LAB1

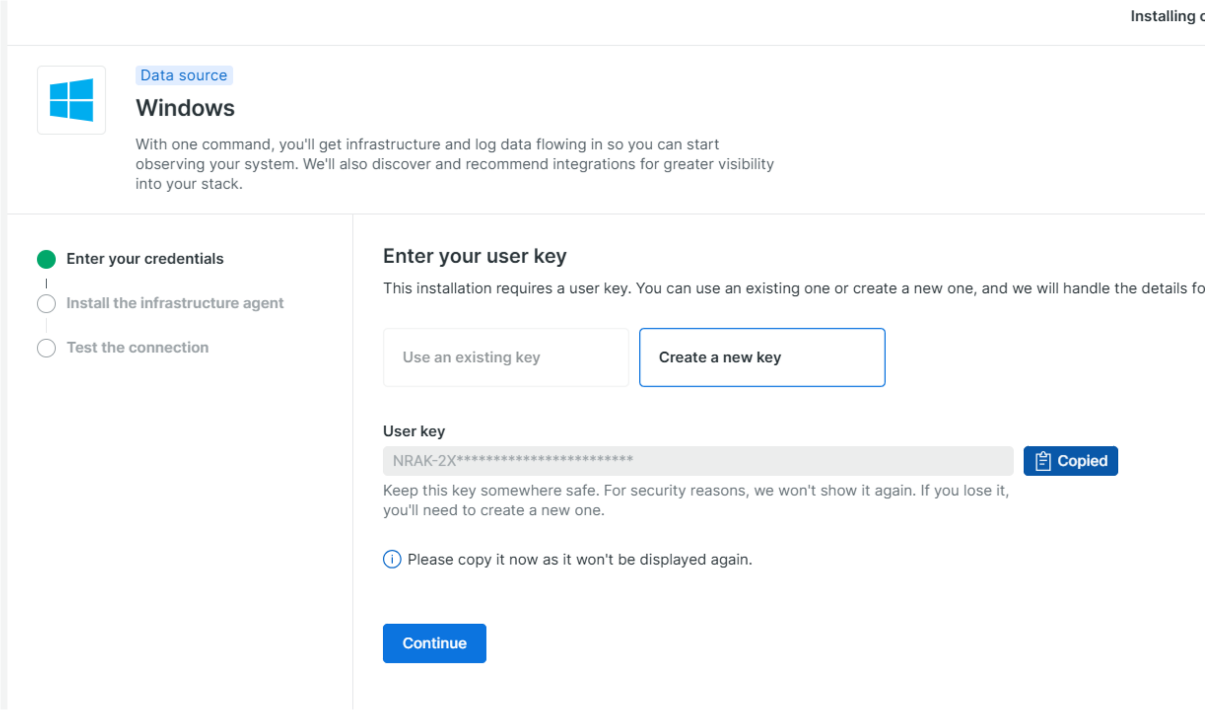
Capturing and Analyzing the Logs of a computer using GFI Events Manager

Lab objectives:

The objective of this lab is to help the forensic investigator understand and perform log capturing of a computer using various techniques , to obtain:

- Security event
- Application events
- System events

Installed Event Manager but cant get the license. So that installed new relic which will use to get event logs of windows



Installing c

Data source

Windows

With one command, you'll get infrastructure and log data flowing in so you can start observing your system. We'll also discover and recommend integrations for greater visibility into your stack.

● Enter your credentials

○ Install the infrastructure agent

○ Test the connection

Enter your user key

This installation requires a user key. You can use an existing one or create a new one, and we will handle the details fo

Use an existing key

Create a new key

User key

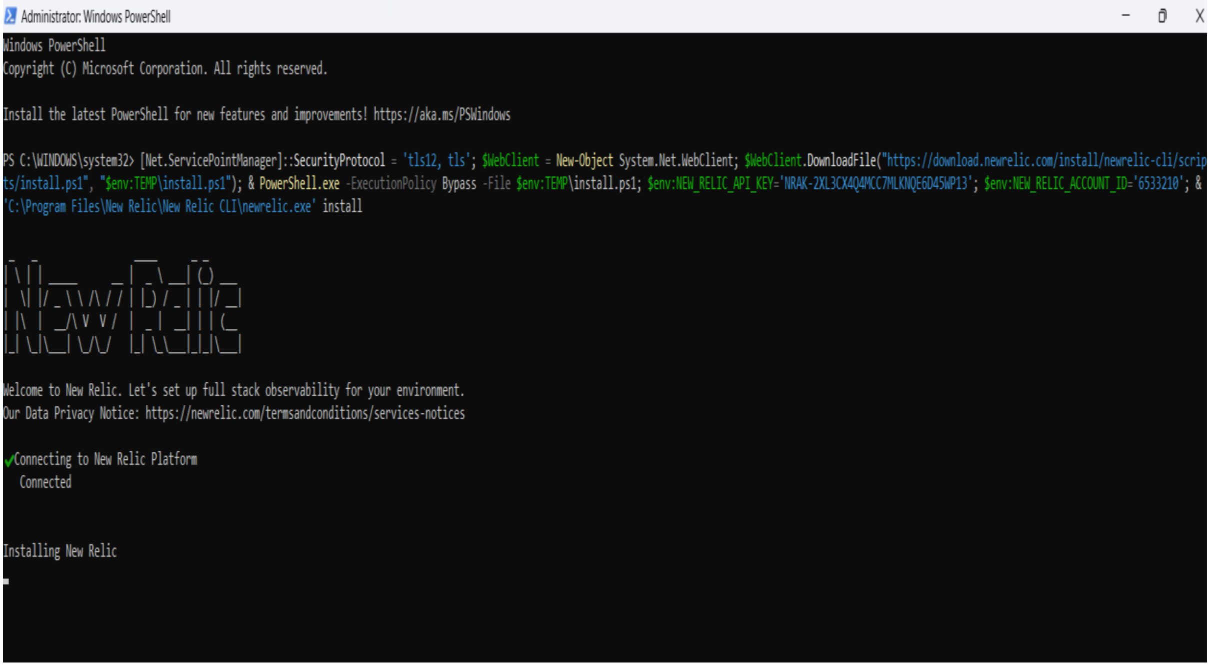
NRAK-2X************************

Copied

Keep this key somewhere safe. For security reasons, we won't show it again. If you lose it, you'll need to create a new one.

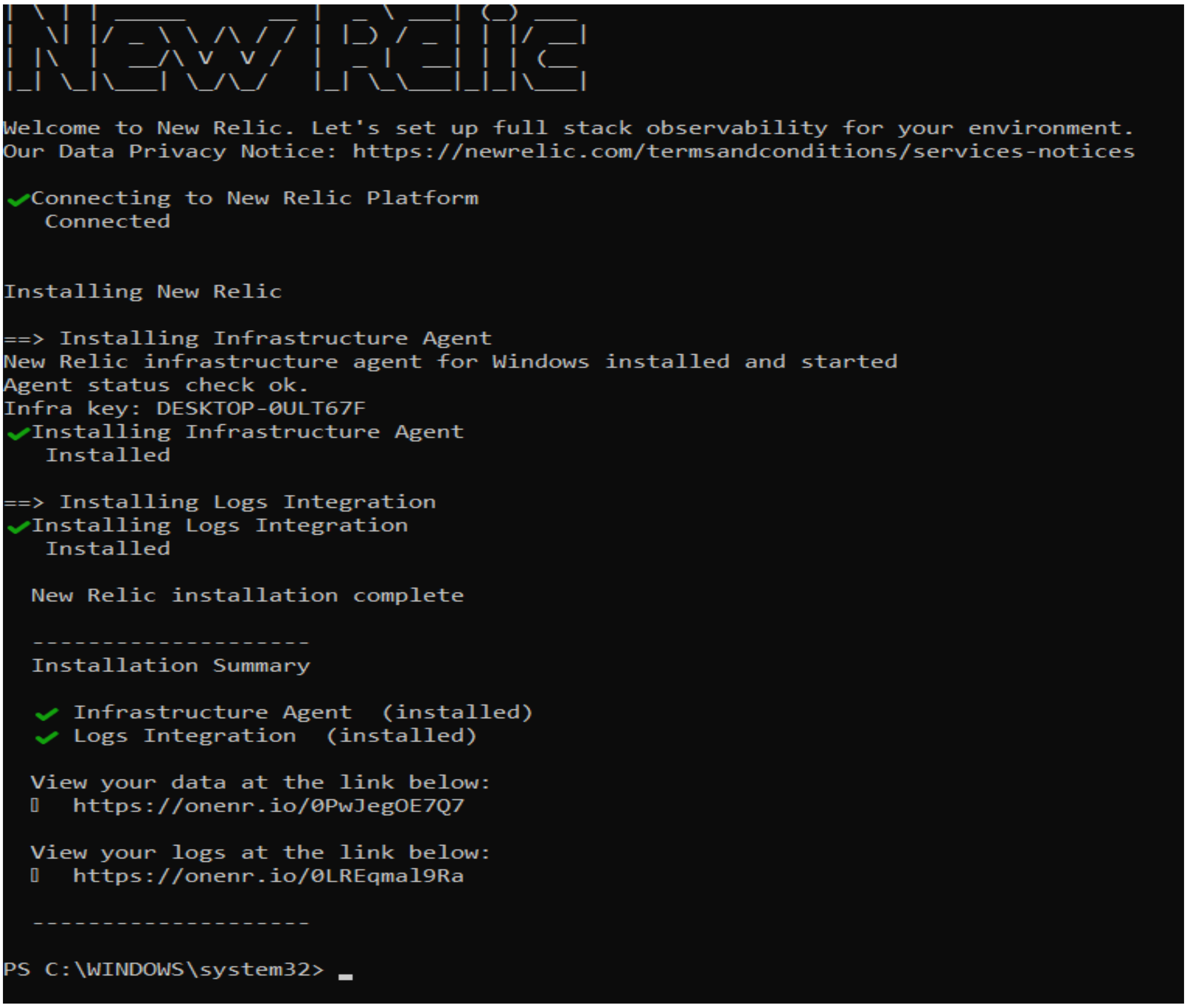
ⓘ Please copy it now as it won't be displayed again.

Continue

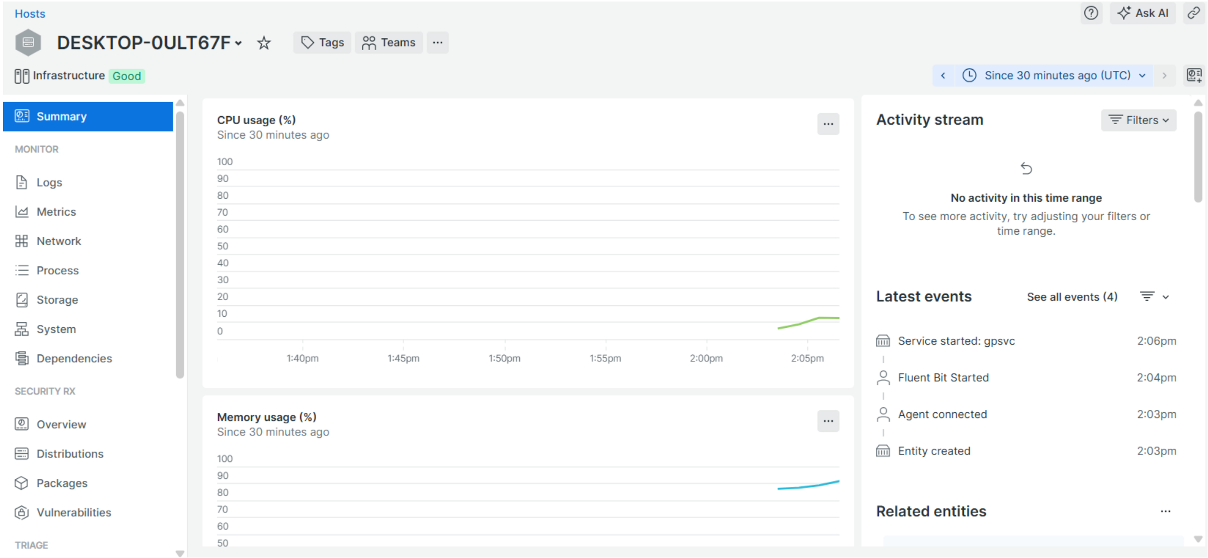


Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> [Net.ServicePointManager]::SecurityProtocol = 'tls12, tls'; $WebClient = New-Object System.Net.WebClient; $WebClient.DownloadFile("https://download.newrelic.com/install/newrelic-cli/scrip
ts/install.ps1", "$env:TEMP\install.ps1"); & PowerShell.exe -ExecutionPolicy Bypass -File $env:TEMP\install.ps1; $env:NEW_RELIC_API_KEY='NRAK-2XL3CX4Q4MCC7MLKNQE6D45WP13'; $env:NEW_RELIC_ACCOUNT_ID='6533210'; &
'C:\Program Files\New Relic\New Relic CLI\newrelic.exe' install


 _   _                 ____      _ _
| \ | | _____      __ |  _ \ ___| (_) ___
|  \| |/ _ \ \ /\ / / | |_) / _ \ | |/ __|
| |\  |  __/\ V  V /  |  _ <  __/ | | (__
|_| \_|\___| \_/\_/   |_| \_\___|_|_|\___|


Welcome to New Relic. Let's set up full stack observability for your environment.
Our Data Privacy Notice: https://newrelic.com/termsandconditions/services-notices

✓Connecting to New Relic Platform
  Connected


Installing New Relic
```



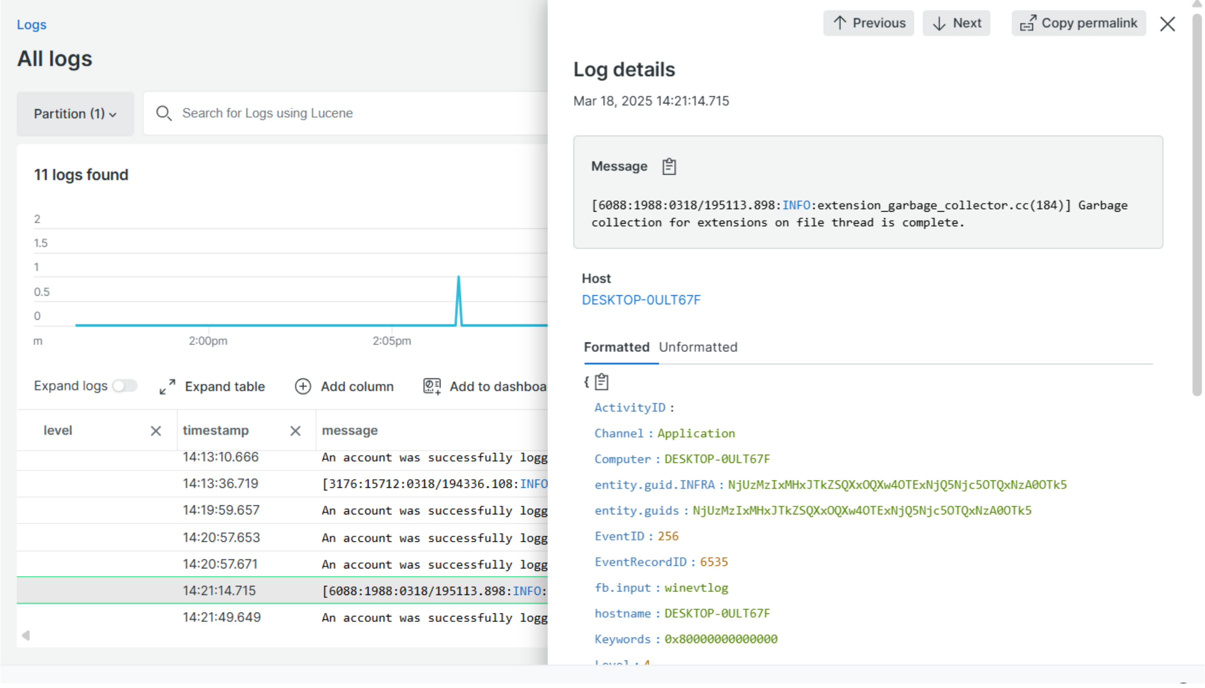
```
| \ | | _____      __ |  _ \ ___| (_) ___
|  \| |/ _ \ \ /\ / / | |_) / _ \ | |/ __|
| |\  |  __/\ V  V /  |  _ <  __/ | | (__
|_| \_|\___| \_/\_/   |_| \_\___|_|_|\___|

Welcome to New Relic. Let's set up full stack observability for your environment.
Our Data Privacy Notice: https://newrelic.com/termsandconditions/services-notices

✓Connecting to New Relic Platform
  Connected


Installing New Relic

==> Installing Infrastructure Agent
New Relic infrastructure agent for Windows installed and started
Agent status check ok.
Infra key: DESKTOP-0ULT67F
✓Installing Infrastructure Agent
  Installed

==> Installing Logs Integration
✓Installing Logs Integration
  Installed

  New Relic installation complete

  --------------------
  Installation Summary

  ✓ Infrastructure Agent  (installed)
  ✓ Logs Integration  (installed)

