DIGITAL FORENSICS LAB

Exercise 3	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulgara
Date	24th August, 2021

AIM

Working with Windows Event Viewer and the Event Log Explorer tool to find security related events.

EVENT VIEWER

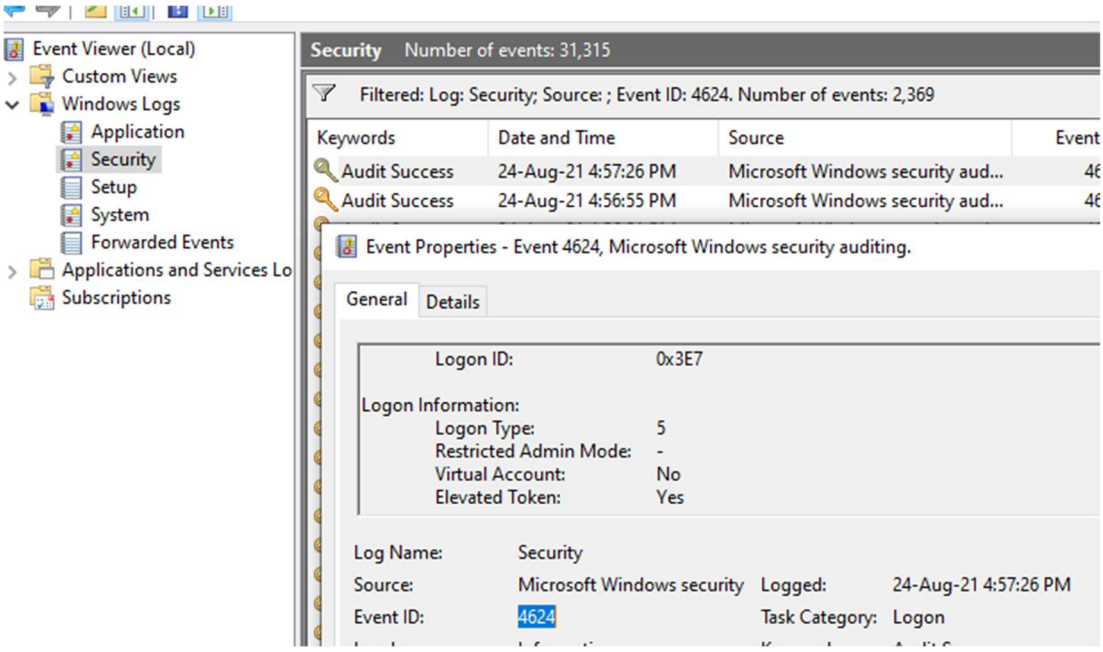
This is a tool built into Windows Operating Systems to let administrators and users view event logs on a machine. We use this to find security events such as logon, logoff using Event IDs.

To find an Event by its ID, click on the 'Find' option under the 'Actions' pane on the right. Then enter the Event id that needs to be found.

STEPS

1. Open Event Viewer
2. Go to Windows Logs>Security
3. Select 'Filter Current Log' in the pane on the right side.
4. Enter the Event ID needed and click 'Ok'.

