
All-IP Signaling and Traffic Analysis

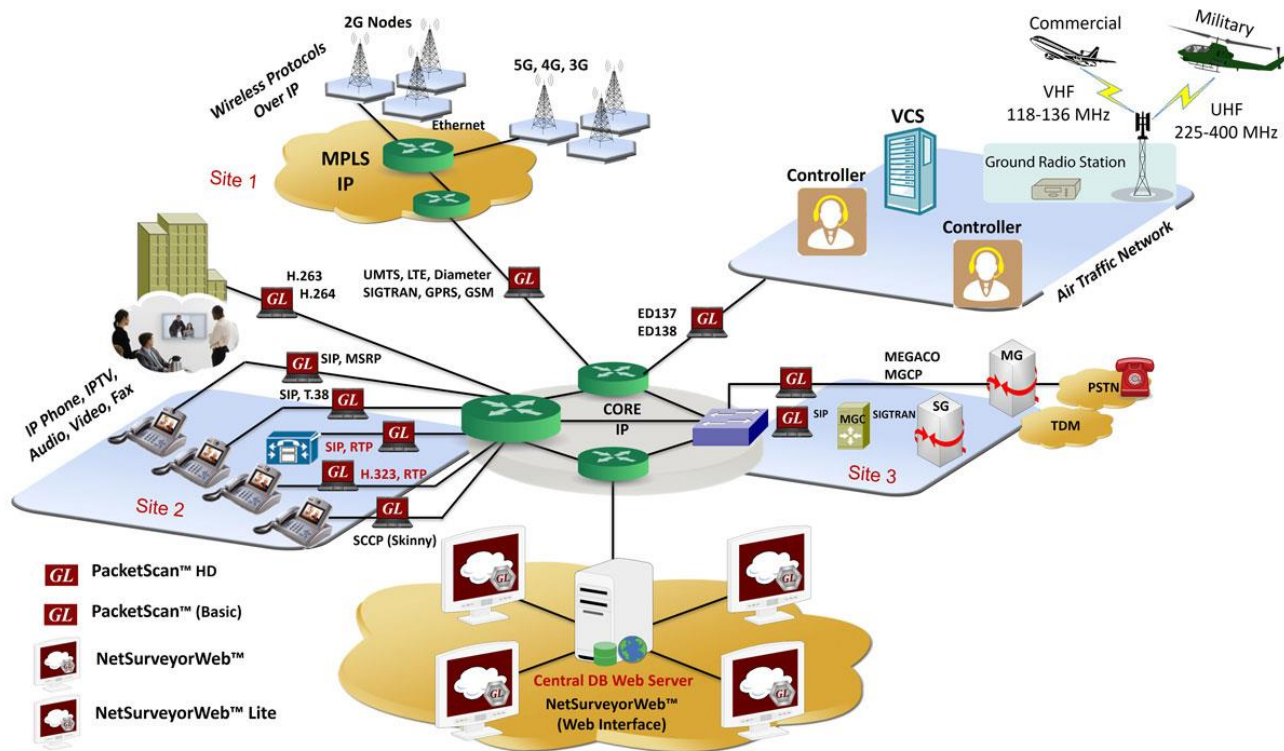
RTP/RTCP/Fax (T.38) Analysis



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

PacketScan™ All-IP Signaling and Traffic Analysis

(5G/4G/3G/2G/VoIP/RTP, RTCP/ Video Analysis)



What the Software does?

- Captures, segregates, and monitors packets; perform voice quality testing in real-time over VoIP network
- Non-intrusively capture real-time signaling and traffic packets for infinite time and provide call details of per call and aggregated protocol statistics
- Supports monitoring of 5G networks. It captures, segregates, monitors and collects statistics on all calls over N1/N2, N4, N8, N10, N11, N12 and N13 interfaces of the 5G network
- Can be deployed as a Probe for a centralized monitoring system with Oracle database

Applications

- **Real-time VoIP Traffic Analysis** –
 - Analyze 5G Calls
 - View RTP, SIP, MSRP, H.323, and MEGACO Calls
 - Trigger on Called and / or Calling Party, Packet Impairments
 - Save .HDL (GL's proprietary format) or .PCAP (Ethereal format) or *.PCAPNG file format
 - Save .WAV – time stamped file names
 - Save CDRs
 - MOS R-factor – view quality as the call proceeds
 - Traffic limited only by hard drive capacity
 - T.38 Fax packets decoding
- **Network Monitoring Solutions** –
 - Multiple probes can be used for network monitoring
 - CDRs can be exported in a text format to a flat file or a remote computer
- **Network Monitoring Solutions (Contd.)** –
 - CDRs can also be exported to an Oracle data base
 - Results can be accessed remotely using NetSurveyorWeb™, a simple web browser-based application
- Air Traffic Monitoring Solution
- Gateway Delay Measurement along with our TDM Protocol Analyzer

Main Features

<p><u>Comprehensive Analysis Tool</u></p>	<ul style="list-style-type: none">• Capture calls in real-time for infinite time non-intrusively• Detail Signaling, Audio, Video QoS statistics• Call flow graph and Pictorial representation of the statistics• Inband/Outband Detection, Wave graph, Audio play back, Audio/Video recording• Ability to export Call Data Records of completed calls in CSV file format• Complex Filtering and Search capabilities• Option to create multiple aggregate column groups and prioritize the groups as per the requirement to display the summary results efficiently• Allows the user to automatically create search/filter criteria from the current screen selection• Decode support for multi-layer tunneled traffic - GTP, GRE, VXLAN• Support export frame summary for tunneled traffic
<p><u>QOS Parameters and Performance Metrics</u></p>	<ul style="list-style-type: none">• E-model (G.107) based MOS/R-Factor scores• Media Delivery Index for video calls• H.263, H.264 codec support• Jitter, Delay, and Gap for Audio and Video traffic• Minimum, maximum, and average Round Trip Delay (RTD)• Reports Inband (DTMF & MF) events, Outband events as per RFC 2833 or RFC 4733 events, RTP/RTCP packet count per direction
<p><u>Triggers and Actions</u></p>	<ul style="list-style-type: none">• Captures calls based on filter criteria and performs set of actions for the completed calls such as recording, sending email, extraction of voice or fax traffic file

Main Features (Contd.)

<u>SIP Registration Details</u>	<ul style="list-style-type: none">• Registration statistics and trace messages depicted graphically
<u>As a Probe with Central Monitoring System – NetSurveyorWeb™</u>	<ul style="list-style-type: none">• PacketScan™ can send summary fields, frame octets, status, call detail records, along with traffic summary of captured calls to a central database.• NetSurveyorWeb™ displays the data from the database in a simple web-based browser. It features rich graphics, ladder diagrams, CDRs (Call Data Records), custom report and filter configurations
<u>Single Point Analysis System</u>	<ul style="list-style-type: none">• Enhanced to work with GL's Voice Band Analyzer and Call Data Records applications to provide useful call detail records for further analysis using <u>built-in tool in Excel®</u>.
Utilities	<ul style="list-style-type: none">• Provides HDL File Conversion utility to convert ethereal format file (*.PCAP, *.CAP, and *.PCAPNG) to GL's file format (*.HDL) and vice-versa• Includes Excel® Addins to import CDRs into Excel® to analyze using Pivot Table, and Pivot Charts.

Supported Protocols

- Session Initiation Protocol (SIP) - RFC 3261
- Media Gateway Control Protocol (MGCP) - RFC 2705/3435 (3991)
- Media Gateway Control (MEGACO) - RFC 3525 and 3015
- Message Session Relay Protocol (MSRP)
- H.323
- RTP/RTCP
- SCTP - RFC 2960
- Connection Oriented Transport Protocol (COTP, ISO 8073)
- 5G – N1N2, N4, N8, N12, N13
- SCCP (Skinny)
- SS7 SIGTRAN
- ISDN-SIGTRAN
- GSM A over IP
- GPRS over IP
- UMTS over IP
- LTE
- Diameter

Supported Codecs

- G.711 (mu-Law and A-Law), G.711 Application II (A-law and μ -law with VAD)
- G726 (40, 32, 24, 16kbps)
- GSM (13.2kbps), GSM EFR (12.2 kbit/s), GSM HR
- G729, G729B (8kbps)
- G.722, G.722.1
- ILBC_15_2 (for 20 msec), ILBC_13_33 (for 30 msec)
- SPEEX (Narrow band and Wideband)
- SMV* (Modes - 0, 1, 2 and 3)
- Video codecs include H263++ CIF 190, 350, 512 kbps, QCIF 64, 80, 128 kbps, and H264 codec offers video compression
- Other optional codec include (must be purchased with additional license)
 - AMR (Narrow band and Wideband)
 - EVRC, EVRC0 (Rates - 1/8, 1/2 and 1)
 - EVRCB, EVRCB0 (Rates - 1/8, 1/2 and 1); EVRC-C
 - Opus and EVS (Narrow Band, Wideband, Super Wideband, Full Band)

PacketScan™ Analyzer View

The screenshot displays the PacketScan 64-bit [off-line] interface with four main panes:

- Summary View:** A table listing network traffic. The first few rows are:

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4
✓	2	00:00:08.505065000	214		Internet IPI(IPv4)	RTP	192.168.1.103	192.168.1.200
✓	179	00:00:08.512592000	214		Internet IPI(IPv4)	RTP	192.168.1.200	192.168.1.103
✓	180	00:00:08.525697000	214		Internet IPI(IPv4)	RTP	192.168.1.103	192.168.1.200
✓	181	00:00:08.534167000	214		Internet IPI(IPv4)	RTP	192.168.1.200	192.168.1.103
✓	182	00:00:08.545392000	214		Internet IPI(IPv4)	RTP	192.168.1.103	192.168.1.200
✓	183	00:00:08.547365000	92		Internet IPI(IPv4)		192.168.1.75	192.168.1.255
✓	184	00:00:08.553866000	214		Internet IPI(IPv4)	RTP	192.168.1.200	192.168.1.103
- Detail View:** Shows Ethernet Frame Data for Device2 Frame=178. It lists fields such as Destination Address (x001676122661), Source Address (x0011116AF6D7), Length/Protocol Type (x0800 Internet IP(IPv4)), and IP Version (0100... (4)).
- Hex Dump View:** Displays the raw hex data of the frame, with ASCII characters on the right side for readability.
- CDR View:** A table showing Call Detail Records (CDR) with columns for Call ID, Call Status, Protocol, Call Originating (Number / Address), Call Destination (Number / Address), Call Start Date & Time, and Call Duration.

Summary View

Detail View

Hex Dump View

CDR View

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

Layer Copy/Show/Hide Options

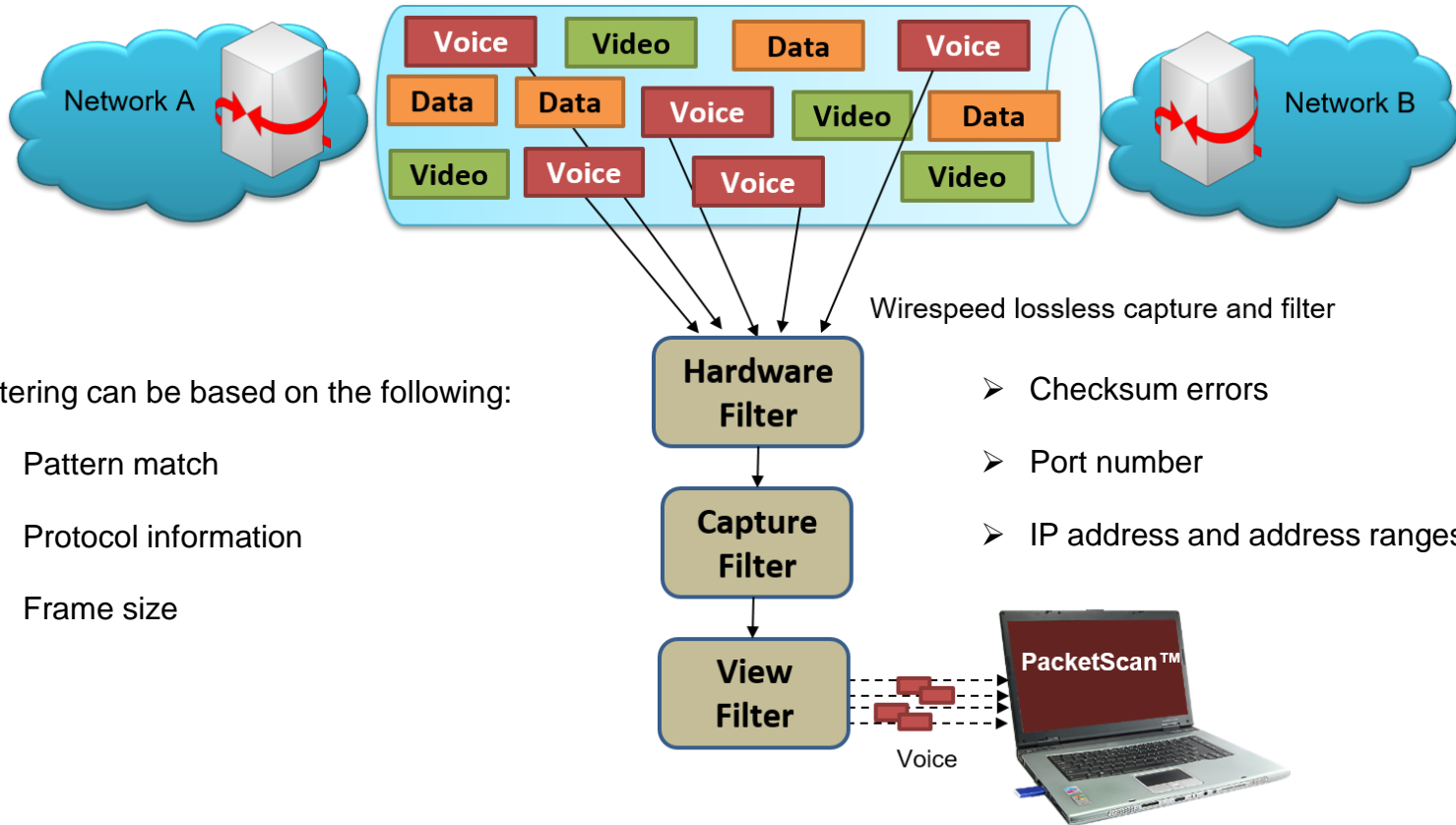
- Provides option to copy the entire layer decode information to the clipboard

The screenshot displays the PacketScan 64-bit application interface. The top window shows a table of captured packets with columns for Device, Frame#, TIME (Relative), Length (Bytes), Error, Length/Protocol Type MAC, Packet Type MAC, Source IP Address IPv4, and Destination IP IPv4. The bottom window shows the detailed view of an Ethernet frame, with the IPv4 layer selected and a context menu open. The context menu has two options: "Copy view to clipboard" and "Layer show/hide". A red arrow points from the "Copy view to clipboard" option to the right.

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP IPv4
✓ 2	0	00:00:00.00000000	82		Internet IPIIPv4		192.168.1.70	192.168.1.255
✓ 2	1	00:00:01.841976000	82		Internet IPIIPv4		192.168.1.142	255.255.255.255
✓ 2	2	00:00:02.347154000	836		Internet IPIIPv4	SIP	192.168.1.200	192.168.1.103
✓ 2	3	00:00:02.347730000	354		Internet IPIIPv4	SIP	192.168.1.103	192.168.1.200
✓ 2	4	00:00:02.349375000	355		Internet IPIIPv4	SIP	192.168.1.103	192.168.1.200
✓ 2	5	00:00:02.349532000	820		Internet IPIIPv4	SIP	192.168.1.103	192.168.1.200
✓ 2	6	00:00:04.467457000	92		Internet IPIIPv4		192.168.1.103	192.168.1.255
✓ 2	7	00:00:05.748389000	64		Internet IPIIPv4			
✓ 2	8	00:00:05.830627000	64		Internet IPIIPv4			
✓ 2	9	00:00:05.847465000	82		Internet IPIIPv4			
✓ 2	10	00:00:06.038679000	92		Internet IPIIPv4			

```
Ethernet Frame Data
***** MAC Layer *****
0000 Destination Address = xFFFFFFFFFFFF
0006 Source Address      = x0016760CFBD4
000C Length/Protocol Type = x0800 Internet IP(IPv4)
***** IPv4 Layer *****
000E Version = 010
000E Internet Header Length (In 32 bit words) = ...
000F Differentiated Services Field = ...
000F Differentiated Services Codepoint = 000000... Default
000F Explicit Congestion Notification = ...
IP Hdr No TCP SegmentationOffload =
0010 Total Length = 68 (x0044)
0012 Identification = 24272 (x5ED0)
0014 Reserved Bit = 0...
0014 Don't fragment = .0...
0014 More fragments = .0...
0014 Fragment Offset = 0 (...
0016 Time To Live = 128 (x80)
0017 Protocol = 00010001 UDP
0018 Header Check Sum = x5743
001A Source IP Address = 192.168.1.70 (xC0A80146)
001E Destination IP Address = 192.168.1.255 (xC0A801FF)
***** UDP Layer *****
0022 Source Port = 1025 (x0401)
0024 Destination Port = 1947 (x079B)
0026 Length (Header + Data) = 48 (x0030)
0028 Checksum = x9AC4
```

WireSpeed Filtering



- Filtering can be based on the following:

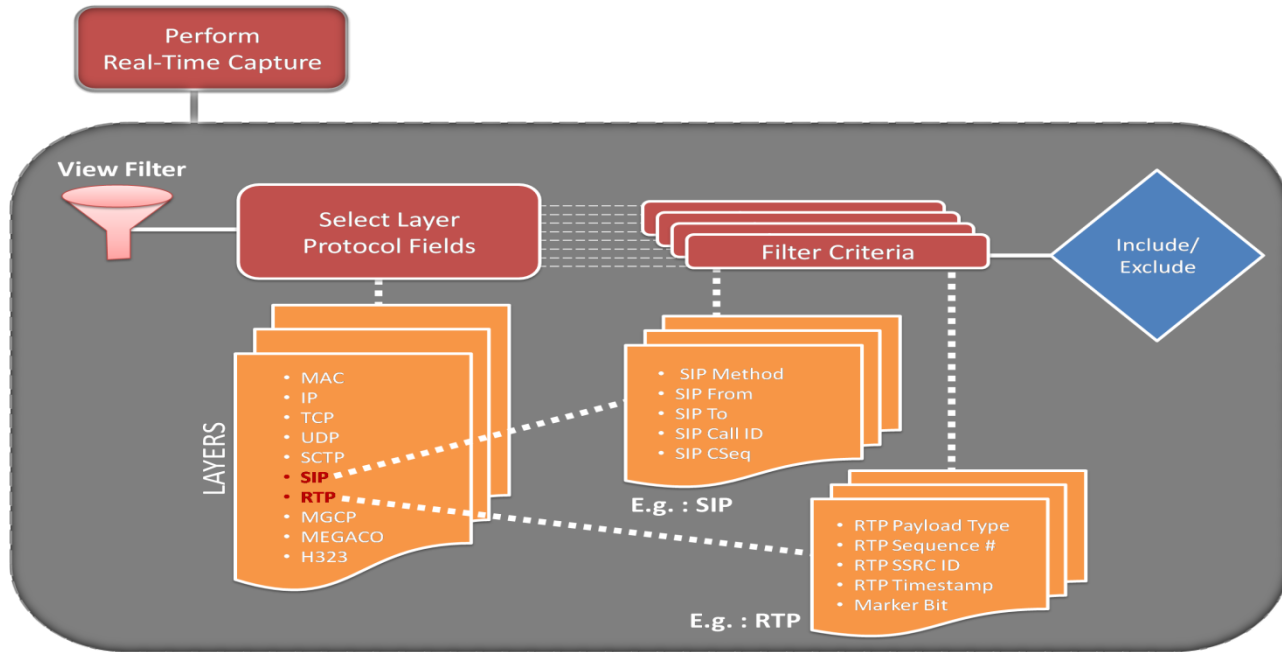
- Pattern match
- Protocol information
- Frame size

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

3 Stages of Filtering

- HardwareFilter (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

Real-time and Offline Filters



- Filtering and search capability isolates required frames from original frames in real-time / offline based on parameters set in Data Link layer, MAC layer, IP, TCP/UDP and more

Real-time Capture Filter

The screenshot shows the 'Protocol Capture Configuration' window. On the left, a sidebar contains 'Capture File Options', 'Card & Stream Selection', 'Capture Filter', and 'Gui & Protocol Options'. The main area is titled 'Capture Filters' and includes a 'Filter Selection' list on the left and a 'Filters' configuration panel on the right. A red arrow points from the 'RTP' entry in the list to the 'Filters' panel. The 'Filters' panel has checkboxes for 'Filter all RTP data' (checked), 'Auto Detect RTP' (checked), and 'Truncate RTP Packets' (unchecked). A 'Truncated Packet Length' field is set to '54'. At the top, there are options for 'Record Frames As Is' (checked with a help icon) and 'Packet Slicing' (unchecked) with a 'Length' field set to '14'. At the bottom, there are radio buttons for 'Include' (selected) and 'Exclude', and buttons for 'Deactivate Sel' and 'Deactivate All'.

