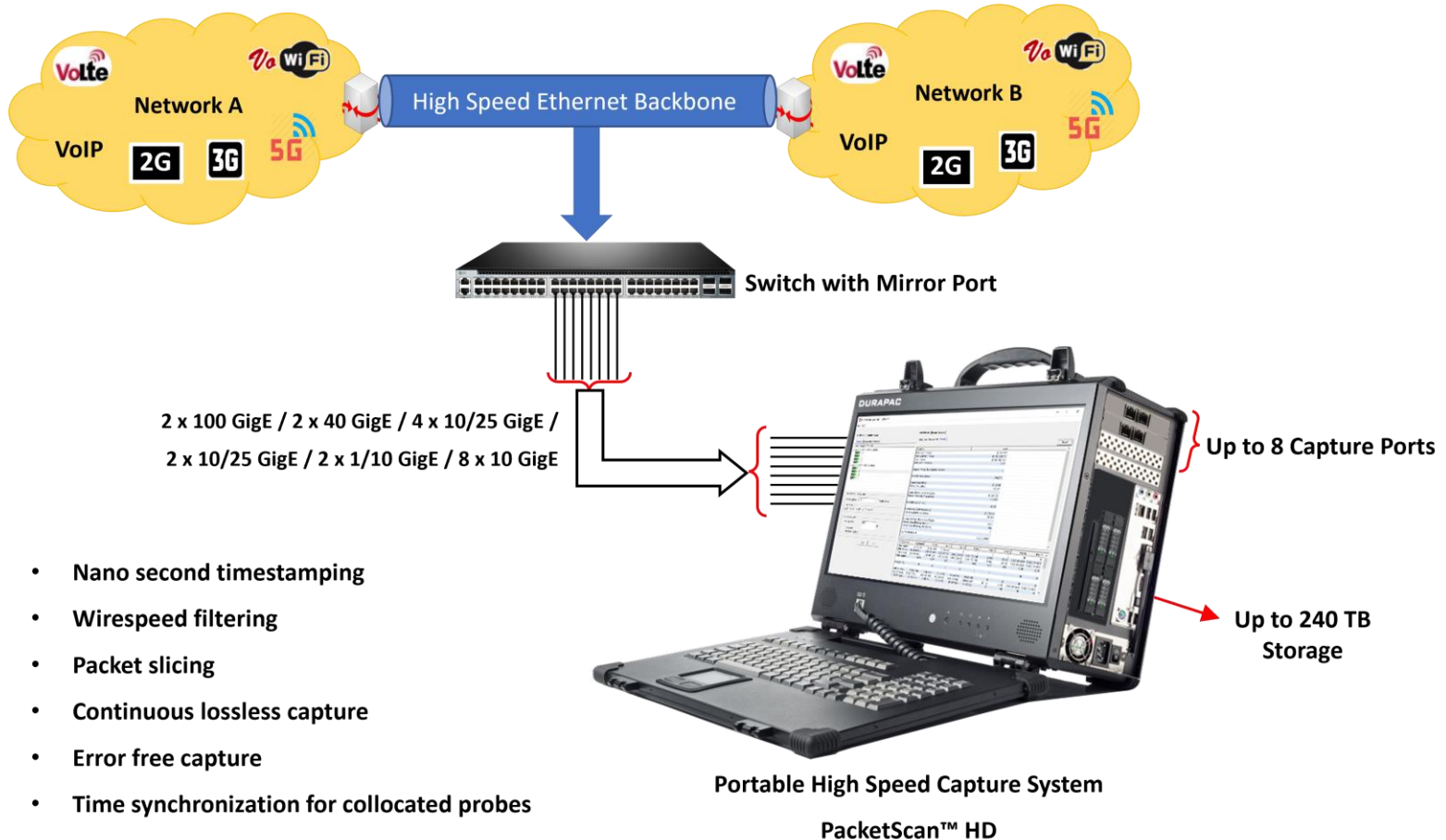

FastRecorder™ and PacketExtractor™ for Monitoring IP Networks



818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878
Phone: (301) 670-4784 Fax: (301) 670-9187 Email: info@gl.com
Website: <https://www.gl.com>

Overview



PacketScan™ HD, FastRecorder™ & PacketExtractor™

(2x1/10 GigE, 8x10 GigE, 2x10/25 GigE, 4x10/25 GigE, 2x40 GigE, 2x100 GigE)



**Also available as a rack mounted unit

PacketScan™ HD, FastRecorder™ & PacketExtractor™ 2 (4 x 1/10 GigE)



PacketScan™ HD - Lunch Box



Lunchbox specs are:

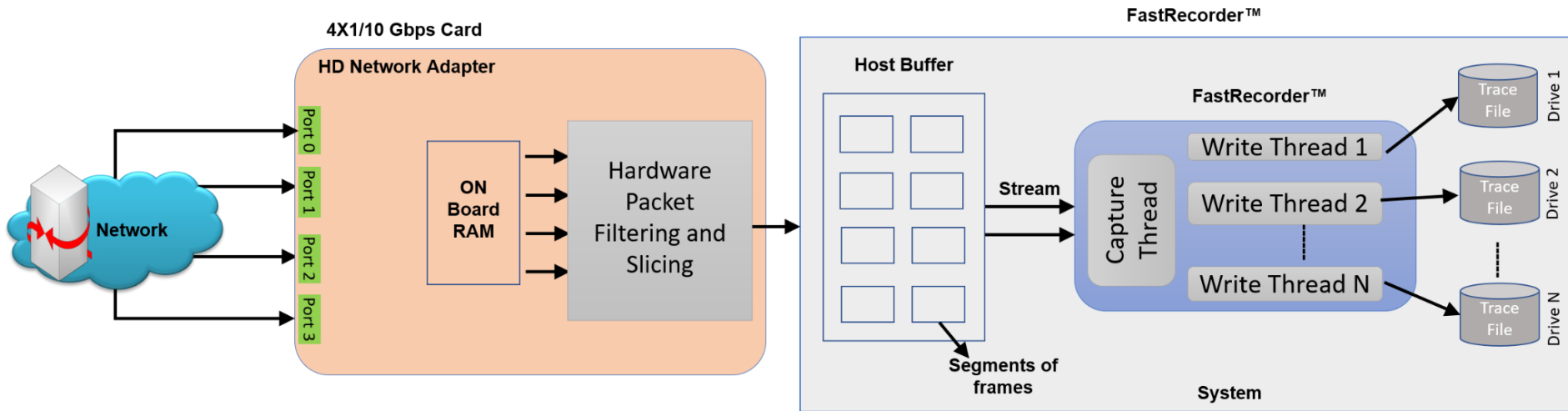
- Intel Xeon Silver 4210
- 64GB RAM
- 500GB SSD for OS
- 4x 3.84TB NVME SSD



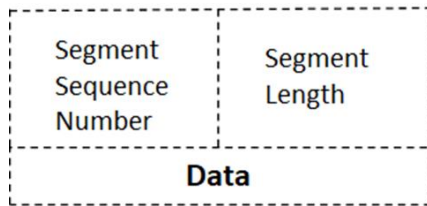
What the Software Does?

- The Record feature includes a powerful Hardware Filter that allows user to filter out unwanted traffic, and continuously capture the traffic of interest
- The previously recorded traffic is extracted into single or multiple files and can be analyzed using GL's PacketScan™ and Wireshark® application
- Can create own filters using custom filter option which provides flexibility to check the fields and use the logical AND, OR conditions more efficiently
- Trigger based Start or Stop writing to disk based on the condition is configured based on Capture Rate, Filter Rate, per-port Capture Rate, and Filter Rate
- E-mail alert for specified trigger condition
- Supports Encapsulating Security Payload (ESP) protocol to decrypt ESP packets on both IPv4 and IPv6 by providing ESP SAs value
- Supports Data and Rate analysis
- BERT verification analyzes the received BERT pattern and provides various vital measurements

FastRecorder™ Architecture

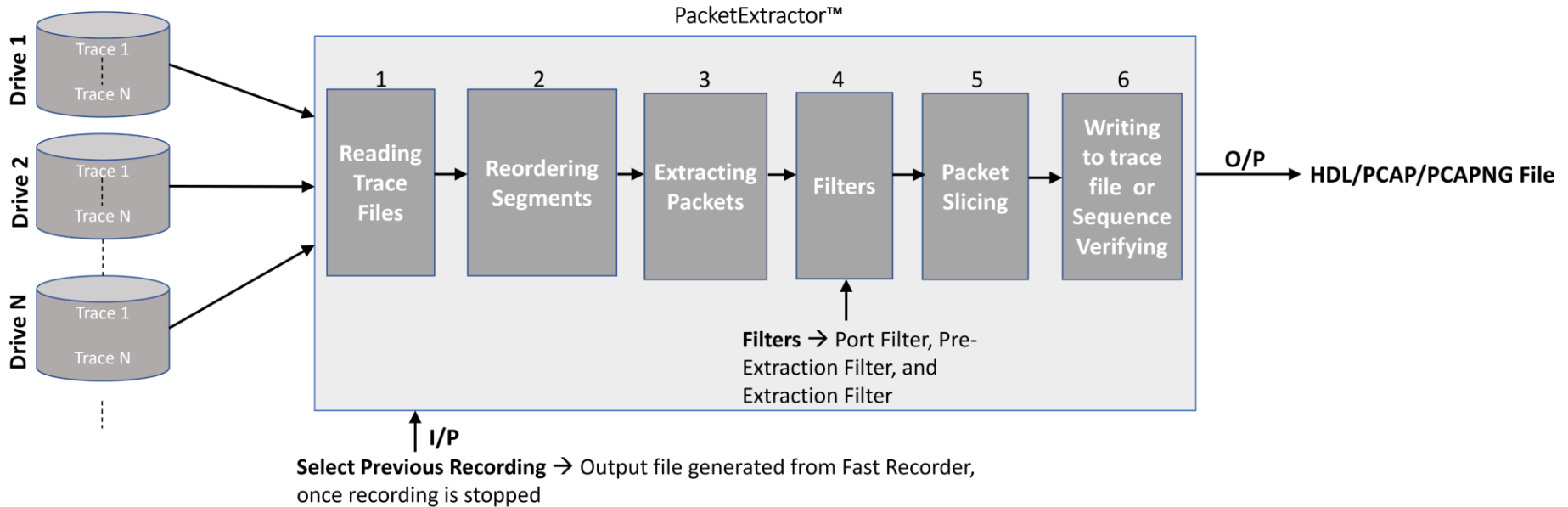


Buffer segments stored internally in files:



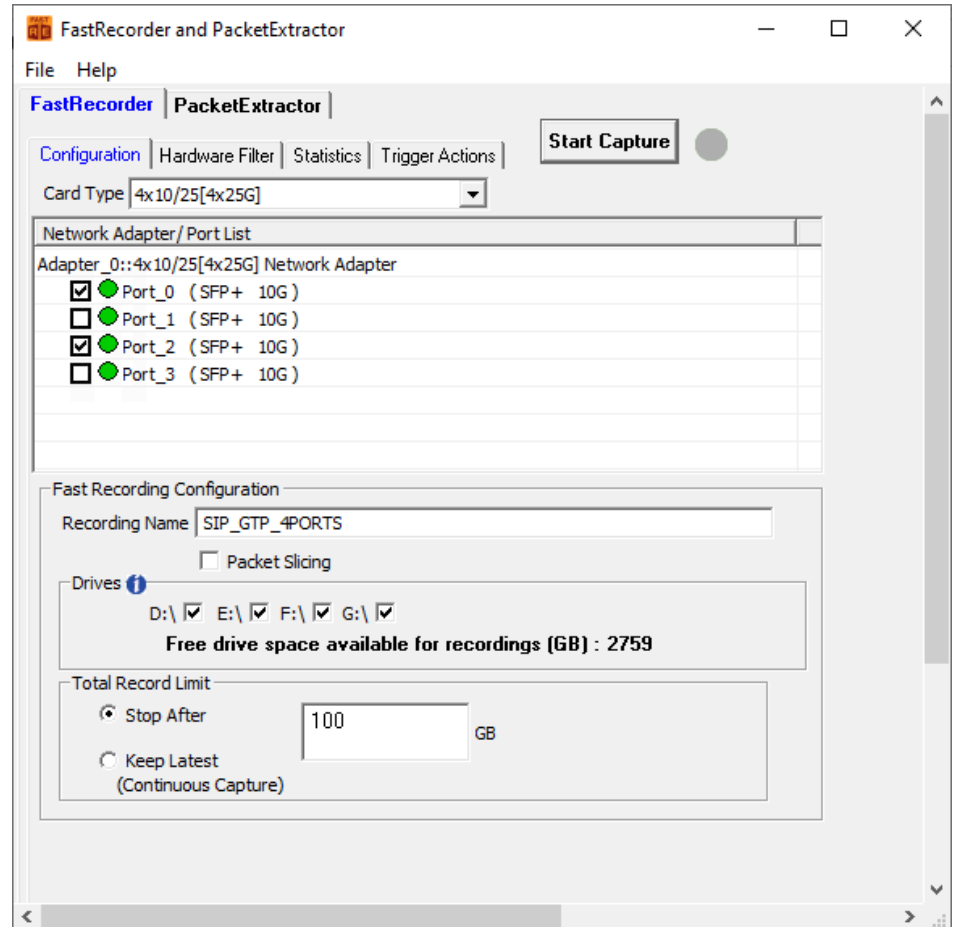
Segment Sequence Number and Segment Length is used while analysing/ Re-assembling the segments in Packet Extractor.

PacketExtractor™ Architecture



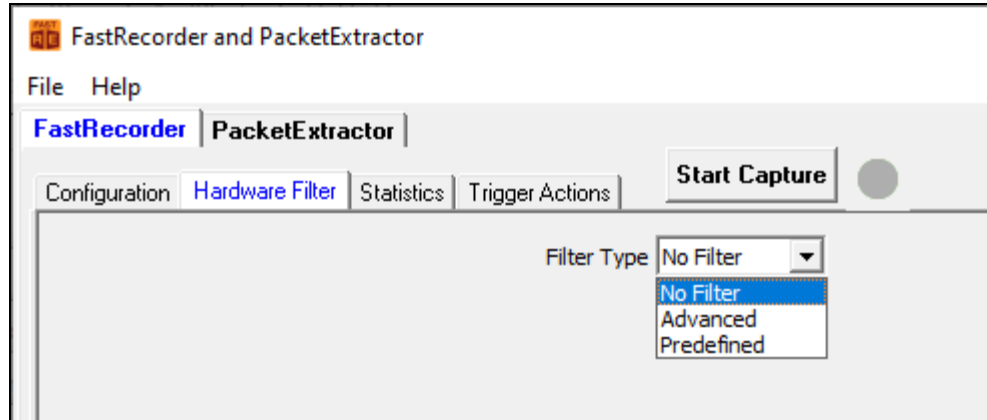
FastRecorder™ Operations

- FastRecorder™ application provides various options to capture the high-density real-time traffic on disk drives and store the recorded traffic into a file
- The application can capture the traffic continuously until user stops the recorder or specify the size limit to stop the traffic capture



Hardware Filters

- Hardware filters options are useful to capture traffic based on user interest
- User can select Filter Type as per the test requirements



Advanced Hardware Filter Type

- Up to 10 filters can be defined based on various parameters in the protocol layers
- User can configure the parameters as per test requirements

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The 'Hardware Filter' tab is active, and the 'Filter Type' is set to 'Advanced'. A table lists the filter configuration:

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	IPLIST	Ip List	==		

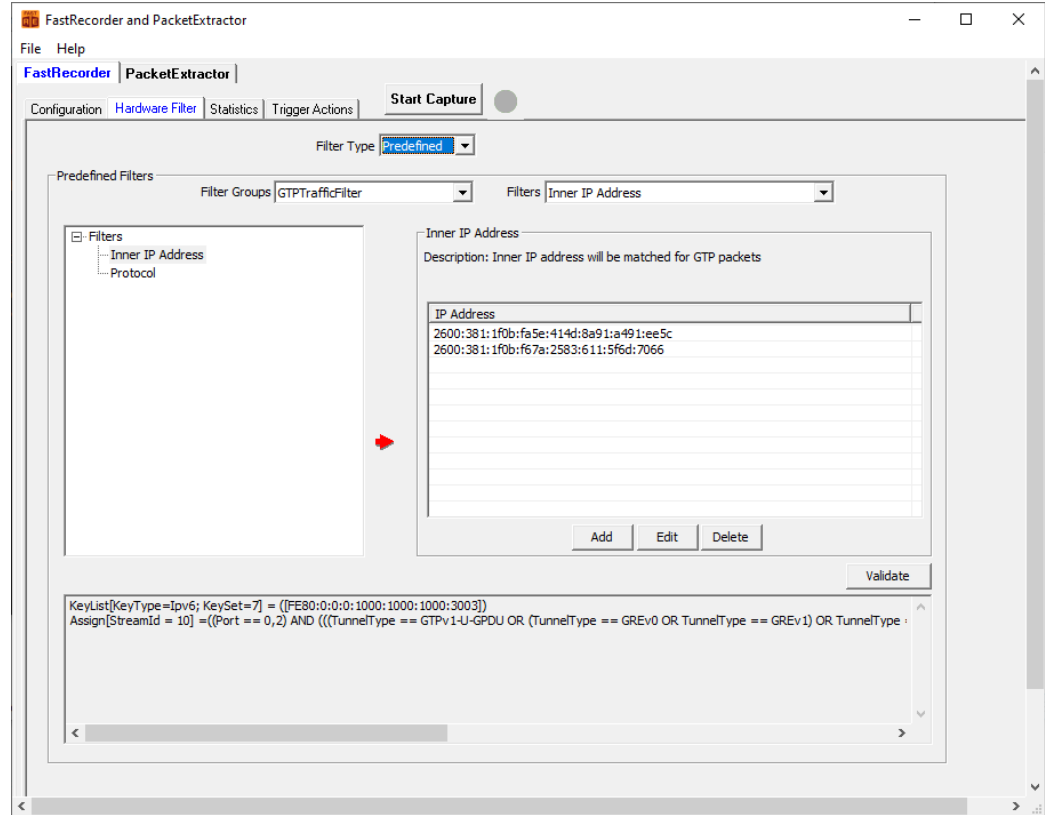
Below the table, the 'IP List Type' is set to 'IP Address List' and the 'IP Layer Type' is set to 'Tunnel-1 IP'. The 'IP Address' field contains the value 'FE80:0:0:1000:1000:3003'. Buttons for 'Add', 'Edit', and 'Delete' are visible. The 'Tunnel Type' is set to 'GTP, GRE, VXLAN'. A 'Custom Expression' field is empty, and a 'Validate & Update' button is present. The 'Selected Filter Expression' field shows the following logic:

```
KeyList[keyType=Ipv6; KeySet=7] = ((FE80:0:0:1000:1000:3003])  
Assign[StreamId = 10] = (((TunnelType == GTPv1-U-GPDU OR (TunnelType == GREv0 OR TunnelType == GREv1) OR TunnelType == VXLAN) AND ((InnerLayer3Protoc
```

The 'Final Configured Expressions' and 'Final Applied Expressions' fields show the same logic. A 'Clear All Filters' button is located at the bottom left.

