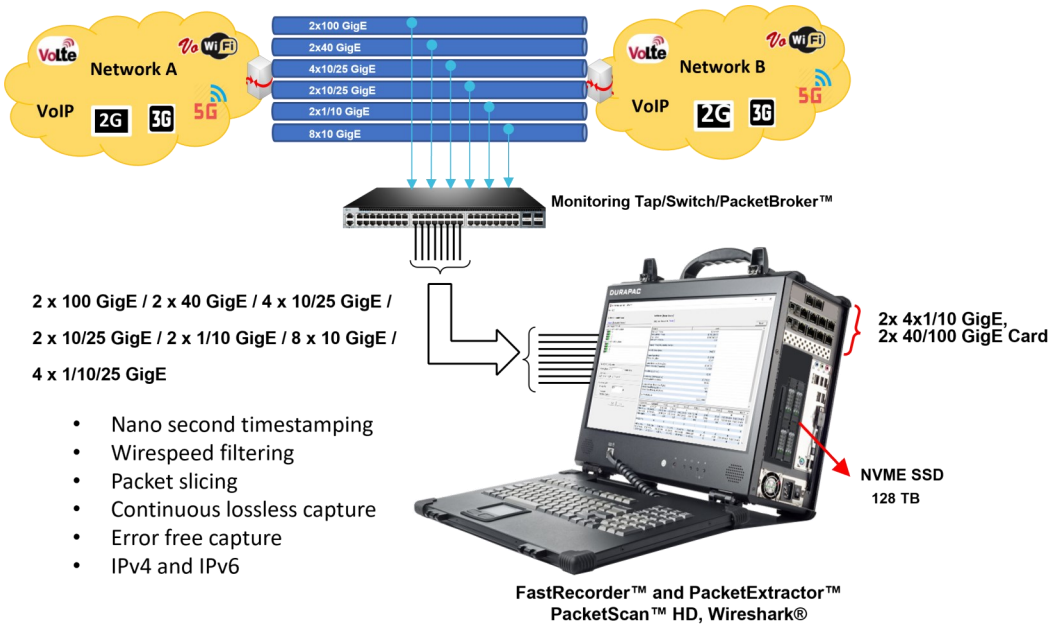
High Speed Ethernet and IP Capture

(FastRecorder™ and PacketExtractor™)



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

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.

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 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

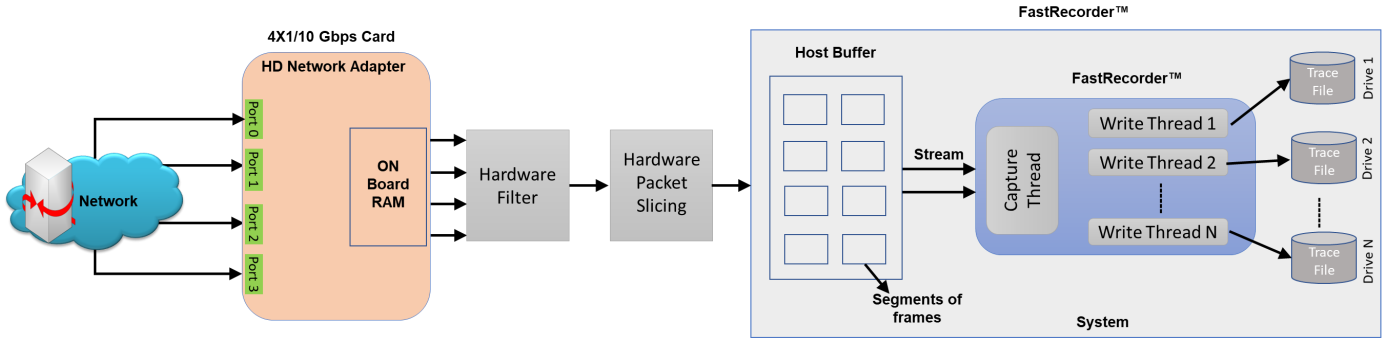
Hardware Requirements	**Requires GL's HD Network Interface adapters** • High Density Network Adapters can be any of the following types – – **4 x 1/10 Gbps** – requires 10GBASE-SR SFP+; Optical only – **2 x 40/100 Gbps** – requires MTP/MPO Connector for CFP2; Optical only • **Hard Disk**: SSD hard disk (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.



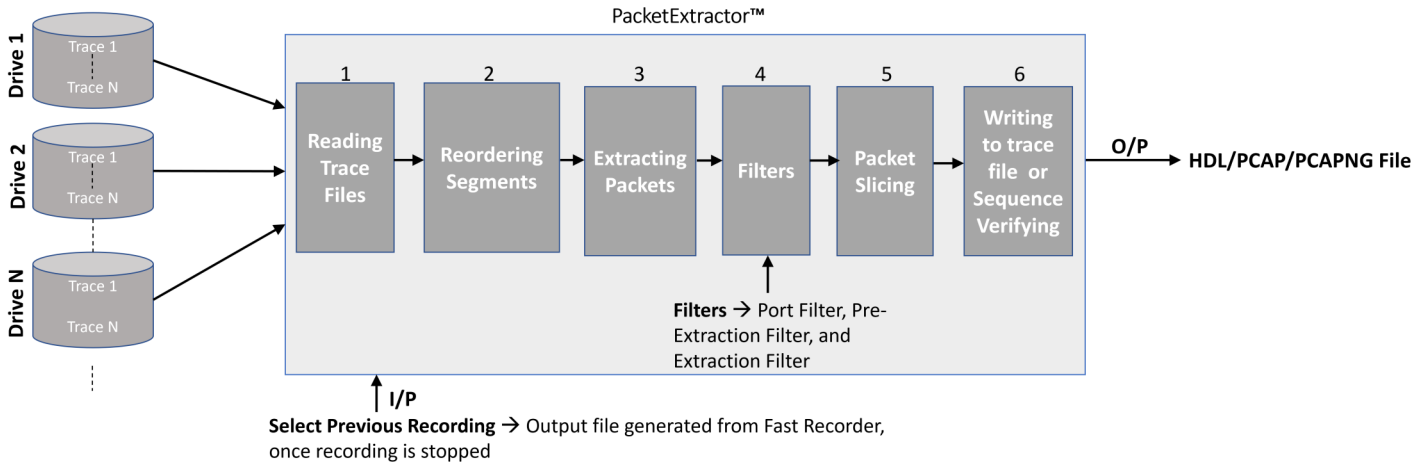
PacketExtractor™

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.

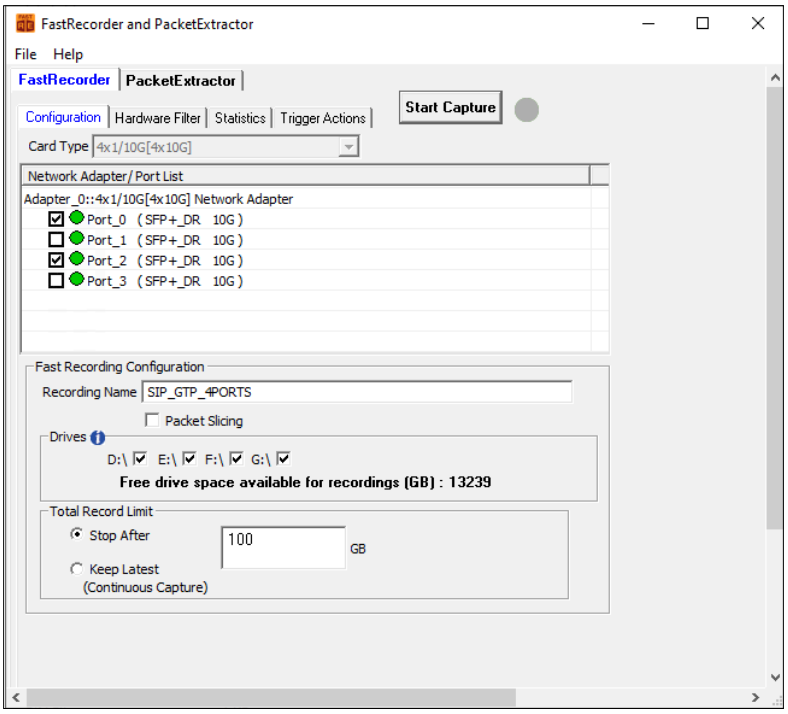
Extractor Module: The Extractor module then extracts packets from the reassembled segments.

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 .



