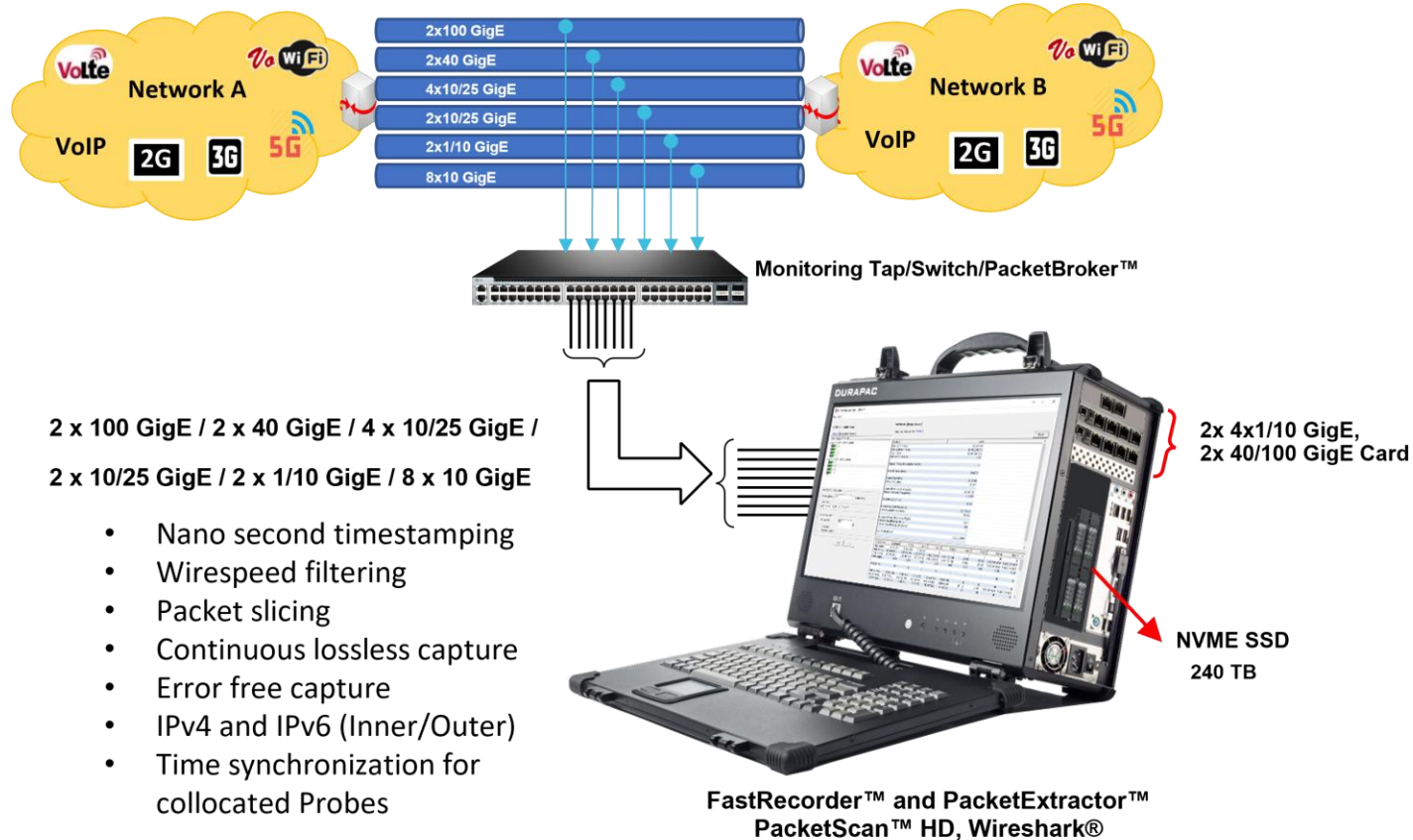

FastRecorder™ and PacketExtractor™ for Monitoring IP Networks



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



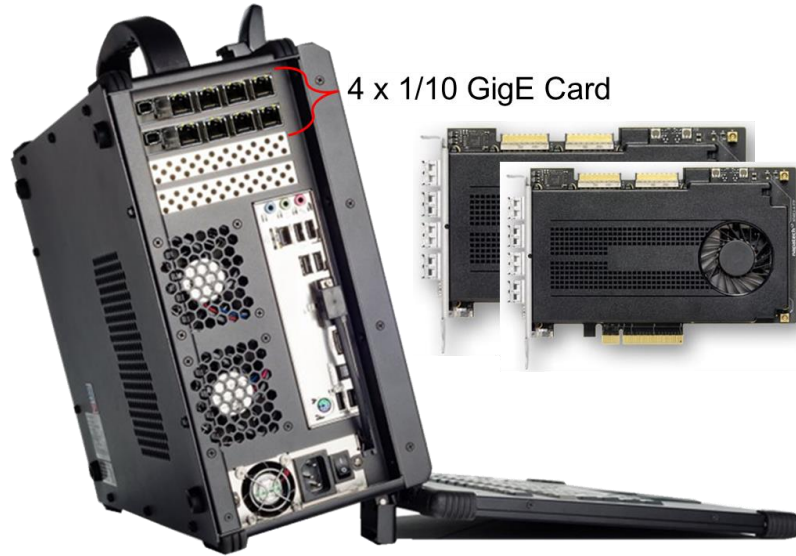
PacketScan™ HD, FastRecorder™ & PacketExtractor™

(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)



4 x 1/10 GigE Card

PacketScan™ HD - Lunch Box



Lunchbox specs are:

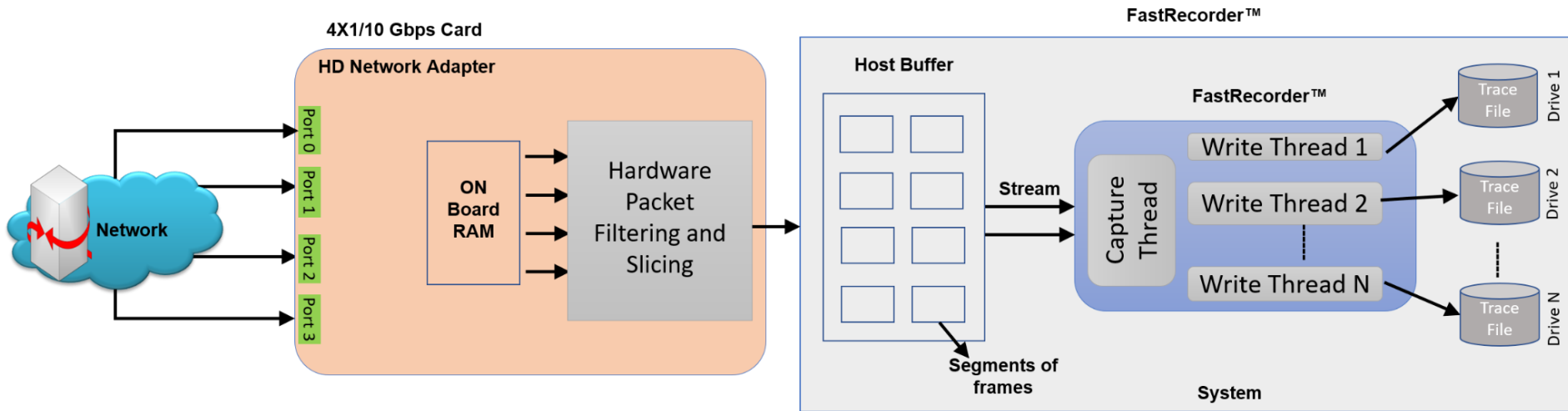
- Intel Xeon Silver 4210
- 64GB RAM
- 500GB SSD for OS
- 4x 3.84TB NVME SSD



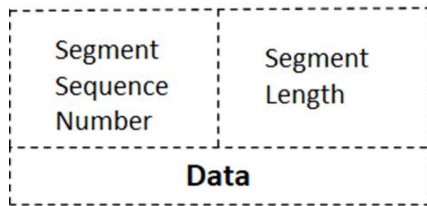
What the Software Does?

- 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
- BERT verification analyzes the received BERT pattern and provides various vital measurements

FastRecorder™ Architecture

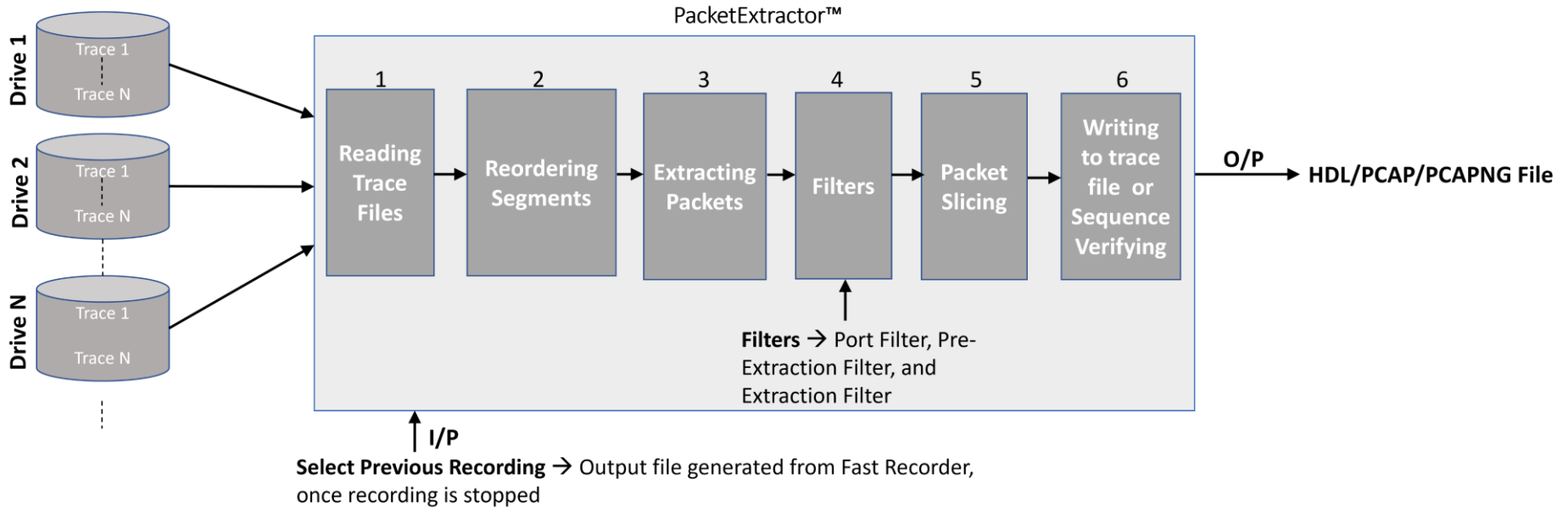


Buffer segments stored internally in files:



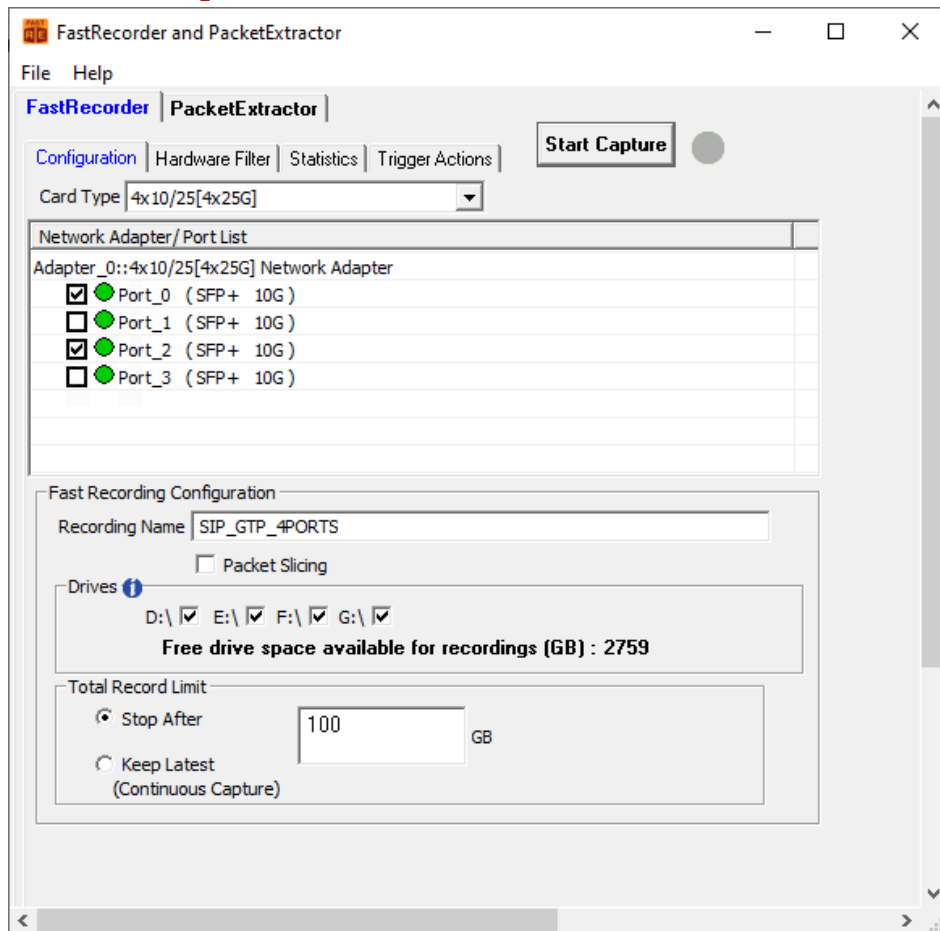
Segment Sequence Number and Segment Length is used while analysing/ Re-assembling the segments in Packet Extractor.

PacketExtractor™ Architecture



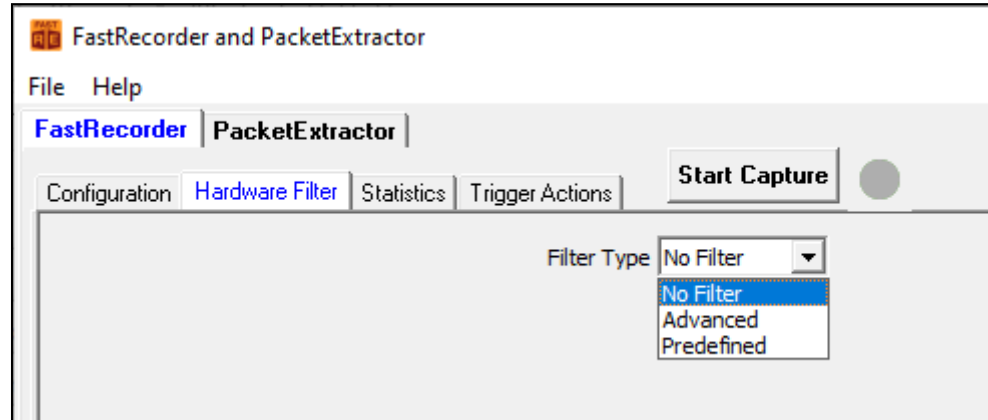
FastRecorder™ Operations

- 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, showing a configuration for an 'Advanced' filter. The filter is named 'F1' and is based on the 'IP List' field. The configuration includes a table for filter rules, a list of filters on the left, and a detailed view of the selected filter's parameters and expressions.

