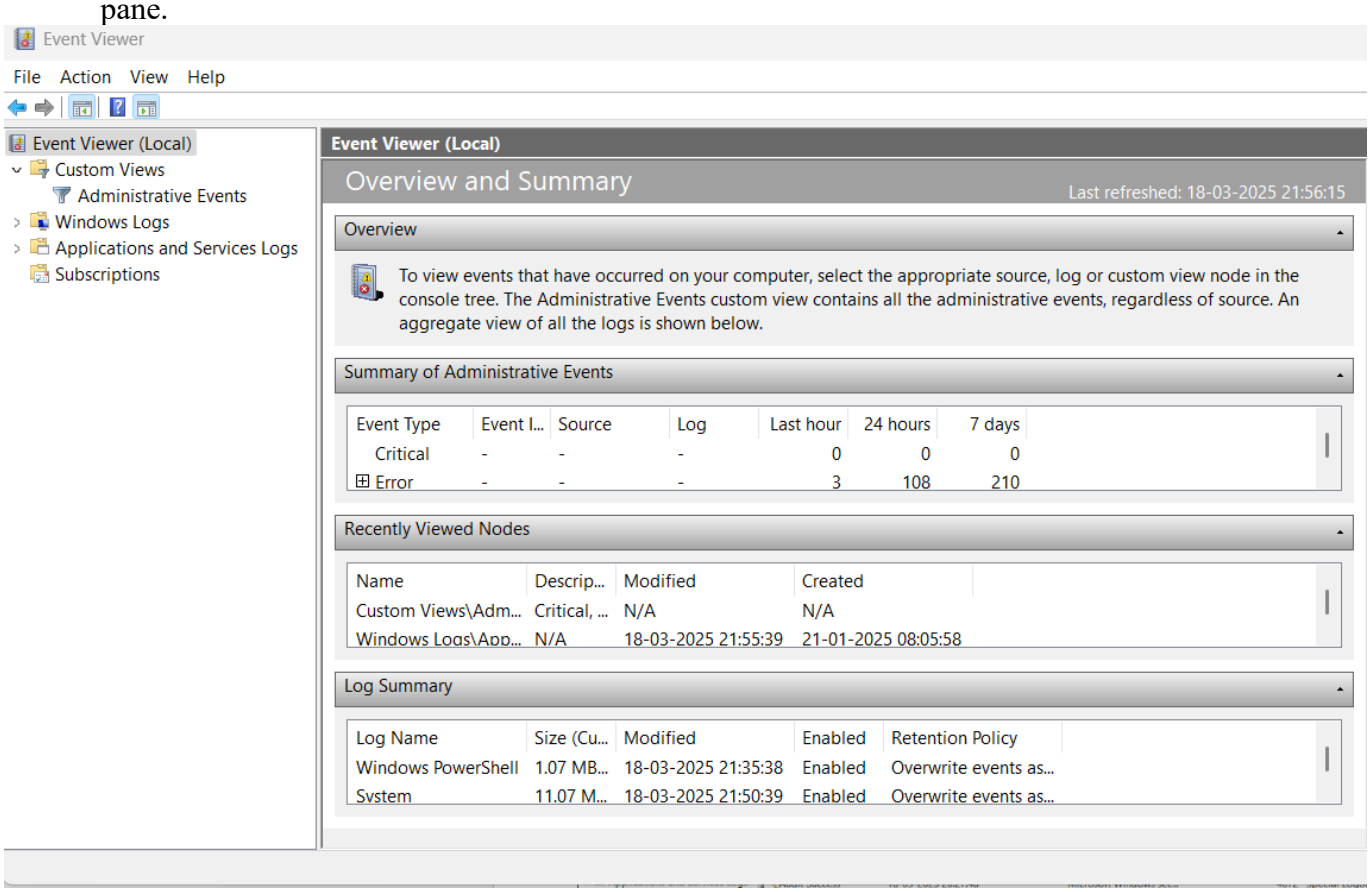
Cyber Forensics - 24CY611

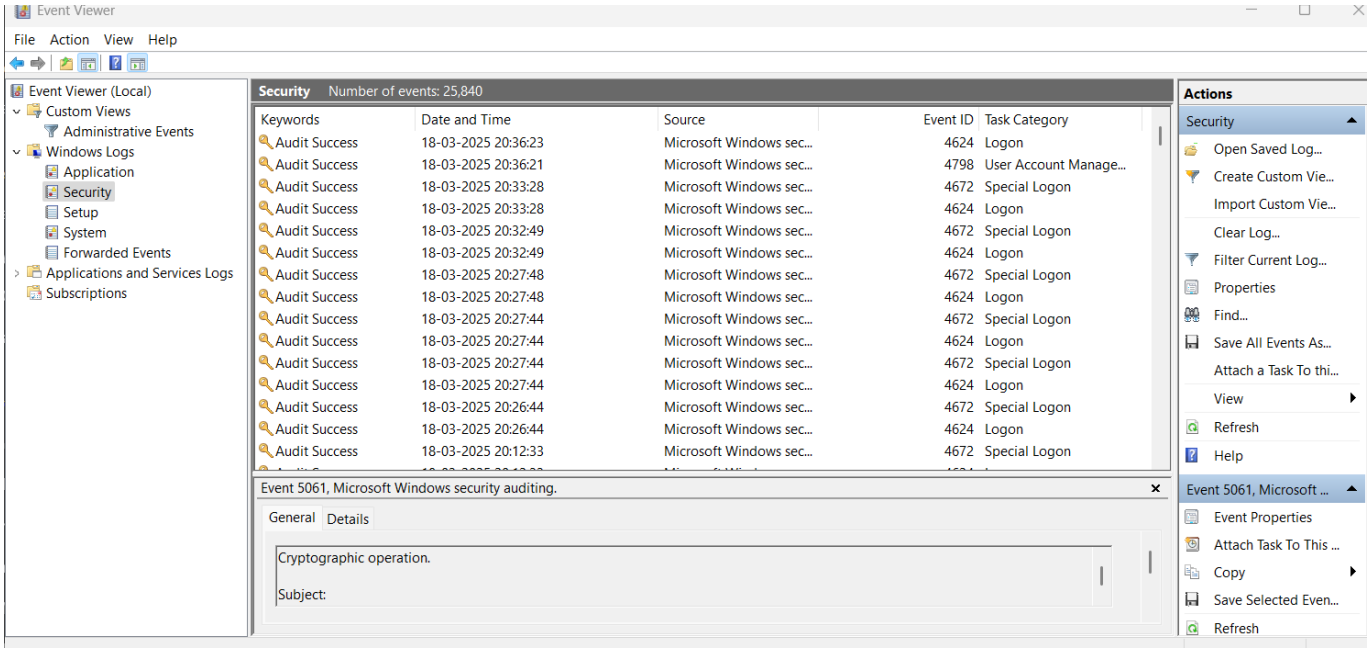
Lab 7 - Network Forensics

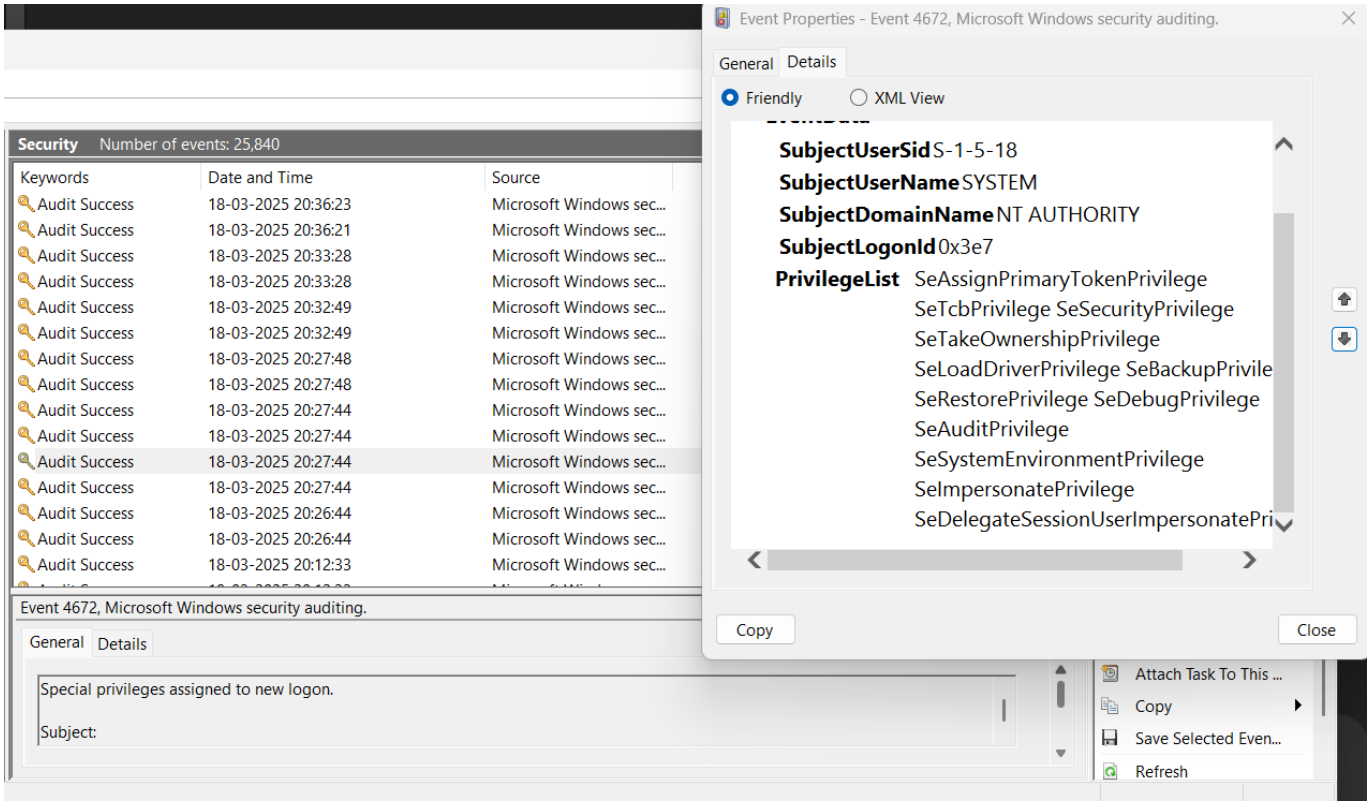
Capturing and Analyzing Logs Using Windows Event Viewer

- **Open Event Viewer**: Launch the Event Viewer application on your Windows system.
- **Expand Event Viewer (Local)**: If not already expanded, click to reveal its contents in the left pane.



- **Access Windows Logs**: Expand the "Windows Logs" section to view different log categories.
- **Select a Log Category**: Choose from options like "Application," "Security," "Setup," "System," or "Forwarded Events" to analyze specific logs.