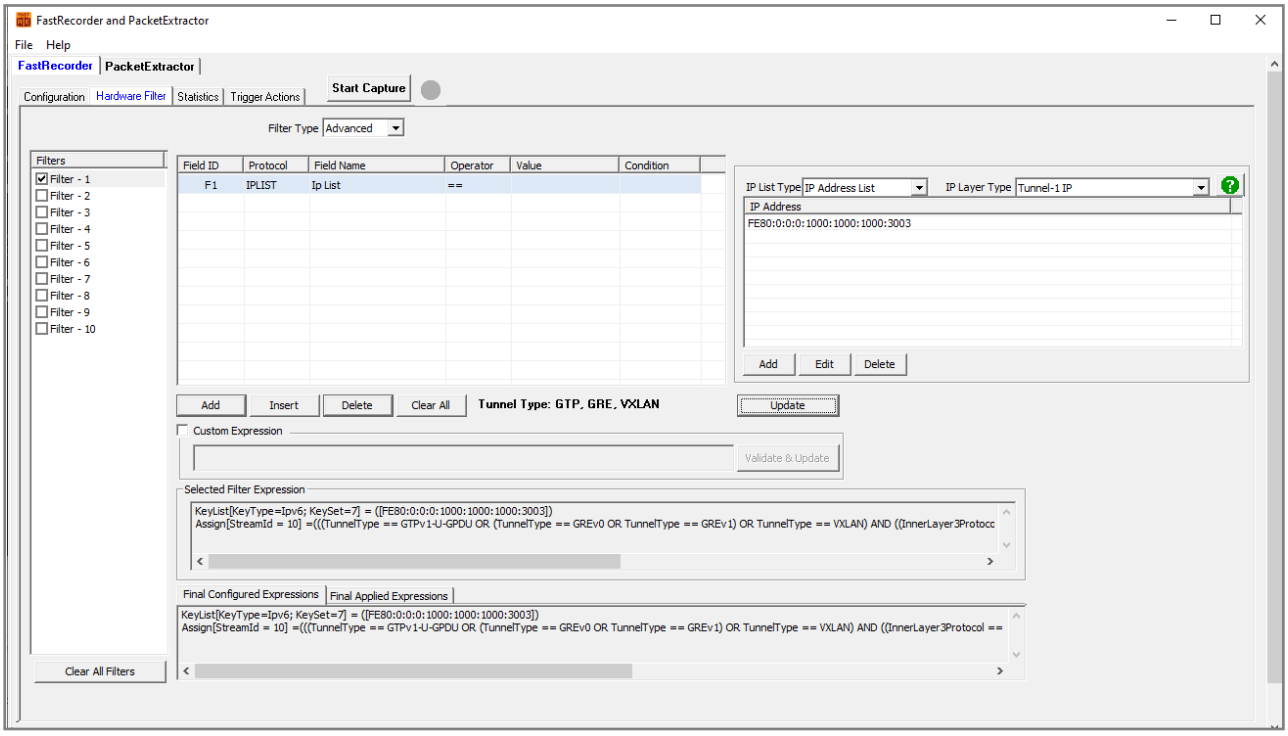
FastRecorder™

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

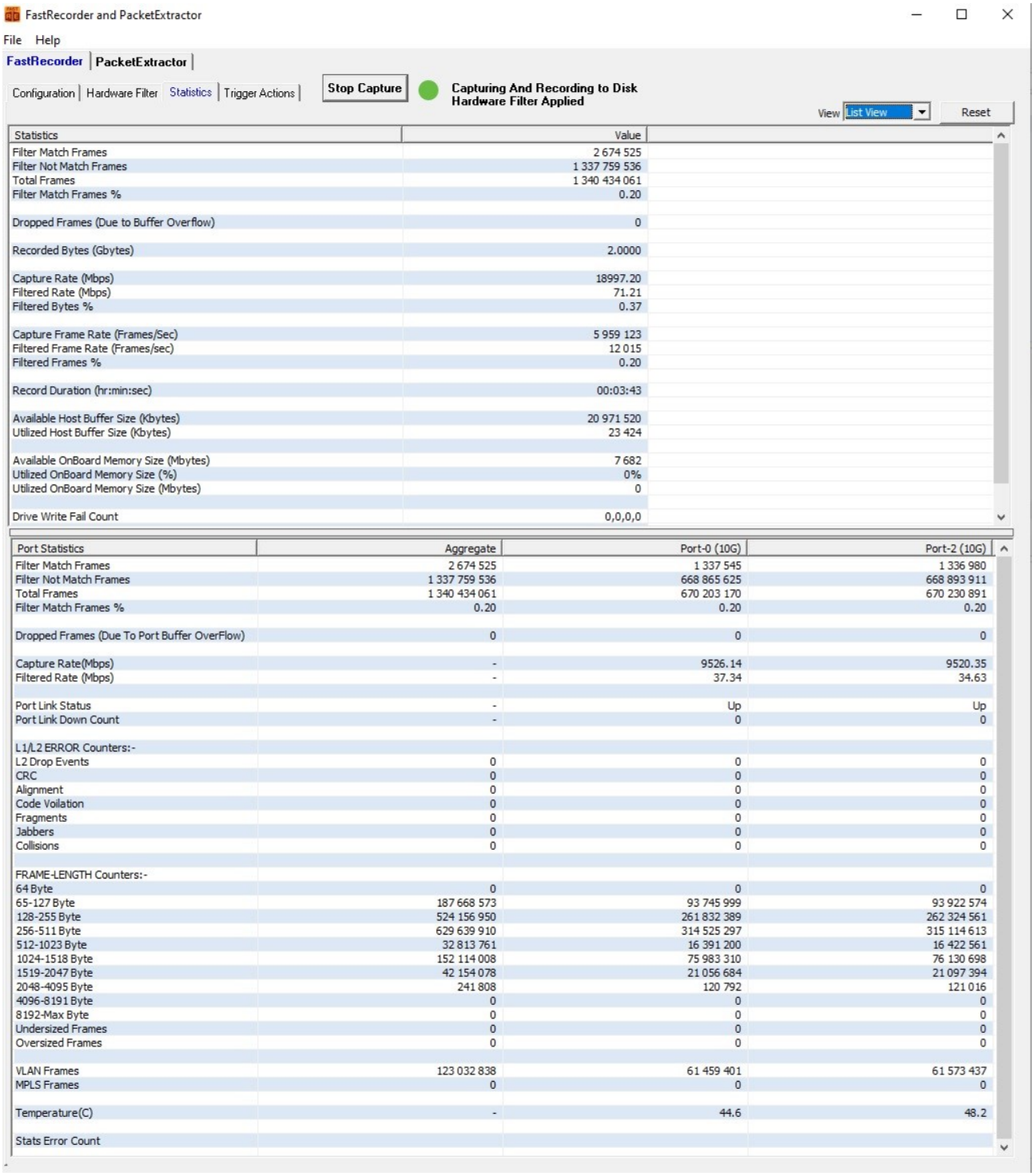
The Hardware Filter option enables users to easily set up filter conditions to capture traffic of interest continuously at line rate. For instance, it can be used to filter GTP traffic as shown below.



FastRecorder™ 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

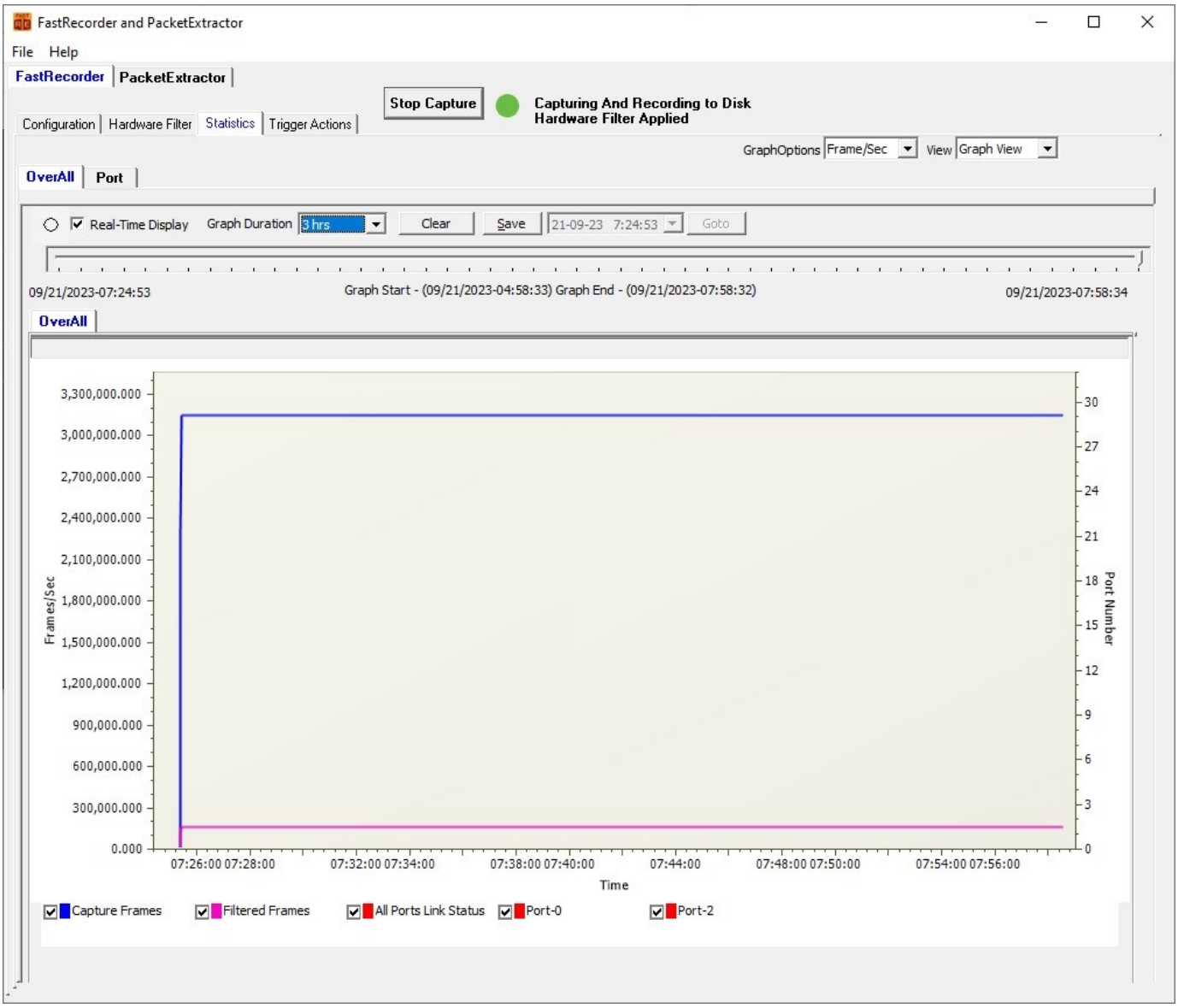


Statistics	Value
Filter Match Frames	2 674 525
Filter Not Match Frames	1 337 759 536
Total Frames	1 340 434 061
Filter Match Frames %	0.20
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	2.0000
Capture Rate (Mbps)	18997.20
Filtered Rate (Mbps)	71.21
Filtered Bytes %	0.37
Capture Frame 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			

