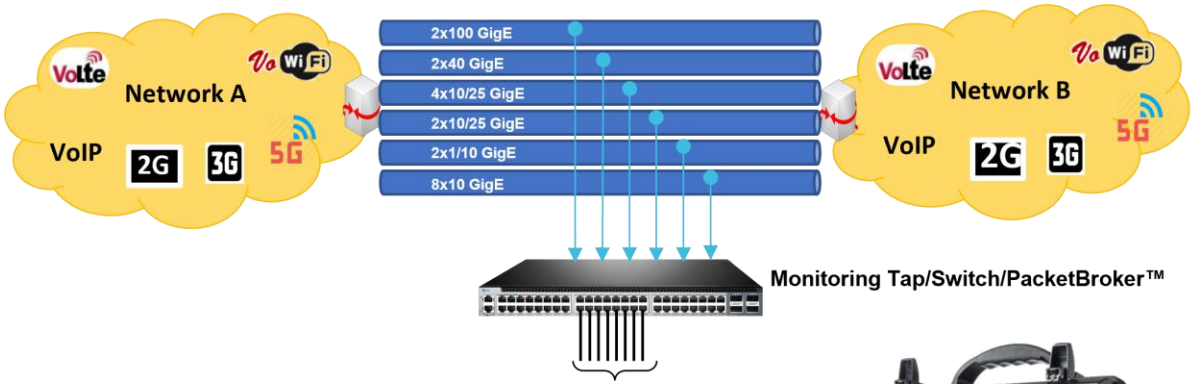
FastRecorder™ and PacketExtractor™ for Monitoring IP Networks

GL Communications Inc.
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



2 x 100 GigE / 2 x 40 GigE / 4 x 10/25 GigE /

2 x 10/25 GigE / 2 x 1/10 GigE / 8 x 10 GigE /

4 x 1/10/25 GigE

FastRecorder™ and PacketExtractor™
PacketScan™ HD, Wireshark®

- Nano second timestamping
- Wirespeed filtering
- Packet slicing
- Continuous lossless capture
- Error free capture
- IPv4 and IPv6

GL Communications

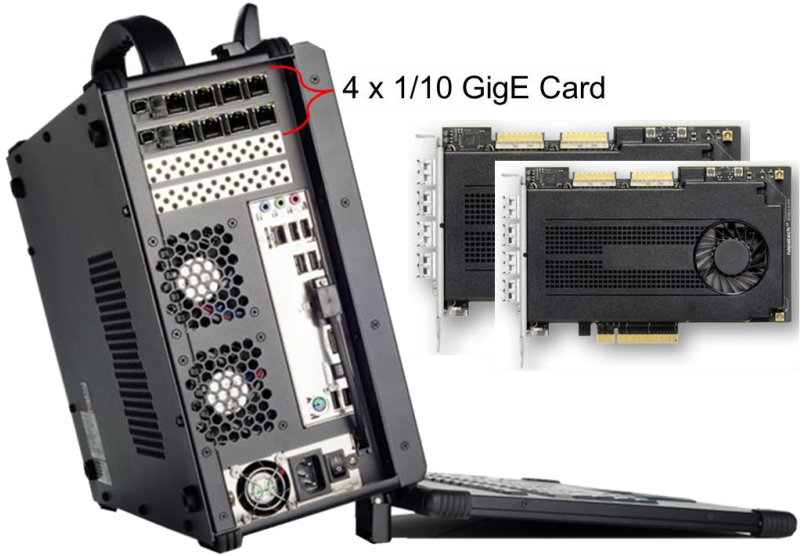
PacketScan™ HD, FastRecorder™ & PacketExtractor™

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

**Also available as a rack mounted unit

GL Communications

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



PacketScan™ HD - Lunch Box

Lunchbox specs are:

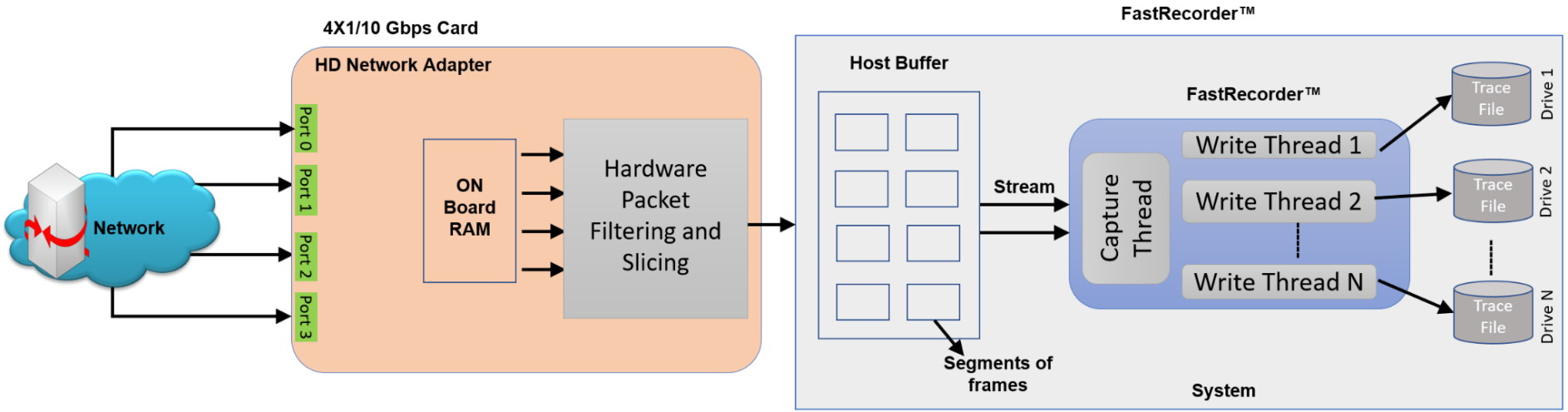
- Intel Xeon Silver 4210
- 64GB RAM
- 500GB SSD for OS
- 4x 3.84TB NVME SSD

GL Communications

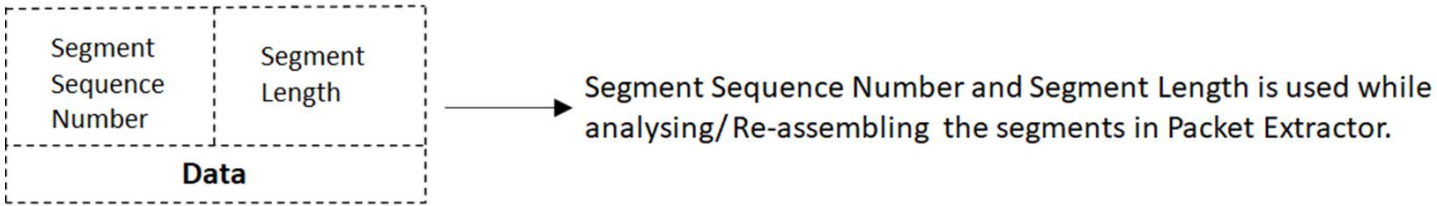
What the Software Does?

- 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

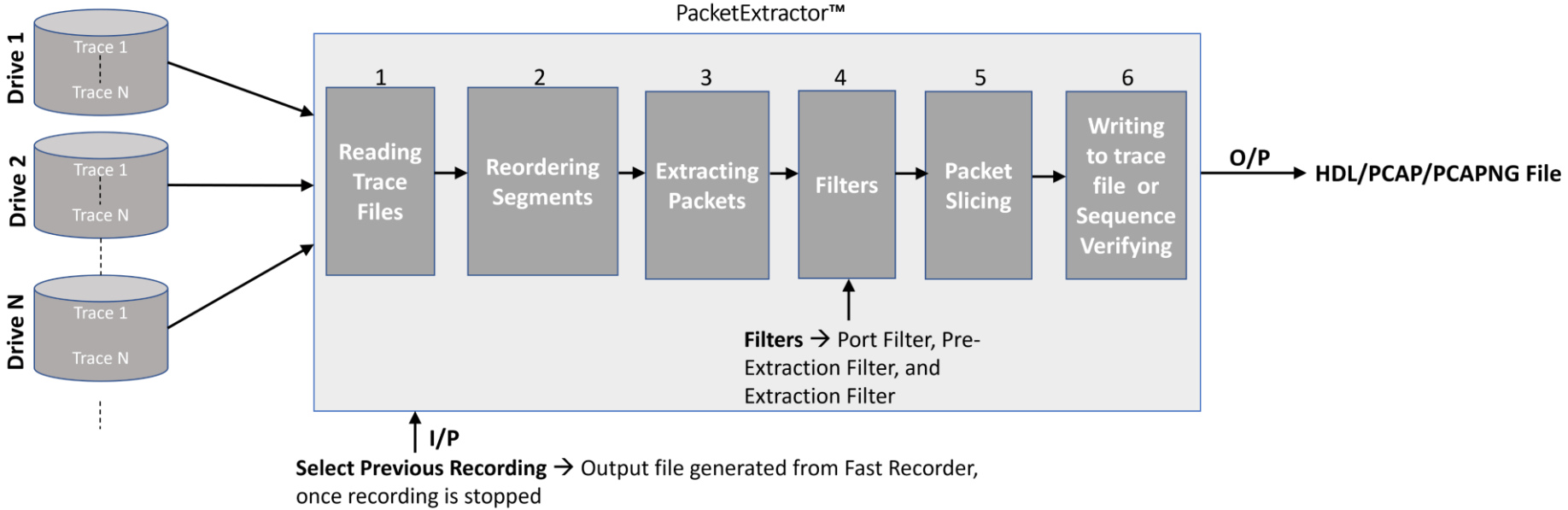


Buffer segments stored internally in files:



