PacketScan™ High Density All-IP Analyzer (1, 10, 25, 40, or 100 GigE Networks)

PacketScan™ HD All-IP Signaling and Traffic Analysis (2G/3G/4G/5G/VoIP/RTP, RTCP/Fax Analysis)
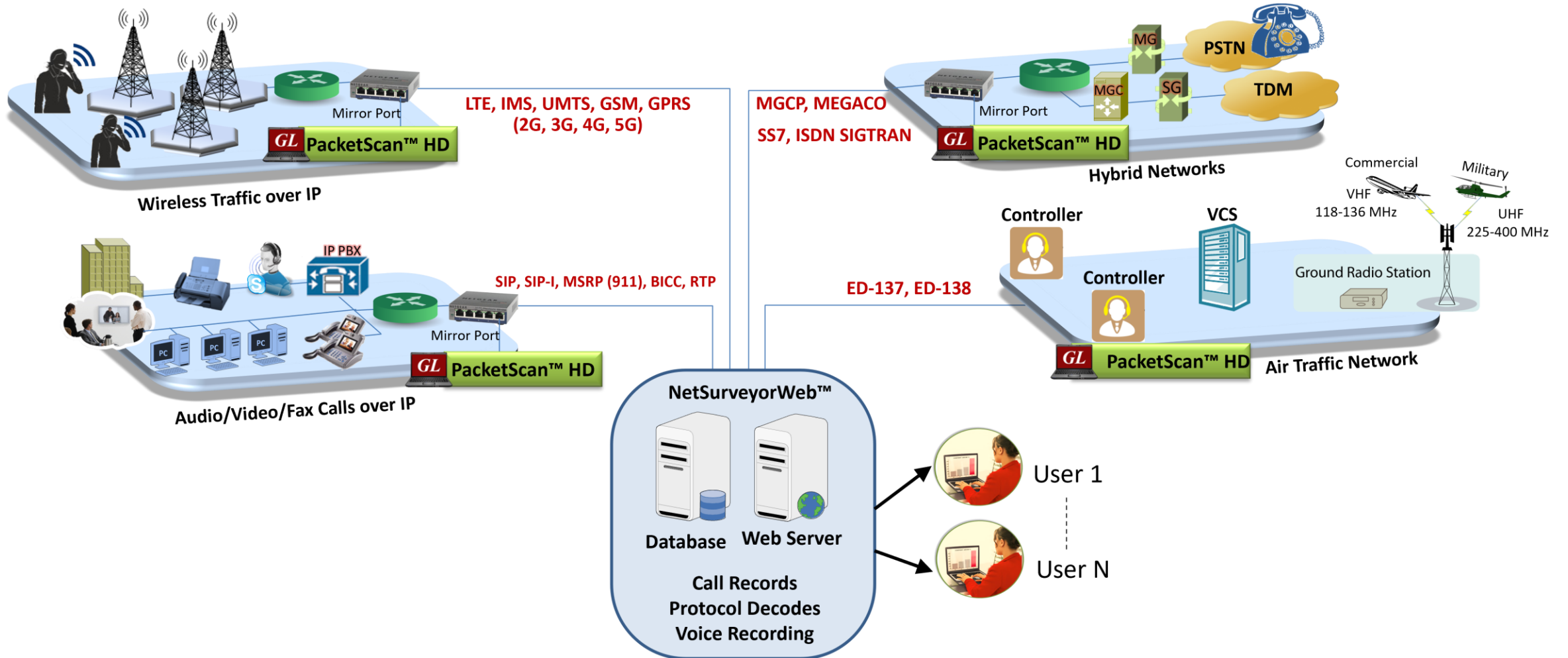
PacketScan™ HD Features

- **Signaling** – Protocol analysis: SIP, MGCP, MEGACO, H.323, SCTP, SCCP (Skinny), SS7 SIGTRAN, ISDN-SIGTRAN, GSM A over IP, GPRS over IP, UMTS over IP, LTE, Diameter

- **Voice/Fax** - Captures, segregates, and monitors packets; perform voice quality testing in real-time over VoIP network. G.711, G726, GSM, GSM EFR, GSM HR, G729/B, G.722, G.722.1, ILBC, SPEEX, SMV, T.38

- **Video Calls** - Video quality statistics such as MDI (Media Delivery Index), Packet Lost, Duplicate, out of sequence and Frame Rates are provided for each video session

- **5G Analyzer** - Captures, decodes, and collects statistics over N1N2, N4, N8, N12 and N13 interfaces of the 5G network

- **NetSurveyorWeb** - Can be deployed as a Probe for a centralized monitoring system connected to an Oracle database

Why this product?

- 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 at nano-second time precision

- Filter on inner layer of GTP tunnel traffic like inner IPv4/IPv6 addresses

- Ability to capture and analyse high volume calls with traffic. Process up to 20000 simultaneous calls with bidirectional RTP traffic. Up to 50,000 calls can be achieved by scaling with higher configurations

- PacketScan™ HD available in both Portable as well as 2U rack mounted Network Monitoring Appliance w/ 4x 1GigE (PKV120) or 2x 10GigE (PKV122) network interface cards

- Create up to 10 user defined hardware filters to filter-out traffic based on MAC, 802.1Q (VLANs), IPv4, TCP, UDP, SIP, and RTP parameters

- Supports almost all industry standard IP and Wireless Protocols (from SIP to LTE)

- Supports all RTP traffic – Voice, Video, Fax T.38, Digits, Tones, Impairments

- Capture and Call processing is enhanced to handle different Tunnel traffic (VXLAN, GRE and GTP) and multiple tunnelling

- Support for eCPRI decode

GL Communications

Key Features

- User can create their own filters using custom filter option which provides flexibility to check the fields and use the logical conditions more efficiently

- Supports decoding of eCPRI protocol

- Long-Term activity reporting

- Captures, Segregates, Monitors, Build CDRs, and Collects Statistics on all IP calls

- In-depth real-time and post-process data investigation using Packet Data Analysis (PDA) feature

- Complex Filtering and Search capabilities to record all or filtered traffic into a trace file

- Supports TCP Analytics application analyzes TCP connections between both internal Local Area Network (LAN) and external Wide Area Network (WAN) computers including servers and clients. The application helps troubleshoot large bandwidth consumption, failed TCP sessions, packet loss, poor TCP throughput and more

- Provides Call Quality Scores like MOS, R-Factor, Delay, Jitter, Packet Loss and more

- Supports Centralized Remoter Network Monitoring with NetSurveyorWeb™ - a web-based client that can connect to PacketScan™ probes through a web server that facilitates display of call data records using a web interface

Supported Protocols and Codecs

Supported Codecs	Supported Protocols
• G.711 A/µ-law • G.722, G.722.2 (AMR-WB), G.722.1, G.726, G.729A/B • GSM (EFR, FR and HR) • AMR (Narrowband and Wideband) • EVRC, EVRCB, EVRC-C, iLBC, Speex, SpeexWB, RFC 2833, and user-defined codecs for voice and tones. • EVS OPUS Visit Voice Codec webpage for more details	• SIP, SIP-I, SIP-T, H.323, MEGACO, MGCP, Diameter, Skinny (SCCP) • LTE • 5G N1N2, N4, N12, N13 • SIGTRAN – SS7, ISDN • GSM A and Abis over IP • GPRS Gb and Gn over IP • UMTS IuCS and IuPS over IP • T.38 Fax and Video calls Visit Supported Protocols for more details

For more information on other features, refer to PacketScan™ Basic (PKV100) presentation.

PacketScan™ HD
(4x1 GigE, 2x1/10 GigE, 2x25 GigE, 8x10 GigE, and 2x40/100 GigE)

2x40/100 GigE

PacketScan™ HD

**Also available as a rack mounted unit

PacketScan™ HD with 2 x 25/40/100 GigE or 8 x 10 GigE

2x40/100 GigE

8X10 GigE

Smart Switch with monitor ports
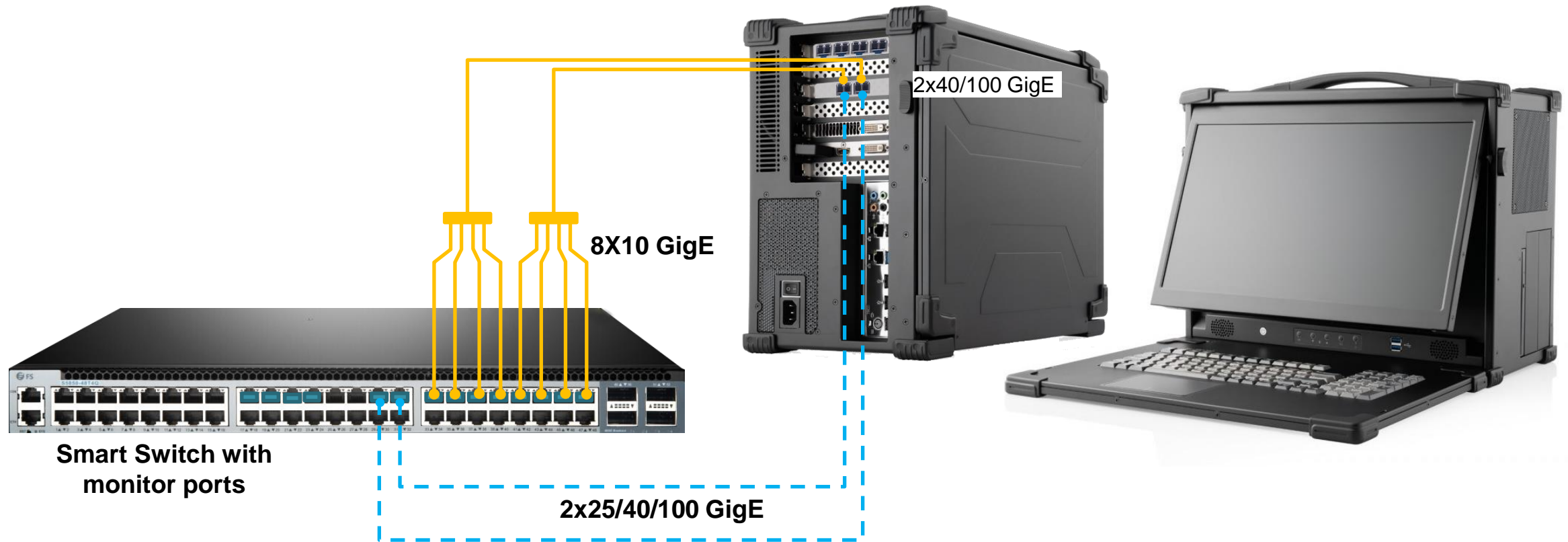
2x25/40/100 GigE

The above setup could manage rates as below:

- 2 x 25/40/100 GigE card can also be used as 8 x 10 GigE (with Breakout)
- System can also be outfitted with multiple cards with easy switching

PacketScan™ HD 2U Rack Appliance

Front Panel

PacketScan™ HD Hardware + Software
4 or 8 x1G / 2x1/10G / 2x25G / 2x40G / 2x100G

Back Panel

PacketScan™ HD Systems

- PacketScan™ HD appliance is also available in three systems "**Low End**", **"Medium End"** and "**High End**"

	Low End	Medium End	High End
Data Rate	4x1GigE	4x1/10GigE Or 2x1/10GigE	8x10GigE, 2x10/25GigE, 2x40GigE, 2x100GigE
RAM	16 GB RAM	32 GB RAM	128 GB RAM
NVME Storage [SSD]	2 TB	4x SSDs user configurable disk size (4x 1.92 TB in the base configuration)	8x SSDs user configurable disk size (8x 3.84 TB in the base configuration)

High Density Traffic
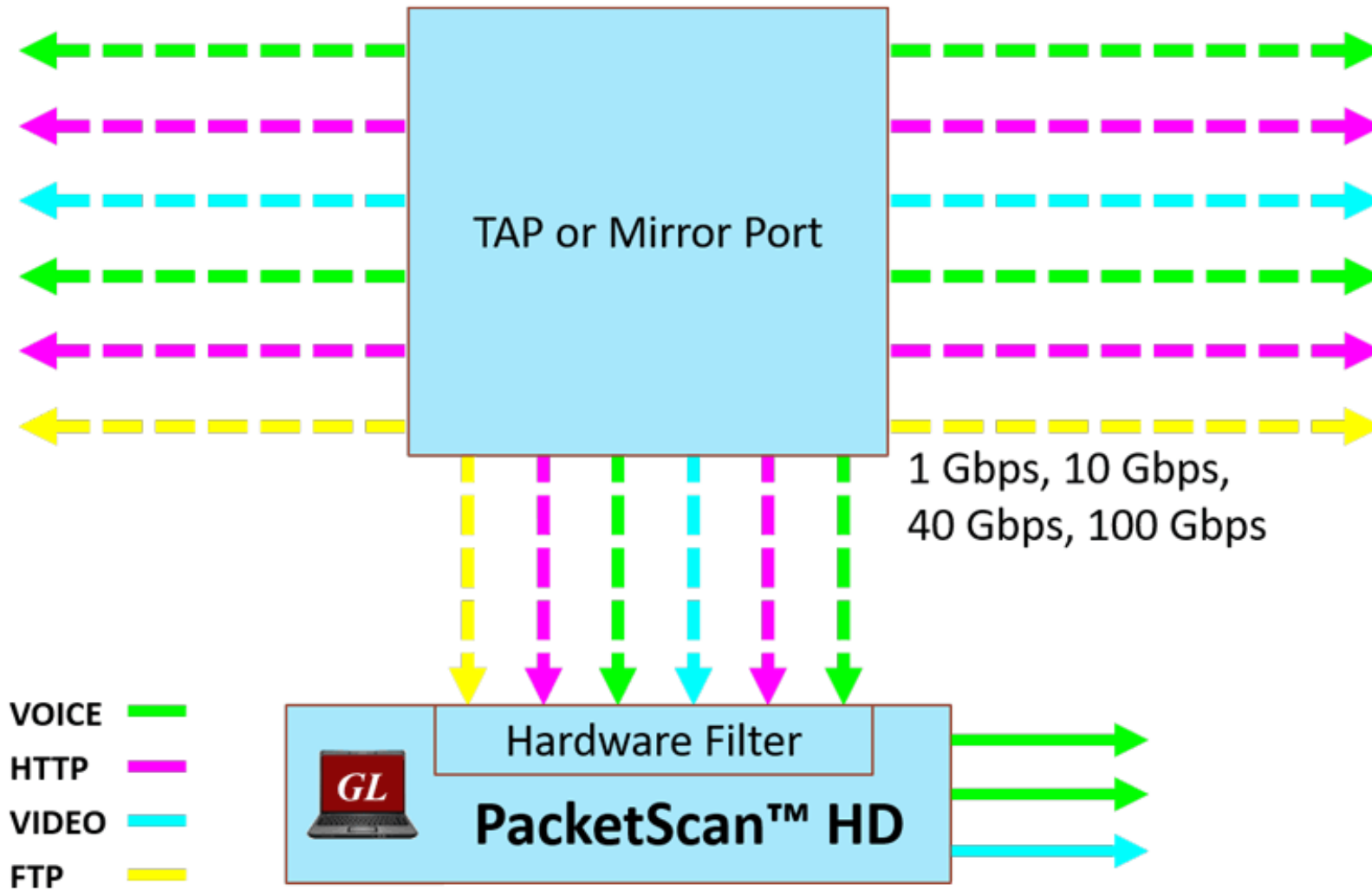
RTP Traffic Capabilities and Performance

