd forensic image was mounted into Autopsy.
I navigated to the Data Artifacts section and then selected Operating System Information under the available artifacts.
This section displayed key information about the system, including the computer name, source file, file path, processor architecture, and the installed operating system version.

Findings

operating system artifact information	Details
Program name	**Windows 10 Enterprise Evaluation**
Computer Name	**DESKTOP-2GA7FPC**
Source File	**win10_Portfolio3-disk.vhd**
Path	**C:\Windows**

Evidence


vol1 (Unallocated: 0-204
vol2 (NTFS / exFAT (0x0
vol3 (NTFS / exFAT (0x0
vol4 (Unallocated: 8278
vol5 (Unknown Type (0x
vol6 (Unallocated: 83881
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (47)
Chromium Profiles (1)
Favicon (44)
Metadata (32)
Operating System Information
Recent Documents (30)
Run Programs (3968)
Shell Bags (27)
USB Device Attached (2)
Web Bookmarks (1)
Web Cache (1225)
Web Cookies (202)
Web History (56)
Web Search (7)
Analysis Results
Encryption Suspected (1)
EXIF Metadata (2)
Extension Mismatch Detected
Save Table as CSV
Source Name S C O Name Program Name Processor Architecture Temporary Files Directory Path Prod
win10_Portfolio3-disk.vhd DESKTOP-2GA7FPC Windows 10 Enterprise Evaluation AMD64 %SystemRoot%\TEMP C:\Windows 0032
Result: 1 of 1 Result
Operating System Information
Type Value Source(s)
Name DESKTOP-2GA7FPC Recent Activity
Program Name Windows 10 Enterprise Evaluation Recent Activity
Processor Archite AMD64 Recent Activity
Temporary Files %SystemRoot%\TEMP Recent Activity
Path C:\Windows Recent Activity
Product ID 00329-20000-00001-AA510 Recent Activity
Owner Student Recent Activity
Source File Path /img_win10_Portfolio3-disk.vhd
Artifact ID -9223372036854775699

Who is the owner of this device?

Approach

The goal was to identify the registered owner of the device to link the system to a user. Since the operating system information was already examined, I continued by reviewing the same Operating System Information artifact in Autopsy.

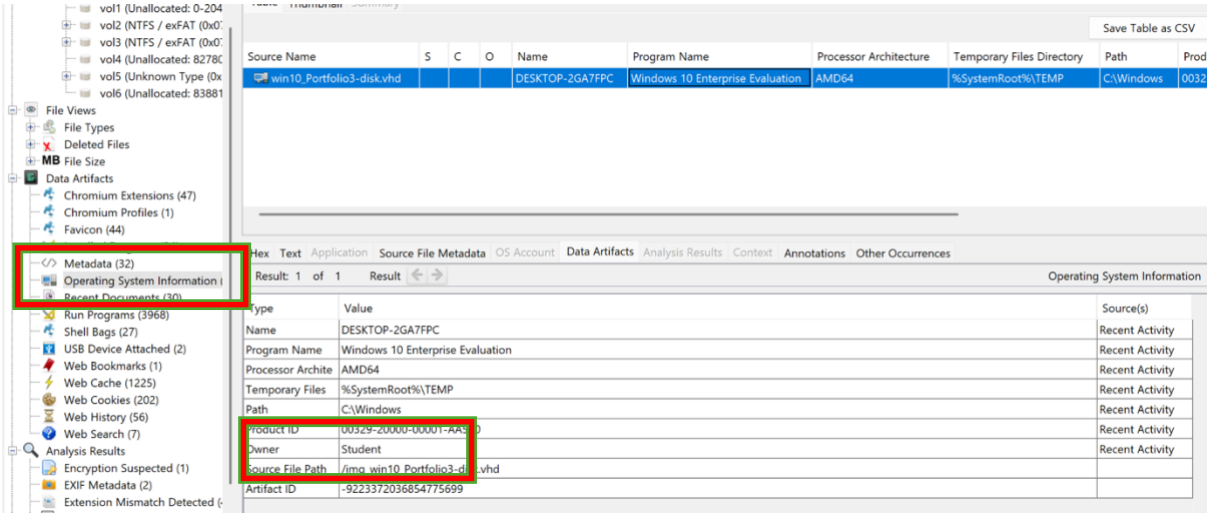
Methodology:

Tools: Autopsy
After mounting win10_Portfolio3-disk.vhd in Autopsy, I accessed the Data Artifacts section and selected Operating System Information. Same approach as I did to find the operating system I located the Owner field.

Findings

Owner: Student

Evidence :



What is the Time zone setting.

Approach

Finding the correct time zone of the suspect's device is important to make sure all the dates and times on the files and records are accurate.
If the time zone is wrong or unknown, it can cause mistakes when building a timeline of events. At the start of the investigation, I checked the time zone settings so that I could correctly match up activities on this device.

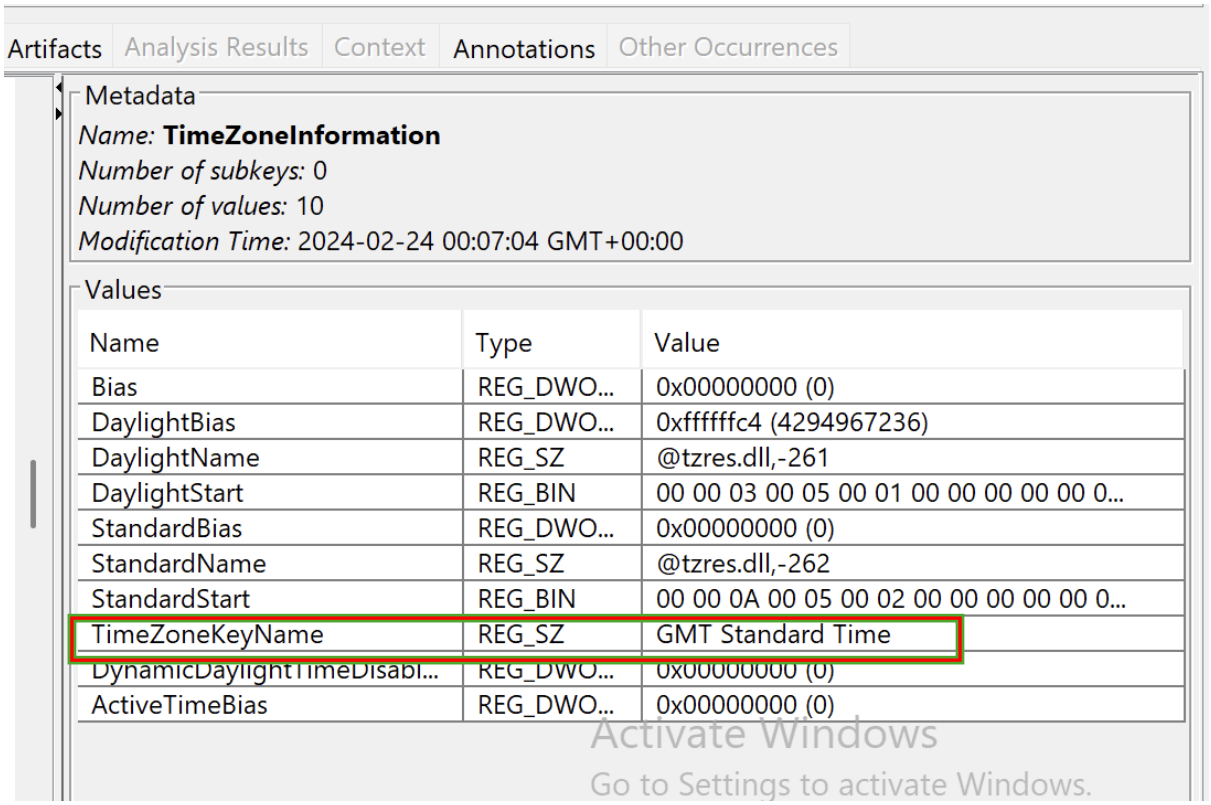
Methodology:

Tools Autopsy
I used Autopsy to extract the SYSTEM hive from the forensic image.: SYSTEM\CurrentControlSet\Control\TimeZoneInformation.In this location, I found the time zone settings.

Findings

I extracted the TimeZoneInformation key from the SYSTEM hive and reviewed the values. The TimeZoneKeyName field showed "GMT Standard Time", confirming the device was set to Greenwich Mean Time (GMT).

Evidence


Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Metadata
Name: TimeZoneInformation
Number of subkeys: 0
Number of values: 10
Modification Time: 2024-02-24 00:07:04 GMT+00:00
Values
Name
Type
Value
Bias
REG_DWO...
0x00000000 (0)
DaylightBias
REG_DWO...
0xffffffc4 (4294967236)
DaylightName
REG_SZ
@tzres.dll,-261
DaylightStart
REG_BIN
00 00 03 00 05 00 01 00 00 00 00 00 0...
StandardBias
REG_DWO...
0x00000000 (0)
StandardName
REG_SZ
@tzres.dll,-262
StandardStart
REG_BIN
00 00 0A 00 05 00 02 00 00 00 00 00 0...
TimeZoneKeyName
REG_SZ
GMT Standard Time
ActiveTimeBias
REG_DWO...
0x00000000 (0)
Activate Windows
Go to Settings to activate Windows.

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

Approach

To find the Device ID for the win10_Portfolio3-disk.vhd, I looked at the GUID (Globally Unique Identifier) displayed under the Windows\System32\config\SOFTWARE\Microsoft\Cryptography in Autopsy.
The GUID acts as a unique identifier for the device, making it important to find it early in the investigation. Identifying the correct GUID ensures that all evidence is accurately linked to the correct system. It also helps distinguish this device from others, supports building an event timeline, verifies the integrity of the evidence, and assists in linking devices to incidents if needed. This is critical for maintaining the chain of custody.

Methodology:

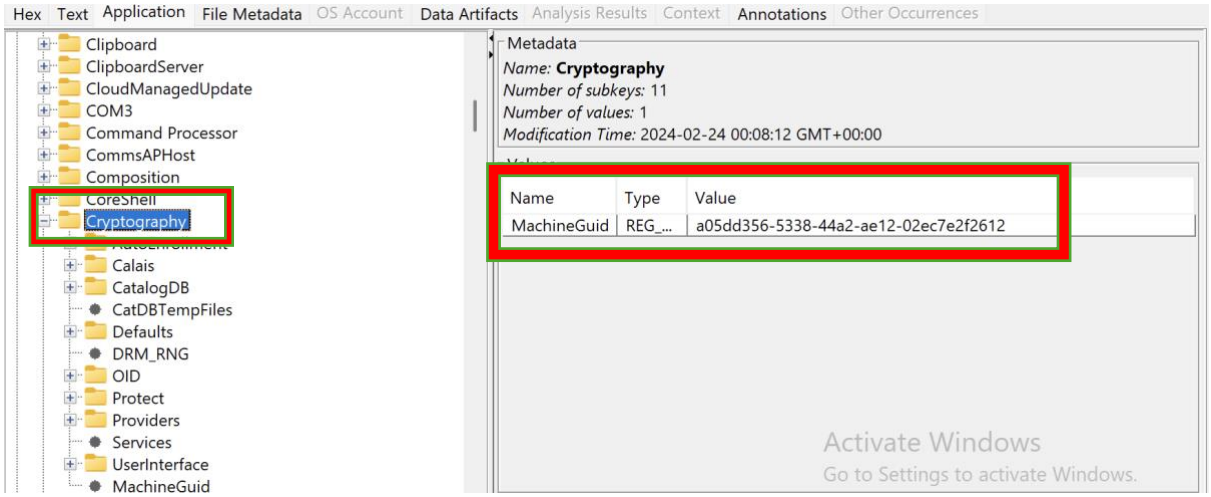
Tools: Autopsy

I mounted the win10_Portfolio3-disk.vhd forensic image into Autopsy.
Inside Autopsy, I navigated to the Extracted Content → Windows Registry → SOFTWARE hive.
From there, I browsed to the path: Microsoft\Cryptography where the MachineGuid value was listed. This GUID provided the Device ID for the system.

Findings:

MachineGuid : a05dd356-5338-44a2-ae12-02ec7e2f2612

Evidence


Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Clipboard
ClipboardServer
CloudManagedUpdate
COM3
Command Processor
CommsAPHost
Composition
CoreShell
Cryptography
Calais
CatalogDB
CatDBTempFiles
Defaults
DRM_RNG
OID
Protect
Providers
Services
UserInterface
MachineGuid
Metadata
Name: Cryptography
Number of subkeys: 11
Number of values: 1
Modification Time: 2024-02-24 00:08:12 GMT+00:00
Name
Type
Value
MachineGuid
REG_...
a05dd356-5338-44a2-ae12-02ec7e2f2612
Activate Windows
Go to Settings to activate Windows.

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

Approach

To identify the network interface with an IP address assigned by DHCP, I examined the registry data in the forensic image using Autopsy. Since DHCP automatically assigns IP addresses to devices, checking the network configuration helps determine how the device vice connected to the network. I specifically looked for IP addresses assigned through DHCP to understand the network setup and any possible external connections the device made.

Methodology:

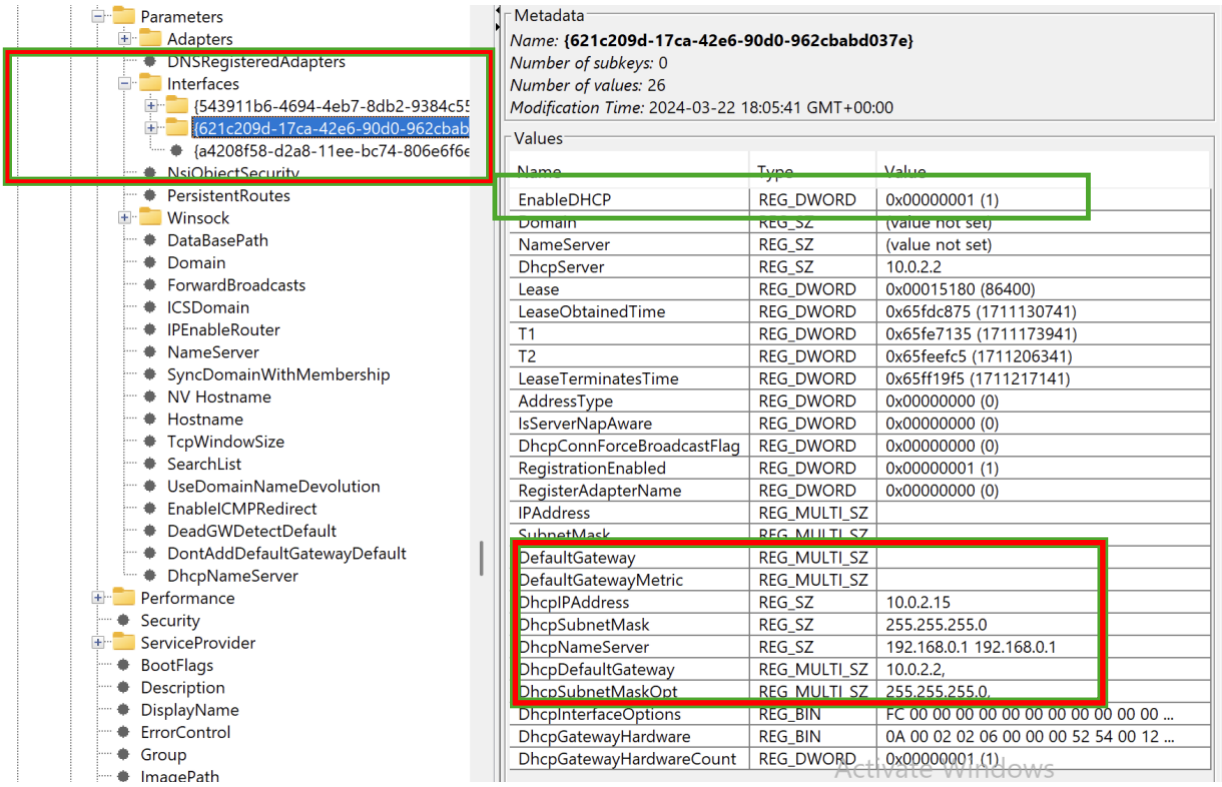
Tools: Autopsy

I navigated to the extracted registry files and opened the following path inside the SYSTEM hive:CurrentControlSet\Services\Tcpip\Parameters\Interfaces.Under this location, I reviewed the different network interfaces listed. I checked each interface's settings to find entries showing DHCP enabled (like DhcpIPAddress, DhcpSubnetMask, and DhcpServer). I identified the network interface and recorded the DHCP IP address assigned to the device.

Findings

Inside the Interfaces folder, I located a network interface showing DHCP settings enabled (EnableDHCP = 0x1). The DhcpIPAddress field showed that the IP address assigned by DHCP was 192.168.0.105. Other related fields like DhcpSubnetMask and DhcpDefaultGateway confirmed that this IP was dynamically assigned.

Evidence


Parameters
Adapters
DNSRegisteredAdapters
Interfaces
{543911b6-4694-4eb7-8db2-9384c5
{621c209d-17ca-42e6-90d0-962cbab
{a4208f58-d2a8-11ee-bc74-806e6f6e
NsiObjectSecurity
PersistentRoutes
Winsock
DataBasePath
Domain
ForwardBroadcasts
ICSDomain
IPEnableRouter
NameServer
SyncDomainWithMembership
NV Hostname
Hostname
TcpWindowSize
SearchList
UseDomainNameDevolution
EnableICMPRedirect
DeadGWDetectDefault
DontAddDefaultGatewayDefault
DhcpNameServer
Performance
Security
ServiceProvider
BootFlags
Description
DisplayName
ErrorControl
Group
ImagePath
Metadata
Name: {621c209d-17ca-42e6-90d0-962cbabd037e}
Number of subkeys: 0
Number of values: 26
Modification Time: 2024-03-22 18:05:41 GMT+00:00
Values
Name
Type
Value
EnableDHCP
REG_DWORD
0x00000001 (1)
Domain
REG_SZ
(value not set)
NameServer
REG_SZ
(value not set)
DhcpServer
REG_SZ
10.0.2.2
Lease
REG_DWORD
0x00015180 (86400)
LeaseObtainedTime
REG_DWORD
0x65fdc875 (1711130741)
T1
REG_DWORD
0x65fe7135 (1711173941)
T2
REG_DWORD
0x65feefc5 (1711206341)
LeaseTerminatesTime
REG_DWORD
0x65ff19f5 (1711217141)
AddressType
REG_DWORD
0x00000000 (0)
IsServerNapAware
REG_DWORD
0x00000000 (0)
DhcpConnForceBroadcastFlag
REG_DWORD
0x00000000 (0)
RegistrationEnabled
REG_DWORD
0x00000001 (1)
RegisterAdapterName
REG_DWORD
0x00000000 (0)
IPAddress
REG_MULTI_SZ
SubnetMask
REG_MULTI_SZ
DefaultGateway
REG_MULTI_SZ
DefaultGatewayMetric
REG_MULTI_SZ
DhcpIPAddress
REG_SZ
10.0.2.15
DhcpSubnetMask
REG_SZ
255.255.255.0
DhcpNameServer
REG_SZ
192.168.0.1 192.168.0.1
DhcpDefaultGateway
REG_MULTI_SZ
10.0.2.2,
DhcpSubnetMaskOpt
REG_MULTI_SZ
255.255.255.0,
DhcpInterfaceOptions
REG_BIN
FC 00 00 00 00 00 00 00 00 00 00 ...
DhcpGatewayHardware
REG_BIN
0A 00 02 02 06 00 00 00 52 54 00 12 ...
DhcpGatewayHardwareCount
REG_DWORD
0x00000001 (1)
Activate Windows

How many user accounts are listed?

Approach:

In a forensic investigation, it is important to identify and list all user accounts on the system. This helps link specific activities to specific users, detect any unauthorised or suspicious accounts, and understand the access level of each user.
During the examination, I focused on extracting user account information early in the process to support timeline analysis, privilege review, and user behaviour tracking.

Methodology

Tools: Autopsy
I navigated to the extracted SAM registry hive inside Autopsy. From there, I followed the path: System32\config\SAM\Domains\Account\Users\Names. This location lists all user account names that exist on the system. By reviewing the entries under "Names," I identified all the registered user accounts on the device.

Findings

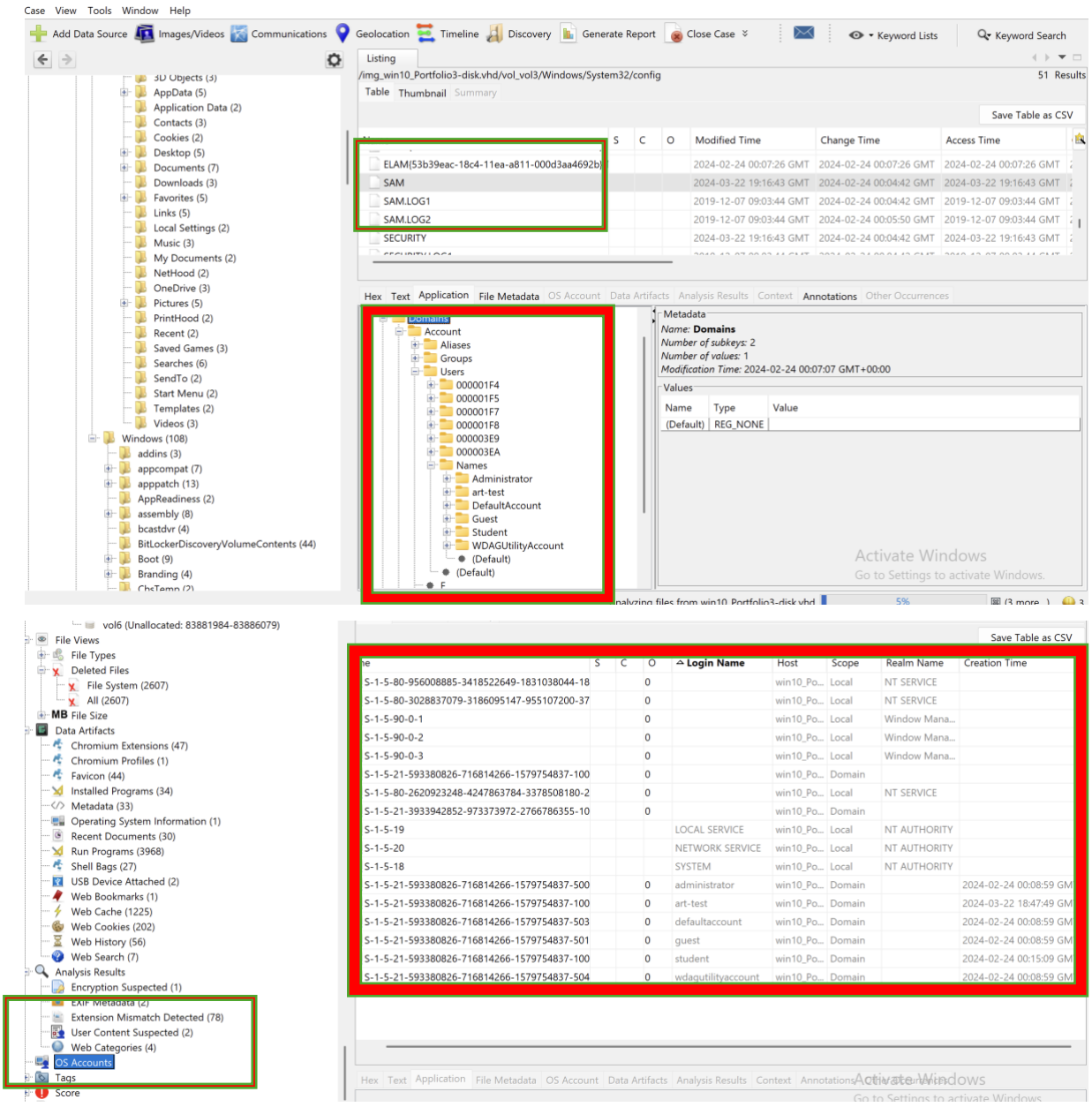
During the forensic examination of the SAM registry hive, I identified a total of six user accounts on the system. These were:

- Administrator
- Guest
- DefaultAccount
- WDAGUtilityAccount
- student
- art-test

Out of these six accounts, four (Administrator, Guest, DefaultAccount, and WDAGUtilityAccount) are default system accounts automatically created by Windows. Notably, the WDAGUtilityAccount is specifically associated with Windows Defender Application Guard, used to run secure, isolated browser sessions or sandboxed environments.

