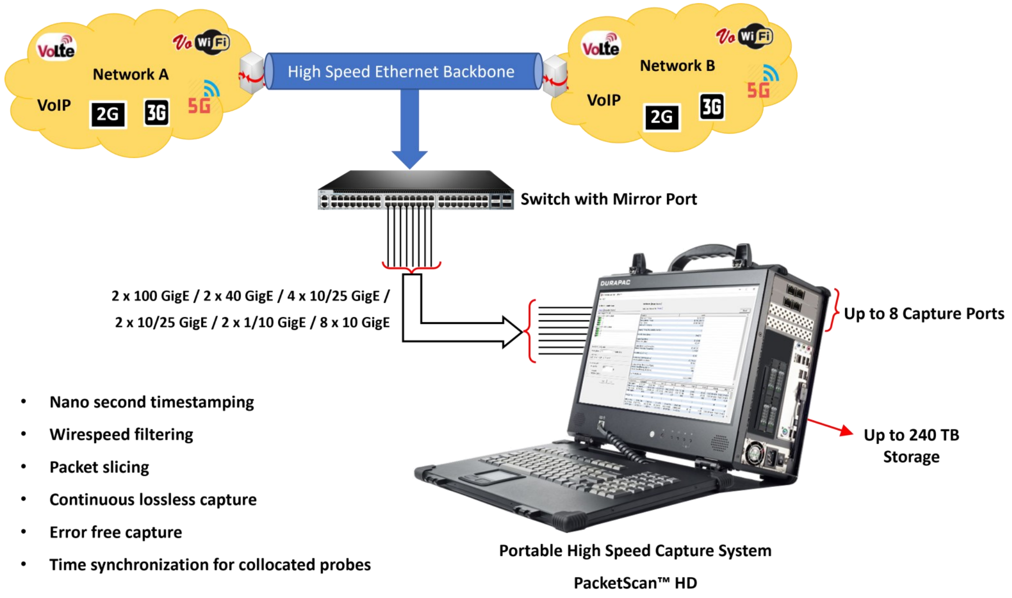
High Speed Ethernet and IP Capture

(FastRecorder™ and PacketExtractor™)



Overview

GL offers the portable or rackmount versions of FastRecorder™ and PacketExtractor™, providing the ultimate packet capture and analysis solutions for managing networks of all sizes. These tools ensure lossless capture of high-speed IP traffic. The FastRecorder™ and PacketExtractor™ applications are compatible with GL's network appliance, PacketScan™ HD, and can also be used with Wireshark® packet analyzers. They support a wide range of Ethernet interface configurations, including:

- 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

The application includes four modules - FastRecorder™, PacketExtractor™, PacketRecorder™, and PacketReplay™. FastRecorder™ is a dedicated application designed for seamless interconnection with multiple interfaces, rapid configuration, and continuous, error-free capture to large NVMe SSDs for extended durations. Users have the flexibility to define filters to capture only packets of interest and set triggers to record incoming traffic based on user-defined conditions.

PacketExtractor™ allows users to extract packets of interest by defining complex filters, specifying streams, setting time periods, controlling storage size, and even selecting specific portions of packets, such as headers, among other customizable parameters for diagnosing network issues. The extracted data can be saved in PCAP, PCAPNG, or HDL (GL’s proprietary) formats for in-depth analysis. Additionally, PacketExtractor™ supports monitoring and analysis of the eCPRI protocol. For more details, refer to eCPRI Protocol Analysis webpage.

GL's IP Analytics™ (PKV410) is an optional application that works with FastRecorder™ and PacketExtractor™ used to ensure Quality of Service (QoS) by analyzing IP-based data streams, offering detailed statistics for Layer 3, COS, Layer 4, IPv4/IPv6 Endpoints, UDP/TCP Endpoints, SCTP/PING, Conversations, Packet Count, Byte Count, Packets/sec, and Bits/sec, crucial for real-time network optimization with millisecond precision.

FastRecorder™ and PacketExtractor™ applications are compatible with GL’s PacketScan™ HD Packet Analyzers, as well as Wireshark®. PacketScan™ HD represents a comprehensive IP traffic analysis solution for its enhanced capabilities compared to Wireshark®. For instance, it offers real-time voice quality assessment, fax quality analysis, call and session separation, and powerful ladder diagrams.

The PacketRecorder™ and PacketReplay™ provide record and replay of IP traffic up to 10 Gbps.

For more details, refer to High Speed Ethernet and IP Capture webpage.

GL Communications Inc.

818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878, U.S.A
(Web) www.gl.com - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) info@gl.com

Main Features

- **FastRecorder™:**
  - – Lossless wirespeed capture of IP traffic across high-speed (1, 10, 25, 40, and 100 GigE) links
  - – Non-intrusive capture and record over Ethernet (Electrical and Optical) interfaces with nanosecond precision
  - – Recording on multiple ports by merging traffic with high-precision timestamps
  - – Up to 240 TB of total storage (NVMe SSD) in the portable platform
  - – Record only traffic of interest by applying efficient hardware filters based on MAC, 802.1Q (VLANs), IPv4/IPv6, Tunnel Traffic (Tunnel 1 and Tunnel 2), TCP, UDP, SCTP, SIP, and RTP parameters
  - – Filter on inner layers of GTP, GRE, and VXLAN tunnel traffic, such as inner IPv4/IPv6 addresses and Transport Protocol (UDP, TCP, and SCTP) port numbers
  - – Create custom filters using the custom filter option, providing flexibility to check fields and use logical conditions more efficiently
  - – Slice packets to limited lengths to store only selected packet content
  - – Optimized distributed disk operation to achieve wirespeed recording to disk
  - – Supports recording of eCPRI traffic based on eCPRI message types and UDP port numbers
  - – Option to record traffic continuously by retaining the latest traffic with a user-defined record size
  - – Statistics, such as captured, filtered/unfiltered, dropped frame percentage, and error counts per Ethernet interface or aggregated
  - – Create custom filters based on added fields using the custom filter option, providing flexibility in checking fields and using logical conditions efficiently
  - – Start recording without specifying the recording name; the current time is taken as the recording name in the format "YYYY-MM-DD_HH-Min-Sec"
  - – Option to view graphical representations of history, including overall rate, frames/second, per-port rate, per-port frames/second, and port link status, with Zoom In and Zoom Out options
  - – Configure trigger-based conditions based on capture rate, filter rate, per-port capture rate, and per-port filter rate
  - – Supports email alerts for specified trigger conditions
  - – Provides the option to schedule recording start/stop by setting triggering conditions based on datetime/time format
- **PacketExtractor™:**
  - – Extract the intended traffic from previous recordings into PCAP, PCAPNG (Wireshark® format), or HDL (GL Proprietary format) output traces
  - – Analyze the extracted trace in PacketScan™ HD or Wireshark®
  - – Choose to extract the packets into single or multiple output traces
  - – The extraction filter provides options for IP, TCP, UDP, Inner IP, Inner UDP, and other protocols
  - – Extract traces with file size, time period, or packet count as the limit criteria
  - – Slice packets to a limited length to optimize output trace size
  - – Option to compress extracted trace files using 7-Zip for storage optimization
  - – Supports eCPRI analysis to monitor eCPRI traffic for packet impairments such as Missed Packets, Out of Order, Duplicate Packets, One-Way Delay, etc.
  - – Display recorded aggregated and per-port statistics, including captured, filtered/unfiltered, dropped frame percentage, and counts
  - – Graph option to view selected recording statistics and history of overall rate, frames/sec, per-port rate, per-port frames/sec, and port link status from the record start time to end time, along with Zoom In and Zoom Out options
  - – View applied hardware filters
  - – Supports Encapsulating Security Payload (ESP) protocol to decrypt ESP packets on both IPv4 and IPv6 by providing ESP SAs value
  - – Extraction can be performed from user-specified start and end times
  - – Supports renaming of recorded filenames
  - – Provides Recording Status options as Complete or Partial
  - – Enhanced to support Data Analysis and Rate Analysis

Specifications

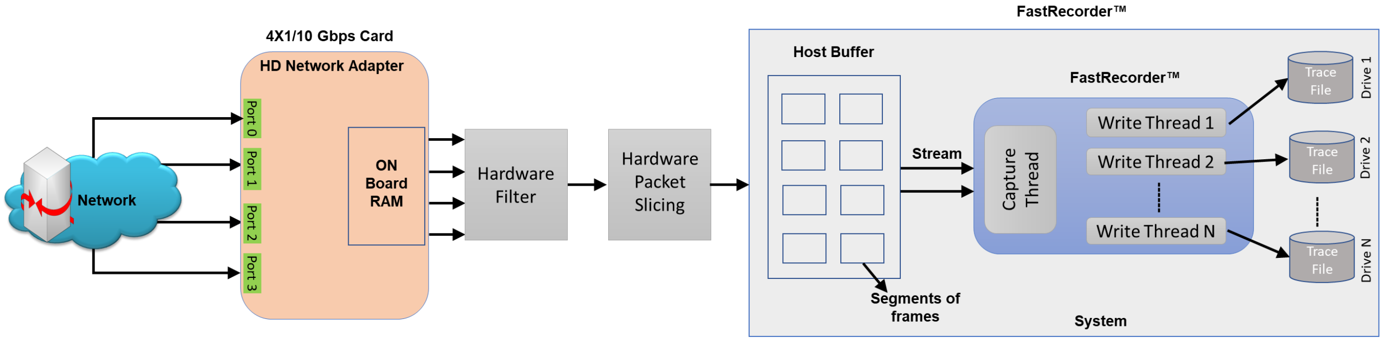
Hardware Requirements	**Requires GL's HD Network Interface adapters** • High Density Network Adapters can be any of the following types – – **4 x 1/10 Gbps** – requires 10GBASE-SR SFP+; Optical only – **2 x 40/100 Gbps** – requires MTP/MPO Connector for CFP2; Optical only • **Hard Disk**: SSD hard disk (For faster I/O operations) compatible with SATA verIII or RAM Disk • **System Configuration**: 2U system with 32 GB to 128 GB RAM
Hardware Filters	• Supports defining up to 10 filters at Layer 2, 3, 4, and 5 – **MAC**: Frames can be filtered out based on Ether Type and FCS Error – **VLAN 0, 1, 2**: Filters frames based on Tag protocol ID, User Priority, CFI, and VLAN ID – **IPv4**: Frames can be filtered based on Source IP Address, Destination IP Address, Protocol Type, Header Length, Differentiated Services, Ds_ECN, DS_CodePoint, Total Length, Check Sum Error, IP Datagram ID, Fragmentation Offset, Flag_DontFragment and Flag_MoreFragments – **IPv6**: Frames can be filtered based on Source IP address, Destination IP address, Next Header, and Payload Length – **Tunnel Traffic**: Tunnel filter provides a method to filter the packets of one protocol within another protocol. GTP, GRE and VXLAN are available tunneling methods. Hardware filters can be applied to Tunnel 1 and Tunnel 2 layers – **ARP**: Frames can be filtered based on Sender MAC Address, Target MAC Address, Sender IP Address, Target IP Address and Option Code – **TCP**: In TCP layer Frames, can be filtered based on source port, destination port and check sum error – **UDP**: In UDP layer Frames can be filtered based on source port, destination port, check sum error, UDP length and payload – **SCTP**: SCTP packets can also be filtered based on source port or destination port – **SIP and RTP**: SIP and RTP packets can also be filtered based on source port or destination port
Record Rate	• Max Rate is 320 Gbps

Working Principle

FastRecorder™

At the hardware level, FastRecorder™ captures traffic on the selected port. This captured traffic is timestamped and then transmitted to the Host Buffer within the hardware. If Hardware Filters are applied, only the filtered traffic is directed to the Host Buffer. When multiple ports are selected, the filtered traffic from these selected ports is aggregated and presented as a single stream.

The FastRecorder™ application consists of two primary modules: the Capture Module and the Write Module. Within the host buffer, packets are segmented into different frames based on segment sequence number and segment sequence length. These frames are then captured from the selected network interface. The Write Module is responsible for saving the captured traffic in trace files in metadata format to either the SSD or RAM Disk.



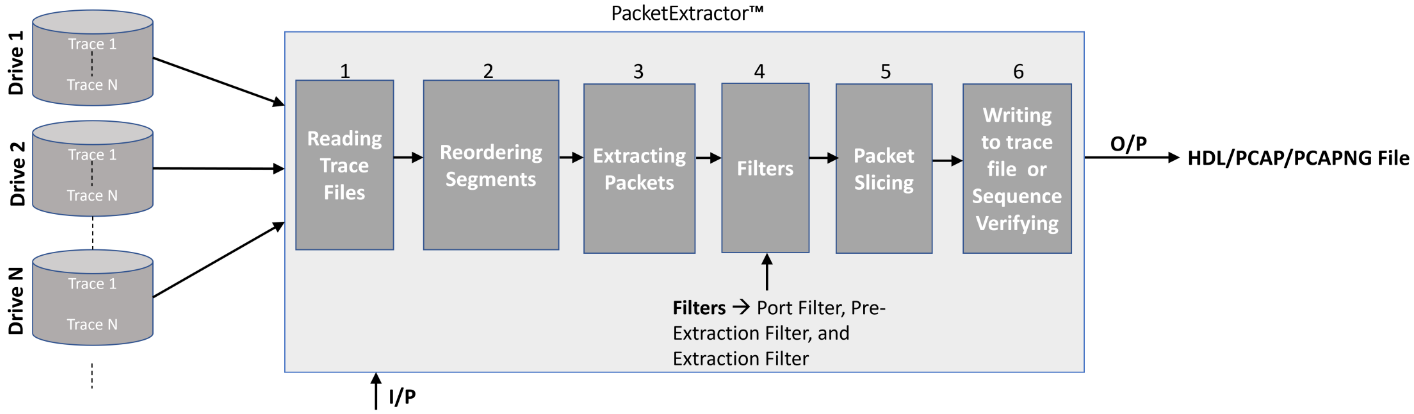
PacketExtractor™

Once the pre-recorded captured files (in .dat format) stored on the SSD/RAM disk are sent to the PacketExtractor™ application, the following steps are carried out:

Read Module: This module reads the metadata file, which contains information about the recorded data on each drive along with timestamps. Users can apply filters to extract specific traffic of interest. The trace file segments are reassembled based on the segment sequence numbers. During analysis or reassembly, both the segment sequence number and segment length are utilized.

Extractor Module: The Extractor module then extracts packets from the reassembled segments.

Write Module: Subsequently, the write module saves the extracted packets in HDL, PCAP, or PcapNG formats. Furthermore, the BERT verify option can be utilized to analyze the sequence numbers of the extracted packets.

