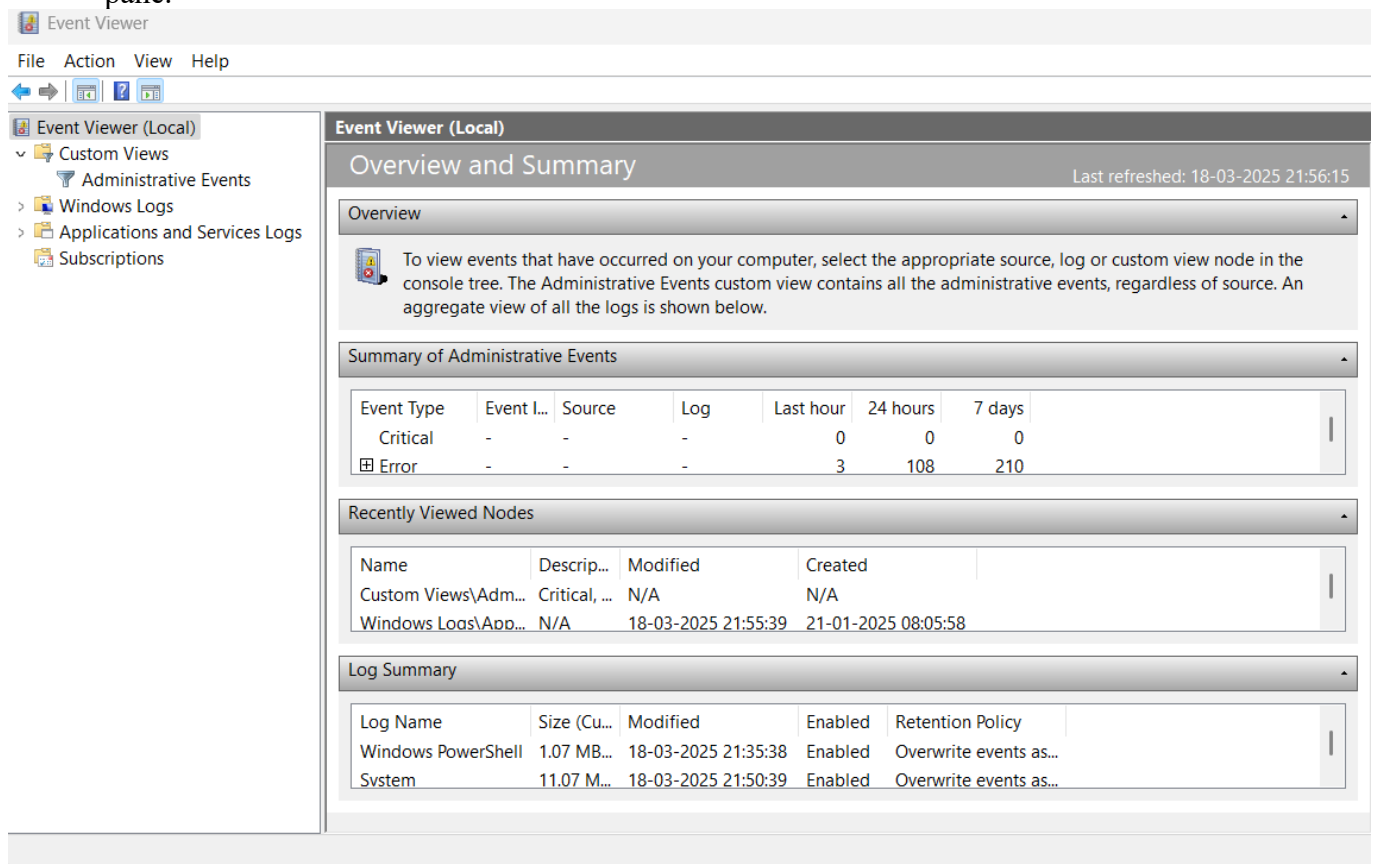


Cyber Forensics - 24CY611

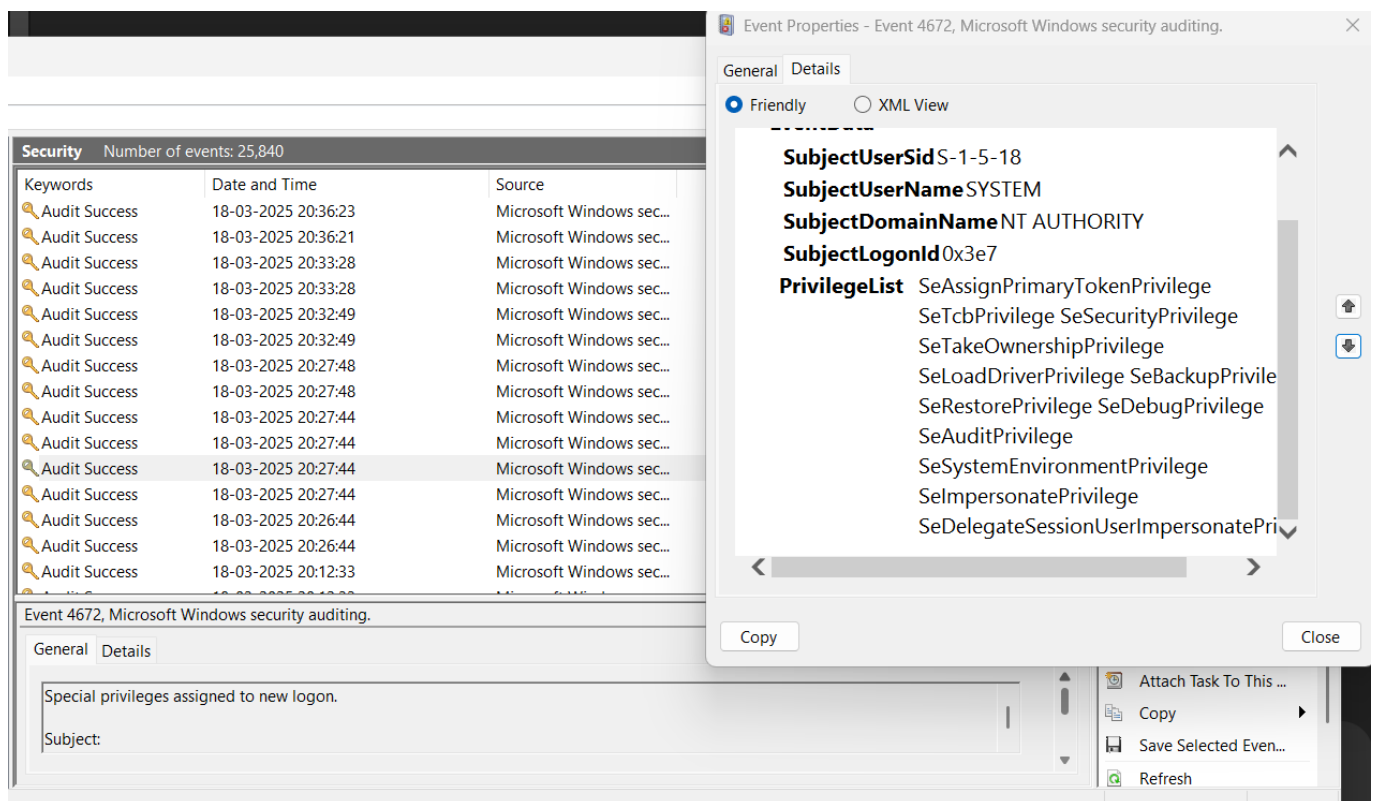
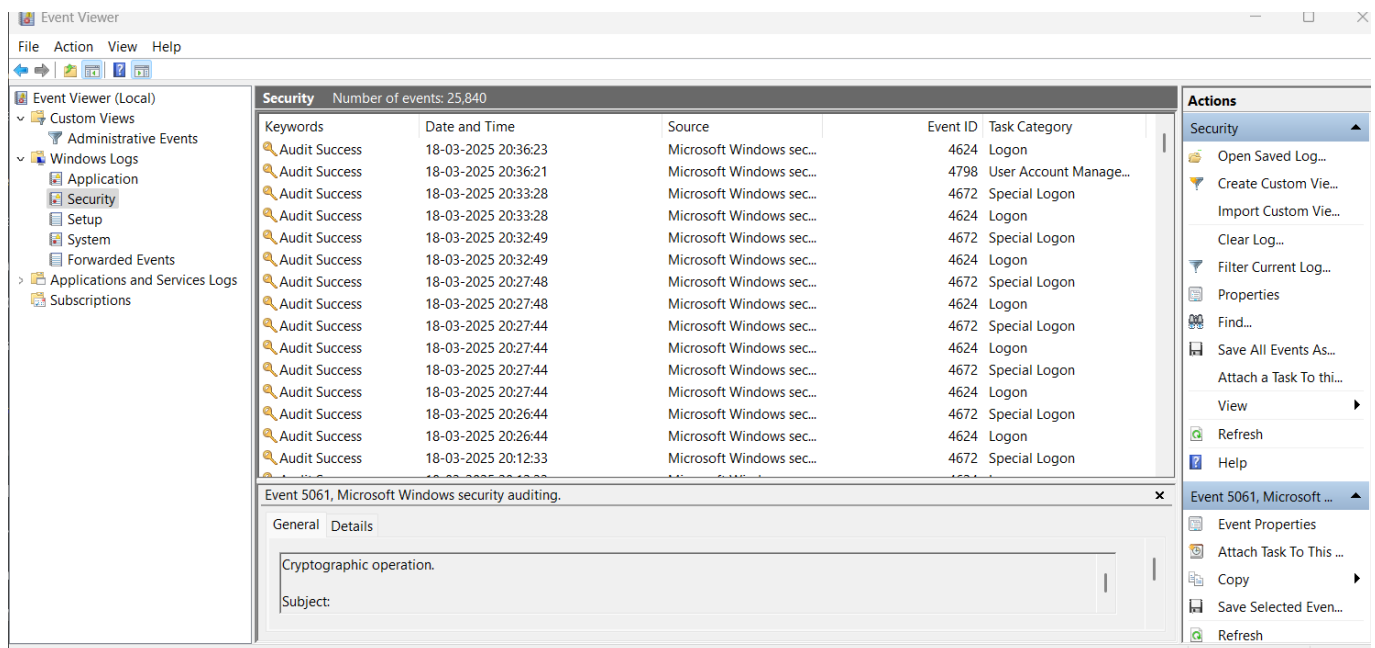
Lab 7 - Network Forensics

