

---

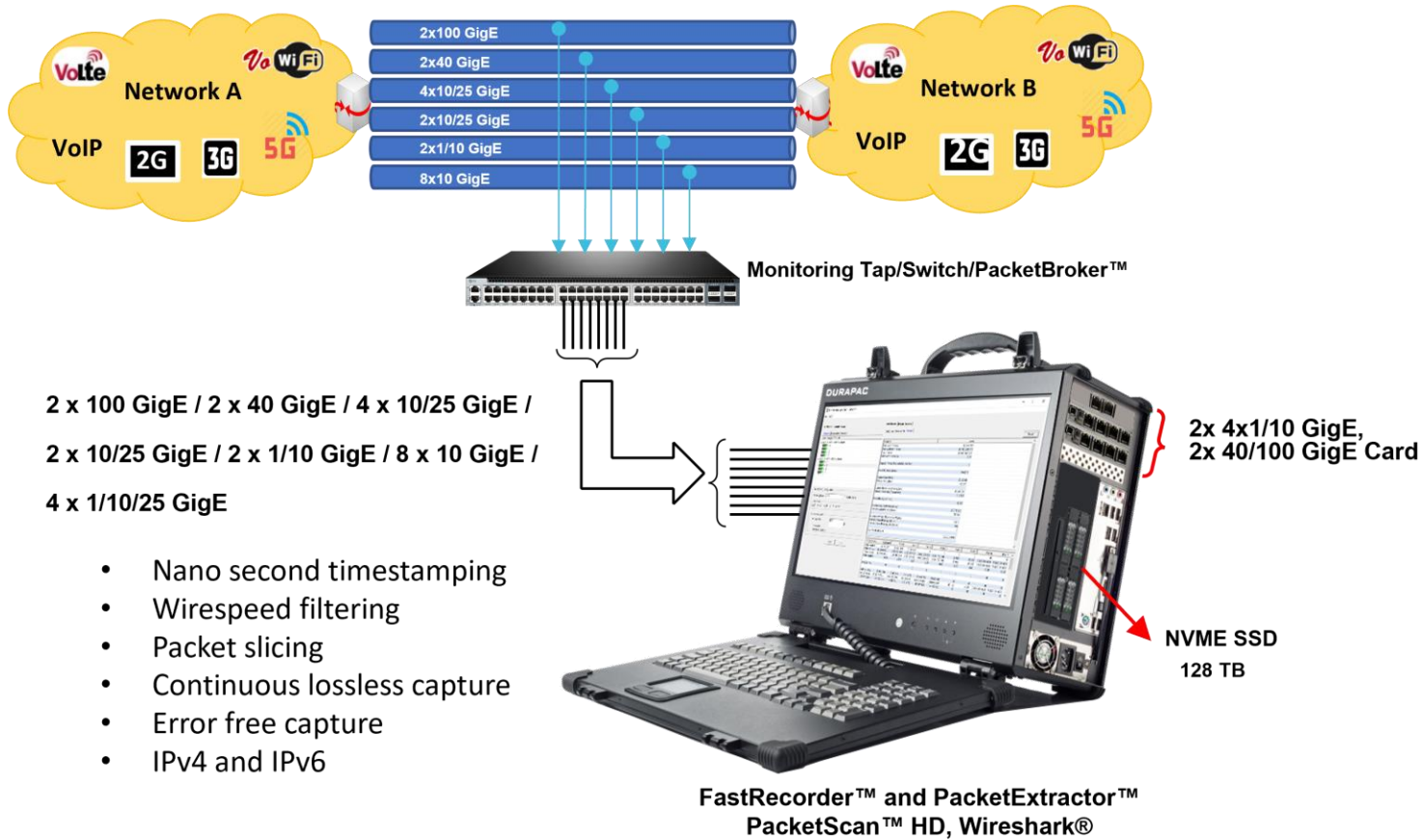
# FastRecorder™ and PacketExtractor™ for Monitoring IP Networks

---



818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878  
Phone: (301) 670-4784 Fax: (301) 670-9187 Email: [info@gl.com](mailto:info@gl.com)  
Website: <https://www.gl.com>

# Overview



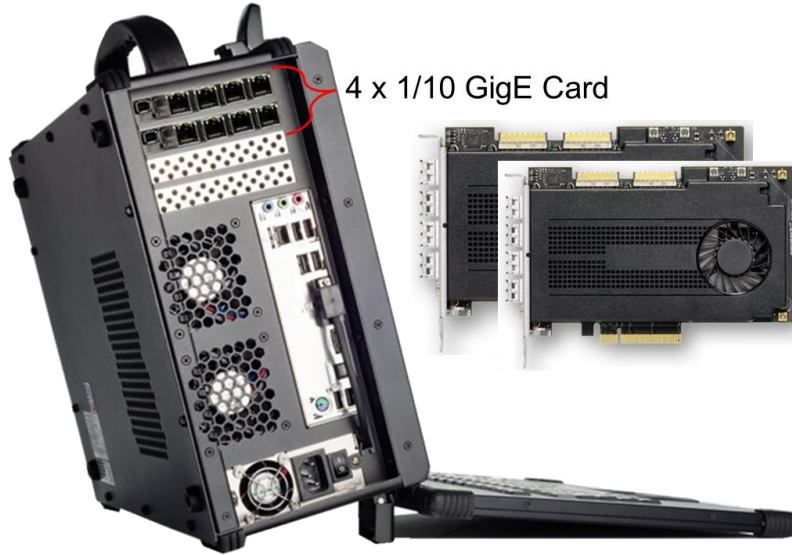
# PacketScan™ HD, FastRecorder™ & PacketExtractor™

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



\*\* Also available as a rack mounted unit

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



PacketScan™ HD - Lunch Box



Lunchbox specs are:

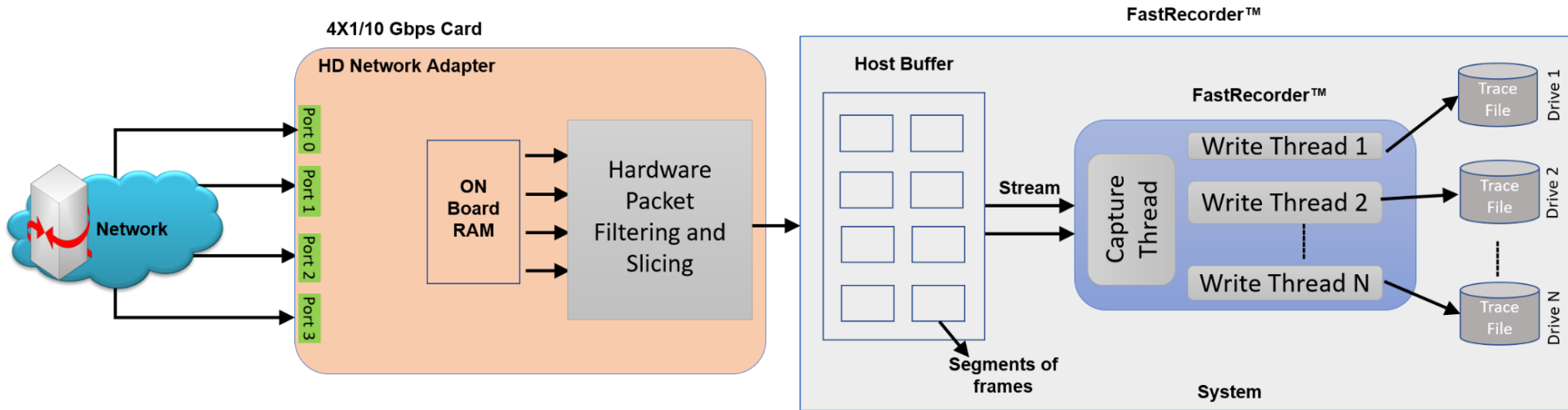
- Intel Xeon Silver 4210
- 64GB RAM
- 500GB SSD for OS
- 4x 3.84TB NVME SSD



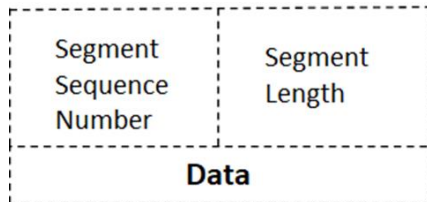
# What the Software Does?

- The Record feature includes a powerful Hardware Filter that allows user to filter out unwanted traffic, and continuously capture the traffic of interest
- The previously recorded traffic is extracted into single or multiple files and can be analyzed using GL's PacketScan™ and Wireshark® application
- Can create own filters using custom filter option which provides flexibility to check the fields and use the logical AND, OR conditions more efficiently
- Trigger based Start or Stop writing to disk based on the condition is configured based on Capture Rate, Filter Rate, per-port Capture Rate, and Filter Rate
- E-mail alert for specified trigger condition
- Supports Encapsulating Security Payload (ESP) protocol to decrypt ESP packets on both IPv4 and IPv6 by providing ESP SAs value
- BERT verification analyzes the received BERT pattern and provides various vital measurements

