National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

# M.Tech. Artificial Intelligence & Data Science (Specialization in Cyber Security)

School of Cyber Security and Digital Forensics

# Incident Response and Audit Compliances Laboratory

Lab practical Work

Semester: 1

Session: 2024-25

Date: 16/12/2024


Submitted to

Mr. Prakash Khasor Sir

Submitted by

Pratham Badge

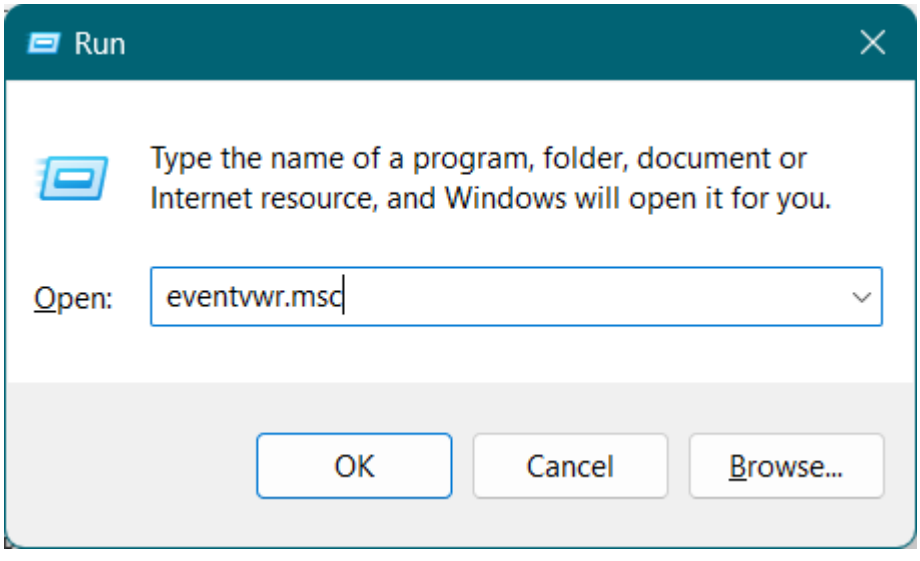
# Windows Event Viewer Practical Tasks

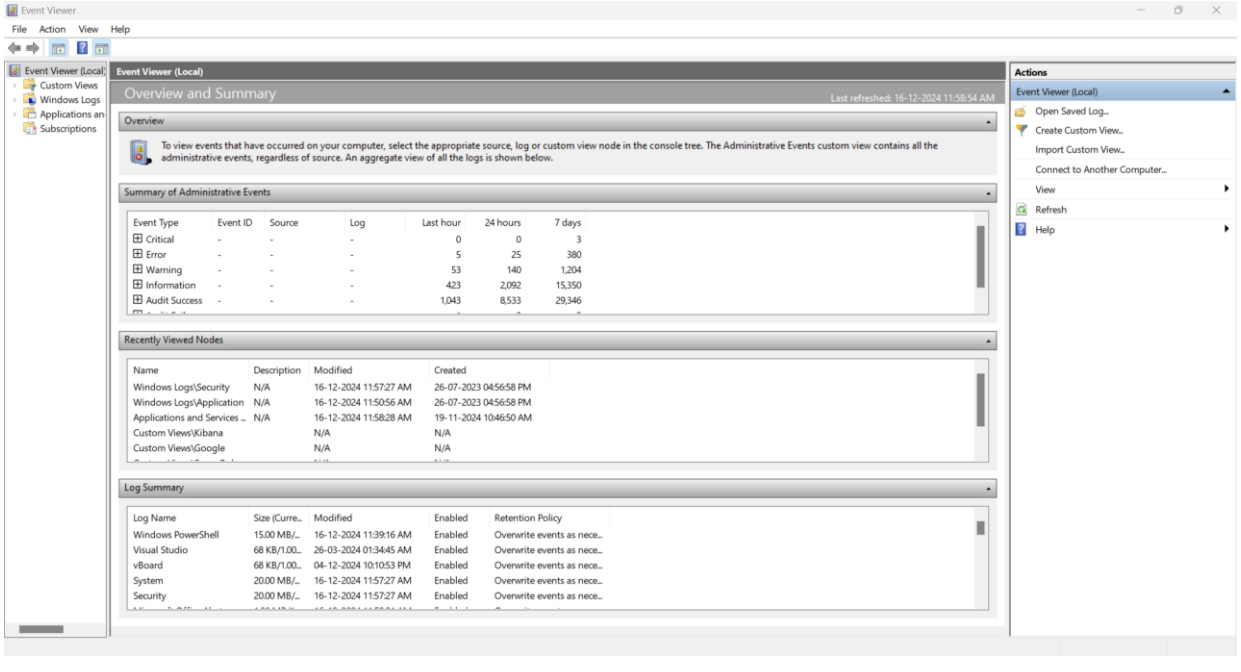
## Practical 1: Basic Navigation and Event Filtering

**Objective:** Understand how to navigate and filter events in the Event Viewer.

**Steps:**

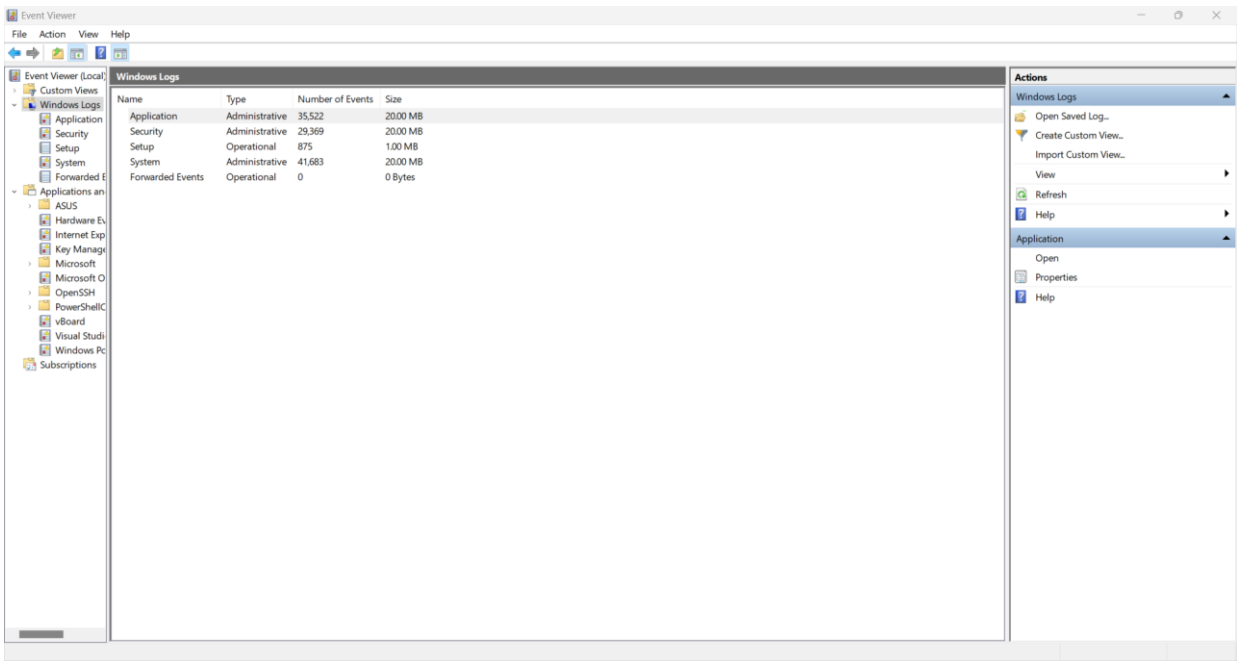
1. Open Event Viewer (`eventvwr.msc` via the Run dialog).



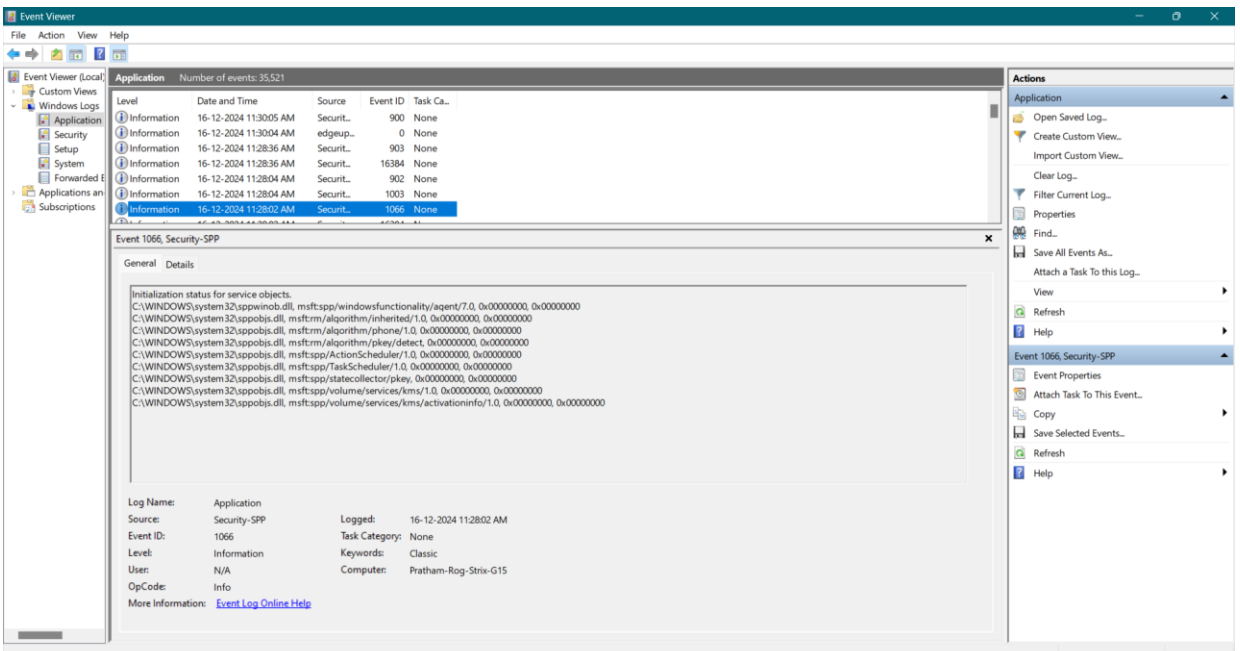



**2.** Explore the main sections:

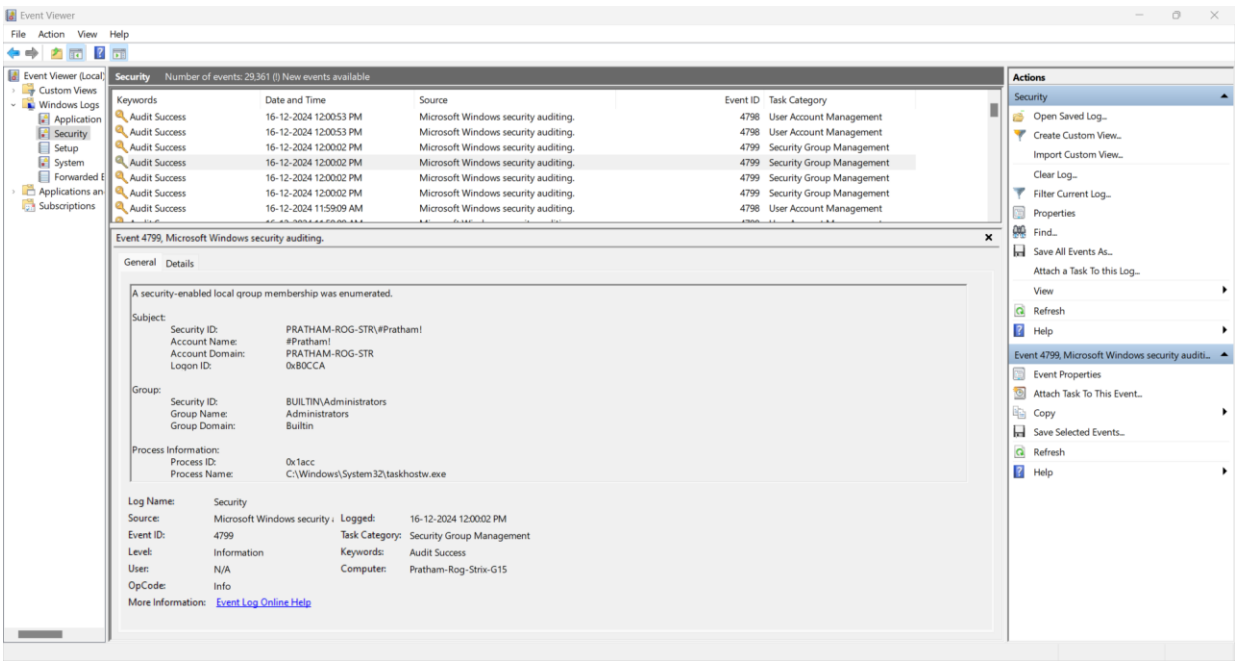
2.1. - Windows Logs (Application, Security, System, etc.)



