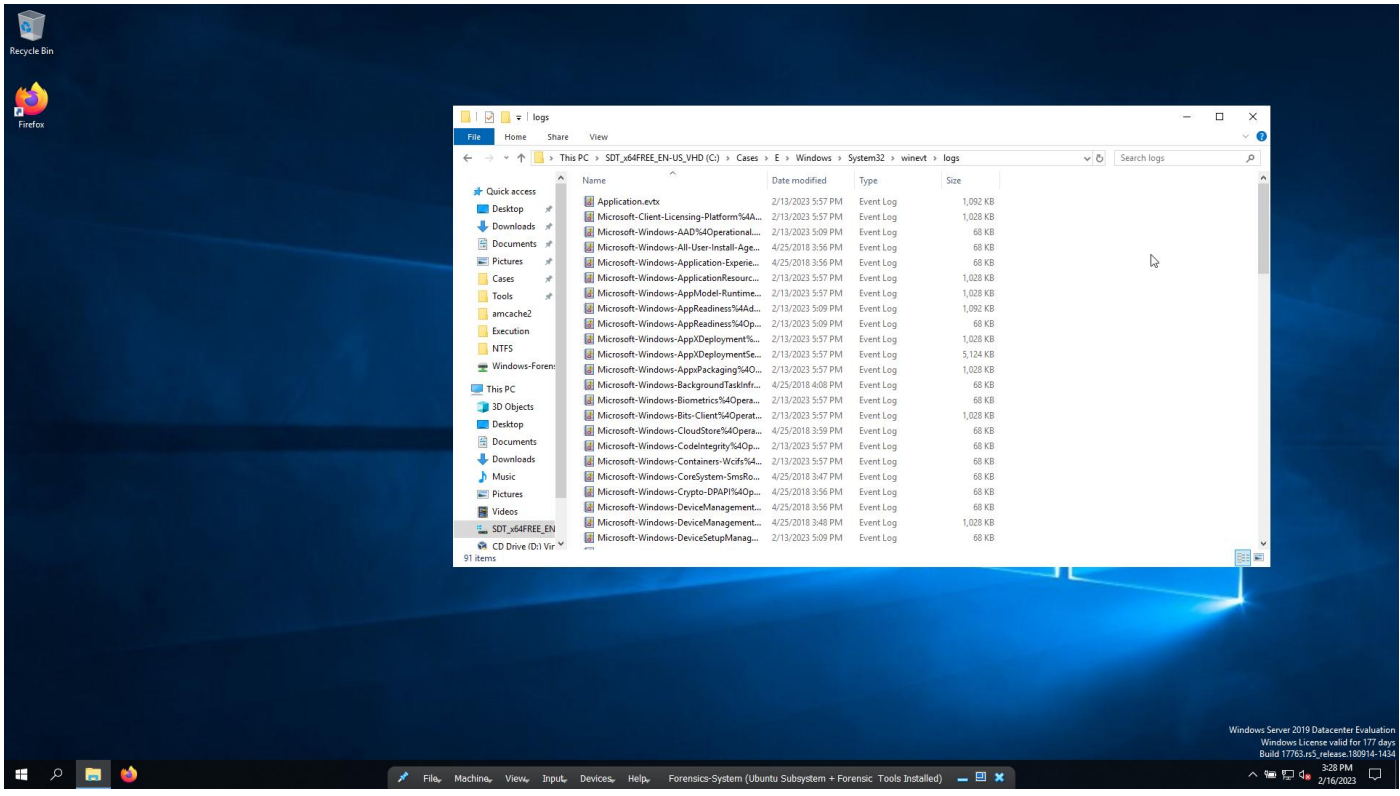
Evidence of malicious activity:

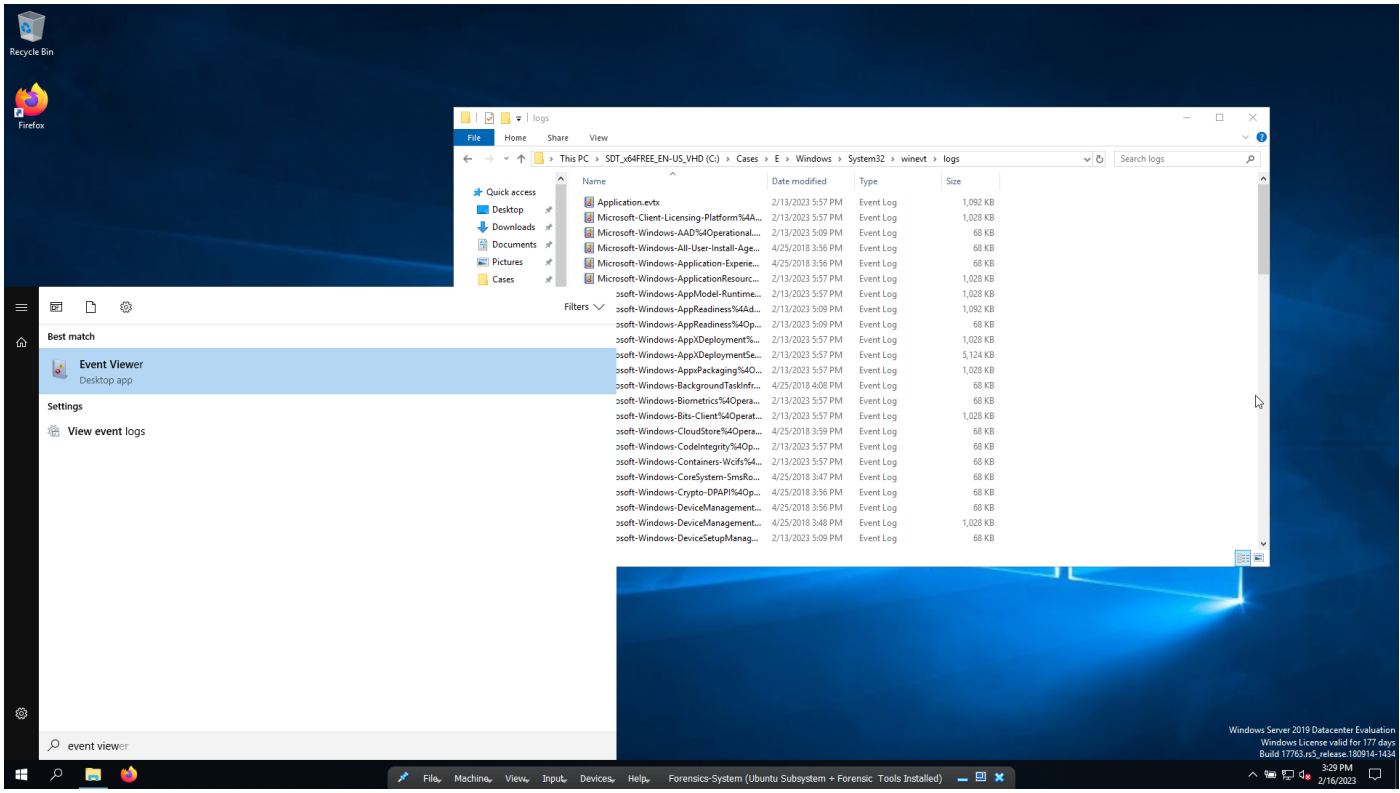
- Event Logs
- EventLogExplorer & EvtxECmd
- Windows Defender
- Service installs
- Security event log
- Authentication
- Powershell
- Malicious Powershell
- Sysmon & Malicious Sysmon

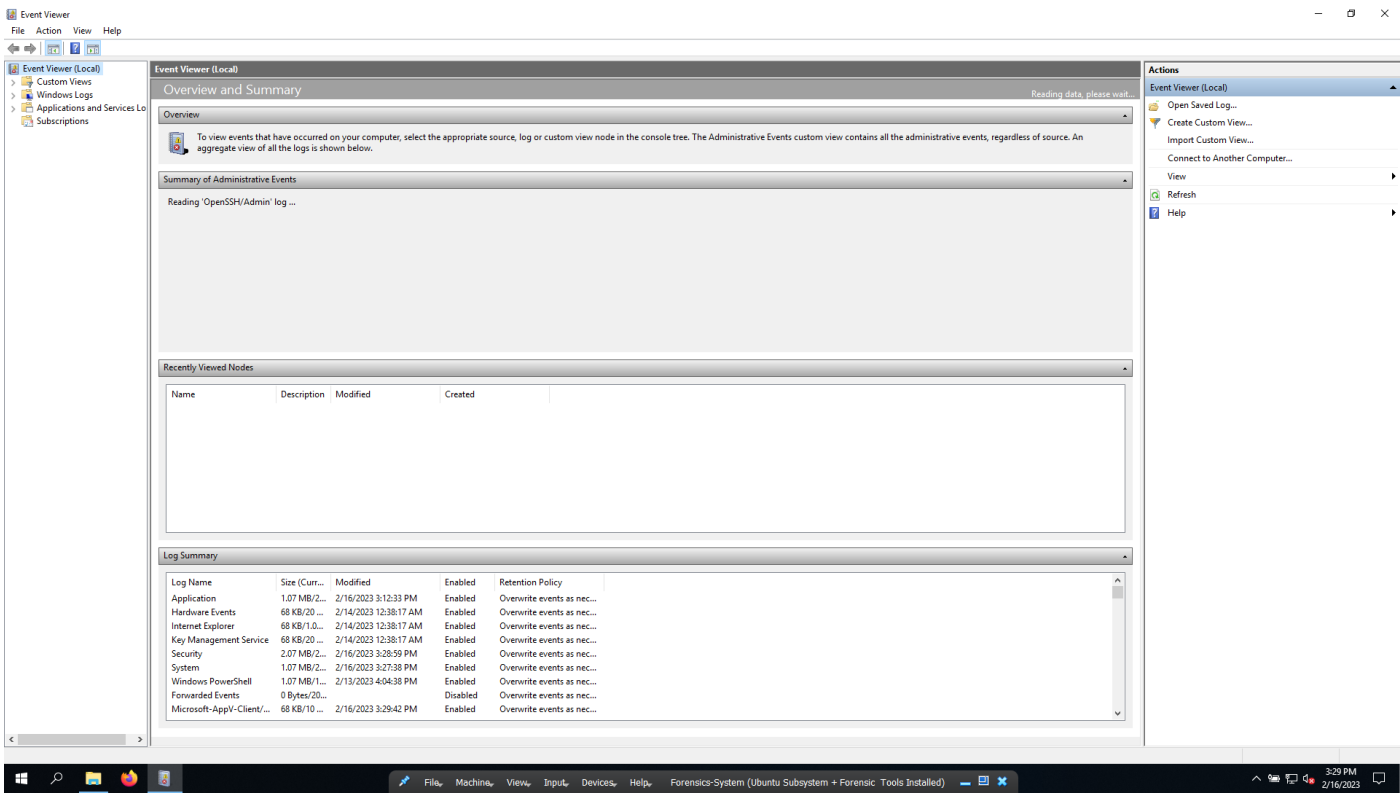
Event Logs

- Location logs artifacts:
    - C:\Windows\System32\winevt\logs



- You can use the event log viewer that comes with windows:



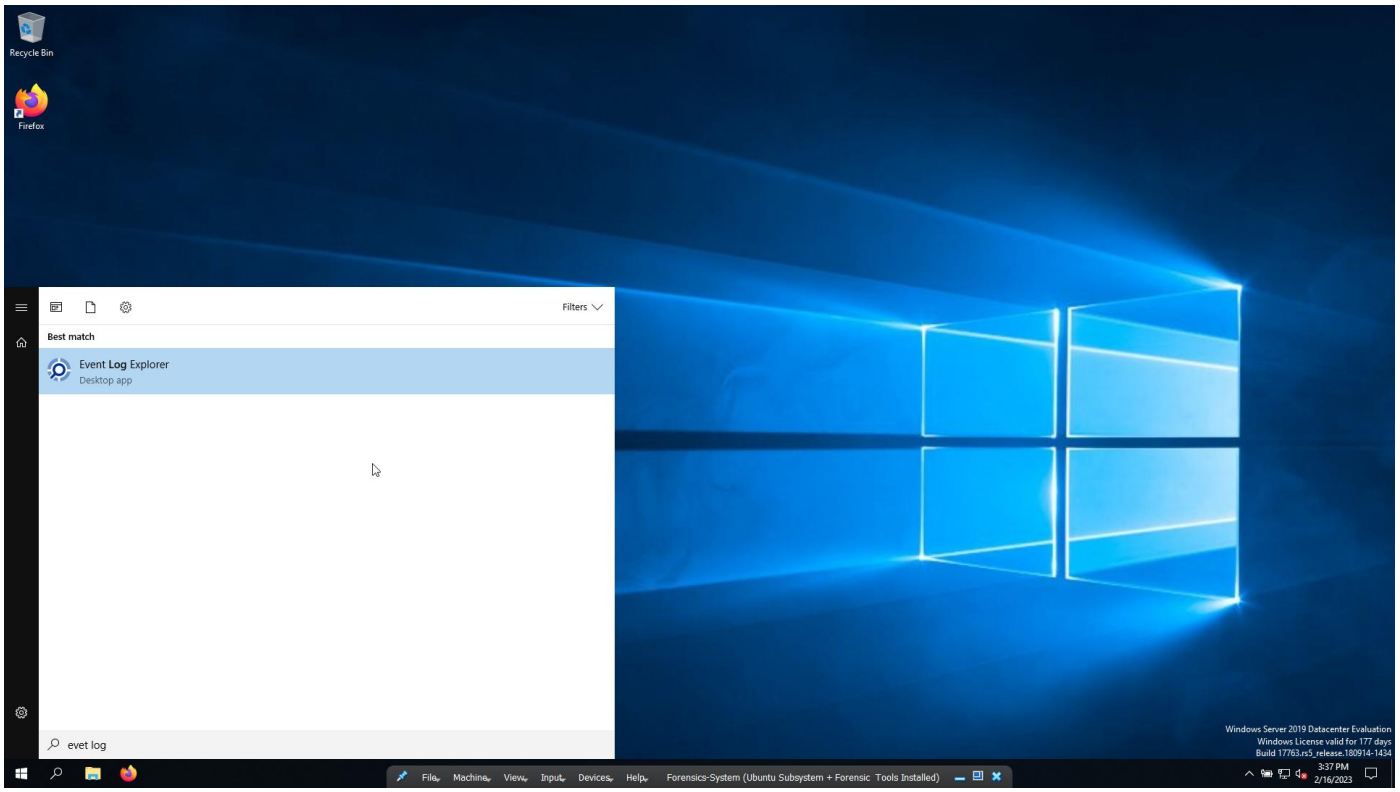


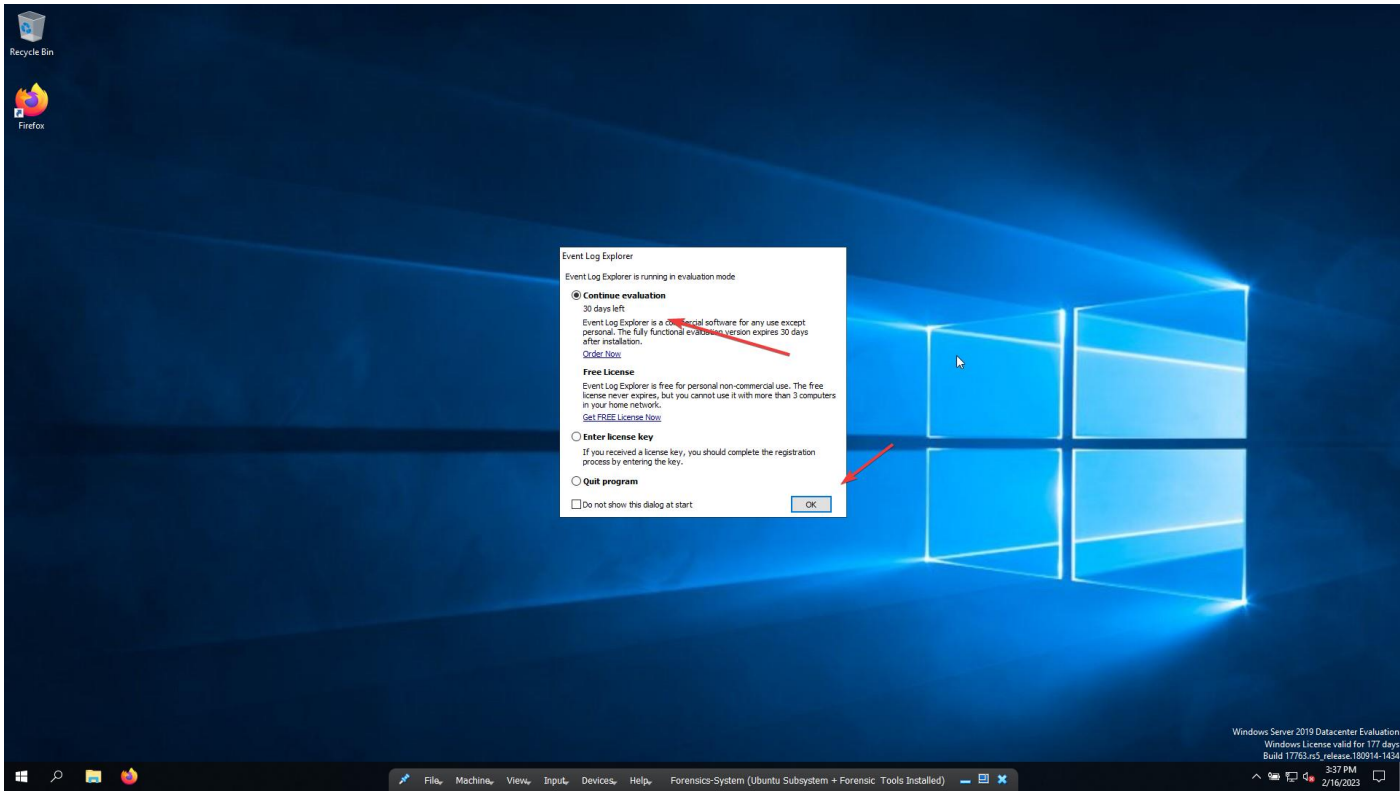
- Important logs are:
  - Application – information about application in the operating system, service stopped, started, etc

    - Security – information about users, loggin of users, when, how it logged
- You can start investigation event logs based on particular:
    - Timestamps
    - Applications
    - Users : Event ID example is 4624.
- More information on Event IDs : https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

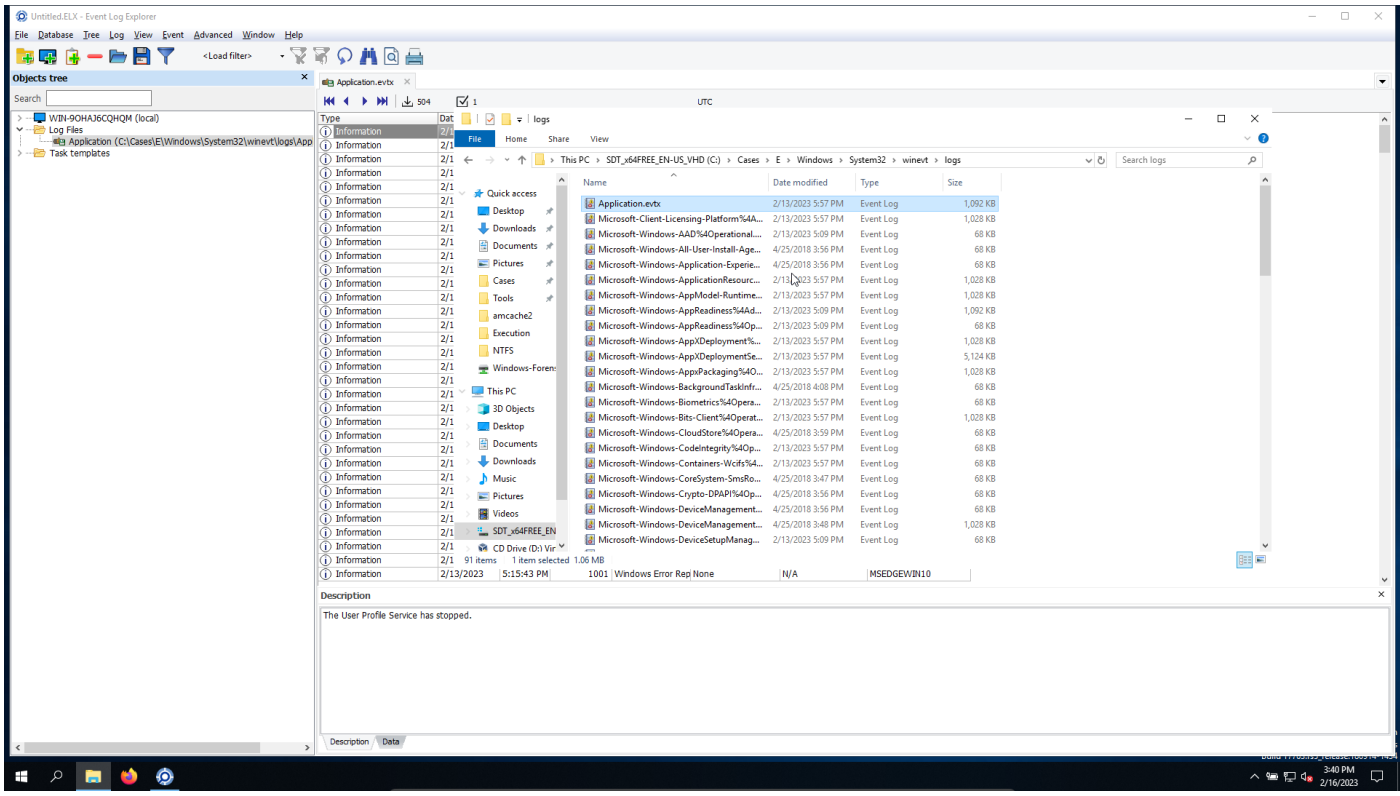
EventLogExplorer & EvtxECmd

- Tools used in forensic analysis of event logs:
    - Event Log Explorer

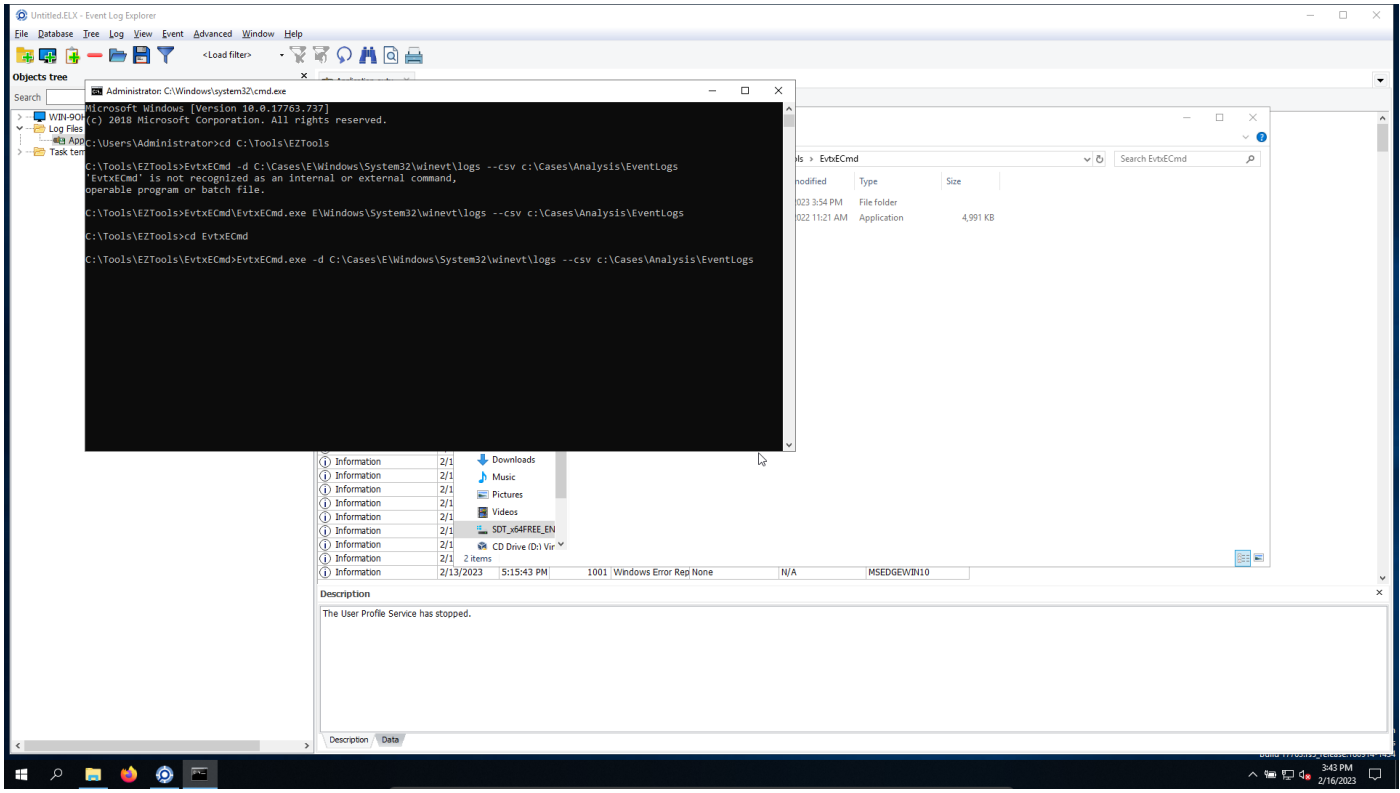


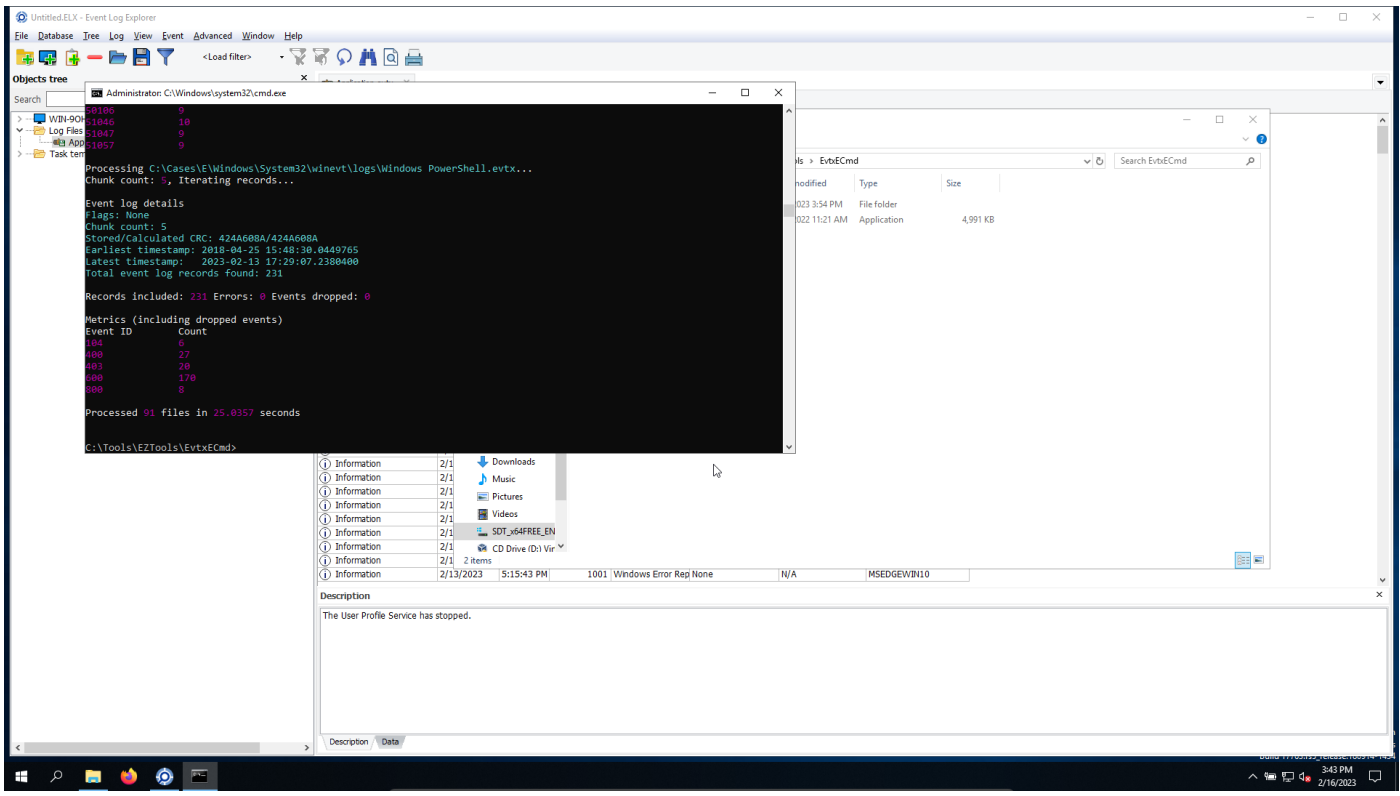


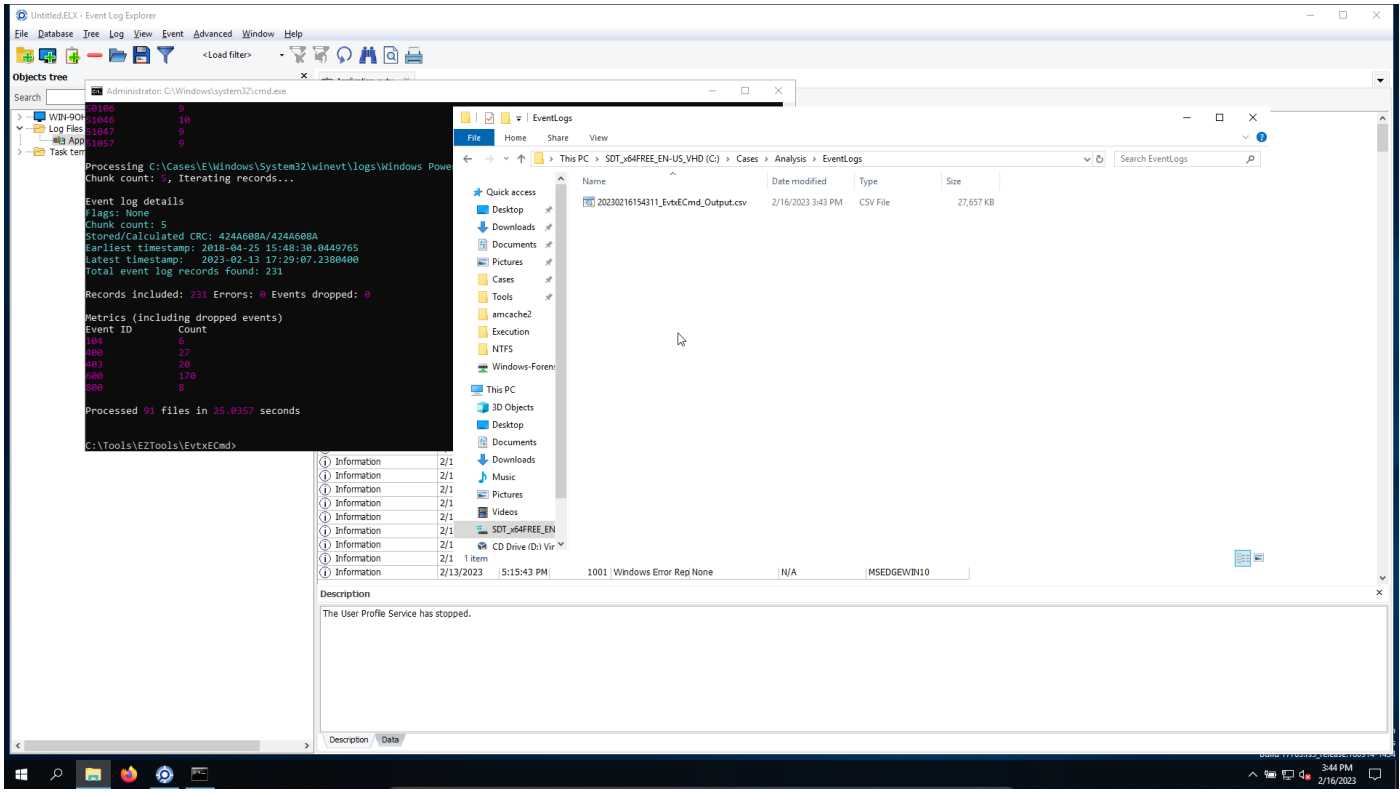
- Drag and drop the .evtx file.

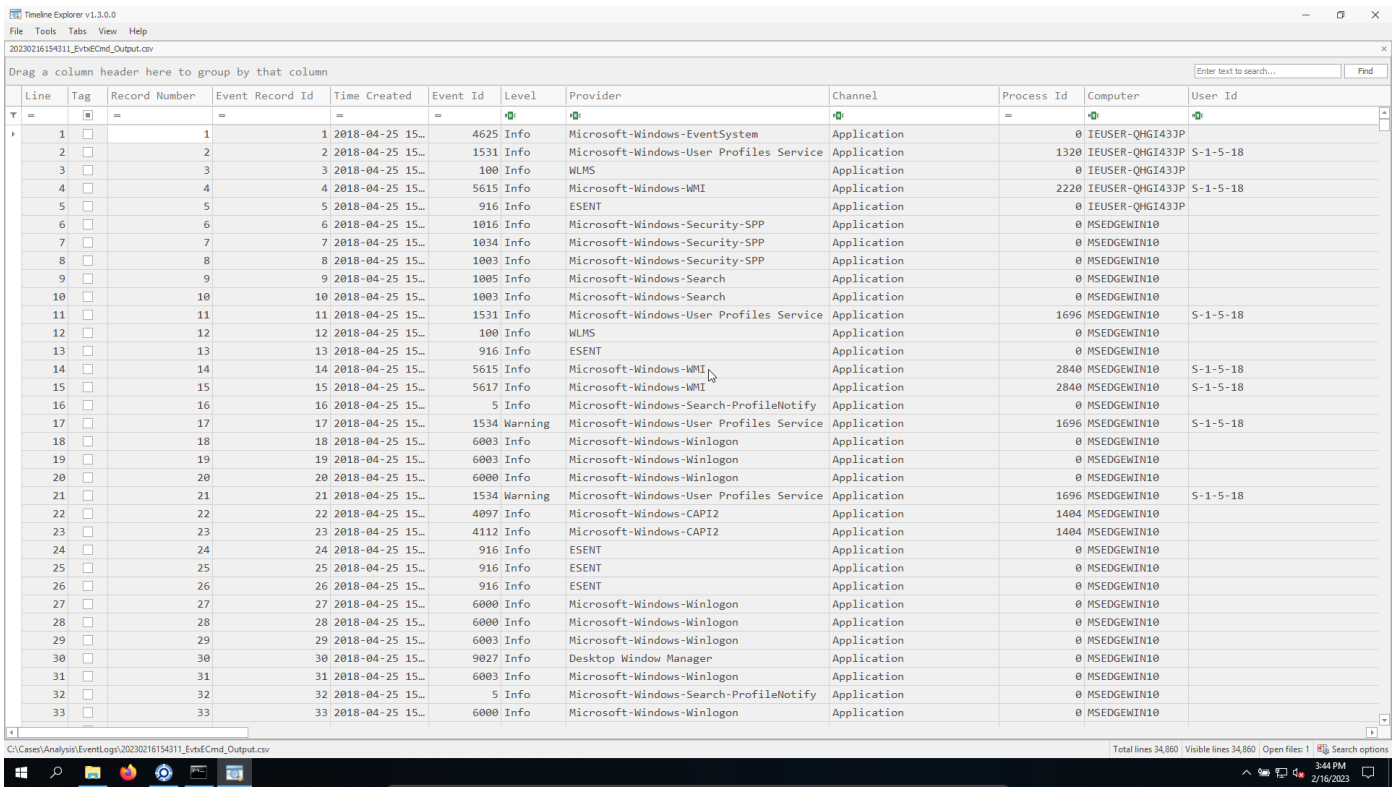


  - EvtxECmd


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\Tools\EZTools
C:\Tools\EZTools>EvtxECmd -d C:\Cases\E\Windows\System32\winevt\logs --csv c:\Cases\Analysis\EventLogs
'EvtxECmd' is not recognized as an internal or external command,
operable program or batch file.
C:\Tools\EZTools>EvtxECmd\EvtxECmd.exe E\Windows\System32\winevt\logs --csv c:\Cases\Analysis\EventLogs
C:\Tools\EZTools>cd EvtxECmd
C:\Tools\EZTools\EvtxECmd>EvtxECmd.exe -d C:\Cases\E\Windows\System32\winevt\logs --csv c:\Cases\Analysis\EventLogs
The User Profile Service has stopped.

