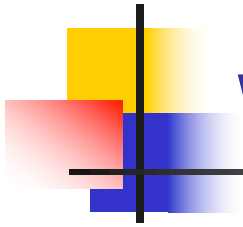
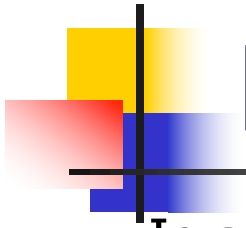


Windows Event Log for User Logon/Logoff

- Windows records successful or failed logon/logoff events under the Security events category. Logon events are very useful for tracking user activity.

- Event ID - 4624 – **Successful Logon**
- Event ID - 4625 – Failed Logon
- Event ID - 4634 – **Successful Logoff**
- Event ID - 4624 – Successful Network Logon

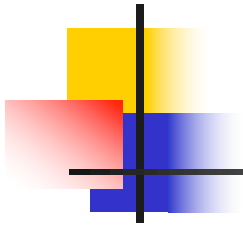


Logon Type

- In addition to date, time, username, hostname, and success/failure status of a logon, we can also determine by exactly what means a logon was attempted.

Logon type values:

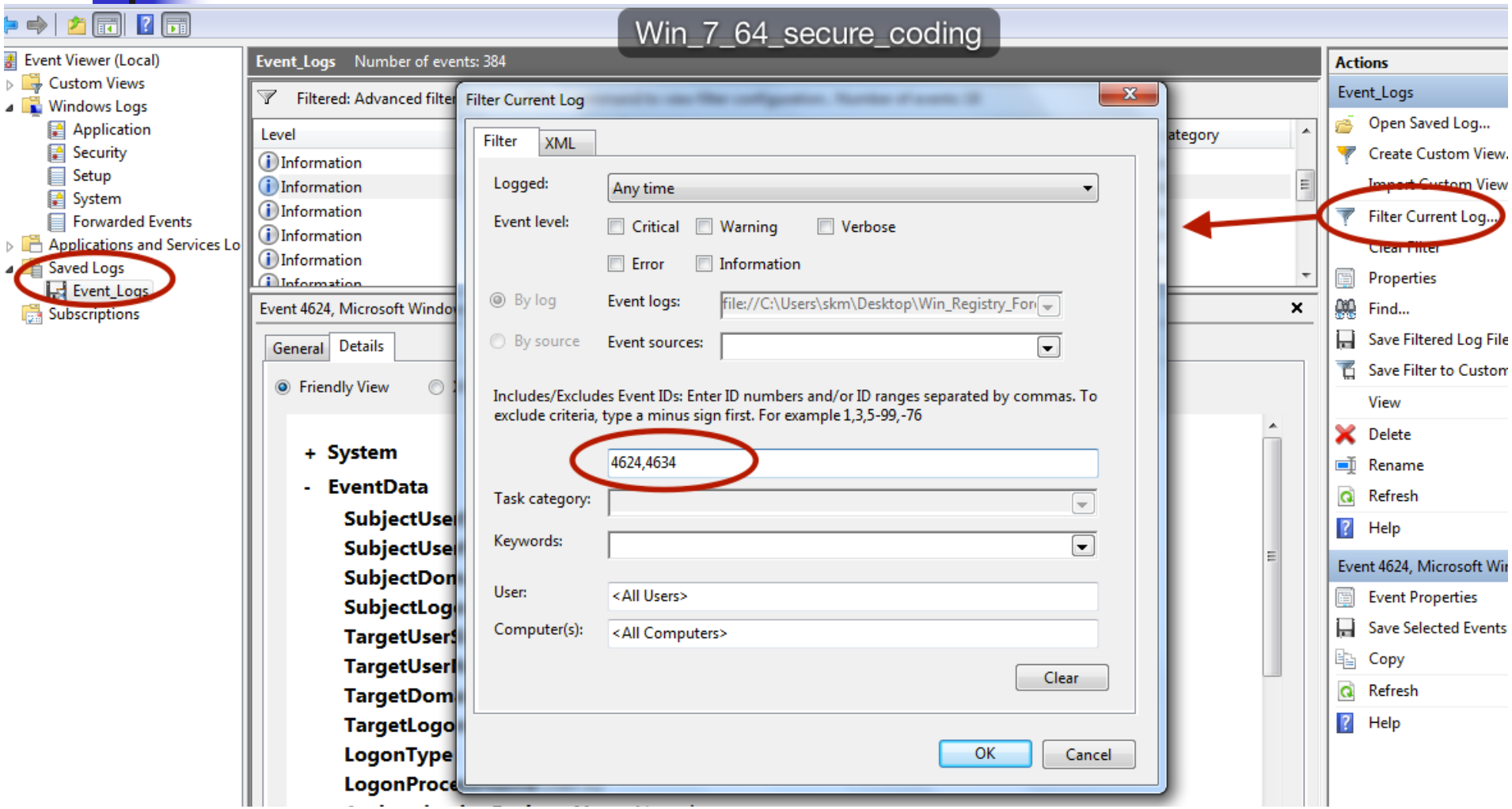
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (cleartext)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon



Filter Event Logs for Logon

- Event Viewer is a built-in tool for exploring event logs.
- By default, it displays the live system event logs. It can also be used to explore the saved/exported event log files.
  1. Open the saved event log files using event viewer.
  2. Event viewer will open the log file under 'saved logs' category.
  3. Click on 'Filter Current Log' from Actions menu on the right. A window will open.
  4. Select 'Filter' tab and enter the event IDs (e.g. 4624,4634) in the Event ID box and select 'OK'.
  5. Filtered event logs will be displayed.
  6. Click on 'Details' tab in lower pane for more details of the event.

Filter Event Logs for Logon



Manually Filter Event Logs

- Open ‘Filter Current Log’ window. (Follow step 1-3 from previous section.)
- Select ‘XML’ tab.
- Check the ‘Edit query manually’ box and hit ‘ok’ for confirmation.
- Enter the XML query to filter and click ‘ok’.
- E.g. To filter all logon attempts by using explicit credentials:

```
<QueryList>
  <Query Id="0" Path="file://C:\Users\IPAR\Desktop\Cases\Win_Registry_Forensics\Event_Logs.evtx">
    <Select Path="file://C:\Users\IPAR\Desktop\Cases\Win_Registry_Forensics\Event_Logs.evtx ">*
 [System[(EventID=4624)]] and *[EventData[Data[@Name='LogonType'] and (Data=2)]]</Select>
  </Query>
</QueryList>
```

Manually Filter Event Logs (Contd.)