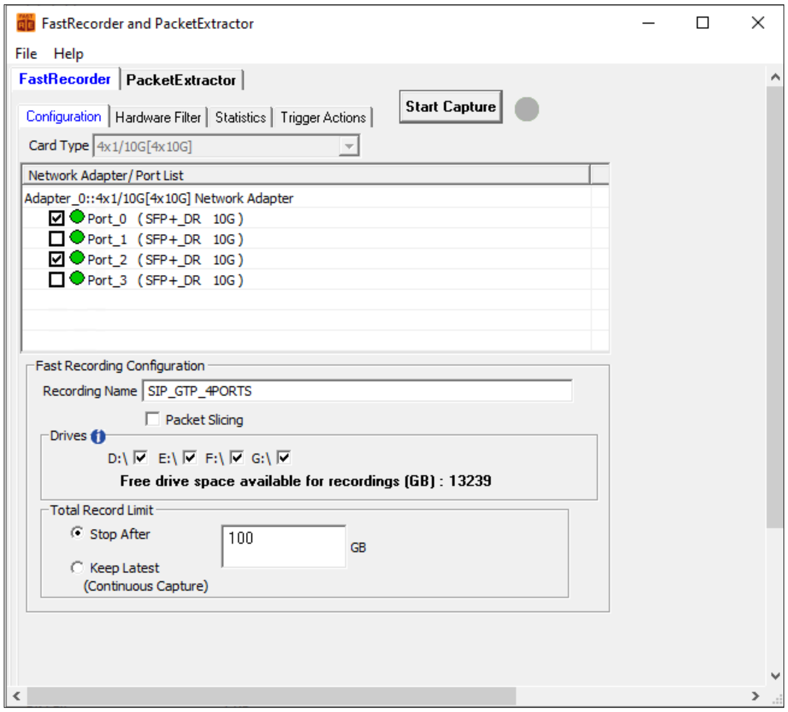


Filters → Port Filter, Pre-Extraction Filter, and Extraction Filter

Select Previous Recording → Output file generated from Fast Recorder, once recording is stopped

FastRecorder™

In the FastRecorder™ application, users can configure ports on the selected card to receive traffic at the full line rate. They can also choose the disk drives where the recorded traffic will be saved. If necessary, users can access drive information details, including Usage and Health Status. The **Total Record Limit** Option, known as "Stop After," allows users to halt recording once the file size reaches a specified limit. Alternatively, the "Keep Latest (Continuous Capture)" limit option enables continuous recording. When the recording limit is reached, users can retrieve the latest recorded traffic up to the specified size from the Total Record Limit.



Card Type: 4x1/10G[4x10G]

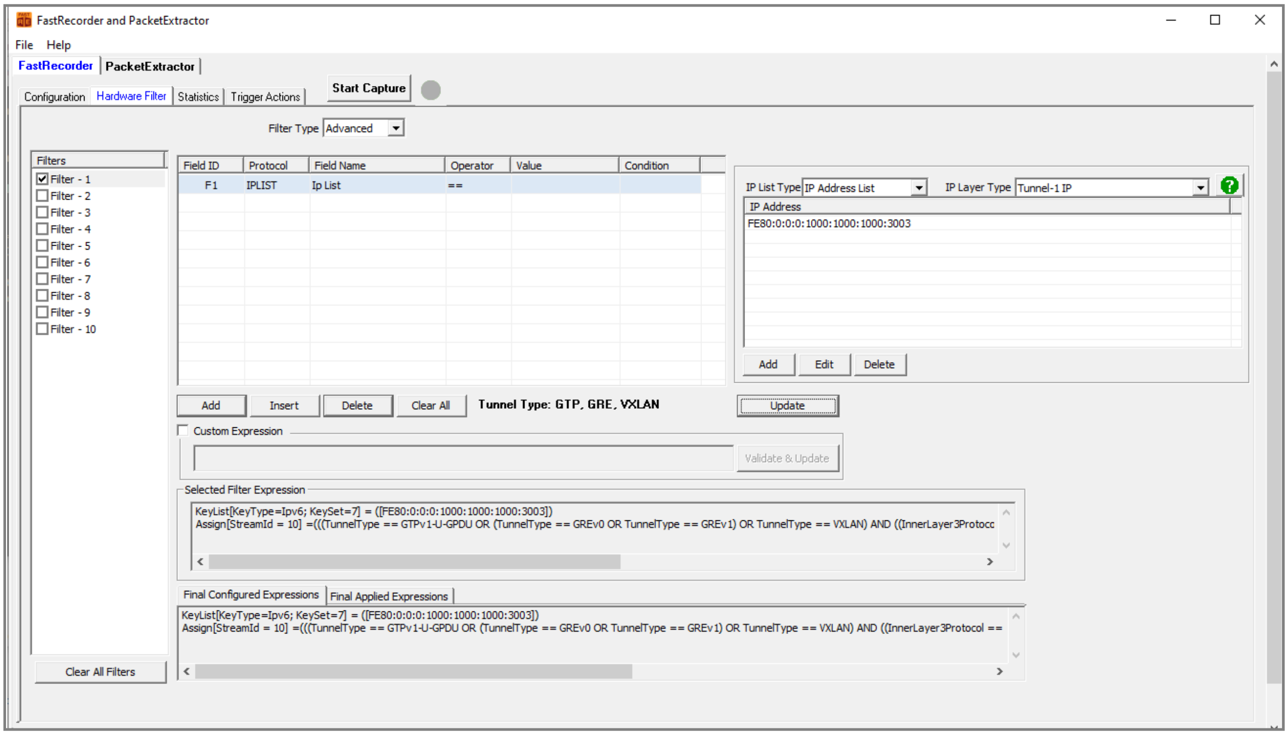
Network Adapter/ Port List
Adapter_0::4x1/10G[4x10G] Network Adapter
- ☑ Port_0 (SFP+_DR 10G)
- □ Port_1 (SFP+_DR 10G)
- ☑ Port_2 (SFP+_DR 10G)
- □ Port_3 (SFP+_DR 10G)

Fast Recording Configuration
Recording Name: SIP_GTP_4PORTS
□ Packet Slicing
Drives: D:\ ☑ E:\ ☑ F:\ ☑ G:\ ☑
Free drive space available for recordings (GB) : 13239

Total Record Limit
- ● Stop After 100 GB
- ○ Keep Latest (Continuous Capture)

Hardware Filters

The Hardware Filter option enables users to easily set up filter conditions to capture traffic of interest continuously at line rate. For instance, it can be used to filter GTP traffic as shown below.



Filter Type: Advanced

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

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

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

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

Tunnel Type: GTP, GRE, VXLAN

□ Custom Expression

Selected Filter Expression

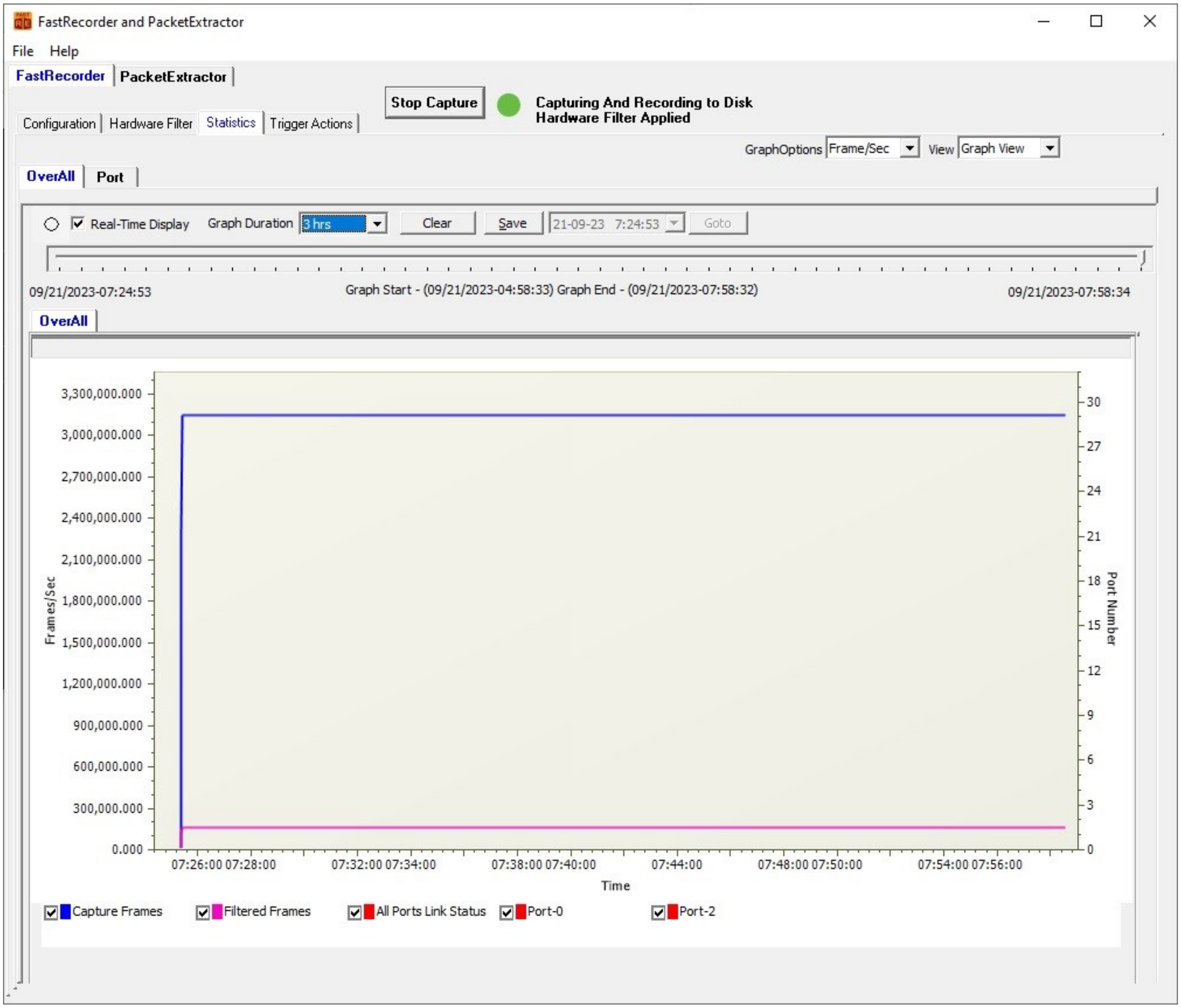
```
KeyList[KeyType=Ipv6; KeySet=7] = ([FE80:0:0:0:1000:1000:1000:3003])
Assign[StreamId = 10] =(((TunnelType == GTPv1-U-GPDU OR (TunnelType == GREv0 OR TunnelType == GREv1) OR TunnelType == VXLAN) AND ((InnerLayer3Protocc
```

Final Configured Expressions

```
KeyList[KeyType=Ipv6; KeySet=7] = ([FE80:0:0:0:1000:1000:1000:3003])
Assign[StreamId = 10] =(((TunnelType == GTPv1-U-GPDU OR (TunnelType == GREv0 OR TunnelType == GREv1) OR TunnelType == VXLAN) AND ((InnerLayer3Protocol ==
```

FastRecorder™ Overall Graph View

Users can monitor real-time graphs displaying Time vs. Rate, Capture Rate, Filter Rate, and Port Link Status for the past 7 days.



FastRecorder and PacketExtractor

Capturing And Recording to Disk
Hardware Filter Applied

GraphOptions Frame/Sec

View Graph View

○ ☑ Real-Time Display

Graph Duration 3 hrs

21-09-23 7:24:53

09/21/2023-07:24:53

Graph Start - (09/21/2023-04:58:33) Graph End - (09/21/2023-07:58:32)

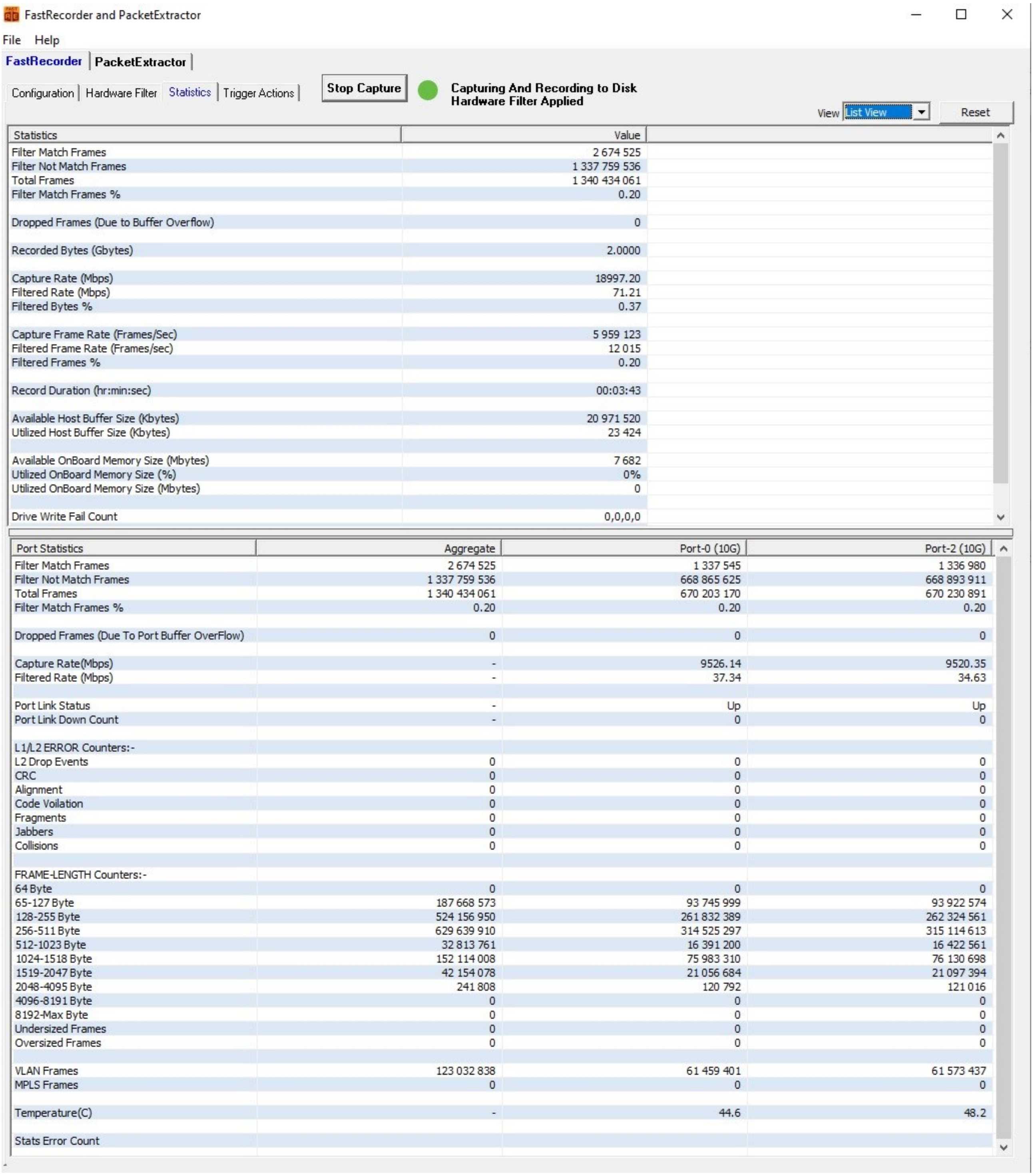
09/21/2023-07:58:34

☑ 🟦 Capture Frames ☑ 🟪 Filtered Frames ☑ 🟥 All Ports Link Status ☑ 🟥 Port-0 ☑ 🟥 Port-2

FastRecorder™ Statistics

The **Statistics** tab provides the below statistics information.