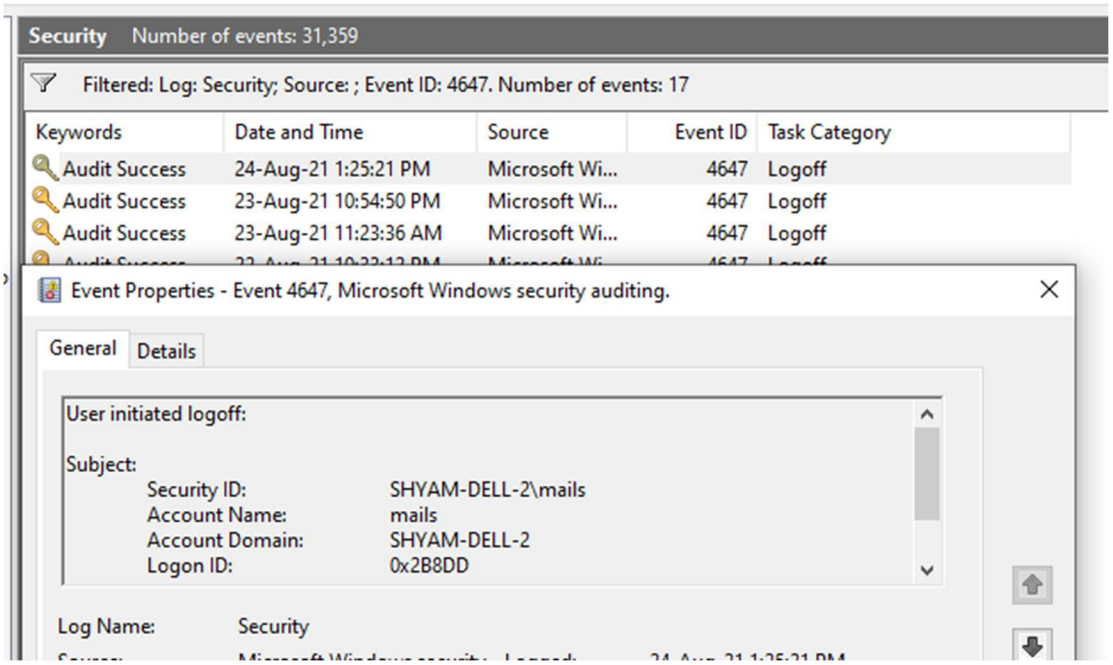
LOGON (Event ID – 4624)



OBSERVATION

This event documents each and every successful attempt to logon to the local computer for all types of logons. Logon type 7 shown in the screenshot above is used to indicate 'Unlock', i.e., password protected screen saver was shown as it was unattended. We see that this event has happened 2376 times.

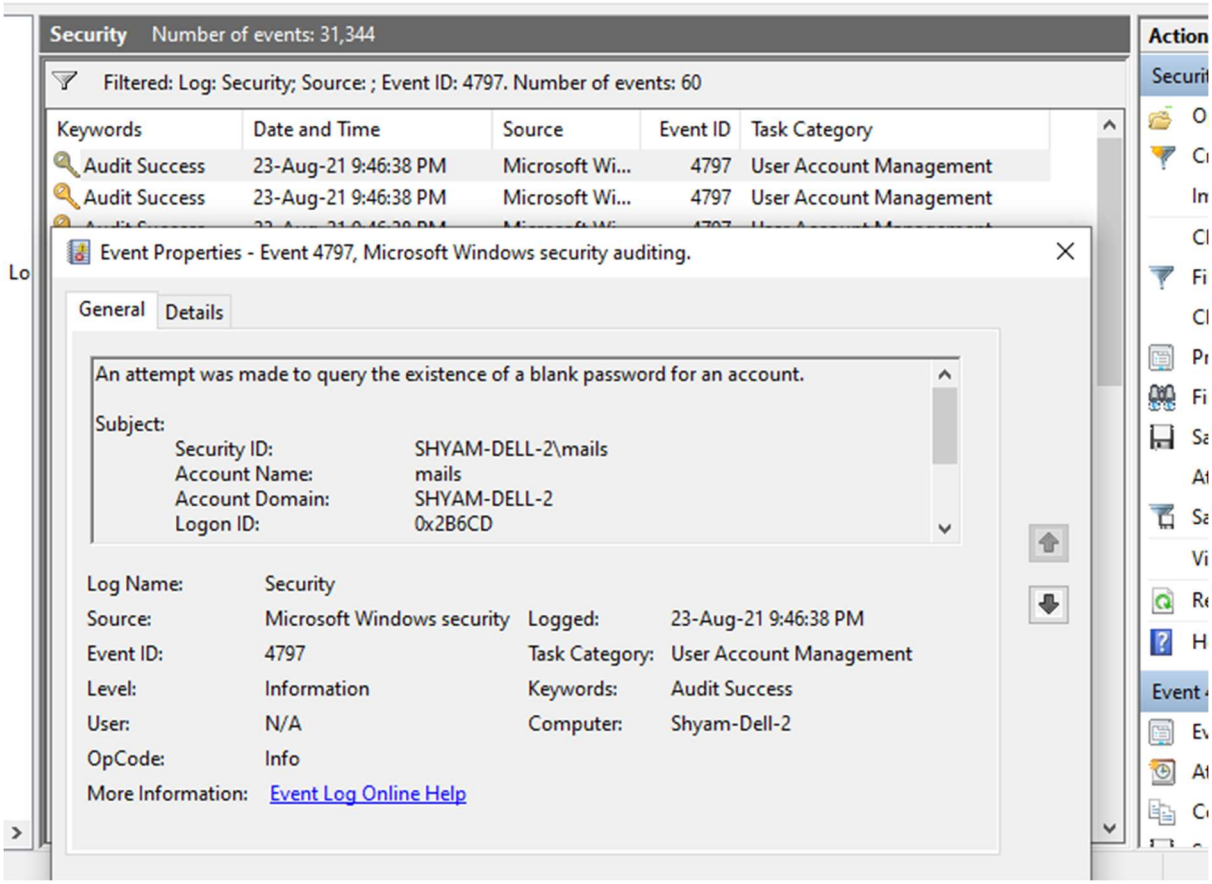
LOGOFF (Event ID – 4647)



