Digital Forensics - Lab 3

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

- 19 August 2021

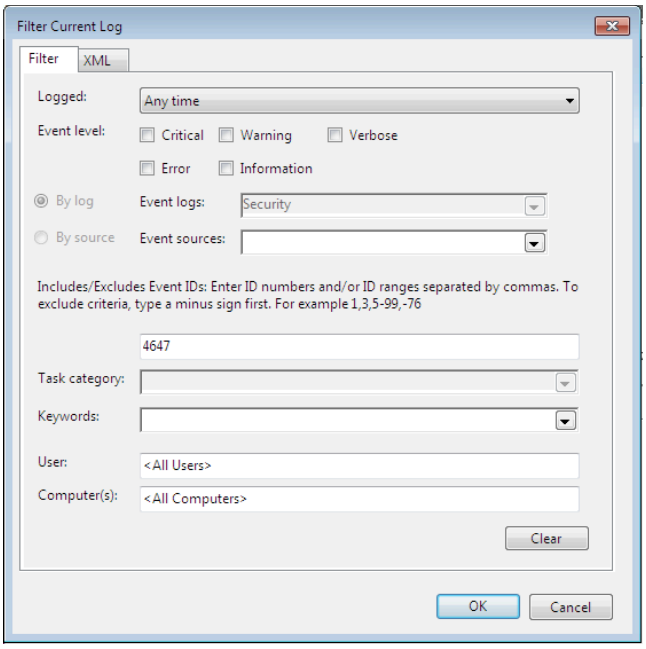
Question 1 :

Use the Event Viewer tool in a Microsoft Windows computer and take screenshots of THREE security related events such as

"Logon", "Logoff", & "Attempt made to query the existence of a blank password for an account"

The Microsoft Event Viewer tool is used to display a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. But here our purpose is to use this tool to perform forensic analysis into the system. These logs are very useful as they provide elaborate and detailed occurrences of events in the computer which can be used to build a timeline in the case of an investigation, or to perform any other number of operations.

In this exercise, we will use this tool to find the events like log in log out and an attempt to query the existence of blank password user account. Each event has a particular Event ID which can be used to query the logs available and filter out the results. The following image shows how a filter can be applied to the logs :



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4647

Task category:

Keywords:

User: <All Users>

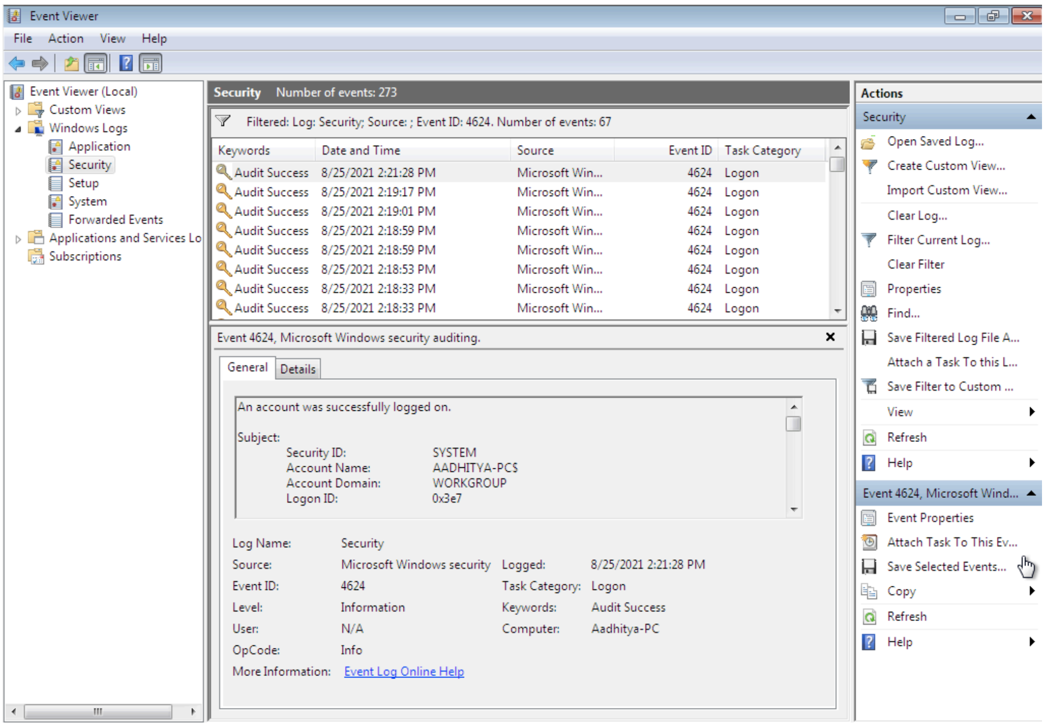
Computer(s): <All Computers>

After we have entered the required event ID, the event viewer filters out events of this category and presented them, each of whose details have been displayed in the details section below.

We shall see the events in the below sections :

A. Logon Event

The **Login** Event has the event ID as 4624. This means that the account was successfully logged on.



Security Number of events: 273

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 67

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/25/2021 2:21:28 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:19:17 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:19:01 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:18:59 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:18:59 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:18:53 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:18:33 PM	Microsoft Win...	4624	Logon
Audit Success	8/25/2021 2:18:33 PM	Microsoft Win...	4624	Logon

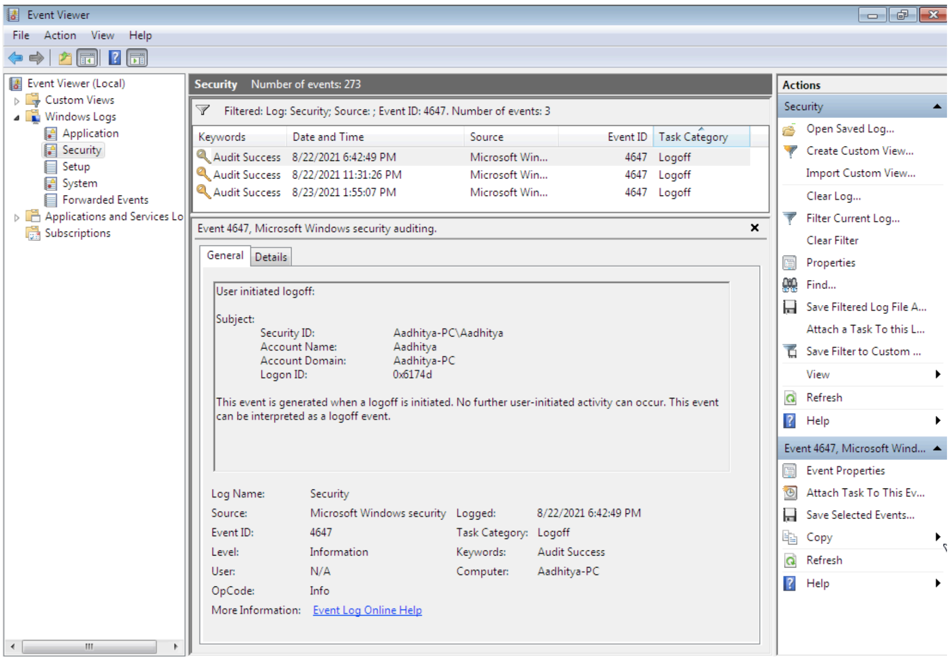
Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           AADHITYA-PC$
        Account Domain:         WORKGROUP
        Logon ID:               0x3e7
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/25/2021 2:21:28 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Aadhitya-PC
OpCode:	Info		
More Information:	Event Log Online Help		

B. Logoff Event

The **Logoff** Event has the event ID as 4647. This means that the account was successfully logged out by the initiation of the user.