The remaining two accounts, student and art-test were manually created by users. These accounts are more likely to be linked to direct user activity relevant to the investigation.

Evidence


Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/System32/config
51 Results
Table
Thumbnail
Summary
Save Table as CSV
Modified Time
Change Time
Access Time
ELAM{53b39eac-18c4-11ea-a811-000d3aa4692b}
SAM
SAM.LOG1
SAM.LOG2
SECURITY
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000001F7
000001F8
000003E9
000003EA
Names
Administrator
art-test
DefaultAccount
Guest
Student
WDAGUtilityAccount
(Default)
Metadata
Name: Domains
Number of subkeys: 2
Number of values: 1
Modification Time: 2024-02-24 00:07:07 GMT+00:00
Values
Name
Type
Value
(Default)
REG_NONE
Activate Windows
Go to Settings to activate Windows.
vol6 (Unallocated: 83881984-83886079)
File Views
File Types
Deleted Files
File System (2607)
All (2607)
MB File Size
Data Artifacts
Chromium Extensions (47)
Chromium Profiles (1)
Favicon (44)
Installed Programs (34)
Metadata (33)
Operating System Information (1)
Recent Documents (30)
Run Programs (3968)
Shell Bags (27)
USB Device Attached (2)
Web Bookmarks (1)
Web Cache (1225)
Web Cookies (202)
Web History (56)
Web Search (7)
Analysis Results
Encryption Suspected (1)
Extension Mismatch Detected (78)
User Content Suspected (2)
Web Categories (4)
OS Accounts
Tags
Score
Login Name
Host
Scope
Realm Name
Creation Time
S-1-5-80-956008885-3418522649-1831038044-18
S-1-5-80-3028837079-3186095147-955107200-37
S-1-5-90-0-1
S-1-5-90-0-2
S-1-5-90-0-3
S-1-5-21-593380826-716814266-1579754837-100
S-1-5-80-2620923248-4247863784-3378508180-2
S-1-5-21-3933942852-973373972-2766786355-10
S-1-5-19
S-1-5-20
S-1-5-18
S-1-5-21-593380826-716814266-1579754837-500
S-1-5-21-593380826-716814266-1579754837-100
S-1-5-21-593380826-716814266-1579754837-503
S-1-5-21-593380826-716814266-1579754837-501
S-1-5-21-593380826-716814266-1579754837-100
S-1-5-21-593380826-716814266-1579754837-504
LOCAL SERVICE
NETWORK SERVICE
SYSTEM
administrator
art-test
defaultaccount
guest
student
wdagutilityaccount
win10_Po...
Local
Domain
NT SERVICE
NT AUTHORITY
Window Mana...
2024-02-24 00:08:59 GM
2024-03-22 18:47:49 GM
2024-02-24 00:15:09 GM

Who was the last user to log in to the PC?

Approach

To determine who the last user to log into the PC was, I examined the forensic image using the software Hive on Autopsy focused on reviewing the system's registry artifacts and login event data to find the most recent login records. Identifying the last logged-in user early is important because it connects user actions to the timeline of events being investigated.

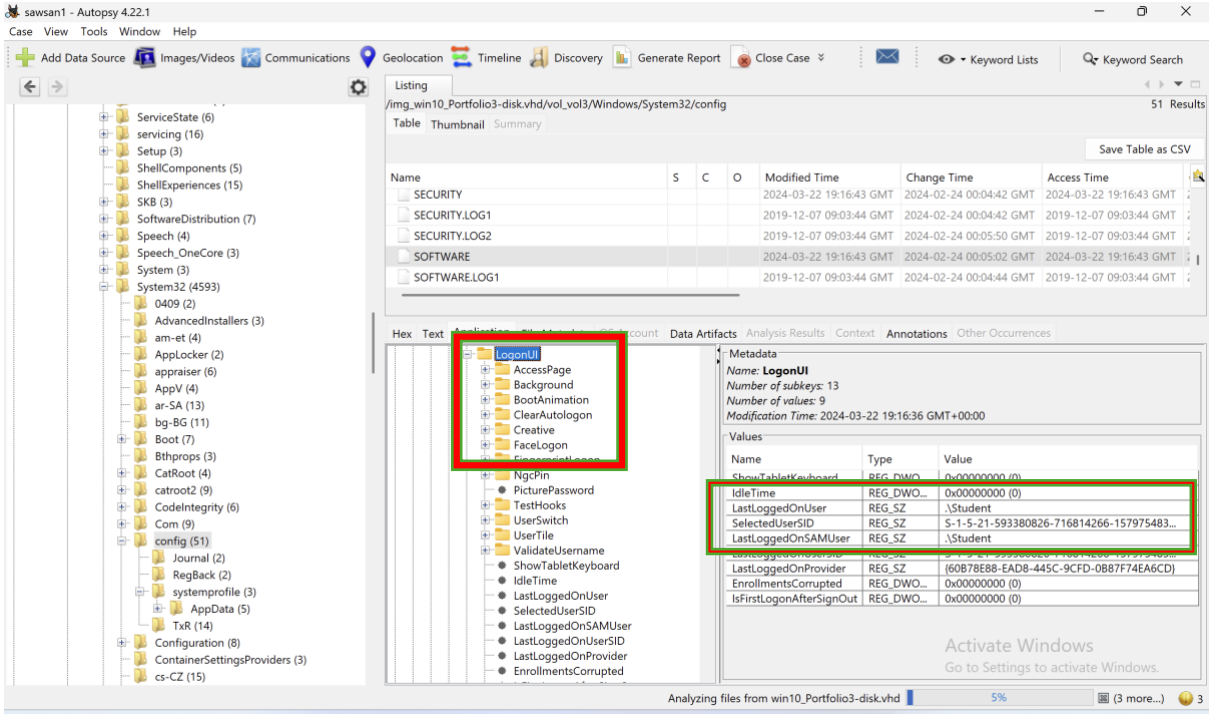
Methodology:

Tools: Autopsy
I navigated to the Extracted Content section and examined the Windows Registry files. Specifically, I looked under the Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI path.
In this location, the value for LastLoggedOnUser showed which user account was last successfully logged into the system.

Findings

The LastLoggedOnUser value showed that the student account was the last user to log into the system.

Evidence


sawsan1 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/System32/config
51 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time
SECURITY 2024-03-22 19:16:43 GMT 2024-02-24 00:04:42 GMT 2024-03-22 19:16:43 GMT
SECURITY.LOG1 2019-12-07 09:03:44 GMT 2024-02-24 00:04:42 GMT 2019-12-07 09:03:44 GMT
SECURITY.LOG2 2019-12-07 09:03:44 GMT 2024-02-24 00:05:50 GMT 2019-12-07 09:03:44 GMT
SOFTWARE 2024-03-22 19:16:43 GMT 2024-02-24 00:05:02 GMT 2024-03-22 19:16:43 GMT
SOFTWARE.LOG1 2019-12-07 09:03:44 GMT 2024-02-24 00:04:44 GMT 2019-12-07 09:03:44 GMT
Hex Text Data Artifacts Analysis Results Context Annotations Other Occurrences
LogonUI
AccessPage
Background
BootAnimation
ClearAutologon
Creative
FaceLogon
NgcPin
PicturePassword
TestHooks
UserSwitch
UserTile
ValidateUsername
ShowTabletKeyboard
IdleTime
LastLoggedOnUser
SelectedUserSID
LastLoggedOnSAMUser
LastLoggedOnUserSID
LastLoggedOnProvider
EnrollmentsCorrupted
Metadata
Name: LogonUI
Number of subkeys: 13
Number of values: 9
Modification Time: 2024-03-22 19:16:36 GMT+00:00
Values
Name Type Value
IdleTime REG_DWO... 0x00000000 (0)
LastLoggedOnUser REG_SZ .\Student
SelectedUserSID REG_SZ S-1-5-21-593380826-716814266-157975483...
LastLoggedOnSAMUser REG_SZ .\Student
LastLoggedOnProvider REG_SZ {60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}
EnrollmentsCorrupted REG_DWO... 0x00000000 (0)
IsFirstLogonAfterSignOut REG_DWO... 0x00000000 (0)
Activate Windows
Go to Settings to activate Windows.
Analyzing files from win10_Portfolio3-disk.vhd 5% (3 more...)

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

Approach:

To find out which user account mostly used the computer, I examined the forensic image by reviewing user activity data. Identifying the primary user is important because it helps focus the investigation on the account responsible for most of the actions on the device. I focused on the logon counts for each account to determine which user had the most logins.

Methodology:

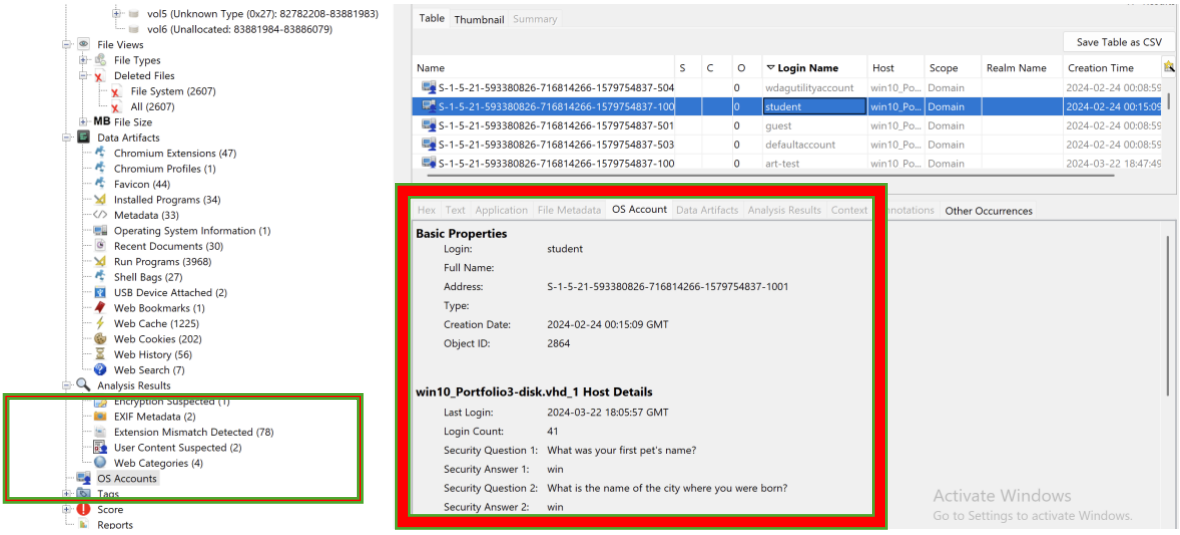
Tool Used: Autopsy

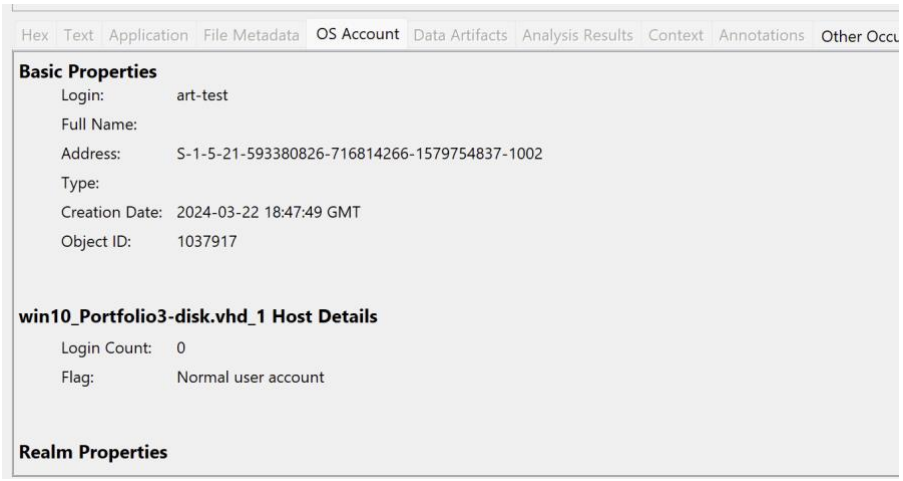
I navigated to the Data Artifacts section and selected Operating System Accounts**.**
I reviewed each user account and checked the Logon Count field for each one.
By comparing the login counts, I identified which account had been used to log in the most times.

Findings:

The review showed that the student account was the only account with actual logon activity. This indicates that the student was the primary user of the computer.

Evidence





For example, art-test has no login counts.

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

Approach:

To find the last shutdown time of the computer, I examined the forensic image using Autopsy. Identifying the shutdown time is important because it helps build an accurate timeline of the device's usage and can indicate when the system was last powered off, which may be linked to suspicious activity or important events during the investigation.

Methodology:

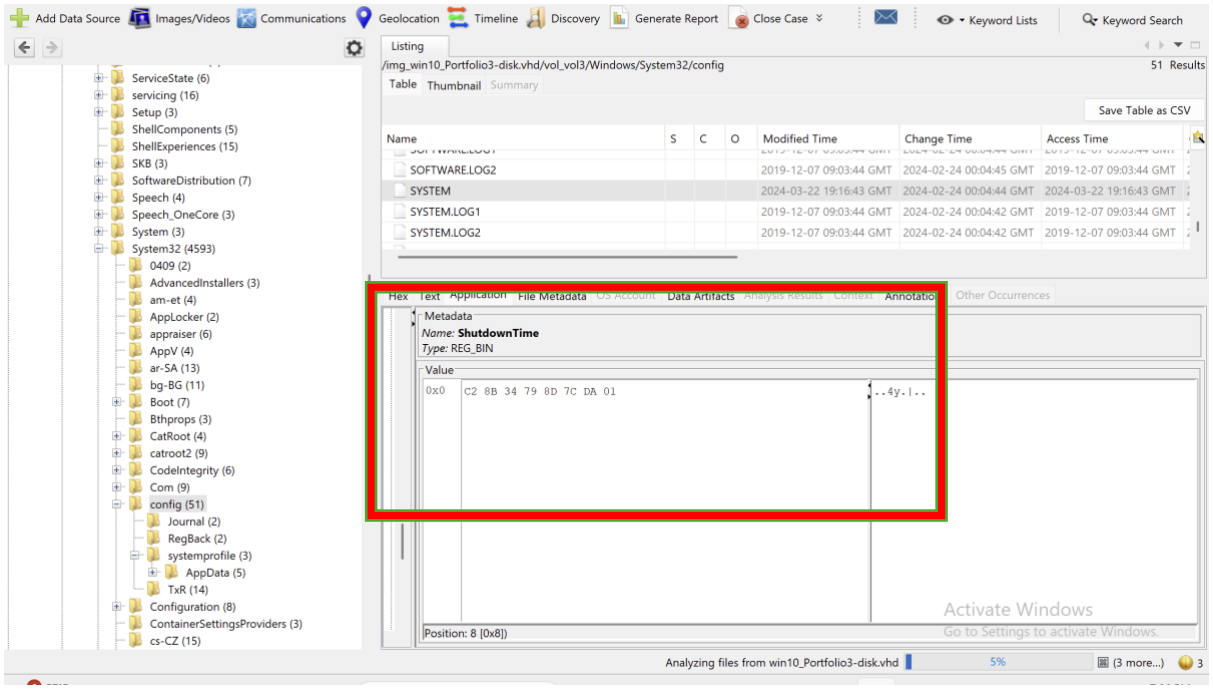
Tools Used: Autopsy, Time Format, Rapid Tables

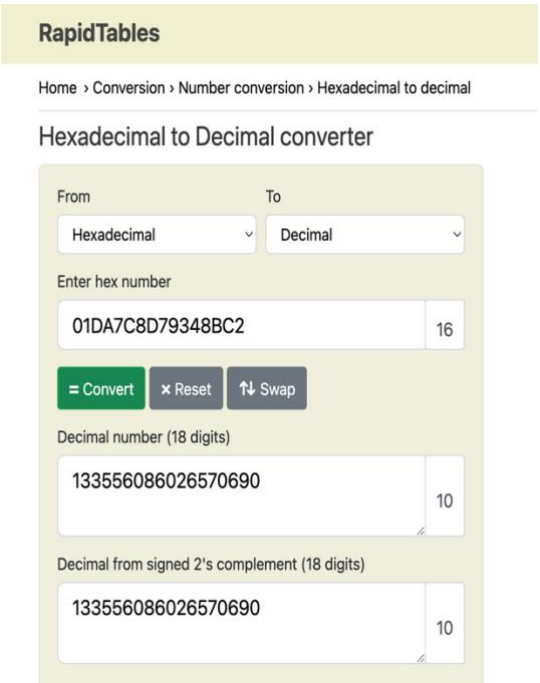
I navigated to the extracted Windows Registry file under the path: Windows\System32\config\SYSTEM\ControlSet001\Control\Windows.At this location, I found the Shutdown Time registry value, which was stored in hexadecimal format. I manually reversed the hex-byte pairs and converted the value into a decimal timestamp. To decode the timestamp into a human-readable date and time, I used Time Format and Rapid Tables online converters.

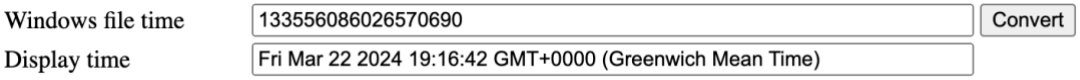
Findings:

The Shutdown Time value originally appeared as: C2 8B 34 79 8D 7C DA 01 (hexadecimal).After reversing the bytes and converting the value, the decoded shutdown time was:133961009604786882 (decimal). By converting the decimal timestamp into a readable format using online tools, the final shutdown time was determined to be Friday, March 22, 2024, at 19:16:42 (GMT). This timestamp corresponds to the last time the system was properly shut down, as decoded using forensic time format converters.

Evidence:


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/System32/config
51 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
SOFTWARE.LOG2
2019-12-07 09:03:44 GMT
2024-02-24 00:04:45 GMT
2019-12-07 09:03:44 GMT
SYSTEM
2024-03-22 19:16:43 GMT
2024-02-24 00:04:44 GMT
2024-03-22 19:16:43 GMT
SYSTEM.LOG1
2019-12-07 09:03:44 GMT
2024-02-24 00:04:42 GMT
2019-12-07 09:03:44 GMT
SYSTEM.LOG2
2019-12-07 09:03:44 GMT
2024-02-24 00:04:42 GMT
2019-12-07 09:03:44 GMT
Hex
Text
Application
File Metadata
Data Artifacts
Other Occurrences
Metadata
Name: ShutdownTime
Type: REG_BIN
Value
0x0
C2 8B 34 79 8D 7C DA 01
..4y.|..
Position: 8 [0x8])
Activate Windows
Go to Settings to activate Windows.
Analyzing files from win10_Portfolio3-disk.vhd
5%
(3 more...)
ServiceState (6)
servicing (16)
Setup (3)
ShellComponents (5)
ShellExperiences (15)
SKB (3)
SoftwareDistribution (7)
Speech (4)
Speech_OneCore (3)
System (3)
System32 (4593)
0409 (2)
AdvancedInstallers (3)
am-et (4)
AppLocker (2)
appraiser (6)
AppV (4)
ar-SA (13)
bg-BG (11)
Boot (7)
Bthprops (3)
CatRoot (4)
catroot2 (9)
CodeIntegrity (6)
Com (9)
config (51)
Journal (2)
RegBack (2)
systemprofile (3)
AppData (5)
TxR (14)
Configuration (8)
ContainerSettingsProviders (3)
cs-CZ (15)


RapidTables
Home › Conversion › Number conversion › Hexadecimal to decimal
Hexadecimal to Decimal converter
From
To
Hexadecimal
Decimal
Enter hex number
01DA7C8D79348BC2
16
= Convert
× Reset
⇅ Swap
Decimal number (18 digits)
133556086026570690
10
Decimal from signed 2's complement (18 digits)
133556086026570690
10


Windows file time
133556086026570690
Convert
Display time
Fri Mar 22 2024 19:16:42 GMT+0000 (Greenwich Mean Time)

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

Approach:

To determine which user was logged into the device on 22nd March 2024, I reviewed the system's user account activity. Identifying the active user on a specific date is important because it links device activity to a particular user and helps build an accurate timeline for the investigation.

Methodology:

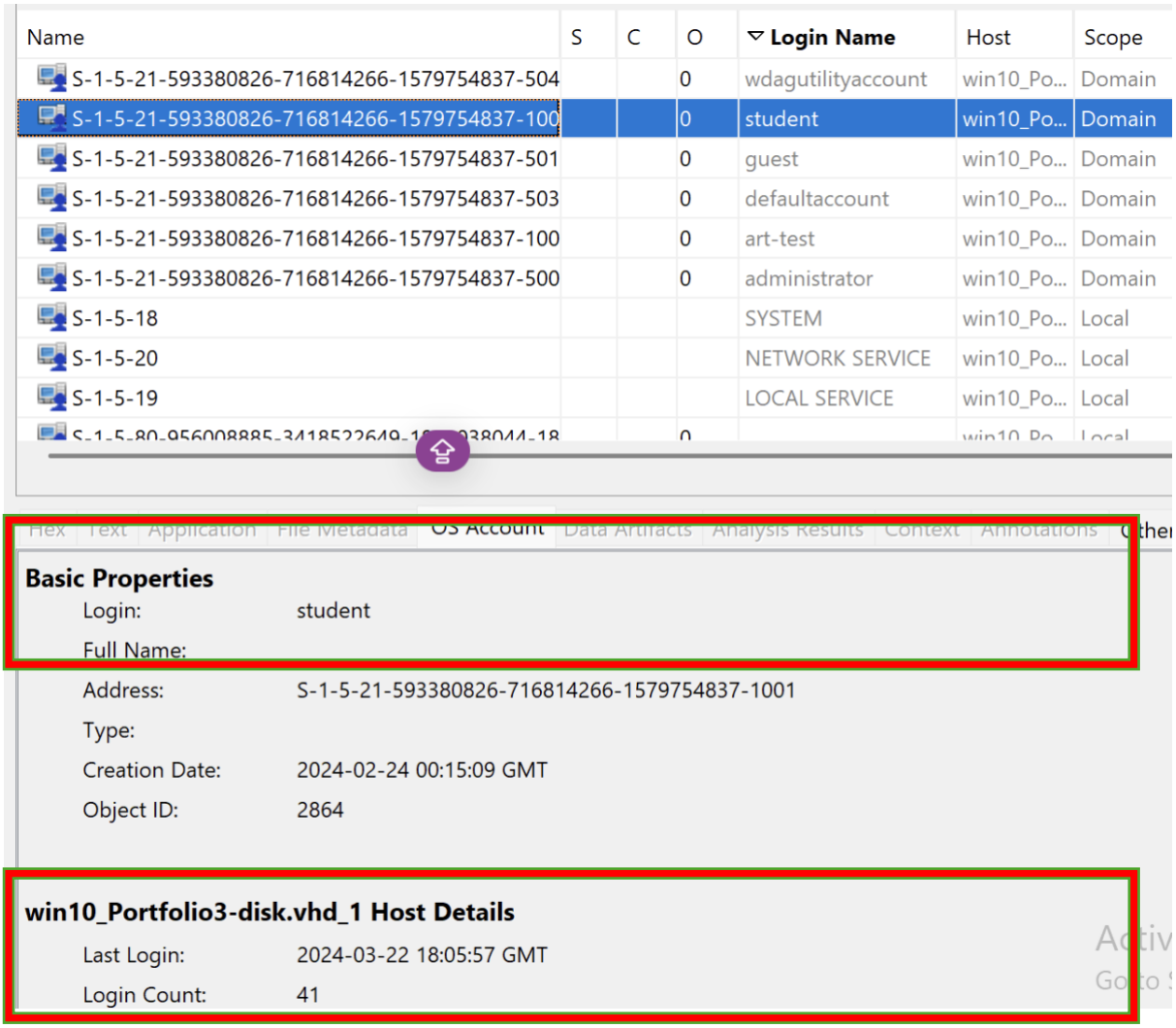
Tool Used: Autopsy

I navigated to the Data Artifacts section and selected Operating System Accounts**.**
I examined each user account's Last Login date and compared it to the target date (22nd March 2024). The student account showed a Last Login timestamp matching the 22nd of March 2024 date.