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

Filters:

- Filter - 1
- Filter - 2
- Filter - 3
- Filter - 4
- Filter - 5
- Filter - 6
- Filter - 7
- Filter - 8
- Filter - 9
- Filter - 10

IP List Type: IP Address List | IP Layer Type: Tunnel-1 IP

IP Address: FE80:0:0:1000:1000:1000:3003

Buttons: Add, Edit, Delete, Update

Tunnel Type: GTP, GRE, VXLAN

Custom Expression: [Empty]

Selected Filter Expression:

```
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 ((InnerLayer3Protocol ==
```

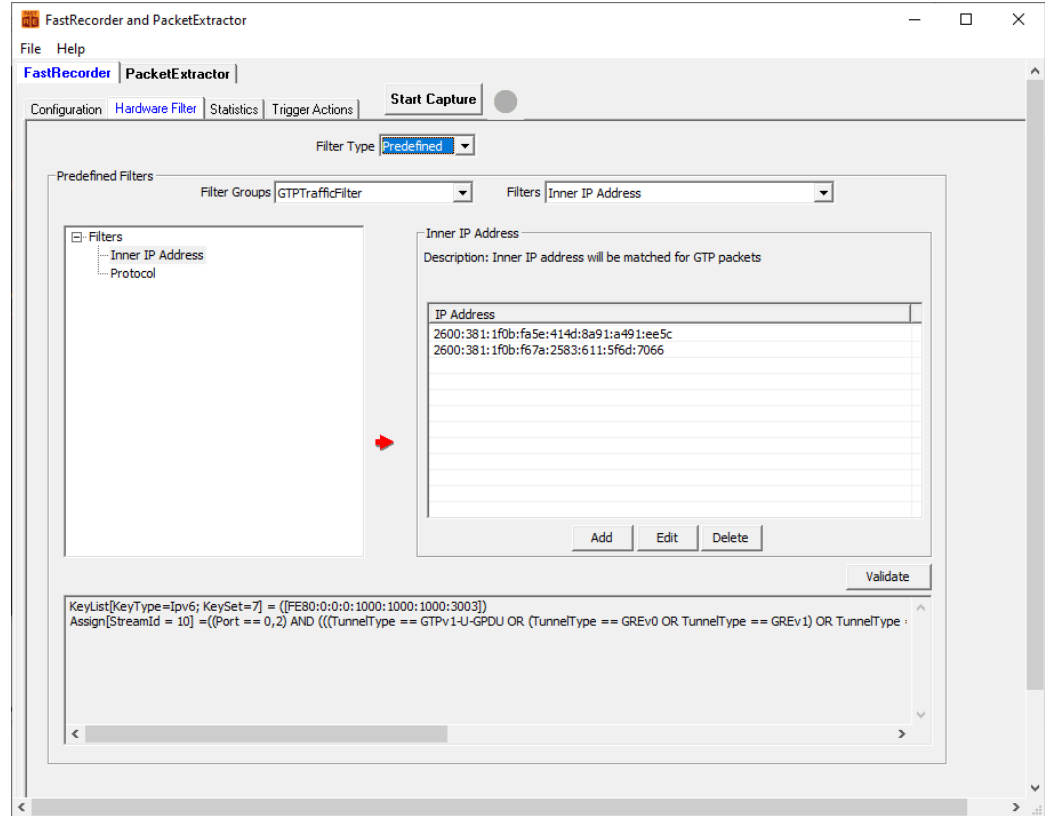
Final Configured Expressions | Final Applied Expressions

```
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 ((InnerLayer3Protocol ==
```

Clear All Filters

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 several filters, with 'F4' selected. Below the table, a 'Custom Expression' is defined as '(f2 && f4) || f1'. A 'Validate & Update' button is highlighted, and a message indicates '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

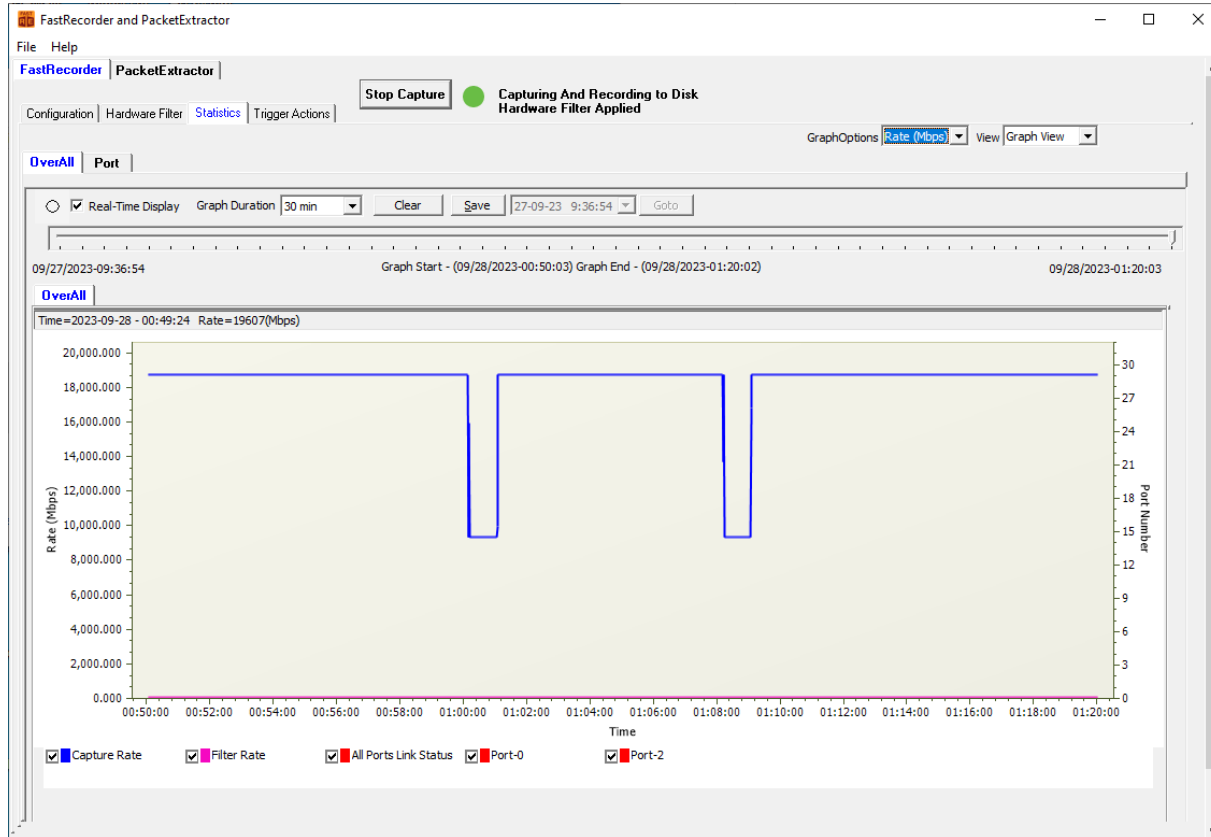
Statistics	Value
Filter Match Frames	58 447 757
Filter Not Match Frames	0
Total Frames	58 447 757
Filter Match Frames %	100.00
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	15.0000
Capture Rate (Mbps)	10215.26
Filtered Rate (Mbps)	10205.14
Filtered Bytes %	100.00
Capture Frame Rate (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 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	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			

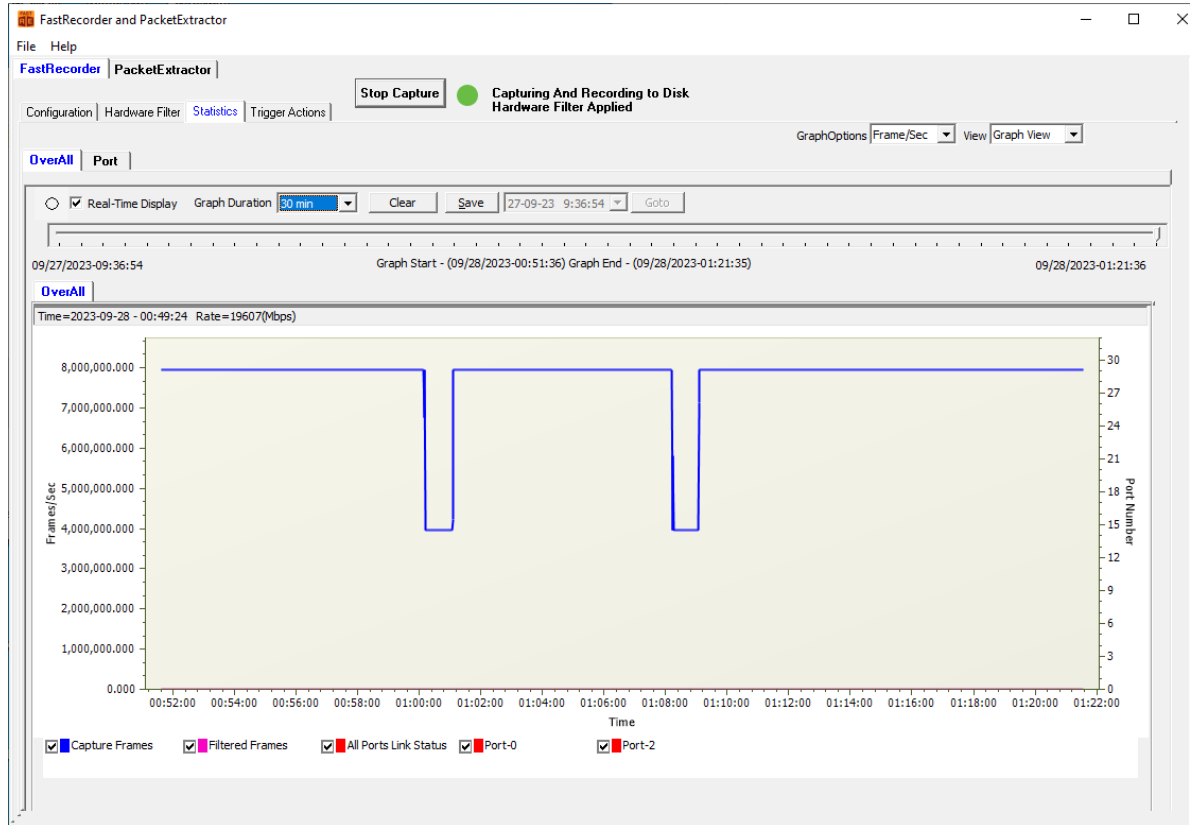
Real time and Historical Graph

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



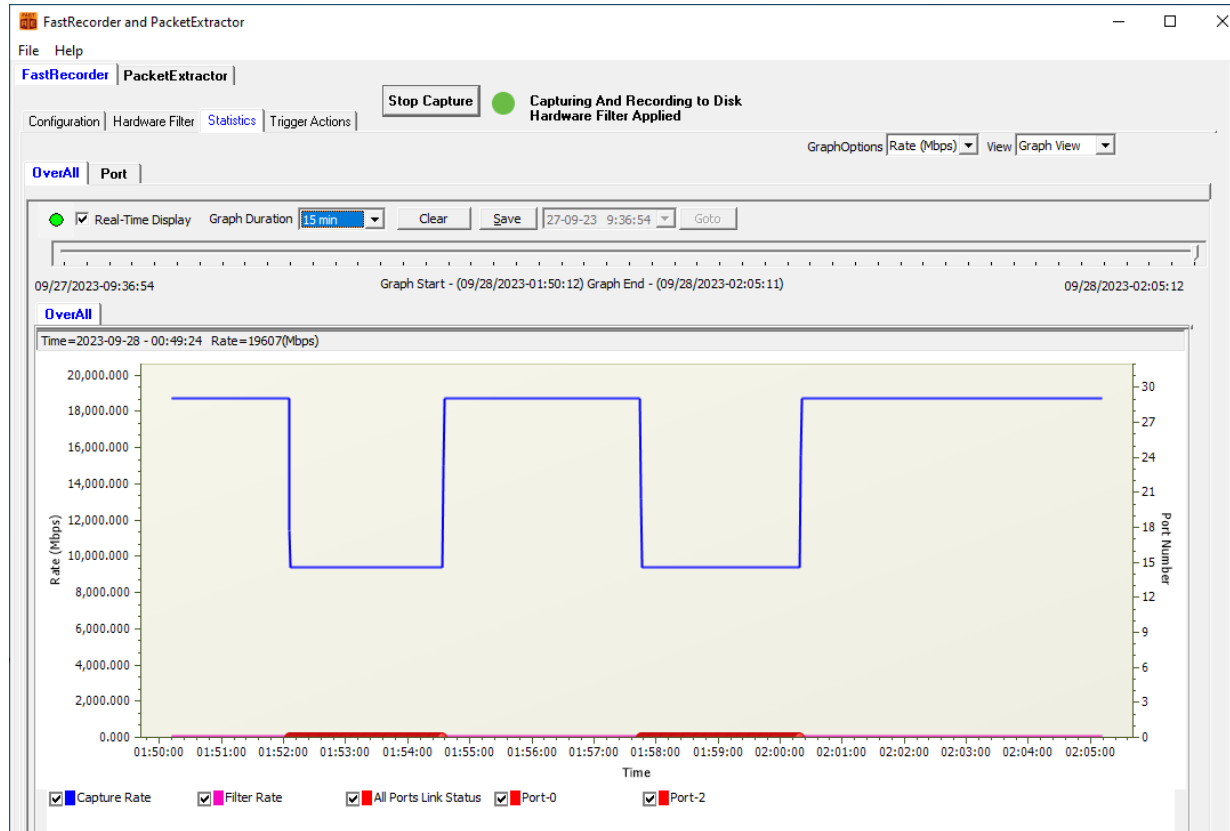
Realtime and Historical Graph (Contd.)