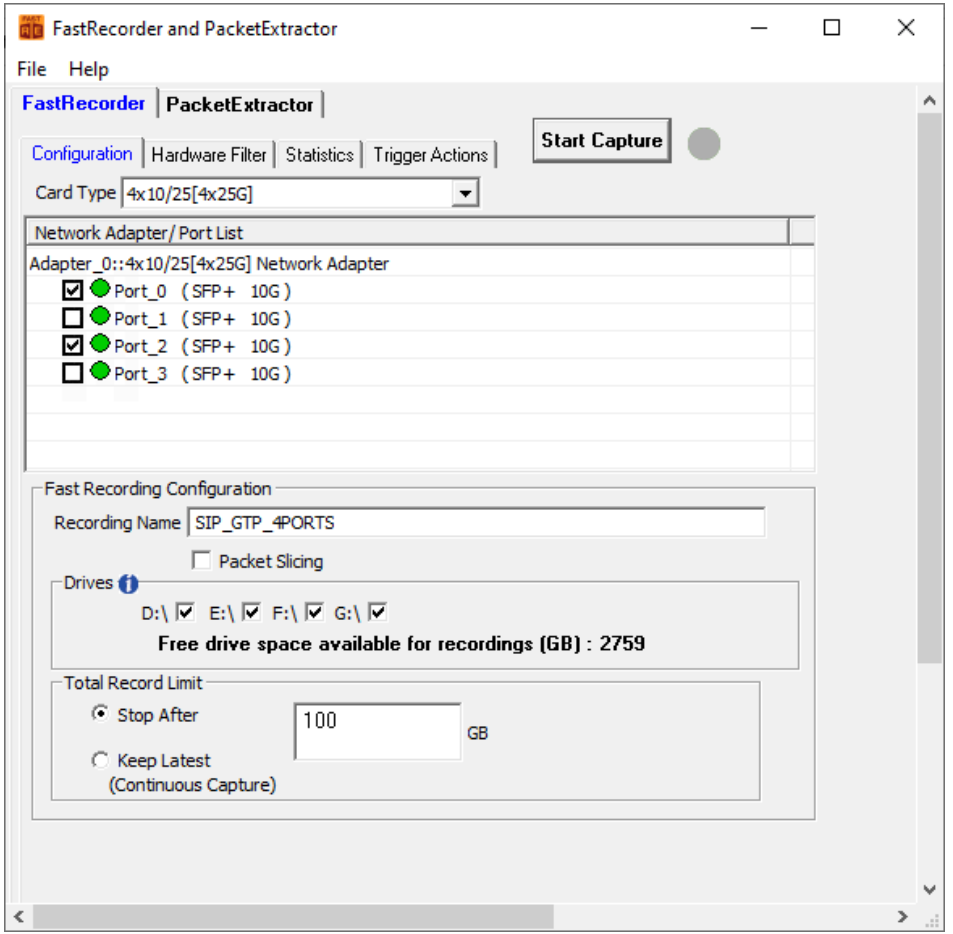
GL Communications

PacketExtractor™ Architecture



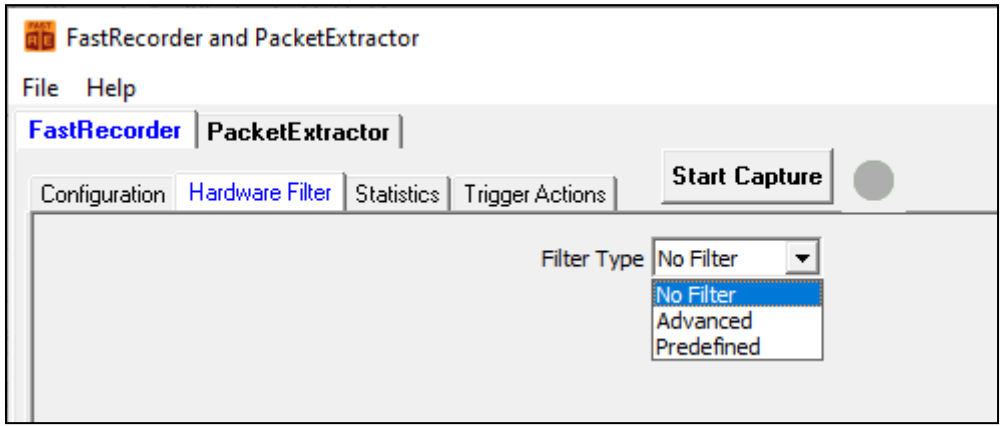
FastRecorder™ Operations

- 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



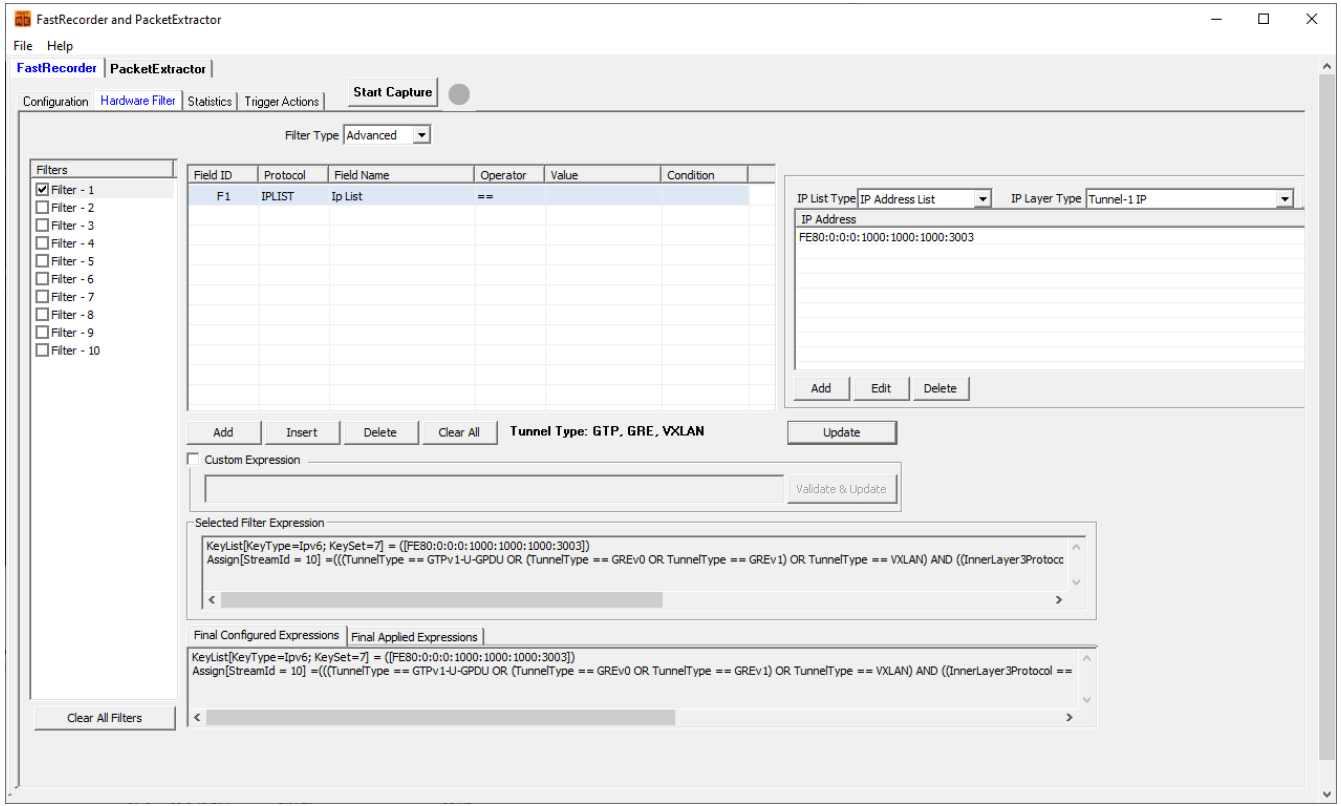
Hardware Filters

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



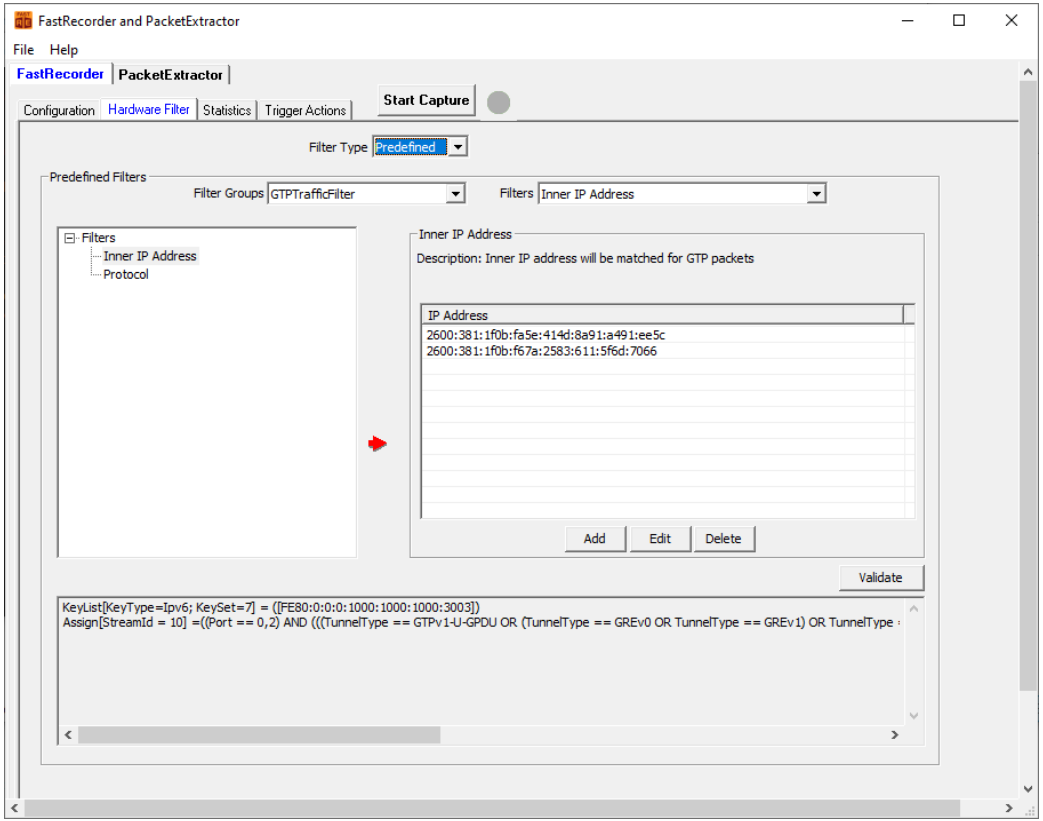
Advanced Hardware Filter Type

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



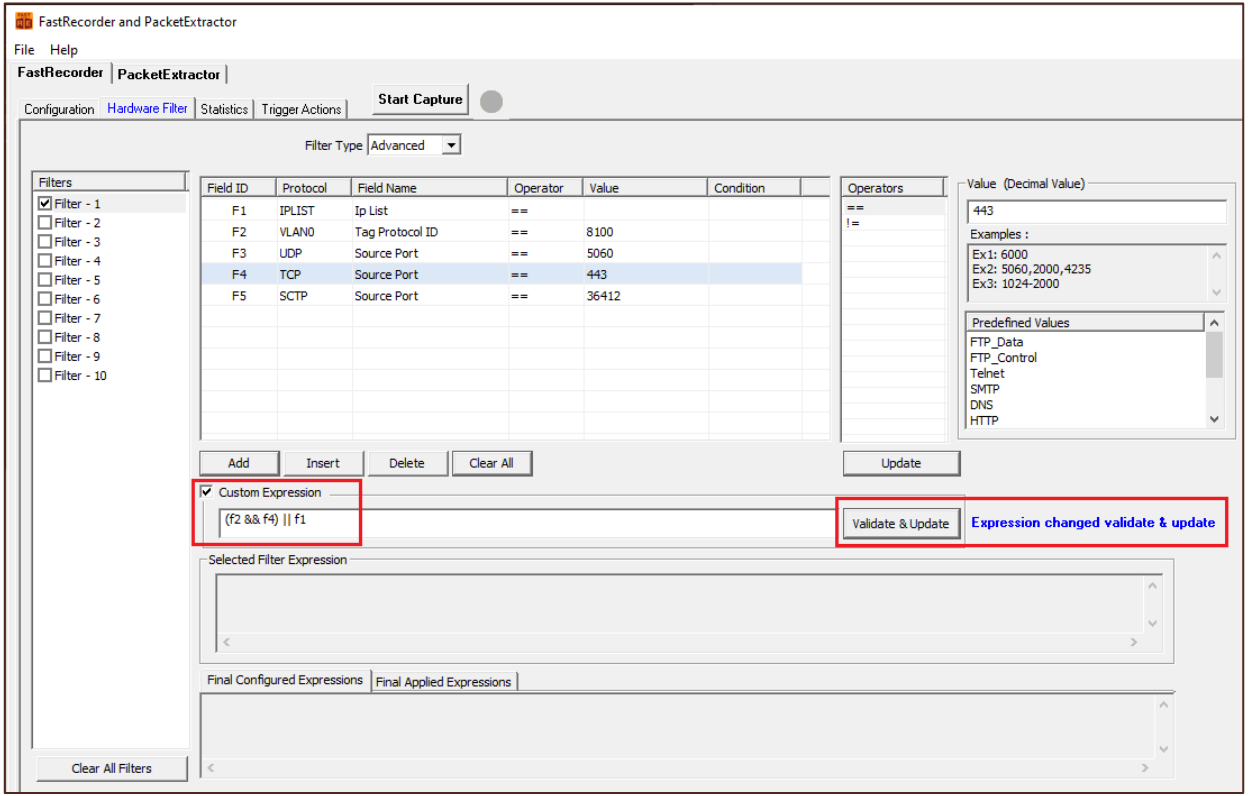
Predefined Hardware Filter Type

- 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

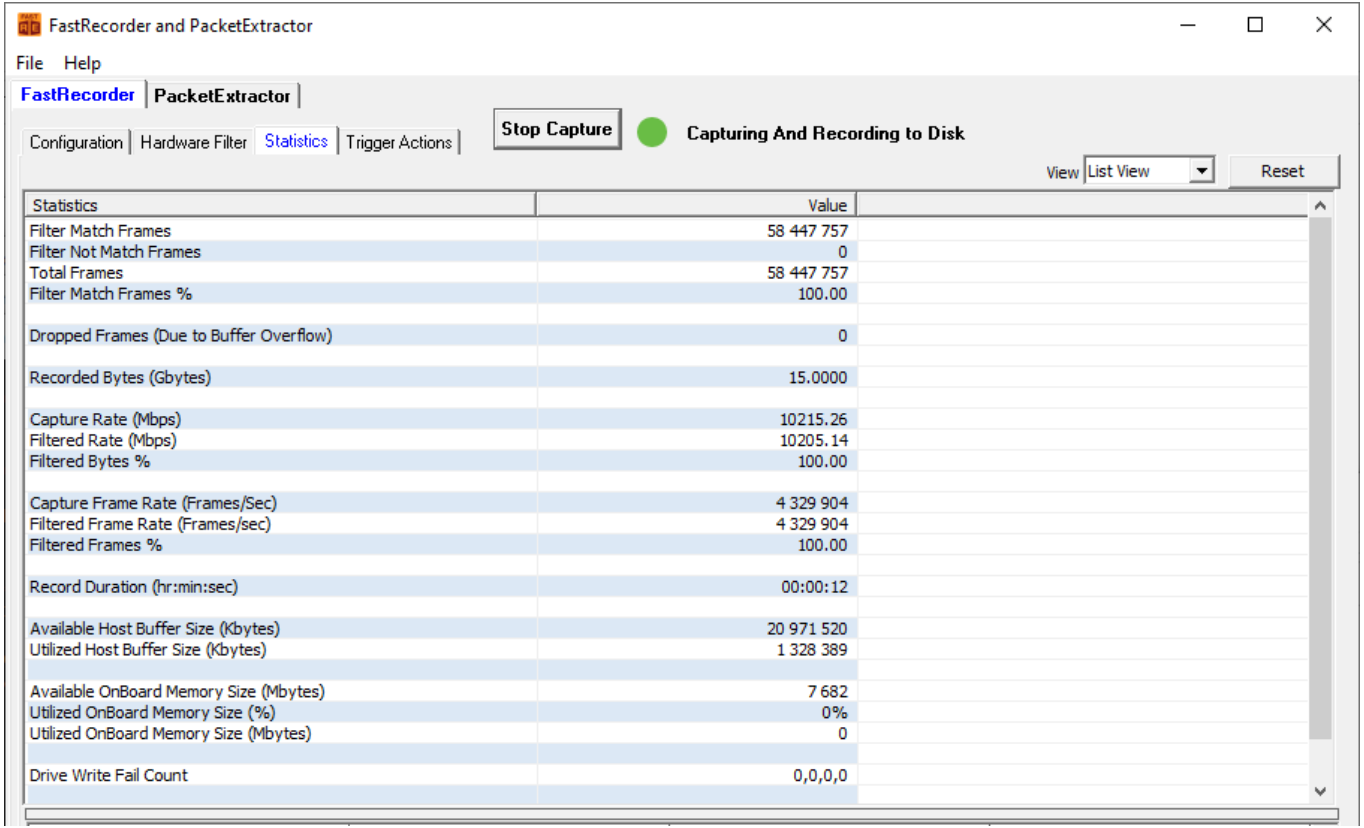


Custom Expression Filter

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



FastRecorder™ Statistics



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

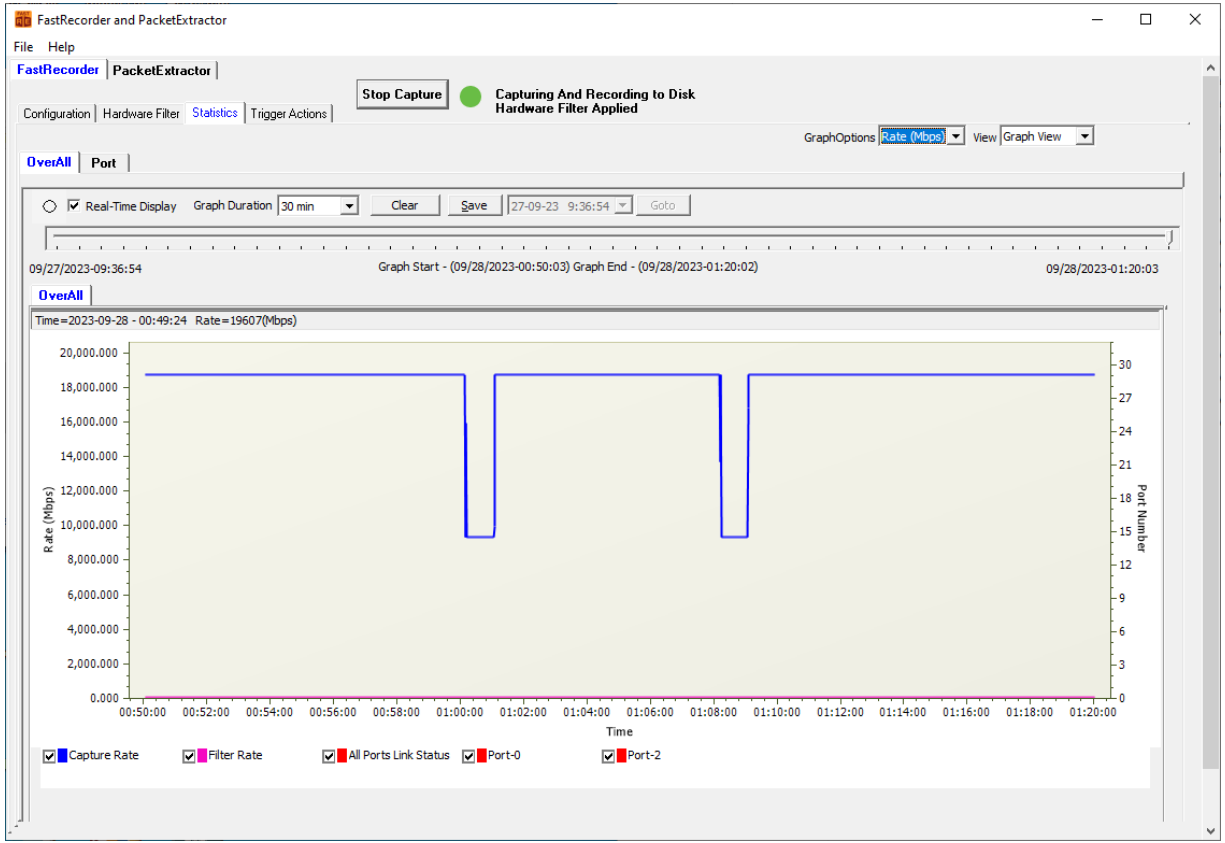
FastRecorder™ - Per Port and Aggregated Statistics

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			

GL Communications

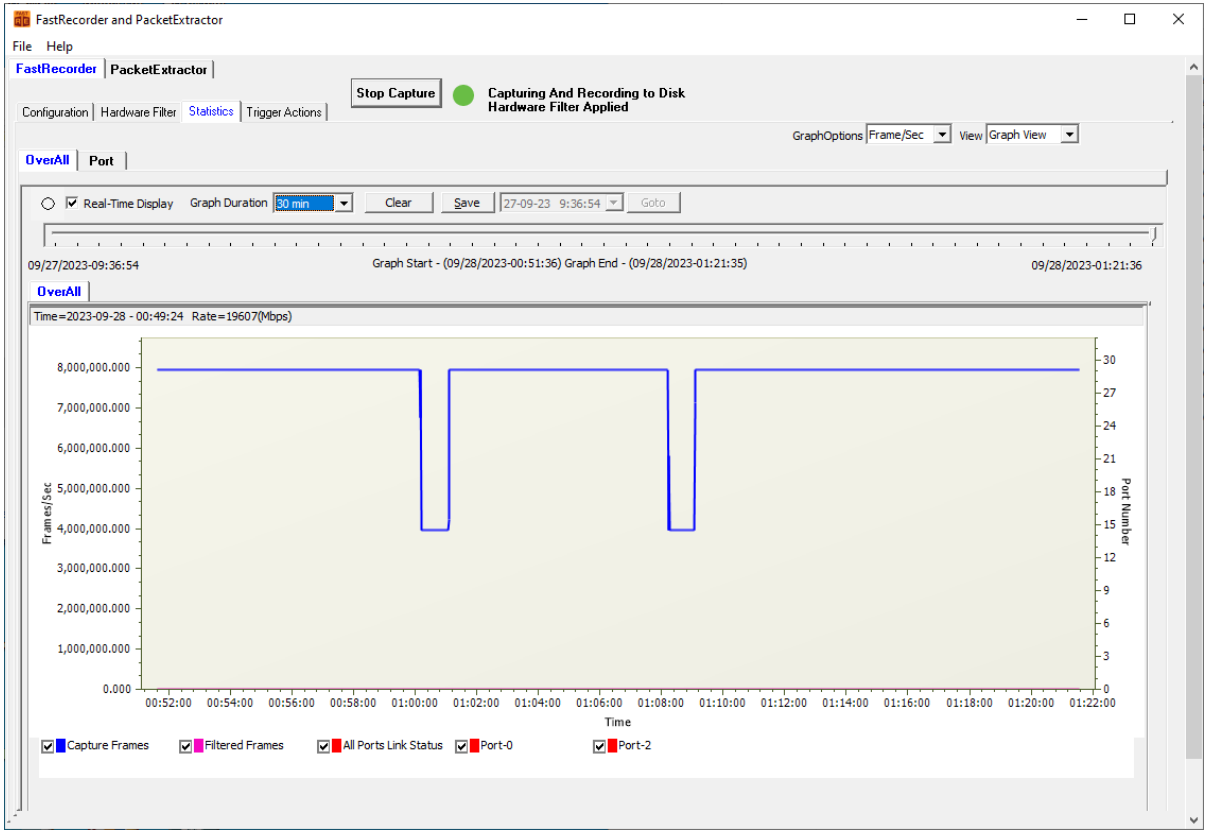
Real time and Historical Graph

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



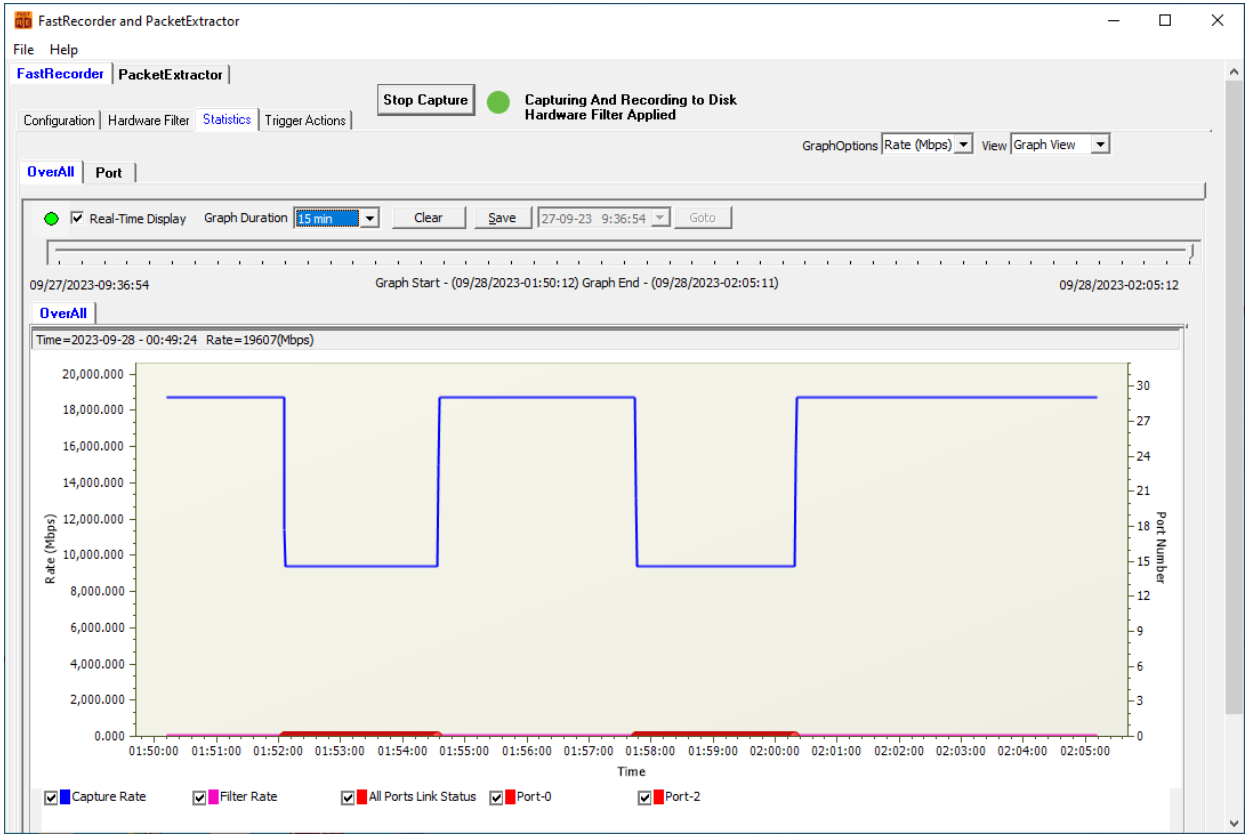
Realtime and Historical Graph (Contd.)

- Overall capture and frame rate for Frame/Secs



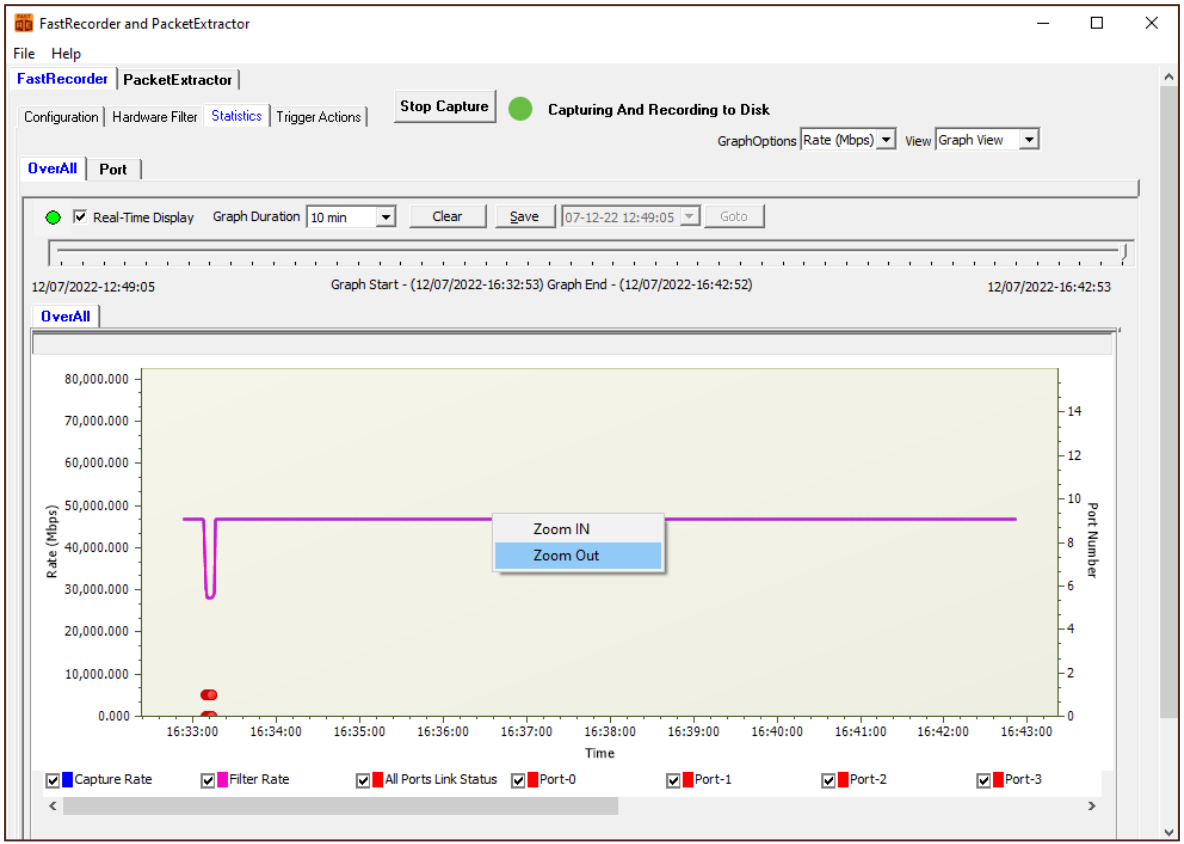
Graphs - Port Link Down

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



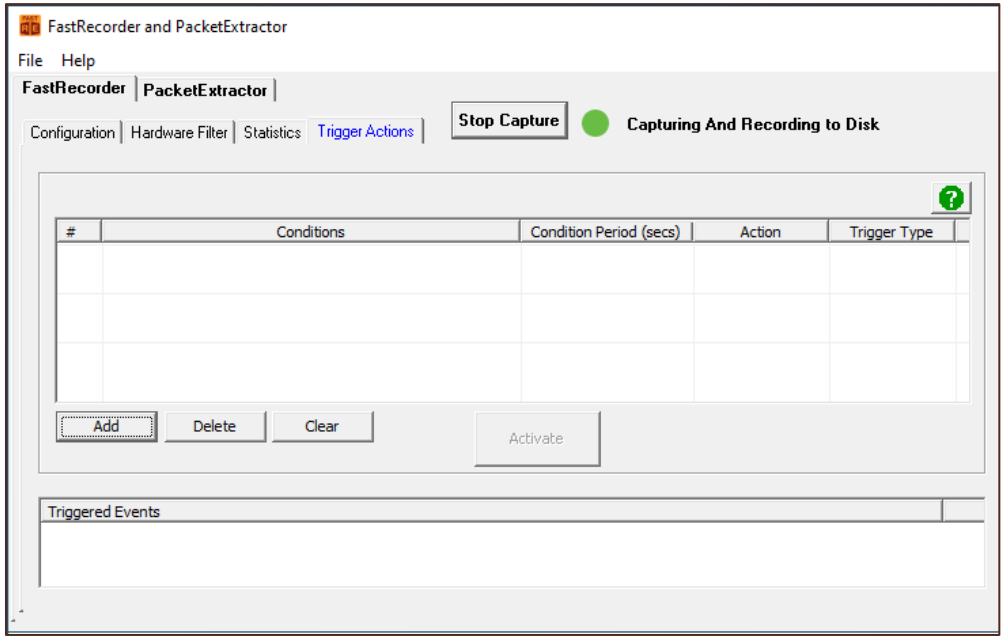
Graphs - Zoom IN and Zoom Out

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



Trigger based Start/Stop Recording

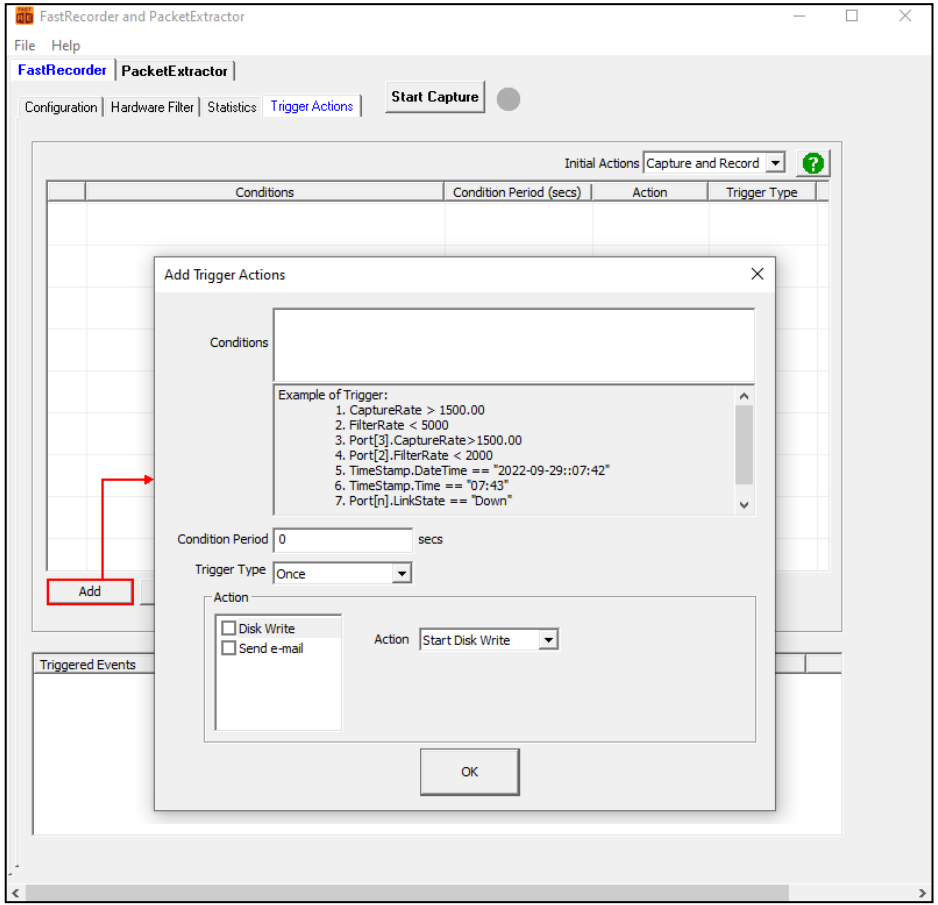
- User can specify the triggers to perform action based on the following conditions
  - CaptureRate (Mbps)
  - FilterRate (Mbps)
  - Port[n].CaptureRate (Mbps)
  - Port[n].FilterRate (Mbps): where n is port number
  - TimeStamp based