Protocol Capture Configuration


Save Load Default

Capture File Options

Card & Stream Selection

Capture Filter

Gui & Protocol Options

Record Frames As Is  Packet Slicing Length

Capture Filters

Filter Selection

- Layers
 - Protocol
 - MAC
 - VLAN
 - IP (All Levels)
 - IP (Outer)
 - ESP
 - TCP
 - UDP
 - Inner IP
 - Inner UDP
 - SCTP
 - SIP
 - RTP**
 - MSRP
 - MGCP
 - MEGACO
 - H323
 - RTSP

Filters

- Filter all RTP data
- Auto Detect RTP
- Truncate RTP Packets
 - Truncated Packet Length :

Include Exclude

Deactivate Sel Deactivate All

Display Filter (Offline)

The screenshot shows the 'Analyzer GUI and Protocol Configuration' window. On the left is a sidebar with various configuration options, including 'View Filter' which is highlighted. The main area is divided into three sections:

- Filter Selection:** A tree view showing protocol layers. 'RTP' is expanded, and 'RTP Payload Type' is selected with a red checkmark. A red arrow points from this selection to the right panel.
- RTP Payload Type Value:** A list of audio payload types. 'Comfort Noise' is selected and highlighted in blue. Below the list are 'Activate' and 'Deactivate' buttons.
- All Selected:** A table showing the current filter configuration.

Layer	Field	Filter Value
RTP	RTP Payload Type	Comfort Noise

At the bottom, there are radio buttons for 'Conditions for all selections': AND, OR, Include, and Exclude. The 'OR' and 'Include' options are selected. There are also 'Deactivate Sel' and 'Deactivate All' buttons.

Encapsulated Security Payload (ESP) Deciphering

The image shows two overlapping windows from a network analysis tool. The top window is titled "Protocol Capture Configuration" and has a sidebar with options like "Capture File Options", "Card & Stream Selection", "Capture Filter", and "Gui & Protocol Options". The main area shows "Capture Filters" with a tree view of layers including Protocol, MAC, VLAN, IP (All Levels), IP (Outer), ESP, TCP, and UDP. The "Filters" section has checkboxes for "Filter all ESP data" and "Decode Encrypted ESP Payload", with a sub-section for "Extract" containing radio buttons for "Original Encrypted Payload" and "Deciphered Payload". An "ESP SAs" button is visible.

The bottom window is titled "ESP SAs" and contains a table with the following columns: IP Protocol, Src IP, Dest IP, SPI, Encryption, Encryption Key, Authentication, and Authentication Key. The table lists several entries for IPv4 with various IP addresses and SPI values.

IP Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key	Authentication	Authentication Key
IPv4	192.168.12.86	192.168.12.45	0x05d2ede0	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.45	x.x.x.x	0x467113ba	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.86	192.168.12.251	0xd02382c2	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.251	192.168.12.86	0x129e7b1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.90	192.168.12.45	0xa5e7259a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.45	*	0x9637e4c8	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	192.168.12.90	192.168.12.251	0x57be7f1a	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...
IPv4	*	192.168.12.90	*	AES-CBC [RFC3602]	0x97D055ABC4E0826C394DC0F2CCBE6...	HMAC-MD5-96 [RFC2403]	0x6CC1C7BE902D253286386E7B7C...

- ESP filter is used to provide **ESP SAs value** to decrypt ESP packets

Comparison of Before and After ESP Deciphering

PacketScan 64-bit

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type	Packet Type	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓	1	00:00:00.0000000000	822		Internet IPIPV4		192.168.12.86	192.168.12.45	
✓	1	00:00:00.515721000	822		Internet IPIPV4		192.168.12.86	192.168.12.45	
✓	1	00:00:01.537143000	822		Internet IPIPV4		192.168.12.86	192.168.12.45	
✓	1	00:00:03.558945000	822		Internet IPIPV4		192.168.12.86	192.168.12.45	
✓	1	00:00:04.626310000	806		Internet IPIPV4		192.168.12.90	192.168.12.45	
✓	1	00:00:05.143077000	806		Internet IPIPV4		192.168.12.90	192.168.12.45	
✓	1	00:00:06.165570000	806		Internet IPIPV4		192.168.12.90	192.168.12.45	

Device Frame# at 00:00:00.0000000000 OK Len=822

Ethernet Frame Data

```

***** MAC Layer *****
0000 Destination Address      = xE0D5EADFBD
0006 Source Address          = xFCAA1492AB2F
000C Length/Protocol Type    = x0800 Internet IP(IPv4)
***** IP4 Layer *****
000E Version                  = 0100.... (4)
000E Internet Header Length (In 32 bit words) = ...0101 (5)
0016 Differentiated Services Field
000F Differentiated Services Codepoint      = 00000000... Default
000F Explicit Congestion Notification      = .....00 Not-ECT (Not ECN-Capable Transport)
IP Hdr No TCP Segmentation/Offset
0010 Total Length                = 808 (x0328)
0012 Identification              = 31181 (x79CD)
0014 Reserved Bit                 = 0..... Not Set
0014 Don't fragment               = 0..... Not Set
0014 More fragments               = 0..... Not Set
0014 Fragment Offset              = 0 (.....000000 00000000)
0016 Time To Live                 = 128 (x80)
0017 Protocol                     = 00110010 Encap Security Payload
0018 Header Check Sum             = x2403
001A Source IP Address            = 192.168.12.86 (xC0A80C56)
001E Destination IP Address      = 192.168.12.45 (xC0A80C2D)
***** Encapsulating Security Payload (Protocol) Layer *****
0022 Security Parameter Index     = 97709536 (x05D2EDE0)
0026 Sequence Number              = 1 (x00000001)
ESP Payload Data                  = x49F74319A723AF44...BFA3074B9C6D5534 (Length=

```

*** Right click to SHOW/HIDE layer details or copy ***

Before Deciphering

PacketScan 64-bit

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type	Packet Type	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓	1	00:00:00.0000000000	768		Internet IPIPV4	SIP	192.168.12.86	192.168.12.45	
✓	1	00:00:00.515721000	768		Internet IPIPV4	SIP	192.168.12.86	192.168.12.45	
✓	1	00:00:01.537143000	768		Internet IPIPV4	SIP	192.168.12.86	192.168.12.45	
✓	1	00:00:03.558945000	768		Internet IPIPV4	SIP	192.168.12.86	192.168.12.45	
✓	1	00:00:04.626310000	764		Internet IPIPV4	SIP	192.168.12.90	192.168.12.45	

0018 Header Check Sum = x2403

001A Source IP Address = 192.168.12.86 (xC0A80C56)

001E Destination IP Address = 192.168.12.45 (xC0A80C2D)

***** UDP Layer *****

0022 Source Port = 5060 (x13C4)

0024 Destination Port = 5060 (x13C4)

0026 Length (Header + Data) = 735 (x02DF)

0028 Checksum = x16FB

***** SIP Layer *****

```

HDR
HDR = INVITE sip:0001@192.168.12.45 SIP/2.0
HDR = Via: SIP/2.0/UDP 192.168.12.86:5060;branch=z9hG4bK-29-103772070-10509-4472
HDR = Max-Forwards: 70
HDR = Allow: INVITE, BYE, CANCEL, ACK, INFO, OPTIONS, SUBSCRIBE, NOTIFY, REFER, REGISTER, UPDATE
HDR = From: 0001 <sip:0001@192.168.12.86>;tag=FromTag-26-103772070-10506-4472
HDR = To: 0001 <sip:0001@192.168.12.45>
HDR = Call-ID: GL-NAPS-28-103772070-10508-4472@192.168.12.86
HDR = CSeq: 1 INVITE
HDR = Contact: 0001 <sip:0001@192.168.12.86>
HDR = Content-Type: application/sdp
HDR = Content-Length: 238
HDR =
HDR = v=0
HDR = o=0001 31062954 1 IN IP4 192.168.12.90
HDR = s=SIP Call
HDR = c=IN IP4 192.168.12.90
HDR = t=0
HDR = m=audio 1034 RTP/AVP 0 8 101
HDR = a=rtpmap:0 PCMU/8000
HDR = a=rtpmap:8 PCMA/8000
HDR = a=rtpmap:101 telephone-event/8000
HDR = a=rtsp:101 0-15
HDR = a=ptime:20
HDR = a=sendrecv

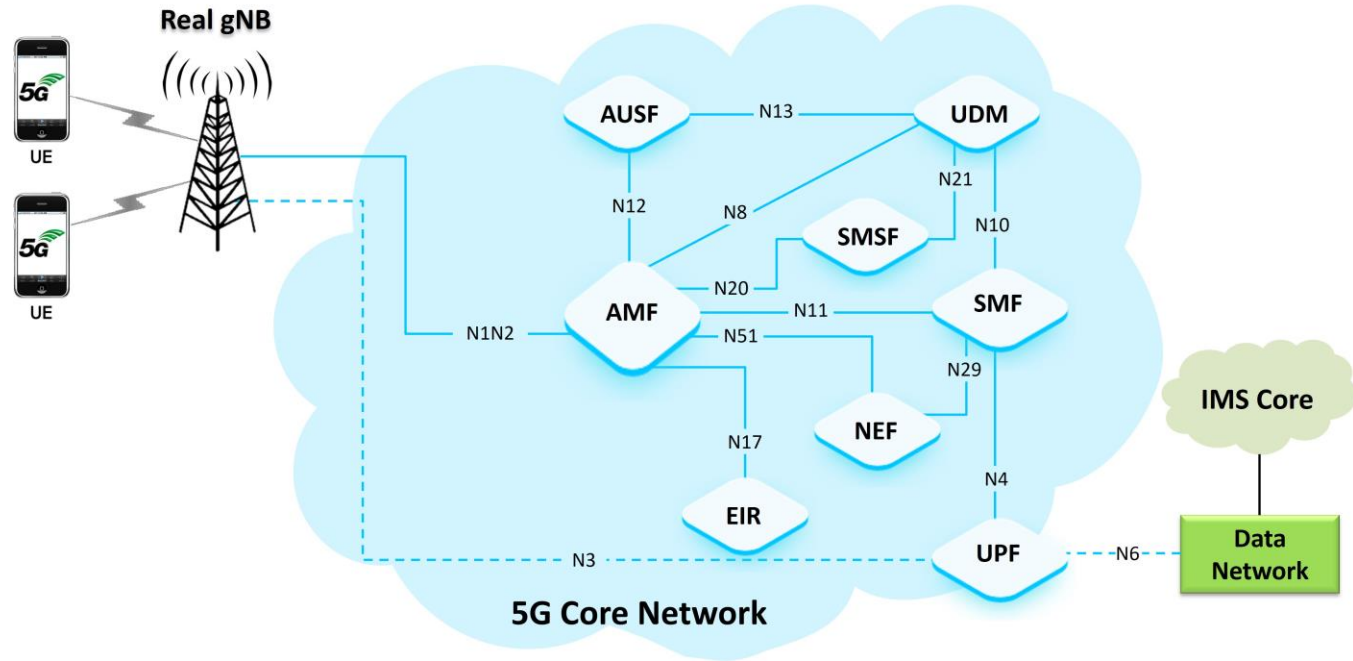
```

Off-line Viewing. C:\Users\Sunil\Desktop\FastRecorderAndPacketExtractor, 56 Frames

After Deciphering

5G Analyzer

- Captures, segregates, monitors and collects statistics on all calls over N1/N2, N4, N8, N12 and N13 interfaces of the 5G network
- Provides VoNR call statistics such as caller, callee, MOS scores, discarded packets and voice storage



Decode View - 5G NGAP Layer

PacketScan G4-bit

File View Capture Statistics Database Call Detail Records Configure Help

2609 GoTo

Device	Frame#	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓	2609	2023-06-13 15:02:20.228319000	158		Internet IPIIPv4		192.168.13.181	192.168.13.184	
✓	2610	2023-06-13 15:02:20.228391000	277		Internet IPIIPv4		192.168.13.184	192.168.13.191	
✓	2611	2023-06-13 15:02:20.228391000	162		Internet IPIIPv4		192.168.13.184	192.168.13.191	
✓	2612	2023-06-13 15:02:20.228391000	169		Internet IPIIPv4		192.168.13.184	192.168.13.191	
✓	2613	2023-06-13 15:02:20.228496000	162		Internet IPIIPv4		192.168.13.184	192.168.13.191	
✓	2614	2023-06-13 15:02:20.228601000	169		Internet IPIIPv4		192.168.13.184	192.168.13.191	
✓	2615	2023-06-13 15:02:20.228706000	315		Internet IPIIPv4		192.168.13.191	192.168.13.188	
✓	2616	2023-06-13 15:02:20.228706000	193		Internet IPIIPv4		192.168.13.191	192.168.13.188	
✓	2617	2023-06-13 15:02:20.228706000	176		Internet IPIIPv4		192.168.13.191	192.168.13.188	
✓	2618	2023-06-13 15:02:20.229812000	193		Internet IPIIPv4		192.168.13.191	192.168.13.188	
✓	2619	2023-06-13 15:02:20.229917000	176		Internet IPIIPv4		192.168.13.191	192.168.13.188	
✓	2620	2023-06-13 15:02:20.230022000	393		Internet IPIIPv4		192.168.13.188	192.168.13.191	
✓	2621	2023-06-13 15:02:20.230022000	82		Internet IPIIPv4		192.168.13.188	192.168.13.191	
✓	2622	2023-06-13 15:02:20.230022000	365		Internet IPIIPv4		192.168.13.188	192.168.13.191	
✓	2623	2023-06-13 15:02:20.230127000	82		Internet IPIIPv4		192.168.13.188	192.168.13.191	
✓	2624	2023-06-13 15:02:20.230232000	365		Internet IPIIPv4		192.168.13.188	192.168.13.191	
✓	2625	2023-06-13 15:02:20.230336000	60		Internet IPIIPv4		192.168.13.191	192.168.13.184	

003A - Payload Protocol Identifier = x0000003C NGAP

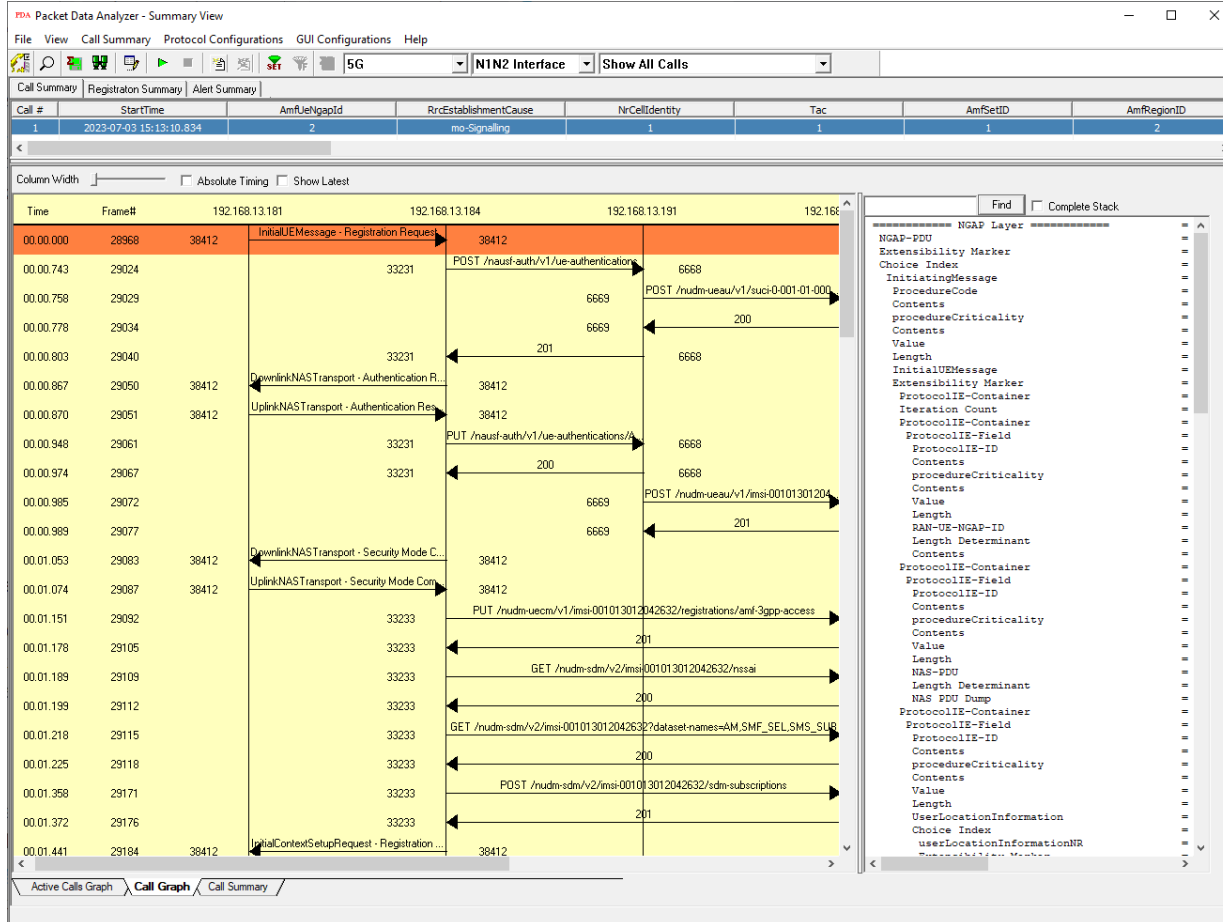
===== NGAP Layer =====

- NGAP-PDU = CHOICE
- Extensibility Marker = 0
- Choice Index = 0
- InitiatingMessage = SEQUENCE
- ProcedureCode = INTEGER
- Contents = 15 id-InitialUEMessage
- procedureCriticality = ENUMERATOR
- Contents = 0 reject(0)
- Value = Open Type
- Length = 92
- InitialUEMessage = SEQUENCE
- Extensibility Marker = 0
- ProtocolIE-Container = SEQUENCE OF
- Iteration Count = 6
- ProtocolIE-Container = Instance 0
- ProtocolIE-Field = SEQUENCE
- ProtocolIE-ID = INTEGER
- Contents = 85 id-RAN-UE-NGAP-ID
- procedureCriticality = ENUMERATOR
- Contents = 0 reject(0)
- Value = Open Type
- Length = 2
- RAN-UE-NGAP-ID = INTEGER
- Length Determinant = 1
- Contents = 2
- ProtocolIE-Container = Instance 1
- ProtocolIE-Field = SEQUENCE
- ProtocolIE-ID = INTEGER
- Contents = 38 id-NAS-PDU
- procedureCriticality = ENUMERATOR
- Contents = 0 reject(0)
- Value = Open Type
- Length = 44
- NAS-PDU = OCTET STRING
- Length Determinant = 43
- NAS PDU Dump = x7E00417100D0100F11000000003214062231001002E02C0E02F0201015200F110000001180100530101
- ProtocolIE-Container = Instance 2
- ProtocolIE-Field = SEQUENCE
- ProtocolIE-ID = INTEGER