Product Version	Max Simultaneous Calls
	Signaling + RTP Voice Traffic
PacketScan 1G (4x 1GigE) SIP 64-bit	20000 calls with bi-directional RTP traffic Extracting/recording voice 2500 simultaneous calls (maximum) - Option to record filtered calls of interest only
PacketScan 10G (2x 10GigE) SIP 64-bit	30000 calls with bi-directional RTP traffic Extracting/recording voice 2500 simultaneous calls (maximum) - Option to record filtered calls of interest only

** The above performance is evaluated on a high-end Core i7 system with typical 12GB RAM

GL

Communications

Wirespeed Filtering
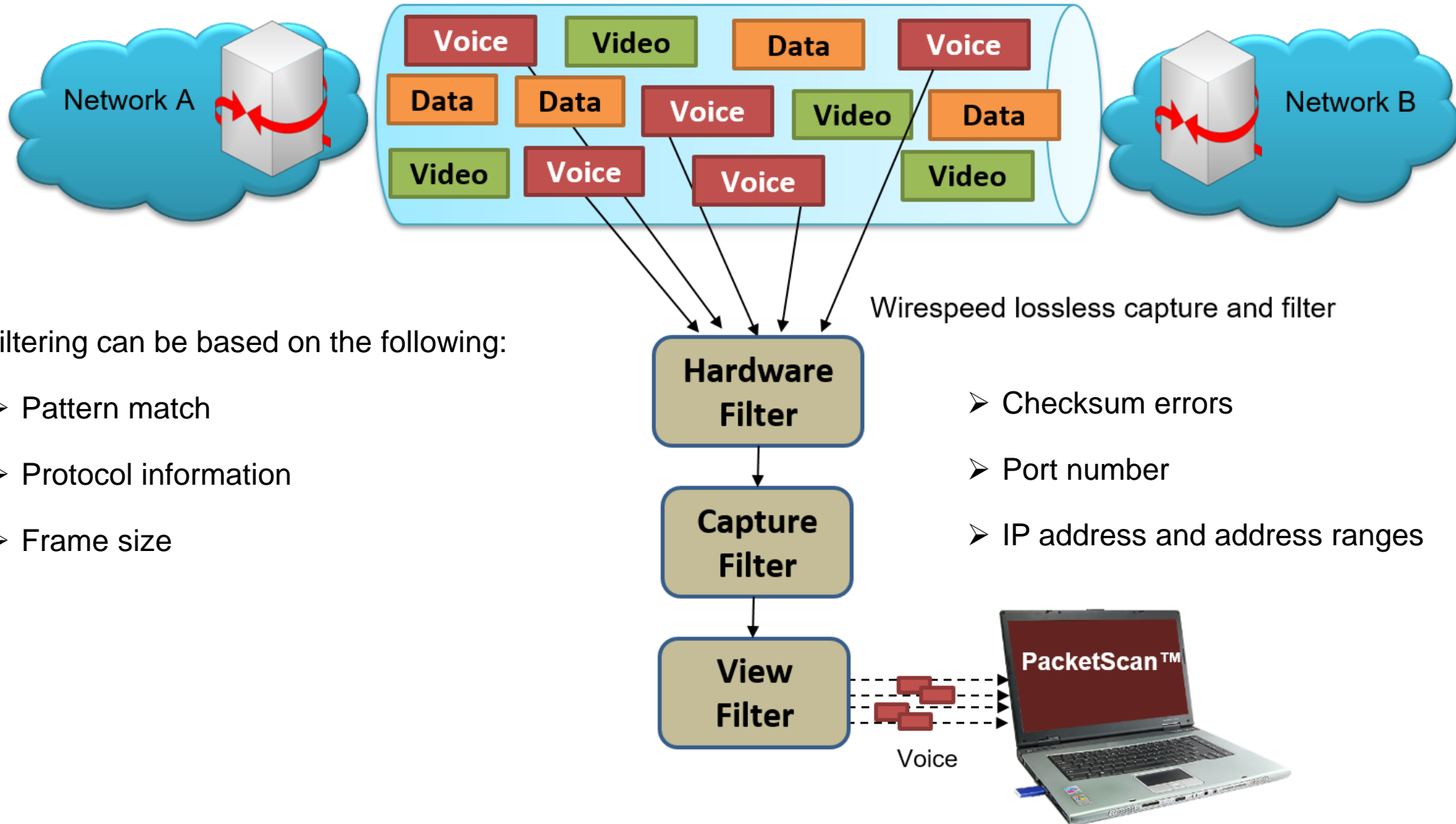
- Filtering can be based on the following:
  - ➢ Pattern match
  - ➢ Protocol information
  - ➢ Frame size

Wirespeed lossless capture and filter

- ➢ Checksum errors
- ➢ Port number
- ➢ IP address and address ranges

3 Stages of Filtering

- Hardware Filter (HWF) – "Special NIC" with hardware filtering - very fast

- Capture Filter (CF) – Powerful software filtering but a little slower

- View Filter (VF) – applies on the captured frames to filter only frames of interest

- PacketScan™ HD captured files to/from Wireshark®

- PacketScan™ HD PDA – for detailed voice, fax, and video analysis

3 Stages of Filtering (Contd.)

PacketScan Summary View

PacketScan™ HD Hardware

Hardware Filter

Filter Passed

Filter Not Passed

Packets Discarded

Standalone NIC

Capture Filter

Filter Passed

Filter Not Passed

Packets Discarded

Capture Buffer

Capture Saved to Files

Ex: SIP, RTP (100 Frames)

View Filter

Filter Passed

Filter only SIP (10 out of 100 Frames)

PacketScan PDA View

All SIP, RTP (100 Frames)

Demo

- Generate VoIP calls (SIP signaling and RTP traffic) with MAPS™ SIP

- Connect PacketScan™ HD to a mirror port

- Capture and analyze the VoIP calls

Link and Ports Interface Testing

Ethernet Frame Structure

RTP

Protocol - UDP

RTP ports – even

RTCP ports - odd

1024-65534

RTP Version

SIP   Port 5060

          TLS 5061

Destination Address		
Destination Address (cont)		Source Address
Source Address (cont)		
Type/Length		Priority/VLAN

Layer 2 - Ethernet

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live		Protocol	Header Checksum
Source Address			
Destination Address			

Layer 3 - IP

Source Port	Destination Port
Length	Checksum

Layer 4 - UDP

V=2	P	X	CC	M	PT	Sequence Number
Timestamp						

Layer 5 - Real Time Protocol

Audio Data (6 to 1480 bytes)

Data

Check

Layer 2 - Ethernet

Open System Interconnection

Layer

Cables, NIC Basic Network Hardware 10BASE-T, 100BASE-T, 1000BASE-T

Routers   Internet layer - packet forwarding path determination, logical addressing IPv4, IPv6, MPLS

Session/Port Layer – interhost connection. SIP, RTP, HTTP, DNS

Network process to application E-mail, Database

1	Physical
2	Data Link
3	Network
4	Transport
5	Session
6	Presentation
7	Application

Switches Link Layer – physical addressing MAC, ARP, L2TP

Transport layer – End-to-end connection and reliability UDP, TCP, SCTTP

Presentation layer – Data representation Encryption

OSI TCP Model

The Transmission Control Protocol/Internet Protocol (TCP/IP) suite was created by the U.S. Department of Defense (DoD) to ensure that communications could survive any conditions and that data integrity wouldn't be compromised under malicious attacks.
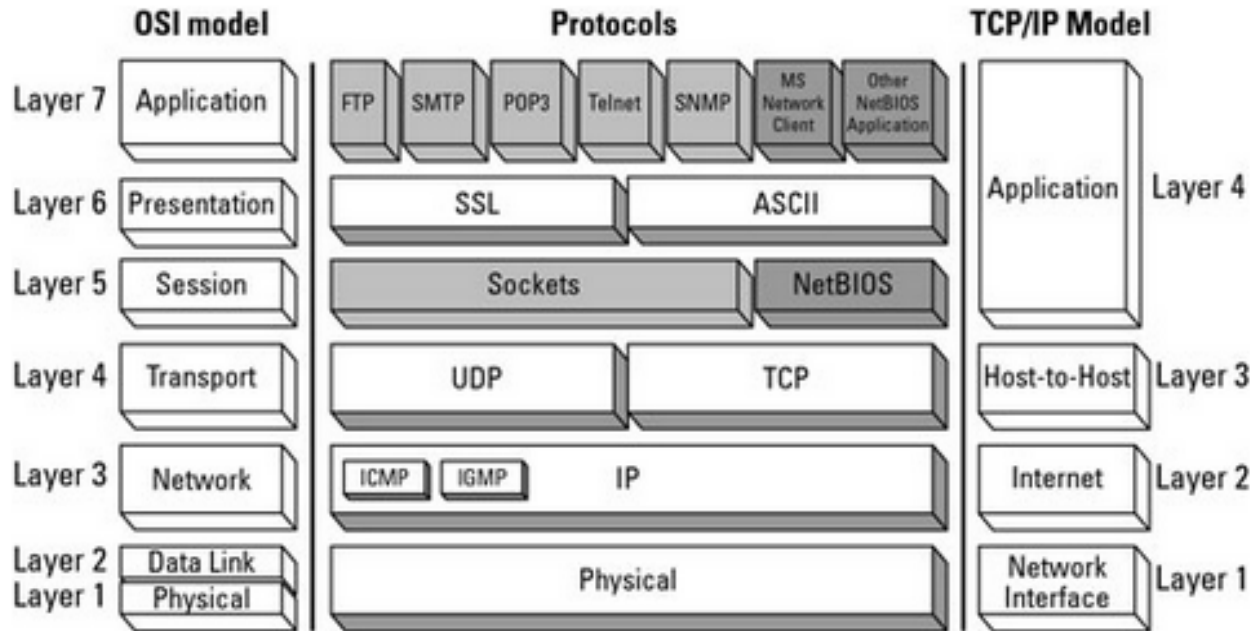
Application (layer 4): Acts as final endpoints at either end of a communication session between two network hosts

Host-to-host (layer 3): Manages the flow of traffic between two hosts or devices, ensuring that data arrives at the application on the host for which it is targeted

Internet (layer 2): Contains all functionality that manages the movement of data between two network devices over a routed network

Network interface (layer 1): Deals with all physical components of network connectivity between the network and the IP protocol

Ethernet Frame (FCS)

Insertion of 802.1Q VLAN tag (32 bit) into Ethernet-II frame. A typical VLAN arrangement with a TPID EtherType value of 0x8100. A QinQ arrangement would add another 32-bit tag containing 16-bit TPID using various EtherType values. Triple tagging QinQinQ has three 32-bit tags besides the original 16-bit EtherType field.
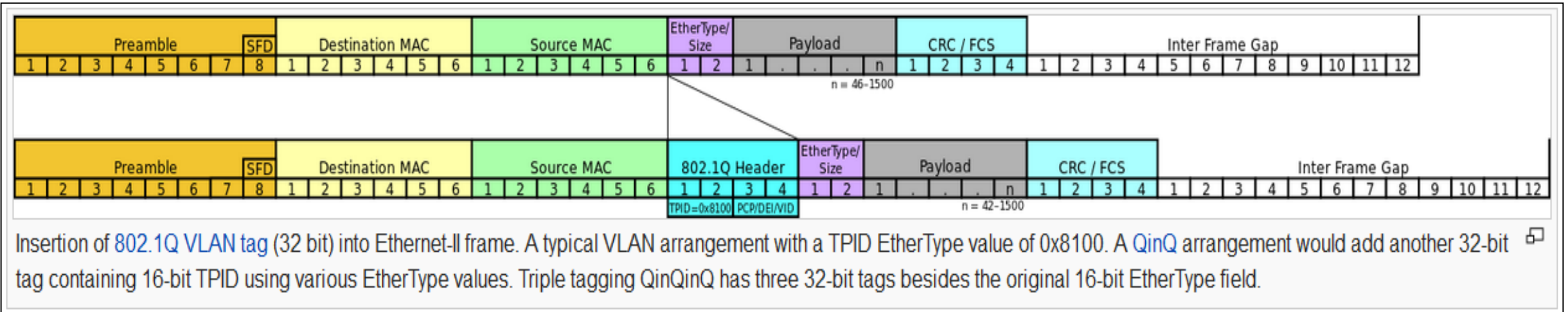
- Frame Check Sequence (FCS)
  - The FCS field contains a number that is calculated by the source node based on the data in the frame
  - TRUE/FALSE