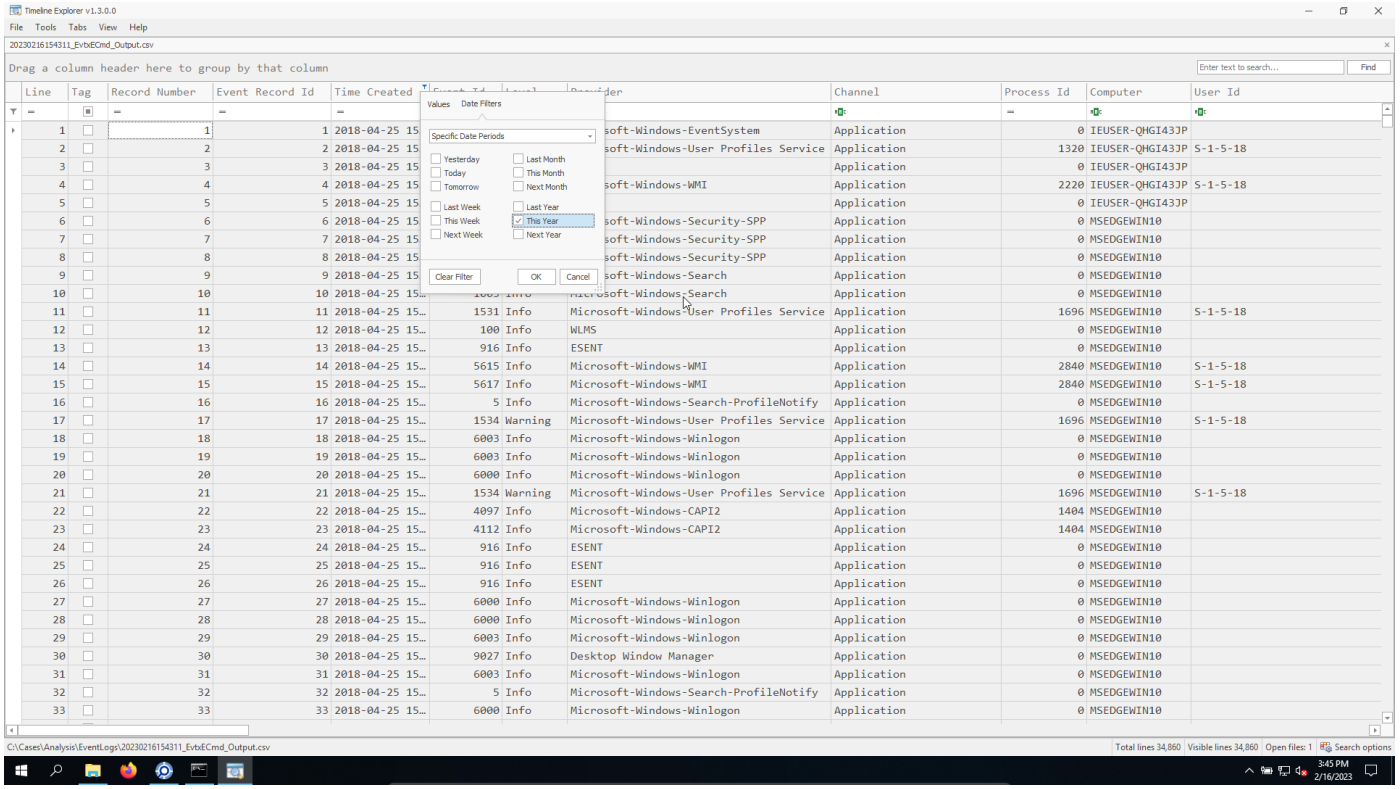

Administrator: C:\Windows\system32\cmd.exe
Processing C:\Cases\E\Windows\System32\winevt\logs\Windows PowerShell.evtx...
Chunk count: 5, Iterating records...
Event log details
Flags: None
Chunk count: 5
Stored/Calculated CRC: 424A608A/424A608A
Earliest timestamp: 2018-04-25 15:48:30.0449765
Latest timestamp: 2023-02-13 17:29:07.2380400
Total event log records found: 231
Records included: 231 Errors: 0 Events dropped: 0
Metrics (including dropped events)
Event ID Count
104 6
400 27
403 20
600 170
800 8
Processed 91 files in 25.0357 seconds
C:\Tools\EZTools\EvtxECmd>
The User Profile Service has stopped.

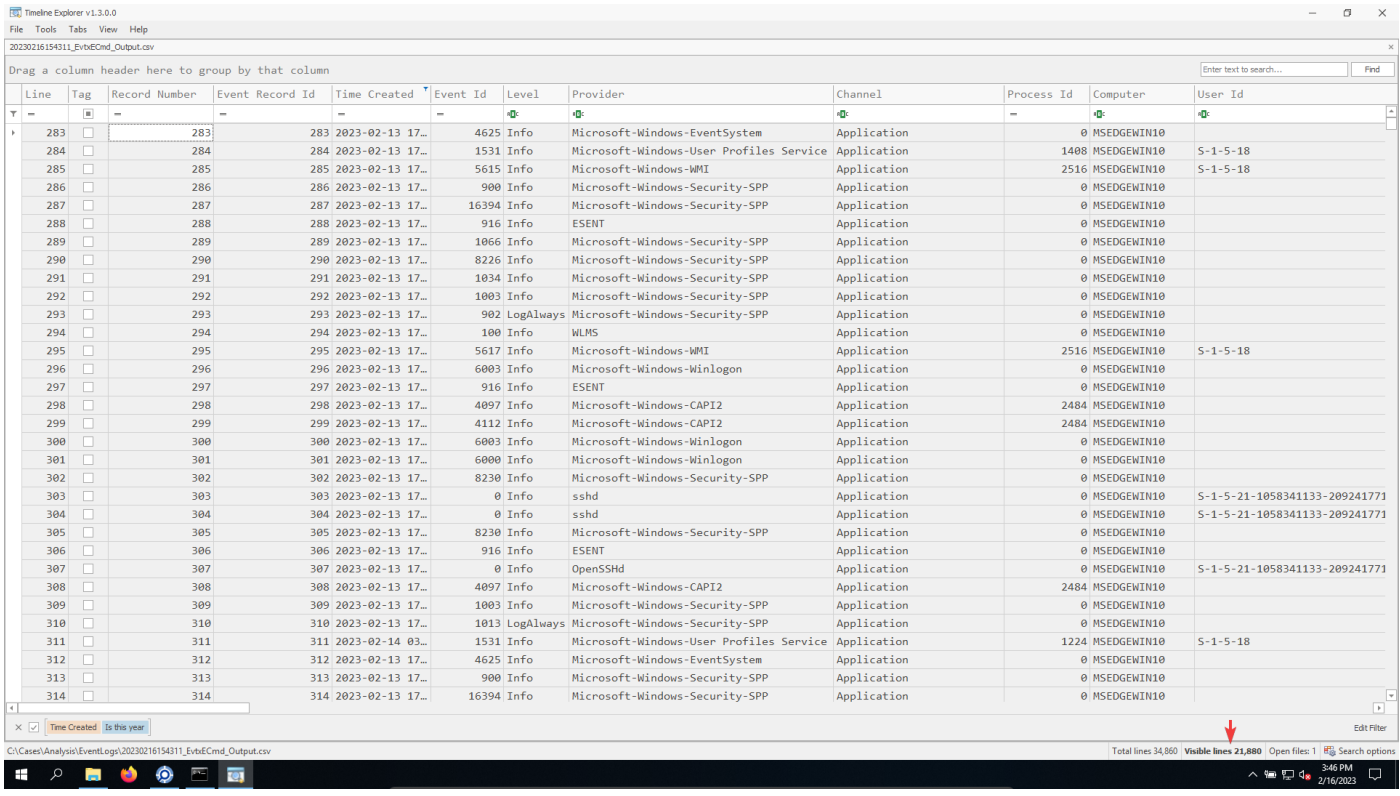




Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel	Process Id	Computer	User Id
1		1	1	2018-04-25 15...	4625	Info	Microsoft-Windows-EventSystem	Application	0	IEUSER-QHGI43JP	
2		2	2	2018-04-25 15...	1531	Info	Microsoft-Windows-User Profiles Service	Application	1320	IEUSER-QHGI43JP	S-1-5-18
3		3	3	2018-04-25 15...	100	Info	WLMS	Application	0	IEUSER-QHGI43JP	
4		4	4	2018-04-25 15...	5615	Info	Microsoft-Windows-WMI	Application	2220	IEUSER-QHGI43JP	S-1-5-18
5		5	5	2018-04-25 15...	916	Info	ESENT	Application	0	IEUSER-QHGI43JP	
6		6	6	2018-04-25 15...	1016	Info	Microsoft-Windows-Security-SPP	Application	0	MSEDGEWIN10	
7		7	7	2018-04-25 15...	1034	Info	Microsoft-Windows-Security-SPP	Application	0	MSEDGEWIN10	
8		8	8	2018-04-25 15...	1003	Info	Microsoft-Windows-Security-SPP	Application	0	MSEDGEWIN10	
9		9	9	2018-04-25 15...	1005	Info	Microsoft-Windows-Search	Application	0	MSEDGEWIN10	
10		10	10	2018-04-25 15...	1003	Info	Microsoft-Windows-Search	Application	0	MSEDGEWIN10	
11		11	11	2018-04-25 15...	1531	Info	Microsoft-Windows-User Profiles Service	Application	1696	MSEDGEWIN10	S-1-5-18
12		12	12	2018-04-25 15...	100	Info	WLMS	Application	0	MSEDGEWIN10	
13		13	13	2018-04-25 15...	916	Info	ESENT	Application	0	MSEDGEWIN10	
14		14	14	2018-04-25 15...	5615	Info	Microsoft-Windows-WMI	Application	2840	MSEDGEWIN10	S-1-5-18
15		15	15	2018-04-25 15...	5617	Info	Microsoft-Windows-WMI	Application	2840	MSEDGEWIN10	S-1-5-18
16		16	16	2018-04-25 15...	5	Info	Microsoft-Windows-Search-ProfileNotify	Application	0	MSEDGEWIN10	
17		17	17	2018-04-25 15...	1534	Warning	Microsoft-Windows-User Profiles Service	Application	1696	MSEDGEWIN10	S-1-5-18
18		18	18	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
19		19	19	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
20		20	20	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
21		21	21	2018-04-25 15...	1534	Warning	Microsoft-Windows-User Profiles Service	Application	1696	MSEDGEWIN10	S-1-5-18
22		22	22	2018-04-25 15...	4097	Info	Microsoft-Windows-CAPI2	Application	1404	MSEDGEWIN10	
23		23	23	2018-04-25 15...	4112	Info	Microsoft-Windows-CAPI2	Application	1404	MSEDGEWIN10	
24		24	24	2018-04-25 15...	916	Info	ESENT	Application	0	MSEDGEWIN10	
25		25	25	2018-04-25 15...	916	Info	ESENT	Application	0	MSEDGEWIN10	
26		26	26	2018-04-25 15...	916	Info	ESENT	Application	0	MSEDGEWIN10	
27		27	27	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
28		28	28	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
29		29	29	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
30		30	30	2018-04-25 15...	9027	Info	Desktop Window Manager	Application	0	MSEDGEWIN10	
31		31	31	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	
32		32	32	2018-04-25 15...	5	Info	Microsoft-Windows-Search-ProfileNotify	Application	0	MSEDGEWIN10	
33		33	33	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application	0	MSEDGEWIN10	

- Filter the data by Time Created this year.



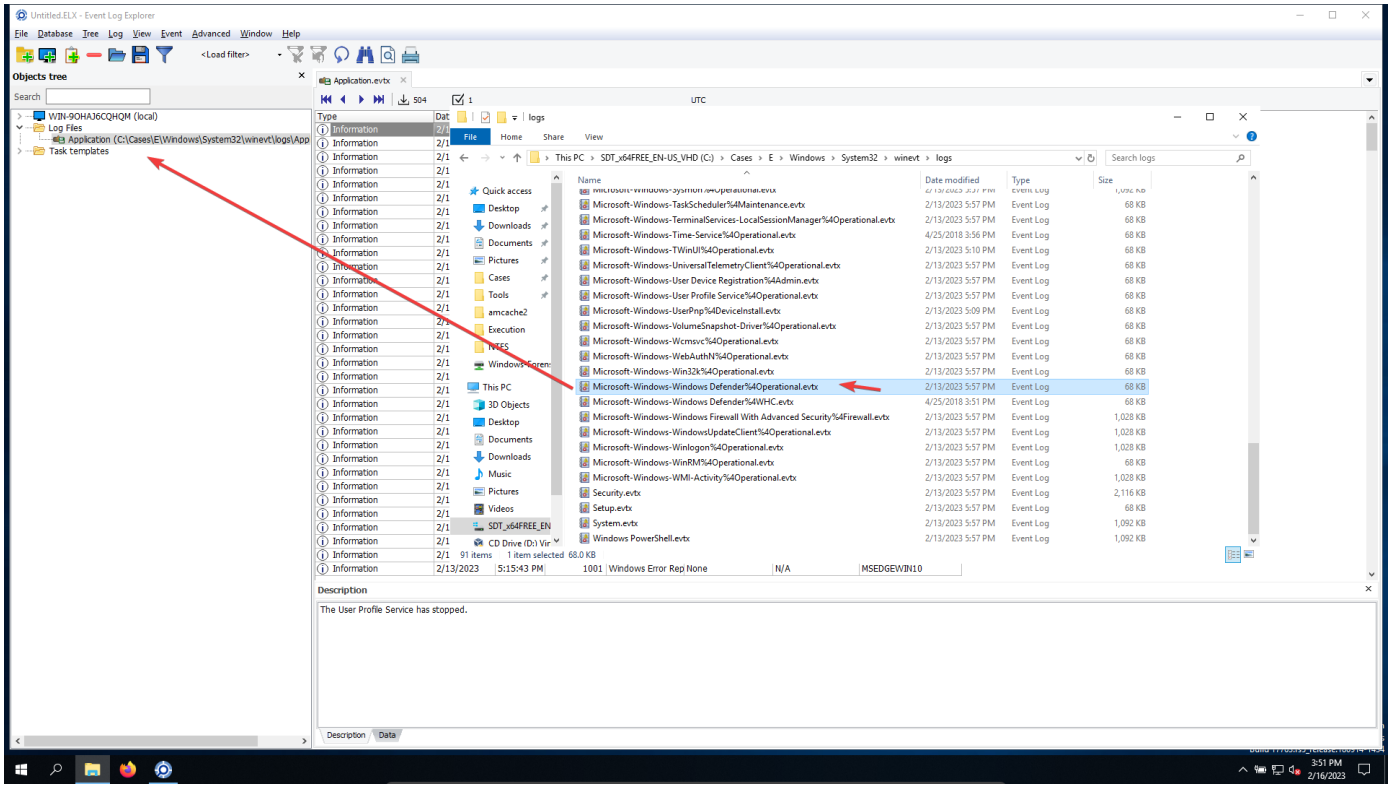


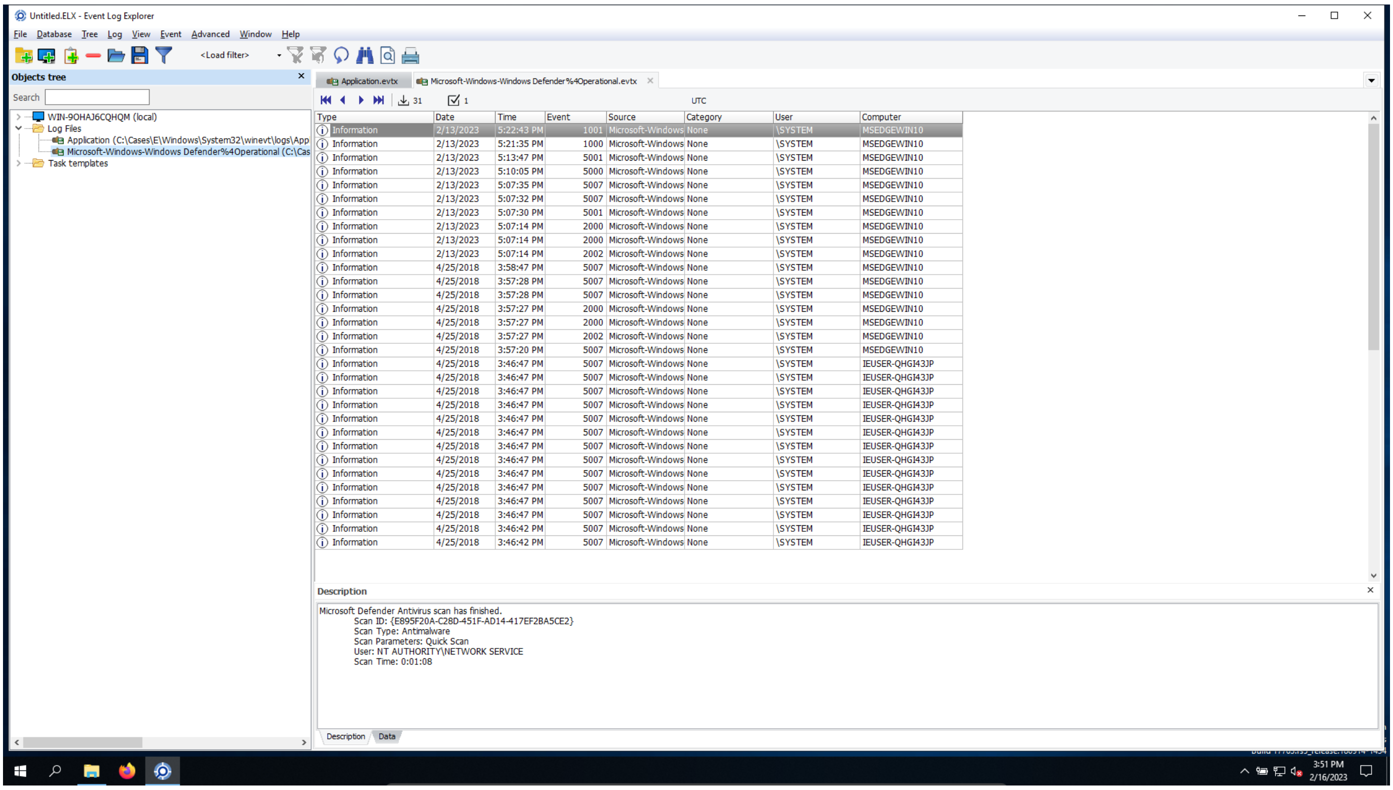
Windows Defender

- Event IDs for Microsoft-Windows-Windows Defender:

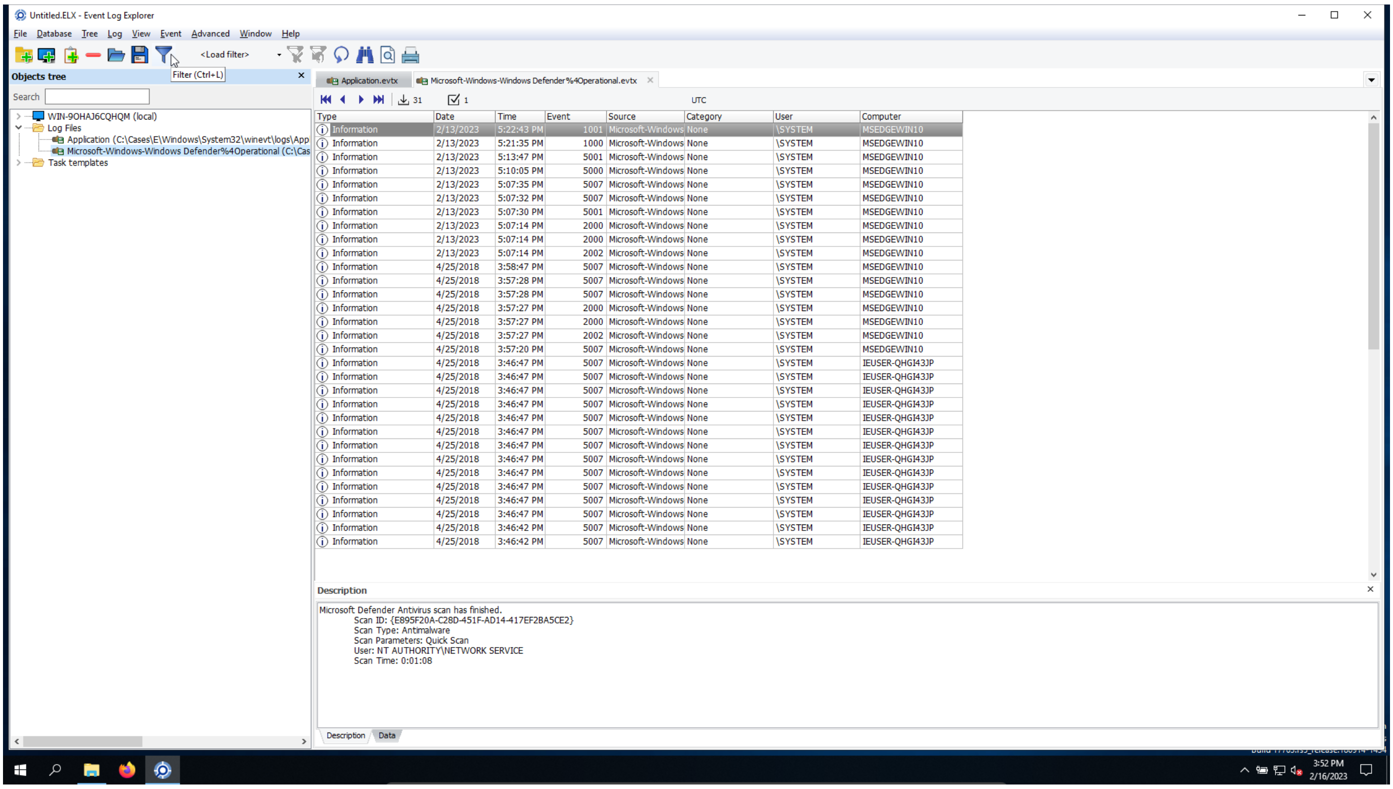
- 5000: Defender enabled
- 5001: Defender disabled

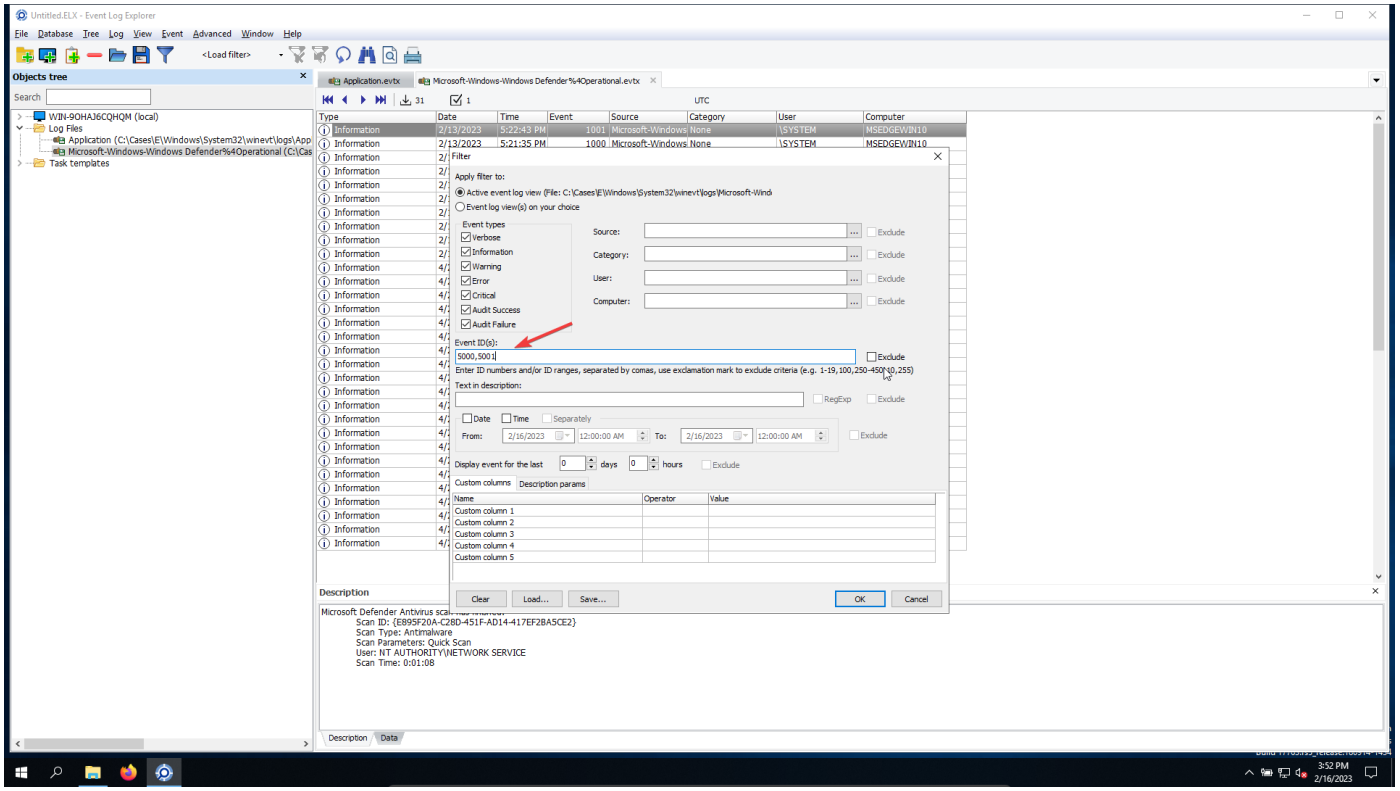
- Load Microsoft-Windows-Windows Defender Operational :

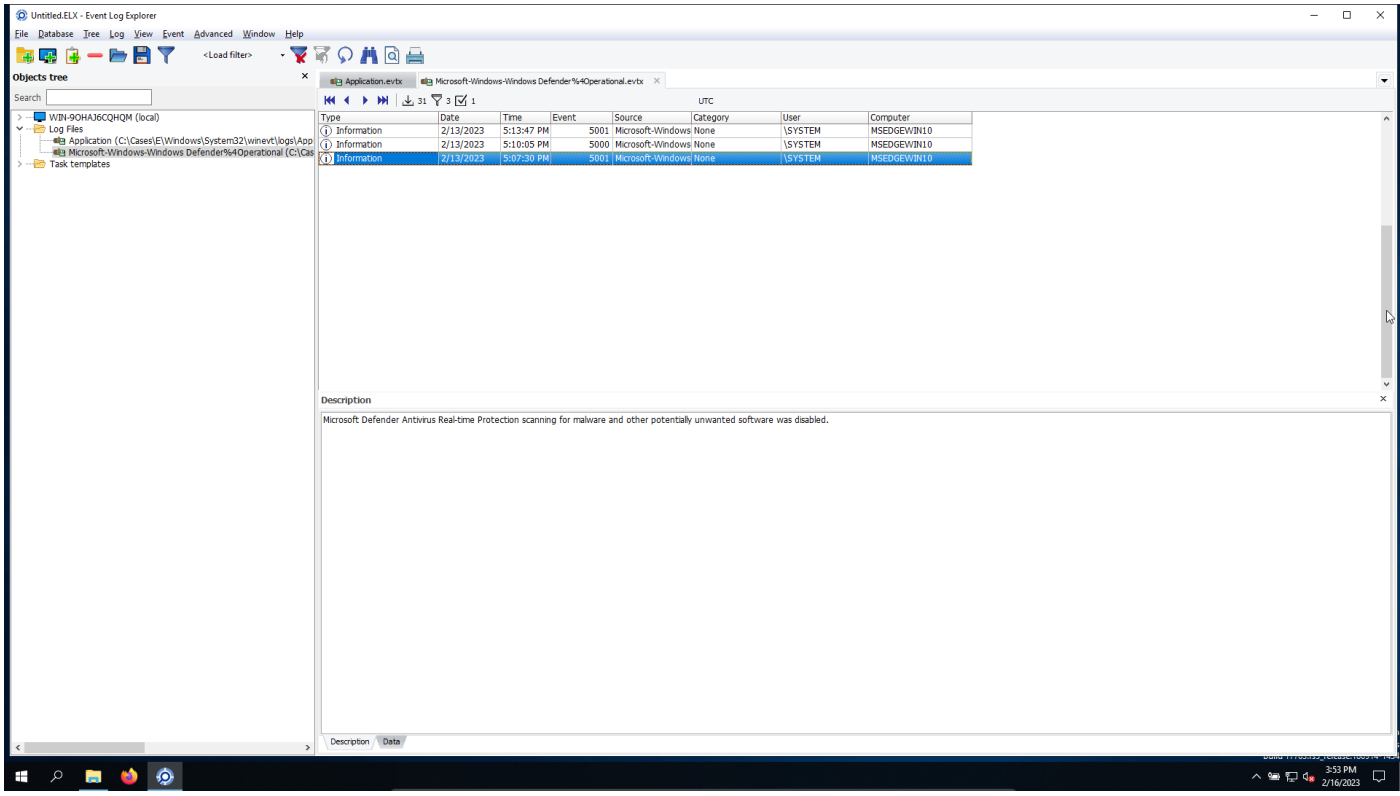


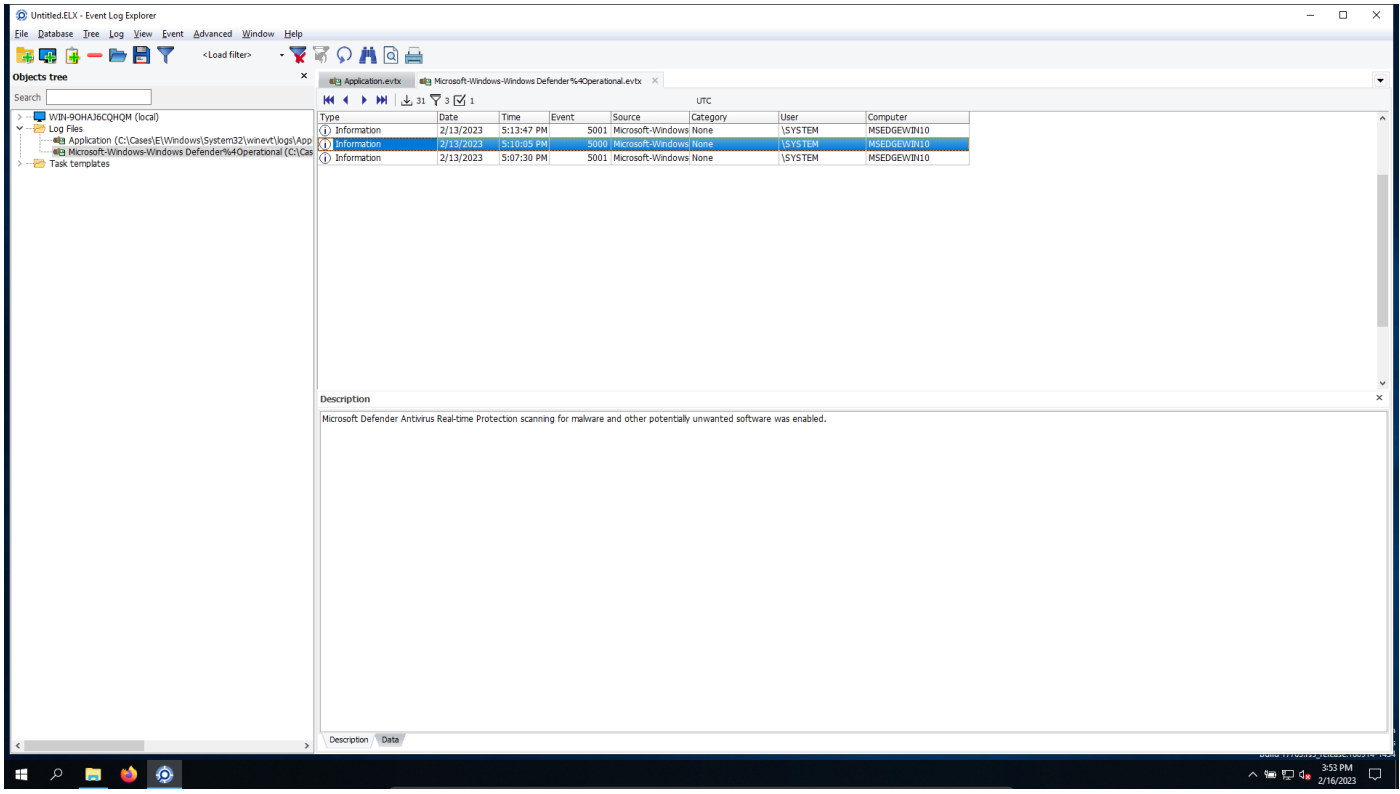


- We can filter the data:




Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:22:43 PM 1001 Microsoft-Windows None \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:21:35 PM 1000 Microsoft-Windows None \SYSTEM MSEDGEWIN10
Filter
Apply filter to:
Active event log view (File: C:\Cases\E\Windows\System32\winevt\logs\Microsoft-Windows-Windows Defender%4Operational.evtx)
Event log view(s) on your choice
Event types
Verbose
Information
Warning
Error
Critical
Audit Success
Audit Failure
Source:
Category:
User:
Computer:
Exclude
Event ID(s):
5000,5001
Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450,!0,255)
Text in description:
RegExp
Date
Time
Separately
From:
To:
2/16/2023
12:00:00 AM
Display event for the last
days
hours
Custom columns
Description params
Name
Operator
Value
Custom column 1
Custom column 2
Custom column 3
Custom column 4
Custom column 5
Clear
Load...
Save...
OK
Cancel
Description
Scan ID: {E895F20A-C28D-451F-AD14-417EF2BA5CE2}
Scan Type: Antimalware
Scan Parameters: Quick Scan
User: NT AUTHORITY\NETWORK SERVICE
Scan Time: 0:01:08
Description
Data
3:52 PM
2/16/2023