GL Communications

C:\Program Files\GL Communications Inc\PacketScan\temp.h Captured 47 036 frames Missed Frames: 0

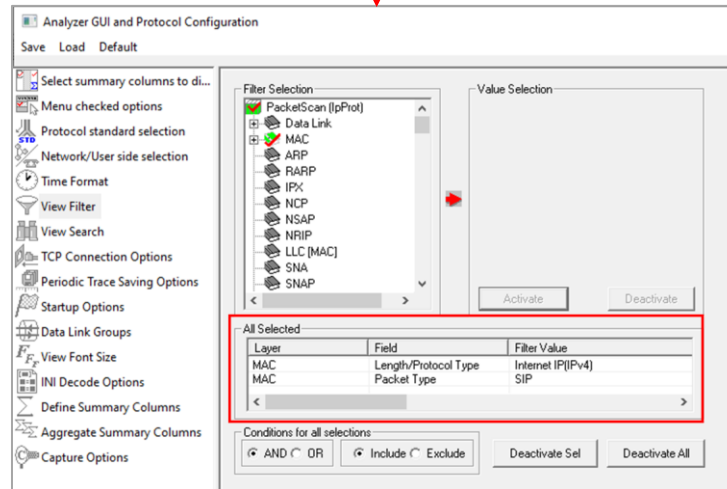
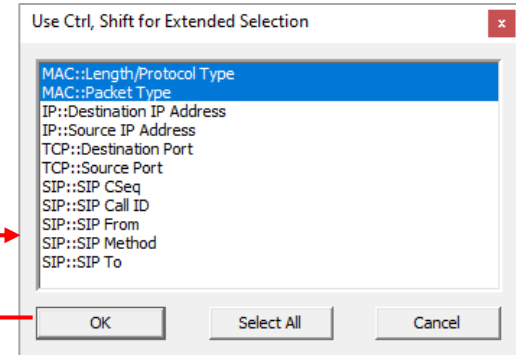
Call Graph – 5G N1N2



Filter Criteria From Screen Selection

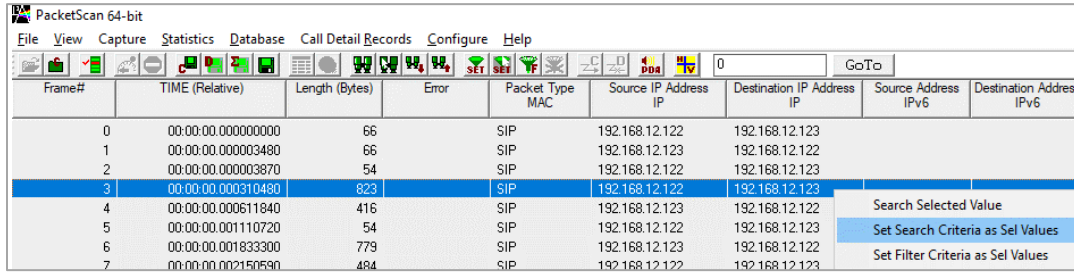
- Allows the user to automatically create filter criteria from the current screen selection

Frame#	TIME (Relative)	Length (Bytes)	Error	Packet Type	Source IP Address	Destination IP Address	Source Address IPv6	Destination Address IPv6
0	00:00:00.000000000	66		SIP	192.168.12.122	192.168.12.123		
1	00:00:00.000003480	66		SIP	192.168.12.123	192.168.12.122		
2	00:00:00.000003870	54		SIP	192.168.12.122	192.168.12.123		
3	00:00:00.000310480	823		SIP	192.168.12.122	192.168.12.123		
4	00:00:00.000611840	416		SIP	192.168.12.123	192.168.12.122		
5	00:00:00.001110720	54		SIP	192.168.12.122	192.168.12.123		
6	00:00:00.001833300	779		SIP	192.168.12.123	192.168.12.122		
7	00:00:00.002150580	484		SIP	192.168.12.122	192.168.12.123		

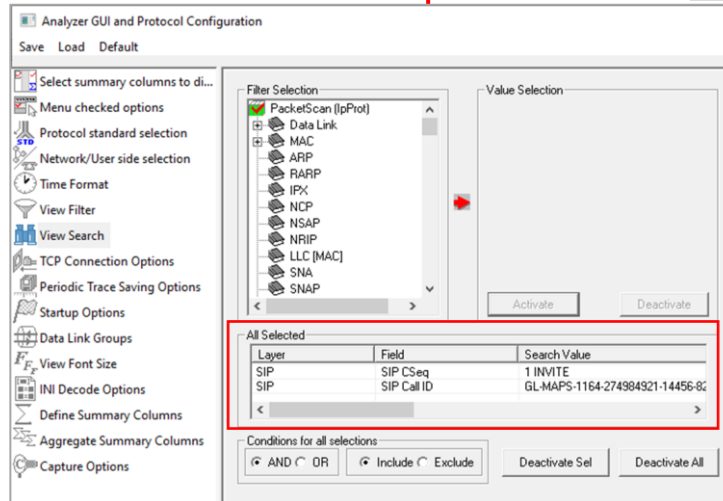
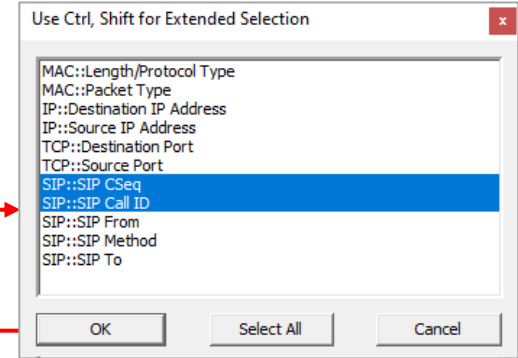


Search Criteria From Screen Selection

- Allows the user to automatically create search criteria from the current screen selection



Frame#	TIME (Relative)	Length (Bytes)	Error	Packet Type MAC	Source IP Address IP	Destination IP Address IP	Source Address IPv6	Destination Address IPv6
0	00:00:00.000000000	66		SIP	192.168.12.122	192.168.12.123		
1	00:00:00.000003480	66		SIP	192.168.12.123	192.168.12.122		
2	00:00:00.000003870	54		SIP	192.168.12.122	192.168.12.123		
3	00:00:00.000310480	823		SIP	192.168.12.122	192.168.12.123		
4	00:00:00.000611840	416		SIP	192.168.12.123	192.168.12.122		
5	00:00:00.001110720	54		SIP	192.168.12.122	192.168.12.123		
6	00:00:00.001833300	779		SIP	192.168.12.123	192.168.12.122		
7	00:00:00.002150590	484		SIP	192.168.12.122	192.168.12.123		



Aggregate Summary Columns

Aggregate Summary Columns

Save Load Default

Select summary columns to di...
Menu checked options
Protocol standard selection
Network/User side selection
Time Format
View Filter
View Search
TCP Connection Options
Periodic Trace Saving Options
Startup Options
Data Link Groups
View Font Size
INI Decode Options
Define Summary Columns
Aggregate Summary Columns
Capture Options

Add Delete Aliases Reorder Reverse Use '_' in the name for multiline headers

Name	Display Format	Summary Columns	Separator
Source IP ----> Destination IP	Concat	Destination IP_Address_IP Source IP_Address_IP	---->

PacketScan 64-bit

File View Capture Statistics Database Call Detail Records Configure Help

Frame#	TIME (Relative)	Length (Bytes)	Packet Type MAC	Source IP -> Destination IP	Error	Length/Protocol Type MAC	Source IP Address IP	Destination IP Address IP	Destinat TC
3	00:00:00.000310480	823	SIP	192.168.12.123 -> 192.168.12.123		Internet IP(IPv4)	192.168.12.122	192.168.12.123	5060
4	00:00:00.000611840	416	SIP	192.168.12.122 -> 192.168.12.123		Internet IP(IPv4)	192.168.12.123	192.168.12.122	57494
5	00:00:00.001110720	54	SIP	192.168.12.123 -> 192.168.12.122		Internet IP(IPv4)	192.168.12.122	192.168.12.123	5060
6	00:00:00.001833000	779	SIP	192.168.12.122 -> 192.168.12.123		Internet IP(IPv4)	192.168.12.123	192.168.12.122	57494
7	00:00:00.002150590	484	SIP	192.168.12.123 -> 192.168.12.122		Internet IP(IPv4)	192.168.12.122	192.168.12.123	5060
8	00:00:00.002188670	214	RTP	192.168.12.123 -> 192.168.12.122		Internet IP(IPv4)	192.168.12.122	192.168.12.123	
9	00:00:00.002216600	214	RTP	192.168.12.122 -> 192.168.12.123		Internet IP(IPv4)	192.168.12.123	192.168.12.122	

Device2 Frame=3 at 00:00:00.000310480 OK Len=823 *** Right click to SHOW/HIDE layer details

Ethernet Frame Data

```
===== MAC Layer =====  
0000 Destination Address      = xFCAA149CBF99  
0006 Source Address          = xFCAA149CBF9B  
000C Length/Protocol Type    = x0800 Internet IP(IPv4)  
===== IP Layer =====  
000E Version                  = 0100.... (4)  
000E Internet Header Length (In 32 bit words) = ...0101 (5)  
Differentiated Services Field  
000F Differentiated Services Codepoint      = 0000000.. Default  
000F Explicit Congestion Notification      = .....00 Not-ECT (Not ECN-Capable Transport)  
IP Hdr No TCP SegmentationOffload  
0010 Total Length                = 809 (x0329)  
0012 Identification              = 28511 (x6F5F)  
0014 Reserved Bit                 = 0..... Not Set  
0014 Don't fragment               = .1..... Set  
0014 More fragments              = .0..... Not Set  
0014 Fragment Offset             = 0 (...000000 00000000)  
0016 Time To Live                 = 128 (x80)  
0017 Protocol                     = 00000110 TCP  
0018 Header Check Sum             = x0000  
001A Source IP Address            = 192.168.12.122 (xC0A80C7A)  
001E Destination IP Address      = 192.168.12.123 (xC0A80C7B)
```

Off-line Viewing. C:\Users\Archana\Desktop\Aggregate Summar 11 Frames

Aggregate Summary Column Group

- The user can create multiple aggregate column groups and prioritize the groups as per the requirement to display the summary results efficiently

The image shows two windows. The top window is titled 'Aggregate Summary Columns' and is used for configuring summary columns. The bottom window is a network traffic capture tool showing a list of packets and a detailed view of a selected packet.

Aggregate Summary Columns Configuration:

Name	Display Format	Summary Columns	Separator
Group-0	Col_Alias Value	SIP Method_SIP SIP From_SIP SIP To_SIP SIP Call ID_SIP SIP CSeq_SIP	,
Group-1	Col_Alias Value	SSRC Identif Sequence N TimeStamp Marker bit	,
Group-2	Concat	Source Port Destination	

Network Traffic Capture (Packetscan 64-bit):

Frame#	TIME (Relative)	Length (Bytes)	Packet Type	MAC	Error	Length/Protocol Type	Source IP / MAC	Destination IP / MAC
3	00:00:00.000310480	823	SIP					
4	00:00:00.000611840	416	SIP					
5	00:00:00.001107020	54	SIP					
6	00:00:00.001603300	779	SIP					
7	00:00:00.002105950	404	SIP					
8	00:00:00.002188670	214	RTP					
9	00:00:00.002216600	214	RTP					

Detailed Packet View (Frame #3):

```

Device2 Frame#3 at 00:00:00.000310480 OK Len=823
Ethernet Frame Data
----- MAC Layer -----
0000 Destination Address          = xFCAA149CBF99
0006 Source Address              = xFCAA149CBF9B
000C Length/Protocol Type       = x8000 Internet IP(IPv4)
----- IP Layer -----
000E Version                     = 0100 (4)
000E Internet Header Length (In 32 bit words) = ...0101 (5)
000F Differentiated Services Codepoint = 00000000 Default
000F Explicit Congestion Notification IP Hdr No TCP SegmentationOffload = .....00 Hot-BCT (Not ECN-Capable Transport)
0010 Total Length                 = 809 (x0329)
0012 Identification              = 28511 (x6F3F)
0014 Reserved Bit                 = 0 (.....) Not Set
0014 Don't fragment              = 1 (.....) Set
0014 More fragments              = 0 (.....) Not Set
0014 Fragment Offset             = 0 (.....00000 00000000)
0016 Time To Live                 = 128 (x80)
0017 Protocol                    = 00000110 TCP
0018 Header Check Sum            = x0000
001A Source IP Address           = 192.168.12.122 (xC0A80C7A)
001E Destination IP Address      = 192.168.12.123 (xC0A80C7B)
----- TCP Layer -----
0022 Source Port                 = 57494 (xE096)
0024 Destination Port           = 5060 (x13C4)
0026 Sequence Number            = 341469455 (xC8B81A9B)
002A Acknowledgement Number     = 3548904125 (xD387FABD)
002E Data Offset                 = 0101 (5)
003E Reserved                   = .....0000 (0)
    
```


Copy Frames to Memory File

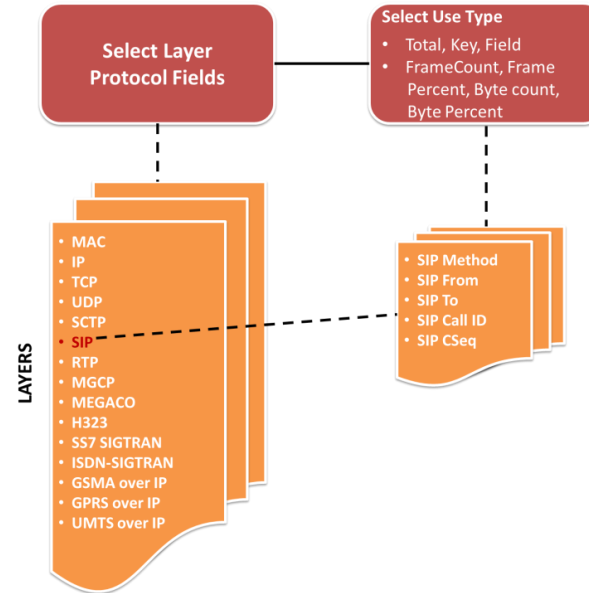
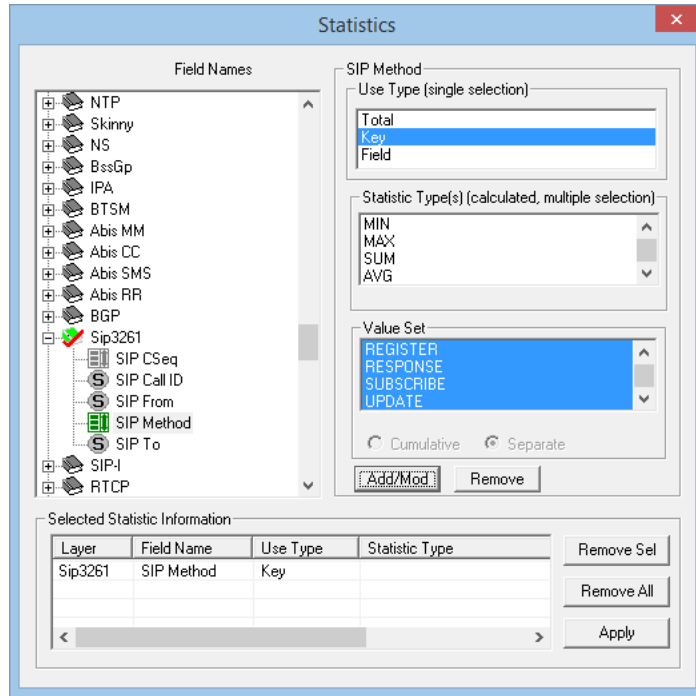
- The user can select and copy the frames (frame range) to the desired location

The screenshot shows the PacketScan 64-bit interface with a list of captured frames. A dialog box titled "Copy Frames to Memory File" is open, allowing the user to specify the number of frames and the range to copy.