- Overall capture and frame rate for Frame/Secs



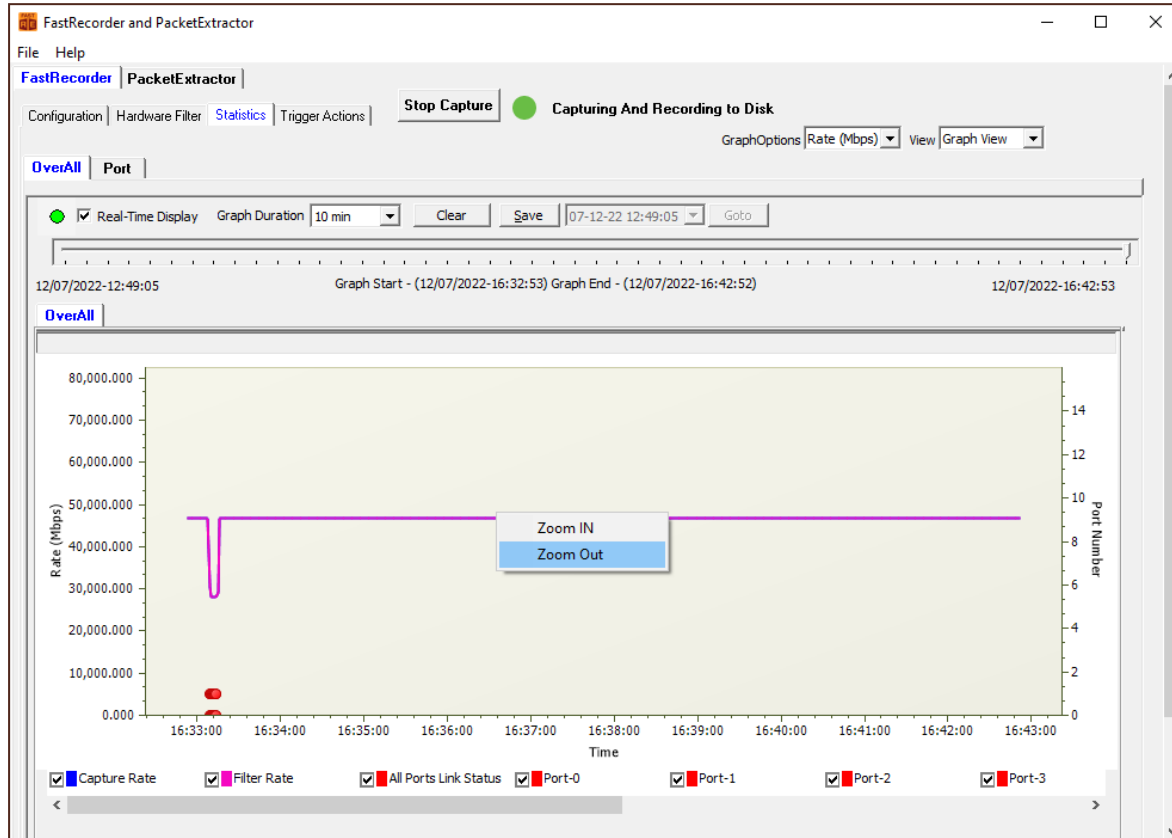
Graphs - Port Link Down

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



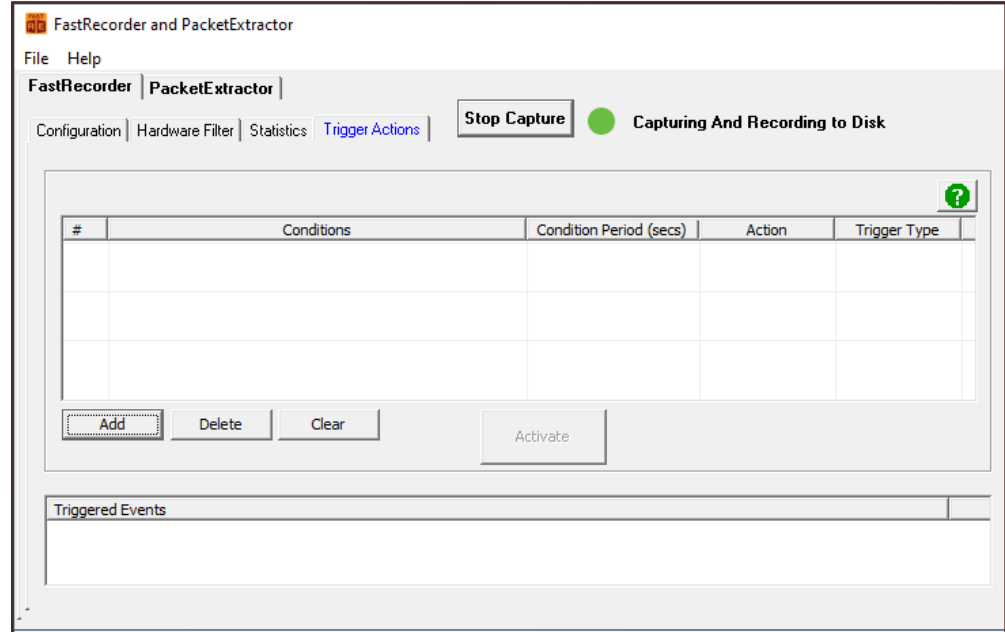
Graphs - Zoom IN and Zoom Out

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



Trigger based Start/Stop Recording

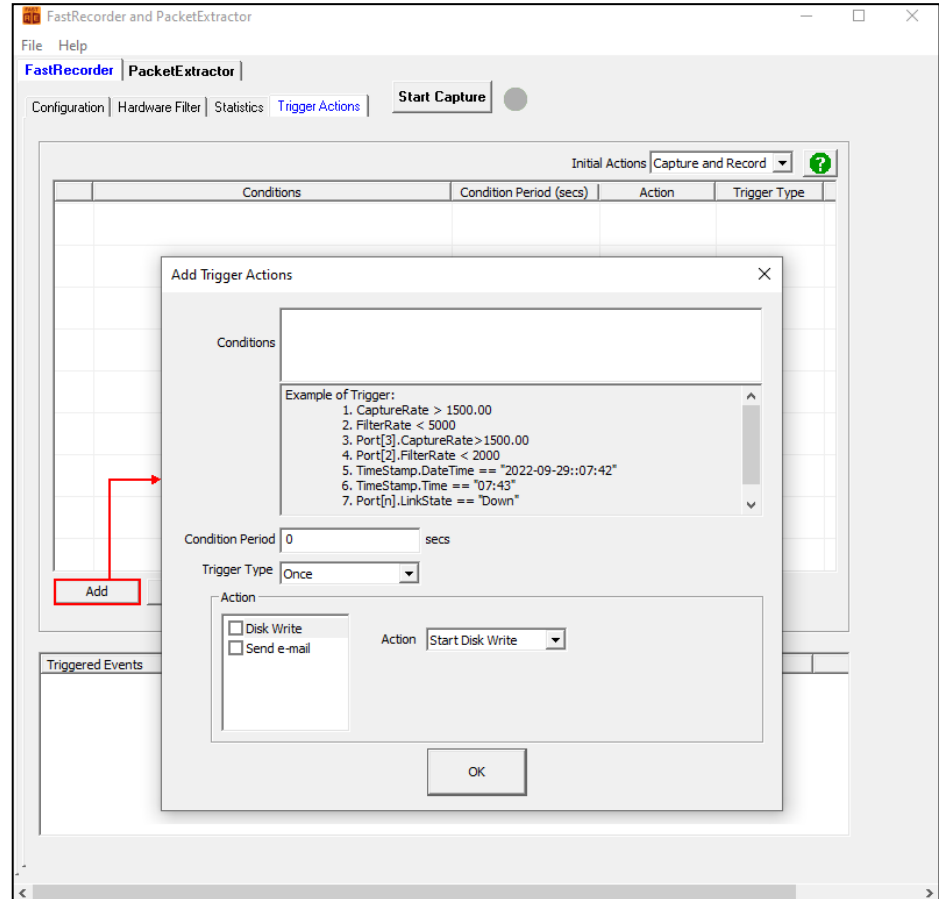
- User can specify the triggers to perform action based on the following conditions
 - CaptureRate (Mbps)
 - FilterRate (Mbps)
 - Port[n].CaptureRate (Mbps)
 - Port[n].FilterRate (Mbps): where n is port number
 - TimeStamp based



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. A yellow circle icon indicates the system is 'Capturing And Waiting for Trigger'. Below the table are buttons for 'Add', 'Delete', 'Clear', and 'Deactivate'. At the bottom, a 'Triggered Events' log 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 displays the 'FastRecorder and PacketExtractor' application window. The 'Trigger Actions' tab is active, showing 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.

FastRecorder and PacketExtractor

File Help

FastRecorder | PacketExtractor

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

Stop Capture Capturing And Recording to Disk

Initial Actions: Capture Only

#	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

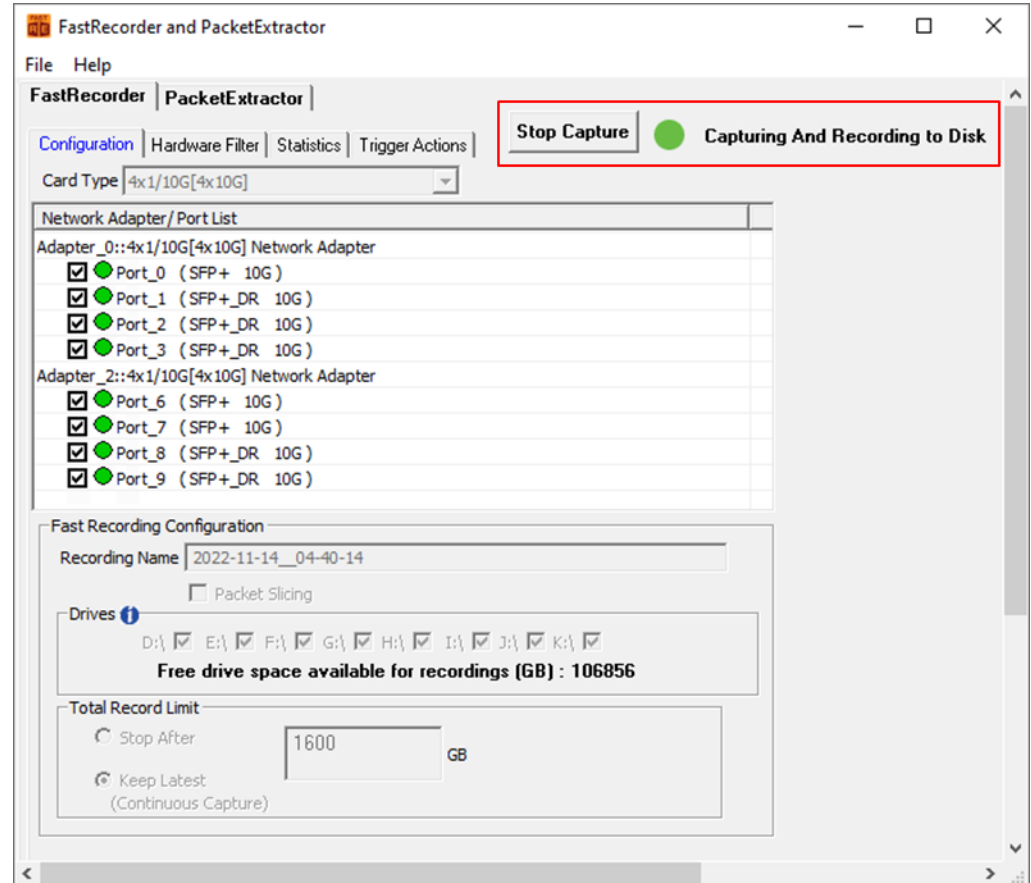
Add Delete Clear Deactivate

Triggered Events

- 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 displays the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, showing the 'Extractor' configuration panel. The 'Recording Information' section indicates the record name is 'SIP_GTP_4PORTS', with a start time of 2023-03-23 06:03:44 and an end time of 2023-03-23 06:11:10. The record duration is 00:07:26 and the record size is 1 048 576.637 MB. The 'PreExtraction Filter' section is currently disabled. The 'Limit Criteria' section has 'Duration' selected with a limit value of 00:07:26. The 'Recorded Ports' field contains '0 2'. The 'Port Filter' section is also disabled, with 'Port' set to '2'. The 'Extraction Filter' section is disabled, with 'Operation' set to 'Packet Extraction', 'Multiple Files' checked, and 'Create New File After' set to 1000 MB. The 'Destination File Name' is 'D:\ExtractTraffic.hdl'. The 'Start' and 'Stop' buttons are visible at the bottom of the configuration panel. The 'Statistics' section at the bottom shows the following results: 'Extraction completed.', 'Processed Frames = 3 538 141 432', 'Processed Bytes = 1 042 150 646 118', 'Extracted Frames = 3 538 141 432 (100.00 %)', 'Extracted Bytes = 1 042 150 646 118', and '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)

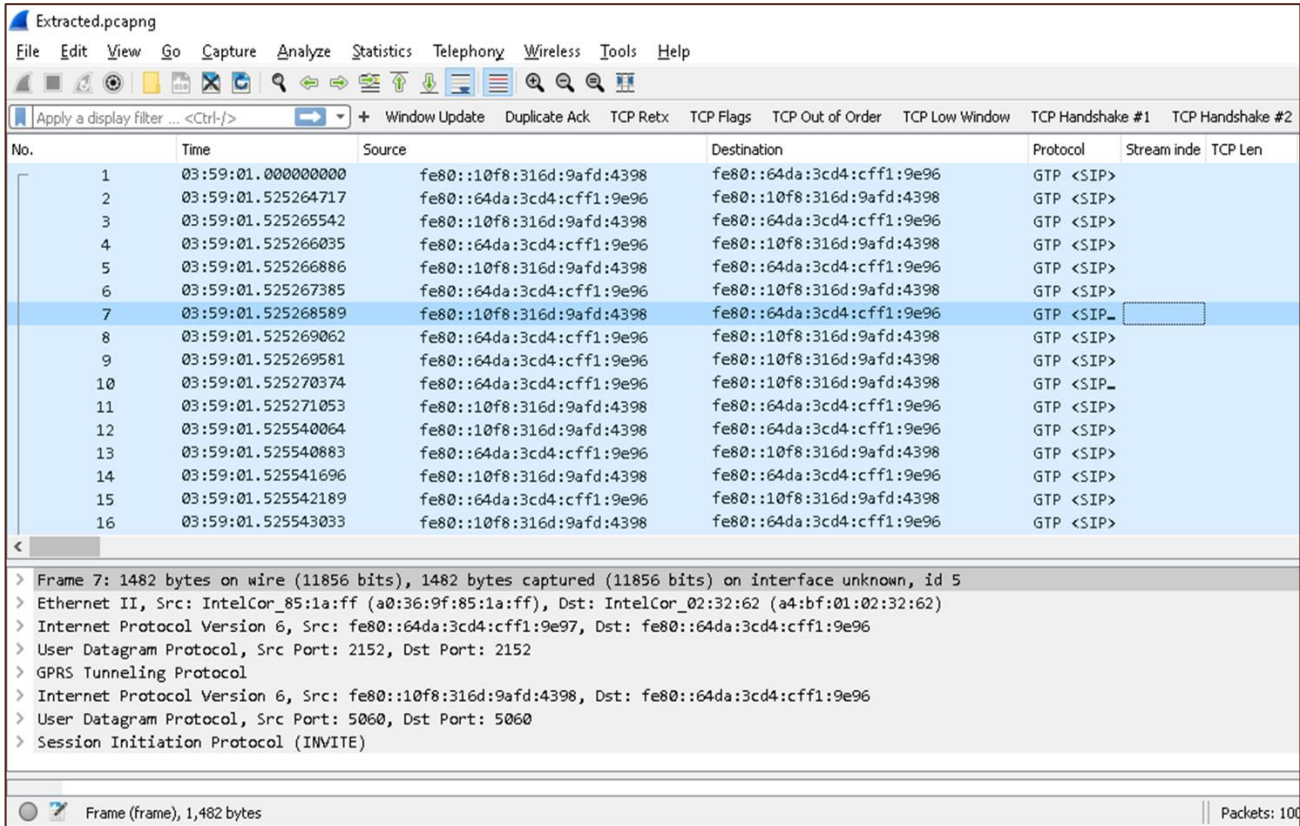
The screenshot displays the PacketScan application interface. The top menu includes File, View, Capture, Statistics, Database, Call Detail Records, Configure, and Help. Below the menu is a toolbar with various icons for file operations and settings. The main window is divided into two panes. The upper pane shows a table of captured frames with columns for Device, Frame#, TIME (Date), Length (Bytes), Error, Length/Protocol Type, Packet Type, Destination IP Address, Source IP Address, Destination Address IPv6, Source Address IPv6, and Dest. The lower pane shows a detailed view of the selected frame (Device2 Frame=1) with fields for Ethernet Frame Data, MAC Layer, IPv6 Layer, Protocol Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, Destination Address, UDP Layer, Source Port, Destination Port, Length (Header + Data), and Checksum.