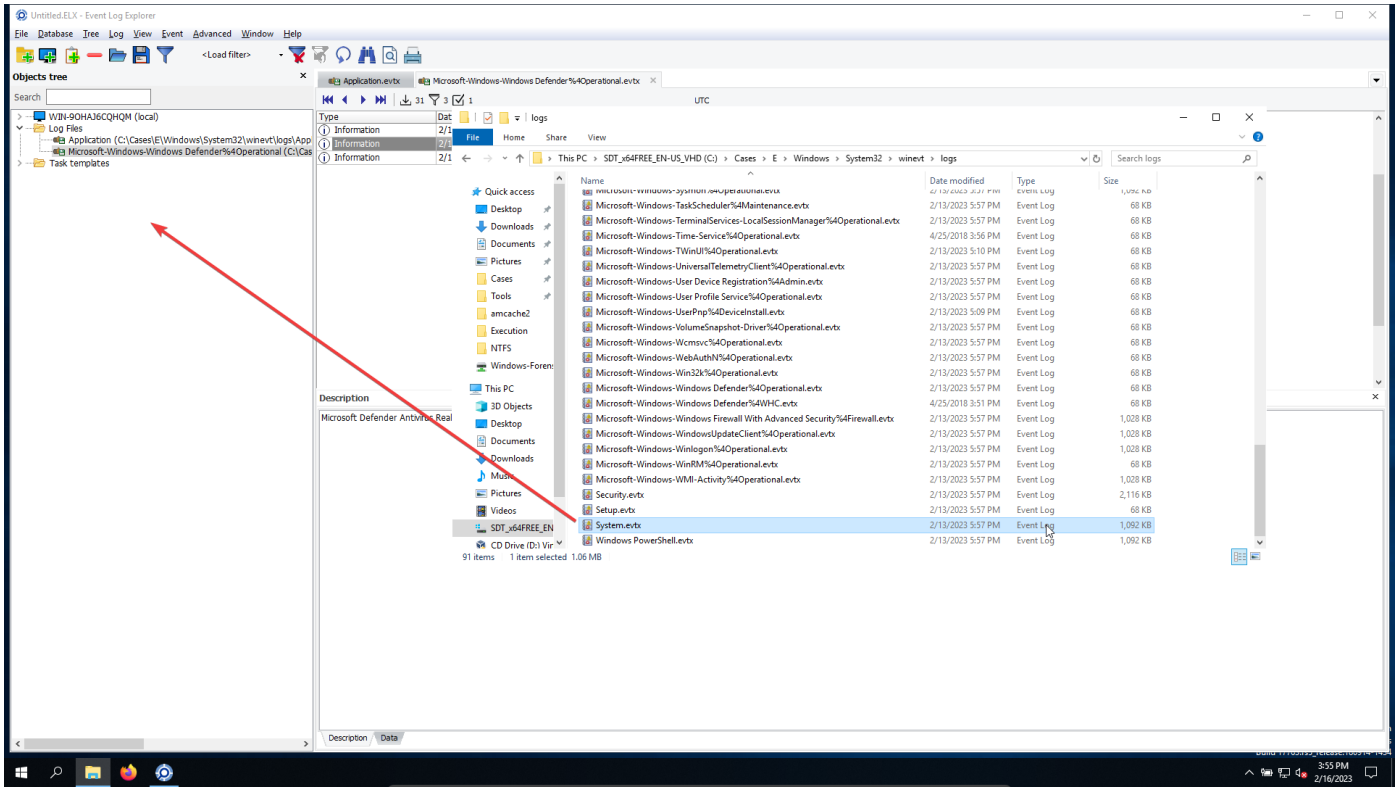

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:13:47 PM 5001 Microsoft-Windows None \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:10:05 PM 5000 Microsoft-Windows None \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:07:30 PM 5001 Microsoft-Windows None \SYSTEM MSEDGEWIN10
Description
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.
Description
Data
3:53 PM
2/16/2023

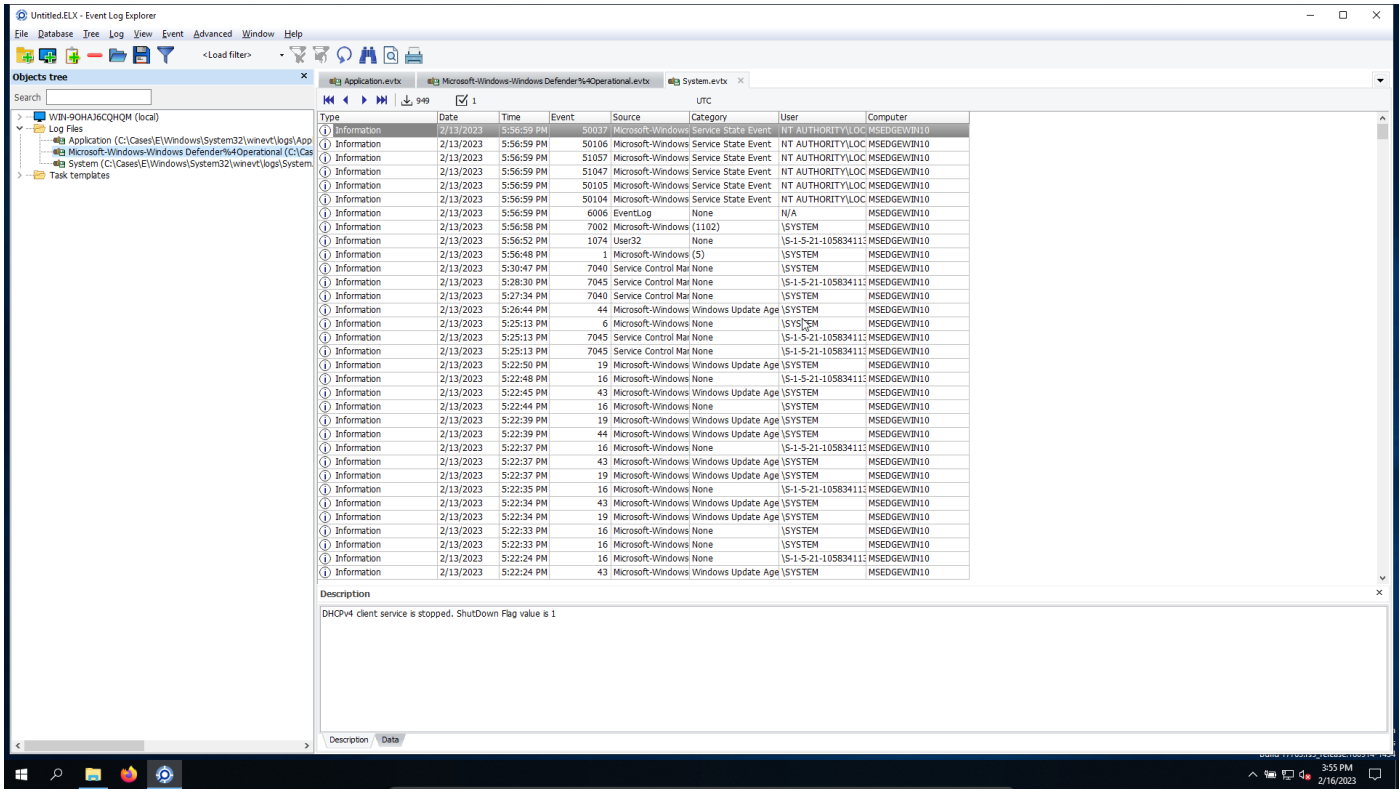


Service installs

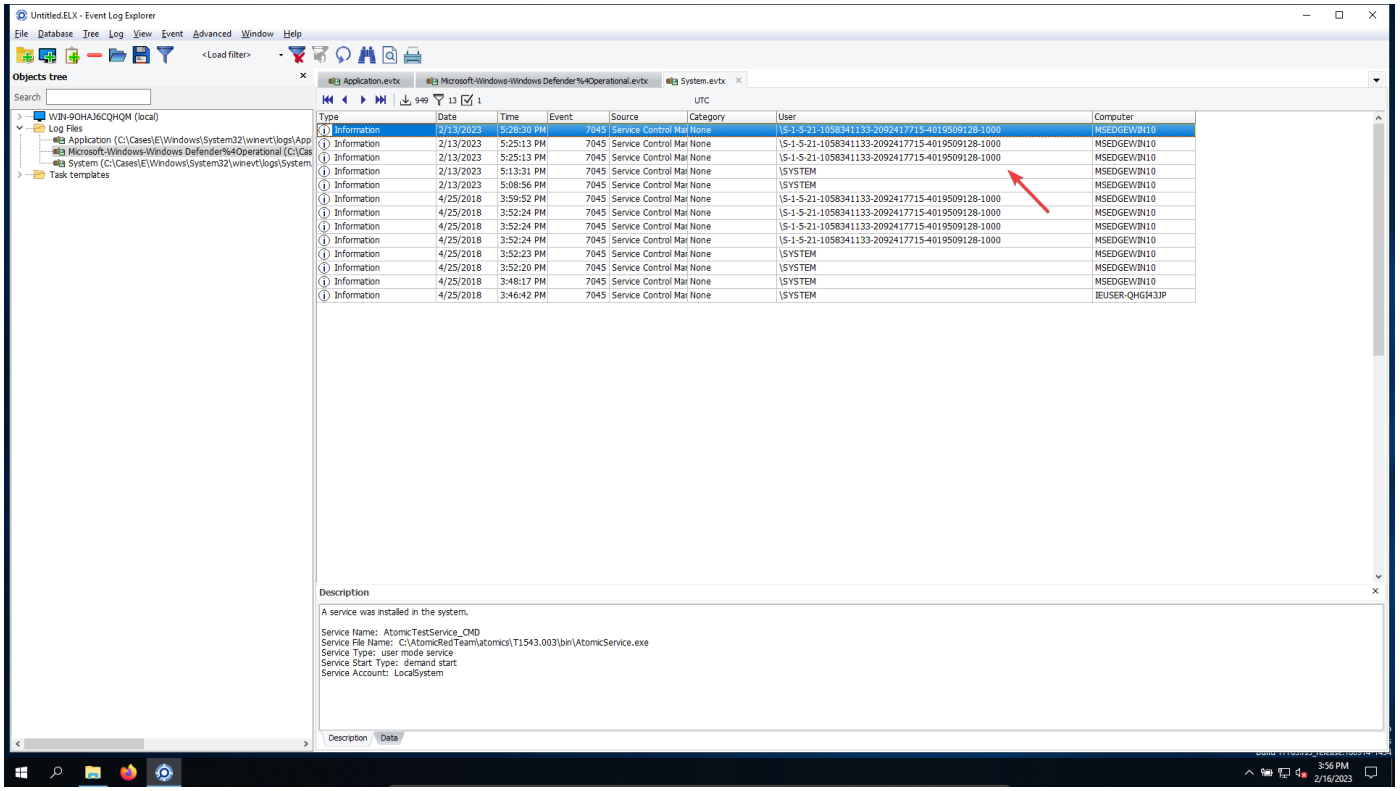
- Event IDs for System:
  - 7045: A new service was installed.

- Load System log:

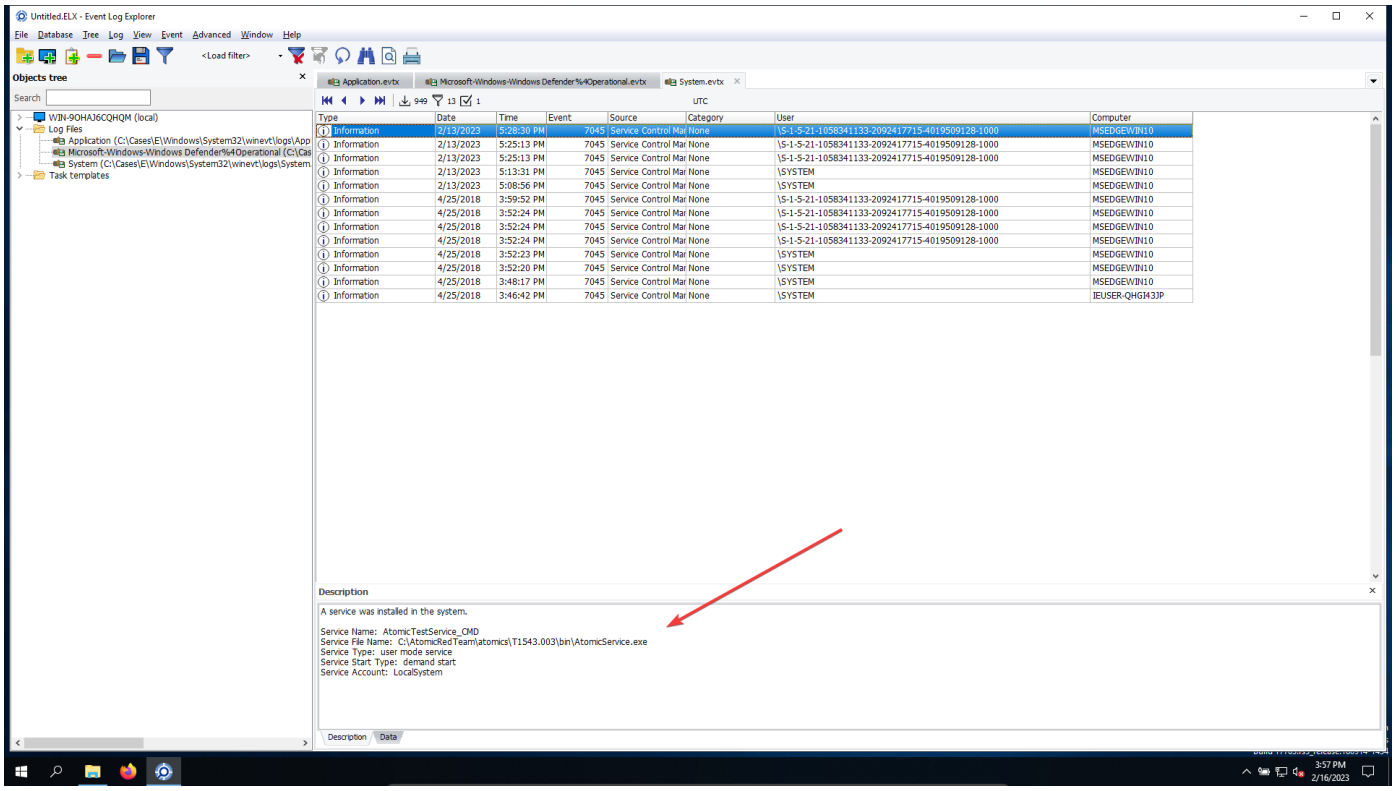




- Query based on event id 7045.



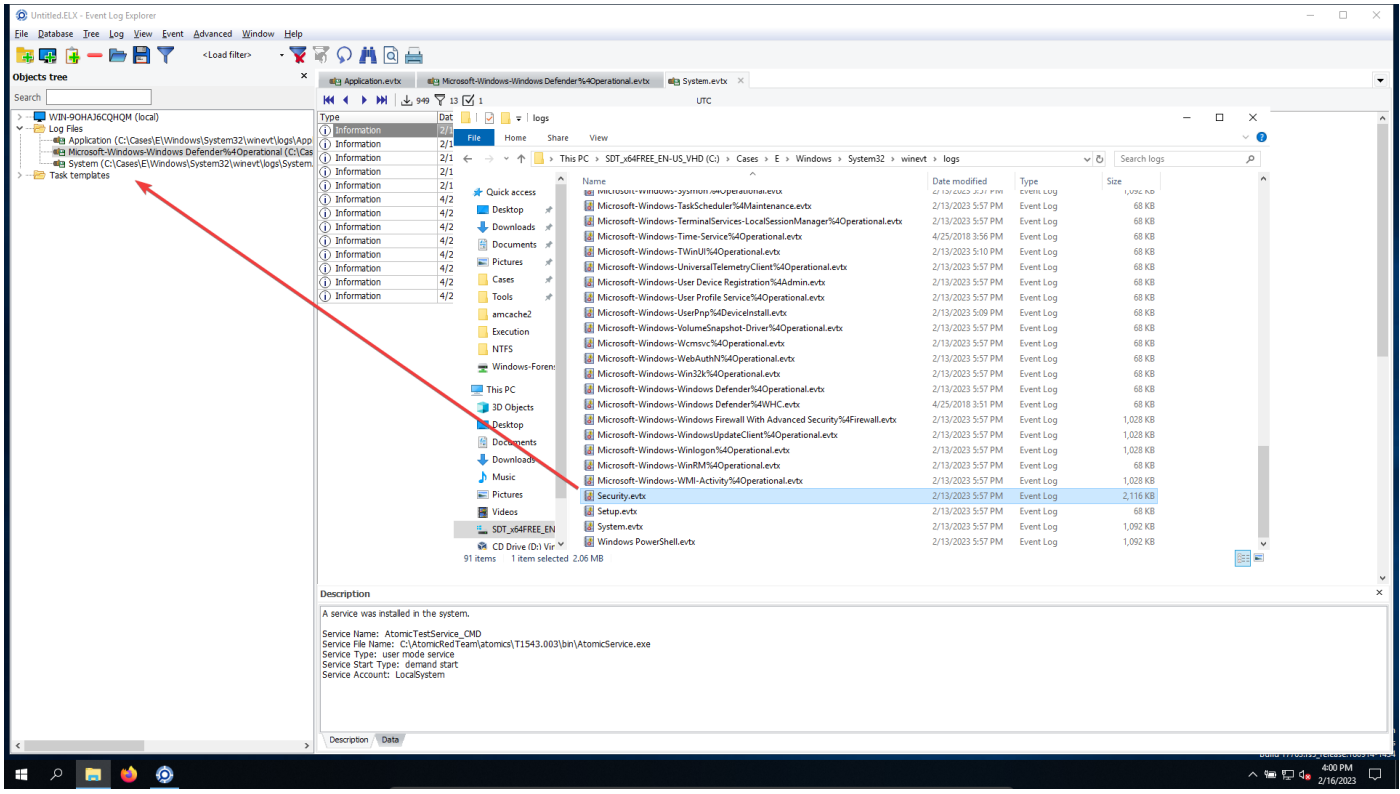
- Installed by user 1000.



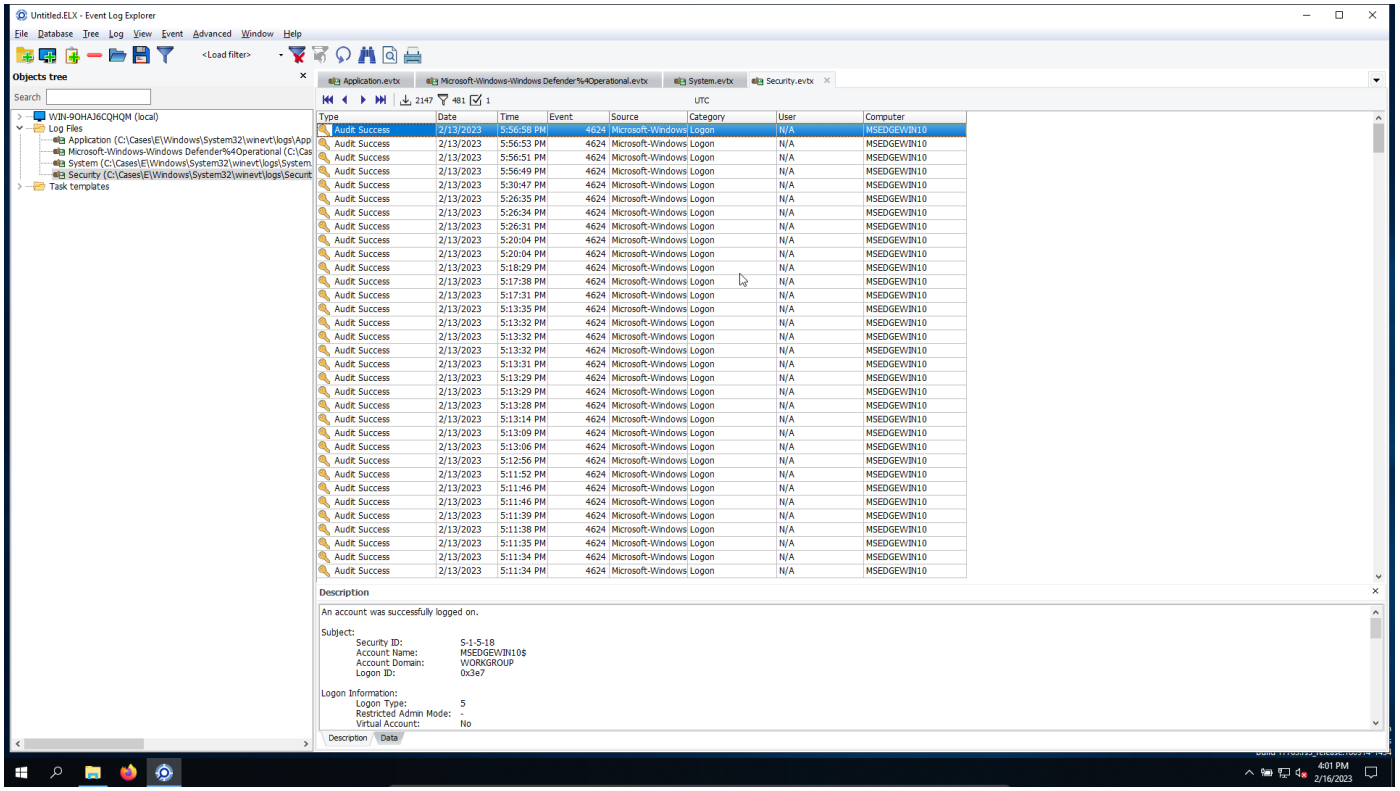
Security event log

- Event IDs for Security:
    - 4624: An account was successfully logged on.

- Load Security log:



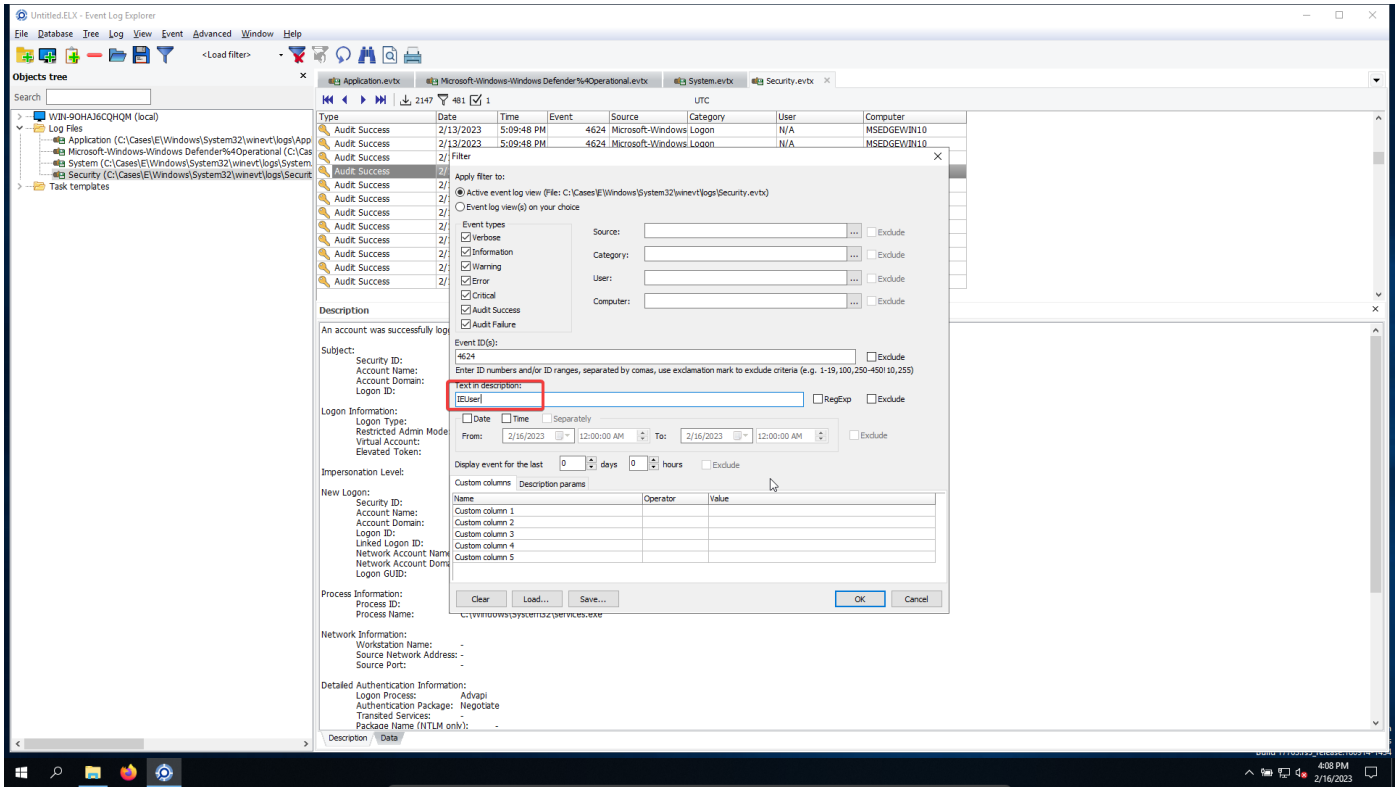
- Query based on event id 4624.

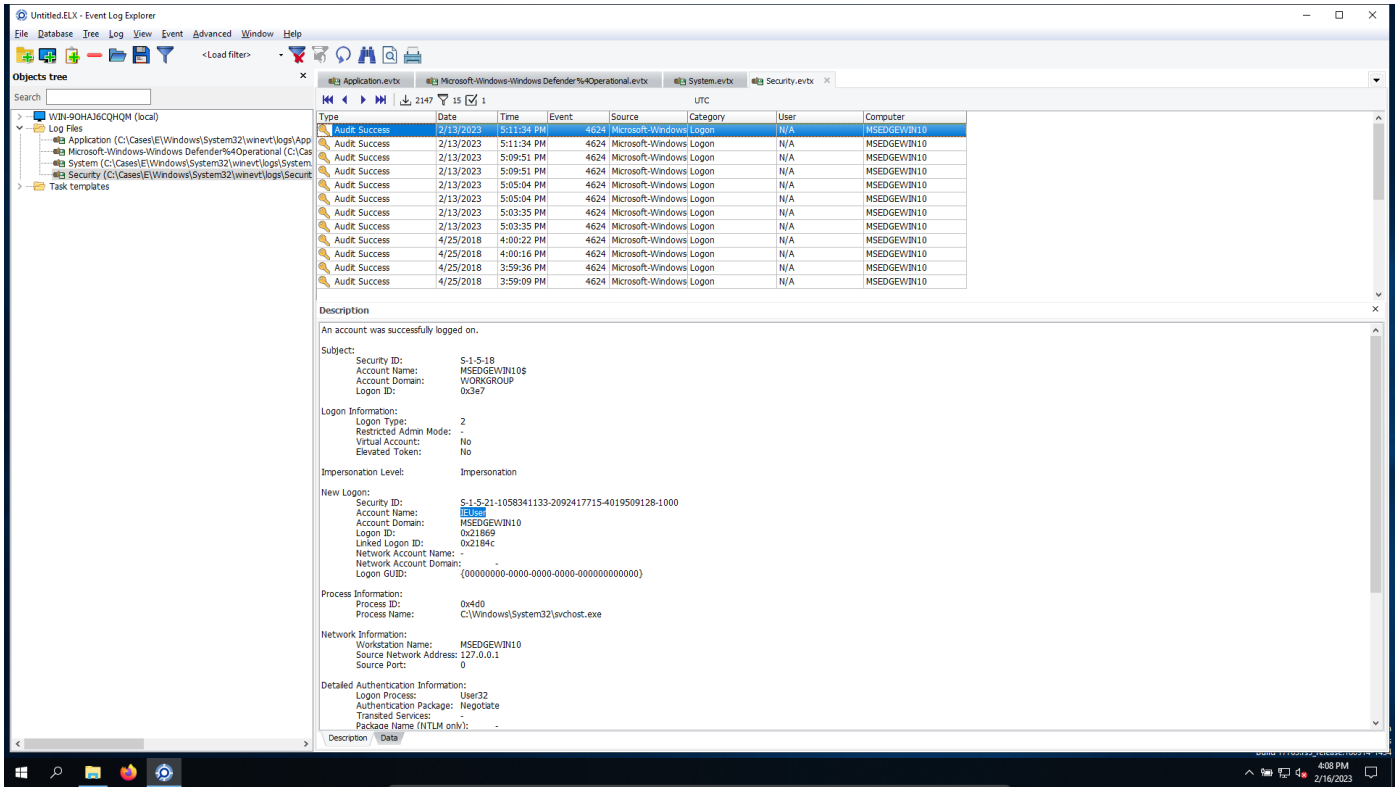


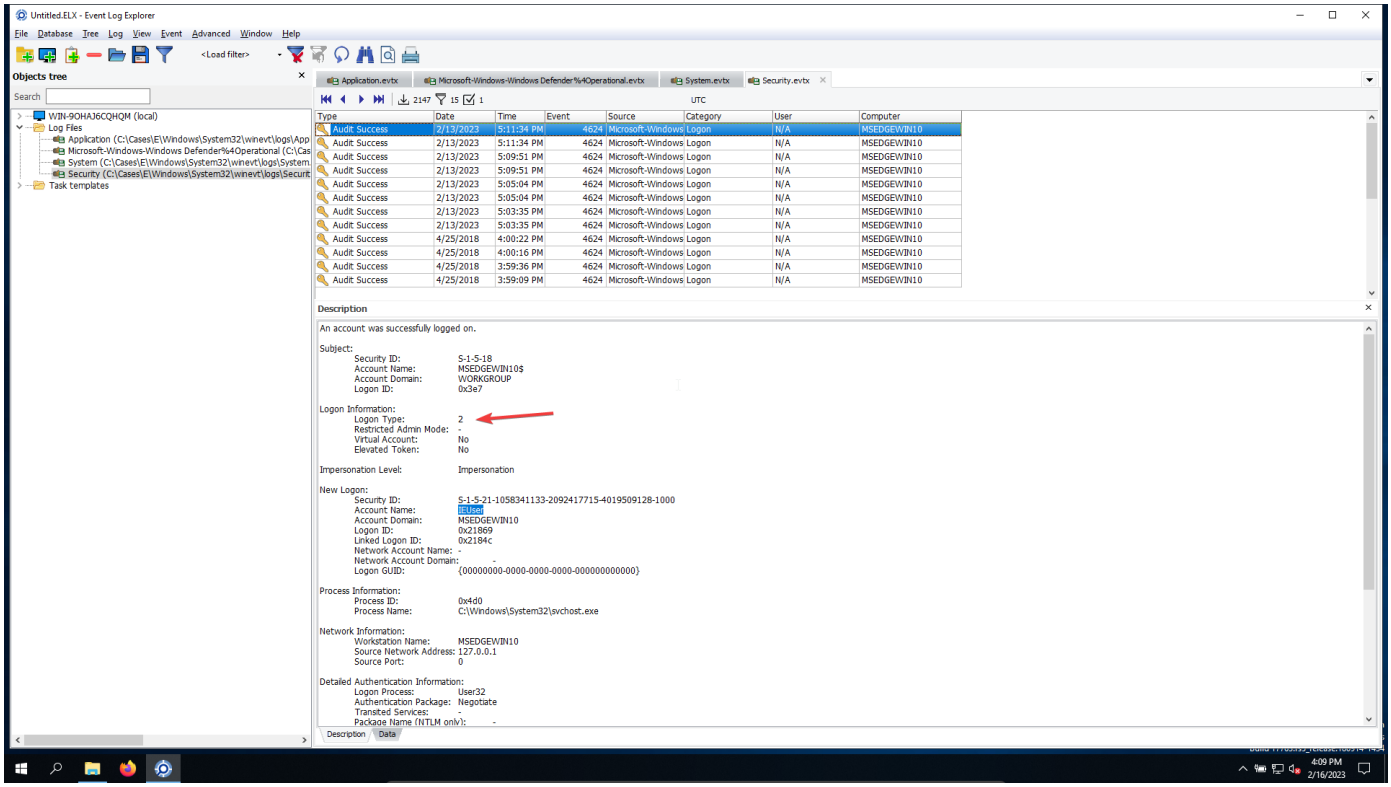
- You can see that there is A Logon Type information, you can find more information about it at : https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

- Important logon types:
  - 2: Interactive – with peripherals access and a monitor
  - 3: Network – logging through the network, remote
  - 10: RemoteInteractive – logging to a computer remotely using Remote Desktop.