Security Number of events: 273

Filtered: Log: Security; Source: ; Event ID: 4647. Number of events: 3

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/22/2021 6:42:49 PM	Microsoft Win...	4647	Logoff
Audit Success	8/22/2021 11:31:26 PM	Microsoft Win...	4647	Logoff
Audit Success	8/23/2021 1:55:07 PM	Microsoft Win...	4647	Logoff

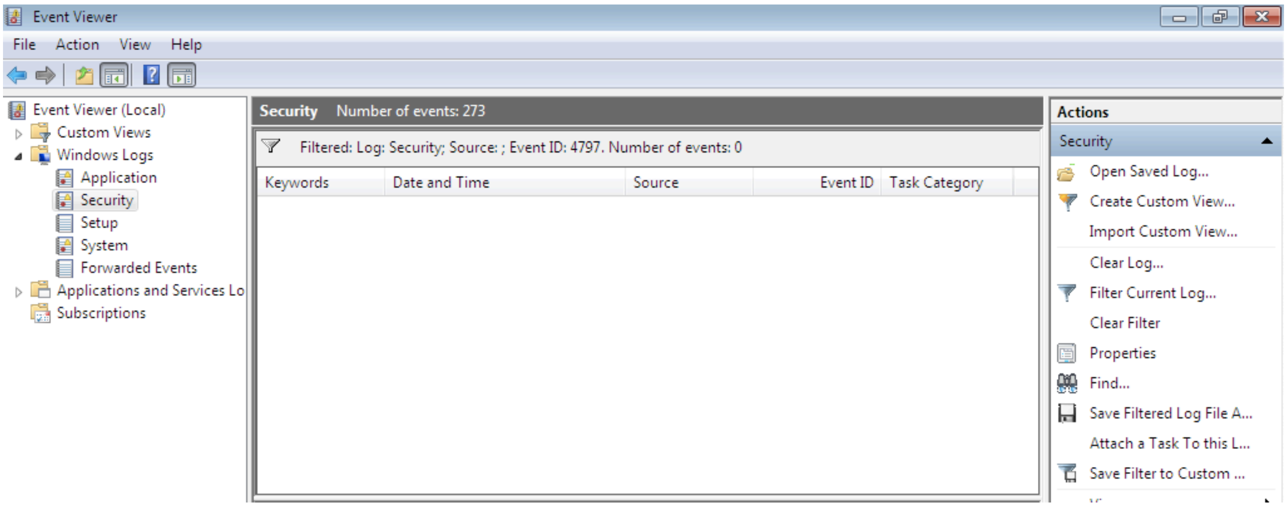
Event 4647, Microsoft Windows security auditing.

```
User initiated logoff:

Subject:
        Security ID:        Aadhitya-PC\Aadhitya
        Account Name:       Aadhitya
        Account Domain:     Aadhitya-PC
        Logon ID:           0x6174d

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event
can be interpreted as a logoff event.
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          8/22/2021 6:42:49 PM
Event ID:          4647                         Task Category:   Logoff
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        Aadhitya-PC
OpCode:            Info
More Information:  Event Log Online Help
```

C. Attempt made to query the existence of a blank password for an account Event

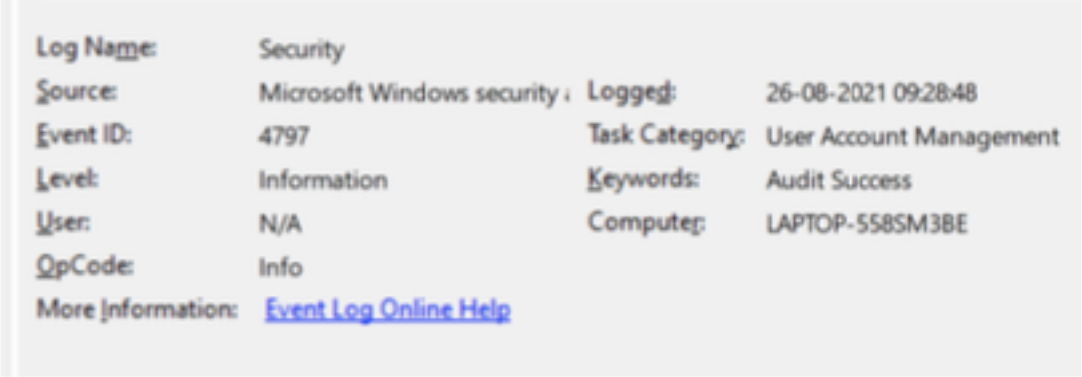
The "**Attempt made to query the existence of a blank password for an account**" Event has the event ID as 4797. We use this for the querying procedure. As this error is relatively rare and because this command has been executed on a fresh installation of windows, it has resulted in an empty query.