Adding Trigger Actions

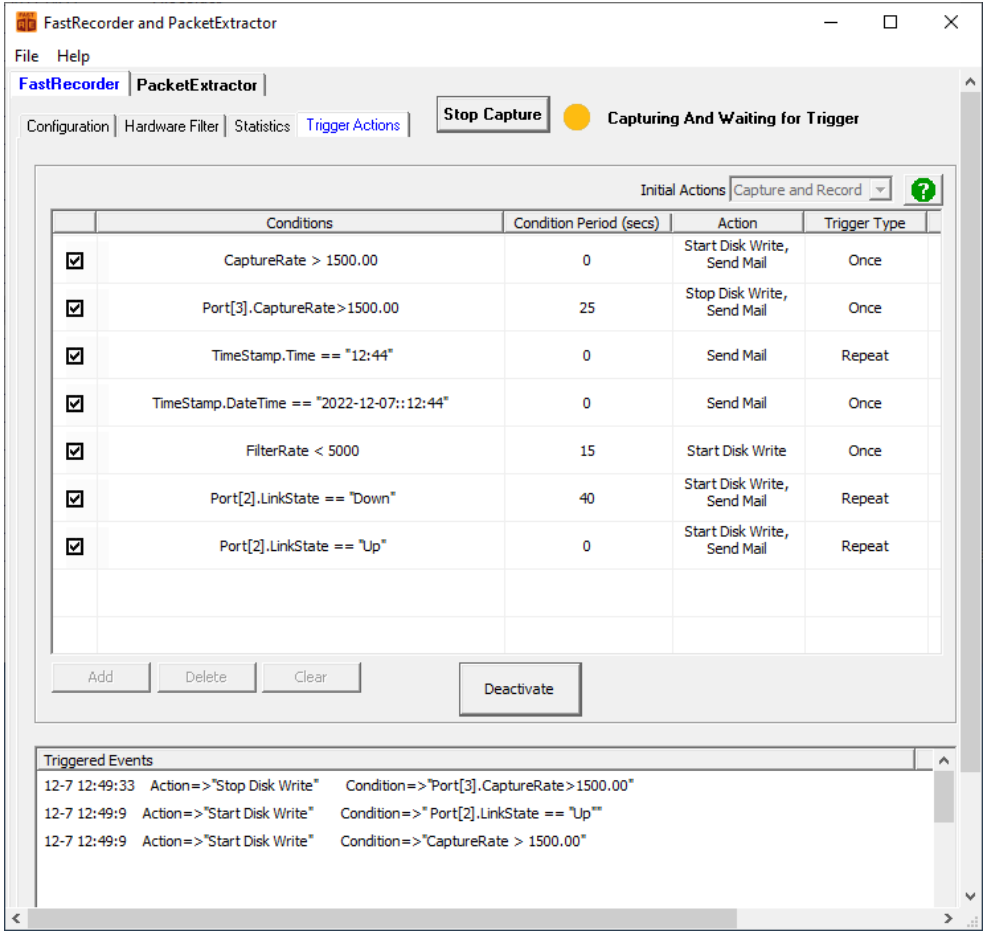
On the **Add Trigger Actions** window,

- 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**

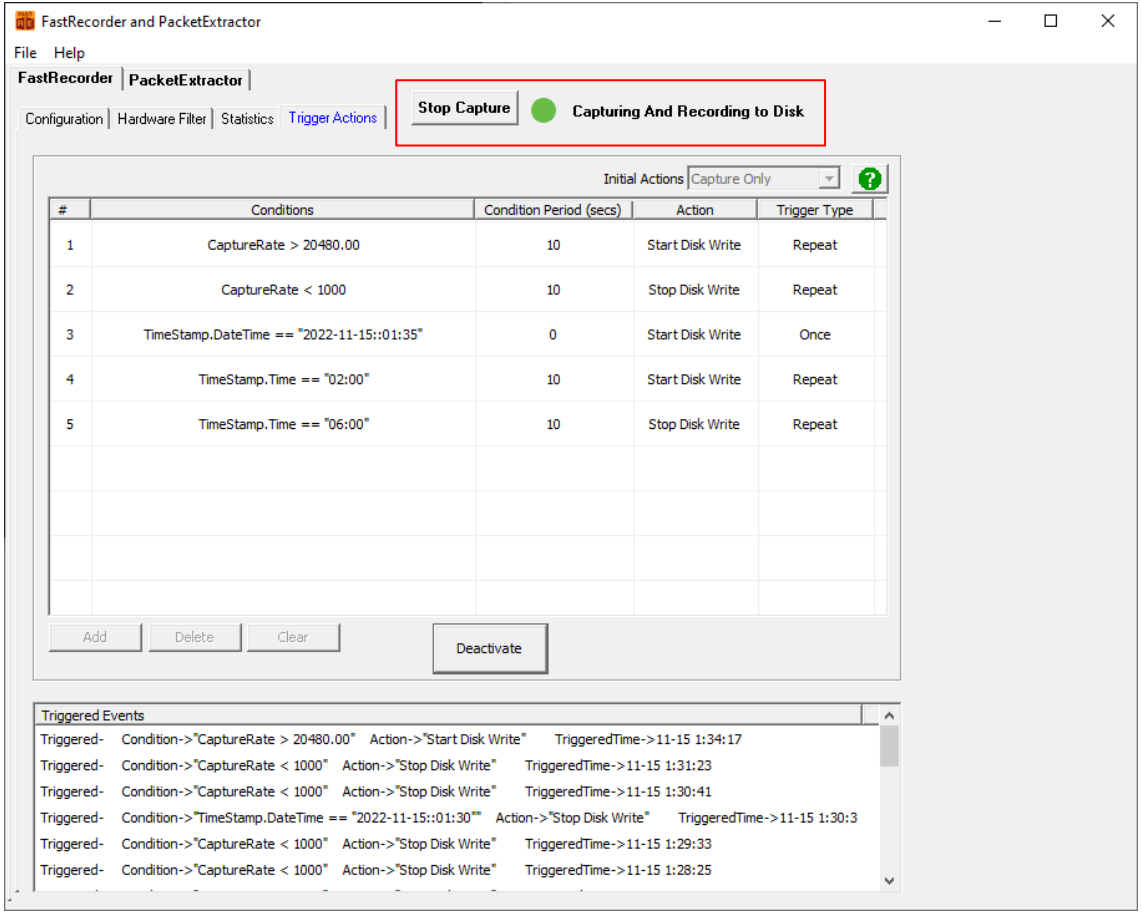


Activated Trigger Actions

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



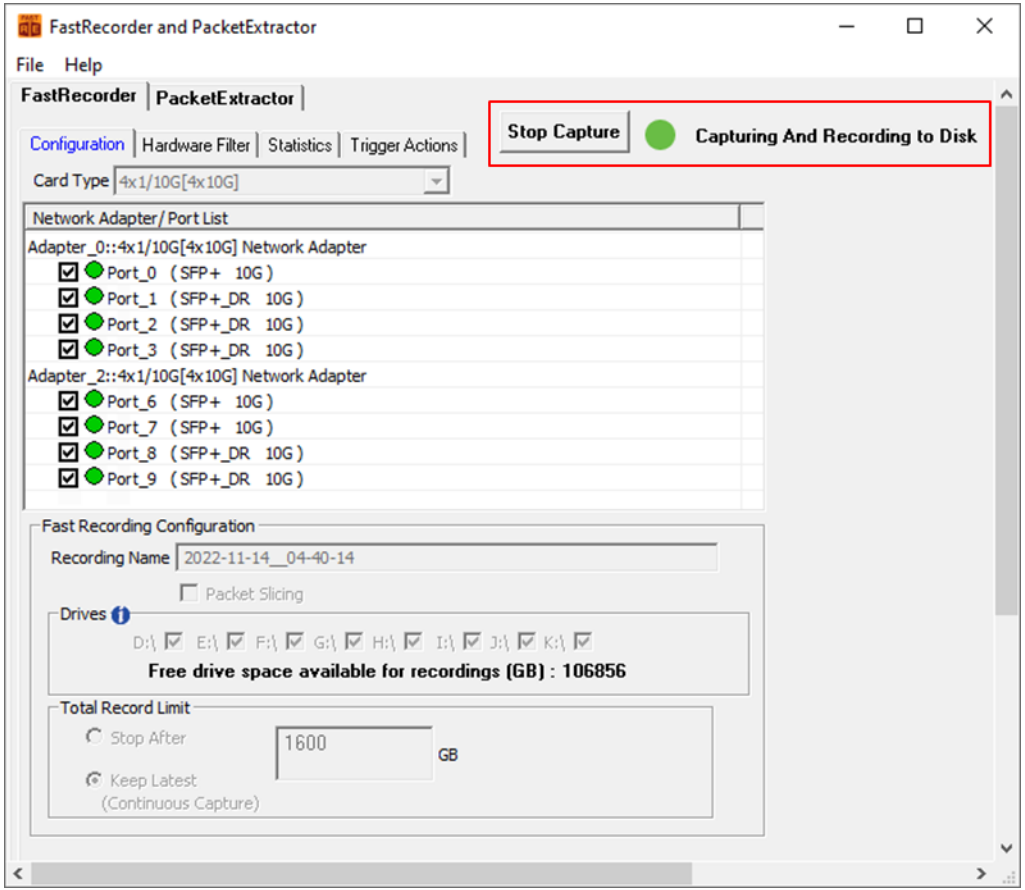
Activated Trigger Actions (Contd.)



GL Communications

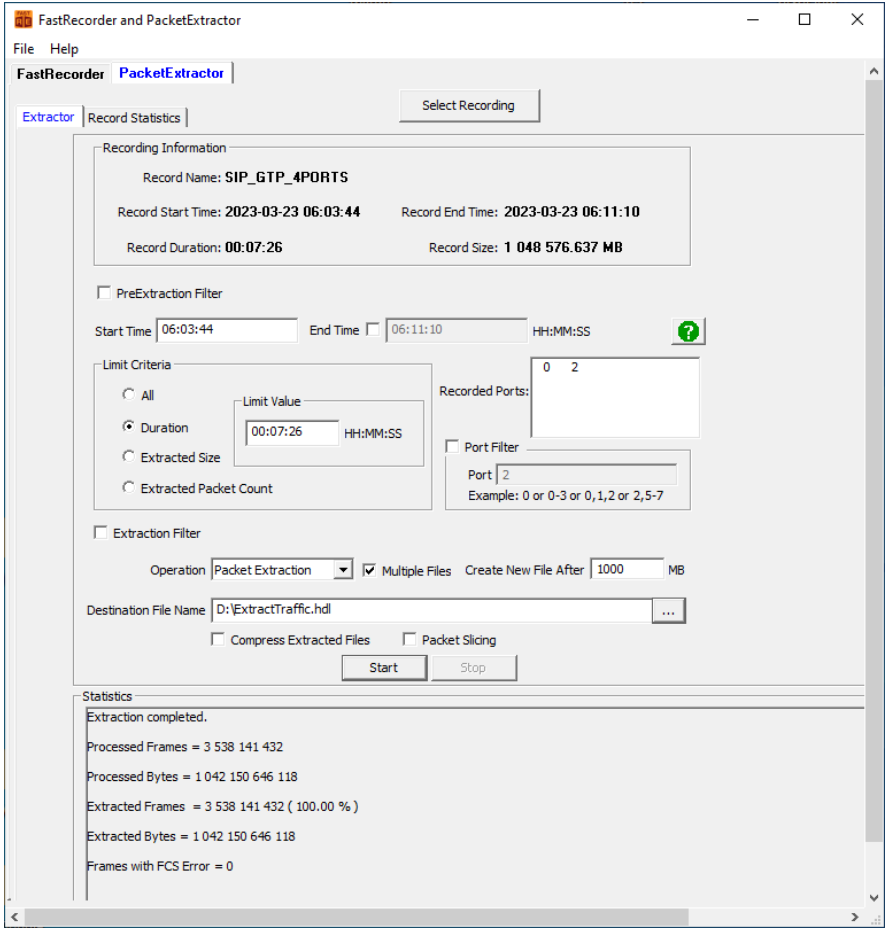
Recording with Default Name

- 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



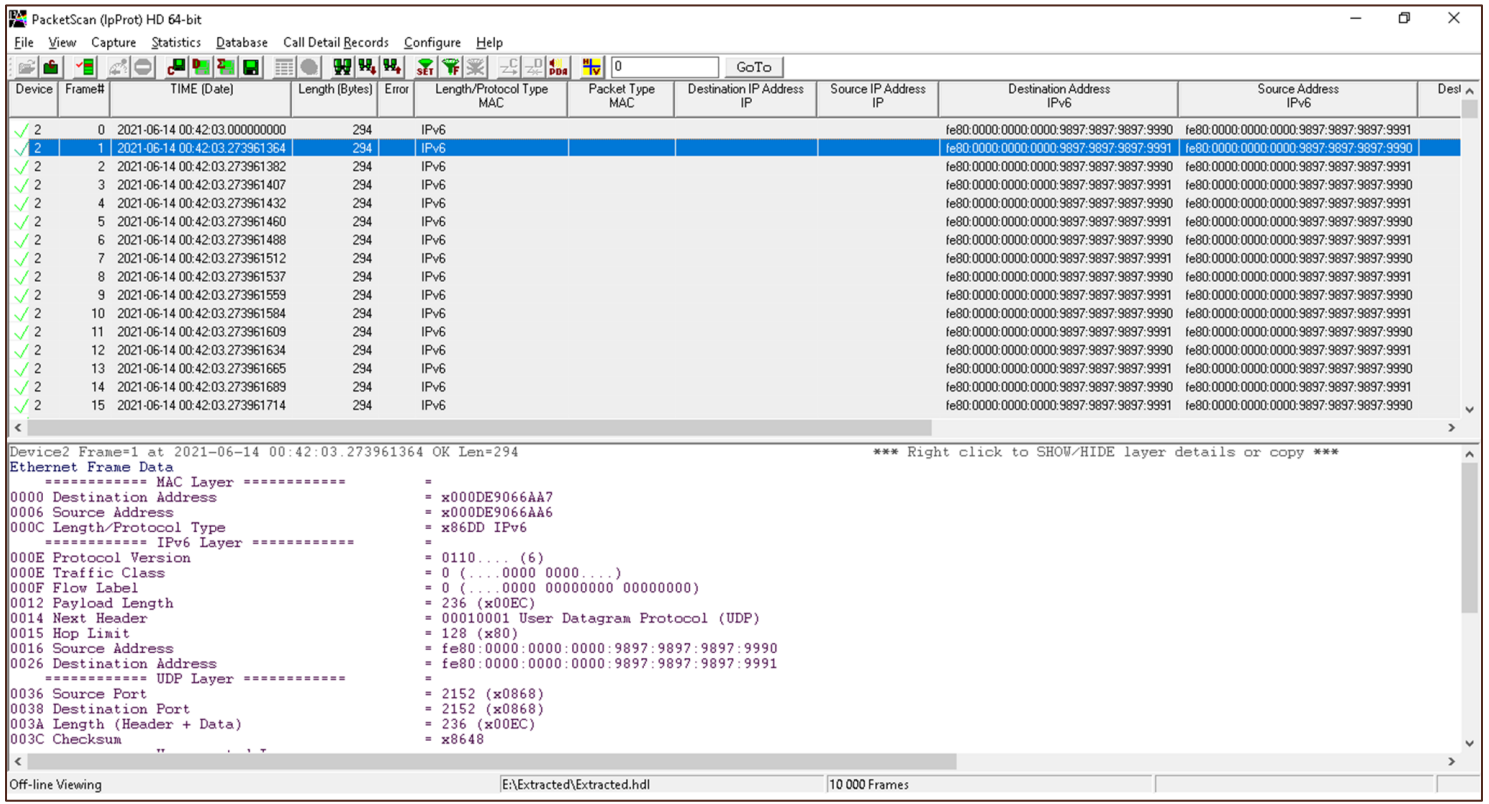
PacketExtractor™

- 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



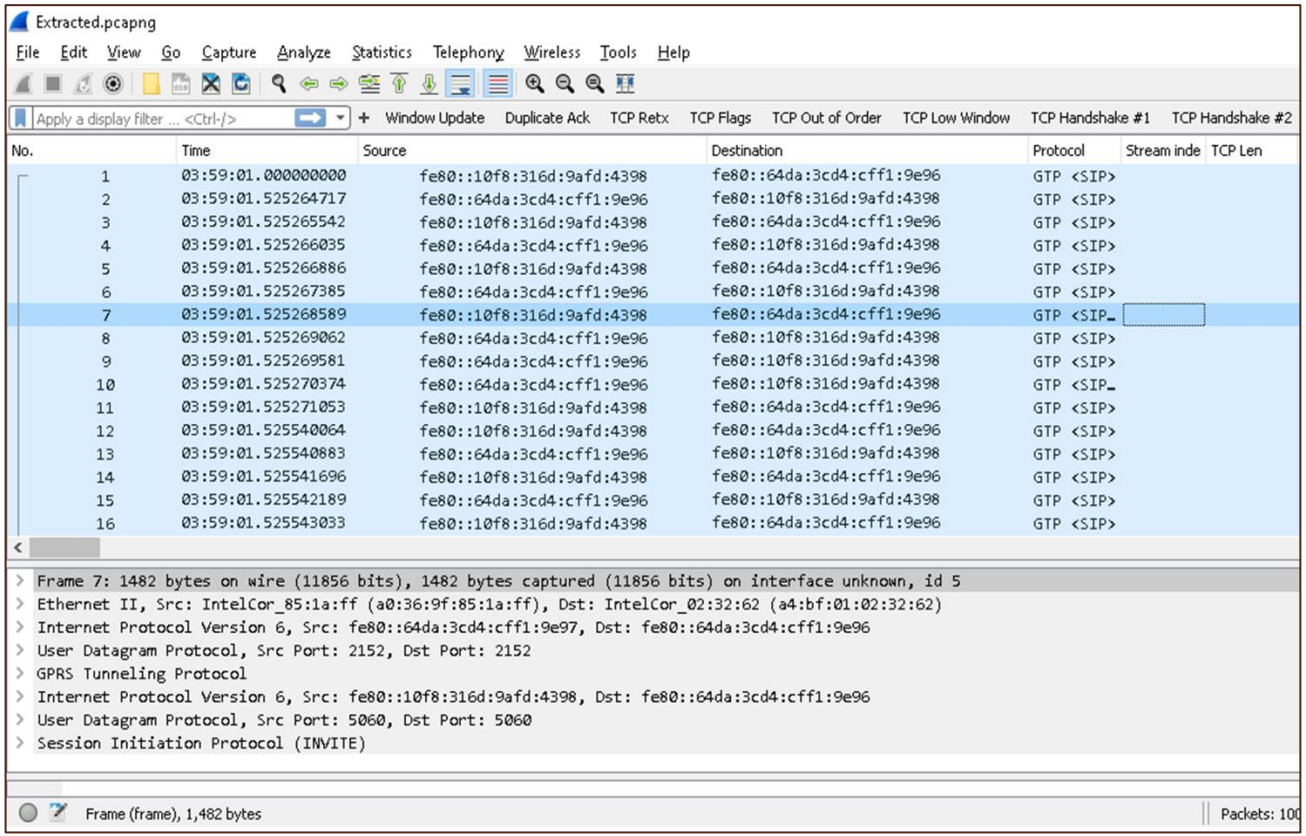
Analysis of Extracted Traffic using PacketScan™

- 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)

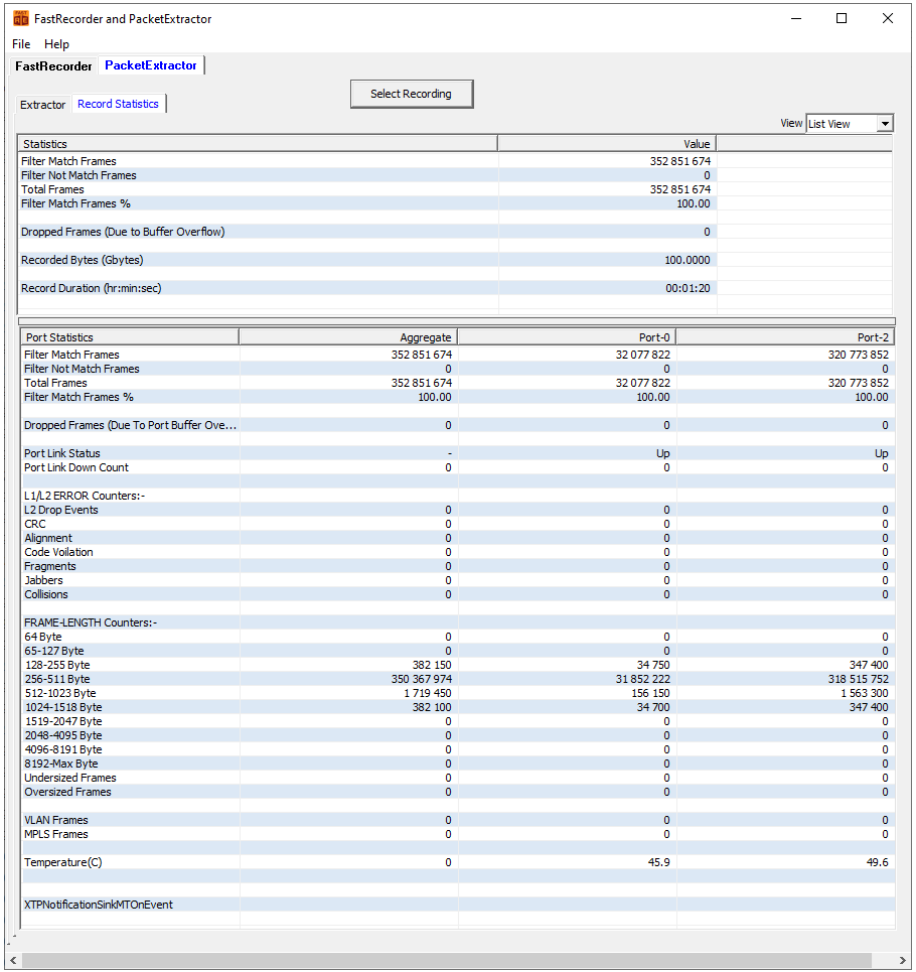


Analysis of Filtered Traffic in Wireshark®

- 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)