- Search for the same eventid but adding the user in text description:

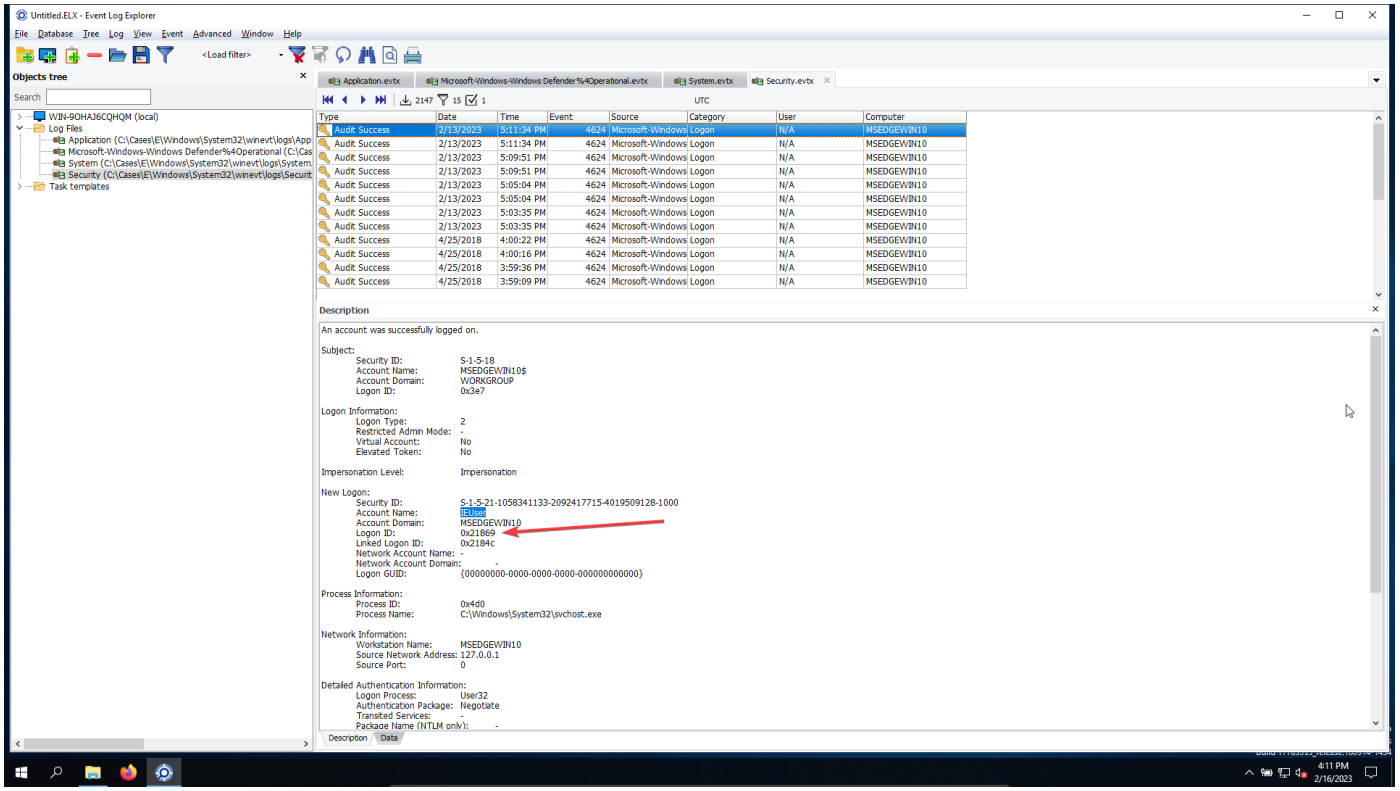

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Type Date Time Event Source Category User Computer
Audit Success 2/13/2023 5:09:48 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Filter
Apply filter to:
Active event log view (File: C:\Cases\E\Windows\System32\winevt\logs\Security.evtx)
Event log view(s) on your choice
Event types
Verbose
Information
Warning
Error
Critical
Audit Success
Audit Failure
Source:
Category:
User:
Computer:
Exclude
Event ID(s):
4624
Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)
Text in description:
IEUser
RegExp
Date
Time
Separately
From:
To:
2/16/2023
12:00:00 AM
Display event for the last
days
hours
Custom columns
Description params
Name
Operator
Value
Custom column 1
Custom column 2
Custom column 3
Custom column 4
Custom column 5
Clear
Load...
Save...
OK
Cancel
Description
An account was successfully log
Subject:
Security ID:
Account Name:
Account Domain:
Logon ID:
Logon Information:
Logon Type:
Restricted Admin Mode
Virtual Account:
Elevated Token:
Impersonation Level:
New Logon:
Security ID:
Account Name:
Account Domain:
Logon ID:
Linked Logon ID:
Network Account Name
Network Account Doma
Logon GUID:
Process Information:
Process ID:
Process Name:
Network Information:
Workstation Name:
Source Network Address:
Source Port:
Detailed Authentication Information:
Logon Process:
Authentication Package:
Transited Services:
Package Name (NTLM only):
Description
Data
4:08 PM
2/16/2023


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Type Date Time Event Source Category User Computer
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:09:51 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:09:51 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:05:04 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:05:04 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:03:35 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:03:35 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 4/25/2018 4:00:22 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 4/25/2018 4:00:16 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 4/25/2018 3:59:36 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 4/25/2018 3:59:09 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Description
An account was successfully logged on.
Subject:
Security ID: S-1-5-18
Account Name: MSEDGEWIN10$
Account Domain: WORKGROUP
Logon ID: 0x3e7
Logon Information:
Logon Type: 2
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No
Impersonation Level: Impersonation
New Logon:
Security ID: S-1-5-21-1058341133-2092417715-401950912B-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x21869
Linked Logon ID: 0x2184c
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
Process ID: 0x4d0
Process Name: C:\Windows\System32\svchost.exe
Network Information:
Workstation Name: MSEDGEWIN10
Source Network Address: 127.0.0.1
Source Port: 0
Detailed Authentication Information:
Logon Process: User32
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Description
Data
4:08 PM
2/16/2023



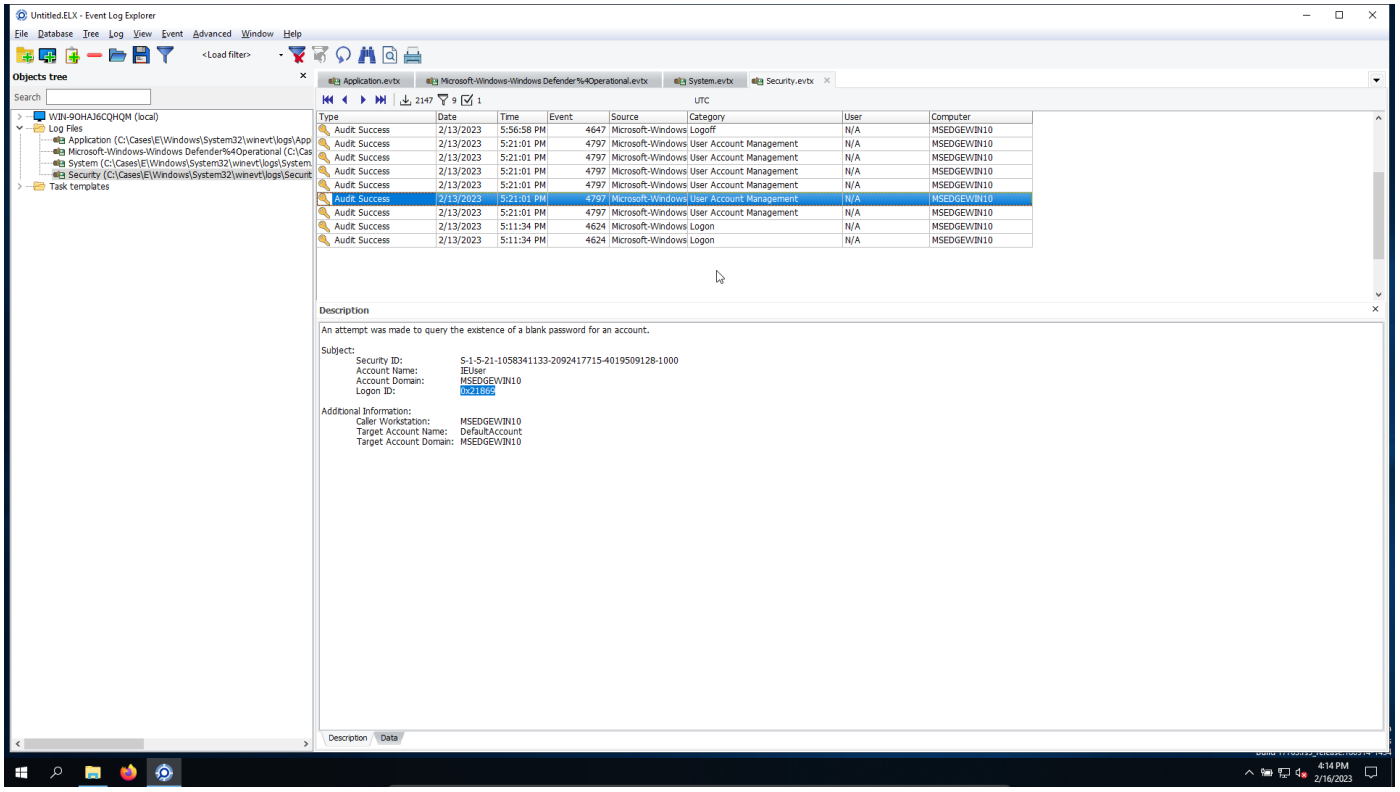
Authentication

- When an Administrator is logging on , two access tokens are issued, one elevated that means high privilege and another that is not elevated and means low privilege. Logon ID being in relation with high or low privilege token.

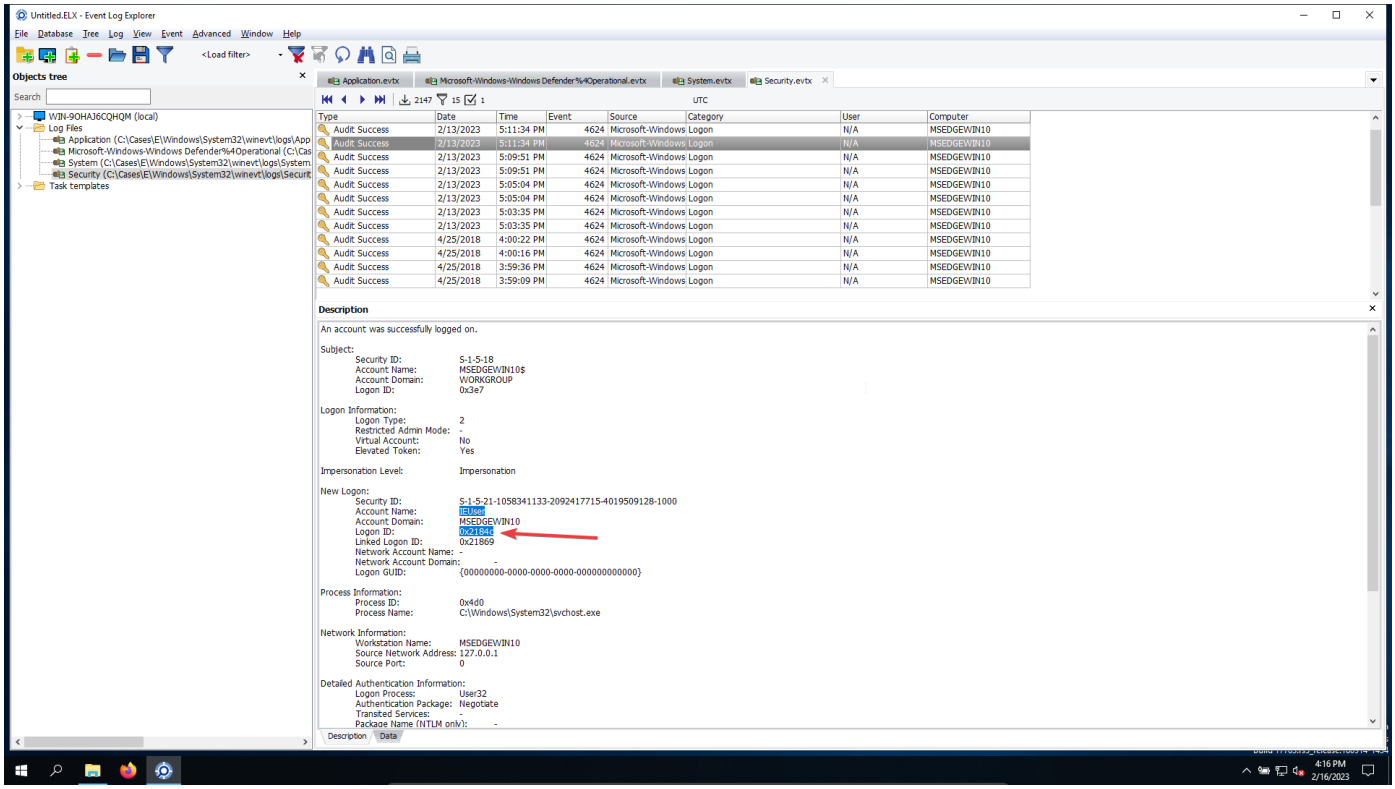


- Search based on Logon ID in text description:

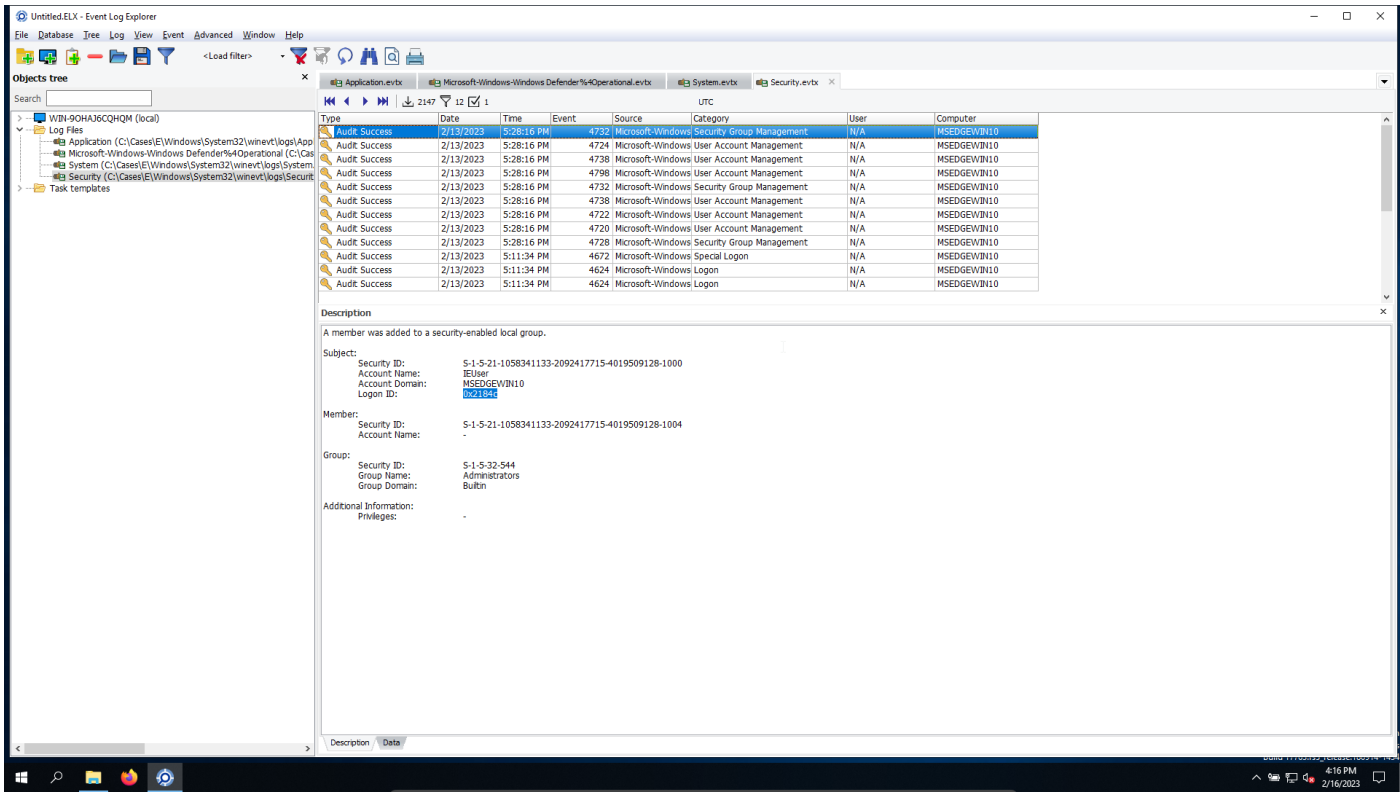
  0x21869



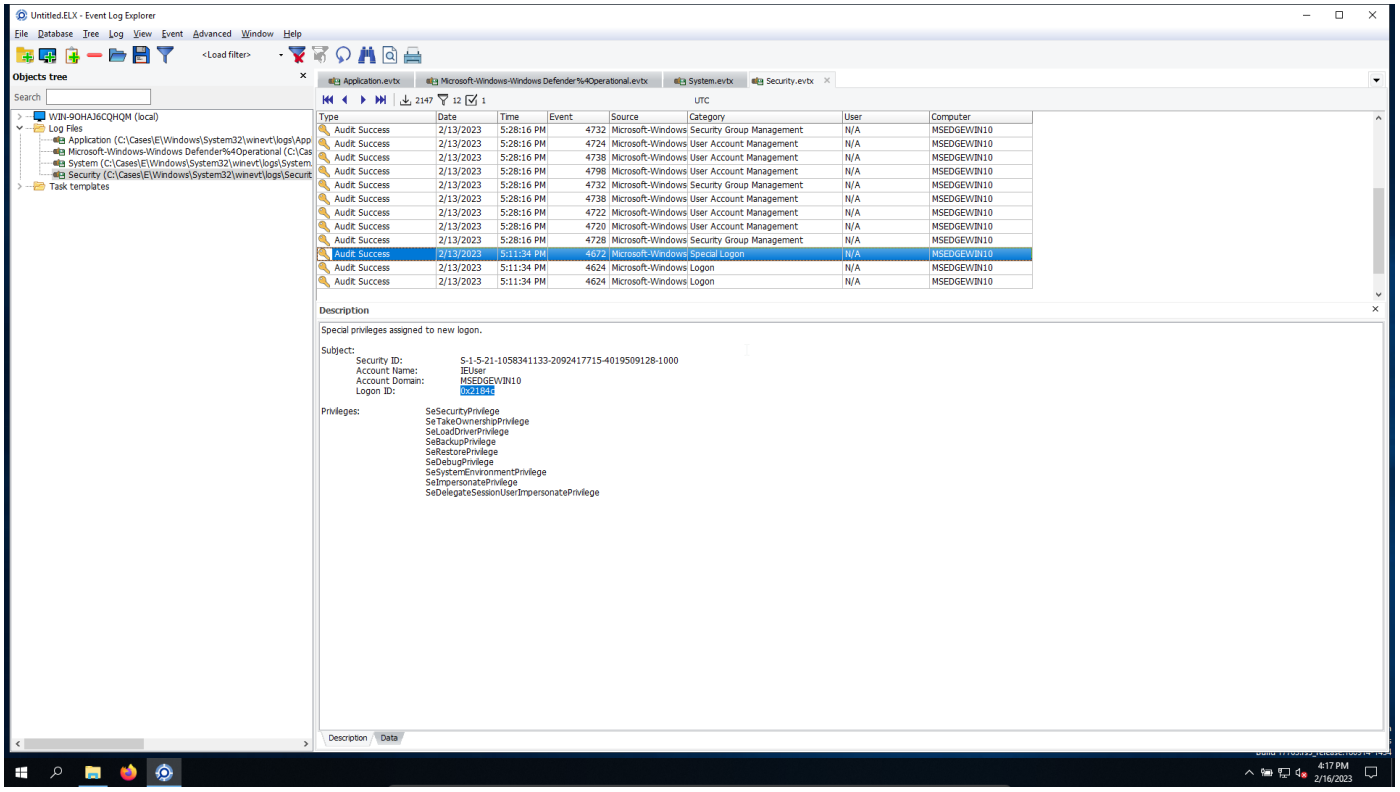
- Go back to the previous search:

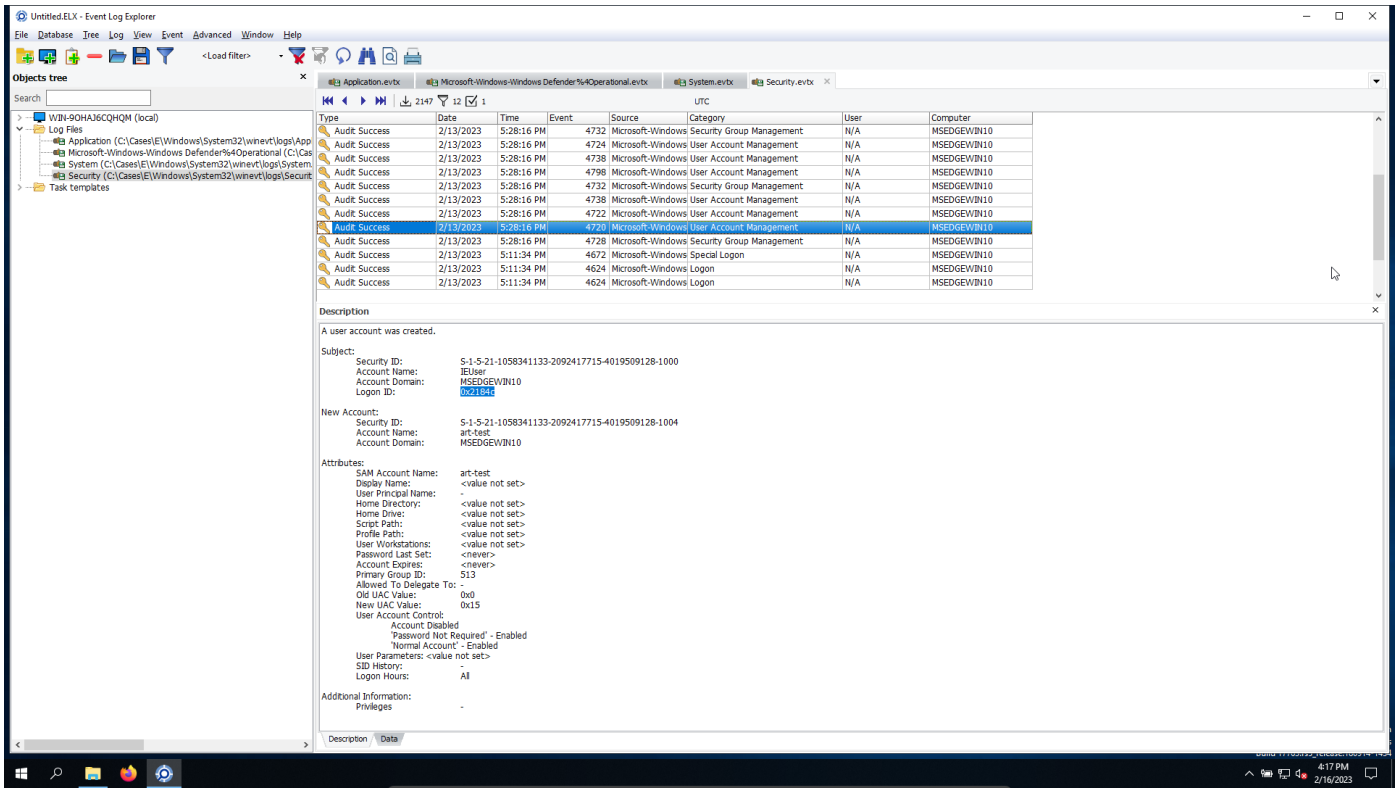


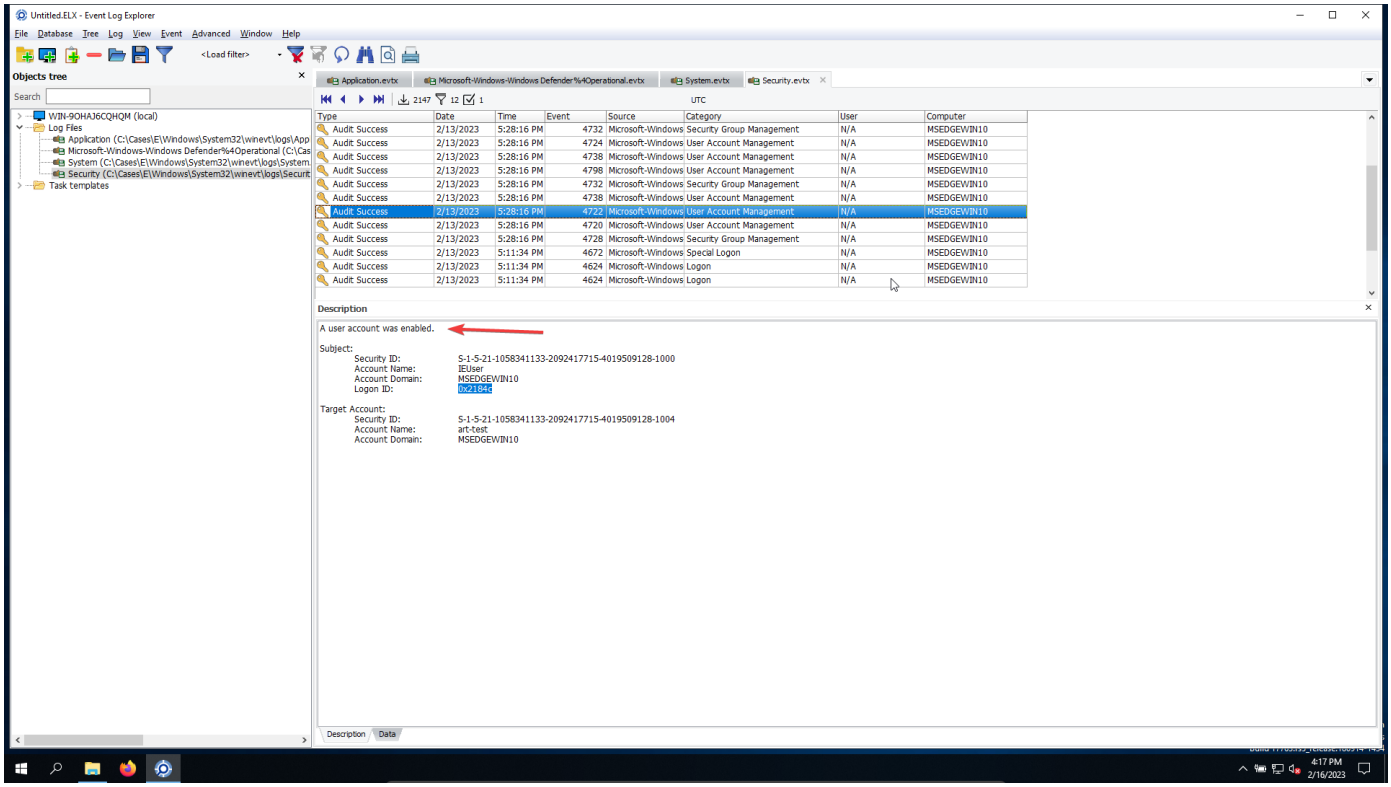
0x2184c

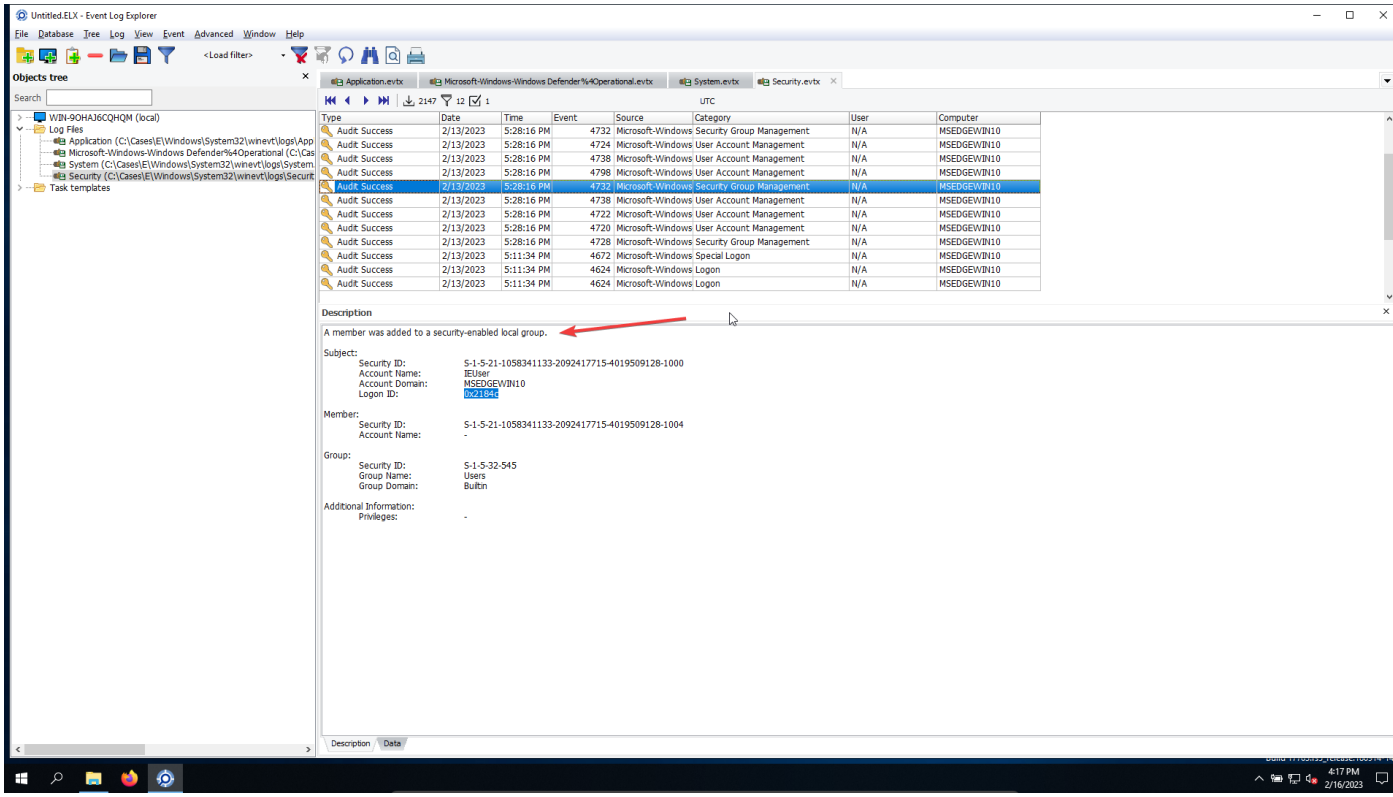


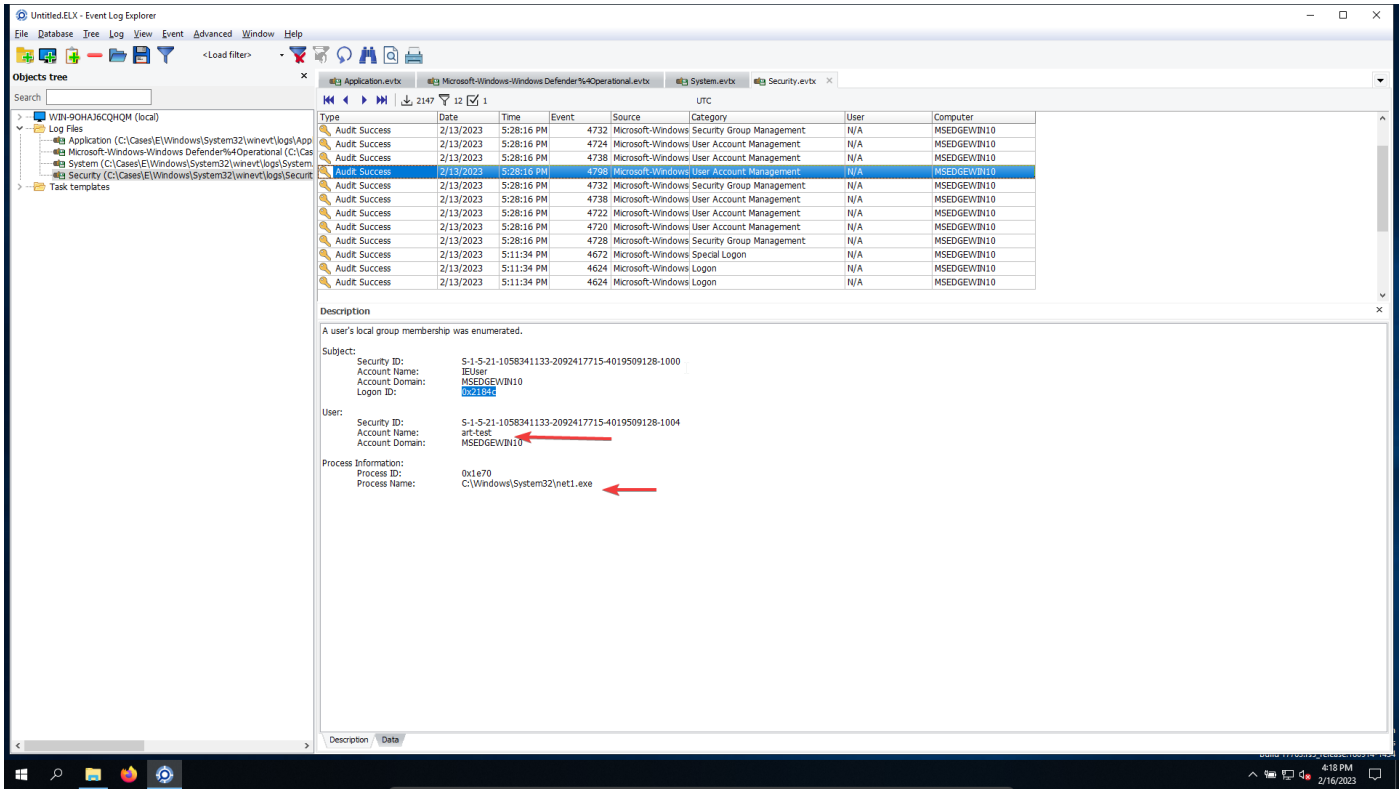
- Example of privileges needed in order to execute malicious activity .