Security Number of events: 273

Filtered: Log: Security; Source: ; Event ID: 4797. Number of events: 0

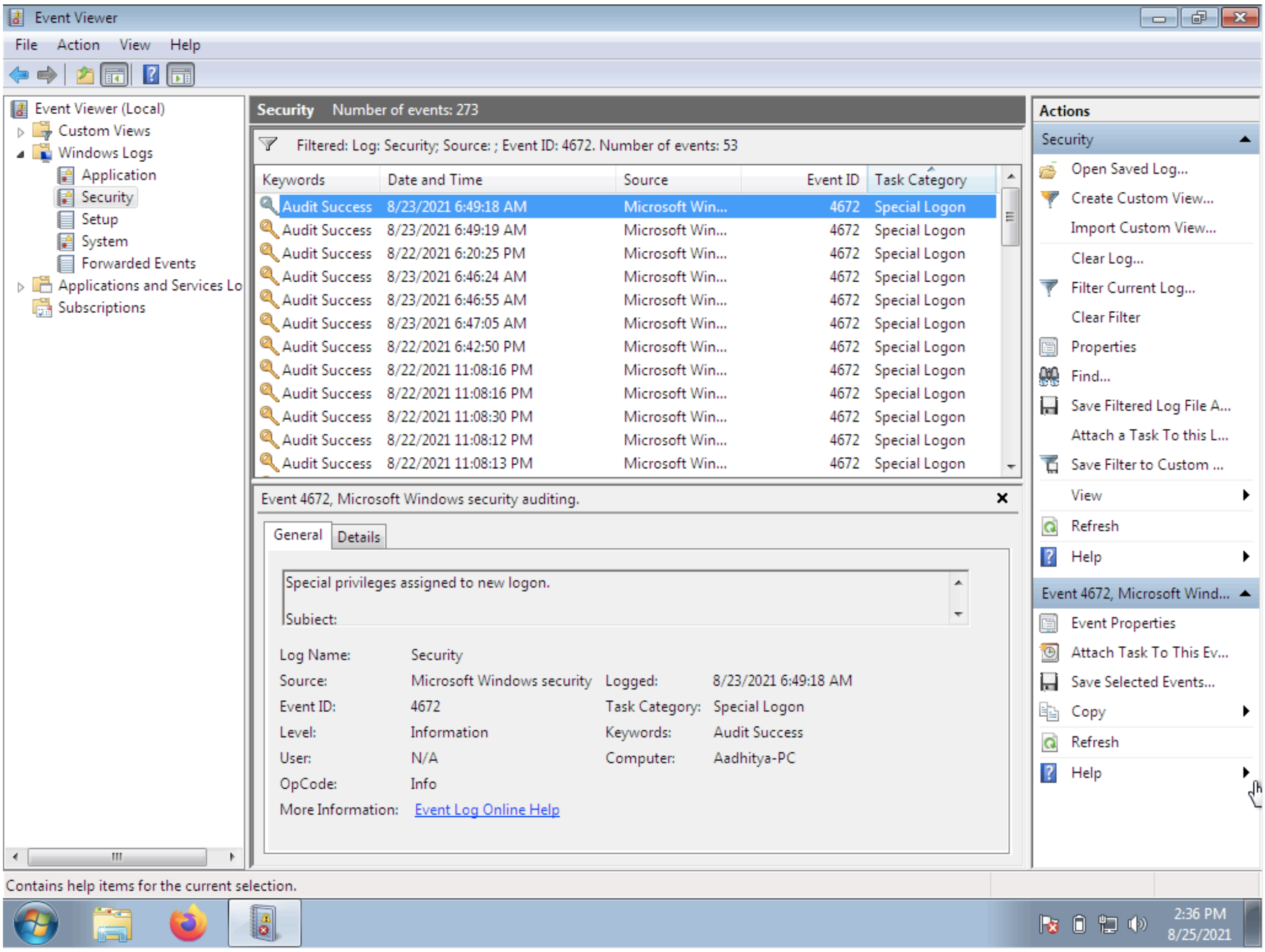
Keywords	Date and Time	Source	Event ID	Task Category