Recorded Statistics in PacketExtractor™



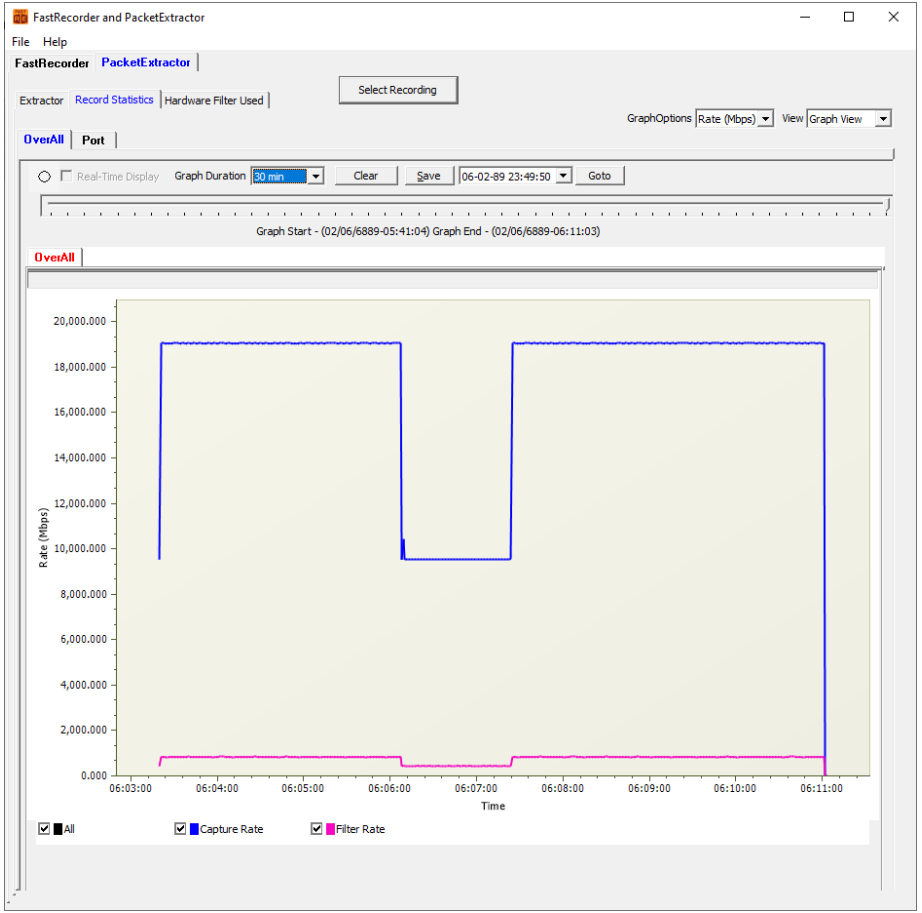
Statistics	Value
Filter Match Frames	352 851 674
Filter Not Match Frames	0
Total Frames	352 851 674
Filter Match Frames %	100.00
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	100.0000
Record Duration (hr:min:sec)	00:01:20

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 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	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
XTPNotificationSinkMTOnEvent			

GL Communications

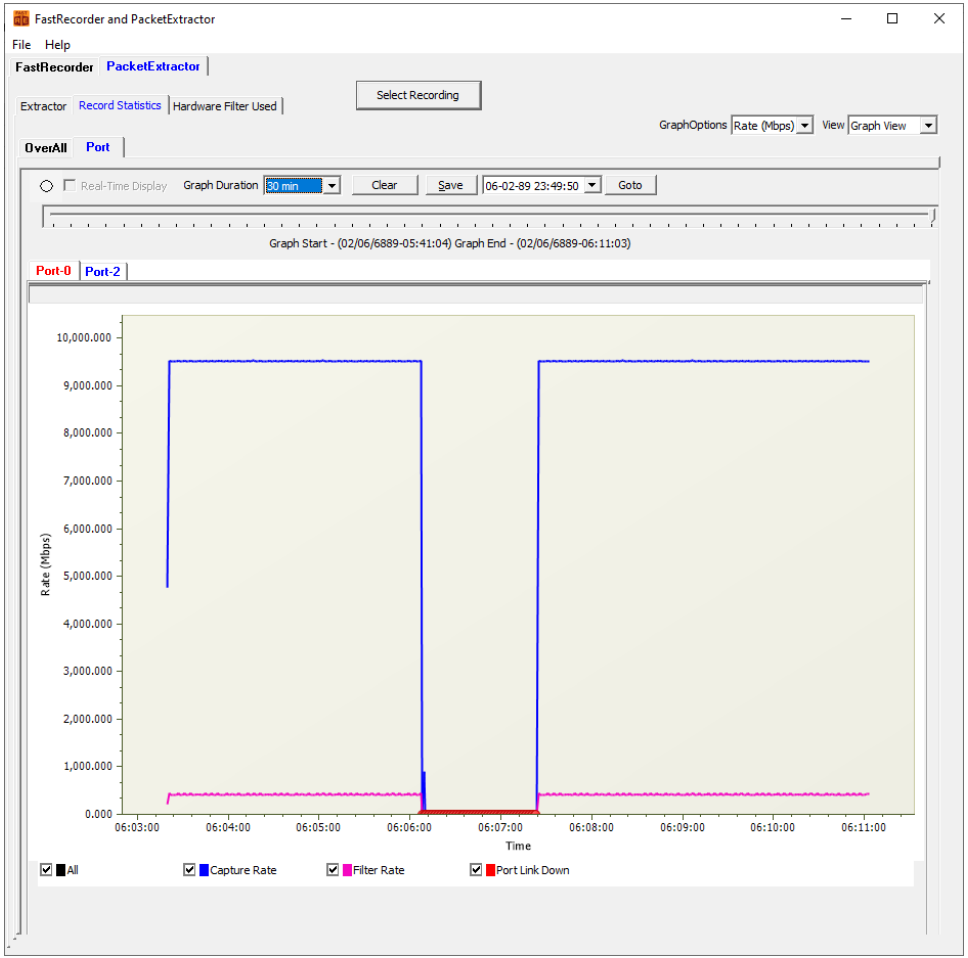
PacketExtractor™ - Overall Graph View

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

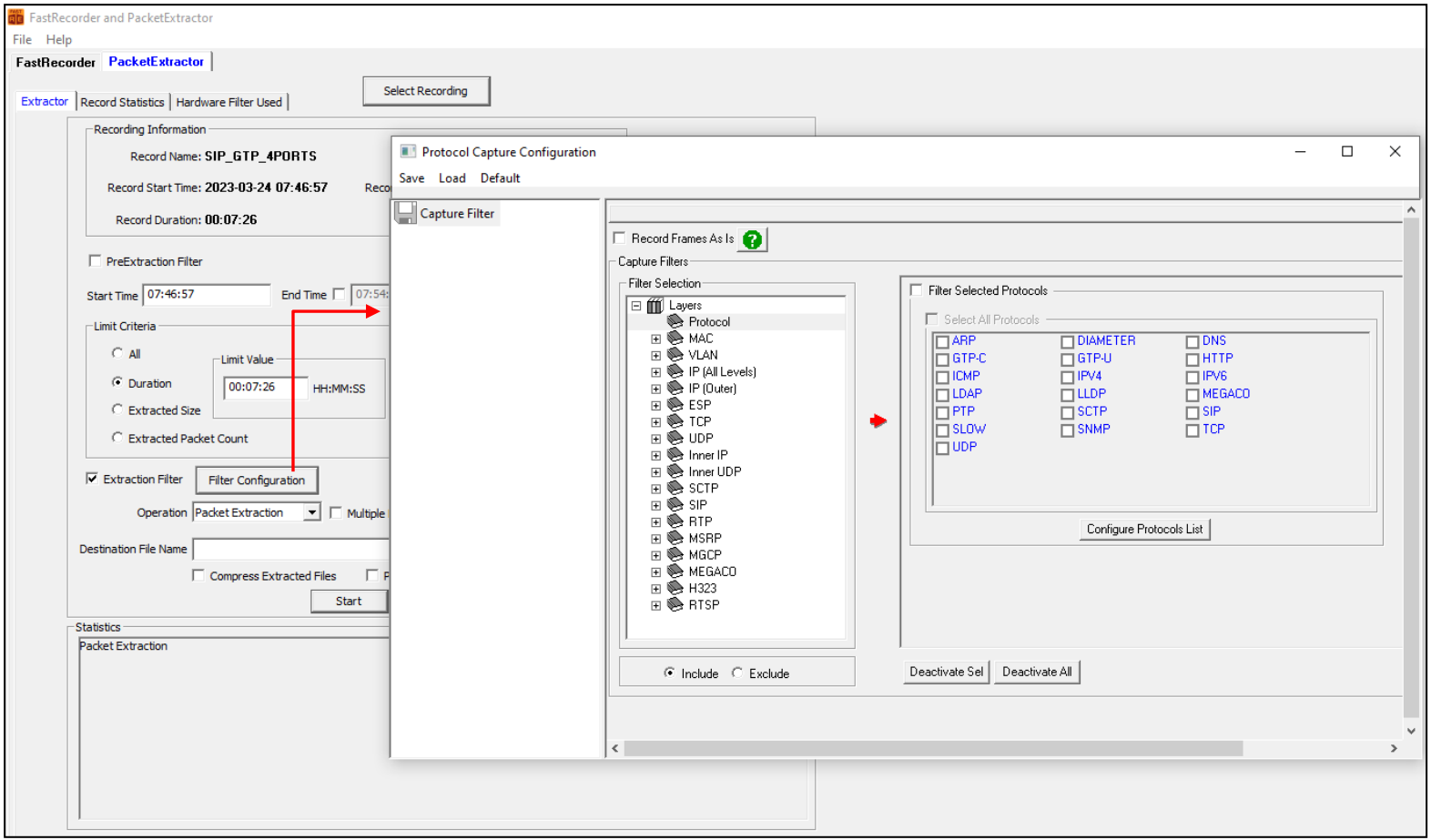


PacketExtractor™ - Port View

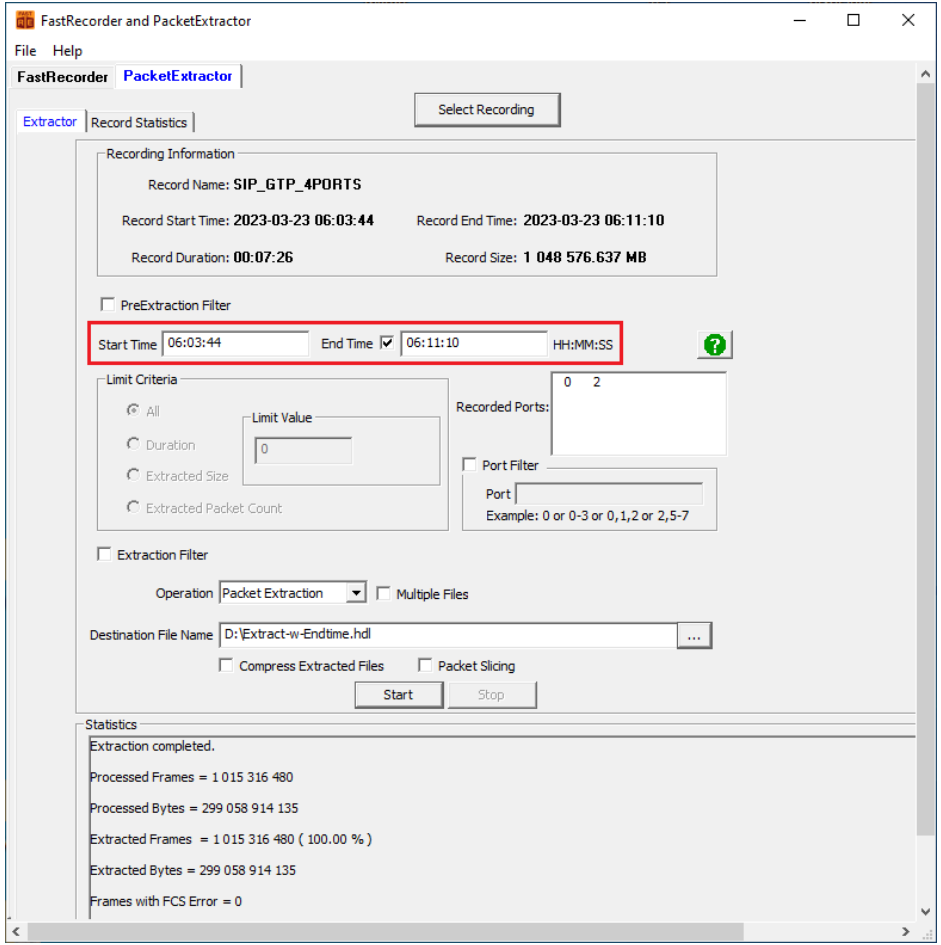
- User can view the per port **capture rate** and **filter rate** of the recorded file