- Filter Match Frames, Filter Not Match Frames, Total Frames, Filter Match Frames %, Dropped Frames (Due to Buffer Overflow)
- Recorded Bytes (Gbytes), Capture Rate (Mbps), Filtered Rate (Mbps), Filtered Bytes, Capture Frame Rate (Frames/Sec)
- Filtered Frame Rate (Frames/Sec), Filtered Frames, Record Duration (hr:min), Available Host Buffer Size (Kbytes)
- Utilized Host Buffer Size (Kbytes), Available OnBoard Memory Size (Mbytes), Utilized OnBoard Memory Size (%)
- Utilized OnBoard Memory Size (Mbytes), Disk Write Fail Count



Capturing And Recording to Disk
Hardware Filter Applied

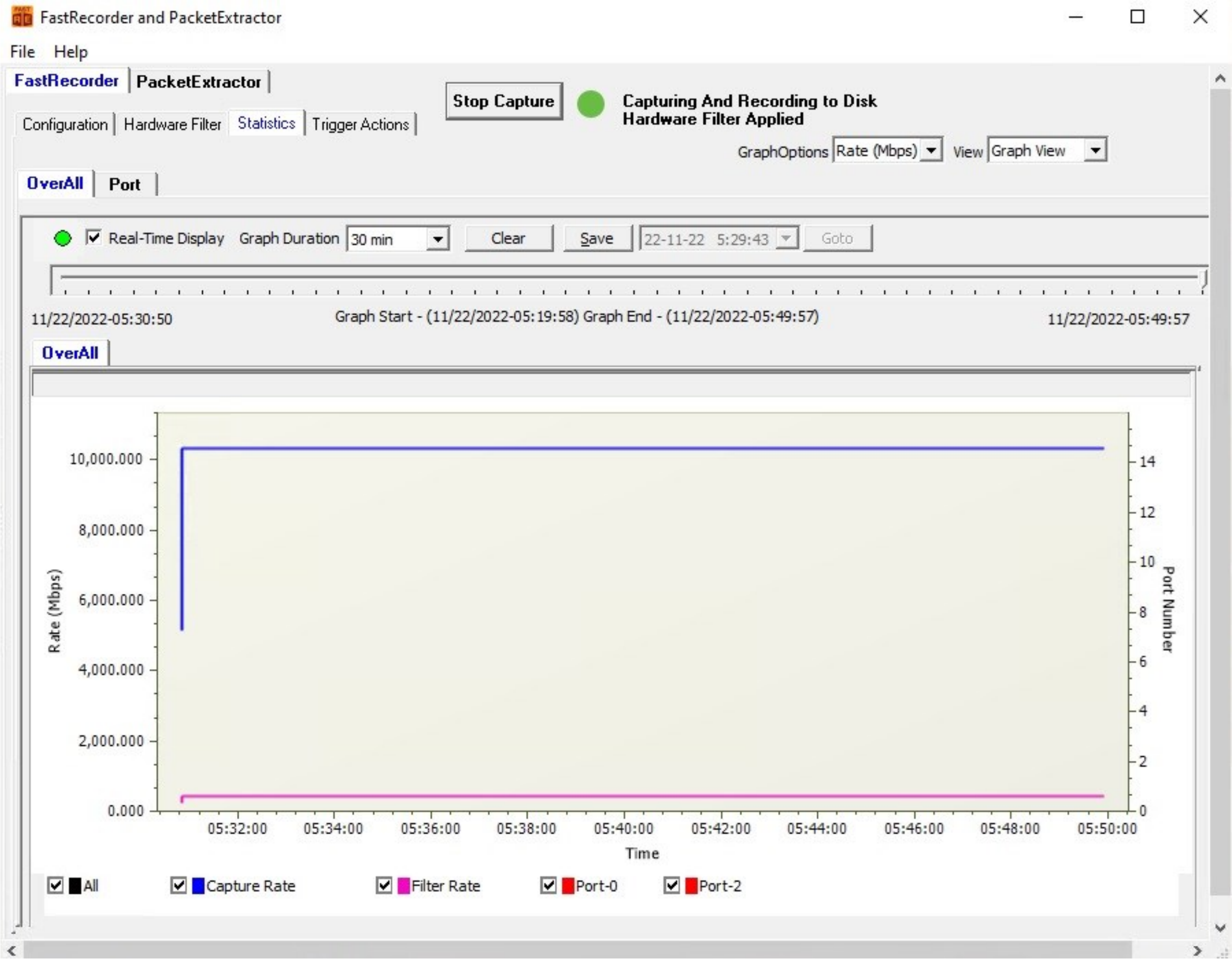
View: List View

Statistics	Value
Filter Match Frames	2 674 525
Filter Not Match Frames	1 337 759 536
Total Frames	1 340 434 061
Filter Match Frames %	0.20
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	2.0000
Capture Rate (Mbps)	18997.20
Filtered Rate (Mbps)	71.21
Filtered Bytes %	0.37
Capture Frame Rate (Frames/Sec)	5 959 123
Filtered Frame Rate (Frames/sec)	12 015
Filtered Frames %	0.20
Record Duration (hr:min:sec)	00:03:43
Available Host Buffer Size (Kbytes)	20 971 520
Utilized Host Buffer Size (Kbytes)	23 424
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

Port Statistics	Aggregate	Port-0 (10G)	Port-2 (10G)
Filter Match Frames	2 674 525	1 337 545	1 336 980
Filter Not Match Frames	1 337 759 536	668 865 625	668 893 911
Total Frames	1 340 434 061	670 203 170	670 230 891
Filter Match Frames %	0.20	0.20	0.20
Dropped Frames (Due To Port Buffer OverFlow)	0	0	0
Capture Rate(Mbps)	-	9526.14	9520.35
Filtered Rate (Mbps)	-	37.34	34.63
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	187 668 573	93 745 999	93 922 574
128-255 Byte	524 156 950	261 832 389	262 324 561
256-511 Byte	629 639 910	314 525 297	315 114 613
512-1023 Byte	32 813 761	16 391 200	16 422 561
1024-1518 Byte	152 114 008	75 983 310	76 130 698
1519-2047 Byte	42 154 078	21 056 684	21 097 394
2048-4095 Byte	241 808	120 792	121 016
4096-8191 Byte	0	0	0
8192-Max Byte	0	0	0
Undersized Frames	0	0	0
Oversized Frames	0	0	0
VLAN Frames	123 032 838	61 459 401	61 573 437
MPLS Frames	0	0	0
Temperature(C)	-	44.6	48.2
Stats Error Count			

FastRecorder™ Per Port Graph View

Users can view real-time port graphs (Time vs. Frames/Sec) displaying Capture and Filtered Frames data for the past 7 days.



Capturing And Recording to Disk
Hardware Filter Applied

GraphOptions Rate (Mbps) View Graph View

● ☑ Real-Time Display Graph Duration 30 min

22-11-22 5:29:43

11/22/2022-05:30:50

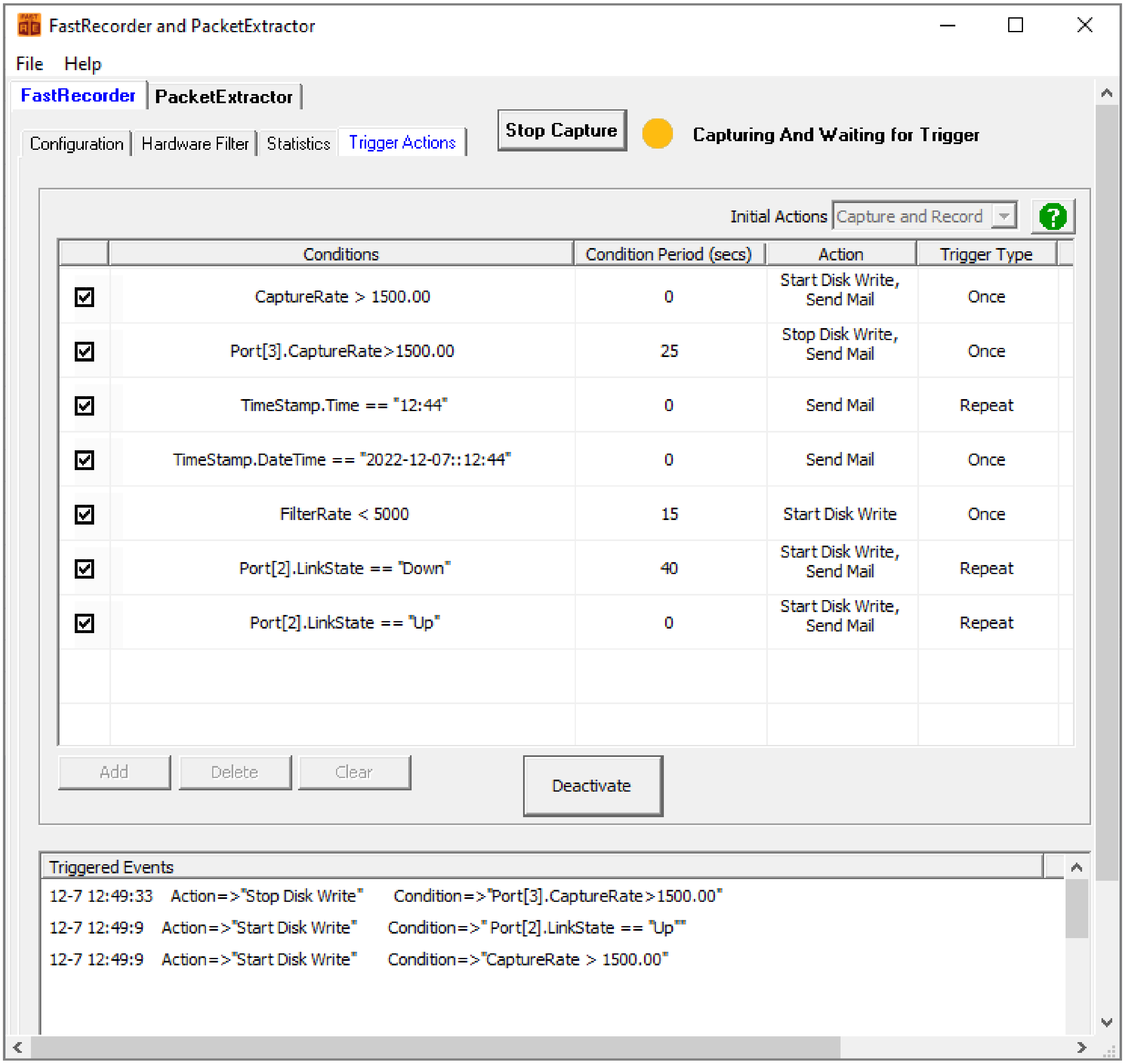
Graph Start - (11/22/2022-05:19:58) Graph End - (11/22/2022-05:49:57)

11/22/2022-05:49:57

Trigger Actions

Users can set triggers to perform actions based on the following specified conditions:

- CaptureRate (Mbps)
- FilterRate (Mbps)
- Port[n].CaptureRate (Mbps)
- Port[n].FilterRate (Mbps): where n is port number
- TimeStamp.DateTime, TimeStamp
- Time (min)



Capturing And Waiting for Trigger

Initial Actions: Capture and Record

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

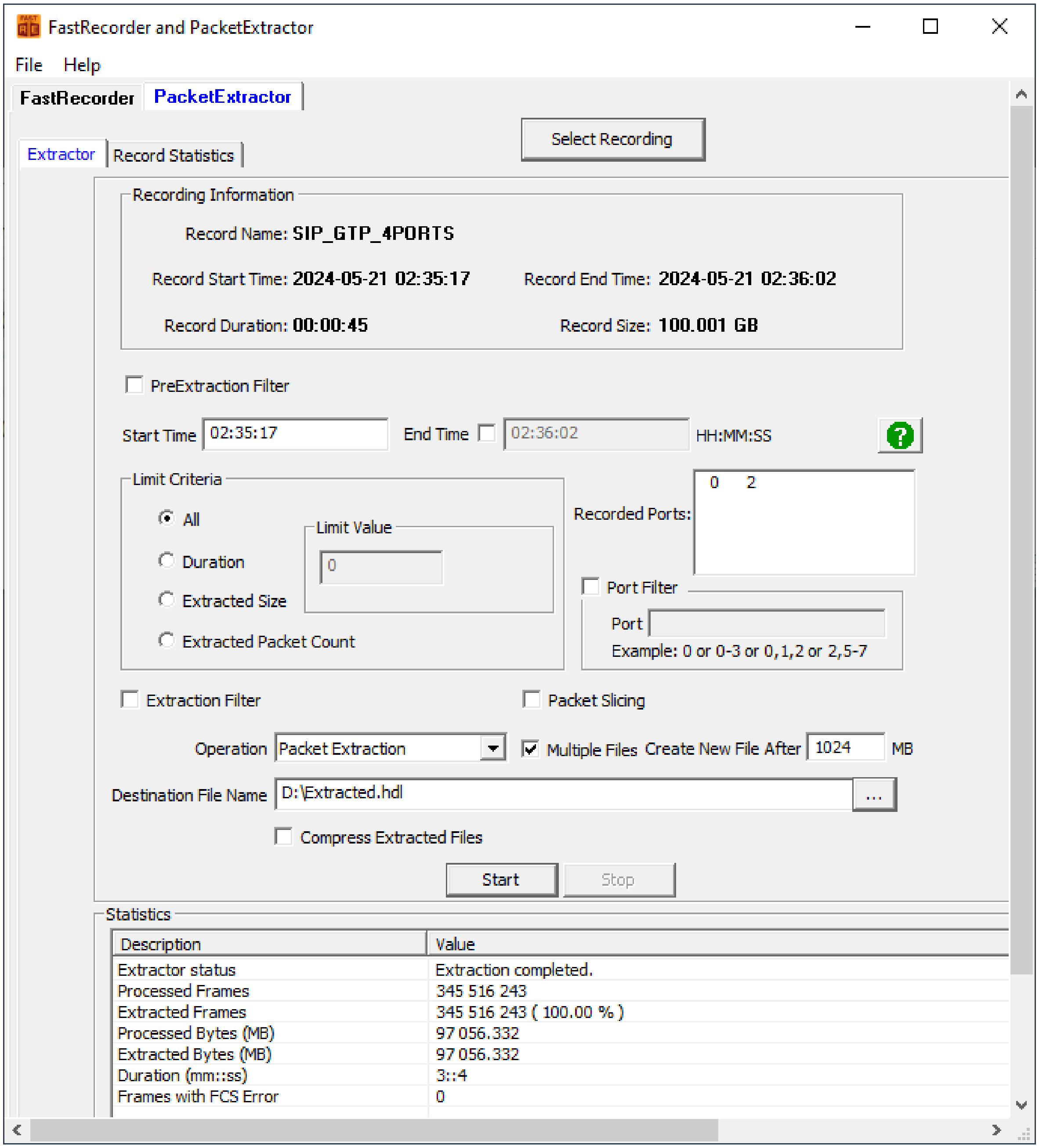
```
Triggered Events
12-7 12:49:33   Action=>"Stop Disk Write"    Condition=>"Port[3].CaptureRate>1500.00"
12-7 12:49:9   Action=>"Start Disk Write"   Condition=>" Port[2].LinkState == "Up""
12-7 12:49:9   Action=>"Start Disk Write"   Condition=>"CaptureRate > 1500.00"
```

PacketExtractor™

In the PacketExtractor™ application, the configuration settings allow users to extract recorded files from the selected HD NIC interface port and specify the desired output file format for offline analysis. Packet extraction from the saved recording files can be done with or without applying filters. A pre-extraction filter has been introduced to eliminate frames captured due to GL's SmartNIC™ limitations. Users can enable the **Port Filter** option and specify the port to be filtered. Various limit criteria options, including **Duration**, **Extracted Size**, and **Extracted Packet Count**, can be applied to extract files based on specified limit values. Users can choose the **Multiple Files** option when dealing with large recorded packet files. This option creates new files with the specified file size, each with a sequence number appended to the file name.