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.

-
- The screenshot shows the Windows Event Viewer application. The left-hand pane displays the tree view under "Event Viewer (Local)", expanded to "Windows Logs" and then "Application". The main pane shows a list of events from the Application log. The title bar indicates "Number of events: 9,960". The event list has columns for Level, Date, Source, ID, and Category Name. Several events are visible, mostly informational messages from vmauthd and CAPI2. At the bottom, a details pane is open for "Event 1001, Windows Error Reporting", showing the "General" tab with information about a fault bucket and kernel event.
- Event Viewer

File Action View Help

Event Viewer (Local)

 - Custom Views
 - Administrative Events
 - Windows Logs
 - Application**
 - Security
 - Setup
 - System
 - Forwarded Events
 - Applications and Services Logs
 - Subscriptions

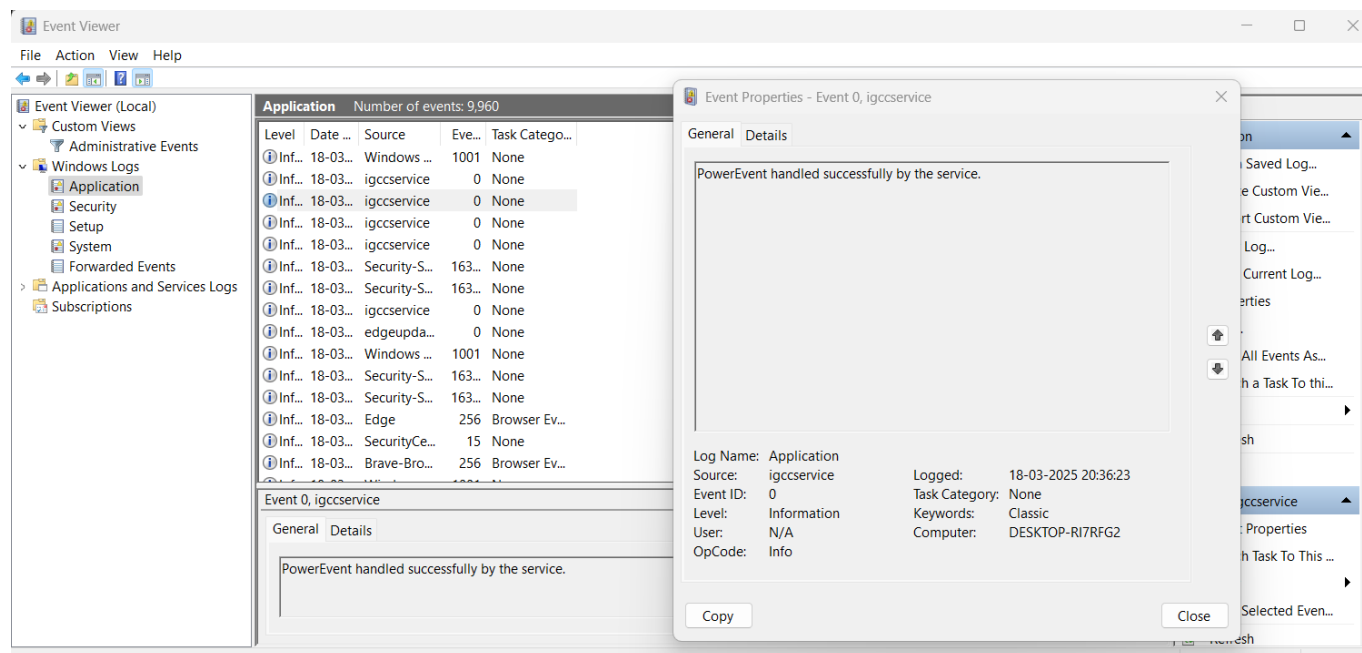
Application Number of events: 9,960

Level	Date ...	Source	Eve...	Task Catego...
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	vmauthd	1000	None
Inf...	18-03...	CAPI2	4097	None
Inf...	18-03...	CAPI2	4097	None
Inf...	18-03...	Security-S...	163...	None
Inf...	18-03...	Security-S...	163...	None
Inf...	18-03...	Brave-Bro...	256	Browser Ev...
Inf...	18-03...	Security-S...	163...	None
Inf...	18-03...	Security-S...	163...	None