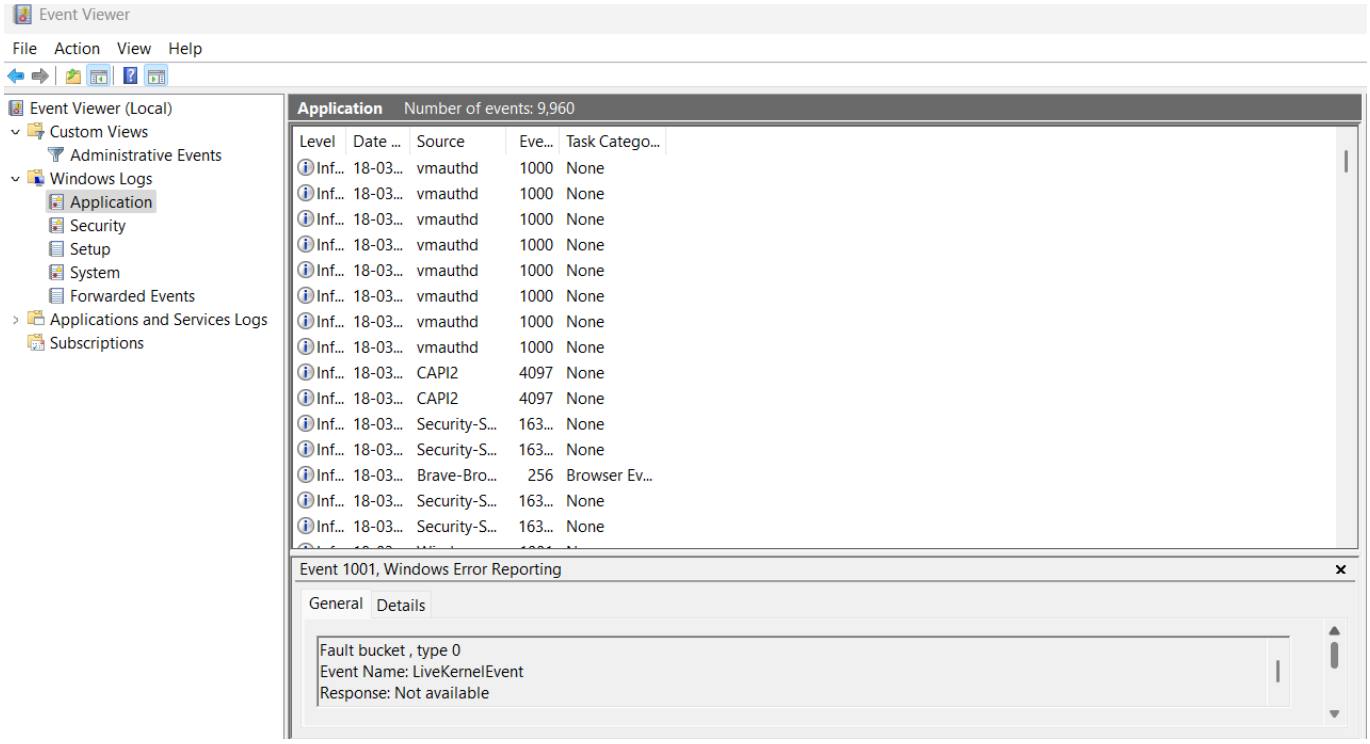


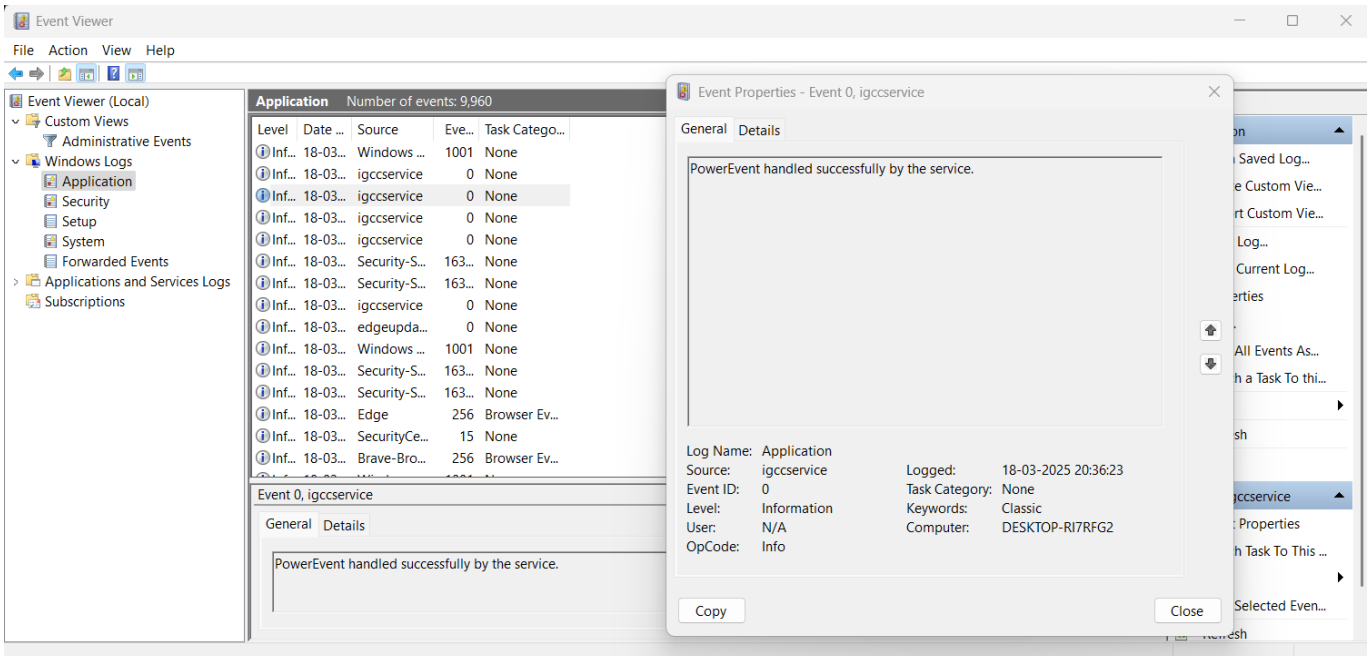


Select an Event: Click on a specific event from the list to display its summary in the lower pane.

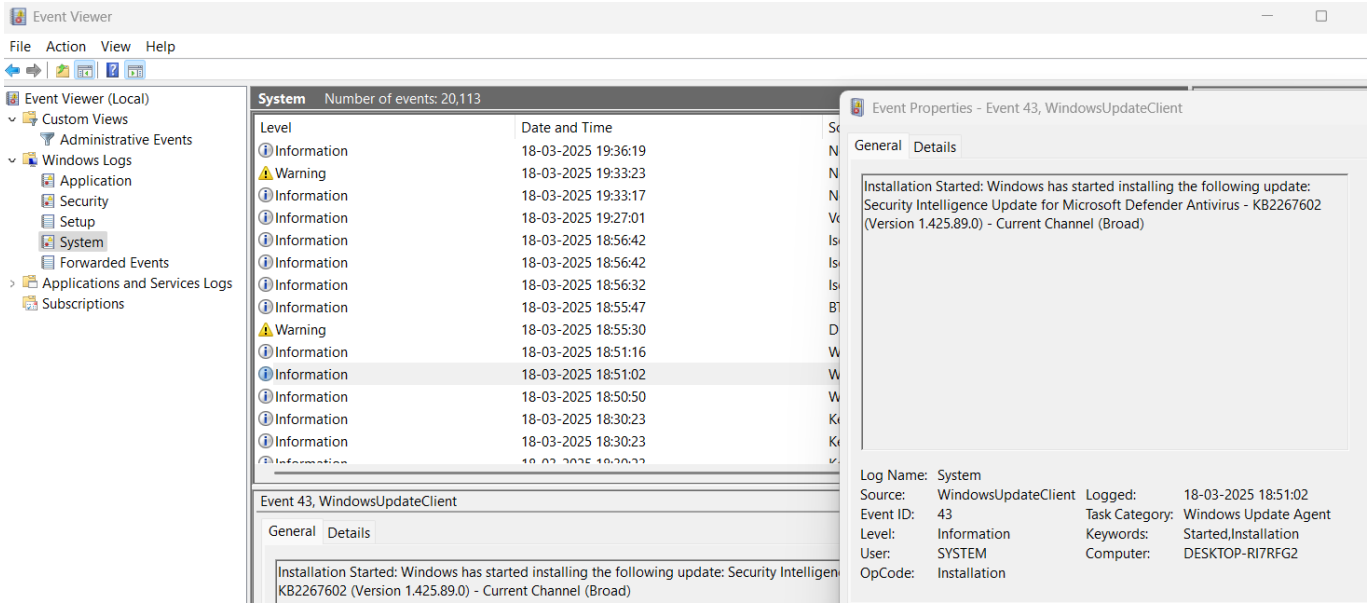
- **Open Full Details**: In the event properties section, select either the **"General"** or **"Details"** tab.

- **Examine Event Information**: This section provides key details such as the **event ID, source, and a detailed description** of the event.