Ethernet Frame (VLANs)

Insertion of 802.1ad double tag in an Ethernet frame
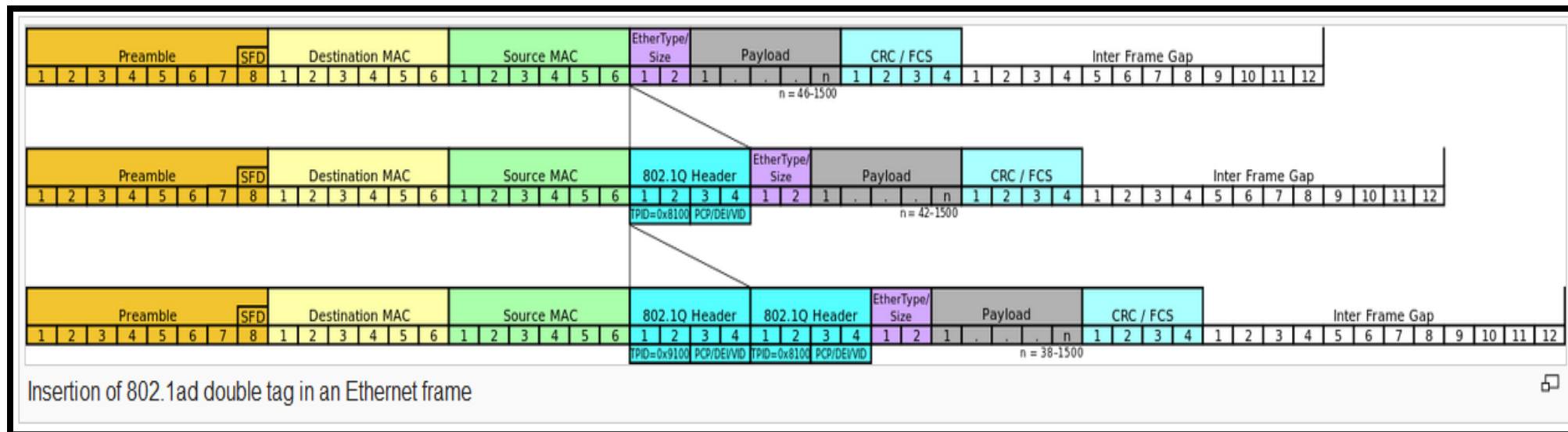
- IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network

Tag Protocol Identifier (TPID)

Tag Control Information (TCI)

The TCI field is further divided into Priority code point (PCP)

Drop eligible indicator (DEI)

VLAN identifier (VID)

16 bits	3 bits	1 bit	12 bits
TPID			TCI
	PCP	DEI	VID
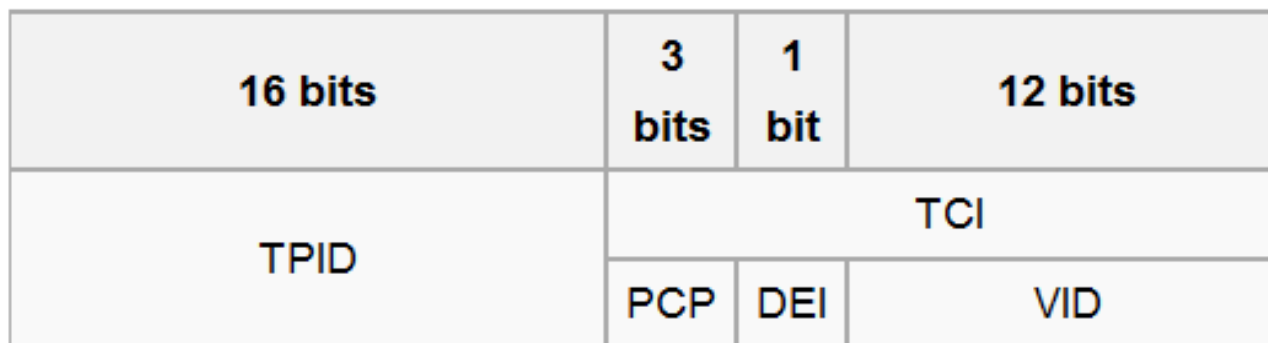
Internet Protocol IPv4

IPv4 Header Format

Offsets	Octet	0																																
		Internet Header Length				**Differentiated Services Code Point**						1						**Explicit Congestion Notification**								3								
Octet	**Bit**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset												
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

Identification – Used for uniquely identifying the group of fragments of a single IP datagram.

Flags – Used to control or identify fragments.

Fragment Offset – 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram.

UDP Frame

UDP Port

FTP – 20 Data Transfer

FTP – 21 FTP Control

SSH – 22

Telnet – 23

SMTP – 25 E-Mail

HTTP – 80

HTTPS – 443

RTP – even 1024 - 65535

RTCP – odd

SIP – 5060 (Destination Port)

SIP over TLS – 5061
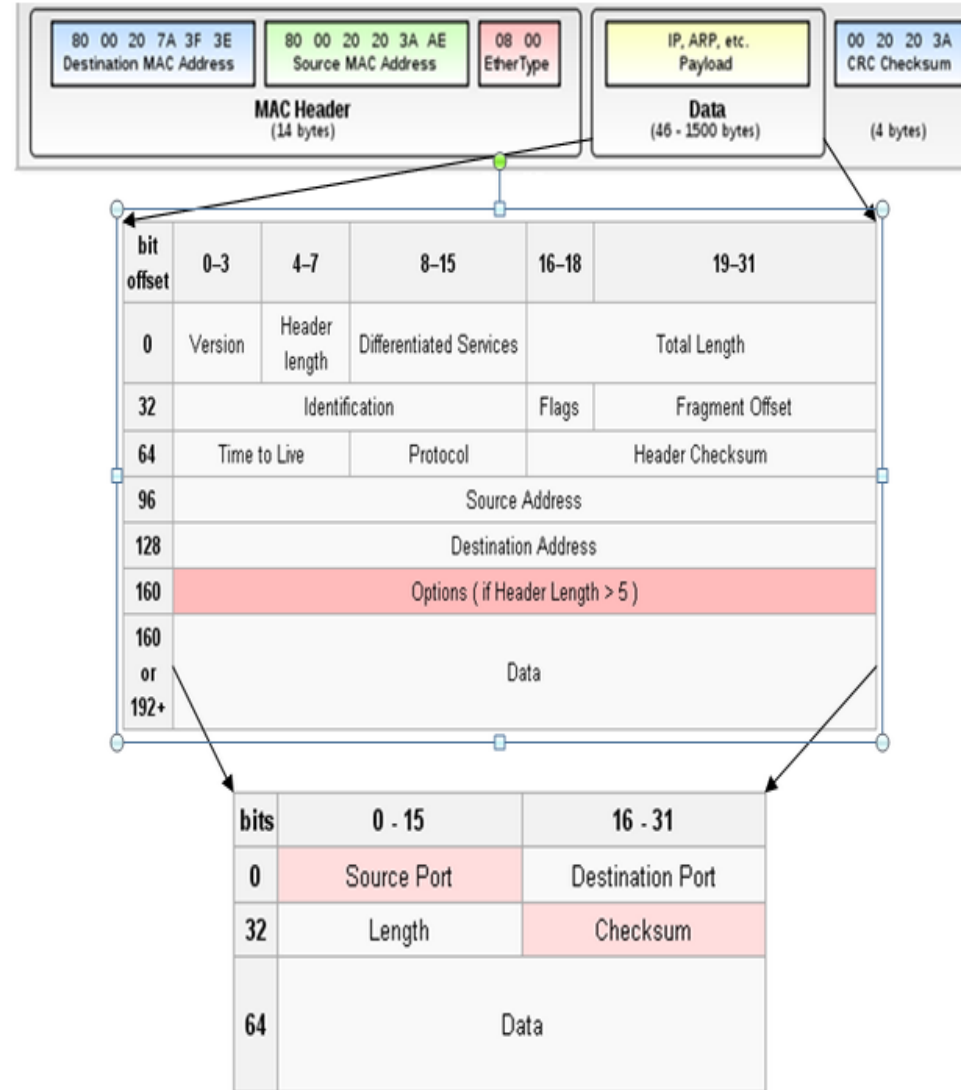
Real-time Analysis

- Default panes - summary, detail, and hex dump of the frame data views
- Optional panes – statistics and call trace views

TCP Frame

Filtering HTTP Traffic

Hardware Filters for Ethernet Fields

Ethernet Frame Structure

Ethernet Frame Format

	Destination MAC Address	Source MAC Address	Type/ Length	Information	CRC
Preamble (8 Bytes)	6	6	2	46-1500	4

IPG (12 Bytes)

Header — Payload

Bytes

Ethernet Frame (Packet) 64-1518 Bytes

Filtering using fields in IP frame

MAC: Media Access Control
IPG: Inter Packet Gap
CRC: Cyclic Redundancy Check

802.3 Ethernet packet and frame structure

Layer	Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46(42)[b]–1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1518(1522) octets →						
Layer 1 Ethernet packet	← 72–1526(1530) octets →								

GL Communications

29

Filtering SIP and RTP Traffic

Packet Data Analyzer (PDA) Summary View

- Summary View displays -
  - Summary of data transmission in each direction including calling number, called number, call id, start time, duration, missing packets, etc.
  - Includes separate statistical counts on total packets, calls, failed calls, captured frames, etc., for SIP, H323, MEGACO, and RTP based calls
  - Provides various graphs to view active calls, average jitter distribution, E-model based measurements for R-factor / MOS/ Packet discarded, RTP packets, T.38 fax analysis, and call signaling, Gap, Jitter, Gap/Jitter Distribution, Wave and Spectral Display for media stream analysis, VoIP calls and more
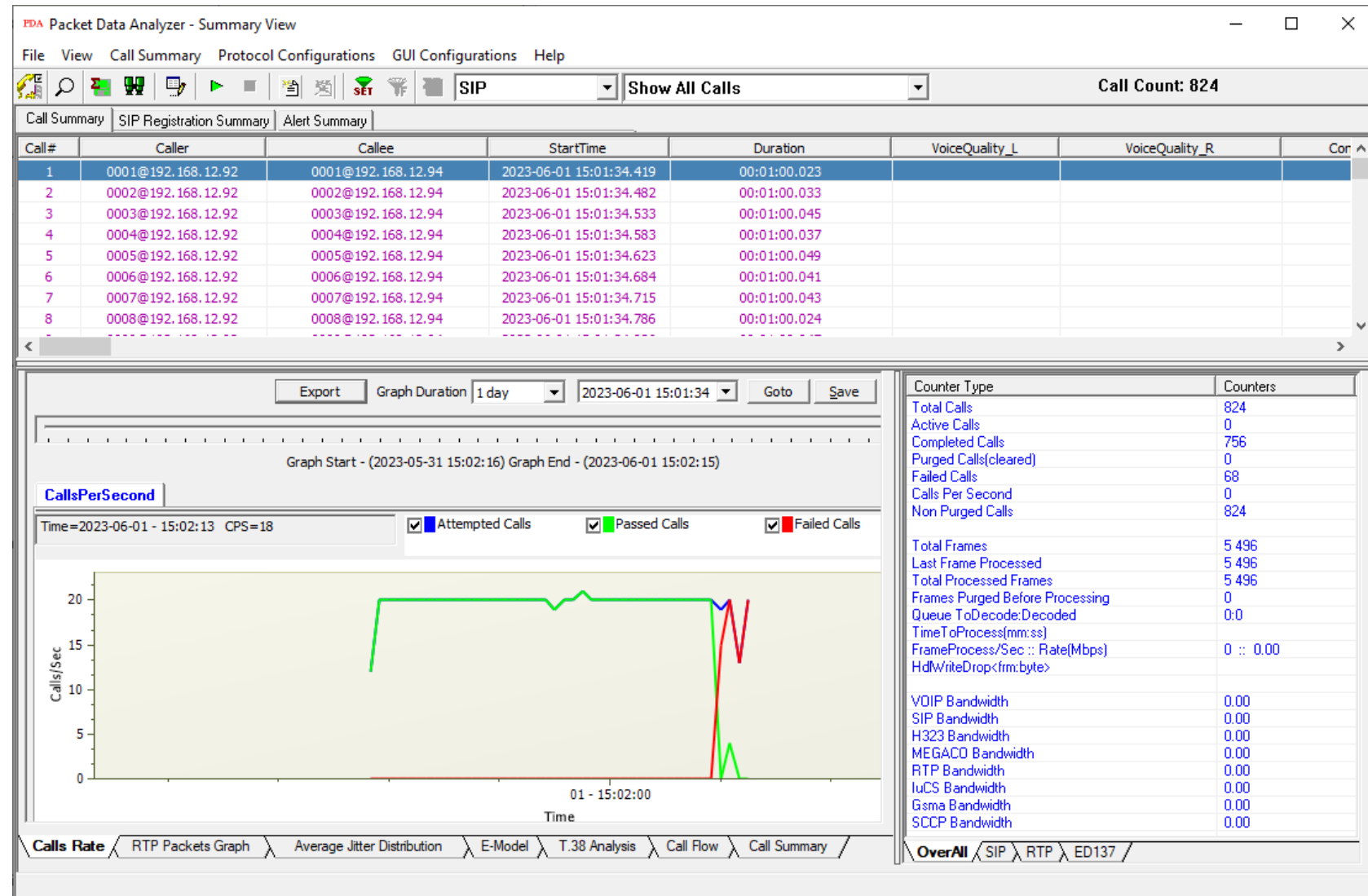
Displaying Filtered Calls using Expressions

- Filter CDRs (Call Detail Records) based on parameters such as caller, time, message count, etc.