Device	Frame#	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type	Packet Type	Destination IP Address	Source IP Address	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
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
```

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 frames. The selected frame (No. 7) is highlighted in blue. The details pane for this frame shows the following information:

- > 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)

At the bottom of the interface, it shows "Frame (frame), 1,482 bytes" and "Packets: 100".

Recorded Statistics in PacketExtractor™

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

Extractor Record Statistics

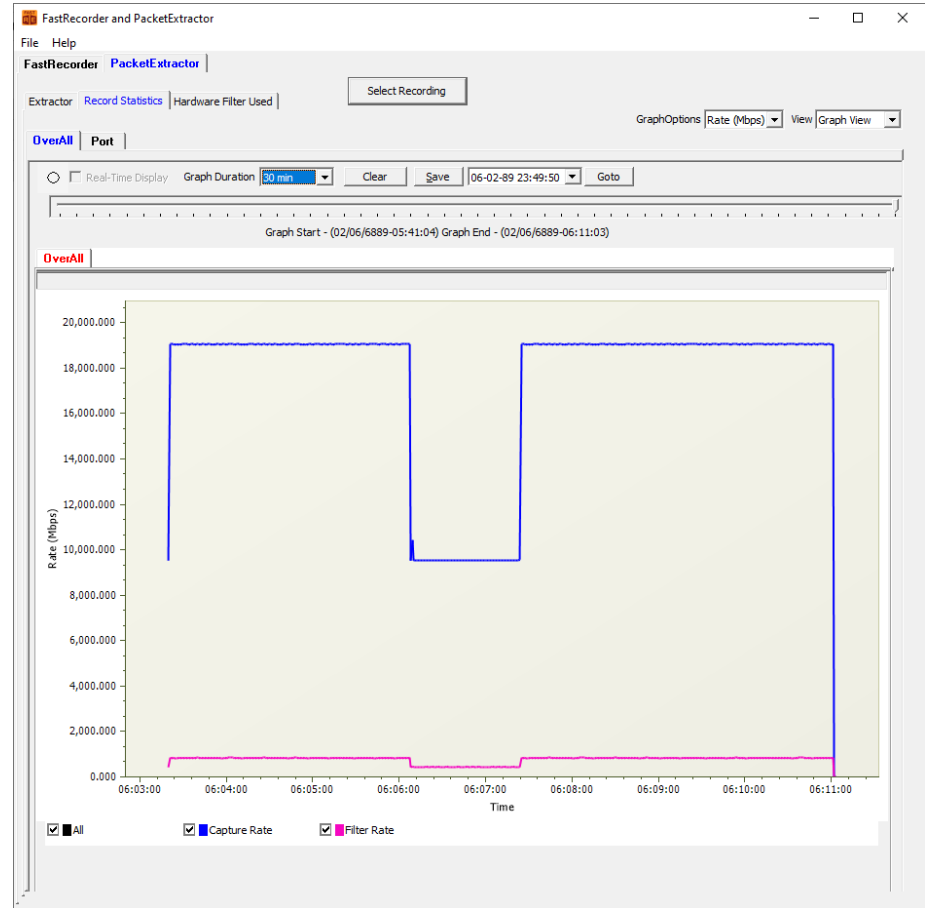
View List View

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
1024-1536 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
XTPNotificationSinkMTONEvent			

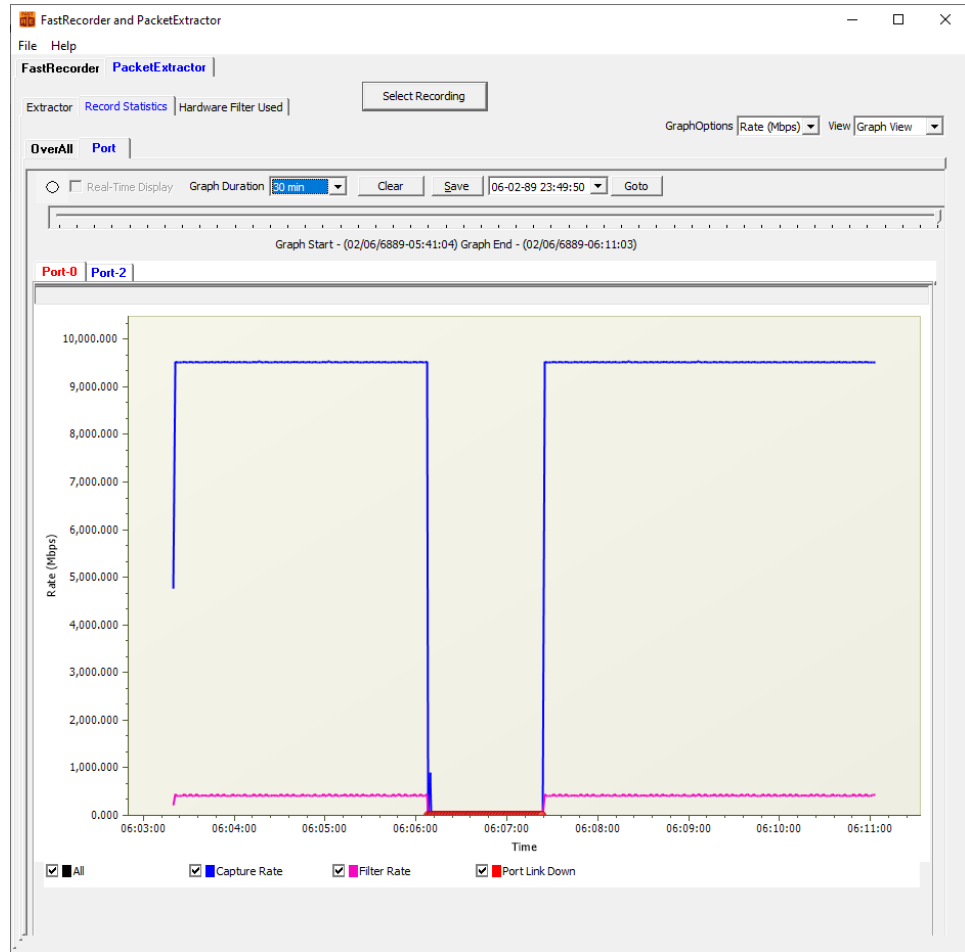
PacketExtractor™ - Overall Graph View

- 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 window. The main interface is divided into several sections:

- Recording Information:** Shows 'Record Name: SIP_GTP_4PORTS', 'Record Start Time: 2023-03-24 07:46:57', and 'Record Duration: 00:07:26'.
- PreExtraction Filter:** Includes 'Start Time' (07:46:57) and 'End Time' (07:54:00) fields. A red arrow points from the 'End Time' field to the 'Filter Configuration' button in the 'Extraction Filter' section.
- Limit Criteria:** Offers options for 'All', 'Duration' (with a 'Limit Value' of 00:07:26), 'Extracted Size', and 'Extracted Packet Count'.
- Extraction Filter:** The 'Filter Configuration' button is highlighted. Below it, 'Operation' is set to 'Packet Extraction'.
- Destination File Name:** A text input field for specifying the output file.
- Statistics:** A section for 'Packet Extraction' results.

The 'Protocol Capture Configuration' dialog box is open, showing:

- Record Frames As Is:** A checkbox with a green question mark icon.
- Capture Filters:** A tree view under 'Filter Selection' listing various protocols and layers such as MAC, VLAN, IP (All Levels), IP (Outer), ESP, TCP, UDP, Inner IP, Inner UDP, SCTP, SIP, RTP, MSRP, MGCP, MEGACO, H323, and RTSP.
- Filter Selected Protocols:** A list of protocols with checkboxes, including ARP, GTP-C, ICMP, LDAP, PTP, SLOW, UDP, DIAMETER, GTP-U, IPV4, LLDP, SCTP, SNMP, DNS, HTTP, IPV6, MEGACO, SIP, and TCP.
- Buttons:** 'Include' and 'Exclude' radio buttons, and 'Deactivate Sel' and 'Deactivate All' buttons.

Specifying End Time for Packet Extraction

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, showing the following configuration:

- Recording Information:**
 - Record Name: SIP_GTP_4PORTS
 - Record Start Time: 2023-03-23 06:03:44
 - Record End Time: 2023-03-23 06:11:10
 - Record Duration: 00:07:26
 - Record Size: 1 048 576.637 MB
- PreExtraction Filter:** (Checked)
 - Start Time: 06:03:44
 - End Time: 06:11:10 (HH:MM:SS)
- Limit Criteria:**
 - All: (Limit Value: 0)
 - Duration: (Limit Value: 0)
 - Extracted Size: (Limit Value: 0)
 - 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:** (Checked)
 - Operation: Packet Extraction
 - Multiple Files:
 - Destination File Name: D:\Extract-w-Endtime.hdl
 - Compress Extracted Files:
 - Packet Slicing:

Buttons for 'Start' and 'Stop' are visible at the bottom of the configuration area.

Statistics:

```
Extraction completed.
Processed Frames = 1 015 316 480
Processed Bytes = 299 058 914 135
Extracted Frames = 1 015 316 480 ( 100.00 %)
Extracted Bytes = 299 058 914 135
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 checked. It consists of five rules (F1-F5) and a custom expression.

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 'Custom Expression' is set to `(f2 && f3) || f1`. The 'Selected Filter Expression' is a complex logical expression: `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 =`

The 'Final Applied Expressions' section shows the resulting expression: `KeyList[KeyType=Ipv4; KeySet=6] = ([192.168.13.187]) Assign[StreamId = 10] = (((mVlan0TPID == 0x8100) AND (mUdpSrcPort == 5060)) OR (((TunnelType == GTPv1-U-GPDU OR (TunnelType == GR`

The interface also includes a table for IP addresses, currently containing '192.168.13.187', and buttons for 'Add', 'Edit', and 'Delete'.

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 PreExtraction Filter, Start Time (07:46:57), End Time (07:54:), and Limit Criteria (All, Duration, Extracted Size, Extracted Packet Count).
- Extraction Filter:** A red box highlights 'Filter Configuration' in the 'Extraction Filter' section, with a red arrow pointing to the 'Protocol Capture Configuration' dialog box.
- Destination File Name:** A text input field for the output file name.
- Statistics:** A section for monitoring 'Packet Extraction'.

The 'Protocol Capture Configuration' dialog box is open, showing the following settings:

- Record Frames As Is:** (with a help icon).
- Capture Filters:** A tree view under 'Filter Selection' showing various protocols like MAC, VLAN, IP (All Levels), IP (Outer), ESP, TCP, UDP, Inner IP, Inner UDP, SCTP, SIP, RTP, MSRP, MGCP, MEGACO, H323, and RTSP.
- Filter Selected Protocols:** A list of protocols to be filtered, including ARP, GTP-C, ICMP, LDAP, PTP, SLOW, UDP, DIAMETER, GTP-U, IPV4, LLDAP, SCTP, SNMP, DNS, HTTP, IPV6, MEGACO, SIP, and TCP.
- Buttons:** 'Deactivate Sel' and 'Deactivate All' are located at the bottom right of the dialog.

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 click to view details
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

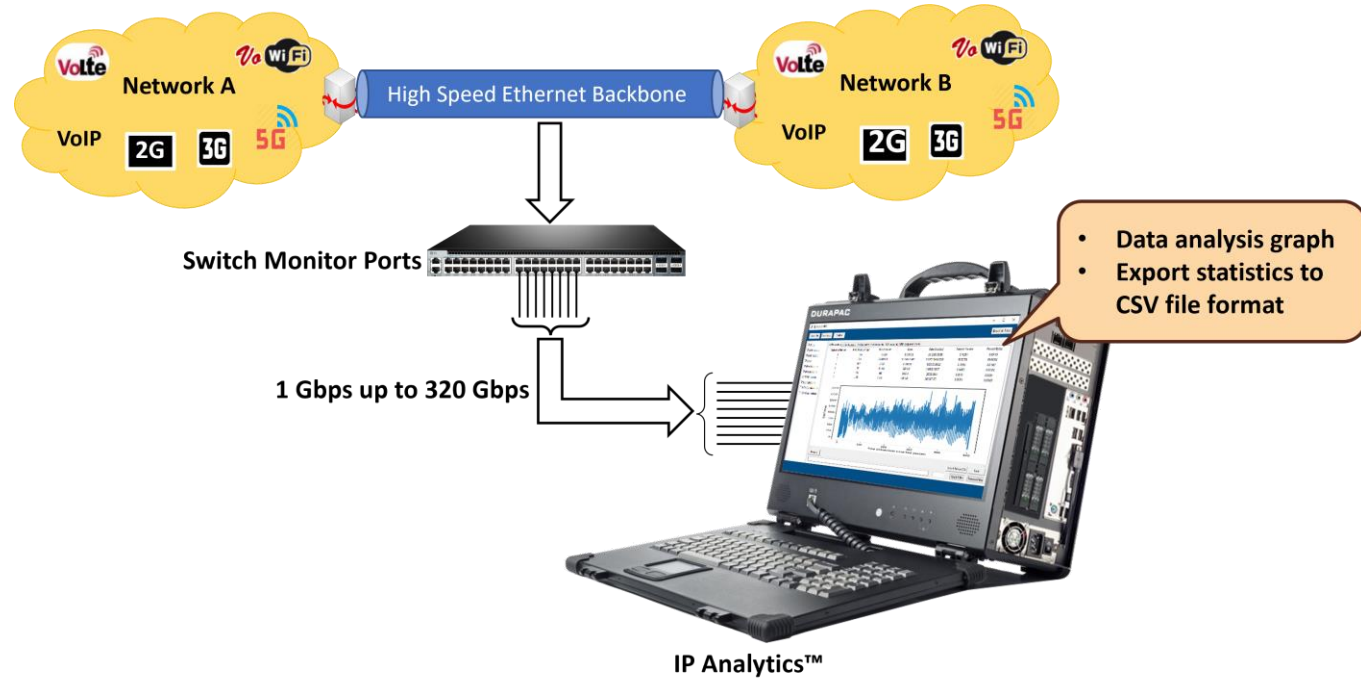
The screenshot shows the 'Protocol Capture Configuration' window. In the 'Filters' section, the 'Decipher Encrypted ESP Payload' checkbox is checked, and the 'Deciphered Payload' radio button is selected. The 'ESP SAs' field is highlighted with a red box, and a red arrow points to the 'Edit' button next to it.

Below the configuration window is the 'ESP SAs' table, which lists the configuration for each captured ESP packet. The table has the following columns: IP Protocol, Src IP, Dest IP, SPI, Encryption, Encryption Key, Authentication, and Authentication Key.

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]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.45	x.x.x.x	0x467113ba	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.86	192.168.12.251	0xd02382c2	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.251	192.168.12.86	0x129e7b1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.90	192.168.12.45	0xa5e7259a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.45	*	0x9637e468	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.90	192.168.12.251	0x57be7f1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	*	192.168.12.90	*	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...

IP Analytics™

- IP Analytics™ 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 is visible. The 'Extraction Filter' is checked, and the 'Filter Configuration' dialog is open, showing the 'Operation' dropdown menu with 'Data Analysis' selected. The 'Destination File Name' field is empty, and the 'Start' button is visible.

Recording Information

Record Name: 2024-02-14__07-21-22

Record Start Time: 2024-02-14 07:21:24 Record End Time: 2024-02-14 07:50:10

Record Duration: 00:28:46 Record Size: 514 987.457 MB

PreExtraction Filter

Start Time: 07:21:24 End Time: 07:50:10 HH:MM:SS

Limit Criteria

All Limit Value: HH:MM:SS

Duration Limit Value: 00:20:00 HH:MM:SS

Extracted Size

Extracted Packet Count

Recorded Ports: 2 3

Port Filter

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

Extraction Filter Filter Configuration

Operation: Data Analysis

Destination File Name: ...