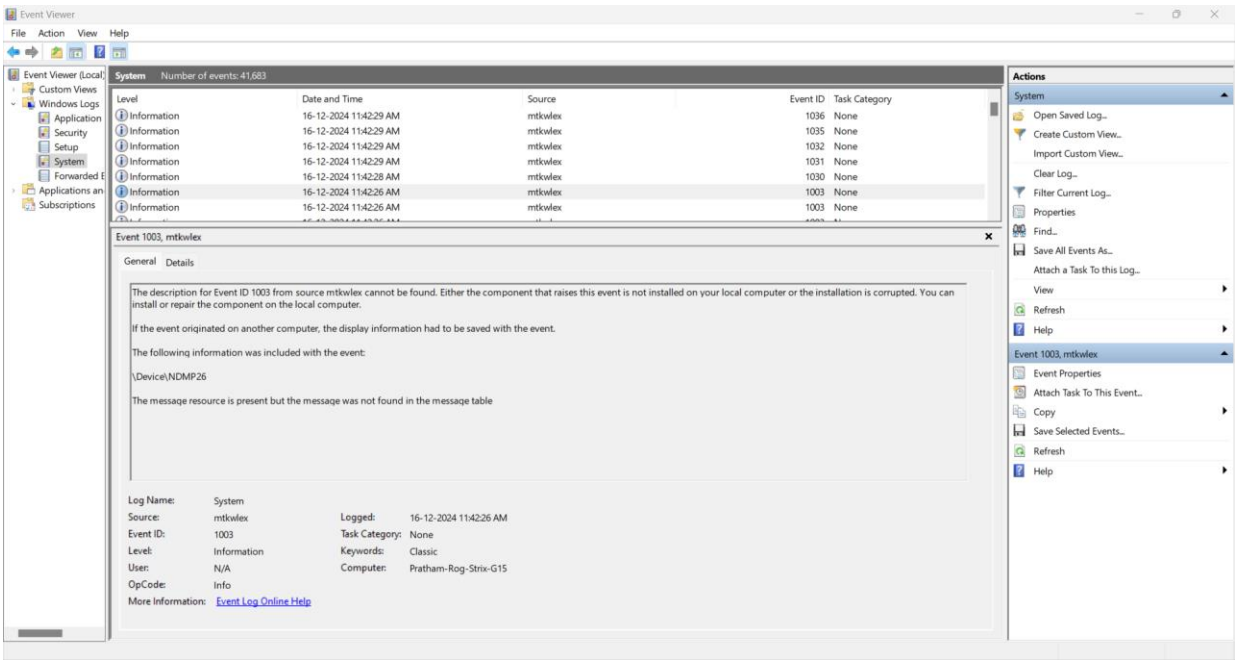

2.1.1. Application



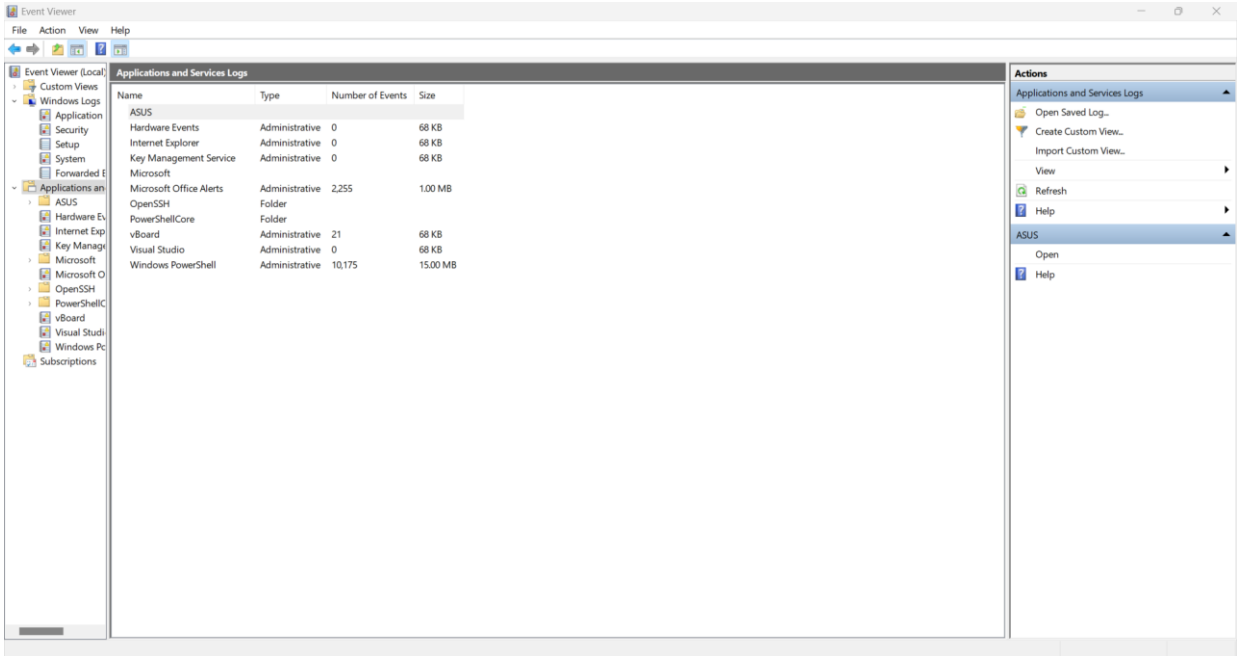

2.1.2. Security



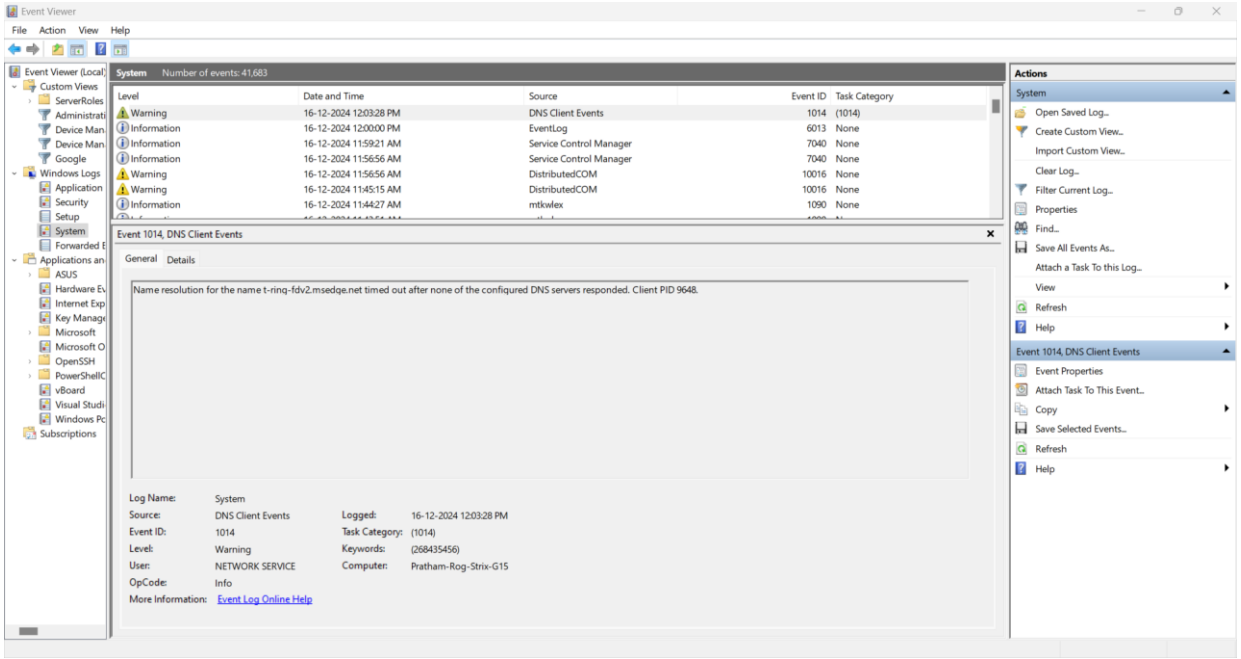

2.1.3. System



## 2.2. - Applications and Services Logs.

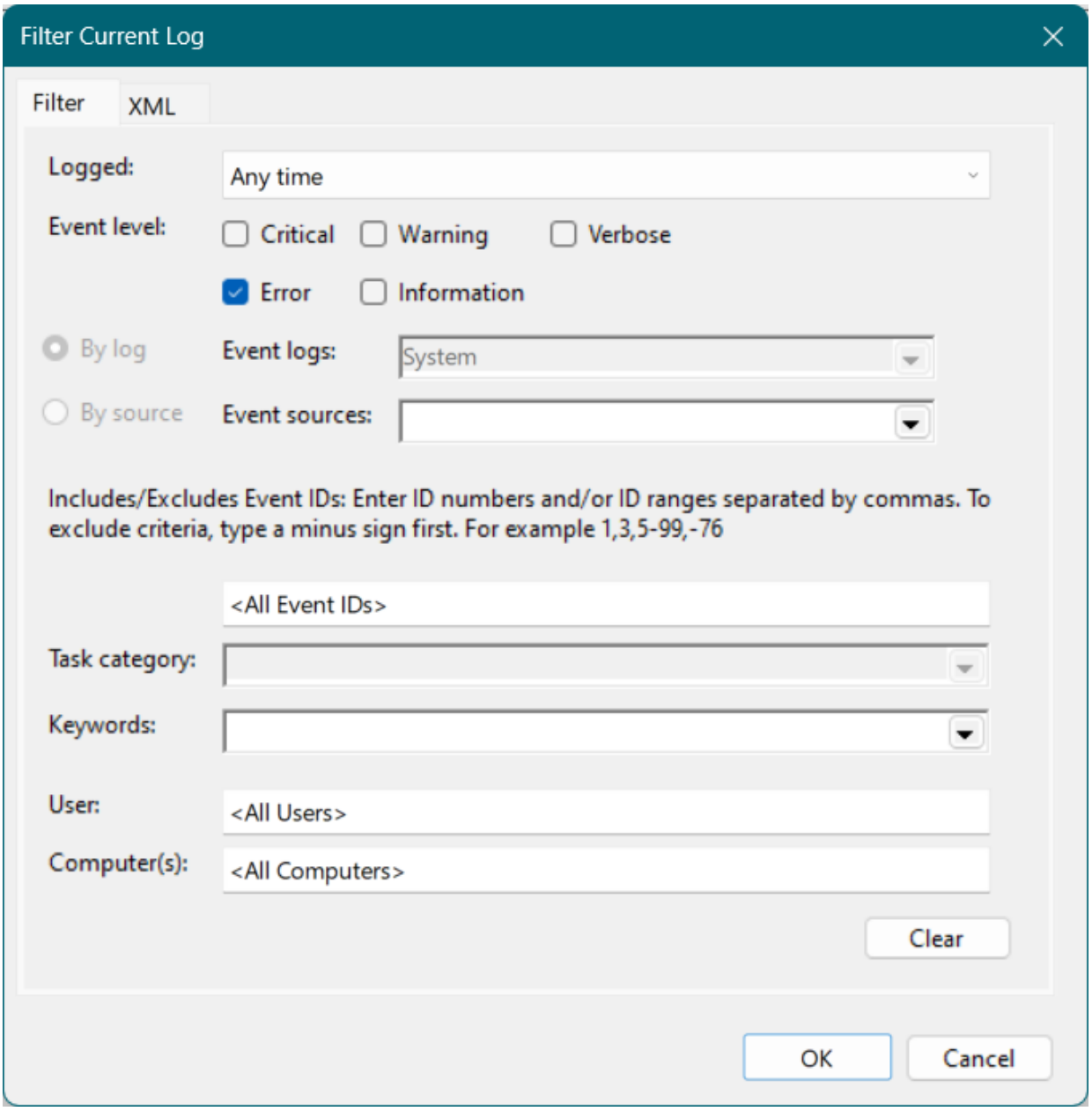


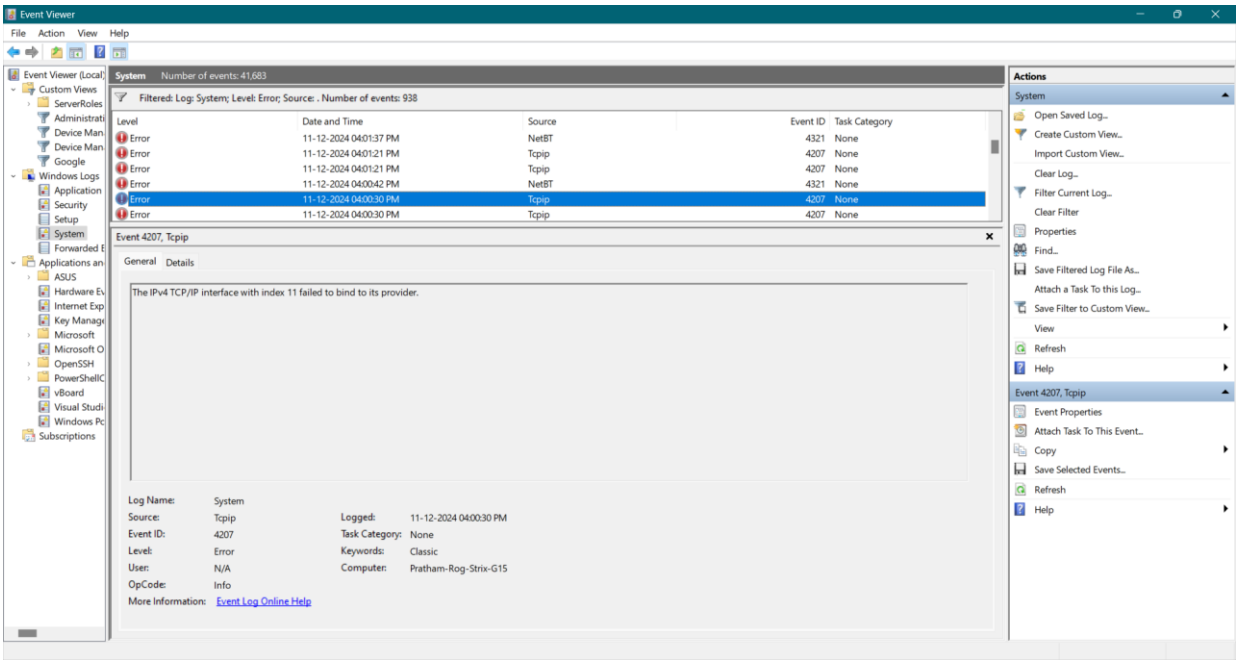
**3.** Select System Logs and filter by:



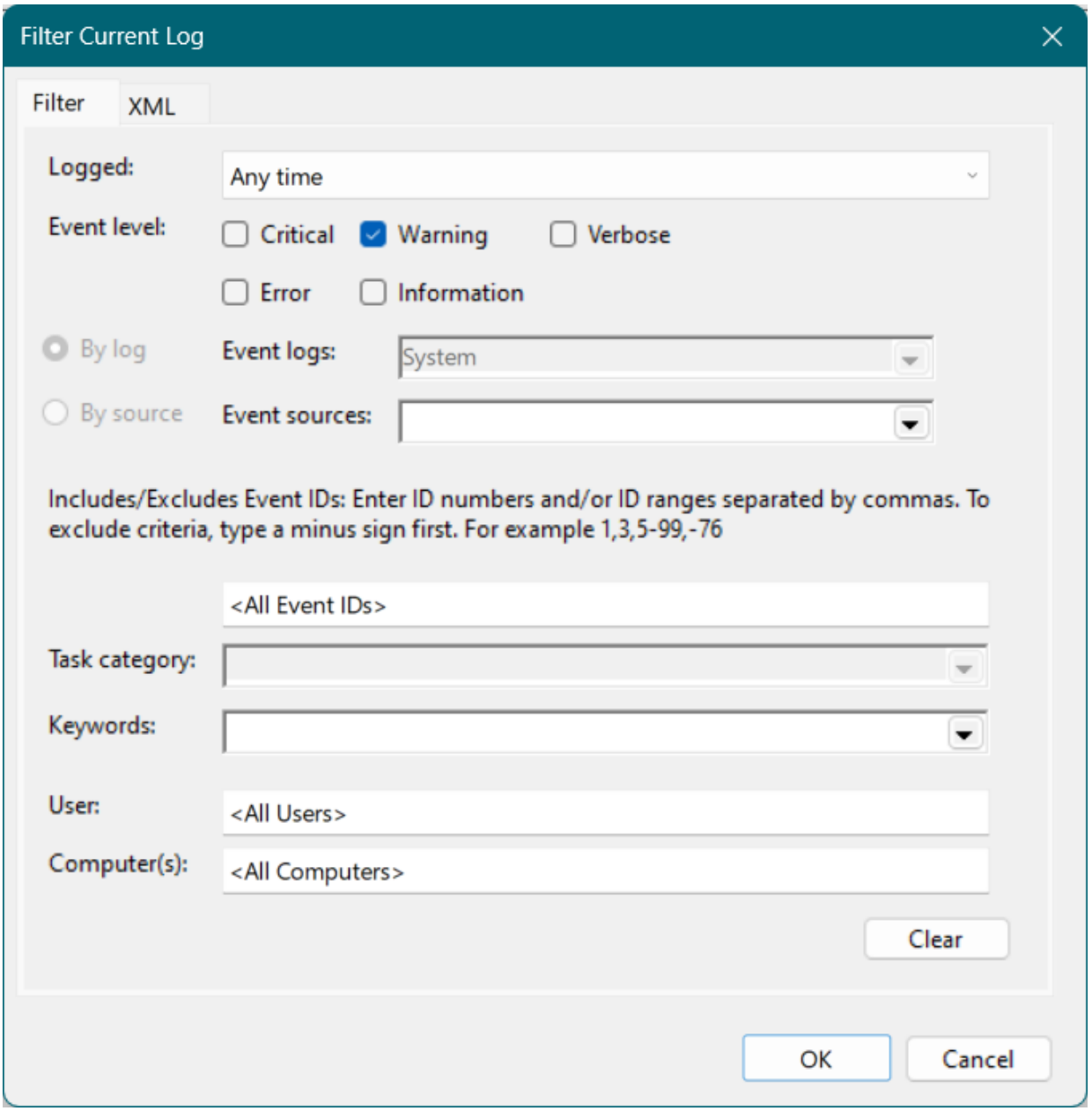
3.1. Event Level (e.g., Errors or Warnings).