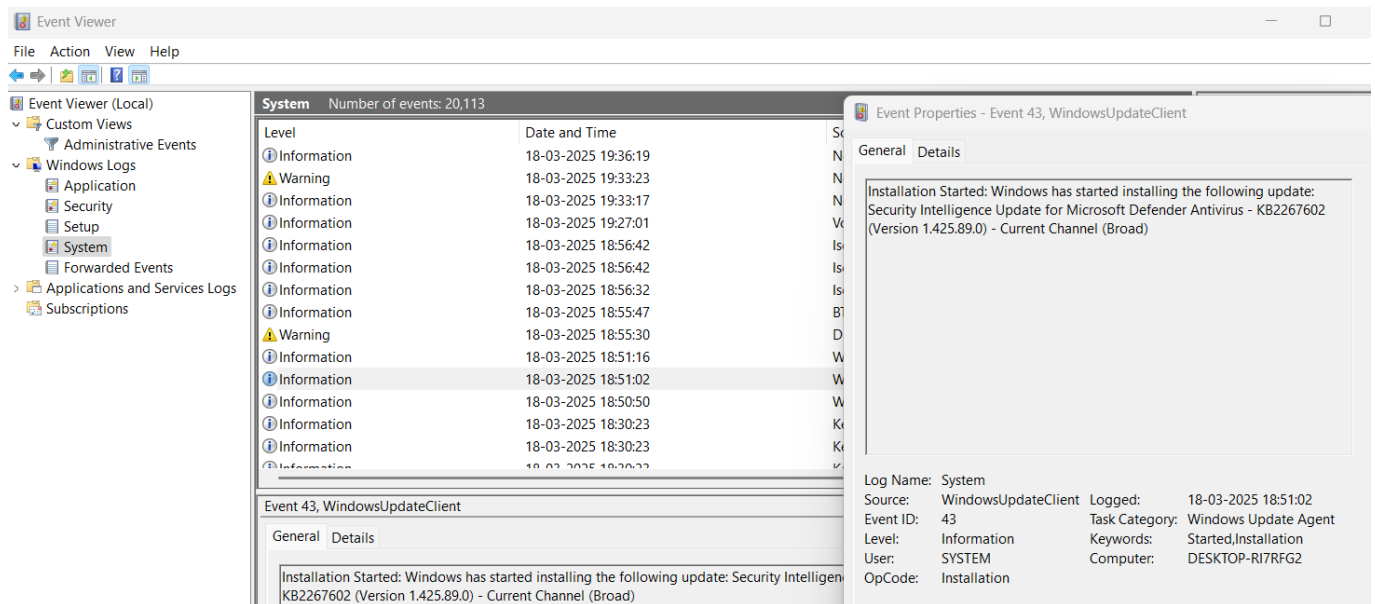
Event 1001, Windows Error Reporting

General Details

Fault bucket , type 0
Event Name: LiveKernelEvent
Response: Not available

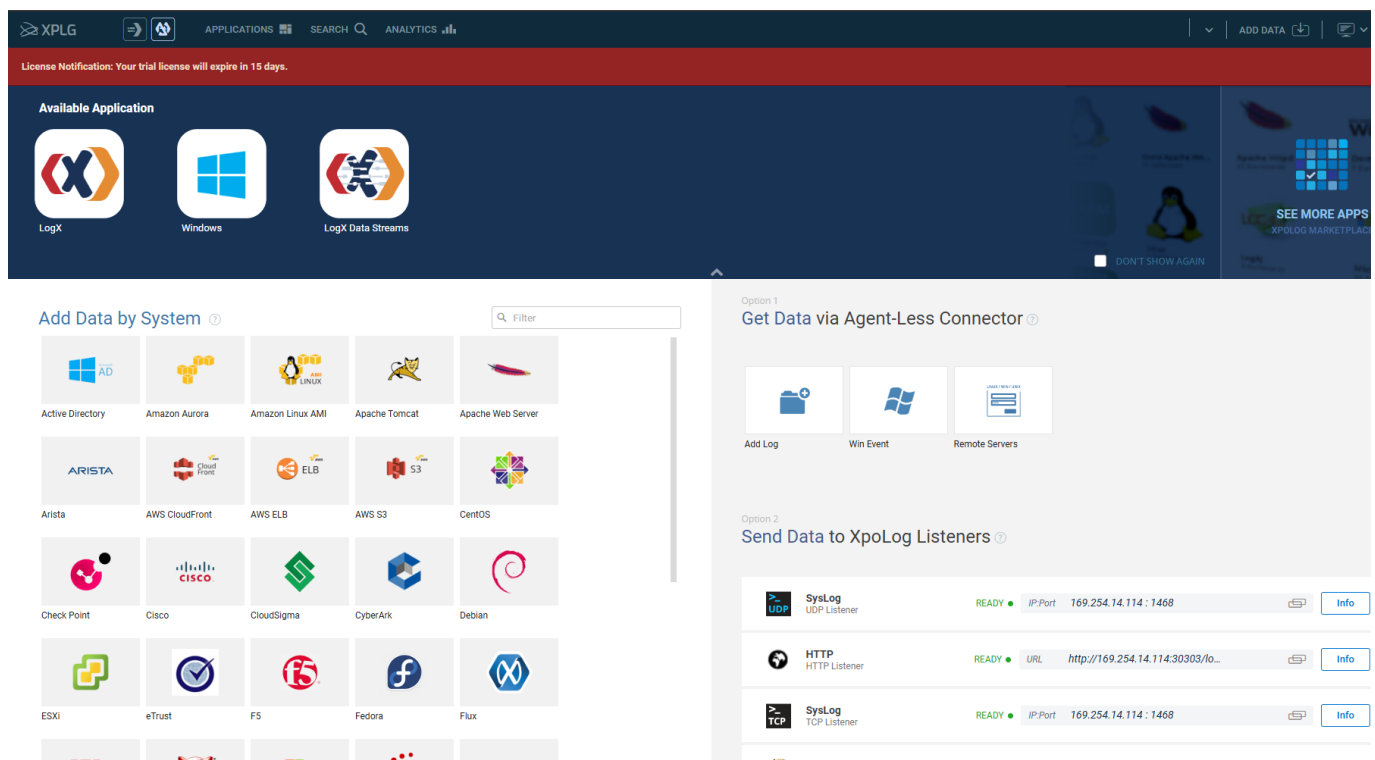


System Log in Windows Event Viewer



Investigating System Log Data Using XpoLog Center Suite

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



Add Data

Source Type [Change](#)

Windows Event

Connection Details

Localhost [EDIT](#) [NEW](#)
Select or create a new account

Select HOST

COLLECT THE FOLLOWING TYPES [Switch to advanced manual log selection](#)

localhost x
Type host, you can add multiple hosts

☒ Application ☒ System ☒ Security

COLLECTION DIRECTLY FROM FILE SYSTEM

☒ Collect *.EVTX file directly from file system [?](#)

COLLECTION SETTINGS (click for advanced options)

File filter, Scan Method, Name patterns

[DONE](#)

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

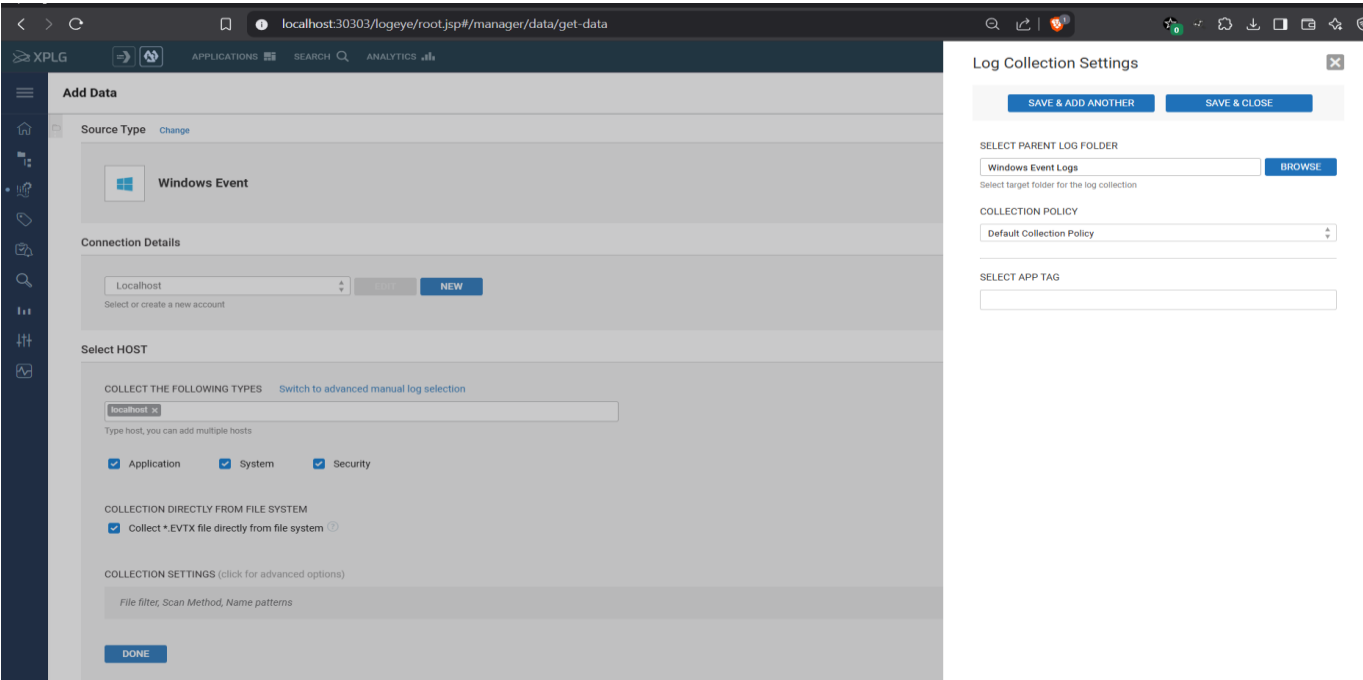
Parent Folder Selection

Filter

- ☐ Folders and Logs
- ☐ Example Applications
- ☐ Example Logs
- ☐ HTTP Listener
- ☐ Monitors
- ☐ SAP Listener
- ☐ Transaction Example
- ☒ Windows Event Logs