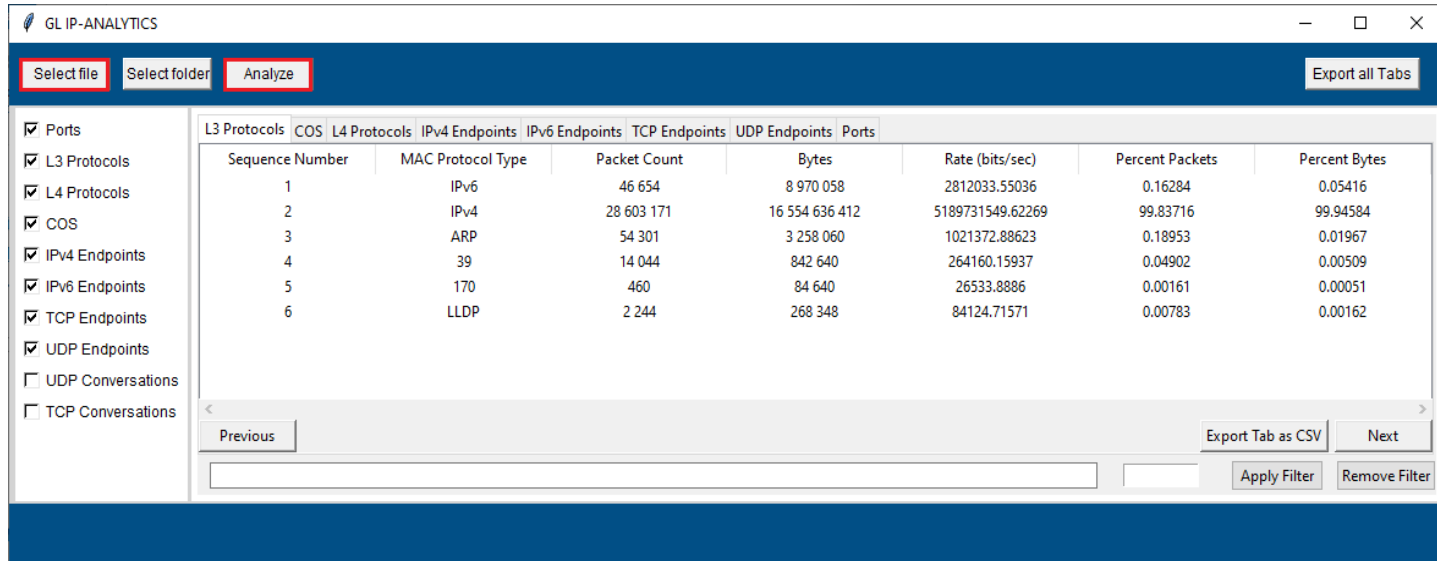
Start Stop

Statistics

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

Configuring GL IP Analytics™ Tool

- Executing **Python scripts** will invoke the GL IP Analytics™ window to perform data analysis
- This analysis will display “L3”, “COS”, “L4”, “IPv4 Endpoints”, “IPv6 Endpoints”, “UDP Endpoints”, “TCP Endpoints”, “UDP Conversation”, “TCP Conversation”, and “Ports” statistics
- Observe the statistics as shown below



The screenshot shows the GL IP-ANALYTICS application window. The interface includes a top navigation bar with buttons for "Select file", "Select folder", "Analyze", and "Export all Tabs". On the left, there is a sidebar with checkboxes for various analysis categories: Ports, L3 Protocols, L4 Protocols, COS, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, UDP Conversations, and TCP Conversations. The main area displays a table with the following data:

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	Sequence Number	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
<input checked="" type="checkbox"/>								1	IPv6	46 654	8 970 058	2812033.55036	0.16284	0.05416
<input checked="" type="checkbox"/>								2	IPv4	28 603 171	16 554 636 412	5189731549.62269	99.83716	99.94584
<input checked="" type="checkbox"/>								3	ARP	54 301	3 258 060	1021372.88623	0.18953	0.01967
<input checked="" type="checkbox"/>								4	39	14 044	842 640	264160.15937	0.04902	0.00509
<input checked="" type="checkbox"/>								5	170	460	84 640	26533.8886	0.00161	0.00051
<input checked="" type="checkbox"/>								6	LLDP	2 244	268 348	84124.71571	0.00783	0.00162

At the bottom of the table, there are navigation buttons: "Previous", "Export Tab as CSV", and "Next". Below these are two input fields and buttons for "Apply Filter" and "Remove Filter".

Statistics

The screenshot shows the GL IP-ANALYTICS interface with the 'L3 Protocols' tab selected. The table displays statistics for various protocols, including L3, L4, COS, IPv4, IPv6, TCP, and UDP endpoints and conversations. The 'L3 Protocols' tab is highlighted with a red box.

Sequence Number	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6	46 654	8 970 058	2812033.55036	0.16284	0.05416
2	IPv4	28 603 171	16 554 636 412	5189731549.62269	99.83716	99.94584
3	ARP	54 301	3 258 060	1021372.88623	0.18953	0.01967
4		14 044	842 640	264160.15937	0.04902	0.00509
5	170	460	84 640	26533.8886	0.00161	0.00051
6	LLDP	2 244	268 348	84124.71571	0.00783	0.00162

Layer 3 Protocols statistics

Class of Service (COS) Statistics

The screenshot shows the GL IP-ANALYTICS interface with the 'COS' tab selected. The table displays statistics for different classes of service, including L3, L4, COS, IPv4, IPv6, TCP, and UDP endpoints and conversations. The 'COS' tab is highlighted with a red box.

Sequence Number	COS	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	0	28 519 280	16 509 370 496	5175541086.80965	99.54434	99.67256
2	48	478	64 432	20198.86	0.00167	0.00039
3	4	130 067	54 171 542	16982297.50339	0.45399	0.32705

Statistics

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports

L3 Protocols COS **L4 Protocols** IPv4 Endpoints IPv6 Endpoints TCP Endpoints UDP Endpoints Ports UDP Conversations TCP Conversations

Sequence Number	IP Protocol	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	TCP	20 035 547	12 625 265 588	3957908679.70464	69.93253	76.22293
2	IGMP	1 034	72 620	22765.72531	0.00361	0.00044
3	ICMP	18 232	3 007 863	942938.34788	0.06364	0.01816
4	IPv6-ICMP	27 346	2 354 972	738262.81549	0.09545	0.01422
5	UDP	8 567 666	3 932 905 427	1232930936.57974	29.90478	23.74426

Previous Next

Export Tab as CSV

Apply Filter Remove Filter

Layer 4 Protocol statistics

IPv4 Endpoints statistics

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports

L3 Protocols COS L4 Protocols **IPv4 Endpoints** IPv6 Endpoints TCP Endpoints UDP Endpoints Ports UDP Conversations TCP Conversations

Sequence Number	IP Address	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes	Avg Tx Packets/s	Avg Tx Bits/sec	Avg Rx Packets/s	Avg Rx Bits/sec	Total Packets
1	104.44.49.142	28	1 960	0	0	1.09722	614.4426	0	0	28
2	34.111.50.114	304	97 808	208	21 824	11.91266	30661.9397	8.15077	6841.63026	512
3	91.189.91.49	600	67 170	924	74 190	23.51183	21057.19869	36.20822	23257.90637	1 524
4	202.83.26.121	1 970	1 117 534	636	63 994	77.19719	350336.98797	24.92254	20061.55089	2 606
5	192.168.12.210	3 972	593 638	2 772	729 954	155.64834	186100.24292	108.62467	228834.09876	6 744
6	142.250.4.188	660	43 816	660	40 240	25.86302	13735.92702	25.86302	12614.88277	1 320

Previous Next

Export Tab as CSV

Apply Filter Remove Filter

Statistics

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports
 L3 Protocols
 L4 Protocols
 COS
 IPv4 Endpoints
 IPv6 Endpoints
 TCP Endpoints
 UDP Endpoints
 UDP Conversations
 TCP Conversations

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	UDP Conversations	TCP Conversations				
Sequence Number	IP Address	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes	Avg Tx Packets/s	Avg Tx Bits/sec	Avg Rx Packets/s	Avg Rx Bits/sec	Total Packets			
1	ff02::1:2	0	0	574	94 276	0	0	22.49299	29554.68905	574			
2	ff02::1:ff5f:118	0	0	32	2 752	0	0	1.25396	862.72757	32			
3	ff02::1:ff68:9882	0	0	16	1 376	0	0	0.62698	431.36378	16			
4	ff02::1:ffa0:28c4	0	0	90	7 740	0	0	3.52678	2426.42129	90			
5	fe80::d431:1f22:4f	184	19 320	0	0	7.2103	6056.64848	0	0	184			
6	fe80::e0a6:b9da:4l	184	19 320	0	0	7.2103	6056.64848	0	0	184			

Previous Export Tab as CSV Next Apply Filter Remove Filter

IPv6 Endpoints statistics

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports
 L3 Protocols
 L4 Protocols
 COS
 IPv4 Endpoints
 IPv6 Endpoints
 TCP Endpoints
 UDP Endpoints
 UDP Conversations
 TCP Conversations

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	UDP Conversations	TCP Conversations				
Sequence Number	Port	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets			
1	58319	11 260	9 197 020	11 442	9 114 084	441.23875	2883184.12248	448.37068	2857184.42275				
2	51094	496	150 064	480	195 440	19.43645	47043.73179	18.80947	61268.70496				
3	64088	384	105 648	400	302 608	15.04757	33119.7101	15.67456	94864.92157				
4	55493	80	6 000	48	2 976	3.13491	1880.94673	1.88095	932.94958				
5	64146	272	52 480	192	13 328	10.6587	16452.0141	7.52379	4178.20968				
6	65182	256	18 320	176	12 256	10.03172	5743.15736	6.8968	3842.1472				

Previous Export Tab as CSV Next Apply Filter Remove Filter

TCP Endpoints statistics

Statistics

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports
 L3 Protocols
 L4 Protocols
 COS
 IPv4 Endpoints
 IPv6 Endpoints
 TCP Endpoints
 UDP Endpoints
 UDP Conversations
 TCP Conversations

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	UDP Conversations	TCP Conversations		
Sequence Number		Port	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes		Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec
1		58314	144	38 000	160	84 544		5.64284	11912.66265	6.26982	26503.79345
2		53762	112	43 600	144	103 040		4.38888	13668.21294	5.64284	32302.12525
3		53438	16	1 488	16	2 688		0.62698	466.47479	0.62698	842.66414
4		62440	16	1 488	16	2 688		0.62698	466.47479	0.62698	842.66414
5		65187	16	1 360	16	2 736		0.62698	426.34793	0.62698	857.71171
6		54739	80	15 312	16	1 680		3.13491	4800.17607	0.62698	526.66509

Previous Export Tab as CSV Next Apply Filter Remove Filter

UDP Endpoints statistics

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports
 L3 Protocols
 L4 Protocols
 COS
 IPv4 Endpoints
 IPv6 Endpoints
 TCP Endpoints
 UDP Endpoints
 UDP Conversations
 TCP Conversations

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	UDP Conversations	TCP Conversations		
Sequence Number		PortNo	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes				
1		0	14 321 395	8 279 803 748	2595644970.16268	49.98772	49.98793				
2		2	14 328 430	8 283 802 722	2596898613.01037	50.01228	50.01207				

Previous Export Tab as CSV Next Apply Filter Remove Filter

Ports statistics

Conversations

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports

L3 Protocols

L4 Protocols

COS

IPv4 Endpoints

IPv6 Endpoints

TCP Endpoints

UDP Endpoints

UDP Conversations

TCP Conversations

L3 Protocols COS L4 Protocols IPv4 Endpoints IPv6 Endpoints TCP Endpoints UDP Endpoints Ports **UDP Conversations** TCP Conversations

Sequence Number	East IP	West IP	East Port	West Port	Tx Packet Count	Tx Bytes	Tx Avg Packets/s	Tx Avg Bits/sec	Rx Packet Count	Rx Bytes
1	8.8.8.8	192.168.12.7	53	58413	16	2 672	0.62698	837.64828	16	1 280
2	192.168.12.26	192.168.1.3	53069	53	15	1 275	0.5878	399.70118	15	4 920
3	192.168.1.3	192.168.12.29	53	49430	16	2 032	0.62698	637.01396	16	2 000
4	192.168.1.3	192.168.12.189	53	50711	16	2 544	0.62698	797.52142	16	1 424
5	192.168.1.3	192.168.12.91	53	60053	16	4 224	0.62698	1324.1865	16	1 248
6	192.168.1.3	192.168.12.83	53	55437	14	1 764	0.54861	552.99834	46	6 670

Previous Export Tab as CSV Next Apply Filter Remove Filter

UDP conversations

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports

L3 Protocols

L4 Protocols

COS

IPv4 Endpoints

IPv6 Endpoints

TCP Endpoints

UDP Endpoints

UDP Conversations

TCP Conversations

L3 Protocols COS L4 Protocols IPv4 Endpoints IPv6 Endpoints TCP Endpoints UDP Endpoints Ports UDP Conversations **TCP Conversations**

Sequence Nu	East IP	West IP	East Port	West Port	Tx Packet Co	Tx Bytes	Tx Avg Packe	Tx Avg Bits/s	Rx Packet Count	Rx Bytes	Rx Avg Packet	Rx Avg Bits/	Total Packets
1	192.168.1.3	192.168.12.12	49155	51237	80	9 696	3.13491	3039.60992	112	14 048	4.38888	4403.92329	192
2	192.168.1.3	192.168.12.5	49161	56441	848	443 728	33.23006	139104.78876	896	545 824	35.11101	171110.9783	1 744
3	192.168.1.169	192.168.12.28	7680	49473	42	2 604	1.64583	816.33088	80	6 416	3.13491	2011.35904	122
4	192.168.31.18	192.168.12.80	1947	62866	16	960	0.62698	300.95148	16	1 056	0.62698	331.04663	32
5	192.168.12.11	192.168.10.93	7680	56071	48	2 976	1.88095	932.94958	80	6 000	3.13491	1880.94673	128
6	192.168.12.41	192.168.1.3	64248	88	70	25 396	2.74305	7961.42054	96	6 288	3.76189	1971.23218	166

Previous Export Tab as CSV Next Apply Filter Remove Filter

TCP conversations

Sorting of Columns (Tabs)

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

Display of columns in Ascending order

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports				
Sequence Number	Port	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes	Avg Tx Packets/s	Avg Tx Bits/sec	Avg Rx Packets/s	Avg Rx Bits/sec		
<input checked="" type="checkbox"/> L3 Protocols	1	62081	0	0	16	960	0	0	0.62698	300.95148	
<input checked="" type="checkbox"/> L4 Protocols	2	61111	0	0	16	960	0	0	0.62698	300.95148	
<input checked="" type="checkbox"/> COS	3	49485	0	0	16	960	0	0	0.62698	300.95148	
<input checked="" type="checkbox"/> IPv4 Endpoints	4	56045	0	0	16	960	0	0	0.62698	300.95148	
<input checked="" type="checkbox"/> IPv6 Endpoints	5	62085	0	0	16	960	0	0	0.62698	300.95148	
<input checked="" type="checkbox"/> TCP Endpoints	6	50393	0	0	16	960	0	0	0.62698	300.95148	

UDP Endpoints

UDP Conversations

TCP Conversations

Previous Export Tab as CSV Next Apply Filter Remove Filter

Display of columns in Descending order

GL IP-ANALYTICS

Select file Select folder Analyze Export all Tabs

Ports

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports				
Sequence Number	Port	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes	Avg Tx Packets/s	Avg Tx Bits/sec	Avg Rx Packets/s	Avg Rx Bits/sec		
<input checked="" type="checkbox"/> L3 Protocols	1	445	4 974 120	5 818 595 220	2 136 399	726 968 176	194917.80772	1824077946.27424	83717.76505	227898069.43897	
<input checked="" type="checkbox"/> L4 Protocols	2	443	3 226 661	3 023 513 877	1 451 380	503 117 627	126441.19731	947844758.87461	56874.34315	157722909.58444	
<input checked="" type="checkbox"/> COS	3	80	2 114 582	1 410 885 967	380 929	70 191 738	82862.83557	442300225.36479	14927.23247	22004486.72841	
<input checked="" type="checkbox"/> IPv4 Endpoints	4	56477	1 262 430	484 926 502	4 022 221	5 499 647 948	49470.07471	152020153.39058	157616.32198	1724090807.99045	
<input checked="" type="checkbox"/> IPv6 Endpoints	5	3389	1 244 245	210 414 097	1 573 770	142 758 898	48757.4702	65962951.43605	61670.36546	44753647.16575	
<input checked="" type="checkbox"/> TCP Endpoints	6	88	359 859	30 313 348	340 003	131 662 269	14101.57523	9502965.48804	13323.49026	41274952.48575	

UDP Endpoints

UDP Conversations

TCP Conversations

Previous Export Tab as CSV Next Apply Filter Remove Filter

Applying Filter

- Users can filter the required data by specifying keywords such as **mac_protocol_type**, **cos**, **ip_protocol**, **ip_address**, **tcp_port**, **udp_port**, **port** (recorded port number), **east_ip**, **west_ip**, **east_port** and **west_port**
- Enter the desired keyword in the filter search box at the bottom of the window and click **Apply Filter**. In this instance, filter is applied for **cos**. The suggestion box recommends keywords for filtering as the user types the keyword

The screenshot shows the GL IP-ANALYTICS application window. The interface includes a top navigation bar with 'Select file', 'Select folder', and 'Analyze' buttons, and an 'Export all Tabs' button. A left sidebar contains a list of categories with checkboxes: Ports, L3 Protocols, L4 Protocols, COS, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, UDP Conversations, and TCP Conversations. The main area displays a table with columns: L3 Protocols, COS, L4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, Ports, UDP Conversations, TCP Conversations, Sequence Number, COS, Packet Count, Bytes, Rate (bits/sec), Percent Packets, and Percent Bytes. The table shows three rows of data. Below the table, there is a 'Filter Search Box' containing the text 'cos==0' and a 'Filter Suggestion Box' showing 'cos'. At the bottom right, there are buttons for 'Previous', 'Export Tab as CSV', 'Next', 'Apply Filter', and 'Remove Filter'.