Predefined Hardware Filter Type

- User can also use **Predefined** hardware filters. These are custom defined filters
- Application provides a framework to create custom filters as per requirements and group them
- By default, it provides configurations for IP addresses and protocol combinations. Wherein user can configure IP address and protocol for the traffic of interest



Custom Expression Filter

- User can create combination of hardware filters using **&&** and **||** operators to get the final expression

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The 'Hardware Filter' tab is active, and the 'Filter Type' is set to 'Advanced'. A table lists five filters (F1-F5) with their respective protocols and values. Below the table, a 'Custom Expression' is defined as '(f2 && f4) || f1'. A 'Validate & Update' button is highlighted, with a message indicating 'Expression changed validate & update'.

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	IPLIST	Ip List	==		
F2	VLAN0	Tag Protocol ID	==	8100	
F3	UDP	Source Port	==	5060	
F4	TCP	Source Port	==	443	
F5	SCTP	Source Port	==	36412	

Operators: ==, !=

Value (Decimal Value): 443

Examples:
Ex1: 6000
Ex2: 5060,2000,4235
Ex3: 1024-2000

Predefined Values:
FTP_Data
FTP_Control
Telnet
SMTP
DNS
HTTP

Buttons: Add, Insert, Delete, Clear All, Update, Validate & Update

Custom Expression: (f2 && f4) || f1

Message: Expression changed validate & update

FastRecorder™ Statistics

FastRecorder and PacketExtractor

File Help

FastRecorder | PacketExtractor

Configuration | Hardware Filter | **Statistics** | Trigger Actions

Stop Capture ● Capturing And Recording to Disk

View List View

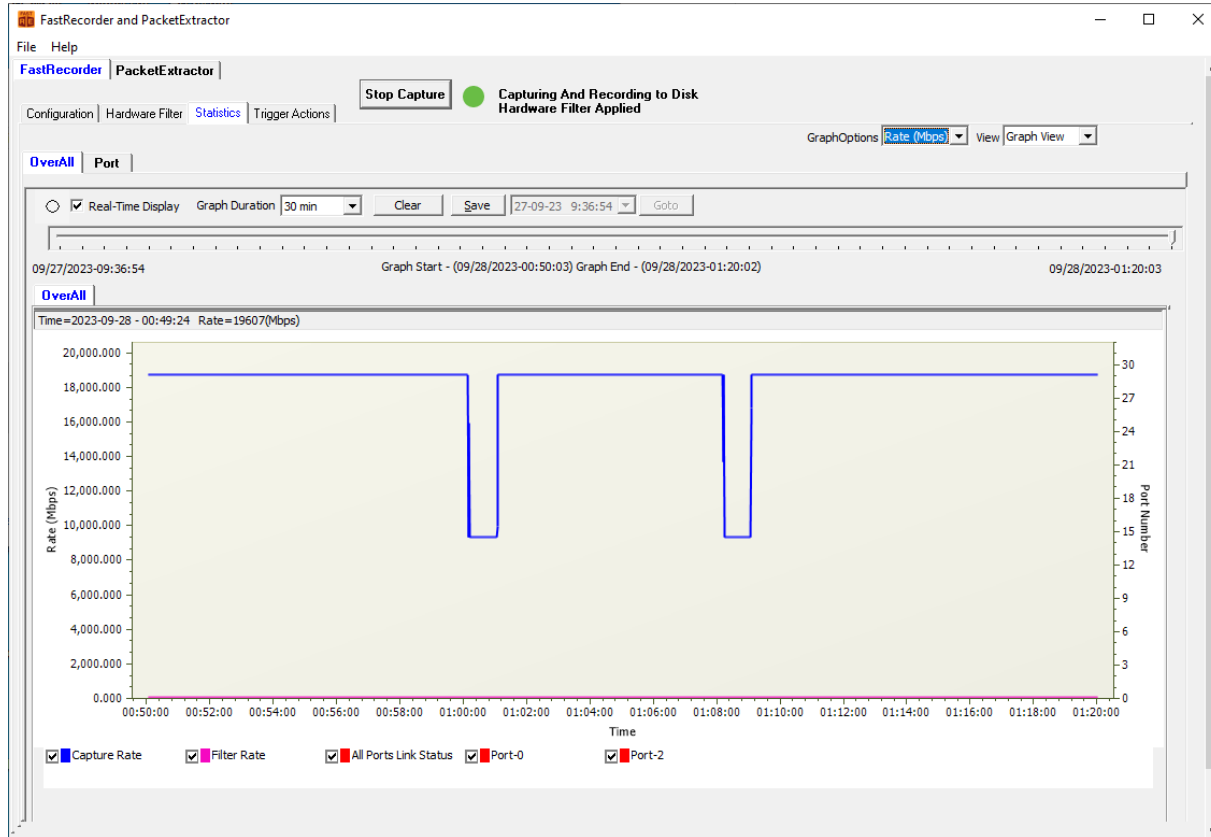
Statistics	Value
Filter Match Frames	58 447 757
Filter Not Match Frames	0
Total Frames	58 447 757
Filter Match Frames %	100.00
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	15.0000
Capture Rate (Mbps)	10215.26
Filtered Rate (Mbps)	10205.14
Filtered Bytes %	100.00
Capture Frame Rate (Frames/Sec)	4 329 904
Filtered Frame Rate (Frames/sec)	4 329 904
Filtered Frames %	100.00
Record Duration (hr:min:sec)	00:00:12
Available Host Buffer Size (Kbytes)	20 971 520
Utilized Host Buffer Size (Kbytes)	1 328 389
Available OnBoard Memory Size (Mbytes)	7 682
Utilized OnBoard Memory Size (%)	0%
Utilized OnBoard Memory Size (Mbytes)	0
Drive Write Fail Count	0,0,0,0

FastRecorder™ - Per Port and Aggregated Statistics

Port Statistics	Aggregate	Port-0 (10G)	Port-2 (10G)
Filter Match Frames	106 071 592	9 642 812	96 428 780
Filter Not Match Frames	0	0	0
Total Frames	106 071 592	9 642 812	96 428 780
Filter Match Frames %	100.00	100.00	100.00
Dropped Frames (Due To Port Buffer Ov...	0	0	0
Capture Rate(Mbps)	-	937.07	9370.22
Filtered Rate (Mbps)	-	937.07	9370.22
Port Link Status	-	Up	Up
Port Link Down Count	-	0	0
L1/L2 ERROR Counters:-			
L2 Drop Events	0	0	0
CRC	0	0	0
Alignment	0	0	0
Code Voilation	0	0	0
Fragments	0	0	0
Jabbers	0	0	0
Collisions	0	0	0
FRAME-LENGTH Counters:-			
64 Byte	0	0	0
65-127 Byte	0	0	0
128-255 Byte	114 800	10 400	104 400
256-511 Byte	105 324 842	9 574 937	95 749 905
512-1023 Byte	517 050	47 025	470 025
1024-1518 Byte	114 900	10 450	104 450
1519-2047 Byte	0	0	0
2048-4095 Byte	0	0	0
4096-8191 Byte	0	0	0
8192-Max Byte	0	0	0
Undersized Frames	0	0	0
Oversized Frames	0	0	0
VLAN Frames	0	0	0
MPLS Frames	0	0	0
Temperature(C)	-	45.0	48.8
Stats Error Count			

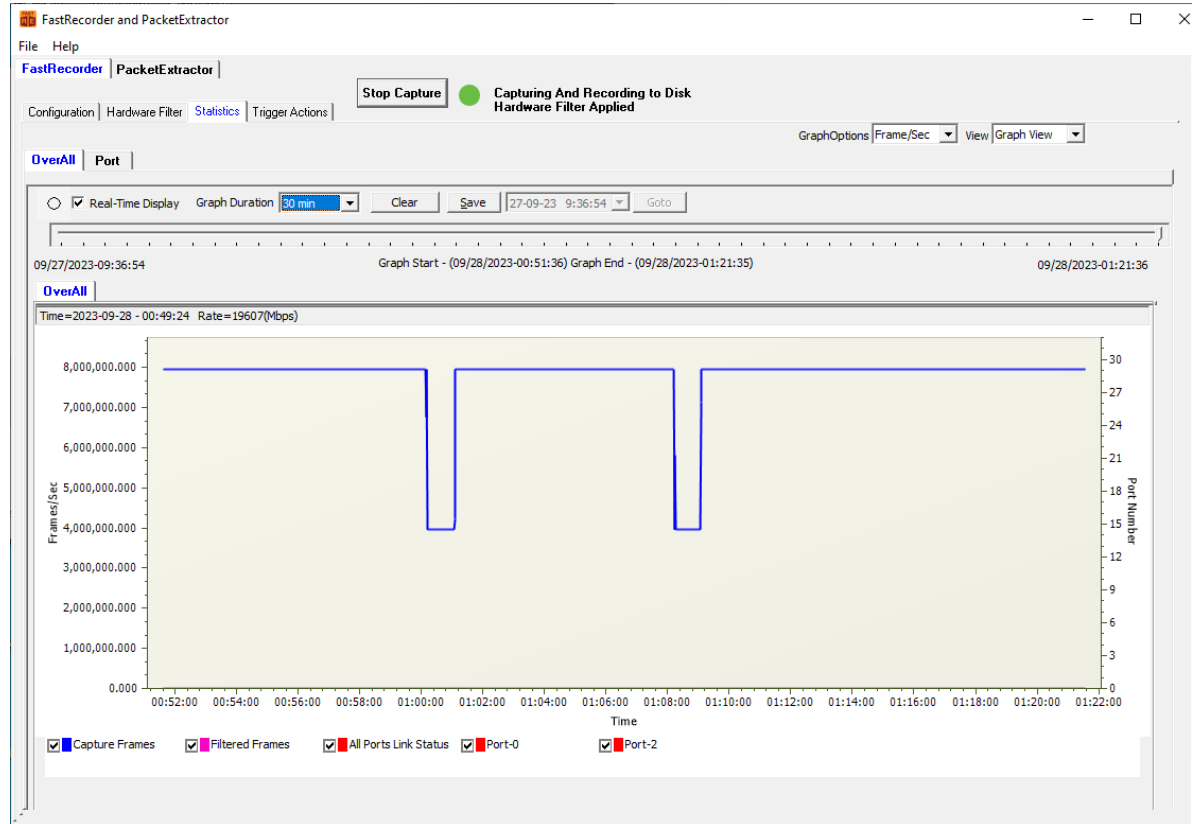
Real time and Historical Graph

- Real time display of graph (Time v/s Rate), Capture Rate and Filter Rate



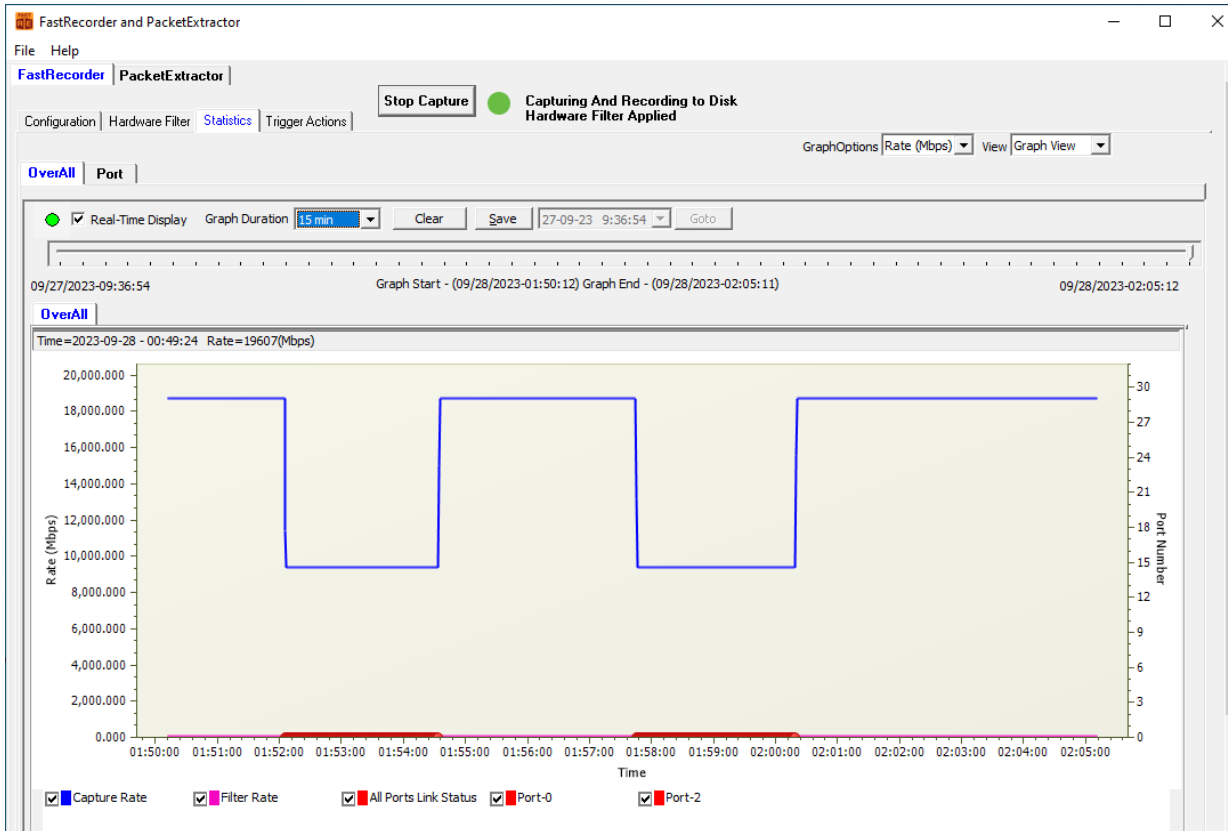
Realtime and Historical Graph (Contd.)

- Overall capture and frame rate for Frame/Secs



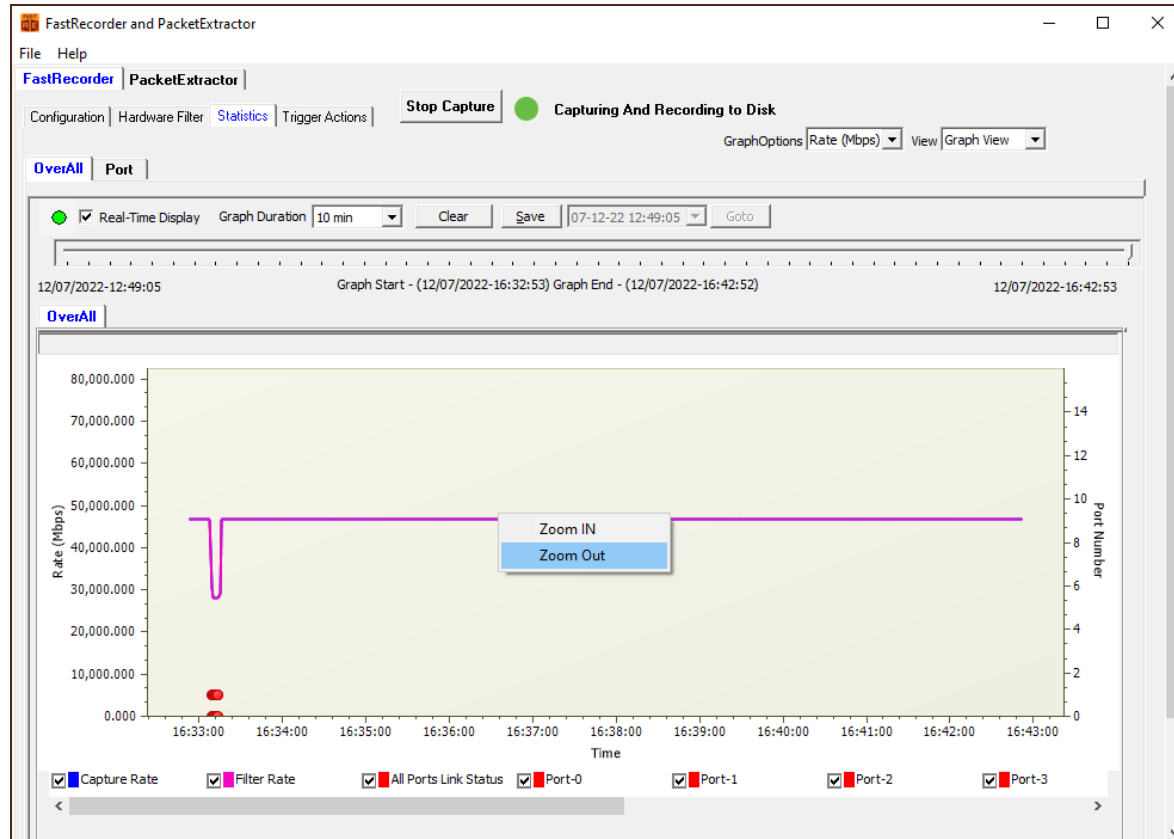
Graphs - Port Link Down

- Port State is changed to **Red** indicating that the Port is down



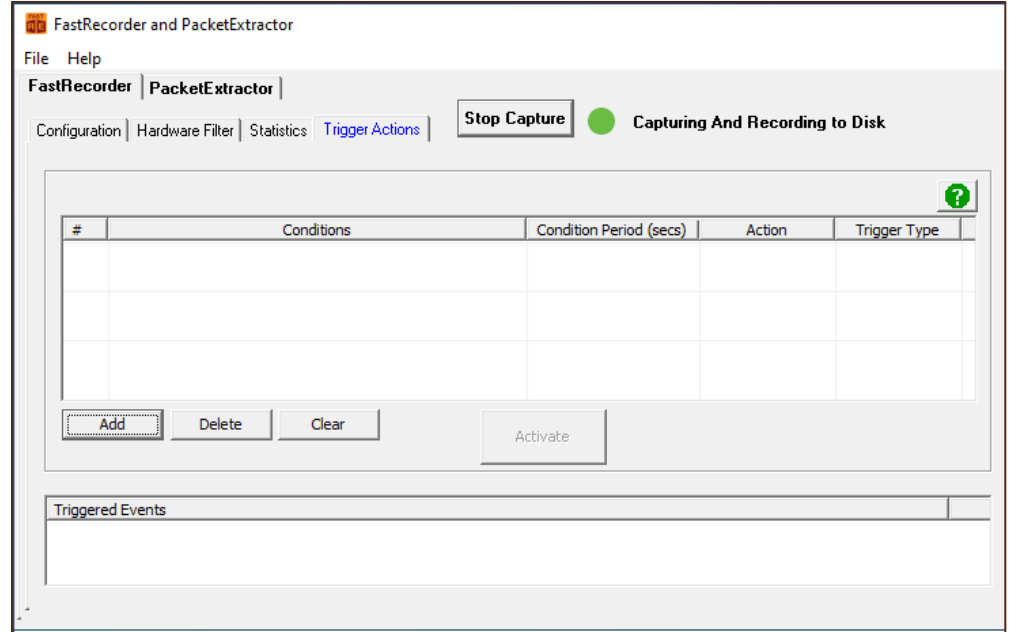
Graphs - Zoom IN and Zoom Out

- User can click on the required area on the graph and select **Zoom IN** or **Zoom Out** as required