OBSERVATION

This event signals the end of a logon session. We see that this event has occurred 17 times.

ATTEMPT MADE TO QUERY THE EXISTENCE OF A BLANK PASSWORD FOR AN ACCOUNT (EVENT ID – 4797)



OBSERVATION

This event can usually be ignored. We also see that this event has occurred 60 times as shown on the bar up top. If this event is logged with multiple other user accounts, only then it is of concern.

EVENT LOG EXPLORER

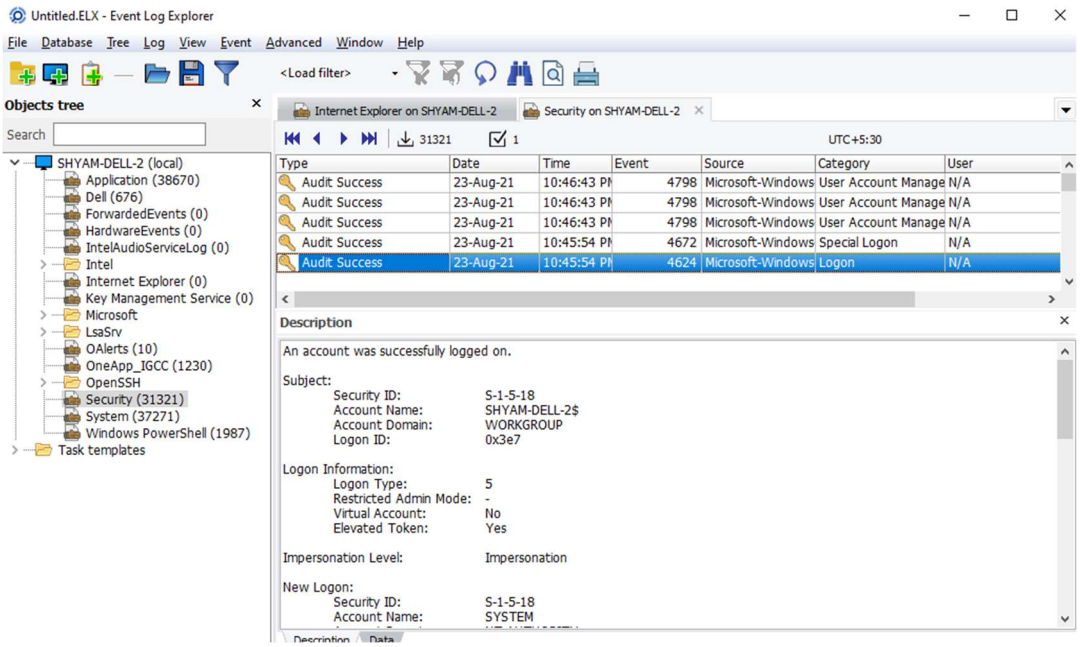
This is a tool built into Windows Operating Systems to let administrators and users view event logs on a machine. We use this to find security events such as logon, logoff using Event IDs.