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	UDP Conversations	TCP Conversations	Sequence Number	COS	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
										1	0	28 519 280	16 509 370 496	5175541086.80965	99.54434	99.67256
										2	48	478	64 432	20198.86	0.00167	0.00039
										3	4	130 067	54 171 542	16982297.50339	0.45399	0.32705

- Click on **Remove Filter** button to remove the applied filter

Display of Applied Filter

- Observe the applied filter is as shown below. In this instance, the filter results are displayed for **cos**

The screenshot shows the GL IP-ANALYTICS application interface. The top navigation bar includes buttons for 'Select file', 'Select folder', 'Analyze', and 'Export all Tabs'. On the left, a sidebar lists various analysis categories with checkboxes: Ports, L3 Protocols, L4 Protocols, COS, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, UDP Conversations, and TCP Conversations. The main area displays a table with columns: L3 Protocols, COS, L4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, Ports, Sequence Number, COS, Packet Count, Bytes, Rate (bits/sec), Percent Packets, and Percent Bytes. A red box highlights the first row of data. Below the table, there are navigation buttons ('Previous', 'Next'), an 'Export Tab as CSV' button, and a filter input field containing 'cos==0' with 'Apply Filter' and 'Remove Filter' buttons.

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	Sequence Number	COS	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
								1	0	28 519 280	16 509 370 496	5175541086.80965	100	100

Exporting All Tabs to CSV File Format

- Click on **Export All Tabs** button to export all the tabs to CSV format

GL IP-ANALYTICS

Select file Select folder Analyze **Export all Tabs**

Ports
 L3 Protocols
 L4 Protocols
 COS
 IPv4 Endpoints
 IPv6 Endpoints
 TCP Endpoints
 UDP Endpoints
 UDP Conversations
 TCP Conversations

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	Sequence Number	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
			IPv6					1		46 654	8 970 058	2812033.55036	0.16284	0.05416
			IPv4					2		28 603 171	16 554 636 412	5189731549.62269	99.83716	99.94584
			ARP					3		54 301	3 258 060	1021372.88623	0.18953	0.01967
			39					4		14 044	842 640	264160.15937	0.04902	0.00509
			170					5		460	84 640	26533.8886	0.00161	0.00051
			LLDP					6		2 244	268 348	84124.71571	0.00783	0.00162

Previous Next Export Tab as CSV

Apply Filter Remove Filter

Export Tabs as CSV

- Click on **Export Tab as CSV** button to export the tab to CSV format. Here, the selected tab is **L3 Protocols**

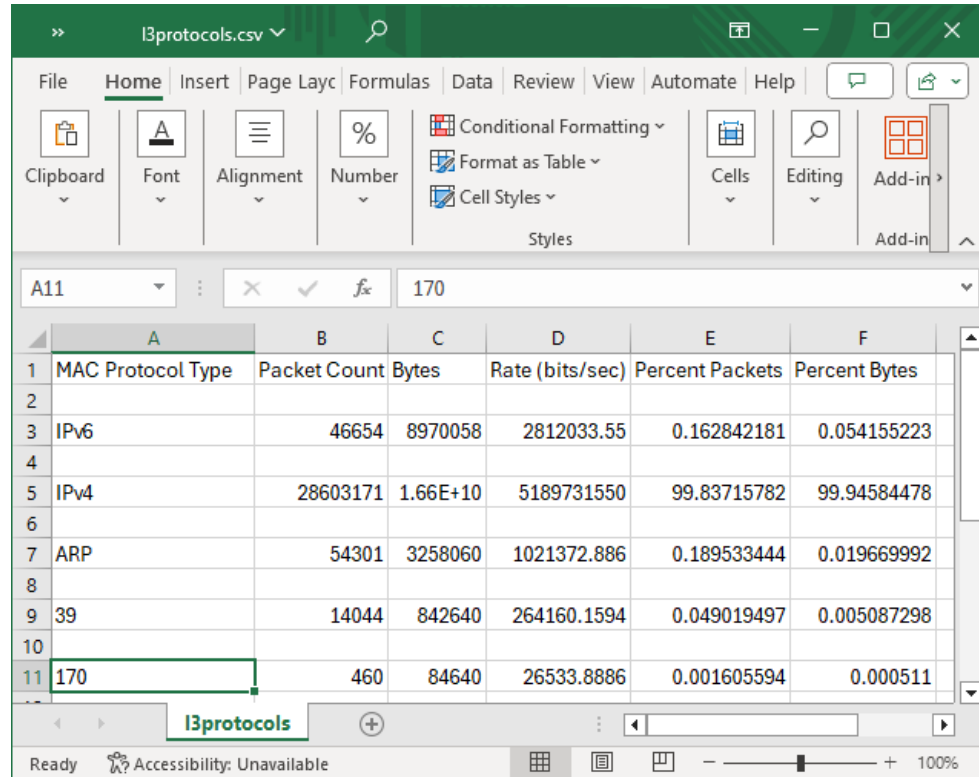
The screenshot shows the GL IP-ANALYTICS application window. The interface includes a top navigation bar with buttons for 'Select file', 'Select folder', 'Analyze', and 'Export all Tabs'. On the left, a sidebar contains a list of analysis categories with checkboxes: Ports, L3 Protocols, L4 Protocols, COS, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, UDP Conversations, and TCP Conversations. The 'L3 Protocols' tab is selected and highlighted with a red box. The main area displays a table with the following data:

Sequence Number	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6	46 654	8 970 058	2812033.55036	0.16284	0.05416
2	IPv4	28 603 171	16 554 636 412	5189731549.62269	99.83716	99.94584
3	ARP	54 301	3 258 060	1021372.88623	0.18953	0.01967
4	39	14 044	842 640	264160.15937	0.04902	0.00509
5	170	460	84 640	26533.8886	0.00161	0.00051
6	LLDP	2 244	268 348	84124.71571	0.00783	0.00162

At the bottom of the interface, there are navigation buttons for 'Previous' and 'Next', and a filter section with 'Apply Filter' and 'Remove Filter' buttons. The 'Export Tab as CSV' button is highlighted with a red box.

Export Tab to CSV (Contd.)

- The sample exported (L3 Protocols) CSV file is as shown below



The screenshot displays the Microsoft Excel interface with the 'Home' ribbon selected. The active worksheet is 'l3protocols.csv'. The data is organized in a table with the following columns: MAC Protocol Type, Packet Count, Bytes, Rate (bits/sec), Percent Packets, and Percent Bytes. The data rows are as follows:

	A	B	C	D	E	F
1	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
2						
3	IPv6	46654	8970058	2812033.55	0.162842181	0.054155223
4						
5	IPv4	28603171	1.66E+10	5189731550	99.83715782	99.94584478
6						
7	ARP	54301	3258060	1021372.886	0.189533444	0.019669992
8						
9	39	14044	842640	264160.1594	0.049019497	0.005087298
10						
11	170	460	84640	26533.8886	0.001605594	0.000511

Data Analysis Graph

- Right-click on the selected row, and choose either **Show IO Bits/sec** or **Show IO Pkts/sec** to view the Input/Output graphs

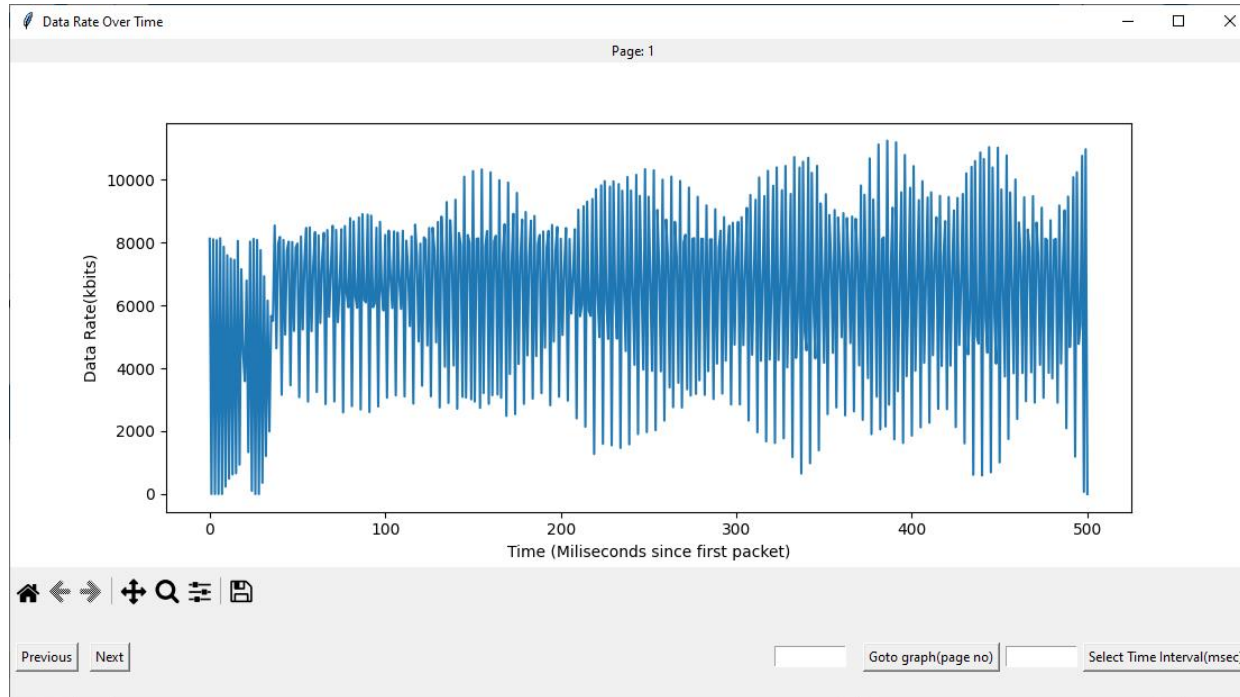
The screenshot displays the GL IP-ANALYTICS application window. The interface includes a top navigation bar with buttons for 'Select file', 'Select folder', 'Analyze', and 'Export all Tabs'. On the left, a sidebar contains a list of checked categories: Ports, L3 Protocols, L4 Protocols, COS, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, and UDP Endpoints. The main area features a table with columns for 'L3 Protocols', 'COS', 'L4 Protocols', 'IPv4 Endpoints', 'IPv6 Endpoints', 'TCP Endpoints', 'UDP Endpoints', and 'Ports'. The table data is as follows:

Sequence Number	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6	46 654	8 970 058	2812033.55036	0.16284	0.05416
2	IPv4	28 603 171	16 554 636 412	5189731549.62269	99.83716	99.94584
3	ARP		3 258 060	1021372.88623	0.18953	0.01967
4	39		842 640	264160.15937	0.04902	0.00509
5	170	460	84 640	26533.8886	0.00161	0.00051
6	LLDP	2 244	268 348	84124.71571	0.00783	0.00162

A context menu is open over the second row (Sequence Number 2), showing two options: 'Show IO Bits/sec' and 'Show IO Pkts/sec'. At the bottom of the interface, there are navigation buttons for 'Previous', 'Next', and 'Export Tab as CSV', along with input fields for 'Apply Filter' and 'Remove Filter'.