- The expression supports the following mathematical operators: ==, <=, >=, !=, <, >, &&, ||

- For example, the filter expression "Error Code==400||Error Code>600" will display calls with Error Code equal to 400 and calls with Error Code greater than 600

Save Call in *.hdl, *.pcap, and *.pcapng Formats

Copy Cell Value to Clipboard

Packet Data Analysis (PDA) Call Graph – SIP Call

- Displays the message sequences of captured VoIP calls
- Decodes of the selected SIP message is displayed on the right pane

Key Performance Indicators (KPIs) Report for SIP Calls

The **SIP Call Summary KPI** chart includes KPIs for the following:

- **Call Success Ratio**: Displays graph for "Successful" and "Unsuccessful Calls," including counts and percentages (%)

- **Calls Per Second**: Shows graph "Total," "Passed," and "Failed Calls per second."

- **Post Dial Delay**: Shows delay counts in milliseconds (0-250ms, 251-500ms, etc.)

- **Error Code Distribution**: Lists Top 10 Call Failure Causes with counts and percentages (%)

- **Answer Seizure Ratio**: Shows "Answered" and "Unanswered Calls," with counts and percentages (%)

- **Call Duration Distribution**: Provides call counts for different durations (0-1 sec, 1-10 sec, etc.)

Call Success Ratio KPI

SIP-CALL KPI CHART

Call Success Ratio | Calls Per Second | Post Dial-delay | Error Code Distribution | Answer Seizure Ratio | Call Duration Distribution

Save as PDF

Call Success Ratio

Total Call(s): 824

Call Status
- Successful Calls - 758 (91.990%)
- InProgress Calls - 0 (0.000%)
- Unsuccessful Calls - 66 (8.010%)

GL Communications
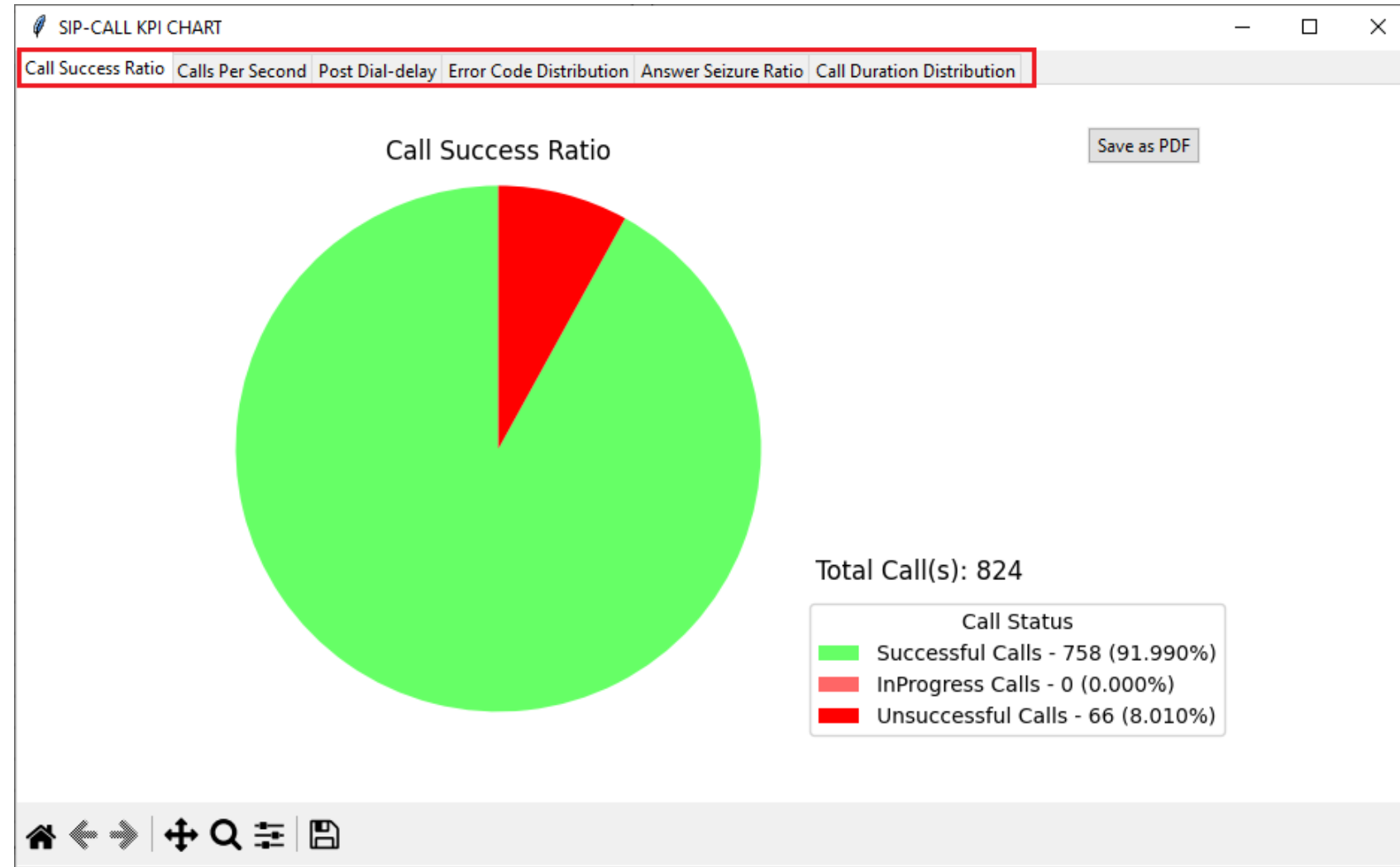
Calls Per Second and Post Delay KPIs
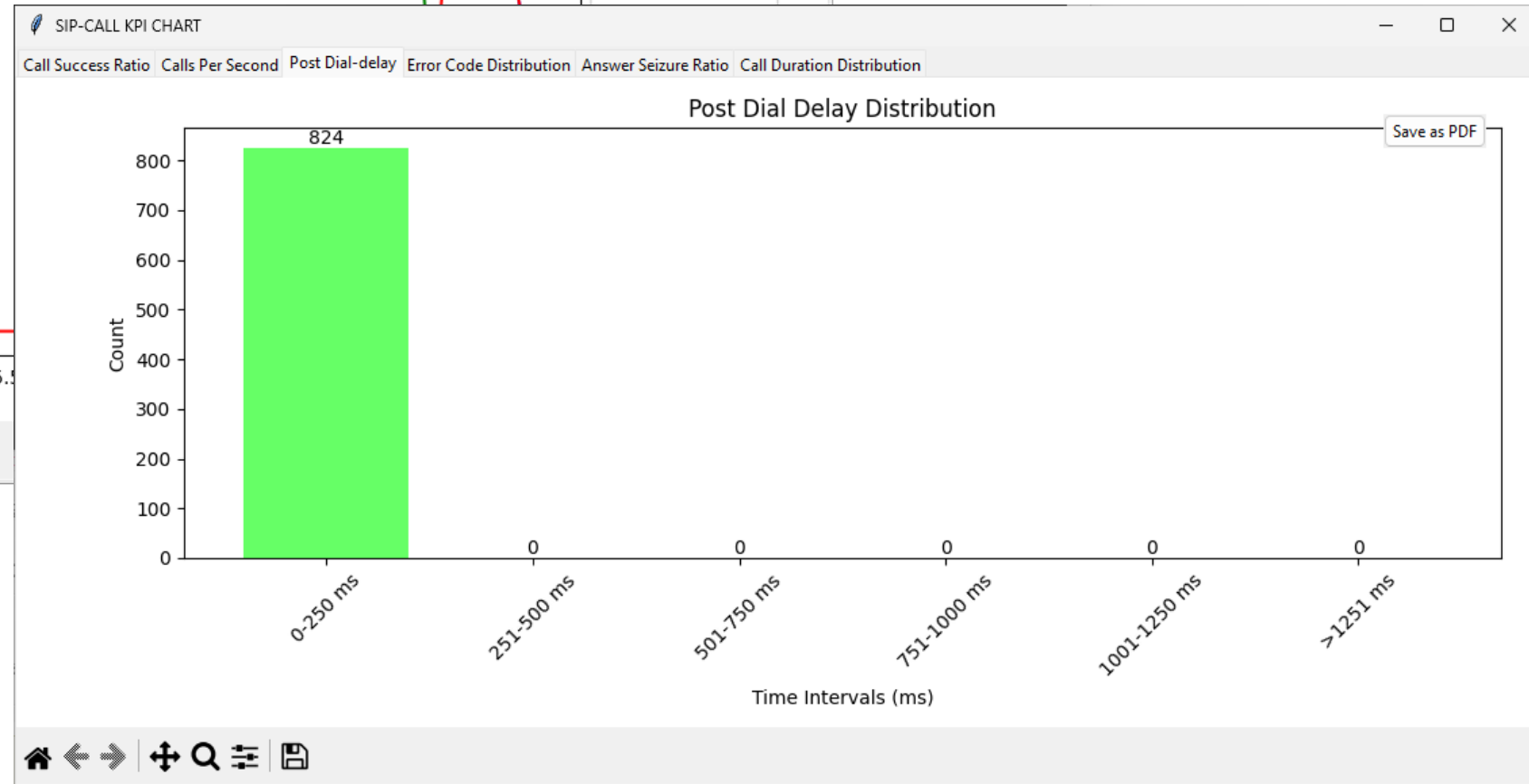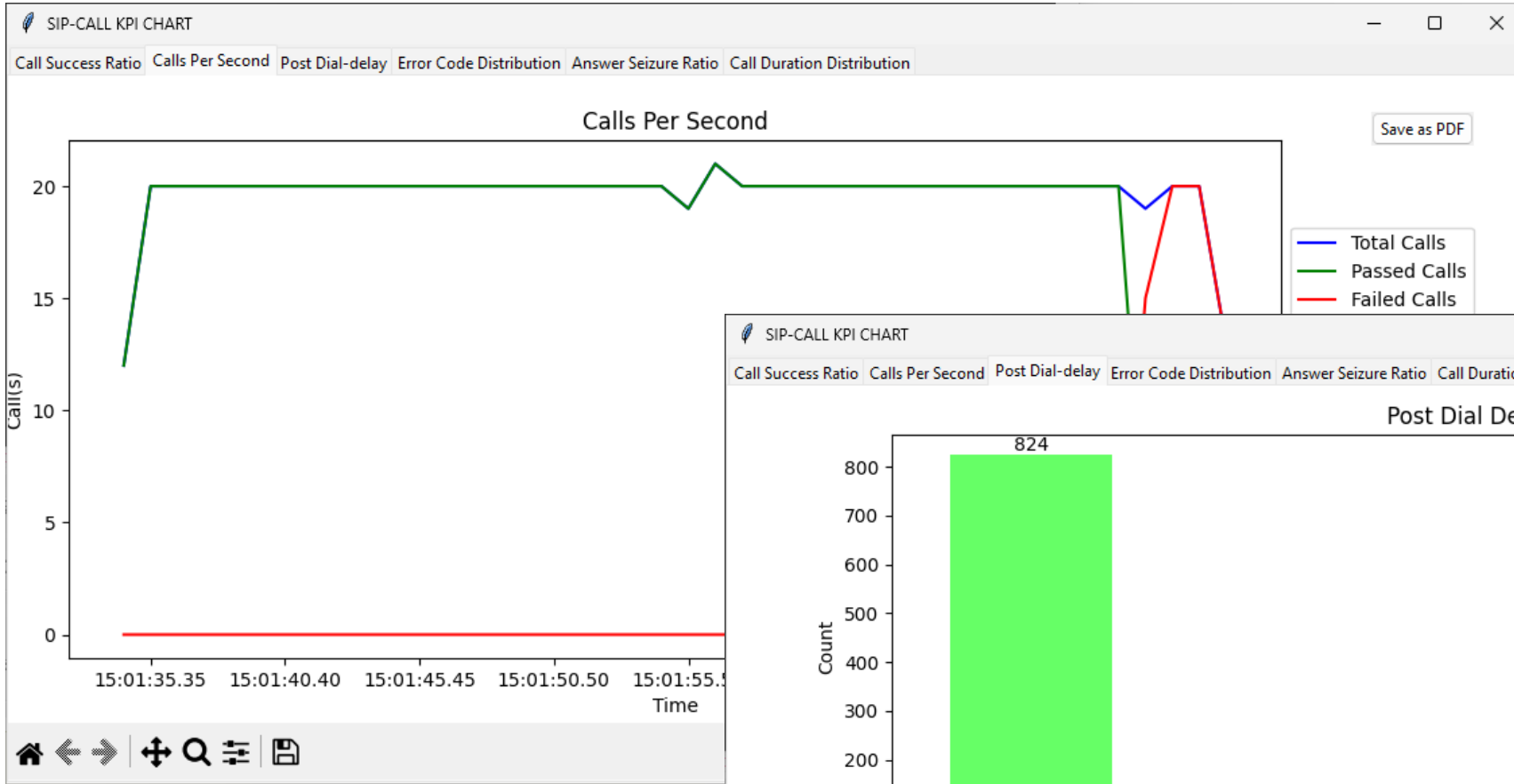
Error Code Distribution KPI
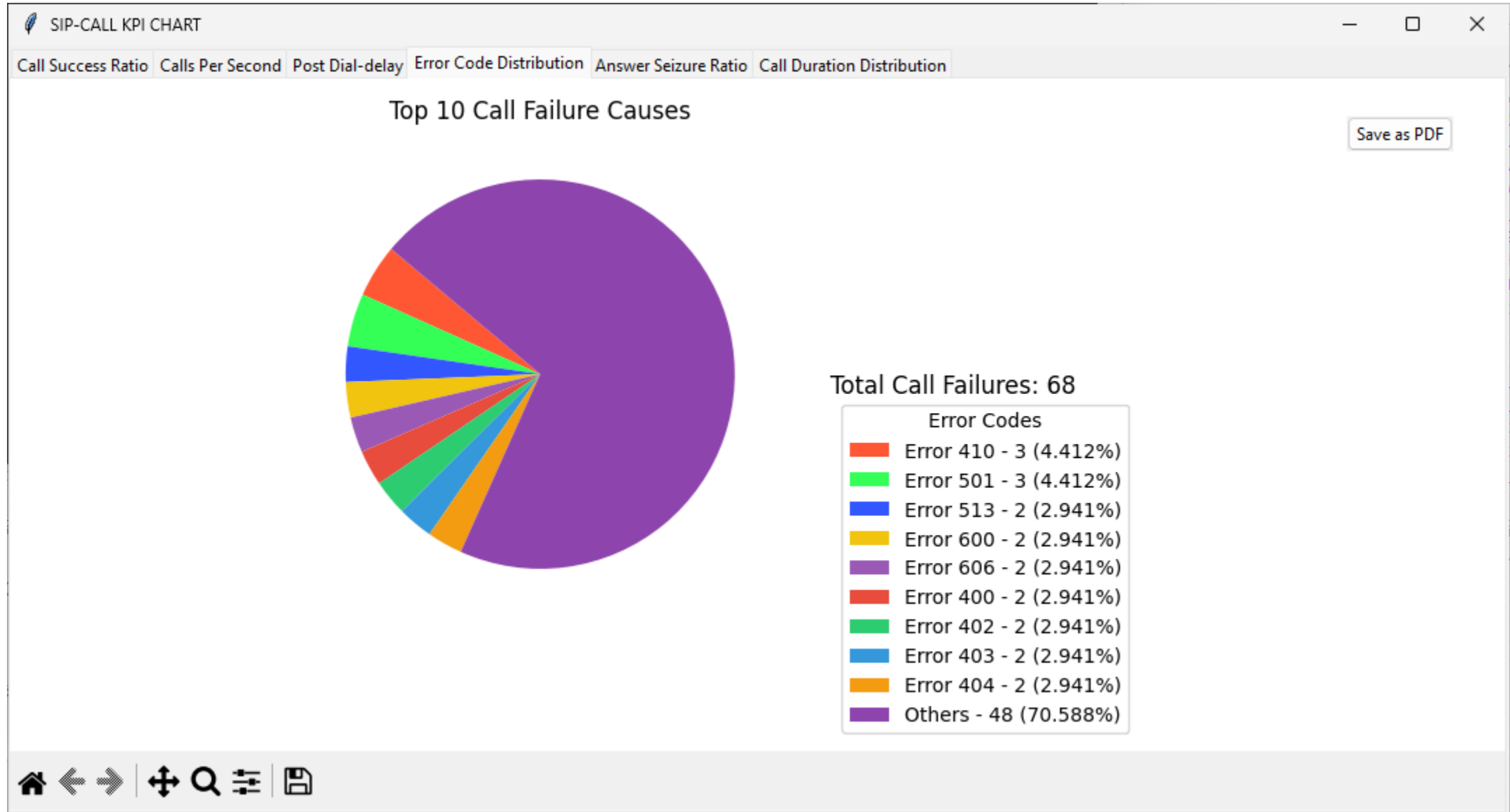
Answer Seizure Ratio and Call Duration Distribution KPIs