Trigger based Start/Stop Recording

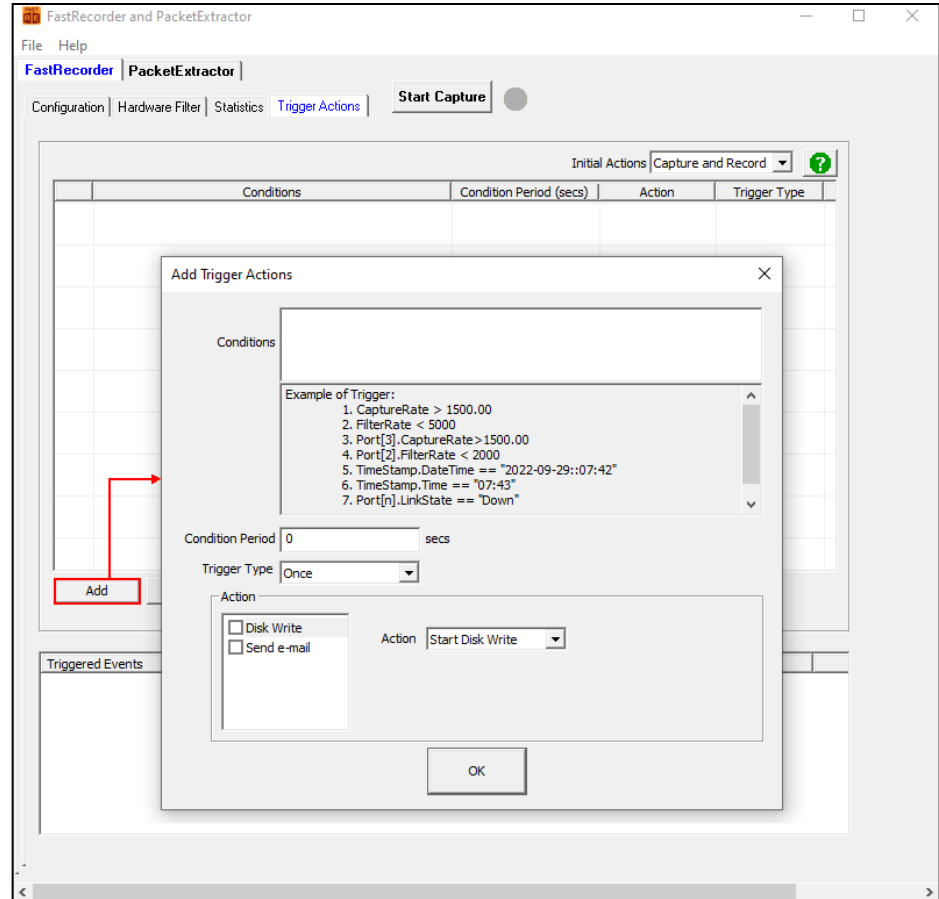
- User can specify the triggers to perform action based on the following conditions
 - CaptureRate (Mbps)
 - FilterRate (Mbps)
 - Port[n].CaptureRate (Mbps)
 - Port[n].FilterRate (Mbps): where n is port number
 - TimeStamp based



Adding Trigger Actions

On the **Add Trigger Actions** window,

- Enter the **Conditions**
- Specify the **Condition period** in seconds
- From the Trigger Type drop-down list select **Once** or **Repeat** as required
- Under **Action** option, check **Disk Write** option
- From the Action drop-down list select **Start Disk Write** or **Stop Disk Write** option as required
- Click on **OK**



Activated Trigger Actions

- Once the trigger is successful, the trigger status changes from **Orange** to **Green** color indicating the recording is started

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'Trigger Actions' tab is active, displaying a table of configured triggers. The status bar indicates 'Capturing And Waiting for Trigger' with a yellow circle. Below the table are buttons for 'Add', 'Delete', 'Clear', and 'Deactivate'. A 'Triggered Events' log at the bottom shows recent actions.

	Conditions	Condition Period (secs)	Action	Trigger Type
<input checked="" type="checkbox"/>	CaptureRate > 1500.00	0	Start Disk Write, Send Mail	Once
<input checked="" type="checkbox"/>	Port[3].CaptureRate > 1500.00	25	Stop Disk Write, Send Mail	Once
<input checked="" type="checkbox"/>	TimeStamp.Time == "12:44"	0	Send Mail	Repeat
<input checked="" type="checkbox"/>	TimeStamp.DateTime == "2022-12-07::12:44"	0	Send Mail	Once
<input checked="" type="checkbox"/>	FilterRate < 5000	15	Start Disk Write	Once
<input checked="" type="checkbox"/>	Port[2].LinkState == "Down"	40	Start Disk Write, Send Mail	Repeat
<input checked="" type="checkbox"/>	Port[2].LinkState == "Up"	0	Start Disk Write, Send Mail	Repeat

Triggered Events

- 12-7 12:49:33 Action=>"Stop Disk Write" Condition=>"Port[3].CaptureRate > 1500.00"
- 12-7 12:49:9 Action=>"Start Disk Write" Condition=>"Port[2].LinkState == "Up"
- 12-7 12:49:9 Action=>"Start Disk Write" Condition=>"CaptureRate > 1500.00"

Activated Trigger Actions (Contd.)

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'Trigger Actions' tab is active, displaying a table of configured trigger actions. A red box highlights the 'Stop Capture' button and the 'Capturing And Recording to Disk' status indicator. Below the table are buttons for 'Add', 'Delete', 'Clear', and 'Deactivate'. At the bottom, a 'Triggered Events' log shows a list of events with their respective conditions, actions, and triggered times.

Initial Actions: Capturing And Recording to Disk

#	Conditions	Condition Period (secs)	Action	Trigger Type
1	CaptureRate > 20480.00	10	Start Disk Write	Repeat
2	CaptureRate < 1000	10	Stop Disk Write	Repeat
3	TimeStamp.DateTime == "2022-11-15::01:35"	0	Start Disk Write	Once
4	TimeStamp.Time == "02:00"	10	Start Disk Write	Repeat
5	TimeStamp.Time == "06:00"	10	Stop Disk Write	Repeat

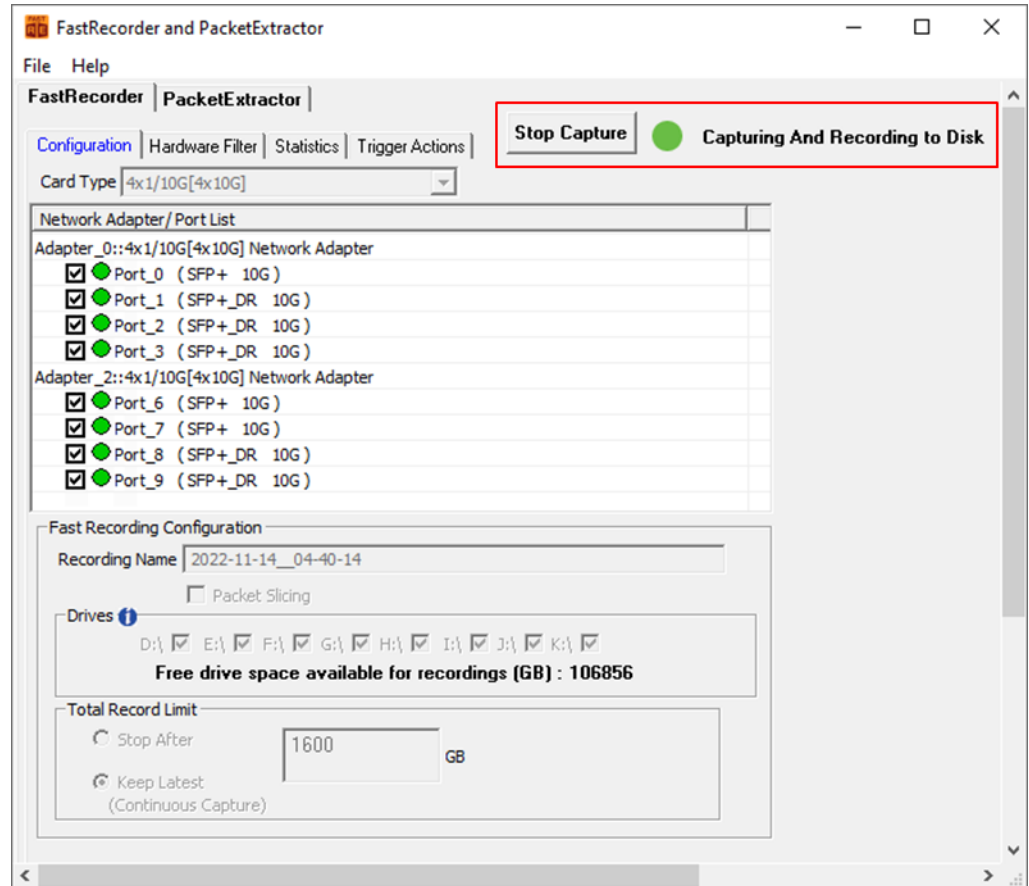
Buttons: Add, Delete, Clear, Deactivate

Triggered Events Log:

- Triggered- Condition->"CaptureRate > 20480.00" Action->"Start Disk Write" TriggeredTime->11-15 1:34:17
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:31:23
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:30:41
- Triggered- Condition->"TimeStamp.DateTime == "2022-11-15::01:30"" Action->"Stop Disk Write" TriggeredTime->11-15 1:30:3
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:29:33
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:28:25

Recording with Default Name

- User can start the capture without specifying **Recording Name** for which current time is taken as recording name
- Network Adapter - Port List display SFP Types and negotiated rates



PacketExtractor™

- PacketExtractor™ configuration settings allows to extract recorded files on the selected HD NIC interface port and required output file format to analyze the results for offline analysis

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, displaying recording information and configuration options. The recording information shows a record named 'SIP_GTP_4PORTS' with a start time of 2024-05-21 02:35:17 and an end time of 2024-05-21 02:36:02, resulting in a duration of 00:00:45 and a record size of 100.001 GB. The configuration section includes checkboxes for 'PreExtraction Filter', 'Extraction Filter', and 'Packet Slicing'. The 'Limit Criteria' section has radio buttons for 'All', 'Duration', 'Extracted Size', and 'Extracted Packet Count', with a 'Limit Value' input field set to 0. The 'Port Filter' section has a 'Port' input field and an example: 'Example: 0 or 0-3 or 0,1,2 or 2,5-7'. The 'Operation' dropdown is set to 'Packet Extraction', and the 'Multiple Files' checkbox is checked. The 'Destination File Name' is 'D:\Extracted.hdl'. The 'Start' and 'Stop' buttons are visible at the bottom of the configuration section.

Recording Information

Record Name: SIP_GTP_4PORTS
Record Start Time: 2024-05-21 02:35:17 Record End Time: 2024-05-21 02:36:02
Record Duration: 00:00:45 Record Size: 100.001 GB

PreExtraction Filter

Start Time: 02:35:17 End Time: 02:36:02 HH:MM:SS

Limit Criteria

All Limit Value: 0
 Duration
 Extracted Size
 Extracted Packet Count

Recorded Ports: 0 2

Port Filter
Port
Example: 0 or 0-3 or 0,1,2 or 2,5-7

Extraction Filter Packet Slicing

Operation: Packet Extraction Multiple Files Create New File After: 1024 MB

Destination File Name: D:\Extracted.hdl

Compress Extracted Files

Start Stop

Statistics

Description	Value
Extractor status	Extraction completed.
Processed Frames	345 516 243
Extracted Frames	345 516 243 (100.00 %)
Processed Bytes (MB)	97 056.332
Extracted Bytes (MB)	97 056.332
Duration (mm:ss)	3::4
Frames with FCS Error	0

Analysis of Extracted Traffic using PacketScan™

- The extracted files can be analyzed using **PacketScan™** application (For HDL file format, maximum file size of 10 GB or having less than 75 million frames is supported)

The screenshot displays the PacketScan application interface. The top menu includes File, View, Capture, Statistics, Database, Call Detail Records, Configure, and Help. Below the menu is a toolbar with various icons for file operations and analysis. The main window is divided into two sections: a frame list and a detailed frame view.

Device	Frame#	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Destination IP Address IP	Source IP Address IP	Destination Address IPv6	Source Address IPv6	Dest ^
✓	2	0	2021-06-14 00:42:03.000000000		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	1	2021-06-14 00:42:03.273961364		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	2	2021-06-14 00:42:03.273961382		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	3	2021-06-14 00:42:03.273961407		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	4	2021-06-14 00:42:03.273961432		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	5	2021-06-14 00:42:03.273961460		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	6	2021-06-14 00:42:03.273961488		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	7	2021-06-14 00:42:03.273961512		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	8	2021-06-14 00:42:03.273961537		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	9	2021-06-14 00:42:03.273961559		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	10	2021-06-14 00:42:03.273961584		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	11	2021-06-14 00:42:03.273961609		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	12	2021-06-14 00:42:03.273961634		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	13	2021-06-14 00:42:03.273961665		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	
✓	2	14	2021-06-14 00:42:03.273961689		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9990	fe80:0000:0000:0000:9897:9897:9897:9991	
✓	2	15	2021-06-14 00:42:03.273961714		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9991	fe80:0000:0000:0000:9897:9897:9897:9990	

Device2 Frame=1 at 2021-06-14 00:42:03.273961364 OK Len=294

*** Right click to SHOW/HIDE layer details or copy ***

```
Ethernet Frame Data
----- MAC Layer -----
0000 Destination Address      = x000DE9066AA7
0006 Source Address          = x000DE9066AA6
000C Length/Protocol Type    = x86DD IPv6
----- IPv6 Layer -----
000E Protocol Version        = 0110... (6)
000E Traffic Class           = 0 (...0000 0000...)
000F Flow Label              = 0 (...0000 00000000 00000000)
0012 Payload Length          = 236 (x00EC)
0014 Next Header              = 00010001 User Datagram Protocol (UDP)
0015 Hop Limit                = 128 (x80)
0016 Source Address          = fe80:0000:0000:0000:9897:9897:9897:9990
0026 Destination Address     = fe80:0000:0000:0000:9897:9897:9897:9991
----- UDP Layer -----
0036 Source Port              = 2152 (x0868)
0038 Destination Port       = 2152 (x0868)
003A Length (Header + Data)  = 236 (x00EC)
003C Checksum                 = x8648
```

Off-line Viewing | E:\Extracted\Extracted.hdl | 10 000 Frames

Analysis of Filtered Traffic in Wireshark®

- The extracted files can be analyzed using Wireshark® application. (For PCAP file format, maximum file size of 5 GB or having less than 53 million frames is supported)

The screenshot displays the Wireshark interface with a list of 16 network packets. The selected packet (No. 7) is expanded to show its protocol stack: Ethernet II, Internet Protocol Version 6, User Datagram Protocol, GPRS Tunneling Protocol, Internet Protocol Version 6, User Datagram Protocol, and Session Initiation Protocol (INVITE).

No.	Time	Source	Destination	Protocol	Stream index	TCP Len
1	03:59:01.000000000	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
2	03:59:01.525264717	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
3	03:59:01.525265542	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
4	03:59:01.525266035	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
5	03:59:01.525266886	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
6	03:59:01.525267385	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
7	03:59:01.525268589	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
8	03:59:01.525269062	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
9	03:59:01.525269581	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
10	03:59:01.525270374	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
11	03:59:01.525271053	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
12	03:59:01.525540064	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
13	03:59:01.525540883	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
14	03:59:01.525541696	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
15	03:59:01.525542189	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
16	03:59:01.525543033	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		

> Frame 7: 1482 bytes on wire (11856 bits), 1482 bytes captured (11856 bits) on interface unknown, id 5
> Ethernet II, Src: IntelCor_85:1a:ff (a0:36:9f:85:1a:ff), Dst: IntelCor_02:32:62 (a4:bf:01:02:32:62)
> Internet Protocol Version 6, Src: fe80::64da:3cd4:cff1:9e97, Dst: fe80::64da:3cd4:cff1:9e96
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
> GPRS Tunneling Protocol
> Internet Protocol Version 6, Src: fe80::10f8:316d:9afd:4398, Dst: fe80::64da:3cd4:cff1:9e96
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (INVITE)

Frame (frame), 1,482 bytes | Packets: 100

Recorded Statistics in PacketExtractor™

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

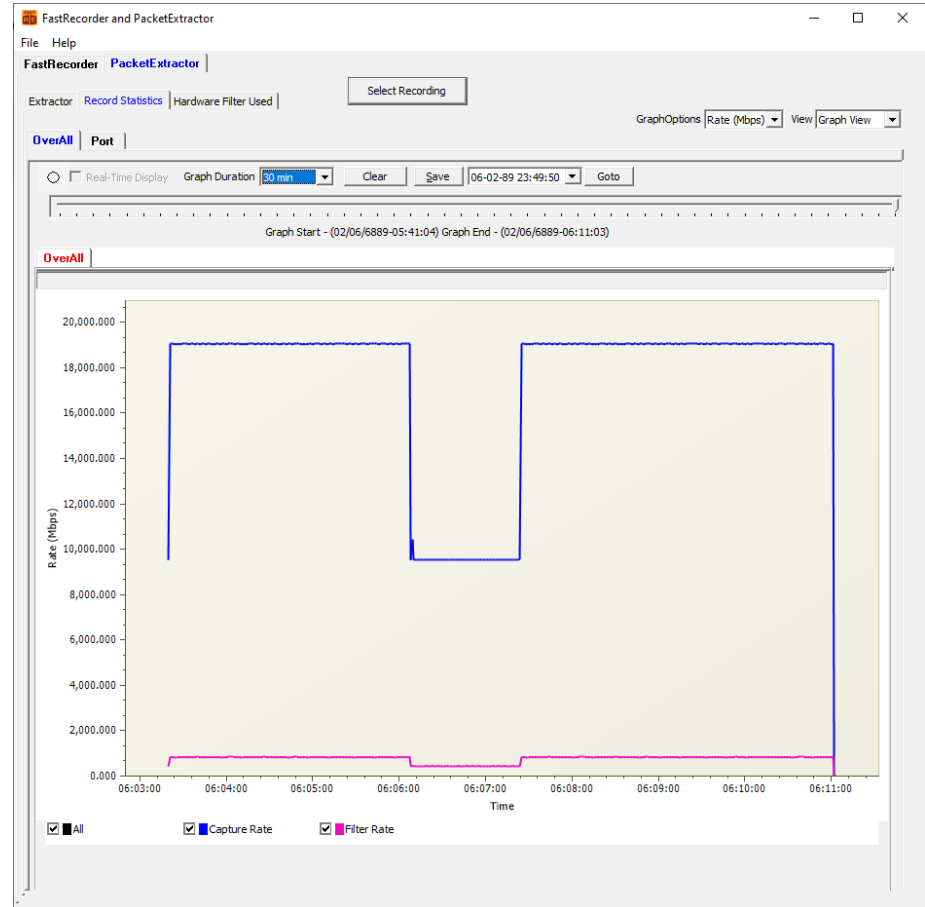
Extractor Record Statistics View List View