Log Name:	Security		
Source:	Microsoft Windows security	Logged:	26-08-2021 09:28:48
Event ID:	4797	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	LAPTOP-558SM3BE
OpCode:	Info		
More Information:	Event Log Online Help		

D. Special Logon Event

The **Special Login Event** has the event ID as 4762. This means that the account was granted special permissions while it was successfully logged on.



Security Number of events: 273

Filtered: Log: Security; Source: ; Event ID: 4672. Number of events: 53

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/23/2021 6:49:18 AM	Microsoft Win...	4672	Special Logon
Audit Success	8/23/2021 6:49:19 AM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 6:20:25 PM	Microsoft Win...	4672	Special Logon
Audit Success	8/23/2021 6:46:24 AM	Microsoft Win...	4672	Special Logon
Audit Success	8/23/2021 6:46:55 AM	Microsoft Win...	4672	Special Logon
Audit Success	8/23/2021 6:47:05 AM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 6:42:50 PM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 11:08:16 PM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 11:08:16 PM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 11:08:30 PM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 11:08:12 PM	Microsoft Win...	4672	Special Logon
Audit Success	8/22/2021 11:08:13 PM	Microsoft Win...	4672	Special Logon

Event 4672, Microsoft Windows security auditing.

Special privileges assigned to new logon.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/23/2021 6:49:18 AM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Aadhitya-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Contains help items for the current selection.

In this manner, the Event Viewer tool helps us to perform Forensic analysis in a computer, which can help investigations of any scale in this age of computers.

Question 2 :

Utilise The Event Log Explorer tool on a Windows computer and take screenshots of two security related events such as those listed in the previous exercise.