# FastRecorder™ Architecture

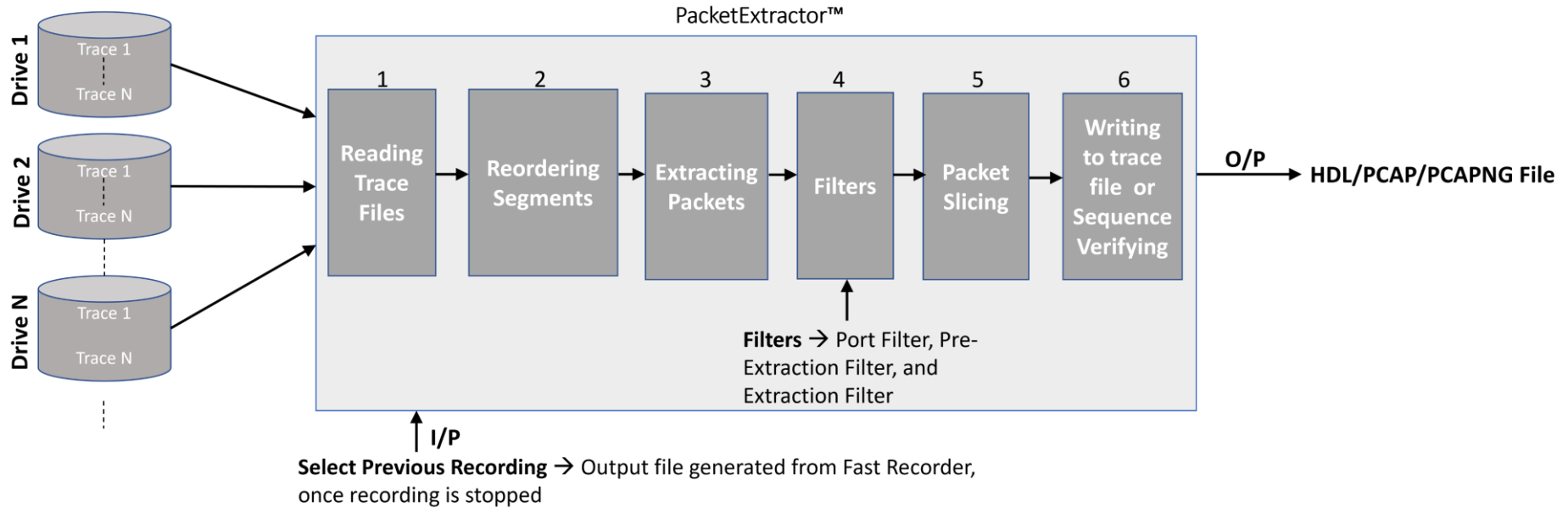


Buffer segments stored internally in files:



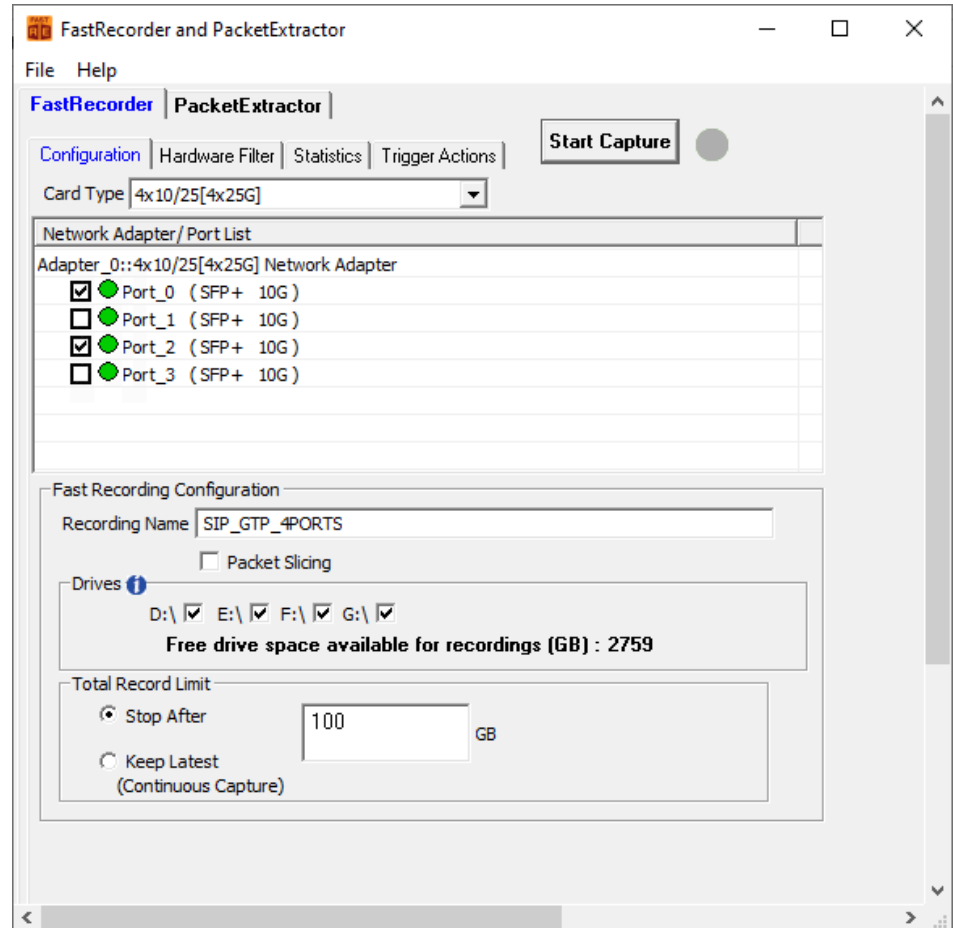
Segment Sequence Number and Segment Length is used while analysing/ Re-assembling the segments in Packet Extractor.

# PacketExtractor™ Architecture



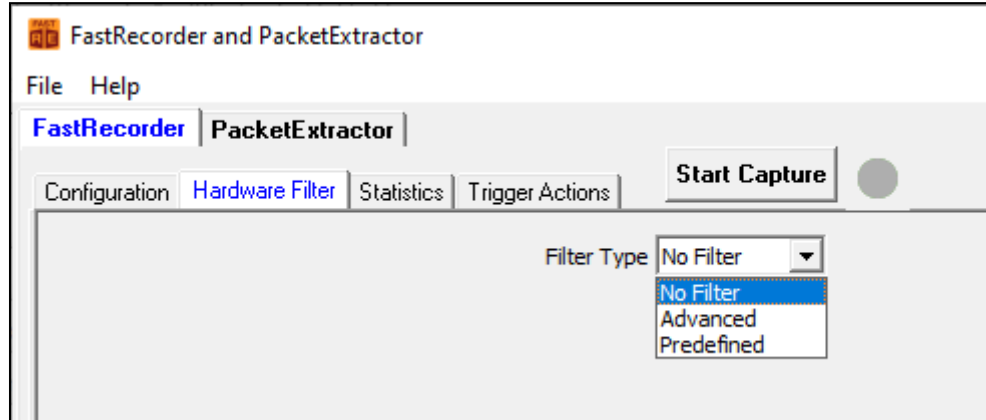
# FastRecorder™ Operations

- FastRecorder™ application provides various options to capture the high-density real-time traffic on disk drives and store the recorded traffic into a file
- The application can capture the traffic continuously until user stops the recorder or specify the size limit to stop the traffic capture