Statistics	Value		
Filter Match Frames	352 851 674		
Filter Not Match Frames	0		
Total Frames	352 851 674		
Filter Match Frames %	100.00		
Dropped Frames (Due to Buffer Overflow)	0		
Recorded Bytes (Gbytes)	100.0000		
Record Duration (hr:min:sec)	00:01:20		

Port Statistics	Aggregate	Port-0	Port-2
Filter Match Frames	352 851 674	32 077 822	320 773 852
Filter Not Match Frames	0	0	0
Total Frames	352 851 674	32 077 822	320 773 852
Filter Match Frames %	100.00	100.00	100.00
Dropped Frames (Due To Port Buffer Ove...)	0	0	0
Port Link Status	-	Up	Up
Port Link Down Count	0	0	0
L1/L2 ERROR Counters:-			
L2 Drop Events	0	0	0
CRC	0	0	0
Alignment	0	0	0
Code Violation	0	0	0
Fragments	0	0	0
Jabbers	0	0	0
Collisions	0	0	0
FRAME-LENGTH Counters:-			
64 Byte	0	0	0
65-127 Byte	0	0	0
128-255 Byte	382 150	34 750	347 400
256-511 Byte	350 367 974	31 852 222	318 515 752
512-1023 Byte	1 719 450	156 150	1 563 300
1024-1518 Byte	382 100	34 700	347 400
1519-2047 Byte	0	0	0
2048-4095 Byte	0	0	0
4096-8191 Byte	0	0	0
8192-Max Byte	0	0	0
Undersized Frames	0	0	0
Oversized Frames	0	0	0
VLAN Frames	0	0	0
MPLS Frames	0	0	0
Temperature(C)	0	45.9	49.6
XTPNotificationSinkMTOntEvent			

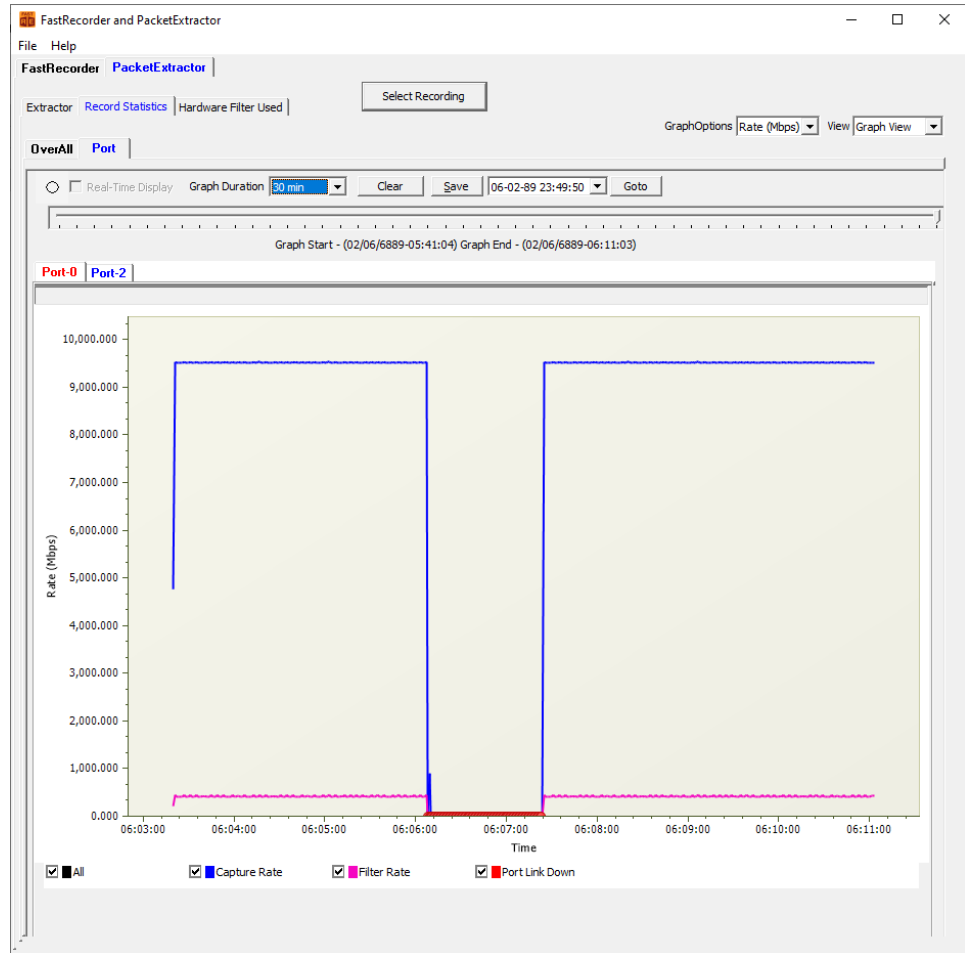
PacketExtractor™ - Overall Graph View

- User can view the capture rate and filter rate of the recording



PacketExtractor™ - Port View

- User can view the per port **capture rate** and **filter rate** of the recorded file



Packet Extraction from the Recordings with Filter

The screenshot displays the 'FastRecorder and PacketExtractor' application interface. The main window is titled 'FastRecorder' and 'PacketExtractor'. A 'Select Recording' button is visible at the top. The 'Recording Information' section shows a record named 'SIP_GTP_4PORTS' with a start time of '2023-03-24 07:46:57' and a duration of '00:07:26'. The 'PreExtraction Filter' section includes 'Start Time' and 'End Time' fields, and 'Limit Criteria' options: 'All', 'Duration' (with a limit value of '00:07:26'), 'Extracted Size', and 'Extracted Packet Count'. A red arrow points from the 'Duration' limit value to the 'End Time' field. The 'Extraction Filter' section is checked, with a 'Filter Configuration' button. The 'Operation' is set to 'Packet Extraction'. The 'Destination File Name' field is empty, and there are checkboxes for 'Compress Extracted Files' and 'Start'.

The 'Protocol Capture Configuration' dialog box is open, showing 'Capture Filter' and 'Record Frames As Is' options. The 'Capture Filters' section includes a 'Filter Selection' tree with categories like 'Layers' and 'Protocol'. The 'Filter Selected Protocols' section lists various protocols with checkboxes, including ARP, GTP-C, ICMP, LDAP, PTP, SLOW, UDP, DIAMETER, GTP-U, IPV4, LLDAP, SCTP, and SNMP. A 'Configure Protocols List' button is present. At the bottom of the dialog, there are 'Include' and 'Exclude' radio buttons, and 'Deactivate Sel' and 'Deactivate All' buttons.

Specifying End Time for Packet Extraction

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, and the 'Extractor' sub-tab is selected. The 'Recording Information' section displays the record name 'SIP_GTP_4PORTS', start time '2024-05-15 05:32:05', end time '2024-05-15 05:32:10', duration '00:00:05', and size '10.001 GB'. The 'PreExtraction Filter' section is checked, and the 'Start Time' and 'End Time' fields are highlighted with a red box. The 'Limit Criteria' section includes options for 'All', 'Duration', 'Extracted Size', and 'Extracted Packet: Count'. The 'Extraction Filter' section is checked, and the 'Operation' is set to 'Packet Extraction'. The 'Destination File Name' is 'D:\Extract-w-Endtime.hdl'. The 'Statistics' section at the bottom shows a table with the following data:

Description	Value
Extractor status	Extraction completed.
Processed Frames	34 556 150
Extracted Frames	34 556 150 (100.00 %)
Processed Bytes (MB)	9 706.907
Extracted Bytes (MB)	9 706.907
Duration (mm:ss)	0::18
Frames with FCS Error	0

Hardware Filter Used while Recording

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The 'Hardware Filter Used' tab is active, showing a configuration for an advanced filter. The filter is named 'Filter - 1' and is currently selected. The filter type is set to 'Advanced'. The filter configuration is as follows:

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	IPLIST	Ip List	==		
F2	VLAN0	Tag Protocol ID	==	8100	
F3	UDP	Source Port	==	5060	
F4	TCP	Source Port	==	443	
F5	SCTP	Source Port	==	36412	

The filter is applied to the 'IP List Type' (IP Address List) and 'IP Layer Type' (Inner Tunnel1 / Outer Non Tunnel). The IP Address list contains the address 192.168.13.187. The filter is configured with a custom expression: `(f2 && f3) || f1`. The final configured expression is: `KeyList[KeyType=Ipv4; KeySet=6] = ([192.168.13.187]) Assign[StreamId = 10] = (((mVlan0TPID == 0x8100) AND (mUdpSrcPort == 5060)) OR (((TunnelType == GTPv1-U-GPDU OR (TunnelType == GREv0 OR TunnelType == GR`

eCPRI Analysis

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The main interface is divided into several sections:

- Recording Information:** Record Name: SIP_GTP_4PORTS, Record Start Time: 2023-03-24 07:46:57, Record Duration: 00:07:26.
- Limit Criteria:** Includes options for 'All', 'Duration' (set to 00:07:26), 'Extracted Size', and 'Extracted Packet Count'.
- Extraction Filter:** A red box highlights the 'Filter Configuration' button, which is linked to the 'Protocol Capture Configuration' dialog box.
- Protocol Capture Configuration Dialog:** This dialog has a 'Capture Filter' tab and a 'Filter Selection' tree. The tree lists various protocols under 'Layers', including MAC, VLAN, IP (All Levels), IP (Outer), ESP, TCP, UDP, Inner IP, Inner UDP, SCTP, SIP, RTP, MSRP, MGCP, MEGACO, H323, and RTSP. Below the tree are 'Include' and 'Exclude' radio buttons.
- Filter Selected Protocols:** A section titled 'Filter Selected Protocols' contains a list of protocols with checkboxes, including ARP, GTP-C, ICMP, LDAP, PTP, SLOW, UDP, DIAMETER, GTP-U, IPv4, LLDP, SCTP, and SNMP. Other protocols like DNS, HTTP, IPv6, MEGACO, SIP, and TCP are also listed but not checked. A 'Configure Protocols List' button is located at the bottom of this section.

View eCPRI Layer Decode Details in PacketScan™

Over UDP

- From the desktop, invoke **PacketScan™** analyzer
- Goto **File** → **Offline**, browse and select any one of the extracted *.hdl file from the **D:\Extracted** folder. Click on **Open**
- Observe the **eCPRI** layer decode details as shown

```
Device0 Frame=6 at 2022-06-09 06:07:36.711206000 OK Len=112 *** Right c
Ethernet Frame Data
===== MAC Layer =====
0000 Destination Address = xFCAA149225C4
0006 Source Address      = x54BEF737CB9A
000C Length/Protocol Type = x86DD IPv6
===== IPv6 Layer =====
000E Protocol Version    = 0110.... (6)
000E Traffic Class      = 0 (...0000 0000....)
000F Flow Label         = 834513 (...1100 10111011 11010001)
0012 Payload Length     = 58 (x003A)
0014 Next Header        = 00010001 User Datagram Protocol (UDP)
0015 Hop Limit          = 64 (x40)
0016 Source Address     = fe80::64f2:5e84:f1db:502
0026 Destination Address = fe80::589e:b2d5:9074:2bec
===== UDP Layer =====
0036 Source Port        = 64000 (xFA00)
0038 Destination Port  = 64000 (xFA00)
003A Length (Header + Data) = 58 (x003A)
003C Checksum          = x7F76
===== eCPRI Layer =====
003E C                  = .....0 eCPRI message is the last one inside the eCPRI PDU
003E eCPRI Protocol Revision = 0001.... (1)
003F eCPRI Message Type = 00000100 Remote Memory Access
0040 eCPRI Payload Size = 28 (x001C)
0042 Remote Memory Access ID = 17 (x11)
0043 Req/Resp           = ...0010 Failure
0043 Read/Write         = 0010.... Write_No_Resp
0044 Element ID        = 8755 (x2233)
0046 Address            = x050403020100
004C Length            = 16 (x0010)
User Data              = xFFEEDDCCBBAA99887766554433221100
```

View eCPRI Layer Decode Details in PacketScan™ (Contd.)

Over MAC

```
Device0 Frame=0 at 2019-02-13 11:36:46.000000000 OK Len=64 *** Right
Ethernet Frame Data
===== MAC Layer =====
0000 Destination Address      = x008016000000
0006 Source Address          = x008016884EFF
000C Length/Protocol Type    = xAEFE eCPRI
===== eCPRI Layer =====
000E C                        = .....0 eCPRI message is the last one inside the eCPRI PDU
000E eCPRI Protocol Revision  = 0001..... (1)
000F eCPRI Message Type      = 00000000 IQ Data
0010 eCPRI Payload Size      = 20 (x0014)
    eCPRI Payload             = x123487650F0E0D0C0B0A09080706050403020100
===== O-RAN Fronthaul CUS Layer =====
    ecpriPoid                  =
0012 BandSector_ID           = ..010010 (18)
0012 DU_Port_ID              = 00..... (0)
0013 RU_Port_ID              = ....0100 (4)
0013 CC_ID                    = 0011..... (3)
    ecpriSeqid                 =
0014 Sequence ID             = 135 (x87)
0015 Subsequence ID          = .1100101 (101)
0015 E bit                    = 0..... More fragments follow
0016 FilterIndex              = ....1111 Reserved
0016 payloadVersion           = .000..... (0)
0016 dataDirection           = 0..... UpLink
0017 frameId                  = 14 (x0E)
0018 subframeId               = 0000..... (0)
0018 slotId                   = 52 (....1101 00.....)
0019 startSymbolId            = ..001100 (12)
001A sectionId                = 176 (00001011 0000....)
001B symInc                   = .....0... use the current symbol number
001B rb                        = ....1... every other RB used
001B startPrbu                = 521 (.....10 00001001)
001D numPrbu                  = 8 (x08)
    udCompHdr                  =
001E udCompMeth               = ....0111 Reserved
001E udIqWidth                = 0000..... I and Q are each 16 bit wide
    Dump                       = x050403020100
```

Encapsulated Security Payload (ESP) Deciphering

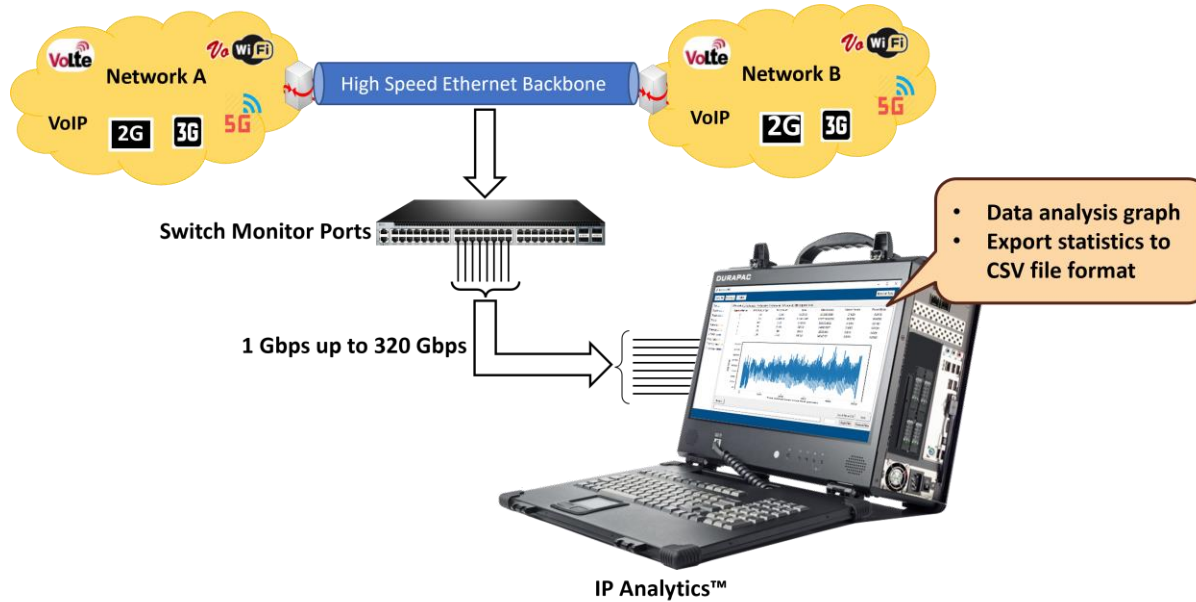
- Supports Encapsulating Security Payload (ESP) to decrypt ESP packets on both IPv4 and IPv6 by providing ESP SAs value

The screenshot shows the 'Protocol Capture Configuration' window with the 'Filters' section expanded to 'Decipher Encrypted ESP Payload'. The 'Extract' options are set to 'Deciphered Payload'. The 'ESP SAs' field has an 'Edit' button highlighted with a red box and a red arrow pointing to it.

Below the configuration window is the 'ESP SAs' table:

IP Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key	Authentication	Authentication Key
IPv4	192.168.12.86	192.168.12.45	0x05d2ede0	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	192.168.12.45	x.x.x.x	0x467113ba	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	192.168.12.86	192.168.12.251	0xd02382c2	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	192.168.12.251	192.168.12.86	0x129e7b1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	192.168.12.90	192.168.12.45	0xa5e7259a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	192.168.12.45	*	0x9637e4e8	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	192.168.12.90	192.168.12.251	0x57be7f1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...
IPv4	*	192.168.12.90	*	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E787C...