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC
✓ 2	0	00:00:00.000000000	82		Internet IP(IPv4)	
✓ 2	1	00:00:01.841976000	82		Internet IP(IPv4)	
✓ 2	2	00:00:02.347154000	836		Internet IP(IPv4)	SIP
✓ 2	3	00:00:02.347730000	354		Internet IP(IPv4)	SIP
✓ 2	4	00:00:02.349375000	355		Internet IP(IPv4)	SIP
✓ 2	5	00:00:02.349532000	820		Internet IP(IPv4)	SIP
✓ 2	6	00:00:04.467457000	82		Internet IP(IPv4)	
✓ 2	7					
✓ 2	8					
✓ 2	9					
✓ 2	10					

Device2 Frame=0 at
Ethernet Frame Data
===== MA
0000 Destination Ad
0006 Source Address
000C Length/Protoc
===== IP
000E Version = 0100.... (4)
000E Internet Header Length (In 32 bit words) =0101 (5)
Differentiated Services Field =
000F Differentiated Services Codepoint = 000000.. Default
000F Explicit Congestion Notification =00 Not-ECT (Not ECN-Capable Transport)
IP Hdr No TCP SegmentationOffload =
0010 Total Length = 68 (x0044)
0012 Identification = 24272 (x5ED0)
0014 Reserved Bit = 0..... Not Set

Statistics

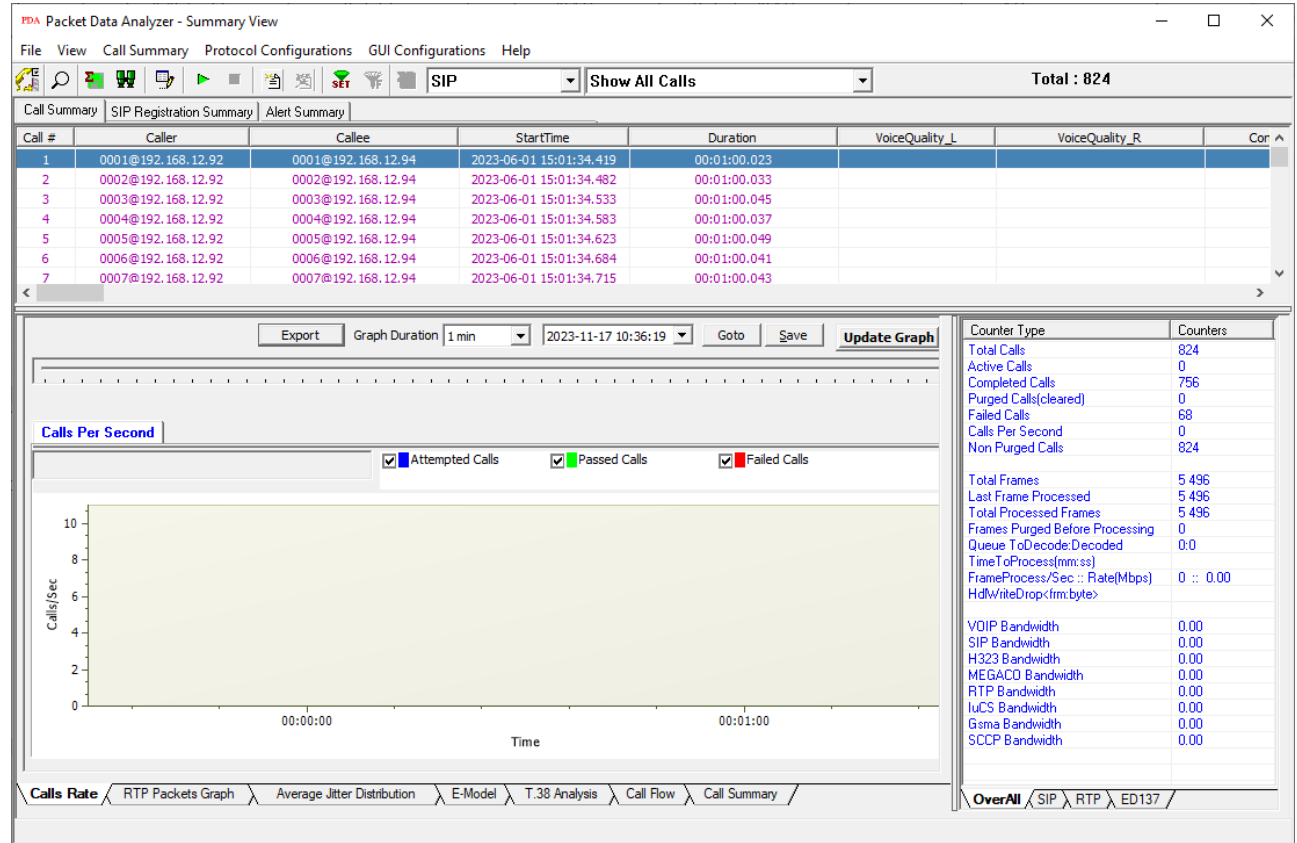


E.g. Device # (Its type Numeric)
 Timestamp (String values)
 ARP Hardware type (with predefined value set)

- Various statistics can be obtained to study the performance and trend in the VoIP network, based on protocol fields and different parameters

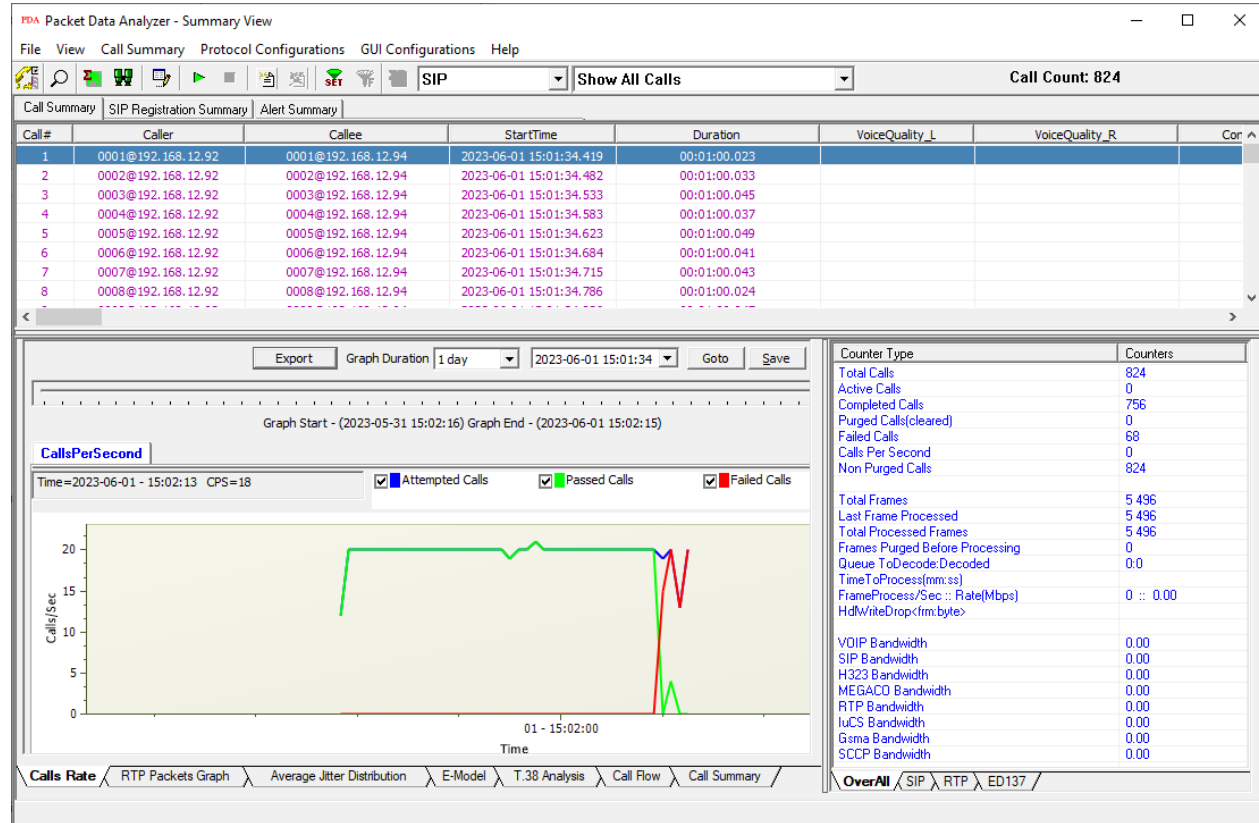
Packet Data Analysis

- Packet Data Analysis in PacketScan™ displays the following views
 - Summary view
 - Detail view
 - Registration summary view



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 Filter 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 "ErrorCode==400||ErrorCode>600" will display calls with ErrorCode equal to 400 and calls with ErrorCode greater than 600

PDA Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

SIP Show Filtered Calls Call Count: 6

ErrorCode==400 || ErrorCode>600

Payload_R	ErrorCode	FailureCause	CallID	EndTime	PostDialDelay	SessionDisconnectDe
	400	5	GL-MAPS-2654-766727097-26124-3688@192.168.12.92	2023-06-01 15:02:12.275	9	0
	603	4	GL-MAPS-2679-766728649-26314-14696@192.168.12.92	2023-06-01 15:02:13.828	9	0
	604	4	GL-MAPS-2677-766728698-26320-13540@192.168.12.92	2023-06-01 15:02:13.879	19	0
	606	4	GL-MAPS-2677-766728748-26326-14572@192.168.12.92	2023-06-01 15:02:13.919	9	0
	400	5	GL-MAPS-2685-766728798-26332-6156@fe80::3f20:7953:f2df:f26a	2023-06-01 15:02:13.973	18	0
	606	4	GL-MAPS-2709-766730449-26530-14696@fe80::3f20:7953:f2df:f26a	2023-06-01 15:02:15.632	9	0

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

The screenshot displays the PDA Packet Data Analyzer interface. The main window shows a table of call records. A context menu is open over the third row, with the 'Save Call' option selected. A dialog box titled 'PDA Save Call - CallNum_3' is open, allowing the user to choose the file format (HDL File, PCAP File, PCAPNG) and the save path. The dialog also includes checkboxes for 'Overwrite Files' and buttons for 'Save Call(s)' and 'Exit'.

Call #	Caller	Callee	StartTime	Duration	VoiceQuality_L	VoiceQuality_R	Cor
1	0001@192.168.12.92	0001@192.168.12.94	2023-06-01 15:01:34.419	00:01:00.023			
2	0002@192.168.12.92	0002@192.168.12.94	2023-06-01 15:01:34.482	00:01:00.033			
3	0003@192.168.12.92	0003@192.168.12.94	2023-06-01 15:01:34.533				
4	0004@192.168.12.92	0004@192.168.12.94	2023-06-01 15:01:34.583				
5	0005@192.168.12.92	0005@192.168.12.94	2023-06-01 15:01:34.623				
6	0006@192.168.12.92	0006@192.168.12.94	2023-06-01 15:01:34.684	00:01:00.041			
7	0007@192.168.12.92	0007@192.168.12.94	2023-06-01 15:01:34.715	00:01:00.043			
8	0008@192.168.12.92	0008@192.168.12.94					

PDA Save Call - CallNum_3

File Type: HDL File PCAP File PCAPNG Link Type: 0

Path: C:\Program Files\GL Communications Inc\PacketScan\

Overwrite Files

Counters:

Counters	Value
824	824
0	0
756	756
0	0
68	68
0	0
824	824
5496	5496
5496	5496
5496	5496
0	0
0.0	0.0
0.0	0.0
0.0	0.0
0.0	0.0
0.0	0.0
0.0	0.0
0.0	0.0
0.0	0.0
0.0	0.0

VOIP Bandwidth: 0.00
SIP Bandwidth: 0.00
H323 Bandwidth: 0.00
MEGACO Bandwidth: 0.00
RTP Bandwidth: 0.00
IuCS Bandwidth: 0.00
Gsm Bandwidth: 0.00
SCCP Bandwidth: 0.00

01 - 15:02:00

Calls/Sec

Time

Call Rate RTP Packets Graph Average Jitter Distribution E-Model T.38 Analysis Call Flow Call Summary

OverAll SIP RTP ED137

Copy Cell Value to Clipboard

Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

SIP Show All Calls Total : 824

Call Summary SIP Registration Summary Alert Summary

Call #	Caller	Callee	StartTime	Duration	VoiceQuality_L	VoiceQuality_R	Cor
1	0001@192.168.12.92	0001@192.168.12.94	2023-06-01 15:01:34.419	00:01:00.023			
2	0002@192.168.12.92	0002@192.168.12.94	2023-06-01 15:01:34.482	00:01:00.033			
3	0003@192.168.12.92	0003@192.168.12.94	2023-06-01 15:01:34.533				
4	0004@192.168.12.92	0004@192.168.12.94	2023-06-01 15:01:34.584				
5	0005@192.168.12.92	0005@192.168.12.94	2023-06-01 15:01:34.635				
6	0006@192.168.12.92	0006@192.168.12.94	2023-06-01 15:01:34.686	00:01:00.041			
7	0007@192.168.12.92	0007@192.168.12.94	2023-06-01 15:01:34.715	00:01:00.043			
8	0008@192.168.12.92	0008@192.168.12.94	2023-06-01 15:01:34.786	00:01:00.024			

Save Call
Copy Cell Value

*Untitled - Notepad

File Edit Format View Help

2023-06-01 15:01:34.533
00:01:00.045
0003@192.168.12.92

Export Graph Duration 5 days 2023-06-01 15:01:34 Goto Save

Graph Start - (2023-05-27 15:02:16) Graph End - (2023-06-01 15:02:15)

Calls Per Second

Attempted Calls Passed Calls Failed Calls

01 - 15:02:00

Calls Rate RTP Packets Graph Average Jitter Distribution E-Model T.38 Analysis Call Flow Call Summary

Active Calls 0
Completed Calls 756
Purged Calls(cleared) 0
Failed Calls 68
Calls Per Second 0
Non Purged Calls 824

Total Frames 5 496
Last Frame Processed 5 496
Total Processed Frames 5 496
Frames Purged Before Processing 0
Queue ToDecode:Decoded 0:0
TimeToProcess(mm:ss)
FrameProcess/Sec :: Rate(Mbps) 0 :: 0.00
HdWriteDrop(rm.byte>

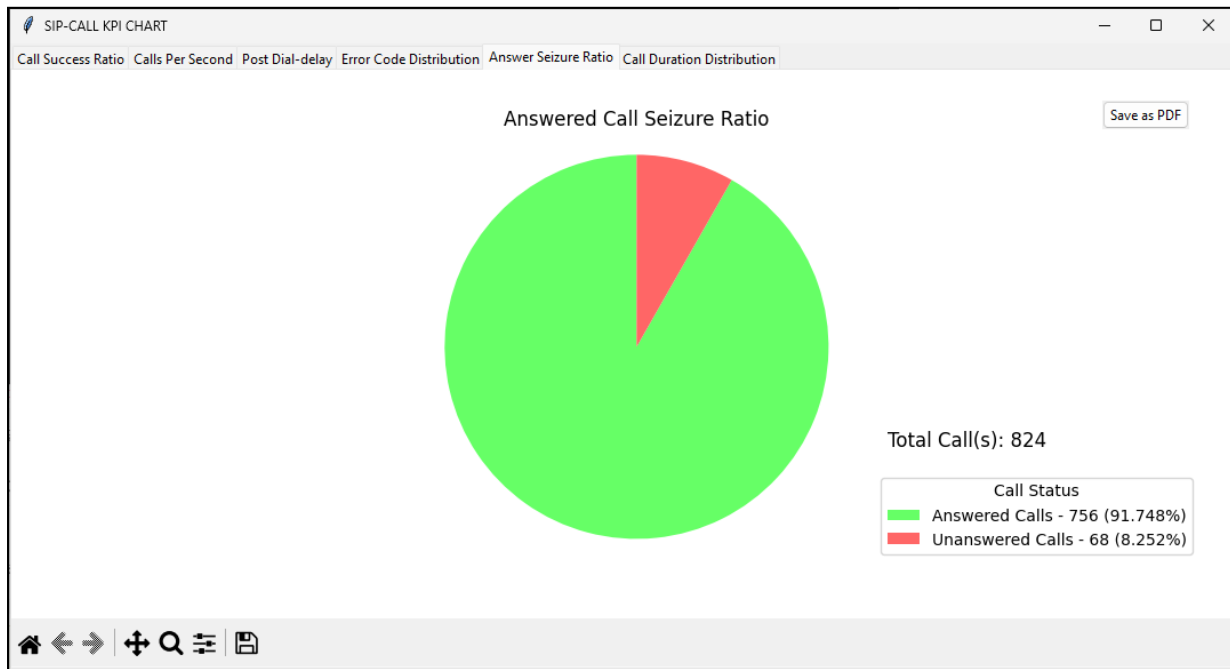
VDIP Bandwidth 0.00
SIP Bandwidth 0.00
H323 Bandwidth 0.00
MEGACO Bandwidth 0.00
RTP Bandwidth 0.00
LuCS Bandwidth 0.00
GsmA Bandwidth 0.00
SCCP Bandwidth 0.00

OverAll SIP RTP ED137

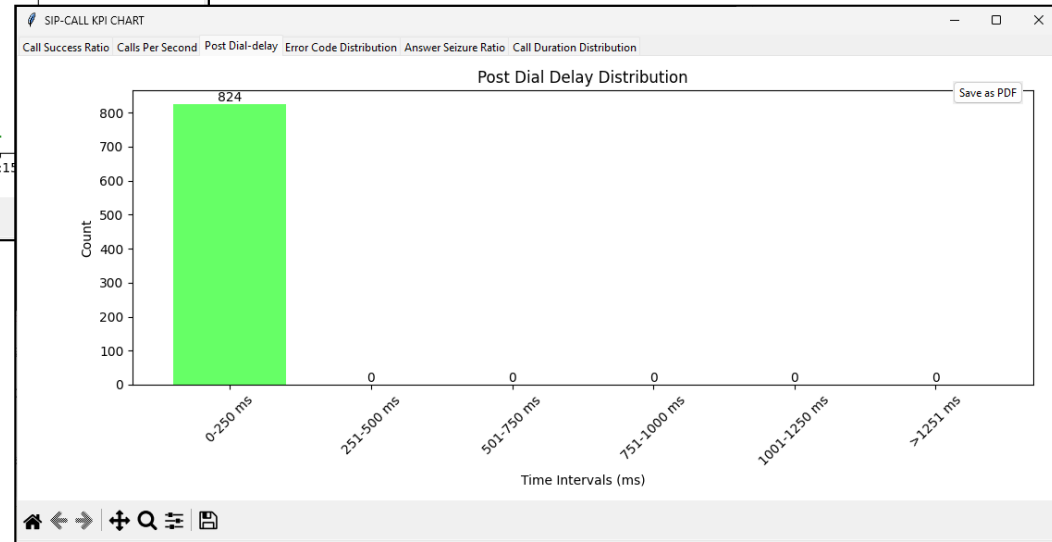
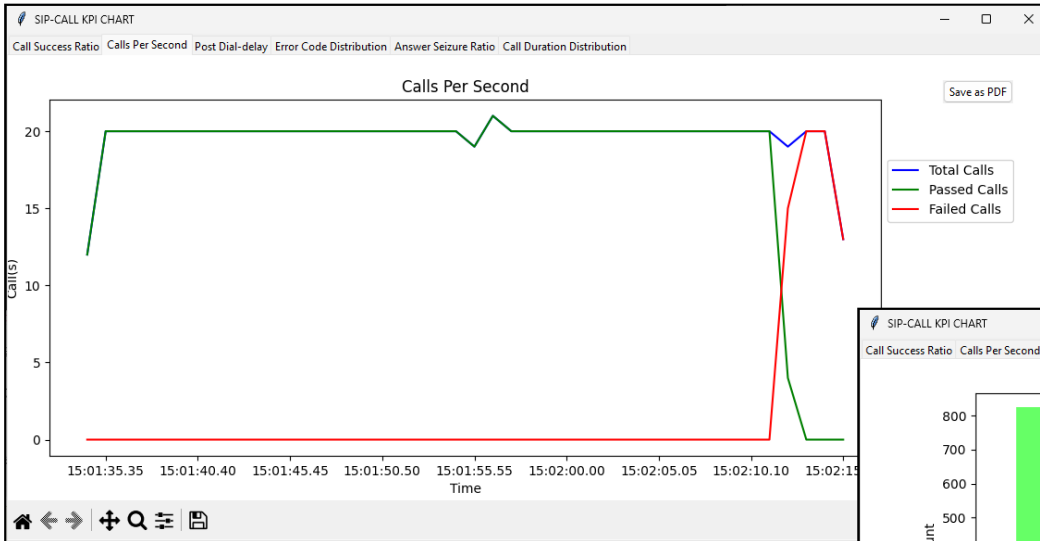
Key Performance Indicators (KPIs) Report for SIP Calls

The SIP Call Summary KPI Report includes KPIs for the following fields:

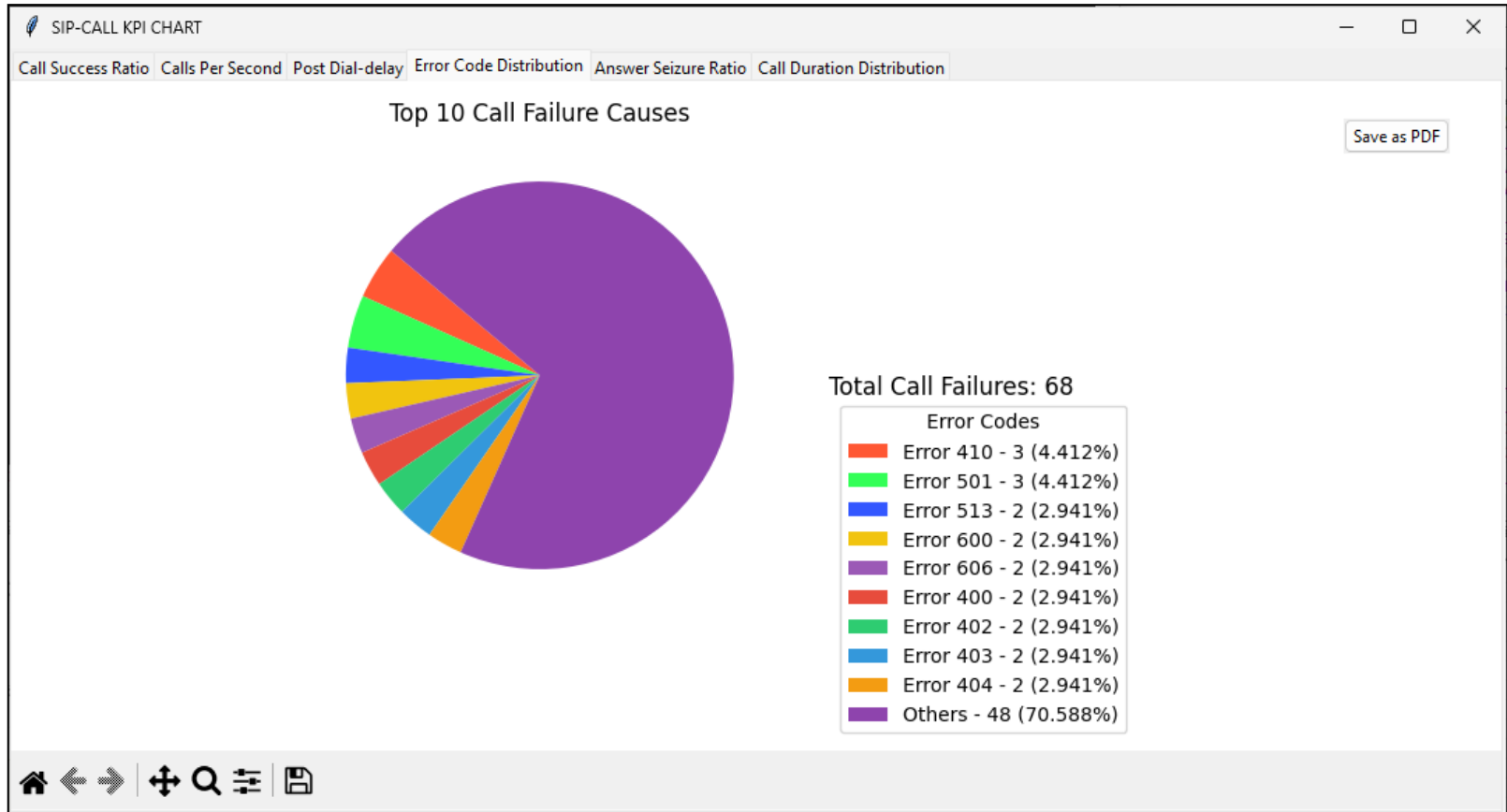
- **Call Success Ratio:** Displays graph for "Successful" and "Unsuccessful Calls," including counts and percentages (%)
- **Calls Per Second:** Shows graph "Total," "Passed," and "Failed Calls per second."
- **Post Dial Delay:** Shows delay counts in milliseconds (0-250ms, 251-500ms, etc.)
- **Error 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.)



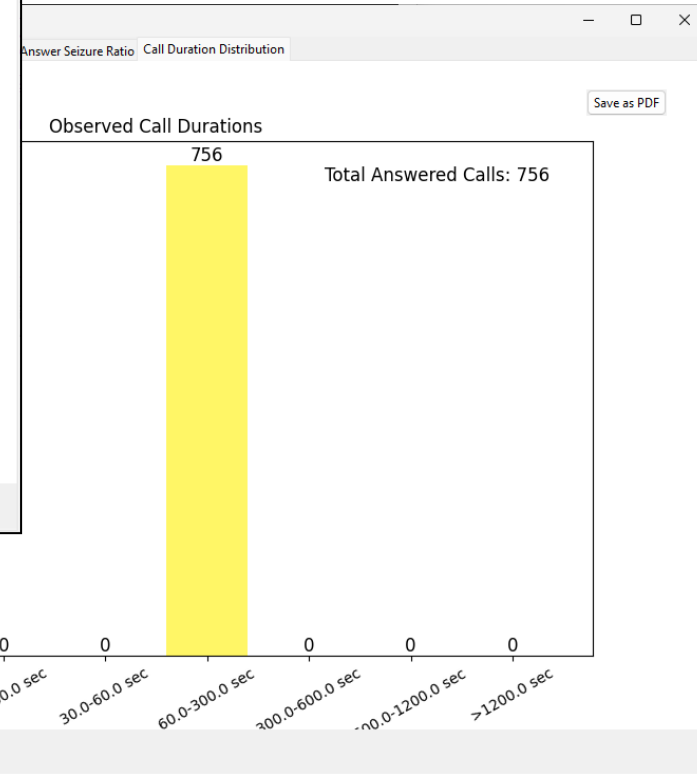
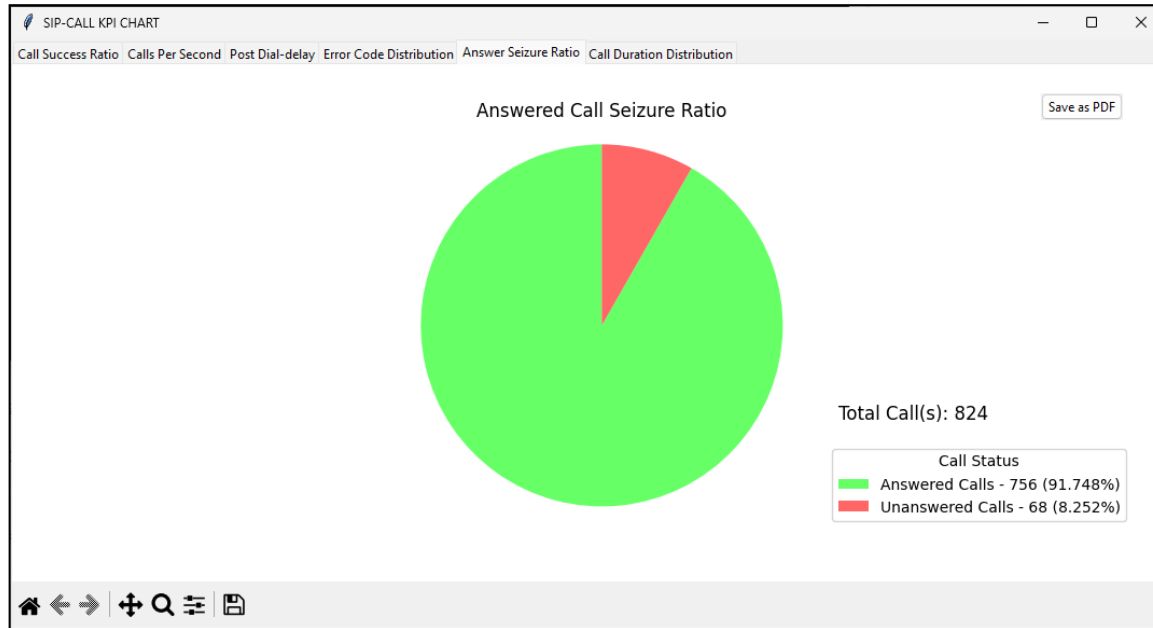
Calls Per Second and Post Delay KPIs



Error Code Distribution KPI



Answer Seizure Ratio and Call Duration Distribution KPIs



Call Graph – SIP Call

- Displays the message sequences of captured VoIP calls
- Decodes of the selected SIP message is displayed on the right pane
- The Complete Stack option enables the user to view the full call details for the selected message on the ladder diagram

The screenshot shows the PDA Packet Data Analyzer interface. The top menu includes File, View, Call Summary, Protocol Configurations, GUI Configurations, and Help. The main window is titled 'PDA Packet Data Analyzer - Summary View' and shows a 'Call Summary' table with columns for Call #, Caller, Callee, StartTime, Duration, VoiceQuality_L, VoiceQuality_R, and Cor. A red box highlights the first call entry (Call # 1).

Call #	Caller	Callee	StartTime	Duration	VoiceQuality_L	VoiceQuality_R	Cor
1	0001@192.168.12.92	0001@192.168.12.94	2023-06-01 15:01:34.419	00:01:00.023			
2	0002@192.168.12.92	0002@192.168.12.94	2023-06-01 15:01:34.482	00:01:00.033			
3	0003@192.168.12.92	0003@192.168.12.94	2023-06-01 15:01:34.533	00:01:00.045			
4	0004@192.168.12.92	0004@192.168.12.94	2023-06-01 15:01:34.583	00:01:00.037			
5	0005@192.168.12.92	0005@192.168.12.94	2023-06-01 15:01:34.623	00:01:00.049			

Below the table is a ladder diagram showing the sequence of SIP messages between 192.168.12.92 and 192.168.12.94. The messages are: INVITE (00.00.000), SIP/2.0 100 Trying (00.00.020), SIP/2.0 180 Ringing (00.00.029), SIP/2.0 200 OK (00.00.153), ACK (00.00.163), BYE (01.00.177), and SIP/2.0 200 OK (01.00.187). A red box highlights the INVITE message.

On the right side, the 'Find' box is checked, and the 'Complete Stack' option is selected. The decoded information for the selected SIP message is displayed, showing the MAC Layer, IP4 Layer, and UDP Layer details.

Displays decoded information of the selected SIP message

Call Graph – SIP ED-137

- Displays the message sequences of SIP ED-137 call
- Decodes of the selected SIP message is displayed on the right pane

The screenshot displays the Packet Data Analyzer (PDA) interface. The top menu includes File, View, Call Summary, Protocol Configurations, GUI Configurations, and Help. The main window shows a 'Call Summary' table with columns for Call #, Caller, Callee, CallID, StartTime, Duration, Src_L, Payload_L, TotalPackets_L, ConversationalMos_L, ConversationalR_L, and Listen. Below the table, a detailed view of a selected SIP message sequence is shown, including a sequence diagram and a protocol stack analysis.

Call #	Caller	Callee	CallID	StartTime	Duration	Src_L	Payload_L	TotalPackets_L	ConversationalMos_L	ConversationalR_L	Listen
1	0001@192.168.1.52	0001@192.168.12.105	GL-MAPS_3_1879751-8...	2017-01-13 12:31:10	00:00:29.844	29014389	PCMA/8000	444	4.20	93	4
2	0001@192.168.1.52	0001@192.168.12.105	GL-MAPS_10_2093727-...	2017-01-13 12:34:44	00:00:00.000						
3	0001@192.168.1.52	0001@192.168.12.105	GL-MAPS_10_2145086-...	2017-01-13 12:35:35	00:00:37.021	21949045	G729/8000	550	4.06	87	4
4	0005@192.168.1.52	0005@192.168.12.117	GL-MAPS_44_2802778-...	2017-01-13 12:46:33	00:00:00.000						
5	0005@192.168.1.52	0001@192.168.12.105	GL-MAPS_3_2920954-1...	2017-01-13 12:48:31	00:00:28.116	2092952065	PCMA/8000	1399	4.20	93	4

TimeStamp	Frame Number	192.168.1.52	192.168.12.105
00.00.000	0	5060	INVITE → 5060
00.00.023	1	5060	SIP/2.0 100 Trying ← 5060
00.00.148	2	5060	SIP/2.0 200 OK ← 5060
00.00.154	3	5060	ACK → 5060
00.00.155	4	6000	Keep Alive → 6000
00.00.161	5	6000	Keep Alive ← 6000
00.01.170	16	5060	SUBSCRIBE → 5060
00.01.176	17	5060	SIP/2.0 200 OK ← 5060
00.01.178	18	5060	NOTIFY ← 5060
00.01.182	19	5060	SIP/2.0 200 OK → 5060


```
===== MAC Layer =====  
Destination Address = xCOEAE484BA90  
Source Address = x54BEF737BC42  
Length/Protocol Type = x0800 Internet IP(IPv4)  
===== IP Layer =====  
Version = 0100.... (4)  
Internet Header Length (In 32 bit words) = ....0101 (5)  
Differentiated Services Field =  
Differentiated Services Codepoint = 100010.. Assured Forwarding 41  
Explicit Congestion Notification = .....00 Not-ECT (Not ECN-Capable Tran  
Total Length = 961 (x03C1)  
Identification = 22542 (x580E)  
Reserved Bit = 0..... Not Set  
Don't fragment = .0..... Not Set  
More fragments = .0..... Not Set  
Fragment Offset = 0 (...000000 00000000)  
Time To Live = 128 (x80)  
Protocol = 00010001 User Datagram  
Header Check Sum = x0000  
Source IP Address = 192.168.1.52 (xCOA80134)  
Destination IP Address = 192.168.12.105 (xCOA80C69)  
===== UDP Layer =====  
Source Port = 5060 (x13C4)  
Destination Port = 5060 (x13C4)
```

Call Graph – MSRP Call

- Decodes of the selected MSRP message is displayed on the right pane

The screenshot displays the PDA Packet Data Analyzer interface. At the top, the 'Call Summary' tab is active, showing a table of call records. Below this, the 'Call Graph' view shows a sequence of messages between two endpoints: 192.168.10.13 and 192.168.10.14. The messages include INVITE, SIP/2.0 100 Trying, SIP/2.0 180 Ringing, SIP/2.0 200 OK, ACK, MSRP/SEND, MSRP/200 OK, MSRP/REPORT, and MSRP/SEND. The MSRP/SEND message at 00.00.194 is highlighted in orange. On the right side, the decoded content of this message is shown in a text area, including fields like To-Path, From-Path, Message-ID, Success-Report, Failure-Report, Byte-Range, and Content-Type.

Call #	Caller	Callee	CallID	StartTime	Duration	EndTime	CallSuccess
2	0002@192.168.10.13	0002@192.168.10.14	GL-MAPS-24652-493054435-1755...	2021-05-11 01:43:17.742	00:02:00.037	2021-05-11 01:45:17.909	1
3	0003@192.168.10.13	0003@192.168.10.14	GL-MAPS-24656-493054534-1755...	2021-05-11 01:43:17.828	00:02:00.057	2021-05-11 01:45:18.028	1
4	0004@192.168.10.13	0004@192.168.10.14	GL-MAPS-24587-493054633-1755...	2021-05-11 01:43:17.915	00:02:00.024	2021-05-11 01:45:18.081	1
5	0005@192.168.10.13	0005@192.168.10.14	GL-MAPS-24670-493054734-1755...	2021-05-11 01:43:18.013	00:02:00.055	2021-05-11 01:45:18.210	1
6	0006@192.168.10.13	0006@192.168.10.14	GL-MAPS-24591-493054834-1755...	2021-05-11 01:43:18.123	00:02:00.022	2021-05-11 01:45:18.297	1
7	0007@192.168.10.13	0007@192.168.10.14	GL-MAPS-24699-493054933-1755...	2021-05-11 01:43:18.231	00:02:00.023	2021-05-11 01:45:18.394	1
8	0008@192.168.10.13	0008@192.168.10.14	GL-MAPS-24659-493055033-1755...	2021-05-11 01:43:18.318	00:00:00.000	2021-05-11 01:43:18.320	0
9	0009@192.168.10.13	0009@192.168.10.14	GL-MAPS-24663-493055133-1755...	2021-05-11 01:43:18.415	00:00:00.000	2021-05-11 01:43:18.425	0

```
MSRP glMapsMrsp226789 SEND
To-Path: msrp://192.168.10.14:21366/GL_MAPS_9CA9E3B3;tcp
From-Path: msrp://192.168.10.13:24339/GL_MAPS_3B40F48D;tcp
Message-ID: glMapsMrsp226789
Success-Report: no
Failure-Report: yes
Byte-Range: 1-270/270
Content-Type: text/plain

GL's Message Automation & Protocol Simulation (MAPS™) is a protocol simulation and
-----glMapsMrsp226789
```

Call Graph – 5G N1N2 Call

- Decodes of the selected 5G N1N2 message is displayed on the right pane

The screenshot displays the PDA interface for a 5G N1N2 call. The top menu includes File, View, Call Summary, Protocol Configurations, GUI Configurations, and Help. The interface is set to '5G' and 'N1N2 Interface'. A table at the top shows call details:

Call #	StartTime	AmfUeNgapId	RrcEstablishmentCause	NrCellIdentity	Tac	AmfSetID	AmRegionID	Amfpointer	Mcc
1	2023-06-16 10:13:09.600	2	mo-Signalling	1	1	1	2	63	001
2	2023-06-16 10:16:47.416	2	mo-Signalling	1	1	1	2	63	001

The main pane shows a call graph with time and frame numbers. Key events include:

- InitialUEMessage - Registration Request (Frame 2736)
- DownlinkNASTransport - Authentication Request (Frame 2761)
- UplinkNASTransport - Authentication Response (Frame 2762)
- DownlinkNASTransport - Security Mode Command (Frame 2787)
- UplinkNASTransport - Security Mode Complete (Frame 2788)
- PUT /nudm-uecm/v1/amsi-001013012042632/registrations/amf-5 (Frame 2791)
- GET /nudm-sdm/v2/amsi-001013012042632/resai (Frame 2800)

The right pane shows the decoded structure of the selected message (InitialUEMessage - Registration Request):

```
==== NGAP Layer =====
= CHOICE
Extensibility Marker      = 0
Choice Index              = 0
InitiatingMessage         = SEQUENCE
ProcedureCode             = INTEGER
  Contents                 = 15 id-InitialUEMessag
procedureCriticality      = ENUMERATOR
  Contents                 = 0 reject(0)
  Value                    = Open Type
  Length                   = 92
InitialUEMessage         = SEQUENCE
Extensibility Marker      = 0
ProtocolIE-Container      = SEQUENCE OF
  Iteration Count          = 6
  ProtocolIE-Container    = SEQUENCE
  ProtocolIE-Field        = INTEGER
  Contents                 = 85 id-RAN-UE-NGAP-ID
  Value                    = Open Type
  Length                   = 2
RAN-UE-NGAP-ID           = INTEGER
Length Determinant       = 1
  Contents                 = 2
ProtocolIE-Container      = Instance 1
  ProtocolIE-Field        = SEQUENCE
  ProtocolIE-ID           = INTEGER
  Contents                 = 38 id-NAS-PDU
  procedureCriticality     = ENUMERATOR
  Contents                 = 0 reject(0)
  Value                    = Open Type
  Length                   = 44
NAS-PDU                  = OCTET STRING
  Length Determinant     = 43
  NAS PDU Dump            = x7E00417100D0100F110
ProtocolIE-Container      = Instance 2
ProtocolIE-Field          = SEQUENCE
```