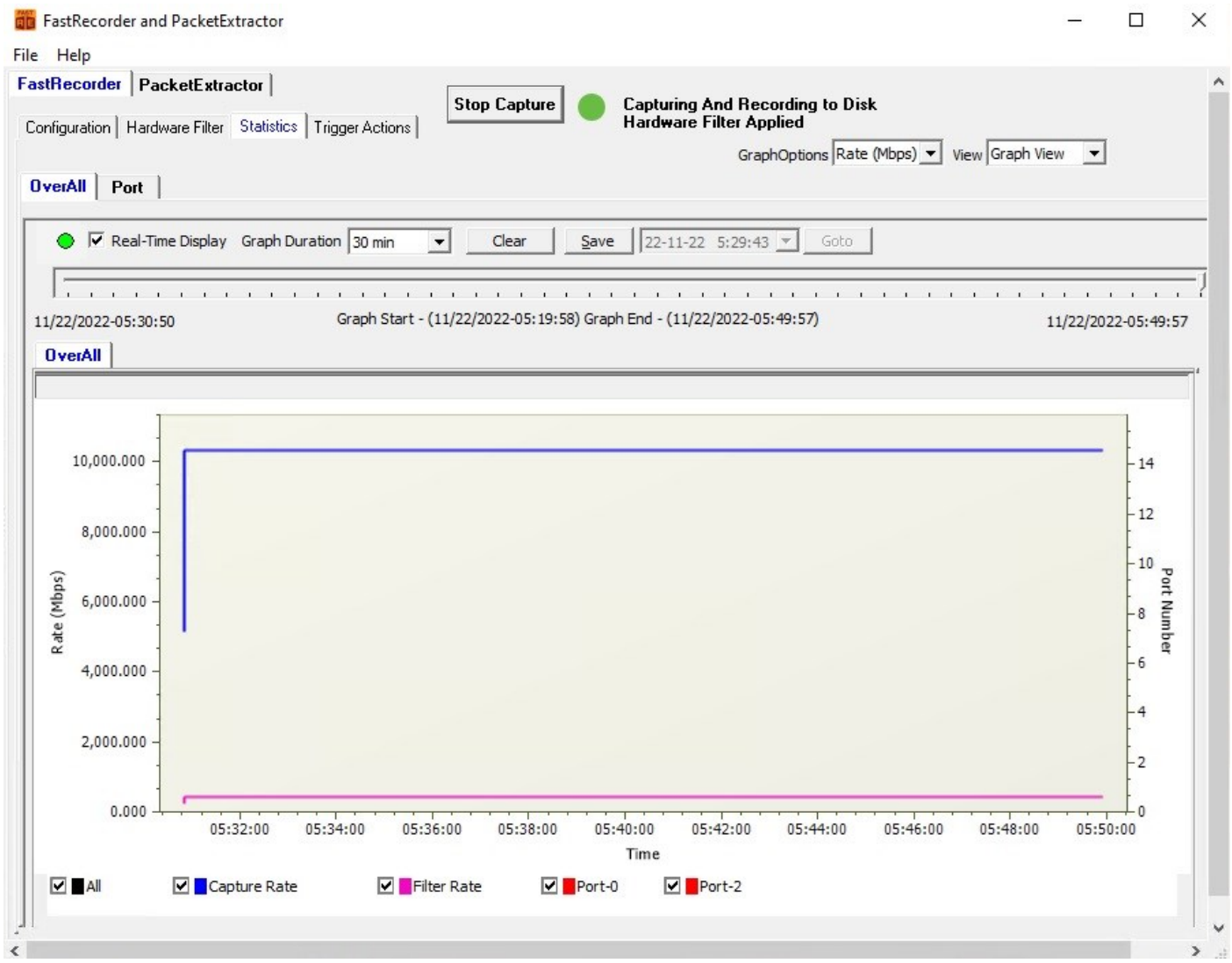
FastRecorder™ Overall Graph View

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



FastRecorder™ Per Port Graph View

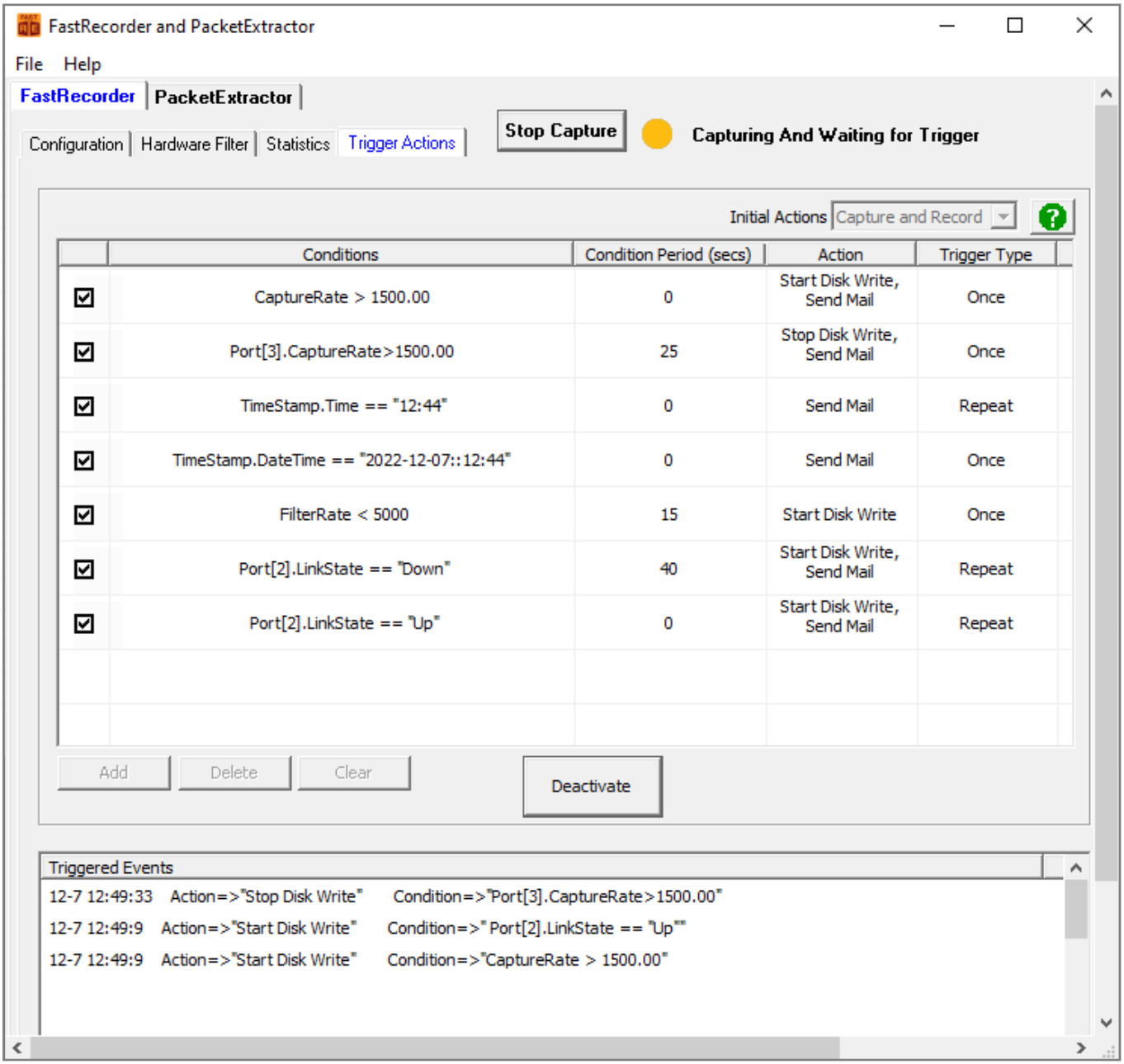
Users can view real-time port graphs (Time vs. Frames/Sec) displaying Capture and Filtered Frames data for the past 7 days.



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)