Packet Extraction from the Recording files without filter

When extracting packets from a recorded file without using a filter, select the file, specify the default record start time, uncheck the Extractor Filter option, choose the desired path to save the extracted data to a file, and view the extracted statistics under the **Statistics** section.



Recording Information

Record Name: SIP_GTP_4PORTS

Record Start Time: 2024-05-21 02:35:17 Record End Time: 2024-05-21 02:36:02

Record Duration: 00:00:45 Record Size: 100.001 GB

□ PreExtraction Filter

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

Limit Criteria: ● All ○ 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 □ Packet Slicing

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

Destination File Name D:\Extracted.hdl

□ Compress Extracted Files

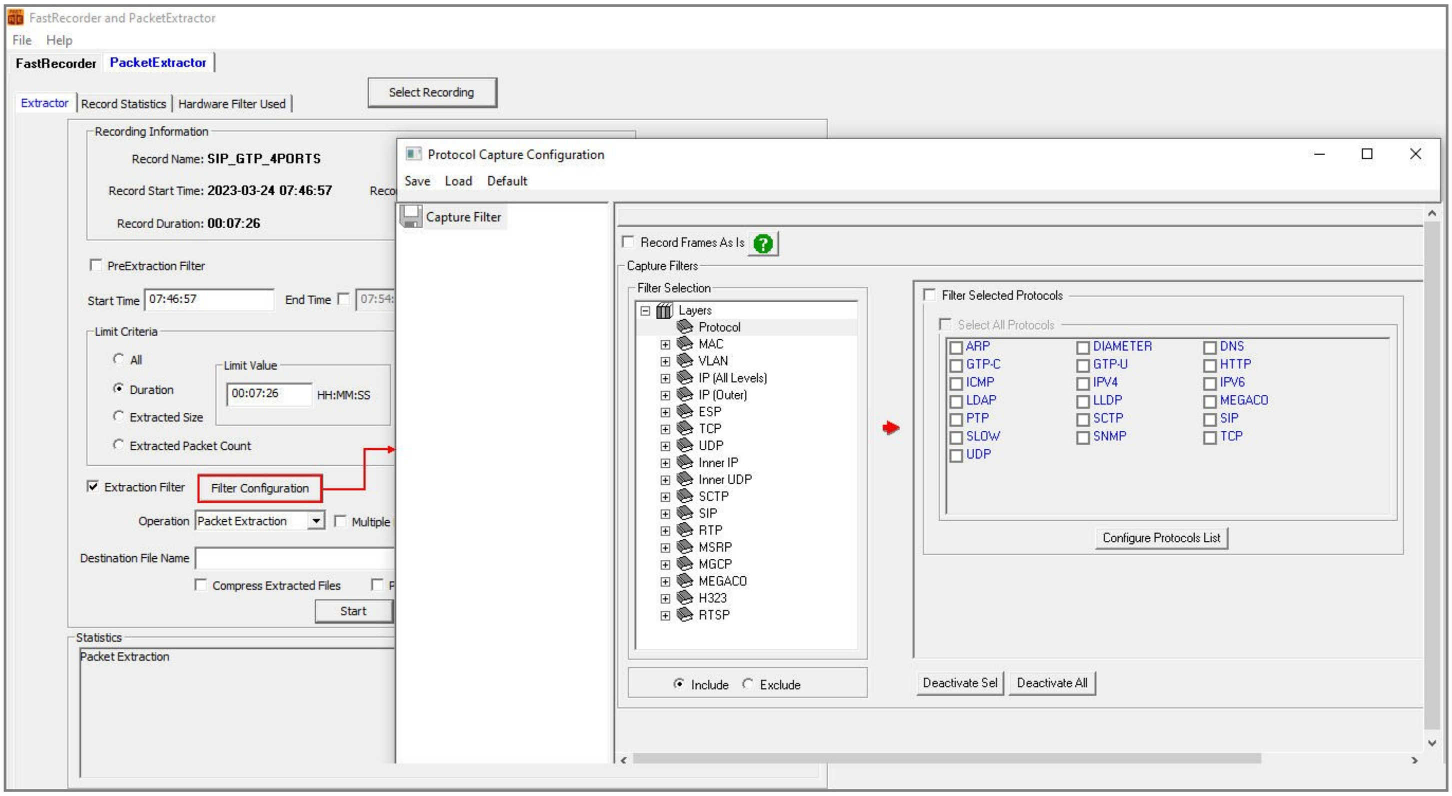
Statistics

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

PacketExtractor (*contd.*)

Packet Extraction from the Recording files with filter

For extracting packets from previously recorded files with filters, select the previously recorded file. Check the **Extractor Filter** option to apply various software filters according to test requirements, and then configure the filters accordingly. Finally, select the desired path for saving the extracted data to a file.



Record Name: SIP_GTP_4PORTS

Record Start Time: 2023-03-24 07:46:57

Record Duration: 00:07:26

□ PreExtraction Filter

Start Time 07:46:57 End Time □ 07:54:

Limit Criteria: ○ All ● Duration ○ Extracted Size ○ Extracted Packet Count

Limit Value 00:07:26 HH:MM:SS

☑ Extraction Filter

Operation Packet Extraction □ Multiple

Destination File Name

□ Compress Extracted Files

□ Record Frames As Is

Filter Selection: Layers – Protocol, MAC, VLAN, IP (All Levels), IP (Outer), ESP, TCP, UDP, Inner IP, Inner UDP, SCTP, SIP, RTP, MSRP, MGCP, MEGACO, H323, RTSP

● Include ○ Exclude

□ Filter Selected Protocols

□ Select All Protocols

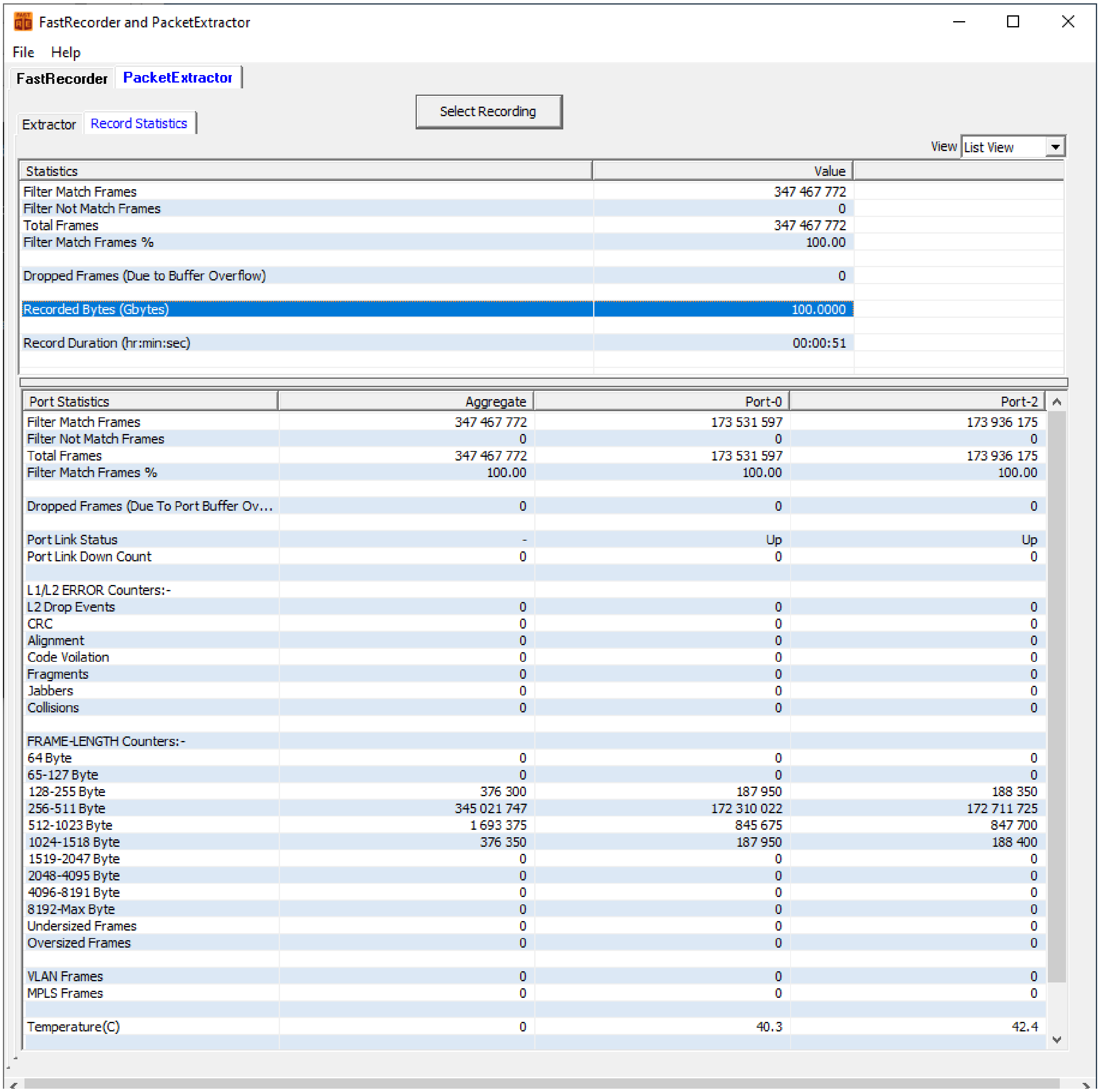
□ ARP	□ DIAMETER	□ DNS
□ GTP-C	□ GTP-U	□ HTTP
□ ICMP	□ IPV4	□ IPV6
□ LDAP	□ LLDP	□ MEGACO
□ PTP	□ SCTP	□ SIP
□ SLOW	□ SNMP	□ TCP
□ UDP		

GL Communications Inc.

Record Statistics

Display the information of :

- Filter Match Frames
- Filter Not Match Frames
- Total Frames
- Filter Match Frames %
- Dropped Frames (Due to Buffer Overflow)
- Record Duration (hr:min:sec)

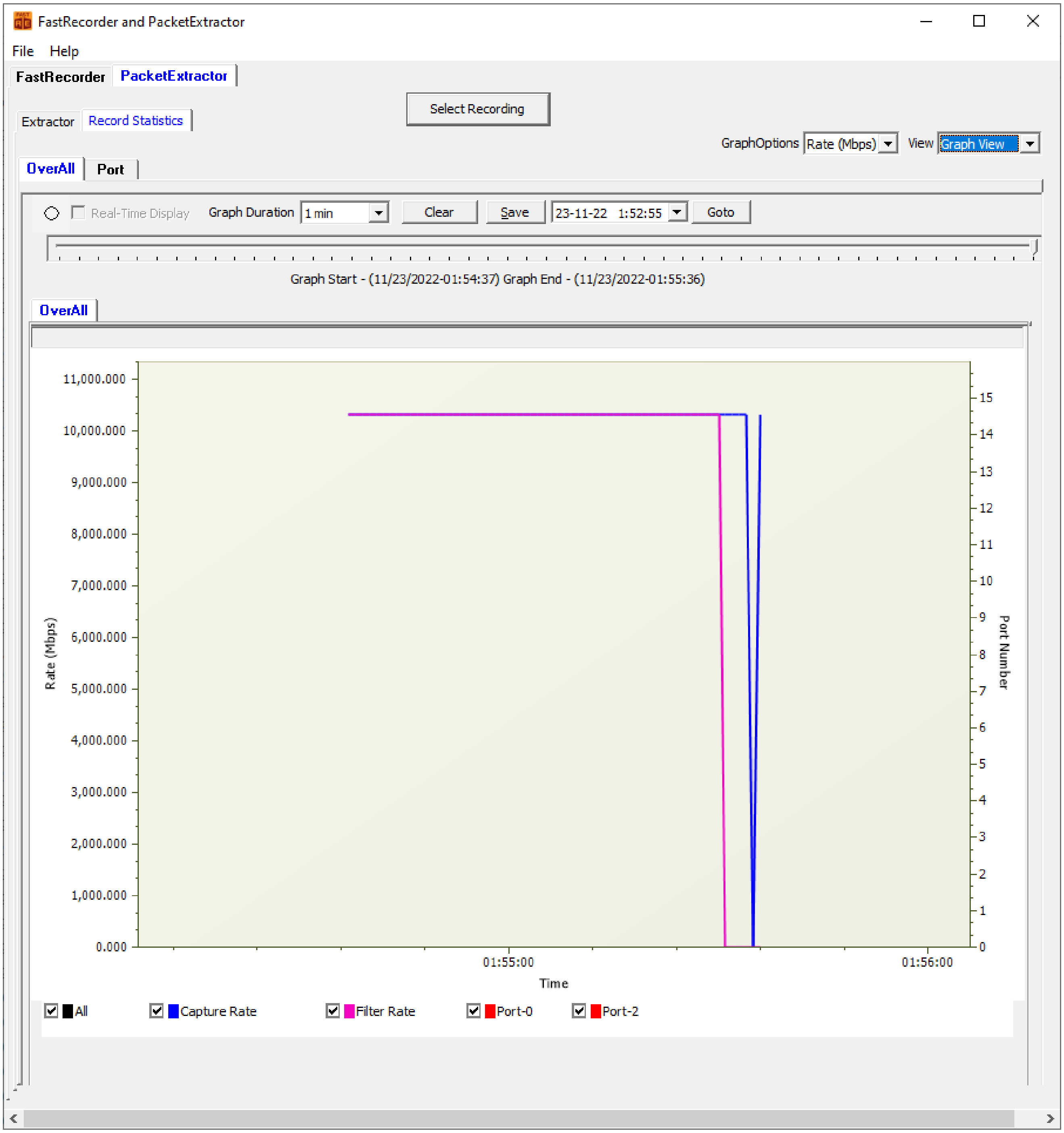


Statistics	Value	
Filter Match Frames	347 467 772	
Filter Not Match Frames	0	
Total Frames	347 467 772	
Filter Match Frames %	100.00	
Dropped Frames (Due to Buffer Overflow)	0	
Recorded Bytes (Gbytes)	100.0000	
Record Duration (hr:min:sec)	00:00:51	

Port Statistics	Aggregate	Port-0	Port-2
Filter Match Frames	347 467 772	173 531 597	173 936 175
Filter Not Match Frames	0	0	0
Total Frames	347 467 772	173 531 597	173 936 175
Filter Match Frames %	100.00	100.00	100.00
Dropped Frames (Due To Port Buffer Ov...	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	376 300	187 950	188 350
256-511 Byte	345 021 747	172 310 022	172 711 725
512-1023 Byte	1 693 375	845 675	847 700
1024-1518 Byte	376 350	187 950	188 400
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	40.3	42.4

Recorder Graph View

User can view the Capture and Filter rates of the recorded file.