  View your data at the link below:
  ▯  https://onenr.io/0PwJegOE7Q7

  View your logs at the link below:
  ▯  https://onenr.io/0LREqmal9Ra

  --------------------

PS C:\WINDOWS\system32> _
```



No activity in this time range

To see more activity, try adjusting your filters or time range.

Service started: gpsvc	2:06pm
Fluent Bit Started	2:04pm
Agent connected	2:03pm
Entity created	2:03pm



level	timestamp	message
	14:13:10.666	An account was successfully logg
	14:13:36.719	[3176:15712:0318/194336.108:INFO
	14:19:59.657	An account was successfully logg
	14:20:57.653	An account was successfully logg
	14:20:57.671	An account was successfully logg
	14:21:14.715	[6088:1988:0318/195113.898:INFO:
	14:21:49.649	An account was successfully logg

Log details

Mar 18, 2025 14:21:14.715

Message

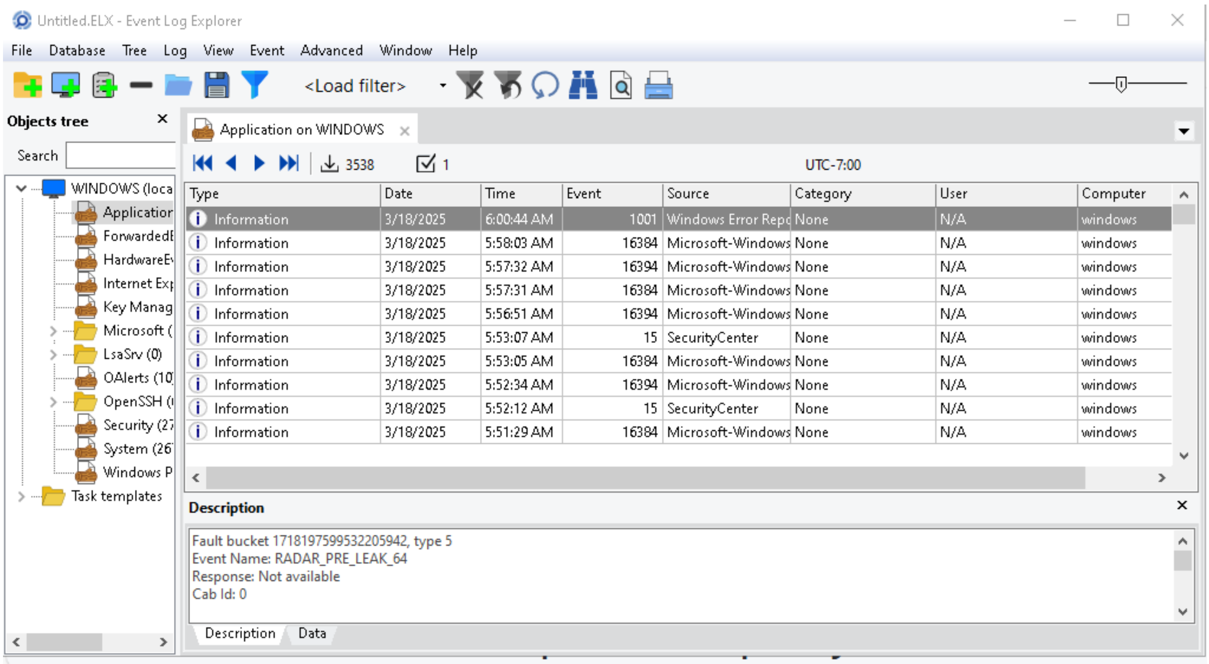
```
[6088:1988:0318/195113.898:INFO:extension_garbage_collector.cc(184)] Garbage
collection for extensions on file thread is complete.
```

Host

DESKTOP-0ULT67F

```
{
  ActivityID :
  Channel : Application
  Computer : DESKTOP-0ULT67F
  entity.guid.INFRA : NjUzMzIxMHxJTkZSQXxOQXw4OTExNjQ5Njc5OTQxNzA0OTk5
  entity.guids : NjUzMzIxMHxJTkZSQXxOQXw4OTExNjQ5Njc5OTQxNzA0OTk5
  EventID : 256
  EventRecordID : 6535
  fb.input : winevtlog
  hostname : DESKTOP-0ULT67F
  Keywords : 0x80000000000000
  Level : 4
```

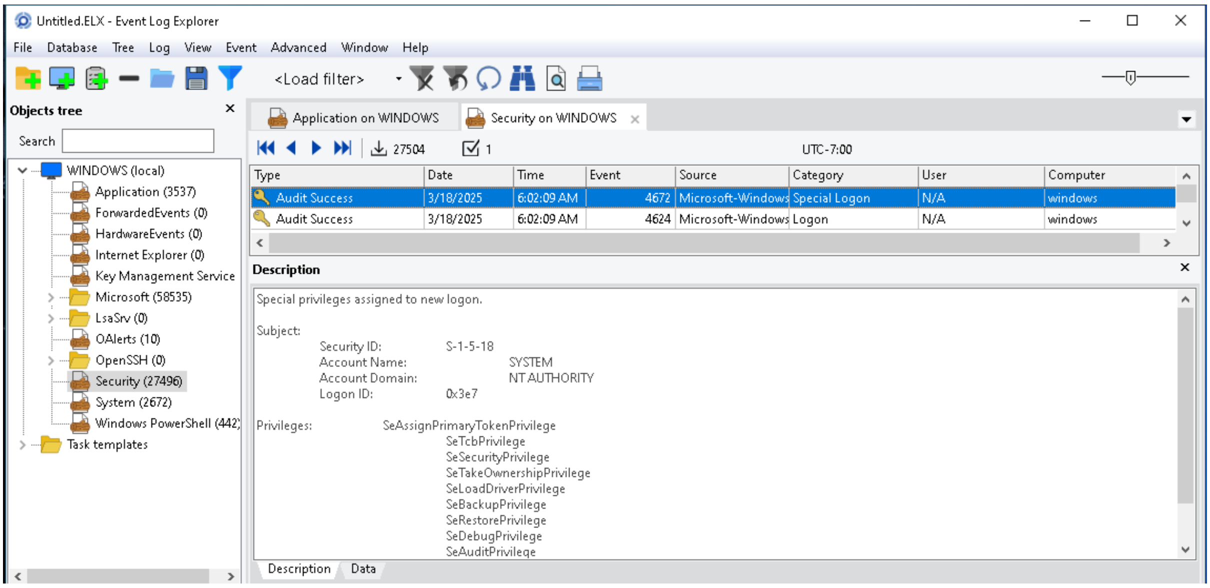
I also tried event log explorer.



Type	Date	Time	Event	Source	Category	User	Computer
Information	3/18/2025	6:00:44 AM	1001	Windows Error Repo	None	N/A	windows
Information	3/18/2025	5:58:03 AM	16384	Microsoft-Windows	None	N/A	windows
Information	3/18/2025	5:57:32 AM	16394	Microsoft-Windows	None	N/A	windows
Information	3/18/2025	5:57:31 AM	16384	Microsoft-Windows	None	N/A	windows
Information	3/18/2025	5:56:51 AM	16394	Microsoft-Windows	None	N/A	windows
Information	3/18/2025	5:53:07 AM	15	SecurityCenter	None	N/A	windows
Information	3/18/2025	5:53:05 AM	16384	Microsoft-Windows	None	N/A	windows
Information	3/18/2025	5:52:34 AM	16394	Microsoft-Windows	None	N/A	windows
Information	3/18/2025	5:52:12 AM	15	SecurityCenter	None	N/A	windows
Information	3/18/2025	5:51:29 AM	16384	Microsoft-Windows	None	N/A	windows

```
Fault bucket 1718197599532205942, type 5
Event Name: RADAR_PRE_LEAK_64
Response: Not available
Cab Id: 0
```

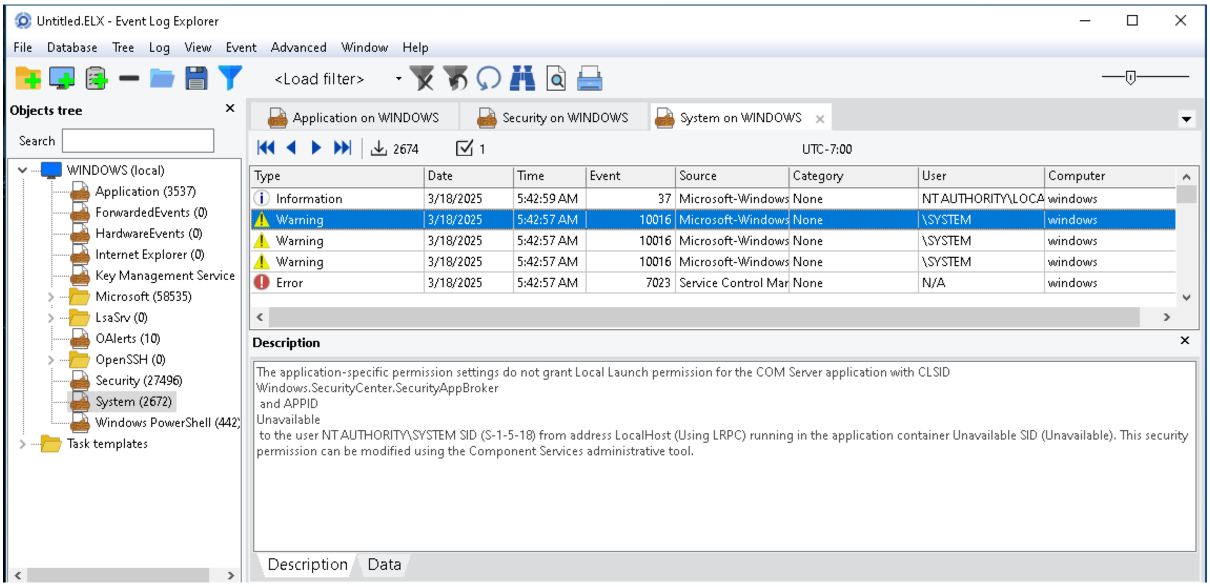
This shows the logs of application on windows.



Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	3/18/2025	6:02:09 AM	4672	Microsoft-Windows	Special Logon	N/A	windows
Audit Success	3/18/2025	6:02:09 AM	4624	Microsoft-Windows	Logon	N/A	windows

```
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-18
        Account Name:                   SYSTEM
        Account Domain:                 NT AUTHORITY
        Logon ID:               0x3e7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeDebugPrivilege
                        SeAuditPrivilege
```

This above figure list out the security events, and its details security ID , Account name etc



Type	Date	Time	Event	Source	Category	User	Computer
Information	3/18/2025	5:42:59 AM	37	Microsoft-Windows	None	NT AUTHORITY\LOCA	windows
Warning	3/18/2025	5:42:57 AM	10016	Microsoft-Windows	None	\SYSTEM	windows
Warning	3/18/2025	5:42:57 AM	10016	Microsoft-Windows	None	\SYSTEM	windows
Warning	3/18/2025	5:42:57 AM	10016	Microsoft-Windows	None	\SYSTEM	windows
Error	3/18/2025	5:42:57 AM	7023	Service Control Mar	None	N/A	windows