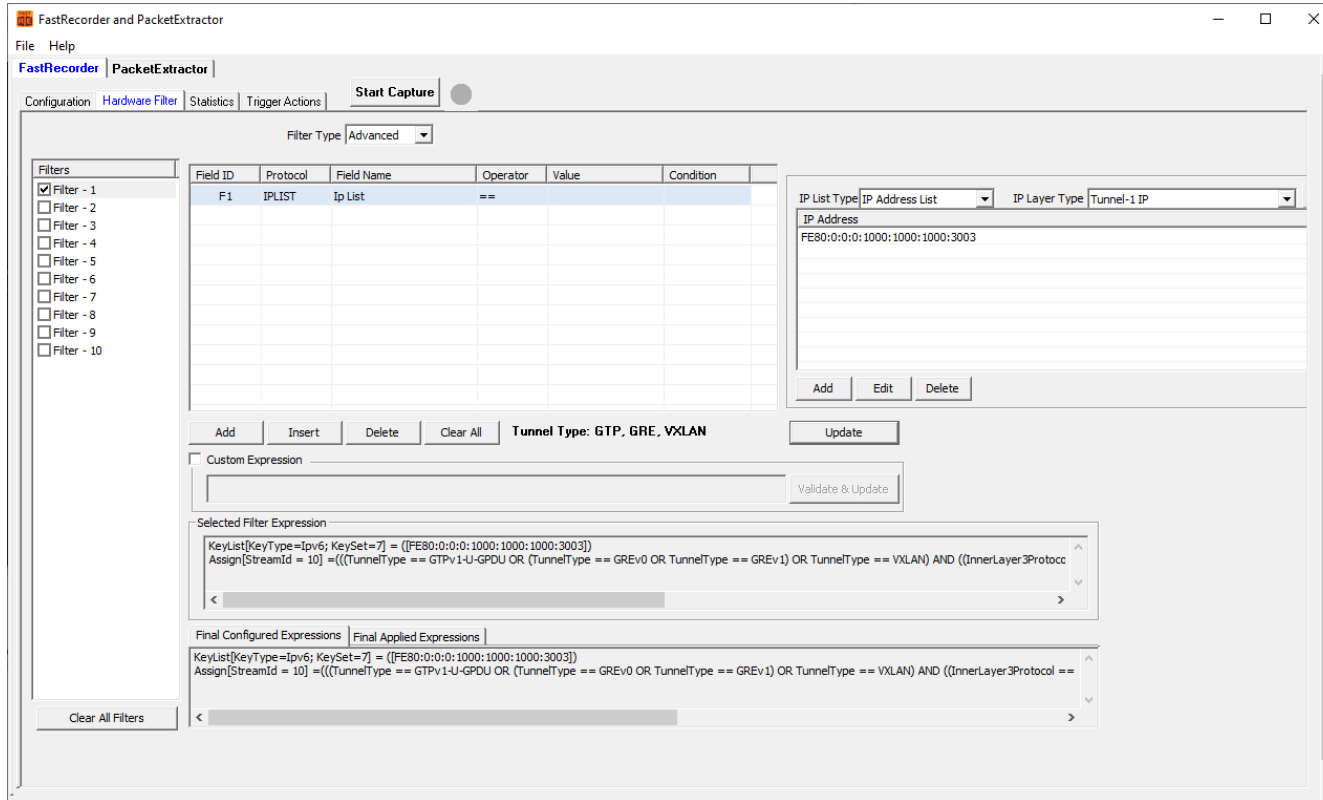
# Hardware Filters

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



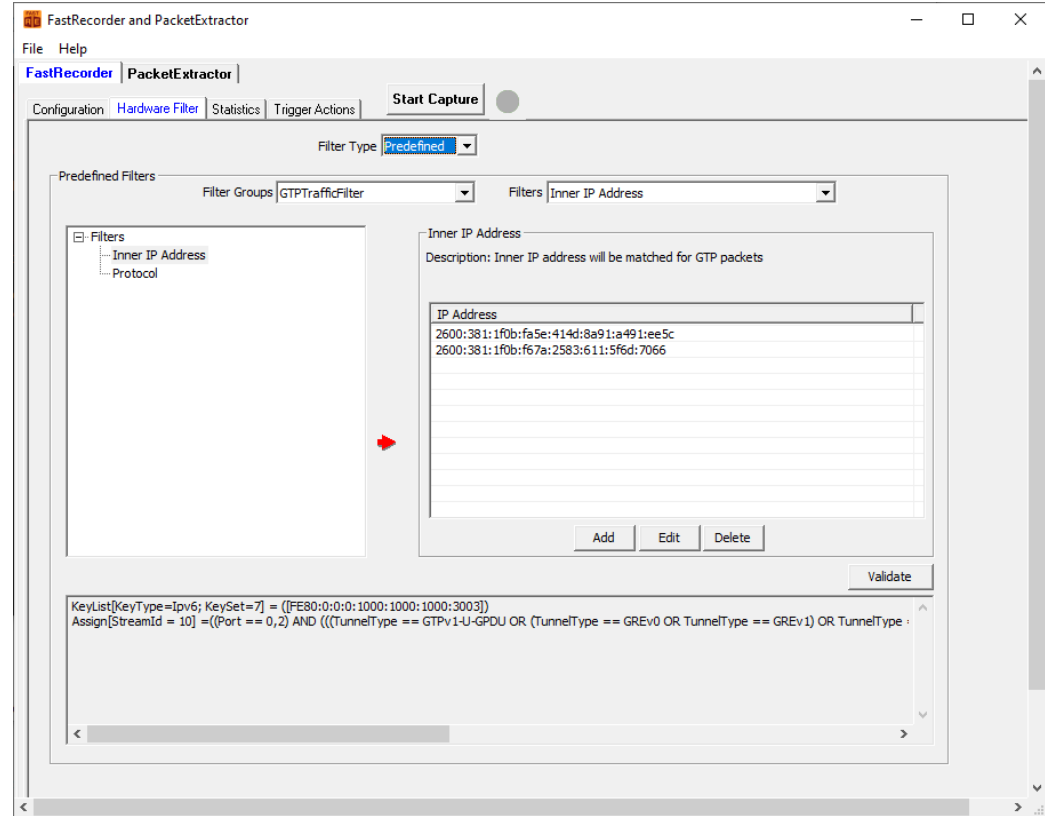
# Advanced Hardware Filter Type

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



# Predefined Hardware Filter Type

- User can also use **Predefined** hardware filters. These are custom defined filters
  - Application provides a framework to create custom filters as per requirements and group them
  - By default, it provides configurations for IP addresses and protocol combinations.
- Wherein user can configure IP address and protocol for the traffic of interest



# Custom Expression Filter

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

The screenshot displays the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, and the 'Hardware Filter' sub-tab is selected. The 'Filter Type' is set to 'Advanced'. A table lists several filters, with F4 (TCP Source Port == 443) highlighted. Below the table, a 'Custom Expression' is defined as '(f2 && f4) || f1'. The 'Validate & Update' button is highlighted, and a message 'Expression changed validate & update' is displayed. The interface also includes a list of filters on the left, a table of operators, and a list of predefined values.

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	IPLIST	Ip List	==		
F2	VLAN0	Tag Protocol ID	==	8100	
F3	UDP	Source Port	==	5060	
F4	TCP	Source Port	==	443	
F5	SCTP	Source Port	==	36412	

Custom Expression: (f2 && f4) || f1

Validate & Update

Expression changed validate & update

# FastRecorder™ Statistics

FastRecorder and PacketExtractor

File Help

**FastRecorder** | PacketExtractor

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

**Stop Capture** ● Capturing And Recording to Disk

View **List View** ▼ **Reset**

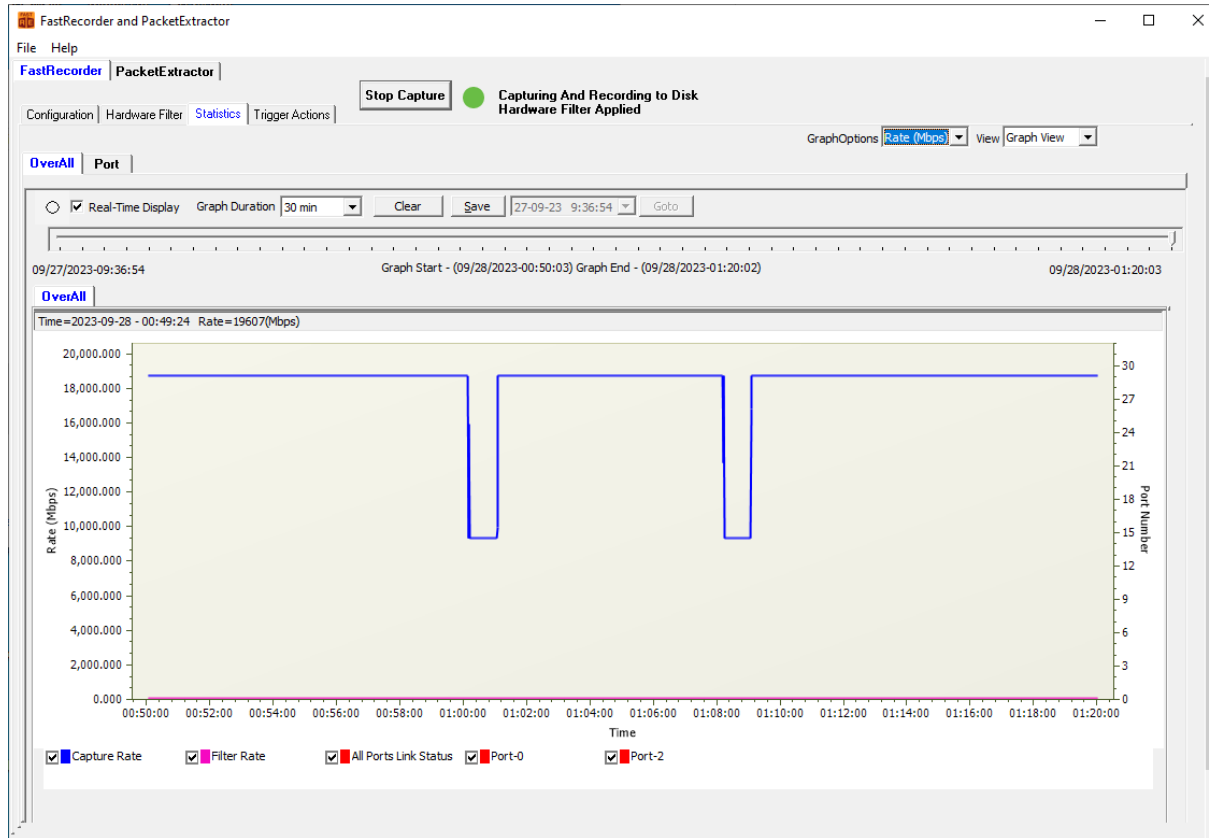
Statistics	Value
Filter Match Frames	58 447 757
Filter Not Match Frames	0
Total Frames	58 447 757
Filter Match Frames %	100.00
Dropped Frames (Due to Buffer Overflow)	0
Recorded Bytes (Gbytes)	15.0000
Capture Rate (Mbps)	10215.26
Filtered Rate (Mbps)	10205.14
Filtered Bytes %	100.00
Capture Frame Rate (Frames/Sec)	4 329 904
Filtered Frame Rate (Frames/sec)	4 329 904
Filtered Frames %	100.00
Record Duration (hr:min:sec)	00:00:12
Available Host Buffer Size (Kbytes)	20 971 520
Utilized Host Buffer Size (Kbytes)	1 328 389
Available OnBoard Memory Size (Mbytes)	7 682
Utilized OnBoard Memory Size (%)	0%
Utilized OnBoard Memory Size (Mbytes)	0
Drive Write Fail Count	0,0,0,0

# FastRecorder™ - Per Port and Aggregated Statistics

Port Statistics	Aggregate	Port-0 (10G)	Port-2 (10G)
Filter Match Frames	106 071 592	9 642 812	96 428 780
Filter Not Match Frames	0	0	0
Total Frames	106 071 592	9 642 812	96 428 780
Filter Match Frames %	100.00	100.00	100.00
Dropped Frames (Due To Port Buffer Ov...	0	0	0
Capture Rate(Mbps)	-	937.07	9370.22
Filtered Rate (Mbps)	-	937.07	9370.22
Port Link Status	-	Up	Up
Port Link Down Count	-	0	0
L1/L2 ERROR Counters:-			
L2 Drop Events	0	0	0
CRC	0	0	0
Alignment	0	0	0
Code Violation	0	0	0
Fragments	0	0	0
Jabbers	0	0	0
Collisions	0	0	0
FRAME-LENGTH Counters:-			
64 Byte	0	0	0
65-127 Byte	0	0	0
128-255 Byte	114 800	10 400	104 400
256-511 Byte	105 324 842	9 574 937	95 749 905
512-1023 Byte	517 050	47 025	470 025
1024-1518 Byte	114 900	10 450	104 450
1519-2047 Byte	0	0	0
2048-4095 Byte	0	0	0
4096-8191 Byte	0	0	0
8192-Max Byte	0	0	0
Undersized Frames	0	0	0
Oversized Frames	0	0	0
VLAN Frames	0	0	0
MPLS Frames	0	0	0
Temperature(C)	-	45.0	48.8
Stats Error Count			