Packet Extraction from the Recordings with Filter

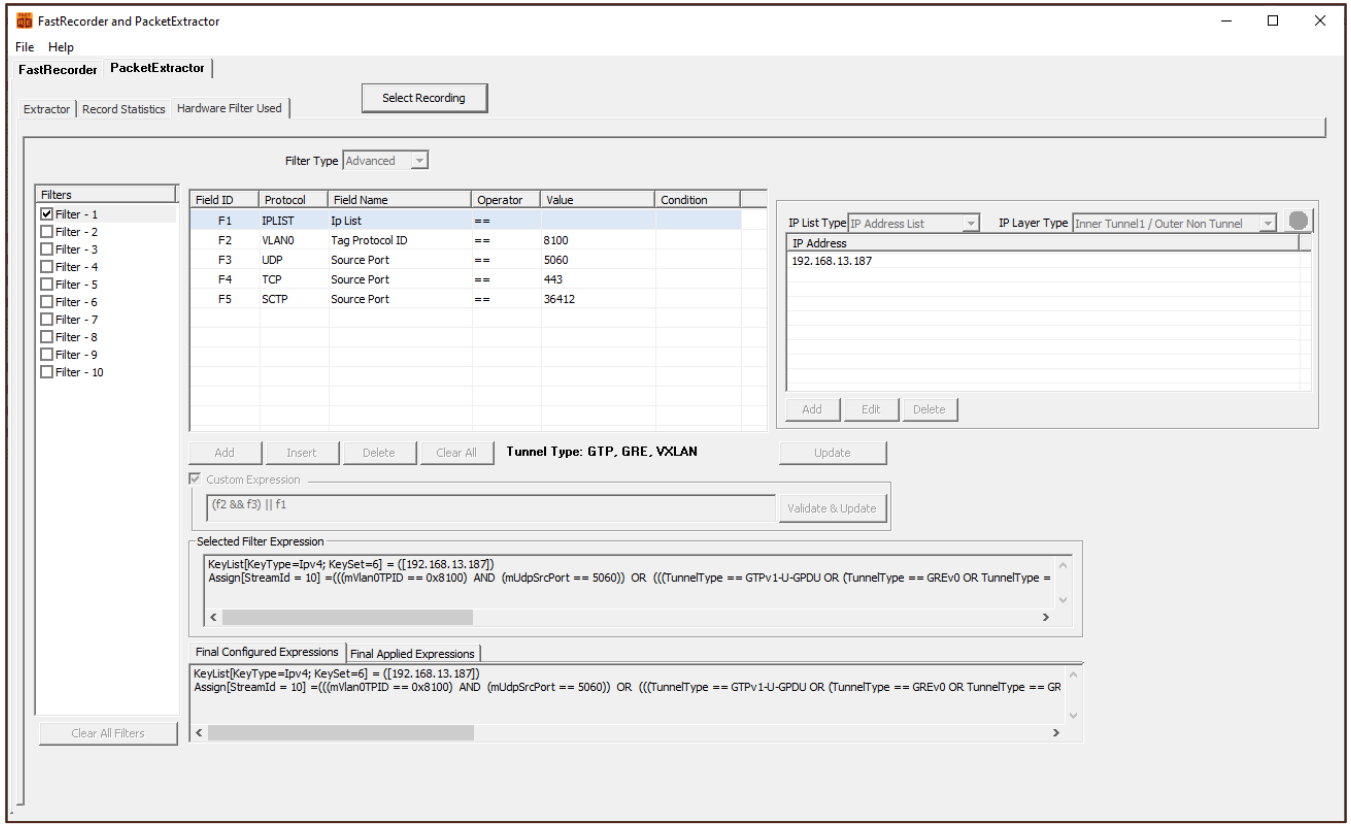


Specifying End Time for Packet Extraction

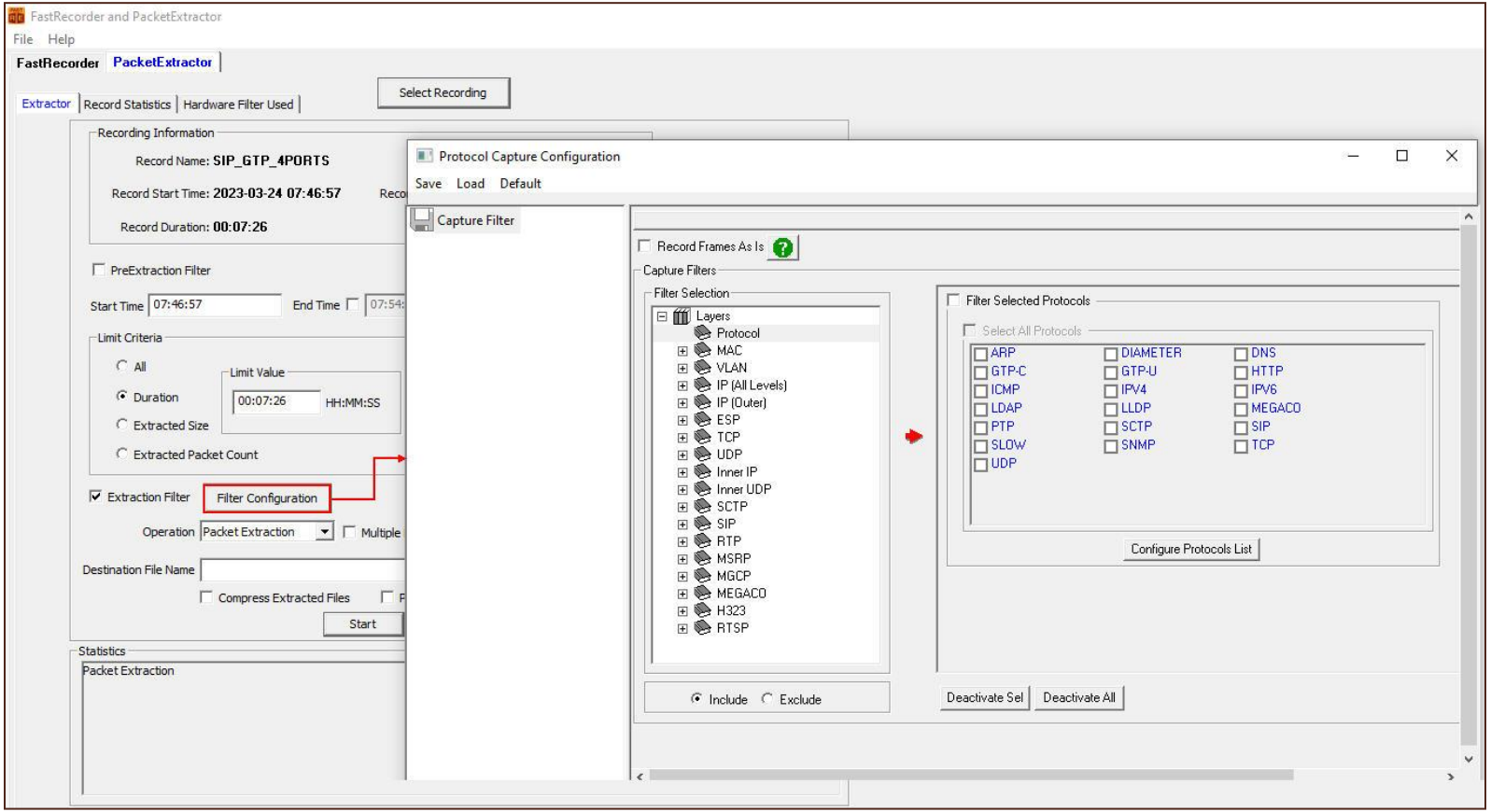


GL Communications

Hardware Filter Used while Recording



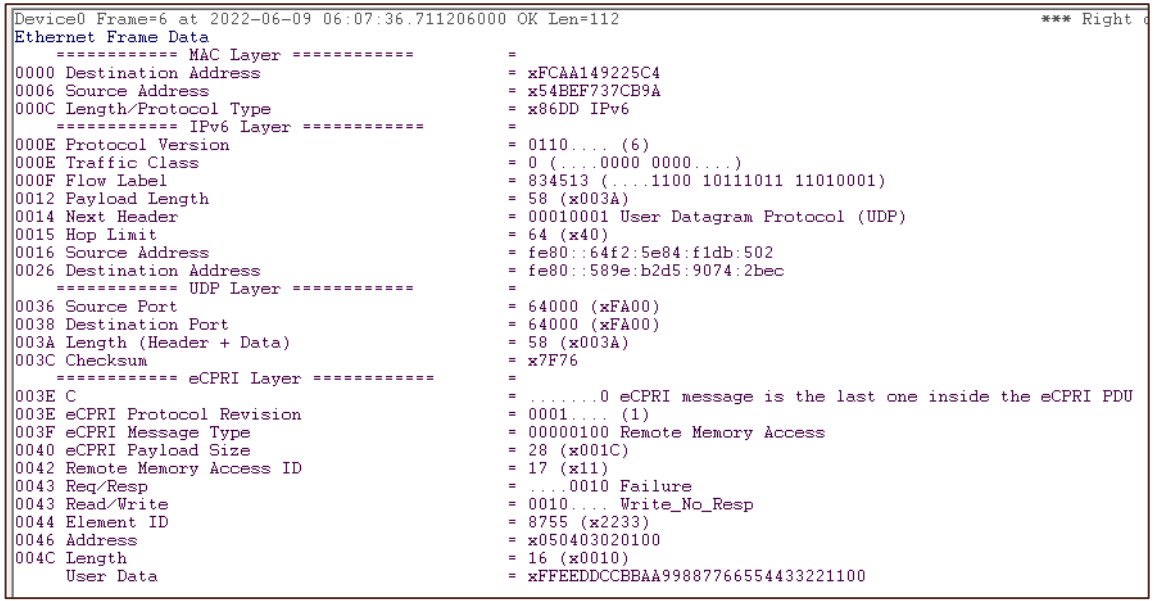
eCPRI Analysis



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:\Exracted** 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
```

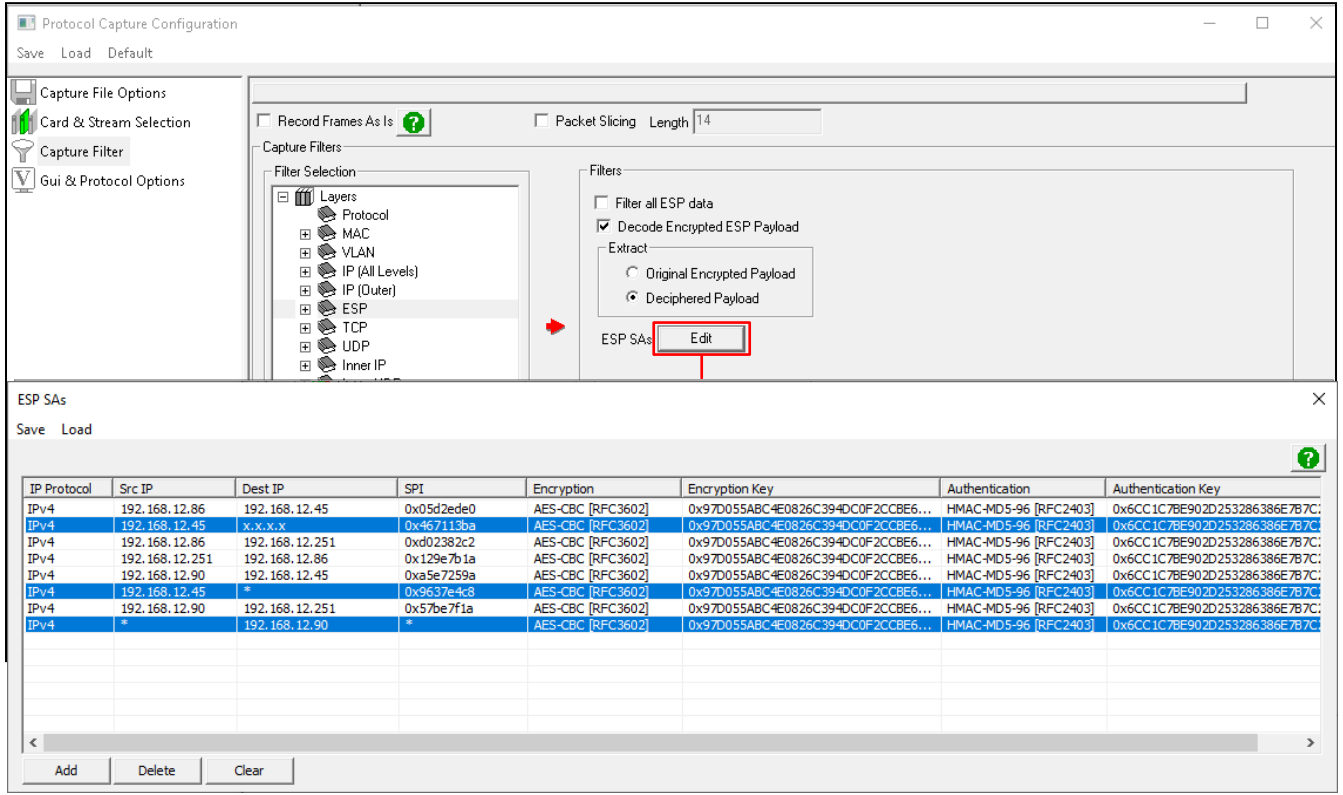
View eCPRI Layer Decode Details in PacketScan™ (Contd.)

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 ============ =
     ecpriPcid                                    =
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
```

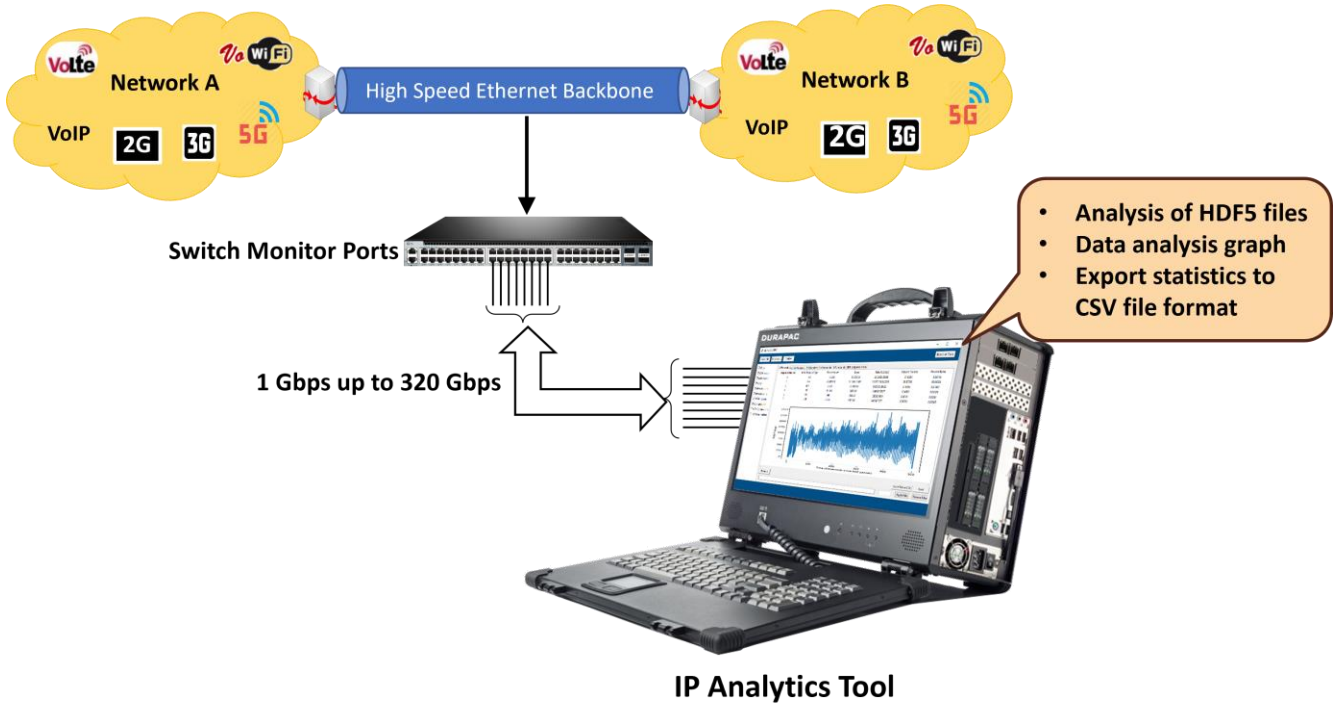
Encapsulated Security Payload (ESP) Deciphering

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



IP Analytics

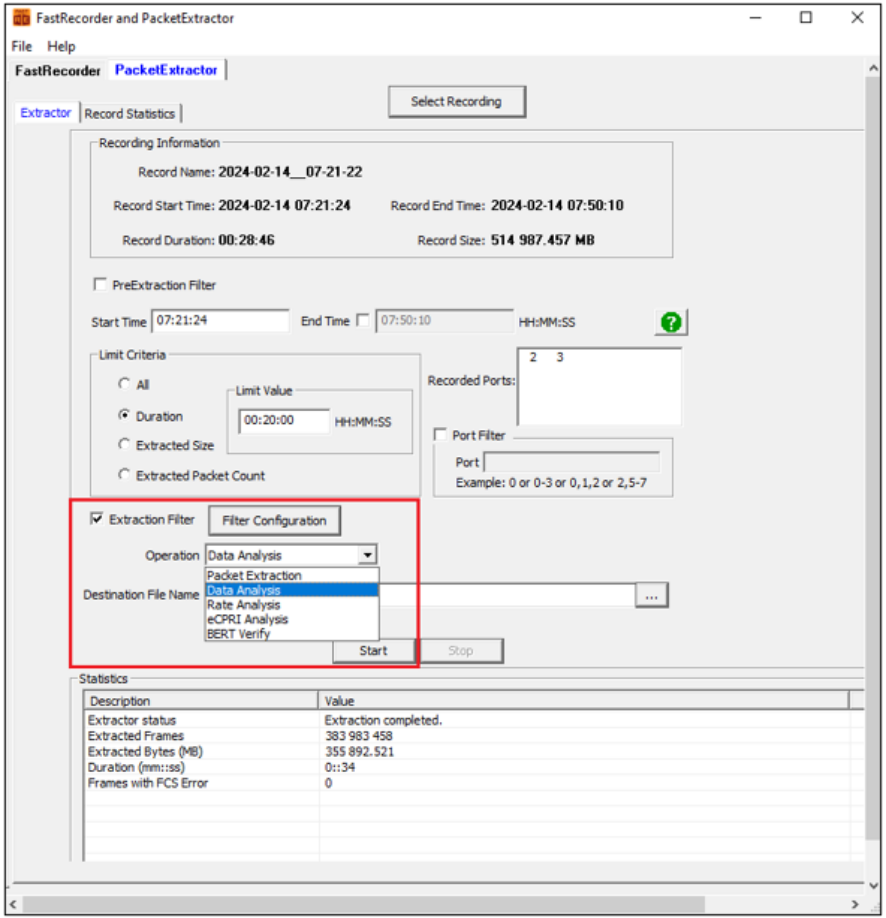
- IP Analytics serves as a critical tool for meticulous monitoring and optimization
- It involves scrutinizing data flows to uphold the integrity of voice, video, and data services, ensuring adherence to predefined performance benchmarks
- Through continuous evaluation of metrics such as Quality of Service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