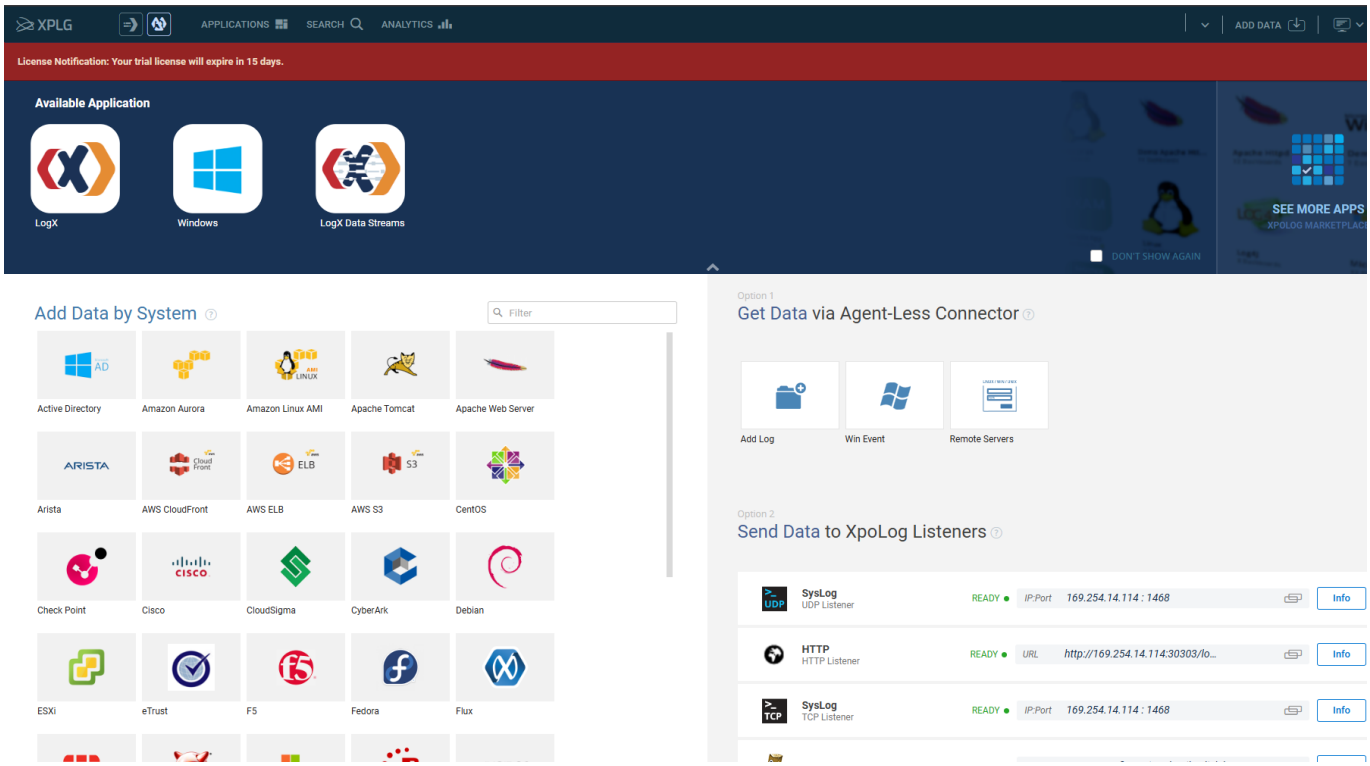


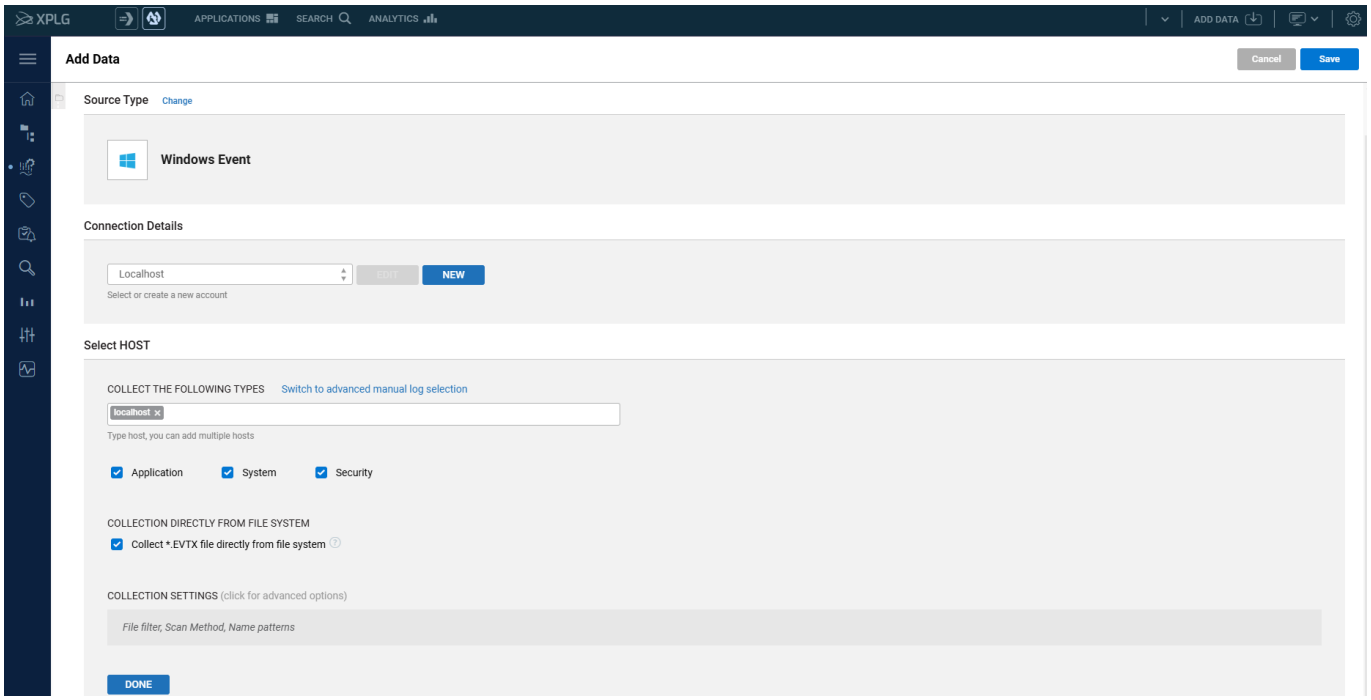
System Log in Windows Event Viewer



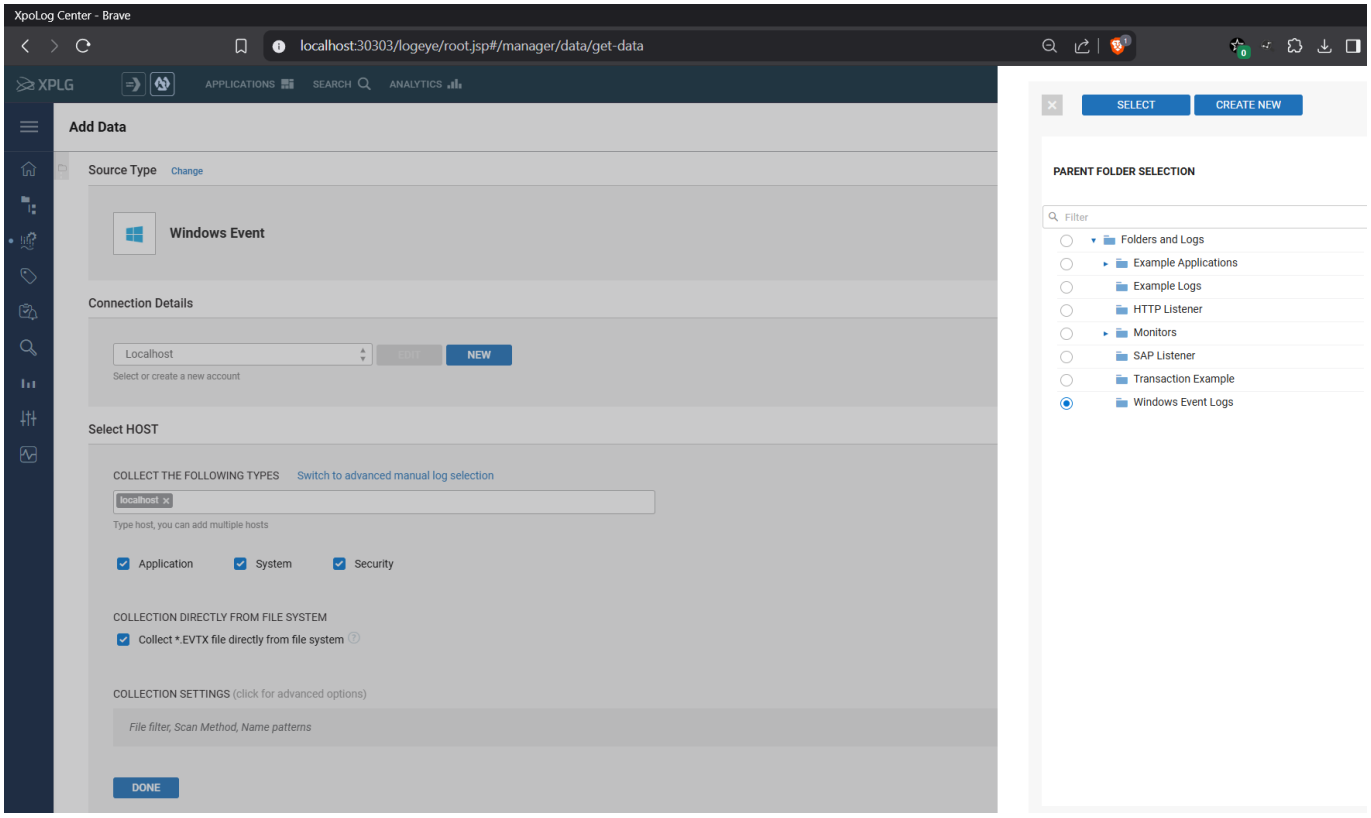
Investigating System Log Data Using XpoLog Center Suite

- **Launch XpoLog GUI**: Open your default web browser and navigate to http://localhost:30303/logeye/root.jsp#/home.
- **Access Windows Event Logs**: Click on **"Win Event"** to begin analyzing system log data.

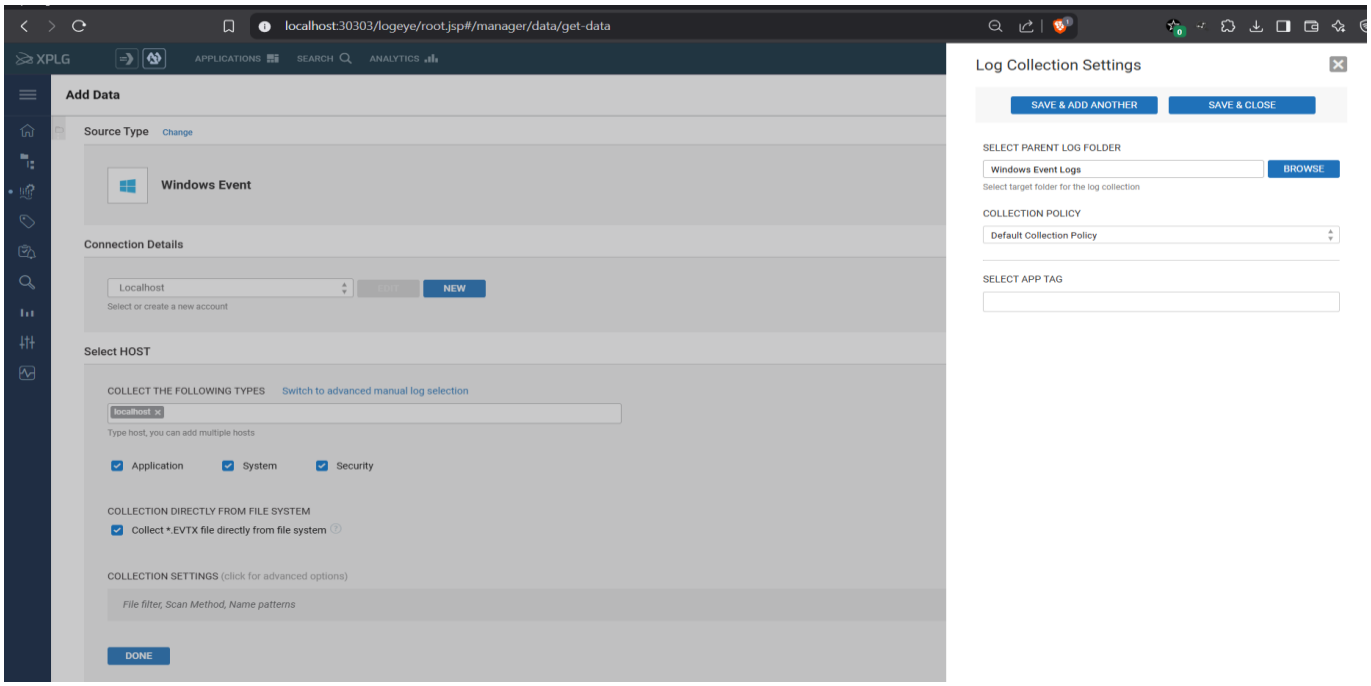




Choose the **Windows Event Logs** from the **Parent Folder Selection** menu.