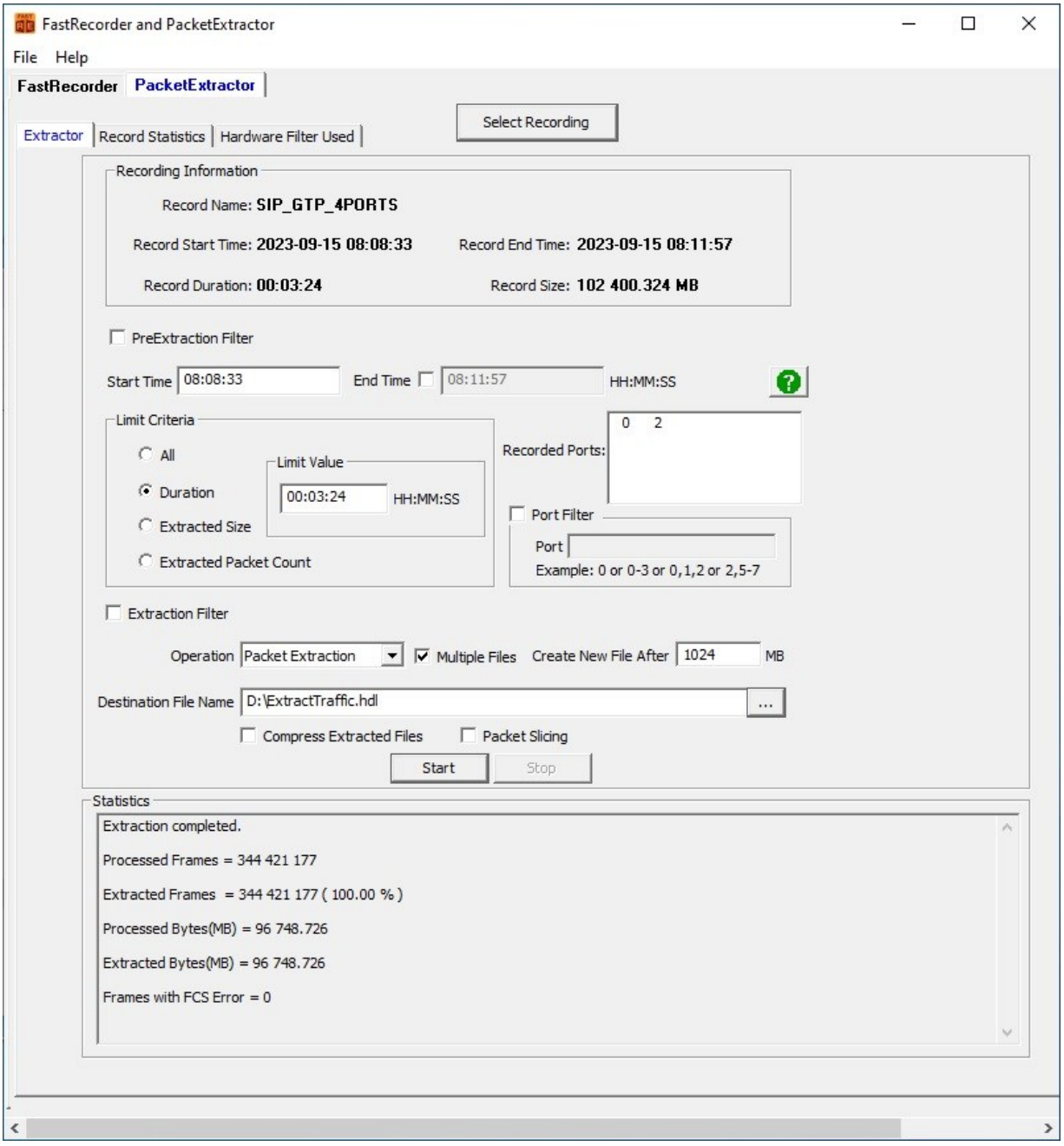


PacketExtractor™

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

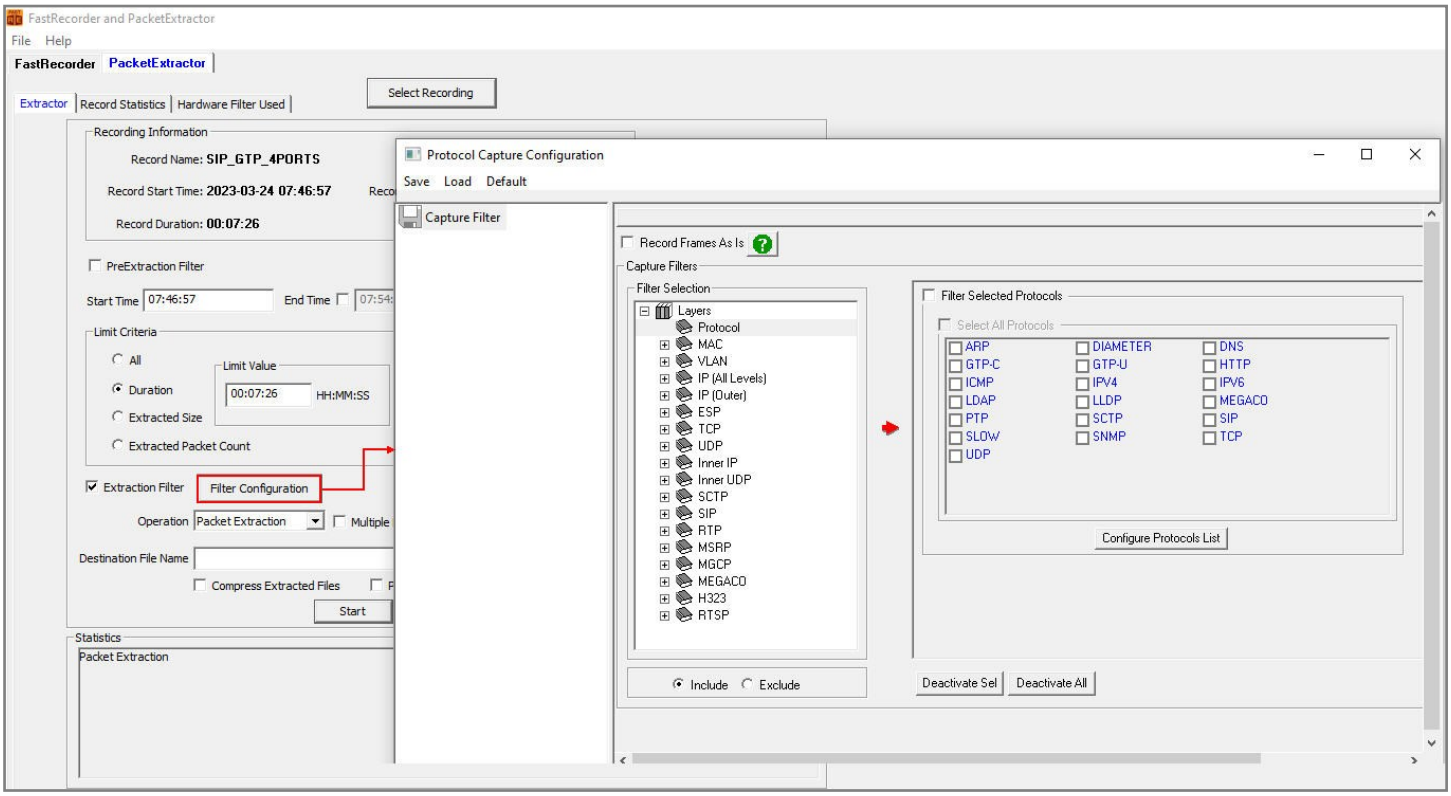
When extracting packets from a recorded file without using a filter, select the file, specify the default record start time, uncheck the Extractor Filter option, choose the desired path to save the extracted data to a file, and view the extracted statistics under the **Statistics** section.



PacketExtractor (*contd.*)

Packet Extraction from the Recording files with filter

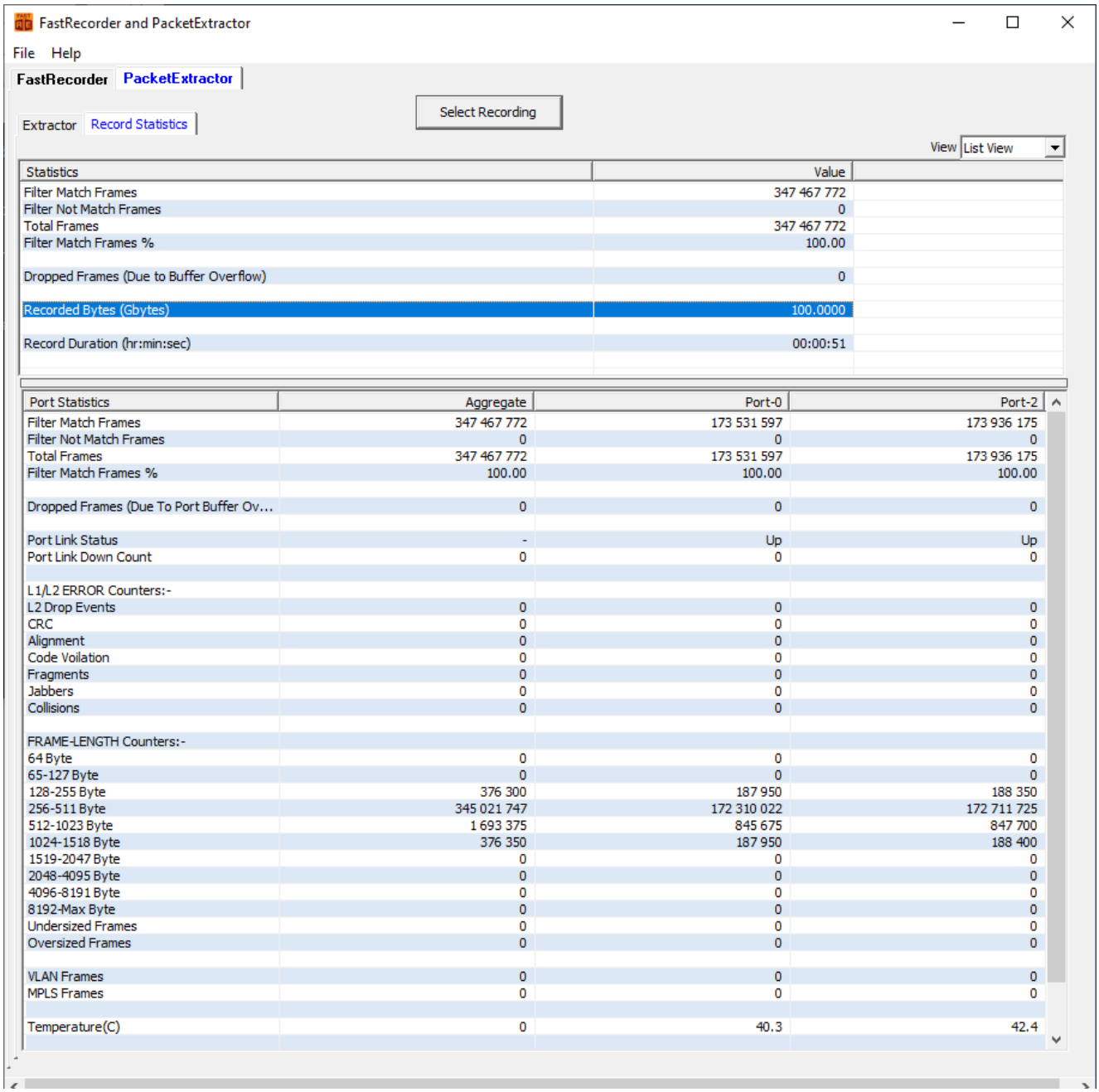
For extracting packets from previously recorded files with filters, select the previously recorded file. Check the **Extractor Filter** option to apply various software filters according to test requirements, and then configure the filters accordingly. Finally, select the desired path for saving the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

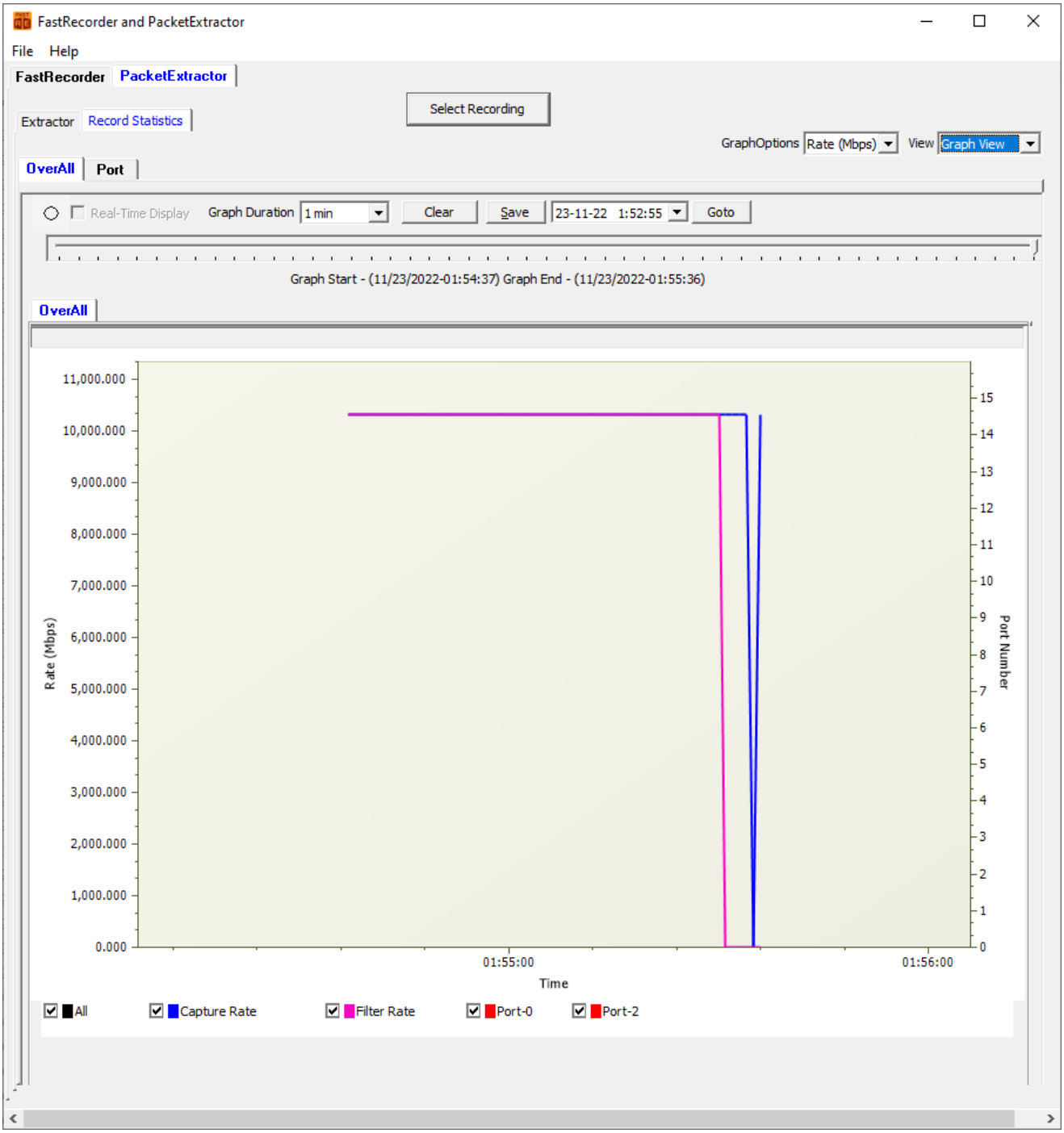


Statistics	Value
Filter Match Frames	347 467 772
Filter Not Match Frames	0
Total Frames	347 467 772
Filter Match Frames %	100.00
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	100.0000
Record Duration (hr:min:sec)	00:00:51