```
The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID
Windows.SecurityCenter.SecurityAppBroker
 and APPID
Unavailable
 to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.
```

The above figure shows that system events and warnings related to system, and its description

For the Report view and statistics report, It needs commercial license to export logs as reports

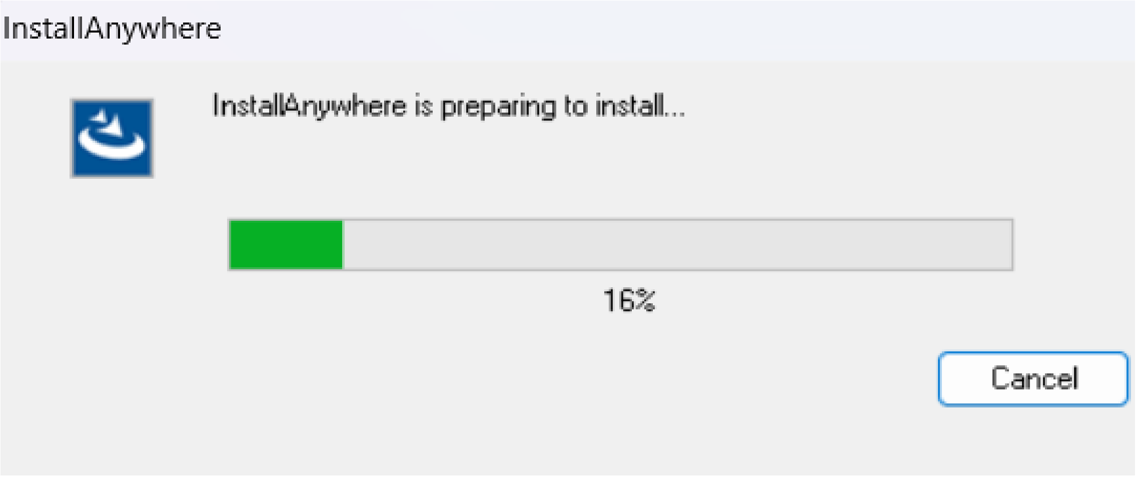
LAB2

INVESTIGATING SYSTEM LOG DATA USING XPOLOG CENTRE SUITE TOOL

Lab objectives:

The objective of this lab is to view the windows logs. We will learn how to

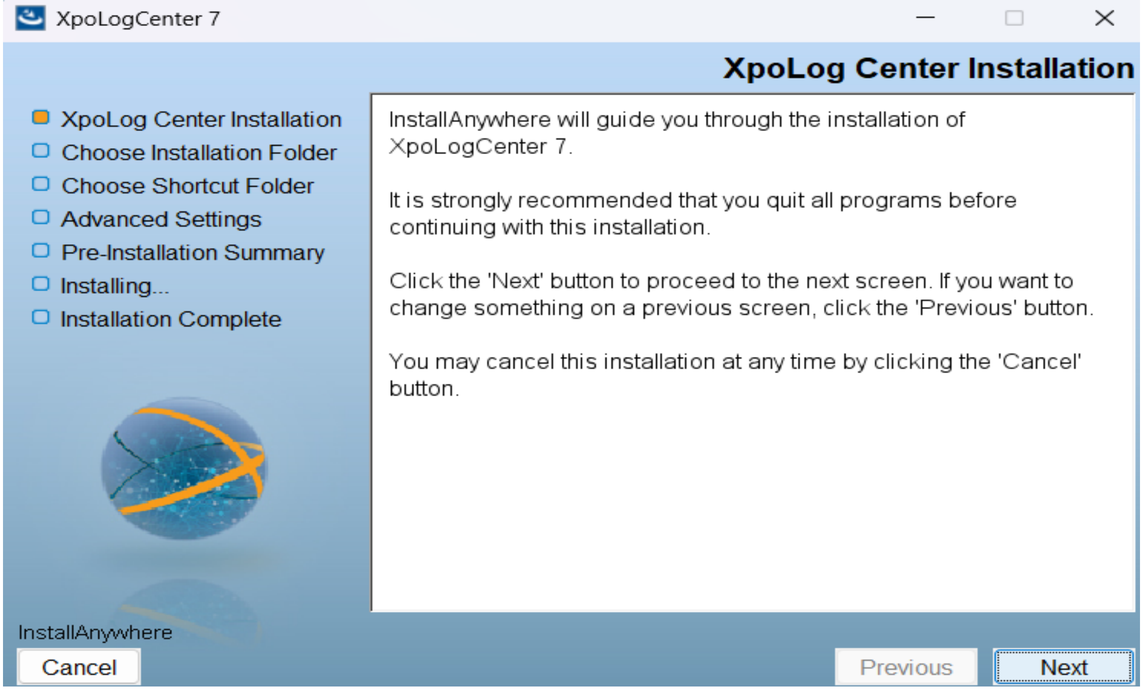
- Collect real time windows logs
- Detect violation in real-time log monitoring and alerting
- Generate comprehensive reports



InstallAnywhere

InstallAnywhere is preparing to install...

16%



XpoLogCenter 7

XpoLog Center Installation

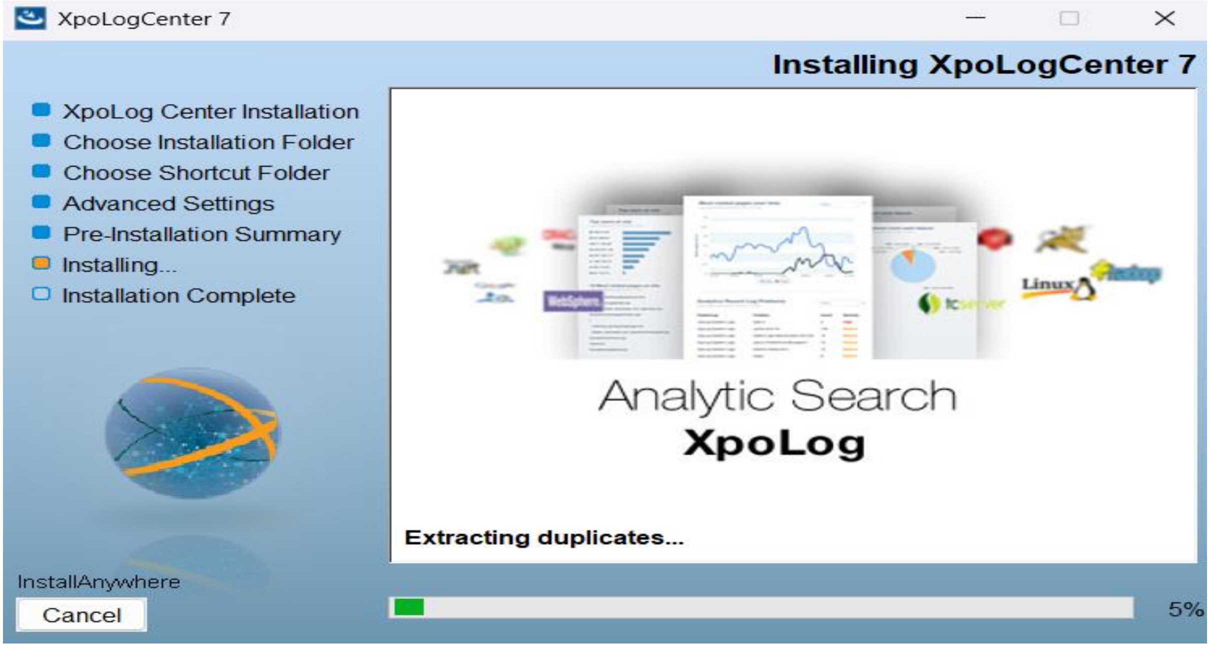
- XpoLog Center Installation
- Choose Installation Folder
- Choose Shortcut Folder
- Advanced Settings
- Pre-Installation Summary
- Installing...
- Installation Complete

InstallAnywhere will guide you through the installation of XpoLogCenter 7.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.



XpoLogCenter 7

Installing XpoLogCenter 7

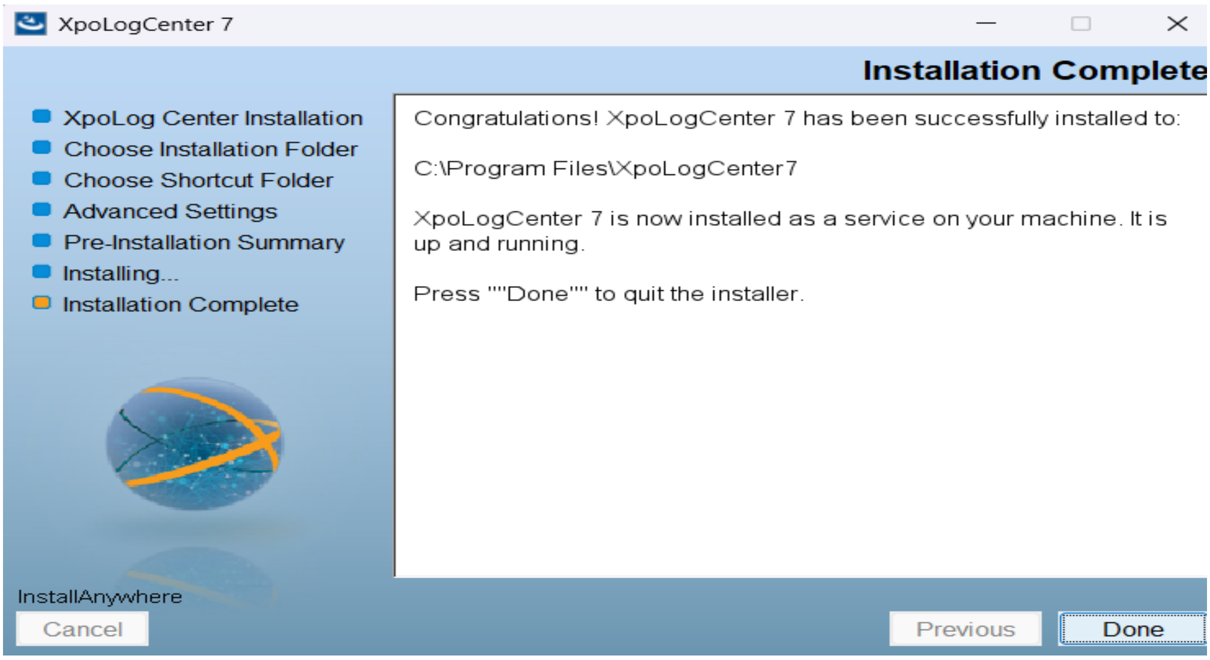
- XpoLog Center Installation
- Choose Installation Folder
- Choose Shortcut Folder
- Advanced Settings
- Pre-Installation Summary
- Installing...
- Installation Complete

Analytic Search

XpoLog

Extracting duplicates...

5%



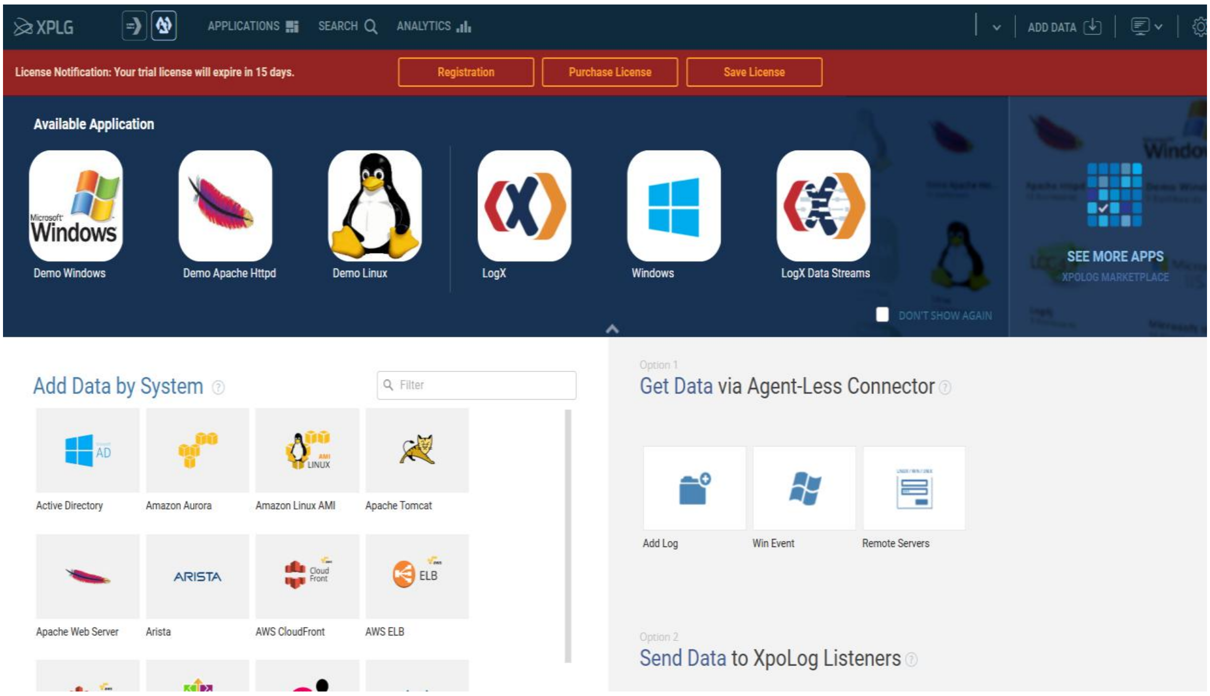
Congratulations! XpoLogCenter 7 has been successfully installed to:

C:\Program Files\XpoLogCenter7

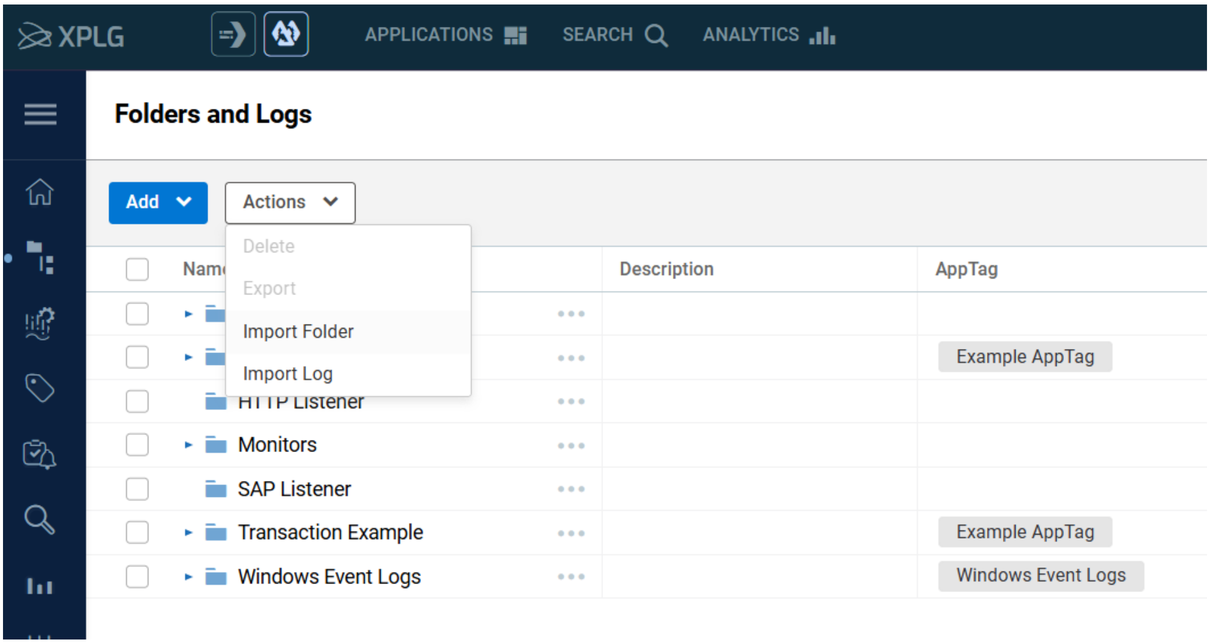
XpoLogCenter 7 is now installed as a service on your machine. It is up and running.

Press ""Done"" to quit the installer.

Once complete the installation , XpoLog GUI appears in the default web browser , click win event.

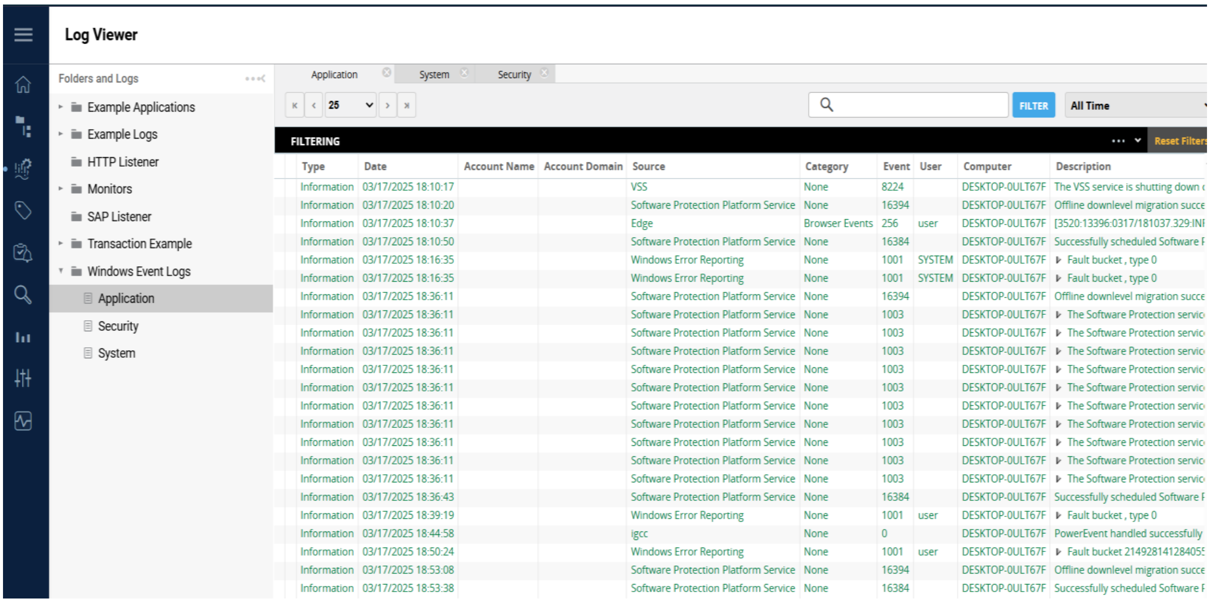


License Notification: Your trial license will expire in 15 days.



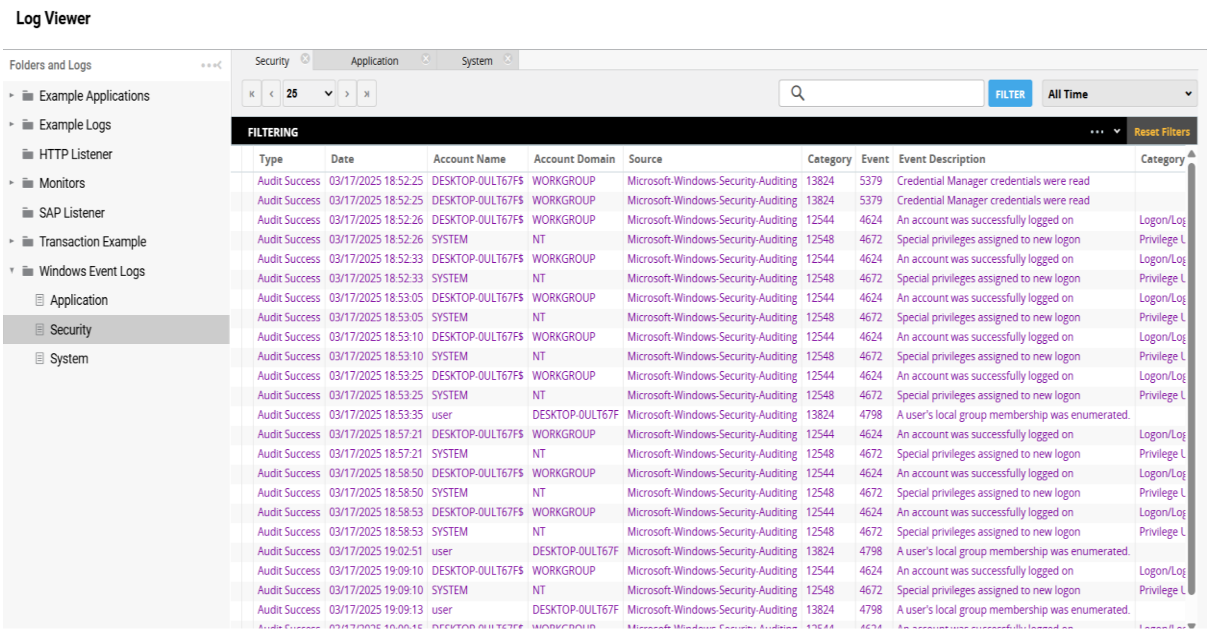
Nam	Description	AppTag
		Example AppTag
HTTP Listener		
Monitors		
SAP Listener		
Transaction Example		Example AppTag
Windows Event Logs		Windows Event Logs

To view windows application logs, click Application



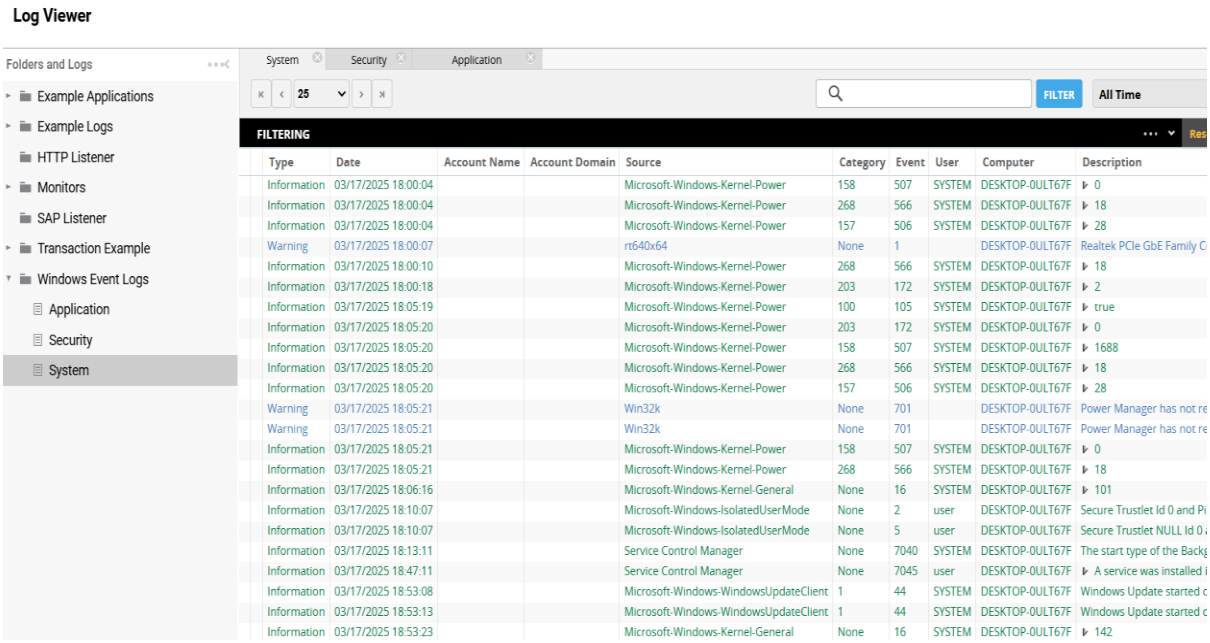
Type	Date	Account Name	Account Domain	Source	Category	Event	User	Computer	Description
Information	03/17/2025 18:10:17			VSS	None	8224		DESKTOP-0ULT67F	The VSS service is shutting down
Information	03/17/2025 18:10:20			Software Protection Platform Service	None	16394		DESKTOP-0ULT67F	Offline downlevel migration succe
Information	03/17/2025 18:10:37			Edge	Browser Events	256	user	DESKTOP-0ULT67F	[3520:13396:0317/181037.329:INF
Information	03/17/2025 18:10:50			Software Protection Platform Service	None	16384		DESKTOP-0ULT67F	Successfully scheduled Software F
Information	03/17/2025 18:16:35			Windows Error Reporting	None	1001	SYSTEM	DESKTOP-0ULT67F	▸ Fault bucket , type 0
Information	03/17/2025 18:16:35			Windows Error Reporting	None	1001	SYSTEM	DESKTOP-0ULT67F	▸ Fault bucket , type 0
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	16394		DESKTOP-0ULT67F	Offline downlevel migration succe
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:11			Software Protection Platform Service	None	1003		DESKTOP-0ULT67F	▸ The Software Protection servic
Information	03/17/2025 18:36:43			Software Protection Platform Service	None	16384		DESKTOP-0ULT67F	Successfully scheduled Software F
Information	03/17/2025 18:39:19			Windows Error Reporting	None	1001	user	DESKTOP-0ULT67F	▸ Fault bucket , type 0
Information	03/17/2025 18:44:58			igcc	None	0		DESKTOP-0ULT67F	PowerEvent handled successfully
Information	03/17/2025 18:50:24			Windows Error Reporting	None	1001	user	DESKTOP-0ULT67F	▸ Fault bucket 214928141284055
Information	03/17/2025 18:53:08			Software Protection Platform Service	None	16394		DESKTOP-0ULT67F	Offline downlevel migration succe
Information	03/17/2025 18:53:38			Software Protection Platform Service	None	16384		DESKTOP-0ULT67F	Successfully scheduled Software F

To view security logs, click security



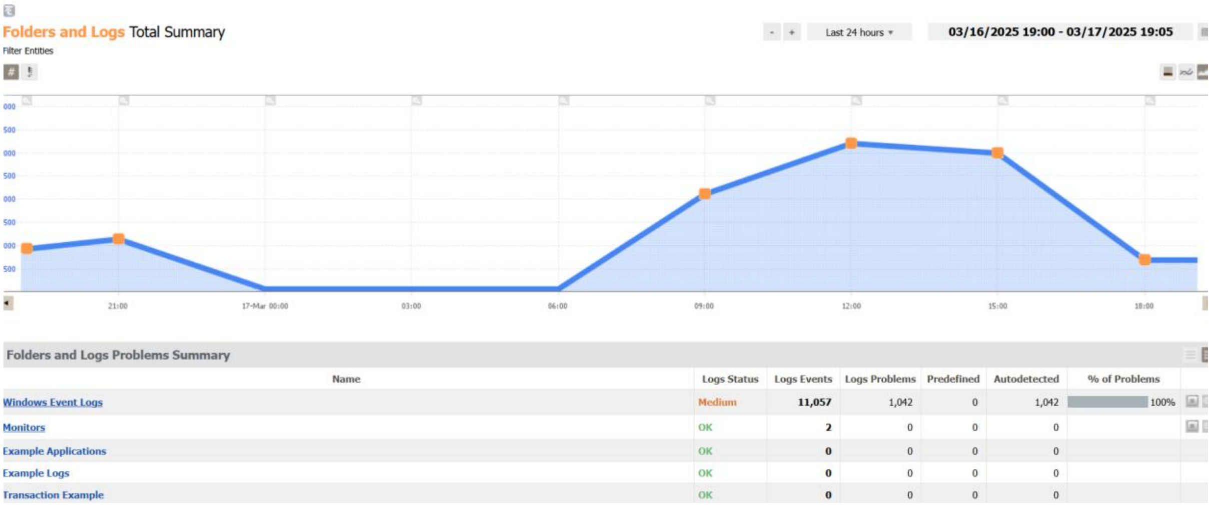
Type	Date	Account Name	Account Domain	Source	Category	Event	Event Description	Category
Audit Success	03/17/2025 18:52:25	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	13824	5379	Credential Manager credentials were read	
Audit Success	03/17/2025 18:52:25	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	13824	5379	Credential Manager credentials were read	
Audit Success	03/17/2025 18:52:26	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:52:26	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:52:33	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:52:33	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:53:05	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:53:05	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:53:10	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:53:10	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:53:25	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:53:25	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:53:35	user	DESKTOP-0ULT67F	Microsoft-Windows-Security-Auditing	13824	4798	A user's local group membership was enumerated.	
Audit Success	03/17/2025 18:57:21	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:57:21	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:58:50	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:58:50	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 18:58:53	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 18:58:53	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 19:02:51	user	DESKTOP-0ULT67F	Microsoft-Windows-Security-Auditing	13824	4798	A user's local group membership was enumerated.	
Audit Success	03/17/2025 19:09:10	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log
Audit Success	03/17/2025 19:09:10	SYSTEM	NT	Microsoft-Windows-Security-Auditing	12548	4672	Special privileges assigned to new logon	Privilege U
Audit Success	03/17/2025 19:09:13	user	DESKTOP-0ULT67F	Microsoft-Windows-Security-Auditing	13824	4798	A user's local group membership was enumerated.	
Audit Success	03/17/2025 19:09:15	DESKTOP-0ULT67F$	WORKGROUP	Microsoft-Windows-Security-Auditing	12544	4624	An account was successfully logged on	Logon/Log

To view window system log click system



Type	Date	Account Name	Account Domain	Source	Category	Event	User	Computer	Description
Information	03/17/2025 18:00:04			Microsoft-Windows-Kernel-Power	158	507	SYSTEM	DESKTOP-0ULT67F	▸ 0
Information	03/17/2025 18:00:04			Microsoft-Windows-Kernel-Power	268	566	SYSTEM	DESKTOP-0ULT67F	▸ 18
Information	03/17/2025 18:00:04			Microsoft-Windows-Kernel-Power	157	506	SYSTEM	DESKTOP-0ULT67F	▸ 28
Warning	03/17/2025 18:00:07			rt640x64	None	1		DESKTOP-0ULT67F	Realtek PCIe GbE Family C
Information	03/17/2025 18:00:10			Microsoft-Windows-Kernel-Power	268	566	SYSTEM	DESKTOP-0ULT67F	▸ 18
Information	03/17/2025 18:00:18			Microsoft-Windows-Kernel-Power	203	172	SYSTEM	DESKTOP-0ULT67F	▸ 2
Information	03/17/2025 18:05:19			Microsoft-Windows-Kernel-Power	100	105	SYSTEM	DESKTOP-0ULT67F	▸ true
Information	03/17/2025 18:05:20			Microsoft-Windows-Kernel-Power	203	172	SYSTEM	DESKTOP-0ULT67F	▸ 0
Information	03/17/2025 18:05:20			Microsoft-Windows-Kernel-Power	158	507	SYSTEM	DESKTOP-0ULT67F	▸ 1688
Information	03/17/2025 18:05:20			Microsoft-Windows-Kernel-Power	268	566	SYSTEM	DESKTOP-0ULT67F	▸ 18
Information	03/17/2025 18:05:20			Microsoft-Windows-Kernel-Power	157	506	SYSTEM	DESKTOP-0ULT67F	▸ 28
Warning	03/17/2025 18:05:21			Win32k	None	701		DESKTOP-0ULT67F	Power Manager has not re
Warning	03/17/2025 18:05:21			Win32k	None	701		DESKTOP-0ULT67F	Power Manager has not re
Information	03/17/2025 18:05:21			Microsoft-Windows-Kernel-Power	158	507	SYSTEM	DESKTOP-0ULT67F	▸ 0
Information	03/17/2025 18:05:21			Microsoft-Windows-Kernel-Power	268	566	SYSTEM	DESKTOP-0ULT67F	▸ 18
Information	03/17/2025 18:06:16			Microsoft-Windows-Kernel-General	None	16	SYSTEM	DESKTOP-0ULT67F	▸ 101
Information	03/17/2025 18:10:07			Microsoft-Windows-IsolatedUserMode	None	2	user	DESKTOP-0ULT67F	Secure Trustlet Id 0 and Pi
Information	03/17/2025 18:10:07			Microsoft-Windows-IsolatedUserMode	None	5	user	DESKTOP-0ULT67F	Secure Trustlet NULL Id 0 a
Information	03/17/2025 18:13:11			Service Control Manager	None	7040	SYSTEM	DESKTOP-0ULT67F	The start type of the Backg
Information	03/17/2025 18:47:11			Service Control Manager	None	7045	user	DESKTOP-0ULT67F	▸ A service was installed i
Information	03/17/2025 18:53:08			Microsoft-Windows-WindowsUpdateClient	1	44	SYSTEM	DESKTOP-0ULT67F	Windows Update started c
Information	03/17/2025 18:53:13			Microsoft-Windows-WindowsUpdateClient	1	44	SYSTEM	DESKTOP-0ULT67F	Windows Update started c
Information	03/17/2025 18:53:23			Microsoft-Windows-Kernel-General	None	16	SYSTEM	DESKTOP-0ULT67F	▸ 142

To view an analytical representation of windowsevent logs click the analytic icon.



Folders and Logs Total Summary

Filter Entities

Last 24 hours ▾

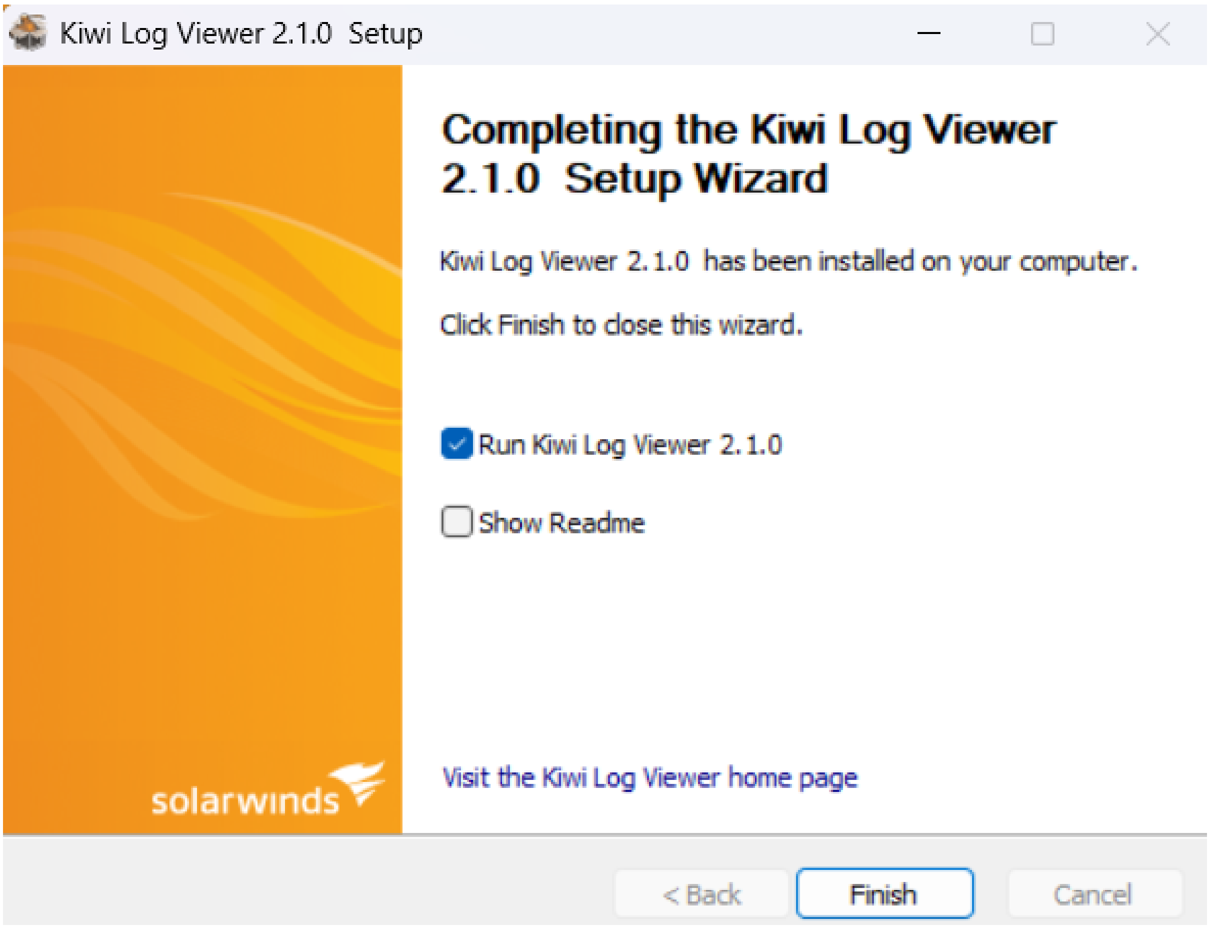
03/16/2025 19:00 - 03/17/2025 19:05

Folders and Logs Problems Summary

Name	Logs Status	Logs Events	Logs Problems	Predefined	Autodetected	% of Problems
Windows Event Logs	Medium	11,057	1,042	0	1,042	100%
Monitors	OK	2	0	0	0	
Example Applications	OK	0	0	0	0	
Example Logs	OK	0	0	0	0	
Transaction Example	OK	0	0	0	0	

LAB-03

Investigating Network Attacks Using Kiwi Log Viewer



Kiwi Log Viewer 2.1.0 Setup

Completing the Kiwi Log Viewer 2.1.0 Setup Wizard

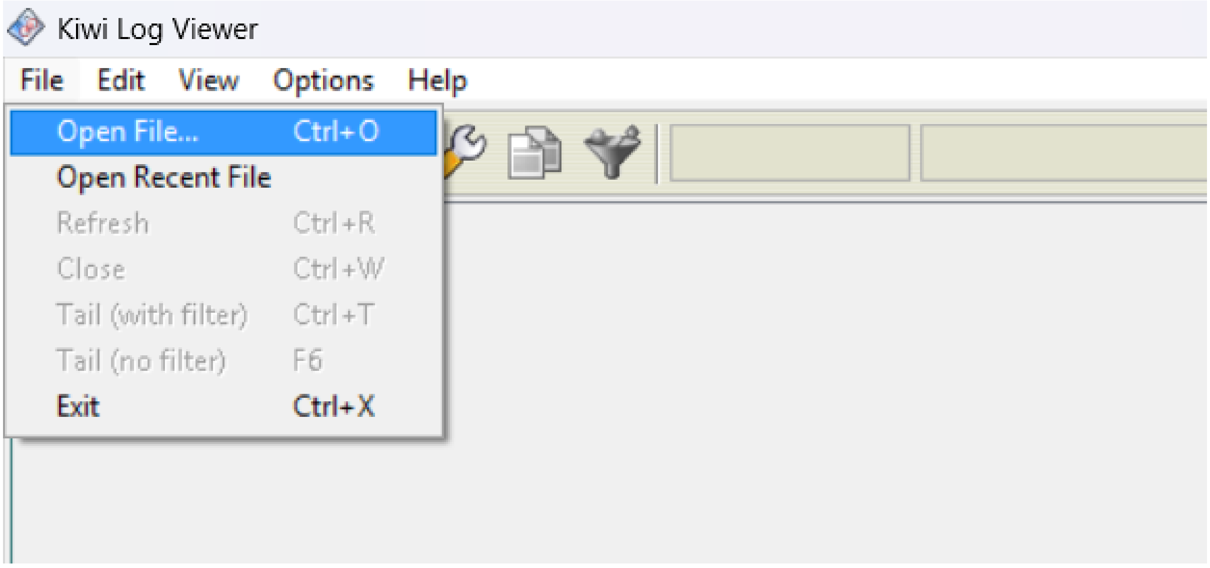
Kiwi Log Viewer 2.1.0 has been installed on your computer.

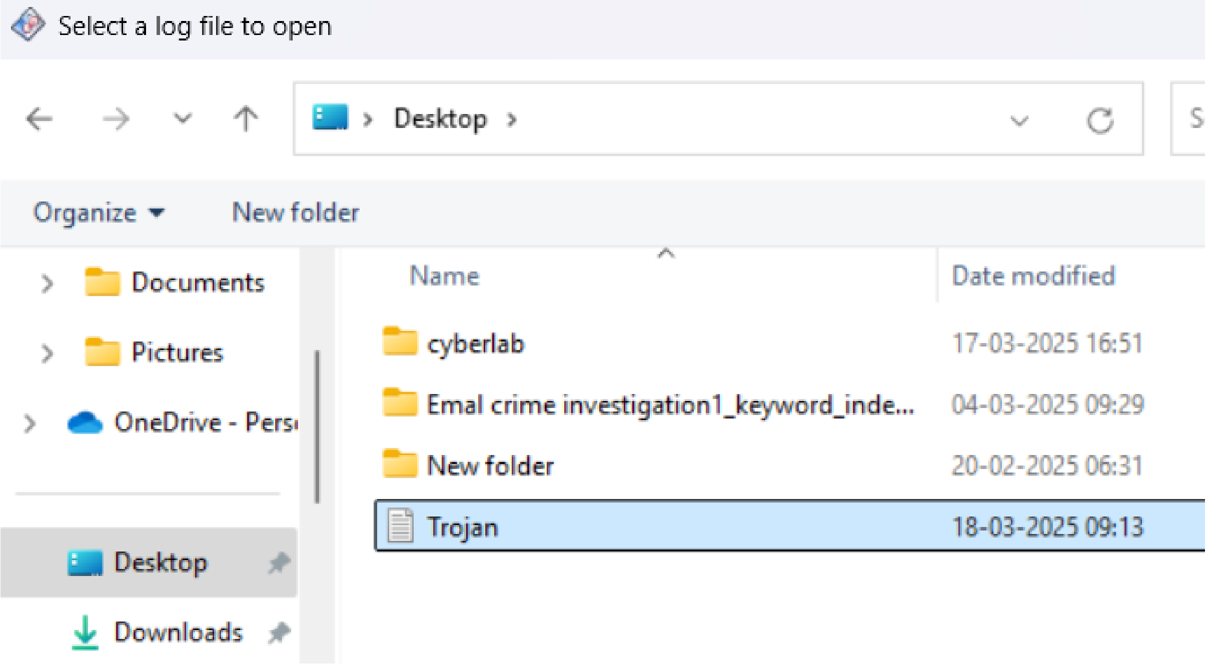
Click Finish to close this wizard.

☑ Run Kiwi Log Viewer 2.1.0

☐ Show Readme

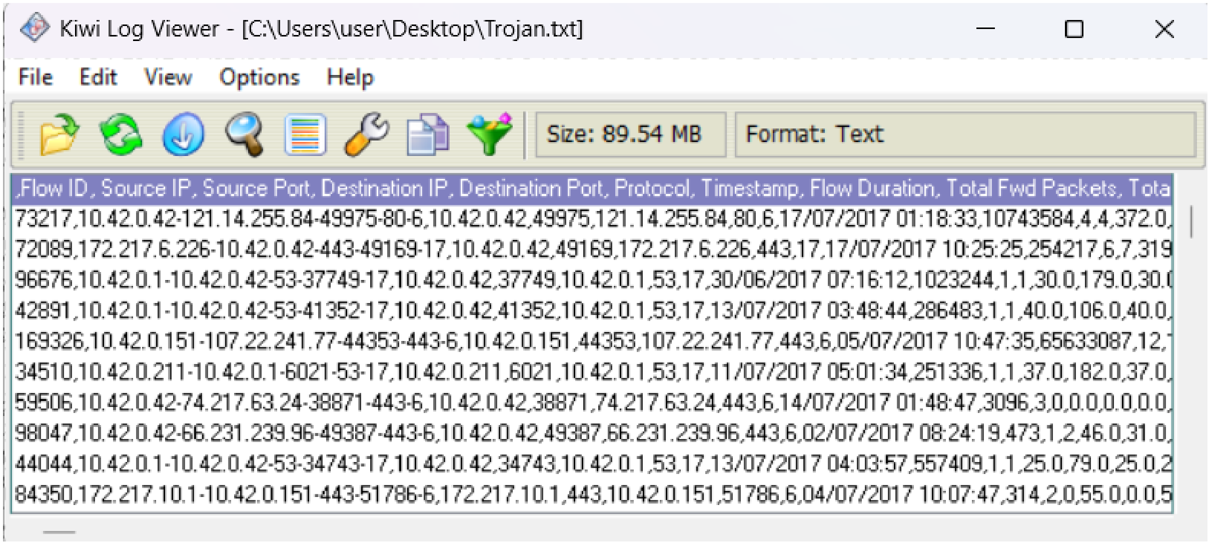
Visit the Kiwi Log Viewer home page





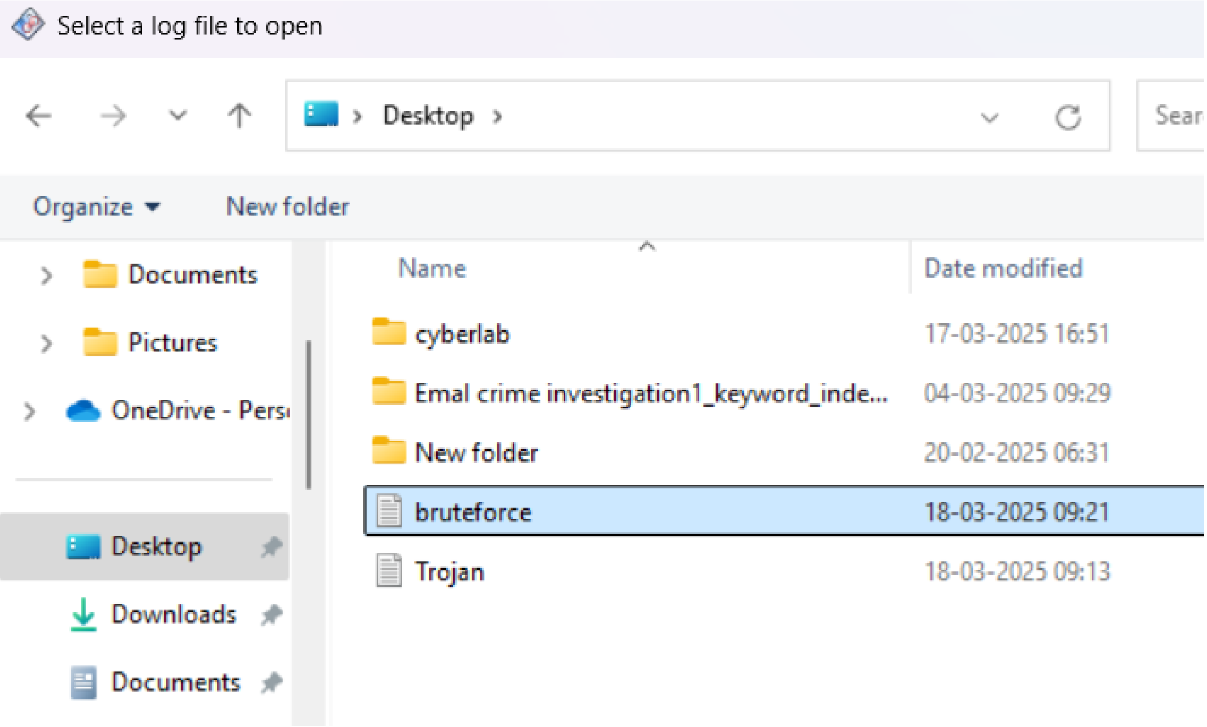
Name	Date modified
cyberlab	17-03-2025 16:51
Emal crime investigation1_keyword_inde...	04-03-2025 09:29
New folder	20-02-2025 06:31
Trojan	18-03-2025 09:13

Kiwi log viewer displays all the logs of the selected file . We can analyze these logs, to determine if there was any malicious activity in the network.



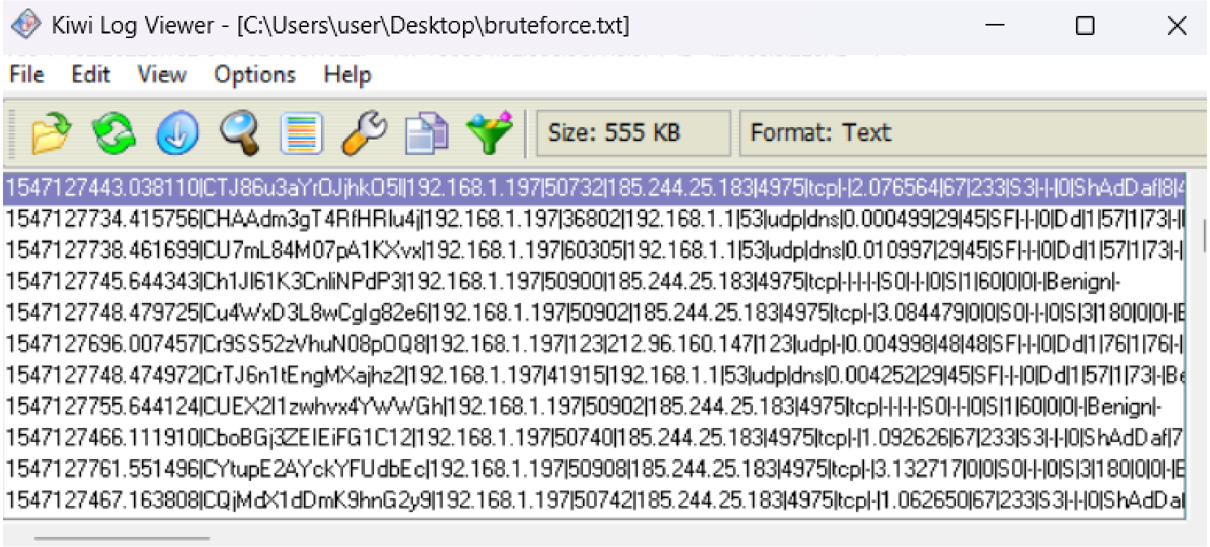
```
,Flow ID, Source IP, Source Port, Destination IP, Destination Port, Protocol, Timestamp, Flow Duration, Total Fwd Packets, Tota
73217,10.42.0.42-121.14.255.84-49975-80-6,10.42.0.42,49975,121.14.255.84,80,6,17/07/2017 01:18:33,10743584,4,4,372.0,
72089,172.217.6.226-10.42.0.42-443-49169-17,10.42.0.42,49169,172.217.6.226,443,17,17/07/2017 10:25:25,254217,6,7,319
96676,10.42.0.1-10.42.0.42-53-37749-17,10.42.0.42,37749,10.42.0.1,53,17,30/06/2017 07:16:12,1023244,1,1,30.0,179.0,30.0
42891,10.42.0.1-10.42.0.42-53-41352-17,10.42.0.42,41352,10.42.0.1,53,17,13/07/2017 03:48:44,286483,1,1,40.0,106.0,40.0,
169326,10.42.0.151-107.22.241.77-44353-443-6,10.42.0.151,44353,107.22.241.77,443,6,05/07/2017 10:47:35,65633087,12,
34510,10.42.0.211-10.42.0.1-6021-53-17,10.42.0.211,6021,10.42.0.1,53,17,11/07/2017 05:01:34,251336,1,1,37.0,182.0,37.0,
59506,10.42.0.42-74.217.63.24-38871-443-6,10.42.0.42,38871,74.217.63.24,443,6,14/07/2017 01:48:47,3096,3,0,0.0,0.0,0.0,
98047,10.42.0.42-66.231.239.96-49387-443-6,10.42.0.42,49387,66.231.239.96,443,6,02/07/2017 08:24:19,473,1,2,46.0,31.0,
44044,10.42.0.1-10.42.0.42-53-34743-17,10.42.0.42,34743,10.42.0.1,53,17,13/07/2017 04:03:57,557409,1,1,25.0,79.0,25.0,2
84350,172.217.10.1-10.42.0.151-443-51786-6,172.217.10.1,443,10.42.0.151,51786,6,04/07/2017 10:07:47,314,2,0,55.0,0.0,5
```

Now we will look another file that contains logs which were recorded during a brute force attack. Select File from the menu bar and click open file and select bruteforce



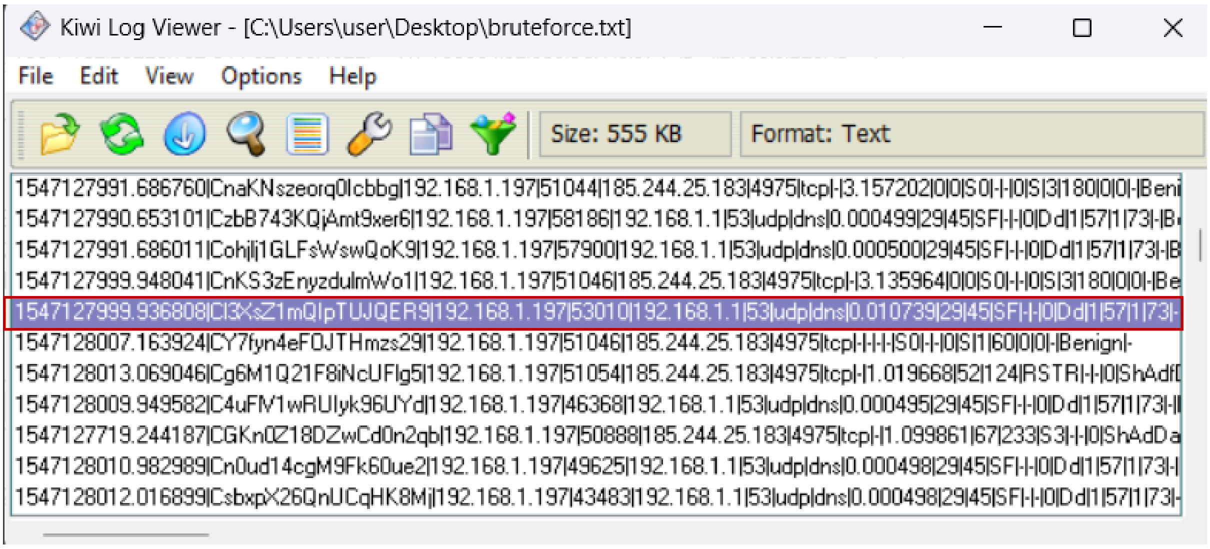
Name	Date modified
cyberlab	17-03-2025 16:51
Emal crime investigation1_keyword_inde...	04-03-2025 09:29
New folder	20-02-2025 06:31
bruteforce	18-03-2025 09:21
Trojan	18-03-2025 09:13

Kiwi log viewer application displays all the logs of the file as shown in below screenshot.



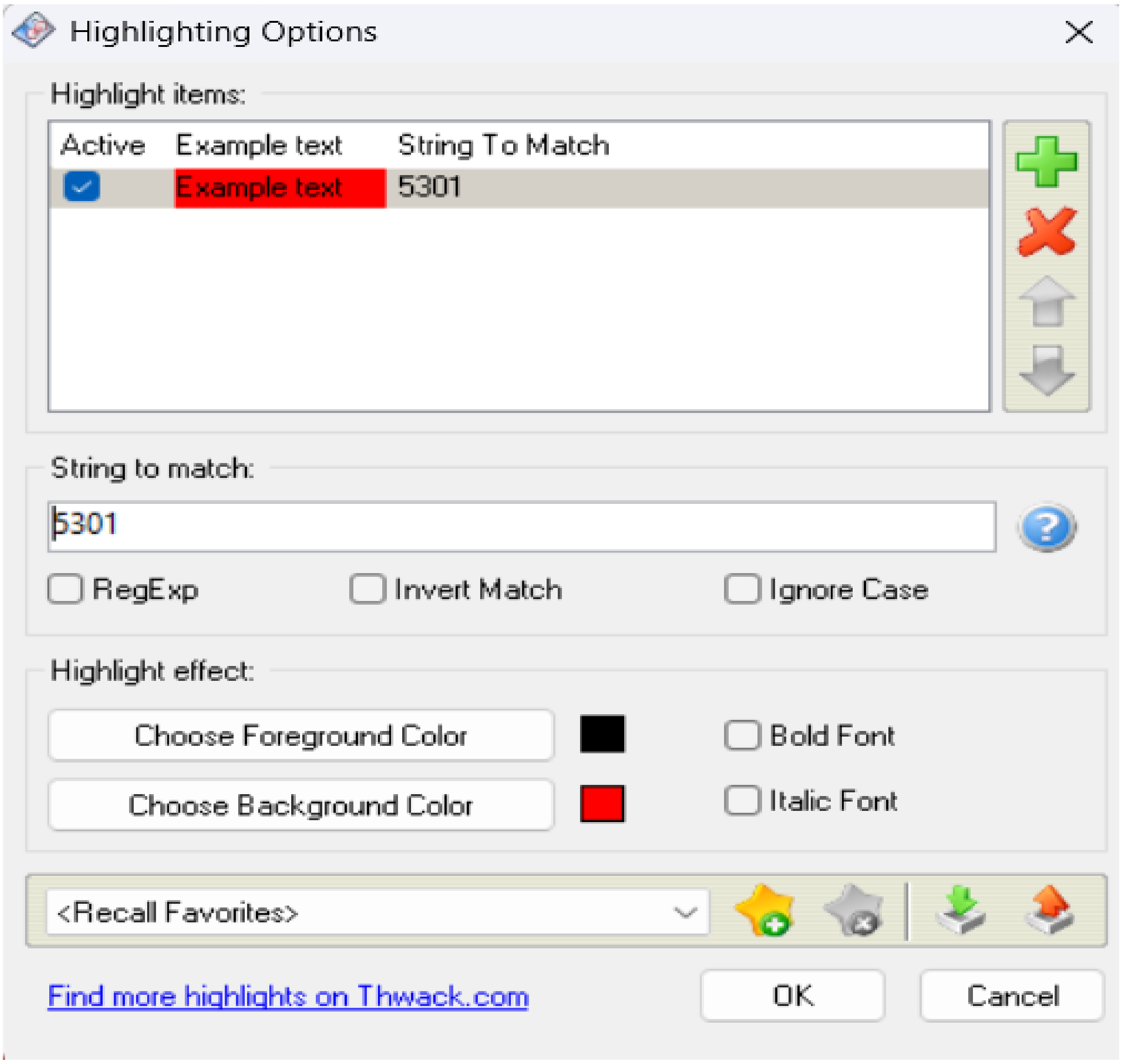
```
1547127443.038110|CTJ86u3aYrOJjhkO5l|192.168.1.197|50732|185.244.25.183|4975|tcp|-|2.076564|67|233|S3|-|-|0|ShAdDaf|8|4
1547127734.415756|CHAAdm3gT4RfHRlu4j|192.168.1.197|36802|192.168.1.1|53|udp|dns|0.000499|29|45|SF|-|-|0|Dd|1|57|1|73|-|
1547127738.461699|CU7mL84M07pA1KXvx|192.168.1.197|60305|192.168.1.1|53|udp|dns|0.010997|29|45|SF|-|-|0|Dd|1|57|1|73|-|
1547127745.644343|Ch1JI61K3CnliNPdP3|192.168.1.197|50900|185.244.25.183|4975|tcp|-|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547127748.479725|Cu4WxD3L8wCglg82e6|192.168.1.197|50902|185.244.25.183|4975|tcp|-|3.084479|0|0|S0|-|-|0|S|3|180|0|0|-|E
1547127696.007457|Cr9SS52zVhuN08pOQ8|192.168.1.197|123|212.96.160.147|123|udp|-|0.004998|48|48|SF|-|-|0|Dd|1|76|1|76|-|
1547127748.474972|CrTJ6n1tEngMXajhz2|192.168.1.197|41915|192.168.1.1|53|udp|dns|0.004252|29|45|SF|-|-|0|Dd|1|57|1|73|-|Be
1547127755.644124|CUEX2I1zwhvx4YWWGh|192.168.1.197|50902|185.244.25.183|4975|tcp|-|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547127466.111910|CboBGj3ZEIEiFG1C12|192.168.1.197|50740|185.244.25.183|4975|tcp|-|1.092626|67|233|S3|-|-|0|ShAdDaf|7
1547127761.551496|CYtupE2AYckYFUdbEc|192.168.1.197|50908|185.244.25.183|4975|tcp|-|3.132717|0|0|S0|-|-|0|S|3|180|0|0|-|E
1547127467.163808|CQjMdX1dDmK9hnG2y9|192.168.1.197|50742|185.244.25.183|4975|tcp|-|1.062650|67|233|S3|-|-|0|ShAdDa
```

The log shows repeated DNS queries over UDP on port 5301. This is unusual because standard DNS traffic occurs on port 53. The use of a non-standard port suggests a potential brute-force attack, DNS tunneling, or an attempt to evade detection. Further investigation is needed to determine whether this activity is malicious or part of a legitimate custom DNS setup.