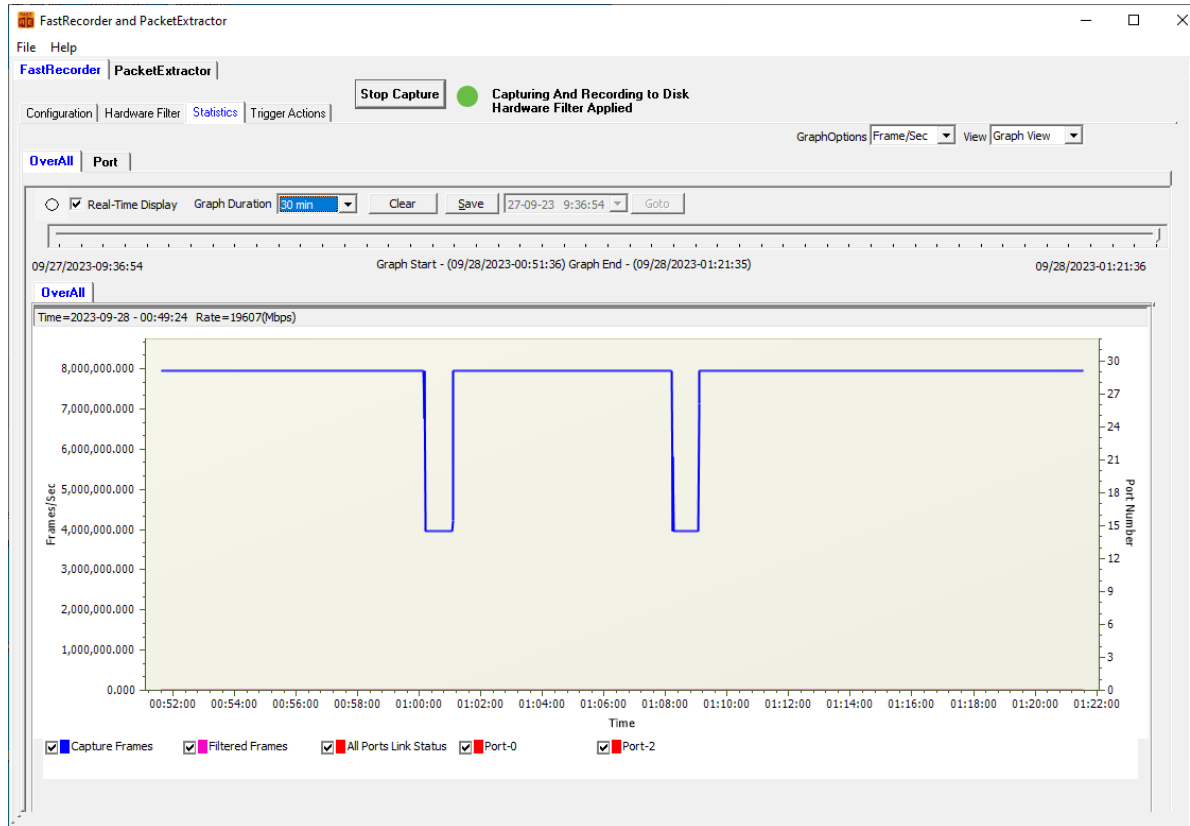
# Real time and Historical Graph

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



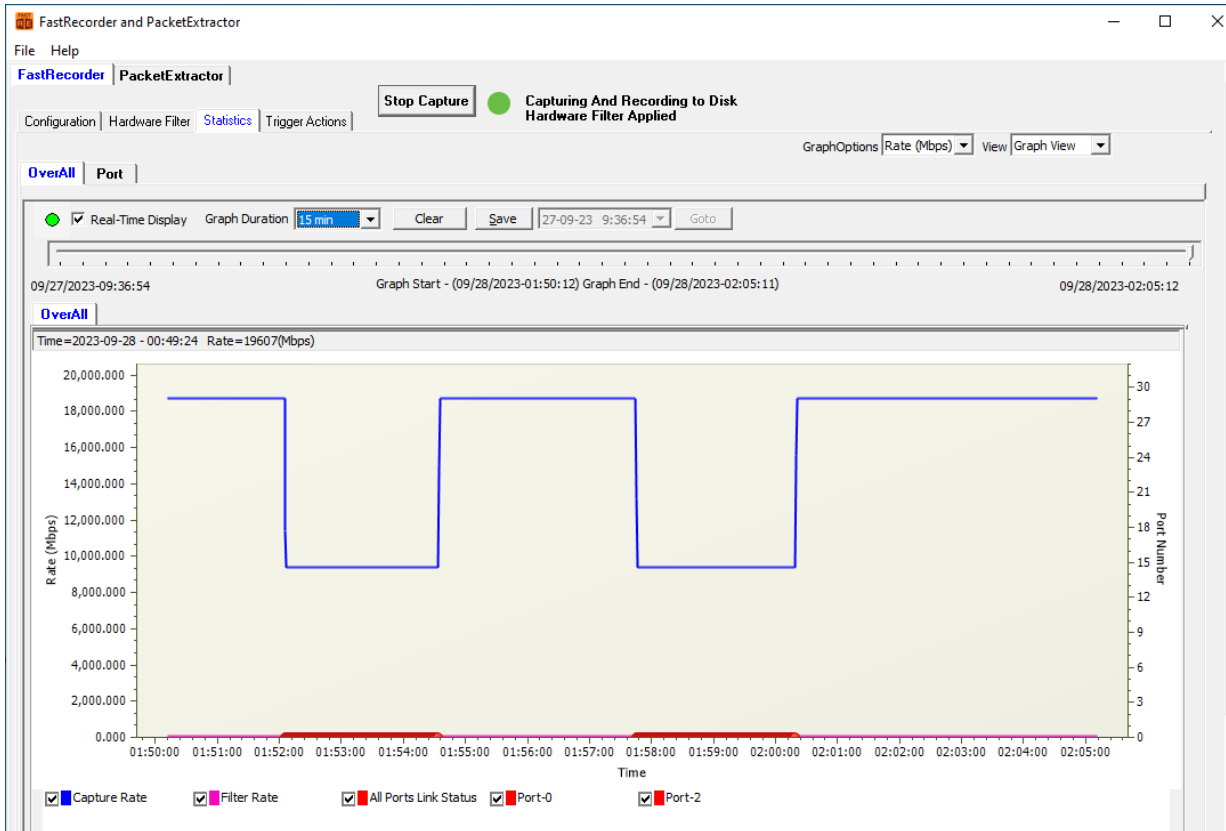
# Realtime and Historical Graph (Contd.)