To find an Event by its ID, click on the 'Find' option under the 'Actions' pane on the right. Then enter the Event id that needs to be found.

STEPS

1. Download and Install Event Log Explorer
2. In the 'Objects Tree' pane, select the local machine and choose 'Security' from the expanded list.
3. Choose the Filter option or just press CTRL+F.
4. Enter the Event ID needed and click 'Ok'.

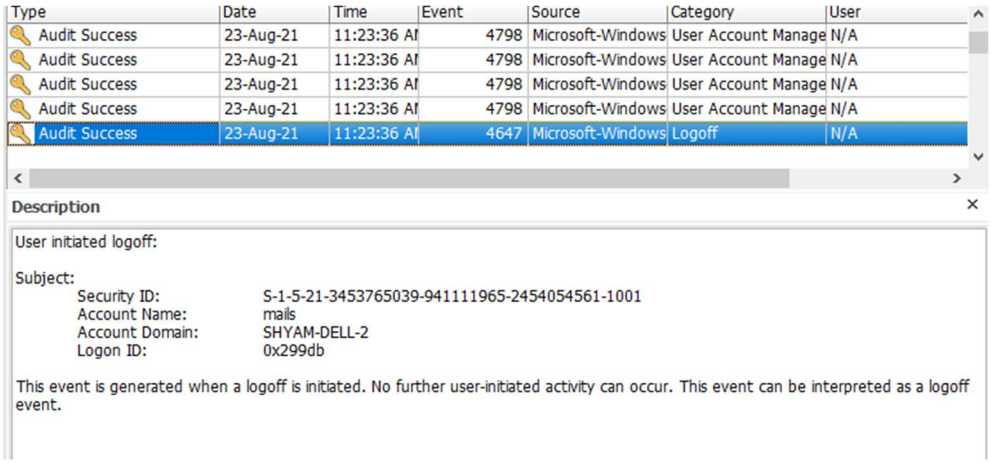
LOGON (Event ID – 4624)



OBSERVATION

This shows the logon event similar to Event Viewer. A description of the event is also shown.

LOGOFF (Event ID – 4647)



Type	Date	Time	Event	Source	Category	User
Audit Success	23-Aug-21	11:23:36 AM	4798	Microsoft-Windows	User Account Manage	N/A
Audit Success	23-Aug-21	11:23:36 AM	4798	Microsoft-Windows	User Account Manage	N/A
Audit Success	23-Aug-21	11:23:36 AM	4798	Microsoft-Windows	User Account Manage	N/A
Audit Success	23-Aug-21	11:23:36 AM	4798	Microsoft-Windows	User Account Manage	N/A
Audit Success	23-Aug-21	11:23:36 AM	4647	Microsoft-Windows	Logoff	N/A

Description

User initiated logoff:

Subject:
Security ID: S-1-5-21-3453765039-941111965-2454054561-1001
Account Name: mails
Account Domain: SHYAM-DELL-2
Logon ID: 0x299db

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.

OBSERVATION

This shows the logoff event similar to Event Viewer. A description is shown too.

CONCLUSION

We have used the Event Viewer and Event Log Explorer tools to search for specific security events. These tools are powerful and aid those in Digital Forensics to get insights as to what happened on the device and how it was used or if it was compromised.