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

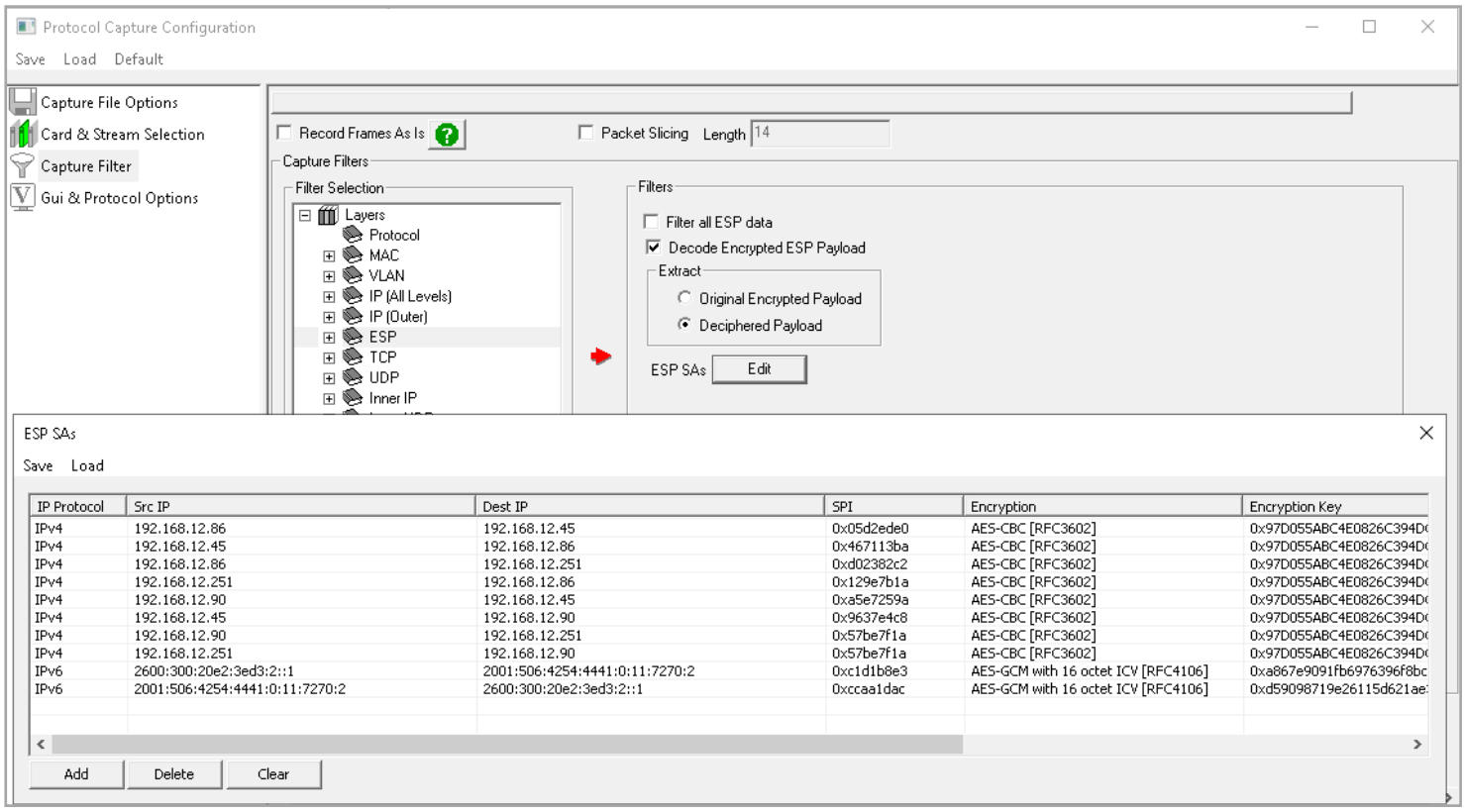
Recorder Graph View

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



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.

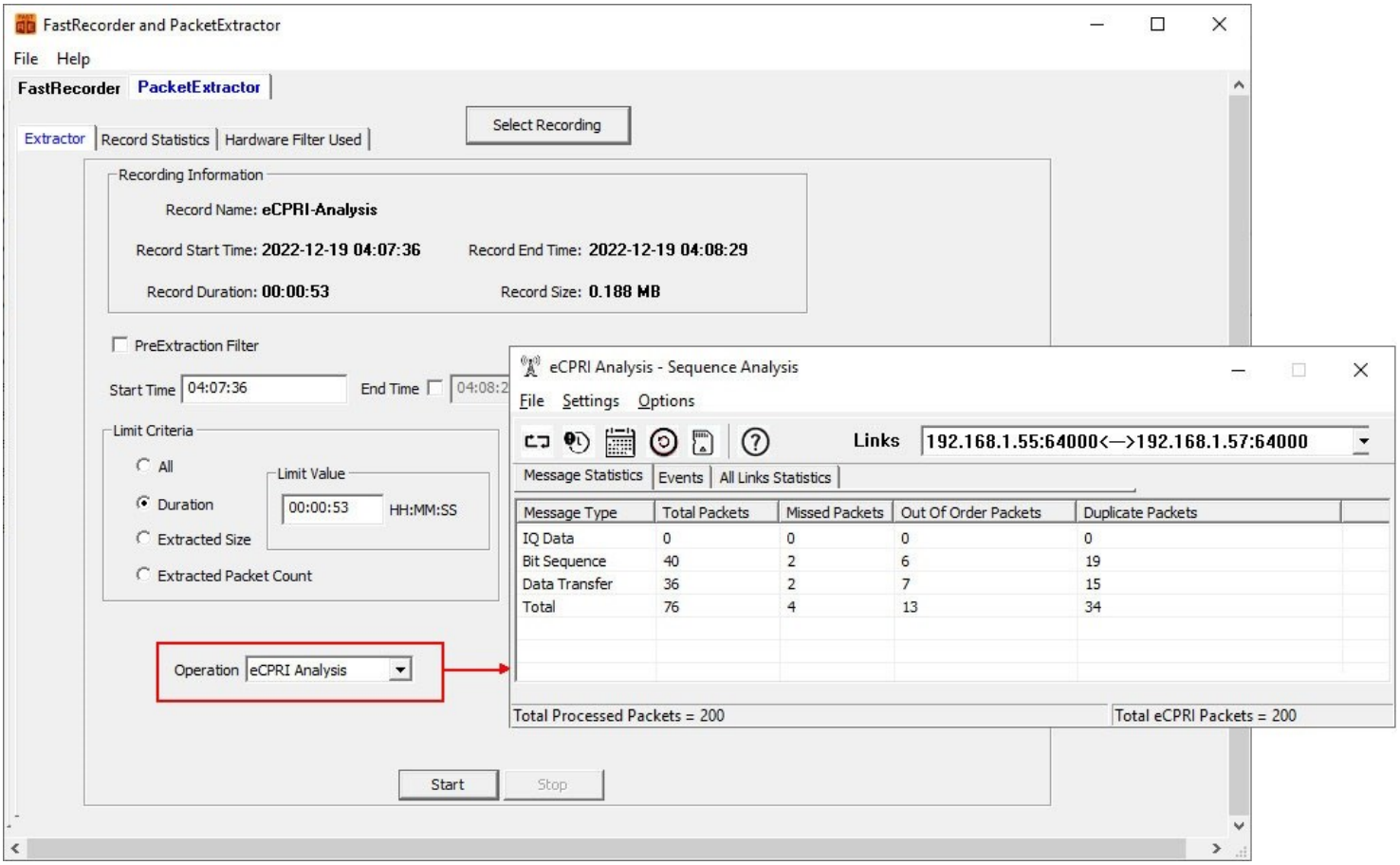


eCPRI Analysis

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

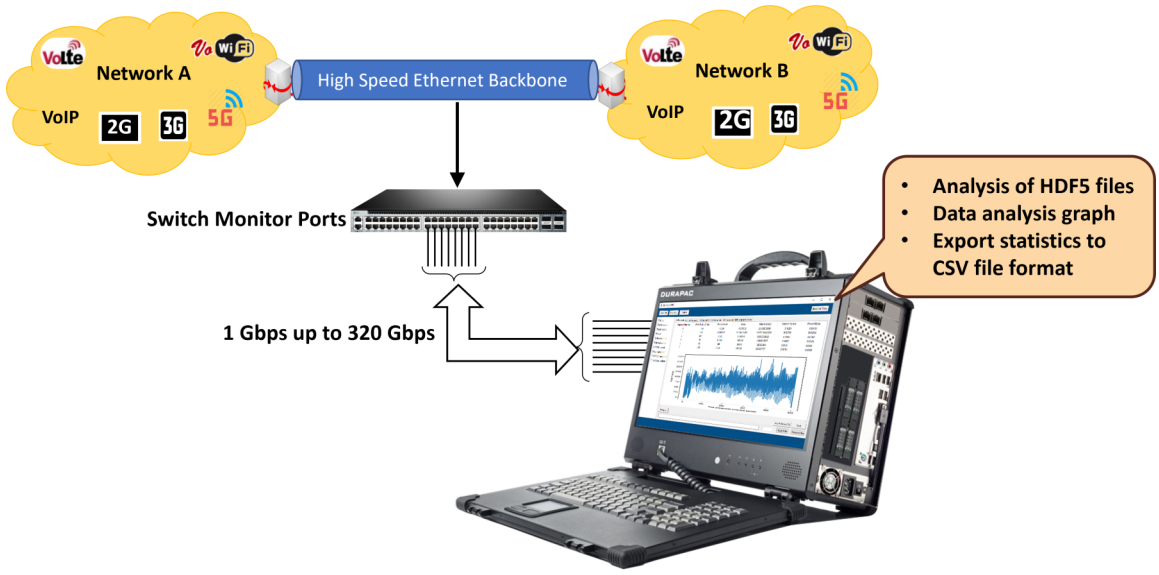


IP Analytics™

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.