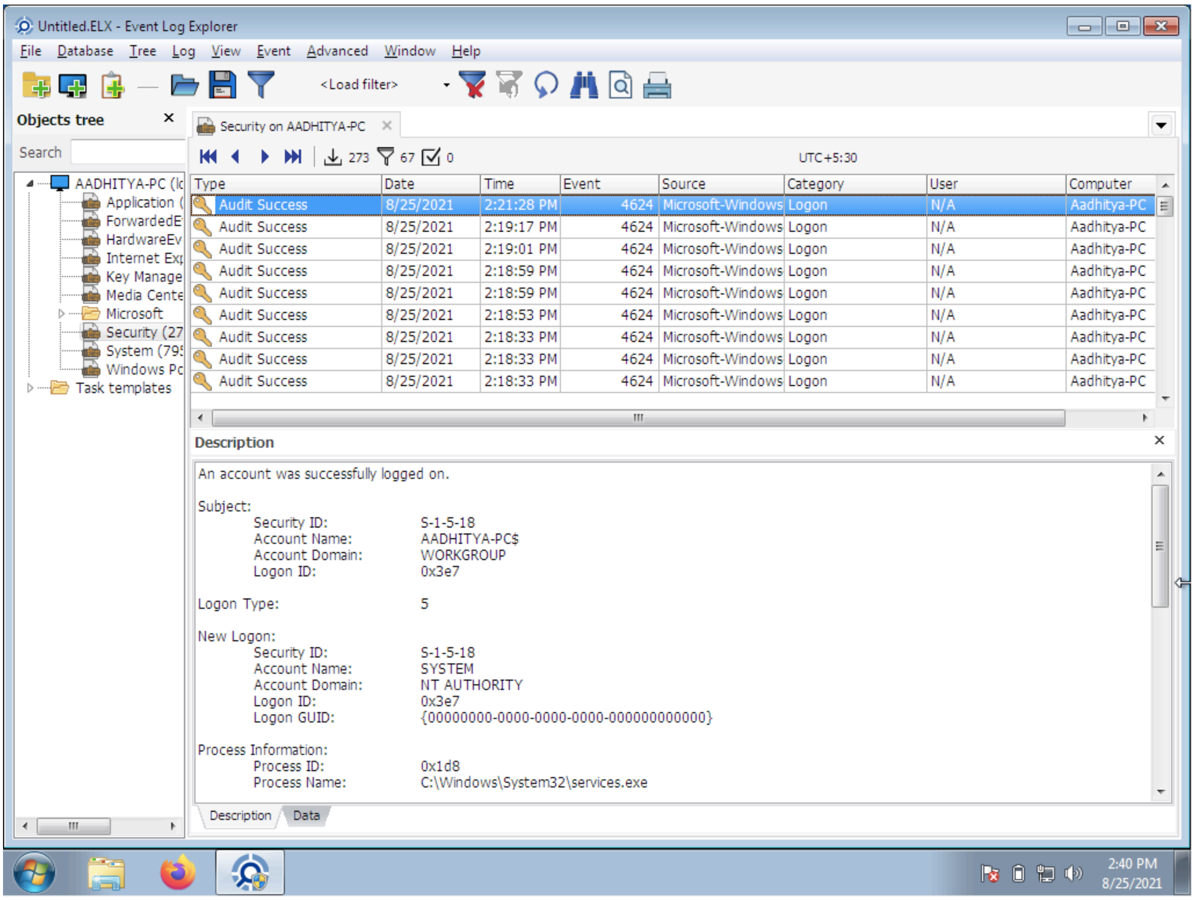
The Event Log Explorer is an effective software solution for viewing, analyzing and monitoring events recorded in Microsoft Windows event logs. Event Log Explorer greatly simplifies and speeds up the analysis of event logs (security, application, system, setup, directory service, DNS and others). Event Log Explorer extends the standard Windows Event Viewer functionality and brings many new features.

Let us now run a few commands and explore this tools and see how this tool is similar to the event viewer as discussed above :

We shall see the events in the below sections :

A. Logon Event

The **Login** Event has the event ID as 4624. This means that the account was successfully logged on.