Triggers and Actions

Voice Quality Measurements + Packet Statistics + Signaling Information

Triggers / Filters

Signaling Parameter | Packet Loss | Average Jitter | MOS Scores | Call Events

Take Action

Save Trace | Record Audio | Alert | Send Email | Export to CSV
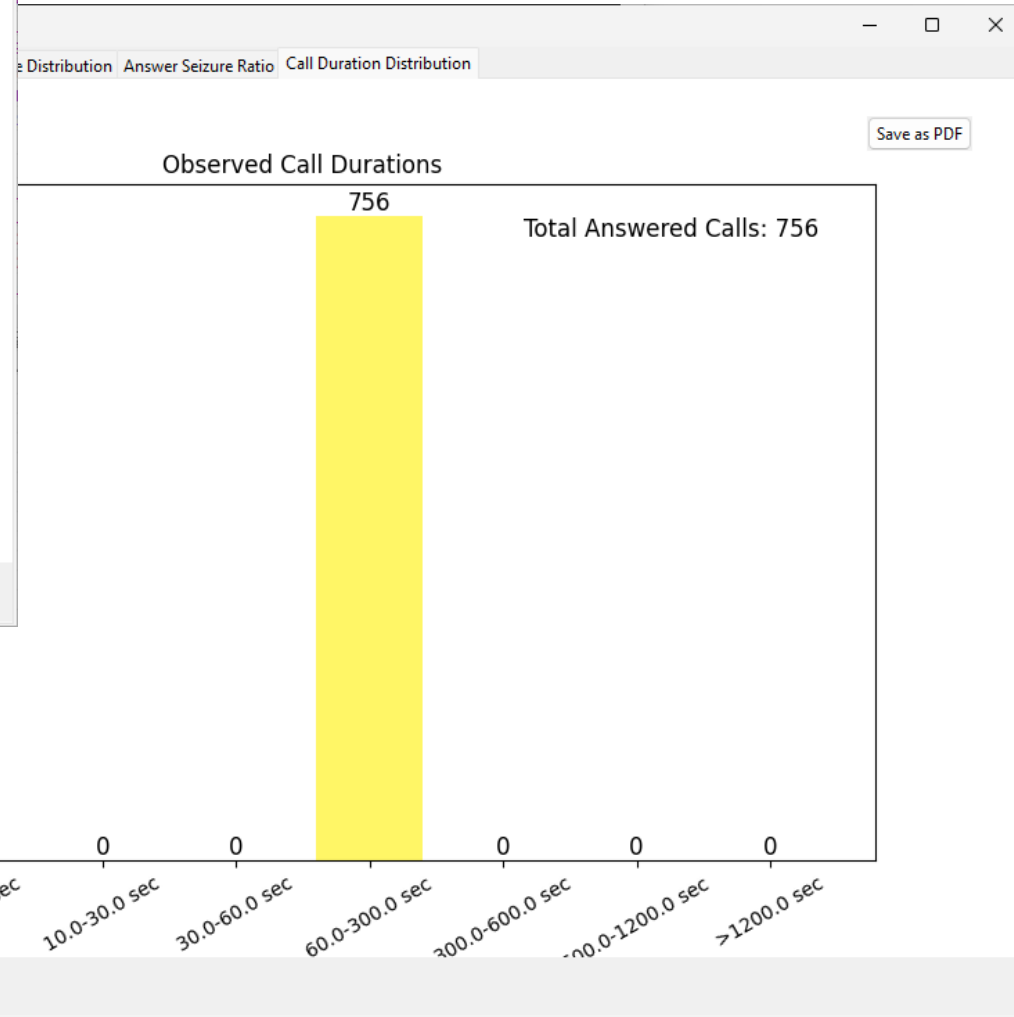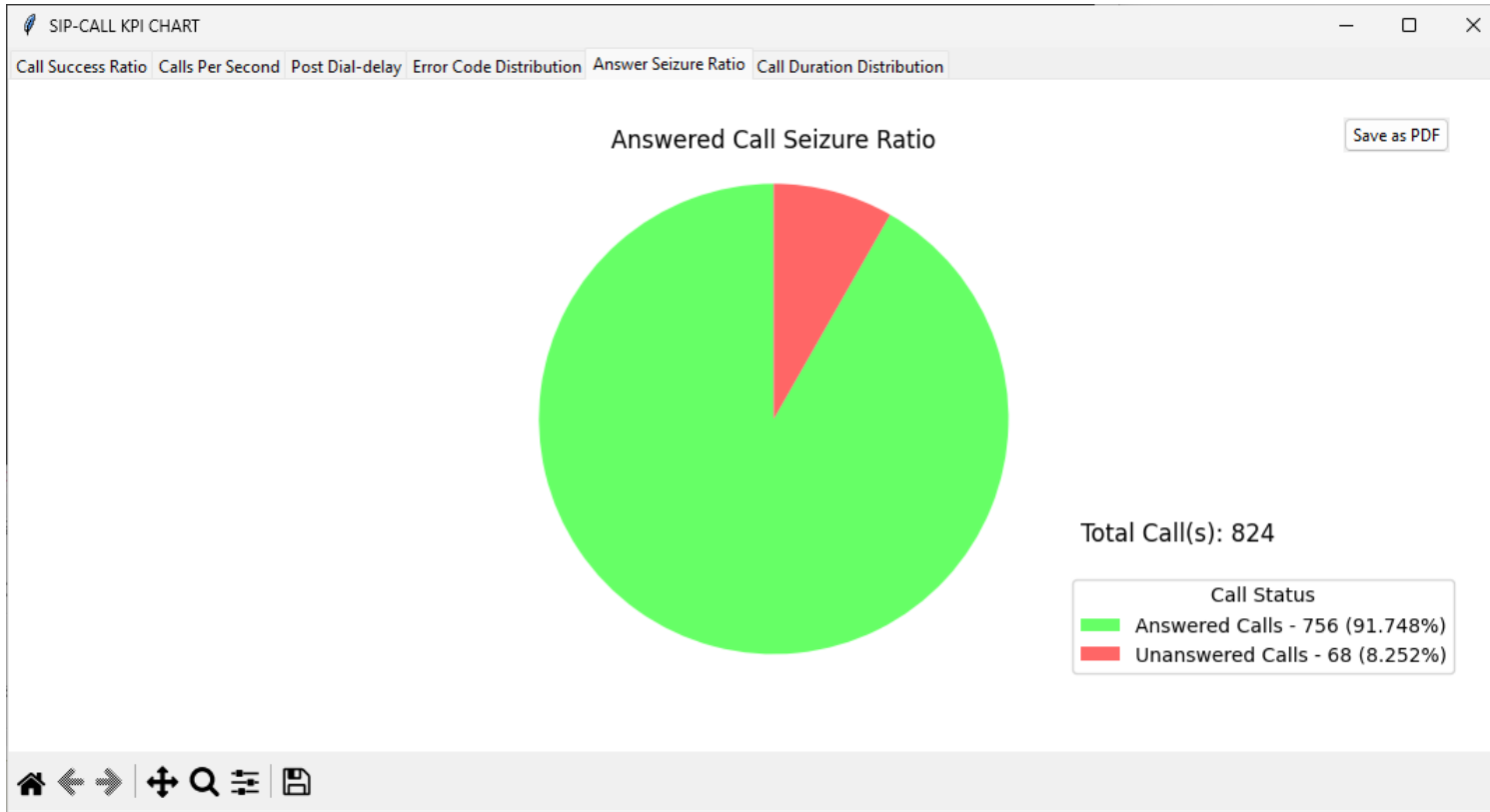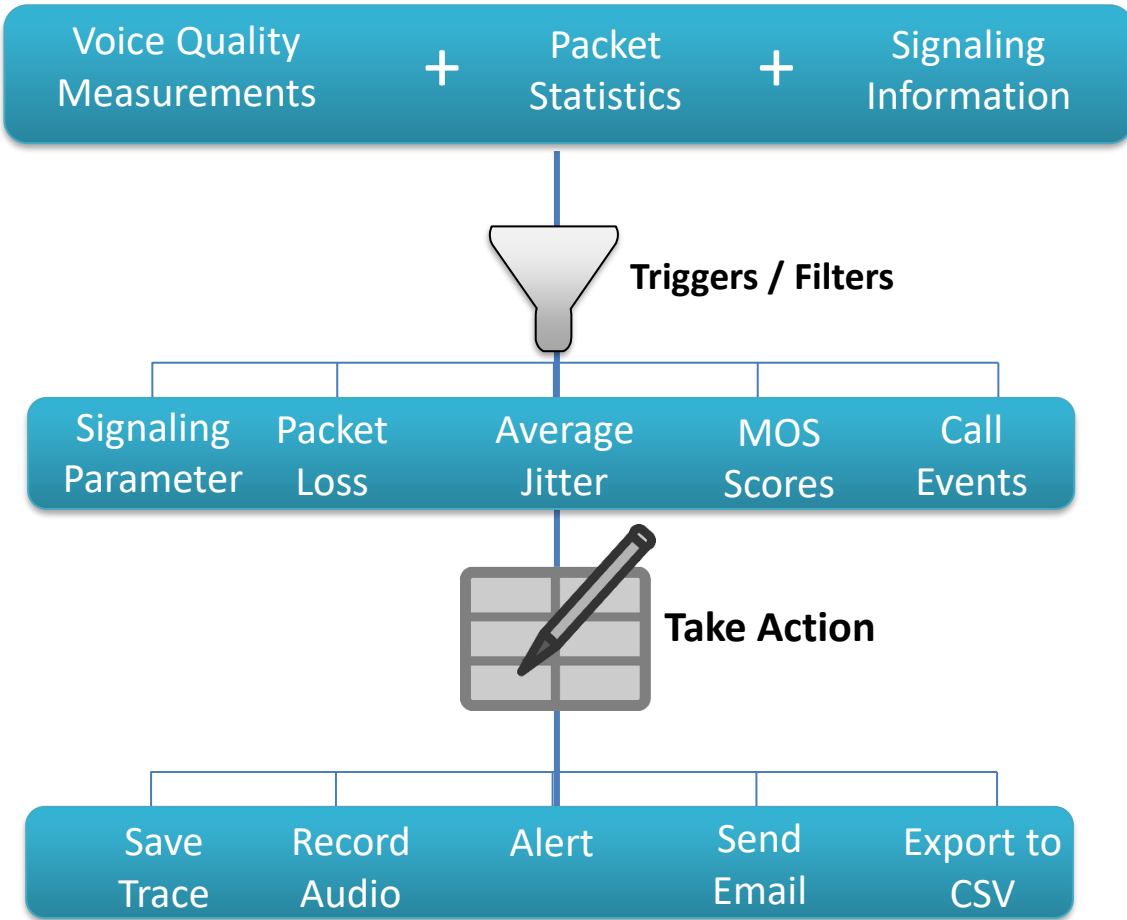
- Triggers can be:
  - Calling/Called Number, Pass/Fail Calls, Voice/SMS/Fax Calls, Call Duration, MOS, SIP Error Code