Findings:

The user account student was logged into the device on 22nd March 2024**.**
This confirms that the student account was active on the system at that time.

Evidence:



Name	S	C	O	Login Name	Host	Scope
S-1-5-21-593380826-716814266-1579754837-504			0	wdagutilityaccount	win10_Po...	Domain
S-1-5-21-593380826-716814266-1579754837-100			0	student	win10_Po...	Domain
S-1-5-21-593380826-716814266-1579754837-501			0	guest	win10_Po...	Domain
S-1-5-21-593380826-716814266-1579754837-503			0	defaultaccount	win10_Po...	Domain
S-1-5-21-593380826-716814266-1579754837-100			0	art-test	win10_Po...	Domain
S-1-5-21-593380826-716814266-1579754837-500			0	administrator	win10_Po...	Domain
S-1-5-18				SYSTEM	win10_Po...	Local
S-1-5-20				NETWORK SERVICE	win10_Po...	Local
S-1-5-19				LOCAL SERVICE	win10_Po...	Local

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

Basic Properties

Login:	student
Full Name:	
Address:	S-1-5-21-593380826-716814266-1579754837-1001
Type:	
Creation Date:	2024-02-24 00:15:09 GMT
Object ID:	2864

win10_Portfolio3-disk.vhd_1 Host Details

Last Login:	2024-03-22 18:05:57 GMT
Login Count:	41

Which account(s) were created on 22nd March 2024 and at what time?

Approach:

To identify which user accounts were created on 22nd March 2024, I reviewed the account creation timestamps recorded in the system's operating system accounts. Identifying account creation times is important because it can show when new users were added to the system, which may link to suspicious or unauthorized activity.

Methodology:

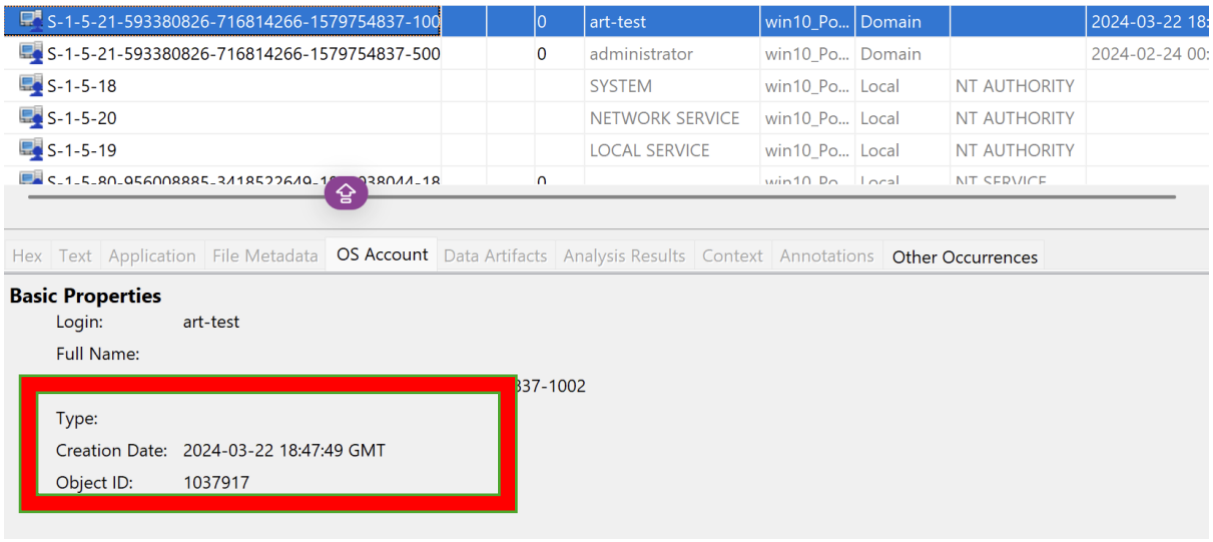
Tool Used: Autopsy

Then, I navigated to the Data Artifacts section and selected Operating System Accounts**.** I reviewed each account's Creation Date property. By checking the creation dates, I identified which accounts were created on 22nd March 2024 and recorded the exact creation times.

Findings:

The art-test account was created on 22nd March 2024 at 18:47:49 GMT**.**
No other user accounts were found to have been created on that date.

Evidence:


S-1-5-21-593380826-716814266-1579754837-100 0 art-test win10_Po... Domain 2024-03-22 18
S-1-5-21-593380826-716814266-1579754837-500 0 administrator win10_Po... Domain 2024-02-24 00
S-1-5-18 SYSTEM win10_Po... Local NT AUTHORITY
S-1-5-20 NETWORK SERVICE win10_Po... Local NT AUTHORITY
S-1-5-19 LOCAL SERVICE win10_Po... Local NT AUTHORITY
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Basic Properties
Login: art-test
Full Name:
Type:
Creation Date: 2024-03-22 18:47:49 GMT
Object ID: 1037917

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

Approach:

To find out which user accounts were members of the Administrator group, I examined the security and account configuration data from the forensic image. Identifying administrator accounts is important because they have full control over the system, including installing software, modifying system settings, and potentially deleting evidence.

Methodology:

Tools Used: Autopsy, Windows Registry Viewer

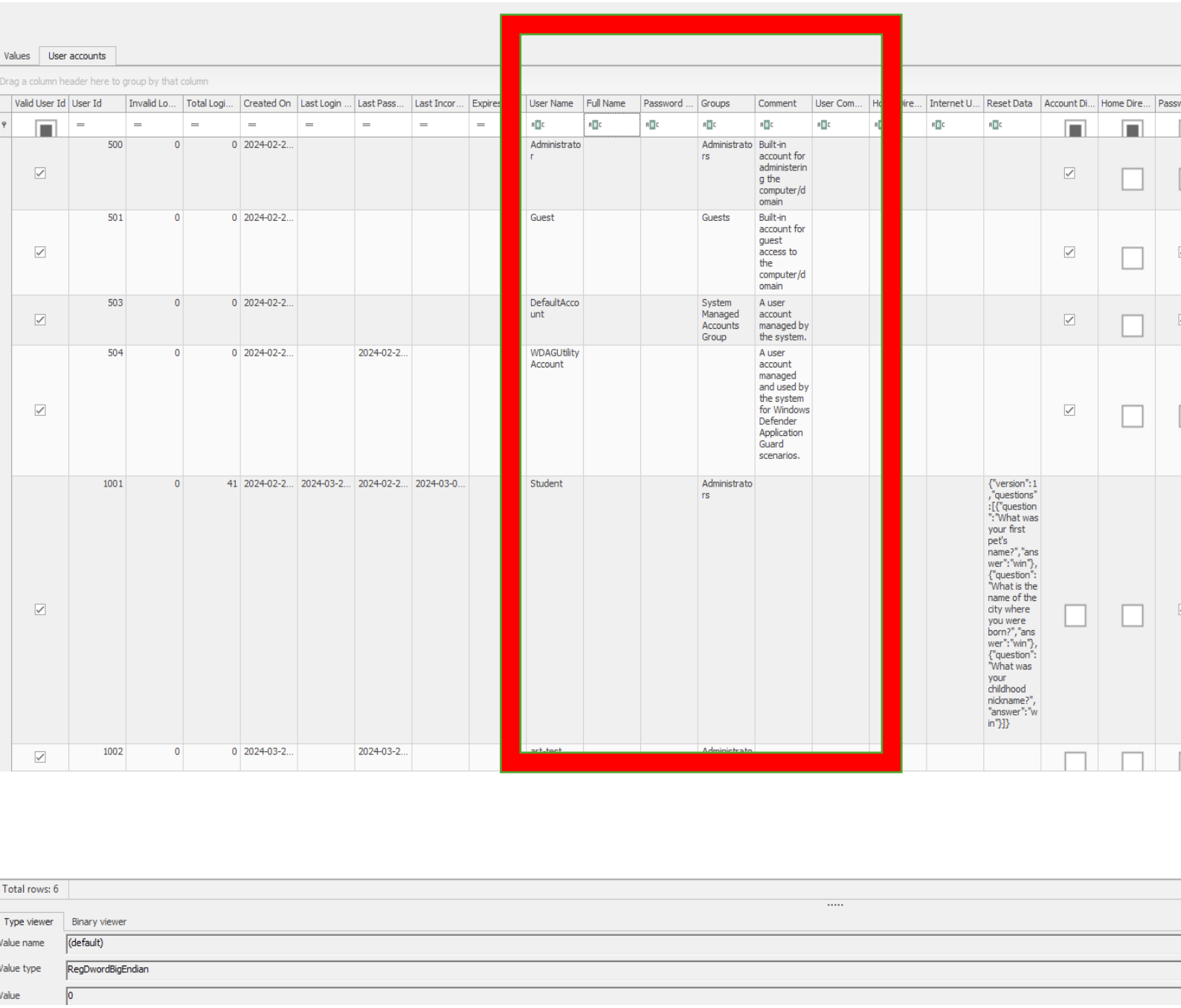
I mounted the win10_Portfolio3-disk.vhd forensic image into Autopsy.
Then, I navigated to the extracted SAM registry hives on the Windows registry. In Autopsy, I viewed the group, specifically focusing on identifying users linked to the Administrators group**.** I confirmed group memberships by checking the group column (which lists group memberships) and verified users who belonged to the administrator group.

Findings:

From examining the group membership information, it was determined that the accounts Administrator**,** art-test**,** and student were all members of the Administrators group**.** The Administrator account is the default Windows administrative account, while art-test and student were manually created user accounts. Both art-test and student had administrative privileges on the system, meaning they had full control

over system settings and access to critical files, alongside the built-in Administrator account.

Evidence



Values | User accounts

Drag a column header here to group by that column

Valid User Id	User Id	Invalid Lo...	Total Logi...	Created On	Last Login ...	Last Pass...	Last Incor...	Expires	User Name	Full Name	Password ...	Groups	Comment	User Com...	Internet U...	Reset Data	Account Di...	Home Dire...
☑	500	0	0	2024-02-2...					Administrator			Administrators	Built-in account for administering the computer/domain				☑	☐
☑	501	0	0	2024-02-2...					Guest			Guests	Built-in account for guest access to the computer/domain				☑	☐
☑	503	0	0	2024-02-2...					DefaultAccount			System Managed Accounts Group	A user account managed by the system.				☑	☐
☑	504	0	0	2024-02-2...		2024-02-2...			WDAGUtility Account				A user account managed and used by the system for Windows Defender Application Guard scenarios.				☑	☐
☑	1001	0	41	2024-02-2...	2024-03-2...	2024-02-2...	2024-03-0...		Student			Administrators				{"version":1,"questions":[{"question":"What was your first pet's name?","answer":"win"},{"question":"What is the name of the city where you were born?","answer":"win"},{"question":"What was your childhood nickname?","answer":"win"}]}	☐	☐
☑	1002	0	0	2024-03-2...		2024-03-2...			art-test			Administrato					☐	☐

Total rows: 6

Type viewer | Binary viewer

Value name: (default)

Value type: RegDwordBigEndian

Value: 0

How many files are under AtomicRedTeam?

Approach:

To find out how many files were stored under the AtomicRedTeam directory, I accessed the forensic image using a Linux terminal environment. Determining the number of files is useful for understanding the size and potential contents of the AtomicRedTeam toolset, which may include scripts or payloads used in simulations or attacks.

Methodology:

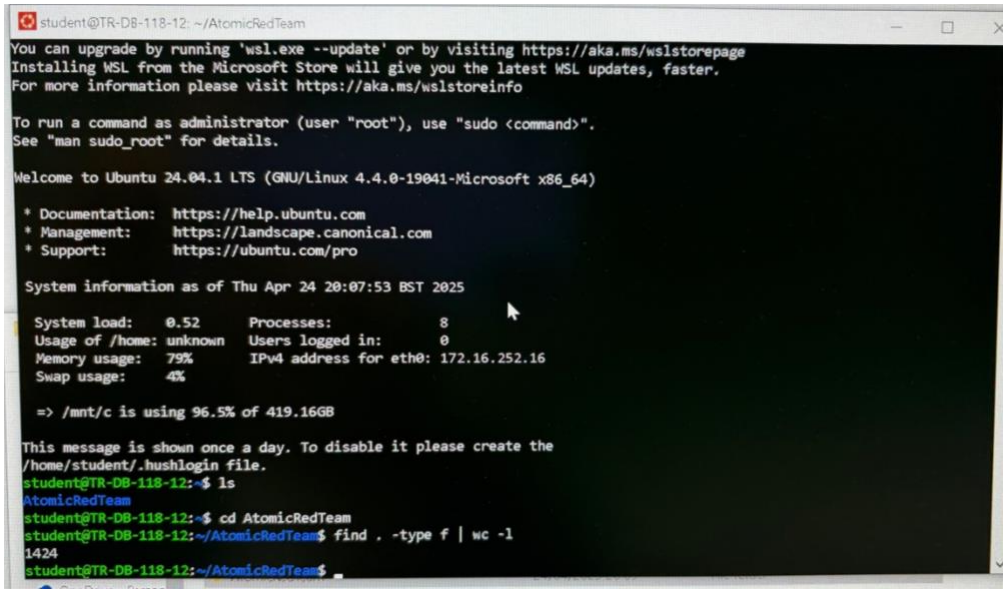
Tools: Autopsy, ubuntu
I used Ubuntu to access the extracted AtomicRedTeam directory.
Once inside the directory, I ran the command: find. -type f | wc -l This command recursively searched through all subdirectories and counted only the regular files (-type f), not directories. This gave me the total number of files located under AtomicRedTeam, including those inside nested folders.

Findings:

The total number of files inside the AtomicRedTeam directory was: 1424.

Evidence

This result was captured from a screenshot of the Ubuntu terminal, where the output of the find command confirmed the count. The full command and result are visible in the image showing the terminal prompt inside the AtomicRedTeam directory.



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

Approach:

To find the Parent MFT Entry Number of the file ART-attack.ps1, I examined its file system metadata using Autopsy. The Parent MFT (Master File Table) Entry Number identifies the directory that contains the file. In NTFS (New Technology File System), every file and folder have an MFT entry, and each file also stores the MFT reference of its parent directory. This information is important because it allows forensic investigators to understand the exact folder structure and trace the file back to its original location on the disk, which is useful for timeline analysis, context, and integrity verification.

Methodology:

Tool Used: Autopsy

I navigated to the ART-attack.ps1 file using Autopsy and viewed its File Metadata**.** At the bottom of the metadata panel, I found the field labelled Parent MFT Entry, which contains the Master File Table record number and sequence number of the directory that contains the file.
This information came directly from the NTFS metadata.

Findings:

Parent MFT Entry: 102162 sequence 9

Evidence

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations

Name:	/img_win10_Portfolio3-disk.vhd/vol_vol3/Users/Student/Desktop/File/ART-attack.ps1
Type:	File System
MIME Type:	text/plain
Size:	3360
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-03-22 17:56:40 GMT
Accessed:	2024-03-22 18:51:28 GMT
Created:	2024-03-22 17:56:40 GMT
Changed:	2024-03-22 18:00:56 GMT
MD5:	39c96d2b7d3902de5318c5ed446152a9
SHA-256:	e51443f6ca5bb45960dcdb651a750a37430daa4b89eb343887fb3d0b893816c5
Hash Lookup Results:	UNKNOWN
Internal ID:	21648

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 83043 Sequence: 12
$LogFile Sequence Number: 1755335818
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 1725 (S-1-5-21-593380826-716814266-1579754837-1001)
Last User Journal Update Sequence Number: 811495744
Created: 2024-03-22 18:56:40.826244000 (BST)
File Modified: 2024-03-22 18:56:40.826244000 (BST)
MFT Modified: 2024-03-22 19:00:56.853319500 (BST)
```

```
$FILE_NAME Attribute Values:
Flags: Archive
Name: ART-AT~1.PS1
Parent MFT Entry: 102162 Sequence: 9
Allocated Size: 4096 Actual Size: 3360
Created: 2024-03-22 18:56:40.826244000 (BST)
File Modified: 2024-03-22 18:56:40.826244000 (BST)
MFT Modified: 2024-03-22 18:56:41.075340400 (BST)
Accessed: 2024-03-22 18:56:40.826244000 (BST)