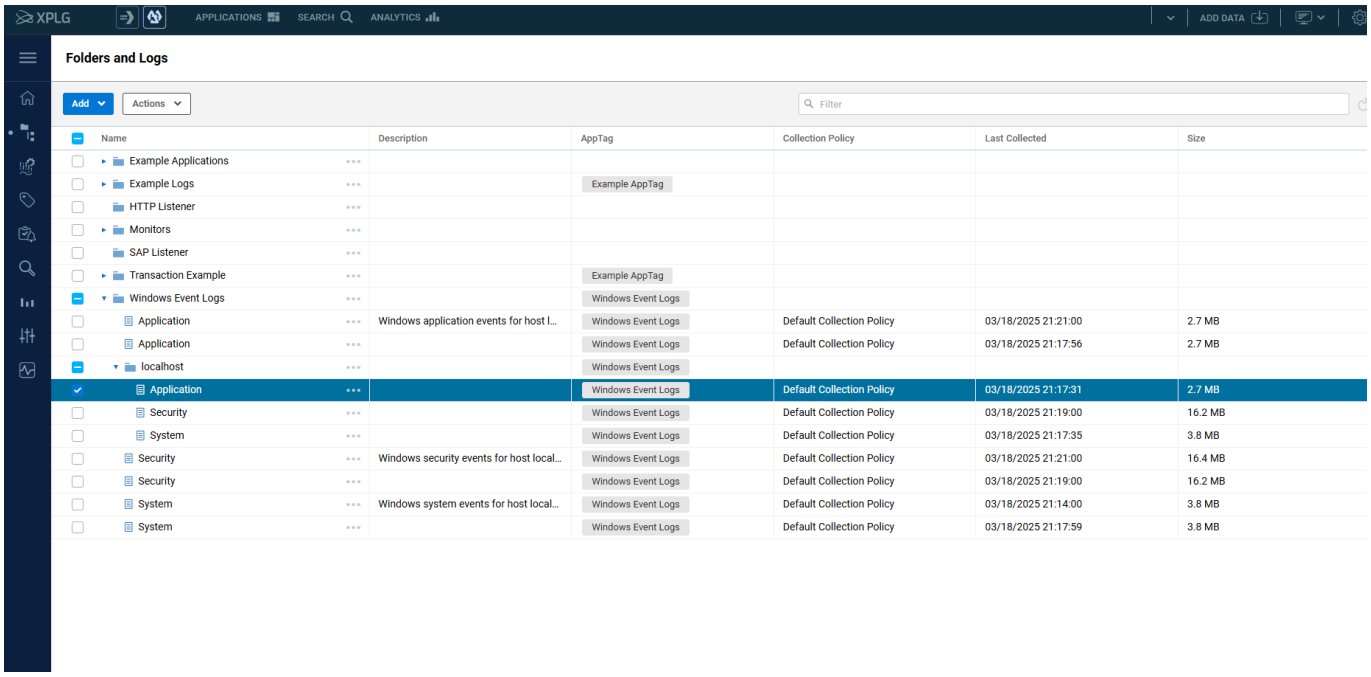


Next, click **"Save"** and then **"Close"** to finalize the selection.

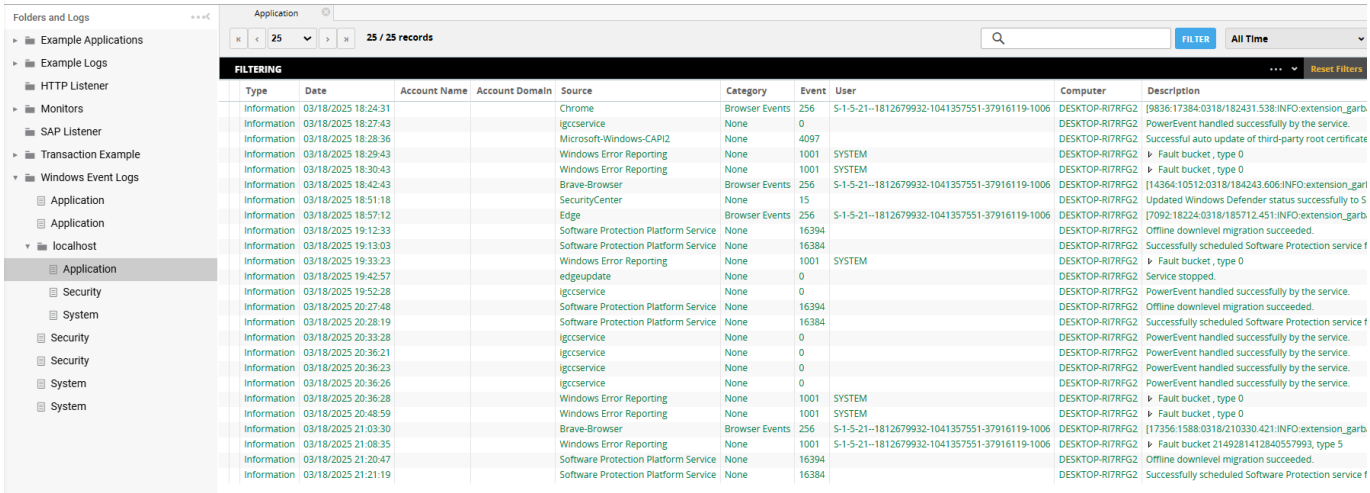


Navigating Windows Event Logs in XpoLog

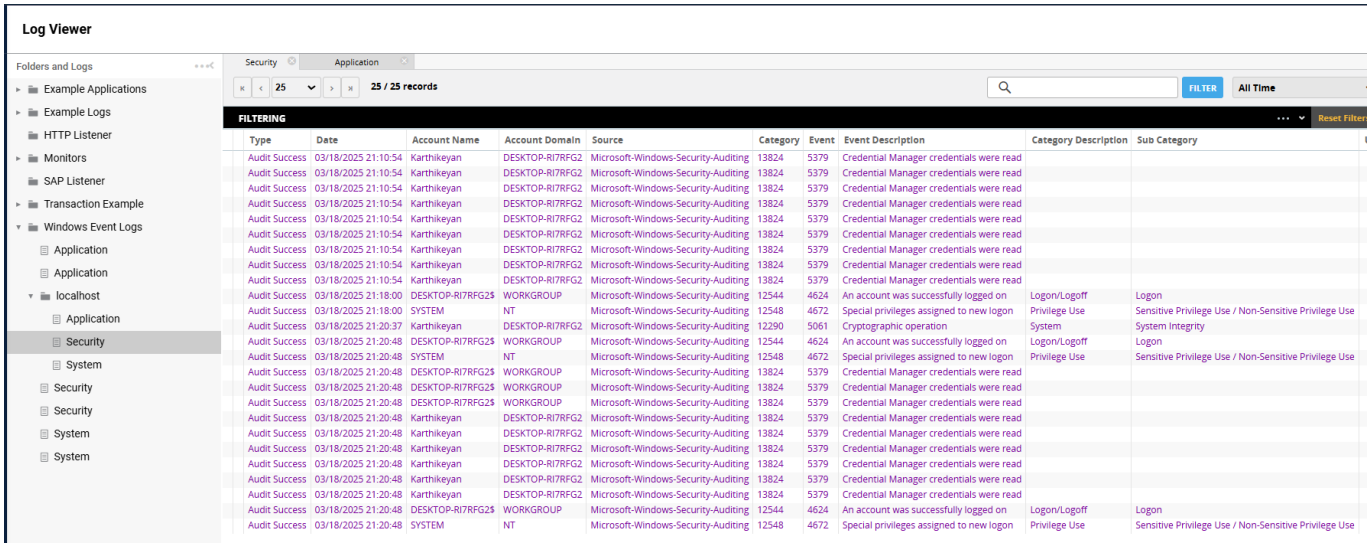
- **Click on the "Folders and Logs" Tab**: Access the log management section.
- **Expand "Windows Event Logs"**: Click to reveal the available log categories.
- **View Log Types**: You will see three main types of logs:
  - **Application Logs**
  - **Security Logs**
  - **System Logs**



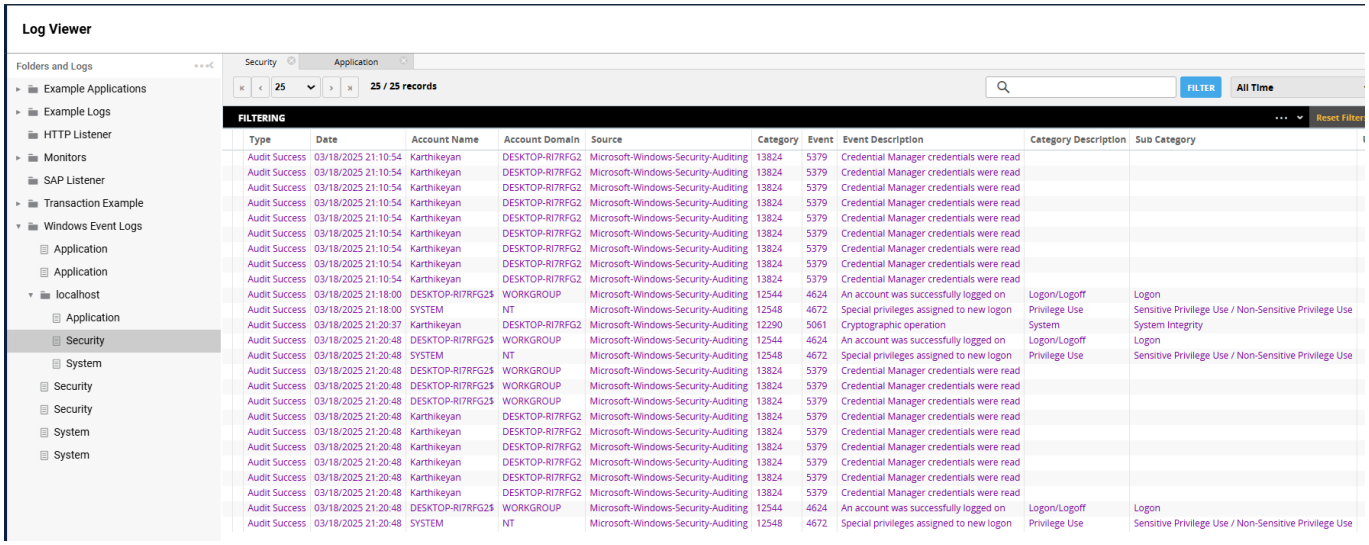
To access Windows application logs, select **"Application"** under **Windows Event Logs**. This will display all available application logs, as shown in the following screenshot.