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
UTC
Type Date Time Event Source Category User Computer
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4724 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4798 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4722 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4720 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4728 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4672 Microsoft-Windows Special Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Description
Special privileges assigned to new logon.
Subject:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x2184c
Privileges: SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege
Description Data
4:17 PM
2/16/2023


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
UTC
Type Date Time Event Source Category User Computer
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4724 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4798 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4722 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4720 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4728 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4672 Microsoft-Windows Special Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Description
A user account was created.
Subject:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x2184c
New Account:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1004
Account Name: art-test
Account Domain: MSEDGEWIN10
Attributes:
SAM Account Name: art-test
Display Name: <value not set>
User Principal Name: -
Home Directory: <value not set>
Home Drive: <value not set>
Script Path: <value not set>
Profile Path: <value not set>
User Workstations: <value not set>
Password Last Set: <never>
Account Expires: <never>
Primary Group ID: 513
Allowed To Delegate To: -
Old UAC Value: 0x0
New UAC Value: 0x15
User Account Control:
Account Disabled
'Password Not Required' - Enabled
'Normal Account' - Enabled
User Parameters: <value not set>
SID History: -
Logon Hours: All
Additional Information:
Privileges -
Description Data
4:17 PM
2/16/2023


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
UTC
Type Date Time Event Source Category User Computer
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4724 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4798 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4722 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4720 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4728 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4672 Microsoft-Windows Special Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Description
A user account was enabled.
Subject:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x2184c
Target Account:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1004
Account Name: art-test
Account Domain: MSEDGEWIN10
Description Data
4:17 PM
2/16/2023

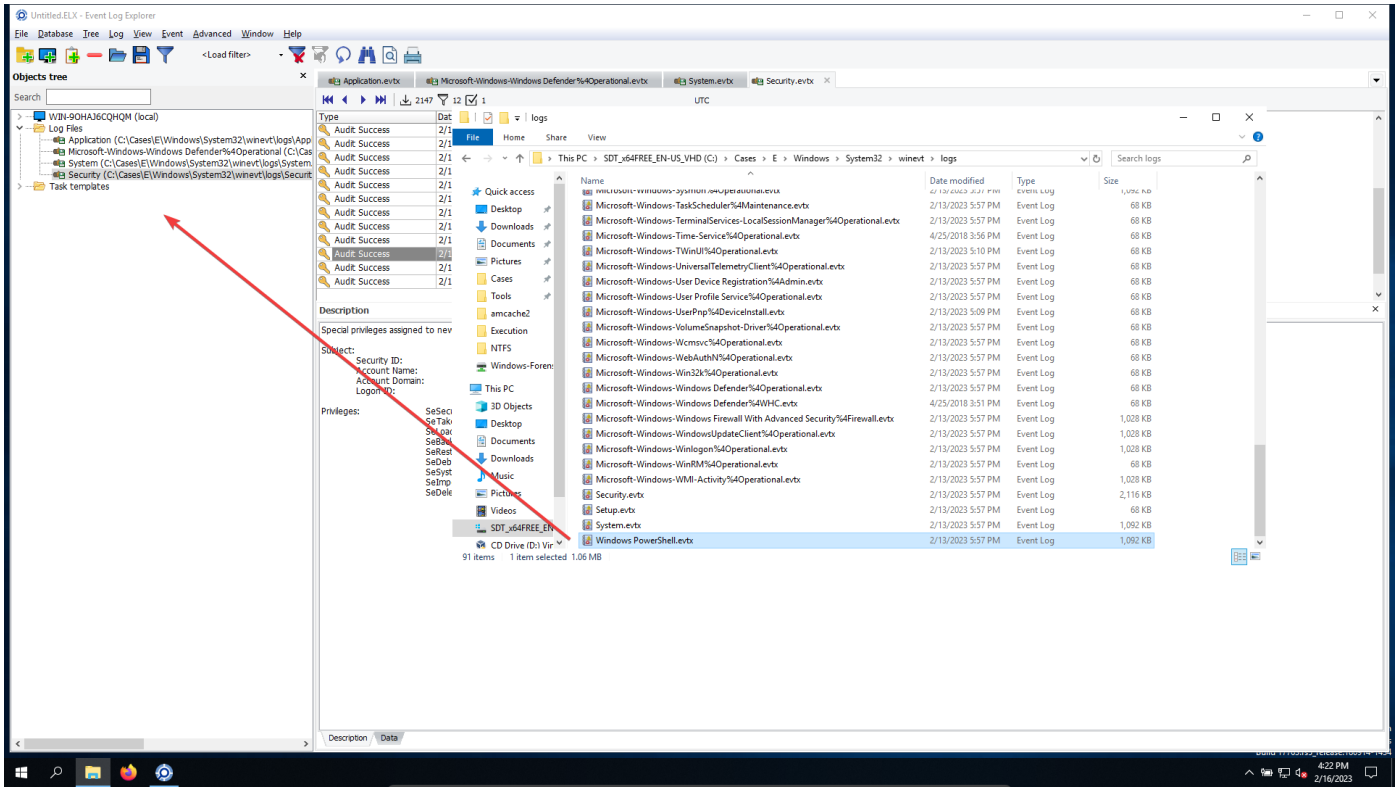

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
UTC
Type Date Time Event Source Category User Computer
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4724 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4798 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4732 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4738 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4722 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4720 Microsoft-Windows User Account Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:28:16 PM 4728 Microsoft-Windows Security Group Management N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4672 Microsoft-Windows Special Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Audit Success 2/13/2023 5:11:34 PM 4624 Microsoft-Windows Logon N/A MSEDGEWIN10
Description
A member was added to a security-enabled local group.
Subject:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x2184c
Member:
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1004
Account Name: -
Group:
Security ID: S-1-5-32-545
Group Name: Users
Group Domain: Builtin
Additional Information:
Privileges: -
Description Data
4:17 PM
2/16/2023

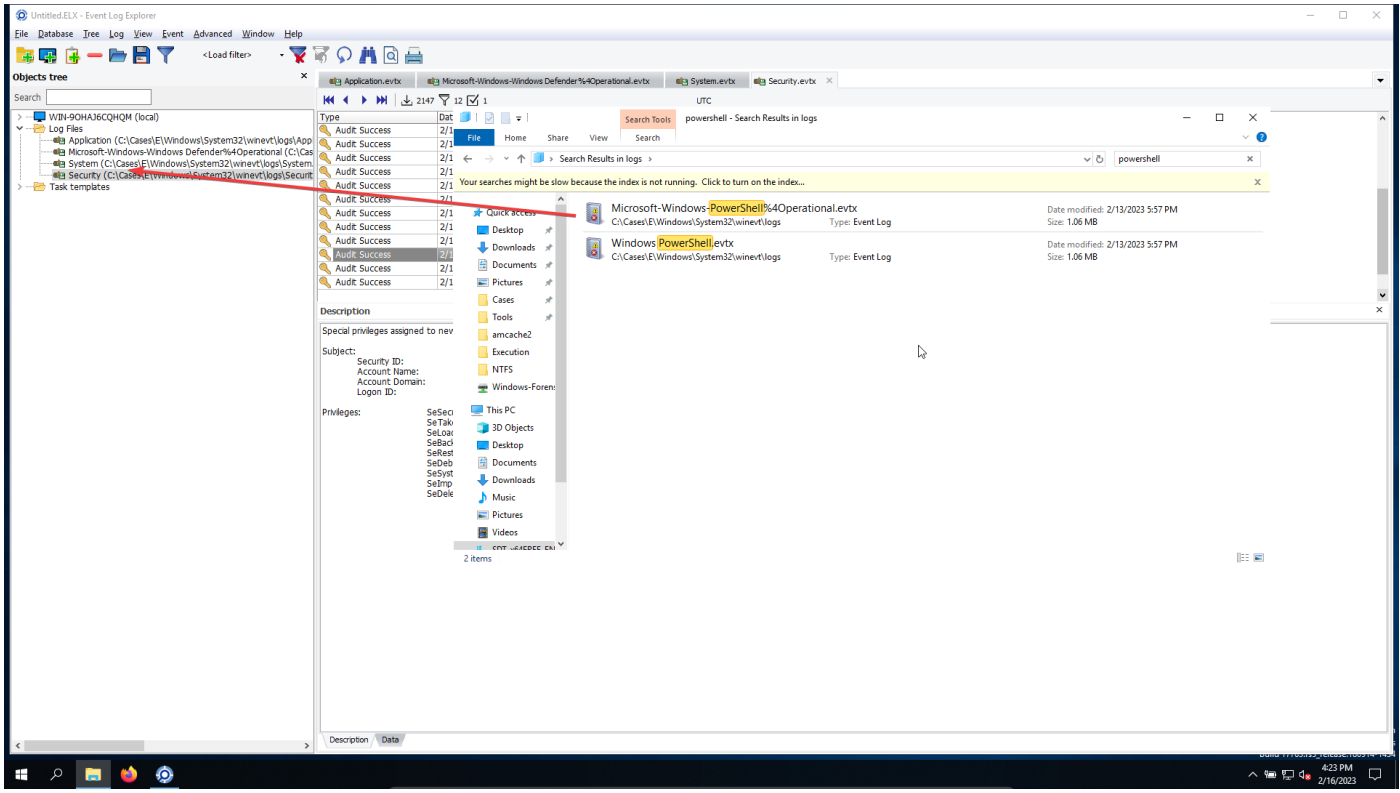


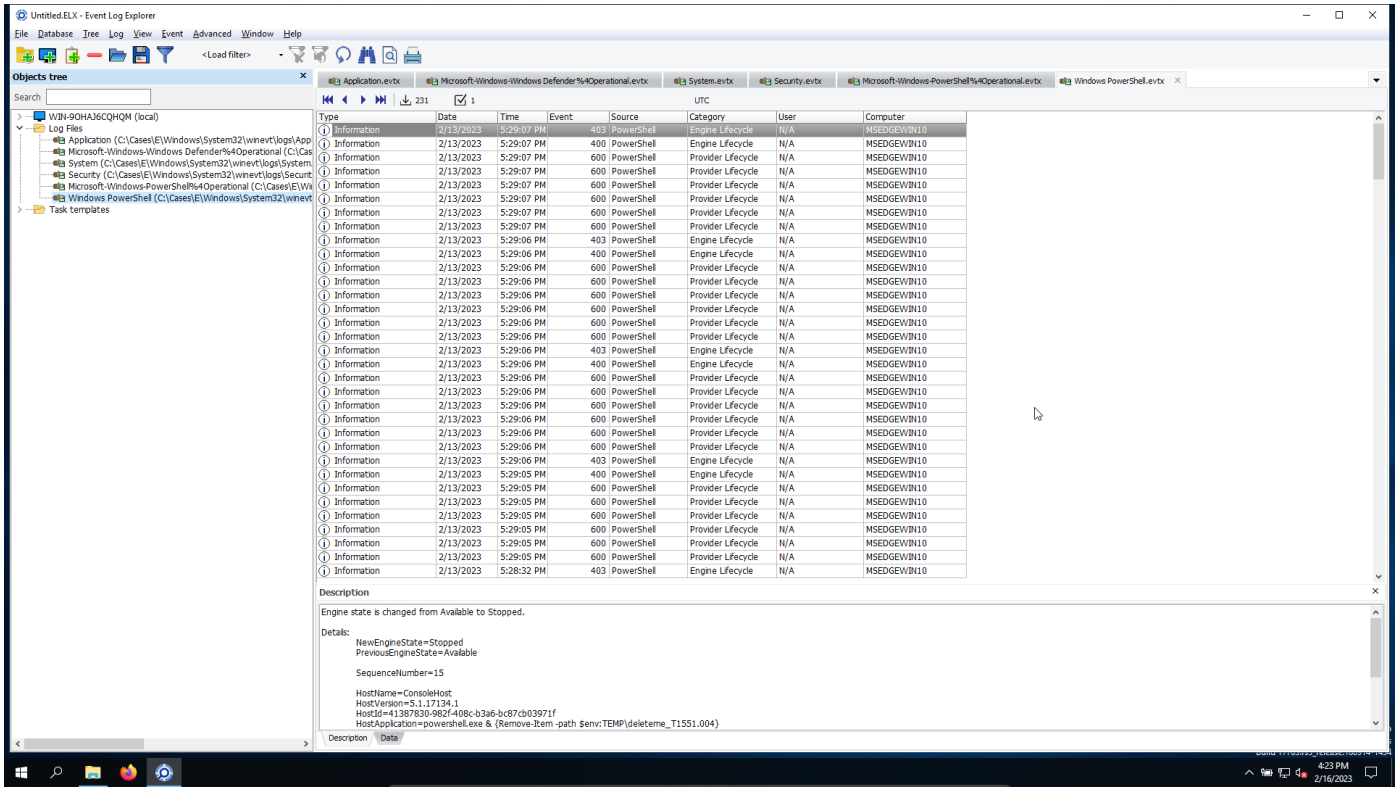
Powershell

- Event IDs for Windows PowerShell:
  - 400: Engine state is changed from None to Available.

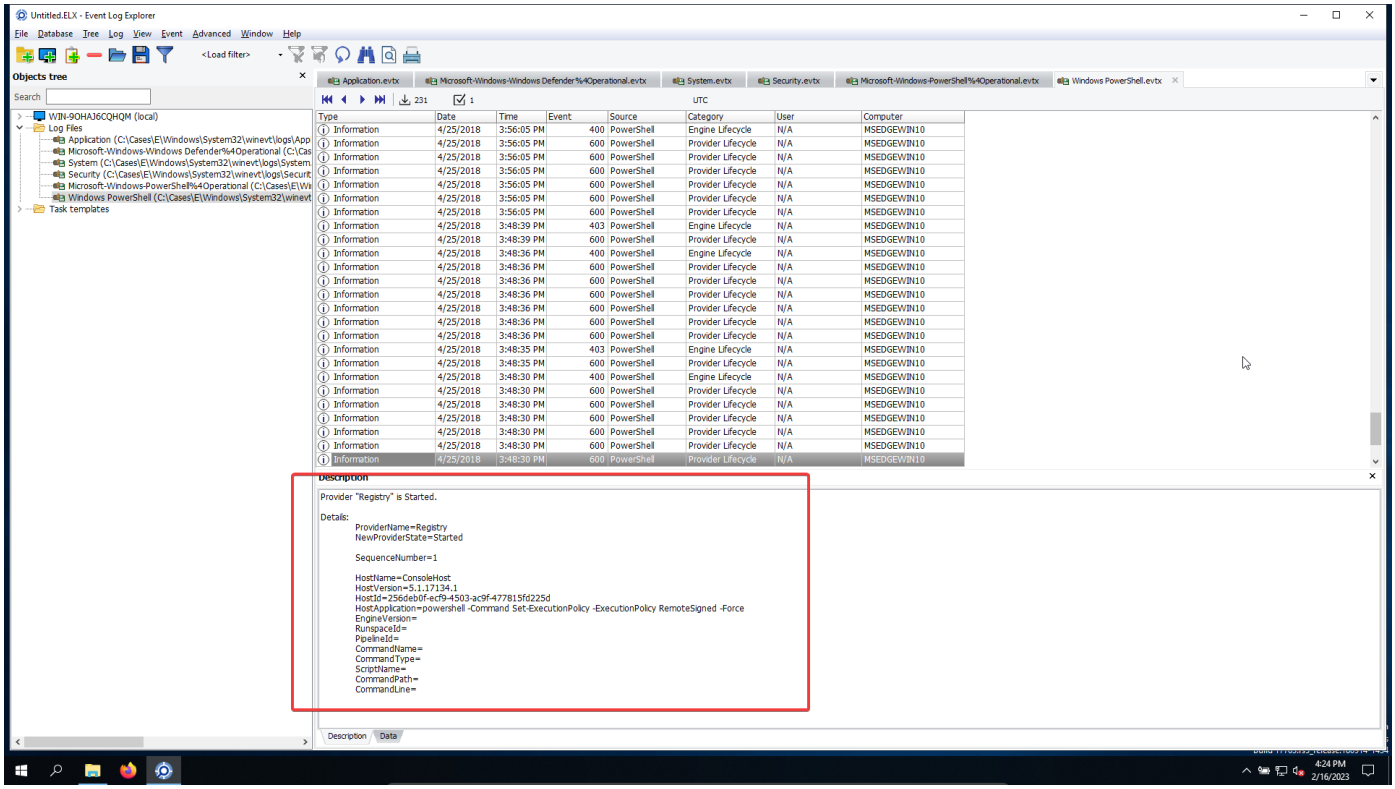
- Load Windows PowerShell:

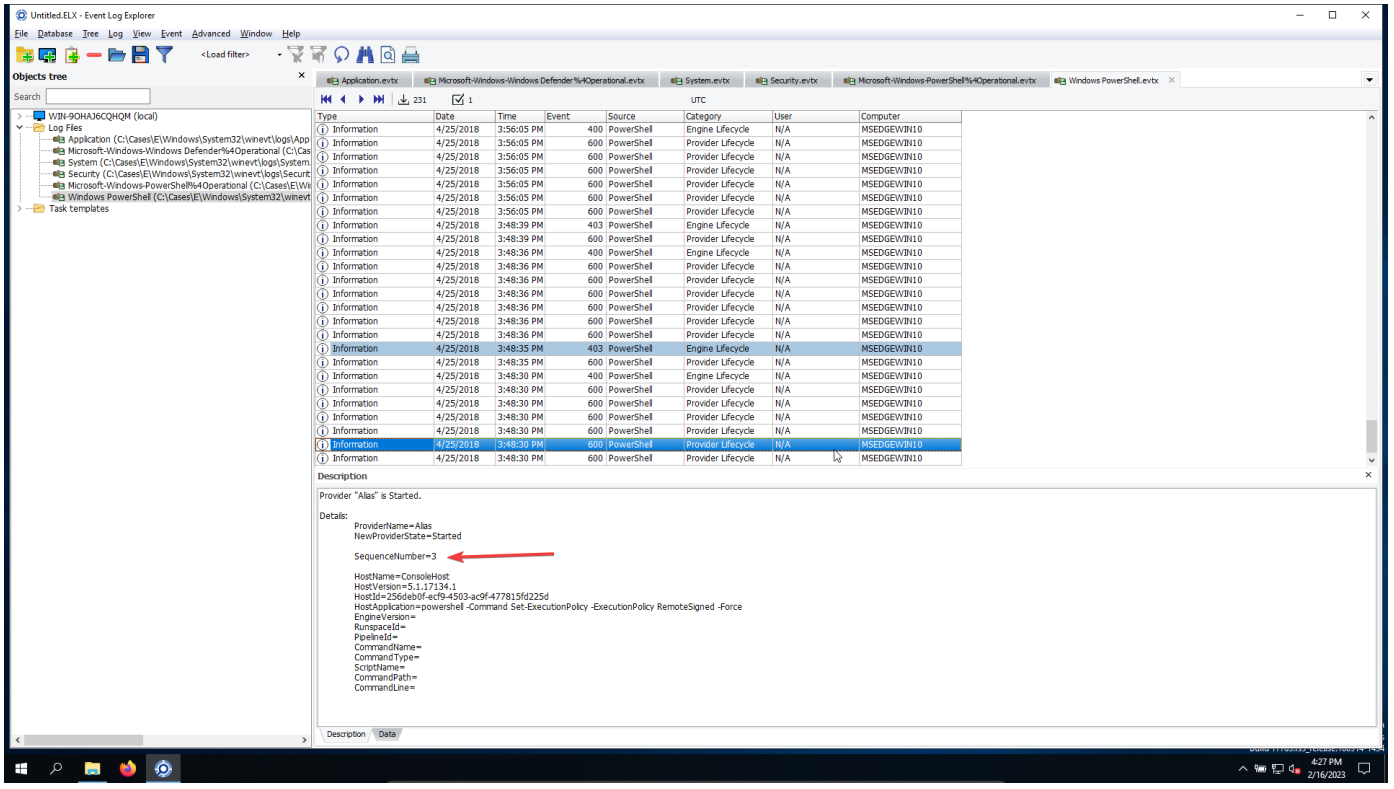

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
UTC
Type
Audit Success
Description
Special privileges assigned to nev
Subject:
Security ID:
Account Name:
Account Domain:
Logon ID:
Privileges:
logs
File Home Share View
This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > E > Windows > System32 > winevt > logs
Search logs
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
amcache2
Execution
NTFS
This PC
3D Objects
Music
Videos
Name
Date modified
Type
Size
Microsoft-Windows-TaskScheduler%4Maintenance.evtx
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Microsoft-Windows-Time-Service%4Operational.evtx
Microsoft-Windows-TWinUI%4Operational.evtx
Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
Microsoft-Windows-User Device Registration%4Admin.evtx
Microsoft-Windows-User Profile Service%4Operational.evtx
Microsoft-Windows-UserPnp%4DeviceInstall.evtx
Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
Microsoft-Windows-Wcmsvc%4Operational.evtx
Microsoft-Windows-WebAuthN%4Operational.evtx
Microsoft-Windows-Win32k%4Operational.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
Microsoft-Windows-Windows Defender%4WHC.evtx
Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
Microsoft-Windows-Winlogon%4Operational.evtx
Microsoft-Windows-WinRM%4Operational.evtx
Microsoft-Windows-WMI-Activity%4Operational.evtx
Security.evtx
Setup.evtx
System.evtx
Windows PowerShell.evtx
91 items 1 item selected 1.06 MB
Description Data
4:22 PM
2/16/2023


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
UTC
Search Tools
powershell - Search Results in logs
File Home Share View Search
Search Results in logs
powershell
Your searches might be slow because the index is not running. Click to turn on the index...
Microsoft-Windows-PowerShell%4Operational.evtx
C:\Cases\E\Windows\System32\winevt\logs
Type: Event Log
Date modified: 2/13/2023 5:57 PM
Size: 1.06 MB
Windows PowerShell.evtx
C:\Cases\E\Windows\System32\winevt\logs
Type: Event Log
Date modified: 2/13/2023 5:57 PM
Size: 1.06 MB
2 items
Description Data
4:23 PM
2/16/2023

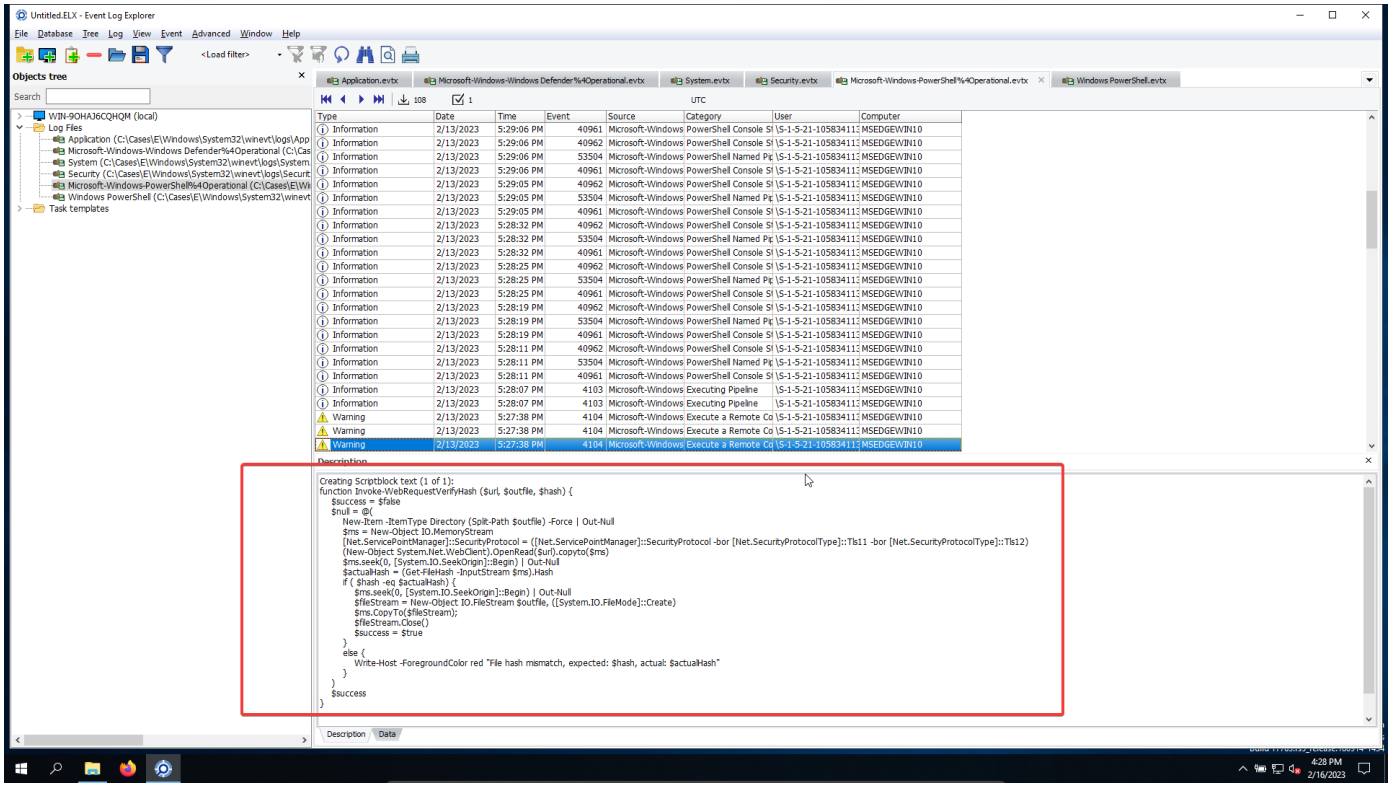


- You can see a lot of information in WIndows Powershell , for example , powershell command executed, sequence number grows until 403, included. The Event goes 400,600 and ends with 403.

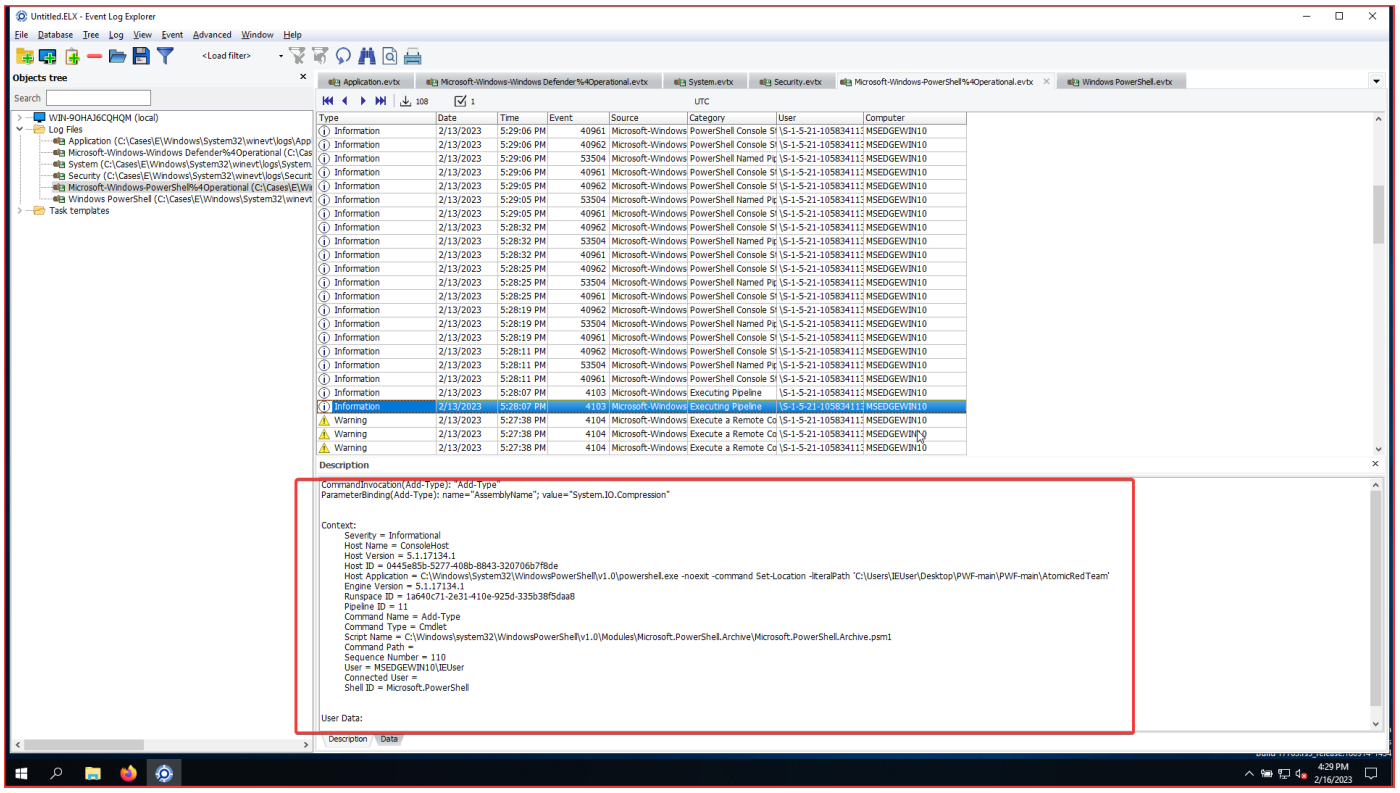




- In Windows Powershell Operational you can see code being executed:

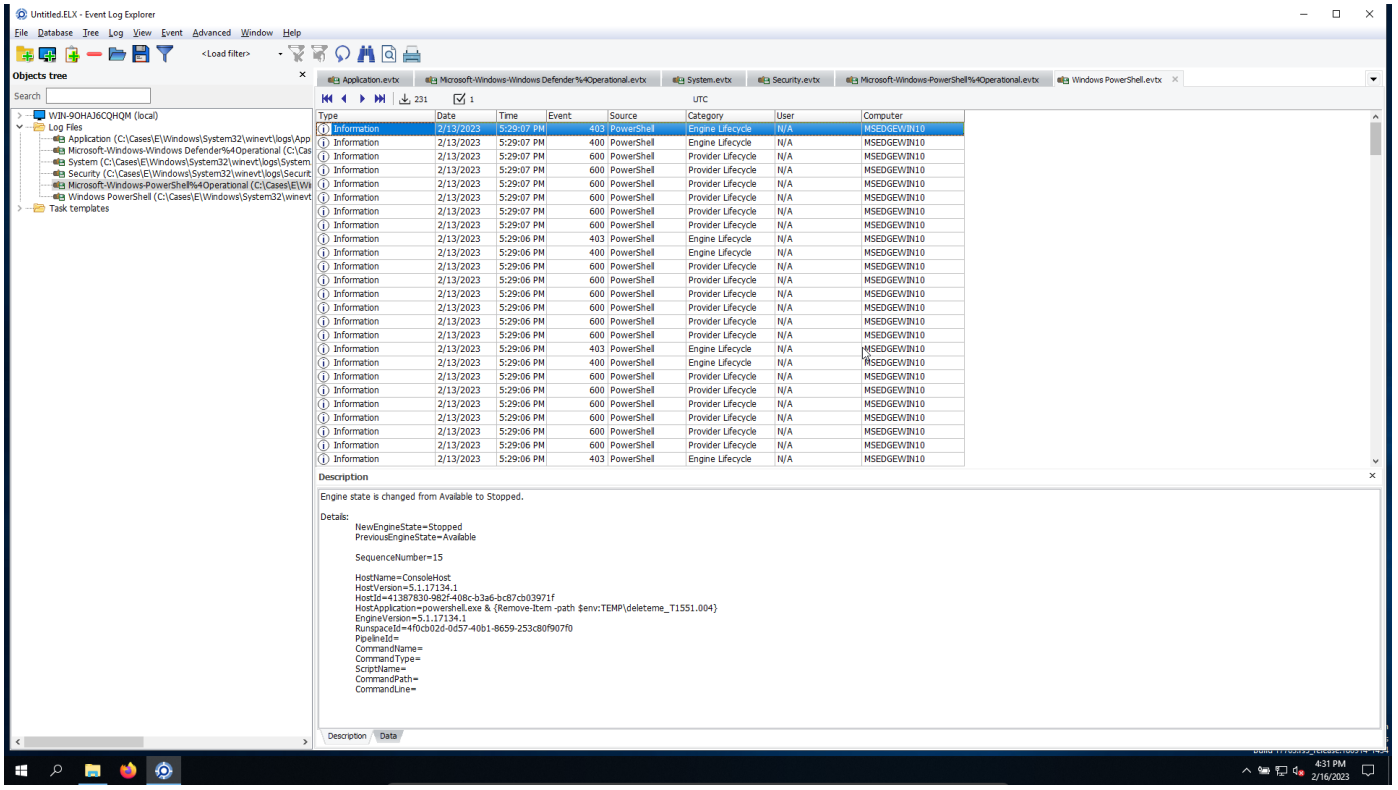


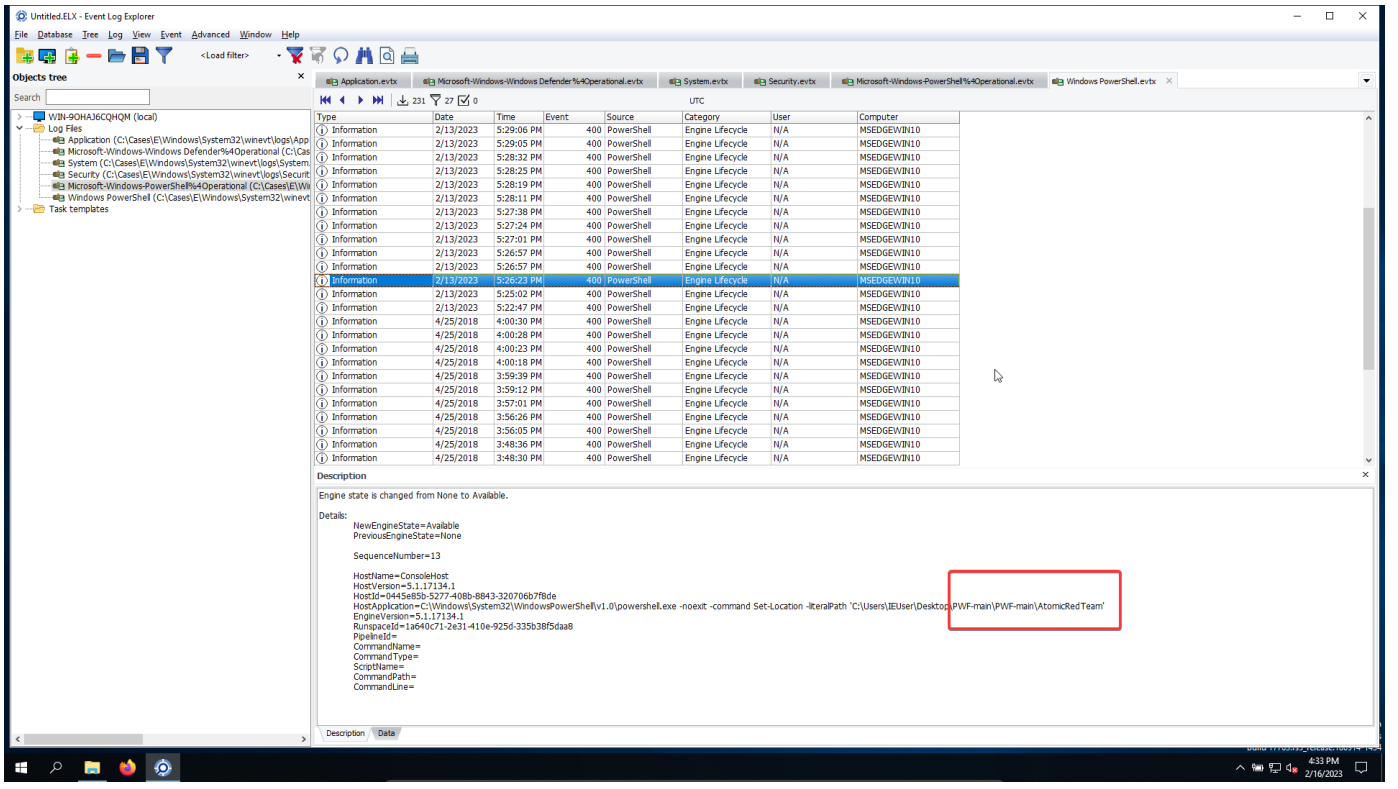
- Important Event ids 4103,4104 for execution analysis, you can gather payloads, commands executed, modules called.

