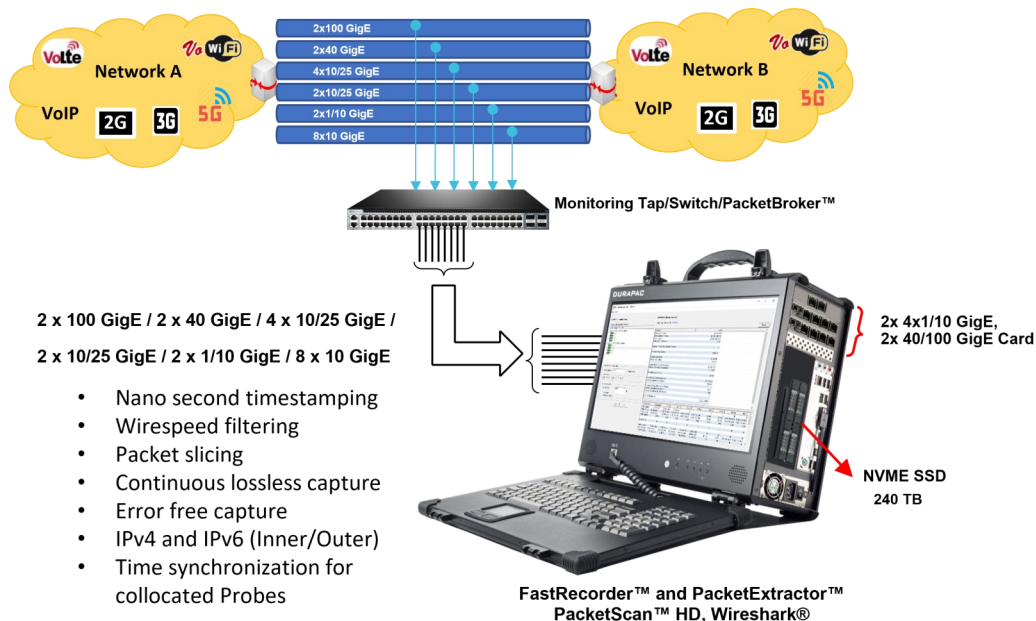


# High Speed Ethernet and IP Capture (FastRecorder™ and PacketExtractor™)



## 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.

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.



818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878, U.S.A  
(Web) [www.gl.com](http://www.gl.com) - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) [info@gl.com](mailto: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 120 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

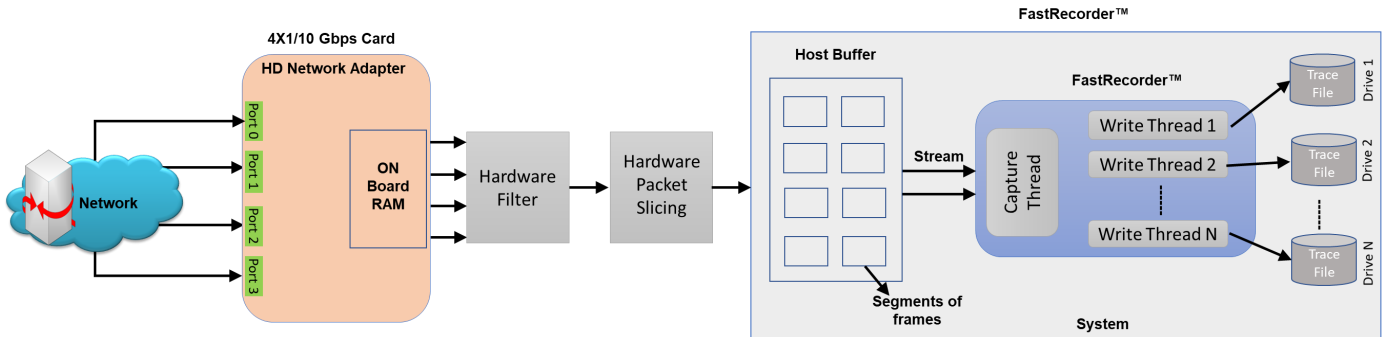
<p><b>Hardware Requirements</b></p>	<p><b>Requires GL's HD Network Interface adapters</b></p> <ul style="list-style-type: none"> <li>• High Density Network Adapters can be any of the following types – <ul style="list-style-type: none"> <li>– <b>4 x 1/10 Gbps</b> – requires 10GBASE-SR SFP+; Optical only</li> <li>– <b>2 x 40/100 Gbps</b> – requires MTP/MPO Connector for CFP2; Optical only</li> </ul> </li> <li>• <b>Hard Disk:</b> SSD hard disk (For faster I/O operations) compatible with SATA verIII or RAM Disk</li> <li>• <b>System Configuration:</b> 2U system with 32 GB to 128 GB RAM</li> </ul>
<p><b>Hardware Filters</b></p>	<ul style="list-style-type: none"> <li>• Supports defining up to 10 filters at Layer 2, 3, 4, and 5 <ul style="list-style-type: none"> <li>– <b>MAC:</b> Frames can be filtered out based on Ether Type and FCS Error</li> <li>– <b>VLAN 0, 1, 2:</b> Filters frames based on Tag protocol ID, User Priority, CFI, and VLAN ID</li> <li>– <b>IPv4:</b> 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</li> <li>– <b>IPv6:</b> Frames can be filtered based on Source IP address, Destination IP address, Next Header, and Payload Length</li> <li>– <b>Tunnel Traffic:</b> 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</li> <li>– <b>ARP:</b> Frames can be filtered based on Sender MAC Address, Target MAC Address, Sender IP Address, Target IP Address and Option Code</li> <li>– <b>TCP:</b> In TCP layer Frames, can be filtered based on source port, destination port and check sum error</li> <li>– <b>UDP:</b> In UDP layer Frames can be filtered based on source port, destination port, check sum error, UDP length and payload</li> <li>– <b>SCTP:</b> SCTP packets can also be filtered based on source port or destination port</li> <li>– <b>SIP and RTP:</b> SIP and RTP packets can also be filtered based on source port or destination port</li> </ul> </li> </ul>
<p><b>Record Rate</b></p>	<ul style="list-style-type: none"> <li>• Max Rate is 320 Gbps</li> </ul>