[SELECT](#) [CREATE NEW](#)

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



Navigating Windows Event Logs in XpoLog

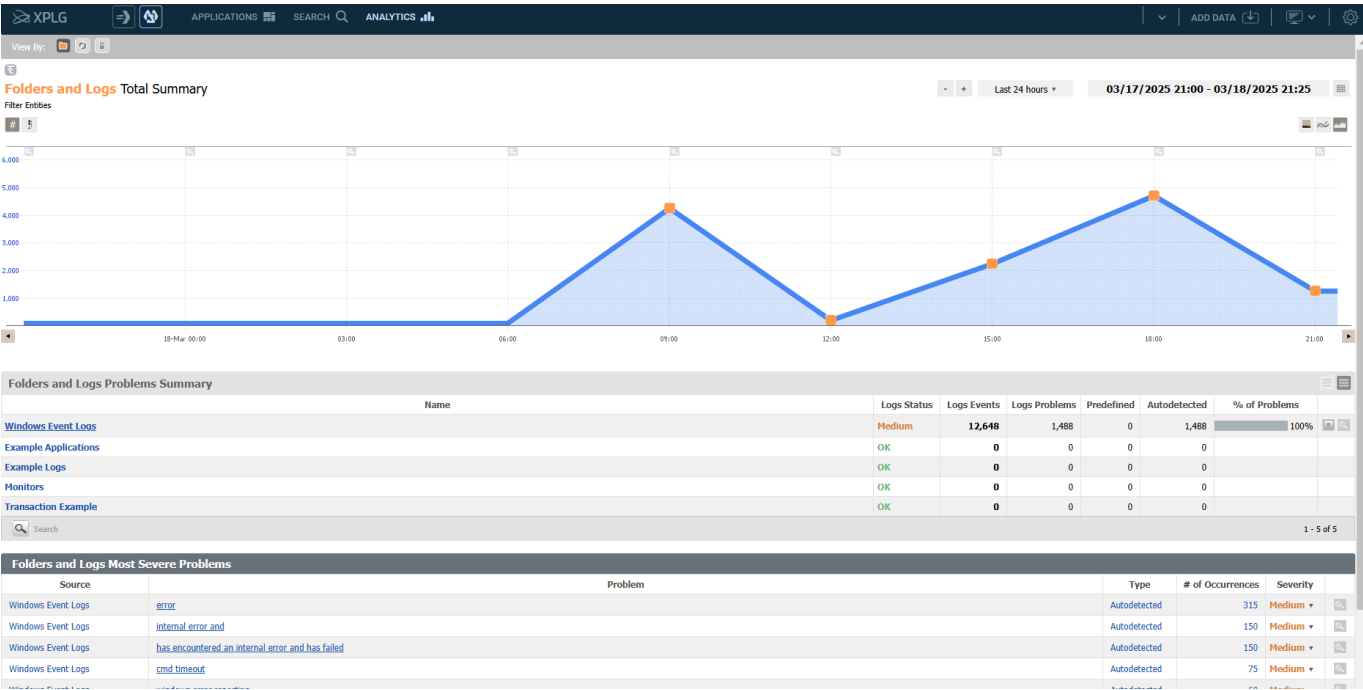
- **Click on the "Folders and Logs" Tab:** Access the log management section.
- **Expand "Windows Event Logs":** Click to reveal the available log categories.
- **View Log Types:** You will see three main types of logs:
 - **Application Logs**
 - **Security Logs**
 - **System Logs**

The screenshot shows the 'Folders and Logs' table in the Xplog application. The table lists various log categories and their details. The 'Application' log under 'Windows Event Logs' is selected.

Name	Description	AppTag	Collection Policy	Last Collected	Size
Example Applications					
Example Logs		Example AppTag			
HTTP Listener					
Monitors					
SAP Listener					
Transaction Example		Example AppTag			
Windows Event Logs		Windows Event Logs			
Application	Windows application events for host local...	Windows Event Logs	Default Collection Policy	03/18/2025 21:21:00	2.7 MB
Application		Windows Event Logs	Default Collection Policy	03/18/2025 21:17:56	2.7 MB
localhost		Windows Event Logs			
Application		Windows Event Logs	Default Collection Policy	03/18/2025 21:17:31	2.7 MB
Security		Windows Event Logs	Default Collection Policy	03/18/2025 21:19:00	16.2 MB
System		Windows Event Logs	Default Collection Policy	03/18/2025 21:17:35	3.8 MB
Security	Windows security events for host local...	Windows Event Logs	Default Collection Policy	03/18/2025 21:21:00	16.4 MB
Security		Windows Event Logs	Default Collection Policy	03/18/2025 21:19:00	16.2 MB
System	Windows system events for host local...	Windows Event Logs	Default Collection Policy	03/18/2025 21:14:00	3.8 MB
System		Windows Event Logs	Default Collection Policy	03/18/2025 21:17:59	3.8 MB