```
1547127991.686760|CnaKNszeorq0lcbbg|192.168.1.197|51044|185.244.25.183|4975|tcp|-|3.157202|0|0|S0|-|-|0|S|3|180|0|0|-|Beni
1547127990.653101|CzbB743KQjAmt9xer6|192.168.1.197|58186|192.168.1.1|53|udp|dns|0.000499|29|45|SF|-|-|0|Dd|1|57|1|73|-|B
1547127991.686011|Cohjlj1GLFsWswQoK9|192.168.1.197|57900|192.168.1.1|53|udp|dns|0.000500|29|45|SF|-|-|0|Dd|1|57|1|73|-|B
1547127999.948041|CnKS3zEnyzdulmWo1|192.168.1.197|51046|185.244.25.183|4975|tcp|-|3.135964|0|0|S0|-|-|0|S|3|180|0|0|-|Be
1547127999.936808|Cl3XsZ1mQIpTUJQER9|192.168.1.197|53010|192.168.1.1|53|udp|dns|0.010739|29|45|SF|-|-|0|Dd|1|57|1|73|-
1547128007.163924|CY7fyn4eFOJTHmzs29|192.168.1.197|51046|185.244.25.183|4975|tcp|-|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547128013.069046|Cg6M1Q21F8iNcUFlg5|192.168.1.197|51054|185.244.25.183|4975|tcp|-|1.019668|52|124|RSTR|-|-|0|ShAdfD
1547128009.949582|C4uFM1wRUIyk96UYd|192.168.1.197|46368|192.168.1.1|53|udp|dns|0.000495|29|45|SF|-|-|0|Dd|1|57|1|73|-|
1547127719.244187|CGKn0Z18DZwCd0n2qb|192.168.1.197|50888|185.244.25.183|4975|tcp|-|1.099861|67|233|S3|-|-|0|ShAdDa
1547128010.982989|Cn0ud14cgM9Fk60ue2|192.168.1.197|49625|192.168.1.1|53|udp|dns|0.000498|29|45|SF|-|-|0|Dd|1|57|1|73|-|
1547128012.016899|CsbxpX26QnUCqHK8Mj|192.168.1.197|43483|192.168.1.1|53|udp|dns|0.000498|29|45|SF|-|-|0|Dd|1|57|1|73|-
```

To differentiate the responses , we will assign color highlights to the responses.To do so, o to options and select highlighting



Highlighting Options

Highlight items:

Active	Example text	String To Match
☑	Example text	5301

String to match: 5301

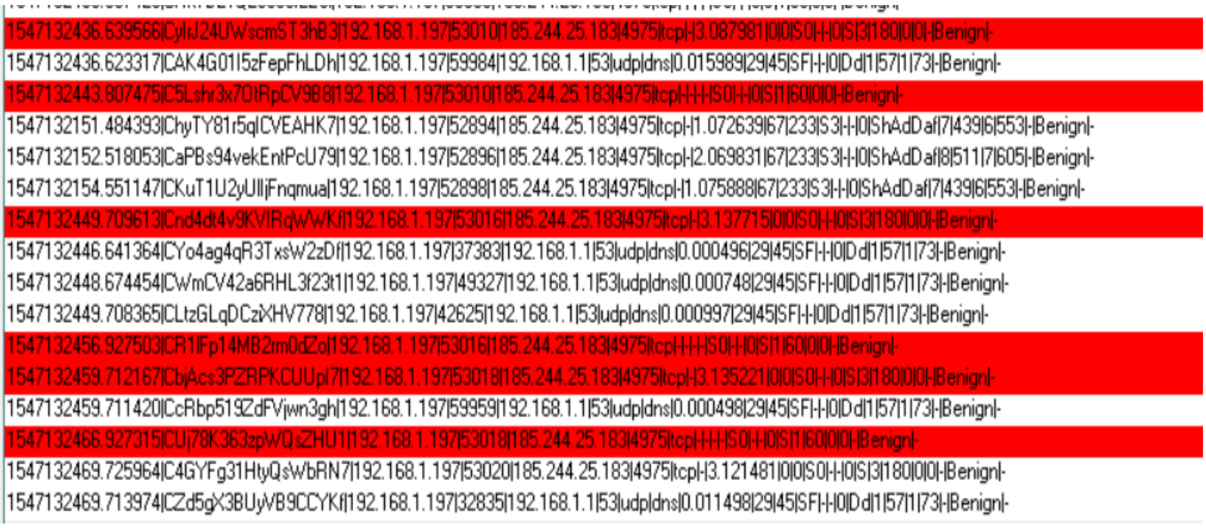
□ RegExp □ Invert Match □ Ignore Case

Highlight effect:

Choose Foreground Color ■ □ Bold Font

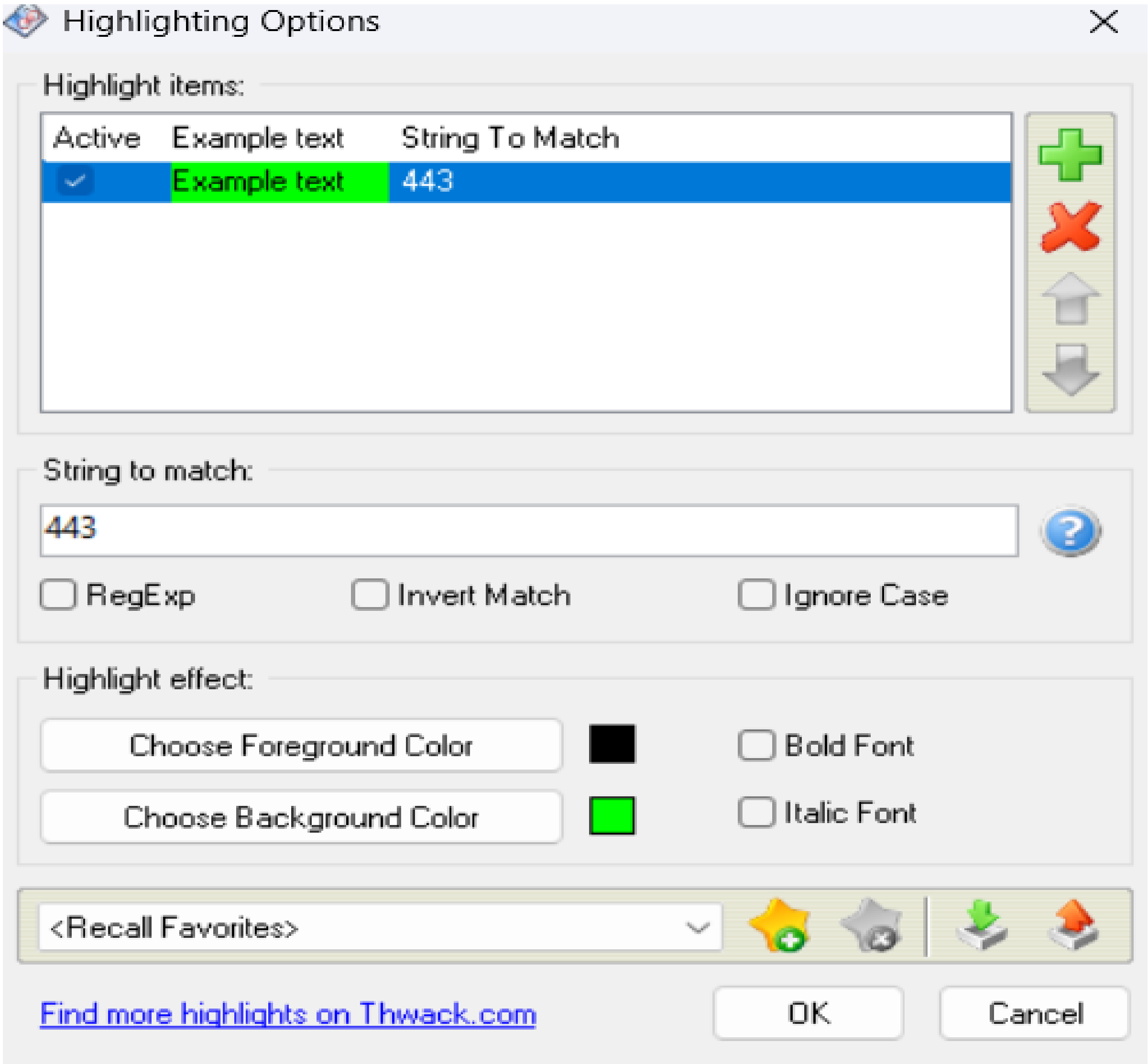
Choose Background Color 🟥 □ Italic Font

By doing this ,all the logs containing string response 5301will be highlighted in red colour