Data Analysis

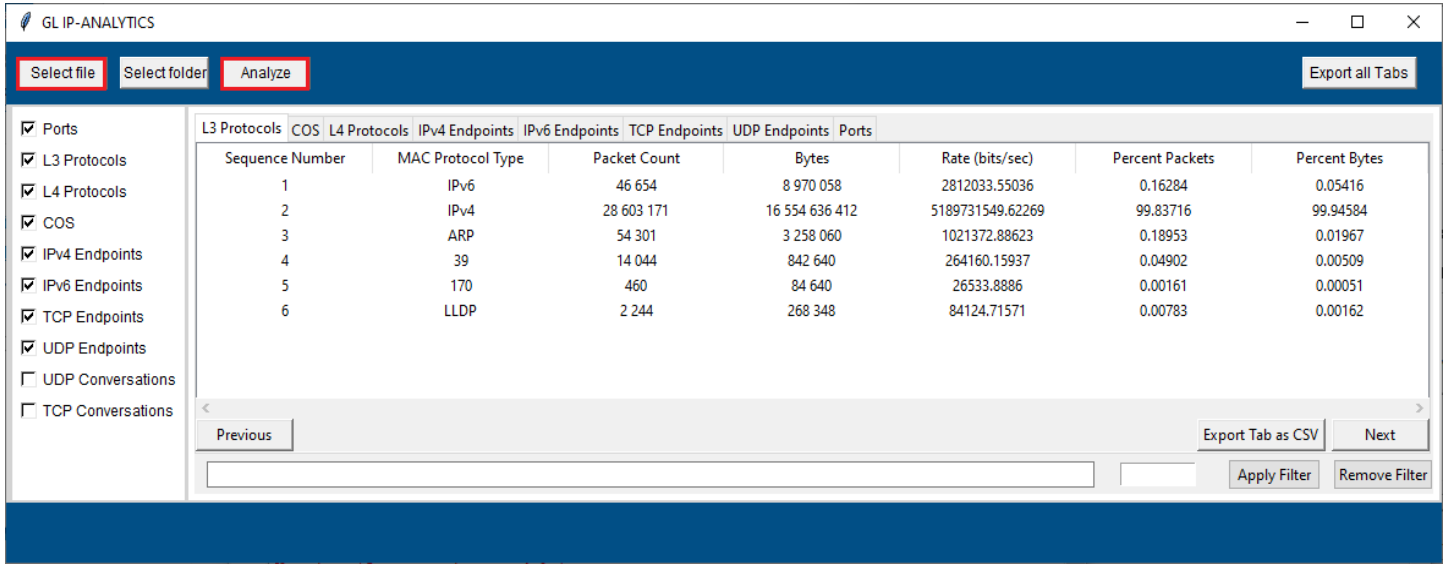
Selecting Data Analysis Option

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

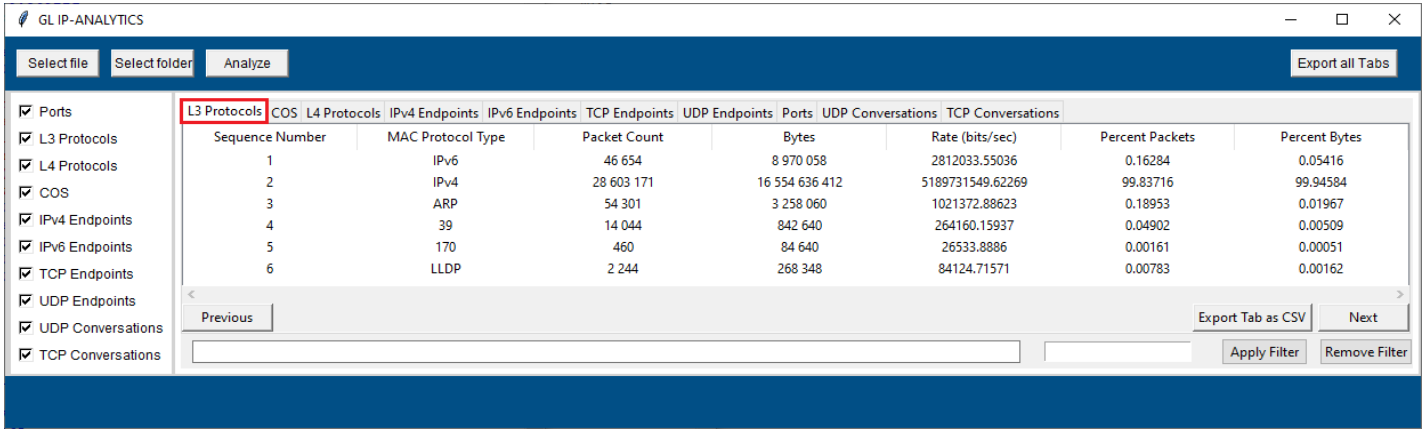


Configuring GL IP Analytics

- 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

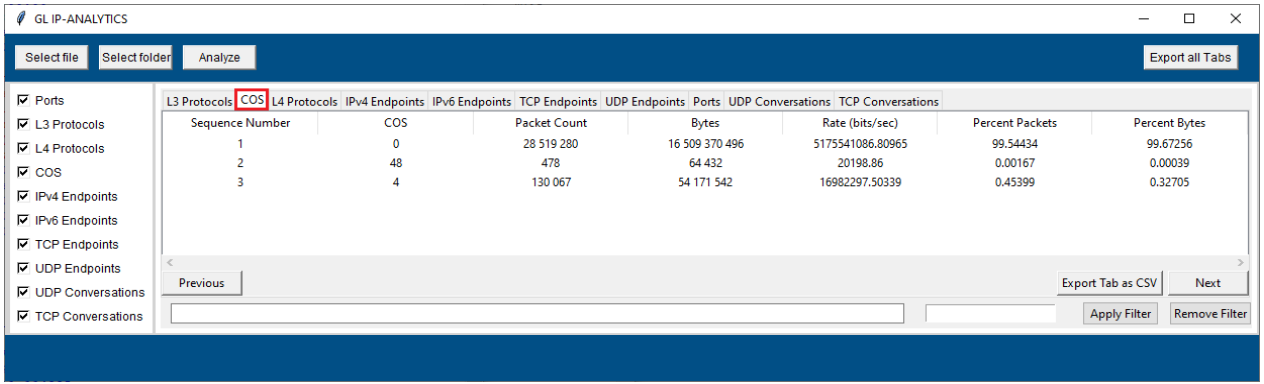


Statistics

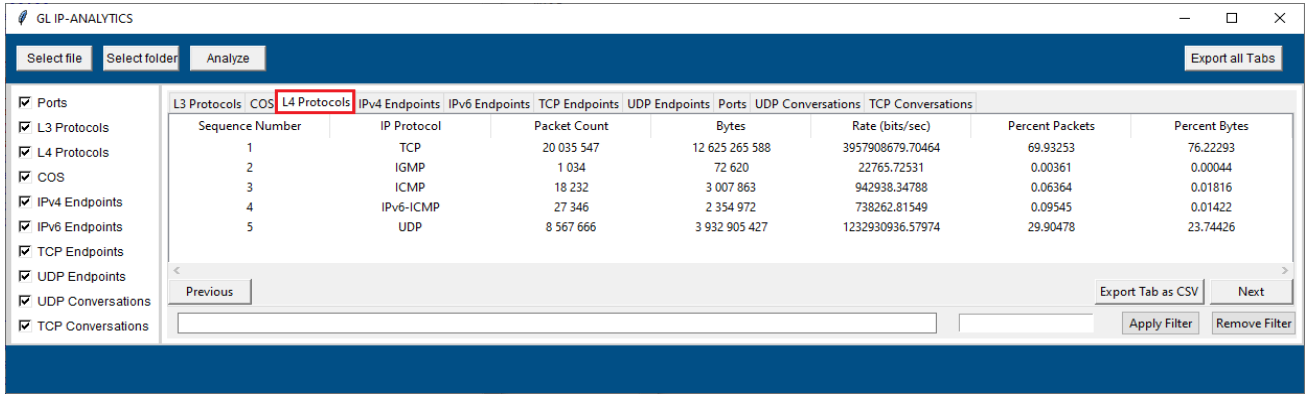


Layer 3 Protocols statistics

Class of Service (COS) Statistics

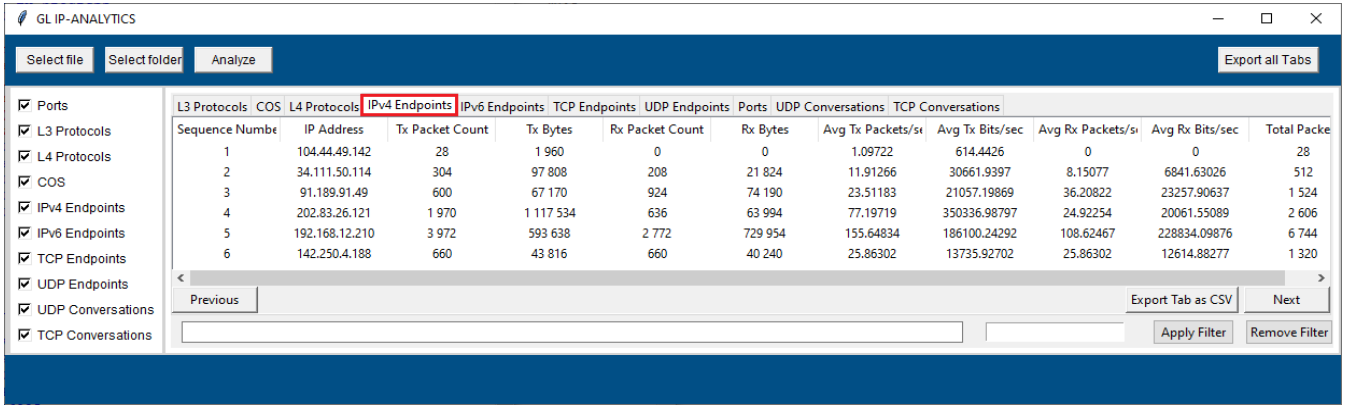


Statistics



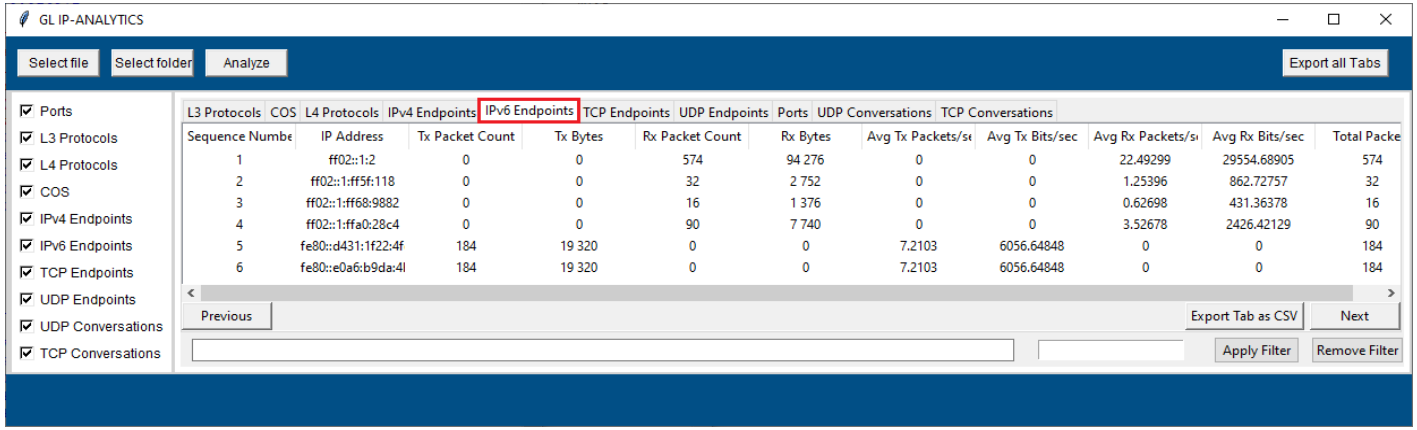
Layer 4 Protocol statistics

IPv4 Endpoints statistics



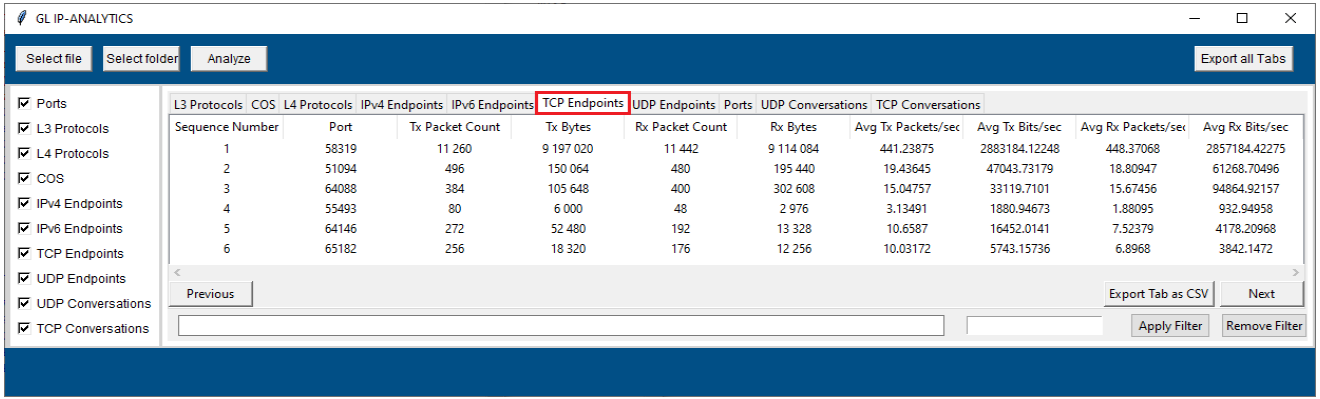
GL Communications

Statistics

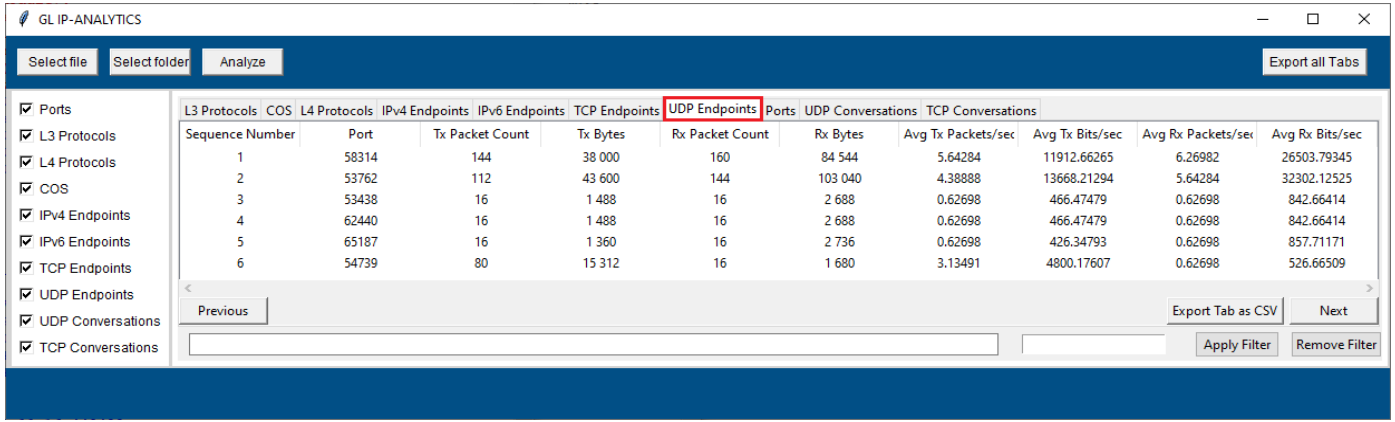


IPv6 Endpoints statistics

TCP Endpoints statistics

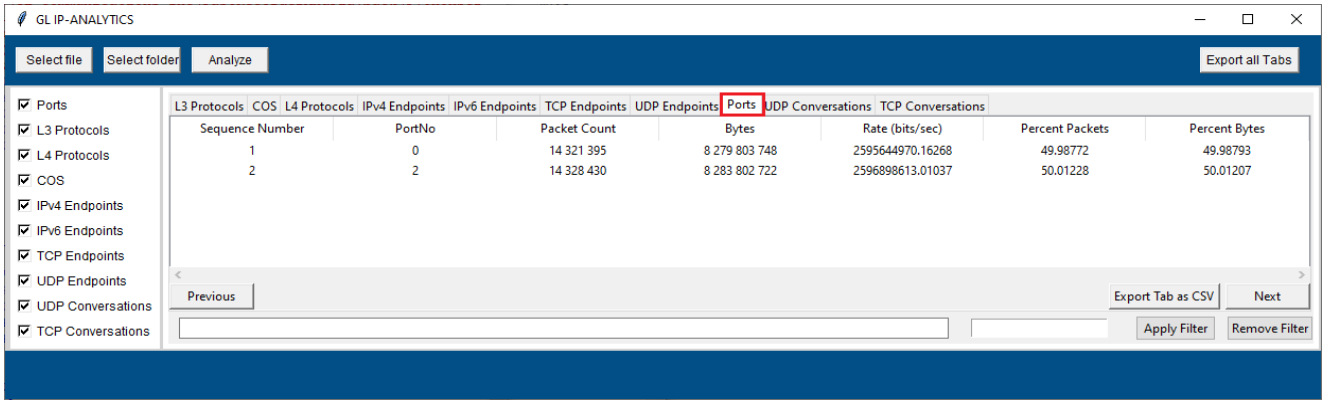


Statistics

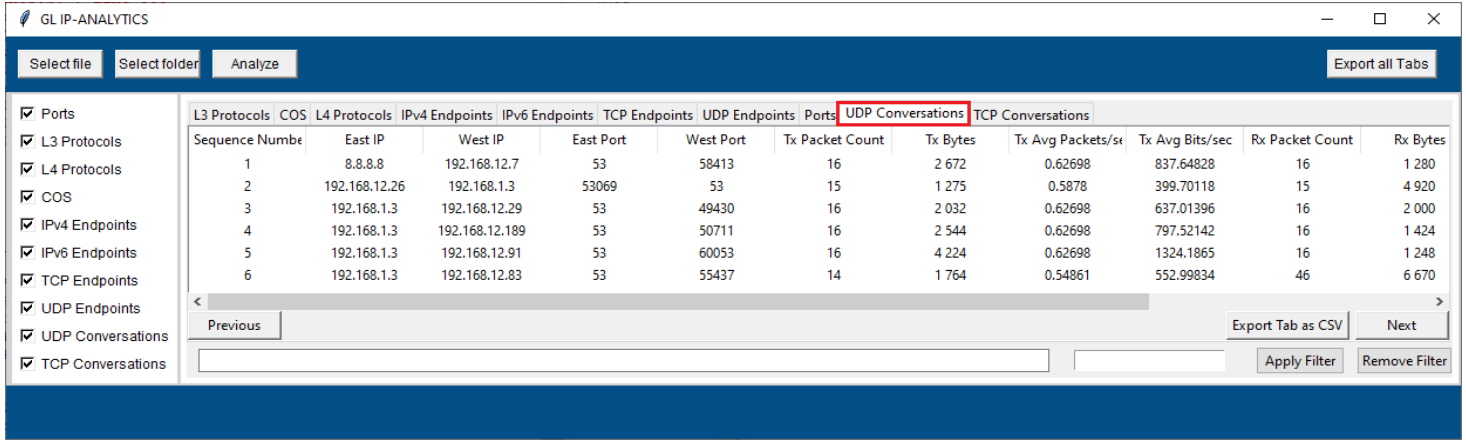


UDP Endpoints statistics

Ports statistics

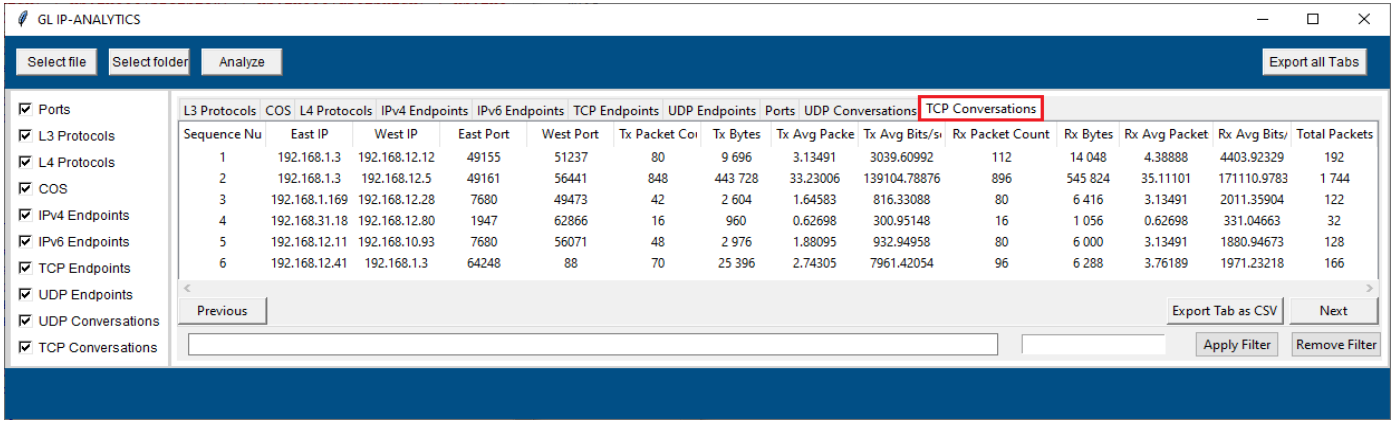


Conversations



UDP conversations

TCP conversations

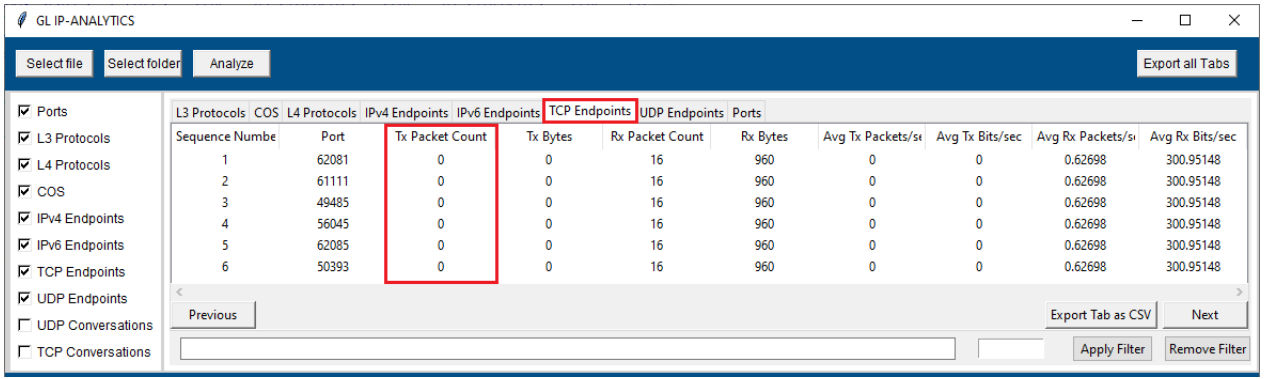


GL Communications

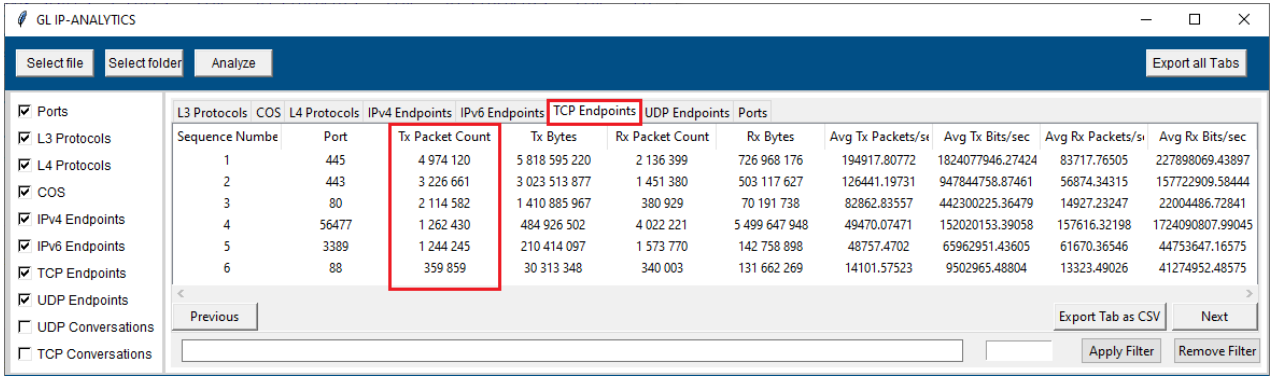
Sorting of Columns (Tabs)

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

Display of columns in Ascending order

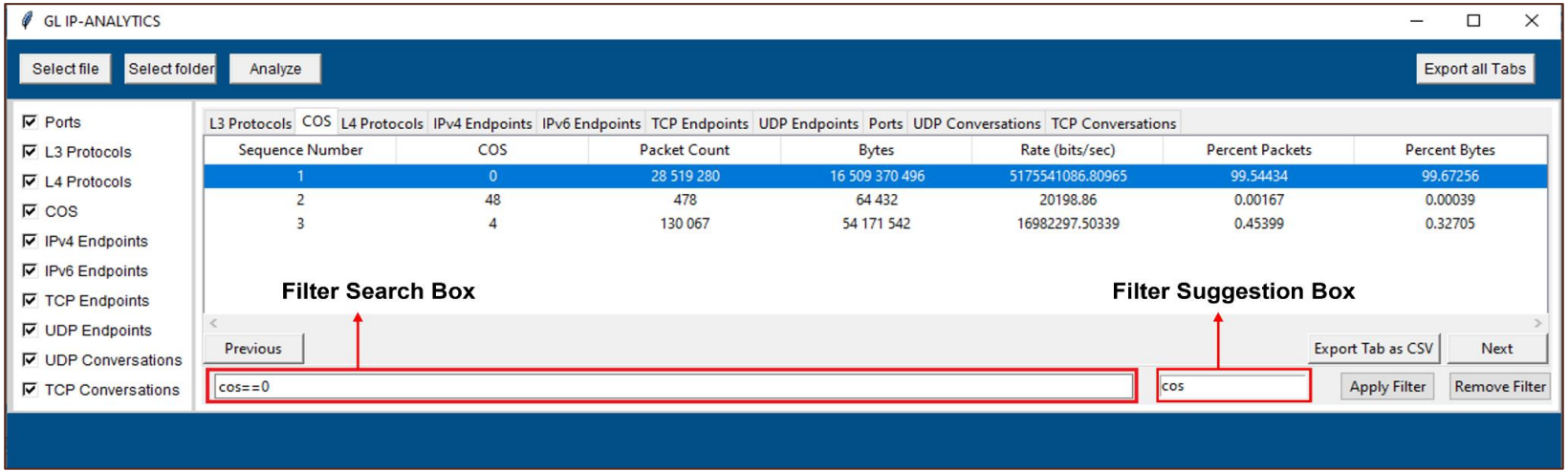


Display of columns in Descending order



Applying Filter in IP Analytics

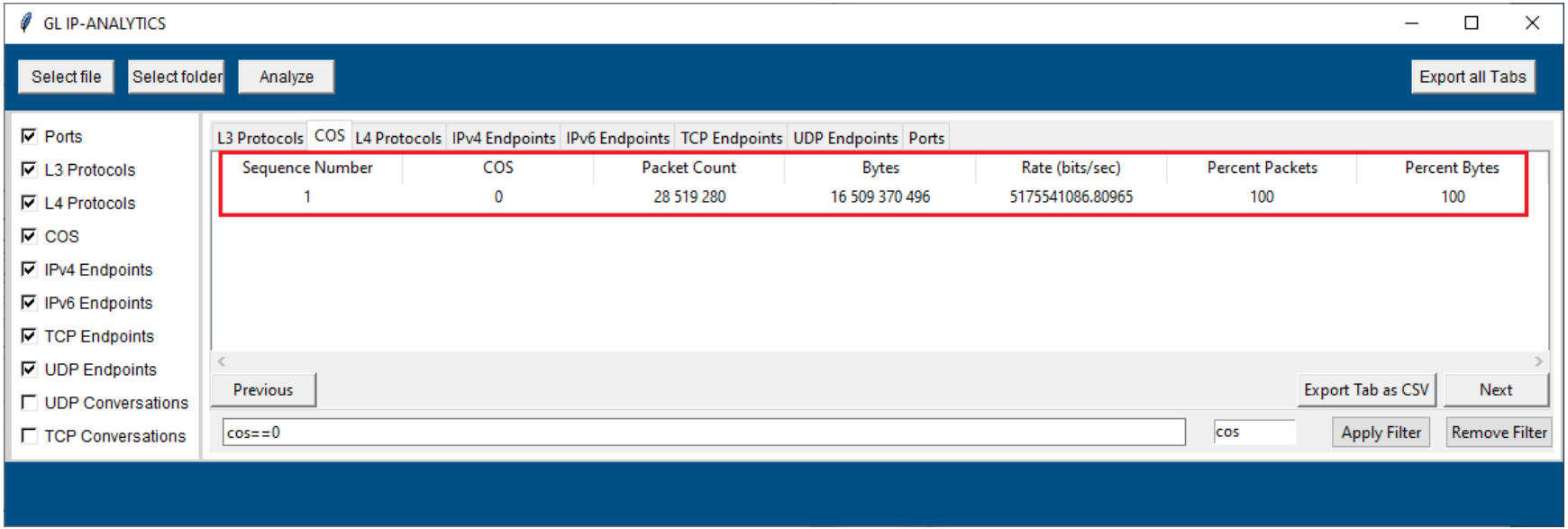
- Users can filter the required data by specifying keywords such as **mac_protocol_type**, **cos**, **ip_protocol**, **ip_address**, **tcp_port**, **udp_port**, **port** (recorded port number), **east_ip**, **west_ip**, **east_port** and **west_port**
- Enter the desired keyword in the filter search 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