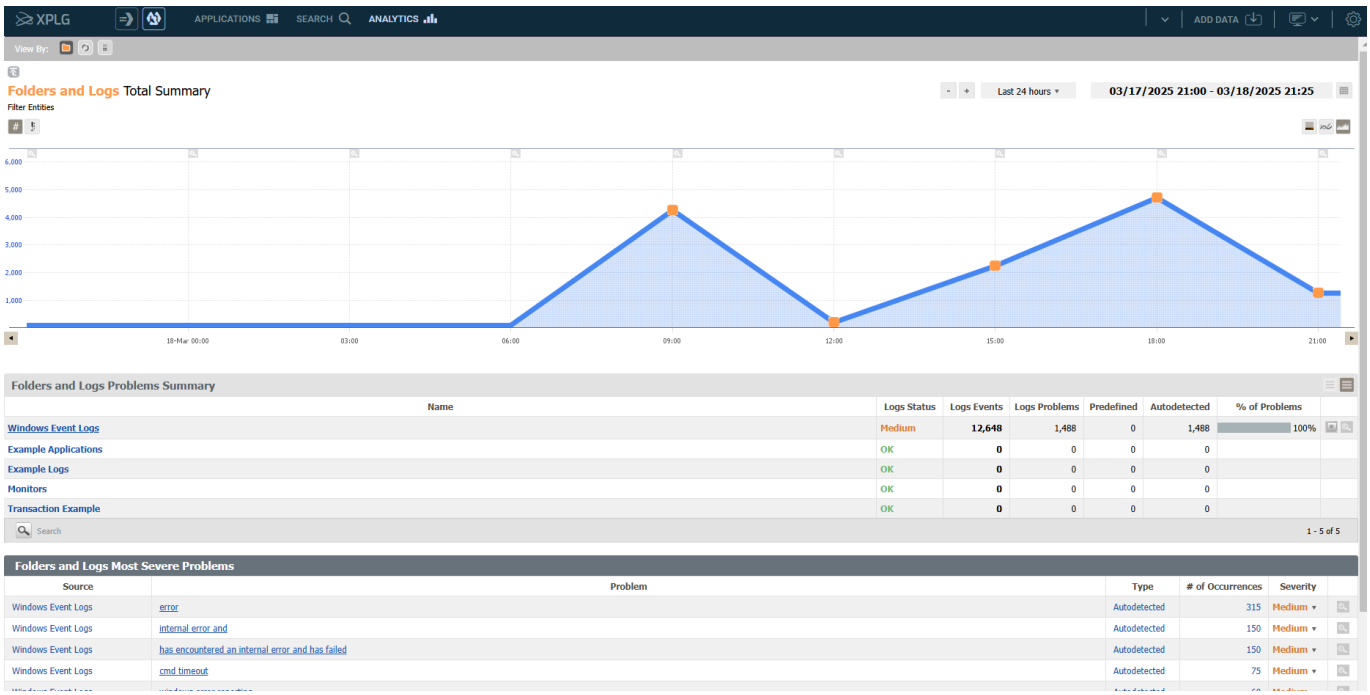
To access Windows security logs, select **"Security"** under **Windows Event Logs**. This will display all security-related logs, as shown in the following screenshot.



To access Windows system logs, select **"System"** under **Windows Event Logs**. All system-related logs will be displayed, as shown in the following screenshot.



To access detailed analytical insights of Windows logs, click on the **"Analytics"** tab.

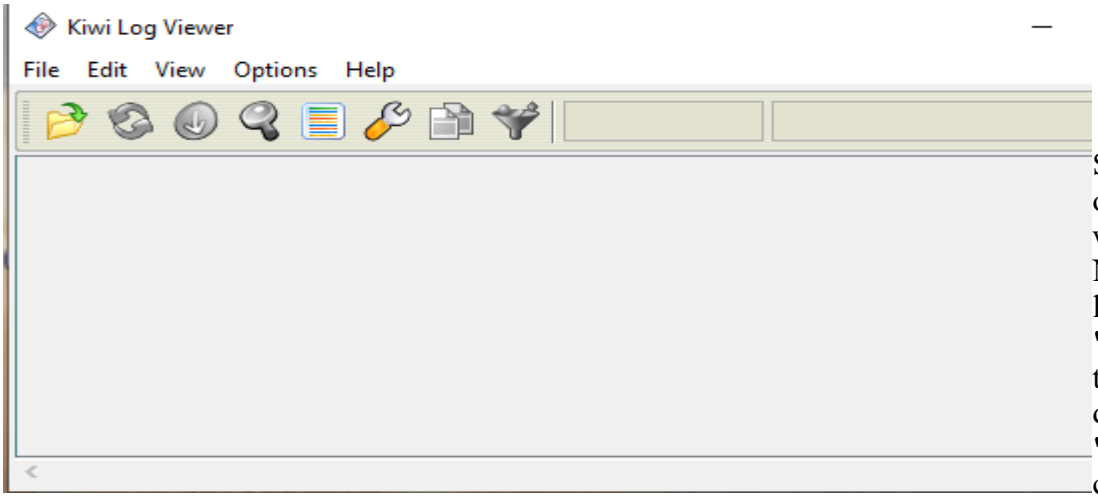


Observation from XpoLog Analytics Dashboard

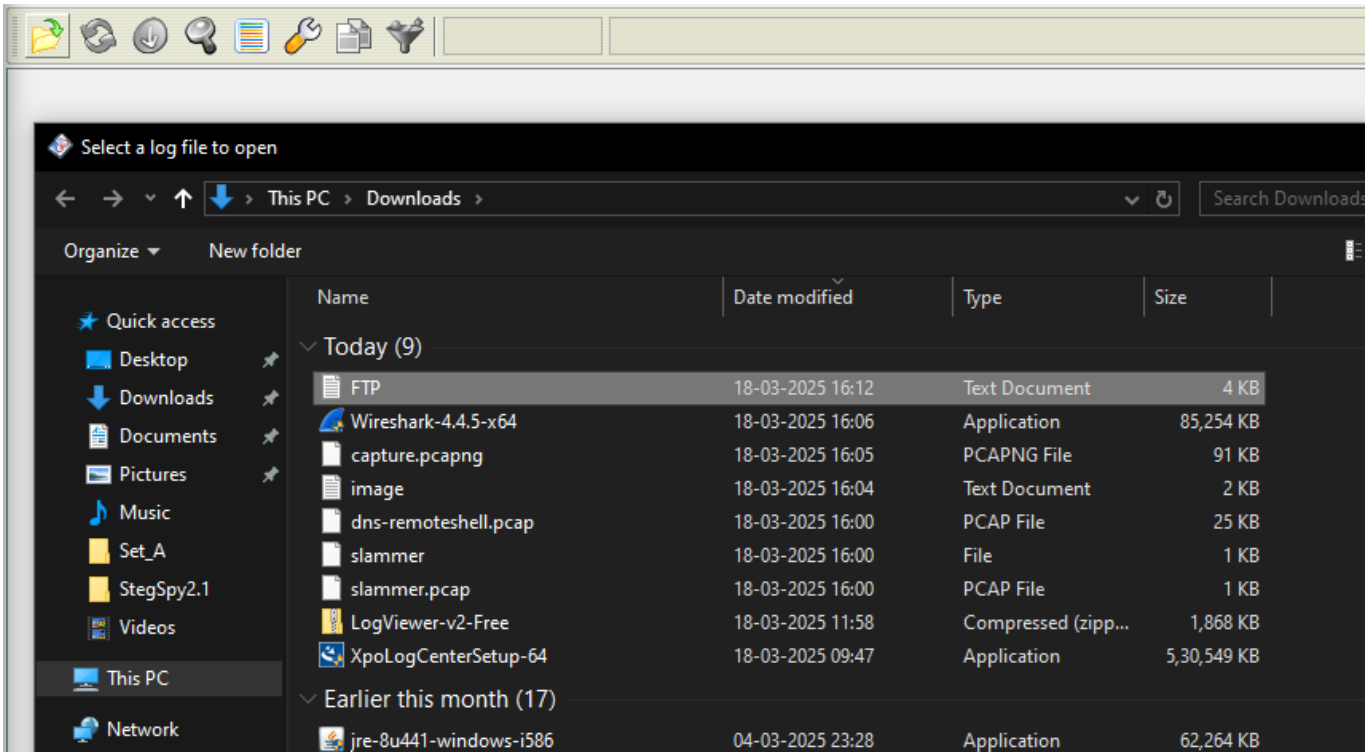
- The **log activity graph** shows peaks around **09:00 and 18:00**, indicating high system activity.
- **Windows Event Logs** have **12,648 events** and **1,488 issues** (medium severity). Other logs show no problems.
- Common errors include **"error" (315 occurrences), "internal error" (150), and "cmd timeout" (75)**.
- The system needs further investigation to resolve recurring issues.

Investigating Network Attacks Using Kiwi Log Viewer

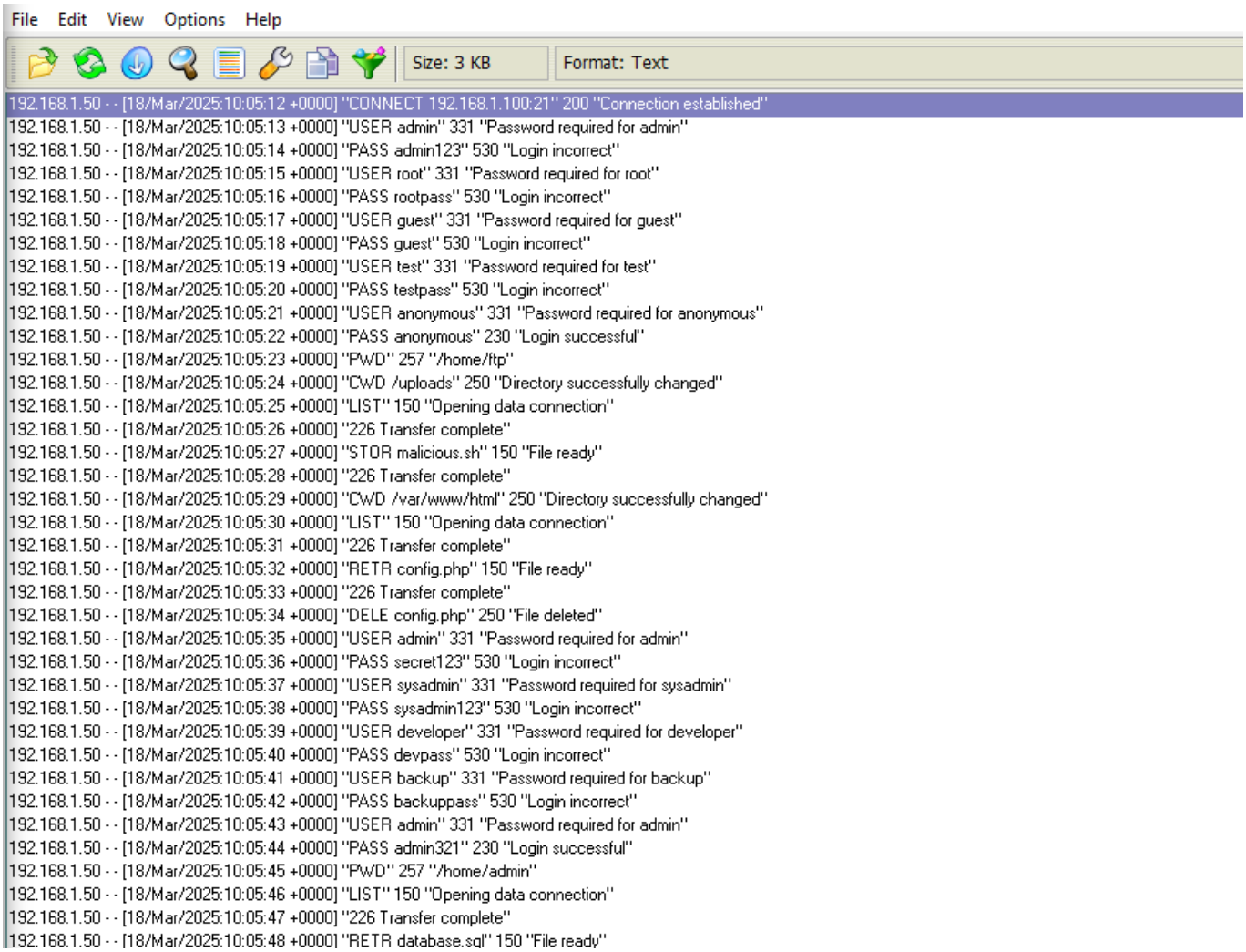
- **Launch Kiwi Log Viewer**: Open the **Kiwi Log Viewer** application on your system.

