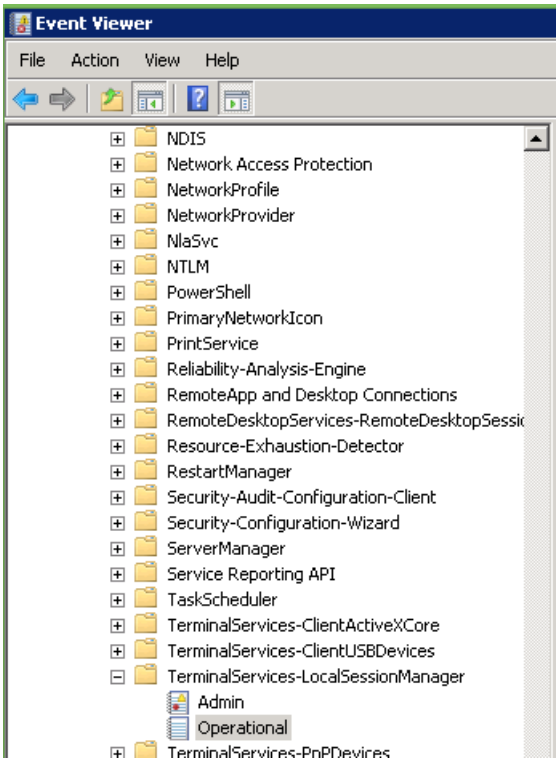
This document empowers us to find who has interrupted the box usage.

Scenario: User2 has interrupted the usage of the current user i.e. User1 for shared machine.

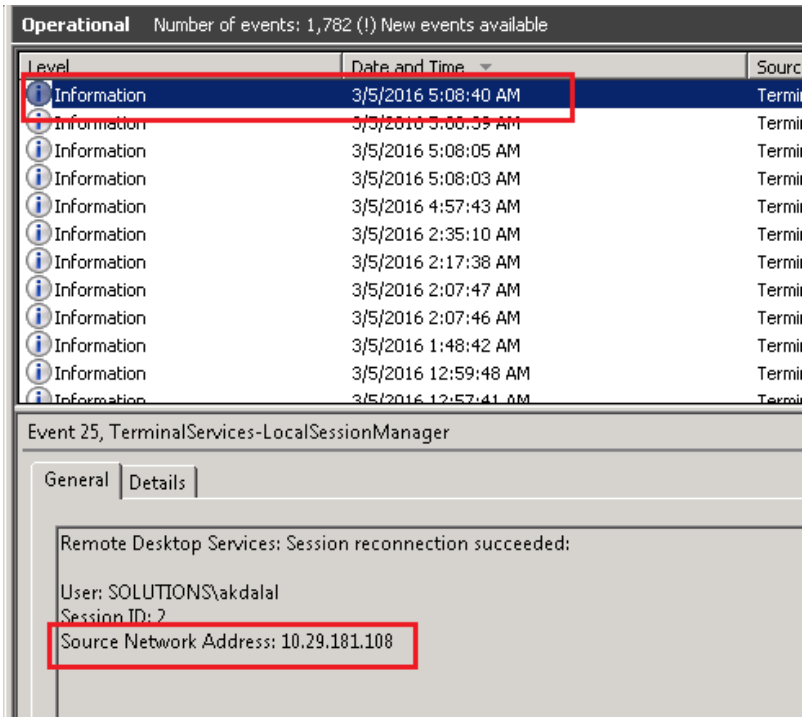
For demonstration, let us consider User1 is saavvaru, User2 is prmodi and Machine is '10.118.20.213'.

Once User1 notices that box is disconnected, he/she has to contact Box owner.
And Box owner has to follow the below steps to locate the User2 hostname.

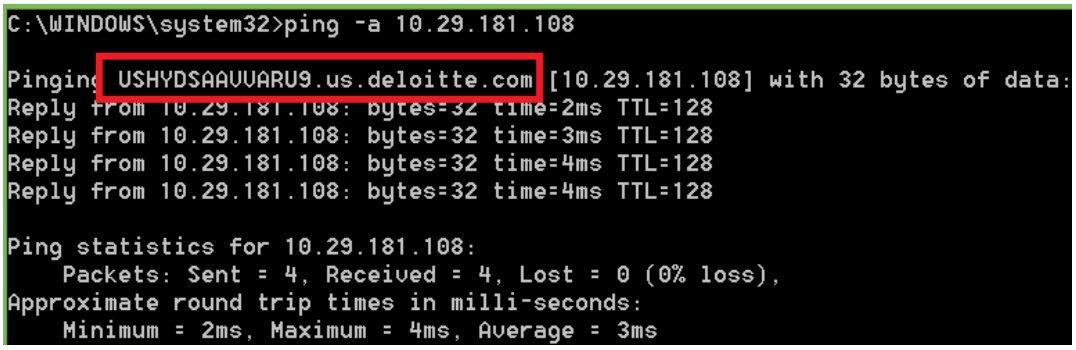
1. Login to box/machine. Press 'windows' button and type/search for 'Event Viewer' program. Click to open.
2. In 'Event Viewer' window, navigate to "*Applications and Service Logs -> Microsoft -> Windows -> TerminalServices-LocalSessionManager -> Operational" as shown below:*