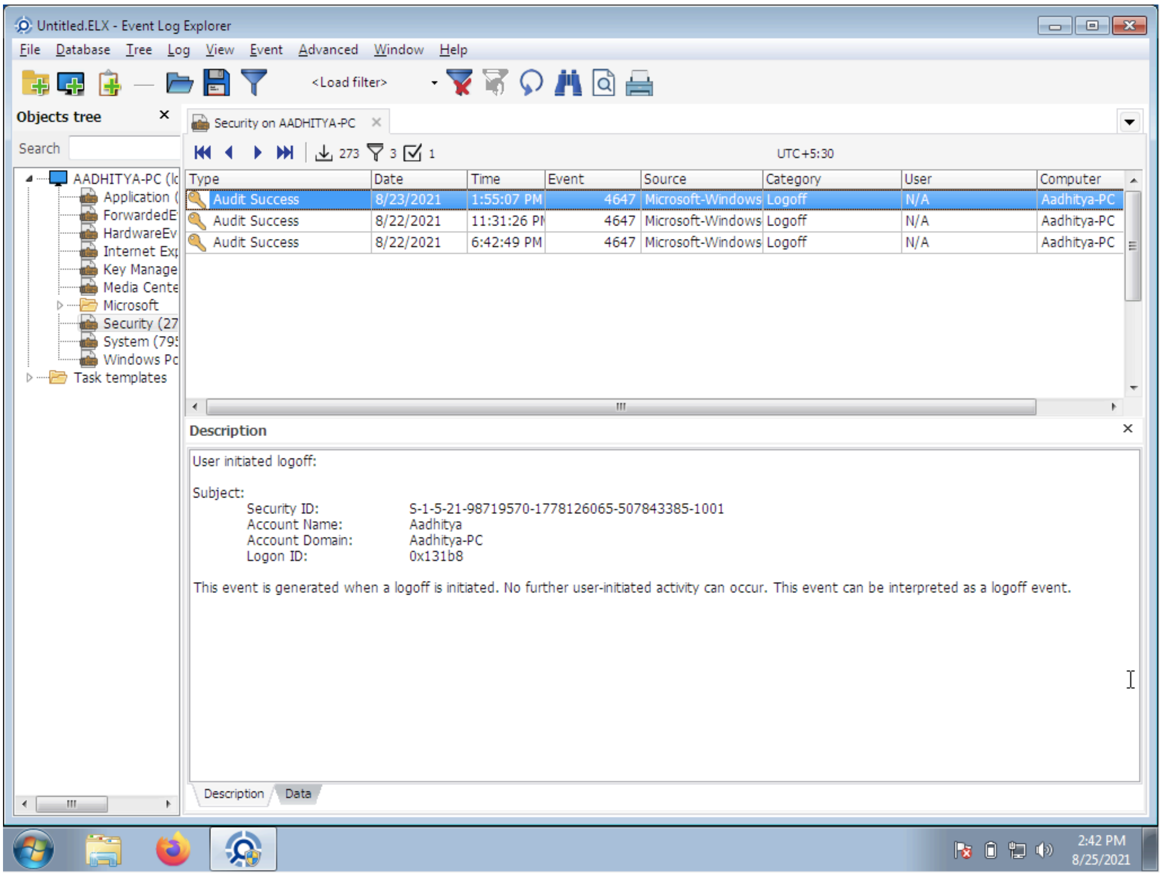
Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	8/25/2021	2:21:28 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:19:17 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:19:01 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:59 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:59 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:53 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:33 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:33 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:33 PM	4624	Microsoft-Windows	Logon	N/A	Aadhitya-PC

Description

```
An account was successfully logged on.

Subject:
          Security ID:              S-1-5-18
          Account Name:             AADHITYA-PC$
          Account Domain:           WORKGROUP
          Logon ID:                 0x3e7

Logon Type:                         5

New Logon:
          Security ID:              S-1-5-18
          Account Name:             SYSTEM
          Account Domain:           NT AUTHORITY
          Logon ID:                 0x3e7
          Logon GUID:               {00000000-0000-0000-0000-000000000000}

Process Information:
          Process ID:               0x1d8
          Process Name:             C:\Windows\System32\services.exe
```

B. Logoff Event

The **Logoff** Event has the event ID as 4647. This means that the account was successfully logged out by the initiation of the user.