IP Analytics™



- IP Analytics™ (Optional with FastRecorder™ and PacketExtractor™) serves as a critical tool for meticulous monitoring and optimization
- It involves scrutinizing data flows to uphold the integrity of voice, video, and data services, ensuring adherence to predefined performance benchmarks
- Through continuous evaluation of metrics such as Quality of Service and packet loss, network operators can fine-tune their infrastructure, guaranteeing an unparalleled user experience

Data Analysis

Selecting Data Analysis Option

- Users can perform **Data Analysis** using the PacketExtractor™ application

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, and the 'Record Statistics' section shows recording details for a record named '2024-02-14__07-21-22'. The recording duration is 00:28:46 and the size is 514,987,457 MB. The 'Extraction Filter' section is highlighted with a red box, showing the 'Operation' dropdown menu open with 'Data Analysis' selected. Other options in the menu include 'Packet Extraction', 'Rate Analysis', 'eCPRI Analysis', and 'BERT Verify'. The 'Destination File Name' field is empty, and the 'Start' button is visible. Below the configuration area, a 'Statistics' table provides a summary of the extraction process.

Description	Value
Extractor status	Extraction completed.
Extracted Frames	383 983 458
Extracted Bytes (MB)	355 892.521
Duration (mm:ss)	0:34
Frames with FCS Error	0

GL IP Analytics™ Tool

- Executing **Python scripts** will invoke the **GL IP Analytics™** window to perform data analysis
- This analysis will display Ports, L3 Protocols, L4 Protocols, DSCP, IPv4 Endpoints, IPv4 Conversations, IPv6 Endpoints, IPv6 Conversations, TCP Endpoints, UDP Endpoints, UDP Conversations, TCP Conversations, SCTP Conversations, and Ping Conversations statistics

The screenshot displays the GL IP-ANALYTICS application window. The interface includes a top navigation bar with 'Select file', 'Select folder', and 'Export analysed tabs' buttons. A left sidebar lists various analysis categories, with 'L3 Protocols' selected. The main area shows a table titled 'L3 Protocols' with the following data:

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
2	IPv4 - (0x800)	28,419,913	16,677,921,882	6,539,530,100.38	99.59	99.92
3	ARP - (0x806)	53,921	3,450,944	1,353,139.33	0.19	0.02
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	0xaa	455	85,540	33,540.83	0.0	0.0
6	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0

Below the table, it indicates 'Total entries: 6' and provides navigation buttons for 'Previous', 'Next', and 'Export Tab as CSV'. At the bottom, there is a 'Filter section' with an input field, a search button, and an 'Erase' button.

Port Statistics

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

Row ID	PortNo	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	0	13,101,139	7,624,353,827	2,989,562,590.61	45.91	45.68
2	2	15,434,921	9,067,342,149	3,555,368,428.59	54.09	54.32

Total entries: 2 Previous Next Export Tab as CSV

Filter section

Erase

Outer Protocol Statistics – L3 and L4

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols**
 - L4 Protocols
 - DSCP
 - IPv4 Endpoints
 - IPv4 Conversations
 - IPv6 Endpoints
 - IPv6 Conversations
 - TCP Endpoints
 - UDP Endpoints
 - UDP Conversations
 - TCP Conversations
 - SCTP Conversations
 - PING Conversations

Total entries: 6

L3 Protocols

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
2	IPv4 - (0x800)	28,419,913	16,677,921,882	6,539,530,100.38	99.59	99.92
3	ARP - (0x806)	53,921	3,450,944	1,353,139.33	0.19	0.02
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	0xaa	455	85,540	33,540.83	0.0	0.0
6	LDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols
 - L4 Protocols**
 - DSCP
 - IPv4 Endpoints
 - IPv4 Conversations
 - IPv6 Endpoints
 - IPv6 Conversations
 - TCP Endpoints
 - UDP Endpoints
 - UDP Conversations
 - TCP Conversations
 - SCTP Conversations
 - PING Conversations

Total entries: 5

L4 Protocols

Row ID	IP Protocol	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	TCP - (6)	19,857,043	12,697,011,859	4,978,587,369.83	69.76	76.09
2	IGMP - (2)	1,062	78,456	30,763.14	0.0	0.0
3	ICMP - (1)	16,620	2,975,820	1,166,839.88	0.06	0.02
4	IPv6-ICMP - (58)	26,314	2,368,260	928,611.35	0.09	0.01
5	UDP - (17)	8,564,491	3,984,558,671	1,562,373,391.00	30.09	23.88

Previous Next Export Tab as CSV

Outer Protocol Statistics – DSCP and IPv4 Endpoints

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols
 - L4 Protocols
 - DSCP**
 - IPv4 Endpoints
 - IPv4 Conversations
 - IPv6 Endpoints
 - IPv6 Conversations
 - TCP Endpoints
 - UDP Endpoints
 - UDP Conversations
 - TCP Conversations
 - SCTP Conversations
 - PING Conversations

DSCP

Row ID	DSCP	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	Best Effort - (0)	28,337,361	16,633,818,424	6,522,236,825.29	99.55	99.68
2	Class selector-CS6 - (48)	468	64,800	25,408.53	0.0	0.0
3	4	127,701	53,109,842	20,824,741.40	0.45	0.32

Total entries: 3

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols
 - L4 Protocols
 - DSCP
 - IPv4 Endpoints**
 - IPv4 Conversations
 - IPv6 Endpoints
 - IPv6 Conversations
 - TCP Endpoints
 - UDP Endpoints
 - UDP Conversations
 - TCP Conversations
 - SCTP Conversations
 - PING Conversations

IPv4 Endpoints

Row ID	IP Address	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets
1	104.44.49.142	30	2,220	0	0	1.47	870.47	0.00	0.00	30
2	34.111.50.114	304	99,024	208	22,656	14.90	38,828.00	10.19	8,883.57	512
3	91.189.91.49	585	67,905	900	75,915	28.67	26,626.02	44.11	29,766.80	1,485
4	202.83.26.121	1,985	1,134,827	646	67,757	97.29	444,973.62	31.66	26,567.99	2,631
5	192.168.12.210	4,001	615,250	2,792	742,619	196.10	241,243.83	136.84	291,186.11	6,793
6	142.250.4.188	655	46,098	655	42,540	32.10	18,075.34	32.10	16,680.23	1,310
7	142.250.196.65	1,305	1,635,945	780	70,590	63.96	641,465.50	38.23	27,678.83	2,085
8	192.168.1.25	3,653	318,478	3,224	261,370	179.04	124,877.45	158.01	102,485.00	6,877
9	192.168.255.25	0	0	318	27,762	0.00	0.00	15.58	10,885.67	318
10	192.168.12.208	1,155	280,770	0	0	56.61	110,091.88	0.00	0.00	1,155
11	35.224.170.84	390	37,380	510	41,580	19.11	14,656.96	24.99	16,303.80	900

Total entries: 1050

Previous Next Export Tab as CSV

Outer Protocol Statistics – IPv4 and IPv6

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols
 - L4 Protocols
 - DSCP
 - IPv4 Endpoints
 - IPv4 Conversations**
 - IPv6 Endpoints
 - IPv6 Conversations
- TCP Endpoint
- UDP Endpoint
- UDP Conversations
- TCP Conversations
- SCTP Conversations
- PING Conversations

Filter section

IPv4 Conversations

Row ID	Address A	Address B	Total Packets	Packets A->B	Packets B->A	Bytes A->B	Bytes B->A	Avg Packets/sec A->B	Avg Packets/sec B->A	Avg Bits/sec A->B	Avg Bits/sec B->A
1	192.168.12.12	142.250.195.226	300	150	150	42,195	36,480	7.35	7.35	16,544.95	14,304.06
2	192.168.12.219	142.250.195.234	3,585	1,770	1,815	297,420	318,975	86.75	88.95	116,620.46	125,072.33
3	192.168.12.11	20.198.118.190	1,432	944	488	107,129	111,000	46.26	23.91	42,006.03	43,523.87
4	40.99.34.146	192.168.12.91	476	300	176	382,260	55,280	14.70	8.62	149,886.82	21,675.67
5	192.168.12.11	52.112.39.48	630	285	345	101,610	278,700	13.96	16.90	39,841.99	109,280.22
6	192.168.12.209	192.168.30.156	33,213	16,379	16,834	1,087,145	1,790,730	802.79	825.09	426,277.17	702,157.78
7	192.168.12.91	74.125.200.188	1,276	638	638	41,452	44,908	31.27	31.27	16,253.61	17,608.74
8	192.168.12.76	192.168.1.61	122	90	32	5,940	4,800	4.41	1.56	2,329.11	1,882.11

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols
 - L4 Protocols
 - DSCP
 - IPv4 Endpoints
 - IPv4 Conversations
 - IPv6 Endpoints**
 - IPv6 Conversations
 - TCP Endpoints
 - UDP Endpoints
 - UDP Conversations
 - TCP Conversations
 - SCTP Conversations
 - PING Conversations

Filter section

IPv6 Endpoints

Row ID	IP Address	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets	Total Bytes
1	ff02::1:2	0	0	577	97,048	0.00	0.00	28.28	38,053.20	577	97,048
2	ff02::1:ff5f:118	0	0	32	2,880	0.00	0.00	1.56	1,129.26	32	2,880
3	ff02::1:ff68:9882	0	0	16	1,440	0.00	0.00	0.78	564.63	16	1,440
4	ff02::1:ffa0:28c4	0	0	93	8,370	0.00	0.00	4.55	3,281.93	93	8,370
5	fe80::d431:1f22:4fe1:6df2	182	19,838	0	0	8.92	7,778.61	0.00	0.00	182	19,838
6	fe80::e0a6:b9da:4b11:90c9	182	19,838	0	0	8.92	7,778.61	0.00	0.00	182	19,838
7	fe80::3447:6c51:73ad:a38	182	19,838	0	0	8.92	7,778.61	0.00	0.00	182	19,838
8	fe80::2c53:e5c3:3a09:7150	5,734	516,060	0	0	281.04	202,350.74	0.00	0.00	5,734	516,060
9	fe80::39cb:1b70:a4ad:f045	322	232,484	0	0	15.78	91,158.60	0.00	0.00	322	232,484
10	fe80::edef:8298:6b5d:737	45	4,770	0	0	2.20	1,870.35	0.00	0.00	45	4,770
11	fe80::ec79:9ba0:1d5f:118	48	7,728	0	0	2.35	3,030.20	0.00	0.00	48	7,728

Total entries: 69

Previous Next Export Tab as CSV

Outer Protocol Statistics – IPv6 and TCP

GL IP-ANALYTICS
Export analysed tabs

Select file
Select folder

Ports

- Protocol Statistics
- L3 Protocols
- L4 Protocols
- DSCP
- IPv4 Endpoints
- IPv4 Conversations
- IPv6 Endpoints
- IPv6 Conversations
- TCP Endpoints
- UDP Endpoints
- UDP Conversations
- TCP Conversations
- SCTP Conversations
- PING Conversations

Filter section

IPv6 Conversations											
Row	Address A	Address B	Total Packets	Packets A->B	Packets B->A	Bytes A->B	Bytes B->A	Avg Packets/sec A->B	Avg Packets/sec B->A	Avg Bits/sec A->B	Avg Bits/sec B->A
1	fe80::d431:1f22:4fe1:6df2	ff02::fb	182	182	0	19,838	0	8.92	0.00	972.32	0.00
2	fe80::e0a6:b9da:4b11:90c	ff02::fb	182	182	0	19,838	0	8.92	0.00	972.32	0.00
3	fe80::3447:6c51:73ad:a38	ff02::fb	182	182	0	19,838	0	8.92	0.00	972.32	0.00
4	fe80::2c53:e5c3:3a09:715	ff02::1:ff00:1	5,734	5,734	0	516,060	0	281.04	0.00	25,293.84	0.00
5	fe80::39cb:1b70:a4ad:f04	ff02::c	322	322	0	232,484	0	15.78	0.00	11,394.82	0.00
6	fe80::edef:8298:6b5d:737	ff02::fb	45	45	0	4,770	0	2.20	0.00	233.79	0.00
7	fe80::ec79:9ba0:1d5f:118	ff02::c	48	48	0	7,728	0	2.35	0.00	378.77	0.00
8	fe80::810d:1ee:30a0:28c4	ff02::1:ff5f:118	16	16	0	1,440	0	0.78	0.00	70.57	0.00

GL IP-ANALYTICS
Export analysed tabs

Select file
Select folder

Ports

- Protocol Statistics
- L3 Protocols
- L4 Protocols
- DSCP
- IPv4 Endpoints
- IPv4 Conversations
- IPv6 Endpoints
- TCP Endpoints
- UDP Endpoints
- UDP Conversations
- TCP Conversations
- SCTP Conversations
- PING Conversations

TCP Endpoints											
Row ID	Port	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets	Total Bytes
1	58319	11,116	9,120,206	11,291	9,039,486	544.83	3,576,096.71	553.41	3,544,445.83	22,407	18,159,692
2	51094	485	149,639	468	187,031	23.77	58,674.50	22.93	73,336.16	953	336,670
3	64088	398	113,093	419	322,825	19.50	44,344.55	20.53	126,581.94	817	435,918
4	55493	85	6,715	51	3,366	4.16	2,632.99	2.49	1,319.83	136	10,081
5	64146	269	54,264	191	14,121	13.18	21,277.29	9.36	5,536.94	460	68,385
6	65182	255	19,320	174	12,744	12.49	7,575.50	8.52	4,997.01	429	32,064
7	64937	1,013	116,229	862	67,596	49.65	45,574.20	42.24	26,504.86	1,875	183,825
8	56266	219	64,949	205	16,442	10.73	25,466.95	10.04	6,447.02	424	81,391
9	64193	312	22,659	220	18,730	15.29	8,884.75	10.78	7,344.16	532	41,389
10	63054	442	256,763	521	225,041	21.66	100,678.57	25.53	88,240.15	963	481,804
11	49352	96	7,648	80	6,624	4.70	2,998.83	3.92	2,597.31	176	14,272

Total entries: 11363

Previous
Next
Export Tab as CSV

Outer Protocol Statistics – SCTP

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

SCTP Conversations

Row ID	Address A	Address B	Port A	Port B	Total Packets	Packets A->B	Packets B->A	Bytes A->B	Bytes B->A	Avg Packets/sec A->B	Avg Packets/sec B->A	Avg E
1	192.168.13.135	192.168.13.131	36412	36412	7,649	3,221	4,428	454,950	582,608	0.00	0.00	

Total entries: 1 Previous Next Export Tab as CSV

Filter section

Erase

Outer Protocol Statistics – PING Conversations

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Ports

- Protocol Statistics
 - L3 Protocols
 - L4 Protocols
 - DSCP
 - IPv4 Endpoints
 - IPv4 Conversations
 - IPv6 Endpoints
 - IPv6 Conversations
 - TCP Endpoints
 - UDP Endpoints
 - UDP Conversations
 - TCP Conversations
 - SCTP Conversations
 - PING Conversations**

PING Conversations

Row ID	Address A	Address B	Requests	Responses
1	192.168.12.192	23.62.12.106	150	15
2	192.168.12.124	23.62.12.106	150	15
3	192.168.12.189	23.62.12.99	150	15
4	192.168.12.55	13.107.21.200	285	15
5	192.168.12.113	23.62.12.67	160	16
6	192.168.12.26	13.107.21.200	285	15
7	192.168.12.163	204.79.197.200	285	15
8	192.168.12.178	23.62.12.59	150	15
9	192.168.12.5	23.62.12.67	150	15
10	192.168.12.3	204.79.197.200	240	15
11	192.168.12.186	23.62.12.106	150	15

Total entries: 20

Previous Next Export Tab as CSV

Filter section

Erase

Tunneled Protocol Statistics

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Tunneled Protocol Statistics

- L4 Protocols
- DSCP
- IPv4 Endpoints
- IPv4 Conversations
- IPv6 Endpoints
- IPv6 Conversations
- TCP Endpoints
- UDP Endpoints
- UDP Conversations
- TCP Conversations
- SCTP Conversations
- PING Conversations

Inner L4 Protocols

Row ID	IP Protocol	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	HOPOPT - (0)	15,411	6,426,224	0.00	0.29	0.16
2	TCP - (6)	5,258,034	4,075,377,645	0.00	99.71	99.84

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

Tunneled Protocol Statistics

- L4 Protocols
- DSCP
- IPv4 Endpoints
- IPv4 Conversations
- IPv6 Endpoints
- IPv6 Conversations
- TCP Endpoints
- UDP Endpoints
- UDP Conversations
- TCP Conversations
- SCTP Conversations
- PING Conversations

Inner DSCP

Row ID	DSCP	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	Best Effort - (0)	5,273,445	4,081,803,869	0.00	100	100

Total entries: 1

Previous Next Export Tab as CSV

Sorting of Columns (Tabs)

- Click on required tab (column) to sort it in either ascending or descending order

Display of columns in Ascending order

The screenshot shows the 'GL IP-ANALYTICS' application window. The 'L3 Protocols' tab is selected in the left sidebar. The main table displays the following data:

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	0xaa	455	85,540	33,540.83	0.0	0.0
2	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0
3	0x27	13,925	891,200	349,445.76	0.05	0.01
4	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
5	ARP - (0x806)	53,921	3,450,944	1,353,139.33	0.19	0.02
6	IPv4 - (0x800)	28,419,913	16,677,921,882	6,539,530,100.38	99.59	99.92

Display of columns in Descending order

The screenshot shows the 'GL IP-ANALYTICS' application window. The 'L3 Protocols' tab is selected in the left sidebar. The main table displays the following data:

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv4 - (0x800)	28,419,913	16,677,921,882	6,539,530,100.38	99.59	99.92
2	ARP - (0x806)	53,921	3,450,944	1,353,139.33	0.19	0.02
3	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0
6	0xaa	455	85,540	33,540.83	0.0	0.0

Total entries: 6

Navigation buttons: Previous, Next, Export Tab as CSV

Applying Filter

- Filter the required data by specifying filter expression syntax for Outer and Tunneled protocol statistics
- In this example, filter is applied for IPv4 end points by providing following expression “ip.addr==192.168.12.92”, click on the right arrow button to filter the data

The screenshot displays the GL IP-ANALYTICS application interface. On the left, a navigation pane shows a tree structure under 'Ports', with 'IPv4 Endpoints' selected. The main area contains a table titled 'IPv4 Endpoints' with 12 rows of data. Below the table, a 'Filter section' contains a text input field with the expression 'ip.addr==192.168.12.92', a right-pointing arrow button, an 'Erase' button, and a dropdown menu currently set to 'inner port'. A progress bar at the bottom right indicates 'Analysing IPv4 Endpoints'.