- Overall capture and frame rate for Frame/Secs



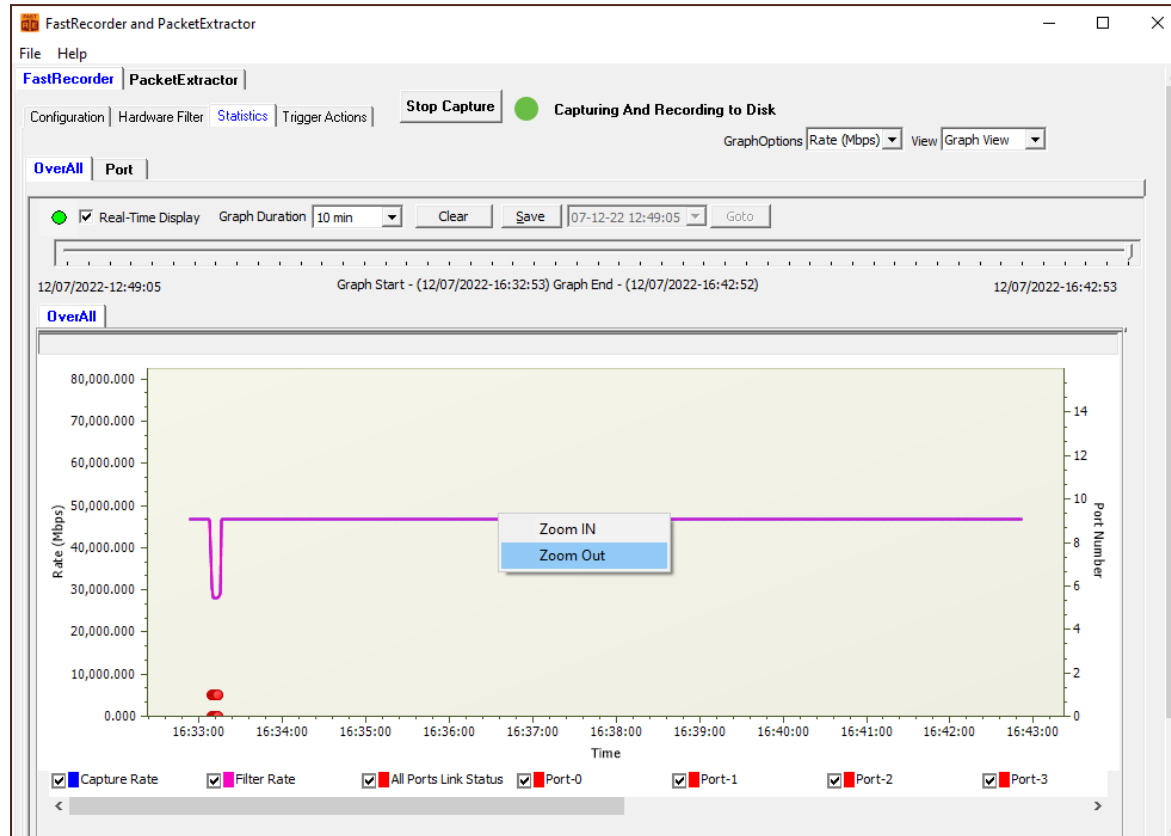
# Graphs - Port Link Down

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



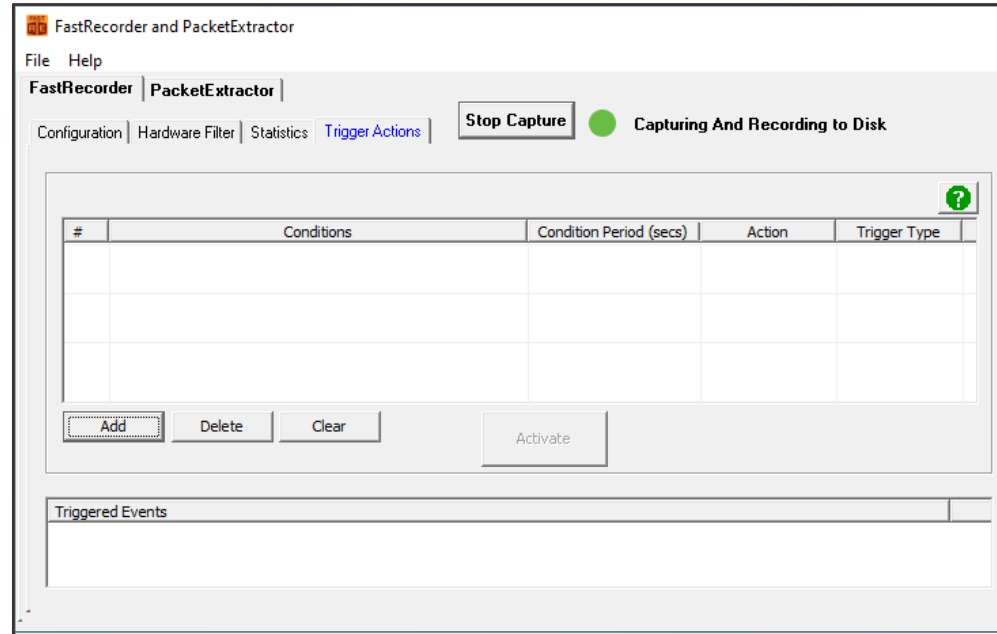
# Graphs - Zoom IN and Zoom Out

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



# Trigger based Start/Stop Recording

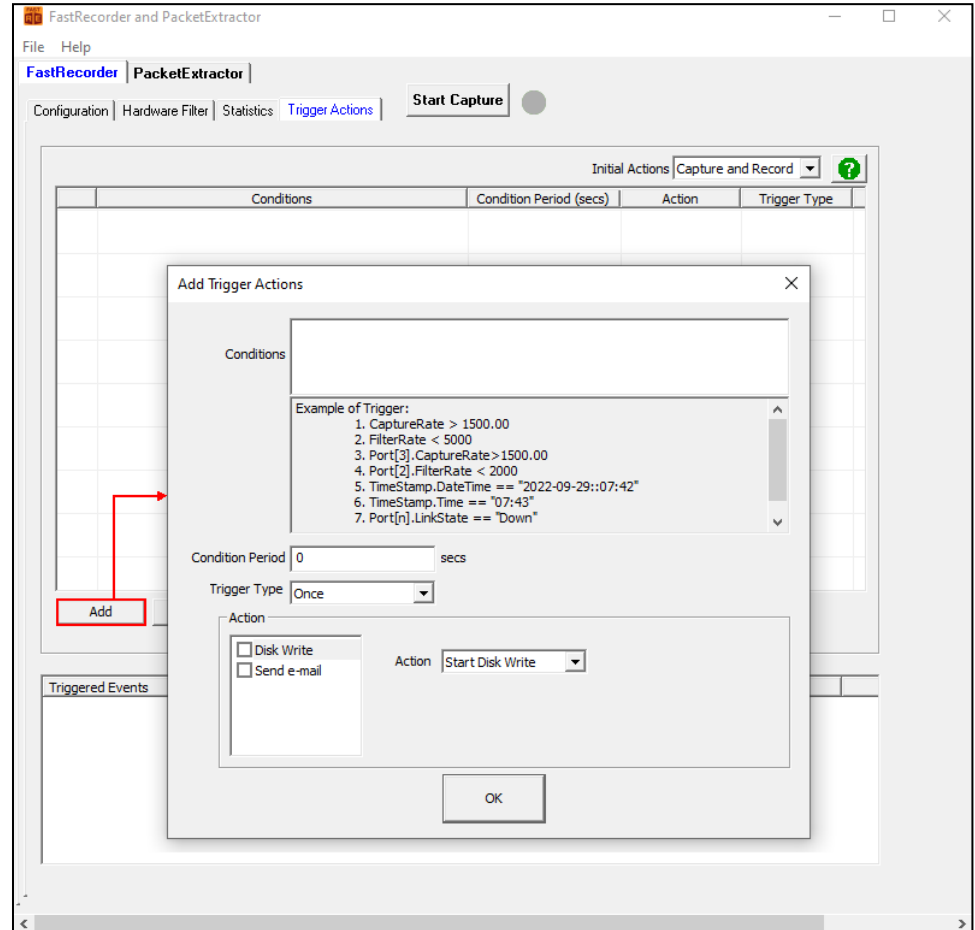
- User can specify the triggers to perform action based on the following conditions
  - CaptureRate (Mbps)
  - FilterRate (Mbps)
  - Port[n].CaptureRate (Mbps)
  - Port[n].FilterRate (Mbps): where n is port number
  - TimeStamp based



# Adding Trigger Actions

On the **Add Trigger Actions** window,

- Enter the **Conditions**
- Specify the **Condition period** in seconds
- From the Trigger Type drop-down list select **Once** or **Repeat** as required
- Under **Action** option, check **Disk Write** option
- From the Action drop-down list select **Start Disk Write** or **Stop Disk Write** option as required
- Click on **OK**



# Activated Trigger Actions

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

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'Trigger Actions' tab is active, displaying a table of configured triggers. The status bar at the top right indicates 'Capturing And Waiting for Trigger' with a yellow circle icon. Below the table are buttons for 'Add', 'Delete', 'Clear', and 'Deactivate'. At the bottom, a 'Triggered Events' log 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

Buttons: Add, Delete, Clear, Deactivate

Triggered Events Log:

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


# Activated Trigger Actions (Contd.)

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

Configuration Hardware Filter Statistics **Trigger Actions**

**Stop Capture**  **Capturing And Recording to Disk**

Initial Actions: Capture Only ?

#	Conditions	Condition Period (secs)	Action	Trigger Type
1	CaptureRate > 20480.00	10	Start Disk Write	Repeat
2	CaptureRate < 1000	10	Stop Disk Write	Repeat
3	TimeStamp.DateTime == "2022-11-15::01:35"	0	Start Disk Write	Once
4	TimeStamp.Time == "02:00"	10	Start Disk Write	Repeat
5	TimeStamp.Time == "06:00"	10	Stop Disk Write	Repeat

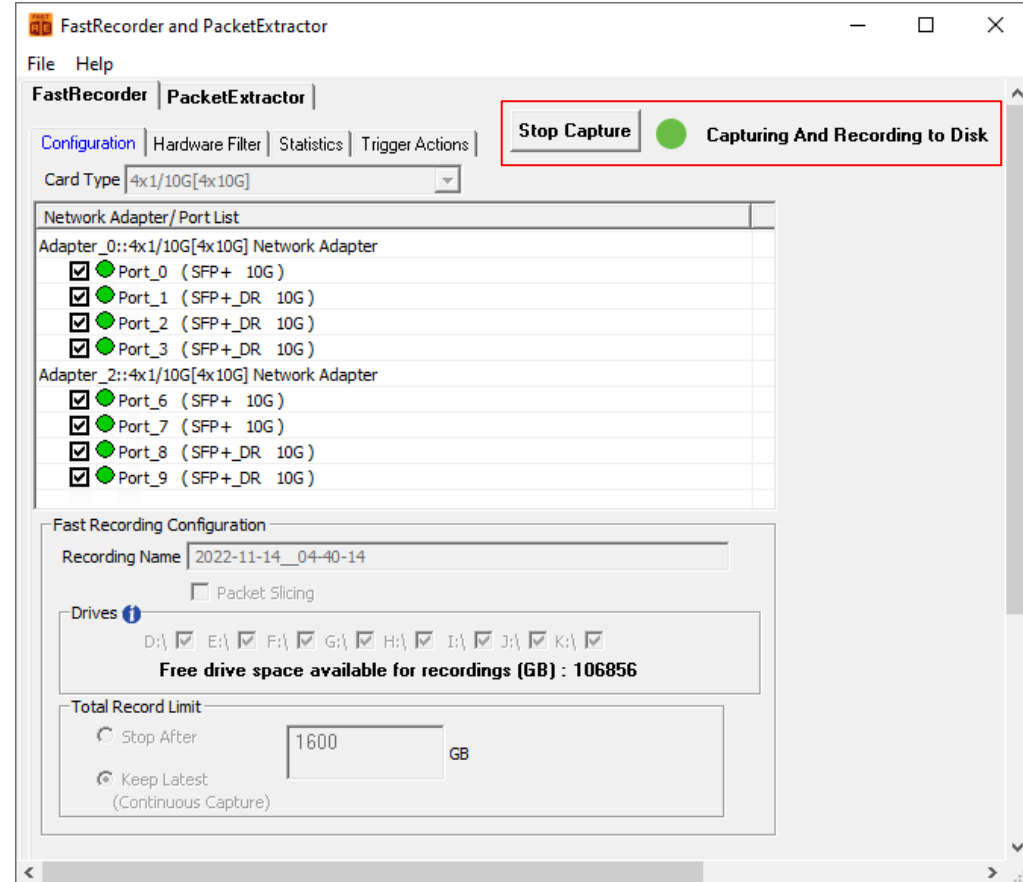
Add Delete Clear Deactivate

Triggered Events

- Triggered- Condition->"CaptureRate > 20480.00" Action->"Start Disk Write" TriggeredTime->11-15 1:34:17
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:31:23
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:30:41
- Triggered- Condition->"TimeStamp.DateTime == "2022-11-15::01:30"" Action->"Stop Disk Write" TriggeredTime->11-15 1:30:3
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:29:33
- Triggered- Condition->"CaptureRate < 1000" Action->"Stop Disk Write" TriggeredTime->11-15 1:28:25

# Recording with Default Name

- User can start the capture without specifying **Recording Name** for which current time is taken as recording name
- Network Adapter - Port List display SFP Types and negotiated rates



# PacketExtractor™

- PacketExtractor™ configuration settings allows to extract recorded files on the selected HD NIC interface port and required output file format to analyze the results for offline analysis

The screenshot shows the 'FastRecorder and PacketExtractor' application window. The 'PacketExtractor' tab is active, displaying various configuration options for extracting recorded data. The 'Recording Information' section shows the record name 'SIP\_GTP\_4PORTS', start time '2023-03-23 06:03:44', end time '2023-03-23 06:11:10', duration '00:07:26', and size '1 048 576.637 MB'. The 'PreExtraction Filter' section includes start and end time fields. The 'Limit Criteria' section has radio buttons for 'All', 'Duration' (selected), 'Extracted Size', and 'Extracted Packet Count', with a 'Limit Value' field set to '00:07:26'. The 'Port Filter' section has a 'Port' field set to '2'. The 'Extraction Filter' section includes an 'Operation' dropdown set to 'Packet Extraction', a checked 'Multiple Files' checkbox, and a 'Create New File After' field set to '1000 MB'. The 'Destination File Name' field is set to 'D:\ExtractTraffic.hdl'. The 'Start' and 'Stop' buttons are visible. The 'Statistics' section at the bottom shows the results of the extraction process.