- Follow on actions can be performed:
  - Saves call in HDL or Wireshark file format
  - Export selected call detail records to CSV file
  - Record audio to file and send email alerts
  - Extracts fax image in the TIFF format from the selected fax call

Voice Quality Metrics
(Sample based)

- MOS is calculated periodically throughout the call which can help to mark the calls with Good, Average and Poor voice quality

5G Protocol Analyzer

- Capture, Decode, and Analysis of Calls in 5G Network

- Supported protocols - Non-Access Stratum (NAS), Next Generation Application Protocol (NGAP), Packet Forwarding Control Protocol (PFCP), XnAP, SCTP, UDP, TCP, and IP

- Following interfaces are supported in Packet Data Analyzer:

  ➢ N1 N2, N4, N8, N10, N11, N12, and N13

  ➢ Packet Data Analyzer feature in Packetscan™ HD provide a complete call flow of a 5G session
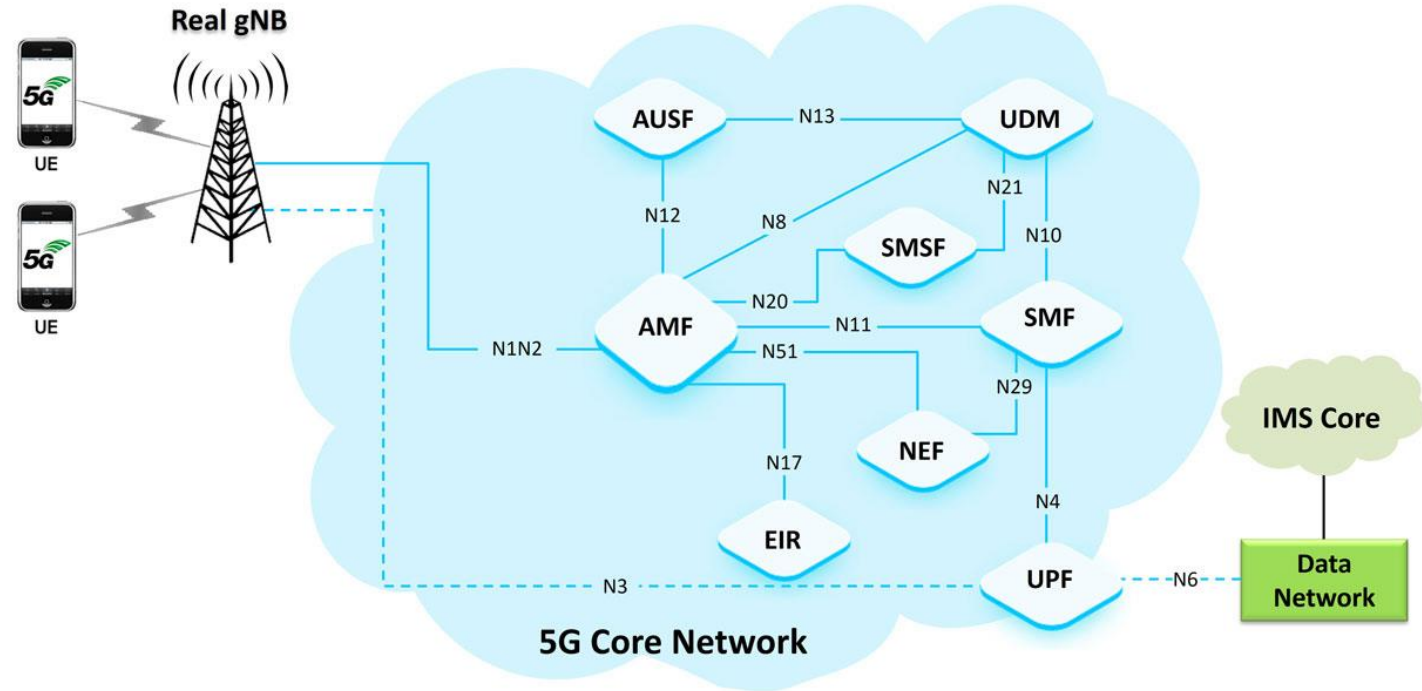
Decode View – 5G NGAP Layer

Call Graph – 5G N1N2

TCP Analytics Network

- Analyze TCP connections between internal company LAN connected computers and outside computers on the WAN

- Analyze TCP connections of a particular client server pair

- Analyze TCP connections on a subset of a LAN

- Display top level statistics

- Communicate with PacketScan™ to display packets that belong to a selected TCP connection

- Export information to CSV files for subsequent Excel or a database import

- Sort tabular information by column values
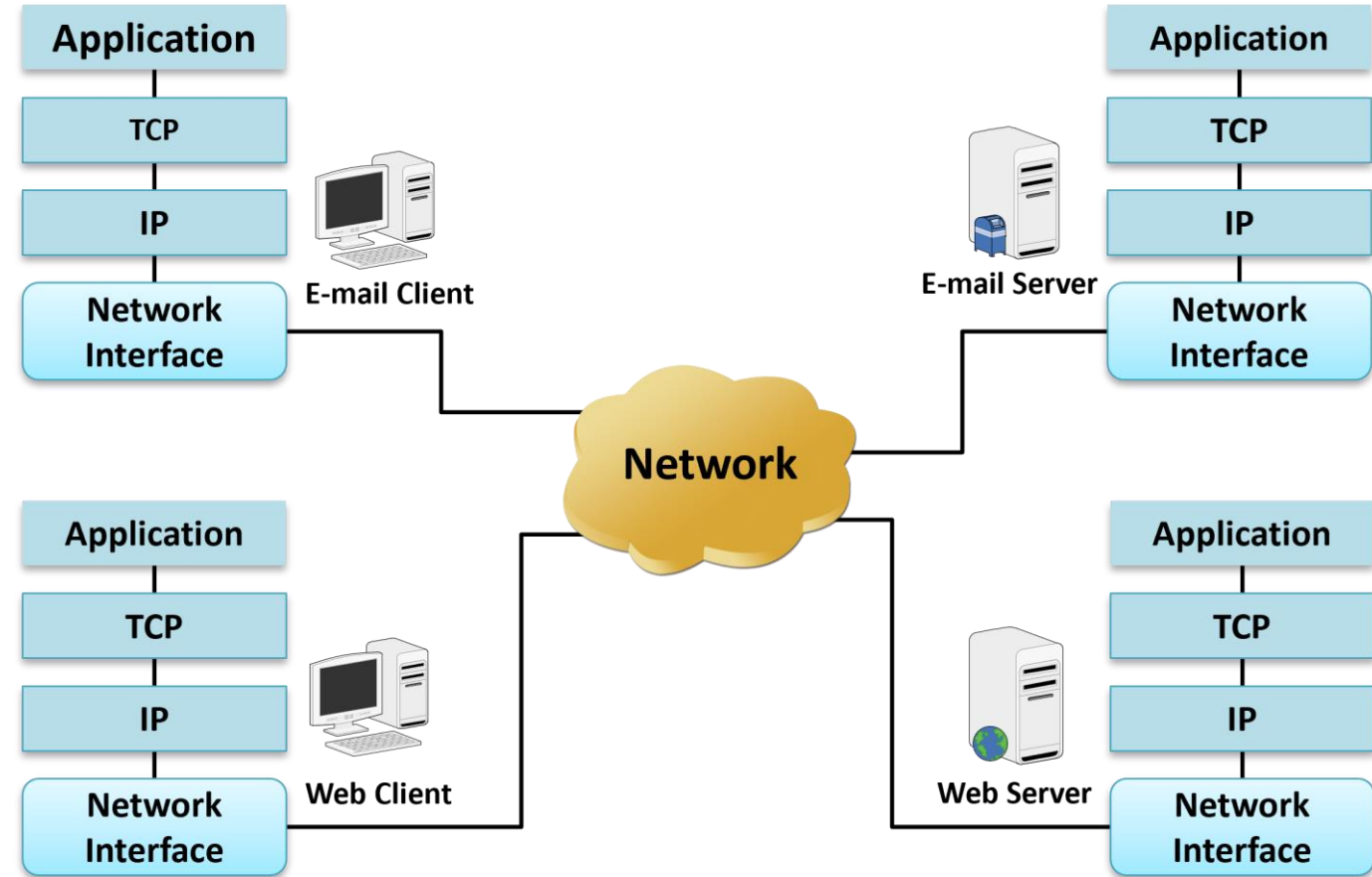
TCP Data Processing in PacketScan™ Application

PacketScan™ with ESP Deciphering Feature

- ESP deciphered packets as shown

Comparison of Before and After Deciphering

Before Deciphering

After Deciphering

Analysis of eCPRI Decodes in Offline PacketScan™ HD

Over UDP
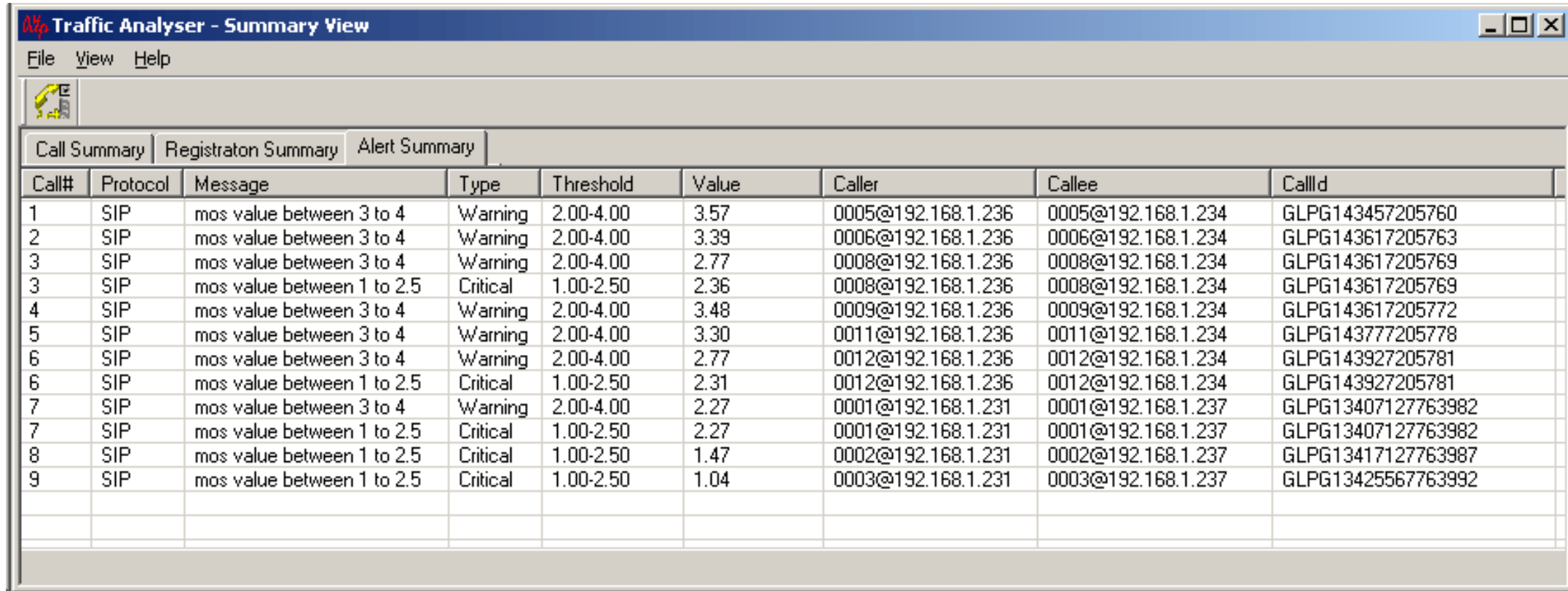

```
Device0 Frame=6 at 2022-06-09 06:07:36.711206000 OK Len=112              *** Right
Ethernet Frame Data
      ============ MAC Layer ============            =
0000 Destination Address                             = xFCAA149225C4
0006 Source Address                                  = x54BEF737CB9A
000C Length/Protocol Type                            = x86DD IPv6
      ============ IPv6 Layer ============           =
000E Protocol Version                                = 0110.... (6)
000E Traffic Class                                   = 0 (....0000 0000....)
000F Flow Label                                      = 834513 (....1100 10111011 11010001)
0012 Payload Length                                  = 58 (x003A)
0014 Next Header                                     = 00010001 User Datagram Protocol (UDP)
0015 Hop Limit                                       = 64 (x40)
0016 Source Address                                  = fe80::64f2:5e84:f1db:502
0026 Destination Address                             = fe80::589e:b2d5:9074:2bec
      ============ UDP Layer ============            =
0036 Source Port                                     = 64000 (xFA00)
0038 Destination Port                                = 64000 (xFA00)
003A Length (Header + Data)                          = 58 (x003A)
003C Checksum                                        = x7F76
      ============ eCPRI Layer ============          =
003E C                                               = .......0 eCPRI message is the last one inside the eCPRI PDU
003E eCPRI Protocol Revision                         = 0001.... (1)
003F eCPRI Message Type                              = 00000100 Remote Memory Access
0040 eCPRI Payload Size                              = 28 (x001C)
0042 Remote Memory Access ID                         = 17 (x11)
0043 Req/Resp                                        = ....0010 Failure
0043 Read/Write                                      = 0010.... Write_No_Resp
0044 Element ID                                      = 8755 (x2233)
0046 Address                                         = x050403020100
004C Length                                          = 16 (x0010)
     User Data                                       = xFFEEDDCCBBAA99887766554433221100
```