## 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.



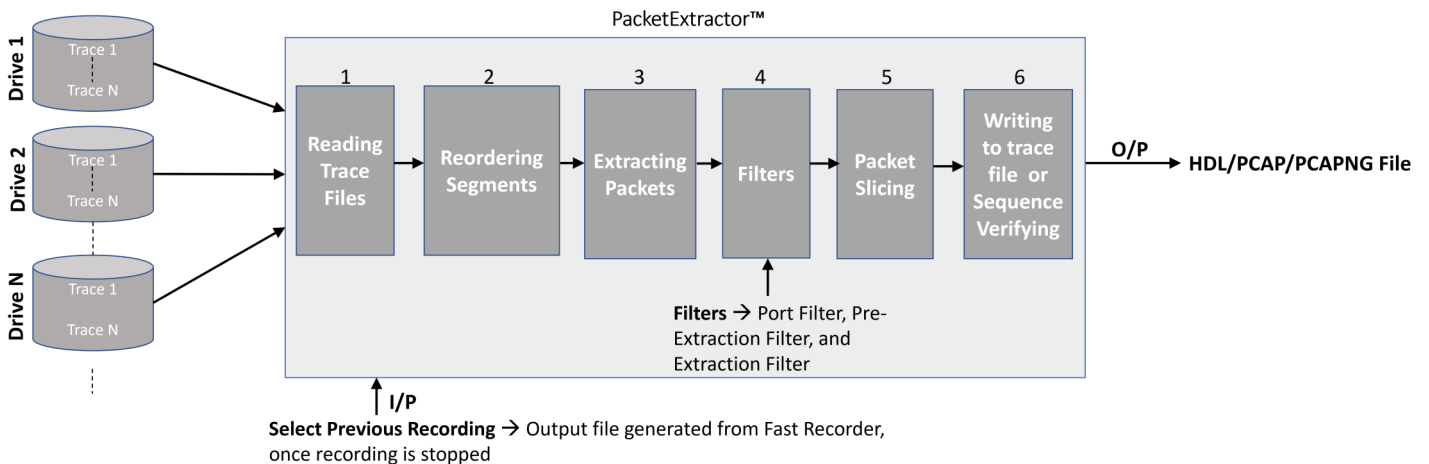
### PacketExtractor™

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.

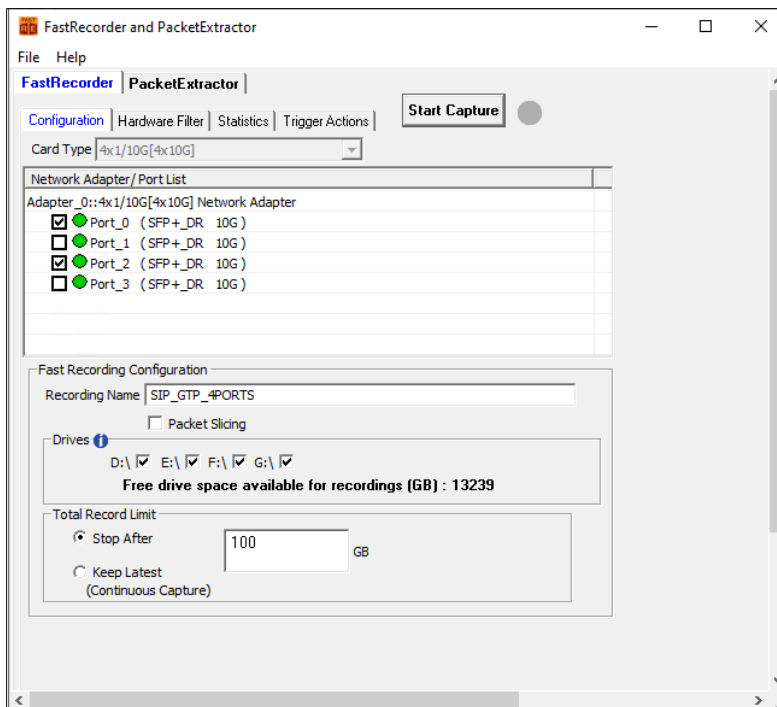
**Extractor Module:** The Extractor module then extracts packets from the reassembled segments.

**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.



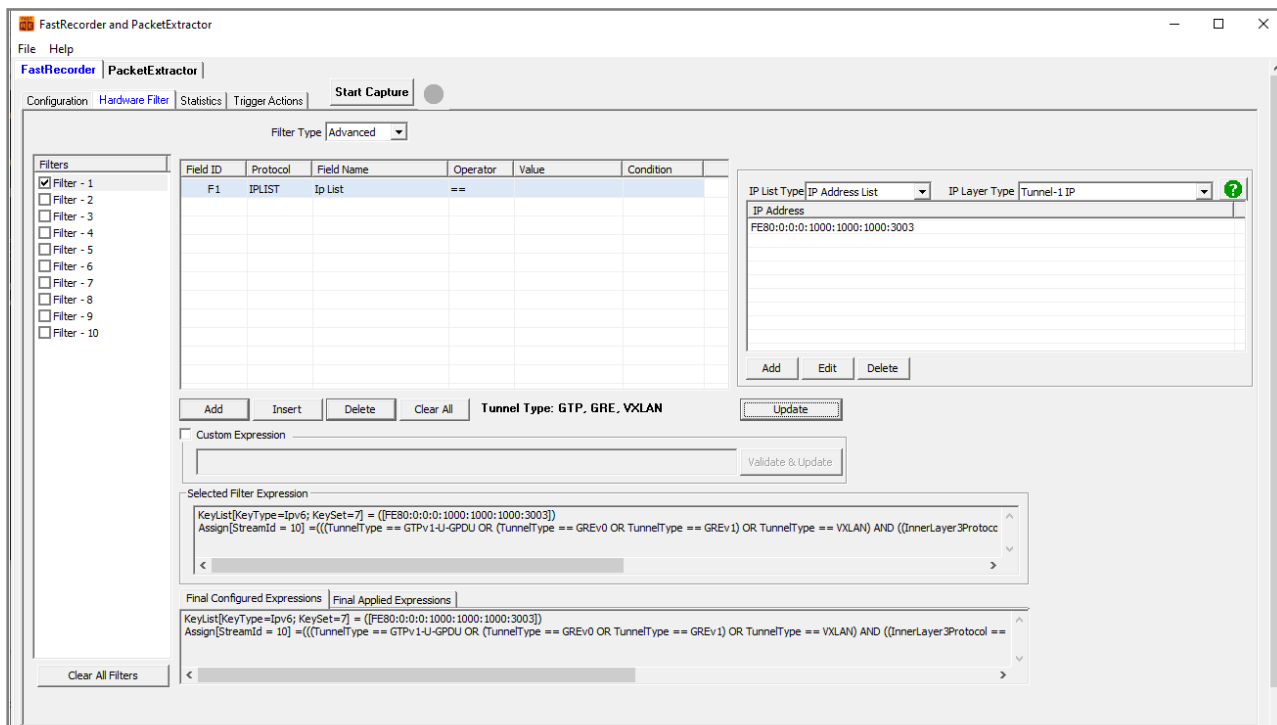
## FastRecorder™

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.