Signaling / Audio/ Video QoS Parameters

Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

SIP Show All Sessions

Call Summary Registrator Summary Alert Summary

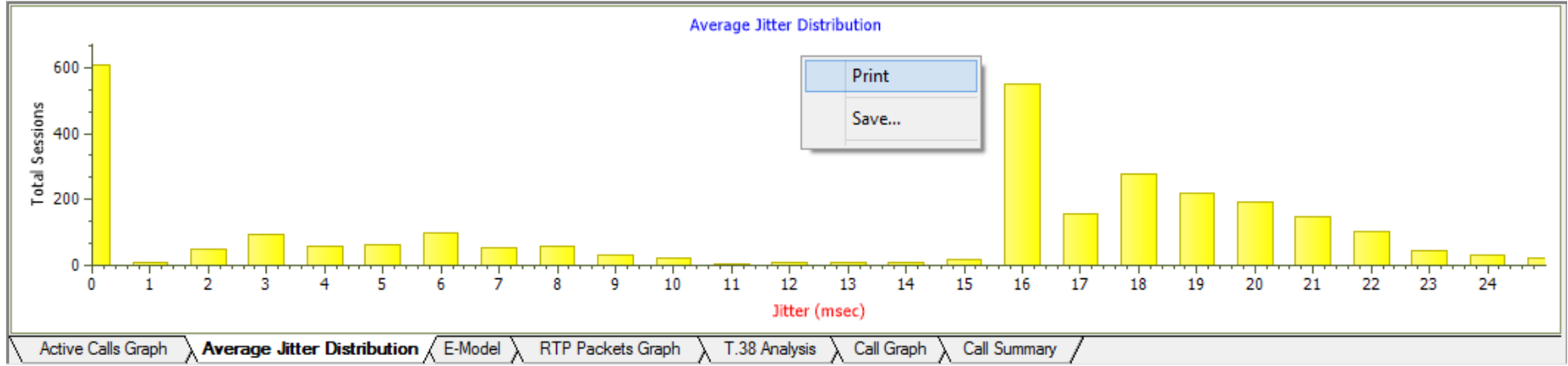
Call #	Caller	Callee	CallID	StartTime	Duration	ConversationalMos_L
1	0001@192.168.1.196	0001@192.168.1.208	GLPG1480778889963	2014-11-11 19:54:18	00:00:30.014	4.20
2	0002@192.168.1.196	0002@192.168.1.208	GLPG1480778889966	2014-11-11 19:54:18	00:00:30.014	4.20
3	0003@192.168.1.196	0003@192.168.1.208	GLPG1480778889969	2014-11-11 19:54:18	00:00:30.014	4.20

Signalling Parameters	Value	Audio Parameters	Value	Video Parameters	Value
Caller	0001@192.168.1.196	Src RTP Channel	192.168.1.196: ...	Src Video Channel	
Callee	0001@192.168.1.208	Src Media Type	PCMU/8000	Src Media Type	
CallID	GLPG1480778889963	Src SSRC	465265921	Src SSrc	
Call Status	Terminated	Src Packets Count	1503	Src Packet Count	
Call Initiated Time	2014-11-11 19:54:18	Src Packets Lost / (%)	0 / 0.00	Src Missing Packets / (%)	
Call Established Time	2014-11-11 19:54:18	Src Duplicate Packets / (%)	0 / 0.00	Src Duplicate Packet / (%)	
Call Stop Time	2014-11-11 19:54:18	Src Out of Sequence Packets / (%)	0 / 0.00	Src Out of Sequence / (%)	
Call Duration	00:00:30.014	Src Conversational MOS/R-Factor	4.20 / 93	Src Video Frame count	
Call Terminator	Caller	Src Listening MOS/R-Factor	4.20 / 93	Src Frame Rate(Frames/sec)	
Call Failure Reason		Src Discarded Packets / (%)	0 / 0.00	Src AvgDelay	
Session Request Delay (msec)	3.29	Src Average Inter Arrival Jitter (RTCP)	0	Src AvgGap	
Session Disconnect Delay (msec)	0.707	Src Average Jitter	0.00	Src MDI (DF:MLR)	
Post PickUP Delay (msec)	2.707	Src Average Delay	0.00	Src AvgMDI(DF:MLR)	
Total Signaling Frames	5	Src Average Gap	20.01	Dest Video Channel	
		Dest RTP Channel	192.168.1.208: ...	Dest Media Type	
		Dest Media Type	PCMU/8000	Dest SSrc	
		Dest SSRC	467701505	Dest Packet Count	
		Dest Packets Count	1502	Dest Missing Packets / (%)	
		Dest Packets Lost / (%)	0 / 0.00	Dest Duplicate Packet / (%)	
		Dest Duplicate Packets / (%)	0 / 0.00	Dest Out of Sequence / (%)	
		Dest Out of Sequence Packets / (%)	0 / 0.00	Dest Video Frame count	
		Dest Conversational MOS/R-Factor	4.20 / 93	Dest Frame Rate(Frames/sec)	
		Dest Listening MOS/R-Factor	4.20 / 93	Dest AvgDelay	
		Dest Discarded Packets / (%)	0 / 0.00	Dest AvgGap	
		Dest Average Inter Arrival Jitter (RTCP)	0	Dest MDI (DF:MLR)	
		Dest Average Jitter	0.00	Dest AvgMDI(DF:MLR)	

Active Calls Graph Average Jitter Distribution E-Model RTP Packets Graph T.38 Analysis Call Graph Call Summary

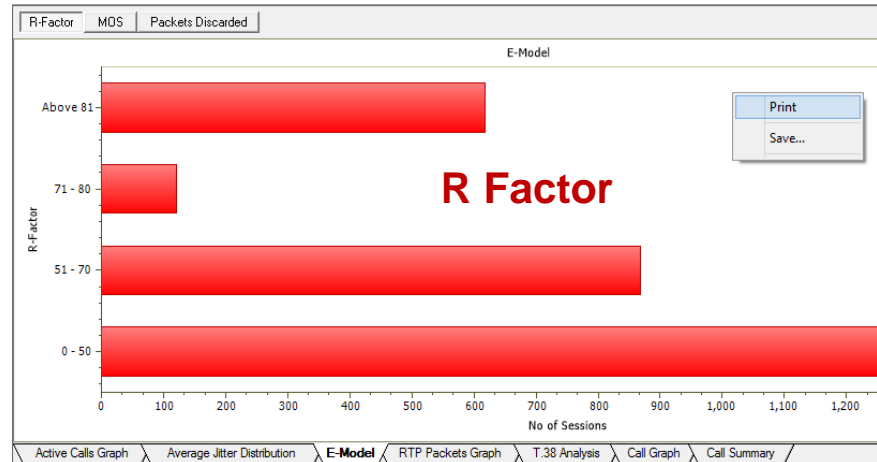
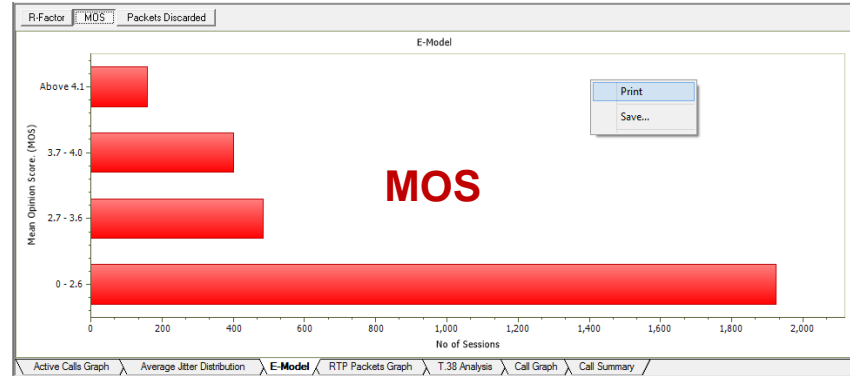
Average Jitter Distribution Graph

- Distribution of the Average Jitter values across Total Sessions

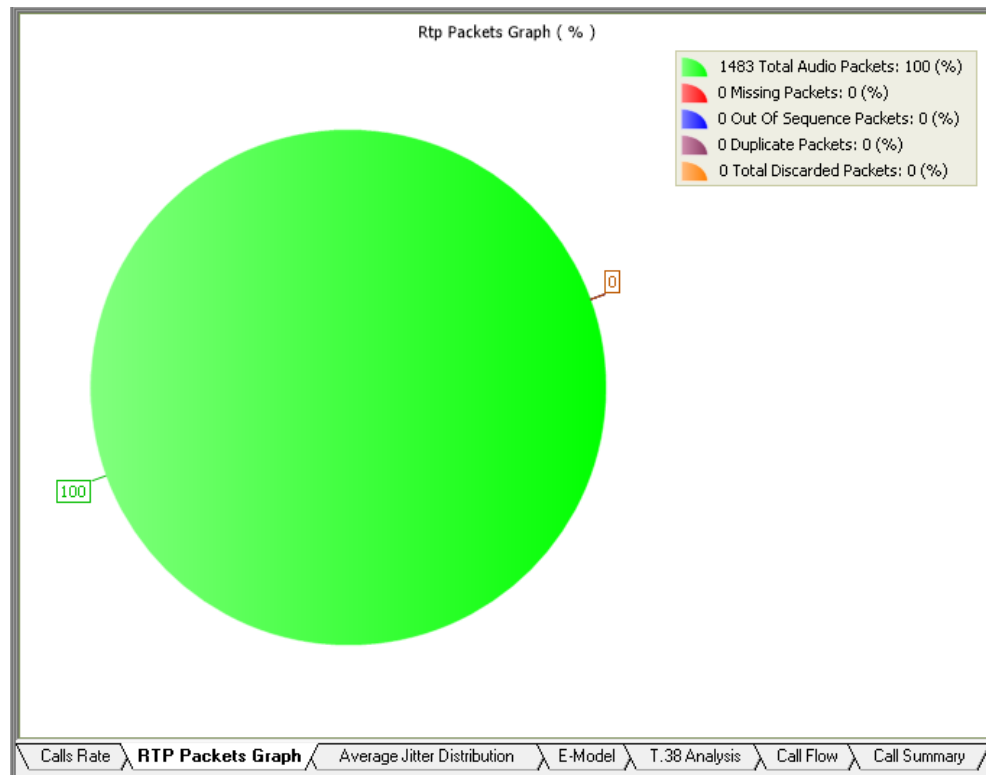


MOS Graph and R-Factor Graph

- E-Model graph provides R-factor, MOS, and packets discarded against number of sessions. All these three graphs show statistics of terminated calls
 - R-Factor – A bar graph that plots R-Factor across No of Sessions
 - MOS – A bar graph that plots Mean Opinion Score across No. of Sessions
 - Packets Discarded – A bar graph that plots Packets Discarded across No. of Sessions



RTP Packets Graph



- RTP Packets graph plots and compares out of ordered packets, missing packets and duplicate packets against Total Audio Packets

T.38 Analysis - Fax over IP

- Supports capturing and decoding of Fax (T.38 data) calls over VoIP
- Decodes of selected FAX message is displayed on the right pane
- Captured fax calls by PacketScan™ can also be analyzed using GLInsight™ by saving the fax calls directly in (*.PCAP) Ethereal file format

The screenshot displays the Packet Data Analyzer (PDA) interface. At the top, the 'Show Fax Calls' filter is selected in a dropdown menu. Below this, a table shows call details for a single call (Call # 1, Src L 390089559, ConversationalMos L 4.20, ConversationalR L 93, ListeningMos L 4.20, ListeningR L 93, PacketsDiscarded L 0, PacketsDiscarded(%) L 0.00).

The main pane shows a list of messages. The selected message is highlighted in orange:

TimeStamp	Src L	Destination	Protocol	Dest L
00.17.274 ...	5004		(Frm:1409)Msg:no-signal	5004
00.17.274 ...	5004		(Frm:1410)Msg:no-signal	5004
00.17.275 ...	5004		(Frm:1411)Msg:no-signal	5004
00.27.343 ...	5004		(Frm:1419)Msg:no-signal	5004
00.27.343 ...	5004		(Frm:1419)Msg:ced	5004
00.30.538 ...	5004		(Frm:1420)Msg:v21-preamble	5004
00.31.580 ...	5004		(Frm:1421)Msg:NSF	5004
00.31.955 ...	5004		(Frm:1422)Msg:CSI NUM:918040488401e	5004
00.32.648 ...	5004		(Frm:1440)Msg:DIS.DSR.ITU-T V.27 ter and V.29	5004
00.33.110 ...	5004		(Frm:1451)Msg:no-signal	5004
00.39.617 ...	5004		(Frm:1561)Msg:v21-preamble	5004
00.40.659 ...	5004		(Frm:1563)Msg:CFR	5004
00.40.834 ...	5004		(Frm:1566)Msg:no-signal	5004
01.11.404 ...	5004		(Frm:2969)Msg:v21-preamble	5004

The right pane shows the decoded T.38 Layer information for the selected message:

```
===== T.38 Layer =====
UDPTLPacket
seq-number          = SEQUENCE
                    = INTEGER
                    = 3
Contents
primary-ifp-packet = Open Type
Length             = 1
IFPPacket
Preamble           = SEQUENCE
                    = 0
type-of-msg        = CHOICE
Choice Index       = 0
t30-indicator      = ENUMERATOR
                    = 0
Extensibility Marker
Contents           = 0 no-signal(0)
error-recovery     = CHOICE
Choice Index       = 0
secondary-ifp-packets
iteration count     = SEQUENCE OF
                    = 1
secondary-ifp-packets
primary-ifp-packet = Instance 0
                    = Open Type
                    = 1
Length             = SEQUENCE
                    = 1
IFPPacket
Preamble           = SEQUENCE
                    = 0
type-of-msg        = CHOICE
Choice Index       = 0
t30-indicator      = ENUMERATOR
                    = 0
Extensibility Marker
Contents           = 0 no-signal(0)
===== MAC Layer =====
Padding octets     = x401188E4C0A8
FCS                 = x013CCA38 (Invalid FCS. Correct FCS is xA72500)
```

A blue arrow points from the selected message in the table to the decoded T.38 Layer information on the right. A text box on the right says "Displays decoded information of the selected FAX message".

Call Detail View

- Provides a detail look at the two (or one) RTP sessions that are part of a single call
- Left and right panes accommodate the two sessions

Packet Data Analyzer - Detail View

File View Detail View Protocol Configurations GUI Configurations Help

SIP Show All Sessions

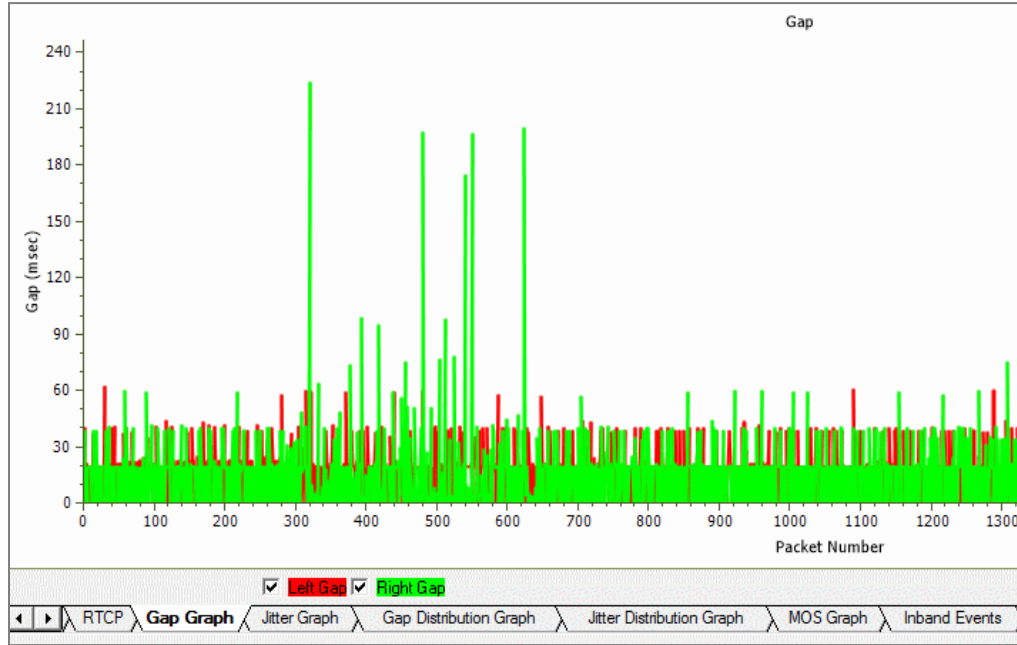
Call Summary | Registrar Summary | Alert Summary

Packet #	Sequen...	RTP ...	Payload Type	Paylo...	Packet Sequ...	Gap(ms)	Ga...	Delay	Jitter	Packet #	Sequen...	RTP ...	Payload Type	Paylo...	Packet Sequ...	Gap(ms)	Ga...	Delay	Jitter
M 5	41763	4325...	PCMU/8000	160	Session In Pr...	0.00	0.00	0	0.00	M 9	47038	3301...	PCMU/8000	160	Session In Pr...	0.00	0.00	0	0.00
6	41764	4325...	PCMU/8000	160	Session In Pr...	20.06	20.00	0	0.00	11	47039	3301...	PCMU/8000	160	Session In Pr...	18.81	20.00	-1	0.08
7	41765	4325...	PCMU/8000	160	In Sequence	19.53	20.00	0	0.03	13	47040	3301...	PCMU/8000	160	In Sequence	20.50	20.00	0	0.10
8	41766	4325...	PCMU/8000	160	In Sequence	19.52	20.00	0	0.06	15	47041	3301...	PCMU/8000	160	In Sequence	19.53	20.00	0	0.13
10	41767	4325...	PCMU/8000	160	In Sequence	21.50	20.00	1	0.14	17	47042	3301...	PCMU/8000	160	In Sequence	21.49	20.00	1	0.21
12	41768	4325...	PCMU/8000	160	In Sequence	19.53	20.00	0	0.17	19	47043	3301...	PCMU/8000	160	In Sequence	19.52	20.00	0	0.23
14	41769	4325...	PCMU/8000	160	In Sequence	19.53	20.00	0	0.19	21	47044	3301...	PCMU/8000	160	In Sequence	19.59	20.00	0	0.24
16	41770	4325...	PCMU/8000	160	In Sequence	20.49	20.00	0	0.20	23	47045	3301...	PCMU/8000	160	In Sequence	19.47	20.00	0	0.27
18	41771	4325...	PCMU/8000	160	In Sequence	19.57	20.00	0	0.22	25	47046	3301...	PCMU/8000	160	In Sequence	20.51	20.00	0	0.28
20	41772	4325...	PCMU/8000	160	In Sequence	20.51	20.00	0	0.23	27	47047	3301...	PCMU/8000	160	In Sequence	19.53	20.00	0	0.29
22	41773	4325...	PCMU/8000	160	In Sequence	19.52	20.00	0	0.25	29	47048	3301...	PCMU/8000	160	In Sequence	20.55	20.00	0	0.31
24	41774	4325...	PCMU/8000	160	In Sequence	20.75	20.00	0	0.28	31	47049	3301...	PCMU/8000	160	In Sequence	19.48	20.00	0	0.33
26	41775	4325...	PCMU/8000	160	In Sequence	19.31	20.00	0	0.31	33	47050	3301...	PCMU/8000	160	In Sequence	20.51	20.00	0	0.34
28	41776	4325...	PCMU/8000	160	In Sequence	19.50	20.00	0	0.32	35	47051	3301...	PCMU/8000	160	In Sequence	19.53	20.00	0	0.35