Row ID	IP Address	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets
1	104.44.49.142	30	2,220	0	0	1.47	870.47	0.00	0.00	30
2	34.111.50.114	304	99,024	208	22,656	14.90	38,828.00	10.19	8,883.57	512
3	91.189.91.49	585	67,905	900	75,915	28.67	26,626.02	44.11	29,766.80	1,485
4	202.83.26.121	1,985	1,134,827	646	67,757	97.29	444,973.62	31.66	26,567.99	2,631
5	192.168.12.210	4,001	615,250	2,792	742,619	196.10	241,243.83	136.84	291,186.11	6,793
6	142.250.4.188	655	46,098	655	42,540	32.10	18,075.34	32.10	16,680.23	1,310
7	142.250.196.65	1,305	1,635,945	780	70,590	63.96	641,465.50	38.23	27,678.83	2,085
8	192.168.1.25	3,653	318,478	3,224	261,370	179.04	124,877.45	158.01	102,485.00	6,877
9	192.168.255.255	0	0	318	27,762	0.00	0.00	15.58	10,885.67	318
10	192.168.12.208	1,155	280,770	0	0	56.61	110,091.88	0.00	0.00	1,155
11	35.224.170.84	390	37,380	510	41,580	19.11	14,656.96	24.99	16,303.80	900
12	52.97.202.18	165	92,445	225	42,960	8.08	36,248.33	11.02	16,844.91	390

Display of Applied Filter

- Observe the applied filter is as shown below

The screenshot displays the GL IP-ANALYTICS application window. The interface includes a sidebar with navigation options, a main data table, and a filter section at the bottom.

GL IP-ANALYTICS

Select file Select folder Export analysed tabs

IPv4 Endpoints

Row ID	IP Address	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets
1	192.168.12.92	2,550	487,640	150	27,540	126.03	192,813.27	7.41	10,889.33	2,700
2	224.0.0.251	0	0	917	140,773	0.00	0.00	45.32	55,661.76	917
3	255.255.255.255	0	0	90	11,610	0.00	0.00	4.44	4,590.60	90
4	224.0.0.22	0	0	180	11,520	0.00	0.00	8.89	4,555.01	180
5	192.168.15.255	0	0	46	11,362	0.00	0.00	2.27	4,492.54	46
6	192.168.1.3	150	27,540	210	26,535	7.41	10,889.33	10.37	10,491.96	360
7	239.255.255.250	0	0	1,107	285,840	0.00	0.00	54.71	113,021.38	1,107

Total entries: 7 Previous Next Export Tab as CSV

Filter section

ip.addr==192.168.12.92 Erase inner port

Exporting Analyzed Tabs to CSV File Format

The screenshot displays the GL IP-ANALYTICS application window. At the top right, the 'Export analysed tabs' button is highlighted with a red box. The main content area shows a table titled 'L3 Protocols' with the following data:

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
2	IPv4 - (0x800)	28,419,913	16,677,921,882	6,539,530,100.38	99.59	99.92
3	ARP - (0x806)	53,921	3,450,944	1,353,139.33	0.19	0.02
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	0xaa	455	85,540	33,540.83	0.0	0.0
6	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0

Below the table, there are navigation buttons: 'Previous', 'Next', and 'Export Tab as CSV'. The 'Export Tab as CSV' button is highlighted. The interface also includes a 'Filter section' at the bottom with an input field, a right arrow button, and an 'Erase' button.

Export Tabs as CSV

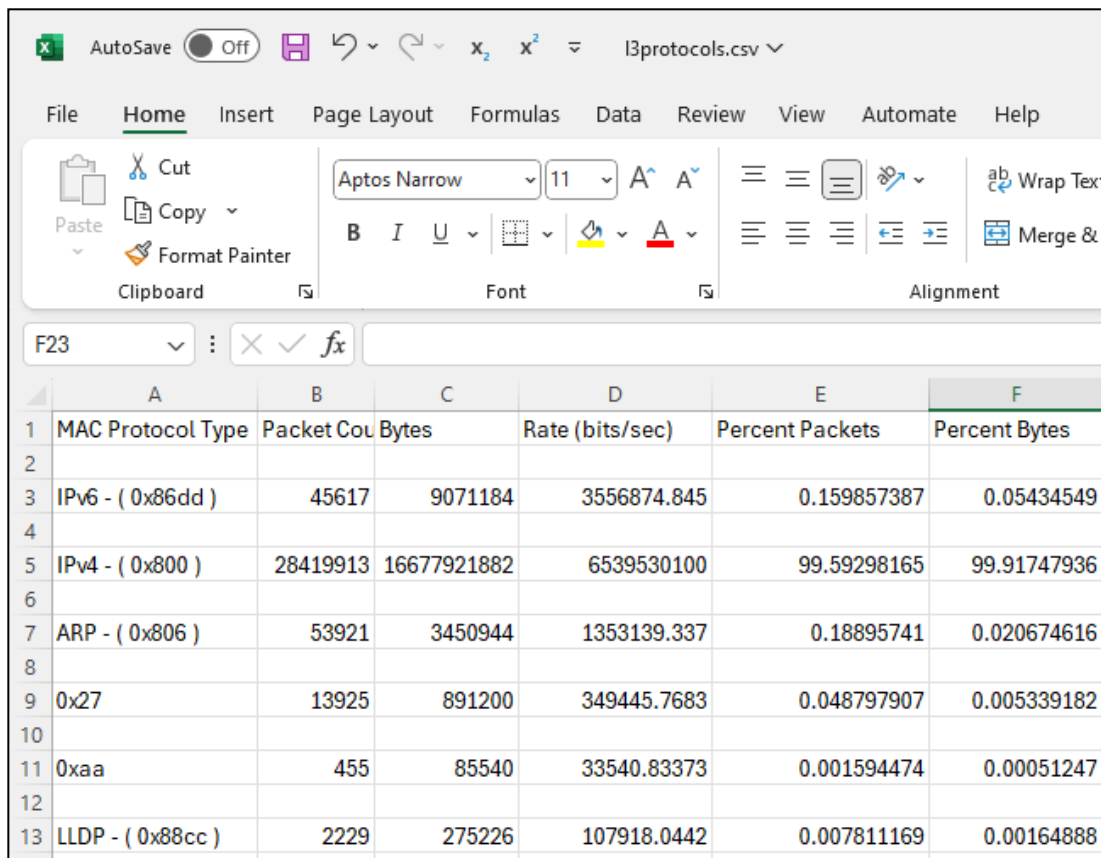
The screenshot displays the GL IP-ANALYTICS application window. On the left, a sidebar menu lists various protocol categories, with 'L3 Protocols' selected. The main area shows a table with the following data:

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
2	IPv4 - (0x800)	28,419,913	16,677,921,882	6,539,530,100.38	99.59	99.92
3	ARP - (0x806)	53,921	3,450,944	1,353,139.33	0.19	0.02
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	0xaa	455	85,540	33,540.83	0.0	0.0
6	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0

Below the table, there is a 'Total entries: 6' label and navigation buttons for 'Previous', 'Next', and 'Export Tab as CSV'. The 'Export Tab as CSV' button is highlighted with a red border. At the bottom, there is a 'Filter section' with an input field, a right-pointing arrow button, an 'Erase' button, and another input field.

Export Tab to CSV (Contd.)

- The sample exported CSV file is shown below



The screenshot shows the Microsoft Excel interface with the 'Home' tab selected. The ribbon includes options for Clipboard, Font, and Alignment. The active cell is F23. The table below displays network protocol statistics for various protocols.

	A	B	C	D	E	F
1	MAC Protocol Type	Packet Cou	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
2						
3	IPv6 - (0x86dd)	45617	9071184	3556874.845	0.159857387	0.05434549
4						
5	IPv4 - (0x800)	28419913	16677921882	6539530100	99.59298165	99.91747936
6						
7	ARP - (0x806)	53921	3450944	1353139.337	0.18895741	0.020674616
8						
9	0x27	13925	891200	349445.7683	0.048797907	0.005339182
10						
11	0xaa	455	85540	33540.83373	0.001594474	0.00051247
12						
13	LLDP - (0x88cc)	2229	275226	107918.0442	0.007811169	0.00164888

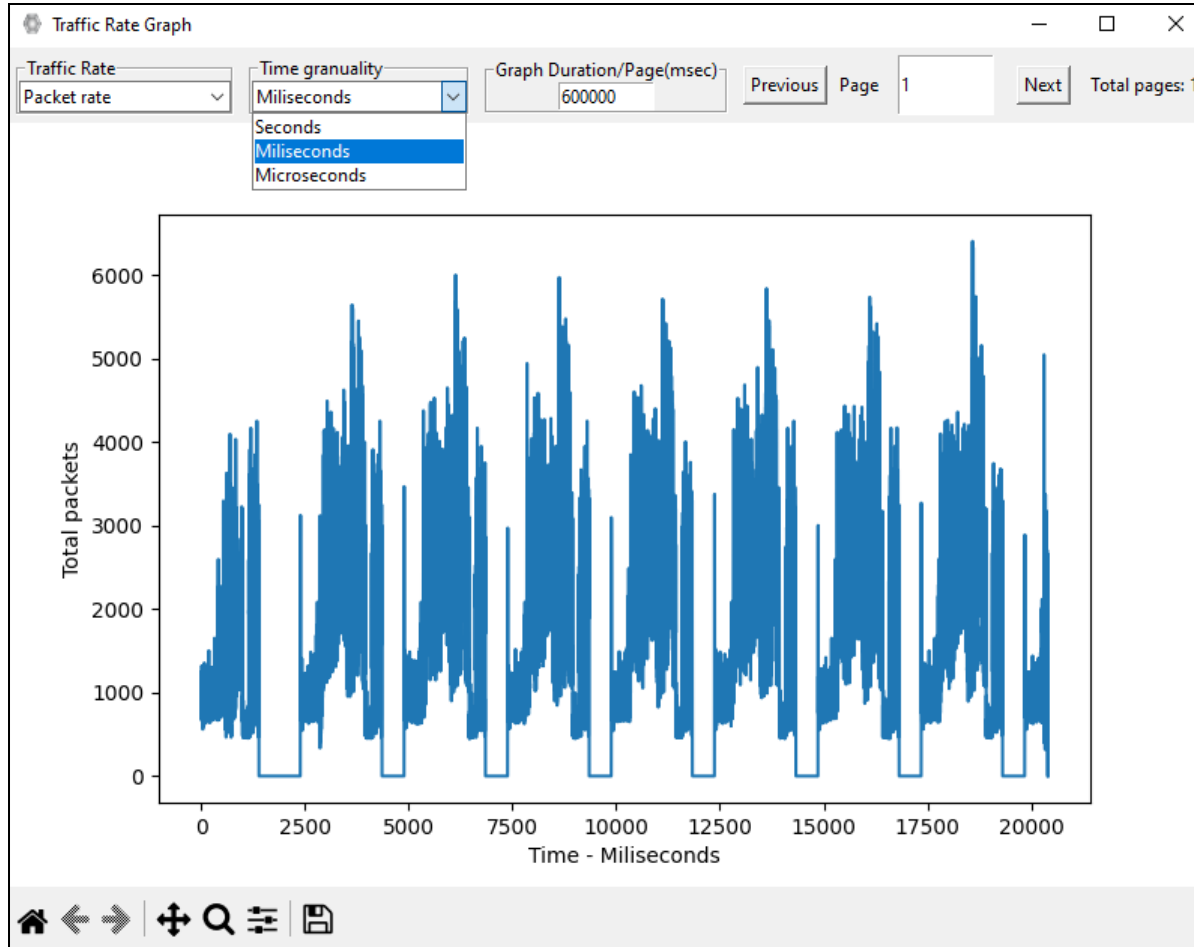
Data Analysis Graph

- Right-click on the selected row, and choose **Display graph** to view the Data and Rate graphs

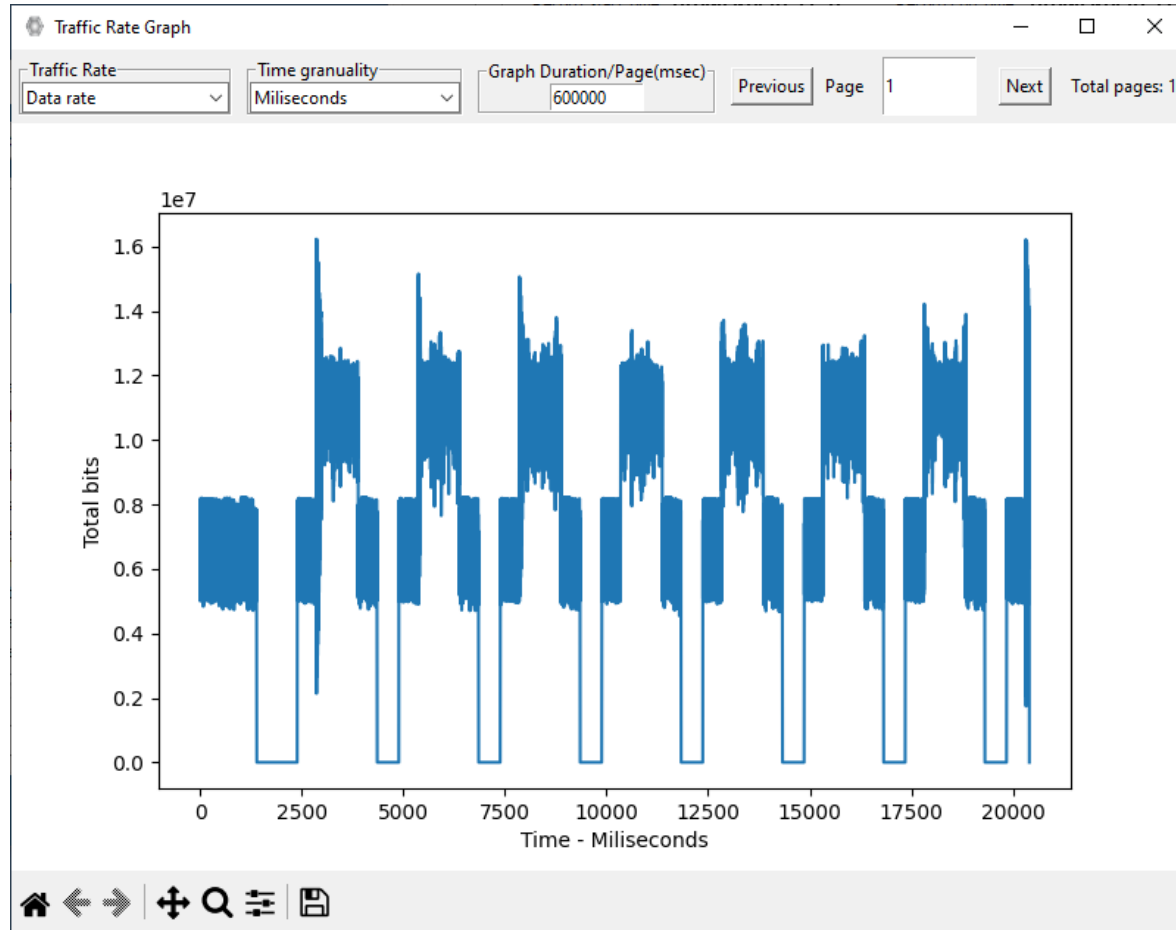
The screenshot shows the GL IP-ANALYTICS application window. On the left is a navigation menu with categories like 'Ports', 'Protocol Statistics', 'L3 Protocols', 'L4 Protocols', 'DSCP', 'IPv4 Endpoints', 'IPv4 Conversations', 'IPv6 Endpoints', 'IPv6 Conversations', 'TCP Endpoints', 'UDP Endpoints', 'UDP Conversations', 'TCP Conversations', 'SCTP Conversations', and 'PING Conversations'. The main area displays a table titled 'L3 Protocols' with columns: Row ID, MAC Protocol Type, Packet Count, Bytes, Rate (bits/sec), Percent Packets, and Percent Bytes. Row 2 is selected, and a 'Display graph' button is overlaid on the 'Packet Count' cell. At the bottom, there is a 'Filter section' with an input field, a right arrow button, and an 'Erase' button. The bottom right of the window has 'Previous', 'Next', and 'Export Tab as CSV' buttons.

Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
2	IPv4 - (0x800)	28,410,012	16,677,921,882	6,539,530,100.38	99.59	99.92
3	ARP - (0x806)		3,450,944	1,353,139.33	0.19	0.02
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	0xaa	455	85,540	33,540.83	0.0	0.0
6	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0

Display of Packet Rate Over Time Graph

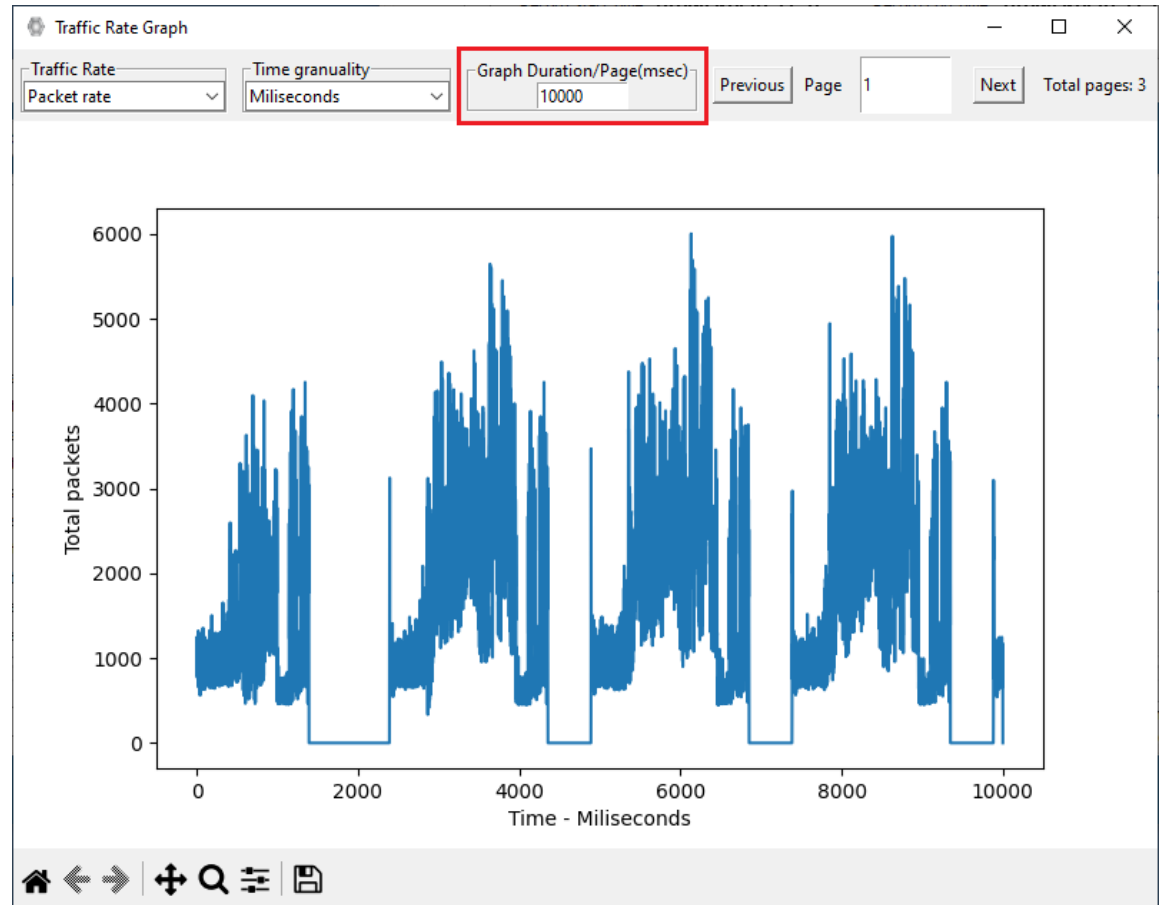


Display of Data Rate Over Time Graph



Graph Duration/Page(msec) Option

- Enter **Graph Duration/Page(msec)** to change the time interval (by default, graph duration is set to **600000**) as required and click on **Enter**
- In this case, the time interval is set to 10000 msec. The graph will be displayed up to the specified time interval (**10000** msec). Refer to the screenshot