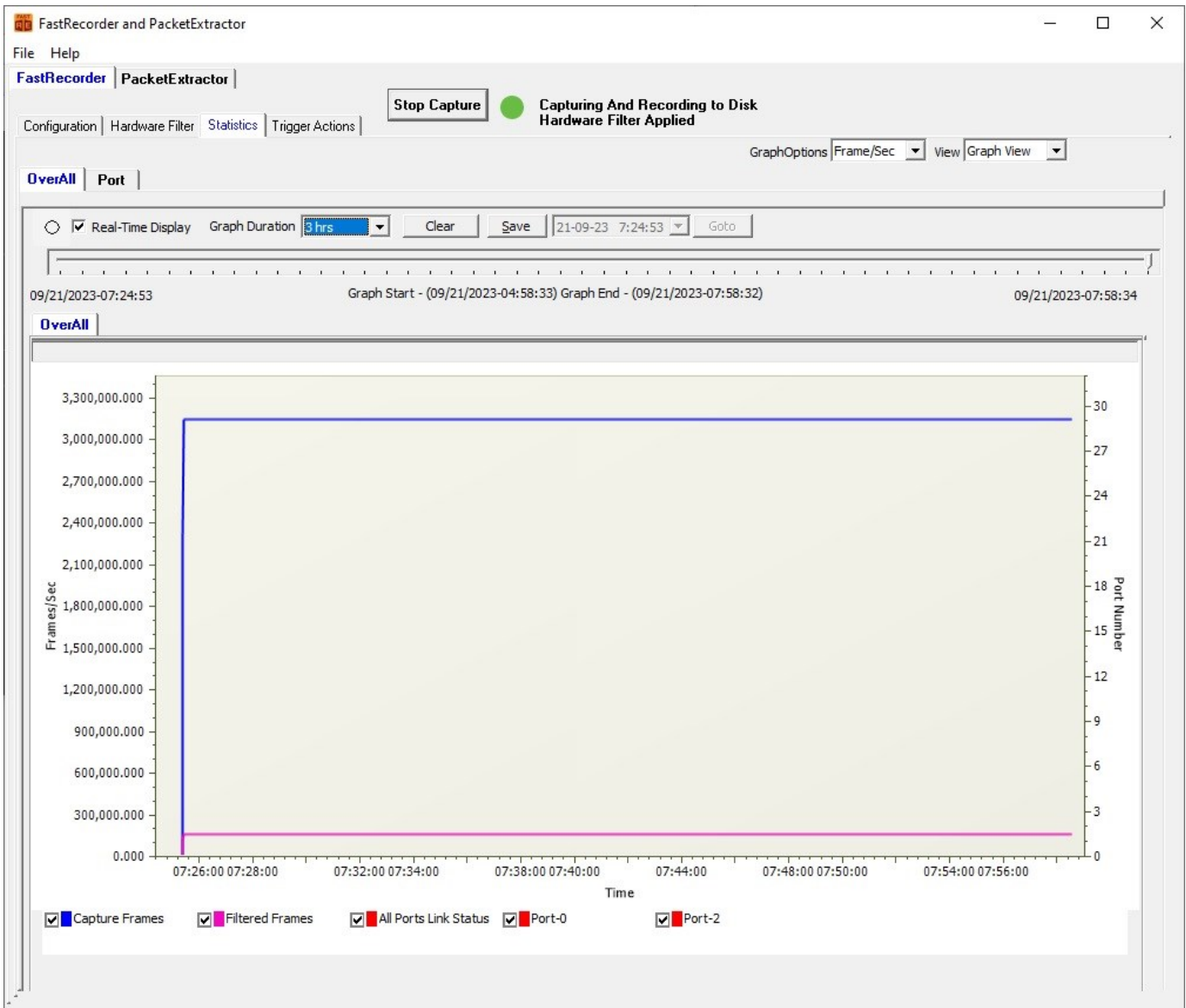
## Hardware Filters

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.



## 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™ 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

**Statistics**

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

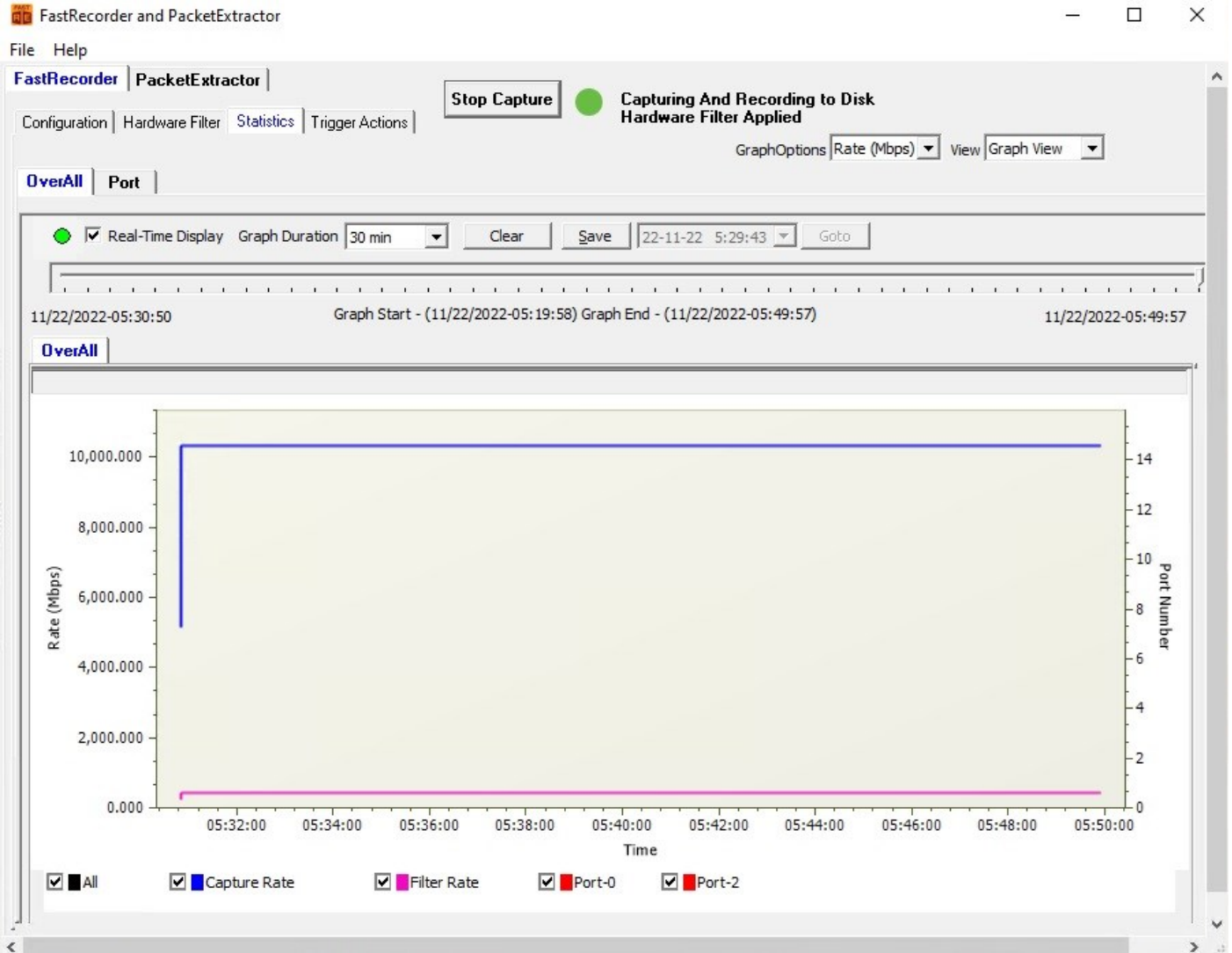
  

**Port Statistics**

	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 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	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.