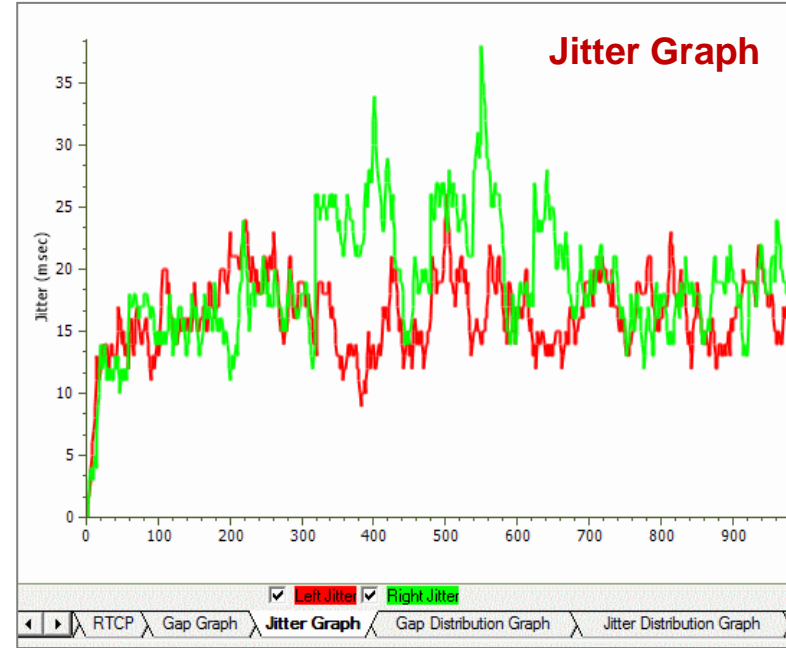
Heading	Value	Heading	Value
SSRC	3365468417	SSRC	3380545537
Source IP Address	192.168.1.200	Source IP Address	192.168.1.103
Destination IP Address	192.168.1.103	Destination IP Address	192.168.1.200
Source Port	1024	Source Port	1024
Destination Port	1024	Destination Port	1024
RTP Packets Count	1271	RTP Packets Count	1268
RTCP Packets Count	2	RTCP Packets Count	1
Packets With Marker Bit	1	Packets With Marker Bit	1
Total Audio Bytes	203201	Total Audio Bytes	202721
RTCP Sender's Reports	2	RTCP Sender's Reports	1
RTCP Receiver's Reports	0	RTCP Receiver's Reports	0
Out Of Sequence Packets \%	0 \ 0.00	Out Of Sequence Packets \%	0 \ 0.00
Missing Packets \%	0 \ 0.00	Missing Packets \%	0 \ 0.00
Duplicate Packets \%	0 \ 0.00	Duplicate Packets \%	0 \ 0.00
MOS-CQ \ Conversational R	4.20 \ 93	MOS-CQ \ Conversational R	4.20 \ 93
MOS-LQ \ Listening R	4.20 \ 93	MOS-LQ \ Listening R	4.20 \ 93
G.107 R	92	G.107 R	92
Nominal MOS \ Nominal R	4.20 \ 93	Nominal MOS \ Nominal R	4.20 \ 93

RTP Statistics | RTCP | Gap Graph | Jitter Graph | Gap Distribution Graph | Jitter Distribution Graph | MOS Graph | Inband Events | RTP Events | Wave Graph | Spectral Display | R-Factor Statistics

Gap and Jitter Graph

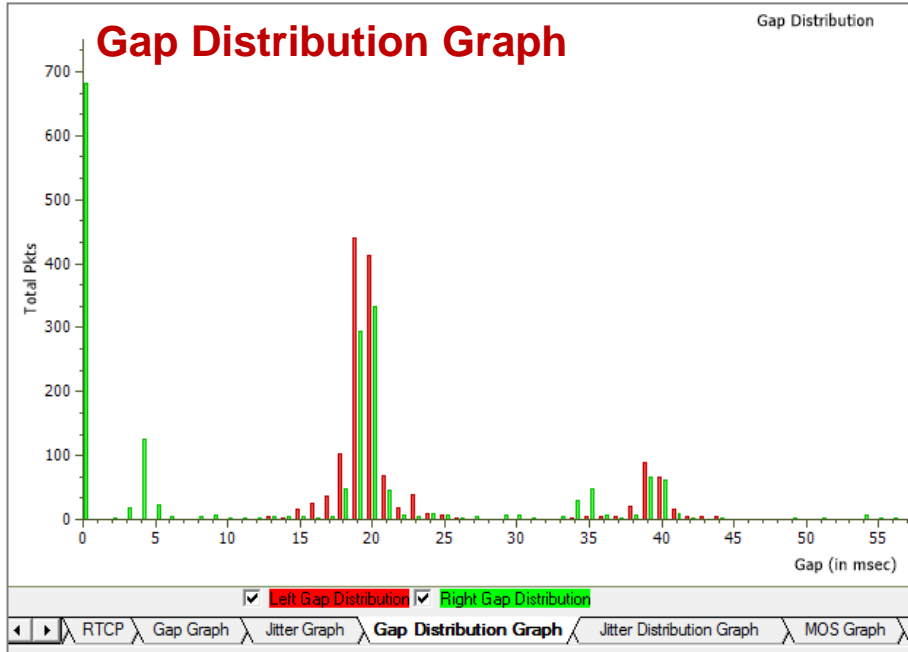


- Gap graph plots the Gap (in milliseconds) versus the packet number

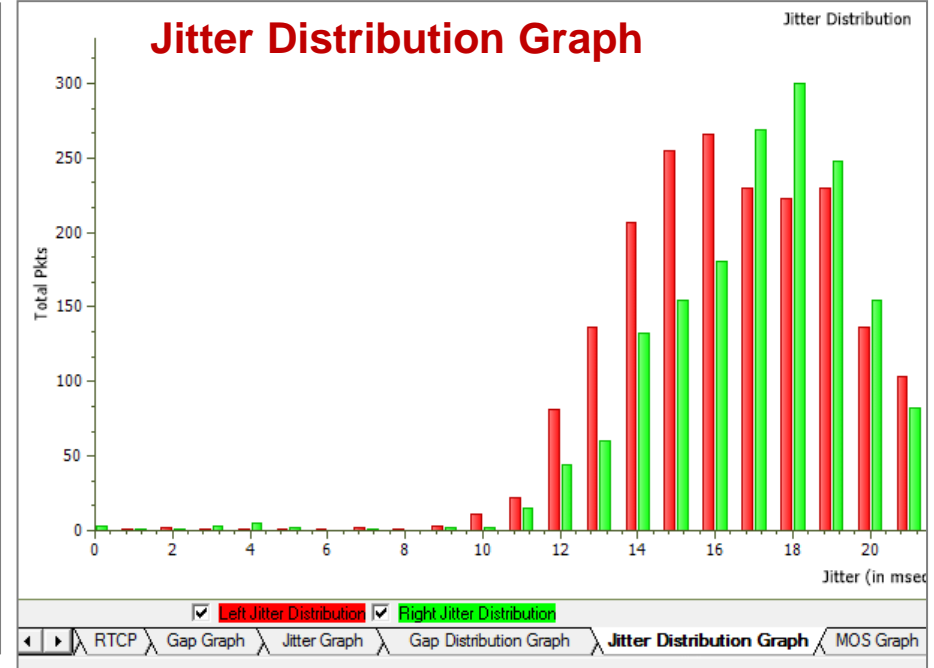


- Jitter graph plots the Jitter versus the packet number

Gap and Jitter Distribution Graph



- Number of packets with a particular value of gap is plotted against the (gap) value



- Number of packets with a particular value of jitter is plotted against the jitter value

MOS Graph



- MOS Graph plots Mean Opinion Score values throughout the duration of the call

Inband and Outband (RTP) Events

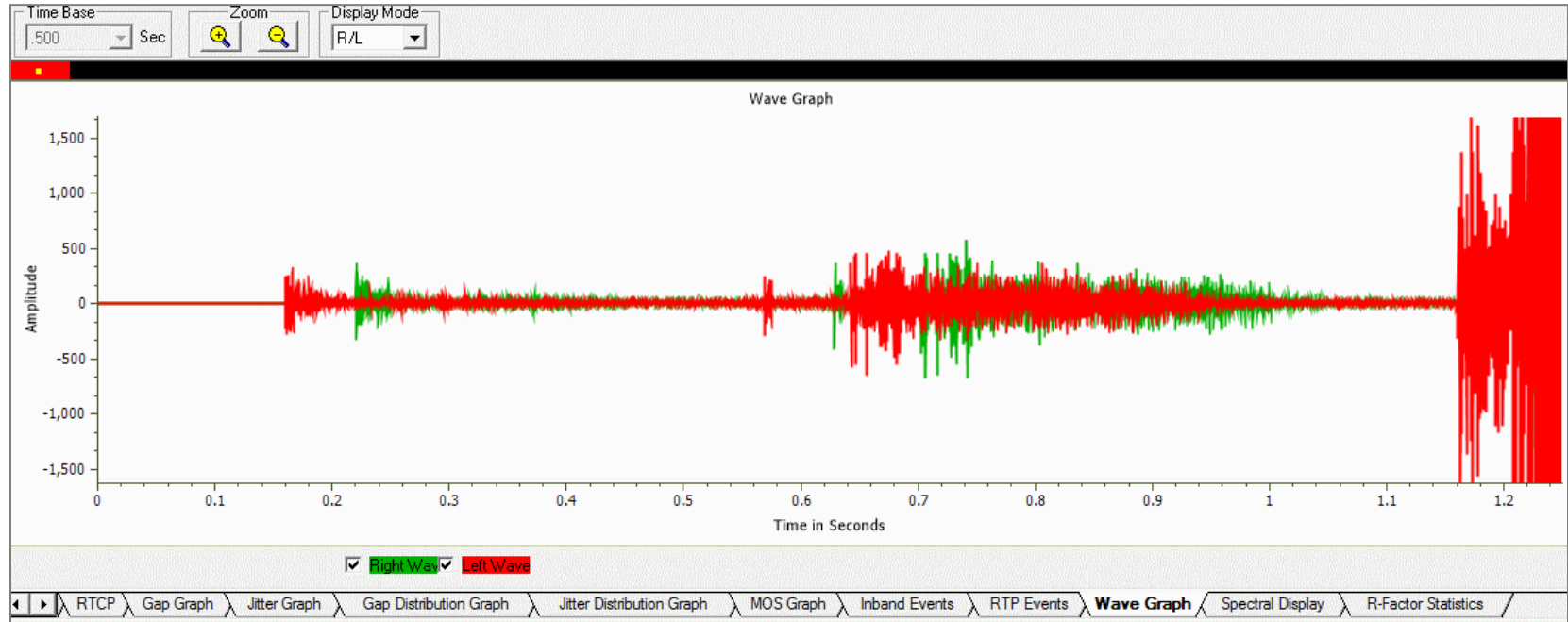
TimeStamp	Type	Event	On(ms)	Power(dBm)	Freq1(Hz)/Pow...	Freq2(Hz)/Pow...
00:00:00.000	IDLE		45470	0.00		
00:00:45.470	DTMF	1	80	-1.89	698/-6.01	1210/-4.01
00:00:45.550	IDLE		80	0.00		
00:00:45.630	DTMF	2	80	-1.87	698/-6.00	1337/-3.99
00:00:45.710	IDLE		80	0.00		
00:00:45.790	DTMF	3	80	-1.85	698/-5.98	1478/-3.99
00:00:45.870	IDLE		80	0.00		
00:00:45.950	DTMF	4	80	-1.86	771/-5.98	1210/-4.01
00:00:46.030	IDLE		80	0.00		
00:00:46.110	DTMF	5	80	-1.86	771/-5.98	1337/-3.99
00:00:46.190	IDLE		80	0.00		
00:00:46.270	DTMF	6	80	-1.87	771/-5.99	1478/-3.99
00:00:46.350	IDLE		80	0.00		
00:00:46.430	DTMF	7	80	-1.86	853/-5.98	1210/-4.01
00:00:46.509	IDLE		80	0.00		
00:00:46.590	DTMF	8	80	-1.89	853/-6.01	1337/-3.99
00:00:46.670	IDLE		80	0.00		

TimeStamp	Event	Volume (-dBm)	Duration (ms)
12:09:02.652	DTMF 1	6	80
12:09:02.812	DTMF 2	6	80
12:09:02.971	DTMF 3	6	80
12:09:03.132	DTMF 4	6	80
12:09:03.292	DTMF 5	6	80
12:09:03.452	DTMF 6	6	80
12:09:03.612	DTMF 7	6	80
12:09:03.772	DTMF 8	6	80
12:09:03.931	DTMF 9	6	80
12:09:04.092	DTMF 0	6	80
12:09:04.252	DTMF A	6	80
12:09:04.412	DTMF B	6	80
12:09:04.572	DTMF C	6	80
12:09:04.732	DTMF D	6	80
12:09:04.891	DTMF #	6	80
12:09:36.324	MF 1	6	80

Inband Events | **RTP Events** | Wave Graph | Spectral Display | R-Factor Statistics

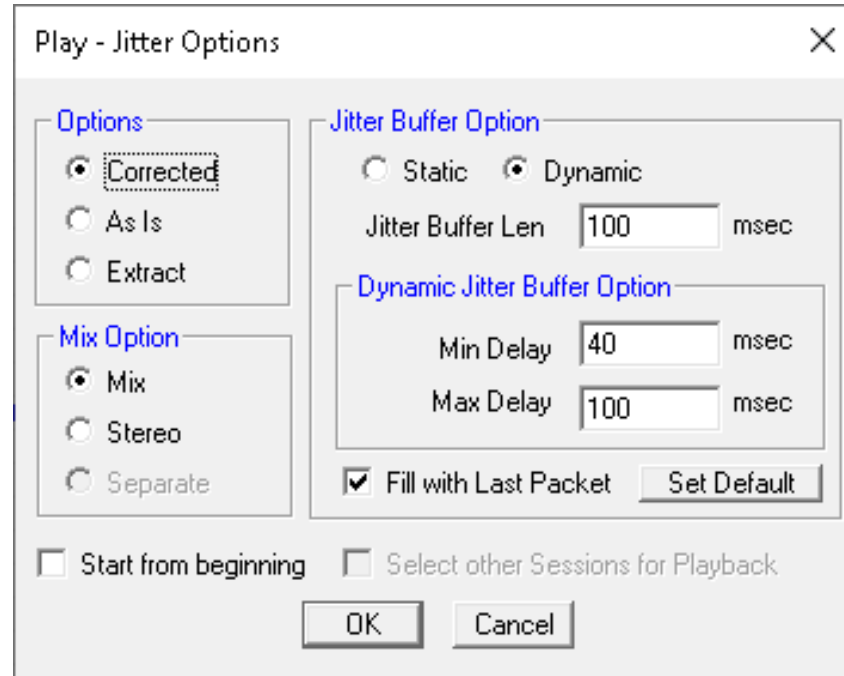
- Inband Event tab displays Inband DTMF and MF digits as they are received on selected RTP stream
- Outband (RTP) Events tab displays all Outband RTP events defined in RFC 2833 or RFC 4733

Wave and Spectral Graphs



- Wave graph - Displays the amplitude of the incoming signal in a selected call as a function of time
- Spectral Display - Displays the power of incoming signal while the capturing is going on as a function of frequency

Play Audio



- Plays the RTP streams of a call to the PC speaker using a soundcard
- Provides a host of options such as jitter buffer settings, audio mixing, and so on to play a live call in real-time or play captured voice files

Write to File

- Various options are provided to save captured calls
- Use the files with voice quality analysis software to calculate the mean opinion score of the call
- Records the RTP stream to a file in *.wav format

Write To File - Jitter Options

Options

Corrected

As Is

Extract

Mix Option

Mix

Stereo

Separate

Jitter Buffer Option

Static Dynamic

Jitter Buffer Len msec

Dynamic Jitter Buffer Option

Min Delay msec

Max Delay msec

Fill with Last Packet

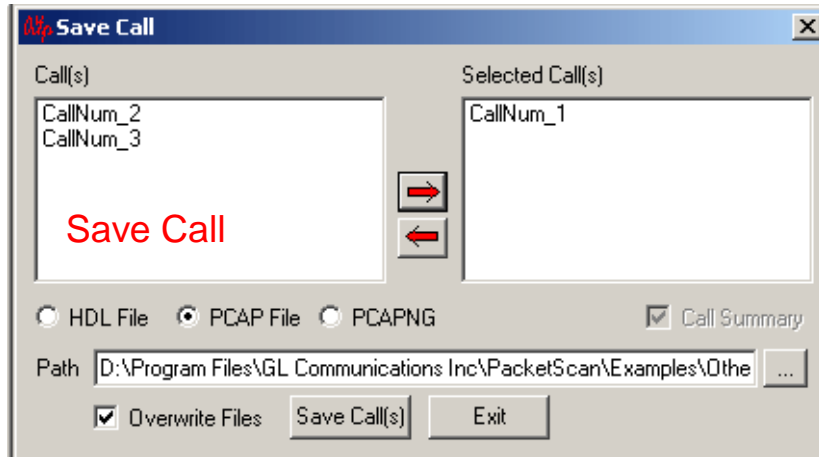
Start from beginning

File Record

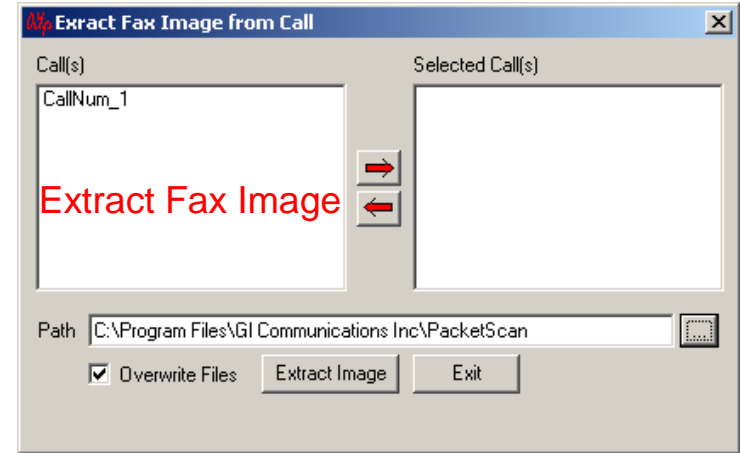
Use SSRC for File Name

C:\Program Files\GL Communications Inc\PacketScan\Sample...