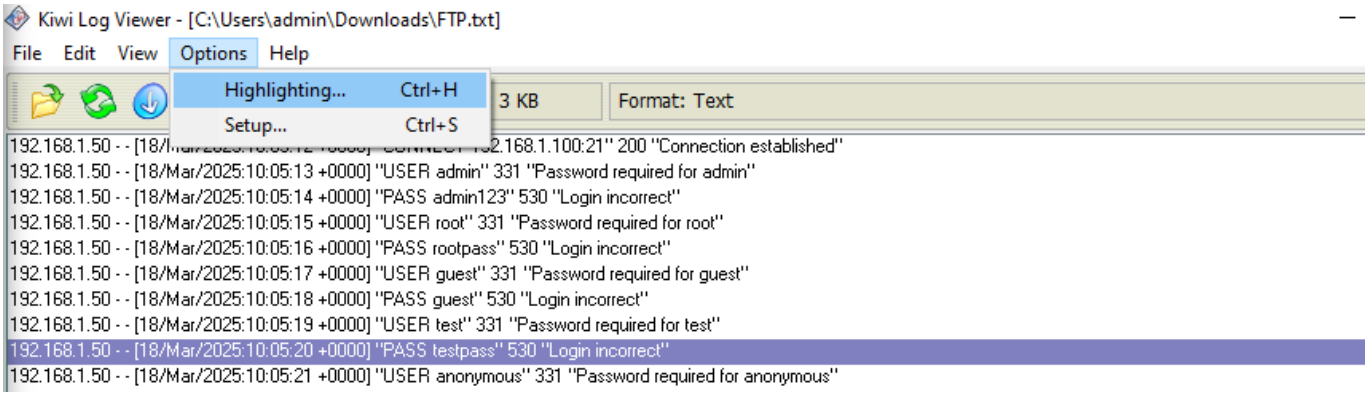


Select a log file to open. A window will appear. Navigate to the location, choose **"All Files"** from the **File Type** drop-down list, select **"FTP"**, and then click **"Open"**.


Select a log file to open
This PC › Downloads ›
Search Downloads
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Set_A
StegSpy2.1
Videos
This PC
Network
Name
Date modified
Type
Size
Today (9)
FTP 18-03-2025 16:12 Text Document 4 KB
Wireshark-4.4.5-x64 18-03-2025 16:06 Application 85,254 KB
capture.pcapng 18-03-2025 16:05 PCAPNG File 91 KB
image 18-03-2025 16:04 Text Document 2 KB
dns-remoteshell.pcap 18-03-2025 16:00 PCAP File 25 KB
slammer 18-03-2025 16:00 File 1 KB
slammer.pcap 18-03-2025 16:00 PCAP File 1 KB
LogViewer-v2-Free 18-03-2025 11:58 Compressed (zipp... 1,868 KB
XpoLogCenterSetup-64 18-03-2025 09:47 Application 5,30,549 KB
Earlier this month (17)
jre-8u441-windows-i586 04-03-2025 23:28 Application 62,264 KB

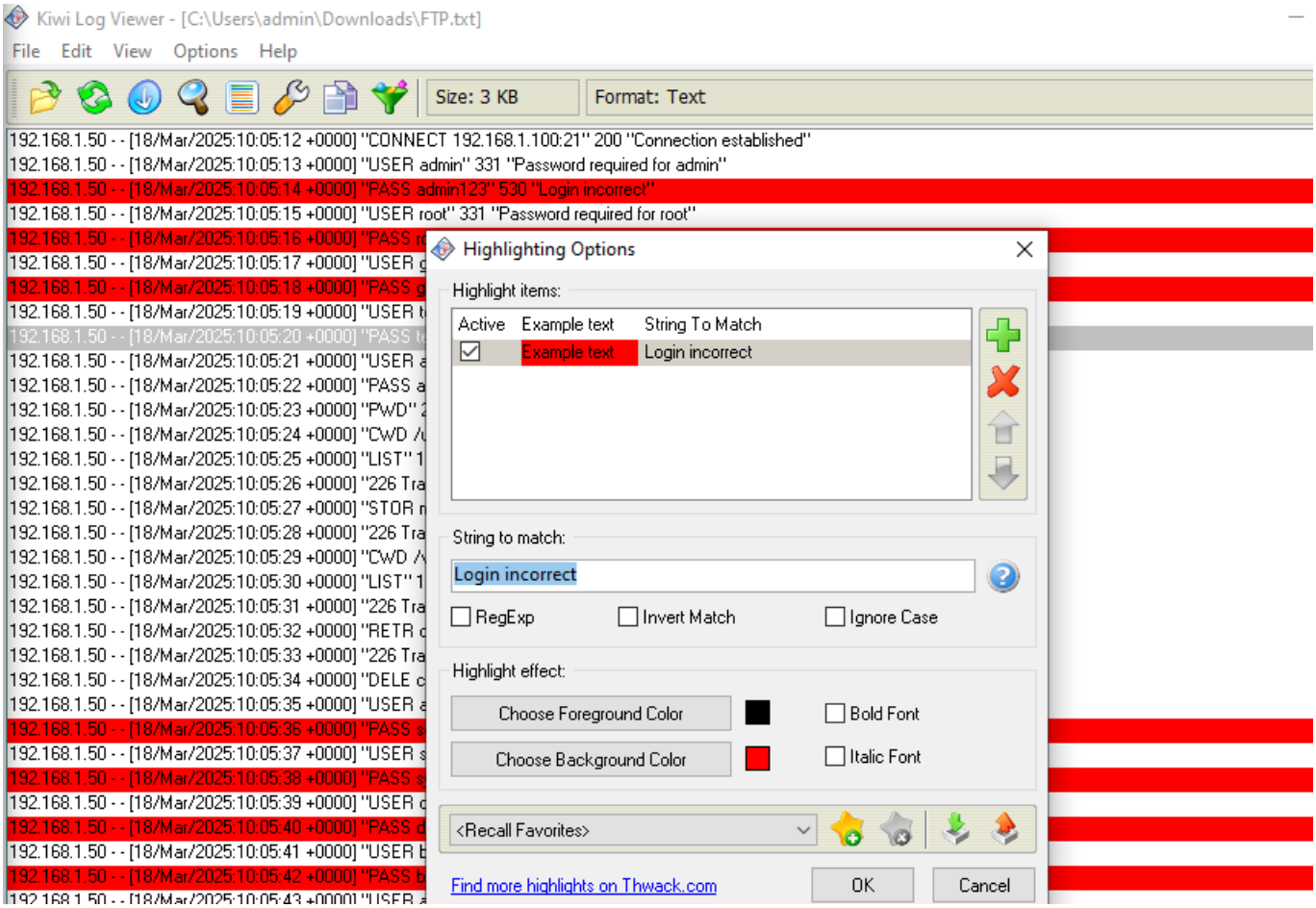
Kiwi Log Viewer loads all logs from the selected file, allowing you to analyze them for any signs of malicious activity in the network.



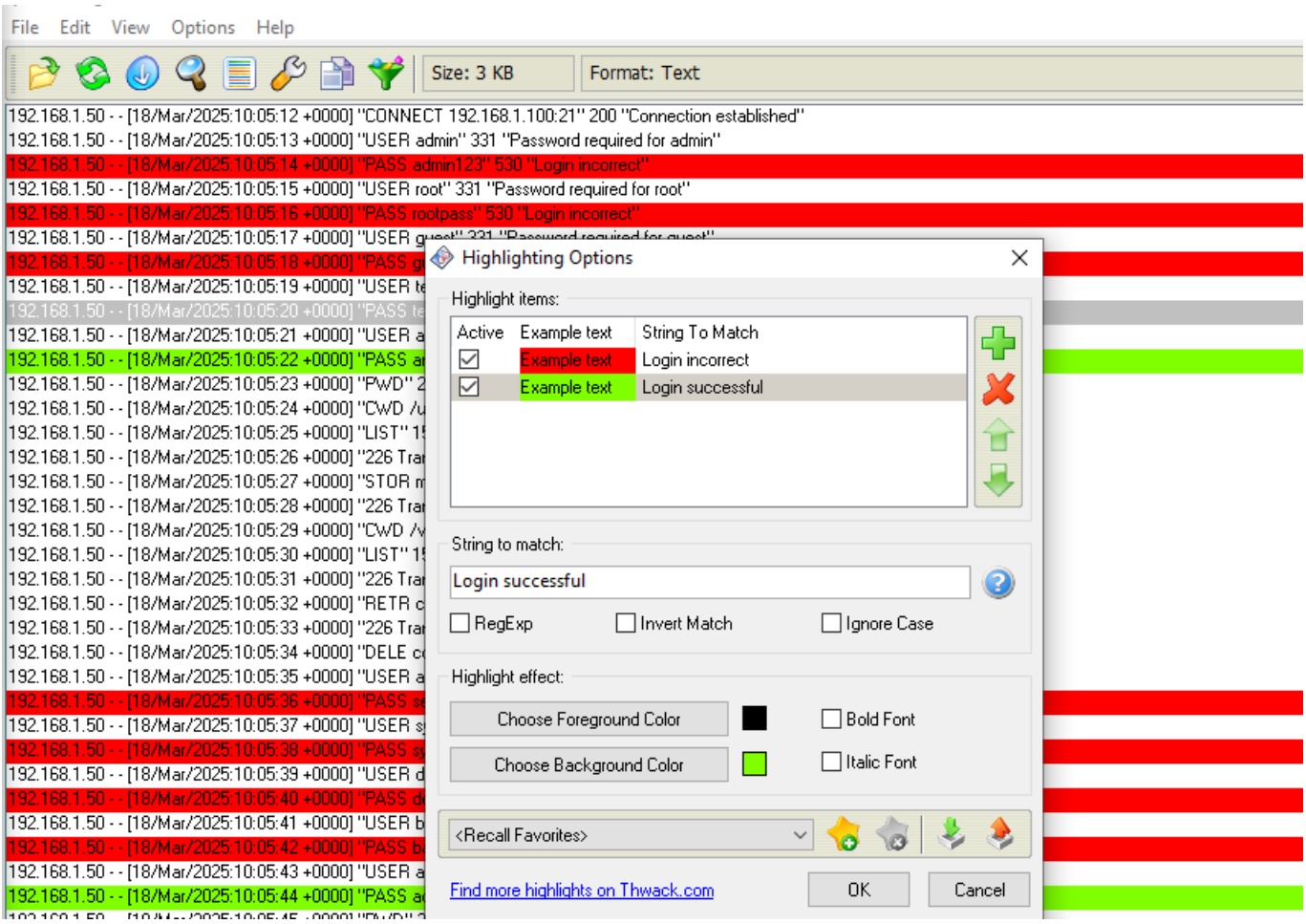


When a client attempts to log in to an FTP server using invalid, valid, or no credentials, the server responds with different status codes, such as **Response: 530, Response: 230**, and other similar messages.

To distinguish between different responses, apply color highlights. Navigate to **Options** and select **Highlighting**



Add a new item and set the string as **"Response: 230"**. Then, in the **Highlight Effect** section, click **"Choose Background Color"**, select **Green**, and click **OK**. This will highlight all logs containing **"Response: 230"**, indicating successful logins with valid credentials.



The **red-highlighted logs** indicate a high number of failed login attempts, suggesting a potential **brute-force attack** on the server.

As you **scroll through the logs**, you will notice that **log no. 329** is **highlighted in green**, meaning the server responded with **code 230**, confirming a **successful brute-force attack**.