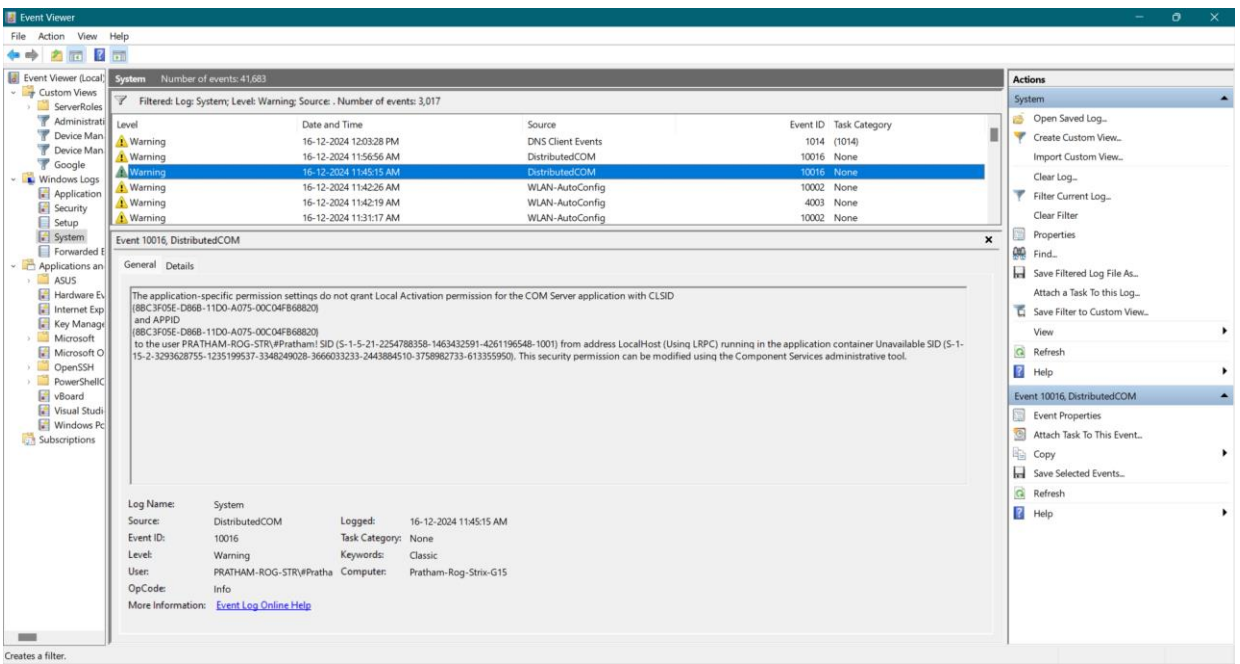
3.1.1. Error



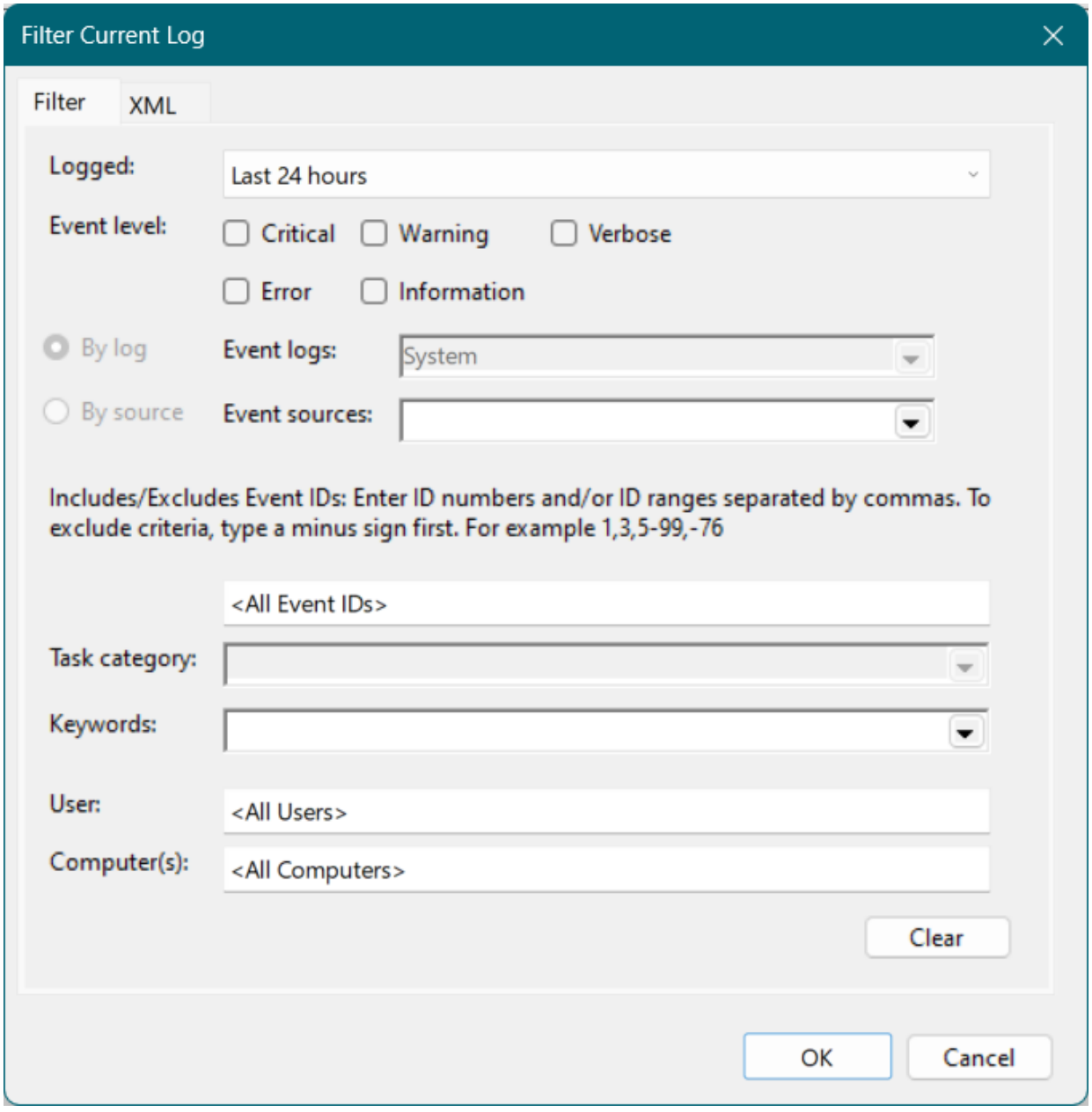



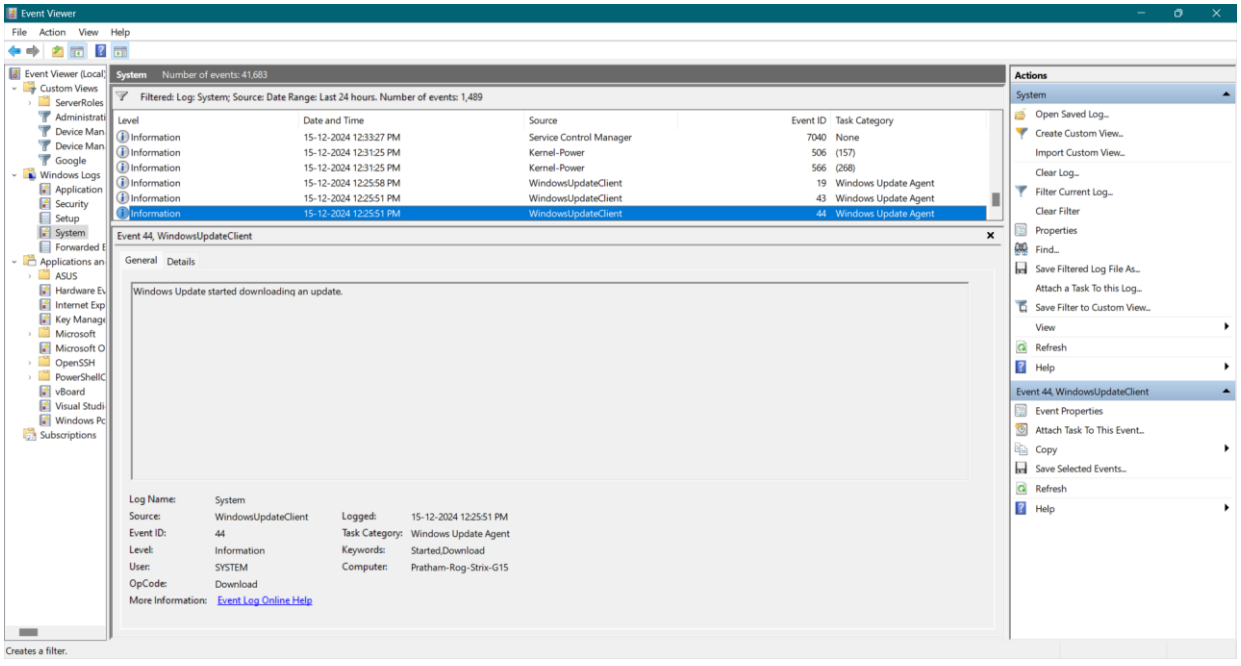
### 3.1.2. Warnings



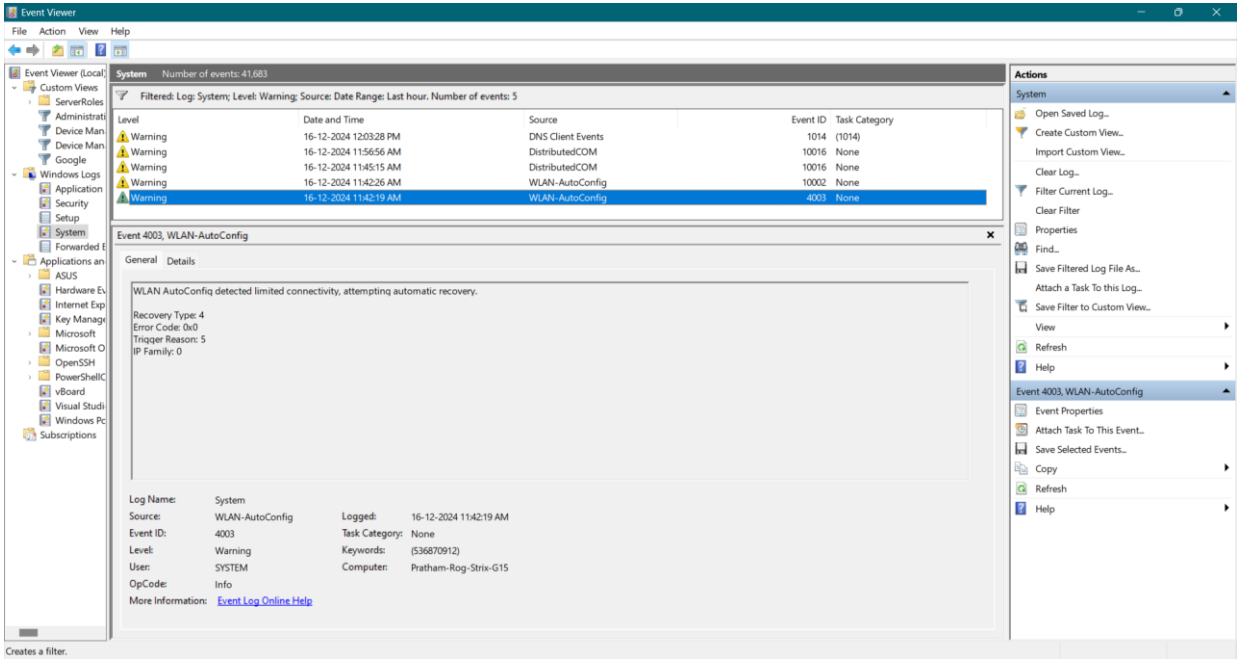



3.2. - Time period (e.g., last 24 hours).



4. Note down a critical or warning event, including the event ID and description.




**Warning Event**

**Event ID:** 4003

**Description:**

WLAN AutoConfig detected limited connectivity, attempting automatic recovery.

Recovery Type: 4

Error Code: 0x0

Trigger Reason: 5

IP Family: 0

5. **Outcome:** Learn how to filter and identify specific events.