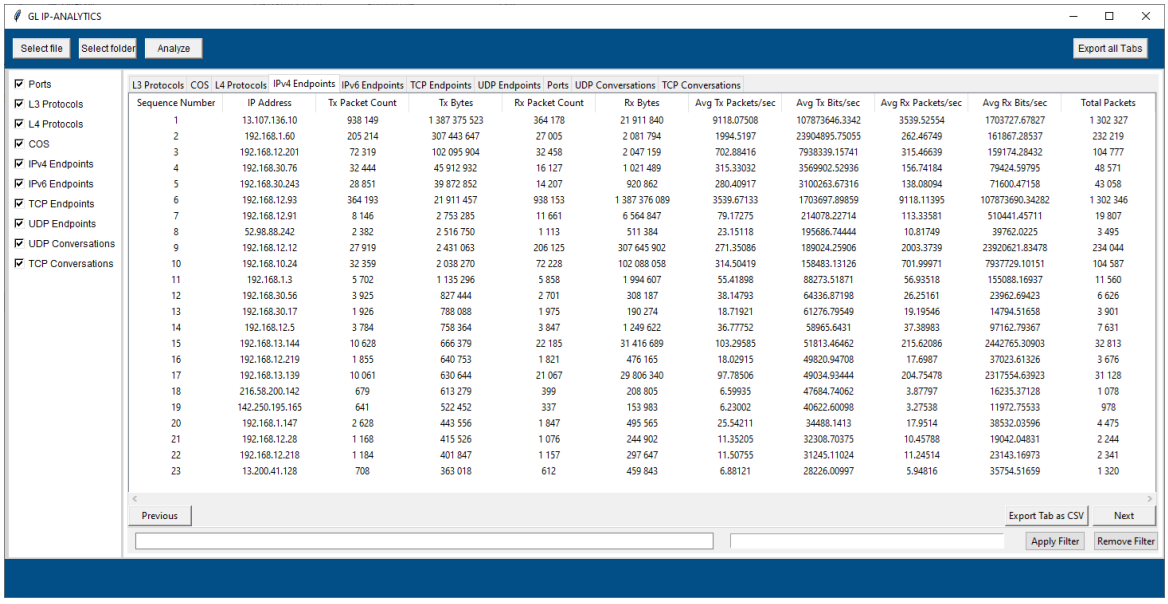
Data Analysis

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**.



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.

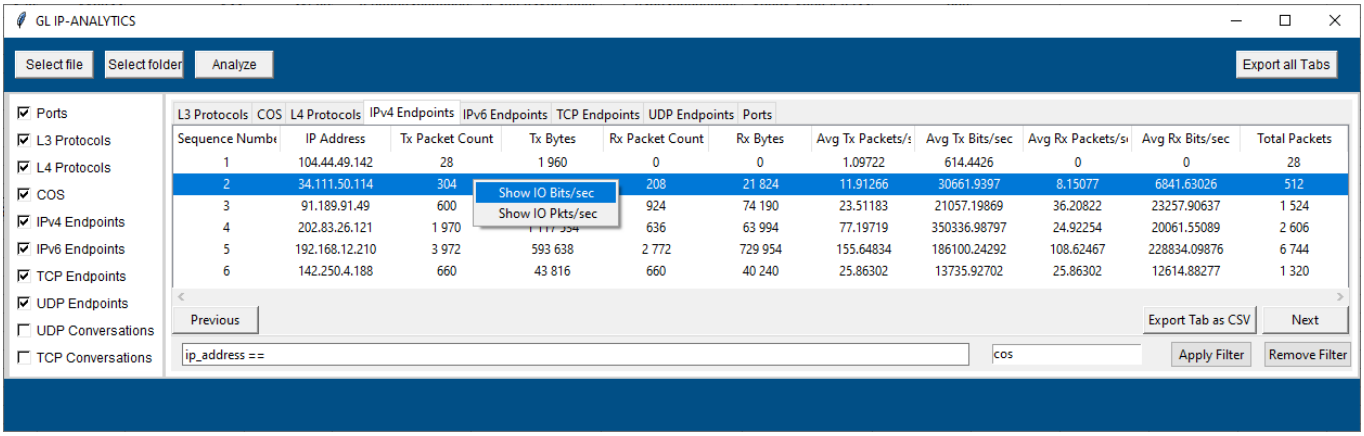


Key Features

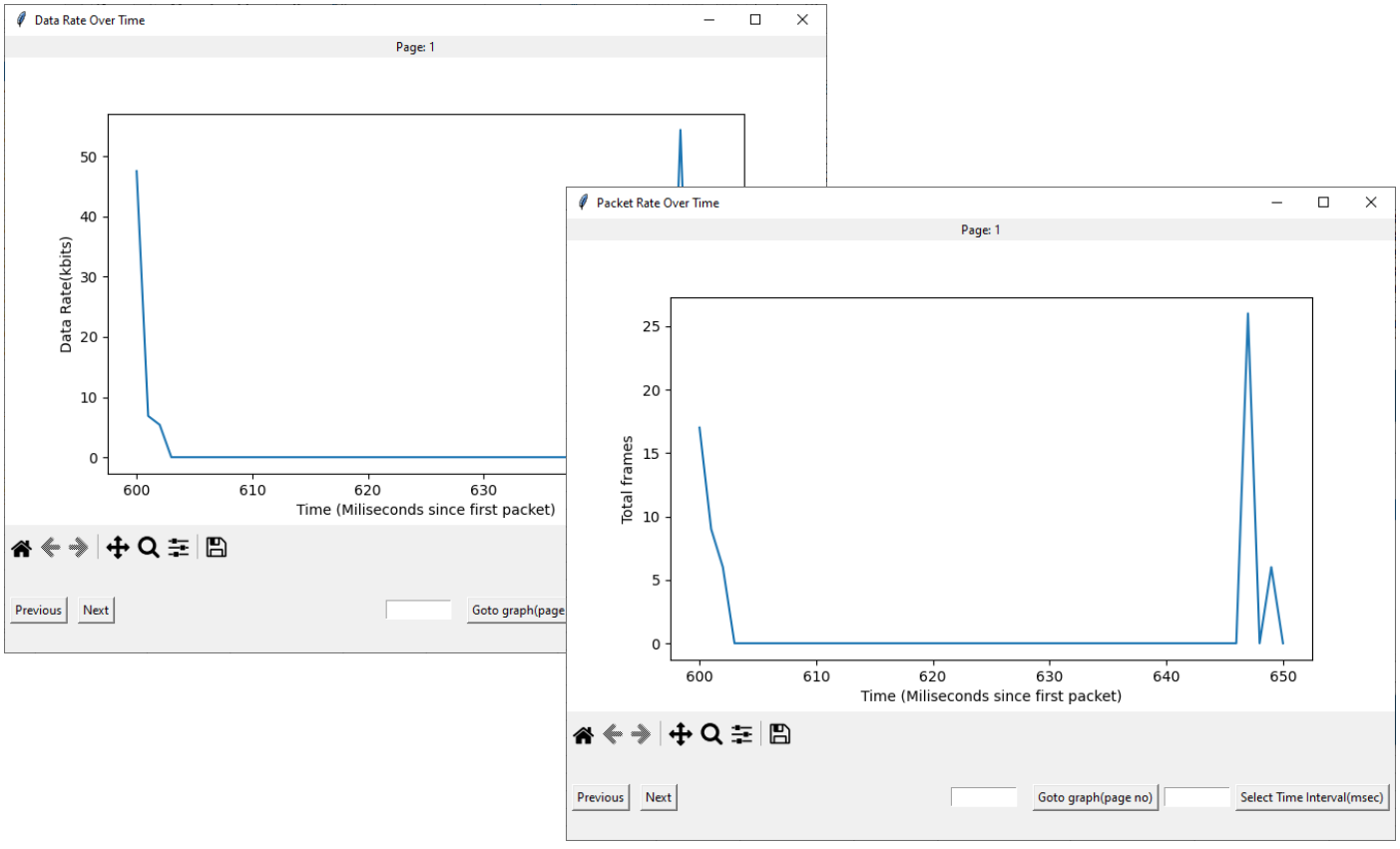
- Includes detailed analysis of different IP layers such as Layer 3 Protocols, Class of Services (DSCP), Layer 4 Protocols, IPv4 Endpoints, IPv6 Endpoints, TCP Endpoints, UDP Endpoints, Recorded Port statistics, UDP Conversations and TCP Conversations along with Port wise details
- Provides in-depth 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**.