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

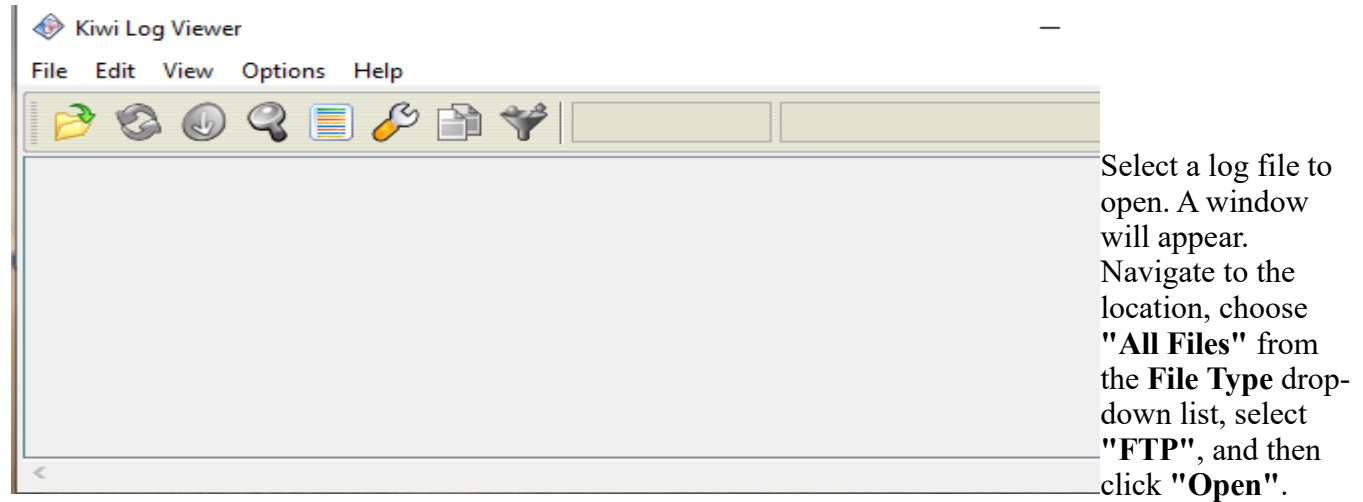


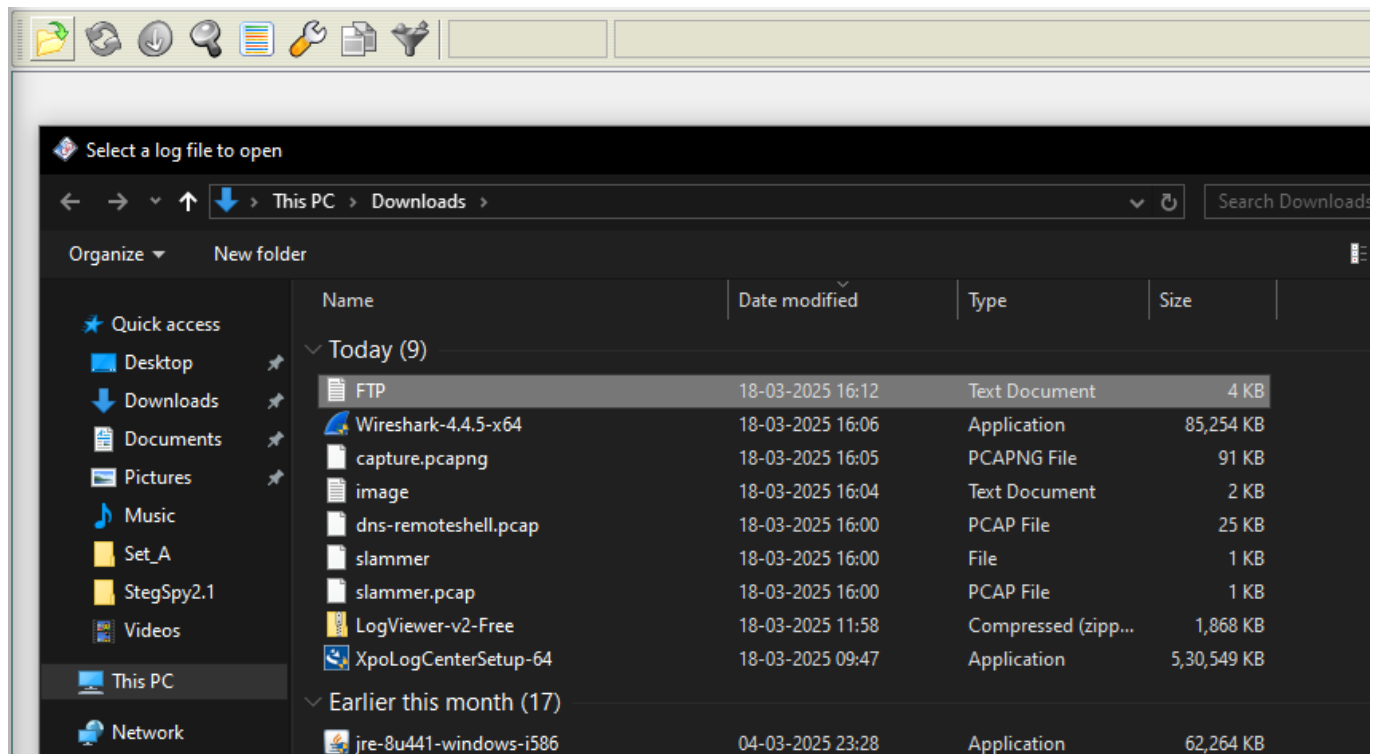
Observation from XpoLog Analytics Dashboard

- 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.

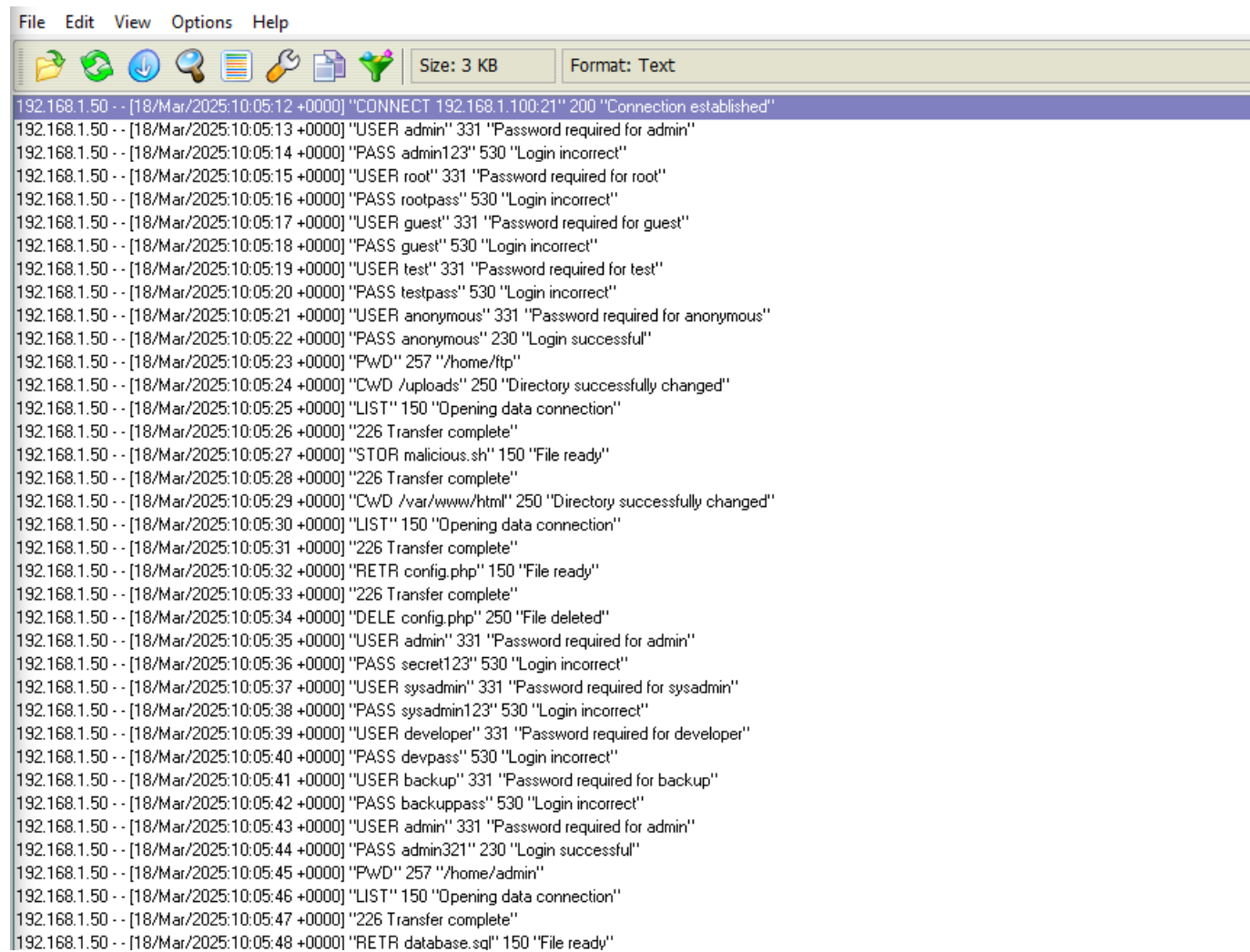
Investigating Network Attacks Using Kiwi Log Viewer