GraphOptions Rate (Mbps) View Graph View

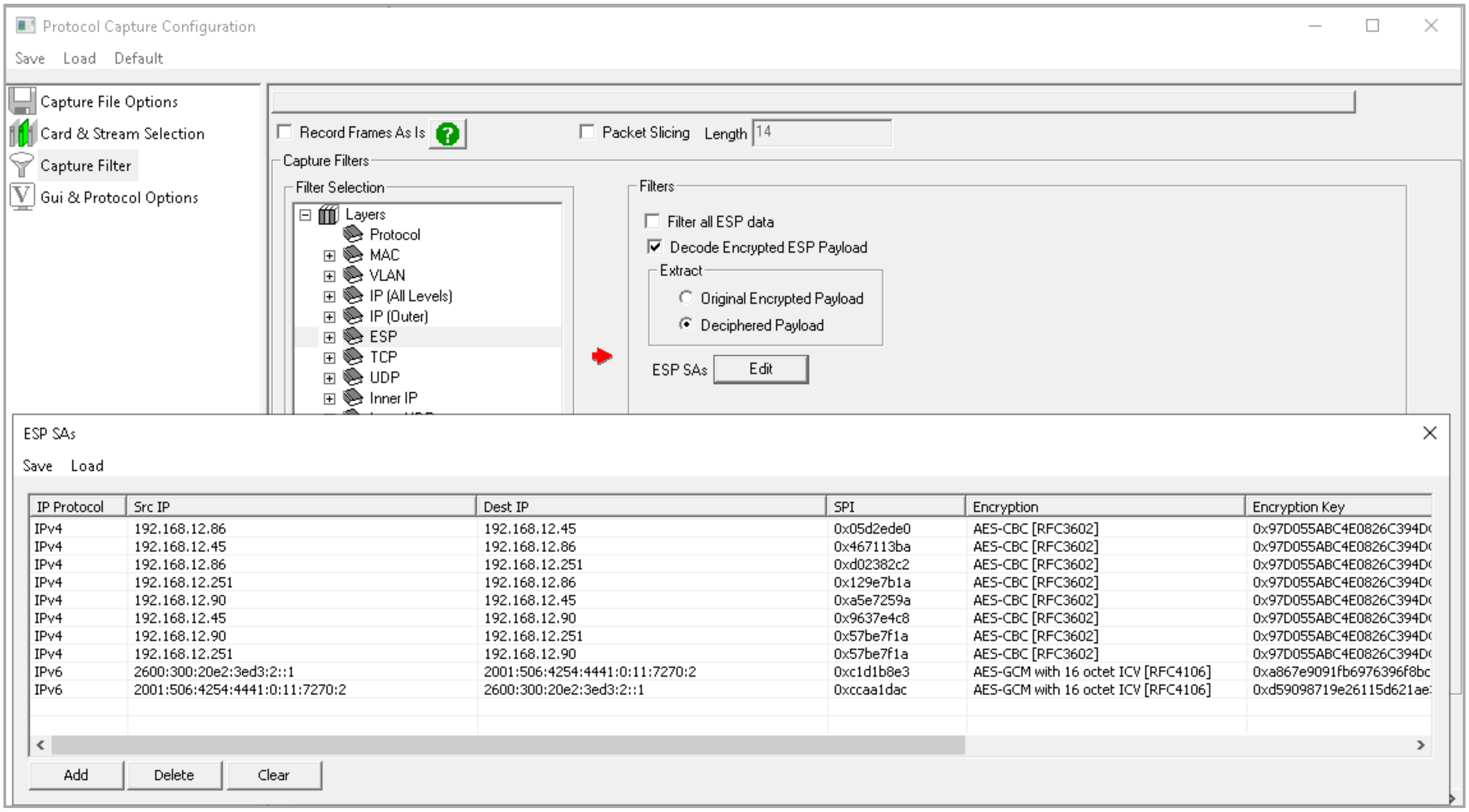
○ ☐ Real-Time Display Graph Duration 1 min 23-11-22 1:52:55

Graph Start - (11/23/2022-01:54:37) Graph End - (11/23/2022-01:55:36)

☑ ■ All ☑ 🟦 Capture Rate ☑ ■ Filter Rate ☑ 🟥 Port-0 ☑ 🟥 Port-2

Encapsulating Security Payload (ESP) Deciphering

FastRecorder™ and PacketExtractor™ analyzer supports the decryption of ESP packets on both IPv4 and IPv6 by providing ESP SAs value.



□ Record Frames As Is

□ Packet Slicing Length 14

□ Filter all ESP data

☑ Decode Encrypted ESP Payload

Extract

○ Original Encrypted Payload

● Deciphered Payload

ESP SAs Edit

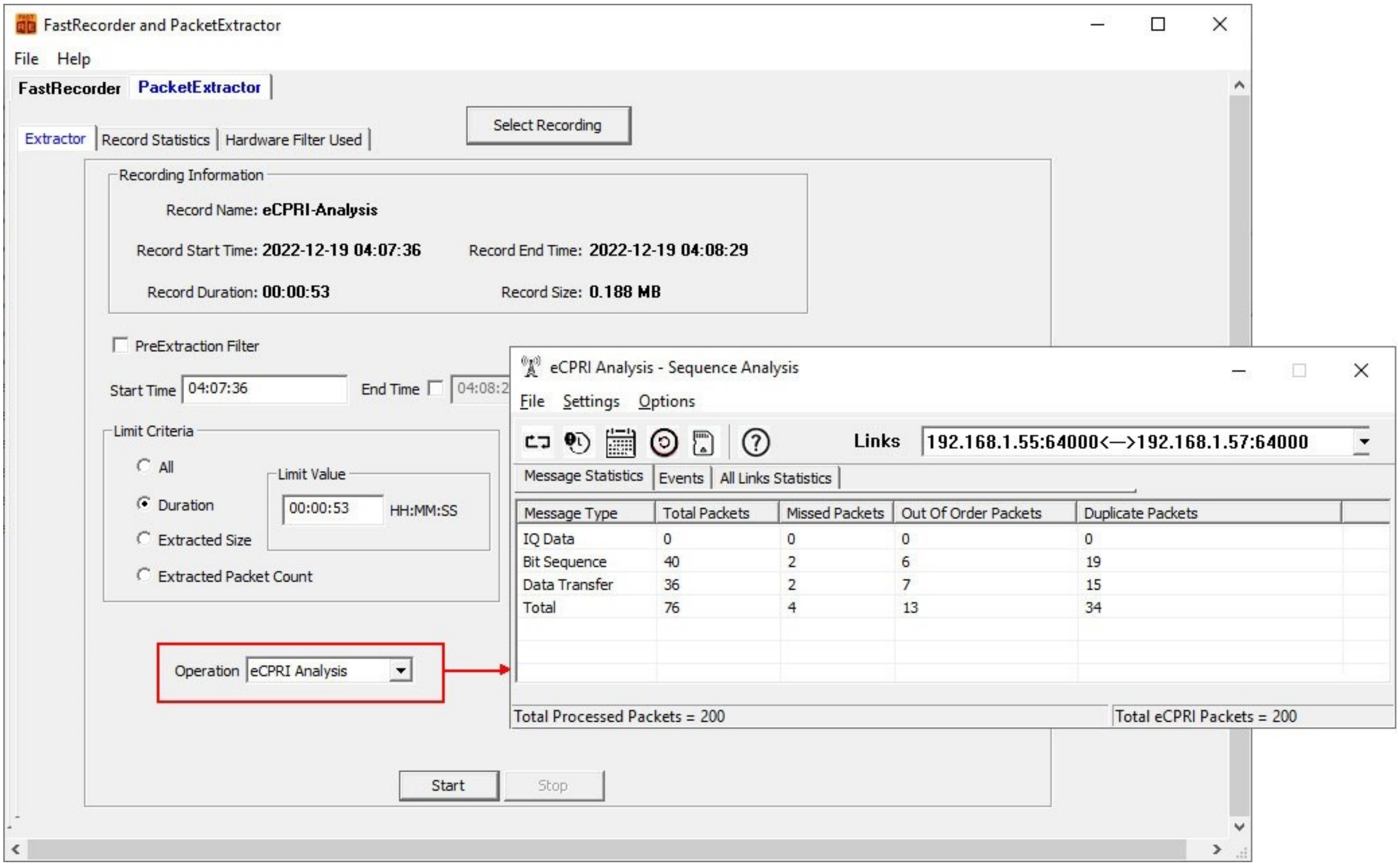
IP Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key
IPv4	192.168.12.86	192.168.12.45	0x05d2ede0	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.45	192.168.12.86	0x467113ba	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.86	192.168.12.251	0xd02382c2	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.251	192.168.12.86	0x129e7b1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.90	192.168.12.45	0xa5e7259a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.45	192.168.12.90	0x9637e4c8	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.90	192.168.12.251	0x57be7f1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv4	192.168.12.251	192.168.12.90	0x57be7f1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394D
IPv6	2600:300:20e2:3ed3:2::1	2001:506:4254:4441:0:11:7270:2	0xc1d1b8e3	AES-GCM with 16 octet ICV [RFC4106]	0xa867e9091fb6976396f8bc
IPv6	2001:506:4254:4441:0:11:7270:2	2600:300:20e2:3ed3:2::1	0xccaa1dac	AES-GCM with 16 octet ICV [RFC4106]	0xd59098719e26115d621ae

eCPRI Analysis

FastRecorder™ and PacketExtractor™ analyzer supports eCPRI analysis to monitor eCPRI traffic for packet impairments such as Missed Packets, Out of Order, Duplicate Packets, One-Way Delay etc.

GL's eCPRI protocol analysis tool supports eCPRI message types such as IQ Data, Bit Sequence, Generic Data Transfer, Remote Memory Access, One-way Delay Measurement, Remote Reset, and Event Indication for analysis and statistics.

- Monitor and decode eCPRI traffic for packet impairments such as Missed Packets, Out of Order, Duplicate Packets, One-Way Delay etc.
- Provides the message statistics for Sequence Analysis, One-Way Delay Measurement, Event Indication, Remote Reset, and Remote Memory Access
- Supports eCPRI analysis for each IPv4 and IPv6 pair address
- All Links statistics provides sequence analysis for all the available eCPRI links
- Supports One-Way Delay calculation in microseconds
- Supports Hardware Faults, Software Faults or Vender specific Faults for the selected Element ID
- Provides graphical representation of Remote reset statistics
- Supports Remote Memory Access statistics for each Element ID and also total statistics for all the elements



Recording Information

Record Name: **eCPRI-Analysis**

Record Start Time: **2022-12-19 04:07:36** Record End Time: **2022-12-19 04:08:29**

Record Duration: **00:00:53** Record Size: **0.188 MB**

□ PreExtraction Filter

Start Time 04:07:36 End Time □ 04:08:2

Limit Criteria

○ All
● Duration
○ Extracted Size
○ Extracted Packet Count

Limit Value 00:00:53 HH:MM:SS

Operation eCPRI Analysis

Links 192.168.1.55:64000<—>192.168.1.57:64000

Message Type	Total Packets	Missed Packets	Out Of Order Packets	Duplicate Packets
IQ Data	0	0	0	0
Bit Sequence	40	2	6	19
Data Transfer	36	2	7	15
Total	76	4	13	34

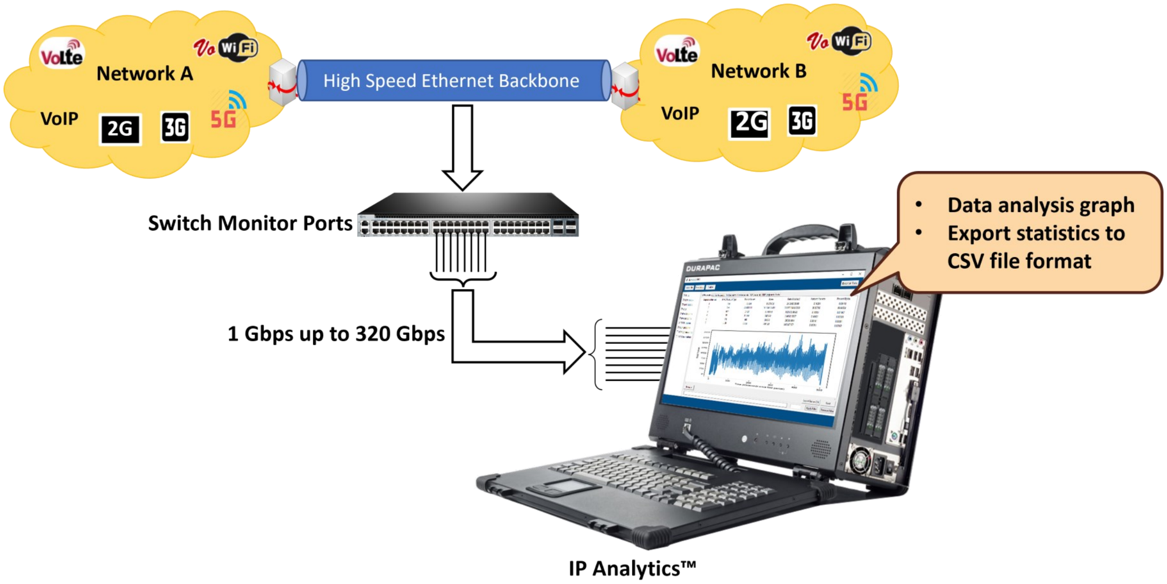
Total Processed Packets = 200 Total eCPRI Packets = 200

IP Analytics™

IP Analytics™ (PKV410), an optional add-on with FastRecorder™ and PacketExtractor™ plays a crucial role for monitoring and maintaining Quality of Service (QoS) in telecom networks. This involves analyzing IP-based data streams to ensure that voice, video, and data services meet predefined performance standards. IP Analytics™ provides detailed insight into recorded IP traffic captured at high speed. By analyzing IP traffic and data, telecom companies can enhance network performance, troubleshoot malfunctioning infrastructure, improve customer satisfaction, and increase operational efficiency . GL IP-ANALYTICS displays statistics for Layer 3, DSCP, Layer 4, IPv4, IPv6, UDP, and TCP Endpoints, IPv4, IPv6, UDP, TCP, SCTP, and PING Conversations.