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

Extractor Record Statistics

Select Recording

Recording Information

Record Name: SIP\_GTP\_4PORTS

Record Start Time: 2023-03-23 06:03:44 Record End Time: 2023-03-23 06:11:10

Record Duration: 00:07:26 Record Size: 1 048 576.637 MB

☐ PreExtraction Filter

Start Time: 06:03:44 End Time: 06:11:10 HH:MM:SS

Limit Criteria

☐ All ☒ Duration ☐ Extracted Size ☐ Extracted Packet Count

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

Recorded Ports: 0 2

☐ Port Filter

Port: 2

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

☐ Extraction Filter

Operation: Packet Extraction ☒ Multiple Files Create New File After: 1000 MB

Destination File Name: D:\ExtractTraffic.hdl

☐ Compress Extracted Files ☐ Packet Slicing

Start Stop

Statistics

Extraction completed.

Processed Frames = 3 538 141 432

Processed Bytes = 1 042 150 646 118

Extracted Frames = 3 538 141 432 ( 100.00 % )

Extracted Bytes = 1 042 150 646 118

Frames with FCS Error = 0

# Analysis of Extracted Traffic using PacketScan™

- The extracted files can be analyzed using **PacketScan™** application (For HDL file format, maximum file size of 10 GB or having less than 75 million frames is supported)

The screenshot displays the PacketScan (IpProt) HD 64-bit application interface. The top menu bar includes File, View, Capture, Statistics, Database, Call Detail Records, Configure, and Help. Below the menu is a toolbar with various icons for file operations, capture, and analysis. The main window is divided into two panes. The top pane shows a list of captured packets with columns for Device, Frame#, TIME (Date), Length (Bytes), Error, Length/Protocol Type, Packet Type, Destination IP Address, Source IP Address, Destination Address IPv6, Source Address IPv6, and Dest. The bottom pane shows a detailed view of the selected packet (Frame 1) with fields for Ethernet Frame Data, MAC Layer, IPv6 Layer, and UDP Layer.

Device	Frame#	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type	Packet Type	Destination IP Address	Source IP Address	Destination Address IPv6	Source Address IPv6	Dest
✓	2	0	2021-06-14 00:42:03.000000000		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	1	2021-06-14 00:42:03.273961364		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	2	2021-06-14 00:42:03.273961382		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	3	2021-06-14 00:42:03.273961407		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	4	2021-06-14 00:42:03.273961432		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	5	2021-06-14 00:42:03.273961460		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	6	2021-06-14 00:42:03.273961488		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	7	2021-06-14 00:42:03.273961512		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	8	2021-06-14 00:42:03.273961537		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	9	2021-06-14 00:42:03.273961559		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	10	2021-06-14 00:42:03.273961584		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	11	2021-06-14 00:42:03.273961609		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	12	2021-06-14 00:42:03.273961634		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	13	2021-06-14 00:42:03.273961665		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	14	2021-06-14 00:42:03.273961689		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	
✓	2	15	2021-06-14 00:42:03.273961714		294	IPv6			fe80:0000:0000:0000:9897:9897:9897:9899	fe80:0000:0000:0000:9897:9897:9897:9899	

Device2 Frame=1 at 2021-06-14 00:42:03.273961364 OK Len=294

Ethernet Frame Data

----- MAC Layer -----

0000 Destination Address = x000DE9066AA7

0006 Source Address = x000DE9066AA6

000C Length/Protocol Type = x86DD IPv6

----- IPv6 Layer -----

000E Protocol Version = 0110... (6)

000E Traffic Class = 0 (...0000 0000...)

000F Flow Label = 0 (...0000 00000000 00000000)

0012 Payload Length = 236 (x00EC)

0014 Next Header = 00010001 User Datagram Protocol (UDP)

0015 Hop Limit = 128 (x80)

0016 Source Address = fe80:0000:0000:0000:9897:9897:9897:9899

0026 Destination Address = fe80:0000:0000:0000:9897:9897:9897:9899

----- UDP Layer -----

0036 Source Port = 2152 (x0868)

0038 Destination Port = 2152 (x0868)

003A Length (Header + Data) = 236 (x00EC)

003C Checksum = x8648

Off-line Viewing [E:\Extracted\Extracted.hdl] 10 000 Frames

# Analysis of Filtered Traffic in Wireshark®

- The extracted files can be analyzed using Wireshark® application. (For PCAP file format, maximum file size of 5 GB or having less than 53 million frames is supported)

Extracted.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> + Window Update Duplicate Ack TCP Retx TCP Flags TCP Out of Order TCP Low Window TCP Handshake #1 TCP Handshake #2

No.	Time	Source	Destination	Protocol	Stream index	TCP Len
1	03:59:01.000000000	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
2	03:59:01.525264717	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
3	03:59:01.525265542	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
4	03:59:01.525266035	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
5	03:59:01.525266886	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
6	03:59:01.525267385	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
7	03:59:01.525268589	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
8	03:59:01.525269062	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
9	03:59:01.525269581	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
10	03:59:01.525270374	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
11	03:59:01.525271053	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
12	03:59:01.525540064	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
13	03:59:01.525540883	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
14	03:59:01.525541696	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		
15	03:59:01.525542189	fe80::64da:3cd4:cff1:9e96	fe80::10f8:316d:9afd:4398	GTP <SIP>		
16	03:59:01.525543033	fe80::10f8:316d:9afd:4398	fe80::64da:3cd4:cff1:9e96	GTP <SIP>		

<

> Frame 7: 1482 bytes on wire (11856 bits), 1482 bytes captured (11856 bits) on interface unknown, id 5

> Ethernet II, Src: IntelCor\_85:1a:ff (a0:36:9f:85:1a:ff), Dst: IntelCor\_02:32:62 (a4:bf:01:02:32:62)

> Internet Protocol Version 6, Src: fe80::64da:3cd4:cff1:9e97, Dst: fe80::64da:3cd4:cff1:9e96

> User Datagram Protocol, Src Port: 2152, Dst Port: 2152

> GPRS Tunneling Protocol

> Internet Protocol Version 6, Src: fe80::10f8:316d:9afd:4398, Dst: fe80::64da:3cd4:cff1:9e96

> User Datagram Protocol, Src Port: 5060, Dst Port: 5060

> Session Initiation Protocol (INVITE)

Frame (frame), 1,482 bytes

Packets: 100

# Recorded Statistics in PacketExtractor™

FastRecorder and PacketExtractor

File
Help

FastRecorder

PacketExtractor

Extractor

Record Statistics

Select Recording

View

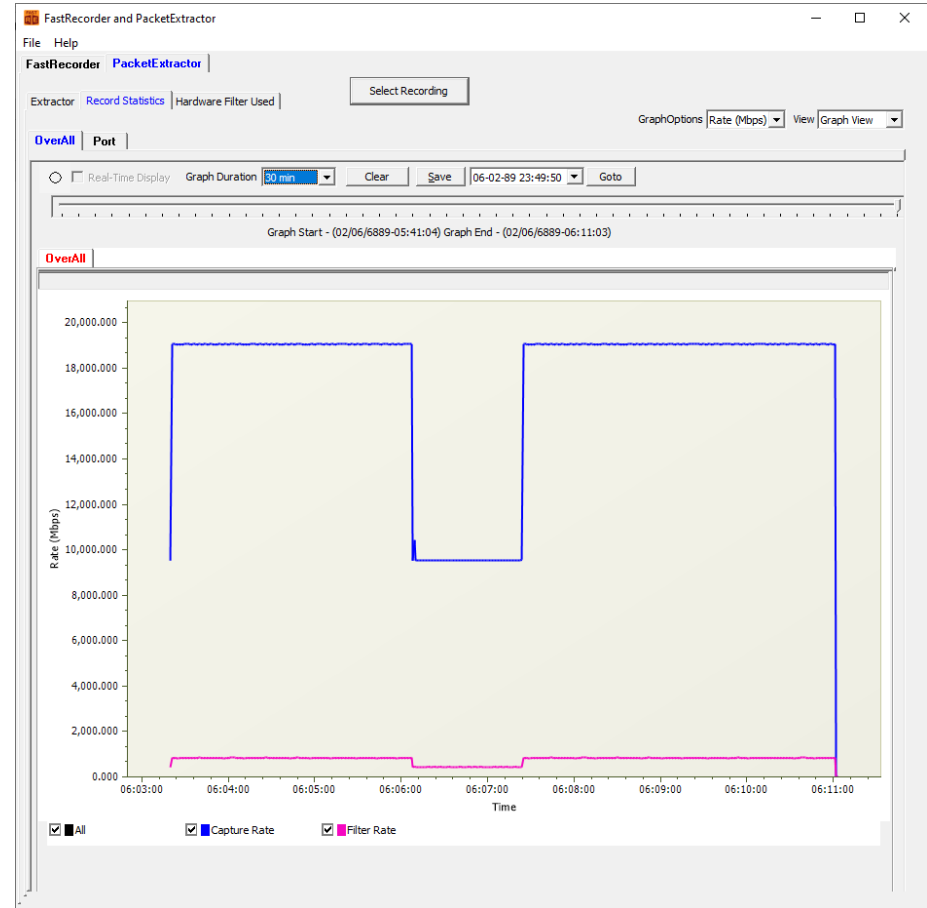
List View

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

Port Statistics	Aggregate	Port-0	Port-2	Port-2
Filter Match Frames	352 851 674	32 077 822	320 773 852	320 773 852
Filter Not Match Frames	0	0	0	0
Total Frames	352 851 674	32 077 822	320 773 852	320 773 852
Filter Match Frames %	100.00	100.00	100.00	100.00
Dropped Frames (Due To Port Buffer Ove...	0	0	0	0
Port Link Status	-	Up	Up	Up
Port Link Down Count	0	0	0	0
L1/L2 ERROR Counters:-				
L2 Drop Events	0	0	0	0
CRC	0	0	0	0
Alignment	0	0	0	0
Code Violation	0	0	0	0
Fragments	0	0	0	0
Jabbers	0	0	0	0
Collisions	0	0	0	0
FRAME-LENGTH Counters:-				
64 Byte	0	0	0	0
65-127 Byte	0	0	0	0
128-255 Byte	382 150	34 750	347 400	347 400
256-511 Byte	350 367 974	31 852 222	318 515 752	318 515 752
512-1023 Byte	1 719 450	156 150	1 563 300	1 563 300
1024-1518 Byte	382 100	34 700	347 400	347 400
1519-2047 Byte	0	0	0	0
2048-4095 Byte	0	0	0	0
4096-8191 Byte	0	0	0	0
8192-Max Byte	0	0	0	0
Undersized Frames	0	0	0	0
Oversized Frames	0	0	0	0
VLAN Frames	0	0	0	0
MPLS Frames	0	0	0	0
Temperature(C)	0	45.9	49.6	49.6
XTPNotificationSinkMTOnEvent				