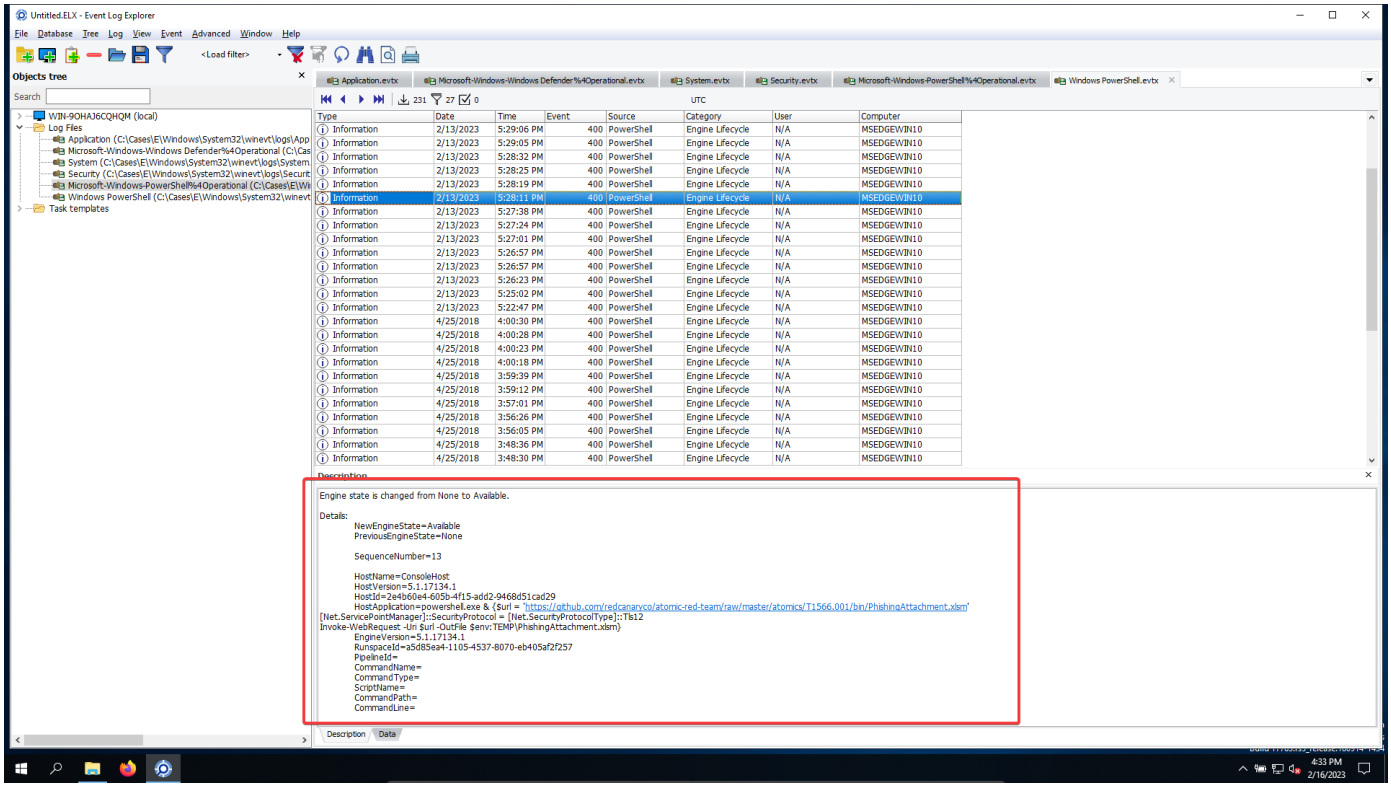


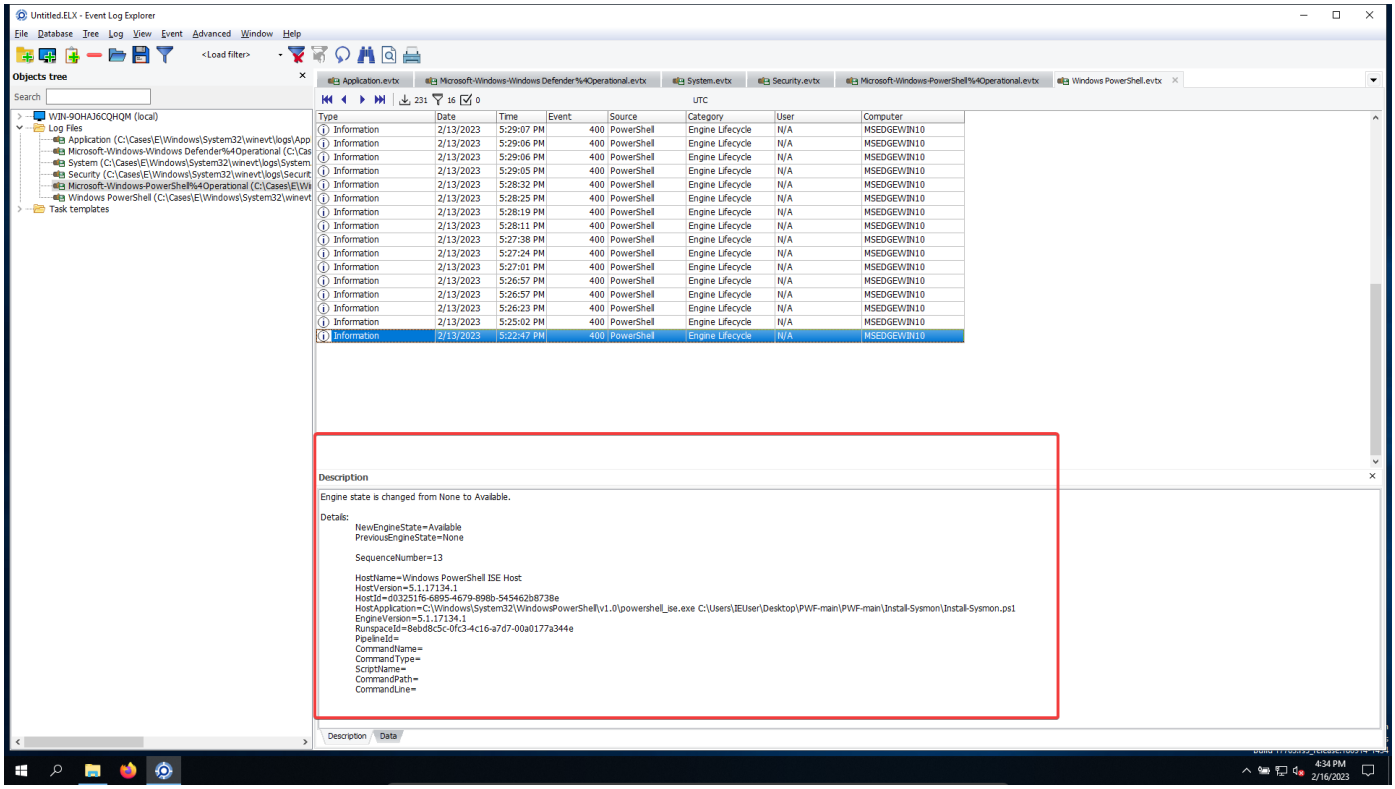
Malicious Powershell

- Search in WIndows PowerShell.evtx, by filtering with Event ID 400:

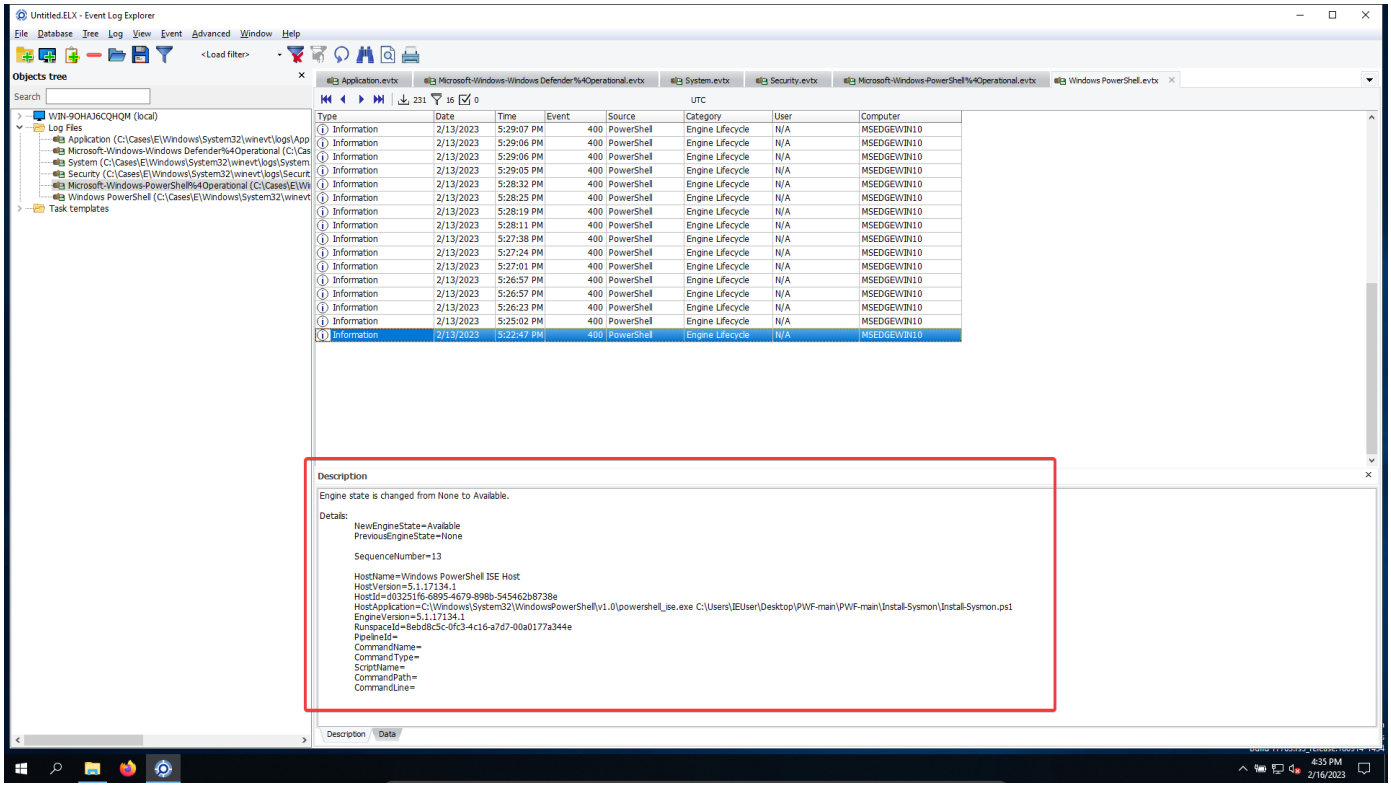




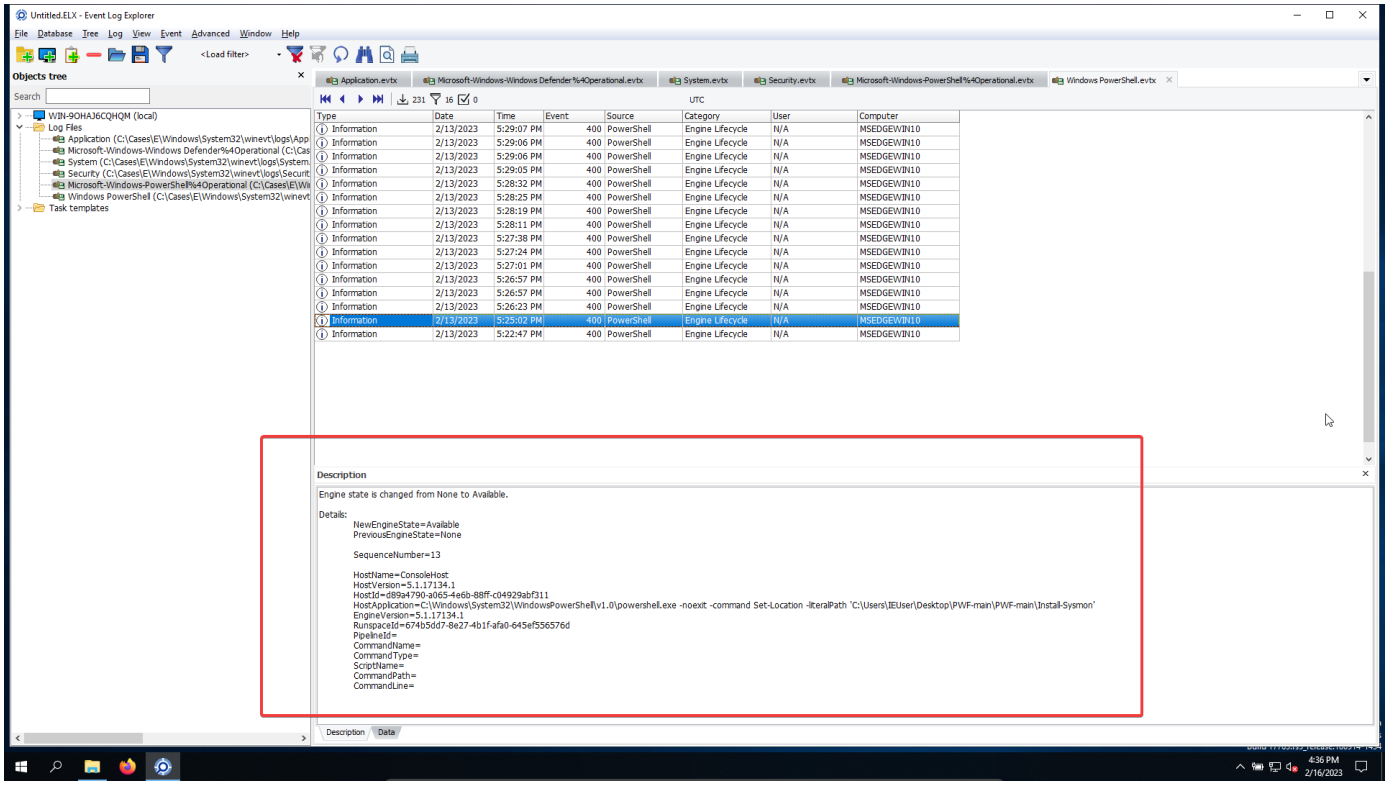




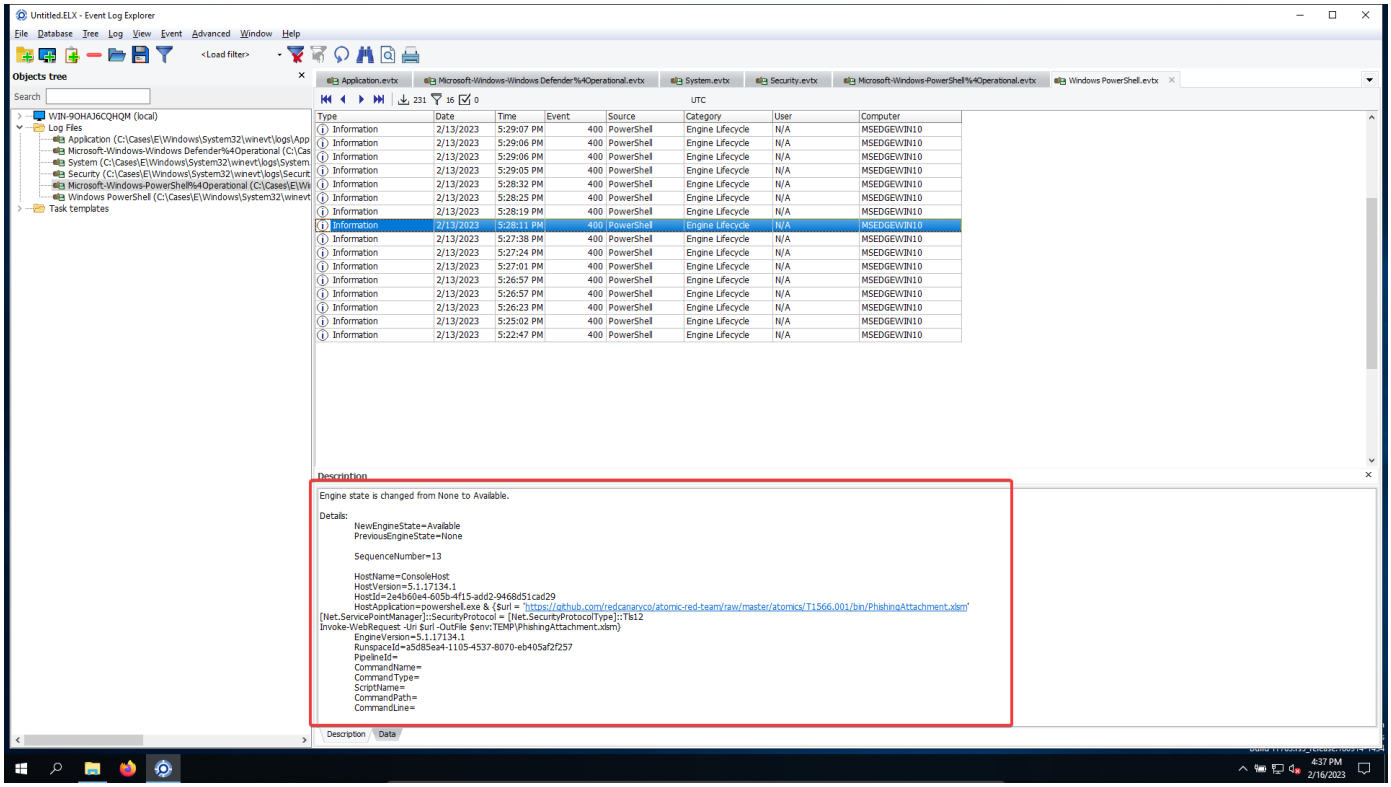
- Execution:
    - Executing powershell from the Sysmon folder:



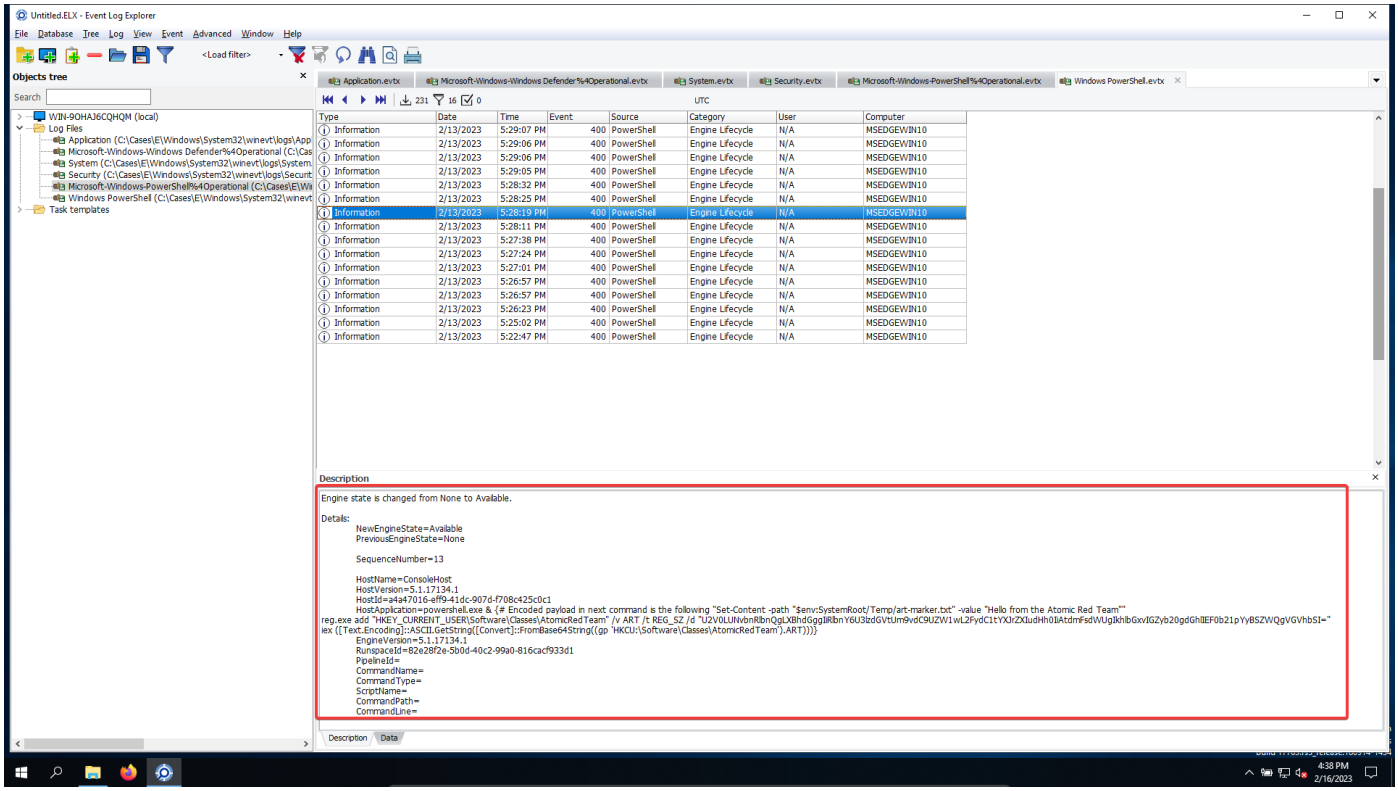
- Executing powershell from the AtomicRedTeam folder:



- Downloading suspicious file from github

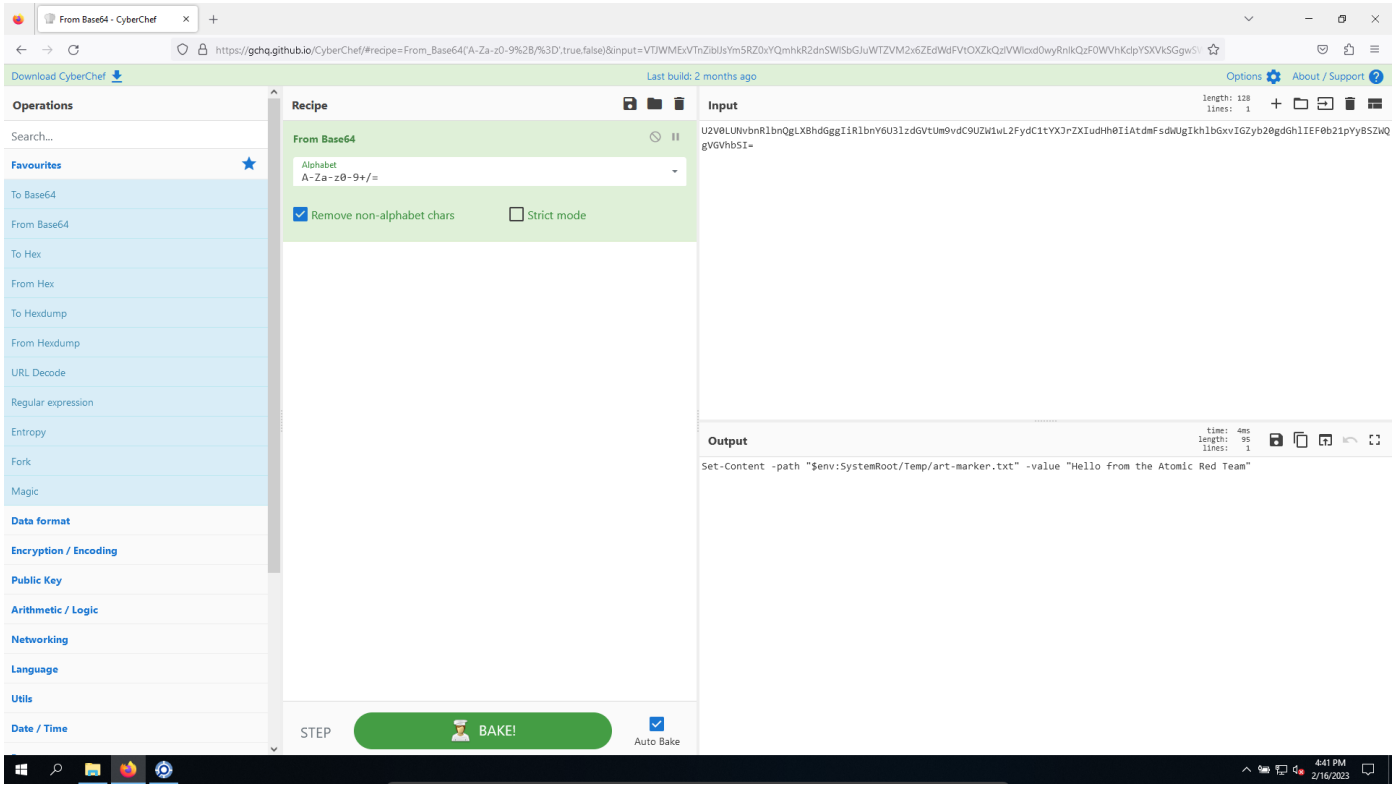


- Fileless attack payload. Registry is being modified .

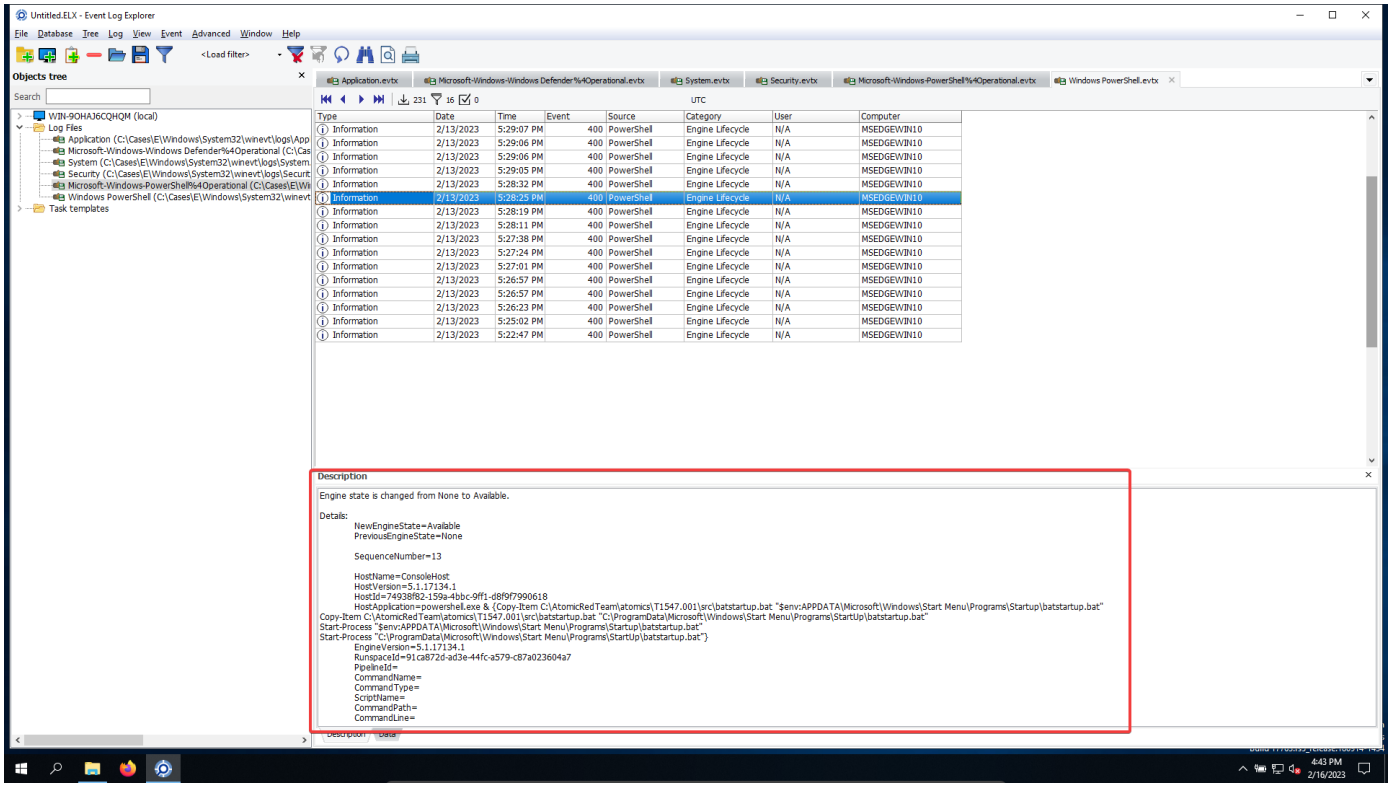


- Going to Cyberchef and decrypting the payload executed by powershell through the registry:

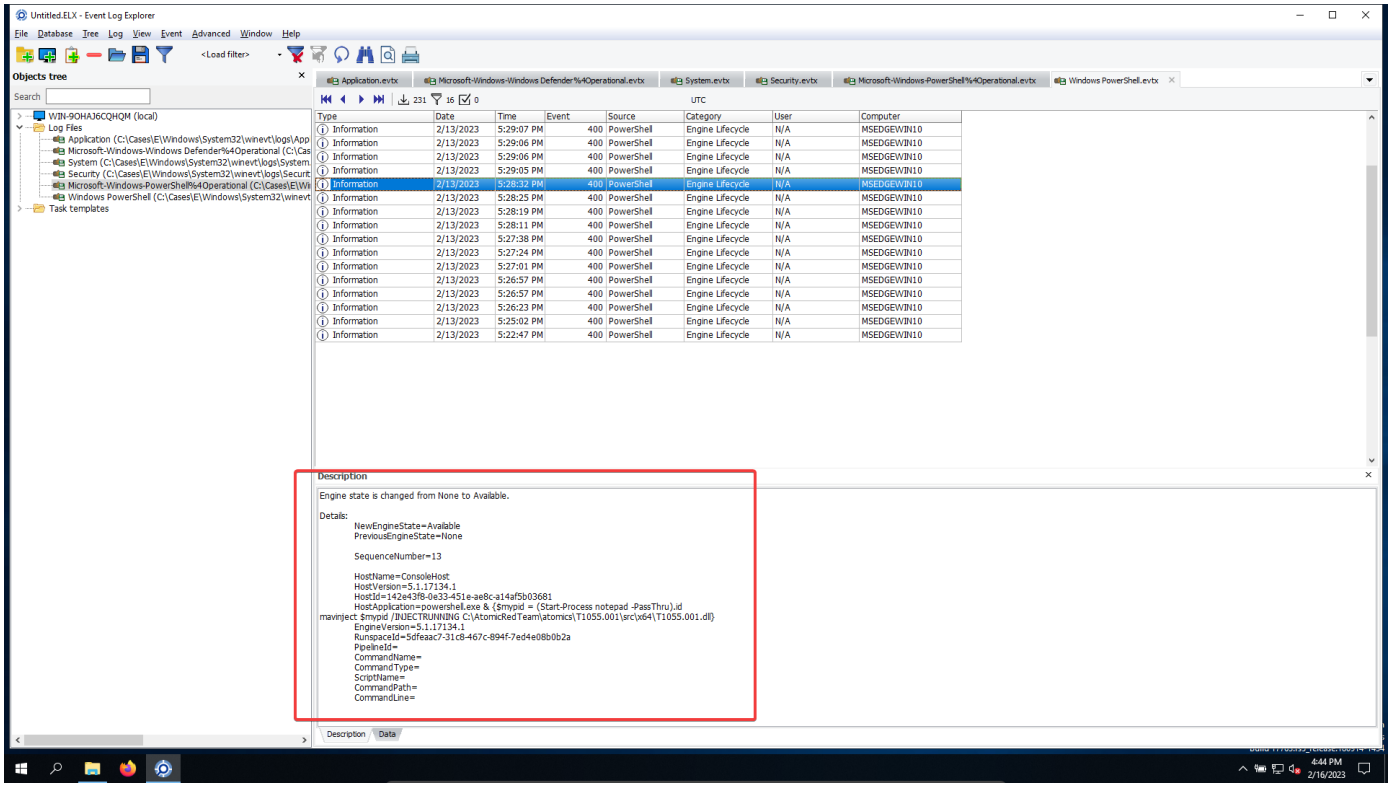
U2V0LUNvbnRlbnQgLXBhdGggIiRlbnY6U3lzdGVtUm9vdC9UZW1wL2FydC1tYXJrZXIudHh0IiAtdmFsdWUgIkhlbGxvIGZyb20gdGhlIEF0b21pYyBSZWQgVGVhbSI=



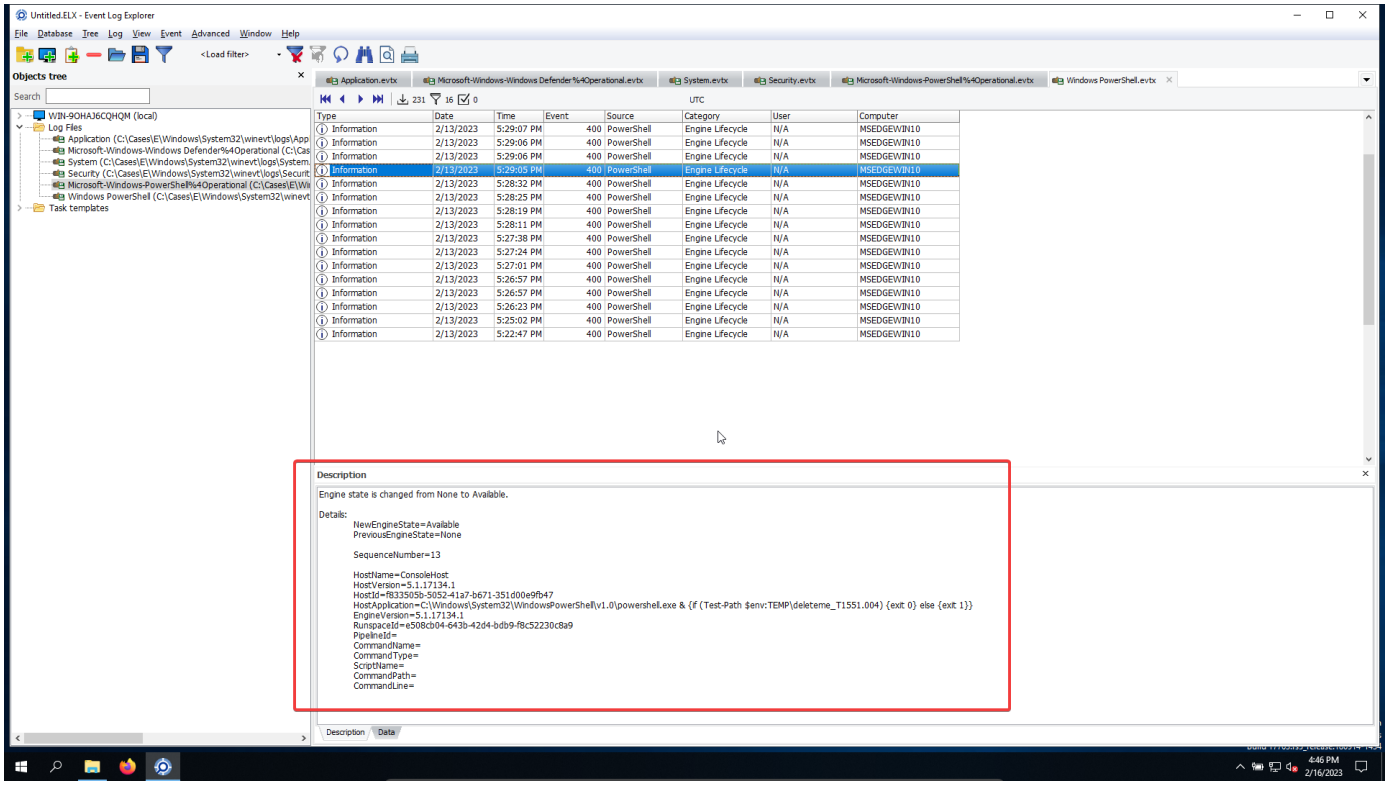
- Persistence mechanism for startup flder



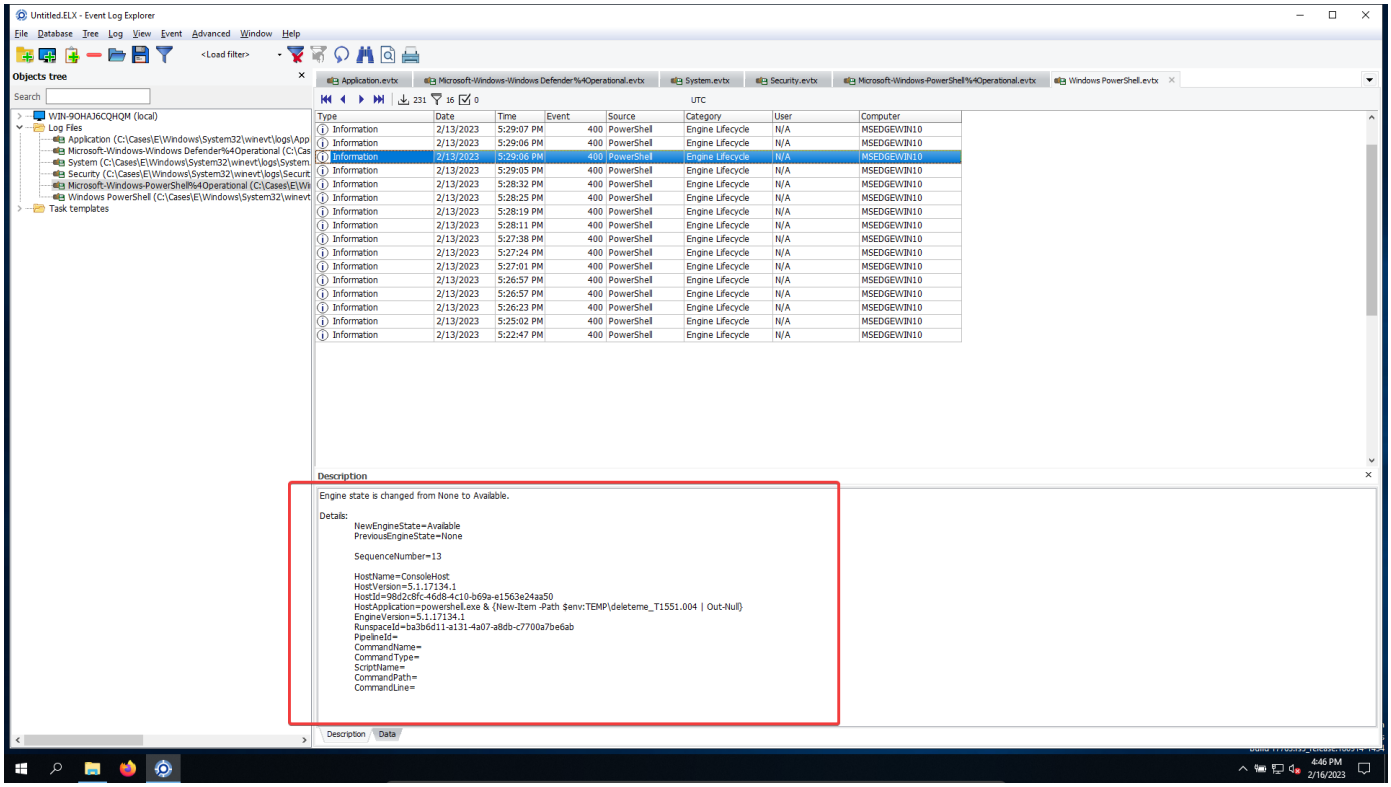
- Process Injection via mavinject.