$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 18:56:40.826244000 (BST)
File Modified: 2024-03-22 18:56:40.826244000 (BST)
Accessed: 2024-03-22 18:56:40.826244000 (BST)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-8) Name: N/A Resident size: 90
Type: $FILE_NAME (48-7) Name: N/A Resident size: 94
Type: $DATA (128-4) Name: N/A Non-Resident size: 3360 init_size: 3360
Starting address: 378134, length: 1
```

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?

Approach:

To find which executable files were recorded by the Background Activity Moderator (BAM) for the user with RID 1001, I examined the registry path that logs background process activity. This information is important because BAM tracks recently run executables, which helps identify what programs a user executed and when a key detail in forensic timeline reconstruction.

Methodology:

Tool Used: Registry Explorer, Autopsy

I loaded the SYSTEM hive from the forensic image using Registry Explorer.
Then I navigated to:HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-593380826-716814266-1579754837-1001This SID corresponds to the user account with RID 1001 (in this case, likely the student account).
I reviewed the list of executable file paths under this key and noted the last execution times shown in the right panel.

Findings:

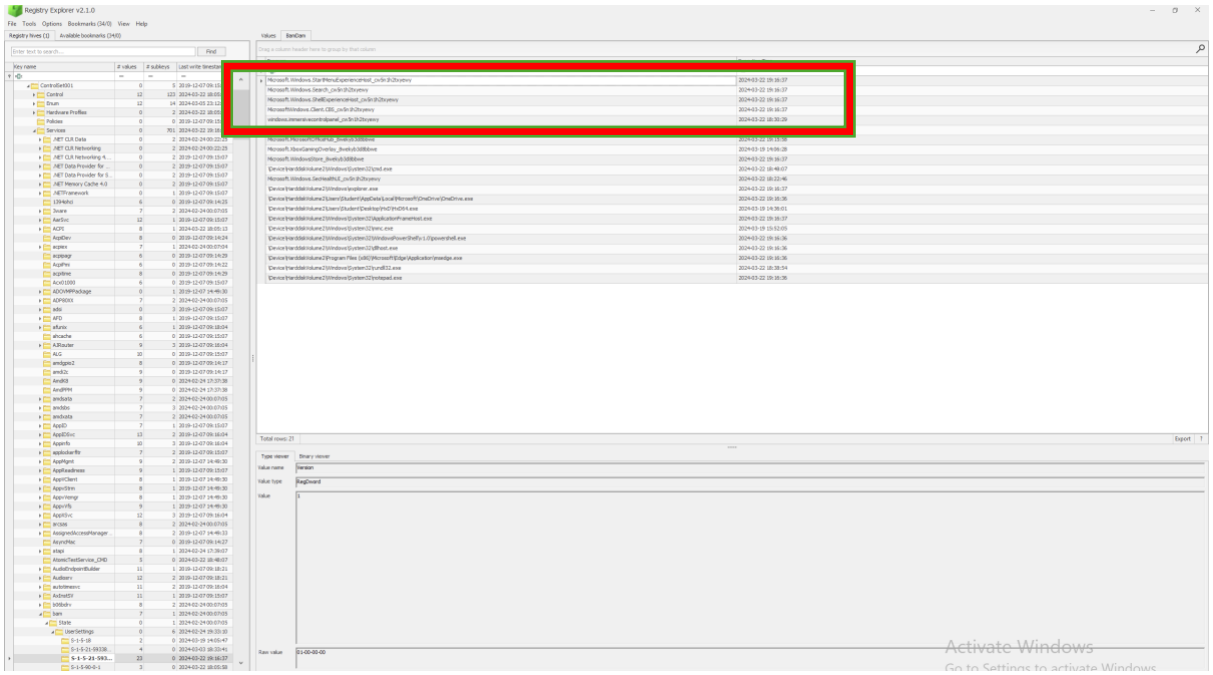
The BAM recorded the following executable files for the user with RID 1001:

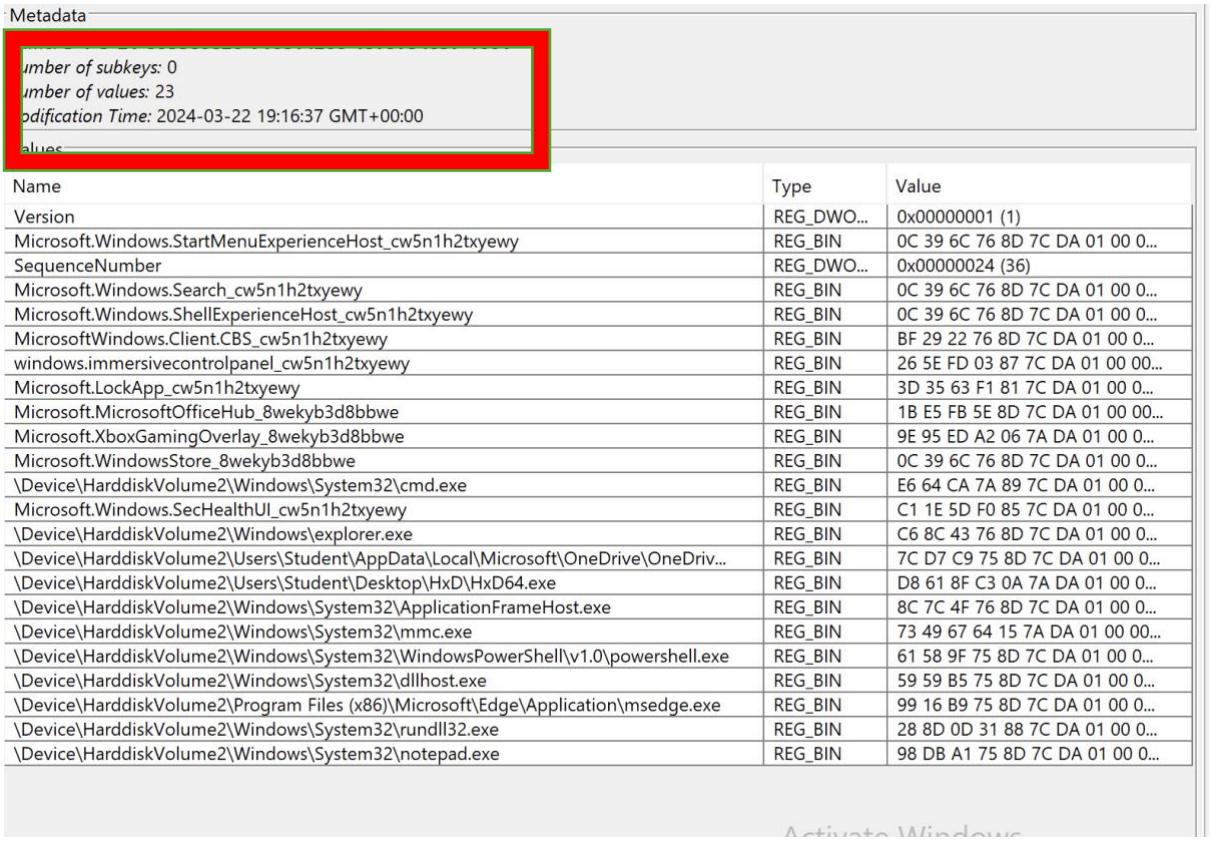
- Microsoft.Windows.StartMenuExperienceHost_cw5n1h2bxyewy – 2024-03-22 19:16:37
- Microsoft.Windows.Search_cw5n1h2bxyewy – 2024-03-22 19:16:37
- Microsoft.Windows.ShellExperienceHost_cw5n1h2bxyewy – 2024-03-22 19:16:37
- Microsoft.Windows.Client.CBS_cw5n1h2bxyewy – 2024-03-22 19:16:37
- windows.immersivecontrolpanel_cw5n1h2bxyewy – 2024-03-22 18:30:29
- Microsoft.LockApp_cw5n1h2bxyewy – 2024-03-22 17:54:10
- Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe – 2024-03-22 19:15:58

- Microsoft.XboxGamingOverlay_8wekyb3d8bbwe – 2024-03-19 14:06:28
- Microsoft.WindowsStore_8wekyb3d8bbwe – 2024-03-22 19:16:37
- System32\cmd.exe – 2024-03-22 18:48:07
- System32\explorer.exe – 2024-03-22 18:22:46
- OneDrive\OneDrive.exe – 2024-03-22 19:16:37
- HxD\HxD64.exe – 2024-03-22 19:16:36
- System32\ApplicationFrameHost.exe – 2024-03-19 14:36:01
- System32\mmc.exe – 2024-03-22 19:16:37
- System32\powershell.exe – 2024-03-19 15:52:05
- System32\dllhost.exe – 2024-03-22 19:16:36
- MicrosoftEdge\Application\msedge.exe – 2024-03-22 19:16:36
- System32\rundll32.exe – 2024-03-22 19:16:36
- System32\notepad.exe – 2024-03-22 18:38:54

The last recorded execution time was:
2024-03-22 19:16:37

Evidence





Metadata

umber of subkeys: 0
umber of values: 23
odification Time: 2024-03-22 19:16:37 GMT+00:00

alues

Name	Type	Value
Version	REG_DWO...	0x00000001 (1)
Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy	REG_BIN	0C 39 6C 76 8D 7C DA 01 00 0...
SequenceNumber	REG_DWO...	0x00000024 (36)
Microsoft.Windows.Search_cw5n1h2txyewy	REG_BIN	0C 39 6C 76 8D 7C DA 01 00 0...
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	REG_BIN	0C 39 6C 76 8D 7C DA 01 00 0...
MicrosoftWindows.Client.CBS_cw5n1h2txyewy	REG_BIN	BF 29 22 76 8D 7C DA 01 00 0...
windows.immersivecontrolpanel_cw5n1h2txyewy	REG_BIN	26 5E FD 03 87 7C DA 01 00 00...
Microsoft.LockApp_cw5n1h2txyewy	REG_BIN	3D 35 63 F1 81 7C DA 01 00 0...
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	REG_BIN	1B E5 FB 5E 8D 7C DA 01 00 00...
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	REG_BIN	9E 95 ED A2 06 7A DA 01 00 0...
Microsoft.WindowsStore_8wekyb3d8bbwe	REG_BIN	0C 39 6C 76 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Windows\System32\cmd.exe	REG_BIN	E6 64 CA 7A 89 7C DA 01 00 0...
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy	REG_BIN	C1 1E 5D F0 85 7C DA 01 00 0...
\Device\HarddiskVolume2\Windows\explorer.exe	REG_BIN	C6 8C 43 76 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Users\Student\AppData\Local\Microsoft\OneDrive\OneDriv...	REG_BIN	7C D7 C9 75 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Users\Student\Desktop\HxD\HxD64.exe	REG_BIN	D8 61 8F C3 0A 7A DA 01 00 0...
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	REG_BIN	8C 7C 4F 76 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Windows\System32\mmc.exe	REG_BIN	73 49 67 64 15 7A DA 01 00 00...
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	REG_BIN	61 58 9F 75 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Windows\System32\dllhost.exe	REG_BIN	59 59 B5 75 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	REG_BIN	99 16 B9 75 8D 7C DA 01 00 0...
\Device\HarddiskVolume2\Windows\System32\rundll32.exe	REG_BIN	28 8D 0D 31 88 7C DA 01 00 0...
\Device\HarddiskVolume2\Windows\System32\notepad.exe	REG_BIN	98 DB A1 75 8D 7C DA 01 00 0...

When T1055.exe and T1036.003.exe were created?

Approach:

To investigate potentially suspicious executables such as T1055.exe and T1036.003.exe, I searched for these files to determine when they were created and potentially executed. These filenames match known attack techniques from the MITRE ATT&CK framework, which catalogues real-world adversarial behaviours.

- T1055.exe refers to Process Injection (MITRE T1055) — a method attackers use to inject malicious code into legitimate processes to evade detection.
- T1036.003.exe refers to Named Binary Proxy Execution: Rundll32 (MITRE T1036.003) — where attackers use trusted Windows utilities to disguise and run malicious code.

These techniques are commonly used in red team simulations and real-world attacks. I used Autopsy's keyword search to locate the executables, then navigated to their paths under /AtomicRedTeam/atomics/, specifically in the /bin/ folders.

Methodology:

Tool Used: Autopsy

I used Autopsy's Keyword Search to filter results for T1055.exe and T1036.003.exe.

Once found, I navigated to their exact directory location within: /img_win10_Portfolio3disk.vhd/vol_vol3/AtomicRedTeam/atomics/T1055.004/bin/

I reviewed the file metadata using Autopsy to examine Modified Time, Change Time, and Access Time.

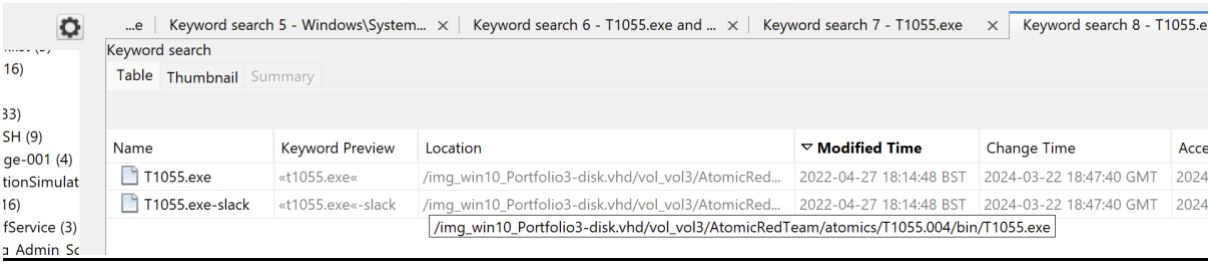
I repeated this for both executables and recorded their creation details.

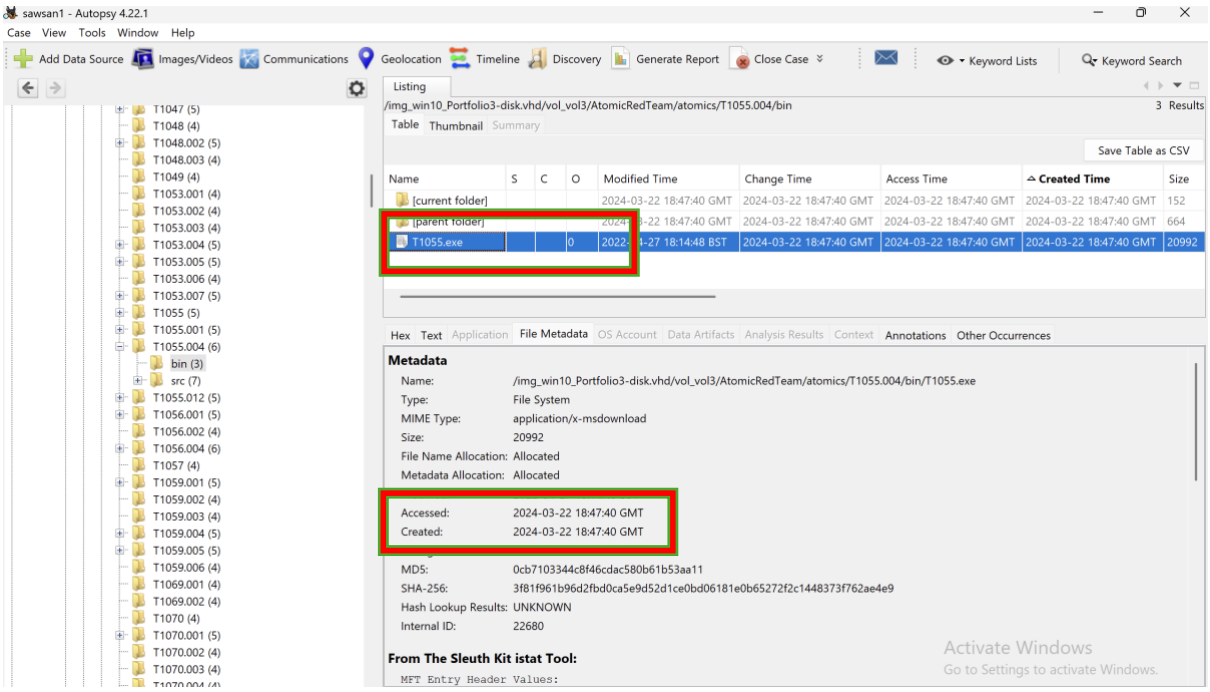
Findings:

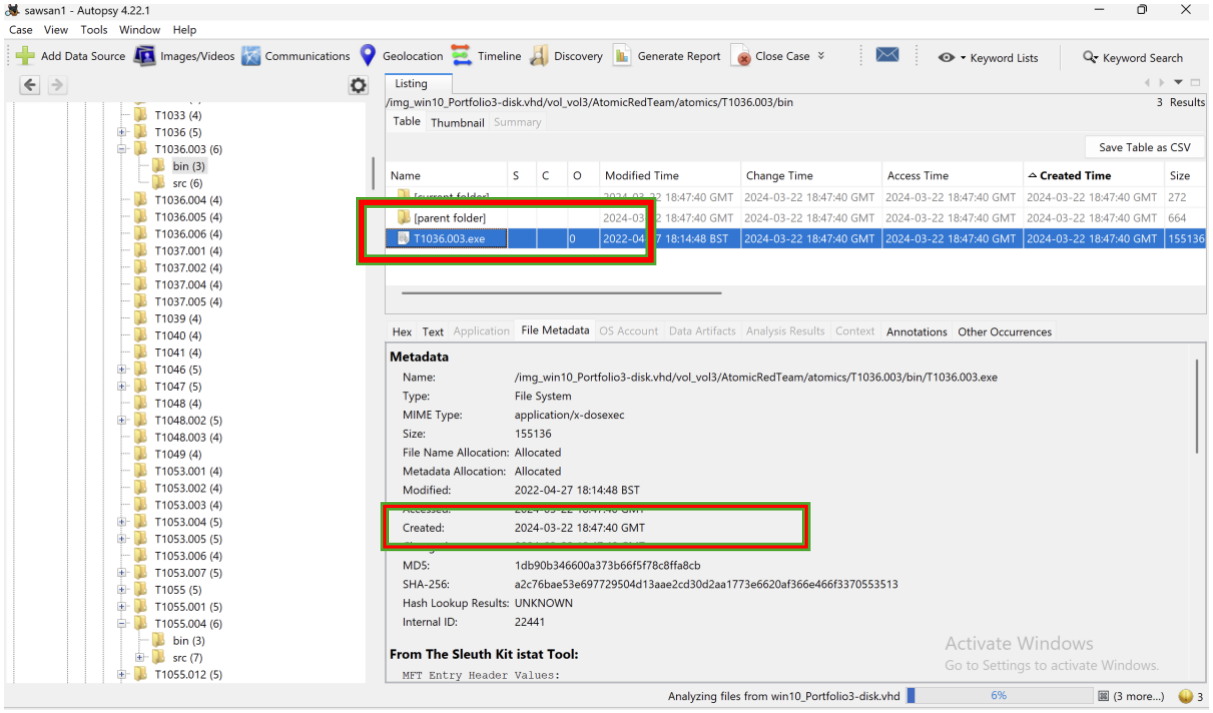
T1055.exe was created on 2024-03-22 at 18:47:40 GMT.

T1036.003.exe was created on 2024-03-22 at 18:47:40 GMT.

Evidence:






sawsan1 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/AtomicRedTeam/atomics/T1036.003/bin
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
[parent folder]
T1036.003.exe
2024-03-22 18:47:40 GMT
2024-04-27 18:14:48 BST
155136
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Metadata
Name: /img_win10_Portfolio3-disk.vhd/vol_vol3/AtomicRedTeam/atomics/T1036.003/bin/T1036.003.exe
Type: File System
MIME Type: application/x-dosexec
Size: 155136
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-04-27 18:14:48 BST
Created: 2024-03-22 18:47:40 GMT
MD5: 1db90b346600a373b66f5f78c8ffa8cb
SHA-256: a2c76bae53e697729504d13aae2cd30d2aa1773e6620af366e466f3370553513
Hash Lookup Results: UNKNOWN
Internal ID: 22441
From The Sleuth Kit istat Tool:
MFT Entry Header Values:
Activate Windows
Go to Settings to activate Windows.
Analyzing files from win10_Portfolio3-disk.vhd
6%
(3 more...)

Was Notepad opened on 22nd March 2024?

Approach:

To determine whether Notepad was opened on 22nd March 2024, I examined the Background Activity Moderator (BAM) registry data. This information is useful in forensic investigations because BAM tracks which executable files were run by each user, along with precise timestamps. Checking for the use of utilities like Notepad can help confirm a user's activity and intent on the system.

Methodology:

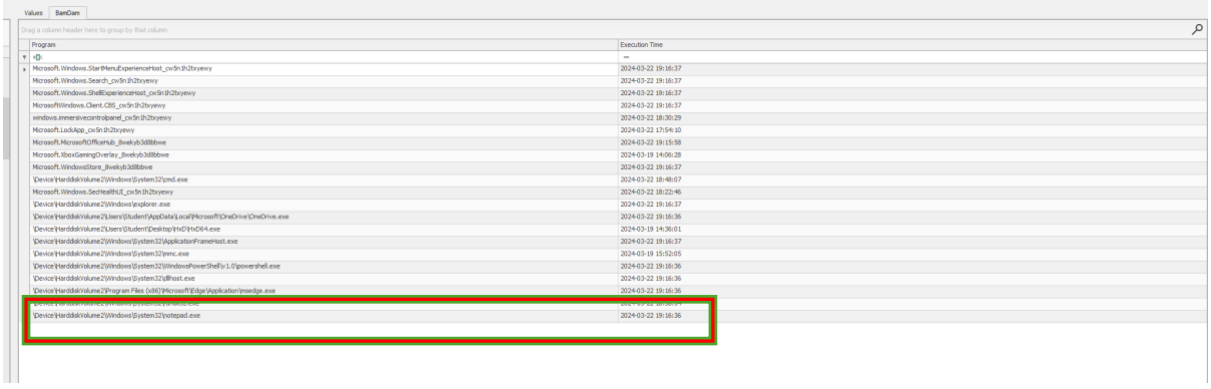
Tool Used: Registry Explorer

I loaded the SYSTEM hive into Registry Explorer and navigated to the following path: HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings I located the user account with RID 1001 (likely the student account) and examined the list of recorded executable paths and their execution times. From this list, I searched for entries referencing notepad.exe.

Findings:

Yes, Notepad was opened on 22nd March 2024.The BAM registry data shows that \Device\HarddiskVolume2\Windows\System32\notepad.exe was executed at: 2024-03-22 19:16:36.

Evidence



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

Approach:

I used Autopsy and went to the “File Types” section, then selected “Executables” to view all .exe files.

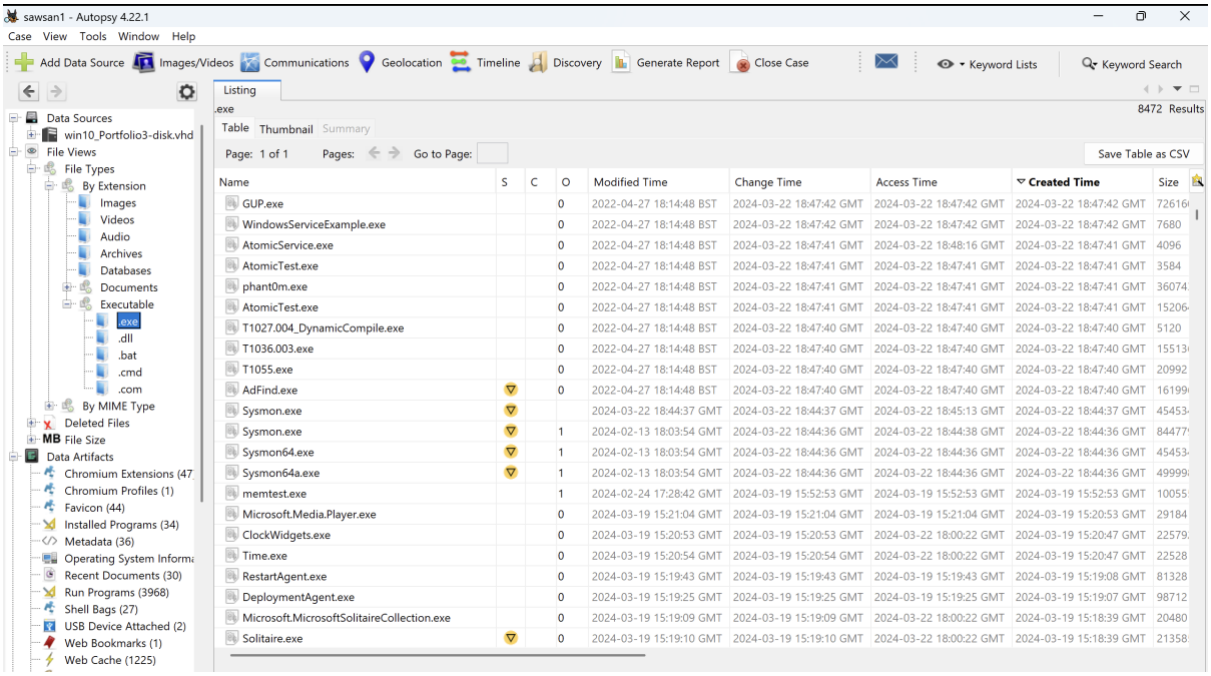
Methodology

Inside the Executables section, I sorted the files by the "Created Time" column to check which .exe files were created (and likely executed) on 22nd March 2024. I counted only the ones with that date.

Findings

11 .exe files were executed on 22nd March 2024.

Evidence



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

Approach

I used Autopsy and navigated to the “File Types” section, selecting “DLL” to view all dynamic link library files on the system.

Methodology

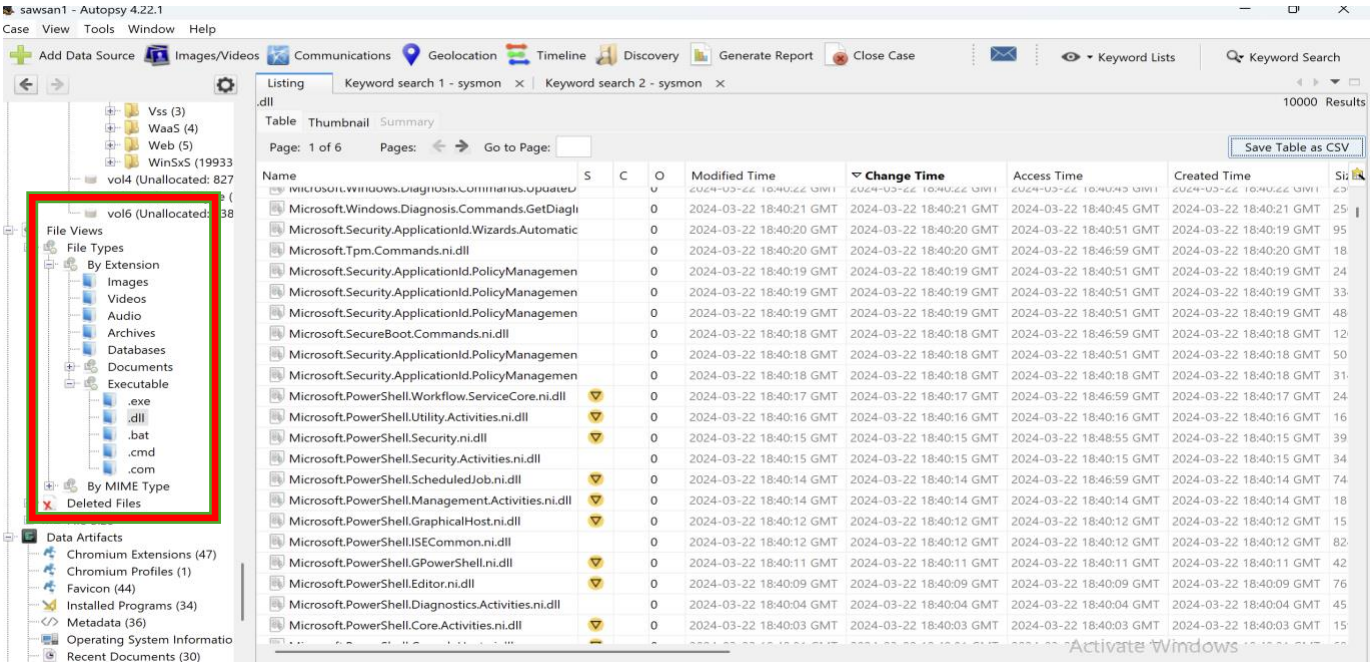
Tools Used: Autopsy and Google Sheets.
Since there were many .dll files, I exported the list to a CSV file and opened it in Google Sheets. I then filtered the "Created Time" column to show only files created on 22nd March 2024, which made counting easier.

Findings

A total of 149 .dll files were created on 22nd March 2024.

Evidence

Autopsy



Google sheet

9978	T1055.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	101888	Allocated	Allocated	unknown	/img_win10_Por	02b502b00c
9979	calc.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	9728	Allocated	Allocated	unknown	/img_win10_Por	8b38ee929a
9980	T1056.004x64.d	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	127488	Allocated	Allocated	unknown	/img_win10_Por	88599d1a42
9981	T1056.004x86.d	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	105472	Allocated	Allocated	unknown	/img_win10_Por	e58cd8fd29
9982	T1056.004.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	82944	Allocated	Allocated	unknown	/img_win10_Por	94a86d8f3d
9983	T1056.004.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	101888	Allocated	Allocated	unknown	/img_win10_Por	02b502b00c
9984	MSIRunner.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	92672	Allocated	Allocated	unknown	/img_win10_Por	52e020cf3fc
9985	calc.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	10240	Allocated	Allocated	unknown	/img_win10_Por	6349c0af16
9986	T1218-2.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	238869	Allocated	Allocated	unknown	/img_win10_Por	f8391705ce
9987	T1218.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	133898	Allocated	Allocated	unknown	/img_win10_Por	b6aefca8e8
9988	T1218.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	101888	Allocated	Allocated	unknown	/img_win10_Por	02b502b00c
9989	T1218-2.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	238869	Allocated	Allocated	unknown	/img_win10_Por	f8391705ce
9990	AllTheThingsx64	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	7168	Allocated	Allocated	unknown	/img_win10_Por	be0315717(
9991	AllTheThingsx86	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	7168	Allocated	Allocated	unknown	/img_win10_Por	bafdf3e64d7
9992	W64Time.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	124928	Allocated	Allocated	unknown	/img_win10_Por	73cb47627e
9993	T1546.010.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	9728	Allocated	Allocated	unknown	/img_win10_Por	55aca1639(
9994	T1546.010x86.d	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	8704	Allocated	Allocated	unknown	/img_win10_Por	6ba1b60c45
9995	AtomicTest.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	71168	Allocated	Allocated	unknown	/img_win10_Por	378783c07c
9996	AtomicTest.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	58880	Allocated	Allocated	unknown	/img_win10_Por	0773482ad7
9997	package.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	93216	Allocated	Allocated	unknown	/img_win10_Por	864d47df21
9998	libcurl.dll	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	10240	Allocated	Allocated	unknown	/img_win10_Por	fa740b2afb(
9999	T1574.012x64.d	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	9728	Allocated	Allocated	unknown	/img_win10_Por	83f016776d
10000	atomicNotepad.(	2022-04-27 18:1	2024-03-22 18:4	2024-03-22 18:4	2024-03-22 18:4	9728	Allocated	Allocated	unknown	/img_win10_Por	83f016776d

9851	bootvhd.dll	2024-02-24 17:2	2024-03-19 15:5	2024-03-19 15:5	2024-03-19 15:5	101232	Allocated	Allocated	unknown	/img_win10_Por	93850097588d2	729f7d96c43f1b application/x-ms dll
9852	AccessControl.d	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	15360	Allocated	Allocated	unknown	/img_win10_Por	d74bb4447af48c	5fd5d8aec97cffa application/x-ms dll
9853	System.dll	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	12288	Allocated	Allocated	unknown	/img_win10_Por	cff85c549d536f8	8dc562cda7217a application/x-ms dll
9854	UserInfo.dll	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	4096	Allocated	Allocated	unknown	/img_win10_Por	2f69afa9d17a52	e54989d2b83e7 application/x-ms dll
9855	nsDialogs.dll	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	9728	Allocated	Allocated	unknown	/img_win10_Por	6c3f8c94d07278	56b96add1978b application/x-ms dll
9856	nsExec.dll	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	7168	Allocated	Allocated	unknown	/img_win10_Por	675c4948e1efc9	1076ca39c449e application/x-ms dll
9857	nsProcess.dll	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	4608	Allocated	Allocated	unknown	/img_win10_Por	f0438a894f3a7e	30c6c3dd3cc7fc application/x-ms dll
9858	VBoxGuestInsta	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	2024-03-22 17:5	693072	Allocated	Allocated	unknown	/img_win10_Por	c5ffcc3285d5ea	3483548ce8d52 application/x-ms dll
9859	mpengine.dll	2024-02-24 03:4	2024-03-22 18:0	2024-03-22 18:1	2024-03-22 18:0	19471480	Allocated	Allocated	unknown	/img_win10_Por	348432b32a3cd	94e37aa3d76ea application/x-ms dll
9860	AuditPolicyGPM	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	17920	Allocated	Allocated	unknown	/img_win10_Por	7fb9477f9dfae7c	6f4f08a2b68b20 application/x-ms dll
9861	EventViewer.ni.c	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	607744	Allocated	Allocated	unknown	/img_win10_Por	97b7b561e6199	49a5de018b3b4 application/x-ms dll
9862	Microsoft.Applic	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	365056	Allocated	Allocated	unknown	/img_win10_Por	118cddb225b805	1fd0f203b85f9b5 application/x-ms dll
9863	Microsoft.Applic	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	792064	Allocated	Allocated	unknown	/img_win10_Por	28f254cb922a36	627ddc3adeee5 application/x-ms dll
9864	Microsoft.Certific	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	679424	Allocated	Allocated	unknown	/img_win10_Por	4ad9cf4ec0b89f	a9634b008106b application/x-ms dll
9865	Microsoft.Config	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	1048064	Allocated	Allocated	unknown	/img_win10_Por	25039f010cd65c	2ab08ffa923768 application/x-ms dll
9866	Microsoft.Dtc.Po	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	134656	Allocated	Allocated	unknown	/img_win10_Por	95bf5d2fdf9ddcc	28fc9c9d31f7c3 application/x-ms dll
9867	Microsoft.Groupl	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	557568	Allocated	Allocated	unknown	/img_win10_Por	2a87e1d27b83d	3a92c463ef2b07 application/x-ms dll
9868	Microsoft.Groupl	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	358400	Allocated	Allocated	unknown	/img_win10_Por	77454e9577161	9c0b038eab786 application/x-ms dll
9869	Microsoft.Groupl	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	5419008	Allocated	Allocated	unknown	/img_win10_Por	e9c3c2ab5b1b6l	37389970bbfd8a application/x-ms dll
9870	Microsoft.Interna	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	89088	Allocated	Allocated	unknown	/img_win10_Por	d06500637495a	6546e50ee7895 application/x-ms dll
9871	Microsoft.Isam.E	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	1647104	Allocated	Allocated	unknown	/img_win10_Por	033126c018daf5	a36ec2be83a2c application/x-ms dll
9872	Microsoft.Isam.E	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:3	1411072	Allocated	Allocated	unknown	/img_win10_Por	f4f0f3e112b8795	baf1df687271ca application/x-ms dll
9873	Microsoft.KeyDis	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	137728	Allocated	Allocated	unknown	/img_win10_Por	a6b1ca1c551bc	35ed77cda11aa2 application/x-ms dll
9874	Microsoft.Manag	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	648704	Allocated	Allocated	unknown	/img_win10_Por	ffe7e7402540b2	e8ac559430e6c5 application/x-ms dll
9875	Microsoft.Manag	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	555520	Allocated	Allocated	unknown	/img_win10_Por	b573d8723bfc9e	3f7ae3a347e118 application/x-ms dll
9876	Microsoft.Manag	2024-03-22 18:3	2024-03-22 18:3	2024-03-22 18:4	2024-03-22 18:3	668160	Allocated	Allocated	unknown	/img_win10_Por	0b992617a374e	8e14cfc7ec08d2 application/x-ms dll

How many .bat file was created on 22nd March 2024?

Approach:

I used Autopsy to go to the “File Types” section and selected .bat files to view all batch scripts on the system.

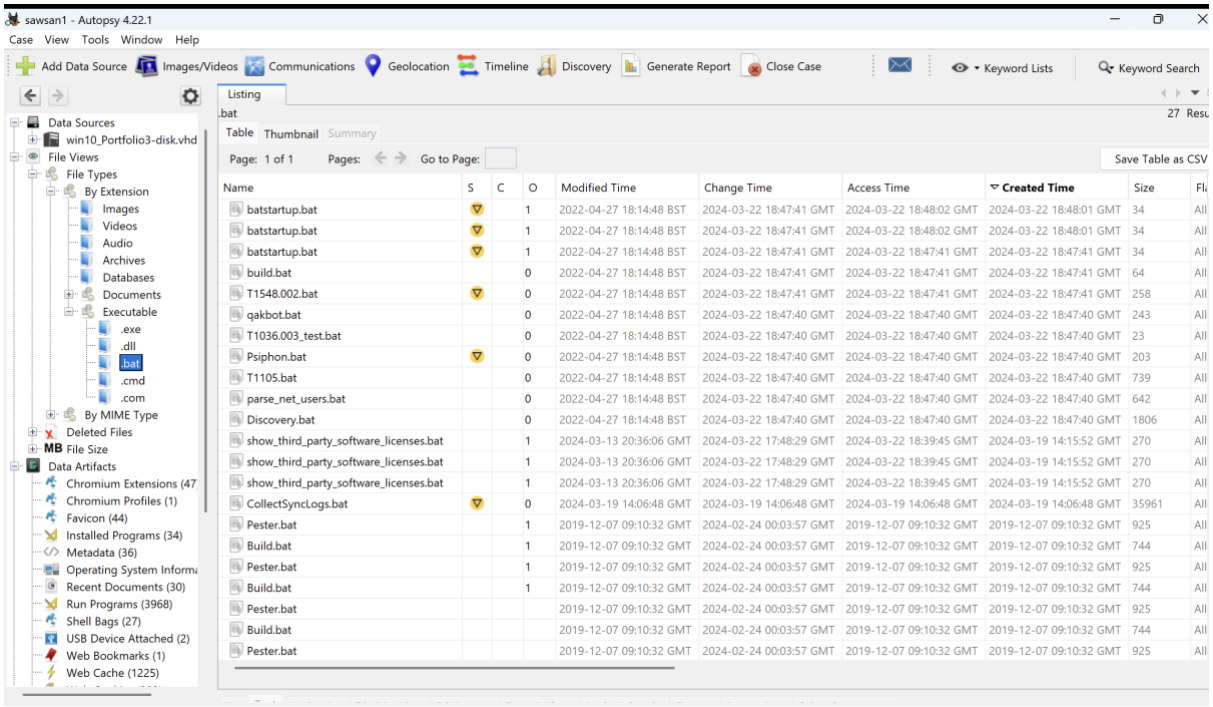
Methodology:

I sorted the .bat files by their "Created Time" directly in Autopsy and manually counted how many were created on 22nd March 2024.

Findings:

A total of 10 **.**bat files were created on 22nd March 2024.

Evidence:



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

Approach:

To determine if any malicious or suspicious file was accessed on 22nd March 2024, I examined the user directories — specifically the Desktop\File location under the student account. There, I found a PowerShell script named ART-attack.ps1, which appeared to be part of the Atomic Red Team framework. This framework is commonly used to simulate real-world attack behaviours for testing purposes. These types of scripts often imitate known techniques used by adversaries.

Methodology:

Tool Used: Autopsy

I navigated to the user directory at:
/Users/Student/Desktop/File/

I identified a PowerShell script named ART-attack.ps1, which appeared to be related to simulated adversarial activity.

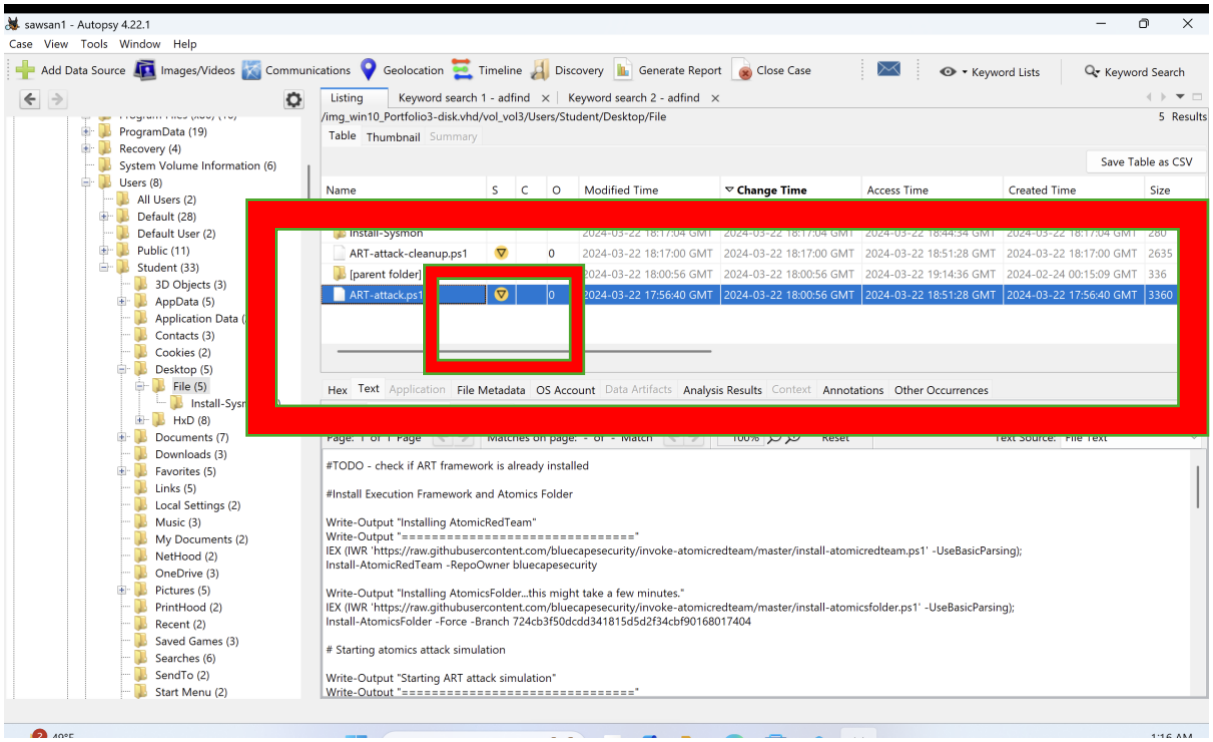
I examined the file metadata within Autopsy and noted the Accessed, Modified, Created, and Changed timestamps.

The folder path and location under the student user profile indicated the script was accessed by the student account.

Findings:

The file ART-attack.ps1 was accessed on 22nd March 2024 at 18:51:28 GMT.
It was found in the path: Users/Student/Desktop/File/ART-attack.ps1 Based on the file location and user folder, it was accessed by the student account.
The script contains commands related to installing and executing Atomic Red Team simulations, which imitate real-world attack behaviours and are often used in Red Team or penetration testing exercises.

Evidence:


sawsan1 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Keyword search 1 - adfind
Keyword search 2 - adfind
/img_win10_Portfolio3-disk.vhd/vol_vol3/Users/Student/Desktop/File
5 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
ART-attack-cleanup.ps1
[parent folder]
ART-attack.ps1
2024-03-22 18:17:00 GMT
2024-03-22 18:00:56 GMT
2024-03-22 17:56:40 GMT
2024-03-22 18:51:28 GMT
2024-02-24 00:15:09 GMT
2635
336
3360
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
ProgramData (19)
Recovery (4)
System Volume Information (6)
Users (8)
All Users (2)
Default (28)
Default User (2)
Public (11)
Student (33)
3D Objects (3)
AppData (5)
Contacts (3)
Cookies (2)
Desktop (5)
File (5)
HxD (8)
Documents (7)
Downloads (3)
Favorites (5)
Links (5)
Local Settings (2)
Music (3)
My Documents (2)
NetHood (2)
OneDrive (3)
Pictures (5)
PrintHood (2)
Recent (2)
Saved Games (3)
Searches (6)
SendTo (2)
Start Menu (2)
#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 "============================="

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

Approach:

To determine whether the Sysmon program was executed on 22nd March 2024, I examined the system for any artifacts related to its activity.
Since Sysmon is not always running by default, I specifically searched for Prefetch files**,** which are automatically generated by Windows when a program is executed. Prefetch analysis is a strong method for verifying whether an executable was run, and when.

Methodology:

Tool Used: Autopsy

I navigated to the Windows\Prefetch directory using Autopsy.

I searched for any .pf (Prefetch) files related to SYSMON.EXE.