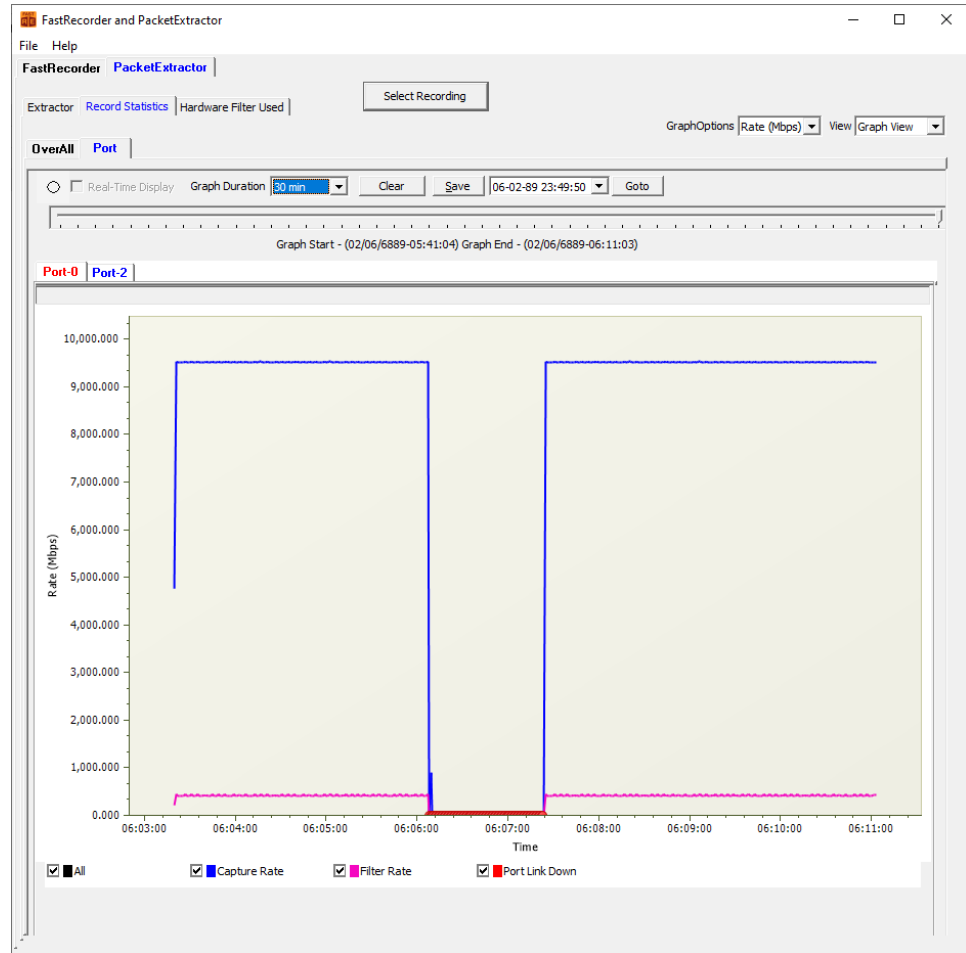
# PacketExtractor™ - Overall Graph View

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



# PacketExtractor™ - Port View

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



# Packet Extraction from the Recordings with Filter

The screenshot displays the FastRecorder and PacketExtractor application interface. The main window is titled "FastRecorder and PacketExtractor" and has a menu bar with "File" and "Help". Below the menu bar, there are tabs for "FastRecorder" and "PacketExtractor", with "PacketExtractor" currently selected. A "Select Recording" button is located at the top right of the main window.

The "PacketExtractor" tab contains several sections:

- Recording Information:** Shows "Record Name: SIP\_GTP\_4PORTS", "Record Start Time: 2023-03-24 07:46:57", and "Record Duration: 00:07:26".
- PreExtraction Filter:** Includes a "Start Time" field set to "07:46:57" and an "End Time" field set to "07:54:00". A red arrow points from the "End Time" field to the "Filter Configuration" button.
- Limit Criteria:** Includes radio buttons for "All", "Duration", "Extracted Size", and "Extracted Packet Count". The "Duration" option is selected, and a "Limit Value" field is set to "00:07:26".
- Extraction Filter:** Includes a checked "Extraction Filter" checkbox, a "Filter Configuration" button, and a "Destination File Name" field.
- Operation:** Includes a dropdown menu set to "Packet Extraction" and a "Multiple" checkbox.
- Compress Extracted Files:** Includes a checkbox.
- Start:** A button to initiate the extraction process.

A "Protocol Capture Configuration" dialog box is open in the foreground, showing a list of protocols under the "Filter Selection" section. The list includes: Protocol, MAC, VLAN, IP (All Levels), IP (Outer), ESP, TCP, UDP, Inner IP, Inner UDP, SCTP, SIP, RTP, MSRP, MGCP, MEGACO, H323, and RTSP. The "Include" radio button is selected. To the right of the protocol list, there is a "Filter Selected Protocols" section with a "Select All Protocols" checkbox and a list of protocols: ARP, GTP-C, ICMP, LDAP, PTP, SLOW, UDP, DIAMETER, GTP-U, IPV4, LLDP, SCTP, SNMP, DNS, HTTP, IPV6, MEGACO, SIP, and TCP. A "Configure Protocols List" button is located below the list. At the bottom of the dialog, there are "Deactivate Sel" and "Deactivate All" buttons.

# Specifying End Time for Packet Extraction

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

Select Recording

Extractor Record Statistics

Recording Information

Record Name: SIP\_GTP\_4PORTS

Record Start Time: 2023-03-23 06:03:44 Record End Time: 2023-03-23 06:11:10

Record Duration: 00:07:26 Record Size: 1 048 576.637 MB

☐ PreExtraction Filter

Start Time 06:03:44 End Time ☒ 06:11:10 HH:MM:SS

Limit Criteria

☒ All Limit Value

☐ Duration 0

☐ Extracted Size

☐ Extracted Packet Count

Recorded Ports: 0 2

☐ Port Filter

Port

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

☐ Extraction Filter

Operation Packet Extraction ☐ Multiple Files

Destination File Name D:\Extract-w-Endtime.hdl

☐ Compress Extracted Files ☐ Packet Slicing

Start Stop

Statistics

Extraction completed.

Processed Frames = 1 015 316 480

Processed Bytes = 299 058 914 135

Extracted Frames = 1 015 316 480 ( 100.00 % )

Extracted Bytes = 299 058 914 135

Frames with FCS Error = 0

# Hardware Filter Used while Recording

FastRecorder and PacketExtractor

File Help

FastRecorder PacketExtractor

Extractor | Record Statistics | Hardware Filter Used | Select Recording

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	==		
F2	VLANID	Tag Protocol ID	==	8100	
F3	UDP	Source Port	==	5060	
F4	TCP	Source Port	==	443	
F5	SCTP	Source Port	==	36412	

Add Insert Delete Clear All Tunnel Type: GTP, GRE, VXLAN Update

☒ Custom Expression

(F2 && F3) || F1 Validate & Update

Selected Filter Expression

```
KeyList[KeyType=Ipv4; KeySet=6] = ([192.168.13.187])
Assign[StreamId = 10] = (((mVlan0TPID == 0x8100) AND (mUdpSrcPort == 5060)) OR (((TunnelType == GTPv1-U-GPDU OR (TunnelType == GREv0 OR TunnelType ==
```

< >

Final Configured Expressions | Final Applied Expressions

```
KeyList[KeyType=Ipv4; KeySet=6] = ([192.168.13.187])
Assign[StreamId = 10] = (((mVlan0TPID == 0x8100) AND (mUdpSrcPort == 5060)) OR (((TunnelType == GTPv1-U-GPDU OR (TunnelType == GREv0 OR TunnelType == GR
```