```
1547132436.639566|CylrJ24UWscmST3hB3|192.168.1.197|53010|185.244.25.183|4975|tcp|-|3.087981|0|0|S0|-|-|0|S|3|180|0|0|-|Benign|-
1547132436.623317|CAK4G01I5zFepFhLDh|192.168.1.197|59984|192.168.1.1|53|udp|dns|0.015989|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547132443.807475|C5Lshr3x7OtRpCV9B8|192.168.1.197|53010|185.244.25.183|4975|tcp|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547132151.484393|ChyTY81r5qlCVEAHK7|192.168.1.197|52894|185.244.25.183|4975|tcp|-|1.072639|67|233|S3|-|-|0|ShAdDaf|7|439|6|553|-|Benign|-
1547132152.518053|CaPBs94vekEntPcU79|192.168.1.197|52896|185.244.25.183|4975|tcp|-|2.069831|67|233|S3|-|-|0|ShAdDaf|8|511|7|605|-|Benign|-
1547132154.551147|CKuT1U2yUlljFnqmua|192.168.1.197|52898|185.244.25.183|4975|tcp|-|1.075888|67|233|S3|-|-|0|ShAdDaf|7|439|6|553|-|Benign|-
1547132449.709613|Cnd4dt4v9KVIRqWWKf|192.168.1.197|53016|185.244.25.183|4975|tcp|-|3.137715|0|0|S0|-|-|0|S|3|180|0|0|-|Benign|-
1547132446.641364|CYo4ag4qR3TxsW2zDf|192.168.1.197|37383|192.168.1.1|53|udp|dns|0.000496|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547132448.674454|CWmCV42a6RHL3f23t1|192.168.1.197|49327|192.168.1.1|53|udp|dns|0.000748|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547132449.708365|CLtzGLqDCzXHV778|192.168.1.197|42625|192.168.1.1|53|udp|dns|0.000997|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547132456.927503|CR1IFp14MB2rm0dZo|192.168.1.197|53016|185.244.25.183|4975|tcp|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547132459.712167|CbjAcs3PZRPKCUUpl7|192.168.1.197|53018|185.244.25.183|4975|tcp|-|3.135221|0|0|S0|-|-|0|S|3|180|0|0|-|Benign|-
1547132459.711420|CcRbp519ZdFVjwn3gh|192.168.1.197|59959|192.168.1.1|53|udp|dns|0.000498|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547132466.927315|CUj78K363zpWQsZHU1|192.168.1.197|53018|185.244.25.183|4975|tcp|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547132469.725964|C4GYFg31HtyQsWbRN7|192.168.1.197|53020|185.244.25.183|4975|tcp|-|3.121481|0|0|S0|-|-|0|S|3|180|0|0|-|Benign|-
1547132469.713974|CZd5gX3BUyVB9CCYKf|192.168.1.197|32835|192.168.1.1|53|udp|dns|0.011498|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
```

In this same way we can highlight successful login attempt by green colour.



Highlighting Options

Highlight items:

Active	Example text	String To Match
☑	Example text	443

String to match:

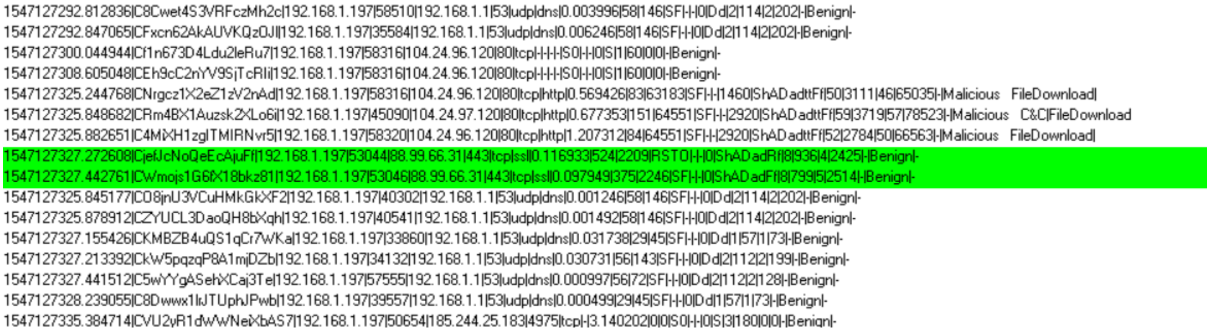
443

□ RegExp □ Invert Match □ Ignore Case

Highlight effect:

Choose Foreground Color ■ □ Bold Font

Choose Background Color 🟩 □ Italic Font