## 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)

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'Trigger Actions' tab is active, showing a table of configured triggers. The status bar indicates 'Capturing And Waiting for Trigger'. Below the table are buttons for 'Add', 'Delete', 'Clear', and 'Deactivate'. At the bottom, a 'Triggered Events' list shows recent actions and their corresponding conditions.

	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

Initial Actions: Capture and Record

Buttons: Add, Delete, Clear, Deactivate

Triggered Events:

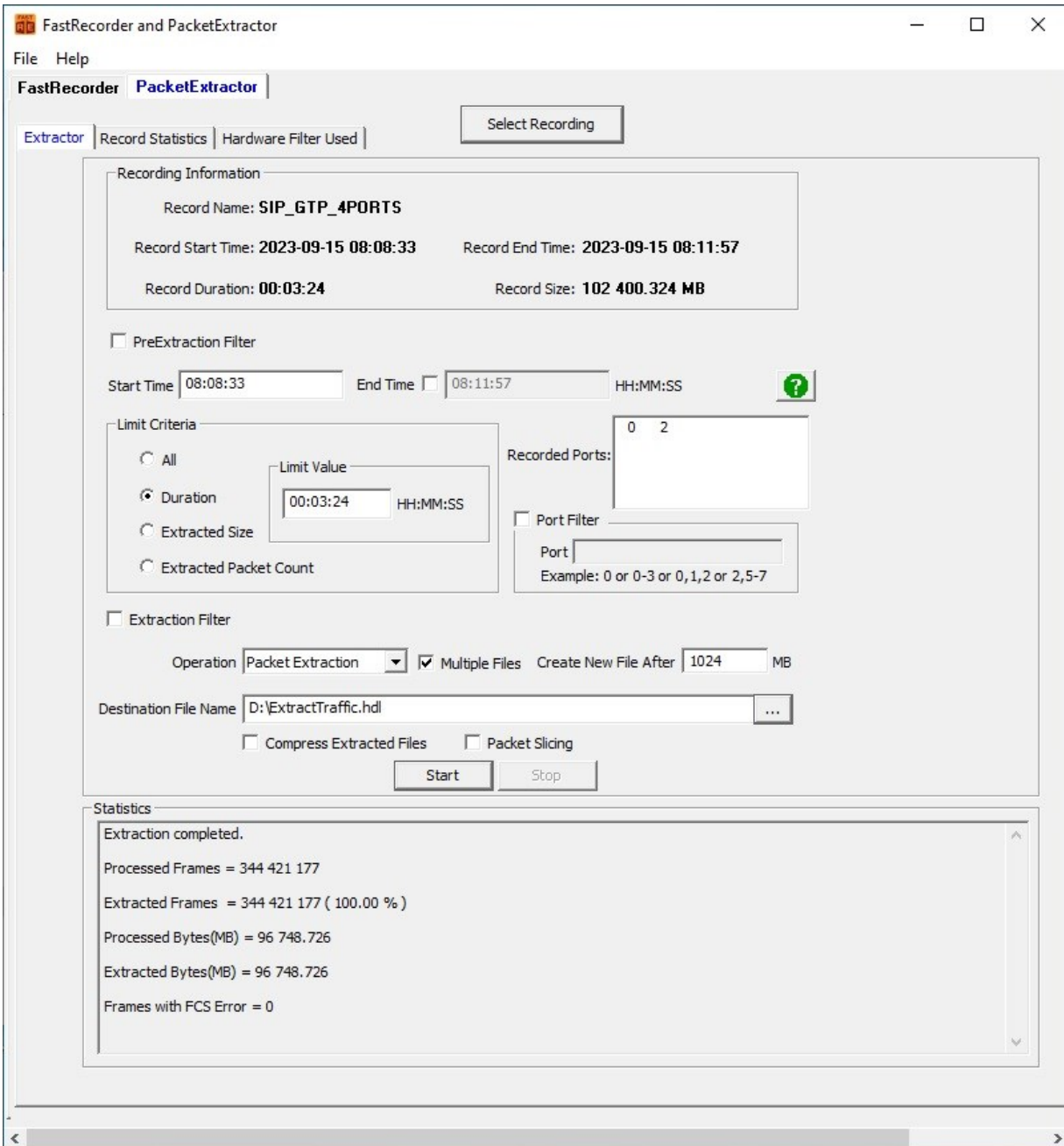
- 12-7 12:49:33 Action=>"Stop Disk Write" Condition=>"Port[3].CaptureRate>1500.00"
- 12-7 12:49:9 Action=>"Start Disk Write" Condition=>"Port[2].LinkState == "Up"
- 12-7 12:49:9 Action=>"Start Disk Write" Condition=>"CaptureRate > 1500.00"

## 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

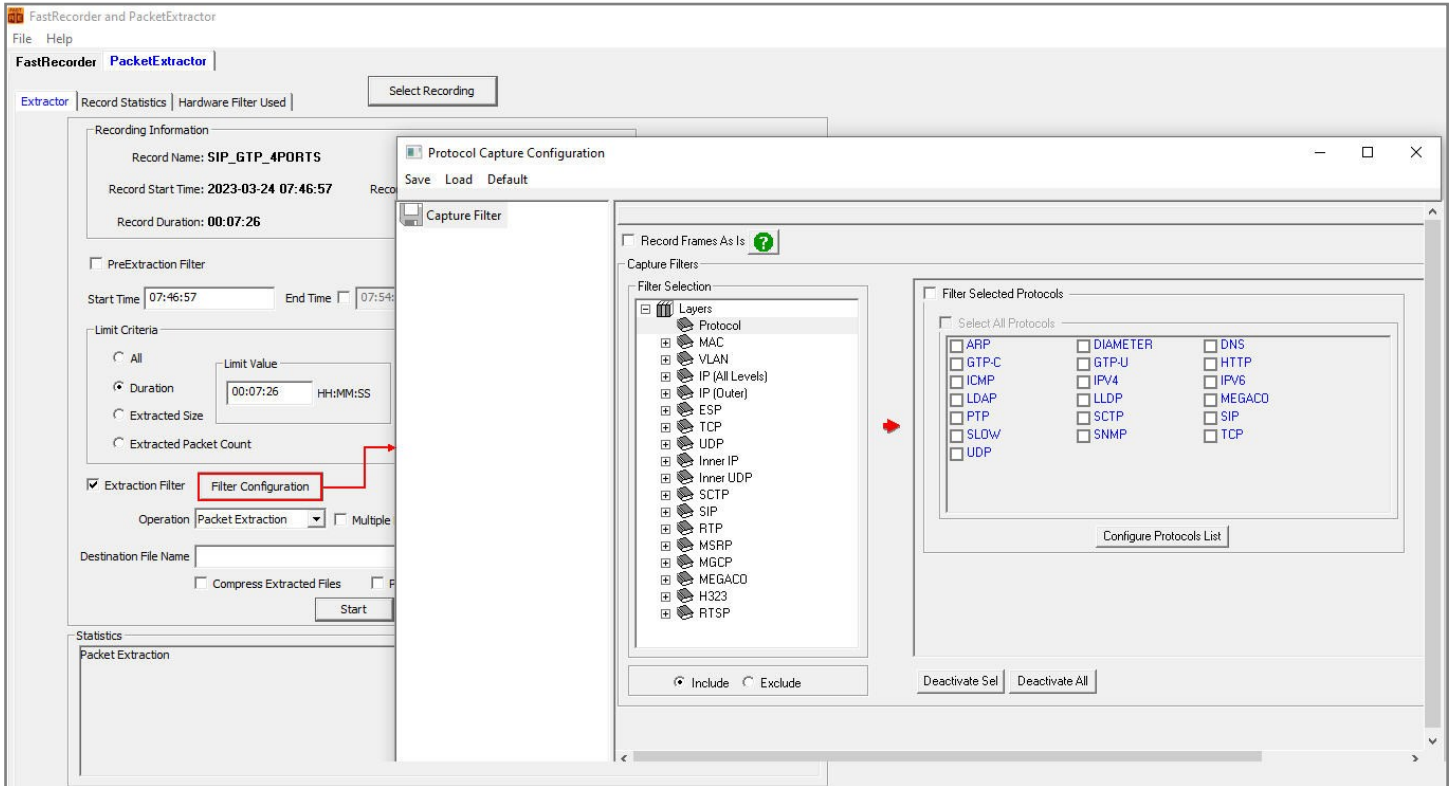
When extracting packets from a recorded file without using a filter, select the file, specify the default record start time, uncheck the Extractor Filter option, choose the desired path to save the extracted data to a file, and view the extracted statistics under the **Statistics** section.