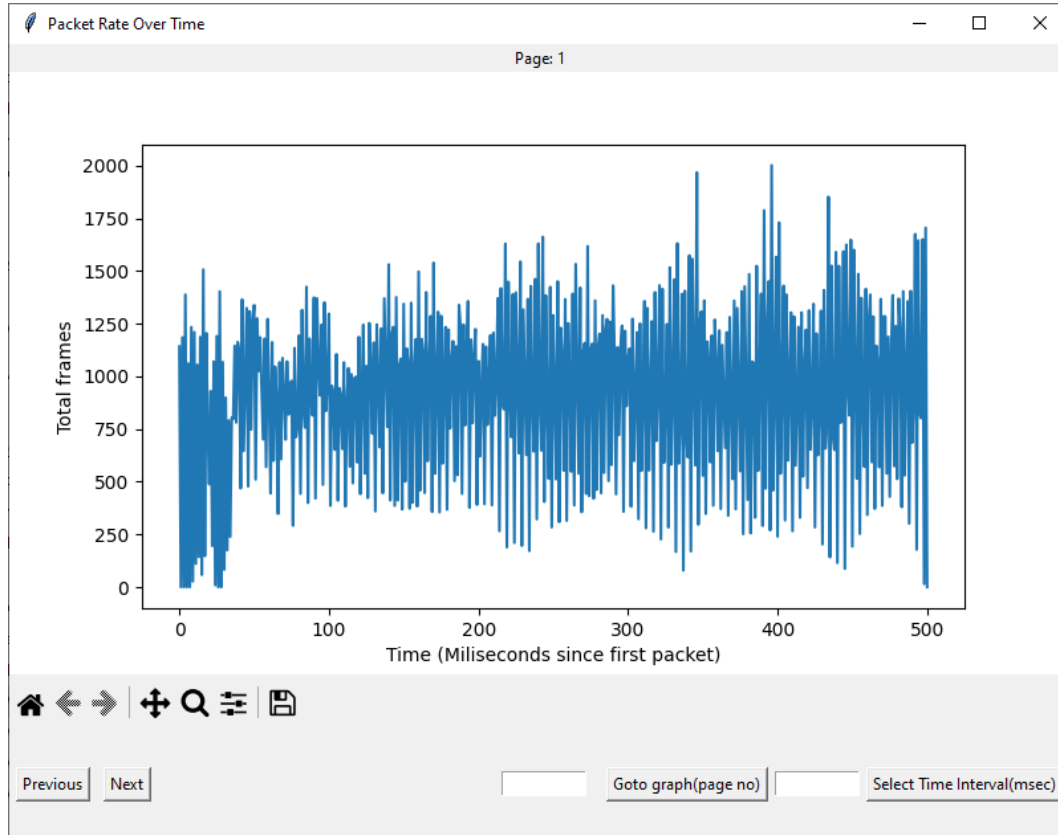
Display of Data Rate Over Time Graph

- Observe the display of **Data Rate Over Time** graph as shown



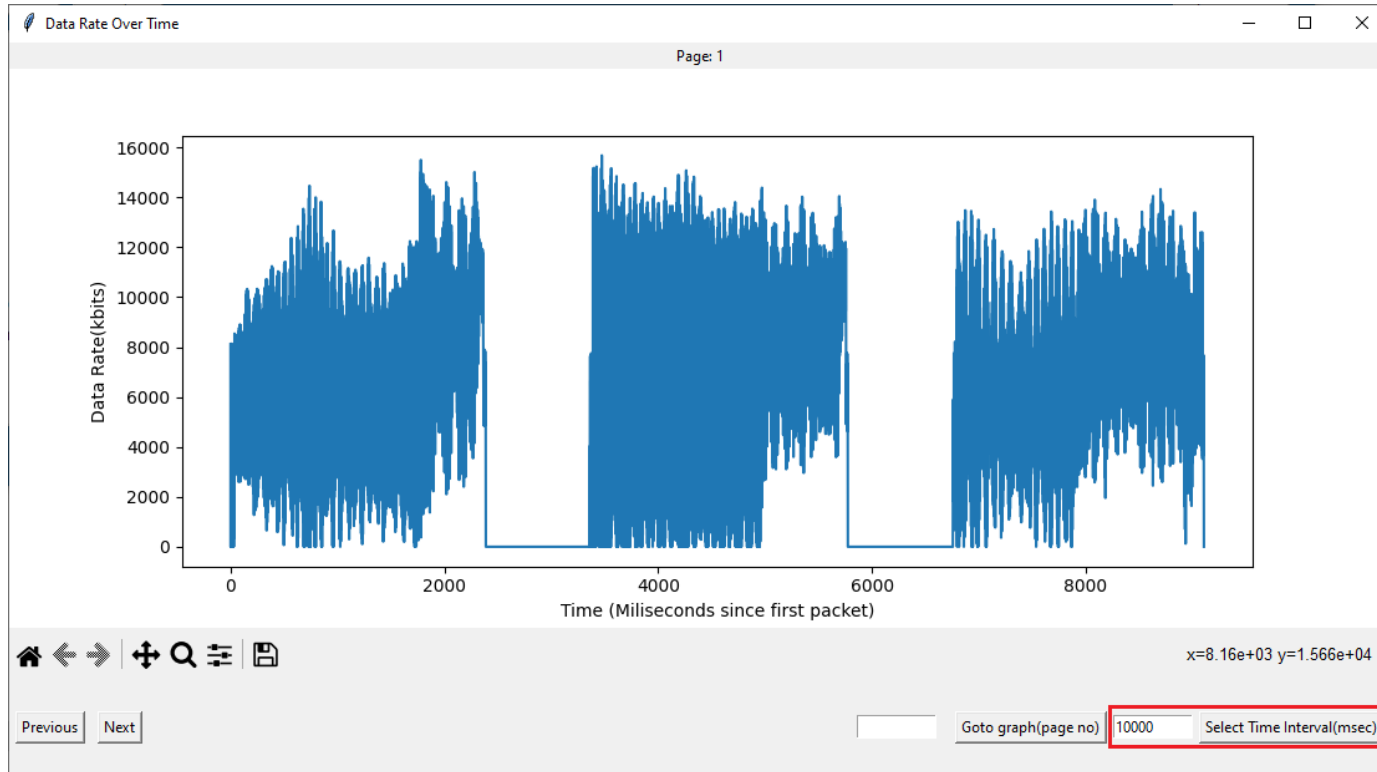
Display of Packet Rate Over Time Graph

- Observe the display of **Packet Rate Over Time** graph as shown



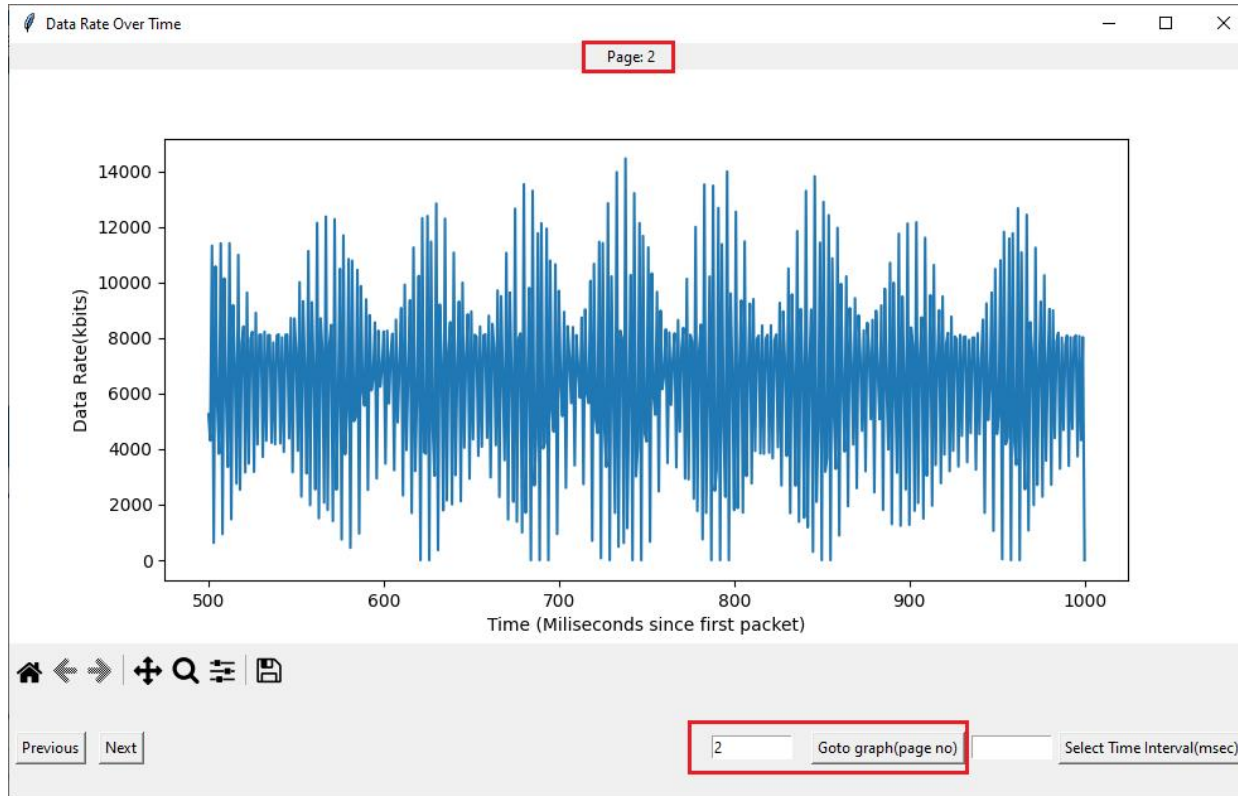
Selecting Time Interval (msec) Option

- Click on **Select Time Interval (msec)** to change the time interval as required. In this instance, the time interval is set to **10000** msec. The graph will be displayed up to the specified time interval (**10000** msec) as shown



Goto Graph Option

- Click on **Goto graph (page no)** to navigate to the next page of the graph (the next set of 10 seconds of the graph), as shown below



Rate Analysis

Rate Analysis in PacketExtractor™

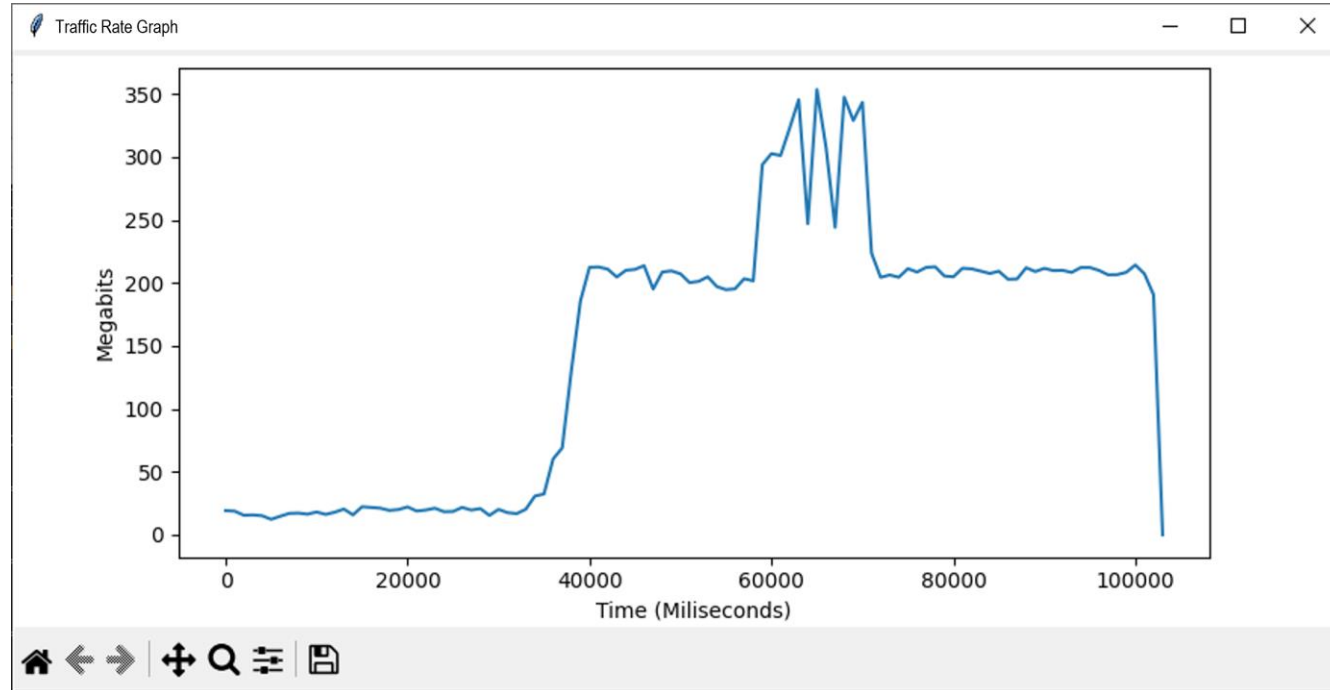
- Users can perform **Rate Analysis** using the PacketExtractor™ application

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' 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

Rate Analysis in PacketExtractor™ (Contd.)

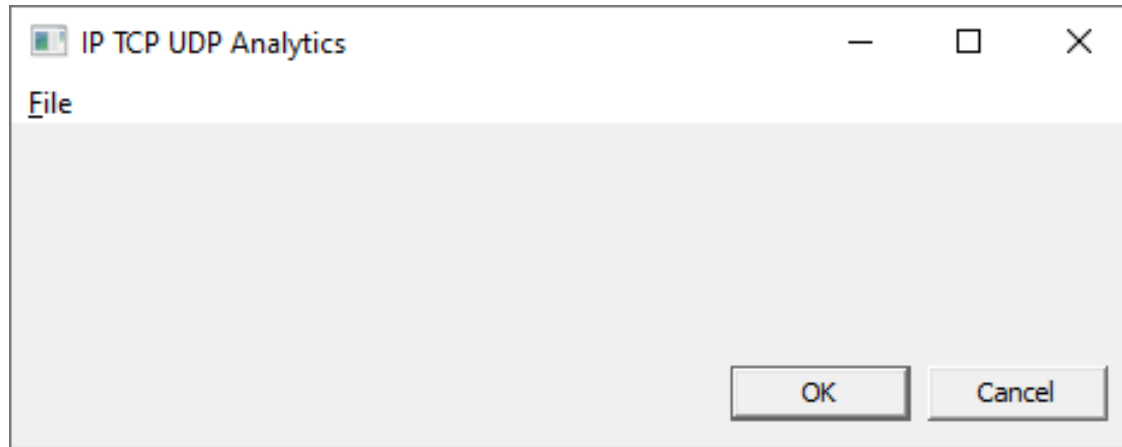
- Once the extraction is completed, the **Traffic Rate Graph** window appears as shown
- The graph indicates a consistent rate of 20 Mbps bandwidth.
- However, at the 40th second, there is a sudden increase to 200 Mbps bandwidth. Additionally, there are spikes in the rate between 60 and 75 seconds.
- These rates analysis helps network provider in troubleshooting bandwidth requirement by examining the graph at various time intervals with millisecond precision