Rate Analysis

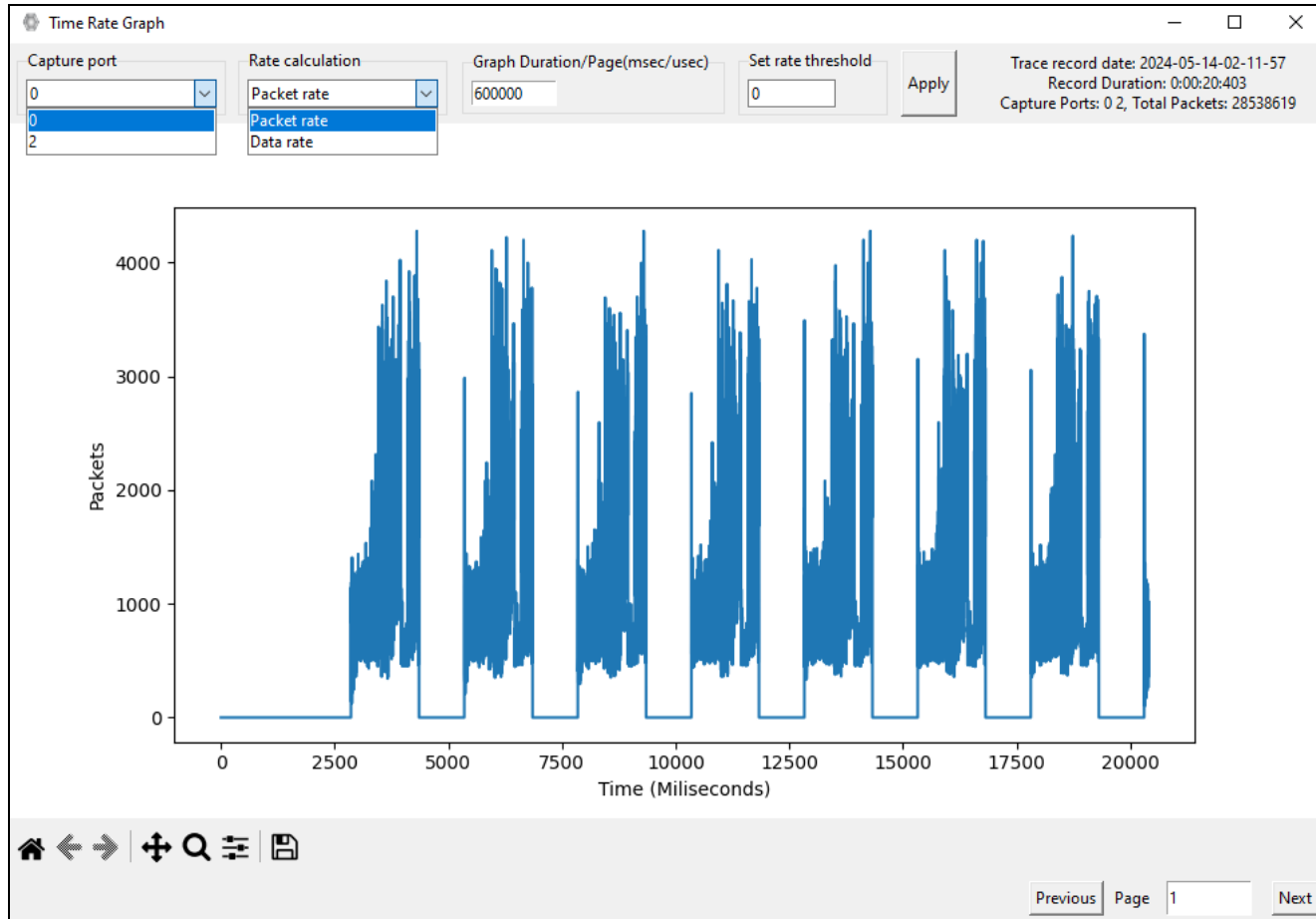
Rate Analysis in PacketExtractor™

- Users can perform **Rate Analysis** using the PacketExtractor™ application

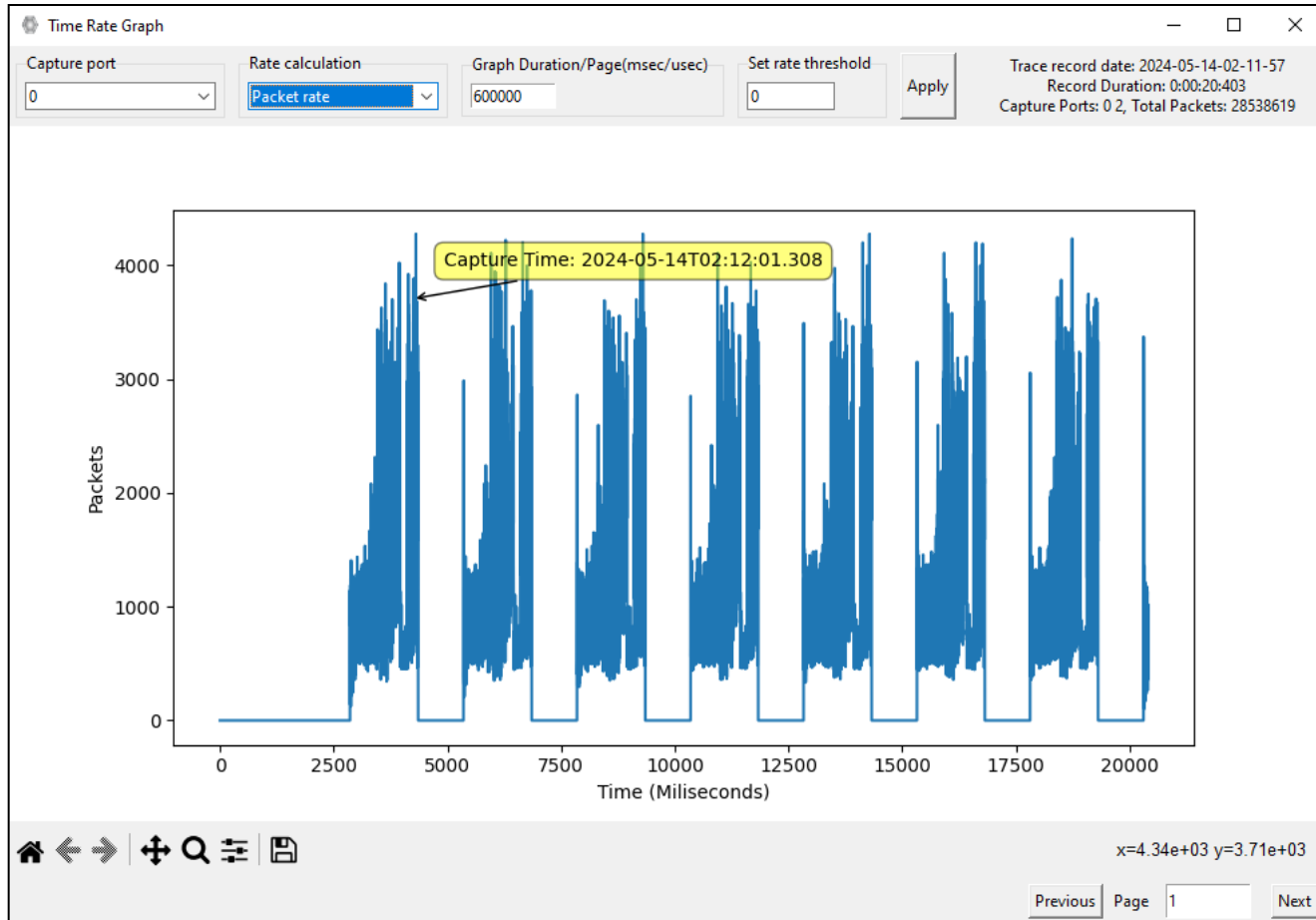
The screenshot displays the PacketExtractor application window. The 'Record Statistics' tab is active, showing recording information for a record named 'Data_Analysis_and_Rate_Analysis'. The recording started at 2024-03-11 05:28:27 and ended at 05:28:54, with a duration of 00:00:27 and a size of 16.000 GB. The 'Limit Criteria' section is set to 'All' with a limit value of 0. The 'Extraction Filter' dropdown is set to 'Rate Analysis', which is highlighted with a red box. The 'Destination File Name' is 'D:\Rate-Analysis\Rate-Analysis.hdf5'. The 'Start' and 'Stop' buttons are visible. The 'Statistics' table at the bottom shows the following data:

Description	Value
Extractor status	Extracting, Please wait....
Extracted Frames	19 281 616
Extracted Bytes (MB)	12 530.099
Extracted Rate (Mbps)	67955.01
Duration (mm:ss)	0::1
Frames with FCS Error	0

Time Rate Graph

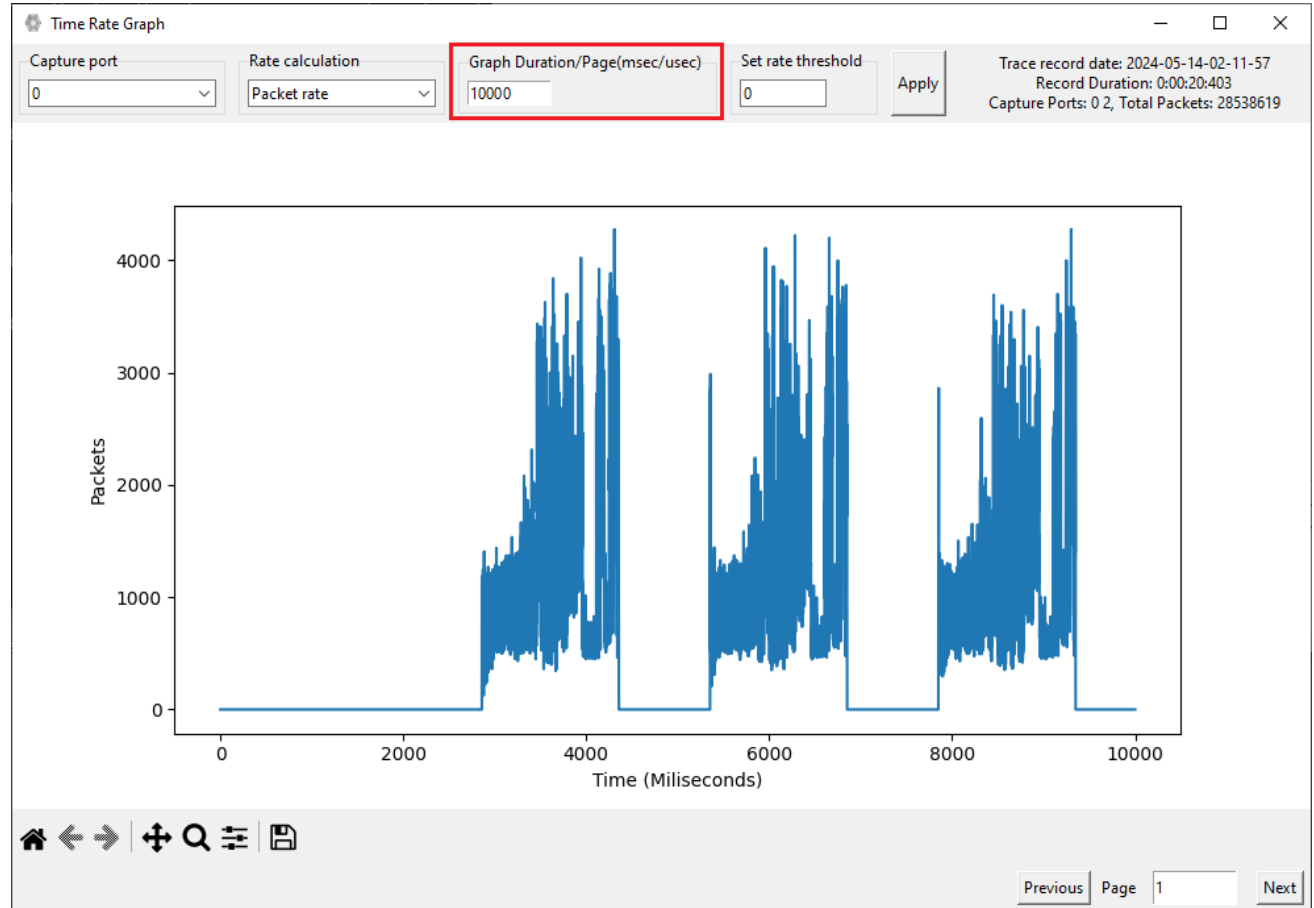


Display of Capture Timestamp



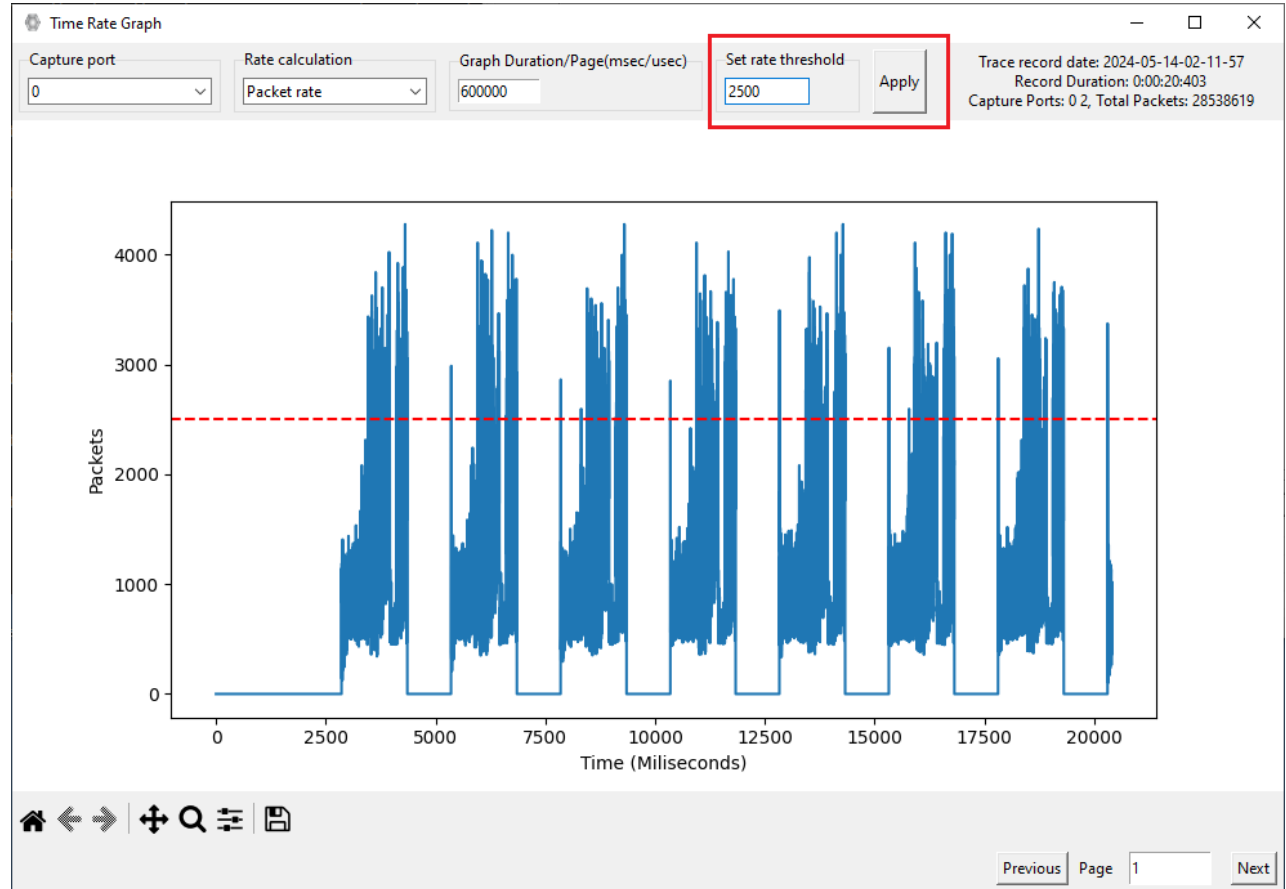
Graph Duration/Page

- In this case, the time interval is set to **10000** msec. The graph will be displayed up to the specified time interval (10000 msec)



Rate Threshold

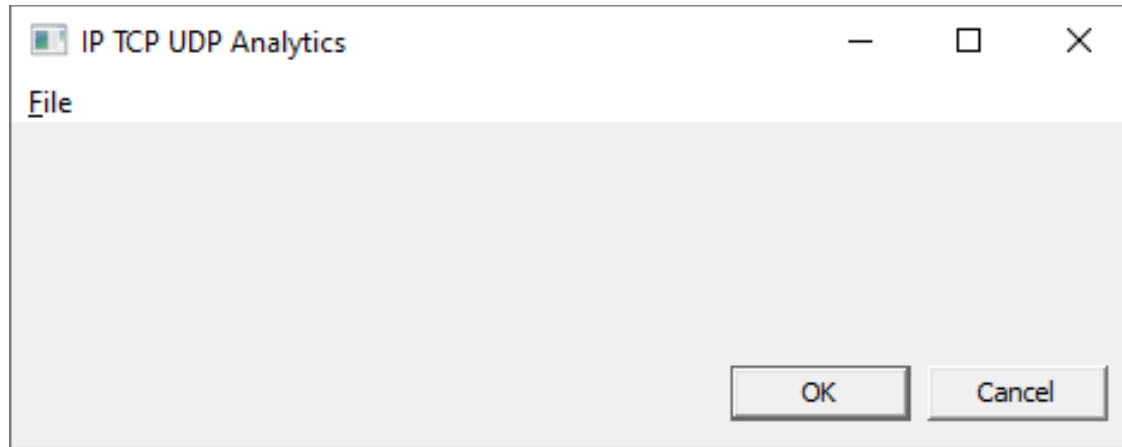
- Enables users to define a threshold value for displaying a horizontal line across the y-axis
- This allows users to easily visualize rates exceeding the threshold.
- Enter the desired Rate Threshold and click on **Apply**. Observe the plotted threshold line for the configured rate as depicted