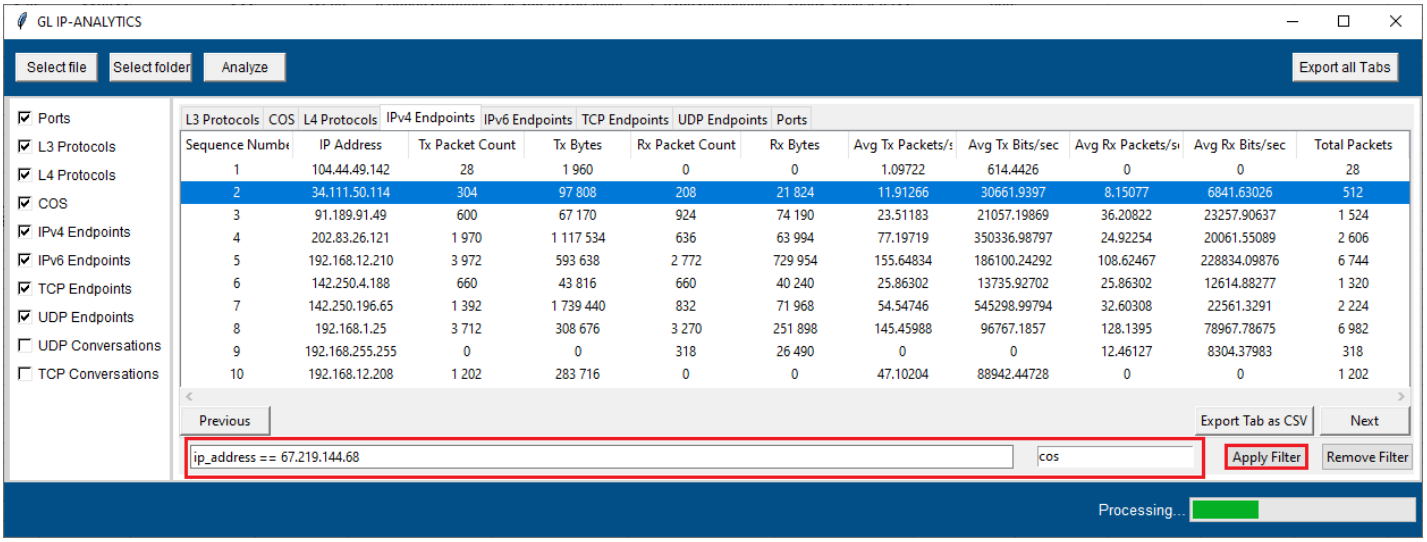


Display of **Data Rate Over Time** and **Packet Rate Over Time** graphs.

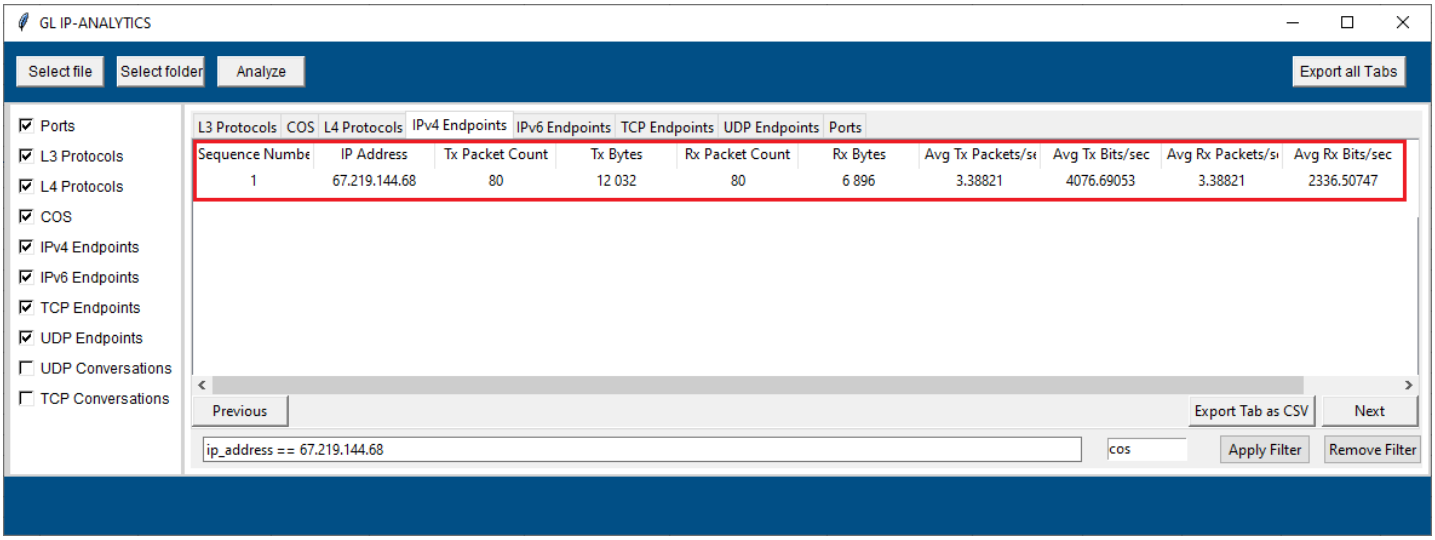


Applying Filter

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**.



Observe the applied filter (for **ip_address == 67.219.144.68**) as shown below.

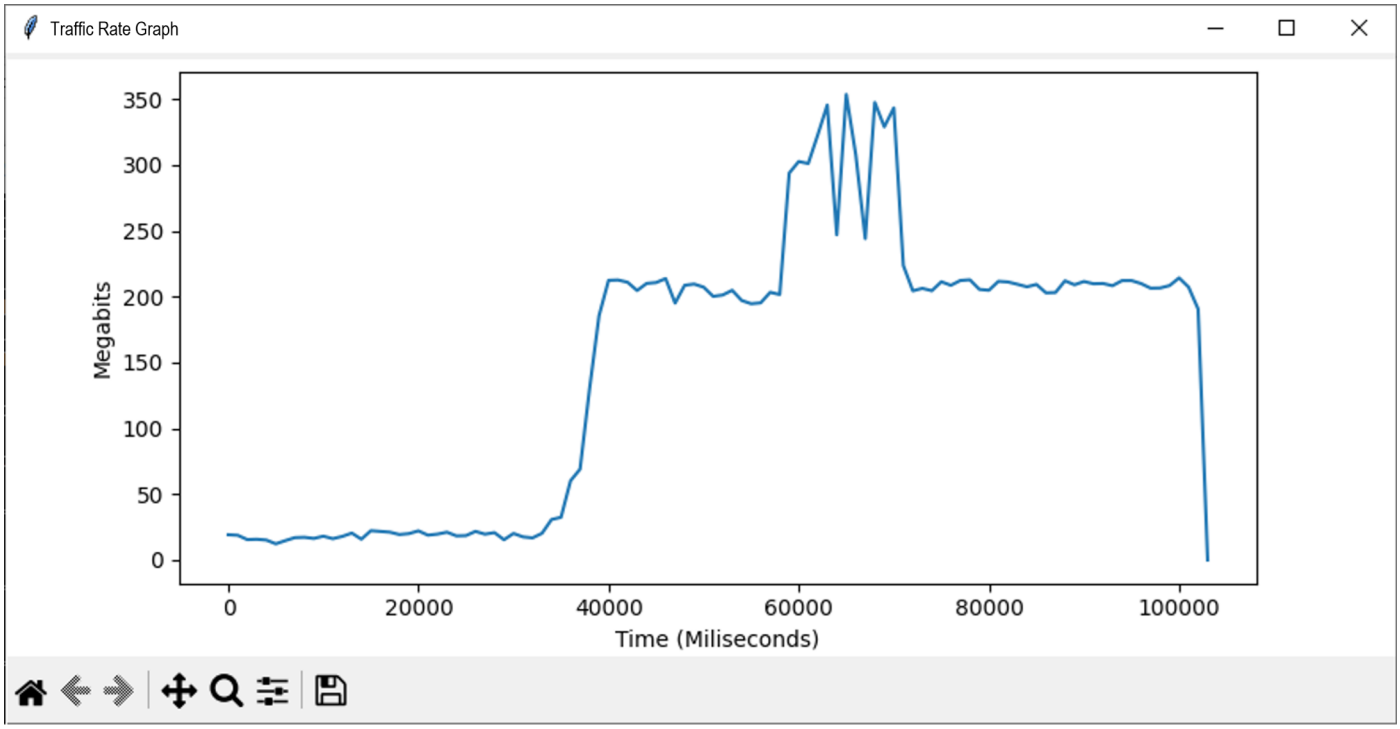


Rate Analysis

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.

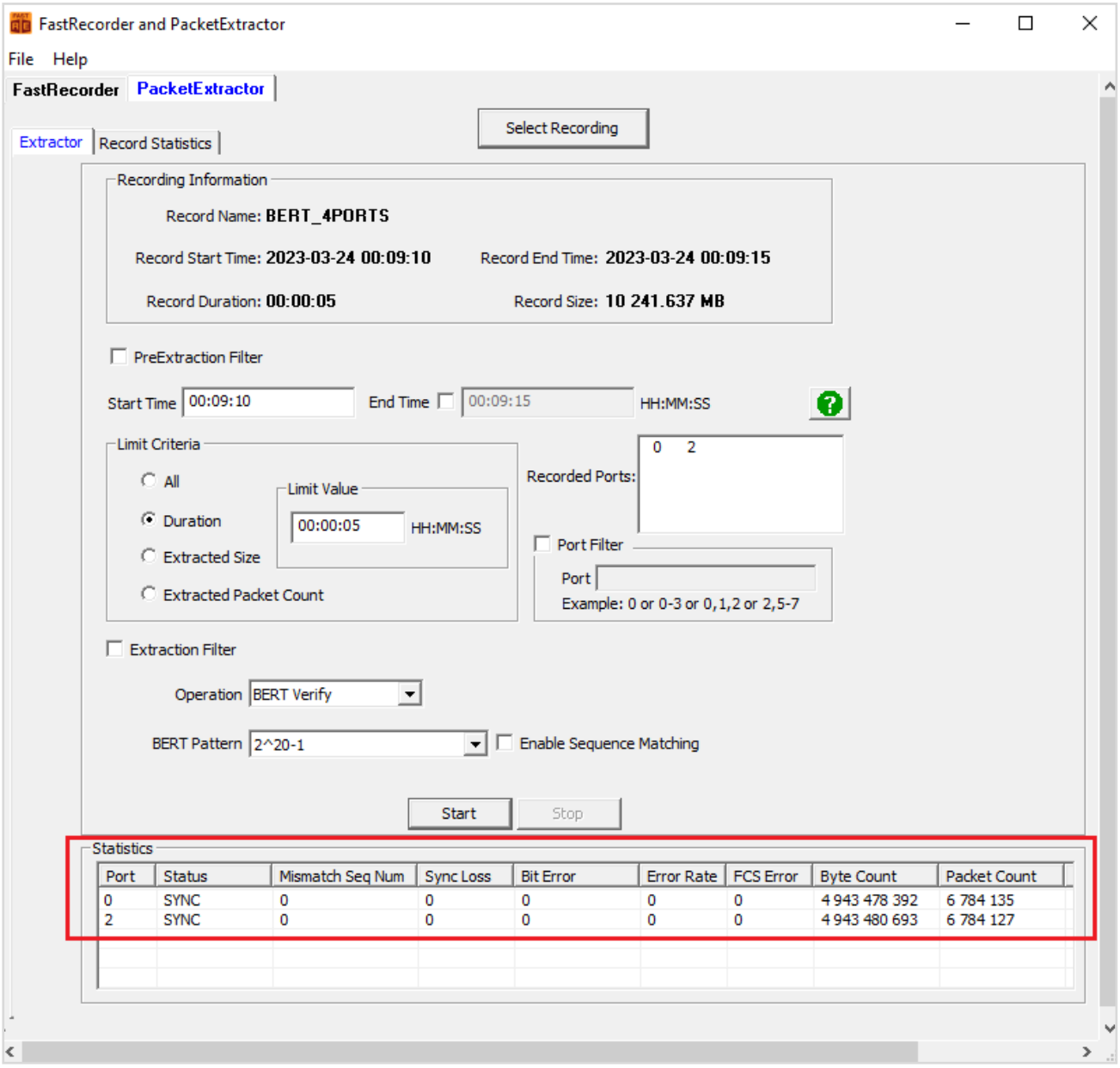
GL's Time Graph Plotter analyzes HDF5 files and generates graphs for **Packets/Sec**, **Megabits/Sec**, **Kilobits/Sec**, and **Bits/Sec** options, for individual recorded ports.