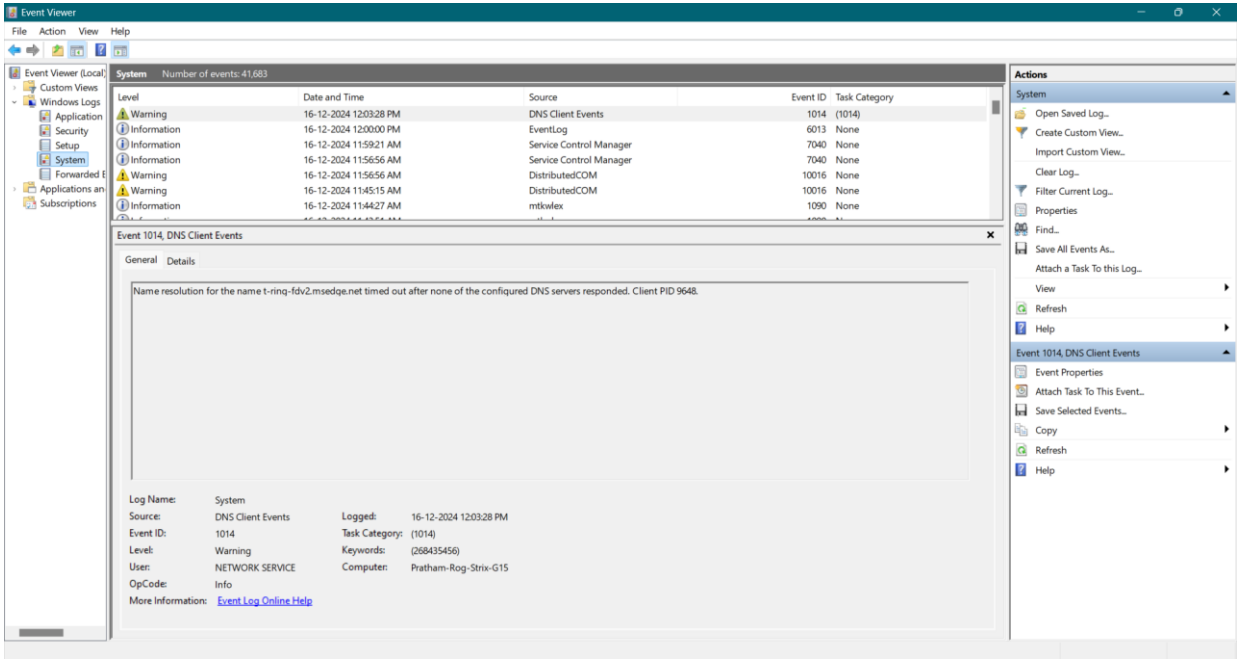
---

# Practical 2: Analyze Boot and Shutdown Events

**Objective:** Track system boot and shutdown activities.

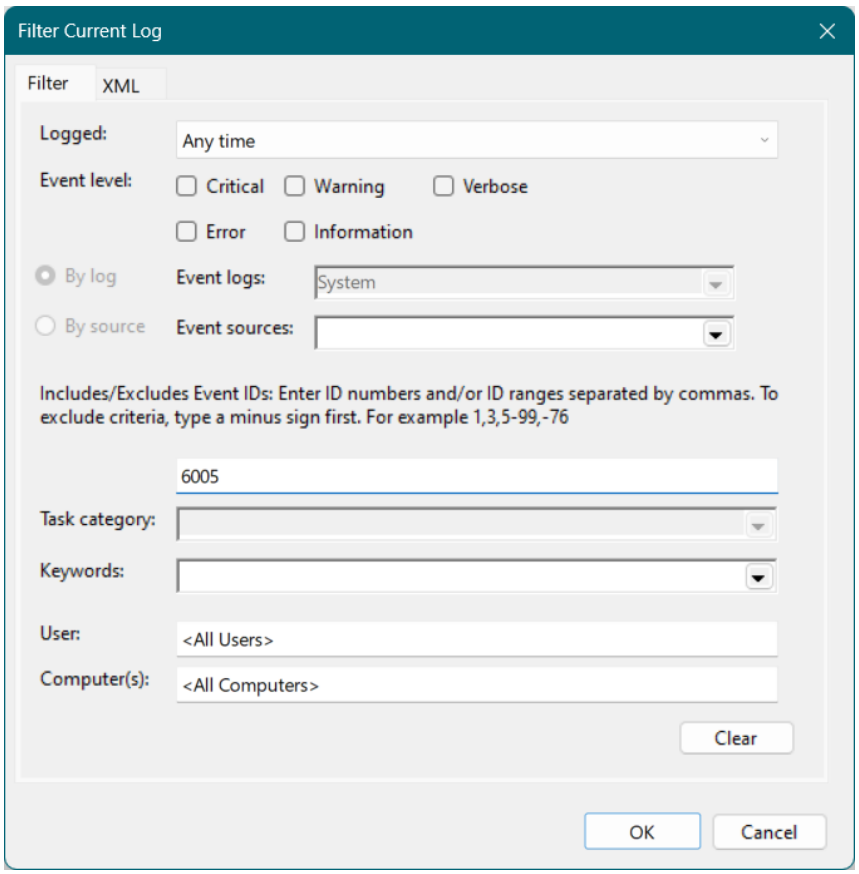
**Steps:**

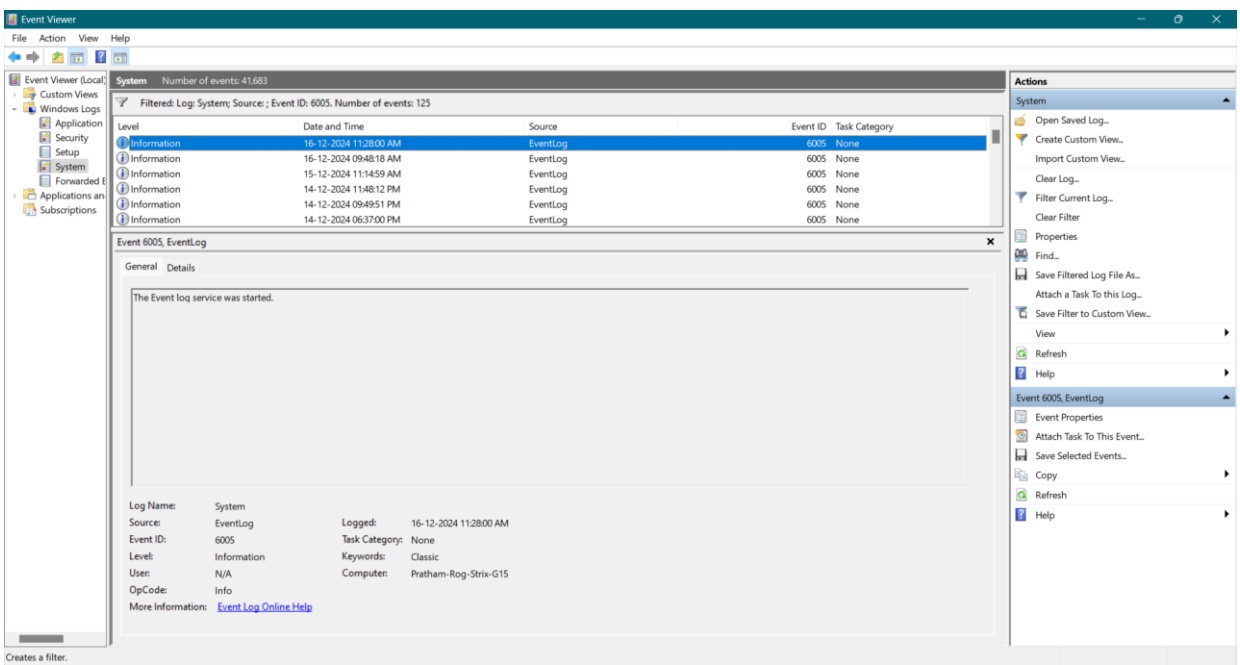
1. Navigate to Windows Logs > System.



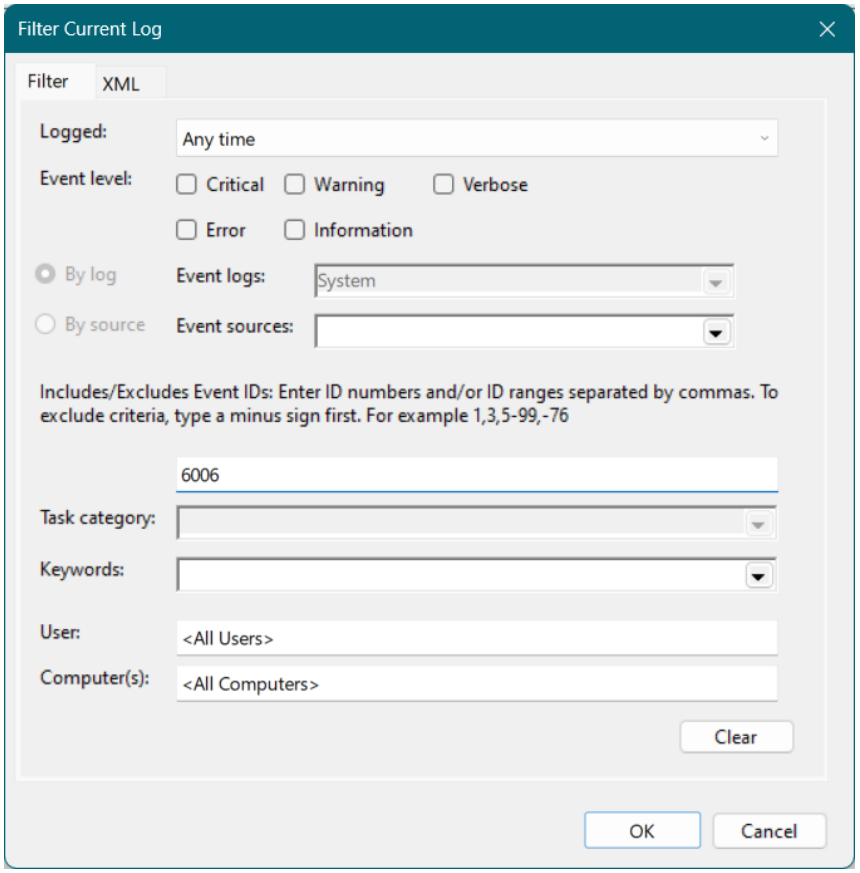
**2.** Use the following Event IDs to filter:

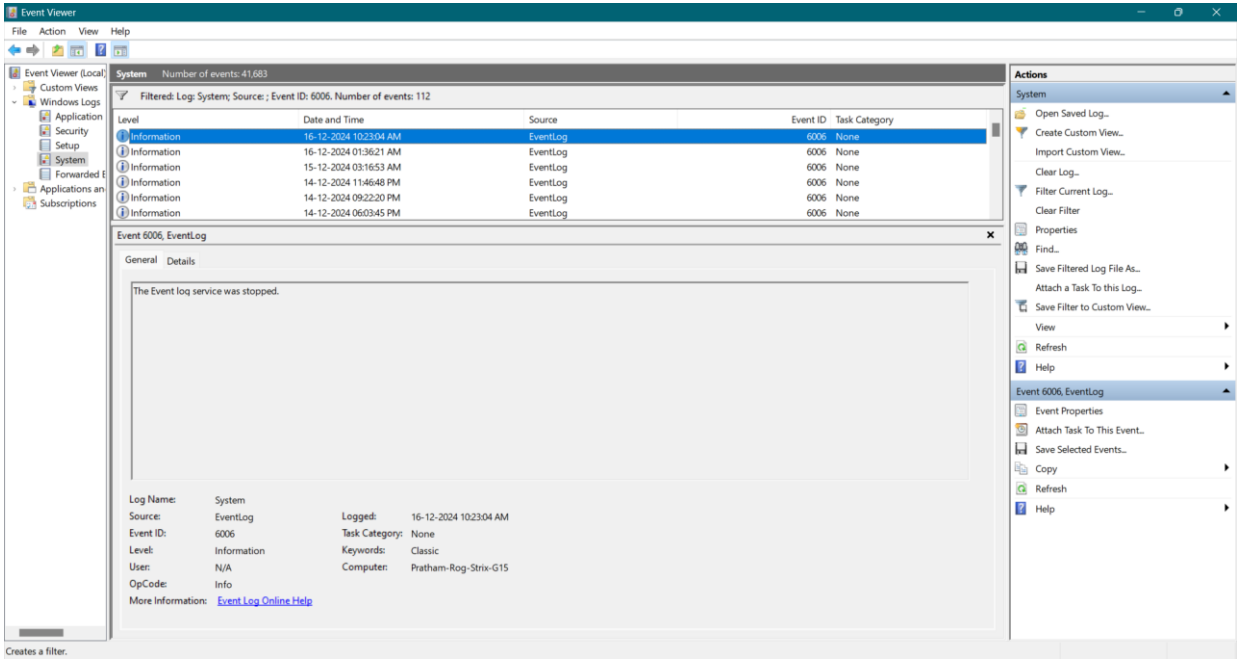
2.1. 6005: System Startup.



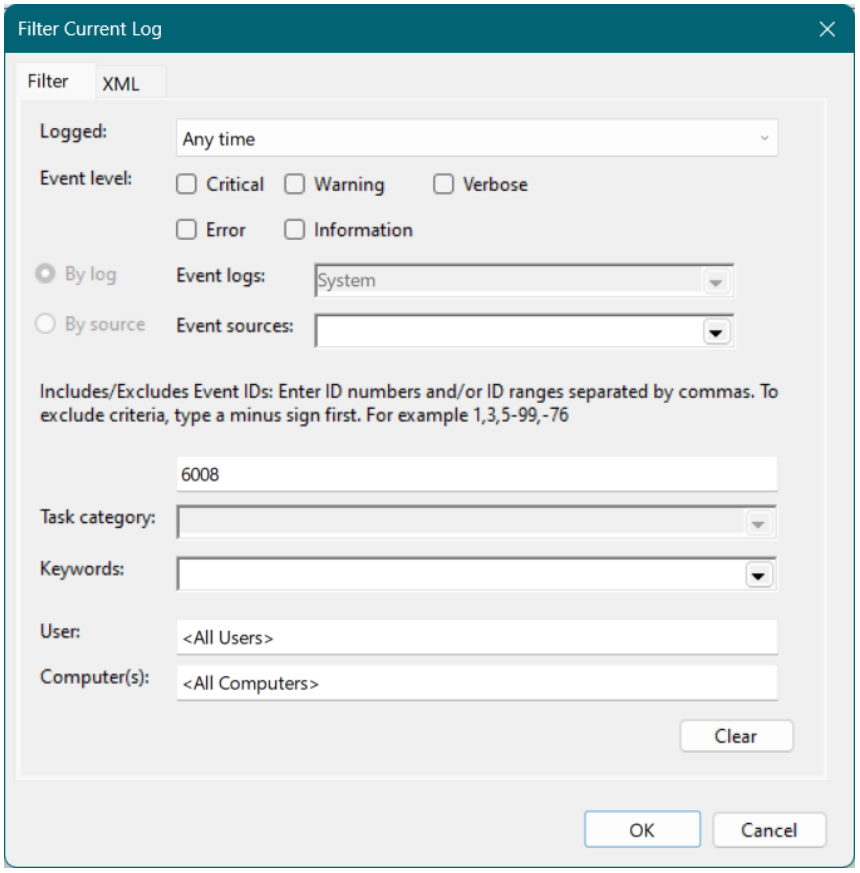



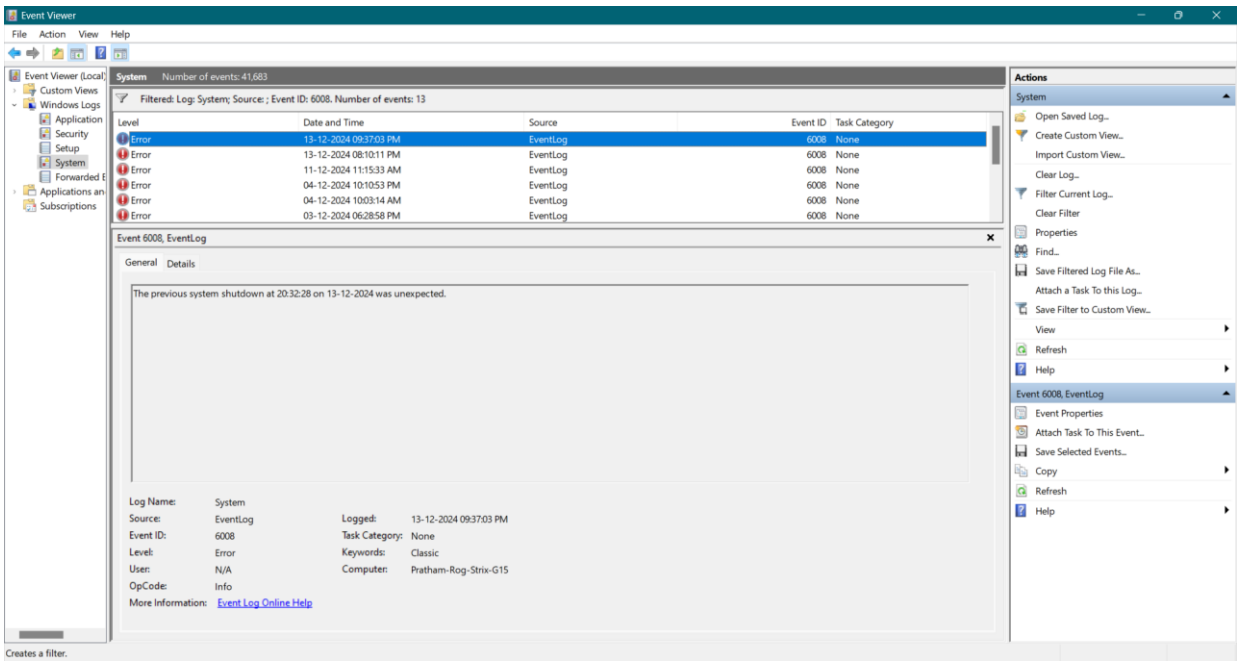
## 2.2. 6006: System Shutdown.