## 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 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)

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'Record Statistics' tab is active, displaying a table of overall statistics. Below this, a 'Port Statistics' table provides a breakdown of data for three ports: Aggregate, Port-0, and Port-2. The 'Recorded Bytes (Gbytes)' row is highlighted in blue.

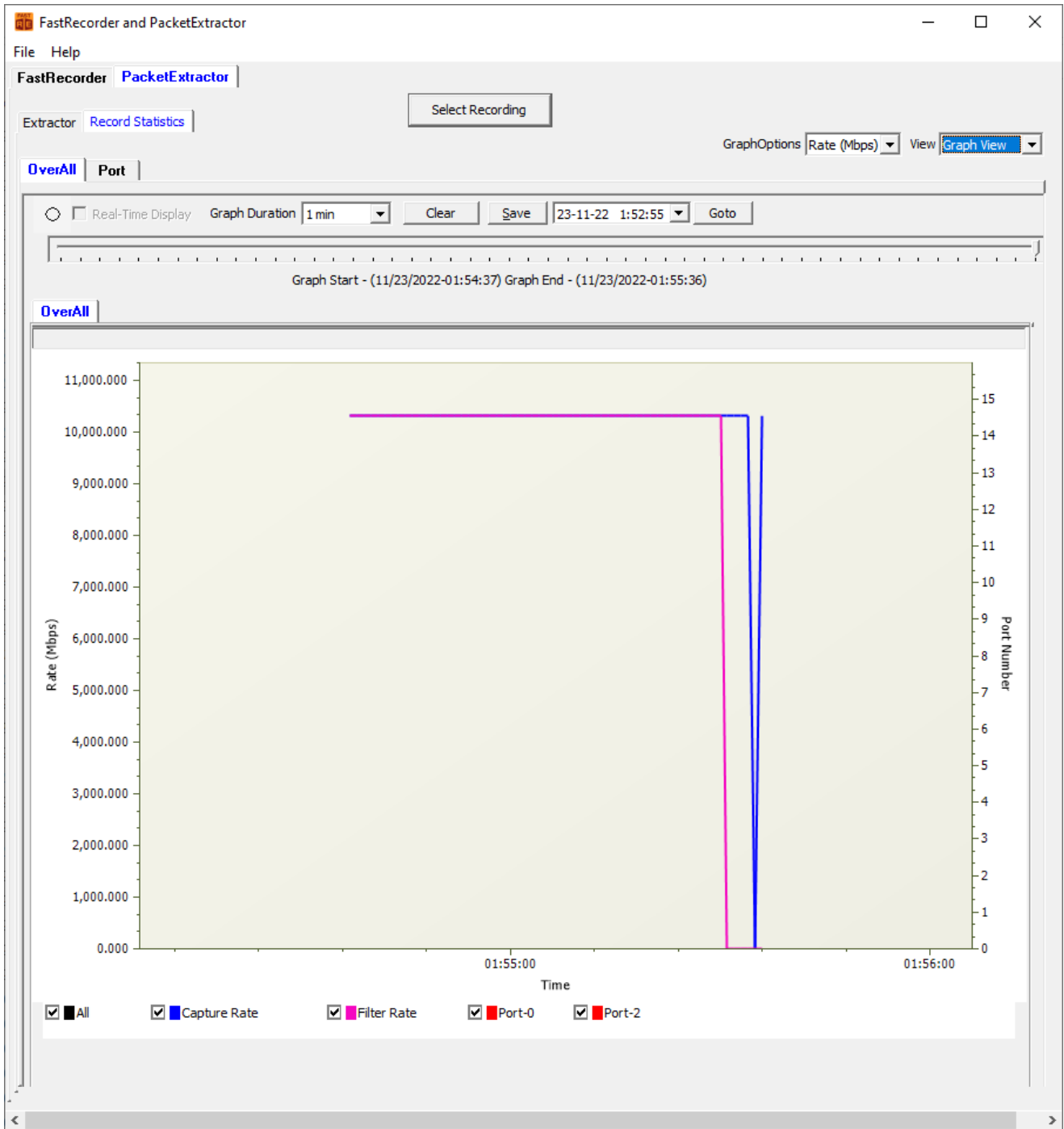
Statistics	Value
Filter Match Frames	347 467 772
Filter Not Match Frames	0
Total Frames	347 467 772
Filter Match Frames %	100.00
Dropped Frames (Due to Buffer Overflow)	0
<b>Recorded Bytes (Gbytes)</b>	<b>100.0000</b>
Record Duration (hr:min:sec)	00:00:51

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.



## 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.

The screenshot displays two windows from a network analysis tool. The top window, 'Protocol Capture Configuration', has the 'ESP' layer selected in the 'Filter Selection' pane. In the 'Filters' pane, 'Deciphered Payload' is selected under the 'Extract' section. The bottom window, 'ESP SAs', contains a table with the following data:

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

The screenshot displays the FastRecorder and PacketExtractor software interface. The main window shows recording information for a record named "eCPRI-Analysis" with a duration of 00:00:53 and a size of 0.188 MB. The recording started at 2022-12-19 04:07:36 and ended at 2022-12-19 04:08:29. The interface includes a "PreExtraction Filter" section with a "Limit Criteria" dropdown set to "Duration" and a "Limit Value" of 00:00:53. The "Operation" dropdown is set to "eCPRI Analysis". A secondary window titled "eCPRI Analysis - Sequence Analysis" is open, showing a table of message statistics for the link 192.168.1.55:64000<-->192.168.1.57:64000. The table includes columns for Message Type, Total Packets, Missed Packets, Out Of Order Packets, and Duplicate Packets. The total processed packets are 200, and the total eCPRI packets are also 200.