I also checked the program's installation folder: ProgramData\Sysmon\Sysmon.exe

I reviewed the Access Time and Modified Time values to determine if Sysmon had been executed on the specified date.

Findings:

There is conclusive evidence that the Sysmon program was executed on 22nd March 2024 at 18:44:52 GMT**.** This is supported by the presence of the Prefetch file named SYSMON.EXE-CF2C172F.pf located in the C:\Windows\Prefetch\ directory. The Prefetch metadata shows:

Program Name: SYSMON.EXE

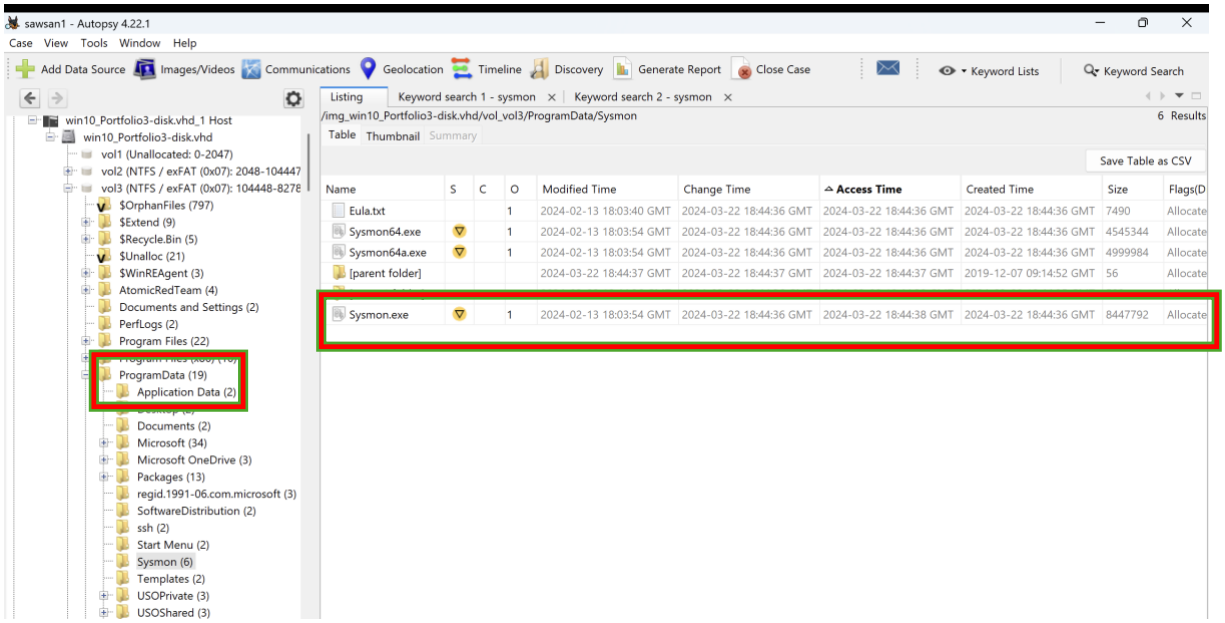
Path: C:\Windows

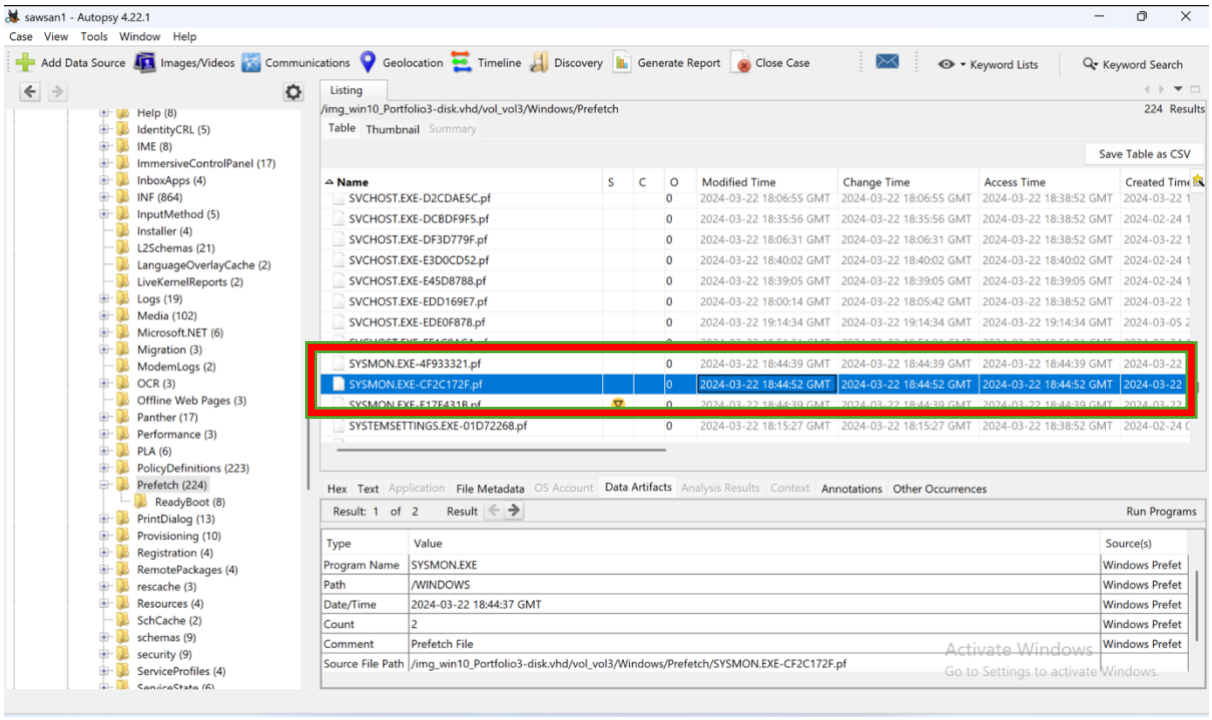
Execution Time: 2024-03-22 18:44:52 GMT

Run Count: 2 (indicating it was executed at least twice)

This confirms that Sysmon was not only installed but also actively run on that date a key indicator in forensic investigations for capturing system activity.

Evidence :




sawsan1 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch
224 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time
SVCHOST.EXE-D2CDAE5C.pf 0 2024-03-22 18:06:55 GMT 2024-03-22 18:06:55 GMT 2024-03-22 18:38:52 GMT 2024-03-22 1
SVCHOST.EXE-DCBDF9F5.pf 0 2024-03-22 18:35:56 GMT 2024-03-22 18:35:56 GMT 2024-03-22 18:38:52 GMT 2024-02-24 1
SVCHOST.EXE-DF3D779F.pf 0 2024-03-22 18:06:31 GMT 2024-03-22 18:06:31 GMT 2024-03-22 18:38:52 GMT 2024-03-22 1
SVCHOST.EXE-E3D0CD52.pf 0 2024-03-22 18:40:02 GMT 2024-03-22 18:40:02 GMT 2024-03-22 18:40:02 GMT 2024-02-24 1
SVCHOST.EXE-E45D8788.pf 0 2024-03-22 18:39:05 GMT 2024-03-22 18:39:05 GMT 2024-03-22 18:39:05 GMT 2024-02-24 1
SVCHOST.EXE-EDD169E7.pf 0 2024-03-22 18:00:14 GMT 2024-03-22 18:05:42 GMT 2024-03-22 18:38:52 GMT 2024-03-22 1
SVCHOST.EXE-EDE0F878.pf 0 2024-03-22 19:14:34 GMT 2024-03-22 19:14:34 GMT 2024-03-22 19:14:34 GMT 2024-03-05 2
SYSMON.EXE-4F933321.pf 0 2024-03-22 18:44:39 GMT 2024-03-22 18:44:39 GMT 2024-03-22 18:44:39 GMT 2024-03-22
SYSMON.EXE-CF2C172F.pf 0 2024-03-22 18:44:52 GMT 2024-03-22 18:44:52 GMT 2024-03-22 18:44:52 GMT 2024-03-22
SYSTEMSETTINGS.EXE-01D72268.pf 0 2024-03-22 18:15:27 GMT 2024-03-22 18:15:27 GMT 2024-03-22 18:38:52 GMT 2024-02-24
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 2 Result
Run Programs
Type Value Source(s)
Program Name SYSMON.EXE Windows Prefet
Path /WINDOWS Windows Prefet
Date/Time 2024-03-22 18:44:37 GMT Windows Prefet
Count 2 Windows Prefet
Comment Prefetch File Windows Prefet
Source File Path /img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch/SYSMON.EXE-CF2C172F.pf
Activate Windows
Go to Settings to activate Windows.
Help (8)
IdentityCRL (5)
IME (8)
ImmersiveControlPanel (17)
InboxApps (4)
INF (864)
InputMethod (5)
Installer (4)
L2Schemas (21)
LanguageOverlayCache (2)
LiveKernelReports (2)
Logs (19)
Media (102)
Microsoft.NET (6)
Migration (3)
ModemLogs (2)
OCR (3)
Offline Web Pages (3)
Panther (17)
Performance (3)
PLA (6)
PolicyDefinitions (223)
Prefetch (224)
ReadyBoot (8)
PrintDialog (13)
Provisioning (10)
Registration (4)
RemotePackages (4)
rescache (3)
Resources (4)
SchCache (2)
schemas (9)
security (9)
ServiceProfiles (4)

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

Approach:

To determine whether the AdFind tool was installed or executed on 22nd March 2024, I used Autopsy to perform a keyword search for AdFind.exe. The file was located under the Atomic Red Team directory at: /AtomicRedTeam/atomics/T1087.002/src/AdFind.exe.
Since AdFind is often used for enumeration in red team operations, verifying its presence and use was important for identifying potential suspicious or simulated attack activity.

Methodology:

Tools Used**:** Autopsy (Timeline Analysis, File View, Prefetch Viewer)

Performed a keyword search to locate AdFind.exe, which was found in the src folder of a test attack script.

Investigated the file path and script text to understand how it was placed on the system.

Checked the C:\Windows\Prefetch directory for a corresponding .pf file (which Windows creates when a program is executed).

Analysed the Timeline between 18:00–19:00 on 22nd March 2024 for any execution records related to AdFind.exe.

Reviewed extracted text from PowerShell-based test scripts included in the Atomic Red Team package.

Invoke-WebRequest -Uri "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1087.002/src/AdFind.exe" -OutFile #{adfind_path}

What this command does:

Invoke-WebRequest: A PowerShell command that downloads files from the internet.

-Uri: Points to the GitHub raw URL of the AdFind executable.

-OutFile: Specifies where to save the file locally (defined by #{adfind_path}).

In summary:
The script connects to GitHub, retrieves AdFind.exe from the /src/ directory of test T1087.002, and stores it locally on the machine for potential use.

Findings:

Yes, the AdFind executable was downloaded to the system as part of a red team test script.

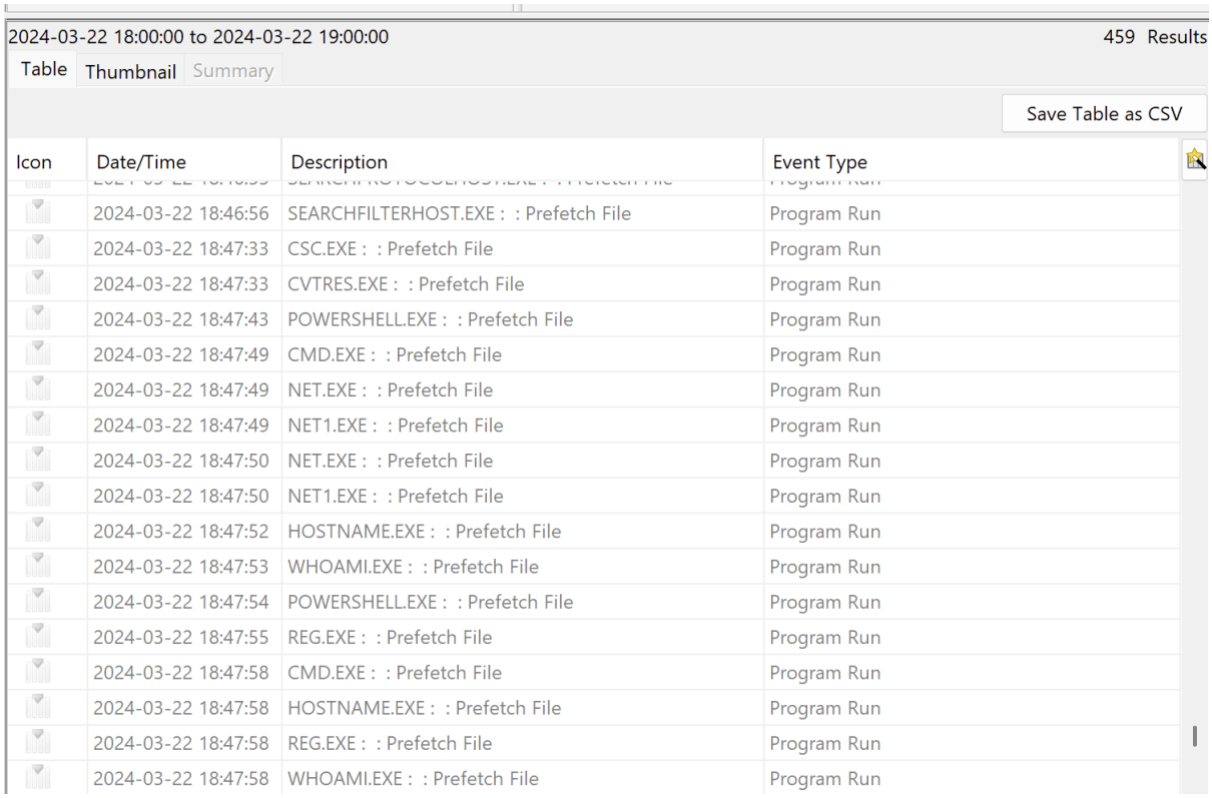
However, there is no evidence it was executed:

- No .pf (Prefetch) file for AdFind.exe was found.
- No execution records or events appeared in the Autopsy timeline for 22nd March 2024.

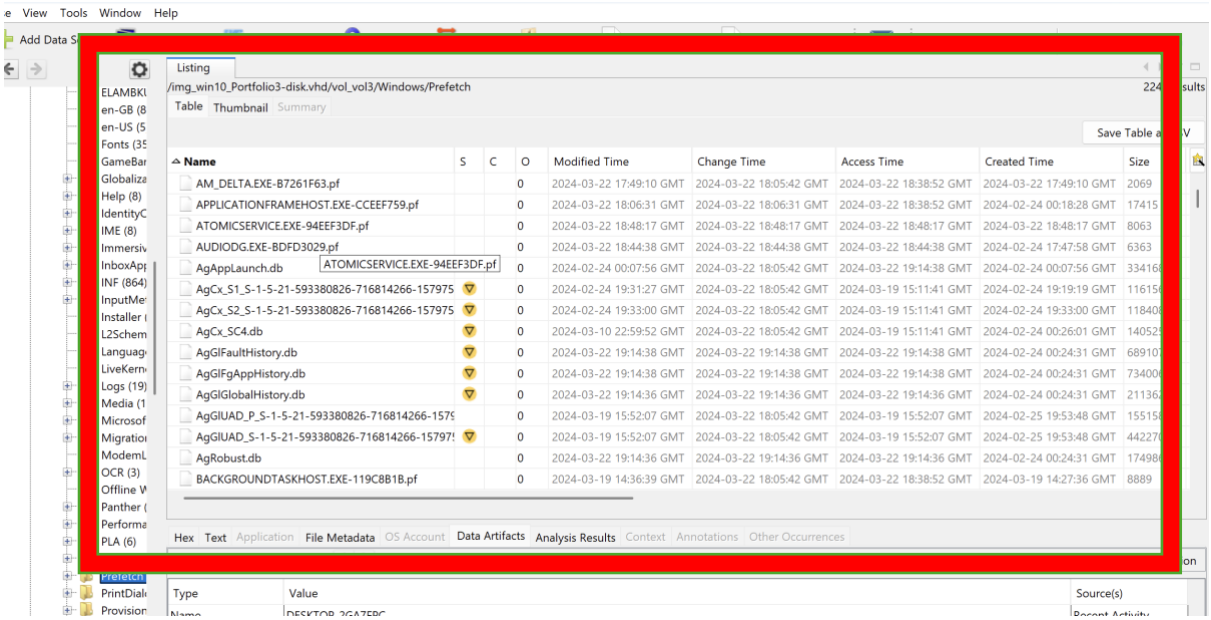
This confirms that AdFind.exe was present but not launched, suggesting the attack simulation was either incomplete or intentionally staged without running the tool.

Evidence:

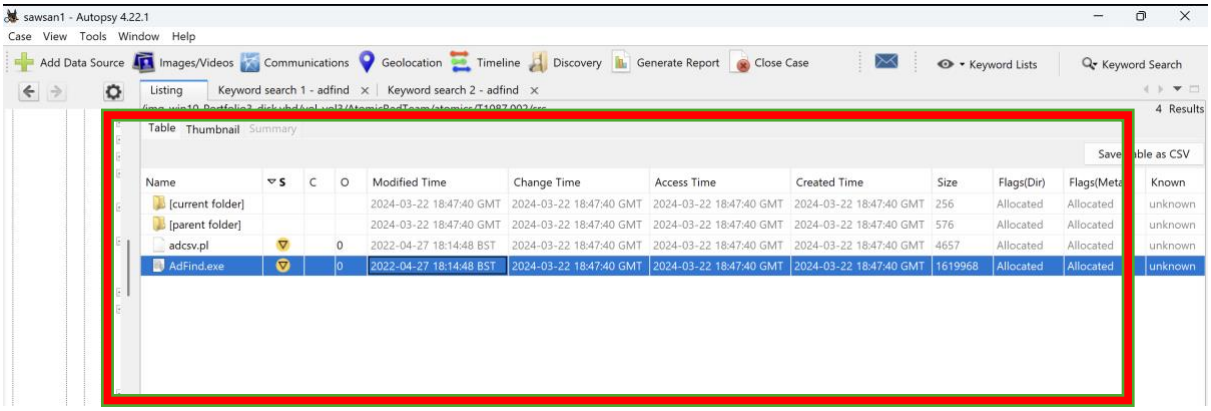
TIMELINE SHOWING NO ADFIND WAS RUNNING

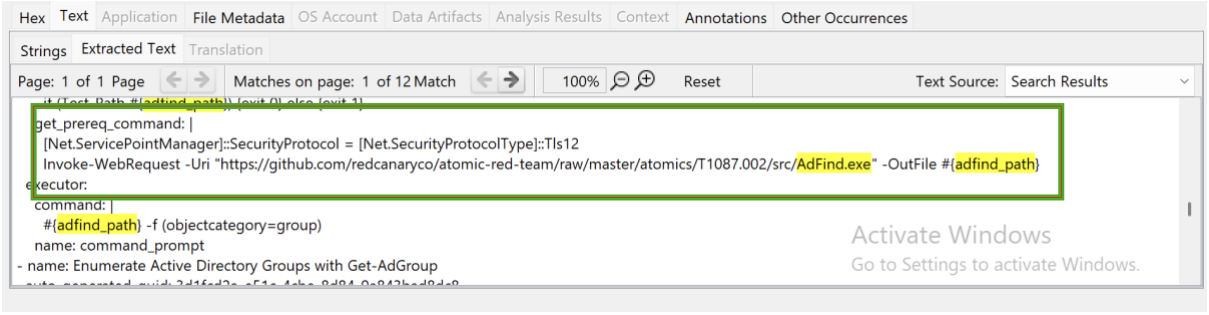


ADfind.exe not found in the prefetch



ADfind.exe was downloaded the text shows where it was downloaded from and how to download it.


sawsan1 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing Keyword search 1 - adfind Keyword search 2 - adfind
4 Results
Table Thumbnail Summary
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known
[current folder] 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 256 Allocated Allocated unknown
[parent folder] 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 576 Allocated Allocated unknown
adcsv.pl 0 2022-04-27 18:14:48 BST 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 4657 Allocated Allocated unknown
AdFind.exe 0 2022-04-27 18:14:48 BST 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 2024-03-22 18:47:40 GMT 1619968 Allocated Allocated unknown


Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 1 Page Matches on page: 1 of 12 Match 100% Reset Text Source: Search Results
get_prereq_command: |
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1087.002/src/AdFind.exe" -OutFile #{adfind_path}
executor:
command: |
#{adfind_path} -f (objectcategory=group)
name: command_prompt
- name: Enumerate Active Directory Groups with Get-AdGroup
Activate Windows
Go to Settings to activate Windows.

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

Approach:

To determine the number of times Command Prompt **(**cmd**.**exe) and PowerShell **(**powershell.exe) were executed on 22nd March 2024, I examined Windows Prefetch files a reliable forensic source for program execution activity. These Prefetch files not only store the name of the executed executable, but also the number of times it was launched and its exact timestamps.

Methodology:

Tool Used: Autopsy

I navigated to the C:\Windows\Prefetch directory using Autopsy's file viewer. I filtered the Prefetch files for:

CMD.EXE

POWERSHELL.EXE

For each .pf file, I reviewed:

The "Run Count**"** field.

The "Date/Time**"** field

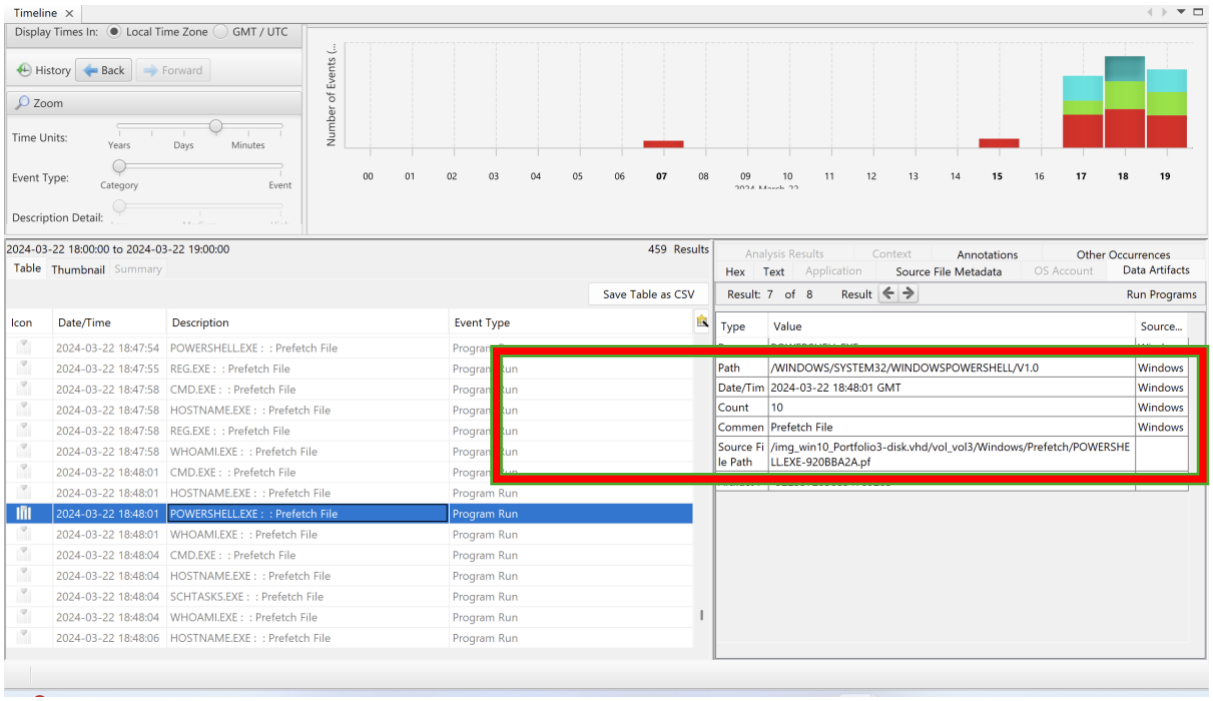
I confirmed the execution activity using Autopsy's Timeline View to cross-reference timestamps and validate the occurrence on the specific date.

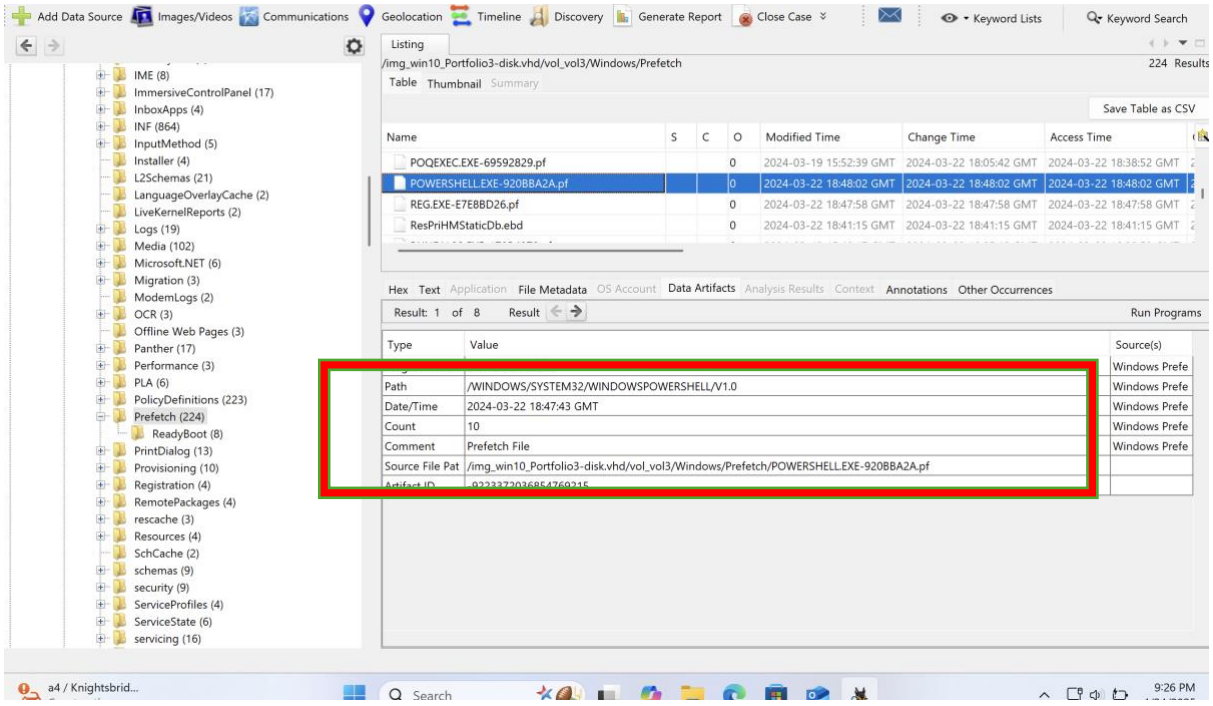
Findings:

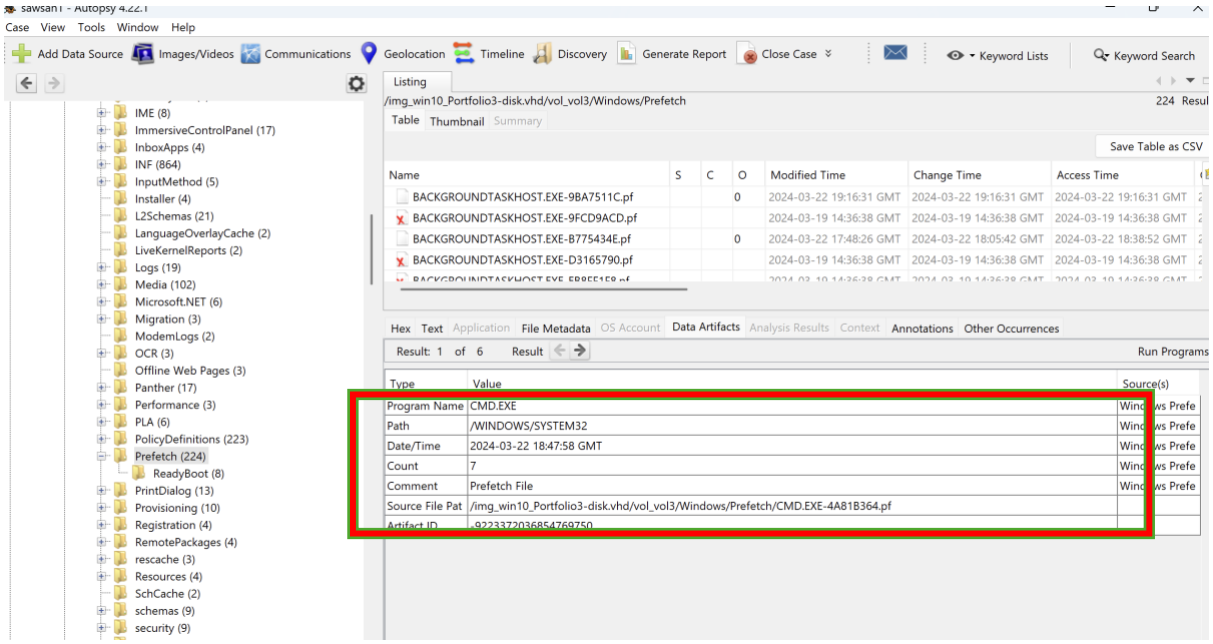
Command Prompt (CMD.EXE) was executed 7 times on 22nd March 2024, with a key execution logged at 18:47:58 GMT.

PowerShell (POWERSHELL.EXE) was executed 10 times at 18:47:43 GMT.

Evidence:


Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail:
Number of Events
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
2024-03-22 18:00:00 to 2024-03-22 19:00:00
459 Results
Table Thumbnail Summary
Save Table as CSV
Icon Date/Time Description Event Type
2024-03-22 18:47:54 POWERSHELL.EXE : : Prefetch File
2024-03-22 18:47:55 REG.EXE : : Prefetch File
2024-03-22 18:47:58 CMD.EXE : : Prefetch File
2024-03-22 18:47:58 HOSTNAME.EXE : : Prefetch File
2024-03-22 18:47:58 REG.EXE : : Prefetch File
2024-03-22 18:47:58 WHOAMI.EXE : : Prefetch File
2024-03-22 18:48:01 CMD.EXE : : Prefetch File
2024-03-22 18:48:01 HOSTNAME.EXE : : Prefetch File
2024-03-22 18:48:01 POWERSHELL.EXE : : Prefetch File Program Run
2024-03-22 18:48:01 WHOAMI.EXE : : Prefetch File
2024-03-22 18:48:04 CMD.EXE : : Prefetch File
2024-03-22 18:48:04 HOSTNAME.EXE : : Prefetch File
2024-03-22 18:48:04 SCHTASKS.EXE : : Prefetch File
2024-03-22 18:48:04 WHOAMI.EXE : : Prefetch File
2024-03-22 18:48:06 HOSTNAME.EXE : : Prefetch File
Analysis Results Context Annotations Other Occurrences
Hex Text Application Source File Metadata OS Account Data Artifacts
Result: 7 of 8 Result
Run Programs
Type Value Source...
Path /WINDOWS/SYSTEM32/WINDOWSPOWERSHELL/V1.0 Windows
Date/Tim 2024-03-22 18:48:01 GMT Windows
Count 10 Windows
Commen Prefetch File Windows
Source Fi le Path /img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch/POWERSHELL.EXE-920BBA2A.pf


Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
IME (8)
ImmersiveControlPanel (17)
InboxApps (4)
INF (864)
InputMethod (5)
Installer (4)
L2Schemas (21)
LanguageOverlayCache (2)
LiveKernelReports (2)
Logs (19)
Media (102)
Microsoft.NET (6)
Migration (3)
ModemLogs (2)
OCR (3)
Offline Web Pages (3)
Panther (17)
Performance (3)
PLA (6)
PolicyDefinitions (223)
Prefetch (224)
ReadyBoot (8)
PrintDialog (13)
Provisioning (10)
Registration (4)
RemotePackages (4)
rescache (3)
Resources (4)
SchCache (2)
schemas (9)
security (9)
ServiceProfiles (4)
ServiceState (6)
servicing (16)
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch
224 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time
POQEXEC.EXE-69592829.pf 0 2024-03-19 15:52:39 GMT 2024-03-22 18:05:42 GMT 2024-03-22 18:38:52 GMT
POWERSHELL.EXE-920BBA2A.pf 0 2024-03-22 18:48:02 GMT 2024-03-22 18:48:02 GMT 2024-03-22 18:48:02 GMT
REG.EXE-E7E8BD26.pf 0 2024-03-22 18:47:58 GMT 2024-03-22 18:47:58 GMT 2024-03-22 18:47:58 GMT
ResPriHMStaticDb.ebd 0 2024-03-22 18:41:15 GMT 2024-03-22 18:41:15 GMT 2024-03-22 18:41:15 GMT
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Run Programs
Type Value Source(s)
Path /WINDOWS/SYSTEM32/WINDOWSPOWERSHELL/V1.0 Windows Prefe
Date/Time 2024-03-22 18:47:43 GMT Windows Prefe
Count 10 Windows Prefe
Comment Prefetch File Windows Prefe
Source File Pat /img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch/POWERSHELL.EXE-920BBA2A.pf
Search
9:26 PM


Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
BACKGROUNDTASKHOST.EXE-9BA7511C.pf
BACKGROUNDTASKHOST.EXE-9FCD9ACD.pf
BACKGROUNDTASKHOST.EXE-B775434E.pf
BACKGROUNDTASKHOST.EXE-D3165790.pf
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 1 of 6
Result
Run Programs
Type
Value
Source(s)
Program Name
CMD.EXE
Path
/WINDOWS/SYSTEM32
Date/Time
2024-03-22 18:47:58 GMT
Count
7
Comment
Prefetch File
Source File Pat
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch/CMD.EXE-4A81B364.pf
IME (8)
ImmersiveControlPanel (17)
InboxApps (4)
INF (864)
InputMethod (5)
Installer (4)
L2Schemas (21)
LanguageOverlayCache (2)
LiveKernelReports (2)
Logs (19)
Media (102)
Microsoft.NET (6)
Migration (3)
ModemLogs (2)
OCR (3)
Offline Web Pages (3)
Panther (17)
Performance (3)
PLA (6)
PolicyDefinitions (223)
Prefetch (224)
ReadyBoot (8)
PrintDialog (13)
Provisioning (10)
Registration (4)
RemotePackages (4)
rescache (3)
Resources (4)
SchCache (2)
schemas (9)
security (9)

What size was recorded for AtomicService.exe?

Approach:

I used Autopsy to examine the C:\Windows\Prefetch folder and located the prefetch file for AtomicService.exe. Checking file size is crucial in forensic investigations as it helps determine the integrity of a file, assess its relevance, and identify potential tampering or malicious activity. File size can indicate if a file has been modified, or fragmented, or if any unexpected space is present, which may suggest malicious behaviour or corruption.

Methodology:

Tool used: Autopsy

- Navigated to C:\Windows\Prefetch
- Found the file named ATOMICSERVICE.EXE-94EEF3DF.pf

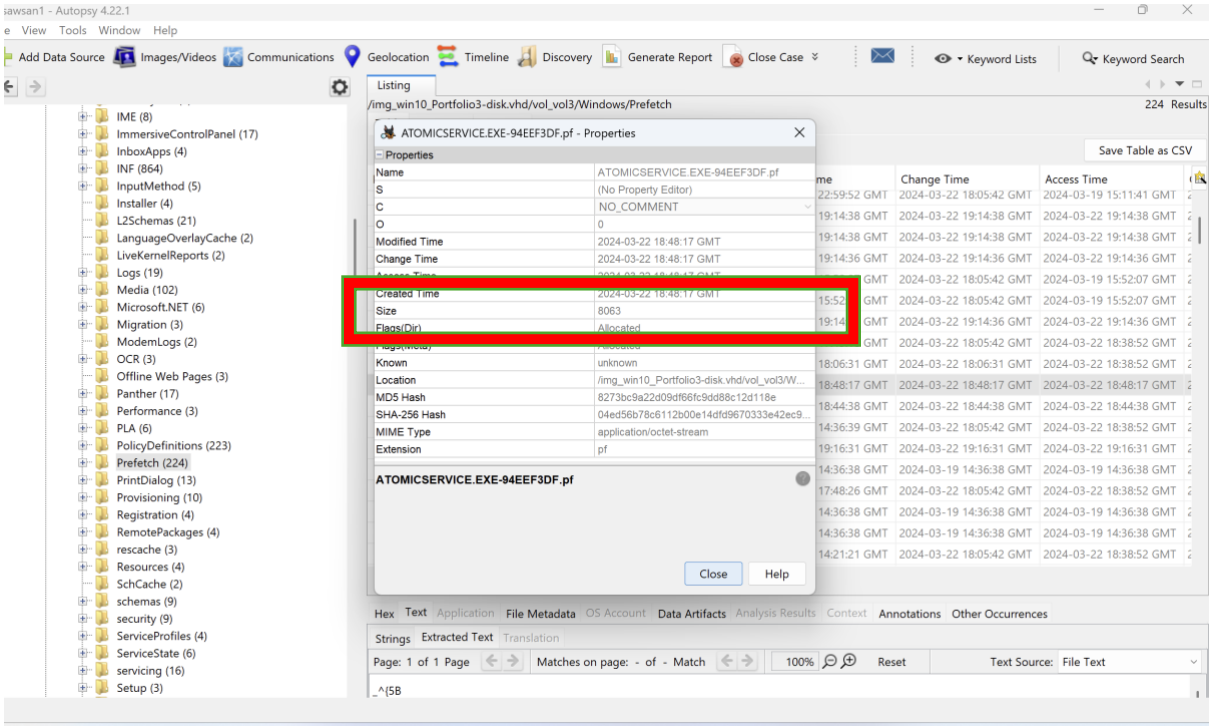
Findings:

File name: ATOMICSERVICE.EXE

Prefetch file: ATOMICSERVICE.EXE-94EEF3DF.pf

Size recorded: 8063 bytes

Evidence:


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_win10_Portfolio3-disk.vhd/vol_vol3/Windows/Prefetch
224 Results
Save Table as CSV
ATOMICSERVICE.EXE-94EEF3DF.pf - Properties
Properties
Name
ATOMICSERVICE.EXE-94EEF3DF.pf
S
(No Property Editor)
C
NO_COMMENT
O
0
Modified Time
2024-03-22 18:48:17 GMT
Change Time
2024-03-22 18:48:17 GMT
Created Time
2024-03-22 18:48:17 GMT
Size
8063
Flags(Dir)
Allocated
Known
unknown
Location
/img_win10_Portfolio3-disk.vhd/vol_vol3/W...
MD5 Hash
8273bc9a22d09df66fc9dd88c12d118e
SHA-256 Hash
04ed56b78c6112b00e14dfd9670333e42ec9...
MIME Type
application/octet-stream
Extension
pf
ATOMICSERVICE.EXE-94EEF3DF.pf
Close
Help
Change Time
Access Time
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Extracted Text
Translation
Page: 1 of 1 Page
Matches on page: - of - Match
100%
Reset
Text Source:
File Text
IME (8)
ImmersiveControlPanel (17)
InboxApps (4)
INF (864)
InputMethod (5)
Installer (4)
L2Schemas (21)
LanguageOverlayCache (2)
LiveKernelReports (2)
Logs (19)
Media (102)
Microsoft.NET (6)
Migration (3)
ModemLogs (2)
OCR (3)
Offline Web Pages (3)
Panther (17)
Performance (3)
PLA (6)
PolicyDefinitions (223)
Prefetch (224)
PrintDialog (13)
Provisioning (10)
Registration (4)
RemotePackages (4)
rescache (3)
Resources (4)
SchCache (2)
schemas (9)
security (9)
ServiceProfiles (4)
ServiceState (6)
servicing (16)
Setup (3)

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

Approach:

To create a timeline of suspicious execution events, I examined the contents of the C:\Windows\Prefetch folder using Autopsy and PECmd. Prefetch files record details about programs that were run, including how many times and when. This information helps identify unusual or repeated program executions that might be linked to suspicious activity.

Methodology:

Tools used: Autopsy, PECmd

Opened the forensic image in Autopsy.

Located the C:\Windows\Prefetch directory.

Extracted the .pf (prefetch) files.

Used PECmd to parse and analyse the files for execution counts and timestamps.

Created a timeline of each suspicious program’s activity based on run history.

Findings:

Executable NAME	Run count	Last run	Previous Run 0	Previous Run1	Previous Run 2	Previous Run3	Previous Run 4	Previous Run5	Previous Run 6
POWERSHELL.EXE	10	2024-03-22 18:47:54	2024-03-22 18:47:54	2024-03-22 18:47:43	2024-03-22 18:47:54	2024-03-22 18:44:26	2024-03-22 18:34:555	2024-03-22 18:39:08	2024-03-22 18:39:08
cmd.exe	7	2024-03-22 18:48:07	2024-03-22 18:48:04	2024-03-22 18:48:01	2024-03-22 18:48:01	2024-03-22 18:47:58	2024-03-22 18:47:49	2024-03-22 17:48:19	
NET.exe	3	2024-03-22 18:47:50	2024-03-22 18:47:50	2024-03-22 18:47:49					
REG.exe	2	2024-03-22 18:47:58	2024-03-22 18:47:55						
SCHTASKS.exe	2	2024-03-22 18:48:04	2024-03-22 18:48:04						
SC.exe	4	2024-03-22 18:48:07	2024-03-22 18:48:07	2024-03-22 18:44:39	2024-03-22 17:53:35				

ATOMICSERVICE.EXE	1	2024-03-22 18:48:07							
MAVINJECT.exe	1	2024-03-22 18:48:10							
NOTEPAD.exe	3	2024-03-22 18:48:10	2024-02-24 19:58:58	2024-02-24 18:17:04					

POWERSHELL.EXE – A tool used to run powerful scripts. Attackers often use it to download or run malicious commands without being noticed. It was used the most (10 times), and attackers use PowerShell for malicious tasks.

CMD.EXE – This is the Command Prompt. It's used to type commands that control the computer. If used a lot, it may mean someone was running scripts or commands manually.

SC.EXE – Used to manage Windows services (like starting or stopping background programs). Attackers can use it to install malicious services that run automatically.

NOTEPAD.EXE – Just the regular Notepad program. Usually harmless, but it can be used to open or write parts of scripts or code.

NET.EXE – A tool to manage users and networks. An attacker might use it to check who’s on the system or change user settings.

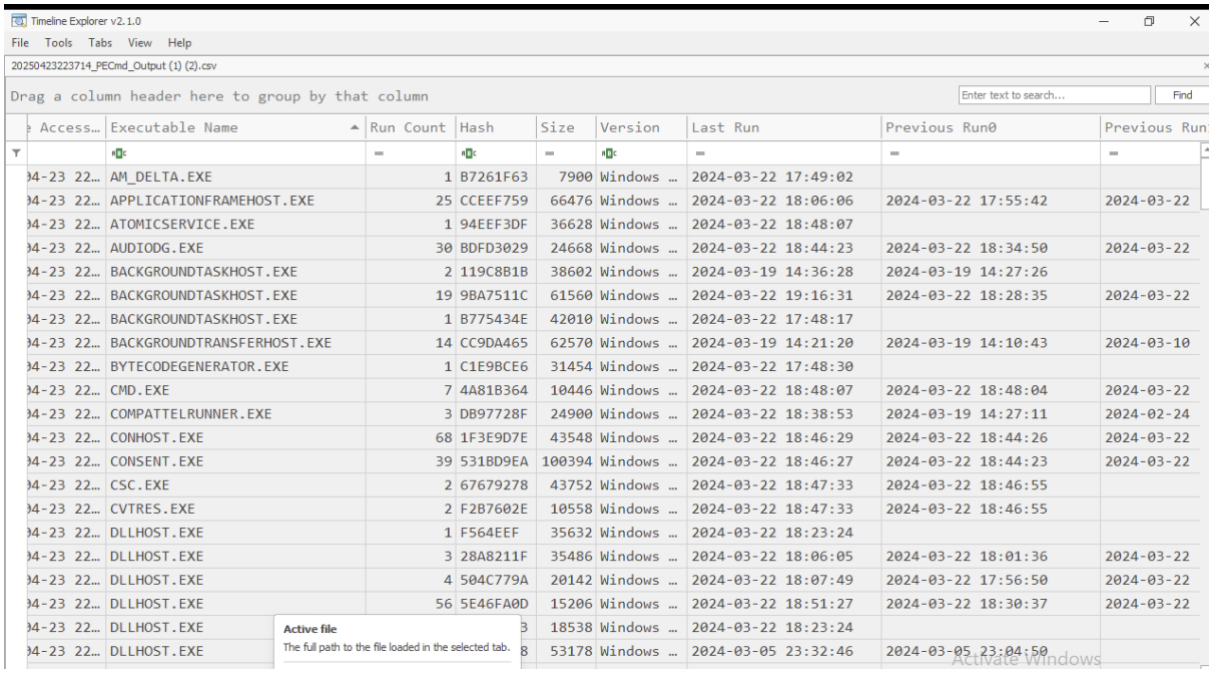
SCHTASKS.EXE – Used to create or manage scheduled tasks (like setting something to run every day). Attackers can use it to make their programs run automatically.

REG.EXE Lets you make changes to the Windows Registry (the system's settings database). Malware often changes registry settings to control system behaviour.

ATOMICSERVICE.EXE – This came from the Atomic Red Team, a tool for simulating real attacks. While used for testing, it mimics actual attacks and could show risky behaviour.

MAVINJECT.EXE – A tool that can inject code into other programs. It's a known way to make malicious code run inside trusted programs.

Evidence:



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

Approach:

Run keys in the Windows Registry are used to automatically start programs every time a user logs into Windows. Malware and persistence mechanisms often abuse these keys to re-launch themselves without needing user interaction. To check for this, I analysed the NTUSER.DAT file from the "student" profile using Registry Explorer to examine the registry path for any Autorun entries.

Methodology:

Tool used: Registry Explorer

Loaded the student's NTUSER.DAT hive.

Navigated to the key:
Software\Microsoft\Windows\CurrentVersion\Run

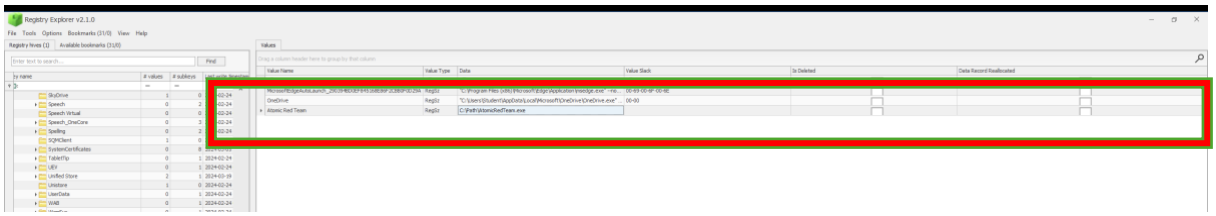
Looked for values that specify executable file paths meant to start on login.

Verified if any of those pointed to AtomicService.exe.

Findings:

The registry entry under the Run key shows a value named AtomicService with the following path: C:\Users\student\OneDrive\Desktop\AtomicService.exeThis indicates that the AtomicService.exe was configured to automatically start whenever the "student" user logged into the system.

Evidence



Identify what is the name of the suspicious script in the StartUp folder?

Approach:

To identify any potentially malicious scripts set to run at startup, I examined the contents of the user's Startup folder. The Startup folder is a common location where attackers place scripts to gain persistence, meaning the script runs each time the user logs in.

Methodology:

Used Autopsy to navigate to the path: C:\Users\student\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

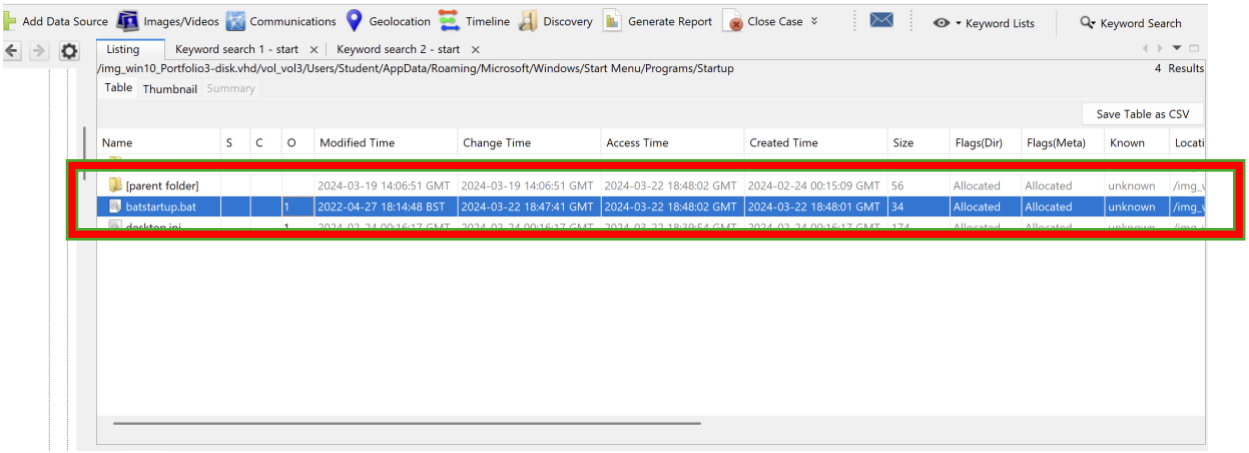
Looked for any unusual or user-created files in that location.

Checked file names and extensions for scripts (.bat, .ps1, .vbs, etc.).

Findings:

A file named desktop.bat was found in the Startup folder. Batch (.bat) files can contain command-line instructions and are often used to launch programs or execute commands automatically. Its presence here strongly suggests it was placed to run malicious or unauthorized code when the system started.

Evidence:



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

Approach:

To identify which tasks were scheduled to run at logon and startup, I used Autopsy to inspect the extracted registry hives for any entries related to task scheduling. I focused on keys that included names like OnLogon and OnStartup, which typically represent tasks triggered when a user logs in or the system starts up.

Methodology:

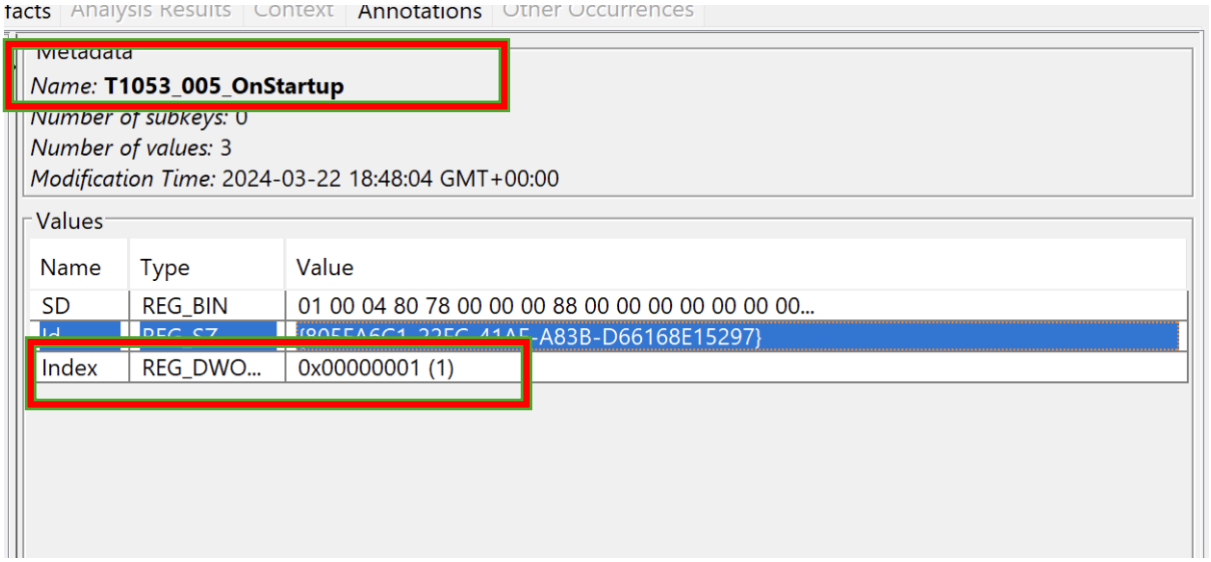
Within Autopsy, I navigated to the Data Artifacts and then to the Registry section. I searched for task-related keys under the TaskCache node. From there, I located entries named T1053_005_OnStartup and T1053_005_OnLogon. The number of times each task was executed was identified by checking the Index value, which represents the run count.

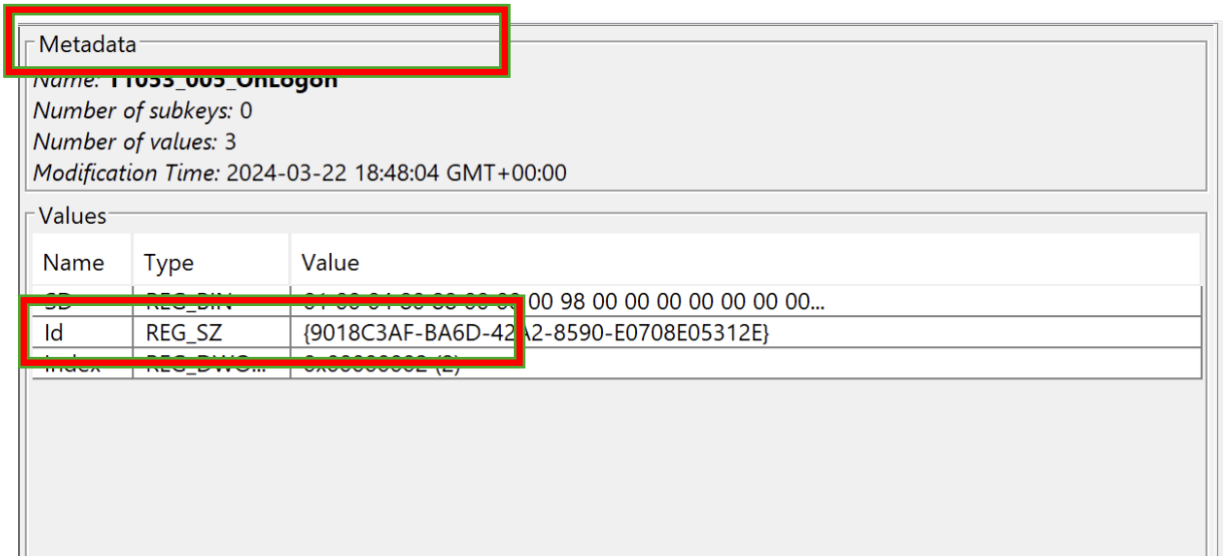
Findings:

T1053_005_OnStartup was executed once (Index: 1)

T1053_005_OnLogon was executed twice (Index: 2)

Evidence:


facts
Analysis Results
Context
Annotations
Other Occurrences
Metadata
Name: T1053_005_OnStartup
Number of subkeys: 0
Number of values: 3
Modification Time: 2024-03-22 18:48:04 GMT+00:00
Values
Name
Type
Value
SD
REG_BIN
01 00 04 80 78 00 00 00 88 00 00 00 00 00 00 00...
Index
REG_DWO...
0x00000001 (1)

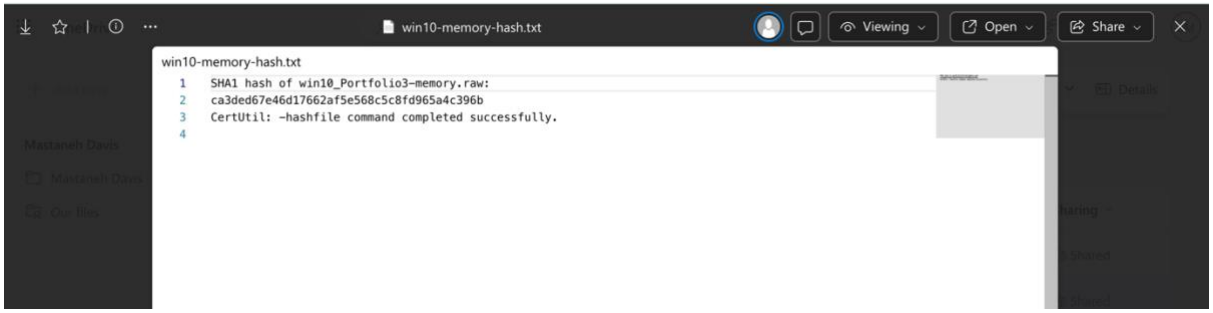

Metadata
Number of subkeys: 0
Number of values: 3
Modification Time: 2024-03-22 18:48:04 GMT+00:00
Values
Name
Type
Value
Id
REG_SZ
{9018C3AF-BA6D-42
2-8590-E0708E05312E}

Component 2

Verification of Evidence Integrity