Over MAC

```
Device0 Frame=0 at 2019-02-13 11:36:46.000000000 OK Len=64                    *** Right
Ethernet Frame Data
    ============ MAC Layer ============           =
0000 Destination Address                         = x008016000000
0006 Source Address                              = x008016884EFF
000C Length/Protocol Type                        = xAEFE eCPRI
    ============ eCPRI Layer ============         =
000E C                                           = .......0 eCPRI message is the last one inside the eCPRI PDU
000E eCPRI Protocol Revision                     = 0001.... (1)
000F eCPRI Message Type                          = 00000000 IQ Data
0010 eCPRI Payload Size                          = 20 (x0014)
     eCPRI Payload                               = x123487650F0E0D0C0B0A09080706050403020100
    ============ O-RAN Fronthaul CUS Layer ============ =
     ecpriPcid                                   =
0012  BandSector_ID                              = ..010010 (18)
0012  DU_Port_ID                                 = 00...... (0)
0013  RU_Port_ID                                 = ....0100 (4)
0013  CC_ID                                      = 0011.... (3)
     ecpriSeqid                                  =
0014  Sequence ID                                = 135 (x87)
0015  Subsequence ID                             = .1100101 (101)
0015  E bit                                      = 0....... More fragments follow
0016 FilterIndex                                 = ....1111 Reserved
0016 payloadVersion                              = .000.... (0)
0016 dataDirection                               = 0....... UpLink
0017 frameId                                     = 14 (x0E)
0018 subframeId                                  = 0000.... (0)
0018 slotId                                      = 52 (....1101 00......)
0019 startSymbolid                               = ..001100 (12)
001A sectionId                                   = 176 (00001011 0000....)
001B symInc                                      = .....0.. use the current symbol number
001B rb                                          = ....1... every other RB used
001B startPrbu                                   = 521 (......10 00001001)
001D numPrbu                                     = 8 (x08)
     udCompHdr                                   =
001E  udCompMeth                                 = ....0111 Reserved
001E  udIqWidth                                  = 0000.... I and Q are each 16 bit wide
     Dump                                        = x050403020100
```

PDA - Alert Summary

Traffic Analyser - Summary View

File View Help

Call Summary | Registraton Summary | Alert Summary

Call#	Protocol	Message	Type	Threshold	Value	Caller	Callee	CallId
1	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.57	0005@192.168.1.236	0005@192.168.1.234	GLPG143457205760
2	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.39	0006@192.168.1.236	0006@192.168.1.234	GLPG143617205763
3	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.77	0008@192.168.1.236	0008@192.168.1.234	GLPG143617205769
3	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.36	0008@192.168.1.236	0008@192.168.1.234	GLPG143617205769
4	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.48	0009@192.168.1.236	0009@192.168.1.234	GLPG143617205772
5	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.30	0011@192.168.1.236	0011@192.168.1.234	GLPG143777205778
6	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.77	0012@192.168.1.236	0012@192.168.1.234	GLPG143927205781
6	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.31	0012@192.168.1.236	0012@192.168.1.234	GLPG143927205781
7	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.27	0001@192.168.1.231	0001@192.168.1.237	GLPG13407127763982
7	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.27	0001@192.168.1.231	0001@192.168.1.237	GLPG13407127763982
8	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	1.47	0002@192.168.1.231	0002@192.168.1.237	GLPG13417127763987
9	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	1.04	0003@192.168.1.231	0003@192.168.1.237	GLPG13425567763992

- Generates alerts when vital parameters go beyond a specified value
- Provides an active list of the alerts for the events in a tabular column
- Displays the summary of call#, user-defined message, threshold value, actual value for which the alert occurred, callee, caller, and callid

Registration Summary

- Displays the SIP registration information in a tabular format which includes user agent, registrar, registered time, status, and so on for each user agent

- Displays the active registration graph of the entire registration summary

- Provides the trace display of each registration
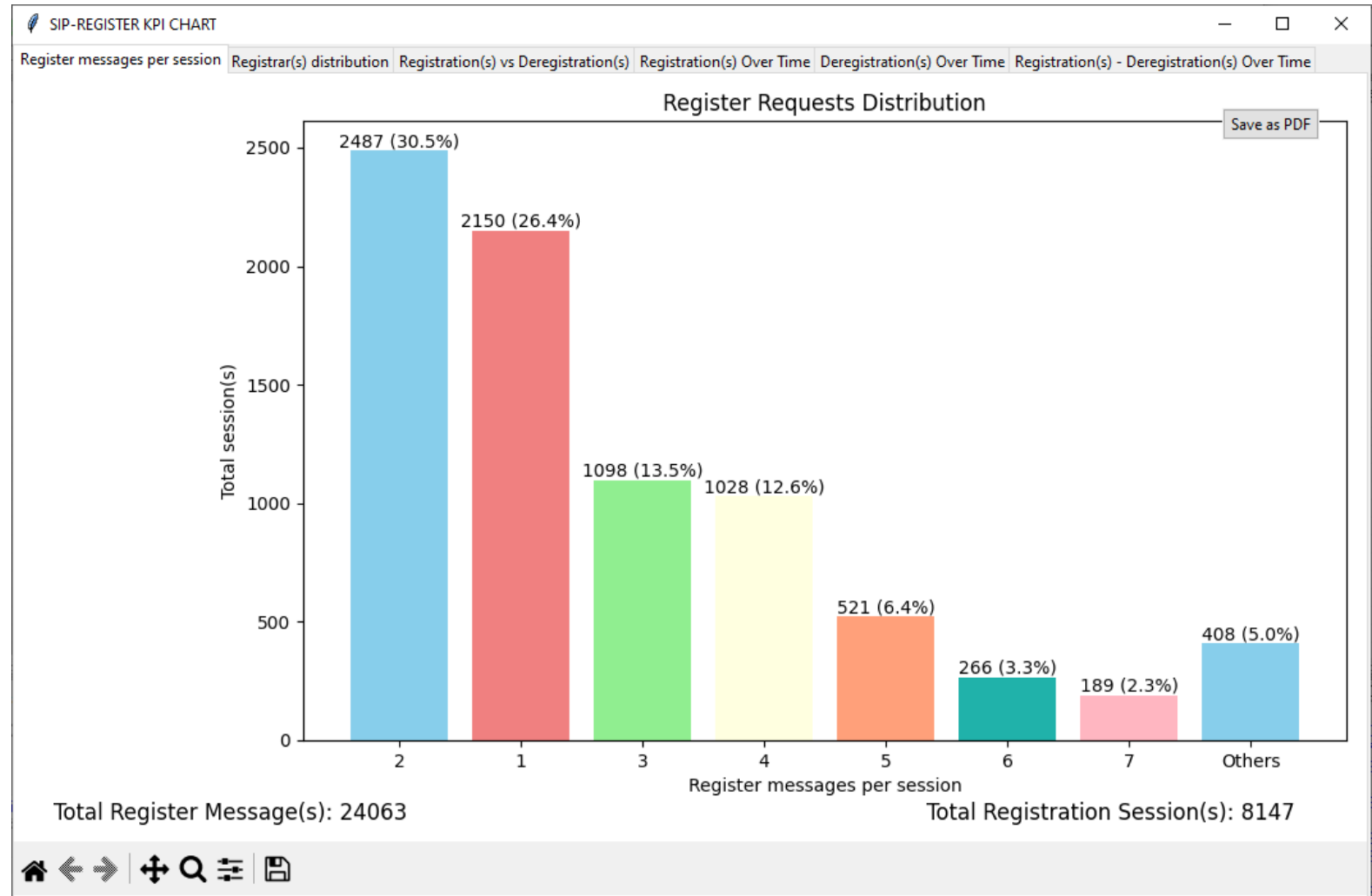
Registration Trace

- Displays the message sequence of registered calls
- Message sequence pictorially displays the messages exchanged for a particular scenario between a user agent and the registrar

KPI Report (Registration)

The SIP Registration Summary KPI Report includes KPIs for the following:

- **Register Messages per Session:** Shows a graph for the distribution of Register Requests

- **Registrar(s) Distribution:** Displays a graph for the number of Registration sessions per Registrar

- **Registration(s) vs Deregistration(s):** Illustrates a graph comparing the distribution of Register and Deregister counts with percentages (%)

- **Registration(s) Over Time:** Show the graphs for "Successful," "Failed," and "Total Attempts" per second

- **Deregistration(s) Over Time:** Displays a graph for "Successful" and "Total Attempts" per second