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.



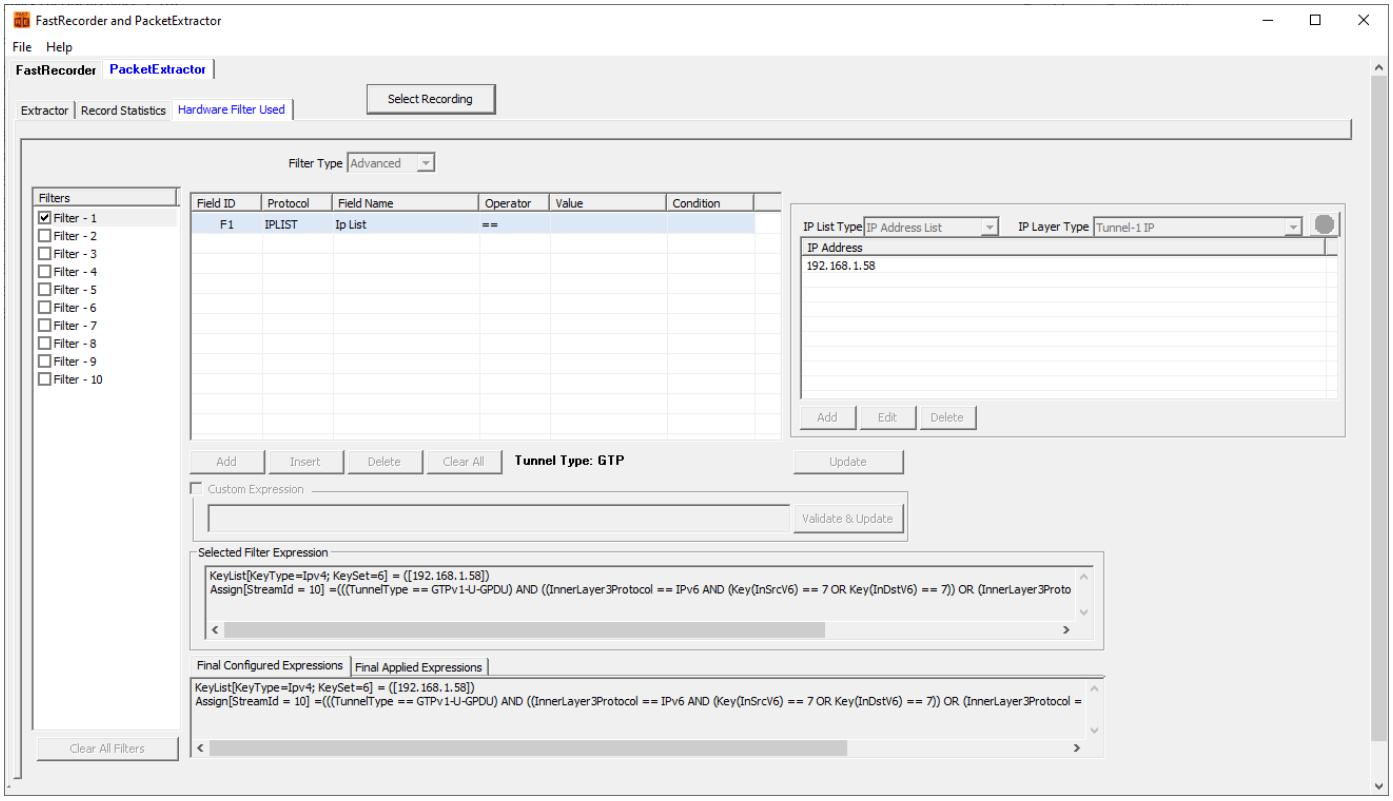
BERT Verification

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.



Hardware Filter Used while Recording

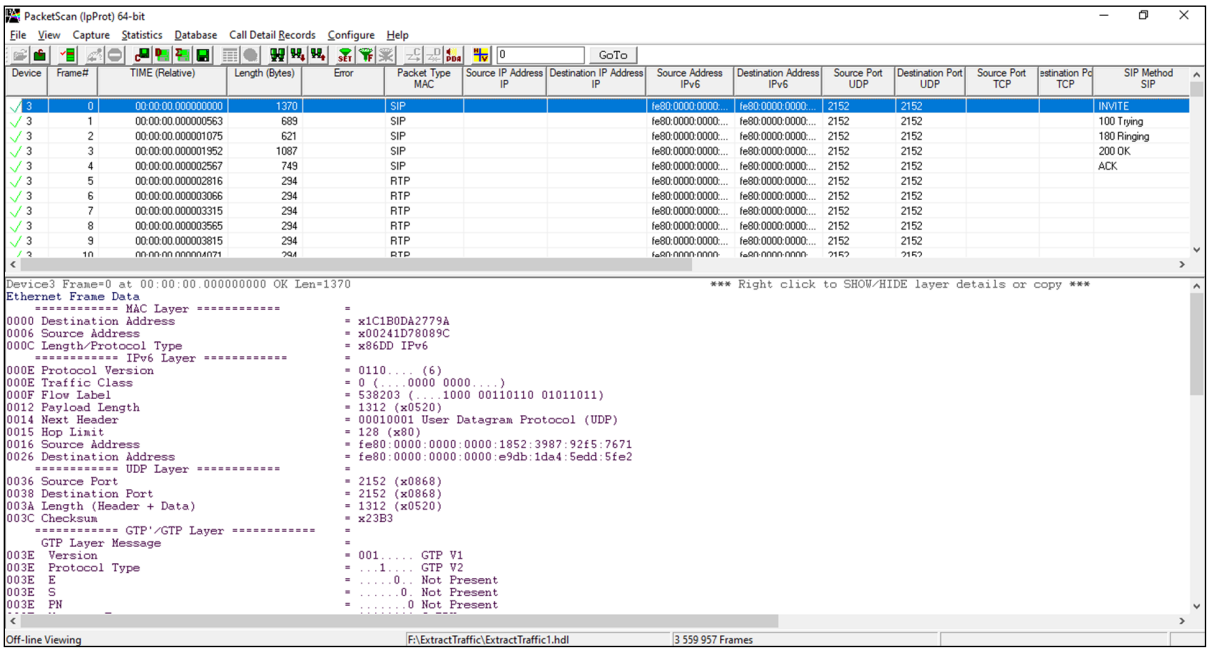
The Hardware Filter Used tab displays the configured hardware filter for the recorded file.



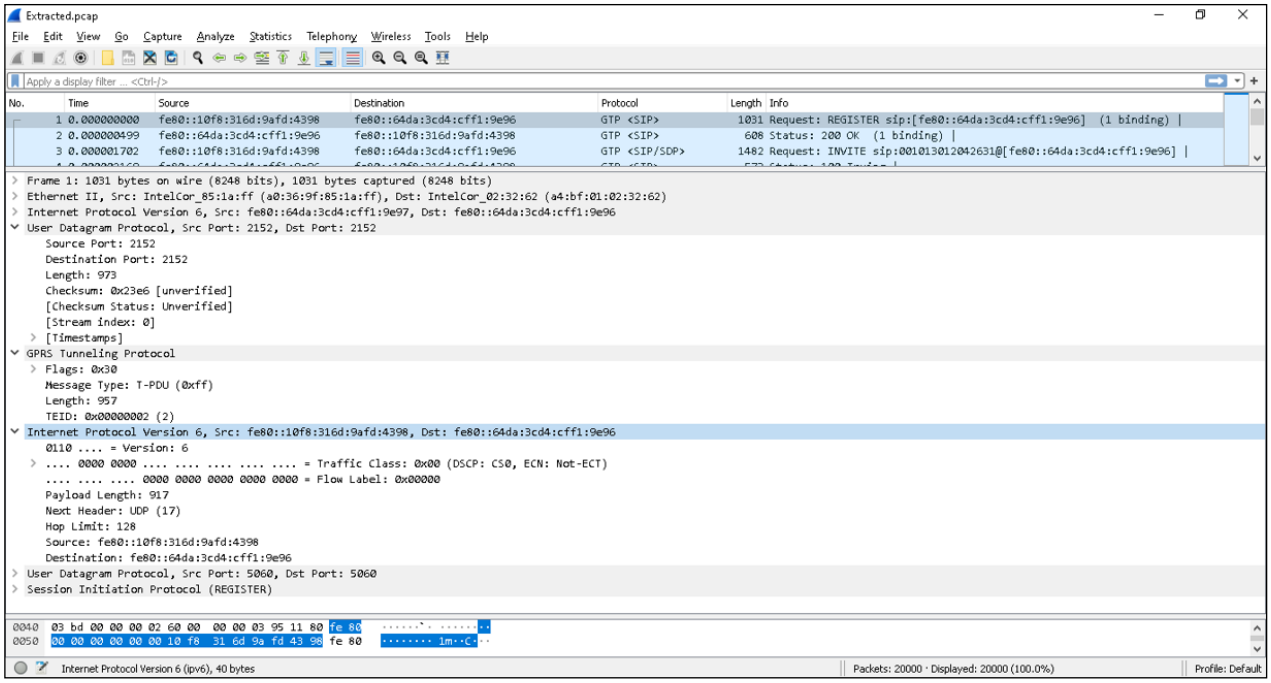
Analysis of Extracted Traffic

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

Traffic Analysis using PacketScan™ Application



Traffic Analysis using Wireshark® application



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
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™

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