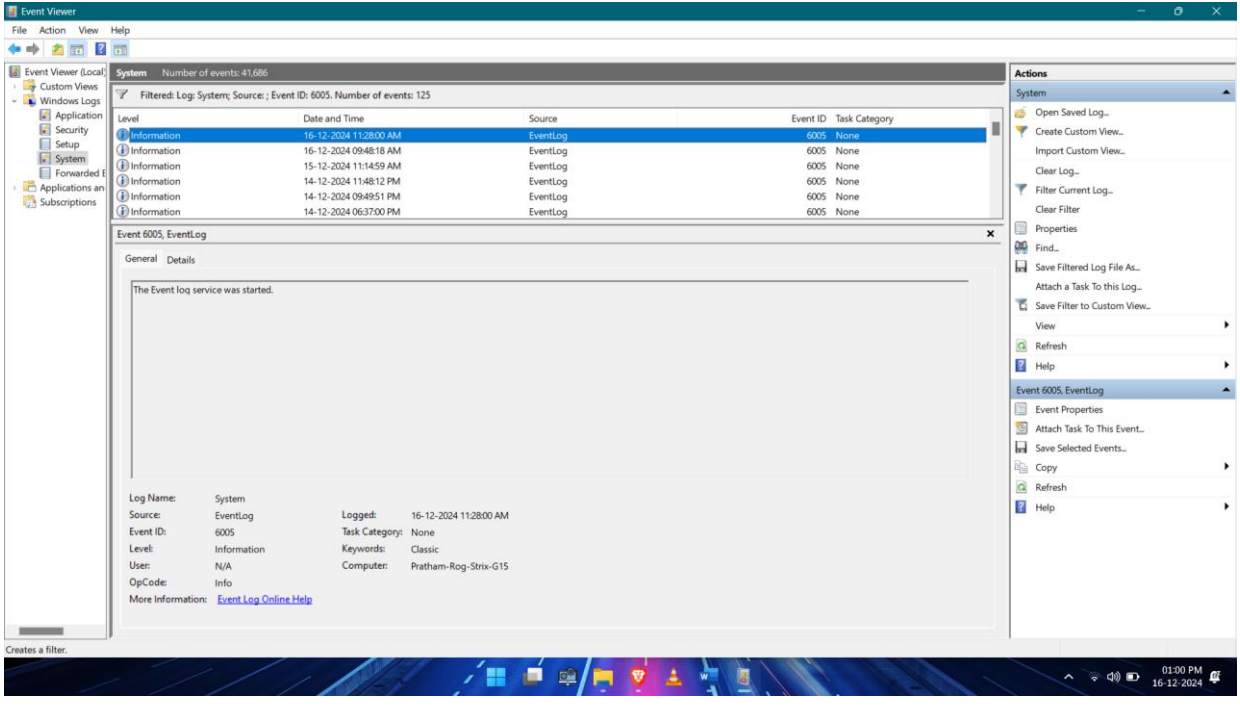



## 2.3. 6008: Unexpected Shutdown.



**3.** Analyze the timestamps to identify system uptime.

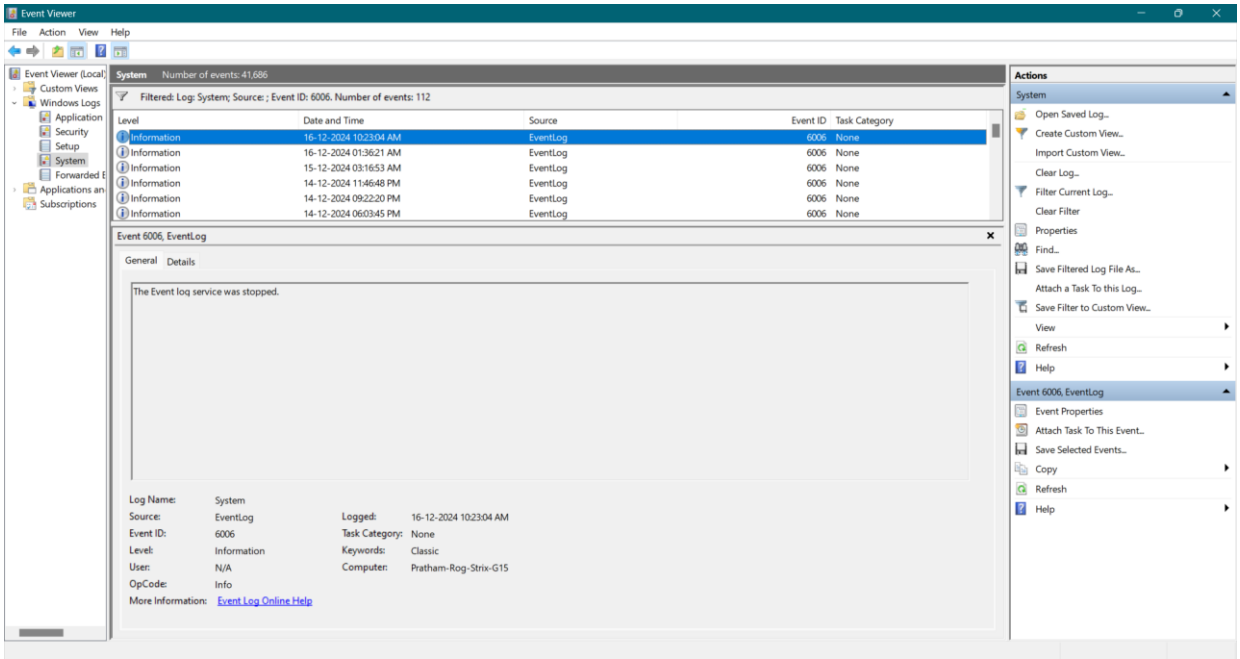



System Startup Time: 16-12-2024 11:28:00 AM

Current Time 16-12-2024 01:00:00 PM

System Uptime: 1 hour 32 minutes

**4.** Document any abnormal shutdowns with their descriptions.




**Event ID:** 6006

**Logged:** 16-12-2024 10:23:04 AM

**Description:** The Event log service was stopped.

**5.** Outcome: Understand how to monitor system startup and shutdown activities.

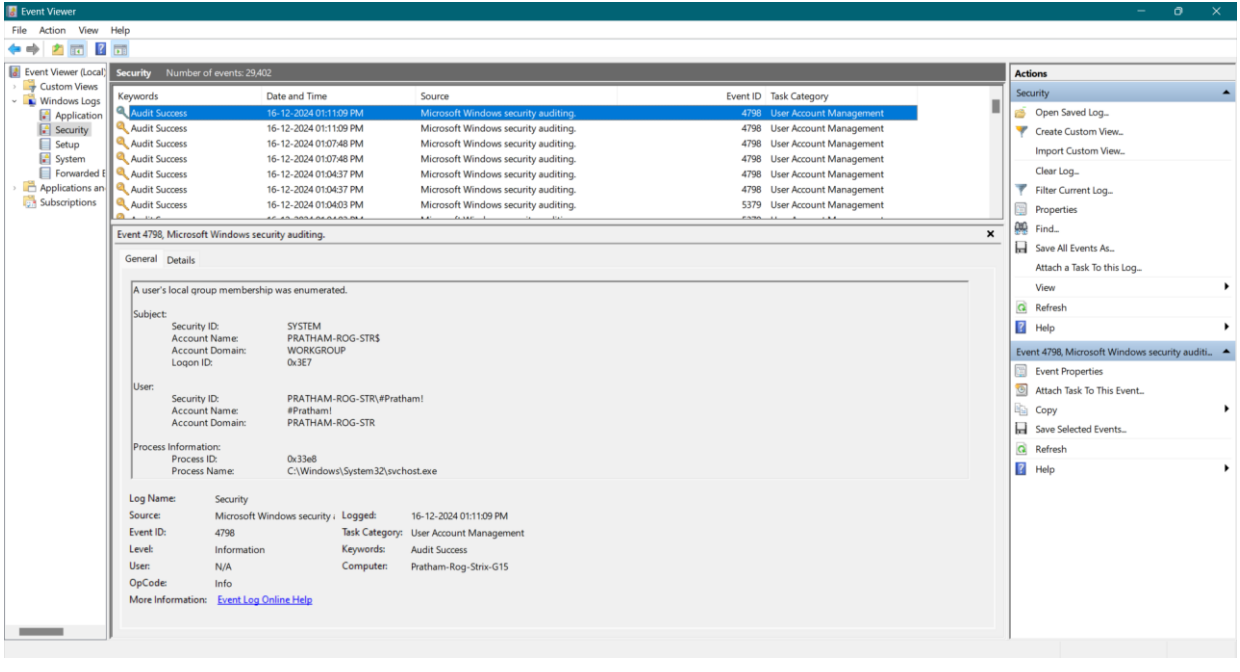
---

## Practical 3: Audit Logon Events

**Objective:** Monitor user logon and logoff events.

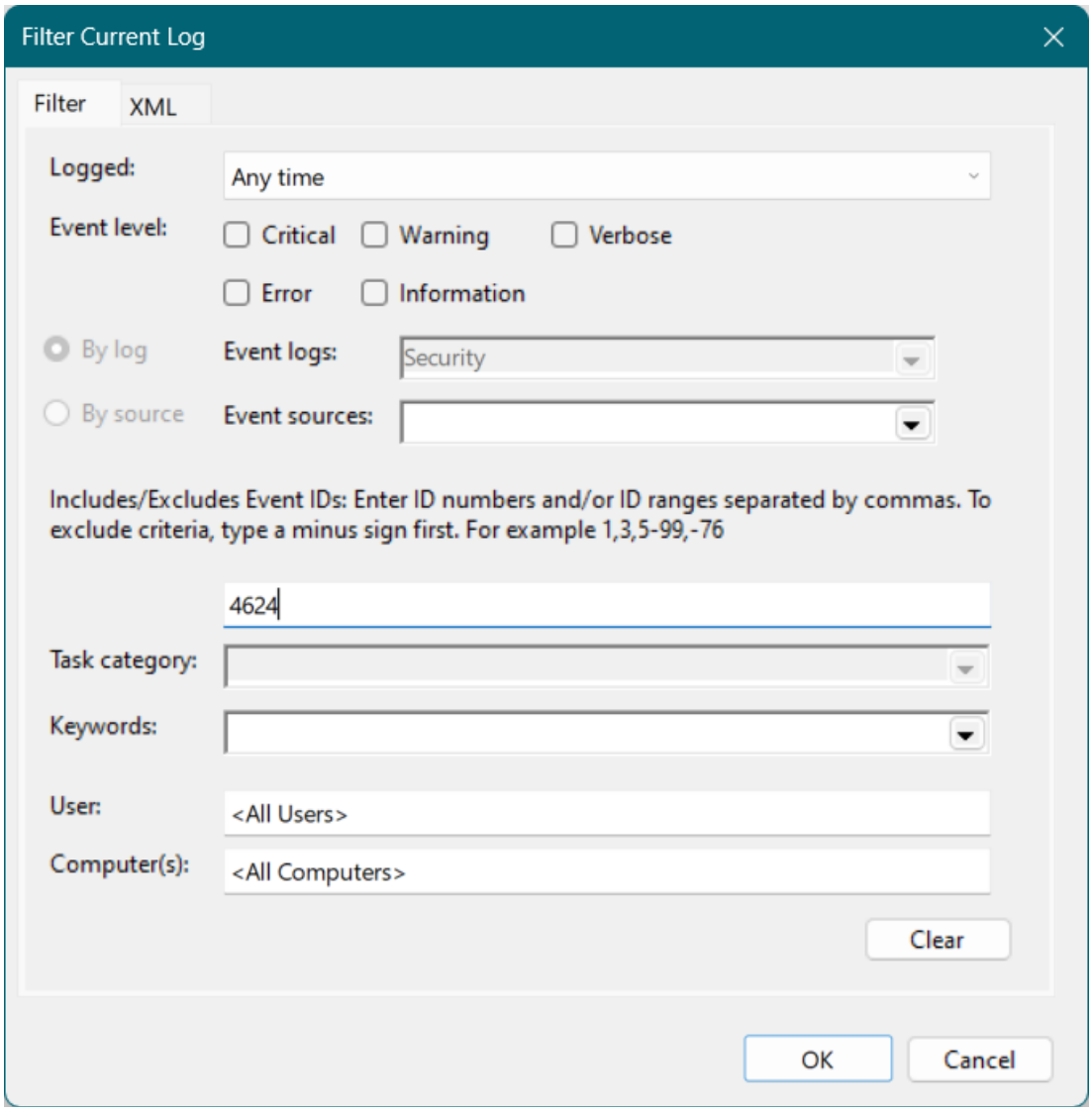
**Steps:**

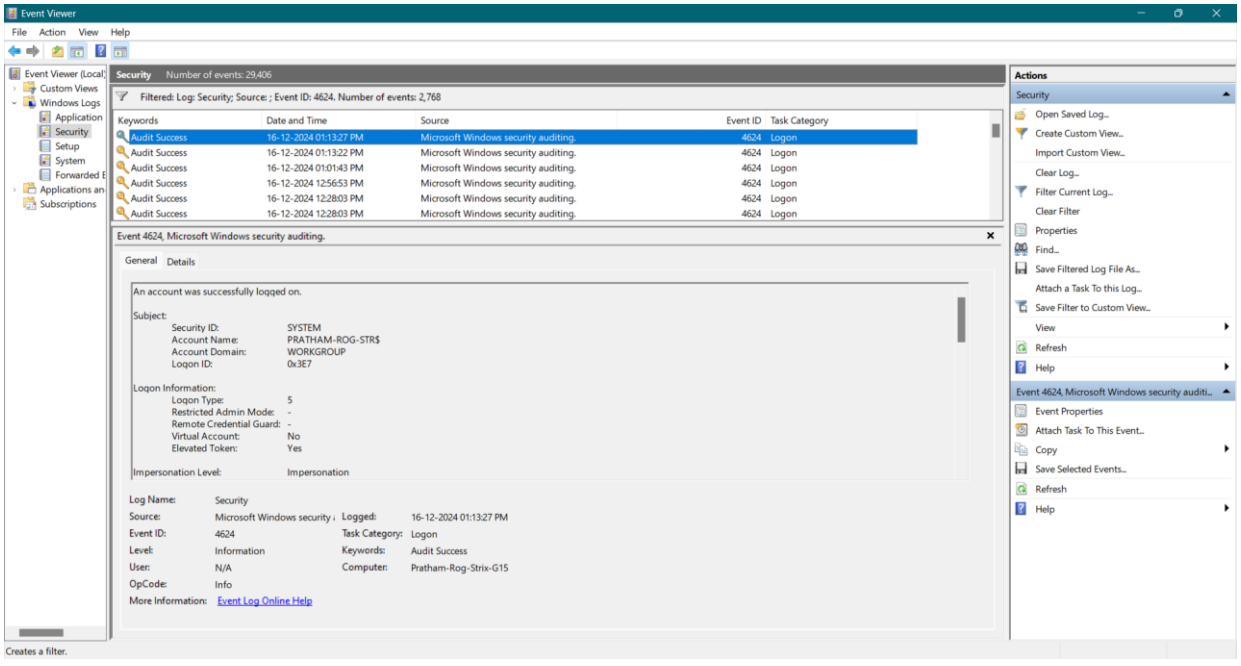
1. Navigate to Windows Logs > Security.