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

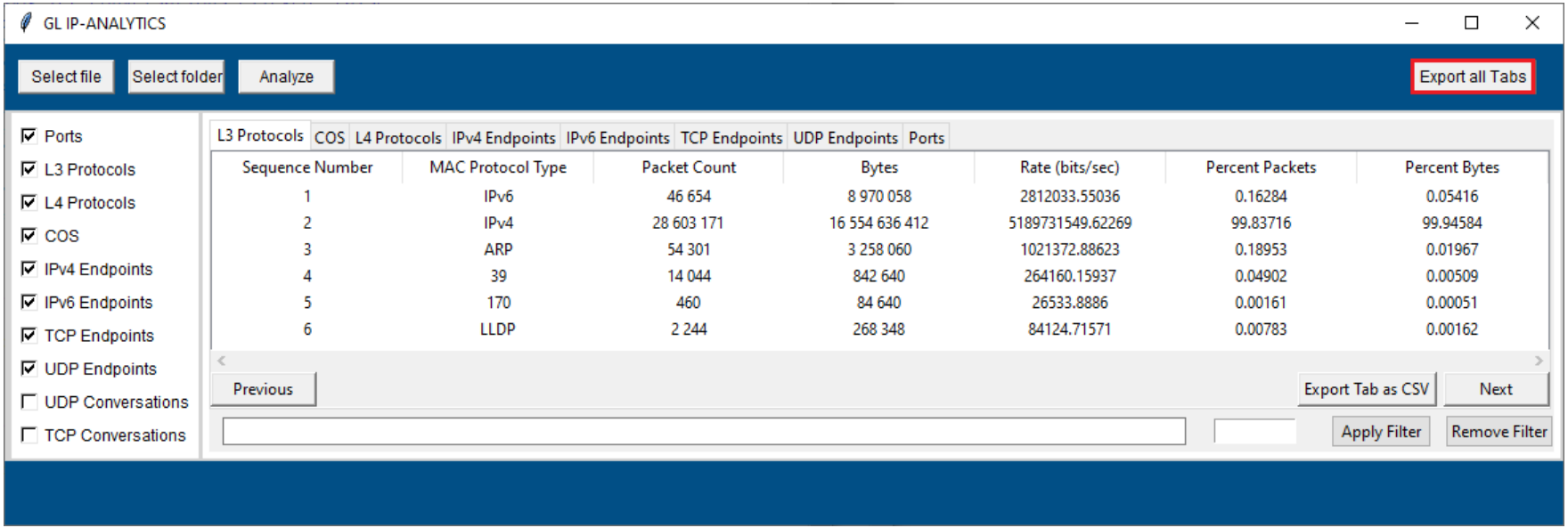
Display of Applied Filter

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



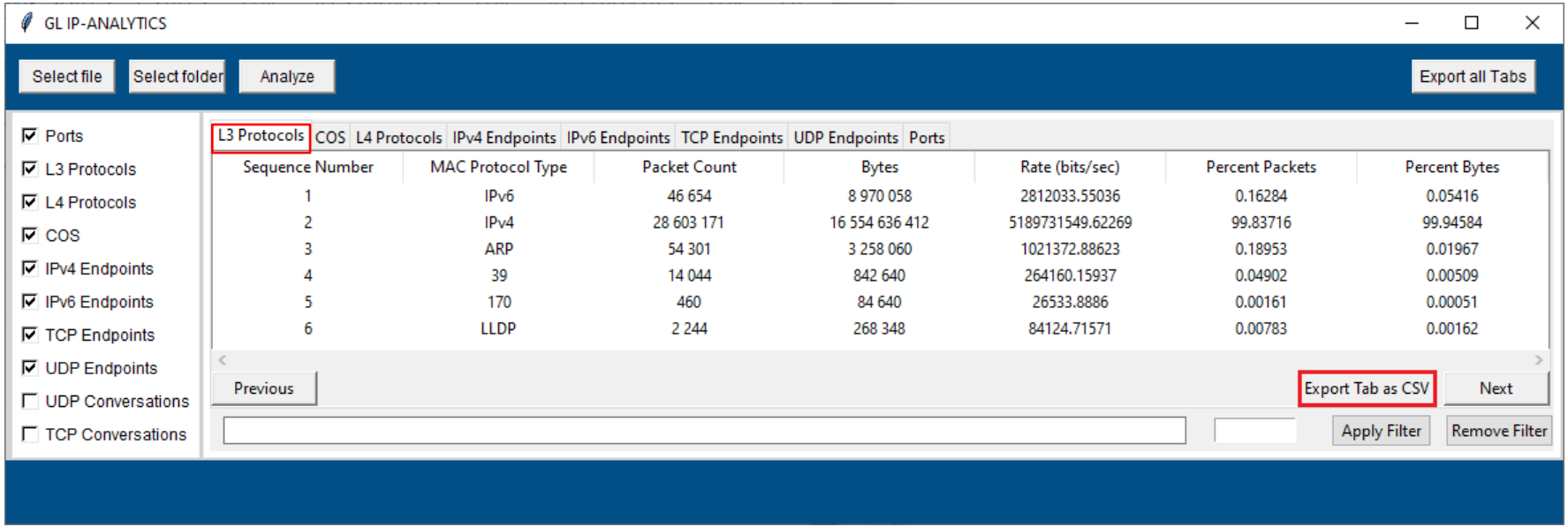
Exporting All Tabs to CSV File Format

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



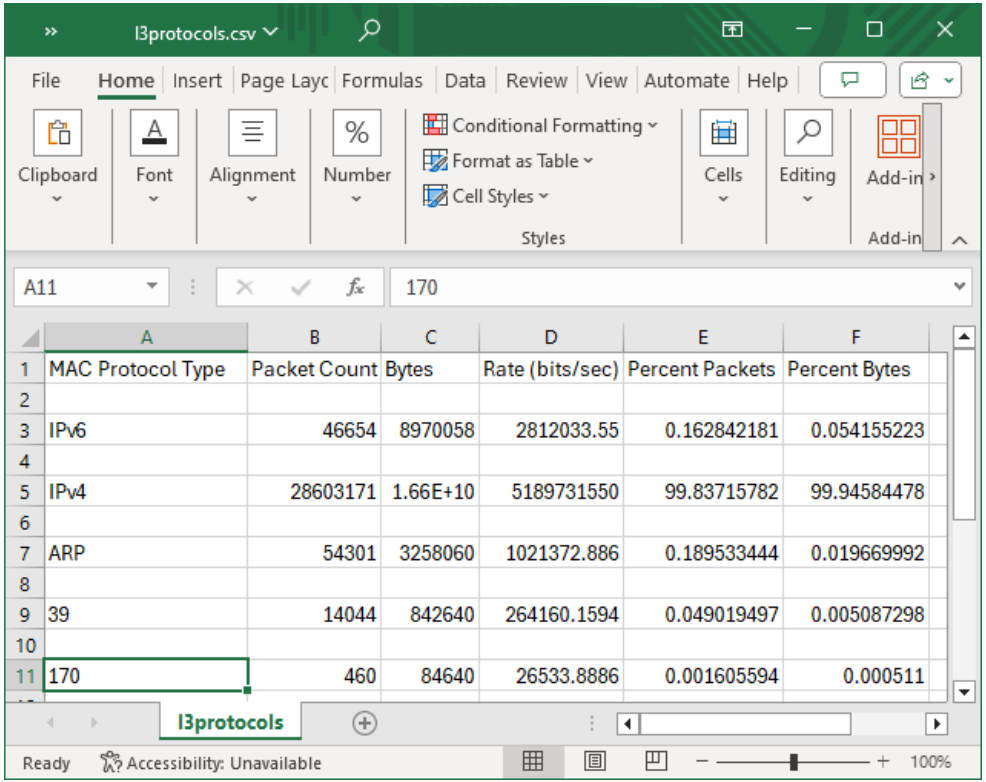
Export Tabs as CSV

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



Export Tab to CSV (Contd.)

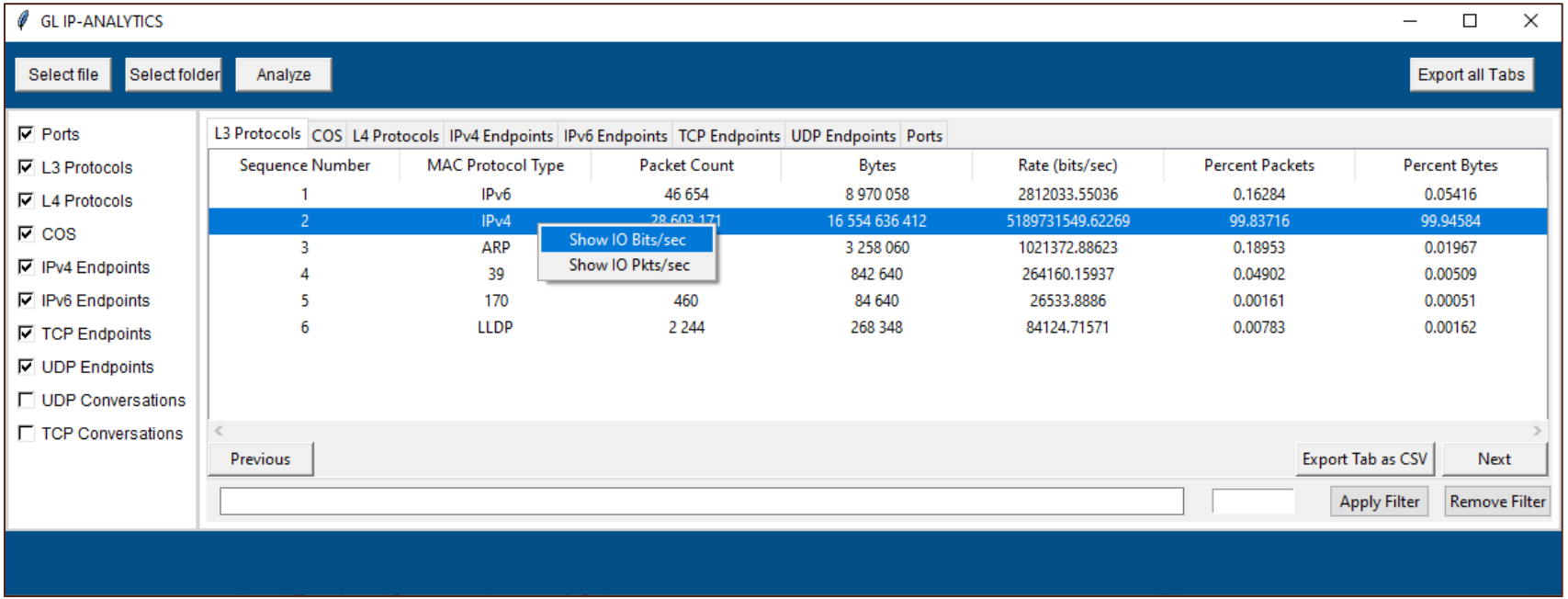
- The sample exported (**L3 Protocols**) CSV file is as shown below



	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

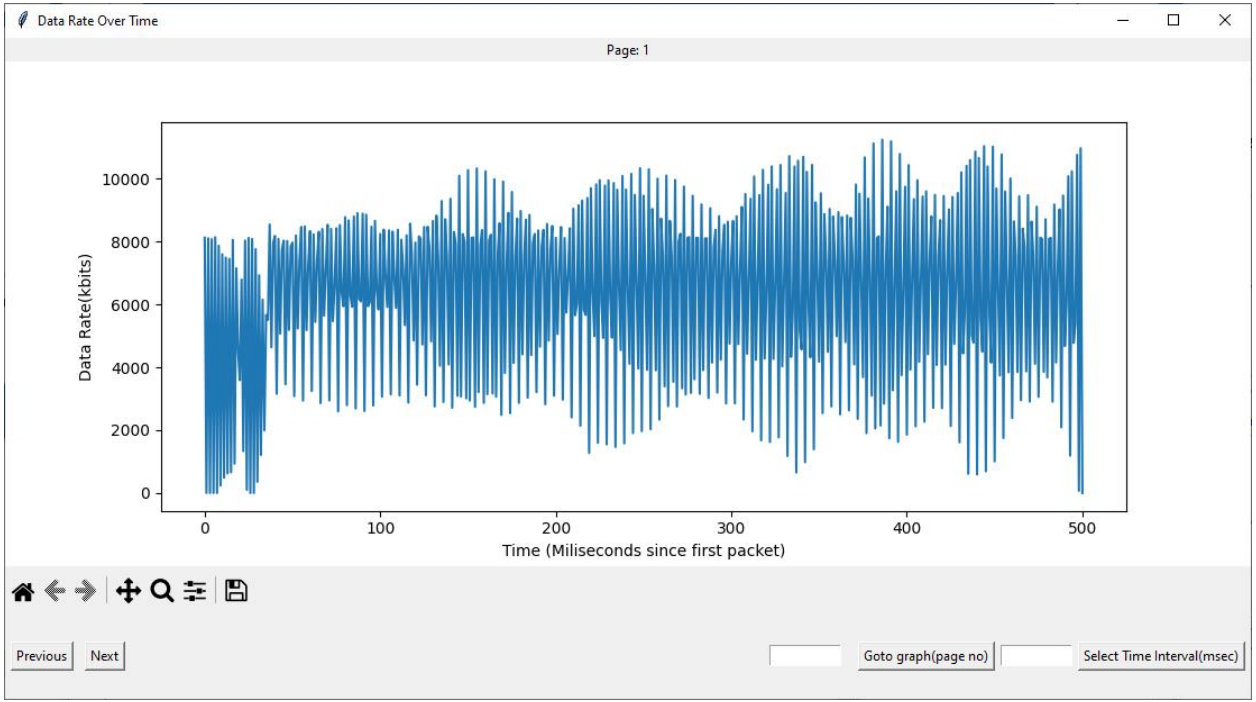
Data Analysis Graph

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



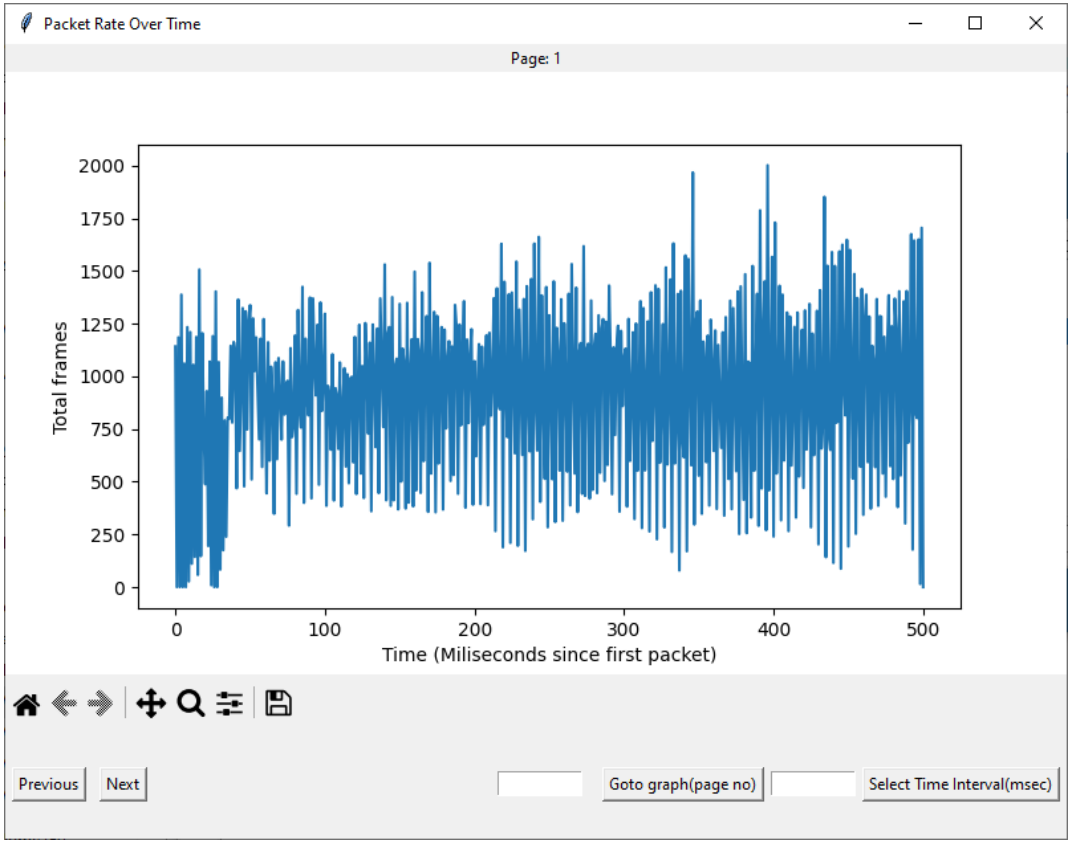
Display of Data Rate Over Time Graph

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



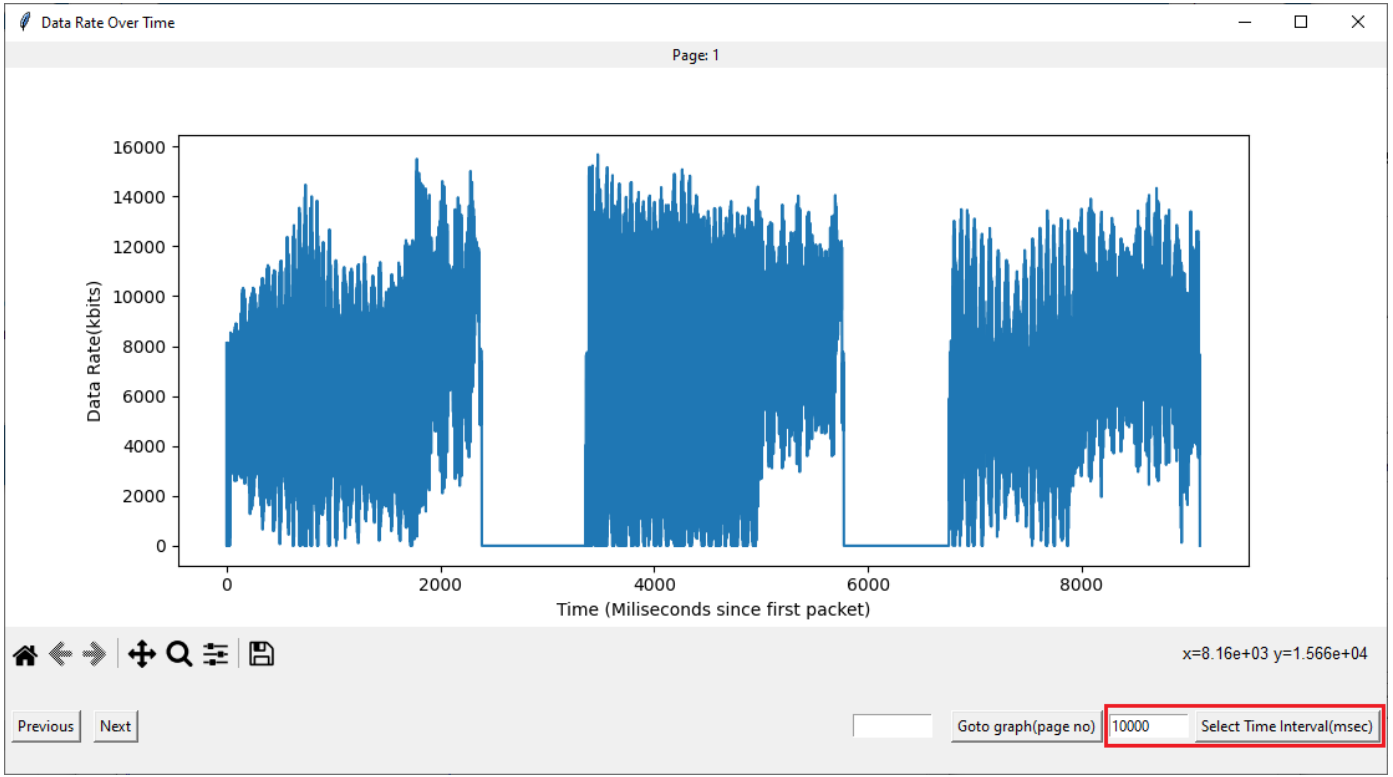
Display of Packet Rate Over Time Graph

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



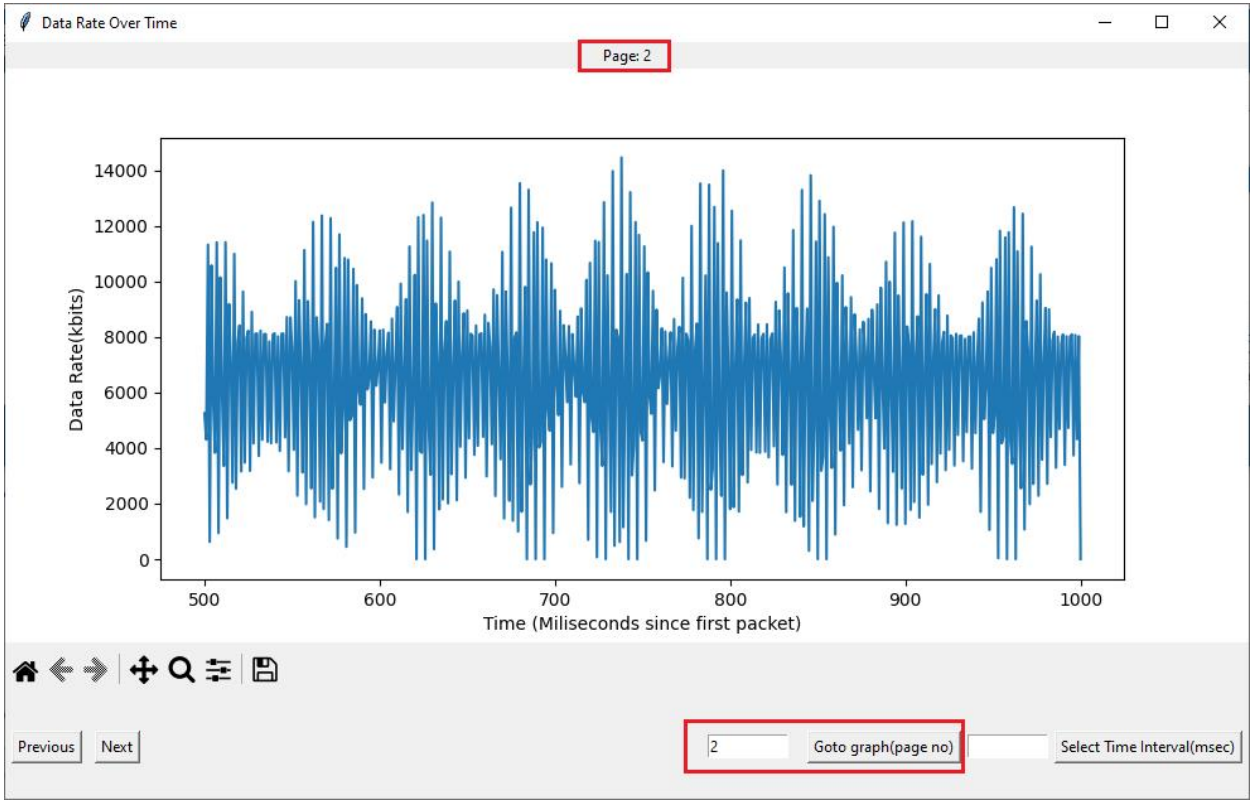
Selecting Time Interval (msec) Option

- 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

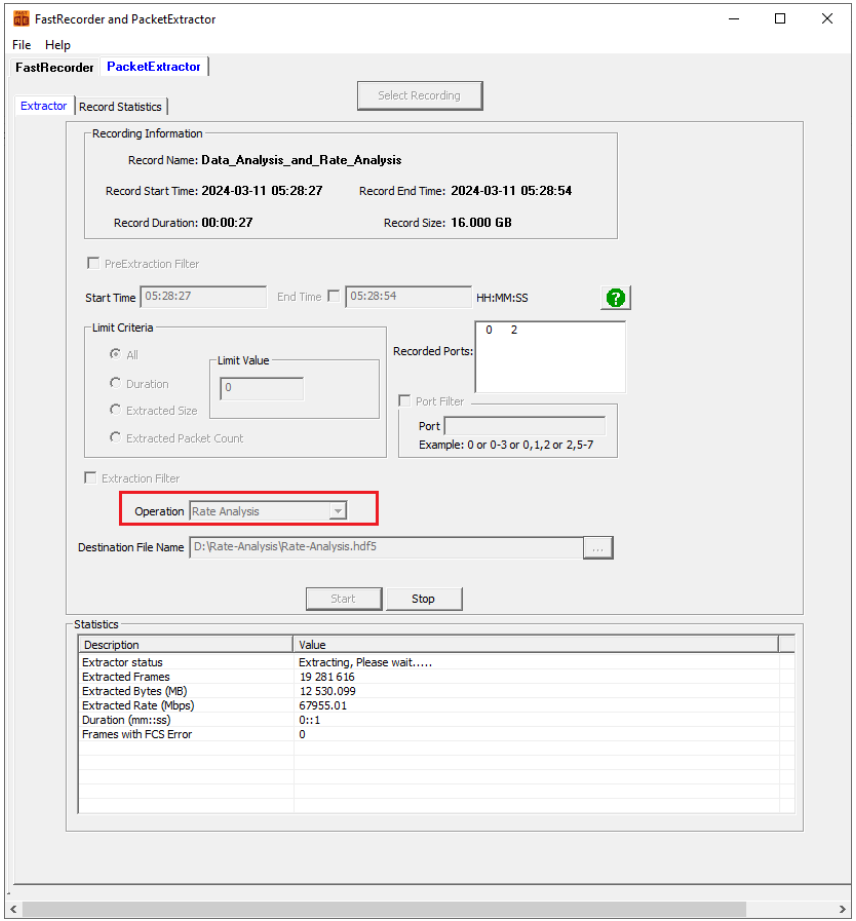
- Click on **Goto graph (page no)** to navigate to the next page of the graph (the next set of 10 seconds of the graph), as shown below