- **Registration(s) - Deregistration(s) Over Time:** Shows a graph for overall "Register & Deregister attempts," "Register & Deregister passed," and "Register & Deregister failed" attempts per second
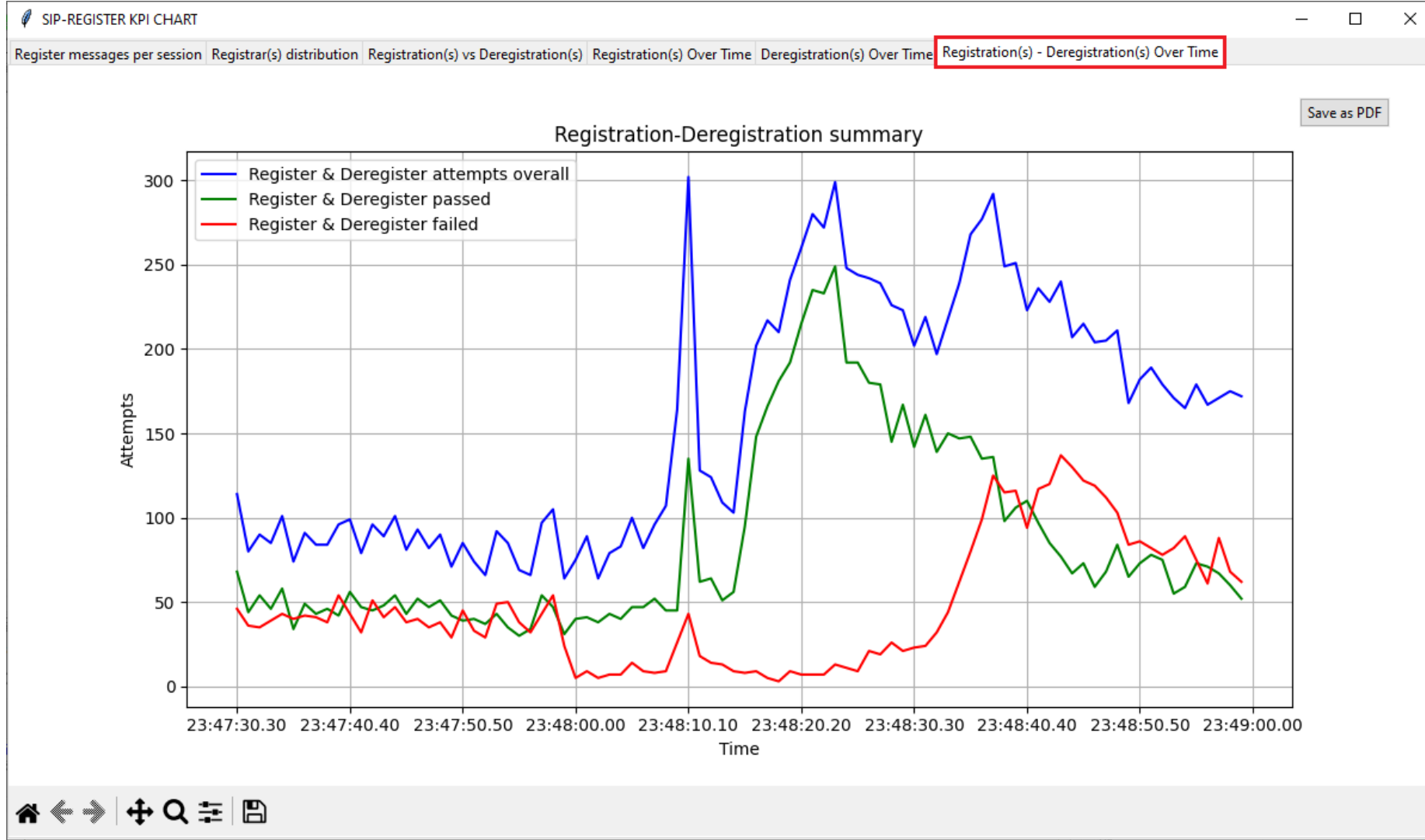
Registrar(s) Distribution, Registration vs Deregistration KPIs
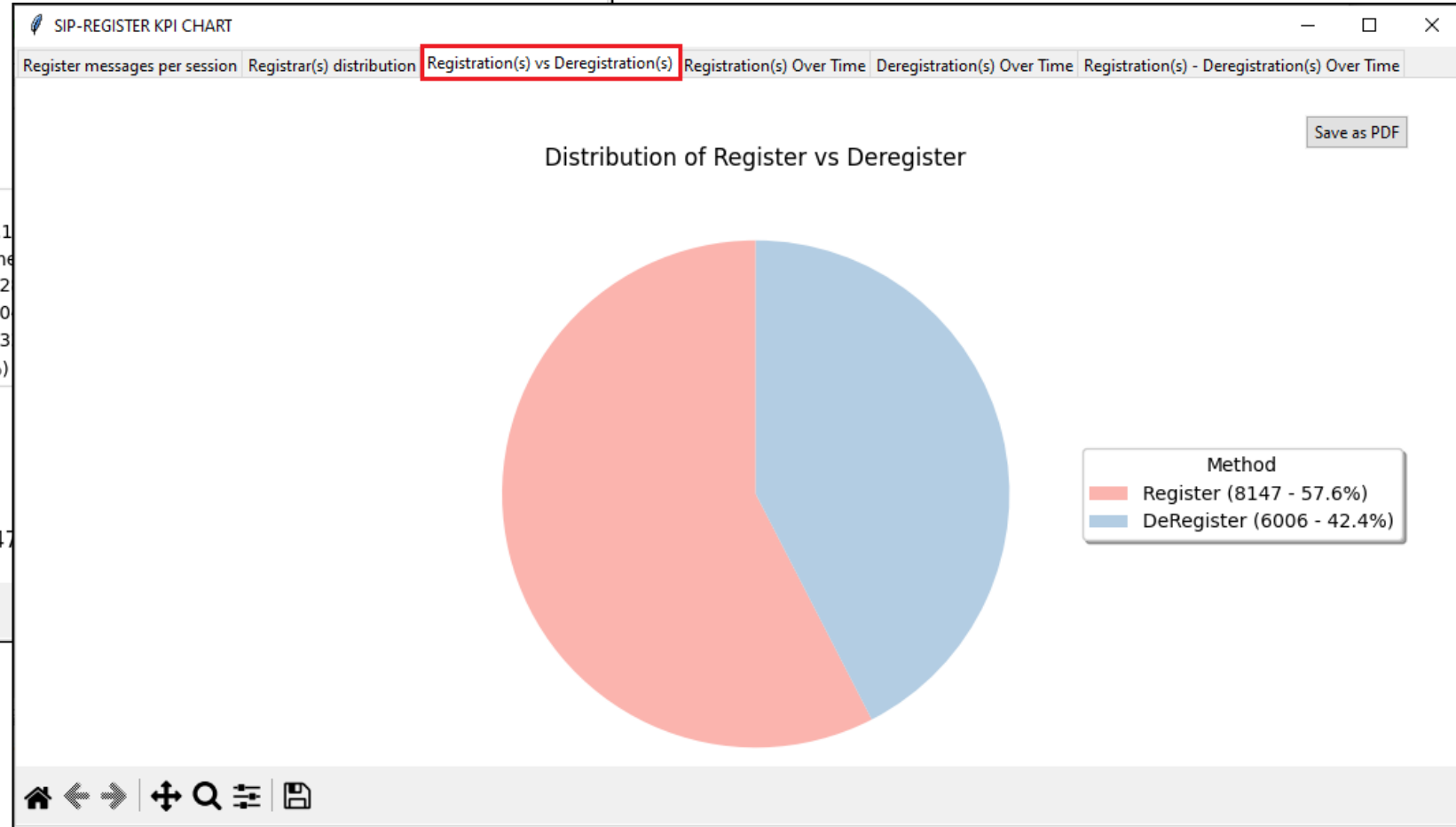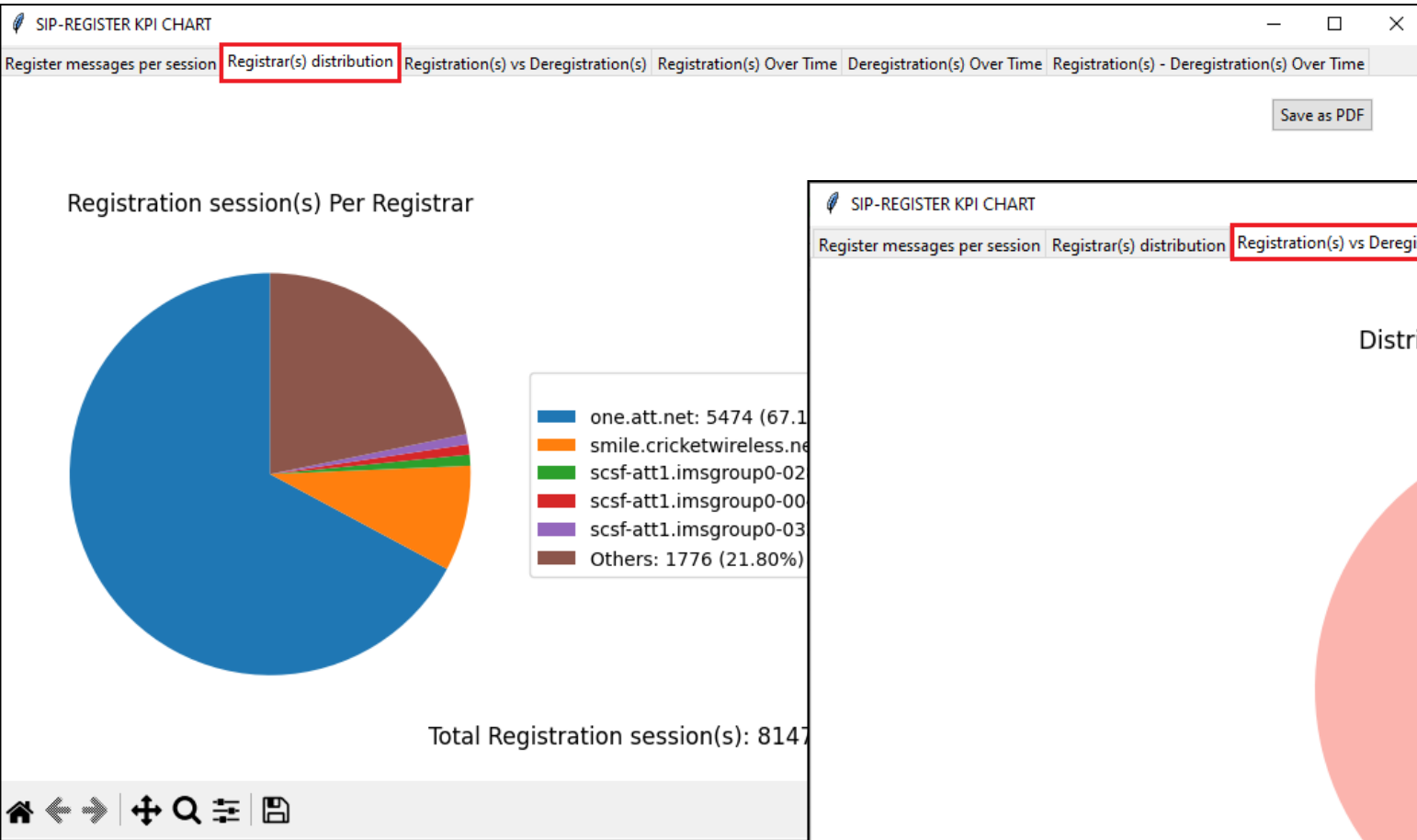
Registration(s) over Time, Deregistration over Time KPIs
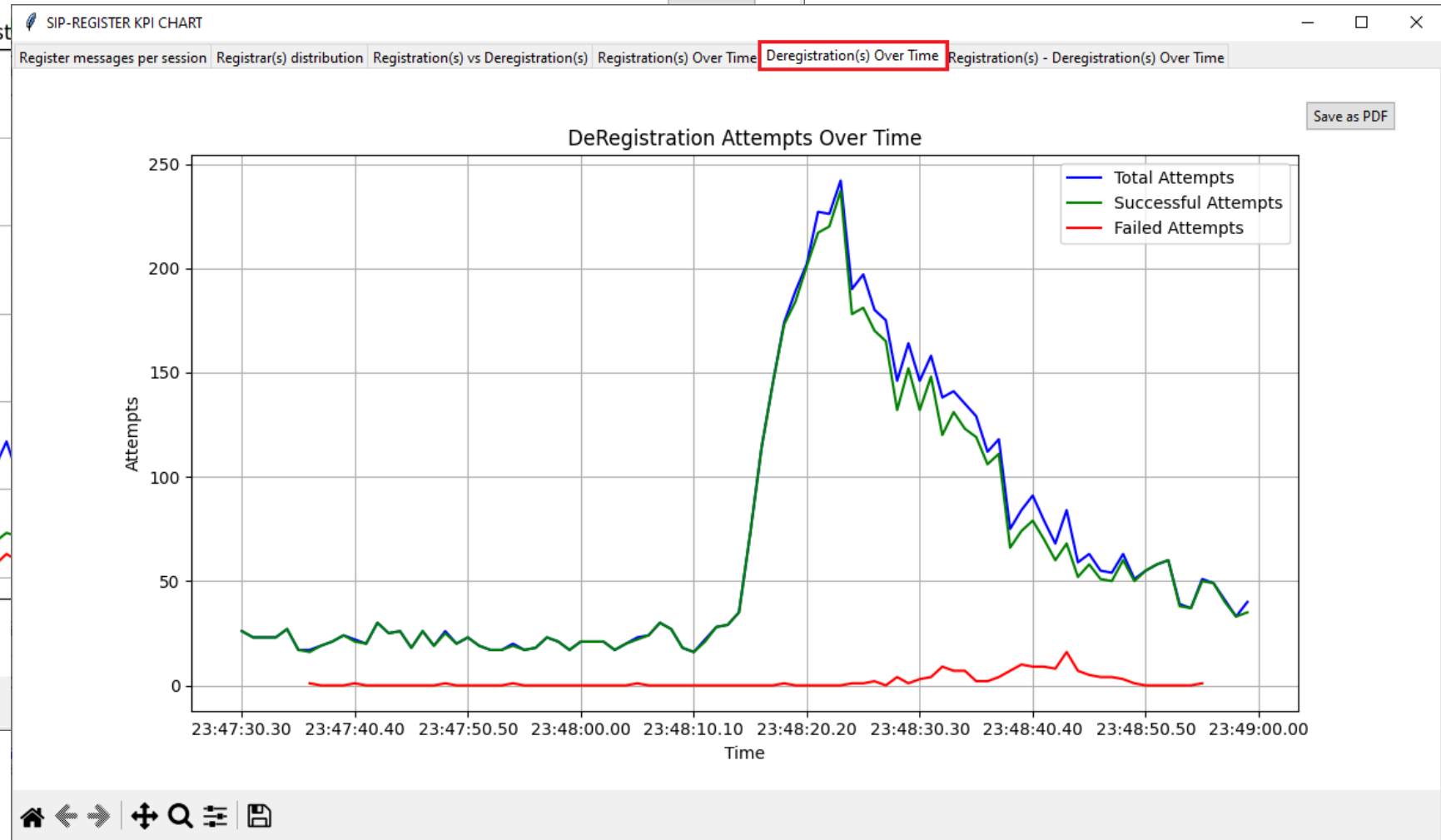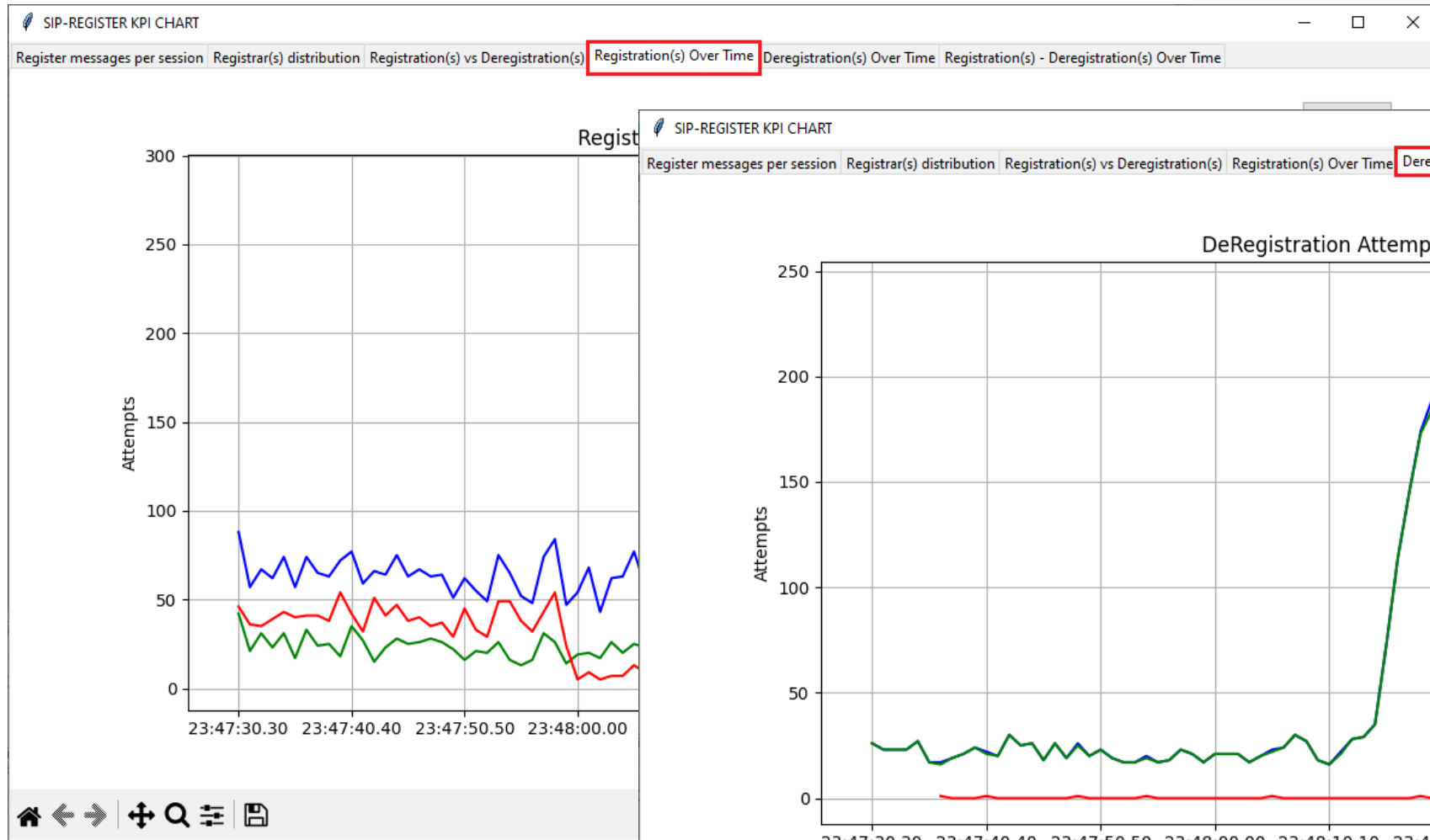
Registration(s)-Deregistration(s) over Time KPI

Thank you