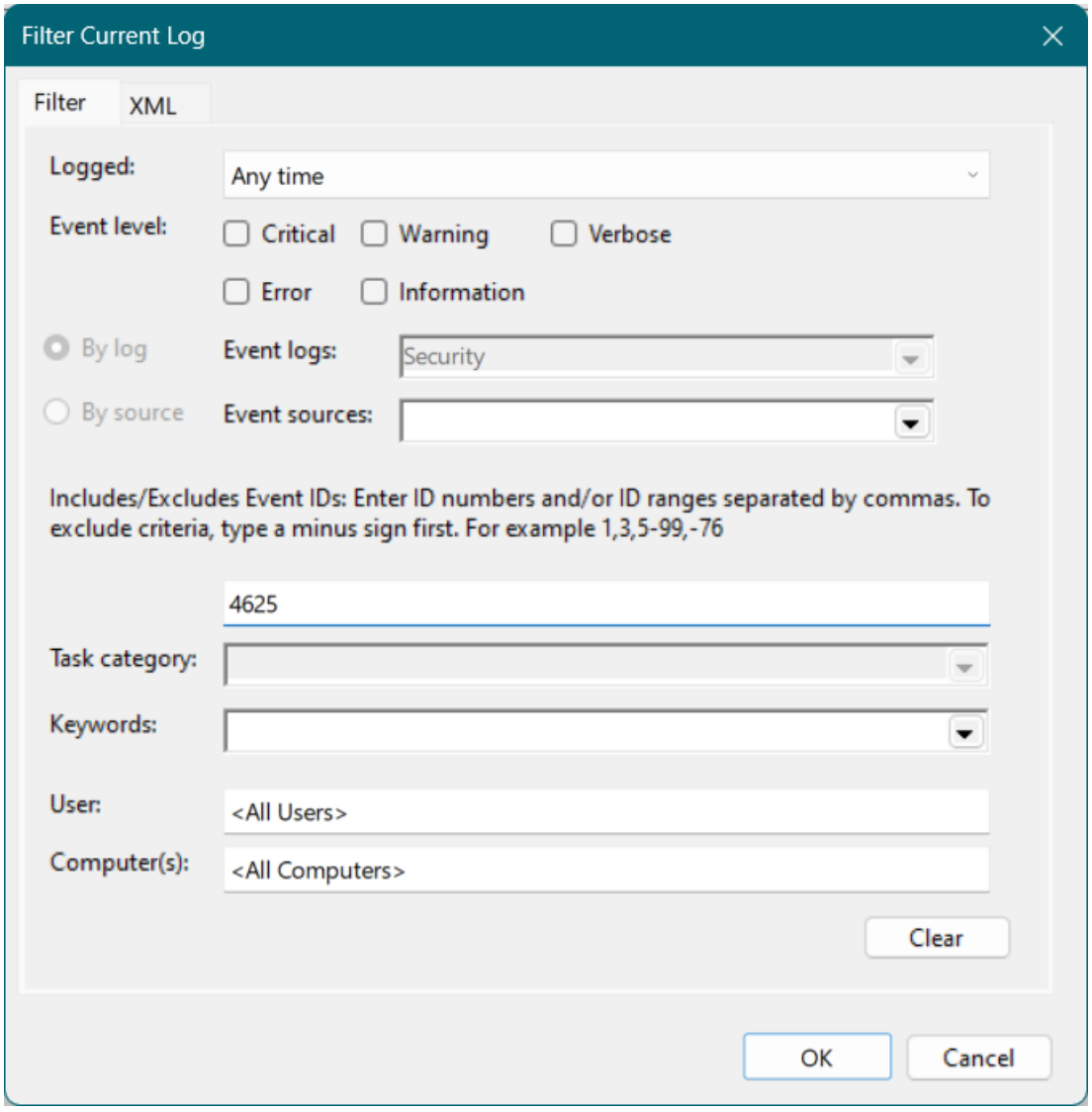
2. Filter by Event IDs:

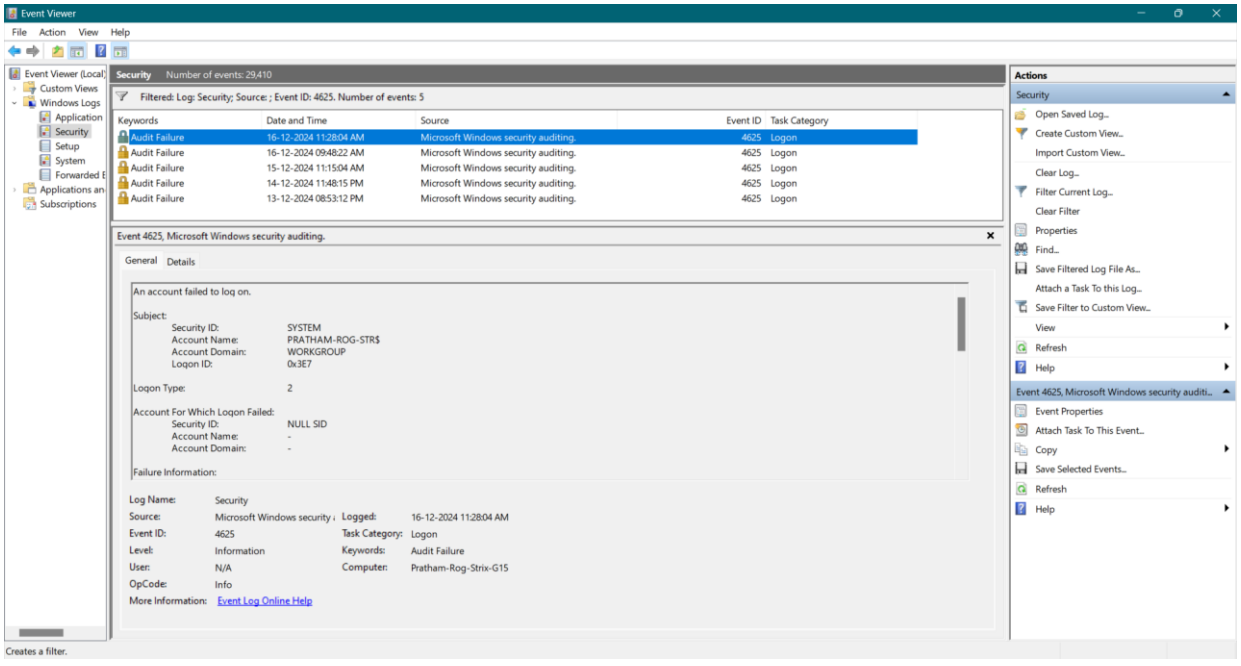
2.1. 4624: Successful logon.



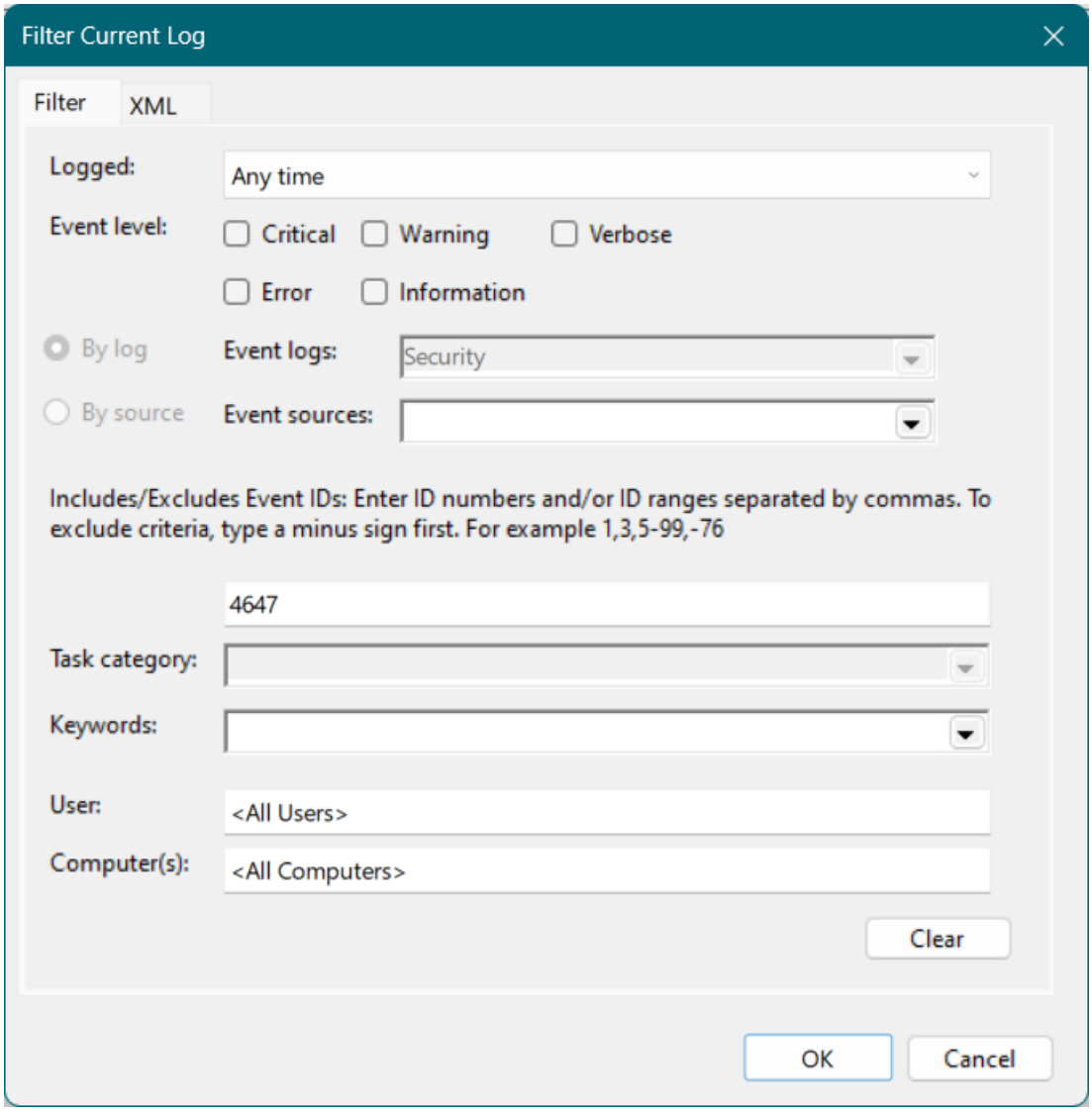



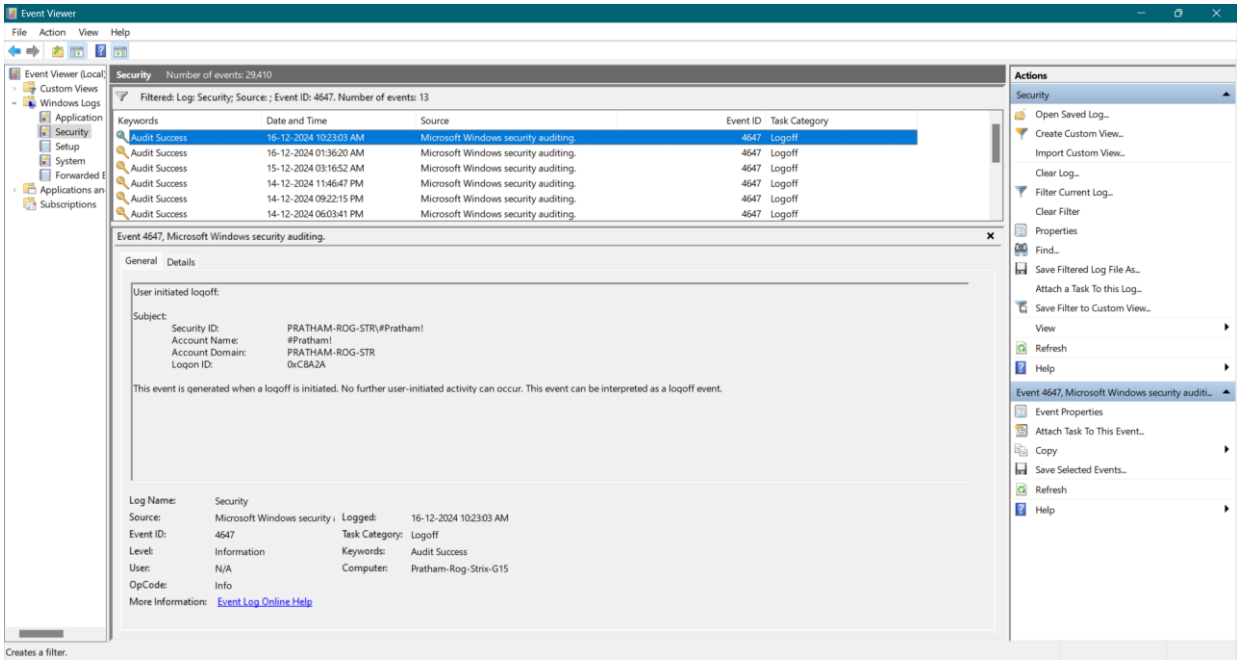
2.2. 4625: Failed logon attempt.



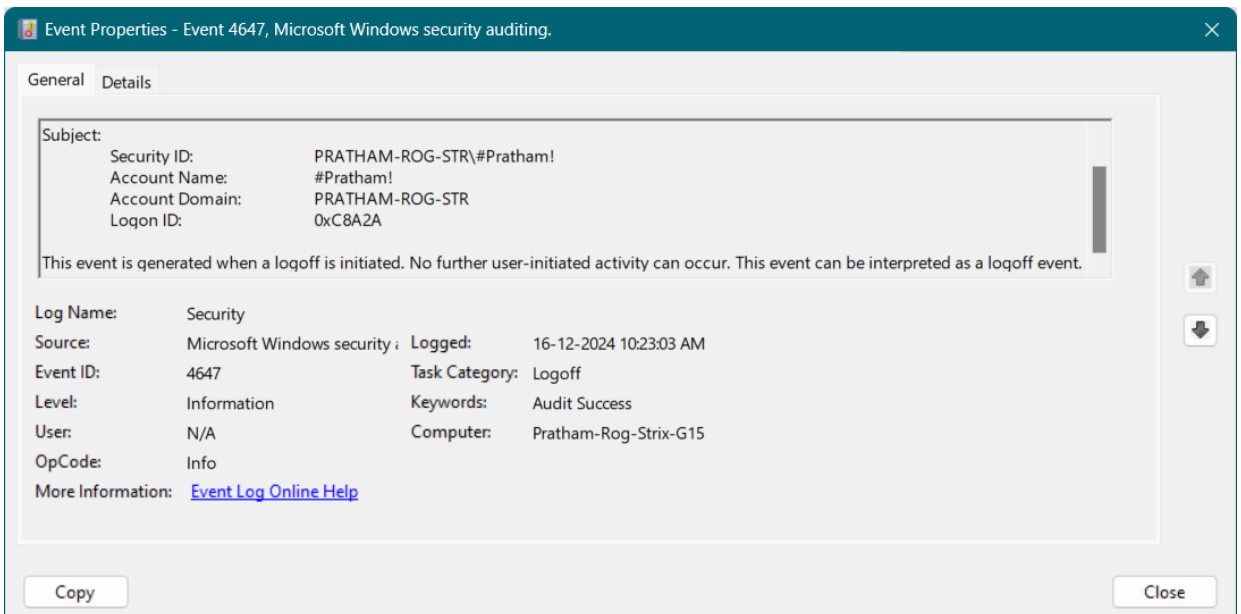
2.3. 4647: User-initiated logoff.