Rate Analysis

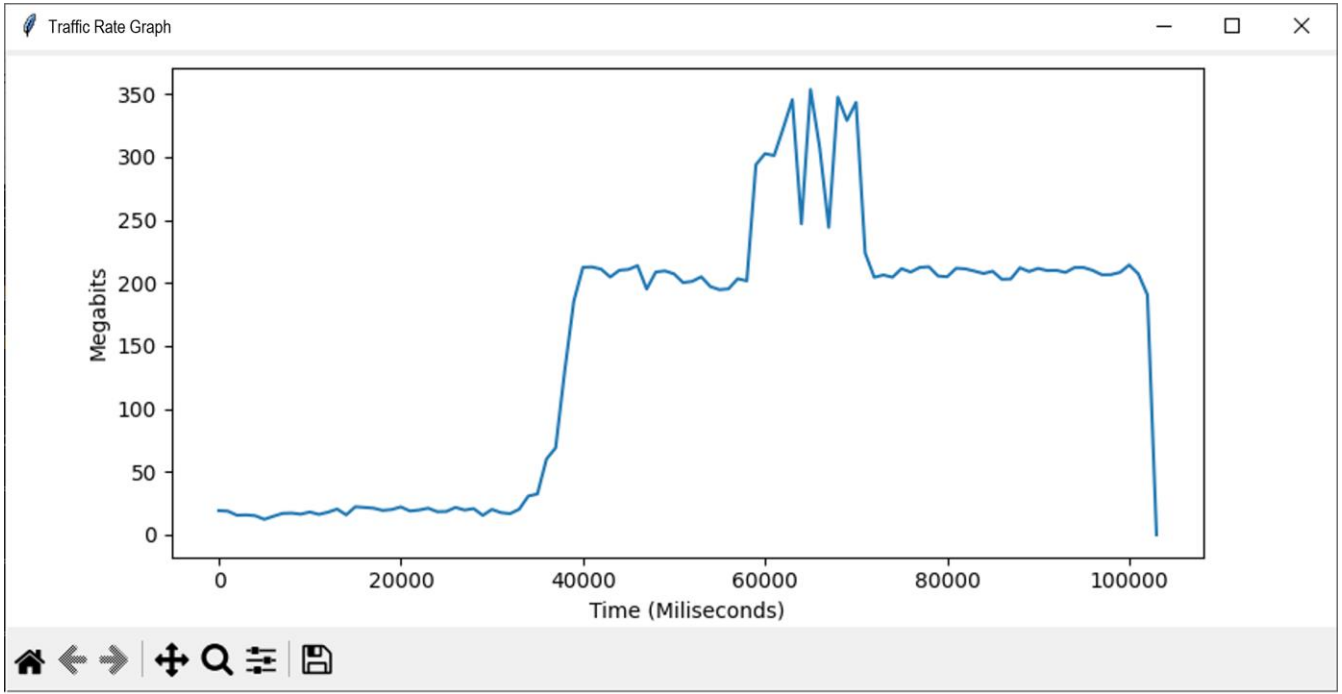
Rate Analysis in PacketExtractor™

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



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



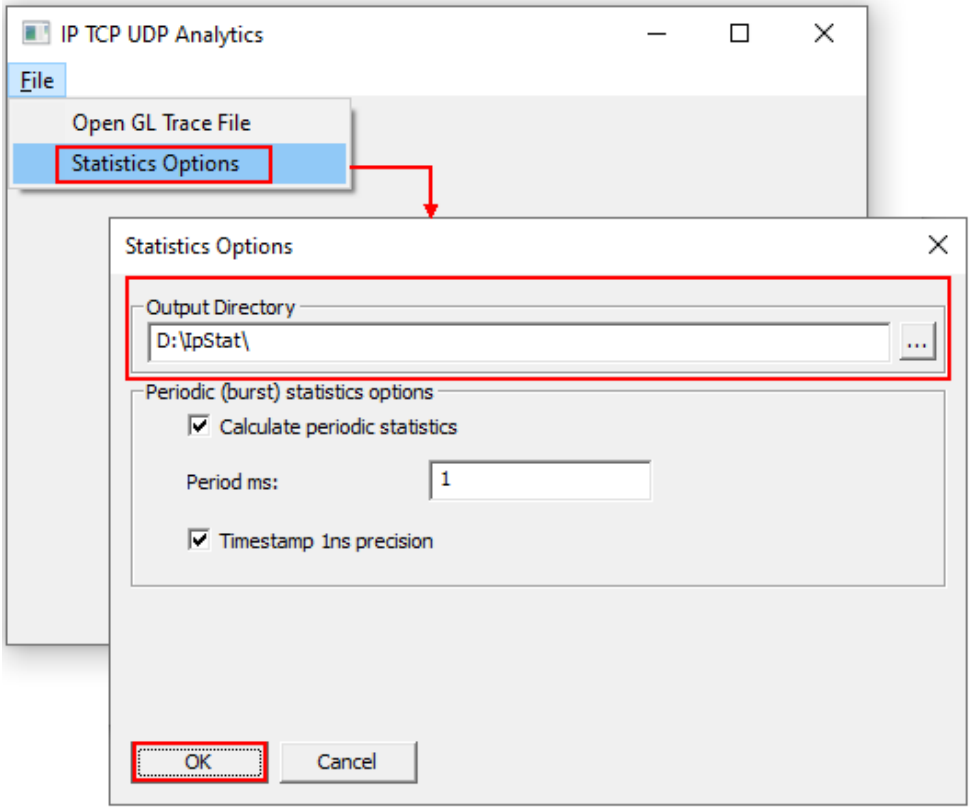
Data Analysis using IP TCP UDP Tool

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

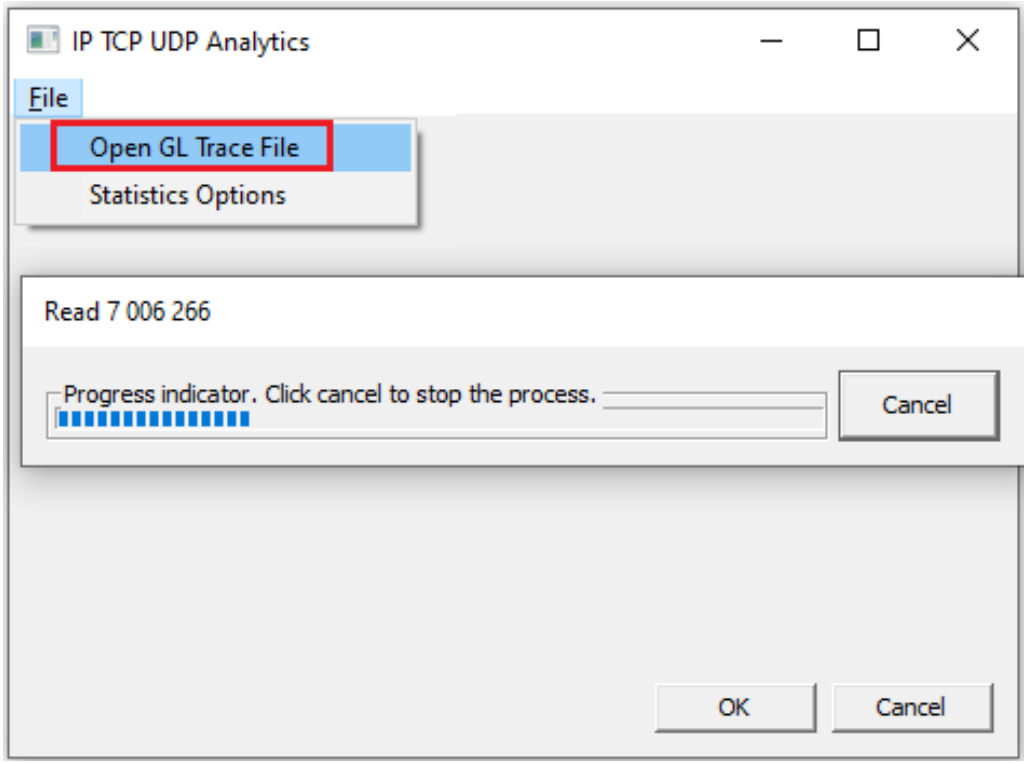
Configuring IP TCP UDP Analysis Tool

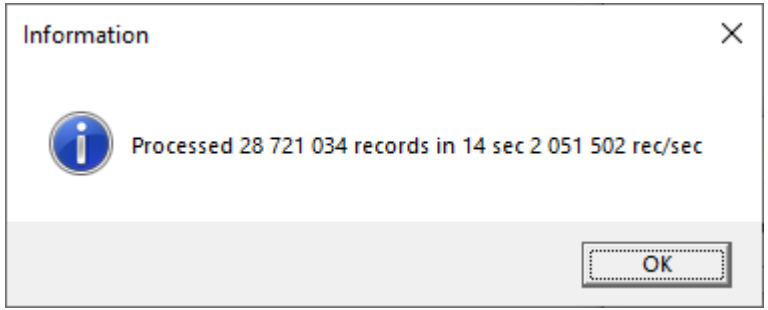
- In the **IP TCP UDP Analytics** window, configure the parameters as required



Configuring IP TCP UDP Analysis Tool (Contd.)

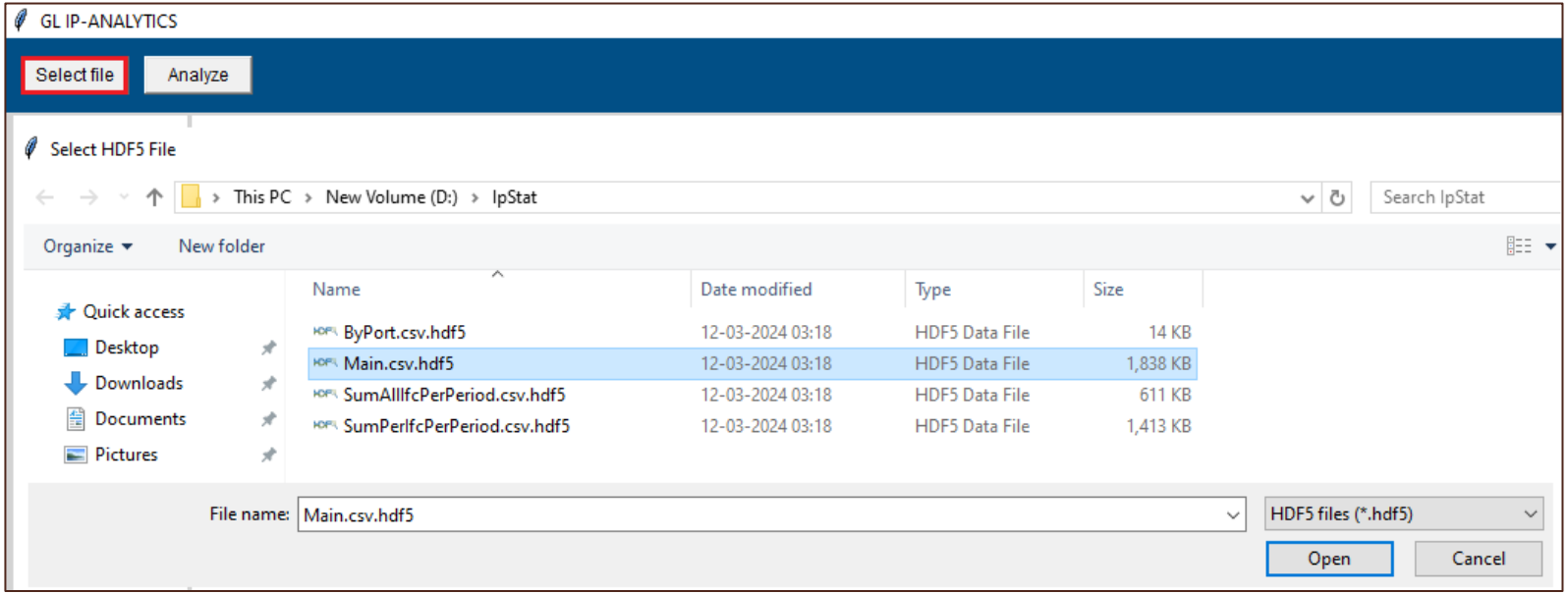
- Go to **File → Open GL Trace File** to browse and select the extracted *.hdl file. In this instance, the *.hdl file is selected as **Data-Analysis.hdl**
- Observe the Progress indicator
- After converting the extracted *.hdl file to csv, the below message will pop-up. Click on **OK** to continue





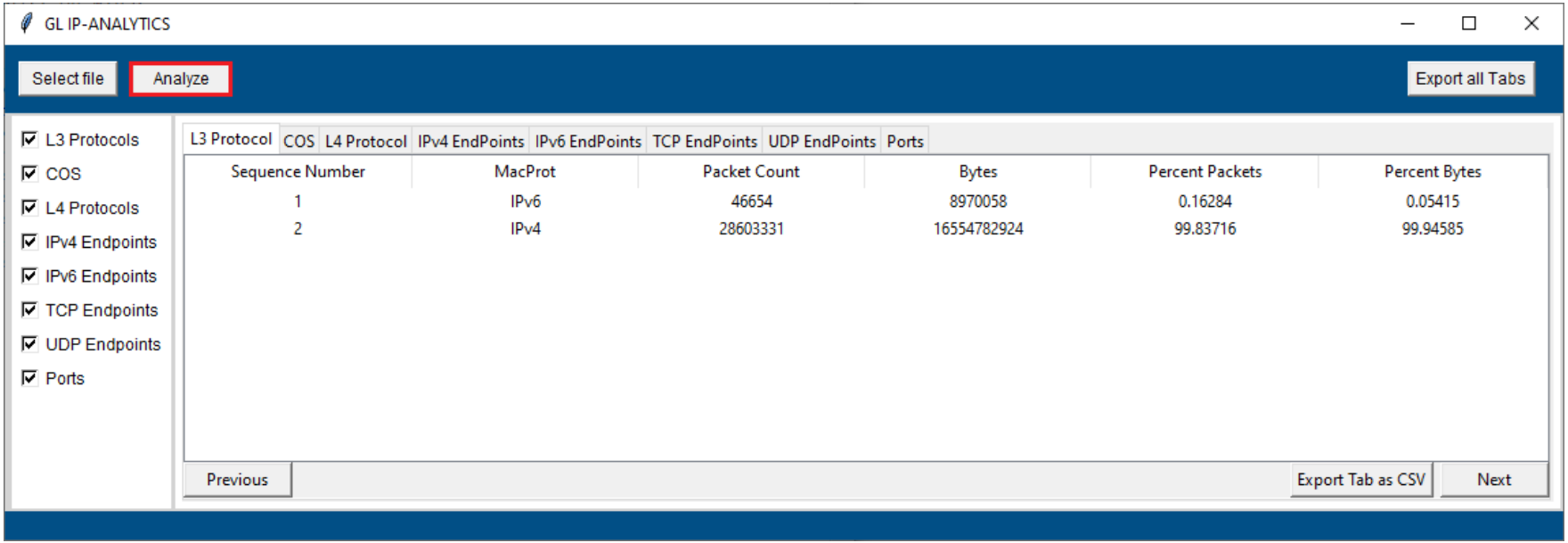
GL IP Analytics

- 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.)

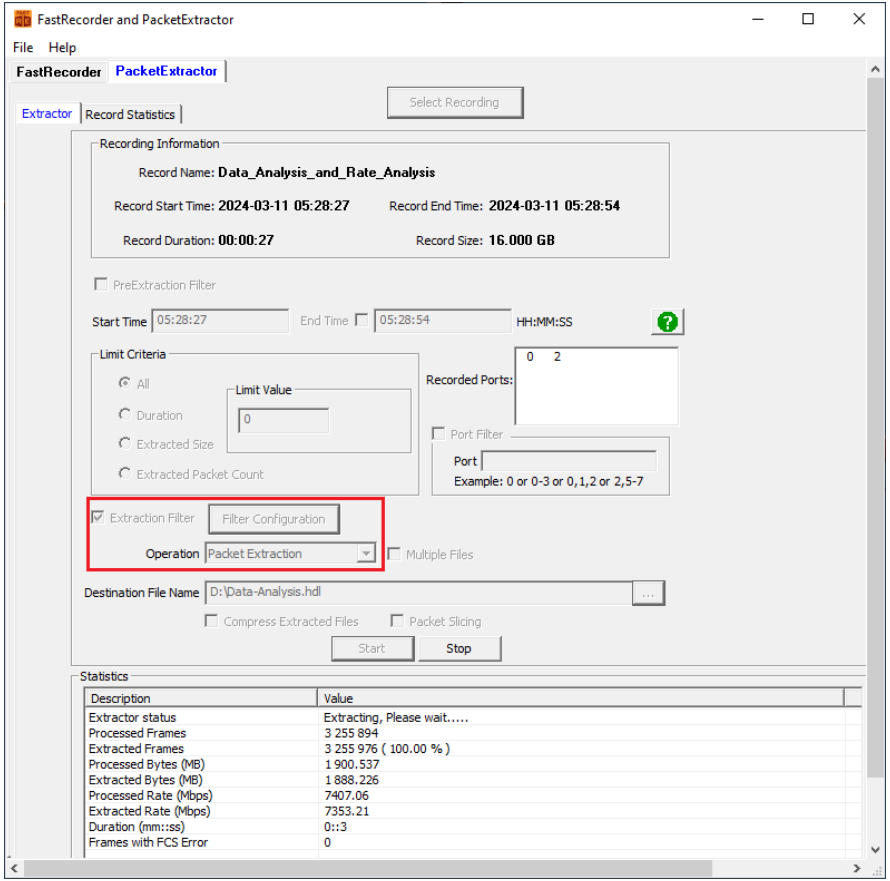
- Click on **Analyze**. This analysis will display L3, COS, L4, IPv4 Endpoints, IPv6 Endpoints, UDP Endpoints, TCP Endpoints, and Ports statistics. Observe the progress bar at the bottom left side indicating the progress
- After completion, observe the statistics as shown below is selected



Rate Analysis using IP TCP UDP Tool

Rate Analysis using IP TCP UDP Tool

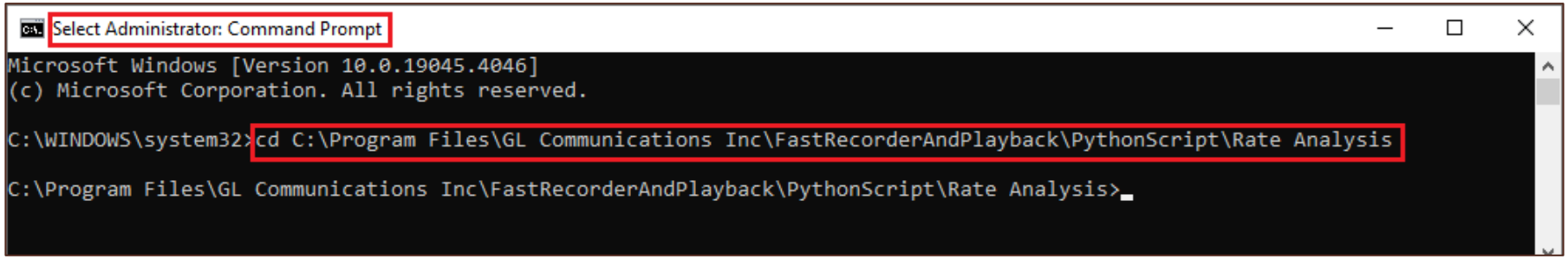
- Users can use the existing HDL format. If not, extract the recoded data into *.hdl format using PacketExtractor™ application



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**



Rate Analysis using Command Prompt (Contd.)

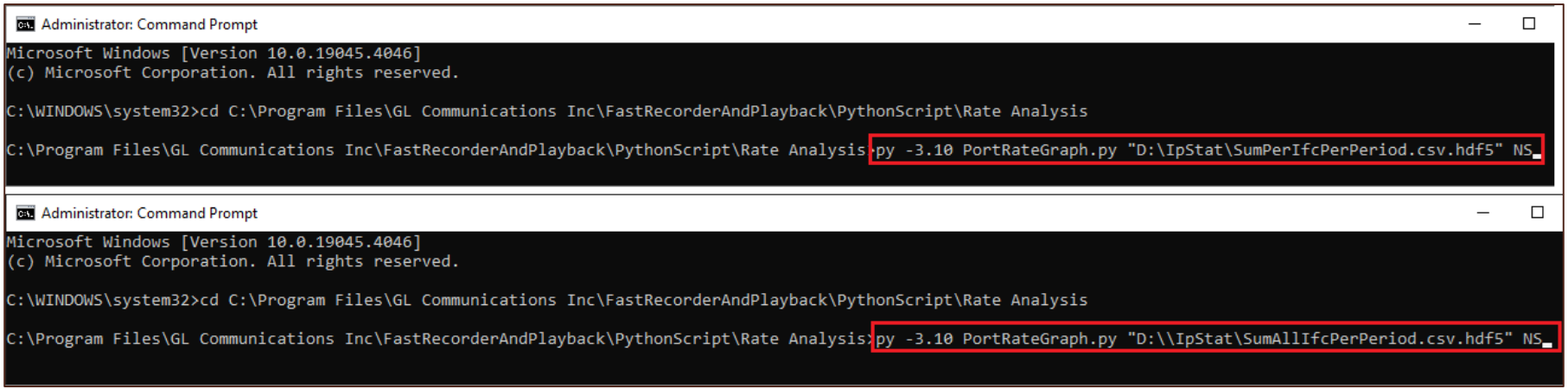
- Run the below commands

  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**



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:\\IpStat\SumPerIfcPerPeriod.csv.hdf5	The specified HDF5 file path for per port. Users can customize the path as needed.
D:\\IpStat\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