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





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

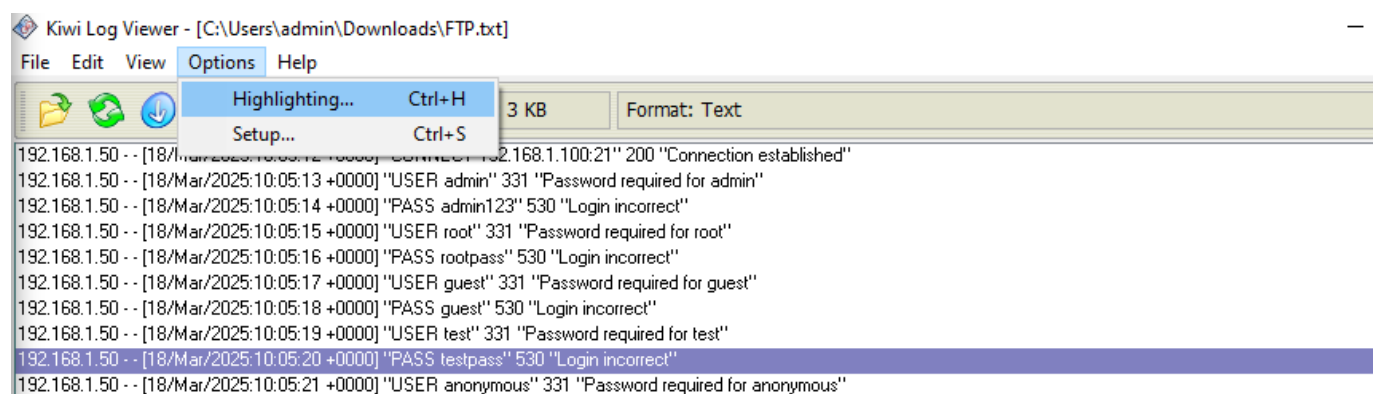


The screenshot shows the Kiwi Log Viewer application window. The menu bar includes File, Edit, View, Options, and Help. The toolbar contains icons for file operations and a status bar showing 'Size: 3 KB' and 'Format: Text'. The main text area displays a list of FTP log entries, each starting with an IP address and a timestamp, followed by a command and a response code. The entries include connection establishment, user authentication attempts (some successful, some with 'Password required' or 'Login incorrect' responses), directory changes, and file transfers.

```

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"
192.168.1.50 -- [18/Mar/2025:10:05:47 +0000] "226 Transfer complete"
192.168.1.50 -- [18/Mar/2025:10:05:48 +0000] "RETR database.sql" 150 "File ready"

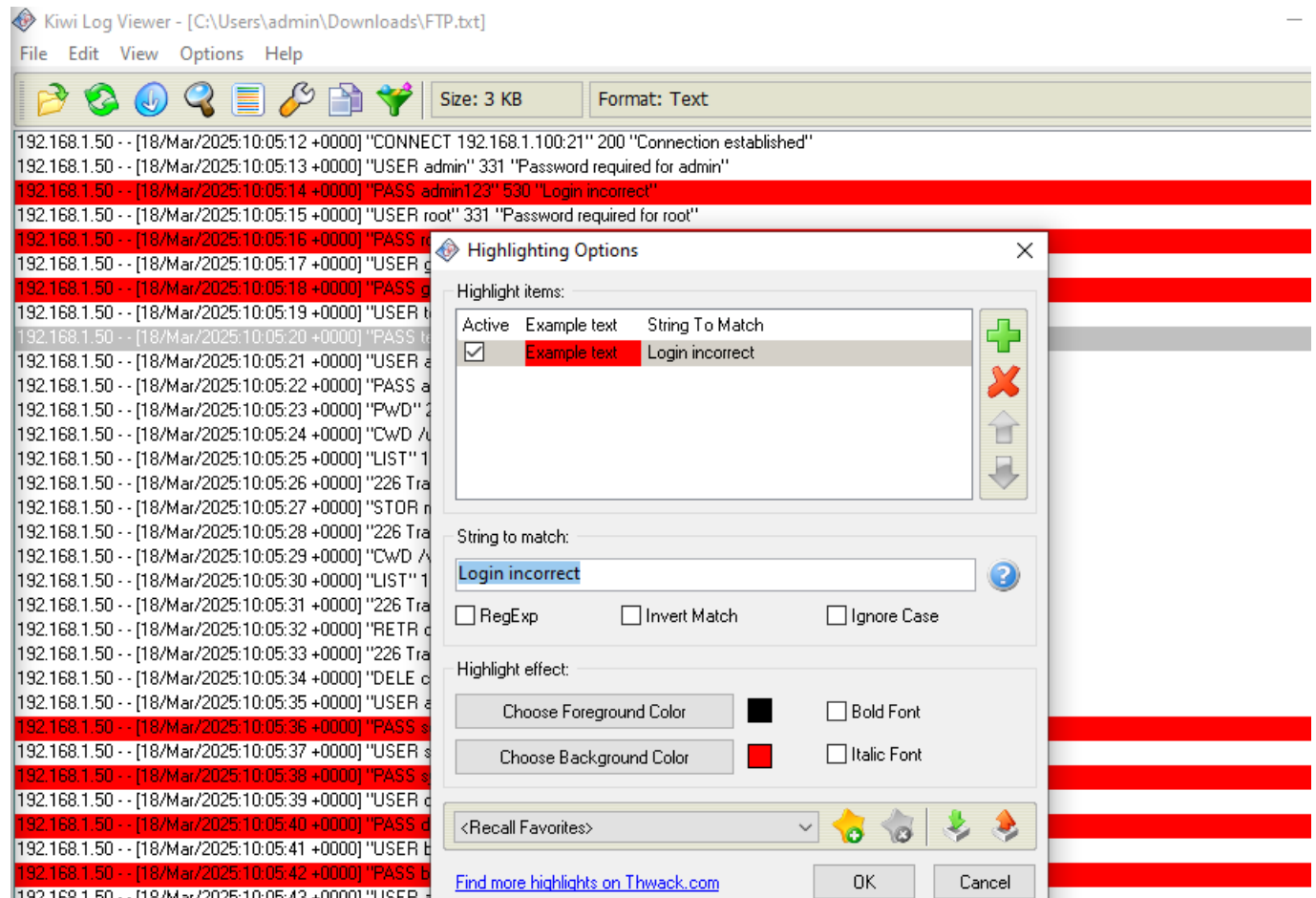
```



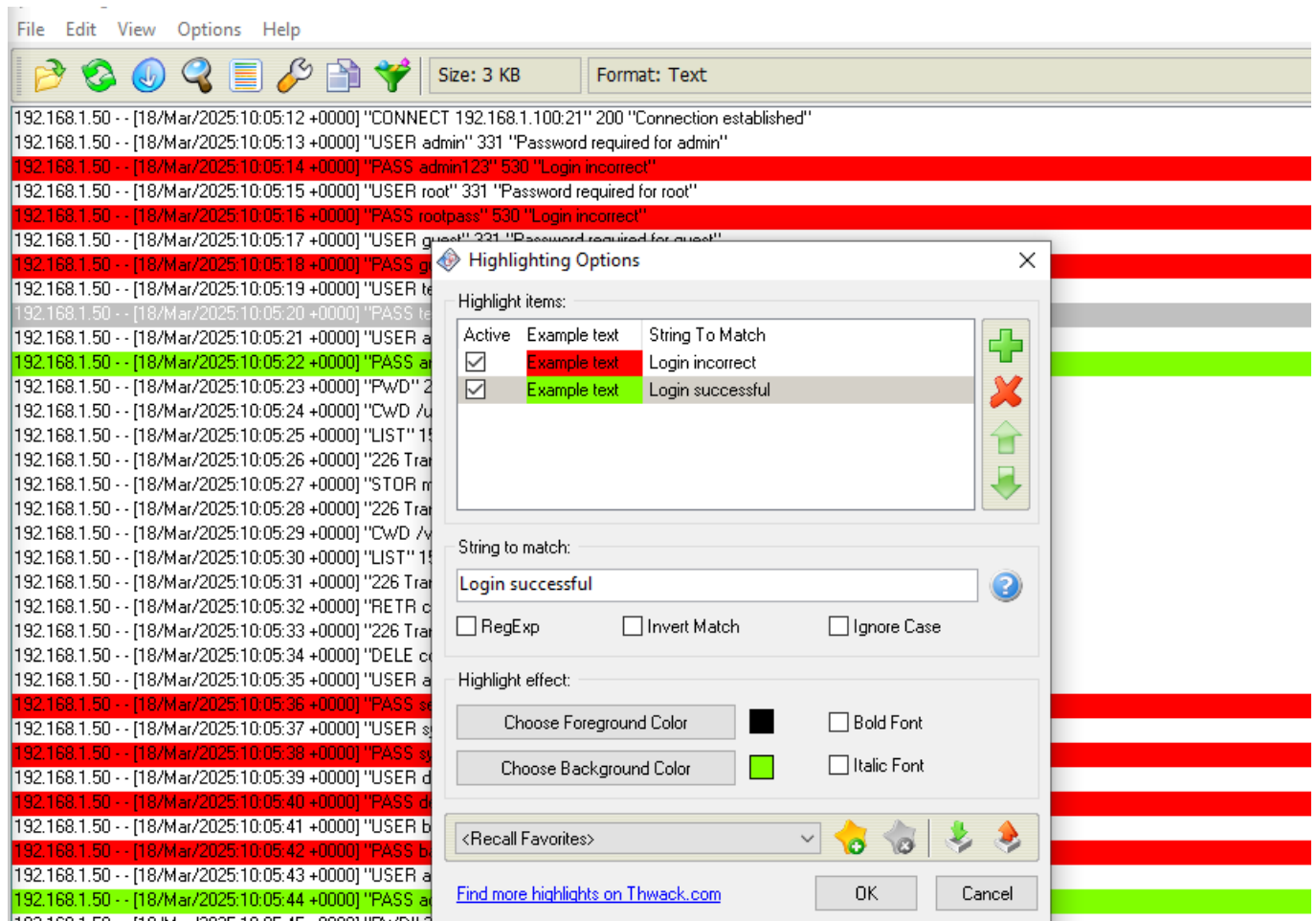
This screenshot shows the same Kiwi Log Viewer window, but with the 'Options' menu open. The menu items are 'Highlighting...' (with a keyboard shortcut of Ctrl+H) and 'Setup...' (with a keyboard shortcut of Ctrl+S). The status bar still shows '3 KB' and 'Format: Text'. The log entries are visible in the background, with the entry for '192.168.1.50 -- [18/Mar/2025:10:05:21 +0000] "USER anonymous" 331 "Password required for anonymous"' highlighted.