This analysis helps in identifying **evidence of unauthorized access**, with the **green-highlighted log standing out** among multiple failed attempts, indicating a breached login.

Kiwi Log Viewer - [C:\Users\admin\Downloads\FTP.txt]

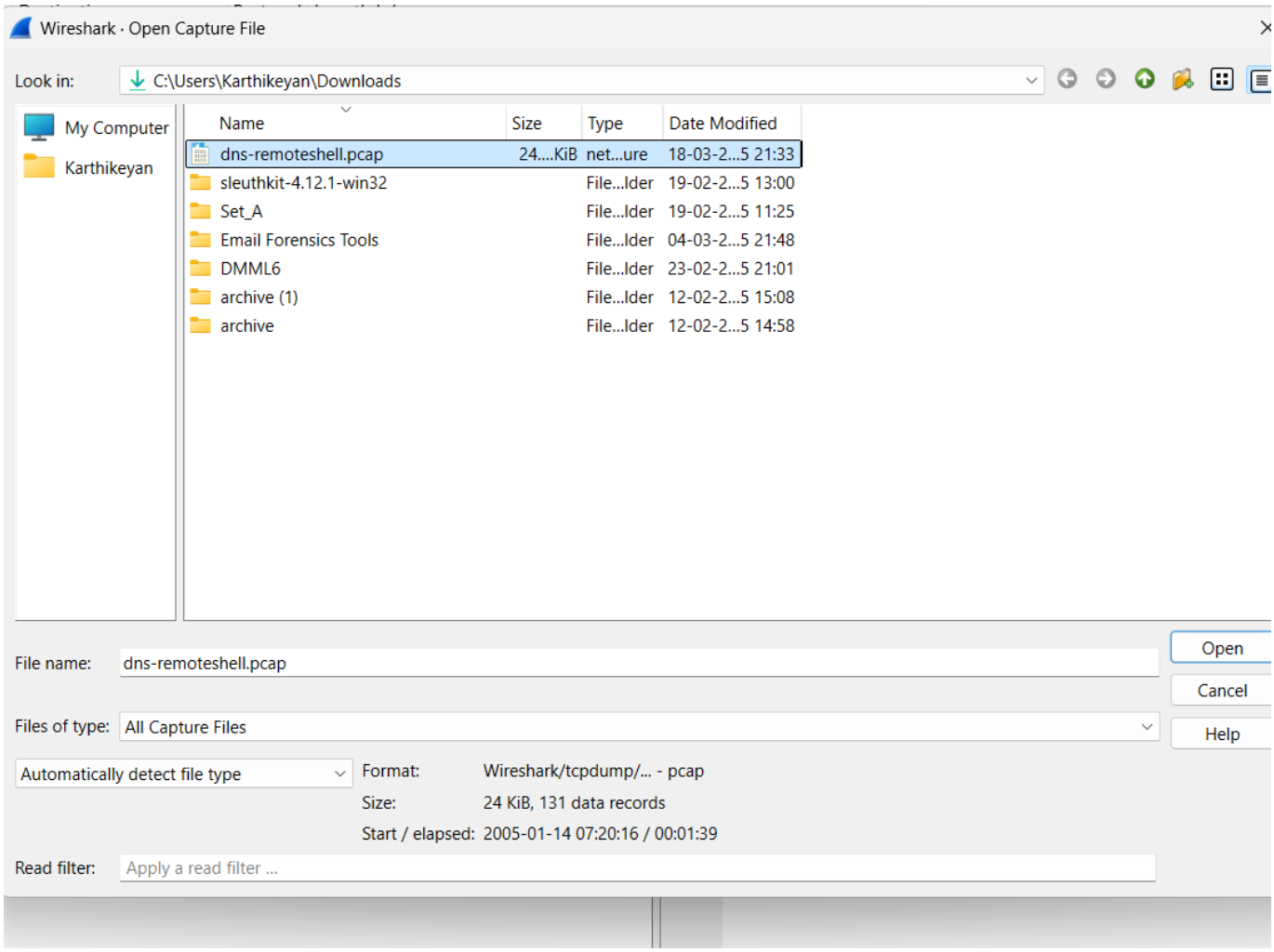
File Edit View Options Help

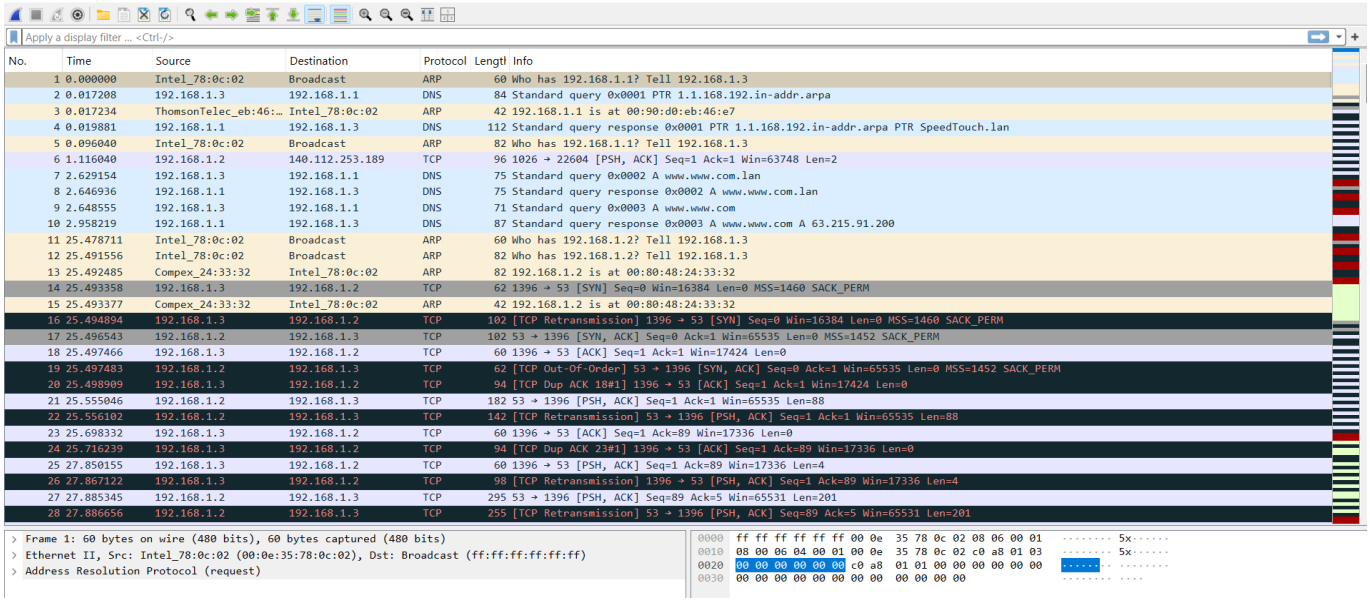
Size: 3 KB Format: Text

```
192.168.1.50 - - [18/Mar/2025:10:05:12 +0000] "CONNECT 192.168.1.100:21" 200 "Connection established"
192.168.1.50 - - [18/Mar/2025:10:05:13 +0000] "USER admin" 331 "Password required for admin"
192.168.1.50 - - [18/Mar/2025:10:05:14 +0000] "PASS admin123" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:15 +0000] "USER root" 331 "Password required for root"
192.168.1.50 - - [18/Mar/2025:10:05:16 +0000] "PASS rootpass" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:17 +0000] "USER guest" 331 "Password required for guest"
192.168.1.50 - - [18/Mar/2025:10:05:18 +0000] "PASS guest" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:19 +0000] "USER test" 331 "Password required for test"
192.168.1.50 - - [18/Mar/2025:10:05:20 +0000] "PASS testpass" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:21 +0000] "USER anonymous" 331 "Password required for anonymous"
192.168.1.50 - - [18/Mar/2025:10:05:22 +0000] "PASS anonymous" 230 "Login successful"
192.168.1.50 - - [18/Mar/2025:10:05:23 +0000] "PWD" 257 "/home/ftp"
192.168.1.50 - - [18/Mar/2025:10:05:24 +0000] "CWD /uploads" 250 "Directory successfully changed"
192.168.1.50 - - [18/Mar/2025:10:05:25 +0000] "LIST" 150 "Opening data connection"
192.168.1.50 - - [18/Mar/2025:10:05:26 +0000] "226 Transfer complete"
192.168.1.50 - - [18/Mar/2025:10:05:27 +0000] "STOR malicious.sh" 150 "File ready"
192.168.1.50 - - [18/Mar/2025:10:05:28 +0000] "226 Transfer complete"
192.168.1.50 - - [18/Mar/2025:10:05:29 +0000] "CWD /var/www/html" 250 "Directory successfully changed"
192.168.1.50 - - [18/Mar/2025:10:05:30 +0000] "LIST" 150 "Opening data connection"
192.168.1.50 - - [18/Mar/2025:10:05:31 +0000] "226 Transfer complete"
192.168.1.50 - - [18/Mar/2025:10:05:32 +0000] "RETR config.php" 150 "File ready"
192.168.1.50 - - [18/Mar/2025:10:05:33 +0000] "226 Transfer complete"
192.168.1.50 - - [18/Mar/2025:10:05:34 +0000] "DELE config.php" 250 "File deleted"
192.168.1.50 - - [18/Mar/2025:10:05:35 +0000] "USER admin" 331 "Password required for admin"
192.168.1.50 - - [18/Mar/2025:10:05:36 +0000] "PASS secret123" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:37 +0000] "USER sysadmin" 331 "Password required for sysadmin"
192.168.1.50 - - [18/Mar/2025:10:05:38 +0000] "PASS sysadmin123" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:39 +0000] "USER developer" 331 "Password required for developer"
192.168.1.50 - - [18/Mar/2025:10:05:40 +0000] "PASS devpass" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:41 +0000] "USER backup" 331 "Password required for backup"
192.168.1.50 - - [18/Mar/2025:10:05:42 +0000] "PASS backuppass" 530 "Login incorrect"
192.168.1.50 - - [18/Mar/2025:10:05:43 +0000] "USER admin" 331 "Password required for admin"
192.168.1.50 - - [18/Mar/2025:10:05:44 +0000] "PASS admin321" 230 "Login successful"
192.168.1.50 - - [18/Mar/2025:10:05:45 +0000] "PWD" 257 "/home/admin"
192.168.1.50 - - [18/Mar/2025:10:05:46 +0000] "LIST" 150 "Opening data connection"
```

Investigating Network Traffic Using Wireshark

- **Open the PCAP File**: Launch **Wireshark** and load the captured **PCAP** file.
- **View Captured Packets**: The network packets will be displayed in the **Wireshark interface**, as shown in the following screenshot.