3. First record will be the current loggedin user i.e. boxowner (or) whoever is performing these steps. {*So, first record can be ignored*}

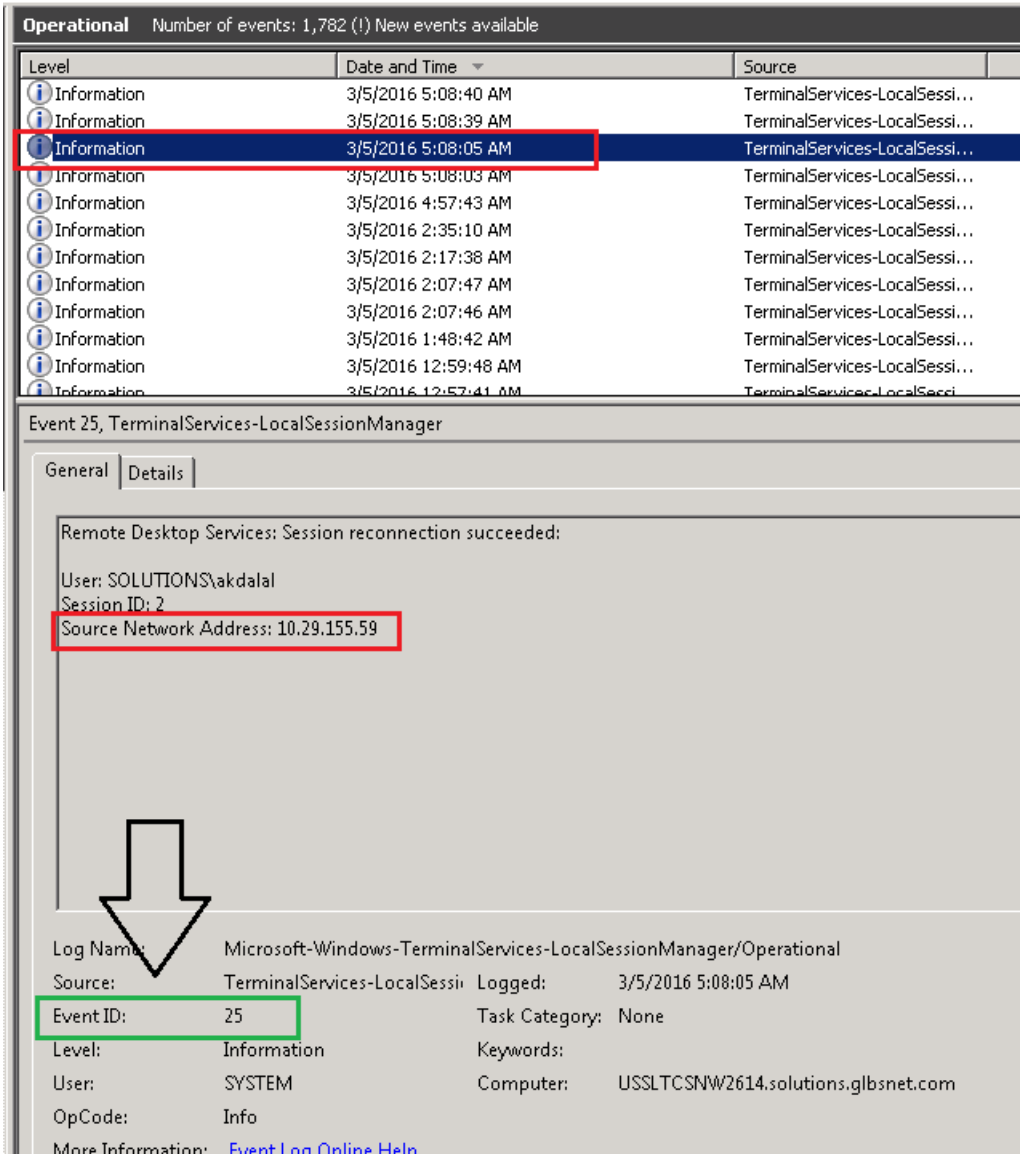


The host name can be found using the IP address in CMD prompt.



In this case, USHYDSAAVVARU9 is User1.

4. This step is to find the user who has interrupted. Based on timestamp when disconnection happened, locate the record. **Make sure the 'Event ID' is 21 or 25**.




```
C:\WINDOWS\system32>ping -a 10.29.155.59

Pinging USHYDPRMODI1 [10.29.155.59] with 32 bytes of data:
Reply from 10.29.155.59: bytes=32 time=492ms TTL=127
Reply from 10.29.155.59: bytes=32 time=518ms TTL=127
Reply from 10.29.155.59: bytes=32 time=521ms TTL=127
Reply from 10.29.155.59: bytes=32 time=496ms TTL=127

Ping statistics for 10.29.155.59:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 492ms, Maximum = 521ms, Average = 506ms
```

In this case, USHYDORMODI1 is User2.

Event IDs

Event ID	Event Description
21	**Logon**
23	**Logoff**
24	**Disconnected**
25	**Reconnection**

If any of the above steps are unclear, please contact saavvaru@deloitte.com

Working on Windows PowerShell Script to fetch this information automatically. Watch this space for more. Please join me if interested.