Data Analysis using IP TCP UDP Tool

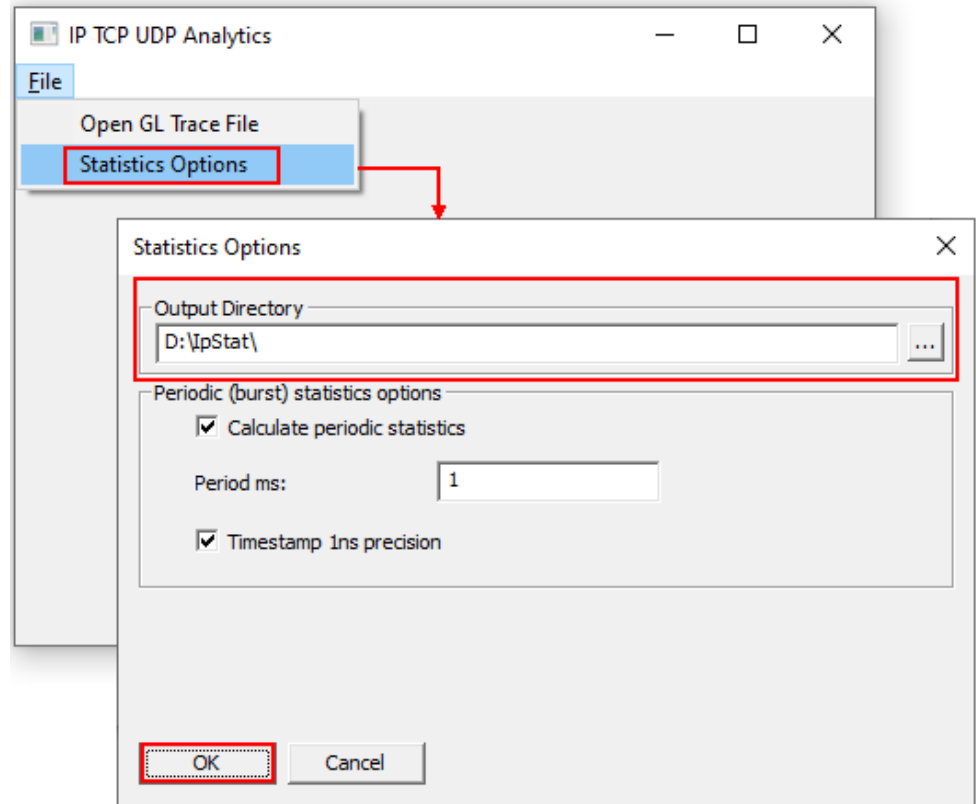
Invoking IP TCP UDP Analysis Tool

- **IP TCP UDP Analysis tool** is used to convert *.hdl file to *.csv file format
- Go to the following path “**C:\Program Files\GL Communications Inc\FastRecorderAndPlayback**”
- Right-click on **IpTcpUdpAn.exe** and select **Run as Administrator** option to run the application
- The **IP TCP UDP Analytics** window appears as shown



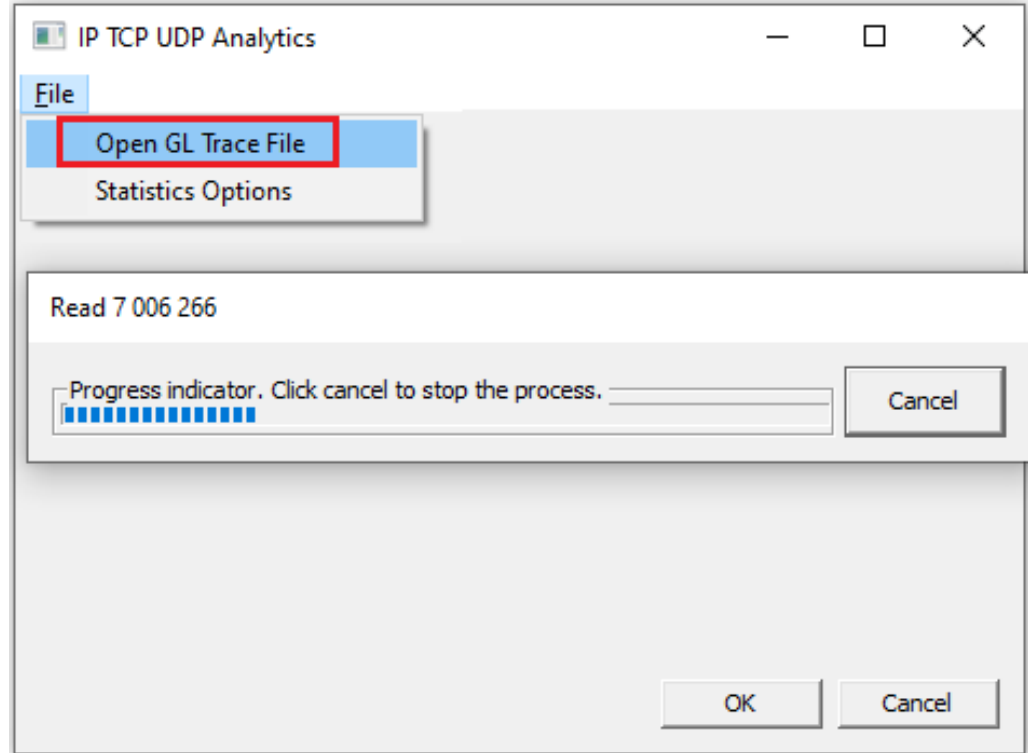
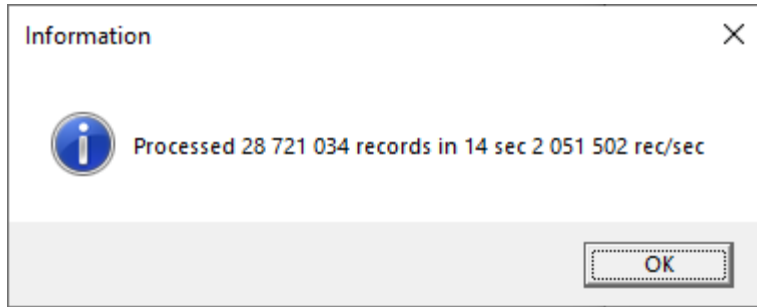
Configuring IP TCP UDP Analysis Tool

- In the **IP TCP UDP Analytics** window, configure the parameters as required



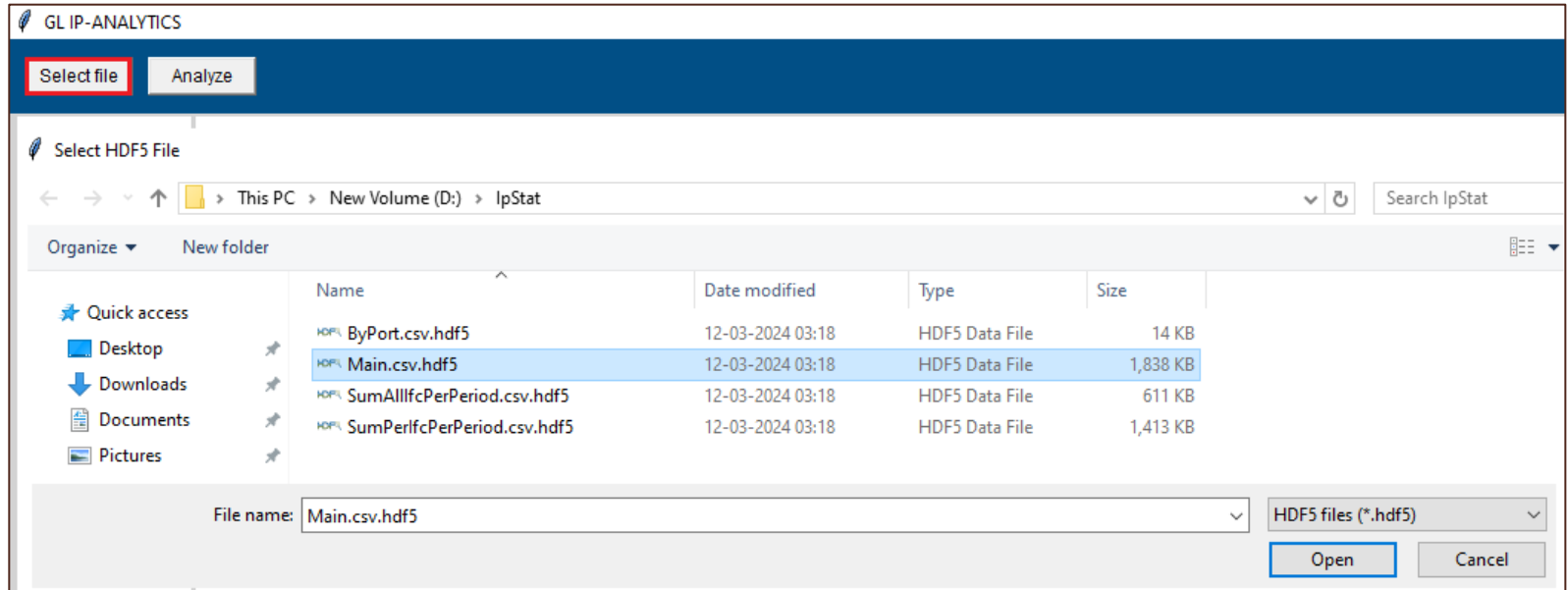
Configuring IP TCP UDP Analysis Tool (Contd.)

- Go to **File** → **Open GL Trace File** to browse and select the extracted *.hdl file. In this instance, the *.hdl file is selected as **Data-Analysis.hdl**
- Observe the Progress indicator
- After converting the extracted *.hdl file to csv, the below message will pop-up. Click on **OK** to continue



GL IP Analytics™

- Upon execution of Python scripts, this will invoke the **GL IP-ANALYTICS™** window. Click on **Select File** button to browse and select *.hdf5 file. In this instance, the **D:\IpStat\ Main.csv.hdf5** file is selected



GL IP Analytics™ (Contd.)

- Click on **Analyze**. This analysis will display L3, COS, L4, IPv4 Endpoints, IPv6 Endpoints, UDP Endpoints, TCP Endpoints, and Ports statistics. Observe the progress bar at the bottom left side indicating the progress
- After completion, observe the statistics as shown below is selected

The screenshot displays the GL IP-ANALYTICS application window. The title bar reads "GL IP-ANALYTICS". The interface includes a dark blue header with "Select file" and "Analyze" buttons (the latter is highlighted with a red box), and an "Export all Tabs" button on the right. On the left, a sidebar lists various analysis categories with checkboxes: L3 Protocols, COS, L4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, and Ports, all of which are checked. The main area contains a table with columns: L3 Protocol, COS, L4 Protocol, IPv4 EndPoints, IPv6 EndPoints, TCP EndPoints, UDP EndPoints, Ports, Sequence Number, MacProt, Packet Count, Bytes, Percent Packets, and Percent Bytes. The table shows two rows of data. At the bottom, there are "Previous", "Export Tab as CSV", and "Next" buttons.

L3 Protocol	COS	L4 Protocol	IPv4 EndPoints	IPv6 EndPoints	TCP EndPoints	UDP EndPoints	Ports	Sequence Number	MacProt	Packet Count	Bytes	Percent Packets	Percent Bytes
								1	IPv6	46654	8970058	0.16284	0.05415
								2	IPv4	28603331	16554782924	99.83716	99.94585

Rate Analysis using IP TCP UDP Tool

Rate Analysis using IP TCP UDP Tool

- Users can use the existing HDL format. If not, extract the recorded data into *.hdl format using PacketExtractor™ application

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

Select Recording

Extractor Record Statistics

Recording Information

Record Name: Data_Analysis_and_Rate_Analysis

Record Start Time: 2024-03-11 05:28:27 Record End Time: 2024-03-11 05:28:54

Record Duration: 00:00:27 Record Size: 16.000 GB

PreExtraction Filter

Start Time: 05:28:27 End Time: 05:28:54 HH:MM:SS

Limit Criteria

All Duration Extracted Size Extracted Packet Count

Limit Value: 0

Recorded Ports: 0 2

Port Filter

Port: Example: 0 or 0-3 or 0,1,2 or 2,5-7

Extraction Filter

Operation: Packet Extraction Multiple Files

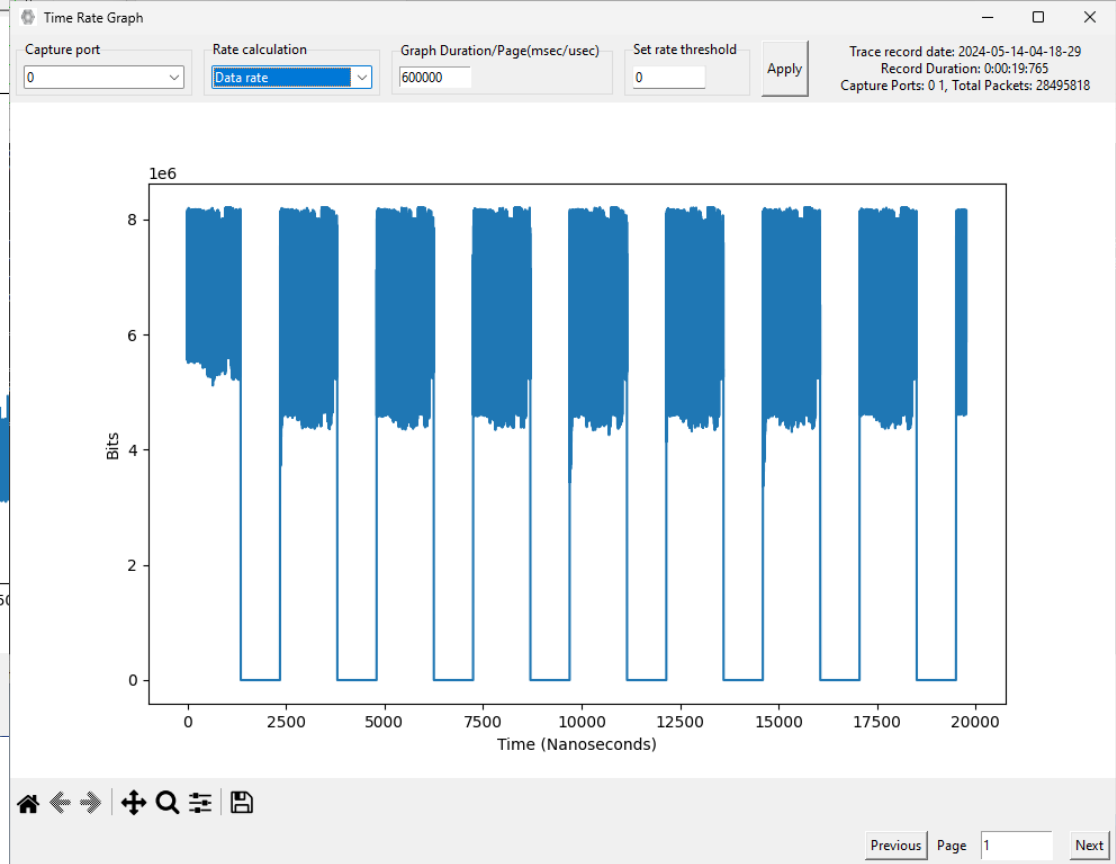
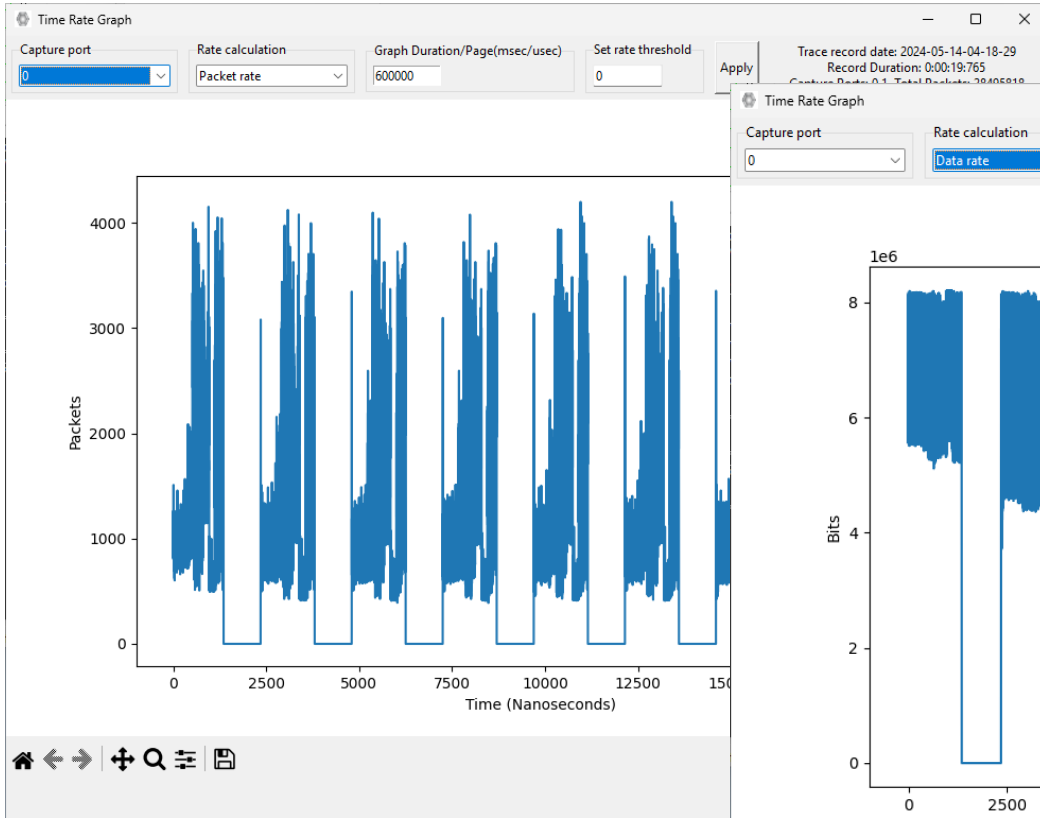
Destination File Name: D:\Data-Analysis.hdl

Compress Extracted Files Packet Slicing

Statistics

Description	Value
Extractor status	Extracting, Please wait....
Processed Frames	3 255 894
Extracted Frames	3 255 976 (100.00 %)
Processed Bytes (MB)	1 900.537
Extracted Bytes (MB)	1 888.226
Processed Rate (Mbps)	7407.06
Extracted Rate (Mbps)	7353.21
Duration (mm:ss)	0::3
Frames with FCS Error	0

Packet Rate and Data Rate Graphs



Thank you