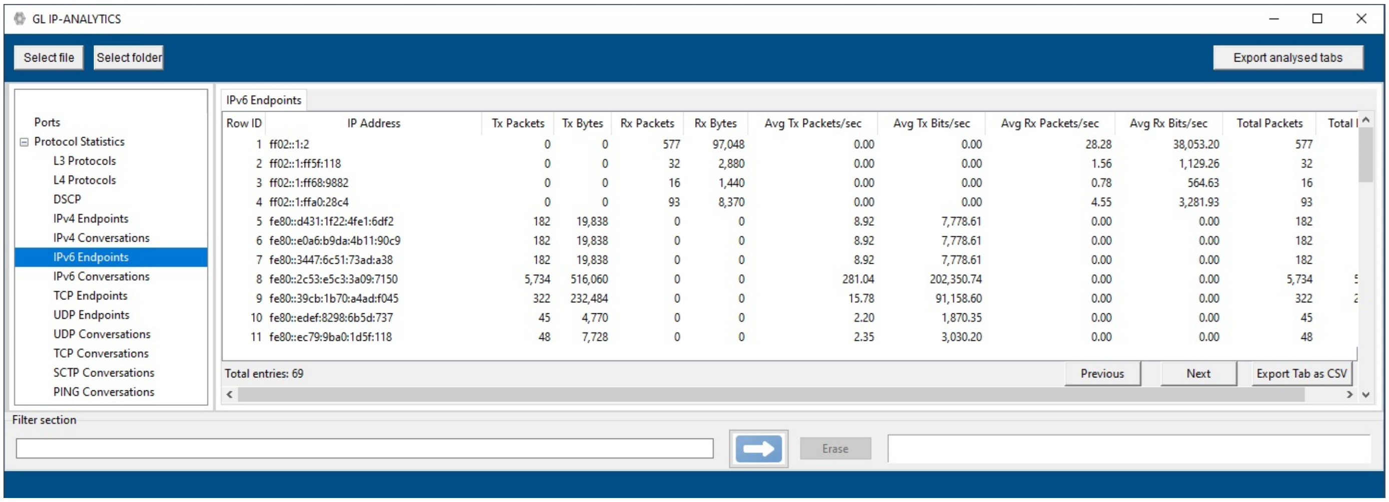
Data Analysis

Analyzing data in IP networks involves examining traffic patterns to understand how data flows through the network. This includes identifying peak usage times, the types of applications consuming bandwidth, and trends in user behavior. By analyzing this data, network administrators can optimize resource allocation and plan for capacity upgrades to meet changing demands. PacketExtractor™ now offers enhanced data analysis capabilities by incorporating GL's **IP Analytics**.



- Data analysis graph
- Export statistics to CSV file format

GL's **IP Analytics** tool is designed for analyzing **HDF5** files and extracting comprehensive statistics. It covers a range of protocols from **Layer 3** to **Layer 4**, providing insights into **IPv4 Endpoints**, **IPv4 Conversations, IPv6 Endpoints**, **IPv6 Conversations, UDP Endpoints**, **TCP Endpoints**, **UDP Conversation**, **TCP Conversation**, **SCTP Conversations, Ping Conversations** and **Ports**. It is an easy-to-use solution for data exploration.



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

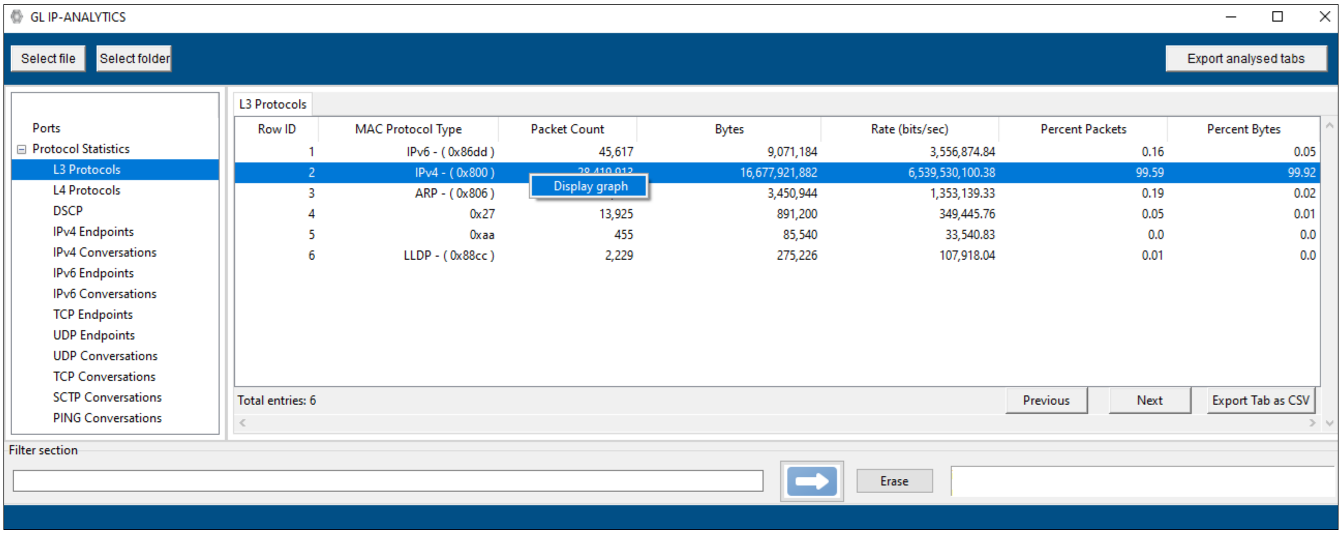
Total entries: 69

Key Features

- Includes detailed analysis of different IP layers such as Ports, Layer 3 Protocols, L4 Protocols, DSCP, IPv4 Endpoints, IPv4 Conversations IPv6 Endpoints, IPv6 Conversations TCP Endpoints, UDP Endpoints, UDP Conversations, UDP Conversations, TCP Conversations, SCTP Conversations, and Ping Conversations
- Supports Tunnel Filtering and displays the statistics
- Provides in-depth graph analysis for both Bits/sec and Packets/sec
- Provides advanced filters to analyze the required packets
- Easily export information from all tabs or specific tab information to CSV file format for further analysis
- Allows selection of either a single Data Analysis HDF5 file or multiple HDF5 files from the folder
- Provides the flexibility to sort columns in Ascending or Descending order for easier data interpretation

Graphs

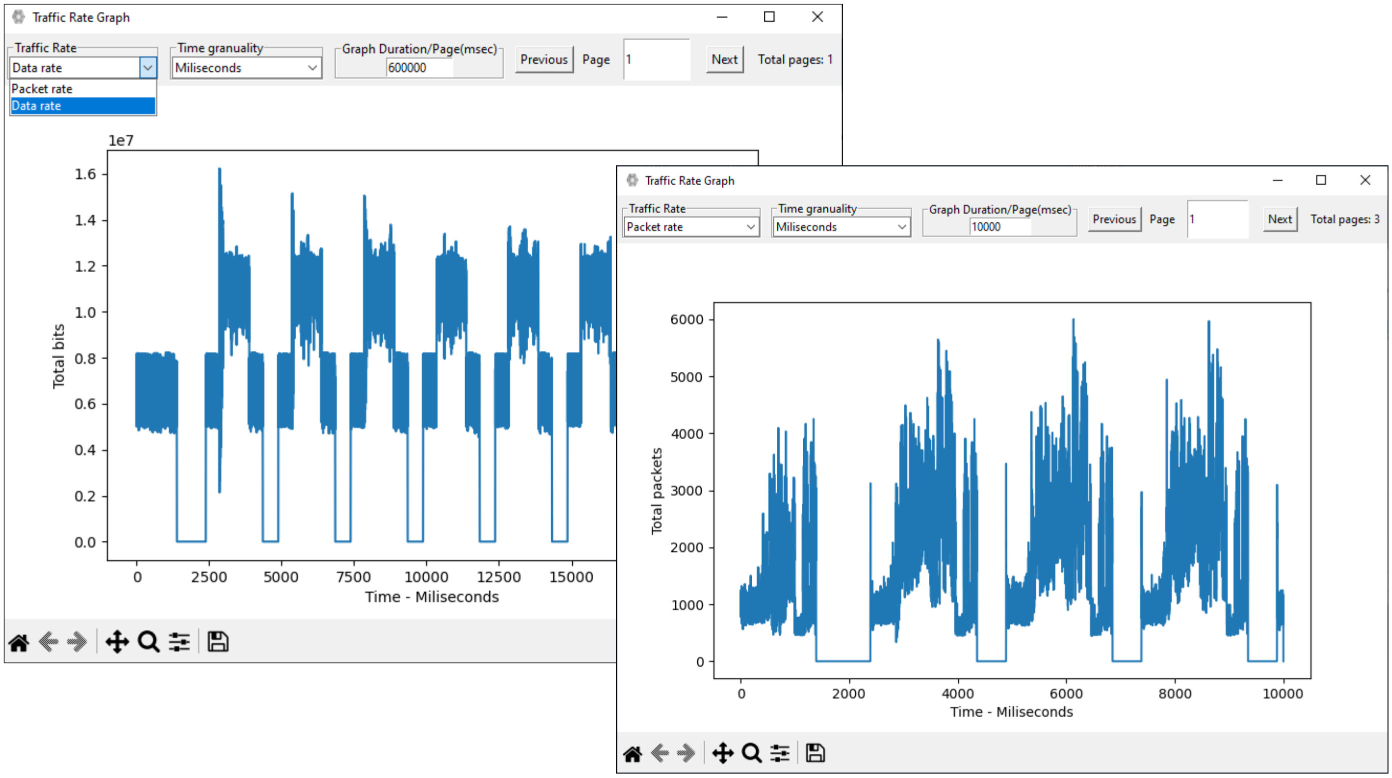
Users can select **Display Graph** option to view the Data/Packets rate graphs.



Row ID	MAC Protocol Type	Packet Count	Bytes	Rate (bits/sec)	Percent Packets	Percent Bytes
1	IPv6 - (0x86dd)	45,617	9,071,184	3,556,874.84	0.16	0.05
2	IPv4 - (0x800)	28,410,912	16,677,921,882	6,539,530,100.38	99.59	99.92
3	ARP - (0x806)	[illegible]	3,450,944	1,353,139.33	0.19	0.02
4	0x27	13,925	891,200	349,445.76	0.05	0.01
5	0xaa	455	85,540	33,540.83	0.0	0.0
6	LLDP - (0x88cc)	2,229	275,226	107,918.04	0.01	0.0

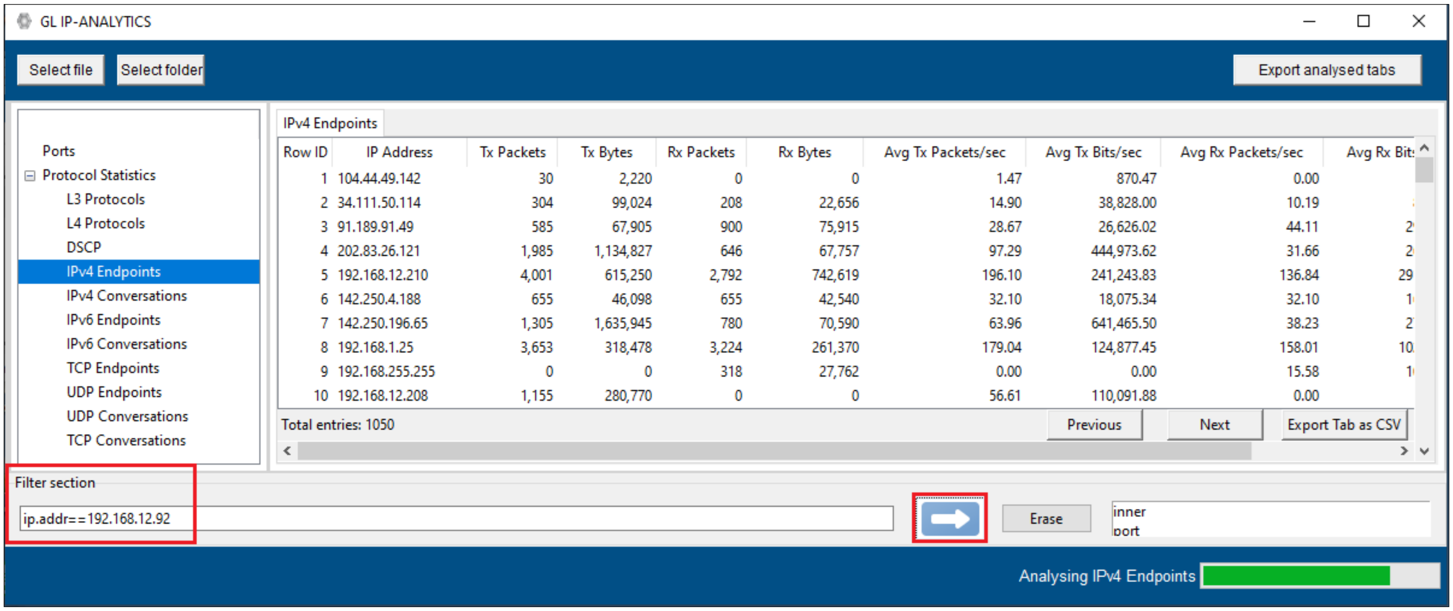
Total entries: 6

Display of **Data Rate Over Time** and **Packet Rate Over Time** graphs.



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. The suggestion box recommends keywords for filtering as the user types the keyword. In this instance, filter is applied for **ip.addr == 192.168.12.92**.