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

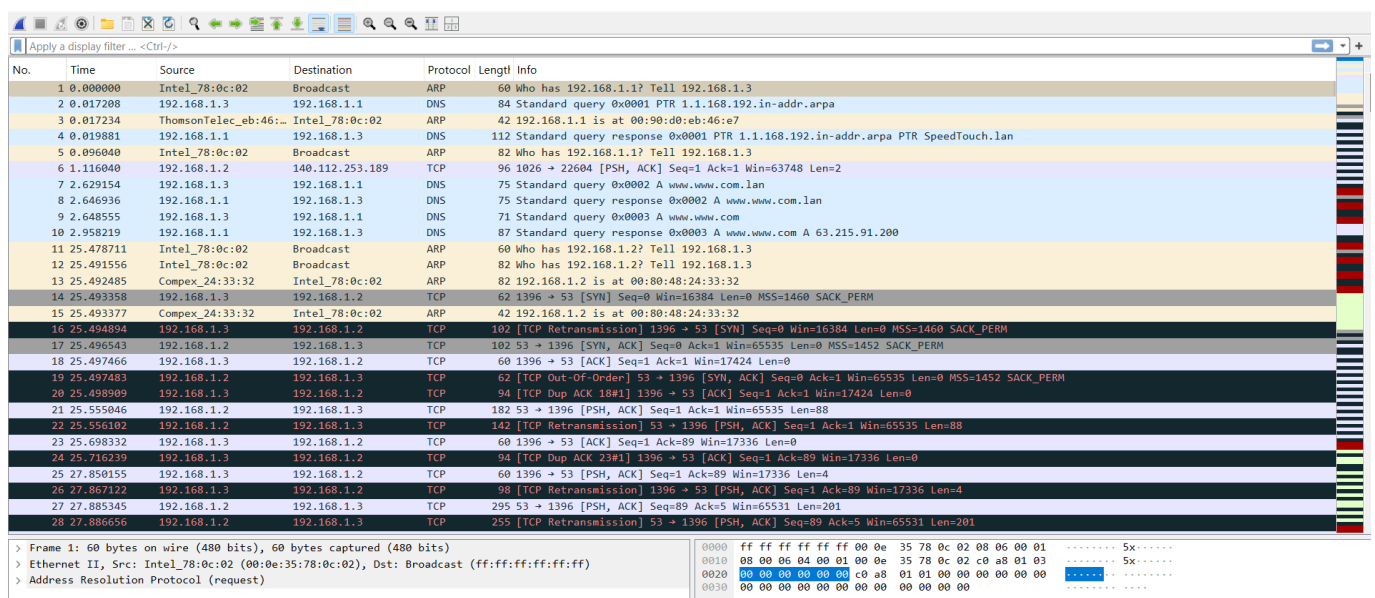
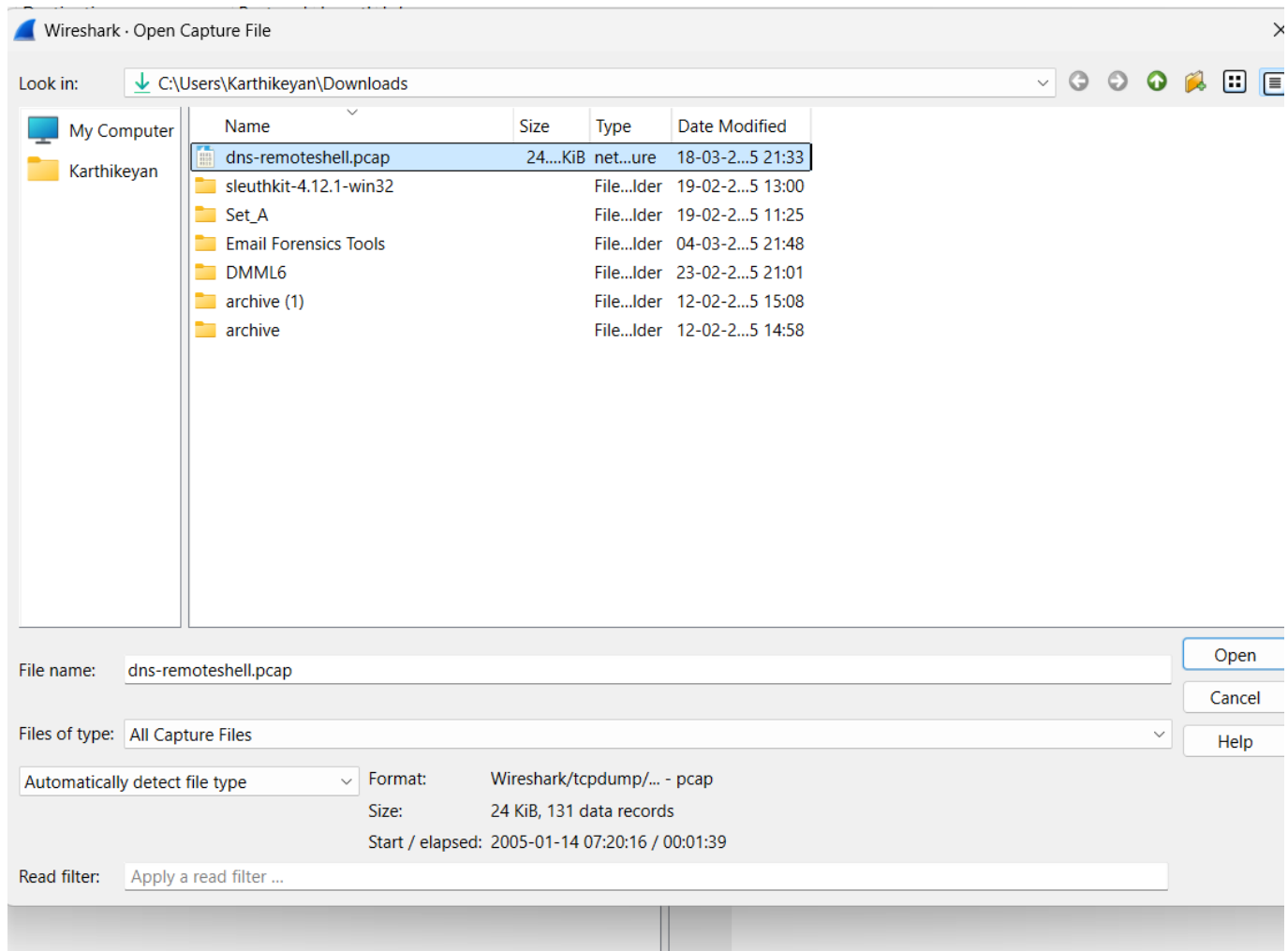
Size: 3 KB Format: Text

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.