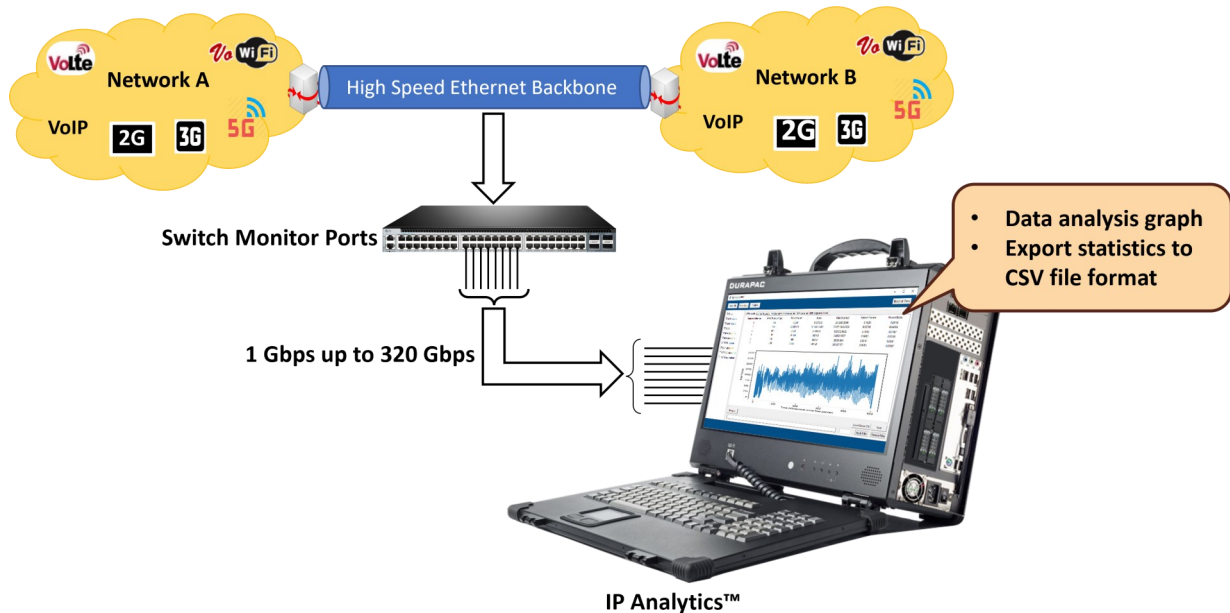
Message Type	Total Packets	Missed Packets	Out Of Order Packets	Duplicate Packets
IQ Data	0	0	0	0
Bit Sequence	40	2	6	19
Data Transfer	36	2	7	15
Total	76	4	13	34

## IP Analytics™

IP Analytics™ 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, COS, Layer 4, IPv4 Endpoints, IPv6 Endpoints, UDP Endpoints, TCP Endpoints, UDP Conversation, and TCP Conversation.

## 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 Tool.



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, IPv6 Endpoints, UDP Endpoints, TCP Endpoints, UDP Conversation, TCP Conversation, and Ports. It is an easy-to-use solution for data exploration.

GL IP-ANALYTICS														
Select file   Select folder   Analyze   Export all Tabs														
<input checked="" type="checkbox"/> Ports <input checked="" type="checkbox"/> L3 Protocols <input checked="" type="checkbox"/> L4 Protocols <input checked="" type="checkbox"/> COS <input checked="" type="checkbox"/> IPv4 Endpoints <input checked="" type="checkbox"/> IPv6 Endpoints <input checked="" type="checkbox"/> TCP Endpoints <input checked="" type="checkbox"/> UDP Endpoints <input checked="" type="checkbox"/> UDP Conversations <input checked="" type="checkbox"/> 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/sec	Avg Tx Bits/sec	Avg Rx Packets/sec	Avg Rx Bits/sec	Total Packets				
1	13.107.136.10	938 149	1 387 375 523	364 178	21 911 840	9118.07508	107873646.3342	3539.52554	1703727.67827	1 302 327				
2	192.168.1.60	205 214	307 443 647	27 005	2 081 794	1994.5197	2390495.75055	262.46749	161867.28537	232 219				
3	192.168.12.201	72 319	102 095 904	32 458	2 047 159	702.88416	7938339.15741	315.46639	159174.28432	104 777				
4	192.168.30.76	32 444	45 912 932	16 127	1 021 489	315.33932	3569902.52936	156.74184	78424.59795	48 571				
5	192.168.30.243	28 851	39 872 852	14 207	920 862	280.40917	3100263.67316	138.08094	71600.47158	43 058				
6	192.168.12.93	364 193	21 911 457	938 153	1 387 376 089	3539.67133	1703697.88959	9118.11395	107873690.34282	1 302 346				
7	192.168.12.91	8 146	2 753 285	11 661	6 564 947	78.17275	214078.22714	113.35581	510441.45711	19 807				
8	52.98.88.242	2 382	2 516 750	1 113	511 394	23.15110	195686.74444	10.81749	39762.0225	3 495				
9	192.168.12.12	27 919	2 431 063	206 125	307 645 902	271.35086	189024.25906	2003.3739	2392662.83478	234 044				
10	192.168.10.24	32 359	2 038 270	72 228	102 088 058	314.50419	158483.13126	701.99971	7937725.10151	104 587				
11	192.168.1.3	5 702	1 135 296	5 588	1 994 607	55.41898	88273.51871	56.93510	155088.16937	11 560				
12	192.168.30.56	3 925	827 444	2 701	308 187	38.14793	64336.87198	26.25161	23962.69423	6 626				
13	192.168.30.17	1 826	788 088	1 975	190 274	18.71921	61276.79549	19.19546	14794.51658	3 901				
14	192.168.12.5	3 794	758 364	3 847	1 249 622	36.77752	50965.6431	37.38983	97162.79367	7 631				
15	192.168.13.144	10 628	666 379	22 185	31 416 889	103.29585	51813.46462	215.62086	2442765.30903	32 813				
16	192.168.12.219	1 855	640 753	1 821	476 165	18.02915	49820.94708	17.6987	37023.61326	3 676				
17	192.168.13.139	10 061	630 644	21 067	29 806 340	97.78506	49034.93444	204.75478	2317554.63923	31 128				
18	216.58.200.142	679	613 279	399	208 805	6.59935	47694.74062	3.87797	16235.37128	1 078				
19	142.250.195.165	641	522 452	337	153 983	6.23002	40622.60098	3.27538	11872.75533	978				
20	192.168.1.147	2 628	442 556	1 847	495 565	25.54211	34488.1413	17.9514	88532.03596	4 475				
21	192.168.12.28	1 168	415 526	1 076	244 902	11.35203	32308.70375	10.45788	19042.04831	2 244				
22	192.168.12.218	1 184	401 847	1 157	297 647	11.50755	31245.11024	11.24514	23143.16973	2 341				
23	13.200.41.128	708	363 018	612	459 843	6.88121	28226.00997	5.94816	35754.51659	1 320				