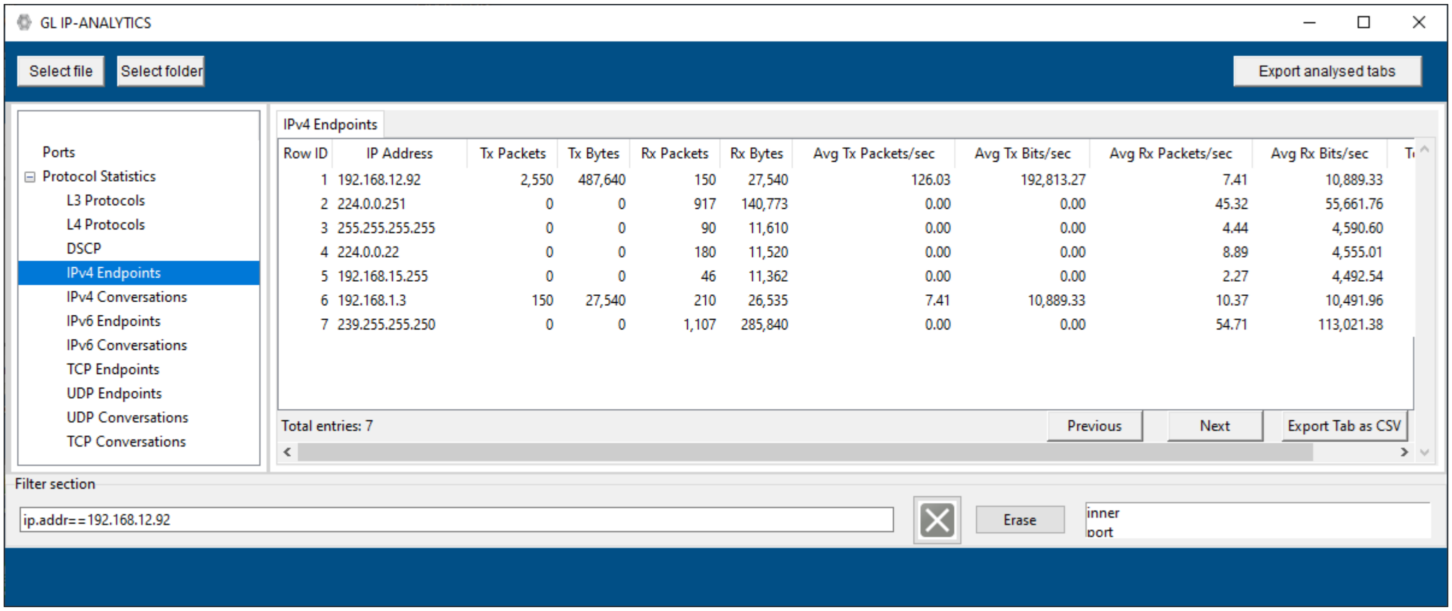


Row ID	IP Address	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Avg Tx Packets/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bit
1	104.44.49.142	30	2,220	0	0	1.47	870.47	0.00	
2	34.111.50.114	304	99,024	208	22,656	14.90	38,828.00	10.19	
3	91.189.91.49	585	67,905	900	75,915	28.67	26,626.02	44.11	2
4	202.83.26.121	1,985	1,134,827	646	67,757	97.29	444,973.62	31.66	2
5	192.168.12.210	4,001	615,250	2,792	742,619	196.10	241,243.83	136.84	29
6	142.250.4.188	655	46,098	655	42,540	32.10	18,075.34	32.10	1
7	142.250.196.65	1,305	1,635,945	780	70,590	63.96	641,465.50	38.23	2
8	192.168.1.25	3,653	318,478	3,224	261,370	179.04	124,877.45	158.01	10.
9	192.168.255.255	0	0	318	27,762	0.00	0.00	15.58	1
10	192.168.12.208	1,155	280,770	0	0	56.61	110,091.88	0.00	

Total entries: 1050

ip.addr==192.168.12.92

Observe the applied filter (for **ip.addr == 192.168.12.92**) as shown below**.**



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

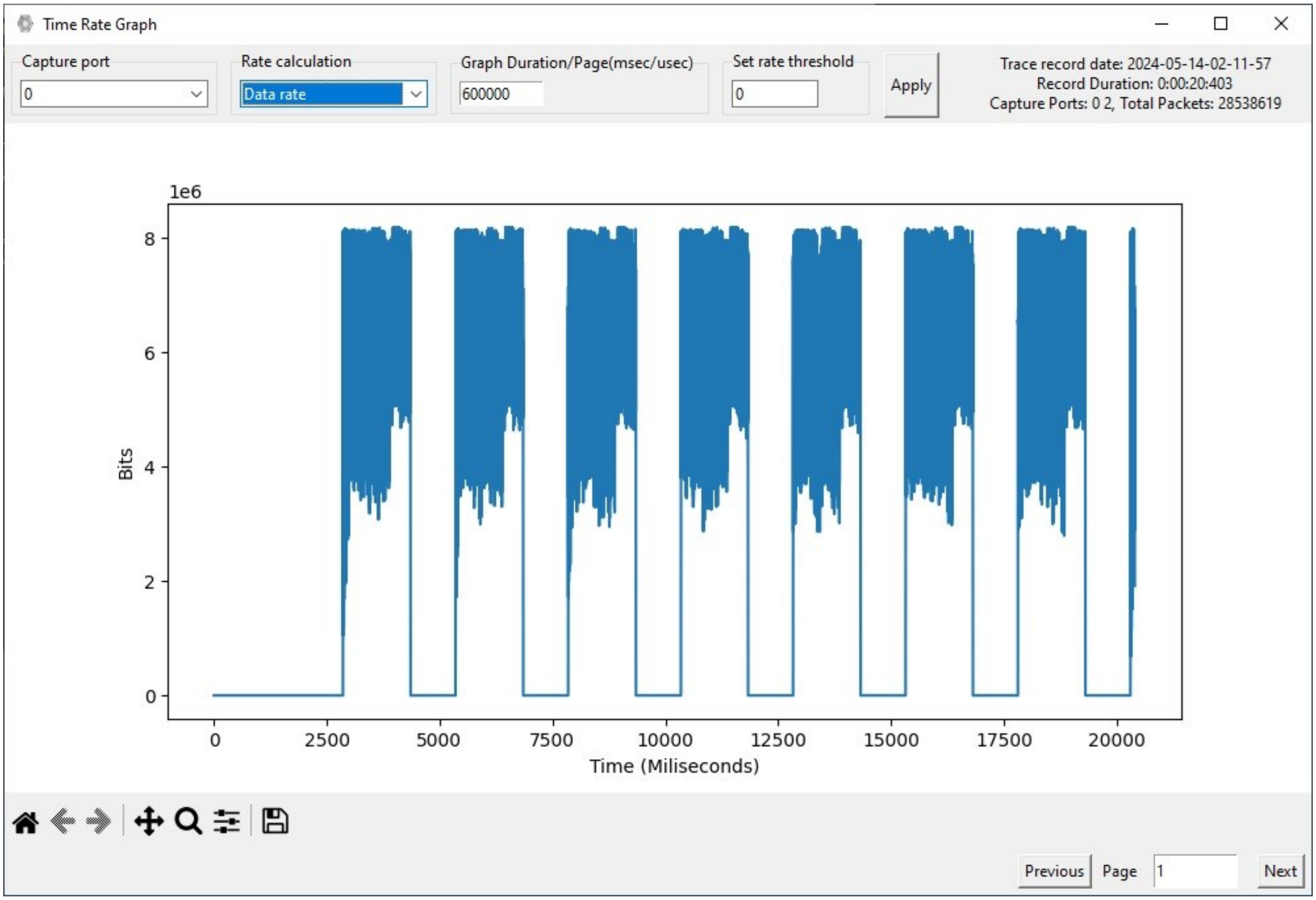
Total entries: 7

ip.addr==192.168.12.92

Rate Analysis

PacketExtractor™, an optional add-on to PacketScan™ HD, now enables users to effortlessly conduct Rate Analysis. Enhanced functionality is achieved through the integration of GL's Time Graph Plotter tool.

- Provides the flexibility to sort columns in Ascending or Descending order for easier data interpretation
- Enhanced to support Milliseconds precision and Microseconds precision in the graph
- Supports both **Packet Rate** and **Data Rate** Graphs
- Rate Analysis graph displays the actual capture time when hovering the mouse over the graph
- Rate Analysis displays “Trace record date”, “Record Duration”, “Capture Ports” and “Total Packets” counts
- “Set Rate Threshold” option which allow users to define a threshold value for displaying a horizontal line across the y-axis



Time Rate Graph

Capture port: 0

Rate calculation: Data rate

Graph Duration/Page(msec/usec): 600000

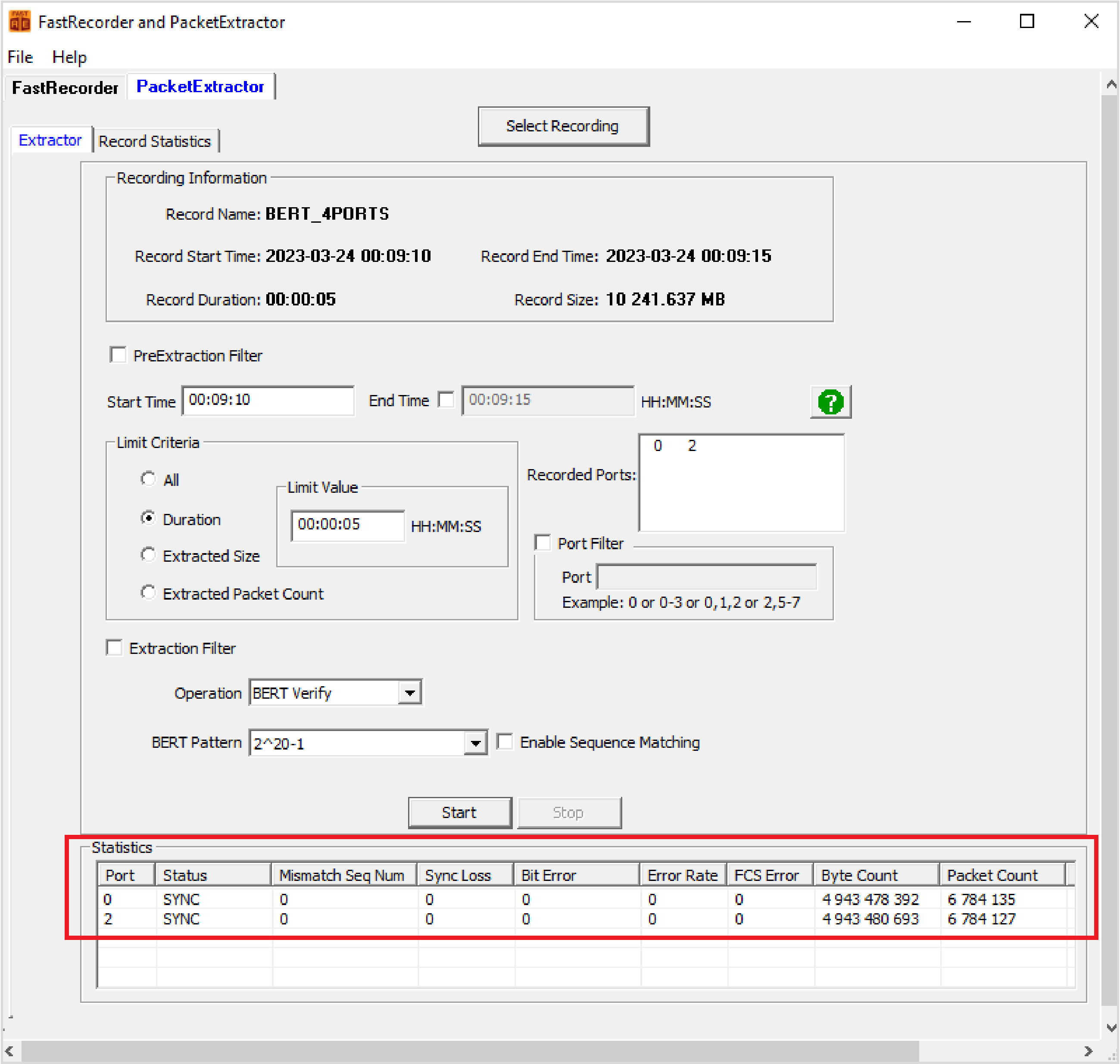
Set rate threshold: 0

Trace record date: 2024-05-14-02-11-57
Record Duration: 0:00:20:403
Capture Ports: 0 2, Total Packets: 28538619

Page: 1

BERT Verification

BERT verification analyzes the received BERT pattern and provides essential measurements, including Port, Status, Mismatch SeqNum, SyncLoss, Bit Error, Error Rate, Byte Count, and more. To verify BERT operation, select the BER Pattern and enable the Sequence Matching option to match packet sequence numbers.