```
Algorithm       Hash
---------       ----
SHA1            CA3DED67E46D17662AF5E568C5C8FD965A4C396B
```

Verification of hashes is matched



Provide additional evidence by carrying out an investigation of digital forensics artefacts such as **log files** or **memory** or **file system. For example,** analyse win10-Portfolio3-memory.raw using the Volatility tool and provide a timeline of execution events and identifying process owners and SIDs for the relevant programmes.

PID	PPID	Process	SID	Owner/Notes	Timestamp	Execution Explanation	Execution Time	Malfind Flag	Netscan Flag
4364	4156	powershell.exe	S-1-5-21-593380826-716814266-1579754837-1001	Student	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-21-593380826-716814266-1579754837-513	Domain Users	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-1-0	Everyone	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-114	Local Account (Member of Administrators)	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES

4364	4156	powershell.exe	S-1-5-32-544	Administrators	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-32-545	Users	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-4	Interactive	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-2-1	Console Logon (Users who are logged onto the physical console)	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-11	Authenticated Users	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-15	This Organization	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-113	Local Account	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-5-0-164167	Logon Session	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-2-0	Local (Users with the ability to log in locally)	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-5-64-10	NTLM Authentication	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES
4364	4156	powershell.exe	S-1-16-12288	High Mandatory Level	2024-03-22 18:46:29.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	YES

2848	648	MsMpEng.exe	S-1-5-18	Local System	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-16-16384	System Mandatory Level	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-1-0	Everyone	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-5-32-545	Users	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-5-6	Service	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-2-1	Console Logon (Users who are logged onto the physical console)	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-5-11	Authenticated Users	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-5-15	This Organization	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736	Win Defend	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-5-5-0-122253	Logon Session	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2848	648	MsMpEng.exe	S-1-2-0	Local (Users with the ability to log in locally)	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO

2848	648	MsMpEng.exe	S-1-5-32-544	Administrators	2024-03-22 18:05:43.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2200	648	AtomicService.	S-1-5-18	Local System	2024-03-22 18:48:07.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2200	648	AtomicService.	S-1-5-32-544	Administrators	2024-03-22 18:48:07.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2200	648	AtomicService.	S-1-1-0	Everyone	2024-03-22 18:48:07.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2200	648	AtomicService.	S-1-5-11	Authenticated Users	2024-03-22 18:48:07.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
2200	648	AtomicService.	S-1-16-16384	System Mandatory Level	2024-03-22 18:48:07.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	N/A	YES	NO
7376	1152	mavinject.exe		Suspicious injection tool;	2024-03-22 18:48:10.000000 UTC	Exit Time missing, the process likely still running at the time of memory capture	43	NO	NO

Volatility Plugin Analysis Summary

1. Malfind – Evidence of Code Injection

The malfind plugin revealed several memory regions marked PAGE_EXECUTE_READWRITE within critical processes such as powershell.exe, AtomicService.exe, and MsMpEng.exe. These permissions are characteristic of in-memory code injection, often used in fileless attacks to execute shellcode without leaving disk traces. Notably, the presence of executable memory within MsMpEng.exe (Windows Defender) is highly anomalous, raising serious concerns about process compromise.

2. netscan – Suspicious Network Activity

The netscan plugin detected outbound connections from powershell.exe (PID 4364) to various external IP addresses:

- 140.82.121.9 – GitHub
- 204.79.197.203, 204.79.197.222 – Microsoft
- 23.48.165.34, 13.107.213.64, 23.37.1.150 – Likely CDNs or attacker-controlled servers

All communications occurred over encrypted HTTPS (port 443). Some sessions remained in CLOSE_WAIT or ESTABLISHED state, suggesting persistent communication typical of command-and-control (C2) beaconing or data exfiltration behaviour. This suggests that the company's network has been tampered with.

3. AtomicService.exe – Possible Local Scanning Tool

AtomicService.exe (PID 2200) is not a known Windows file and seems to be part of the Atomic Red Team toolkit, which is used to test security systems. It didn’t connect to the internet but had injected code in memory and was running with high privileges**,** meaning it could be used to scan or check system settings locally.

4. powershell.exe – Multiple User Contexts and Network Activity

The powershell.exe process (PID 4364) demonstrated behaviour across multiple security identifiers (SIDs), including:

- Administrators
- Domain Users
- Local Account
- Authenticated Users

This diversity of user contexts suggests token manipulation or impersonation. The process was persistent in memory, engaged in outbound network communications, and was flagged by both malfind and netscan, indicating it may have been a command-and-control component or script executor.

5. MsMpEng.exe – Abnormal Code in Antivirus Process

The MsMpEng.exe process (PID 2848), associated with Windows Defender, was marked by malfind as containing anomalous executable memory. Despite lacking network activity, its high-integrity level (System, Administrators) means any compromise could have serious implications. Suspicious behaviour in this typically trusted process indicates it may have been targeted for abuse.

6. mavinject.exe – Brief Process with Injection Behaviour

The mavinject.exe process (PID 7376) appeared only in psscan, not pslist, indicating it had likely terminated or been hidden. It executed briefly for approximately 43 seconds—enough time to perform its native role: injecting code into other processes. Due to its design and timing, its activity is highly indicative of process hollowing or remote thread injection.

Evidence Volatility used:

Pslist.txt