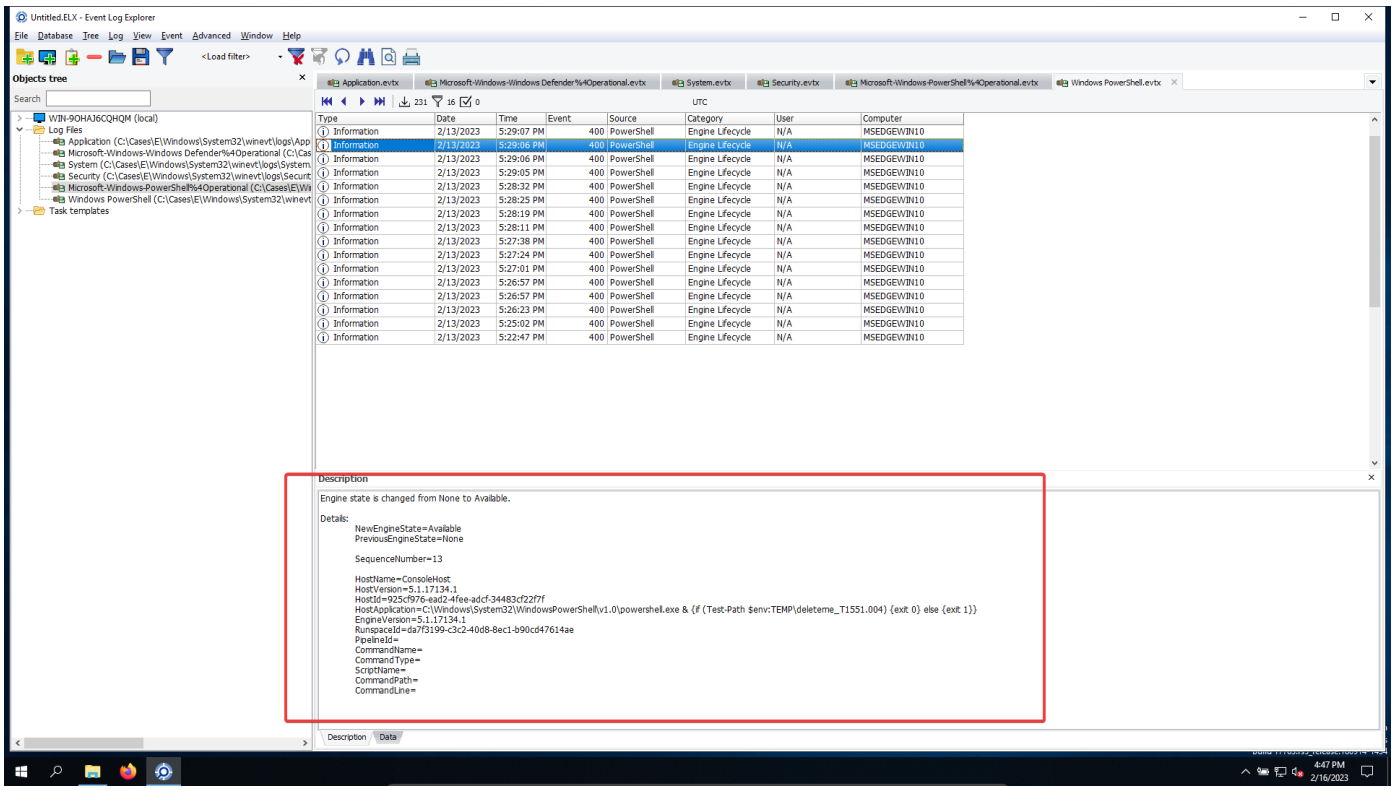
- Testing if the file exists:



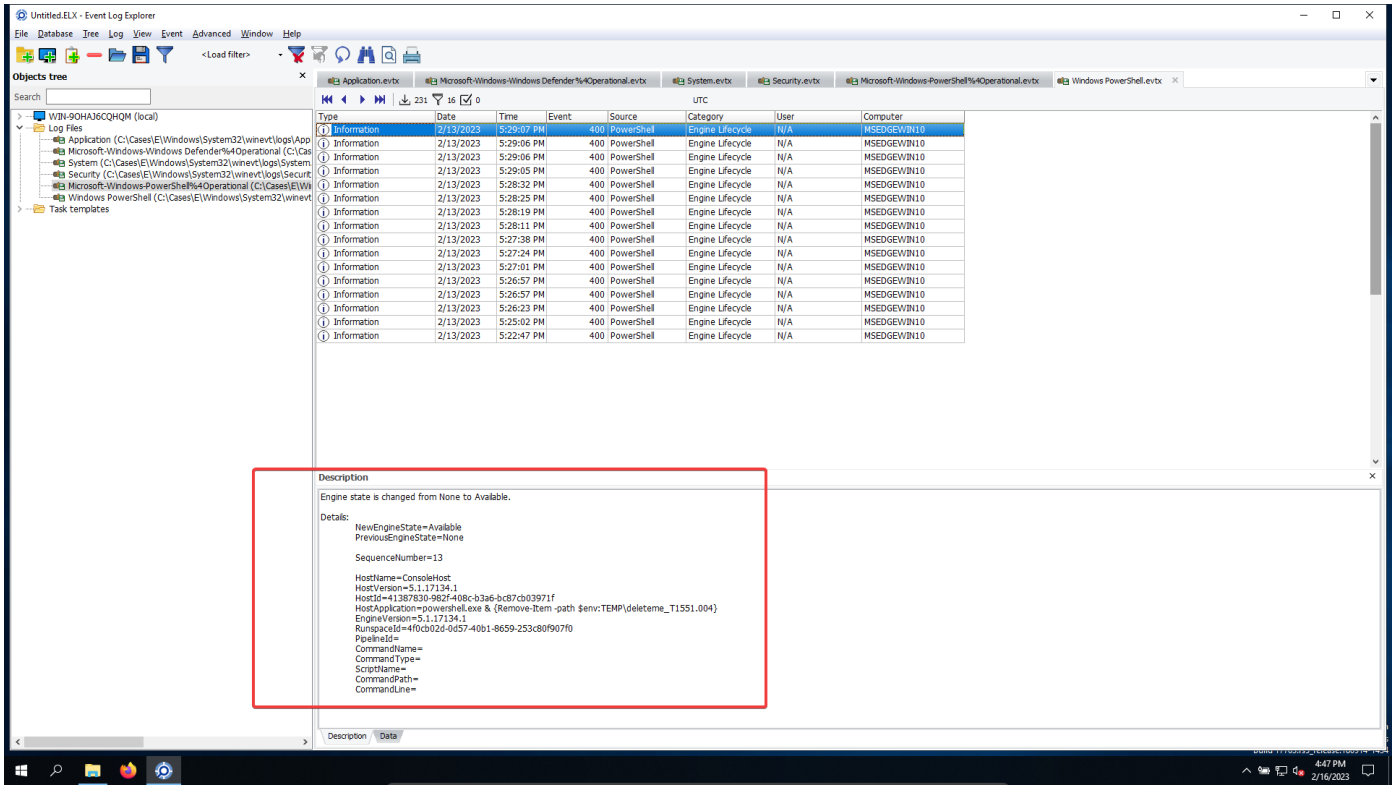
- Creating the file



- File check



- Delete the file

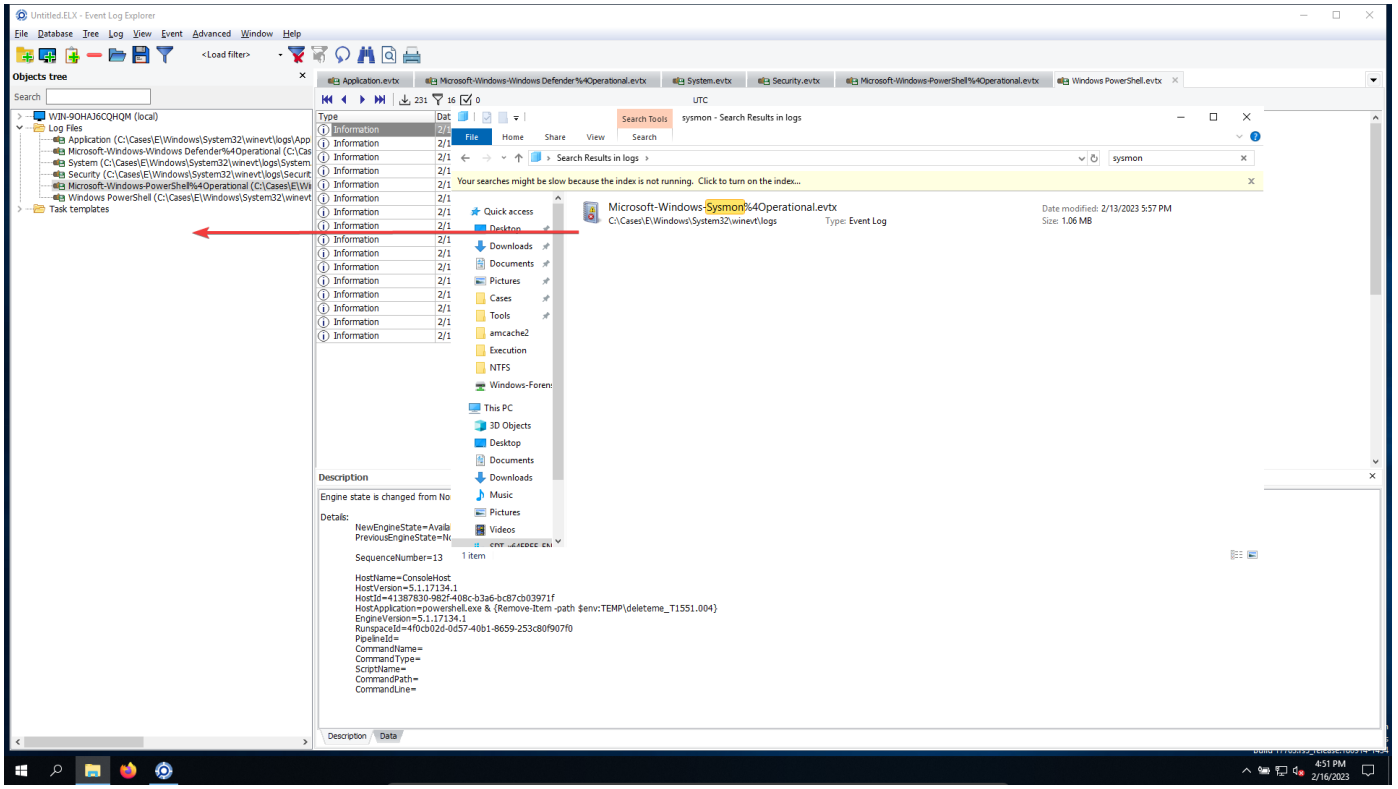


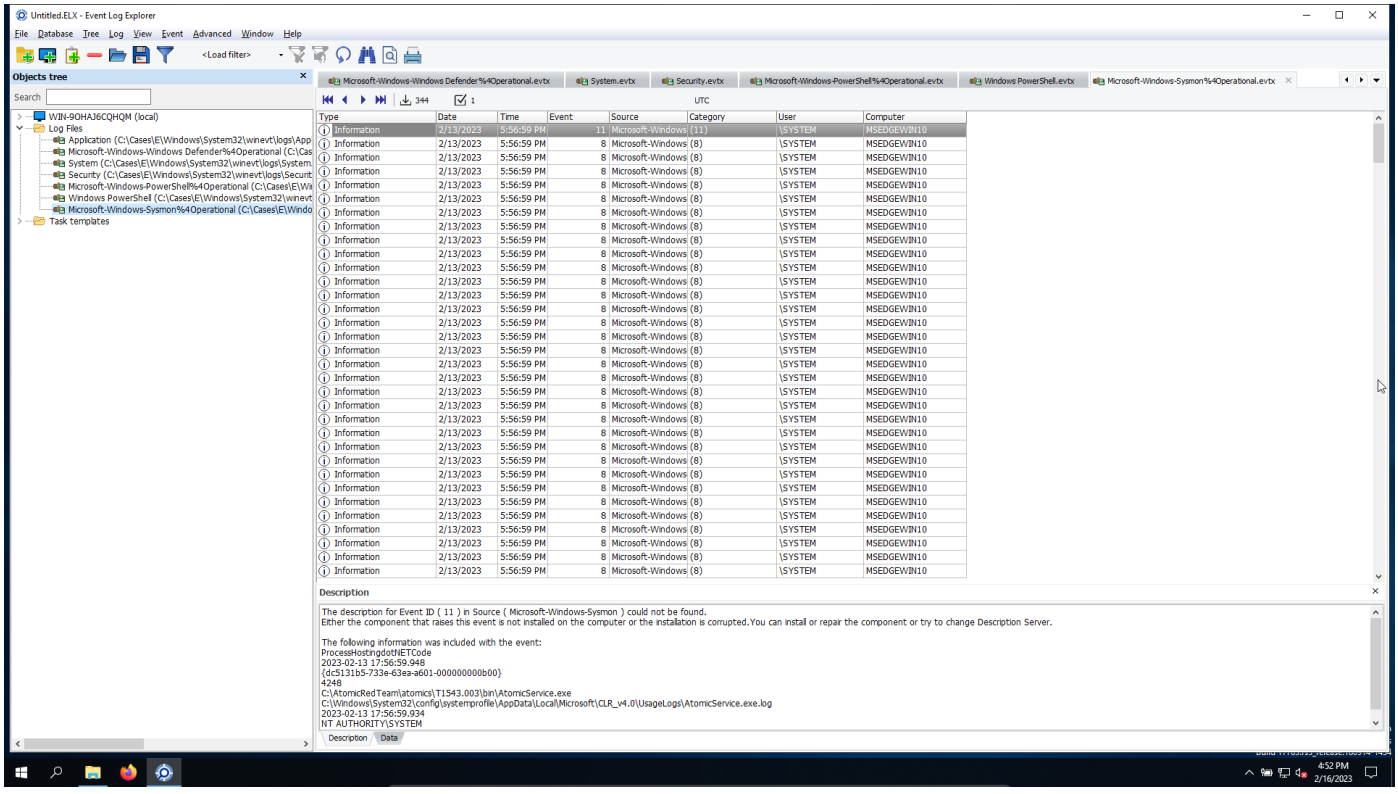
- Summary of deleteme file : If the file didn't existed, create it, if it existed, remove it.

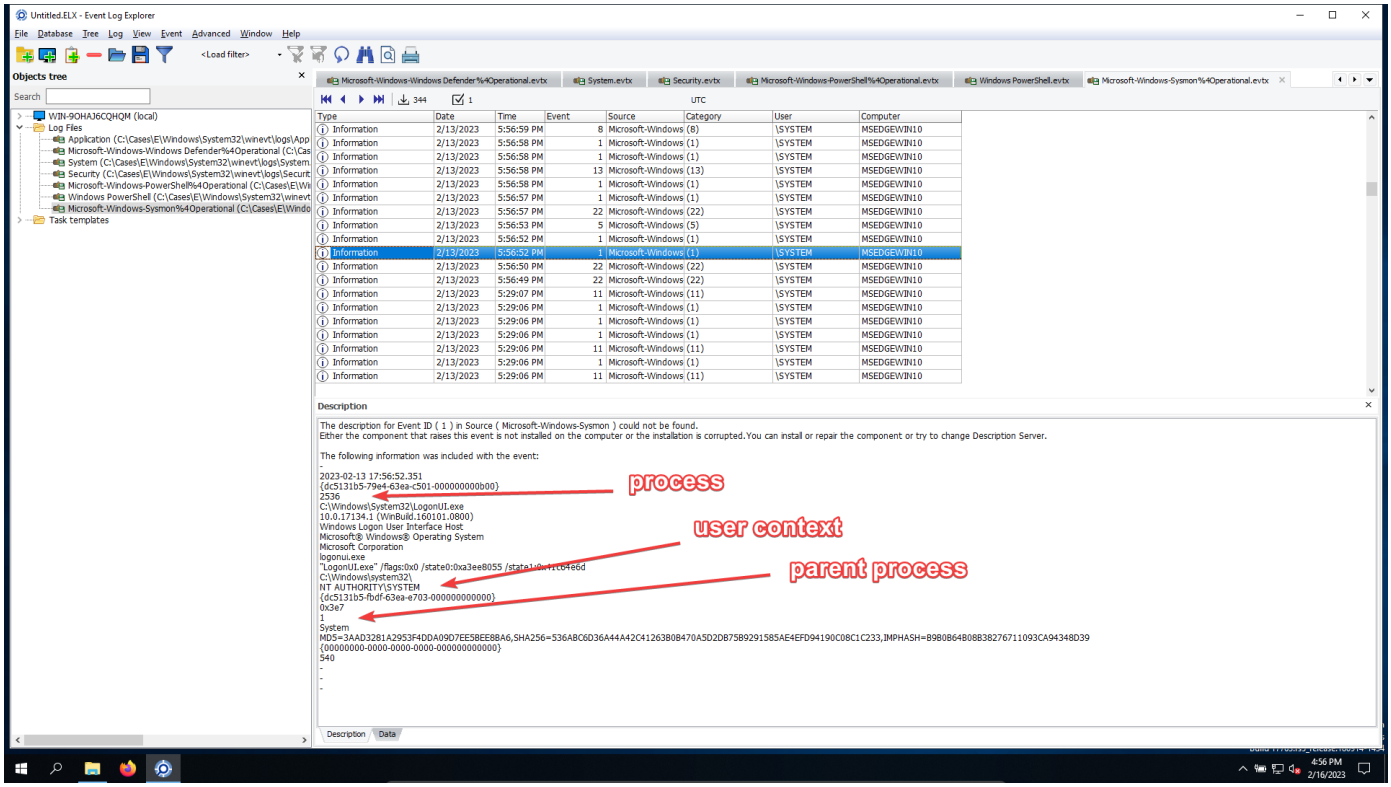
Sysmon & Malicious Sysmon

- Event IDs for Microsoft-Windows-Sysmon:
  - 1: Process creation
  - 3: Network creation
  - 11: File creation
  - 12,13: Registry events
  - 22: DNS query

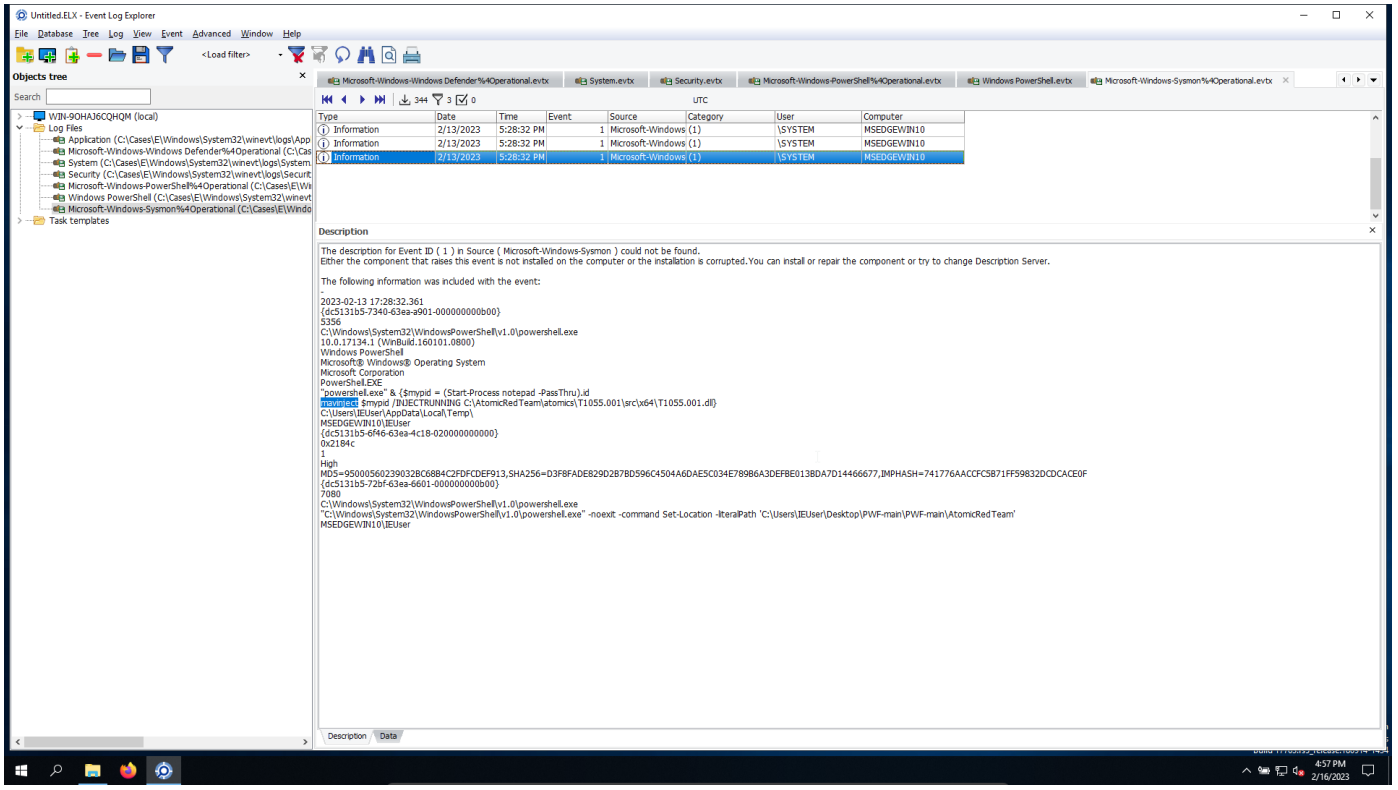
- Load the Sysmon evtx:

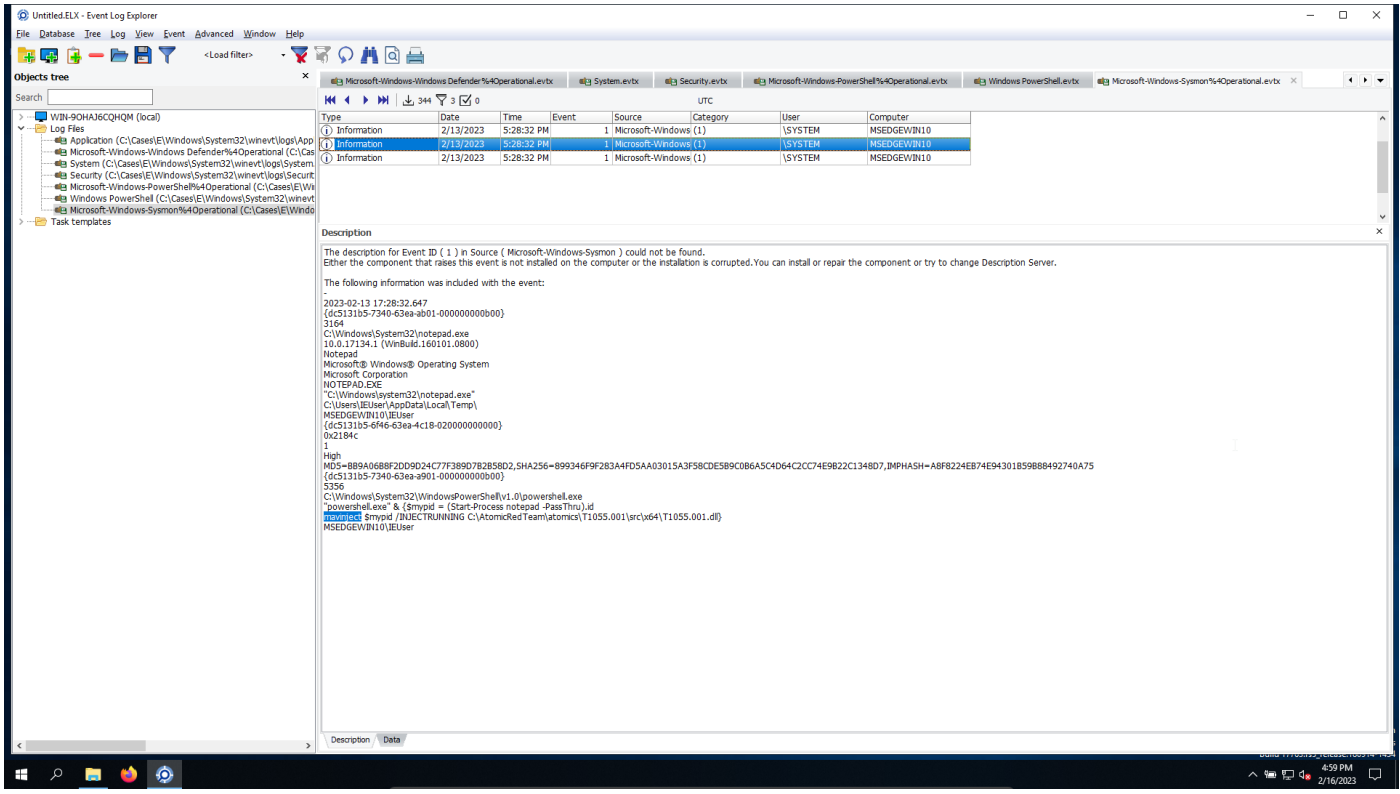

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Microsoft-Windows-PowerShell%4Operational (C:\Cases\E\Wi
Windows PowerShell (C:\Cases\E\Windows\System32\winevt
Task templates
Application.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Windows PowerShell.evtx
Type
Information
Search Tools
sysmon - Search Results in logs
File Home Share View Search
Search Results in logs
sysmon
Your searches might be slow because the index is not running. Click to turn on the index...
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
amcache2
Execution
NTFS
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Microsoft-Windows-Sysmon%4Operational.evtx
C:\Cases\E\Windows\System32\winevt\logs
Type: Event Log
Date modified: 2/13/2023 5:57 PM
Size: 1.06 MB
1 item
Description
Engine state is changed from No
Details:
NewEngineState=Availa
PreviousEngineState=N
SequenceNumber=13
HostName=ConsoleHost
HostVersion=5.1.17134.1
HostId=41387830-982f-408c-b3a6-bc87cb03971f
HostApplication=powershell.exe & {Remove-Item -path $env:TEMP\deleteme_T1551.004}
EngineVersion=5.1.17134.1
RunspaceId=4f0cb02d-0d57-40b1-8659-253c80f907f0
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
Description
Data
4:51 PM
2/16/2023

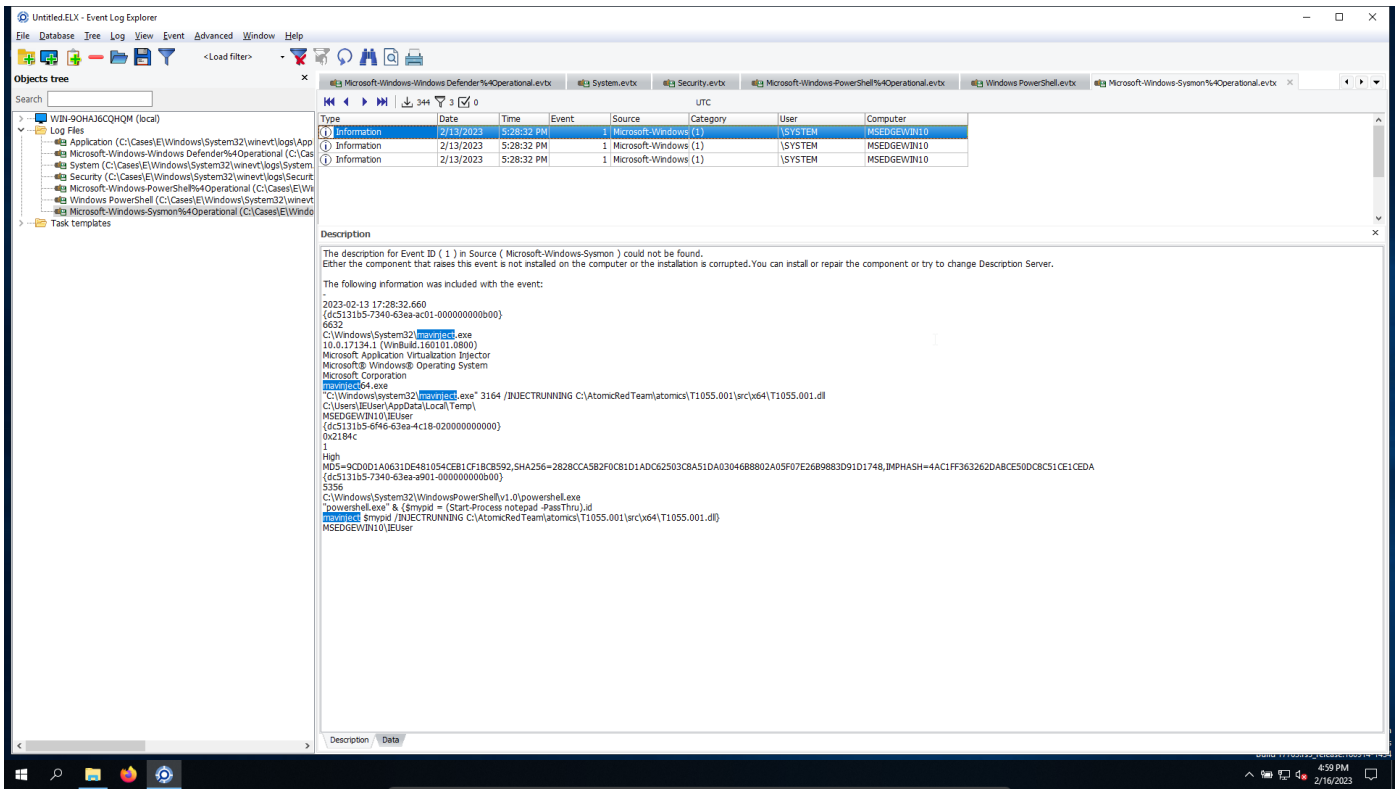

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Microsoft-Windows-PowerShell%4Operational (C:\Cases\E\Wi
Windows PowerShell (C:\Cases\E\Windows\System32\winevt
Microsoft-Windows-Sysmon%4Operational (C:\Cases\E\Windo
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Windows PowerShell.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:56:59 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:56:59 PM 8 Microsoft-Windows (8) \SYSTEM MSEDGEWIN10
Description
The description for Event ID (11) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
ProcessHostingdotNETCode
2023-02-13 17:56:59.948
{dc5131b5-733e-63ea-a601-000000000b00}
4248
C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log
2023-02-13 17:56:59.934
NT AUTHORITY\SYSTEM
Description
Data
4:52 PM
2/16/2023



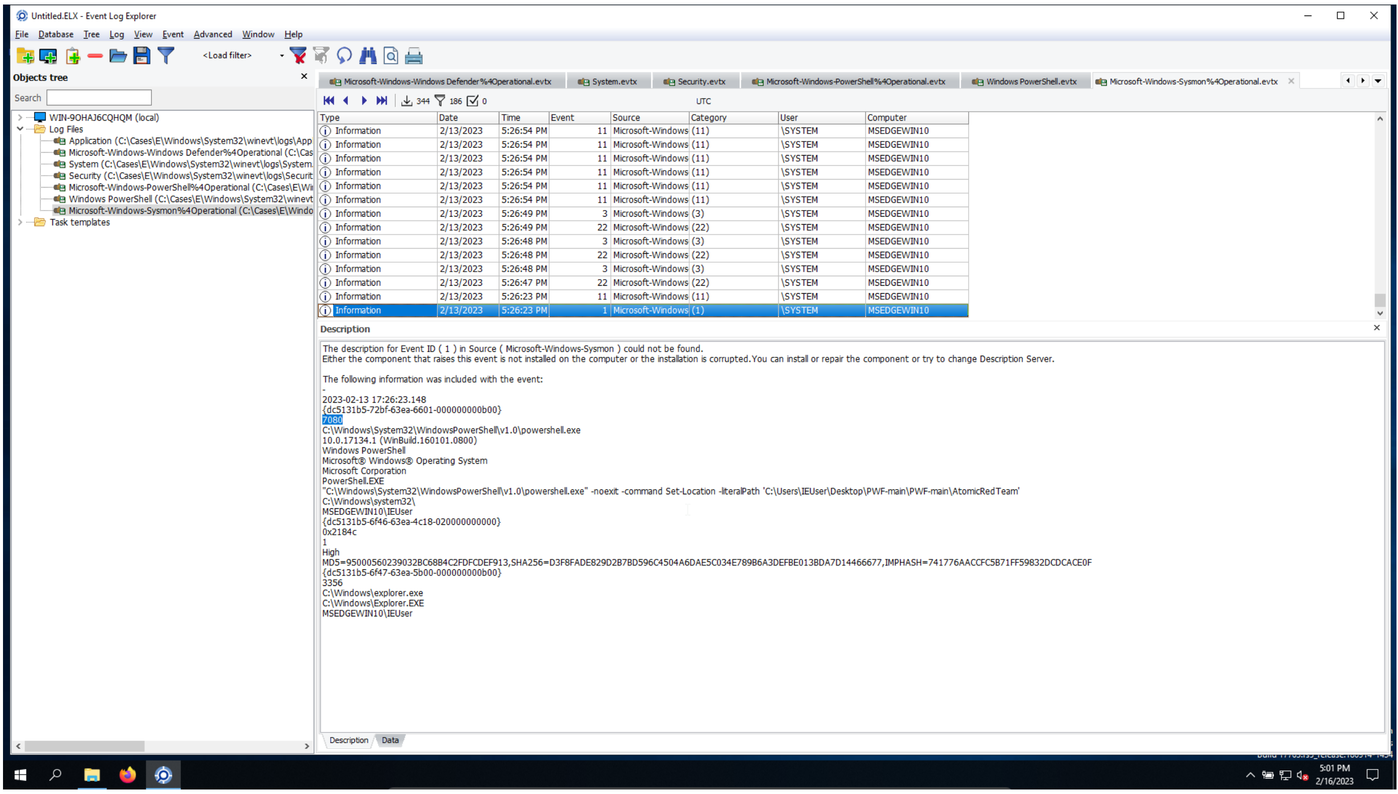
- Search mavinject process with eventid 1, process injection order of execution:

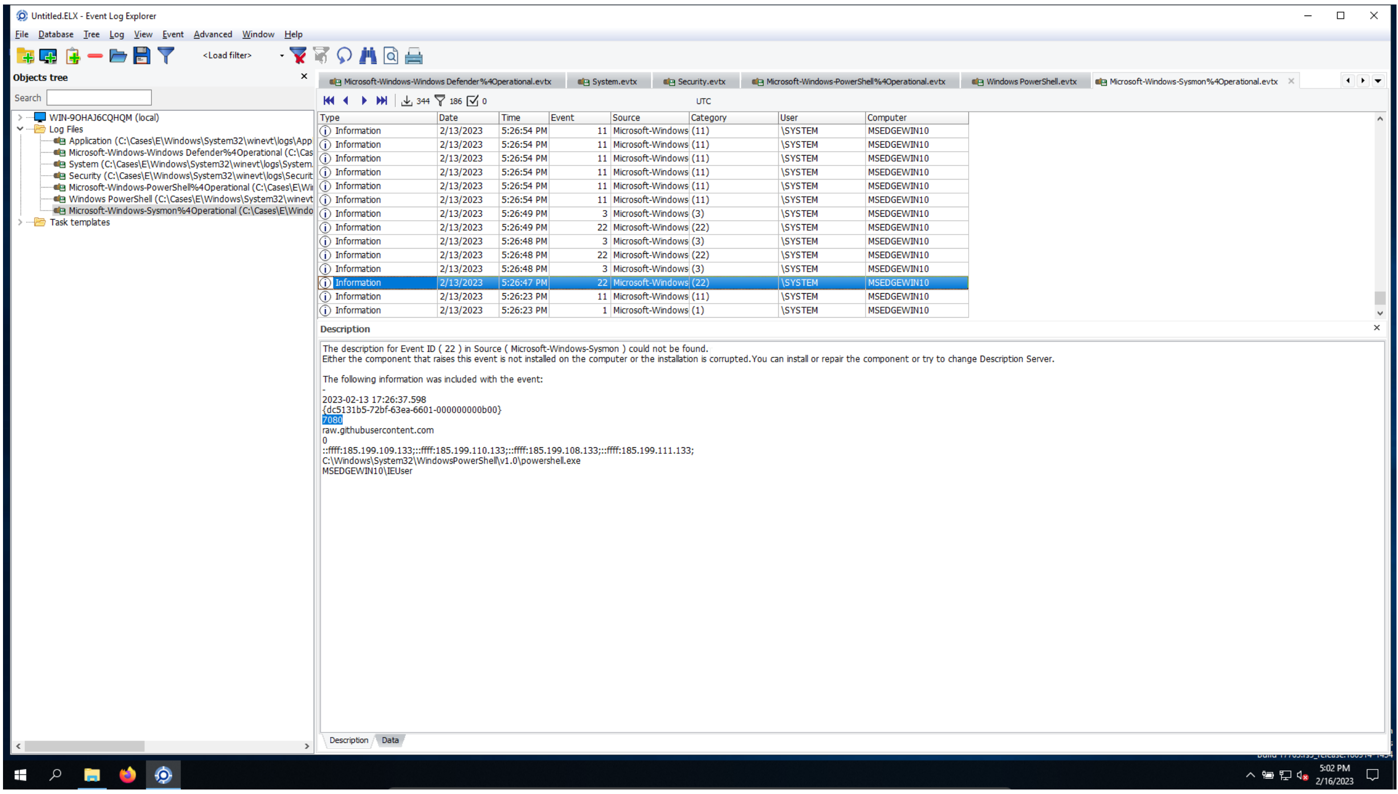


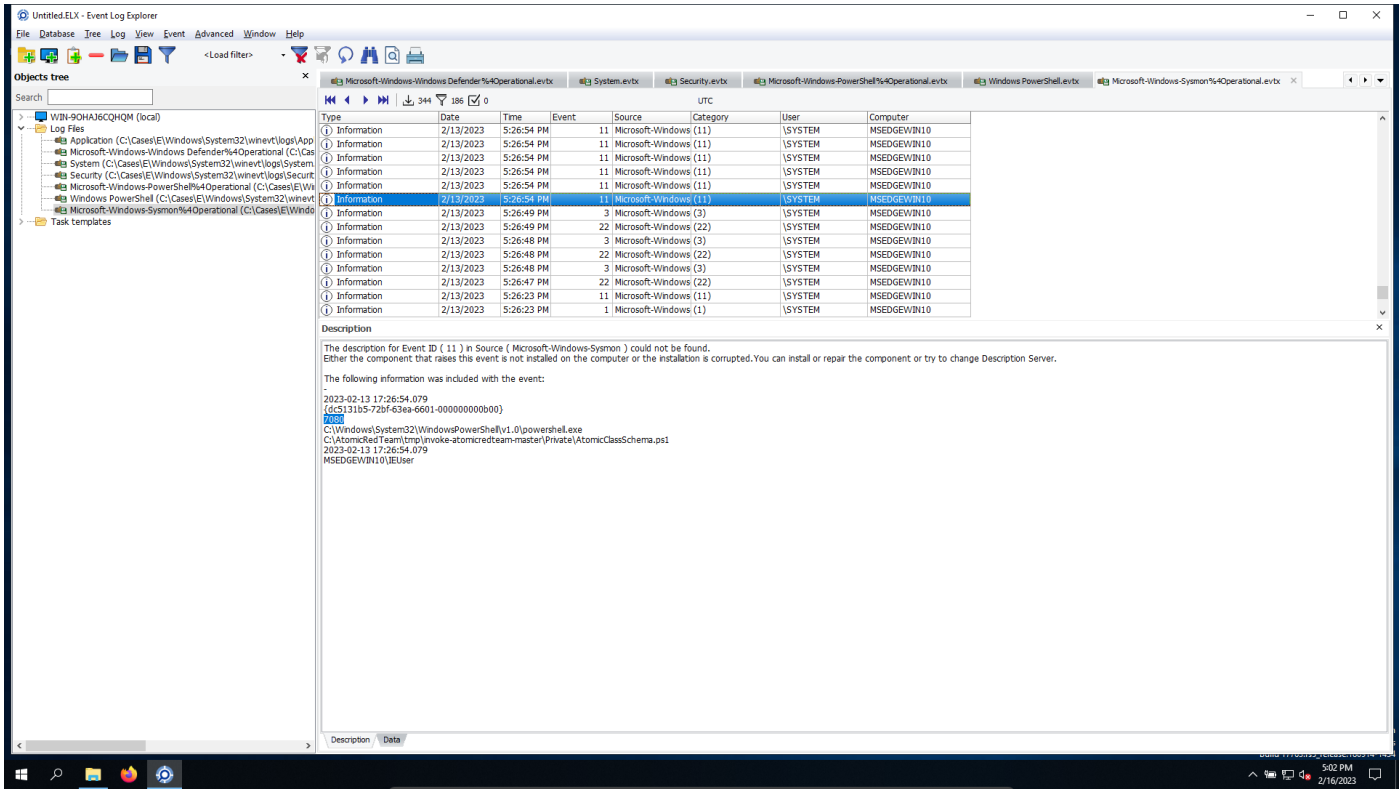




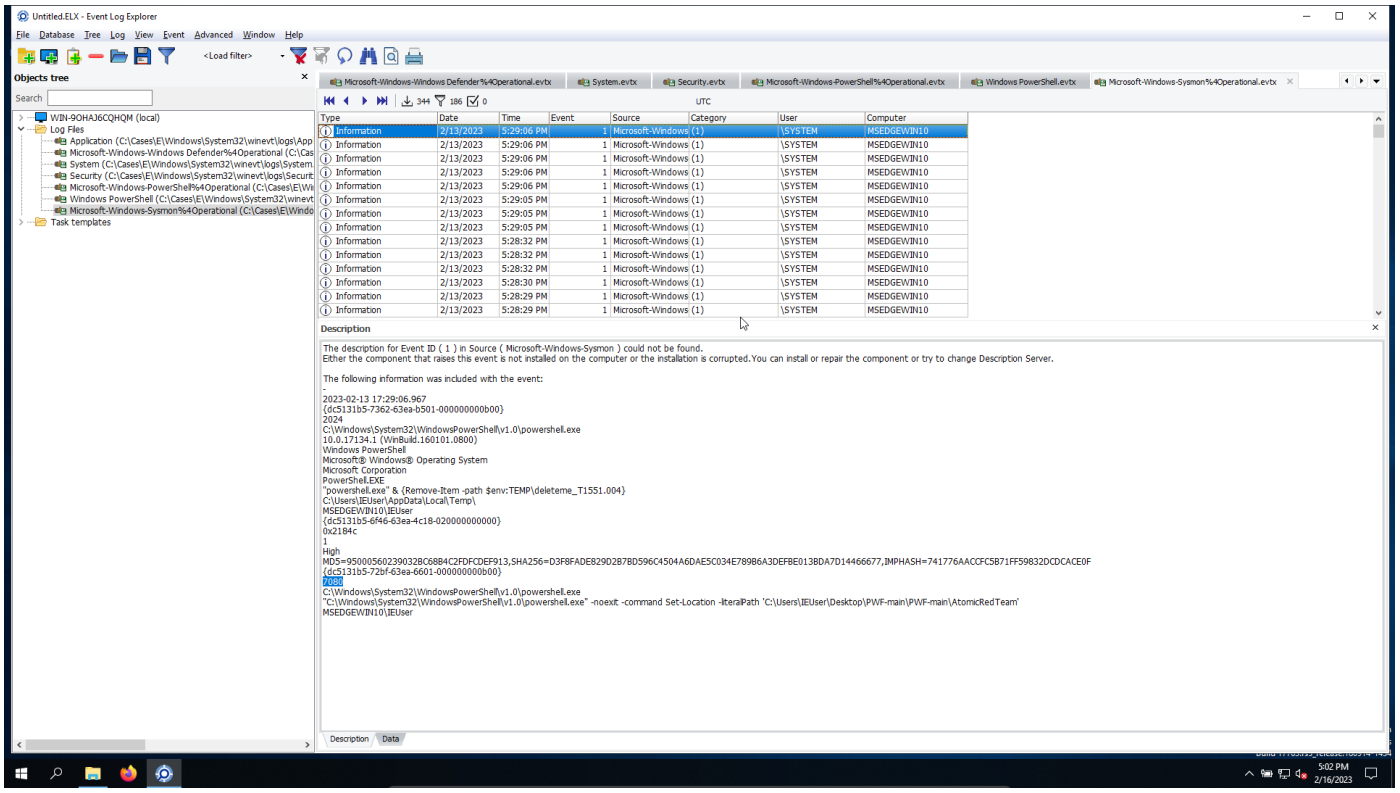
- Search everything based on parent process id: 7080, beggining of the attack:

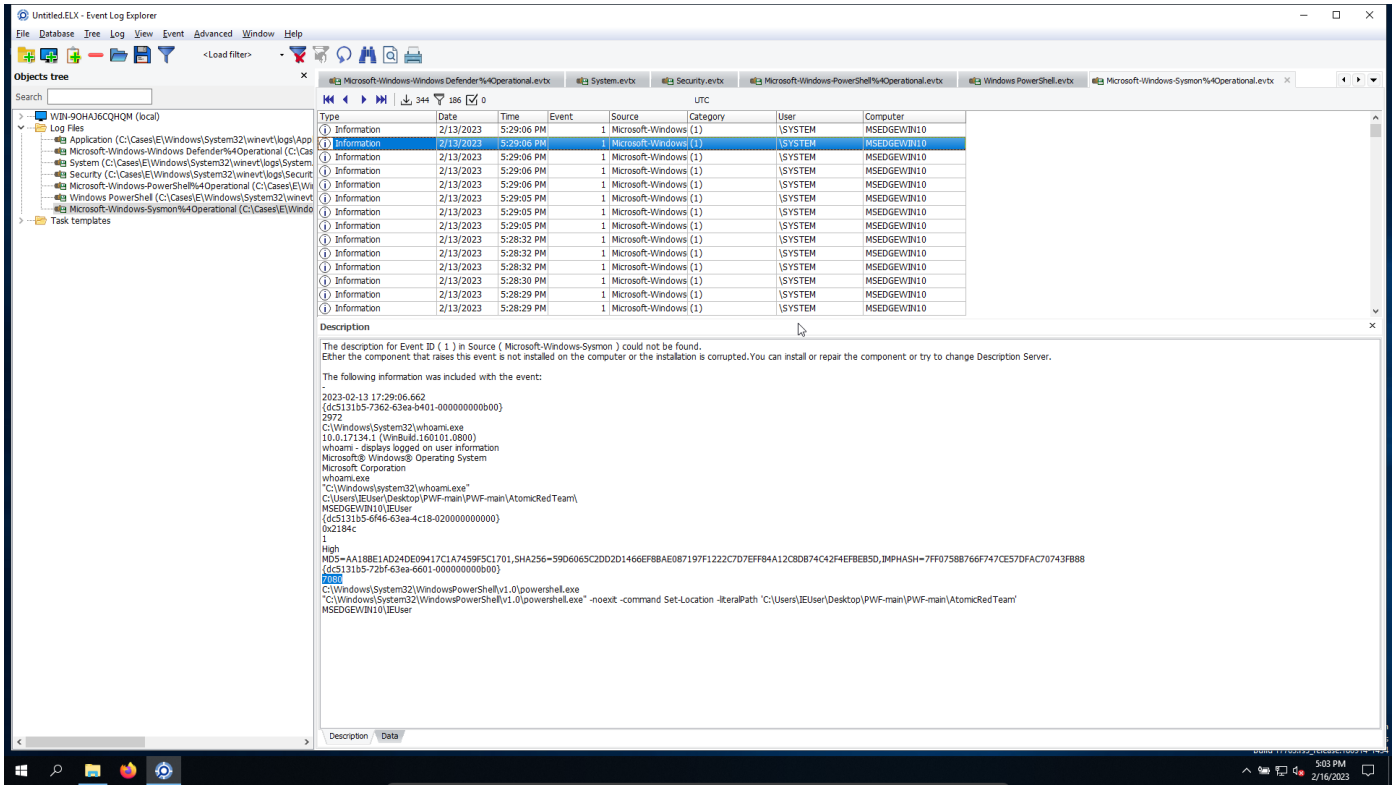

Untitled.ELX - Event Log Explorer
Description
The description for Event ID (1) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
-
2023-02-13 17:26:23.148
{dc5131b5-72bf-63ea-6601-000000000b00}
7080
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17134.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit -command Set-Location -literalPath 'C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam'
C:\Windows\system32\
MSEDGEWIN10\IEUser
{dc5131b5-6f46-63ea-4c18-020000000000}
0x2184c
1
High
MD5=95000560239032BC68B4C2FDFCDEF913,SHA256=D3F8FADE829D2B7BD596C4504A6DAE5C034E789B6A3DEFBE013BDA7D14466677,IMPHASH=741776AACCFC5B71FF59832DCDCACE0F
{dc5131b5-6f47-63ea-5b00-000000000b00}
3356
C:\Windows\explorer.exe
C:\Windows\Explorer.EXE
MSEDGEWIN10\IEUser

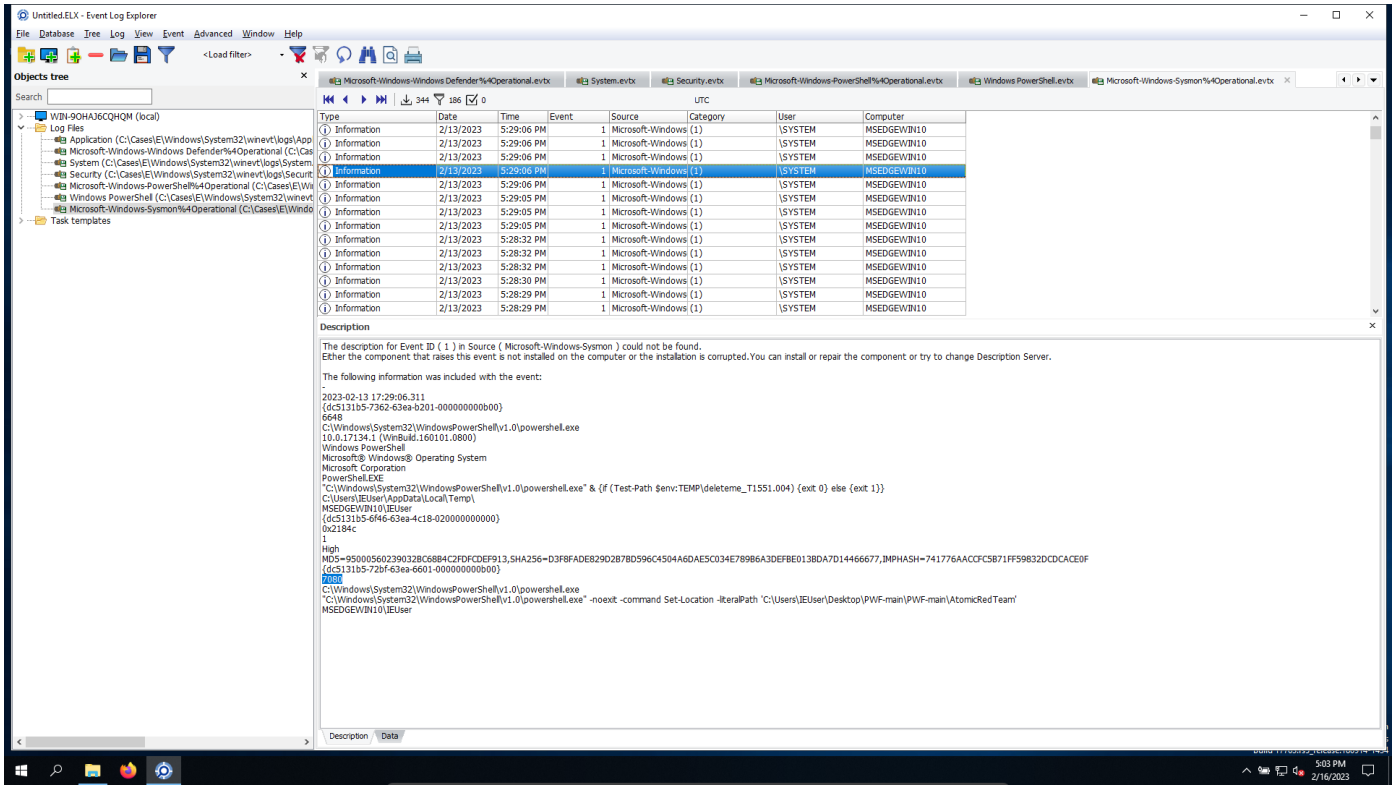

Untitled.ELX - Event Log Explorer
Description
The description for Event ID (22) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
-
2023-02-13 17:26:37.598
{dc5131b5-72bf-63ea-6601-000000000b00}
7080
raw.githubusercontent.com
0
::ffff:185.199.109.133;::ffff:185.199.110.133;::ffff:185.199.108.133;::ffff:185.199.111.133;
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
MSEDGEWIN10\IEUser

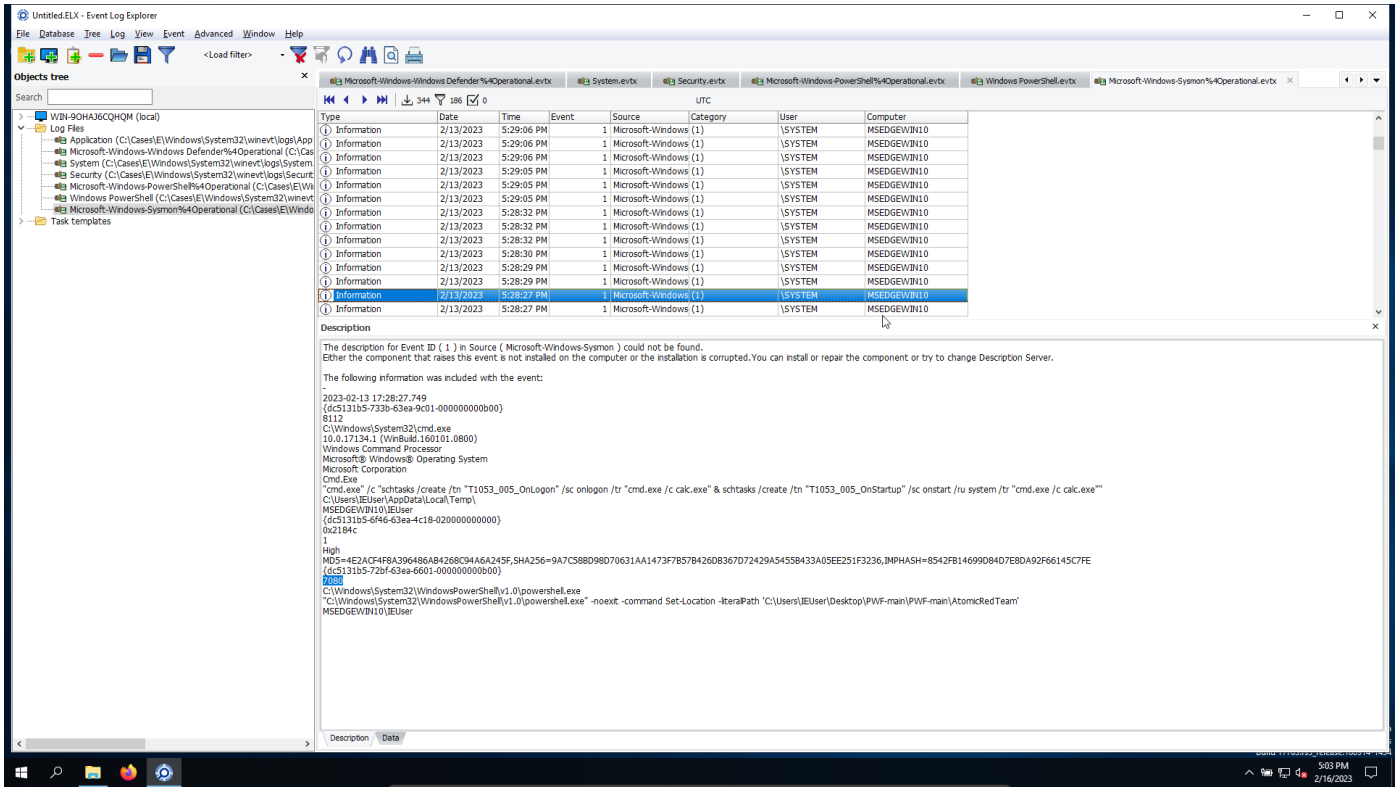


- End of the attack:

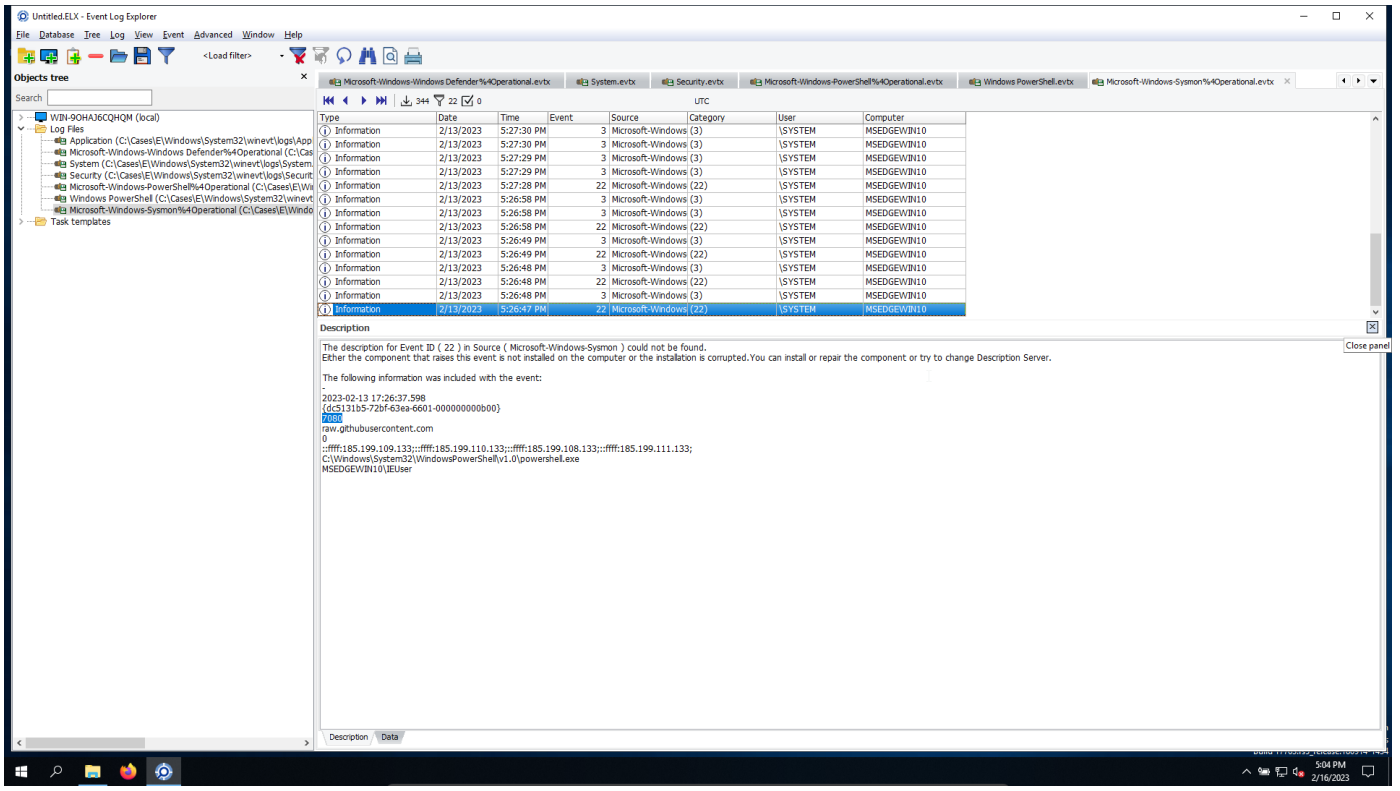


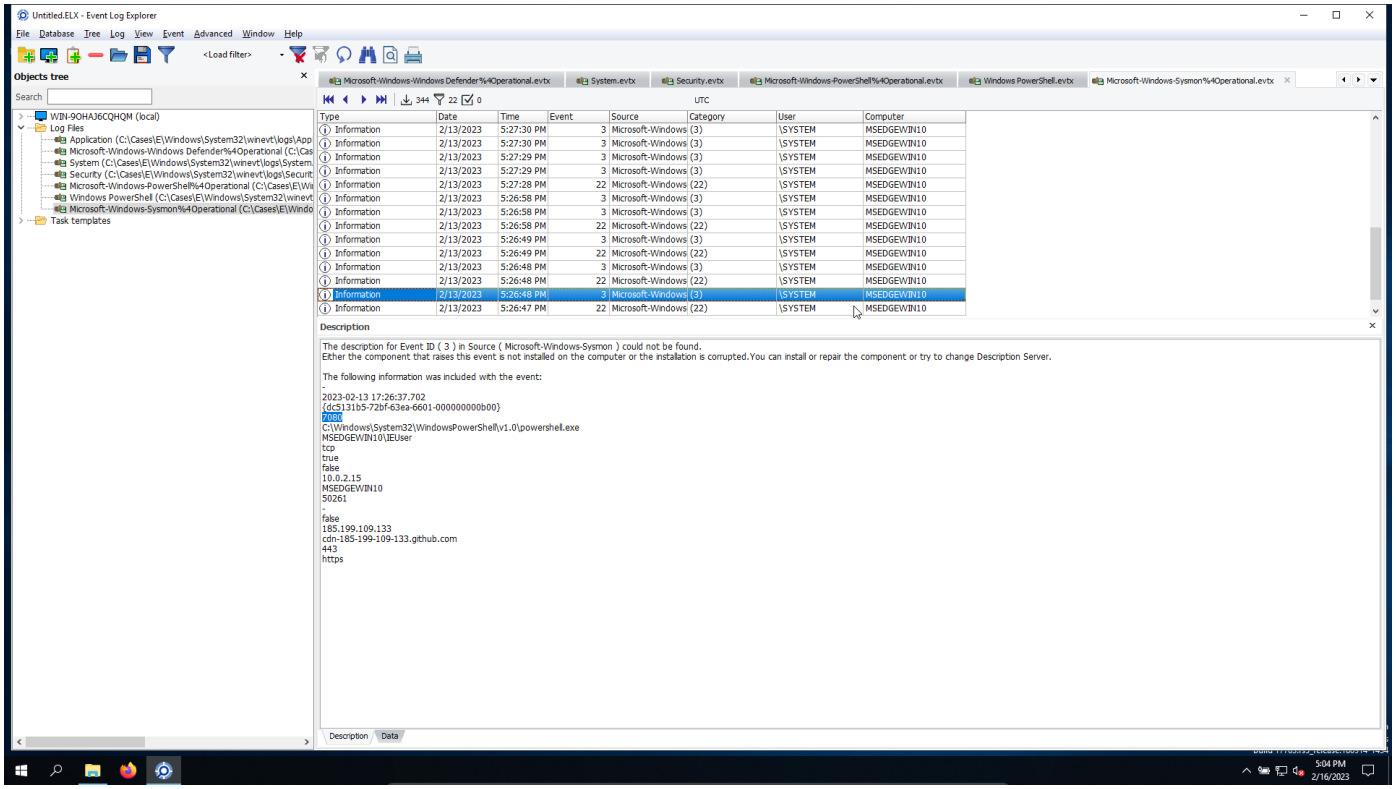

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Microsoft-Windows-PowerShell%4Operational (C:\Cases\E\Wi
Windows PowerShell (C:\Cases\E\Windows\System32\winevt
Microsoft-Windows-Sysmon%4Operational (C:\Cases\E\Windo
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Windows PowerShell.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:29:06 PM 1 Microsoft-Windows (1) \SYSTEM MSEDGEWIN10
Description
The description for Event ID (1) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
2023-02-13 17:29:06.662
{dc5131b5-7362-63ea-b401-000000000b00}
2972
C:\Windows\System32\whoami.exe
10.0.17134.1 (WinBuild.160101.0800)
whoami - displays logged on user information
Microsoft® Windows® Operating System
Microsoft Corporation
whoami.exe
"C:\Windows\system32\whoami.exe"
C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\
MSEDGEWIN10\IEUser
{dc5131b5-6f46-63ea-4c18-020000000000}
0x2184c
1
High
MD5=AA18BE1AD24DE09417C1A7459F5C1701,SHA256=59D6065C2DD2D1466EF8BAE087197F1222C7D7EFF84A12C8DB74C42F4EFBEB5D,IMPHASH=7FF0758B766F747CE57DFAC70743FB88
{dc5131b5-72bf-63ea-6601-000000000b00}
7084
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit -command Set-Location -literalPath 'C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam'
MSEDGEWIN10\IEUser
Description
Data
5:03 PM
2/16/2023

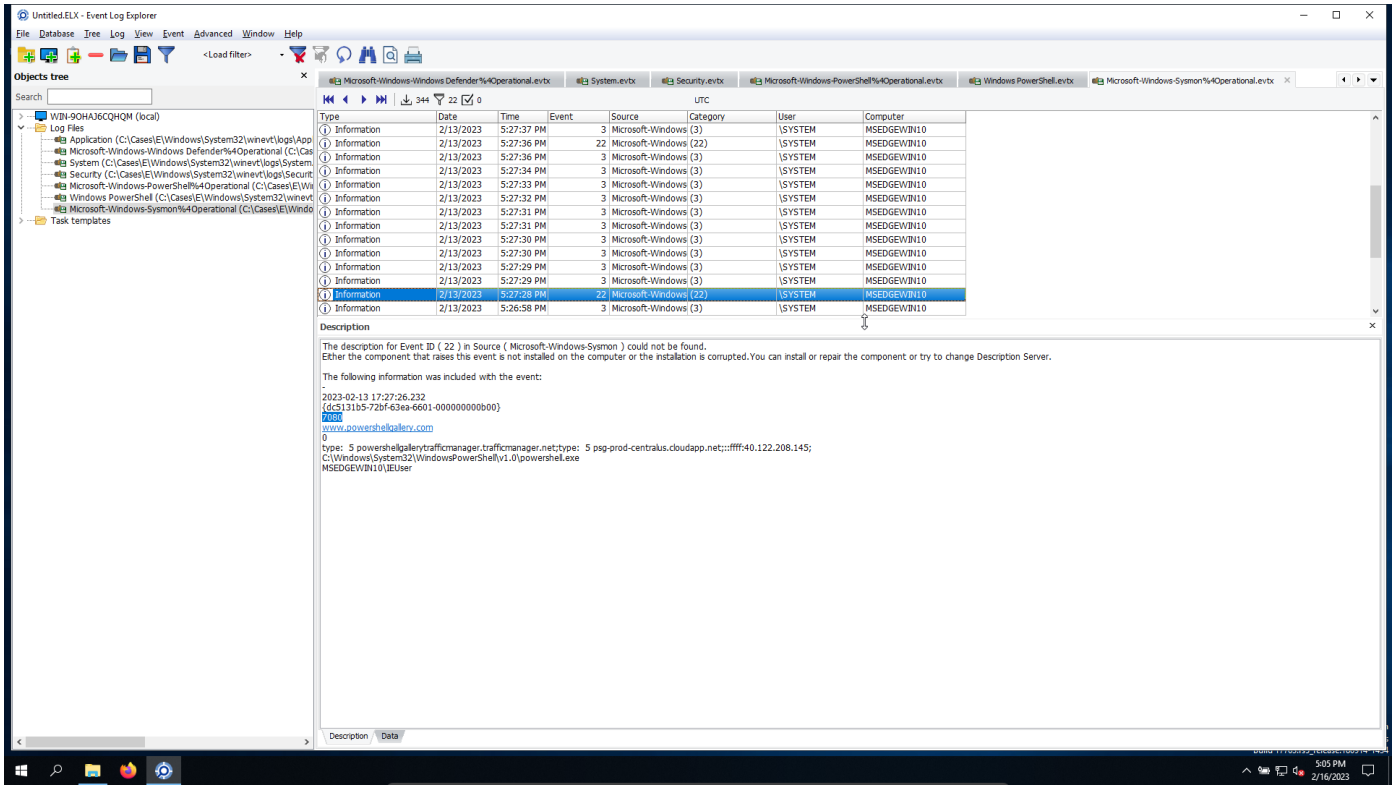

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Microsoft-Windows-PowerShell%4Operational (C:\Cases\E\Wi
Windows PowerShell (C:\Cases\E\Windows\System32\winevt
Microsoft-Windows-Sysmon%4Operational (C:\Cases\E\Windo
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Windows PowerShell.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:29:06 PM 1 Microsoft-Windows (1) \SYSTEM MSEDGEWIN10
Description
The description for Event ID (1) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
2023-02-13 17:29:06.311
{dc5131b5-7362-63ea-b201-000000000b00}
6648
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17134.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & {if (Test-Path $env:TEMP\deleteme_T1551.004) {exit 0} else {exit 1}}
C:\Users\IEUser\AppData\Local\Temp\
MSEDGEWIN10\IEUser
{dc5131b5-6f46-63ea-4c18-020000000000}
0x2184c
1
High
MD5=95000560239032BC68B4C2FDFCDEF913,SHA256=D3F8FADE829D2B7BD596C4504A6DAE5C034E789B6A3DEFBE013BDA7D14466677,IMPHASH=741776AACCFC5B71FF59832DCDCACE0F
{dc5131b5-72bf-63ea-6601-000000000b00}
7084
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit -command Set-Location -literalPath 'C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam'
MSEDGEWIN10\IEUser
Description
Data
5:03 PM
2/16/2023



- Search everything based on parent process id: 7080 and event id 3- Network Connections, 22- DNS names :




Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Microsoft-Windows-PowerShell%4Operational (C:\Cases\E\Wi
Windows PowerShell (C:\Cases\E\Windows\System32\winevt
Microsoft-Windows-Sysmon%4Operational (C:\Cases\E\Windo
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Windows PowerShell.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:27:30 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:30 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:29 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:29 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:28 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:58 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:58 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:58 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:49 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:49 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:48 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:48 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:48 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:47 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Description
The description for Event ID (3) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
-
2023-02-13 17:26:37.702
{dc5131b5-72bf-63ea-6601-000000000b00}
7088
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
MSEDGEWIN10\IEUser
tcp
true
false
10.0.2.15
MSEDGEWIN10
50261
-
false
185.199.109.133
cdn-185-199-109-133.github.com
443
https
Description
Data
5:04 PM
2/16/2023


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
Objects tree
Search
WIN-9OHAJ6CQHQM (local)
Log Files
Application (C:\Cases\E\Windows\System32\winevt\logs\App
Microsoft-Windows-Windows Defender%4Operational (C:\Cas
System (C:\Cases\E\Windows\System32\winevt\logs\System.
Security (C:\Cases\E\Windows\System32\winevt\logs\Securit
Microsoft-Windows-PowerShell%4Operational (C:\Cases\E\Wi
Windows PowerShell (C:\Cases\E\Windows\System32\winevt
Microsoft-Windows-Sysmon%4Operational (C:\Cases\E\Windo
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
System.evtx
Security.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Windows PowerShell.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
UTC
Type Date Time Event Source Category User Computer
Information 2/13/2023 5:27:37 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:36 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:36 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:34 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:33 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:32 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:31 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:31 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:30 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:30 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:29 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:29 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:27:28 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10
Information 2/13/2023 5:26:58 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10
Description
The description for Event ID (22) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.
The following information was included with the event:
-
2023-02-13 17:27:26.232
{dc5131b5-72bf-63ea-6601-000000000b00}
7088
www.powershellgallery.com
0
type: 5 powershellgallerytrafficmanager.trafficmanager.net;type: 5 psg-prod-centralus.cloudapp.net;::ffff:40.122.208.145;
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
MSEDGEWIN10\IEUser
Description
Data
5:05 PM
2/16/2023