Recording Information

Record Name: BERT_4PORTS

Record Start Time: 2023-03-24 00:09:10

Record End Time: 2023-03-24 00:09:15

Record Duration: 00:00:05

Record Size: 10 241.637 MB

□ PreExtraction Filter

Start Time 00:09:10

End Time □ 00:09:15 HH:MM:SS

Limit Criteria

○ All

● Duration

○ Extracted Size

○ Extracted Packet Count

Limit Value 00:00:05 HH:MM:SS

Recorded Ports: 0 2

□ Port Filter

Port

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

□ Extraction Filter

Operation BERT Verify

BERT Pattern 2^20-1

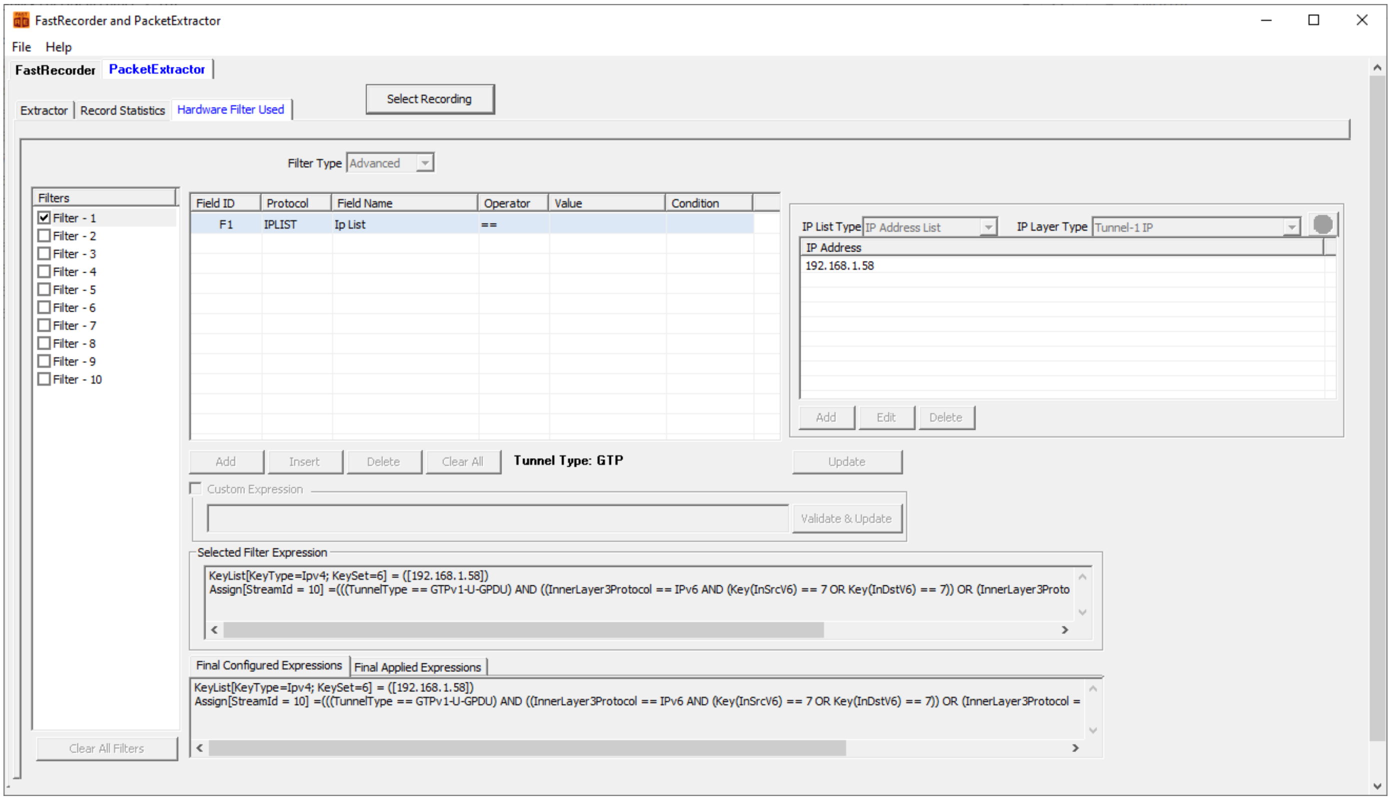
□ Enable Sequence Matching

Statistics

Port	Status	Mismatch Seq Num	Sync Loss	Bit Error	Error Rate	FCS Error	Byte Count	Packet Count
0	SYNC	0	0	0	0	0	4 943 478 392	6 784 135
2	SYNC	0	0	0	0	0	4 943 480 693	6 784 127

Hardware Filter Used while Recording

The Hardware Filter Used tab displays the configured hardware filter for the recorded file.



Filter Type: Advanced

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

IP List Type: IP Address List

IP Layer Type: Tunnel-1 IP

IP Address
192.168.1.58

Tunnel Type: GTP

Selected Filter Expression

```
KeyList[KeyType=Ipv4; KeySet=6] = ([192.168.1.58])
Assign[StreamId = 10] =(((TunnelType == GTPv1-U-GPDU) AND ((InnerLayer3Protocol == IPv6 AND (Key(InSrcV6) == 7 OR Key(InDstV6) == 7)) OR (InnerLayer3Proto
```

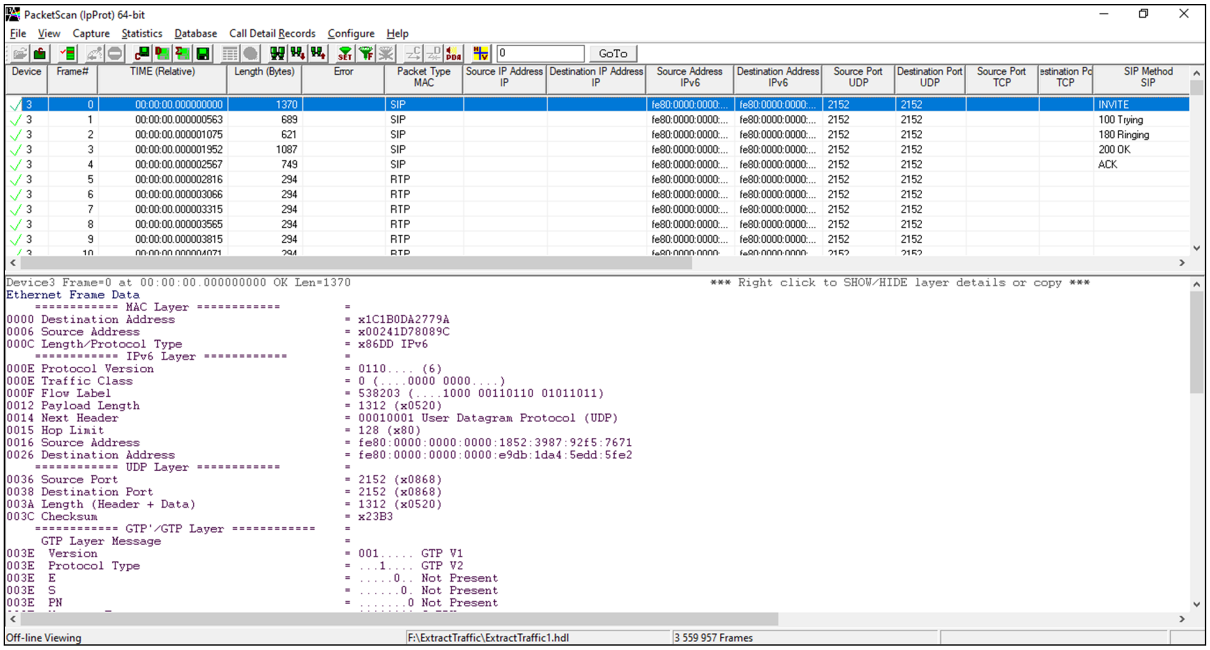
Final Configured Expressions

```
KeyList[KeyType=Ipv4; KeySet=6] = ([192.168.1.58])
Assign[StreamId = 10] =(((TunnelType == GTPv1-U-GPDU) AND ((InnerLayer3Protocol == IPv6 AND (Key(InSrcV6) == 7 OR Key(InDstV6) == 7)) OR (InnerLayer3Protocol =
```

Analysis of Extracted Traffic

The extracted traffic can be analyzed using PacketScan™ and Wireshark® applications.

Traffic Analysis using PacketScan™ Application

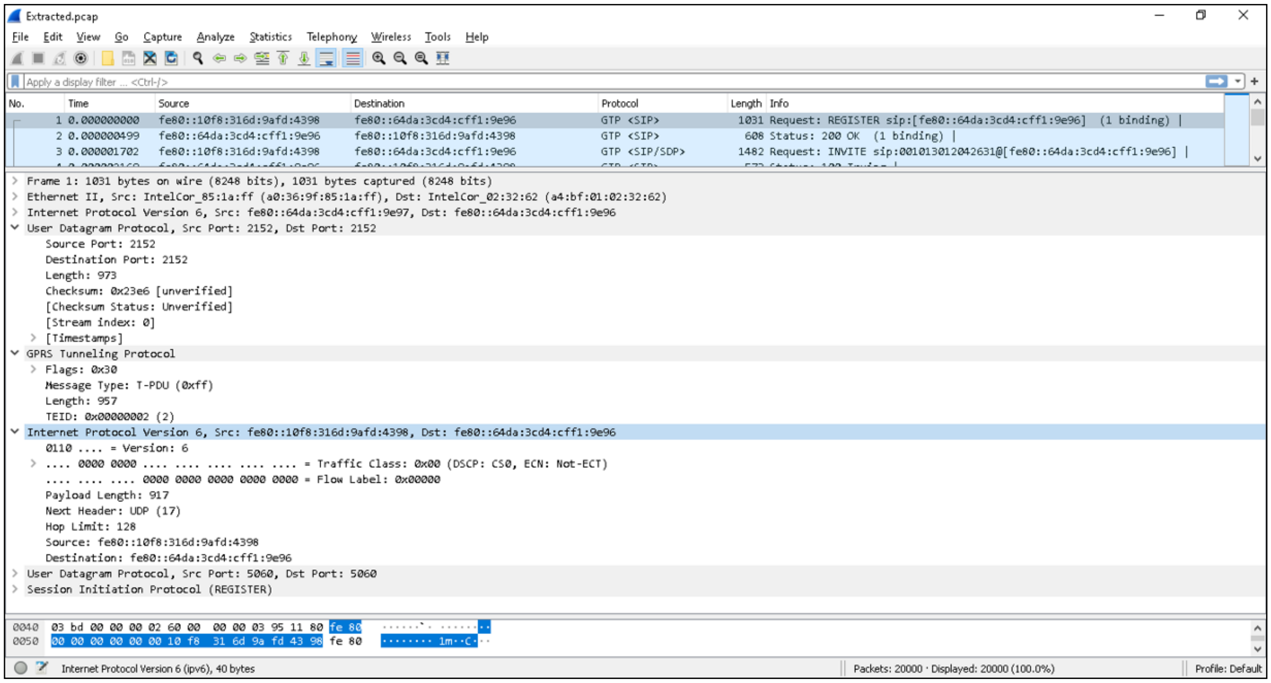

PacketScan (IpProt) 64-bit
File View Capture Statistics Database Call Detail Records Configure Help
0
GoTo

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Packet Type MAC	Source IP Address IP	Destination IP Address IP	Source Address IPv6	Destination Address IPv6	Source Port UDP	Destination Port UDP	Source Port TCP	estination Po TCP	SIP Method SIP
✓ 3	0	00:00:00.000000000	1370		SIP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			INVITE
✓ 3	1	00:00:00.000000563	689		SIP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			100 Trying
✓ 3	2	00:00:00.000001075	621		SIP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			180 Ringing
✓ 3	3	00:00:00.000001952	1087		SIP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			200 OK
✓ 3	4	00:00:00.000002567	749		SIP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			ACK
✓ 3	5	00:00:00.000002816	294		RTP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			
✓ 3	6	00:00:00.000003066	294		RTP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			
✓ 3	7	00:00:00.000003315	294		RTP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			
✓ 3	8	00:00:00.000003565	294		RTP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			
✓ 3	9	00:00:00.000003815	294		RTP			fe80:0000:0000:...	fe80:0000:0000:...	2152	2152			
✓ 3	10	00:00:00.000004071	294		RTP			fe80:0000:0000:	fe80:0000:0000:	2152	2152			

```
Device3 Frame=0 at 00:00:00.000000000 OK Len=1370                    *** Right click to SHOW/HIDE layer details or copy ***
Ethernet Frame Data
    ============ MAC Layer ============          =
0000 Destination Address                         = x1C1B0DA2779A
0006 Source Address                              = x00241D78089C
000C Length/Protocol Type                        = x86DD IPv6
    ============ IPv6 Layer ============         =
000E Protocol Version                            = 0110.... (6)
000E Traffic Class                               = 0 (....0000 0000....)
000F Flow Label                                  = 538203 (....1000 00110110 01011011)
0012 Payload Length                              = 1312 (x0520)
0014 Next Header                                 = 00010001 User Datagram Protocol (UDP)
0015 Hop Limit                                   = 128 (x80)
0016 Source Address                              = fe80:0000:0000:0000:1852:3987:92f5:7671
0026 Destination Address                         = fe80:0000:0000:0000:e9db:1da4:5edd:5fe2
    ============ UDP Layer ============          =
0036 Source Port                                 = 2152 (x0868)
0038 Destination Port                            = 2152 (x0868)
003A Length (Header + Data)                      = 1312 (x0520)
003C Checksum                                    = x23B3
    ============ GTP'/GTP Layer ============     =
     GTP Layer Message                           =
003E  Version                                    = 001..... GTP V1
003E  Protocol Type                              = ...1.... GTP V2
003E  E                                          = .....0.. Not Present
003E  S                                          = ......0. Not Present
003E  PN                                         = .......0 Not Present
```

Off-line Viewing | F:\ExtractTraffic\ExtractTraffic1.hdl | 3 559 957 Frames

Traffic Analysis using Wireshark® application


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

```
No.  Time         Source                       Destination                   Protocol       Length  Info
   1 0.000000000  fe80::10f8:316d:9afd:4398    fe80::64da:3cd4:cff1:9e96     GTP <SIP>        1031  Request: REGISTER sip:[fe80::64da:3cd4:cff1:9e96]  (1 binding) |
   2 0.000000499  fe80::64da:3cd4:cff1:9e96    fe80::10f8:316d:9afd:4398     GTP <SIP>         608  Status: 200 OK  (1 binding) |
   3 0.000001702  fe80::10f8:316d:9afd:4398    fe80::64da:3cd4:cff1:9e96     GTP <SIP/SDP>    1482  Request: INVITE sip:001013012042631@[fe80::64da:3cd4:cff1:9e96] |
```

```
> Frame 1: 1031 bytes on wire (8248 bits), 1031 bytes captured (8248 bits)
> 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
v User Datagram Protocol, Src Port: 2152, Dst Port: 2152
    Source Port: 2152
    Destination Port: 2152
    Length: 973
    Checksum: 0x23e6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v GPRS Tunneling Protocol
  > Flags: 0x30
    Message Type: T-PDU (0xff)
    Length: 957
    TEID: 0x00000002 (2)
v Internet Protocol Version 6, Src: fe80::10f8:316d:9afd:4398, Dst: fe80::64da:3cd4:cff1:9e96
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 917
    Next Header: UDP (17)
    Hop Limit: 128
    Source: fe80::10f8:316d:9afd:4398
    Destination: fe80::64da:3cd4:cff1:9e96
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (REGISTER)

0040  03 bd 00 00 00 02 60 00  00 00 03 95 11 80 fe 80   ······`· ········
0050  00 00 00 00 00 00 10 f8  31 6d 9a fd 43 98 fe 80   ········ 1m··C···
```

Internet Protocol Version 6 (ipv6), 40 bytes | Packets: 20000 · Displayed: 20000 (100.0%) | Profile: Default

GL Communications Inc.

Buyer’s Guide

Item No	Product Description
PKV123	FastRecorder™ and PacketExtractor™ for Monitoring IP Networks (requires any one of PKV120, PKV120p, PKV122, PKV122p, PKV124, PKV124p) PacketRecorder™ and PacketReplay™ (requires any one of PKV120, PKV120p, PKV122, PKV122p)

Item No	Related Software and Hardware
PKV410	IP Analytics™ - Optional with FastRecorder™ and PacketExtractor™ (Gain extensive network intelligence with detailed information on endpoints and conversations for IP, UDP, TCP, and SCTP protocols. Requires PKV123)
PKV122	PacketScan™ HD – High Density IP Traffic Analyzer w/ 2x10GigE
PKV124	PacketScan™ HD – High Density IP Traffic Analyzer w/ 2x40/100GigE
PKV100	PacketScan™ (Real-time and Offline)
PKV101	PacketScan™ - Offline
PKV170	NetSurveyorWeb™

Note: PCs which include GL hardware/software require Intel or AMD processors for compliance.

For more details, refer to High Speed Ethernet and IP Capture webpage.