## Key Features

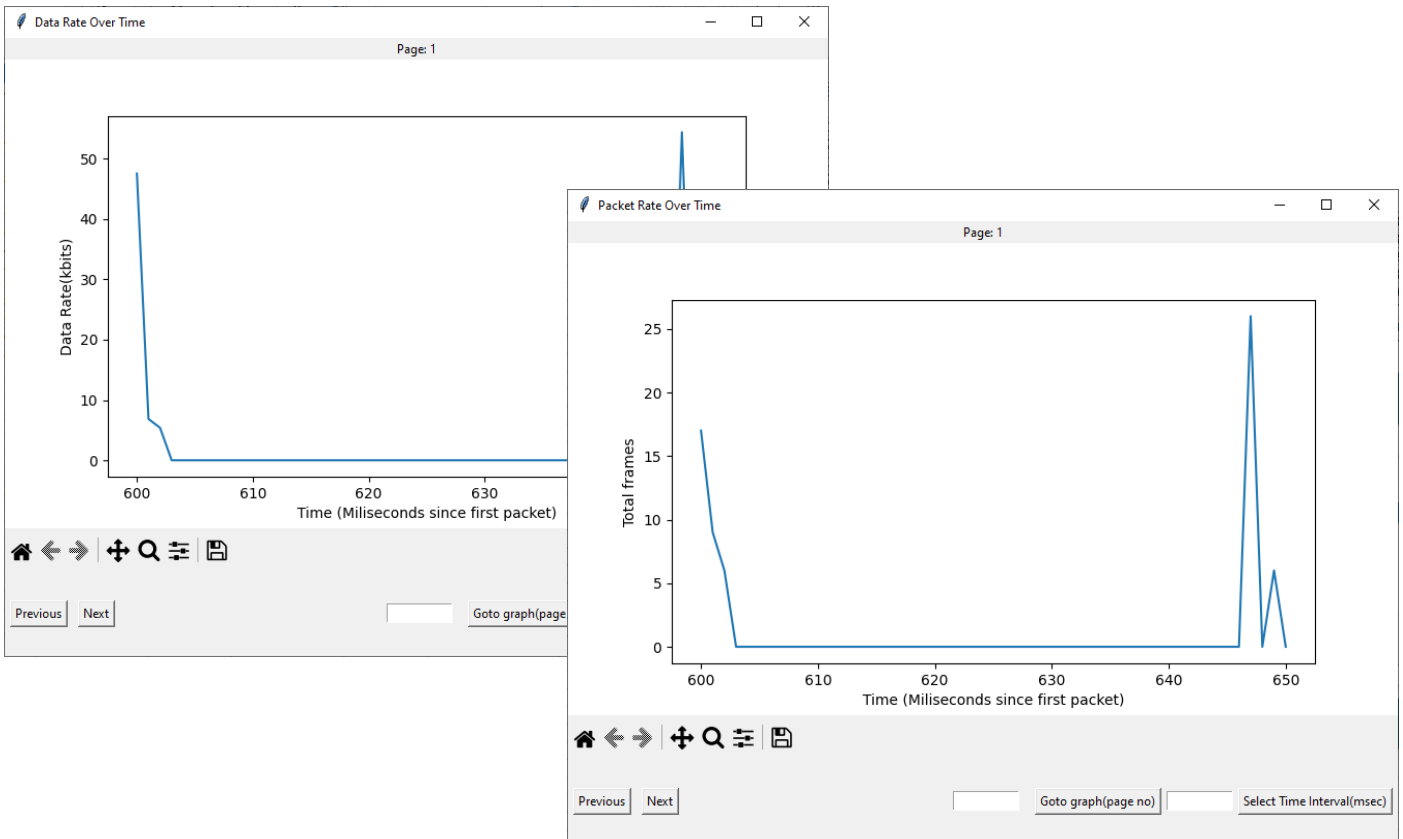
- Includes detailed analysis of different IP layers such as Layer 3 Protocols, Class of Services (DSCP), Layer 4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, Recorded Port statistics, UDP Conversations and TCP Conversations along with Port wise details
- Provides in-depth 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 observe the IO graphs for **Data Rate Over Time** and **Packet Rate Over Time**.

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports			
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	1 117 334	208	21 824	11.91266	30661.9397	8.15077	6841.63026	512
3	91.189.91.49	600	1 117 334	924	74 190	23.51183	21057.19869	36.20822	23257.90637	1 524
4	202.83.26.121	1 970	1 117 334	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

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\_address == 67.219.144.68**.

The screenshot shows the GL IP-ANALYTICS application window. On the left, there is a sidebar with a list of categories and their sub-items, all of which are checked: Ports, L3 Protocols, L4 Protocols, COS, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, and UDP Endpoints. The main area displays a table with columns: L3 Protocols, COS, L4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, Ports, 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, and Total Packets. The table contains 10 rows of data. At the bottom, there is a filter input field containing the text 'ip\_address == 67.219.144.68', a dropdown menu set to 'cos', and buttons for 'Apply Filter' and 'Remove Filter'. A 'Processing...' indicator with a green progress bar is visible at the bottom right.

L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	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
								7	142.250.196.65	1 392	1 739 440	832	71 968	54.54746	545298.99794	32.60308	22561.3291	2 224
								8	192.168.1.25	3 712	308 676	3 270	251 898	145.45988	96767.1857	128.1395	78967.78675	6 982
								9	192.168.255.255	0	0	318	26 490	0	0	12.46127	8304.37983	318
								10	192.168.12.208	1 202	283 716	0	0	47.10204	88942.44728	0	0	1 202

Observe the applied filter (for **ip\_address == 67.219.144.68**) as shown below.

This screenshot shows the same GL IP-ANALYTICS application window after the filter has been applied. The sidebar remains the same. The main table now only displays one row of data, which is highlighted with a red border. The filter input field at the bottom still contains 'ip\_address == 67.219.144.68'.