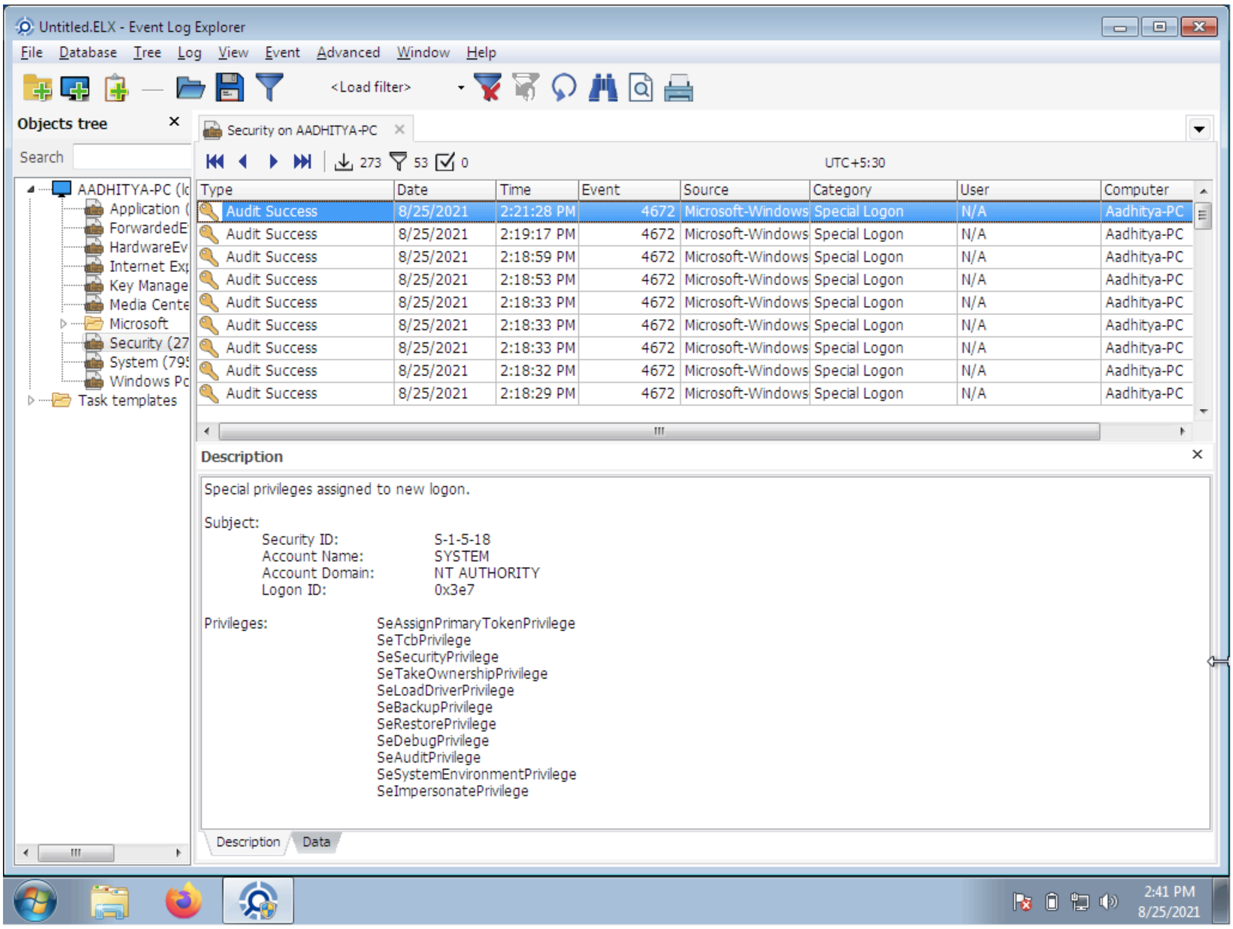


Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	8/23/2021	1:55:07 PM	4647	Microsoft-Windows	Logoff	N/A	Aadhitya-PC
Audit Success	8/22/2021	11:31:26 PM	4647	Microsoft-Windows	Logoff	N/A	Aadhitya-PC
Audit Success	8/22/2021	6:42:49 PM	4647	Microsoft-Windows	Logoff	N/A	Aadhitya-PC

```
User initiated logoff:

Subject:
        Security ID:            S-1-5-21-98719570-1778126065-507843385-1001
        Account Name:           Aadhitya
        Account Domain:         Aadhitya-PC
        Logon ID:               0x131b8

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
```

C. Special Logon Event

The **Special Login Event** has the event ID as 4762. This means that the account was granted special permissions while it was successfully logged on.



Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	8/25/2021	2:21:28 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:19:17 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:59 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:53 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:33 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:33 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:33 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:32 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC
Audit Success	8/25/2021	2:18:29 PM	4672	Microsoft-Windows	Special Logon	N/A	Aadhitya-PC

```
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3e7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeDebugPrivilege
                        SeAuditPrivilege
                        SeSystemEnvironmentPrivilege
                        SeImpersonatePrivilege
```

Thus we can infer that this even log explorer is also a tool similar to the event viewer with many more functionalities than the former

CONCLUSION

In this lab experiments, we have dealt with and seen two softwares which provide functionalities for useful and ease of forensic analysis.