```
Volatility 3 Framework 2.26.2
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xb605a5681080  128     -       N/A     False   2024-03-22 18:05:28.000000 UTC  N/A     Disabled
92      4       Registry        0xb605a57c6040  4       -       N/A     False   2024-03-22 18:05:13.000000 UTC  N/A     Disabled
348     4       smss.exe        0xb605a60d4040  2       -       N/A     False   2024-03-22 18:05:28.000000 UTC  N/A     Disabled
440     428     csrss.exe       0xb605ab709080  10      -       0       False   2024-03-22 18:05:39.000000 UTC  N/A     Disabled
516     428     wininit.exe     0xb605abeed080  1       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
528     508     csrss.exe       0xb605abef3080  12      -       1       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
608     508     winlogon.exe    0xb605abf39080  5       -       1       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
648     516     services.exe    0xb605abee6080  7       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
656     516     lsass.exe       0xb605abef2140  8       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
772     648     svchost.exe     0xb605abfd3240  20      -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
792     516     fontdrvhost.ex  0xb605abfd9140  5       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
800     608     fontdrvhost.ex  0xb605abfdb140  5       -       1       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
884     648     svchost.exe     0xb605ac6e12c0  11      -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
936     648     svchost.exe     0xb605ac720240  4       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1012    608     dwm.exe 0xb605ac755080  16      -       1       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
684     648     svchost.exe     0xb605ac7de2c0  2       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1036    648     svchost.exe     0xb605ac80b300  3       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1044    648     svchost.exe     0xb605ac80c080  2       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1052    648     svchost.exe     0xb605ac81d300  5       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1188    648     svchost.exe     0xb605ac86b240  7       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1196    648     svchost.exe     0xb605ac86d300  8       -       0       False   2024-03-22 18:05:40.000000 UTC  N/A     Disabled
1252    648     svchost.exe     0xb605ac875240  3       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabledx
1316    648     svchost.exe     0xb605ac8c92c0  3       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1328    648     svchost.exe     0xb605ac8cb300  1       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1376    648     svchost.exe     0xb605ac90b240  6       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1408    648     svchost.exe     0xb605ac93f300  6       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1540    648     svchost.exe     0xb605ac983300  5       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1640    648     VBoxService.ex  0xb605ac9c3240  11      -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1656    648     svchost.exe     0xb605ac9c52c0  3       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1696    648     svchost.exe     0xb605ac9c72c0  6       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1708    648     svchost.exe     0xb605a567b080  3       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1728    648     svchost.exe     0xb605a567c080  3       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1804    648     svchost.exe     0xb605ac9c4080  8       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1836    4       MemCompression  0xb605a5680040  54      -       N/A     False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1876    648     svchost.exe     0xb605aca560c0  2       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1904    648     svchost.exe     0xb605abf2d080  2       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1912    648     svchost.exe     0xb605ac9ca080  4       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
2044    648     svchost.exe     0xb605acac3300  4       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
1424    648     svchost.exe     0xb605acac62c0  9       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
2056    648     svchost.exe     0xb605acb0a300  9       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
2064    648     svchost.exe     0xb605acb0b080  4       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
2072    648     svchost.exe     0xb605acb0c080  4       -       0       False   2024-03-22 18:05:41.000000 UTC  N/A     Disabled
2184    648     svchost.exe     0xb605acbae240  6       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2192    648     svchost.exe     0xb605acb93080  2       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2328    648     spoolsv.exe     0xb605acc28200  7       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2392    648     svchost.exe     0xb605acc2a2c0  13      -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2440    648     svchost.exe     0xb605acc52300  3       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2568    648     svchost.exe     0xb605acd18240  4       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2584    648     svchost.exe     0xb605acd20300  3       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2656    648     svchost.exe     0xb605acd74300  7       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2664    648     svchost.exe     0xb605accbf0c0  9       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2672    648     svchost.exe     0xb605acd75080  15      -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2692    648     svchost.exe     0xb605acdd4240  12      -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2772    648     svchost.exe     0xb605ace07240  4       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2796    648     svchost.exe     0xb605ace092c0  1       -       0       False   2024-03-22 18:05:42.000000 UTC  N/A     Disabled
2828    648     svchost.exe     0xb605ace06080  3       -       0       False   2024-03-22 18:05:43.000000 UTC  N/A     Disabled
2836    648     wlms.exe        0xb605ace0e080  2       -       0       False   2024-03-22 18:05:43.000000 UTC  N/A     Disabled
```

psscan.txt