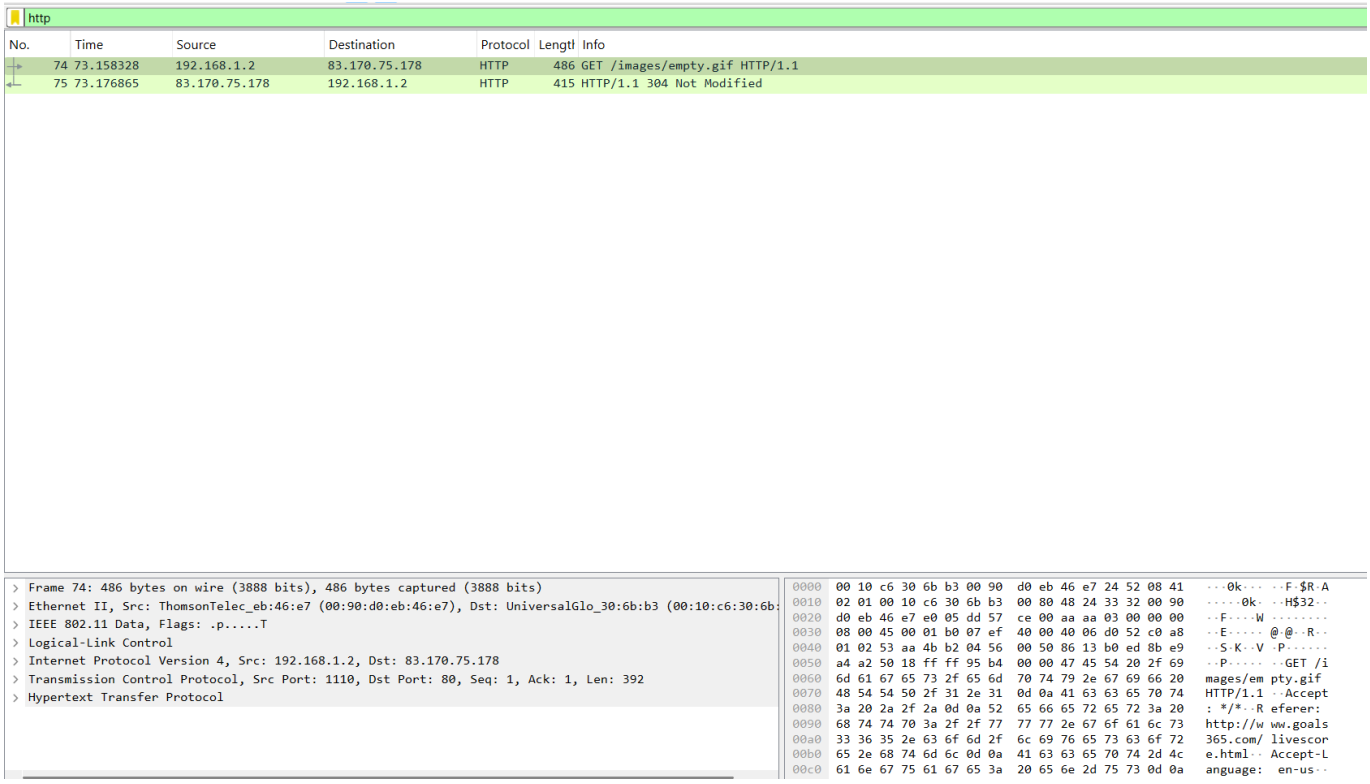


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Intel_78:0c:02	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.3
2	0.017208	192.168.1.3	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
3	0.017234	ThomsonTelec_eb:46:…	Intel_78:0c:02	ARP	42	192.168.1.1 is at 00:90:d0:eb:46:e7
4	0.019881	192.168.1.1	192.168.1.3	DNS	112	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR SpeedTouch.lan
5	0.096040	Intel_78:0c:02	Broadcast	ARP	82	Who has 192.168.1.1? Tell 192.168.1.3
6	1.116040	192.168.1.2	140.112.253.189	TCP	96	1026 → 22604 [PSH, ACK] Seq=1 Ack=1 Win=63748 Len=2
7	2.629154	192.168.1.3	192.168.1.1	DNS	75	Standard query 0x0002 A www.www.com.lan
8	2.646936	192.168.1.1	192.168.1.3	DNS	75	Standard query response 0x0002 A www.www.com.lan
9	2.648555	192.168.1.3	192.168.1.1	DNS	71	Standard query 0x0003 A www.www.com
10	2.958219	192.168.1.1	192.168.1.3	DNS	87	Standard query response 0x0003 A www.www.com A 63.215.91.200
11	25.478711	Intel_78:0c:02	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.3
12	25.491556	Intel_78:0c:02	Broadcast	ARP	82	Who has 192.168.1.2? Tell 192.168.1.3
13	25.492485	Compex_24:33:32	Intel_78:0c:02	ARP	82	192.168.1.2 is at 00:80:48:24:33:32
14	25.493358	192.168.1.3	192.168.1.2	TCP	62	1396 → 53 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
15	25.493377	Compex_24:33:32	Intel_78:0c:02	ARP	42	192.168.1.2 is at 00:80:48:24:33:32
16	25.494894	192.168.1.3	192.168.1.2	TCP	102	[TCP Retransmission] 1396 → 53 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
17	25.496543	192.168.1.2	192.168.1.3	TCP	102	53 → 1396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM
18	25.497466	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=1 Ack=1 Win=17424 Len=0
19	25.497483	192.168.1.2	192.168.1.3	TCP	62	[TCP Out-Of-Order] 53 → 1396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM
20	25.498909	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 18#1] 1396 → 53 [ACK] Seq=1 Ack=1 Win=17424 Len=0
21	25.555046	192.168.1.2	192.168.1.3	TCP	182	53 → 1396 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=88
22	25.556102	192.168.1.2	192.168.1.3	TCP	142	[TCP Retransmission] 53 → 1396 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=88
23	25.698332	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=1 Ack=89 Win=17336 Len=0
24	25.716239	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 23#1] 1396 → 53 [ACK] Seq=1 Ack=89 Win=17336 Len=0
25	27.850155	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [PSH, ACK] Seq=1 Ack=89 Win=17336 Len=4
26	27.867122	192.168.1.3	192.168.1.2	TCP	98	[TCP Retransmission] 1396 → 53 [PSH, ACK] Seq=1 Ack=89 Win=17336 Len=4
27	27.885345	192.168.1.2	192.168.1.3	TCP	295	53 → 1396 [PSH, ACK] Seq=89 Ack=5 Win=65531 Len=201
28	27.886656	192.168.1.2	192.168.1.3	TCP	255	[TCP Retransmission] 53 → 1396 [PSH, ACK] Seq=89 Ack=5 Win=65531 Len=201

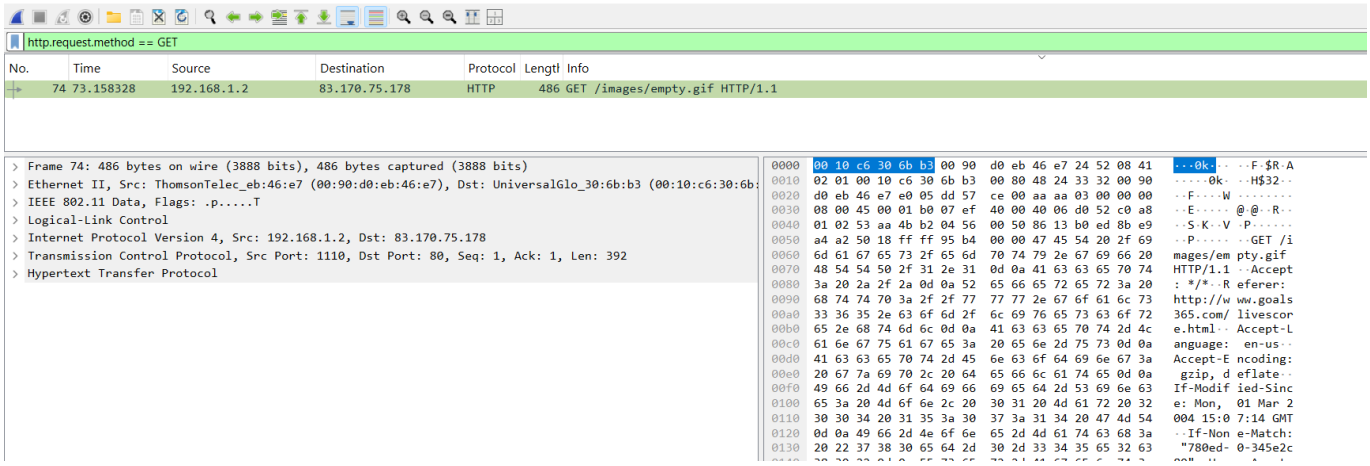
```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Intel_78:0c:02 (00:0e:35:78:0c:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0e  35 78 0c 02 08 06 00 01   ........ 5x......
0010  08 00 06 04 00 01 00 0e  35 78 0c 02 c0 a8 01 03   ........ 5x......
0020  00 00 00 00 00 00 c0 a8  01 01 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Enter **"http"** in the **Filter** field and press **Enter** to display only HTTP traffic.

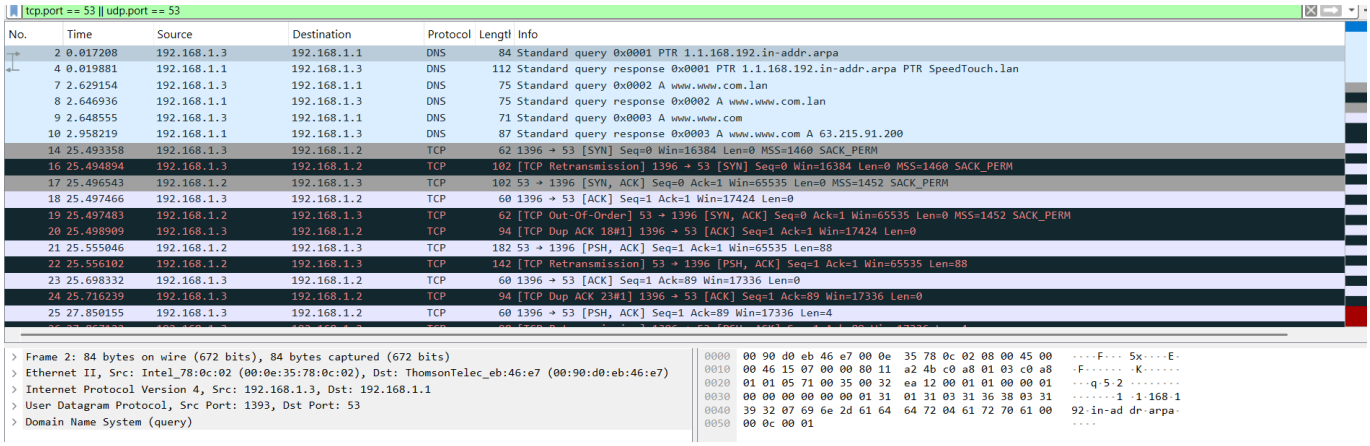


Enter **"http.request.method == GET"** in the **Filter** field and press **Enter**. Wireshark will then filter and display only the traffic containing **GET requests**, as shown in the following screenshot.



Analyzing DNS Anomalies in Wireshark

1. **Close the Current Packet Capture**: Exit the current capture session in Wireshark.
2. **Filter DNS Traffic**: Since **DNS communication uses port 53**, filter the traffic by entering:
   tcp.port == 53 || udp.port == 53
   in the **Filter** field and press **Enter**.
3. **View DNS Packets**: Wireshark will now display all packets using **port 53**, allowing you to analyze DNS anomalies.



To analyze the data flow in sequence, use the **Follow TCP Stream** option in Wireshark:

1. **Right-click** on any packet between **14 and 38** (for example, **packet 16**).
2. Select **"Follow"** from the menu.
3. Click on **"TCP Stream"** from the drop-down list.

This will display the **entire conversation** between the source and destination, allowing for detailed inspection of network activity.