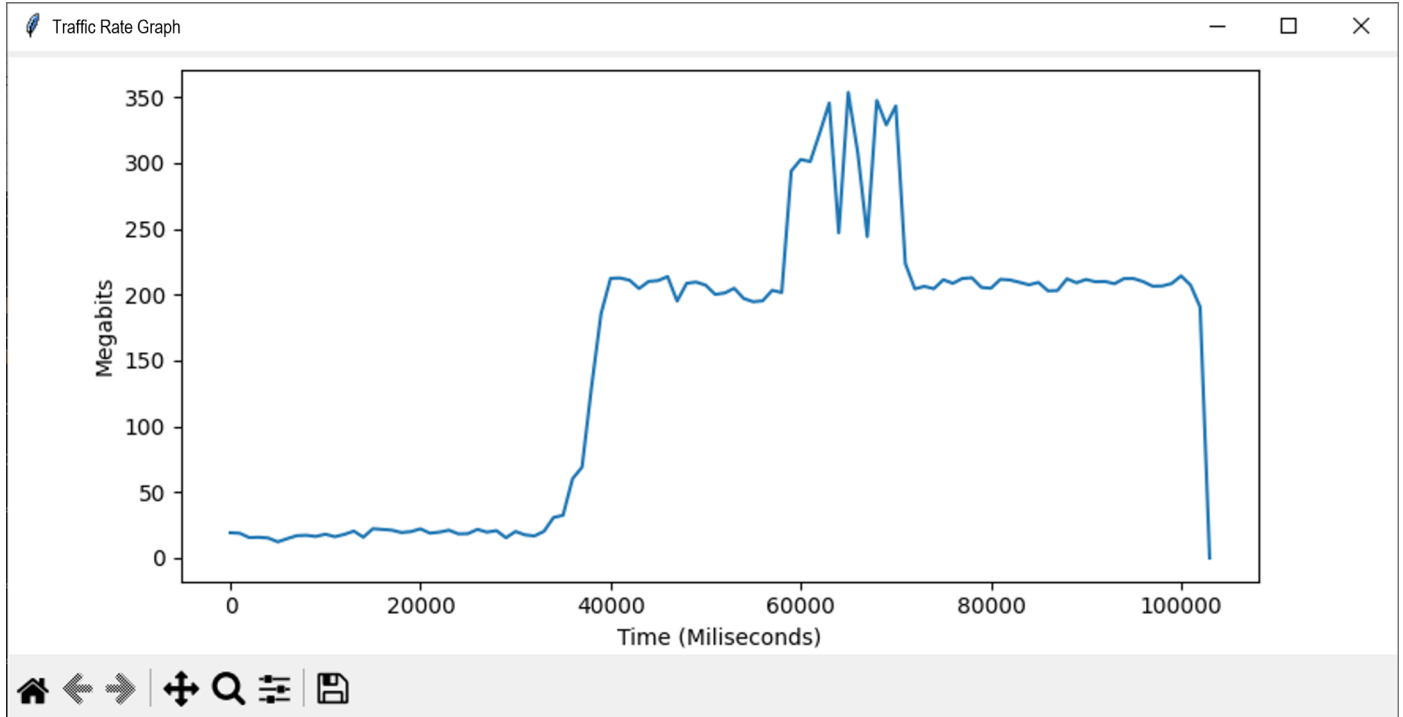
L3 Protocols	COS	L4 Protocols	IPv4 Endpoints	IPv6 Endpoints	TCP Endpoints	UDP Endpoints	Ports	Sequence Number	IP Address	Tx Packet Count	Tx Bytes	Rx Packet Count	Rx Bytes	Avg Tx Packets/s	Avg Tx Bits/sec	Avg Rx Packets/s	Avg Rx Bits/sec
								1	67.219.144.68	80	12 032	80	6 896	3.38821	4076.69053	3.38821	2336.50747

## 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.

GL's Time Graph Plotter analyzes HDF5 files and generates graphs for **Packets/Sec**, **Megabits/Sec**, **Kilobits/Sec**, and **Bits/Sec** options, for individual recorded ports.

The below 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.



## 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.

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, and the 'Extractor' sub-tab is selected. The 'Record Statistics' section is visible, showing recording information for a record named 'BERT\_4PORTS'.

**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:**  (unchecked)

Start Time: 00:09:10 End Time:  00:09:15 HH:MM:SS

**Limit Criteria:**

- All
- Duration (Limit Value: 00:00:05 HH:MM:SS)
- Extracted Size
- Extracted Packet Count

**Recorded Ports:** 0 2

**Port Filter:**  (unchecked)

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

**Extraction Filter:**  (unchecked)

Operation: BERT Verify

BERT Pattern: 2^20-1  Enable Sequence Matching

**Start** **Stop**

**Statistics Table:**

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.

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'Hardware Filter Used' tab is active, displaying a table of filter rules and a configuration panel for the selected filter.

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

The configuration panel for the selected filter (F1) shows:

- IP List Type: IP Address List
- IP Layer Type: Tunnel-1 IP
- IP Address: 192.168.1.58

Buttons for 'Add', 'Edit', and 'Delete' are visible below the IP address list. Below the configuration panel, there are sections for 'Custom Expression', 'Selected Filter Expression', and 'Final Configured Expressions / Final Applied Expressions'.

## Analysis of Extracted Traffic

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

### Traffic Analysis using PacketScan™ Application

The screenshot shows the PacketScan (IpProt) 64-bit application interface. The top section displays a list of captured frames with columns for Device, Frame#, TIME (Relative), Length (Bytes), Error, Packet Type, MAC, Source IP Address, Destination IP Address, Source Address IPv6, Destination Address IPv6, Source Port UDP, Destination Port UDP, Source Port TCP, Destination Port TCP, and SIP Method SIP. The selected frame (Frame 0) is an INVITE message.

The bottom section shows the detailed protocol analysis for the selected frame:

```

Device3 Frame=0 at 00:00:00.000000000 OK Len=1370
Ethernet Frame Data
----- MAC Layer -----
0000 Destination Address      = x1C1E0DA2779A
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
    
```

### Traffic Analysis using Wireshark® application

The screenshot shows the Wireshark application interface. The top section displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. The selected packet is a GTP (SIP) packet.

The bottom section shows the detailed view of the selected packet:

```

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:cff1:9e96, Dst: fe80::64da:3cd4:cff1:9e96
  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]
  GPRS Tunneling Protocol
    Flags: 0x30
    Message Type: T-PDU (0xff)
    Length: 957
    TEID: 0x00000002 (2)
  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 0000 = Flow Label: 0x000000
    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)
    
```

## Buyer's Guide

Item No	Product Description
<a href="#">PKV123</a>	FastRecorder™ and PacketExtractor™ for Monitoring IP Networks (requires any one of PKV120, PKV120p, PKV122, PKV122p, PKV124, PKV124p) <a href="#">PacketRecorder™ and PacketReplay™</a> (requires any one of PKV120, PKV120p, PKV122, PKV122p)

Item No	Related Software
<a href="#">PKV122</a>	PacketScan™ HD – High Density IP Traffic Analyzer w/ 2x10GigE
<a href="#">PKV124</a>	PacketScan™ HD – High Density IP Traffic Analyzer w/ 2x40/100GigE
<a href="#">PKV100</a>	PacketScan™ (Real-time and Offline)
<a href="#">PKV101</a>	PacketScan™ - Offline
<a href="#">PKV170</a>	NetSurveyorWeb™

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](http://www.gl.com) - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) [info@gl.com](mailto:info@gl.com)