```
1547127292.812836|C8Cwet4S3VRFczMh2c|192.168.1.197|58510|192.168.1.1|53|udp|dns|0.003996|58|146|SF|-|-|0|Dd|2|114|2|202|-|Benign|-
1547127292.847065|CFxcn62AkAUVKQzOJl|192.168.1.197|35584|192.168.1.1|53|udp|dns|0.006246|58|146|SF|-|-|0|Dd|2|114|2|202|-|Benign|-
1547127300.044944|Cf1n673D4Ldu2leRu7|192.168.1.197|58316|104.24.96.120|80|tcp|-|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547127308.605048|CEh9cC2nYV9SjTcRIi|192.168.1.197|58316|104.24.96.120|80|tcp|-|-|-|-|S0|-|-|0|S|1|60|0|0|-|Benign|-
1547127325.244768|CNrgcz1X2eZ1zV2nAd|192.168.1.197|58316|104.24.96.120|80|tcp|http|0.569426|83|63183|SF|-|-|1460|ShADadttFf|50|3111|46|65035|-|Malicious   FileDownload|
1547127325.848682|CRm4BX1Auzsk2XLo6i|192.168.1.197|45090|104.24.97.120|80|tcp|http|0.677353|151|64551|SF|-|-|2920|ShADadttFf|59|3719|57|78523|-|Malicious   C&C|FileDownload
1547127325.882651|C4MiXH1zgITMIRNvr5|192.168.1.197|58320|104.24.96.120|80|tcp|http|1.207312|84|64551|SF|-|-|2920|ShADadttFf|52|2784|50|66563|-|Malicious   FileDownload|
1547127327.272608|CjefJcNoQeEcAjuFf|192.168.1.197|53044|88.99.66.31|443|tcp|ssl|0.116933|524|2209|RSTO|-|-|0|ShADadRf|8|936|4|2425|-|Benign|-
1547127327.442761|CWmojs1G6fX18bkz81|192.168.1.197|53046|88.99.66.31|443|tcp|ssl|0.097949|375|2246|SF|-|-|0|ShADadFf|8|799|5|2514|-|Benign|-
1547127325.845177|CO8jnU3VCuHMkGkXF2|192.168.1.197|40302|192.168.1.1|53|udp|dns|0.001246|58|146|SF|-|-|0|Dd|2|114|2|202|-|Benign|-
1547127325.878912|CZYUCL3DaoQH8bXqh|192.168.1.197|40541|192.168.1.1|53|udp|dns|0.001492|58|146|SF|-|-|0|Dd|2|114|2|202|-|Benign|-
1547127327.155426|CKMBZB4uQS1qCr7WKa|192.168.1.197|33860|192.168.1.1|53|udp|dns|0.031738|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547127327.213392|CkW5pqzqP8A1mjDZb|192.168.1.197|34132|192.168.1.1|53|udp|dns|0.030731|56|143|SF|-|-|0|Dd|2|112|2|199|-|Benign|-
1547127327.441512|C5wYYgASehXCaj3Te|192.168.1.197|57555|192.168.1.1|53|udp|dns|0.000997|56|72|SF|-|-|0|Dd|2|112|2|128|-|Benign|-
1547127328.239055|C8Dwwx1lrJTUphJPwb|192.168.1.197|39557|192.168.1.1|53|udp|dns|0.000499|29|45|SF|-|-|0|Dd|1|57|1|73|-|Benign|-
1547127335.384714|CVU2yR1dWWNeiXbAS7|192.168.1.197|50654|185.244.25.183|4975|tcp|-|3.140202|0|0|S0|-|-|0|S|3|180|0|0|-|Benign|-
```

It is seen that more number of logs with red highlights,, which infers that huge number of login attempts have occurred on server , resulting a bruteforce attack.

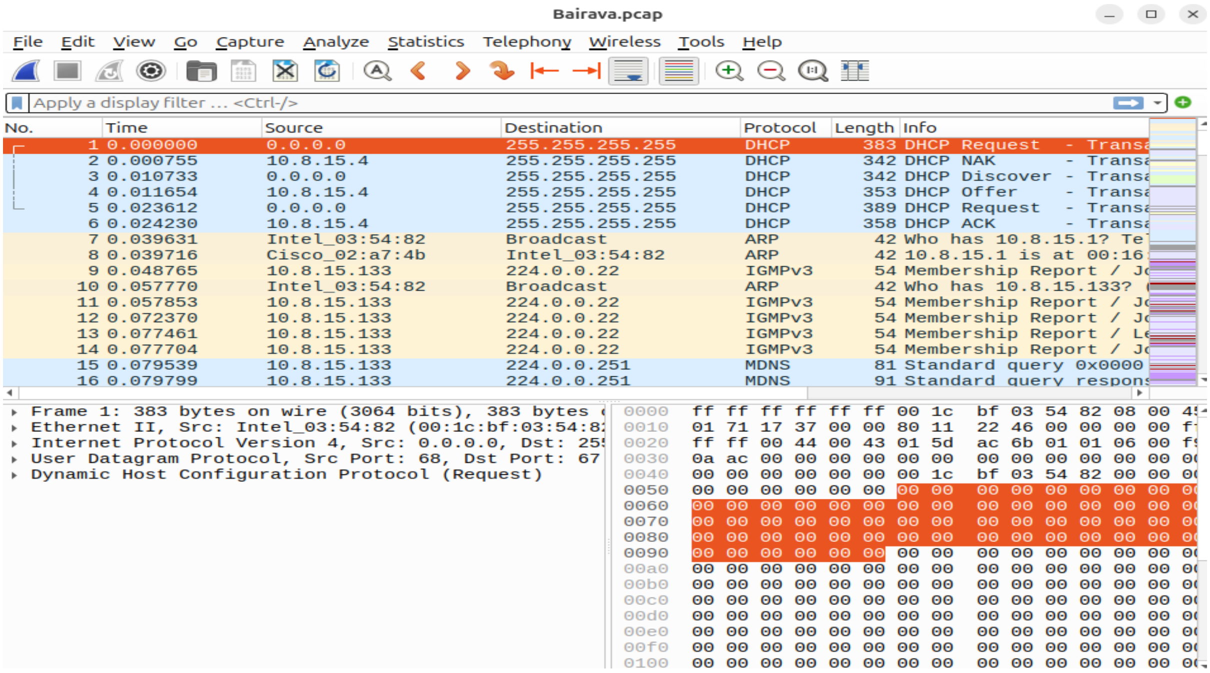
LAB-04

Investigating Network Traffic Using Wireshark

Lab objectives:

The objective of this lab is to demonstrate how to capture the live data packets of a network. The primary objective of this lab are :

- Capturing the packets of a network.
- Analyzing incoming and outgoing packets.

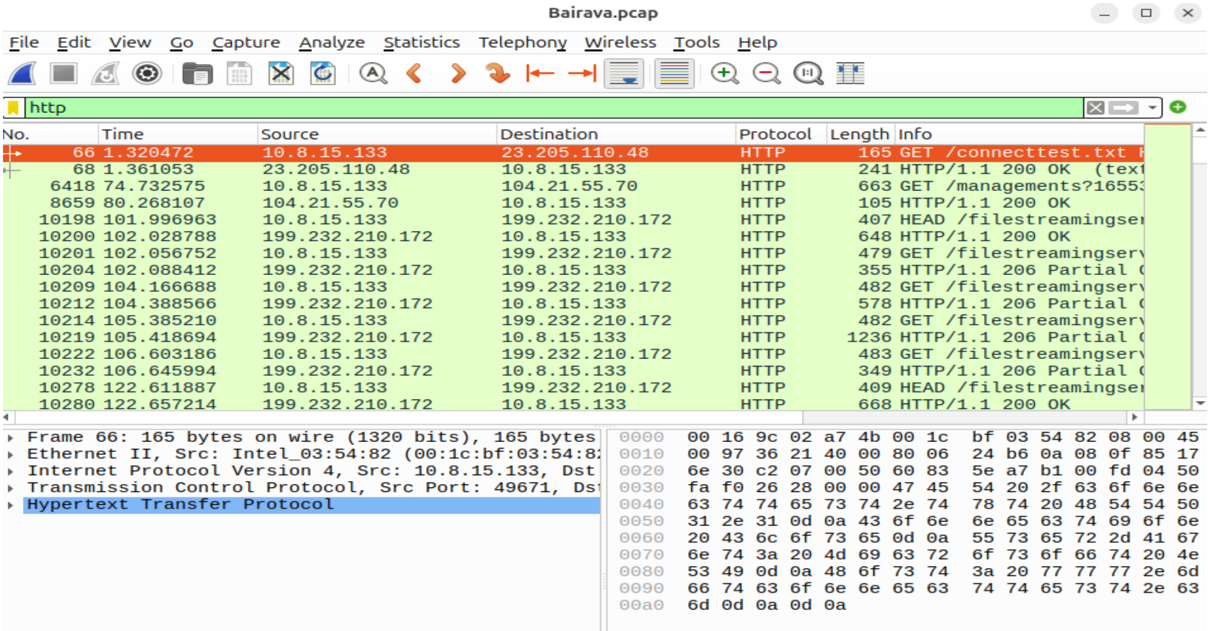


Bairava.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source            Destination       Protocol  Length Info
    1 0.000000   0.0.0.0           255.255.255.255   DHCP        383 DHCP Request  - Transa
    2 0.000755   10.8.15.4         255.255.255.255   DHCP        342 DHCP NAK      - Transa
    3 0.010733   0.0.0.0           255.255.255.255   DHCP        342 DHCP Discover - Transa
    4 0.011654   10.8.15.4         255.255.255.255   DHCP        353 DHCP Offer    - Transa
    5 0.023612   0.0.0.0           255.255.255.255   DHCP        389 DHCP Request  - Transa
    6 0.024230   10.8.15.4         255.255.255.255   DHCP        358 DHCP ACK      - Transa
    7 0.039631   Intel_03:54:82    Broadcast         ARP          42 Who has 10.8.15.1? Te
    8 0.039716   Cisco_02:a7:4b    Intel_03:54:82    ARP          42 10.8.15.1 is at 00:16
    9 0.048765   10.8.15.133       224.0.0.22        IGMPv3       54 Membership Report / Jo
   10 0.057770   Intel_03:54:82    Broadcast         ARP          42 Who has 10.8.15.133? (
   11 0.057853   10.8.15.133       224.0.0.22        IGMPv3       54 Membership Report / Jo
   12 0.072370   10.8.15.133       224.0.0.22        IGMPv3       54 Membership Report / Jo
   13 0.077461   10.8.15.133       224.0.0.22        IGMPv3       54 Membership Report / Le
   14 0.077704   10.8.15.133       224.0.0.22        IGMPv3       54 Membership Report / Jo
   15 0.079539   10.8.15.133       224.0.0.251       MDNS         81 Standard query 0x0000
   16 0.079799   10.8.15.133       224.0.0.251       MDNS         91 Standard query respons
```

```
▸ Frame 1: 383 bytes on wire (3064 bits), 383 bytes c
▸ Ethernet II, Src: Intel_03:54:82 (00:1c:bf:03:54:82
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 25
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▸ Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff 00 1c  bf 03 54 82 08 00 45
0010  01 71 17 37 00 00 80 11  22 46 00 00 00 00 ff
0020  ff ff 00 44 00 43 01 5d  ac 6b 01 01 06 00 f9
0030  0a ac 00 00 00 00 00 00  00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 1c  bf 03 54 82 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
```