```
Volatility 3 Framework 2.26.2

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64
CreateTime      ExitTime        File output

1708    648     svchost.exe     0xb605a567b080  3       -       0       False   2024-03-22
18:05:41.000000 UTC     N/A     Disabled
1728    648     svchost.exe     0xb605a567c080  3       -       0       False   2024-03-22
18:05:41.000000 UTC     N/A     Disabled
1836    4       MemCompression  0xb605a5680040  54      -       N/A     False   2024-03-22
18:05:41.000000 UTC     N/A     Disabled
4       0       System  0xb605a5681080  128     -       N/A     False   2024-03-22
18:05:28.000000 UTC     N/A     Disabled
92      4       Registry        0xb605a57c6040  4       -       N/A     False   2024-03-22
18:05:13.000000 UTC     N/A     Disabled
348     4       smss.exe        0xb605a60d4040  2       -       N/A     False   2024-03-22
18:05:28.000000 UTC     N/A     Disabled
4580    960     msedge.exe      0xb605a6c890c0  46      -       1       False   2024-03-22
18:30:08.000000 UTC     N/A     Disabled
960     7164    msedge.exe      0xb605a6d510c0  0       -       1       False   2024-03-22
18:28:35.000000 UTC     2024-03-22 18:30:09.000000 UTC  Disabled
7376    1152    mavinject.exe   0xb605a6d5e080  0       -       1       False   2024-03-22
18:48:10.000000 UTC     2024-03-22 18:48:53.000000 UTC  Disabled
5548    772     RuntimeBroker.  0xb605a6de9080  3       -       1       False   2024-03-22
18:39:14.000000 UTC     N/A     Disabled
8112    4580    msedge.exe      0xb605a6eca0c0  7       -       1       False   2024-03-22
18:30:08.000000 UTC     N/A     Disabled
4364    4156    powershell.exe  0xb605ab43a080  13      -       1       False   2024-03-22
18:46:29.000000 UTC     N/A     Disabled
8108    648     svchost.exe     0xb605ab4df0c0  3       -       0       False   2024-03-22
```

Getsids.txt

```
Volatility 3 Framework 2.26.2

PID     Process SID     Name

4       System  S-1-5-18        Local System
4       System  S-1-5-32-544    Administrators
4       System  S-1-1-0 Everyone
4       System  S-1-5-11        Authenticated Users
4       System  S-1-16-16384    System Mandatory Level
92      Registry        S-1-5-18        Local System
92      Registry        S-1-5-32-544    Administrators
92      Registry        S-1-1-0 Everyone
92      Registry        S-1-5-11        Authenticated Users
92      Registry        S-1-16-16384    System Mandatory Level
348     smss.exe        S-1-5-18        Local System
348     smss.exe        S-1-5-32-544    Administrators
348     smss.exe        S-1-1-0 Everyone
348     smss.exe        S-1-5-11        Authenticated Users
348     smss.exe        S-1-16-16384    System Mandatory Level
440     csrss.exe       S-1-5-18        Local System
440     csrss.exe       S-1-5-32-544    Administrators
440     csrss.exe       S-1-1-0 Everyone
440     csrss.exe       S-1-5-11        Authenticated Users
440     csrss.exe       S-1-16-16384    System Mandatory Level
516     wininit.exe     S-1-5-18        Local System
516     wininit.exe     S-1-5-32-544    Administrators
516     wininit.exe     S-1-1-0 Everyone
516     wininit.exe     S-1-5-11        Authenticated Users
516     wininit.exe     S-1-16-16384    System Mandatory Level
528     csrss.exe       S-1-5-18        Local System
```

Malfind.txt

```
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

2848    MsMpEng.exe     0x16197e60000   0x16197e60fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x16198090000   0x16198090fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x16198080000   0x16198080fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x161980b0000   0x161980b2fff   VadS    PAGE_EXECUTE_READWRITE  3       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x161980a0000   0x161980a1fff   VadS    PAGE_EXECUTE_READWRITE  2       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x1619d860000   0x1619d860fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x1619d870000   0x1619d871fff   VadS    PAGE_EXECUTE_READWRITE  2       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x1619d880000   0x1619d880fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc ..H.e.].........
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ................        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
2848    MsMpEng.exe     0x1619e6a0000   0x1619e7acfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled        N/A
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(
4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H...8....
49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A\][_^
c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 50 51 ...@.....H..H.PQ        56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e
41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 50 51
2848    MsMpEng.exe     0x1619f480000   0x1619f58cfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled        N/A
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(
```

Netscan.txt

```
Volatility 3 Framework 2.26.2

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x888000159650  UDPv4   0.0.0.0 0       *       0               1640    VBoxService.ex  2024-03-22 18:51:26.000000 UTC
0xb605a5690730  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2328    spoolsv.exe     2024-03-22 18:05:42.000000 UTC
0xb605a5690890  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2024-03-22 18:05:43.000000 UTC
0xb605a5690890  TCPv6   ::      445     ::      0       LISTENING       4       System  2024-03-22 18:05:43.000000 UTC
0xb605a56909f0  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       2584    svchost.exe     2024-03-22 18:05:45.000000 UTC
0xb605a5690e10  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2328    spoolsv.exe     2024-03-22 18:05:42.000000 UTC
0xb605a5690e10  TCPv6   ::      49668   ::      0       LISTENING       2328    spoolsv.exe     2024-03-22 18:05:42.000000 UTC
0xb605a5dbe6d0  UDPv4   0.0.0.0 55857   *       0               7620    SkypeApp.exe    2024-03-22 18:08:03.000000 UTC
0xb605a5dbe6d0  UDPv6   ::      55857   *       0               7620    SkypeApp.exe    2024-03-22 18:08:03.000000 UTC
0xb605a67cd310  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1196    svchost.exe     2024-03-22 18:05:41.000000 UTC
0xb605a67cd310  TCPv6   ::      49666   ::      0       LISTENING       1196    svchost.exe     2024-03-22 18:05:41.000000 UTC
0xb605a67cd470  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       656     lsass.exe       2024-03-22 18:05:40.000000 UTC
0xb605a67cd470  TCPv6   ::      49664   ::      0       LISTENING       656     lsass.exe       2024-03-22 18:05:40.000000 UTC
0xb605a67cd5d0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1188    svchost.exe     2024-03-22 18:05:41.000000 UTC
0xb605a67cd5d0  TCPv6   ::      49667   ::      0       LISTENING       1188    svchost.exe     2024-03-22 18:05:41.000000 UTC
0xb605a67cd890  TCPv4   10.0.2.15       139     0.0.0.0 0       LISTENING       4       System  2024-03-22 18:05:41.000000 UTC
0xb605a67cd9f0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     2024-03-22 18:05:40.000000 UTC
0xb605a67cde10  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1196    svchost.exe     2024-03-22 18:05:41.000000 UTC
0xb605a67ce4f0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       656     lsass.exe       2024-03-22 18:05:40.000000 UTC
0xb605a67ce7b0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1188    svchost.exe     2024-03-22 18:05:41.000000 UTC
0xb605a67cea70  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       516     wininit.exe     2024-03-22 18:05:40.000000 UTC
0xb605a67cebd0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     2024-03-22 18:05:40.000000 UTC
0xb605a67cebd0  TCPv6   ::      135     ::      0       LISTENING       884     svchost.exe     2024-03-22 18:05:40.000000 UTC
0xb605a67cee90  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       516     wininit.exe     2024-03-22 18:05:40.000000 UTC
0xb605a67cee90  TCPv6   ::      49665   ::      0       LISTENING       516     wininit.exe     2024-03-22 18:05:40.000000 UTC
0xb605a6bfda70  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       2584    svchost.exe     2024-03-22 18:05:45.000000 UTC
0xb605a6bfda70  TCPv6   ::      49670   ::      0       LISTENING       2584    svchost.exe     2024-03-22 18:05:45.000000 UTC
0xb605a6fde700  TCPv4   10.0.2.15       50127   2.23.92.198     443     CLOSE_WAIT      4016    SearchApp.exe   2024-03-22 18:47:49.000000 UTC
0xb605ab2cdb40  TCPv4   10.0.2.15       50068   13.107.4.254    443     CLOSED  5644    SearchApp.exe   2024-03-22 18:34:52.000000 UTC
0xb605ab3a34e0  TCPv4   10.0.2.15       50064   52.168.117.169  443     CLOSED  5644    SearchApp.exe   2024-03-22 18:34:40.000000 UTC
0xb605ab40c010  TCPv4   10.0.2.15       50097   23.37.0.153     443     CLOSED  4016    SearchApp.exe   2024-03-22 18:44:43.000000 UTC
0xb605ab55ed30  UDPv6   fe80::a98c:9634:6d6e:dcba       59975   *       0               1920    svchost.exe     2024-03-22 18:14:52.000000 UTC
0xb605ab55f500  UDPv4   10.0.2.15       59977   *       0               1920    svchost.exe     2024-03-22 18:14:52.000000 UTC
0xb605ab560950  UDPv4   127.0.0.1       59978   *       0               1920    svchost.exe     2024-03-22 18:14:52.000000 UTC
0xb605ab5623e0  UDPv6   ::1     59976   *       0               1920    svchost.exe     2024-03-22 18:14:52.000000 UTC
0xb605abfe0010  TCPv4   10.0.2.15       50122   23.48.165.34    443     CLOSE_WAIT      4016    SearchApp.exe   2024-03-22 18:47:47.000000 UTC
0xb605ac8ce010  TCPv4   10.0.2.15       50044   68.219.88.97    443     CLOSED  764     msedge.exe      2024-03-22 18:30:11.000000 UTC
0xb605ac921190  UDPv4   10.0.2.15       138     *       0               4       System  2024-03-22 18:05:41.000000 UTC
0xb605ac921320  UDPv4   10.0.2.15       137     *       0               4       System  2024-03-22 18:05:41.000000 UTC
0xb605acaefc60  UDPv4   0.0.0.0 0       *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaefc60  UDPv6   ::      0       *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaf2e60  UDPv4   0.0.0.0 5353    *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaf3c70  UDPv4   0.0.0.0 5353    *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaf3c70  UDPv6   ::      5353    *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaf3e00  UDPv4   0.0.0.0 5355    *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaf4440  UDPv4   0.0.0.0 5355    *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acaf4440  UDPv6   ::      5355    *       0               2056    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acb2b420  TCPv4   10.0.2.15       50045   13.107.21.200   443     CLOSED  764     msedge.exe      2024-03-22 18:30:11.000000 UTC
0xb605acc3a490  UDPv4   0.0.0.0 500     *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3a490  UDPv6   ::      500     *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3a620  UDPv4   0.0.0.0 500     *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3a940  UDPv4   0.0.0.0 0       *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3a940  UDPv6   ::      0       *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3c560  UDPv4   0.0.0.0 4500    *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3c6f0  UDPv4   0.0.0.0 4500    *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3c6f0  UDPv6   ::      4500    *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc3c880  UDPv4   0.0.0.0 0       *       0               2568    svchost.exe     2024-03-22 18:05:42.000000 UTC
0xb605acc7c1b0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       648     services.exe    2024-03-22 18:05:43.000000 UTC
```

Component 3

Executive Summary and Reflection

This investigation focused on analysing a suspected internal security breach within a corporate virtual machine environment. The forensic examination was conducted using two primary sources of digital evidence:

• win10_Portfolio3-disk.vhd – a virtual hard disk image
• win10-Portfolio3-memory.raw – a memory dump from the same virtual machine

Both artifacts were suspected of containing traces of malicious activity and potential data tampering or exfiltration. The objective was to determine whether sensitive corporate data had been accessed, modified, or extracted, and to identify any insider threats or unauthorized execution of software.

Scope of Analysis and Integrity Validation

Image Validation

Forensic image hash values were verified against provided baselines using Autopsy and manual hashing tools.

No evidence of image tampering or corruption was detected.

Memory Dump Examination

Used Volatility plugins (malfind, pslist, netscan, getsids) to extract execution traces and detect anomalous activity.

Verified with timestamp correlation to support findings from the disk image.

Analytical Methodology

• Disk Image Analysis: Conducted using Autopsy, with a focus on registry hives (SYSTEM, SAM, NTUSER.DAT), Prefetch files, and startup folder configurations to uncover user behaviour and persistence mechanisms.
• Memory Forensics: Performed using Volatility, targeting in-memory code injection,

process anomalies, and unauthorized outbound network connections suggestive of Command & Control (C2) activity.

Key Findings

• Executables such as AtomicService.exe, T1055.exe, and T1036.003.exe were discovered. These correlate with adversarial behaviours catalogued in the MITRE ATT&CK framework and suggest either a red team simulation or a real attack.

• Prefetch and BAM records confirmed that these executables were launched on March 22, 2024, strongly indicating the date of the incident.

• The student account configured AtomicService.exe to auto-run at login using Windows Run keys, a known persistence mechanism.

• Both student and art-test accounts were members of the Administrators group, which introduces the risk of privilege misuse.

Analyst Observation – Possible Network Surveillance

While examining the memory image (win10-Portfolio3-memory.raw), I noted multiple executions of AtomicService.exe. Research indicated it is part of the Atomic Red Team framework, typically used for adversary simulation. However, in this case, its execution pattern and context suggested possible misuse.

Based on Volatility's netscan output, I identified several outbound HTTPS connections, some in CLOSE_WAIT and ESTABLISHED states, a hallmark of ongoing C2 communication or external probing. This led to the hypothesis that the attacker may have been scanning for vulnerabilities or probing other IP ranges or networks.

Further analysis showed the use of mavinject.exe, a known code injection tool, reinforcing the presence of advanced techniques such as remote thread injection or process hollowing.

Reflection and Learning Experience

Working as a forensic cyber analyst on this case provided me with deep, practical insight into real-world digital forensics. While Autopsy served as the primary analysis tool, I quickly realized the need for specialized utilities to uncover deeper layers of evidence.

• I supplemented my analysis by using Eric Zimmerman's PECmd and Registry Timeline tools, which allowed a more detailed reconstruction of registry-based persistence.
• One of the most valuable outcomes was gaining hands-on experience with Volatility, which enabled me to detect malicious scripts and code injections—elements that Autopsy alone could not reveal.
• I learned about Prefetch files and their forensic importance in tracking program executions, which became crucial in validating user behaviour and timeline correlation.

A notable challenge was confirming whether the AdFind tool had been executed. Initially uncertain, I analysed Prefetch and PowerShell scripts and concluded that although the tool was downloaded via GitHub, it had not been executed.

Another key learning area was timeline construction. While I successfully used Prefetch and BAM data to build an activity timeline, I struggled with clarity and interpretation at times. In future work, I would consider using more advanced timeline visualization tools.

What I Would Do Differently

If I were to conduct this investigation again, I would use a tool like FTK Imager to verify the integrity of the forensic images instead of relying on terminal-based hashing. While the terminal worked, FTK Imager offers a more user-friendly interface and better documentation features. The only limitation was the large size of the evidence files, which made using heavier tools more challenging—but in a professional setting, FTK Imager would be more efficient and appropriate for handling and validating such data.

References

Atomicredteam.io. (2024). Available at: https://www.atomicredteam.io/.

attack.mitre.org. (n.d.). *AdFind, Software S0552 | MITRE ATT&CK®*. [online] Available at: https://attack.mitre.org/software/S0552/.

attack.mitre.org. (n.d.). *Masquerading: Rename System Utilities, Sub-technique T1036.003 - Enterprise | MITRE ATT&CK®*. [online] Available at: https://attack.mitre.org/techniques/T1036/003/.

attack.mitre.org. (n.d.). *Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®*. [online] Available at: https://attack.mitre.org/techniques/T1055/.

Forensafe.com. (2022). *Timezone Information Blog*. [online] Available at: https://forensafe.com/blogs/timezoneinformation.html.

Forensics, A. (2020). *The Device and The Volume Serial Number*. [online] Athena Forensics. Available at: https://athenaforensics.co.uk/device-serial-number-and-volume-serial-number-forensics/ [Accessed 9 May 2025].

GeeksforGeeks (2024). *Dynamic Host Configuration Protocol (DHCP) - GeeksforGeeks*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/.

GitHub. (2022). *Atomic Red Team*. [online] Available at: https://github.com/redcanaryco/atomic-red-team.

Infralin.com. (2025). *Convert Windows file time*. [online] Available at: https://www.infralin.com/convertwindowsfiletime.html [Accessed 9 May 2025].

Rapidtables.com. (2025). *Hex to Decimal Converter*. [online] Available at: https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=01DA7C8D79348BC2 [Accessed 9 May 2025].

Zimmerman, E. (n.d.). *Eric Zimmerman's tools*. [online] ericzimmerman.github.io. Available at: https://ericzimmerman.github.io/#.