Data Analysis using IP TCP UDP Tool

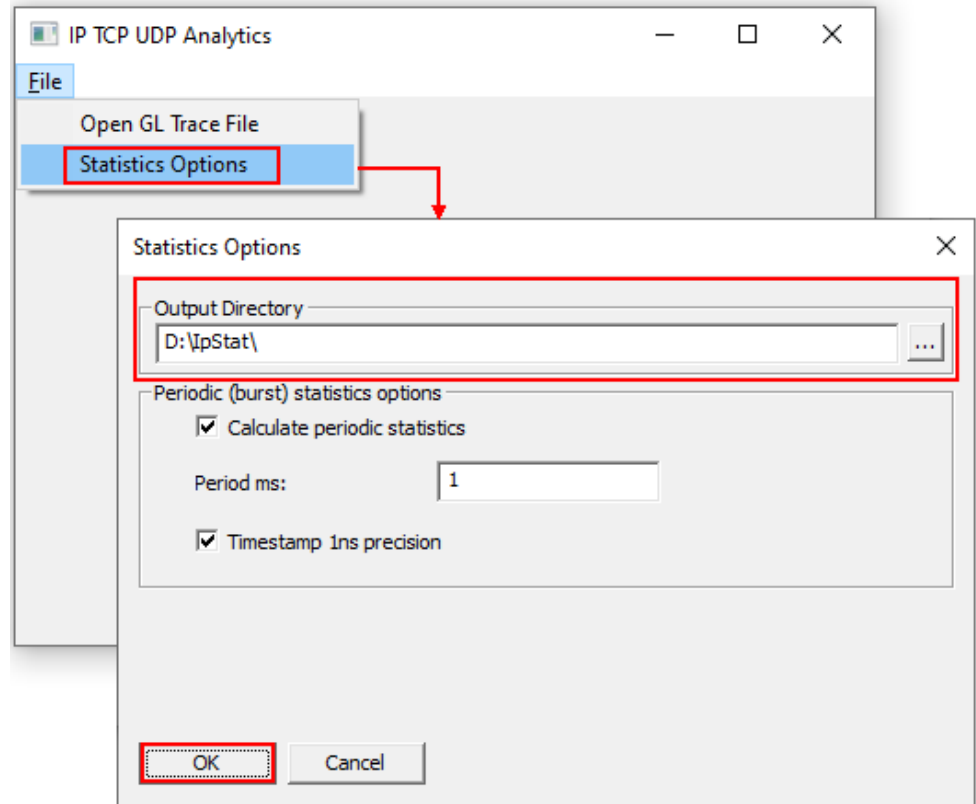
Invoking IP TCP UDP Analysis Tool

- **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



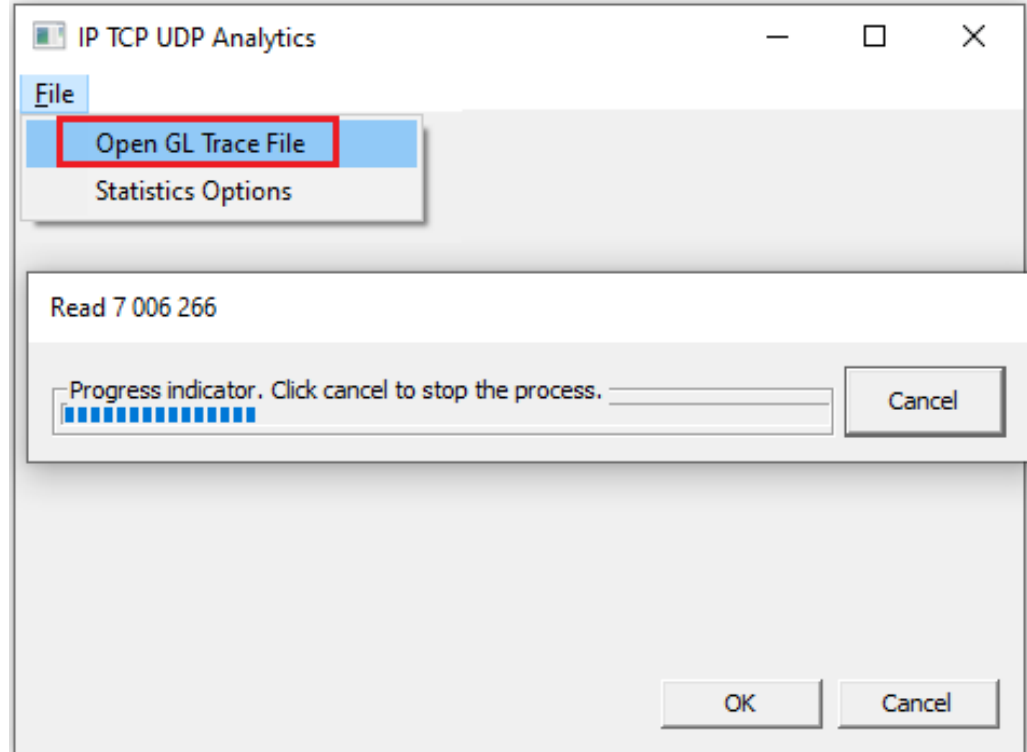
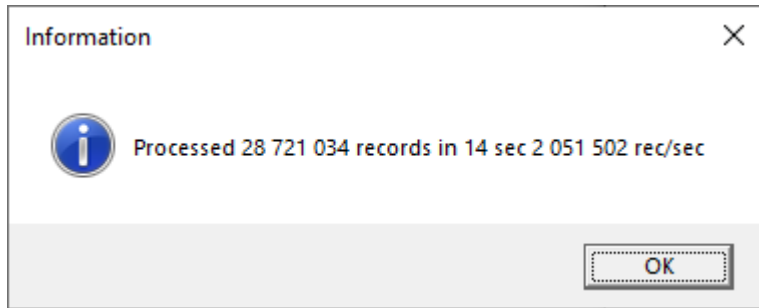
Configuring IP TCP UDP Analysis Tool

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



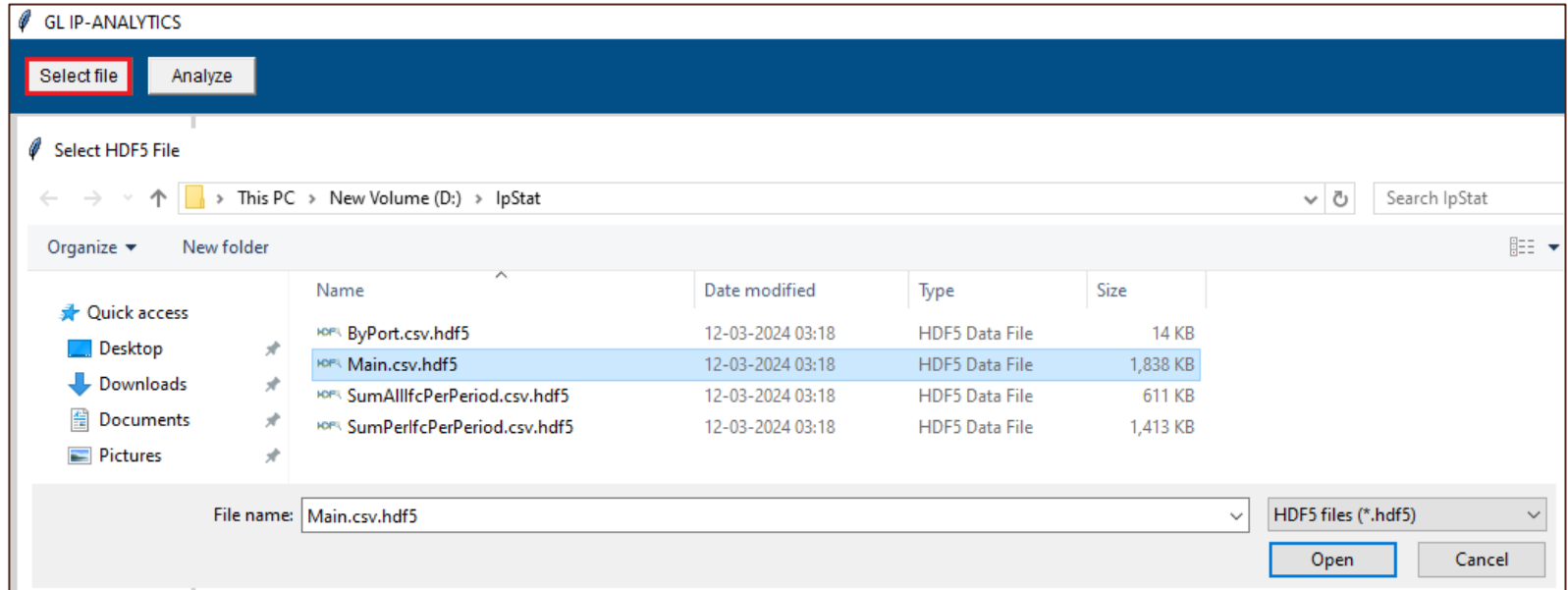
Configuring IP TCP UDP Analysis Tool (Contd.)

- 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



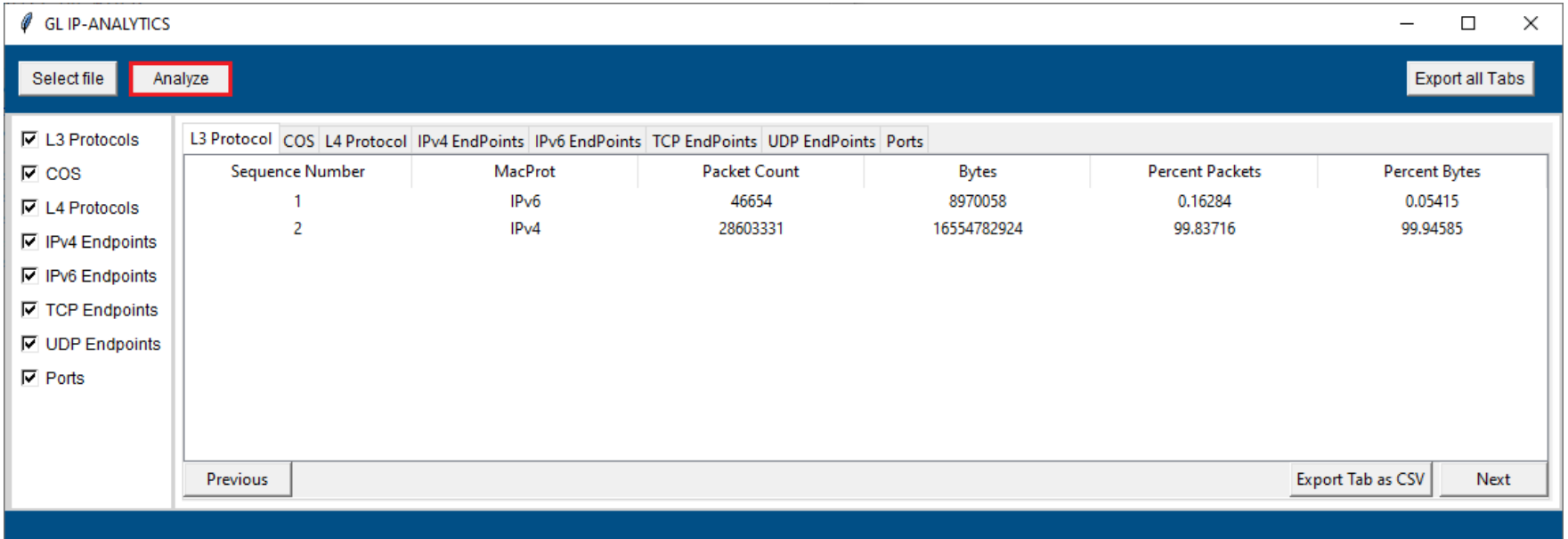
GL IP Analytics™

- 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 interface includes a top navigation bar with a 'Select file' button and a highlighted 'Analyze' button. On the right side of the top bar is an 'Export all Tabs' button. A left-hand sidebar contains a list of analysis categories, all of which are checked: L3 Protocols, COS, L4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, and Ports. The main content area features a table with the following data:

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

At the bottom of the application window, there are three buttons: 'Previous', 'Export Tab as CSV', and 'Next'.

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

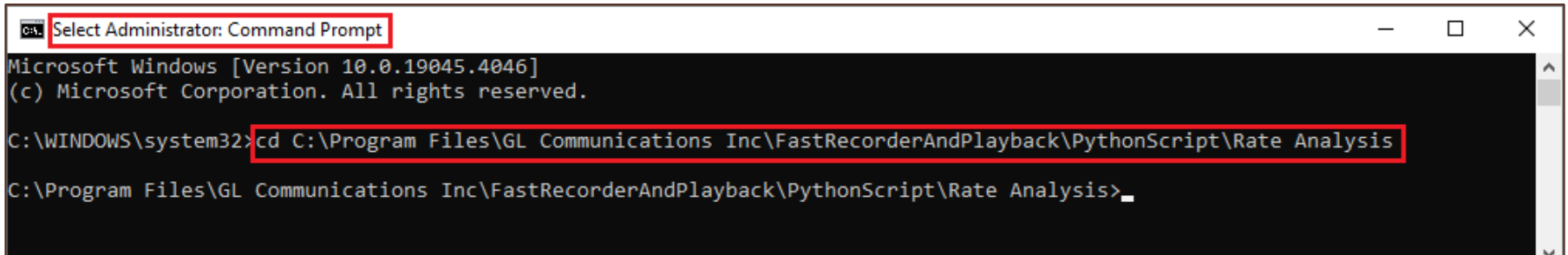
Compress Extracted Files Packet Slicing

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

Rate Analysis using Command Prompt

- To open the command console in administrator mode
- Go to the path “C:\Program Files\GL Communications Inc\FastRecorderAndPlayback\PythonScript\Rate Analysis” and copy the same path
- Type the below command in the console
cd “C:\Program Files\GL Communications Inc\FastRecorderAndPlayback\PythonScript\Rate Analysis”. Click **Enter**



The screenshot shows a Windows Command Prompt window titled "Select Administrator: Command Prompt". The window content is as follows:

```
Microsoft Windows [Version 10.0.19045.4046]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\WINDOWS\system32>cd C:\Program Files\GL Communications Inc\FastRecorderAndPlayback\PythonScript\Rate Analysis  
C:\Program Files\GL Communications Inc\FastRecorderAndPlayback\PythonScript\Rate Analysis>_
```

Rate Analysis using Command Prompt (Contd.)

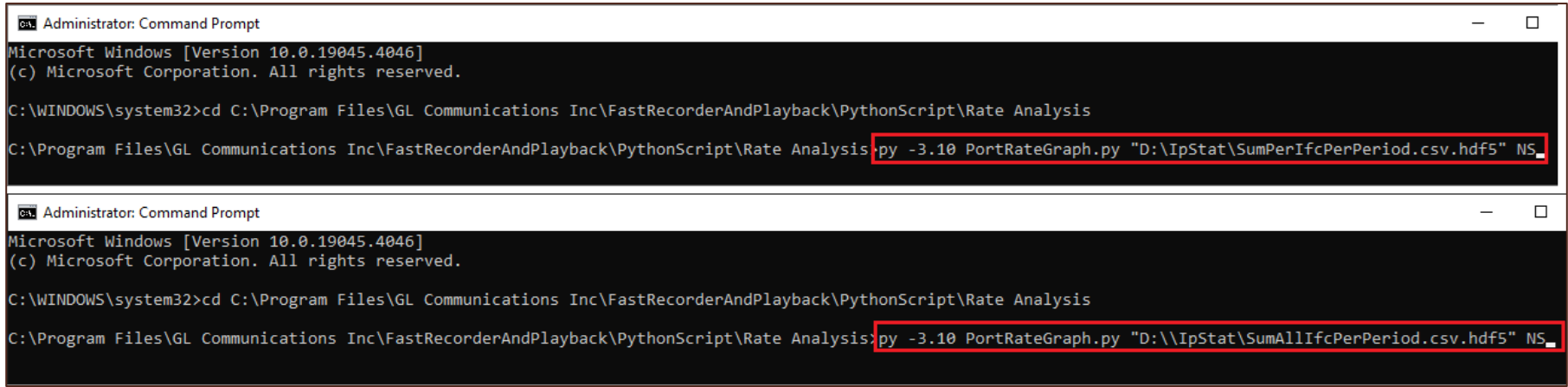
- Run the below commands

For Rate analysis of individual recorded ports:

py -3.10 PortRateGraph.py "D:\\IpStat\\SumPerIfcPerPeriod.csv.hdf5" NS. Click **Enter**

For Rate analysis of all recorded ports:

py -3.10 PortRateGraph.py "D:\\IpStat\\SumAllIfcPerPeriod.csv.hdf5" NS. Click **Enter**



The image shows two screenshots of a Windows Command Prompt window. The first screenshot shows the command prompt with the following text: "Administrator: Command Prompt", "Microsoft Windows [Version 10.0.19045.4046]", "(c) Microsoft Corporation. All rights reserved.", "C:\\WINDOWS\\system32>cd C:\\Program Files\\GL Communications Inc\\FastRecorderAndPlayback\\PythonScript\\Rate Analysis", and "C:\\Program Files\\GL Communications Inc\\FastRecorderAndPlayback\\PythonScript\\Rate Analysis>py -3.10 PortRateGraph.py "D:\\IpStat\\SumPerIfcPerPeriod.csv.hdf5" NS". The second screenshot shows the same command prompt with the following text: "Administrator: Command Prompt", "Microsoft Windows [Version 10.0.19045.4046]", "(c) Microsoft Corporation. All rights reserved.", "C:\\WINDOWS\\system32>cd C:\\Program Files\\GL Communications Inc\\FastRecorderAndPlayback\\PythonScript\\Rate Analysis", and "C:\\Program Files\\GL Communications Inc\\FastRecorderAndPlayback\\PythonScript\\Rate Analysis>py -3.10 PortRateGraph.py "D:\\IpStat\\SumAllIfcPerPeriod.csv.hdf5" NS".

Rate Analysis using Command Prompt (Contd.)

- The following table provides syntax and description

Syntax	Description
py -3.10	Indicates Python 3.10 version.
PortRateGraph.py	Python script used to run the rate analysis.
D:\\lpStat\\SumPerIfcPerPeriod.csv. hdf5	The specified HDF5 file path for per port. Users can customize the path as needed.
D:\\lpStat\\SumAllIfcPerPeriod.csv. hdf5	The specified HDF5 file path for all ports. Users can customize the path as needed.
NS	Time format for IP TCP UDP Analysis tool generated HDF5 file.

Thank you