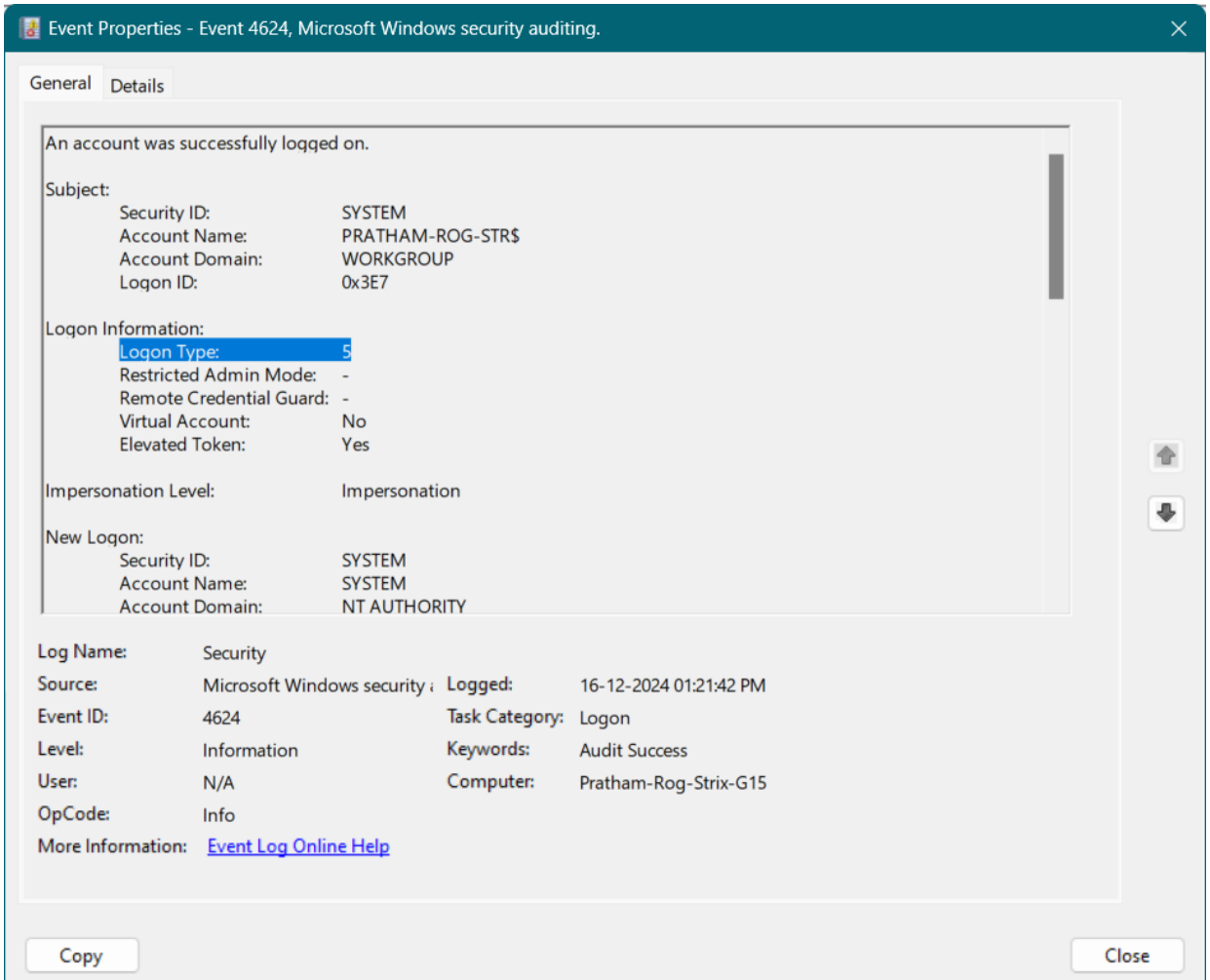
3. Identify:

3.1. The user account involved.



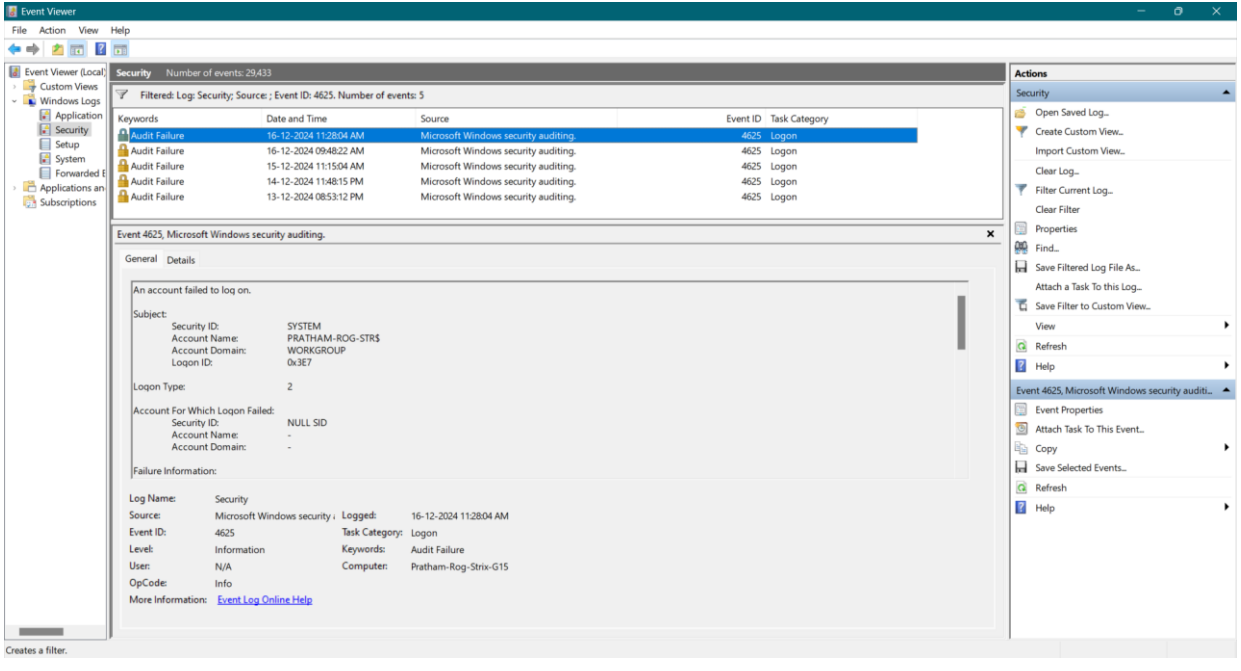

**User:** #Pratham!

3.2. Logon types (interactive, remote desktop, etc.).




Logon Type: 5 - Service Logon

3.3. Investigate any failed logon attempts for potential security issues.




There are only 5 failed login attempts, but any of it are not suspicious.