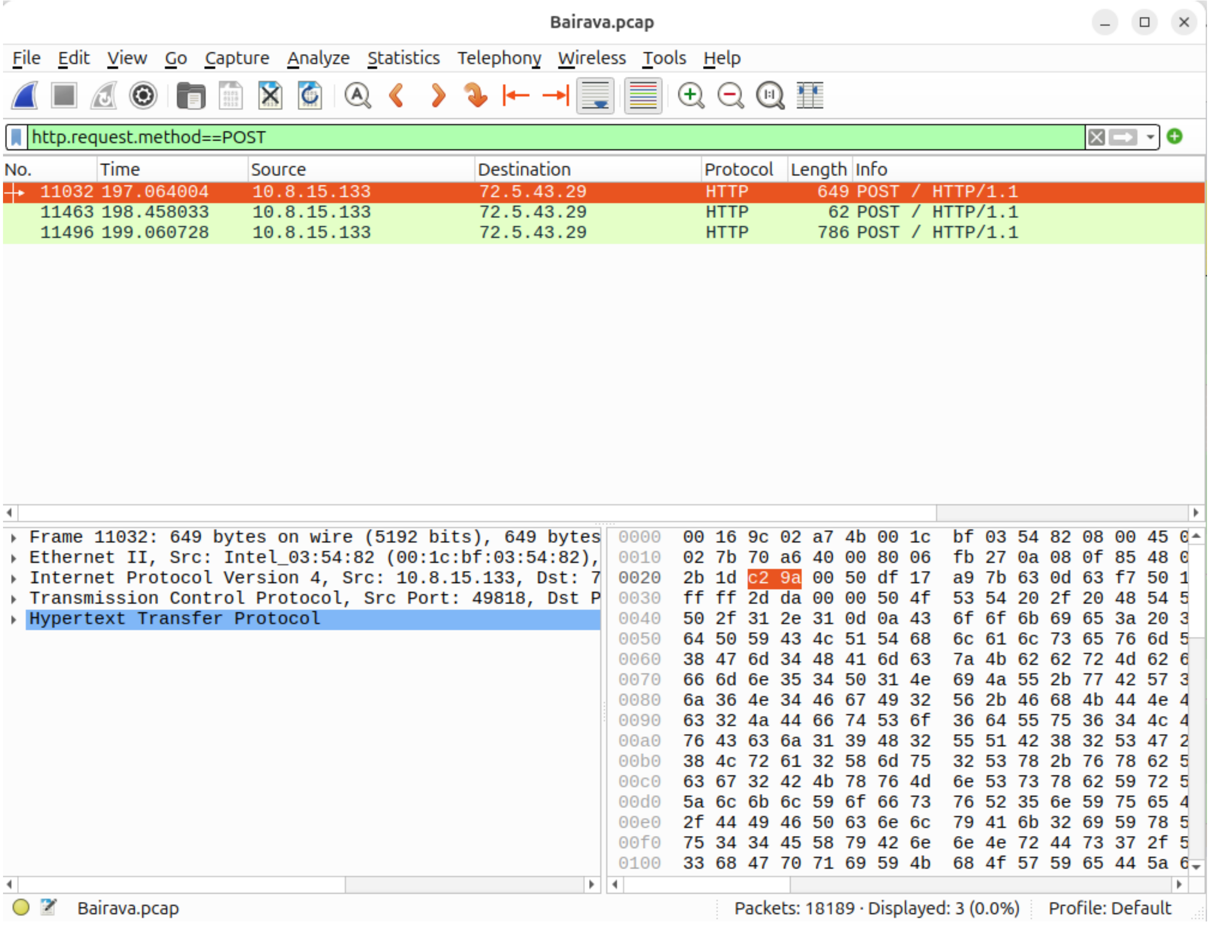
Bairava.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time         Source            Destination       Protocol  Length Info
    66 1.320472     10.8.15.133       23.205.110.48     HTTP        165 GET /connecttest.txt H
    68 1.361053     23.205.110.48     10.8.15.133       HTTP        241 HTTP/1.1 200 OK  (text
  6418 74.732575    10.8.15.133       104.21.55.70      HTTP        663 GET /managements?16553
  8659 80.268107    104.21.55.70      10.8.15.133       HTTP        105 HTTP/1.1 200 OK
 10198 101.996963   10.8.15.133       199.232.210.172   HTTP        407 HEAD /filestreamingser
 10200 102.028788   199.232.210.172   10.8.15.133       HTTP        648 HTTP/1.1 200 OK
 10201 102.056752   10.8.15.133       199.232.210.172   HTTP        479 GET /filestreamingserv
 10204 102.088412   199.232.210.172   10.8.15.133       HTTP        355 HTTP/1.1 206 Partial C
 10209 104.166688   10.8.15.133       199.232.210.172   HTTP        482 GET /filestreamingserv
 10212 104.388566   199.232.210.172   10.8.15.133       HTTP        578 HTTP/1.1 206 Partial C
 10214 105.385210   10.8.15.133       199.232.210.172   HTTP        482 GET /filestreamingserv
 10219 105.418694   199.232.210.172   10.8.15.133       HTTP       1236 HTTP/1.1 206 Partial C
 10222 106.603186   10.8.15.133       199.232.210.172   HTTP        483 GET /filestreamingserv
 10232 106.645994   199.232.210.172   10.8.15.133       HTTP        349 HTTP/1.1 206 Partial C
 10278 122.611887   10.8.15.133       199.232.210.172   HTTP        409 HEAD /filestreamingser
 10280 122.657214   199.232.210.172   10.8.15.133       HTTP        668 HTTP/1.1 200 OK
```

```
▸ Frame 66: 165 bytes on wire (1320 bits), 165 bytes
▸ Ethernet II, Src: Intel_03:54:82 (00:1c:bf:03:54:82
▸ Internet Protocol Version 4, Src: 10.8.15.133, Dst
▸ Transmission Control Protocol, Src Port: 49671, Dst
▸ Hypertext Transfer Protocol
```

```
0000  00 16 9c 02 a7 4b 00 1c  bf 03 54 82 08 00 45
0010  00 97 36 21 40 00 80 06  24 b6 0a 08 0f 85 17
0020  6e 30 c2 07 00 50 60 83  5e a7 b1 00 fd 04 50
0030  fa f0 26 28 00 00 47 45  54 20 2f 63 6f 6e 6e
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67
0070  6e 74 3a 20 4d 69 63 72  6f 73 6f 66 74 20 4e
0080  53 49 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 6d
0090  66 74 63 6f 6e 6e 65 63  74 74 65 73 74 2e 63
00a0  6d 0d 0a 0d 0a
```

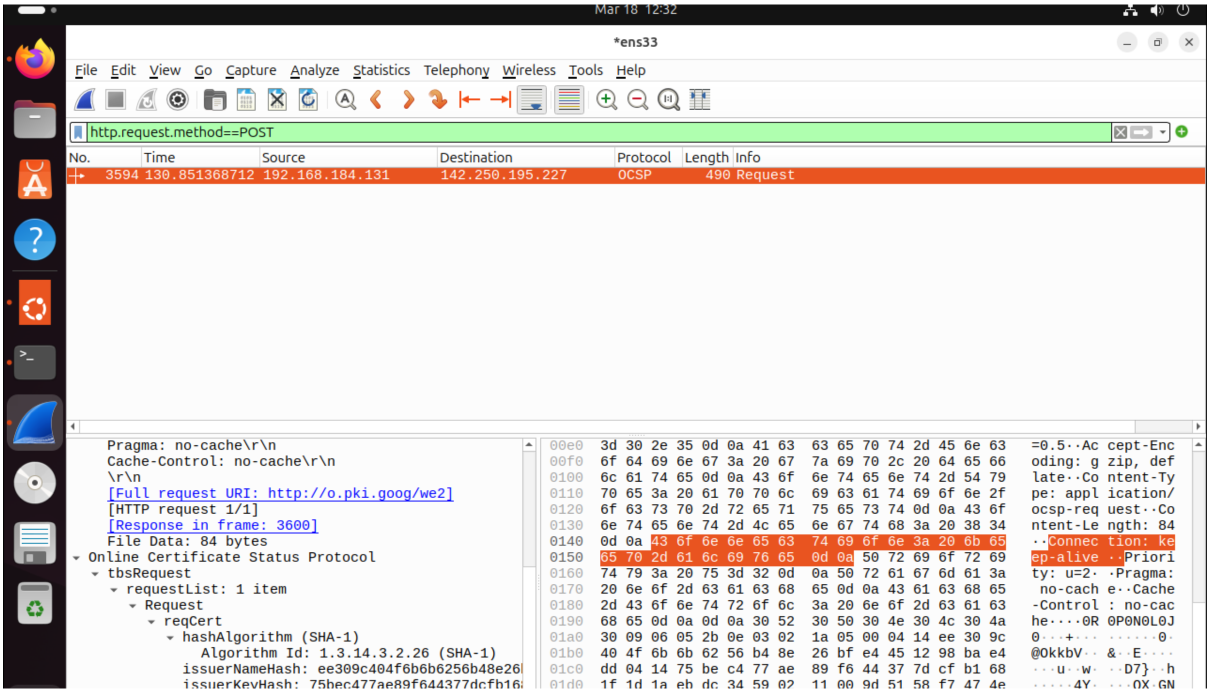

Bairava.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method==POST

No.    Time        Source        Destination   Protocol Length Info
11032 197.064004  10.8.15.133   72.5.43.29    HTTP       649 POST / HTTP/1.1
11463 198.458033  10.8.15.133   72.5.43.29    HTTP        62 POST / HTTP/1.1
11496 199.060728  10.8.15.133   72.5.43.29    HTTP       786 POST / HTTP/1.1
```

```
Frame 11032: 649 bytes on wire (5192 bits), 649 bytes
Ethernet II, Src: Intel_03:54:82 (00:1c:bf:03:54:82),
Internet Protocol Version 4, Src: 10.8.15.133, Dst: 7
Transmission Control Protocol, Src Port: 49818, Dst P
Hypertext Transfer Protocol
```

```
0000  00 16 9c 02 a7 4b 00 1c  bf 03 54 82 08 00 45 0
0010  02 7b 70 a6 40 00 80 06  fb 27 0a 08 0f 85 48 0
0020  2b 1d c2 9a 00 50 df 17  a9 7b 63 0d 63 f7 50 1
0030  ff ff 2d da 00 00 50 4f  53 54 20 2f 20 48 54 5
0040  50 2f 31 2e 31 0d 0a 43  6f 6f 6b 69 65 3a 20 3
0050  64 50 59 43 4c 51 54 68  6c 61 6c 73 65 76 6d 5
0060  38 47 6d 34 48 41 6d 63  7a 4b 62 62 72 4d 62 6
0070  66 6d 6e 35 34 50 31 4e  69 4a 55 2b 77 42 57 3
0080  6a 36 4e 34 46 67 49 32  56 2b 46 68 4b 44 4e 4
0090  63 32 4a 44 66 74 53 6f  36 64 55 75 36 34 4c 4
00a0  76 43 63 6a 31 39 48 32  55 51 42 38 32 53 47 2
00b0  38 4c 72 61 32 58 6d 75  32 53 78 2b 76 78 62 5
00c0  63 67 32 42 4b 78 76 4d  6e 53 73 78 62 59 72 5
00d0  5a 6c 6b 6c 59 6f 66 73  76 52 35 6e 59 75 65 4
00e0  2f 44 49 46 50 63 6e 6c  79 41 6b 32 69 59 78 5
00f0  75 34 34 45 58 79 42 6e  6e 4e 72 44 73 37 2f 5
0100  33 68 47 70 71 69 59 4b  68 4f 57 59 65 44 5a 6
```