< >

Clear All Filters

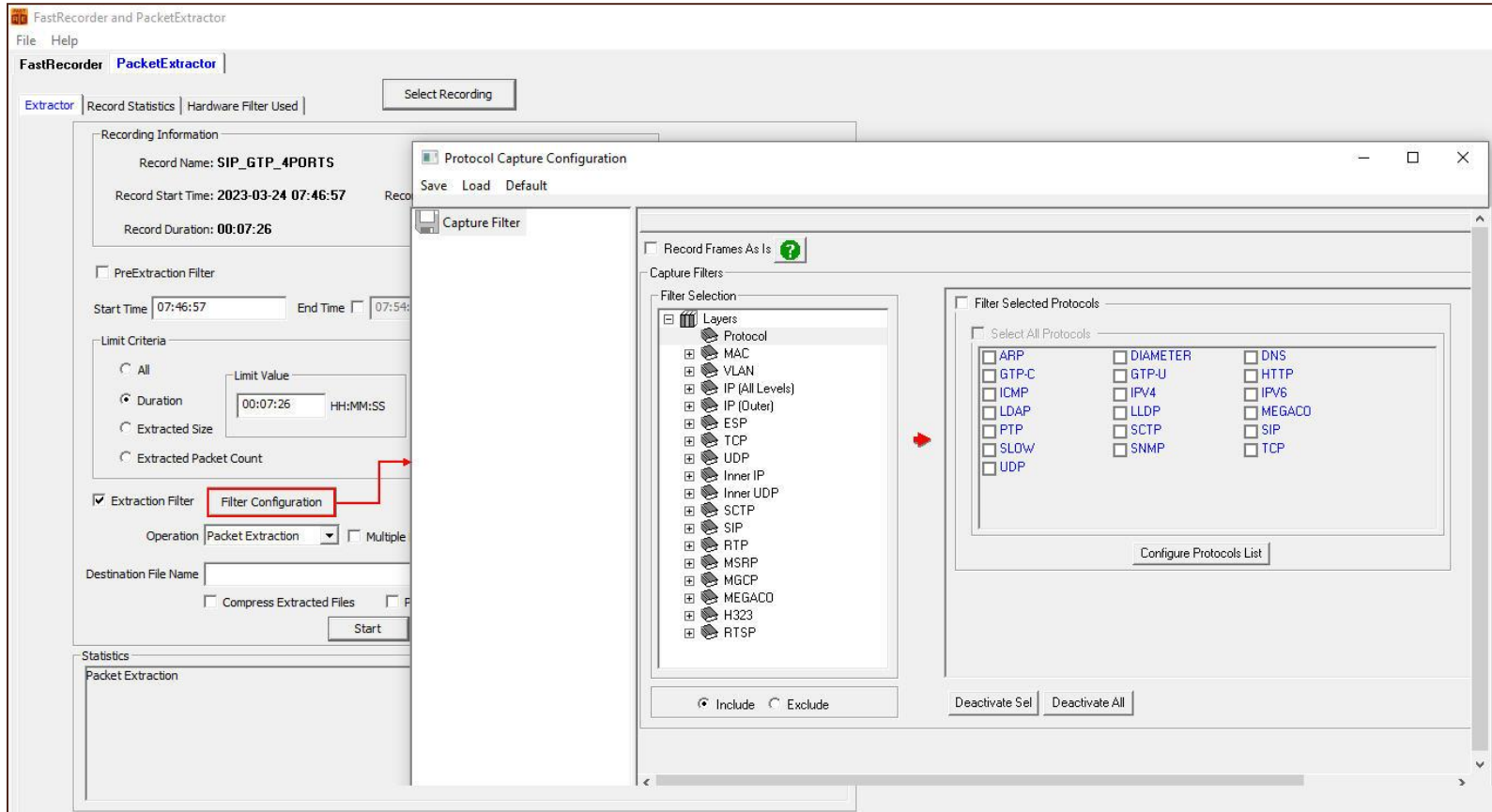
IP List Type: IP Address List IP Layer Type: Inner Tunnel1 / Outer Non Tunnel

IP Address

192.168.13.187

Add Edit Delete

# eCPRI Analysis



# View eCPRI Layer Decode Details in PacketScan™

## Over UDP

- From the desktop, invoke **PacketScan™** analyzer
- Goto **File** → **Offline**, browse and select any one of the extracted \*.hdl file from the **D:\Extracted\** folder. Click on **Open**
- Observe the **eCPRI** layer decode details as shown

```
Device0 Frame=6 at 2022-06-09 06:07:36.711206000 OK Len=112 *** Right c
Ethernet Frame Data
===== MAC Layer =====
0000 Destination Address      = xFCA149225C4
0006 Source Address          = x54BEF737CB9A
000C Length/Protocol Type    = x86DD IPv6
===== IPv6 Layer =====
000E Protocol Version        = 0110.... (6)
000E Traffic Class           = 0 (....0000 0000....)
000F Flow Label              = 834513 (....1100 10111011 11010001)
0012 Payload Length          = 58 (x003A)
0014 Next Header              = 00010001 User Datagram Protocol (UDP)
0015 Hop Limit                = 64 (x40)
0016 Source Address           = fe80::64f2:5e84:f1db:502
0026 Destination Address     = fe80::589e:b2d5:9074:2bec
===== UDP Layer =====
0036 Source Port              = 64000 (xFA00)
0038 Destination Port        = 64000 (xFA00)
003A Length (Header + Data)   = 58 (x003A)
003C Checksum                 = x7F76
===== eCPRI Layer =====
003E C                        = .....0 eCPRI message is the last one inside the eCPRI PDU
003E eCPRI Protocol Revision = 0001.... (1)
003F eCPRI Message Type       = 00000100 Remote Memory Access
0040 eCPRI Payload Size       = 28 (x001C)
0042 Remote Memory Access ID  = 17 (x11)
0043 Req/Resp                  = ....0010 Failure
0043 Read/Write                = 0010.... Write_No_Resp
0044 Element ID               = 8755 (x2233)
0046 Address                   = x050403020100
004C Length                   = 16 (x0010)
User Data                     = xFFEEDDCCBBAA99887766554433221100
```

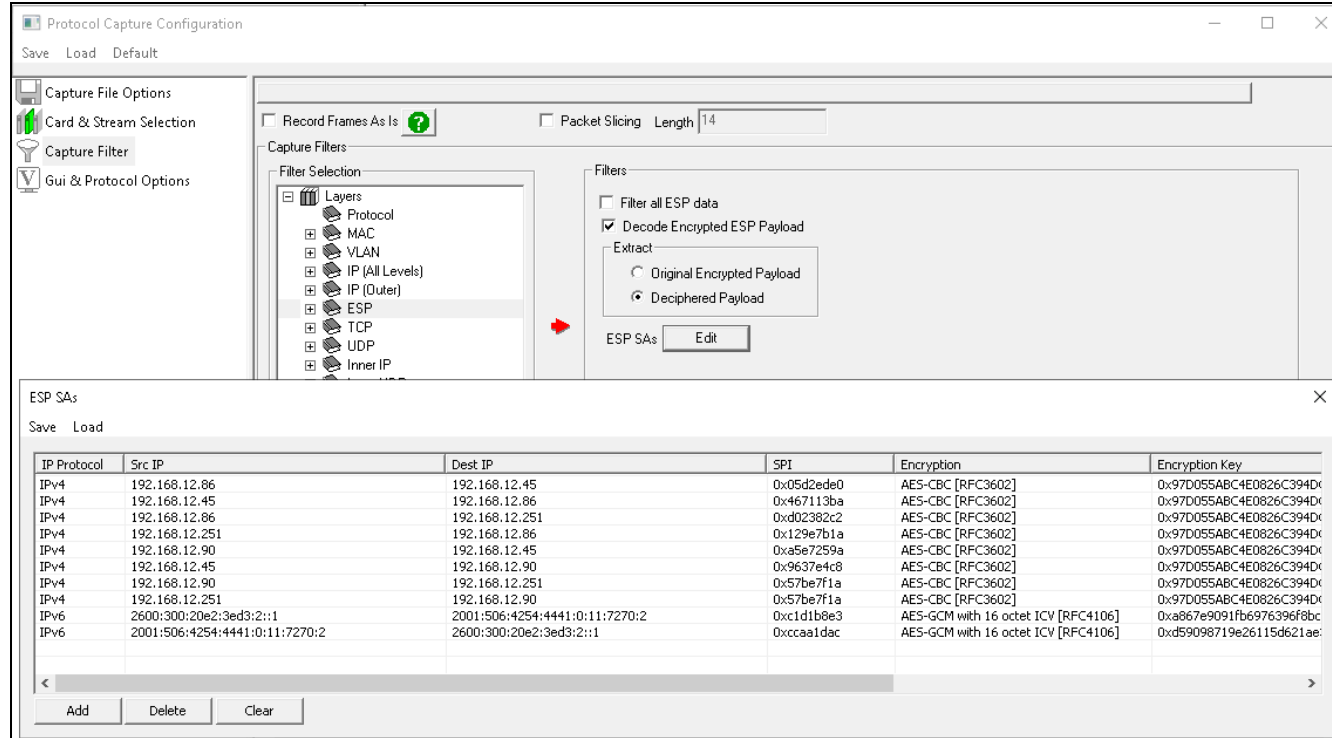
# View eCPRI Layer Decode Details in PacketScan™ (Contd.)

## Over MAC

```
Device0 Frame=0 at 2019-02-13 11:36:46.0000000000 OK Len=64 *** Right
Ethernet Frame Data
===== MAC Layer =====
0000 Destination Address      = x008016000000
0006 Source Address          = x008016884EFF
000C Length/Protocol Type    = xAEFE eCPRI
===== eCPRI Layer =====
000E C                        = .....0 eCPRI message is the last one inside the eCPRI PDU
000E eCPRI Protocol Revision = 0001.... (1)
000F eCPRI Message Type      = 00000000 IQ Data
0010 eCPRI Payload Size      = 20 (x0014)
    eCPRI Payload             = x123487650F0E0D0C0B0A09080706050403020100
===== O-RAN Fronthaul CUS Layer =====
    ecprid
0012 BandSector_ID           = ..010010 (18)
0012 DU_Port_ID              = 00..... (0)
0013 RU_Port_ID              = ....0100 (4)
0013 CC_ID                   = 0011.... (3)
    ecprisecid
0014 Sequence ID             = 135 (x87)
0015 Subsequence ID          = .1100101 (101)
0015 E bit                    = 0..... More fragments follow
0016 FilterIndex              = ....1111 Reserved
0016 payloadVersion           = .000.... (0)
0016 dataDirection            = 0..... UpLink
0017 frameId                  = 14 (x0E)
0018 subframeId               = 0000.... (0)
0018 slotId                   = 52 (....1101 00.....)
0019 startSymbolId            = ..001100 (12)
001A sectionId                = 176 (00001011 0000....)
001B symInc                   = .....0.. use the current symbol number
001B rb                       = ....1... every other RB used
001B startPrbu                = 521 (.....10 00001001)
001D numPrbu                  = 8 (x08)
    udCompHdr
001E udCompMeth               = ....0111 Reserved
001E udIqWidth                = 0000.... I and Q are each 16 bit wide
    Dump                       = x050403020100
```

# Encapsulated Security Payload (ESP) Deciphering

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



**Thank you**