4. Outcome: Learn to track and audit user authentication.

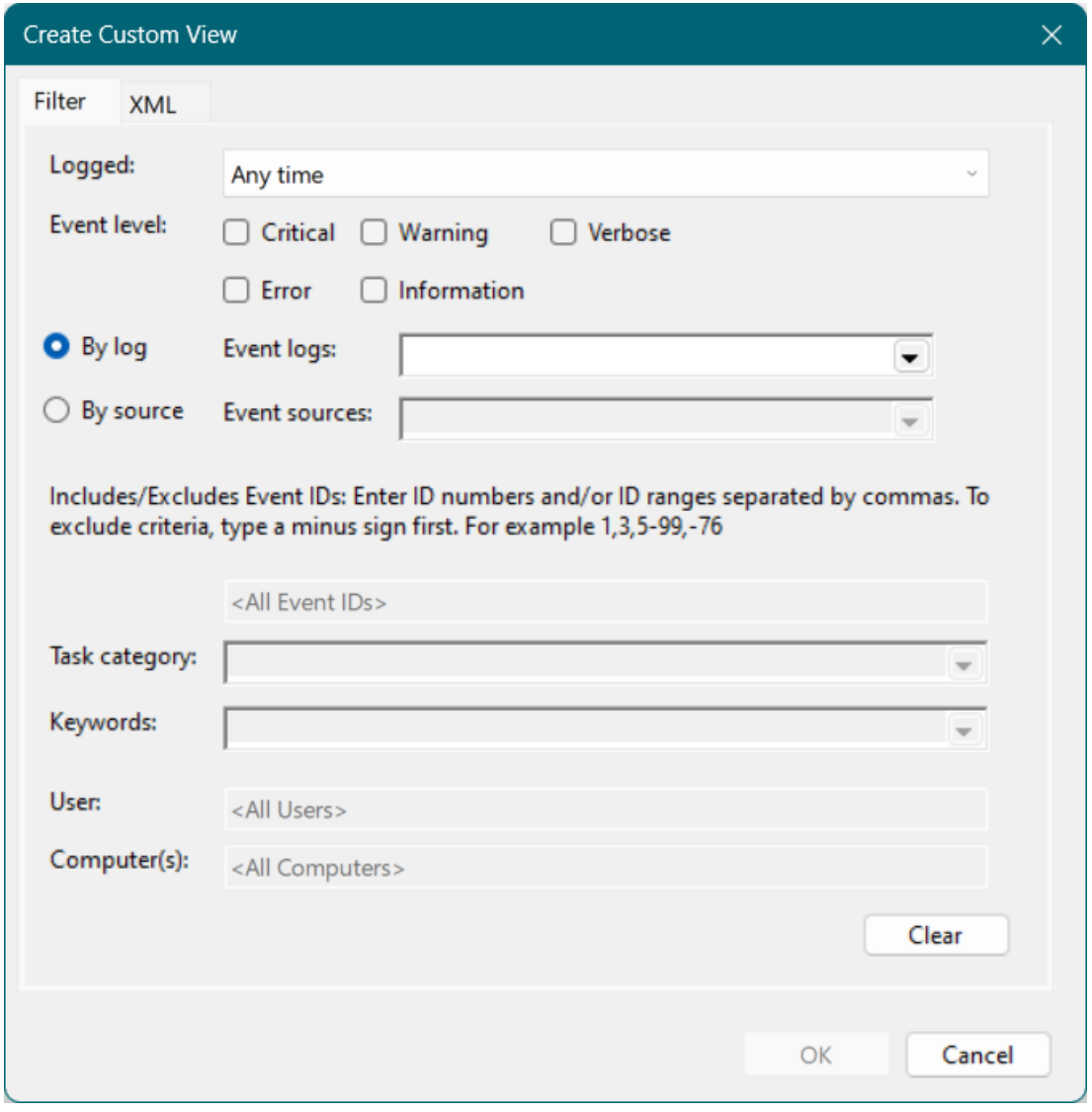
---

## Practical 4: Create a Custom View

**Objective:** Create a custom view for critical system events.

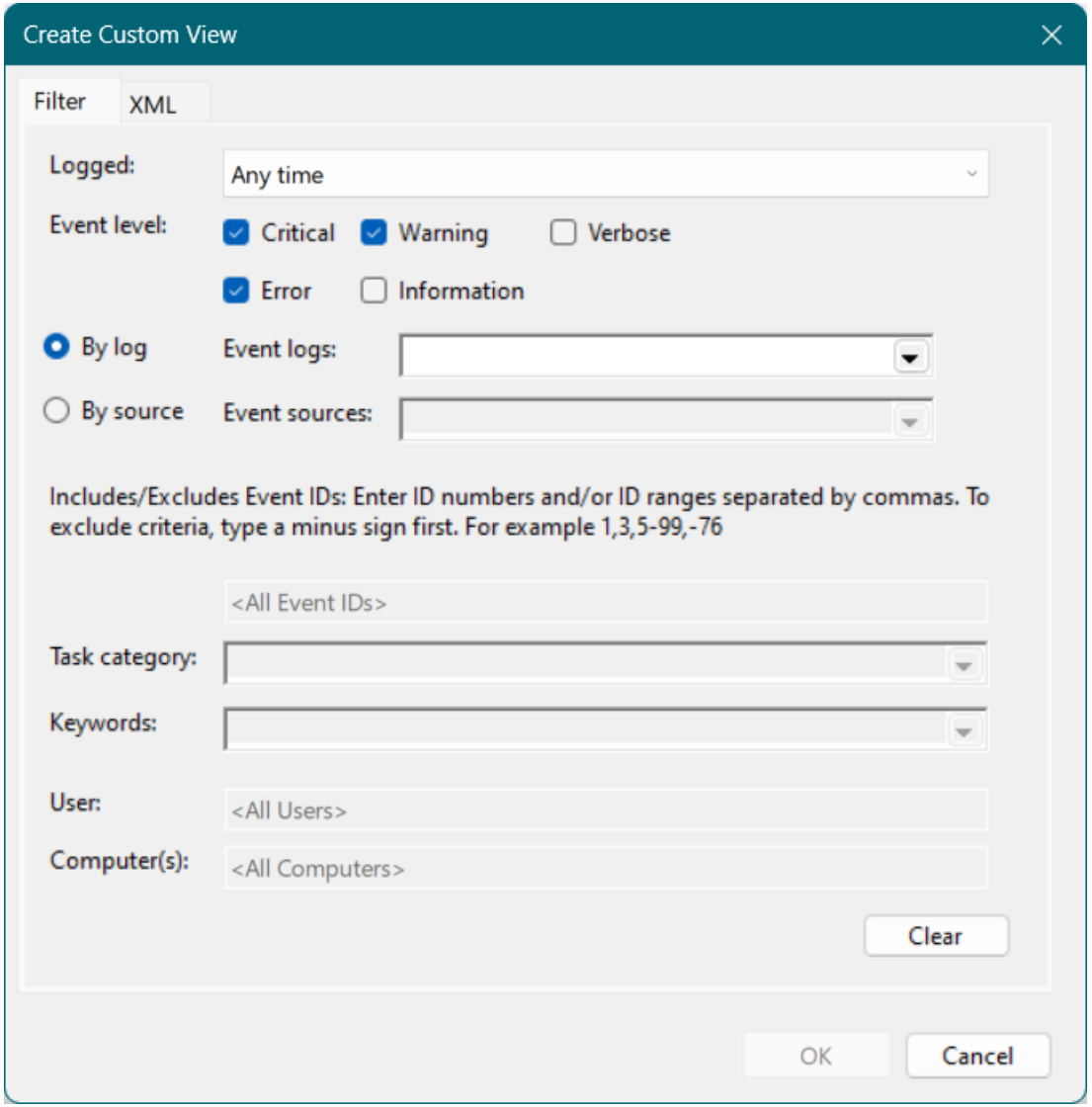
**Steps:**

1. In Event Viewer, click Action > Create Custom View.

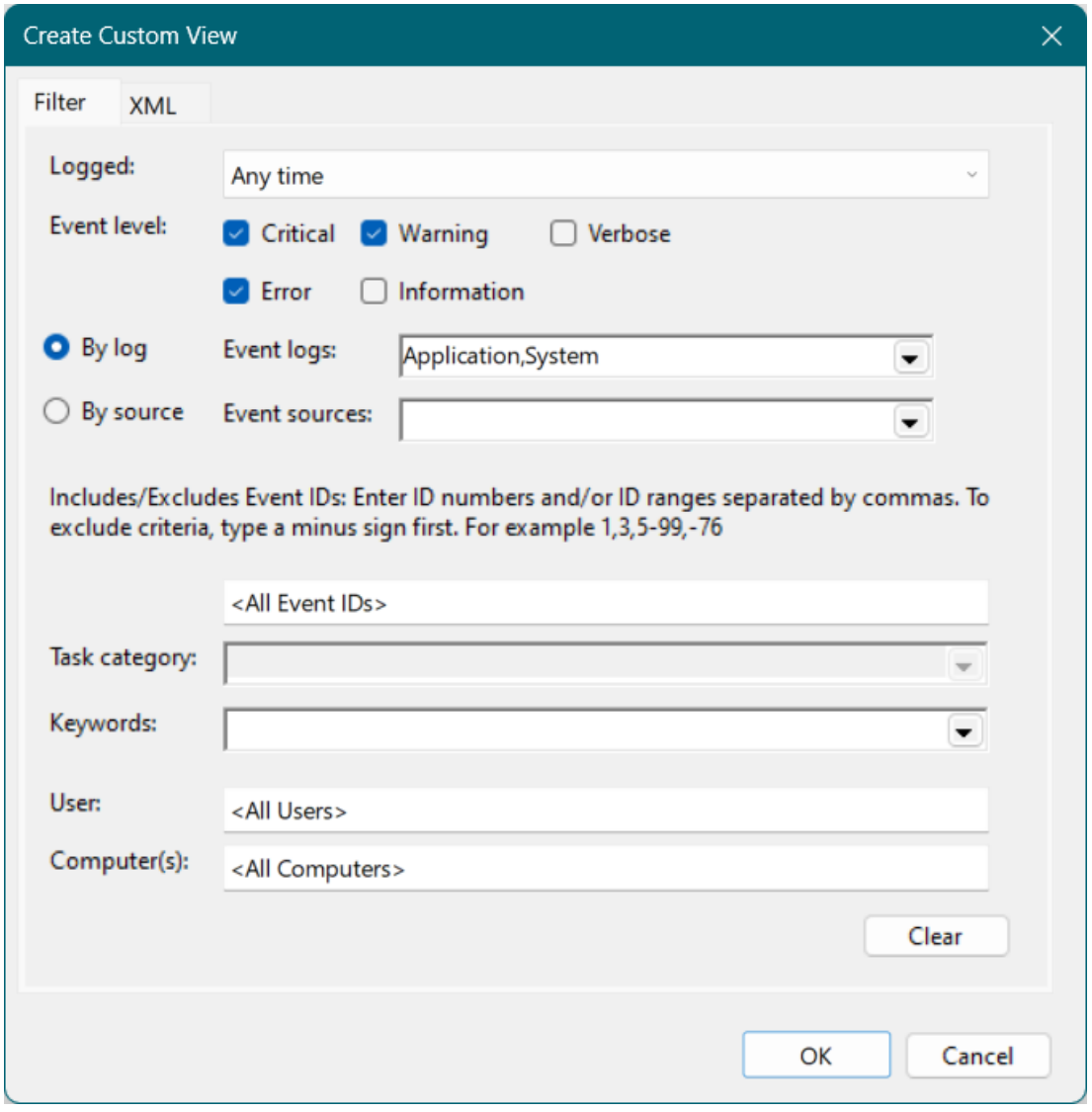


2. Select:

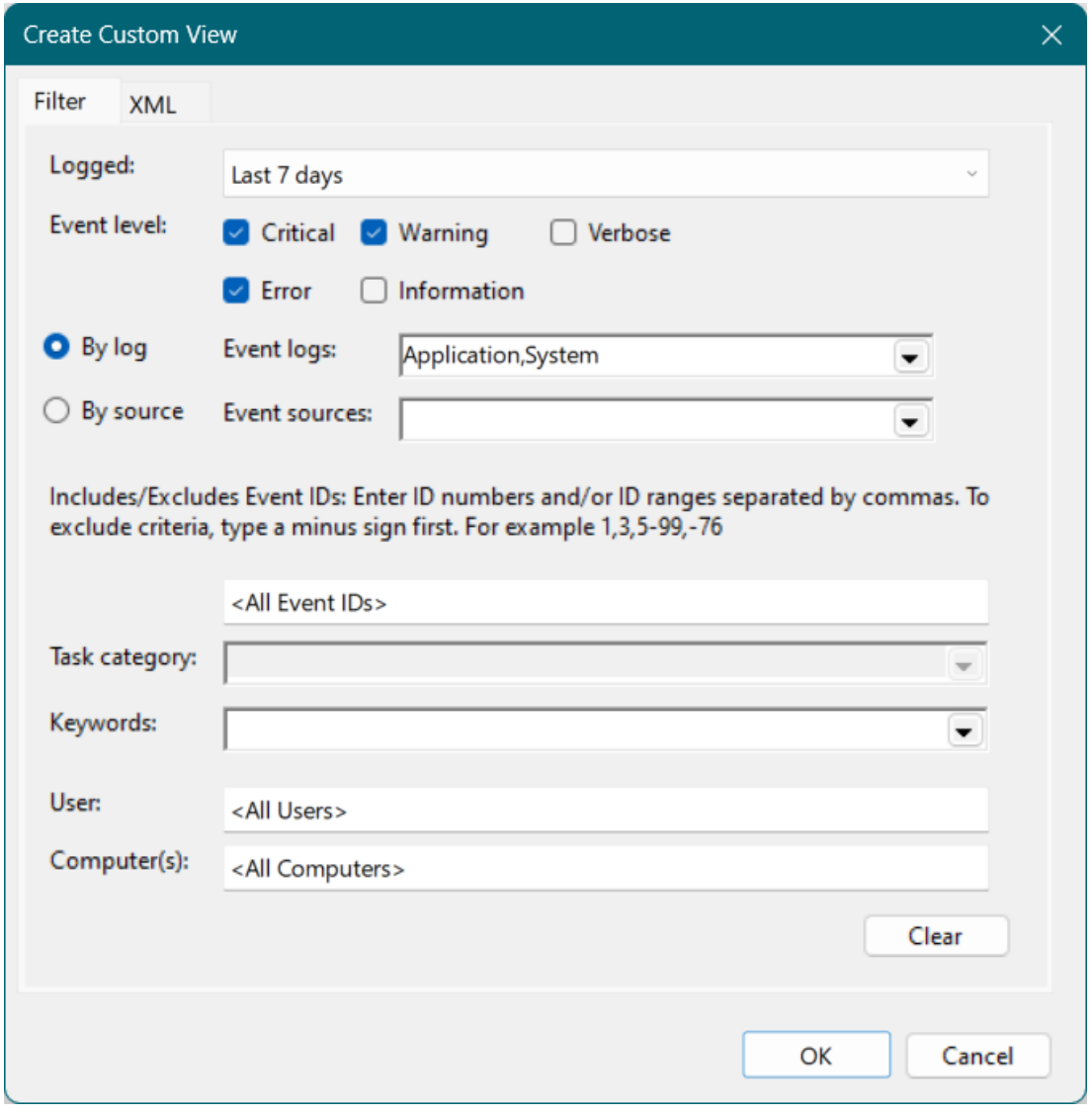
2.1. Event Levels: Critical, Warning, and Error.



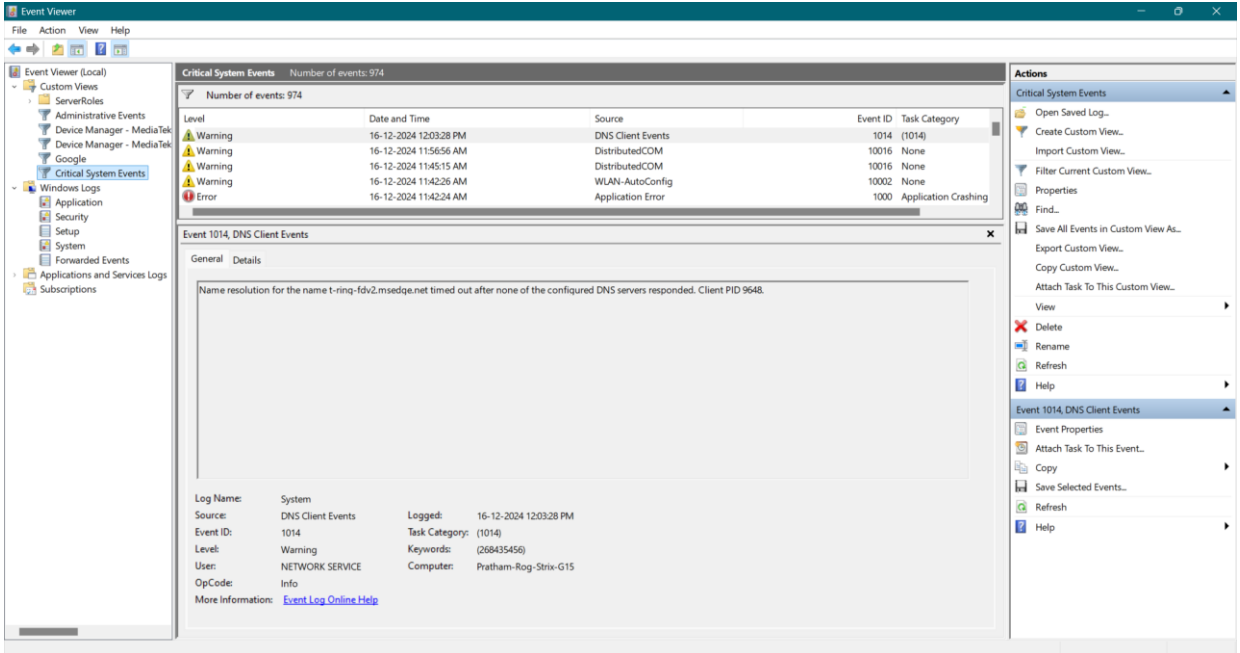
2.2. Logs: System and Application.



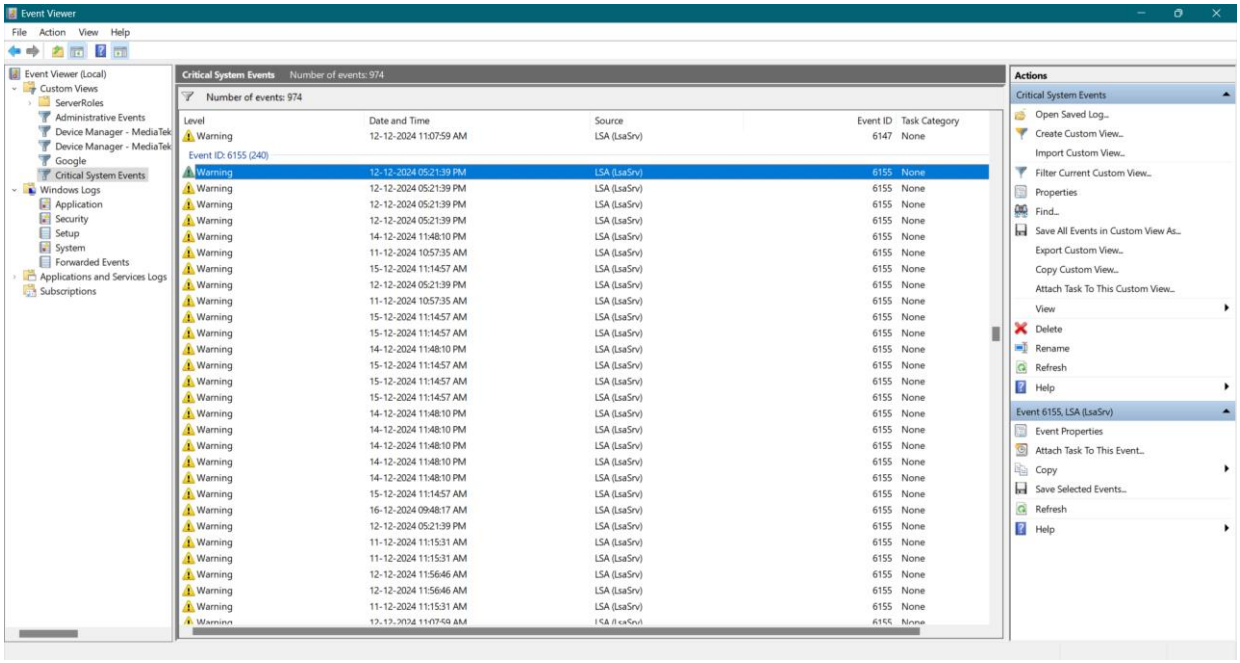
2.3. Time Range: Last 7 days.

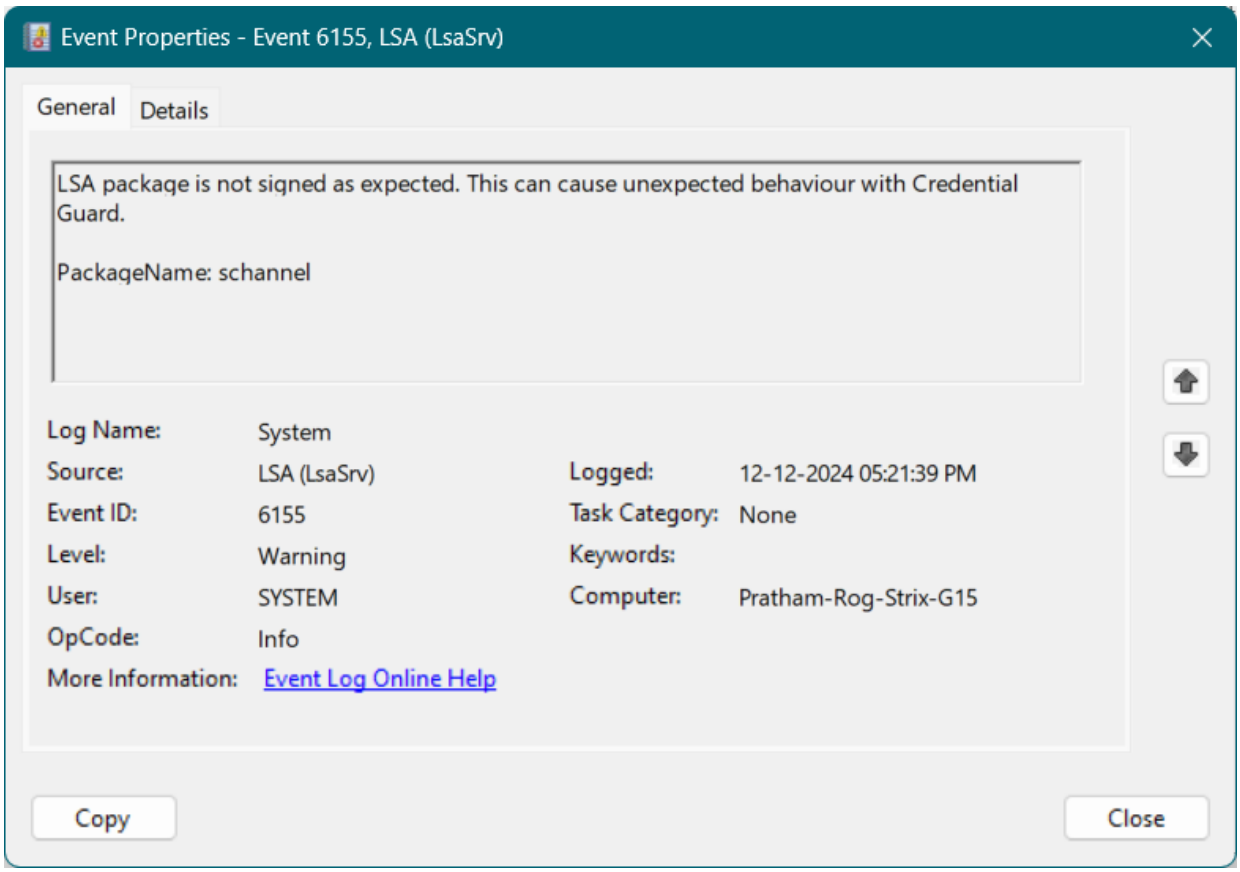


**3.** Save the custom view with a name (e.g., "Critical System Events").



**4.** Document and analyze any recurring critical errors.




There are ***240 Recurring Logs*** of **Event ID: 6155**

Description:

LSA package is not signed as expected. This can cause unexpected behaviour with Credential Guard.

PackageName: schannel

**5.** **Outcome:** Learn to customize event views for efficient monitoring.

---