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

http						
No.	Time	Source	Destination	Protocol	Length	Info
74	73.158328	192.168.1.2	83.170.75.178	HTTP	486	GET /images/empty.gif HTTP/1.1
75	73.176865	83.170.75.178	192.168.1.2	HTTP	415	HTTP/1.1 304 Not Modified

> Frame 74: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) > Ethernet II, Src: ThomsonTelec_eb:46:e7 (00:90:d0:eb:46:e7), Dst: UniversalGlo_30:6b:b3 (00:10:c6:30:6b:b3) > IEEE 802.11 Data, Flags: .p.....T > Logical-Link Control > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 83.170.75.178 > Transmission Control Protocol, Src Port: 1110, Dst Port: 80, Seq: 1, Ack: 1, Len: 392 > Hypertext Transfer Protocol		0000 00 10 c6 30 6b b3 00 90 d0 eb 46 e7 24 52 08 41 ...0k... F \$R A 0010 02 01 00 10 c6 30 6b b3 00 80 48 24 33 32 00 900k... H\$32.. 0020 d0 eb 46 e7 e0 05 dd 57 ce 00 aa aa 03 00 00 00 ...F....W 0030 08 00 45 00 01 b0 07 ef 40 00 40 06 d0 52 c0 a8 ...E.... @-R.. 0040 01 02 53 aa 4b b2 04 56 00 50 86 13 b0 ed 8b e9 ...S K-V P..... 0050 a4 a2 50 18 ff ff 95 b4 00 00 47 45 54 20 2f 69 ...P.... GET /i 0060 6d 61 67 65 73 2f 65 6d 70 74 79 2e 67 69 66 20 mages/em pty.gif 0070 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 Accept 0080 3a 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 72 3a 20 : /*-R eferer: 0090 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 61 6c 73 http://w ww.goals 00a0 33 36 35 2e 63 6f 6d 2f 6c 69 76 65 73 63 6f 72 365.com/ livescor 00b0 65 2e 68 74 6d 6c 0d 0a 41 63 63 65 70 74 2d 4c e.html Accept-L 00c0 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 0d 0a anguage: en-us-
--	--	---

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.

http.request.method == GET						
No.	Time	Source	Destination	Protocol	Length	Info
74	73.158328	192.168.1.2	83.170.75.178	HTTP	486	GET /images/empty.gif HTTP/1.1

> Frame 74: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) > Ethernet II, Src: ThomsonTelec_eb:46:e7 (00:90:d0:eb:46:e7), Dst: UniversalGlo_30:6b:b3 (00:10:c6:30:6b:b3) > IEEE 802.11 Data, Flags: .p.....T > Logical-Link Control > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 83.170.75.178 > Transmission Control Protocol, Src Port: 1110, Dst Port: 80, Seq: 1, Ack: 1, Len: 392 > Hypertext Transfer Protocol		0000 00 10 c6 30 6b b3 00 90 d0 eb 46 e7 24 52 08 41 ...0k... F \$R A 0010 02 01 00 10 c6 30 6b b3 00 80 48 24 33 32 00 900k... H\$32.. 0020 d0 eb 46 e7 e0 05 dd 57 ce 00 aa aa 03 00 00 00 ...F....W 0030 08 00 45 00 01 b0 07 ef 40 00 40 06 d0 52 c0 a8 ...E.... @-R.. 0040 01 02 53 aa 4b b2 04 56 00 50 86 13 b0 ed 8b e9 ...S K-V P..... 0050 a4 a2 50 18 ff ff 95 b4 00 00 47 45 54 20 2f 69 ...P.... GET /i 0060 6d 61 67 65 73 2f 65 6d 70 74 79 2e 67 69 66 20 mages/em pty.gif 0070 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 Accept 0080 3a 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 72 3a 20 : /*-R eferer: 0090 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 61 6c 73 http://w ww.goals 00a0 33 36 35 2e 63 6f 6d 2f 6c 69 76 65 73 63 6f 72 365.com/ livescor 00b0 65 2e 68 74 6d 6c 0d 0a 41 63 63 65 70 74 2d 4c e.html Accept-L 00c0 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 0d 0a anguage: en-us- 00d0 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding: 00e0 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, deflate 00f0 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69 6e 63 If-Modif ied-Sinc 0100 65 3a 20 4d 6f 6e 2c 20 30 31 20 4d 61 72 20 32 e: Mon, 01 Mar 2 0110 30 30 34 20 31 35 3a 30 37 3a 31 34 20 47 4d 54 004 15:0 7:14 GMT 0120 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a --If-Non e-Match: 0130 20 22 37 38 30 65 64 2d 30 2d 33 34 35 65 32 63 "780ed- 0-345e2c
--	--	---

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.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.017208	192.168.1.3	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
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
7	2.629154	192.168.1.3	192.168.1.1	DNS	75	Standard query 0x0002 A wwwl.wwwl.com.lan
8	2.646936	192.168.1.1	192.168.1.3	DNS	75	Standard query response 0x0002 A wwwl.wwwl.com.lan
9	2.648555	192.168.1.3	192.168.1.1	DNS	71	Standard query 0x0003 A wwwl.wwwl.com
10	2.958219	192.168.1.1	192.168.1.3	DNS	87	Standard query response 0x0003 A wwwl.wwwl.com A 63.215.91.200
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
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	25.498989	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	25.555846	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	86	[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

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.

File Edit View Go Capture Analyze

tcp.stream eq 11

No.	Time	Source
79	75.795348	192.168.1.2
90	77.369965	192.168.1.2
94	77.496278	192.168.1.2
106	85.568925	192.168.1.2
100	79.093207	192.168.1.2
84	75.854916	192.168.1.2
77	75.793185	192.168.1.3
98	79.041217	192.168.1.3
104	85.563833	192.168.1.3
88	77.351319	192.168.1.3
81	75.796334	192.168.1.2
96	77.689407	192.168.1.3
92	77.489498	192.168.1.3
86	75.971875	192.168.1.3
82	75.797487	192.168.1.3
102	79.291787	192.168.1.3
83	75.853847	192.168.1.2
97	79.024691	192.168.1.3
105	85.567970	192.168.1.2
103	85.547606	192.168.1.3
87	77.334968	192.168.1.3
78	75.794613	192.168.1.2
108	85.570124	192.168.1.2
107	85.569230	192.168.1.2
89	77.368651	192.168.1.2
76	75.776641	192.168.1.3
91	77.472790	192.168.1.3
95	77.673174	192.168.1.3
101	79.275397	192.168.1.3
85	75.970623	192.168.1.3
80	75.796306	192.168.1.3
99	79.092111	192.168.1.2
93	77.493408	192.168.1.2

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>
dir

dir

Volume in drive C has no label.
Volume Serial Number is FF47-80EB

Directory of C:\

```

01/12/2005  11:59 AM           0 aierrorlog.txt
01/19/2004  09:45 PM           0 AUTOEXEC.BAT
01/19/2004  09:45 PM           0 CONFIG.SYS
06/26/2004  12:12 PM           <DIR>
                Documents and Settings
02/03/2005  11:40 PM           <DIR>
                EasyBoot
02/29/2004  02:51 PM    11,531 installer-debug.txt
12/19/2004  12:50 AM           <DIR>
                mga
12/19/2004  12:51 AM           <DIR>
                mgafold
11/24/2004  07:47 PM           <DIR>
                mnt
10/07/2004  10:01 AM           <DIR>
                movie
06/26/2004  01:03 PM           <DIR>
                My Downloads
01/13/2005  10:52 PM           <DIR>
                Program Files
01/04/2005  10:27 AM           <DIR>
                quarantine
04/19/2004  09:57 PM    7,241 s37g
10/31/2004  08:36 PM           0 s3fs
06/02/2004  08:54 PM    123 systemscandata.txt
08/08/2004  10:48 AM           <DIR>
                Temp
12/12/2004  02:24 PM    94,135,944 temp.mpg
01/13/2005  06:10 PM           <DIR>
                WINDOWS
11/20/2004  09:27 AM           <DIR>
                WUTemp
                8 File(s)      94,154,839 bytes
                12 Dir(s)    7,145,889,792 bytes free

```

C:\>
ls -la

ls -la

'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>
exit

Frame 79: 102 bytes on wire (816 bits)

Ethernet II, Src: Intel_78:0c:00:00:00:00, Dst: Intel_78:0c:00:00:00:00

IEEE 802.11 Data, Flags: D, R, ...

Packet 89: 3 client pkts, 5 server pkts, 6 turns. Click to select.

Entire conversation (1429 bytes)

Show as ASCII

No delta times

Stream 11