Bairava.pcap   Packets: 18189 · Displayed: 3 (0.0%)   Profile: Default

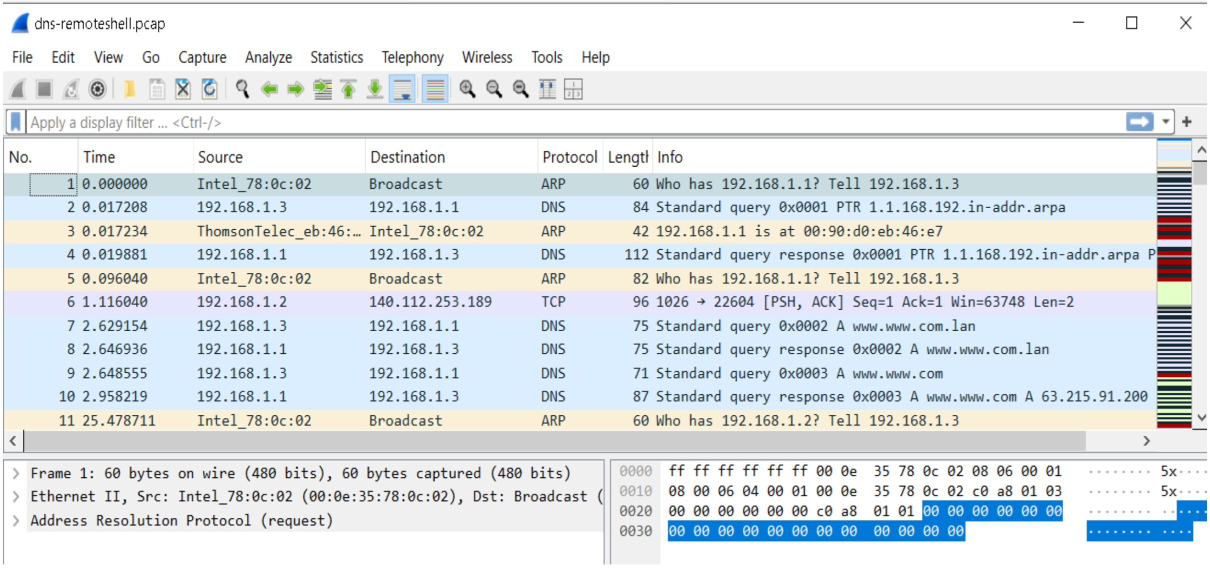

Mar 18 12:32
*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method==POST

No.  Time          Source           Destination      Protocol Length Info
3594 130.851368712 192.168.184.131  142.250.195.227  OCSP        490 Request
```

```
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://o.pki.goog/we2]
    [HTTP request 1/1]
    [Response in frame: 3600]
    File Data: 84 bytes
Online Certificate Status Protocol
  tbsRequest
    requestList: 1 item
      Request
        reqCert
          hashAlgorithm (SHA-1)
            Algorithm Id: 1.3.14.3.2.26 (SHA-1)
          issuerNameHash: ee309c404f6b6b6256b48e26
          issuerKeyHash: 75bec477ae89f644377dcfb16
```

```
00e0  3d 30 2e 35 0d 0a 41 63  63 65 70 74 2d 45 6e 63   =0.5··Ac cept-Enc
00f0  6f 64 69 6e 67 3a 20 67  7a 69 70 2c 20 64 65 66   oding: g zip, def
0100  6c 61 74 65 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   late··Co ntent-Ty
0110  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl ication/
0120  6f 63 73 70 2d 72 65 71  75 65 73 74 0d 0a 43 6f   ocsp-req uest··Co
0130  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 38 34   ntent-Le ngth: 84
0140  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
0150  65 70 2d 61 6c 69 76 65  0d 0a 50 72 69 6f 72 69   ep-alive ··Priori
0160  74 79 3a 20 75 3d 32 0d  0a 50 72 61 67 6d 61 3a   ty: u=2· ·Pragma:
0170  20 6e 6f 2d 63 61 63 68  65 0d 0a 43 61 63 68 65    no-cach e··Cache
0180  2d 43 6f 6e 74 72 6f 6c  3a 20 6e 6f 2d 63 61 63   -Control : no-cac
0190  68 65 0d 0a 0d 0a 30 52  30 50 30 4e 30 4c 30 4a   he····0R 0P0N0L0J
01a0  30 09 06 05 2b 0e 03 02  1a 05 00 04 14 ee 30 9c   0···+··· ······0·
01b0  40 4f 6b 6b 62 56 b4 8e  26 bf e4 45 12 98 ba e4   @OkkbV·· &··E····
01c0  dd 04 14 75 be c4 77 ae  89 f6 44 37 7d cf b1 68   ···u··w· ··D7}··h
01d0  1f 1d 1a eb dc 34 59 02  11 00 9d 51 58 f7 47 4e   ·····4Y· ···QX·GN
```

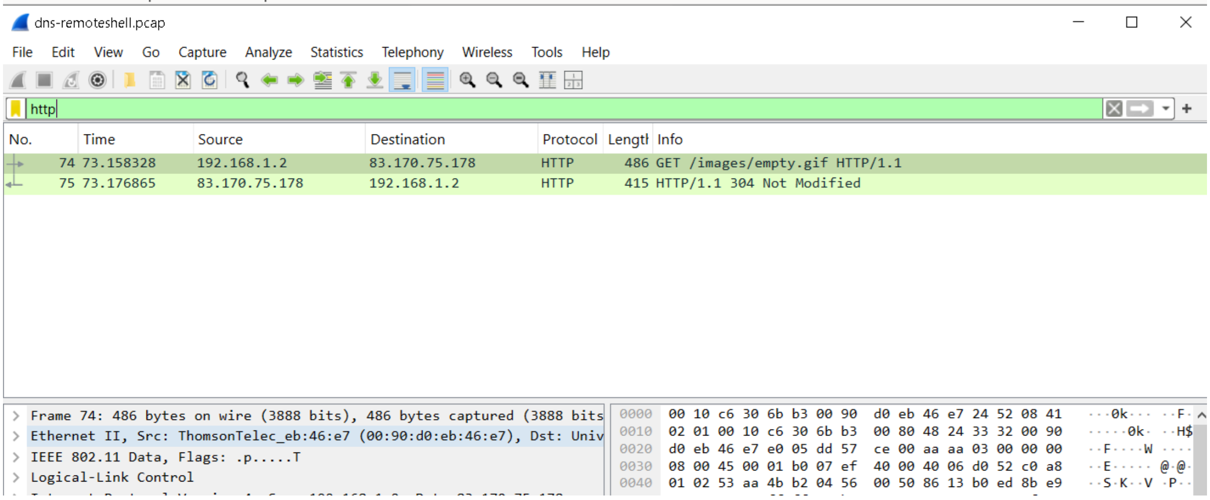
Opened dns remoteshell.pcap


dns-remoteshell.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source              Destination      Protocol Lengtl 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 P
   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
```

```
> 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 (
> 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               ········ ····
```


dns-remoteshell.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

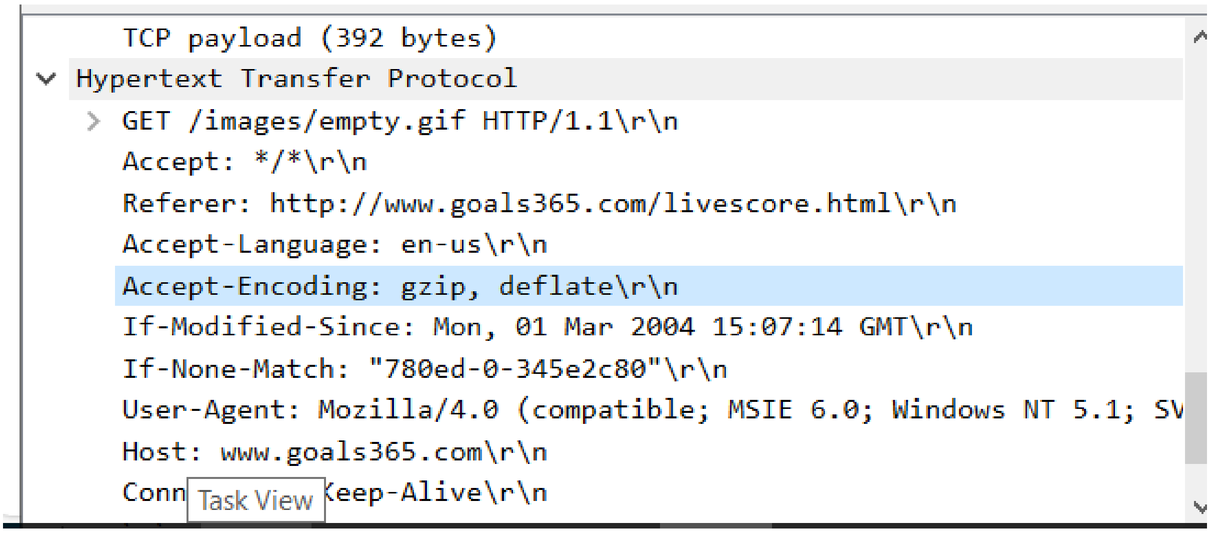
```
http
```

```
No.  Time        Source          Destination     Protocol Lengtl 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: Univ
> IEEE 802.11 Data, Flags: .p.....T
> Logical-Link Control
```

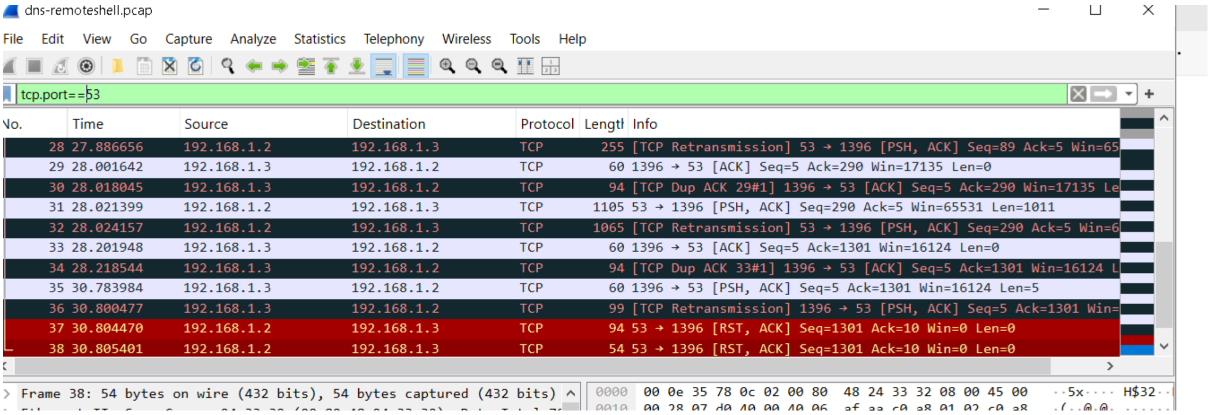
```
0000  00 10 c6 30 6b b3 00 90  d0 eb 46 e7 24 52 08 41   ···0k··· ··F·
0010  02 01 00 10 c6 30 6b b3  00 80 48 24 33 32 00 90   ·····0k· ··H$
0020  d0 eb 46 e7 e0 05 dd 57  ce 00 aa aa 03 00 00 00   ··F····W ····
0030  08 00 45 00 01 b0 07 ef  40 00 40 06 d0 52 c0 a8   ··E····· @·@·
0040  01 02 53 aa 4b b2 04 56  00 50 86 13 b0 ed 8b e9   ··S·K··V ·P··
```

Instead of html url encoding field here shown data transfer happened



```
    TCP payload (392 bytes)
v Hypertext Transfer Protocol
  > GET /images/empty.gif HTTP/1.1\r\n
    Accept: */*\r\n
    Referer: http://www.goals365.com/livescore.html\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    If-Modified-Since: Mon, 01 Mar 2004 15:07:14 GMT\r\n
    If-None-Match: "780ed-0-345e2c80"\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV
    Host: www.goals365.com\r\n
    Conn Task View Keep-Alive\r\n
```

Since DNS uses port 53 for communication, we shall be filtering the traffic flowing on port number 53.To filter type the command tcp.port==53 in the filter field and press enter.


dns-remoteshell.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

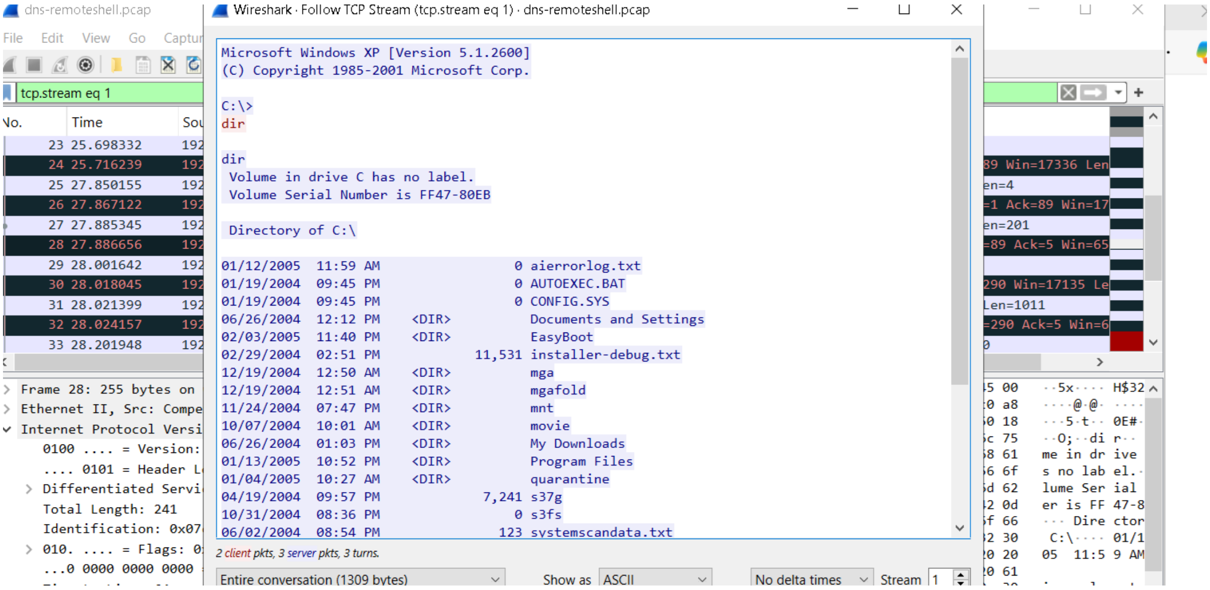
tcp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
28	27.886656	192.168.1.2	192.168.1.3	TCP	255	[TCP Retransmission] 53 → 1396 [PSH, ACK] Seq=89 Ack=5 Win=65
29	28.001642	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=5 Ack=290 Win=17135 Len=0
30	28.018045	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 29#1] 1396 → 53 [ACK] Seq=5 Ack=290 Win=17135 Le
31	28.021399	192.168.1.2	192.168.1.3	TCP	1105	53 → 1396 [PSH, ACK] Seq=290 Ack=5 Win=65531 Len=1011
32	28.024157	192.168.1.2	192.168.1.3	TCP	1065	[TCP Retransmission] 53 → 1396 [PSH, ACK] Seq=290 Ack=5 Win=6
33	28.201948	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=5 Ack=1301 Win=16124 Len=0
34	28.218544	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 33#1] 1396 → 53 [ACK] Seq=5 Ack=1301 Win=16124 L
35	30.783984	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [PSH, ACK] Seq=5 Ack=1301 Win=16124 Len=5
36	30.800477	192.168.1.3	192.168.1.2	TCP	99	[TCP Retransmission] 1396 → 53 [PSH, ACK] Seq=5 Ack=1301 Win=
37	30.804470	192.168.1.2	192.168.1.3	TCP	94	53 → 1396 [RST, ACK] Seq=1301 Ack=10 Win=0 Len=0
38	30.805401	192.168.1.2	192.168.1.3	TCP	54	53 → 1396 [RST, ACK] Seq=1301 Ack=10 Win=0 Len=0

```
> Frame 38: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
0000  00 0e 35 78 0c 02 00 80  48 24 33 32 08 00 45 00   ··5x···· H$32··E·
```

To view the data in a sequence , we will use Follow TCP stream option in wireshark.

Here we can observe that a remoteshell has been established on port 53, and the directory listing has been performed on the remote machine.


Wireshark · Follow TCP Stream (tcp.stream eq 1) · dns-remoteshell.pcap

```
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
```

2 client pkts, 3 server pkts, 3 turns.

Entire conversation (1309 bytes) Show as ASCII No delta times Stream 1