Save Call and Extract Fax Image

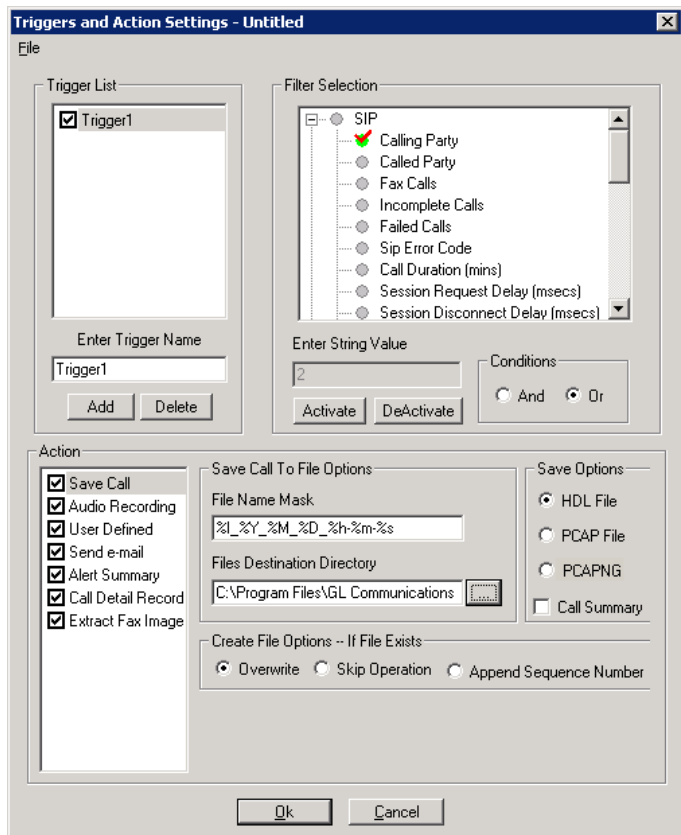


- Saves a particular call in either GL's proprietary HDL file format or Ethernet PCAP file format or PCAPNG file format
- Saves the Call Summary details including signaling and audio / fax/ video parameters for a particular call in *.rtf file
- Helps in getting data from real-time traffic locations to the lab for detailed analysis



- Extracts Fax image in the TIFF format from the selected fax call

Trigger and Action Settings



- Set the triggers and actions criteria to filter calls and perform additional actions on the completed calls
- Trigger actions on certain SIP, RTP, MEGACO, and H.323 parameters
- Triggering factors includes calling number, called number, incomplete calls, fax calls, call duration, MOS factor, sip error code, average jitter, and more
- Actions include
 - Saving call to a file `-.hdl`, `*.pcap`, or `*.pcapng`
 - Recording audio to a file
 - Sending an email alert
 - Generates alerts when particular vital parameters go beyond a specified value
 - Outputs call detail records as CSV
 - Extract Fax in Tiff format

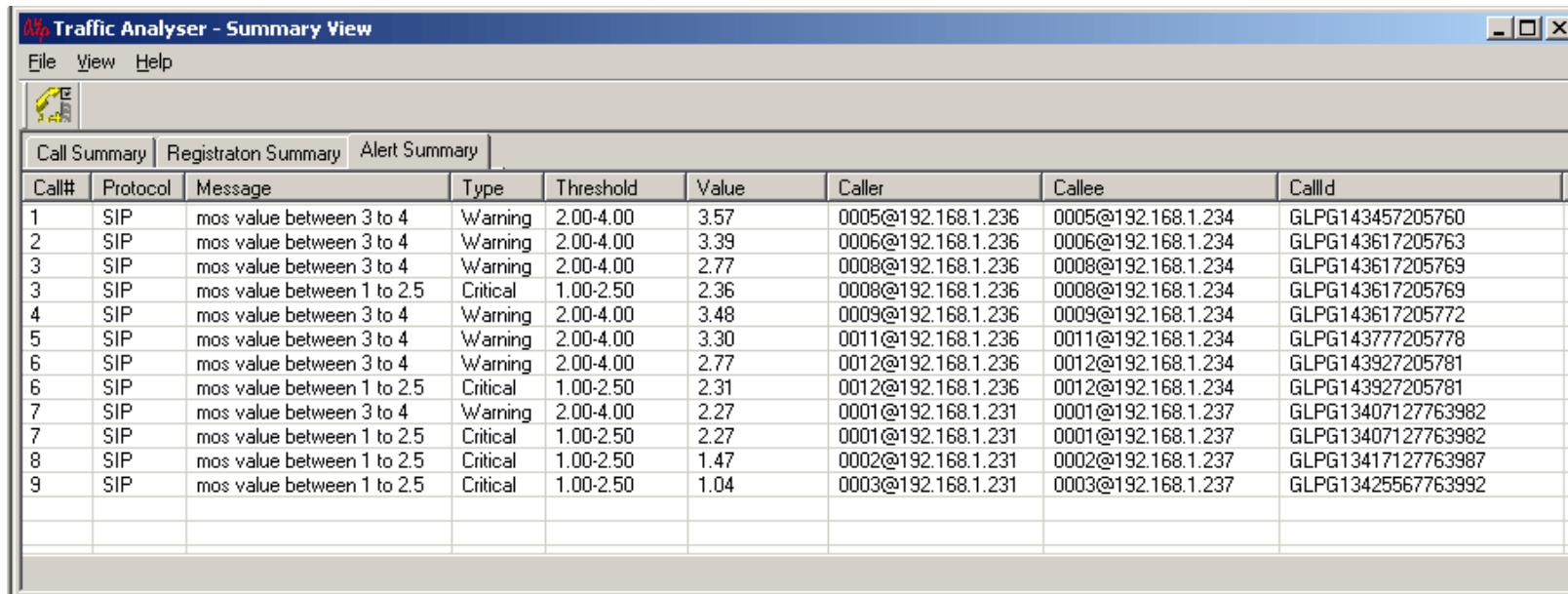
Call Detail Records (CSV)

- Creates three types of Comma Separated Value (CSV) files such as Call Side Record, Call Master Record, and Call Events Record
 - **Call Side Record:** It is a record concerning each party participating in the call. For example: Probe ID, Call ID, Side, Address, File Name, SSRC, Codec, Total Packets, and so on
 - **Call Master Record:** It contains fields concerning the call, For example: Probe ID, CALL ID, Side 1, Side 2, Protocol name, Start & Released dated and time, and so on
 - **Call Event Record:** It gives an event-by-event account of the call. For example: Probe ID, Call ID, Side, Class ID, Start, Duration, Source IP address, Destination IP Address, and so on
- Use Sub Folders option to automatically create the subfolders after some time duration

The screenshot shows a configuration window titled "Action" with the following settings:

- Action List (Left Panel):**
 - Save Call
 - Audio Recording
 - User Defined
 - Send e-mail
 - Alert Summary
 - Call Detail Record
 - Extract Fax Image
- Call Side Record:** (Probe Name: VolIPProbe)
- Call Master Record:**
- Call Events Record:**
- CSV Files Destination Directory:** C:\Program Files\GL Communications ...
- Use Sub Folders:** (Folder Prefix: VolPCaptures, Create Subfolder Every: 1 hr)
- Create File Options -- If File Exists:**
 - Overwrite
 - Skip Operation
 - Append Sequence Number

Alert Summary

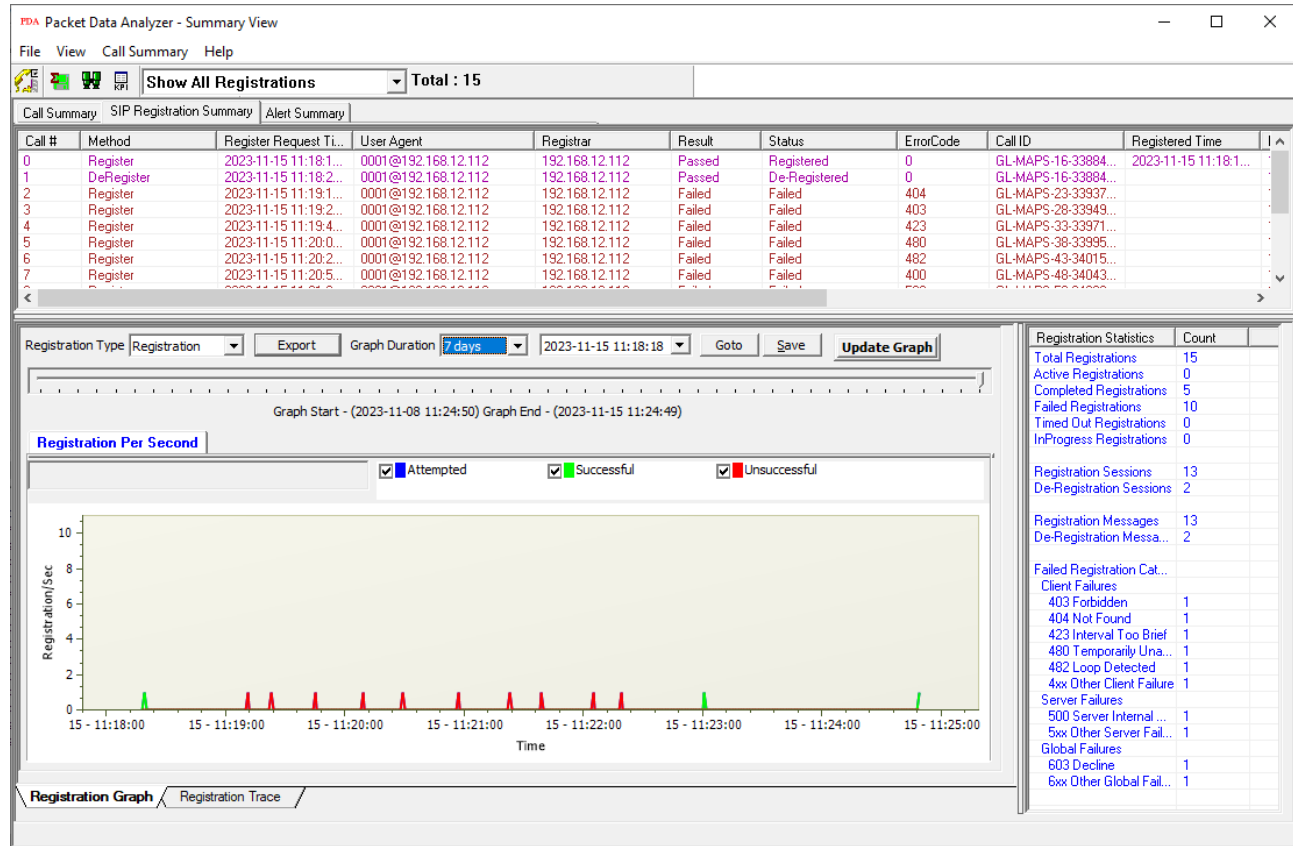


The screenshot shows a software window titled "Traffic Analyser - Summary View". It has a menu bar with "File", "View", and "Help". Below the menu bar is a toolbar with a small icon. The main area contains three tabs: "Call Summary", "Registraton Summary", and "Alert Summary". The "Alert Summary" tab is active, displaying a table with the following columns: Call#, Protocol, Message, Type, Threshold, Value, Caller, Callee, and Callid. The table contains 9 rows of alert data.

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	GLPG14377205778
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

Traffic Analyzer - Summary View

File View Help

Show All Registrations

Call Summary Registraton Summary Alert Summary

Call #	User Agent	Registrar	Status	Registered Time	TTL (secs)	Expiry Time	Remaining Time	RRD (msecs)	Registration...
0	0001@192.168.1.115	192.168.1.190	Registered	2011-01-03 18:31:09	120	2011-01-03 18:33:09		0	1
1	0002@192.168.1.115	192.168.1.190	Re-Registered	2011-01-03 18:35:33	120	2011-01-03 18:37:33		246162	2
2	0001@192.168.1.115	192.168.1.190	De-Registered	2011-01-03 18:32:01	120	2011-01-03 18:34:01		0	1
3	0001@192.168.1.115	192.168.1.190	Registered	2011-01-03 18:33:59	120	2011-01-03 18:35:59		1	1

192.168.1.115 192.168.1.190

54098 REGISTER 5060

5060 SIP/2.0 407 Proxy Authentication Required 5060

54098 REGISTER 5060

5060 SIP/2.0 200 OK 5060

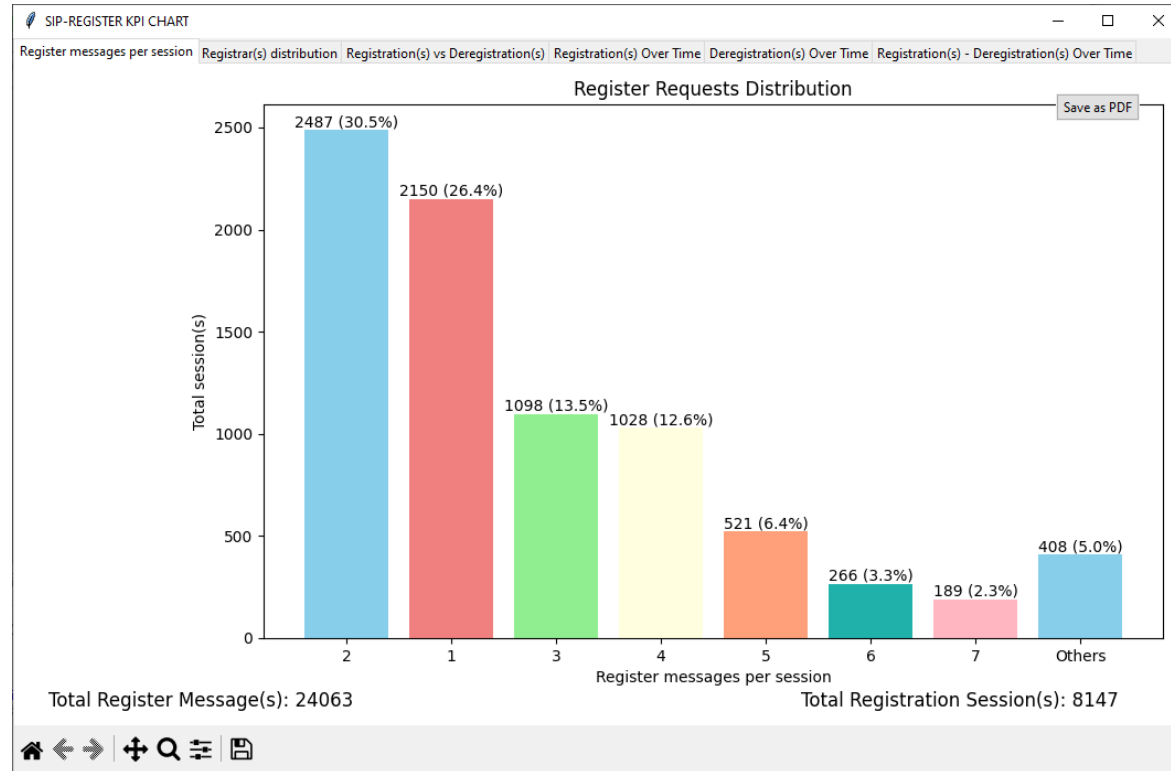
```
REGISTER sip:192.168.1.190 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.115:5060;branch=z9hG4bK3372630384-4779
Max-Forwards: 70
Allow: INVITE,BYE,CANCEL,ACK,INFO,PRACK,COMET,OPTIONS,SUBSCRIBE,NOTI
From: 0001 <sip:0001@192.168.1.115>;tag=GLPG_3372630384-4780
To: sip:0001@192.168.1.115
Call-ID: GLPG-9223369124778
CSeq: 1 REGISTER
Expires: 120
Contact: 0001 <sip:0001@192.168.1.115>
Content-Length: 0
```

Active Registration Graph 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



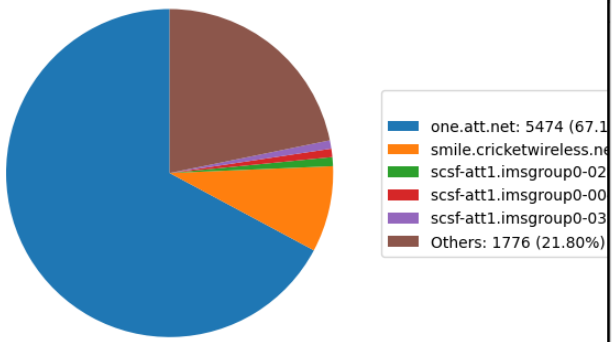
Registrar(s) Distribution, Registration vs Deregistration KPIs

SIP-REGISTER KPI CHART

Registrar messages per session **Registrar(s) distribution** Registration(s) vs Deregistration(s) Registration(s) Over Time Deregistration(s) Over Time Registration(s) - Deregistration(s) Over Time

Save as PDF

Registration session(s) Per Registrar



Total Registration session(s): 8147

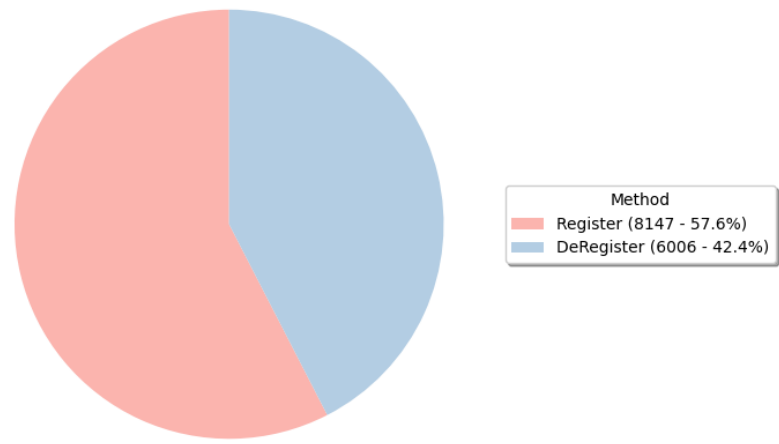
Navigation icons: Home, Back, Forward, Zoom, Filter, Save

SIP-REGISTER KPI CHART

Registrar messages per session Registrar(s) distribution **Registration(s) vs Deregistration(s)** Registration(s) Over Time Deregistration(s) Over Time Registration(s) - Deregistration(s) Over Time

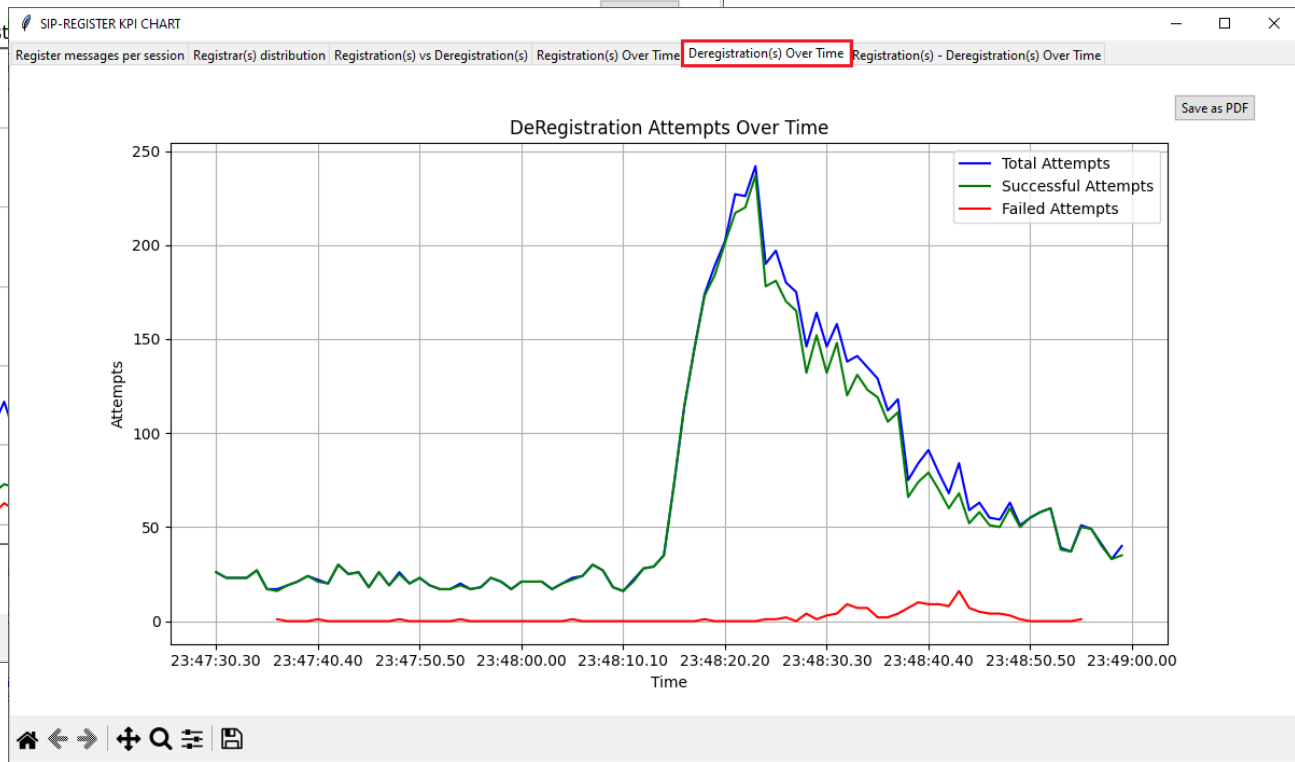
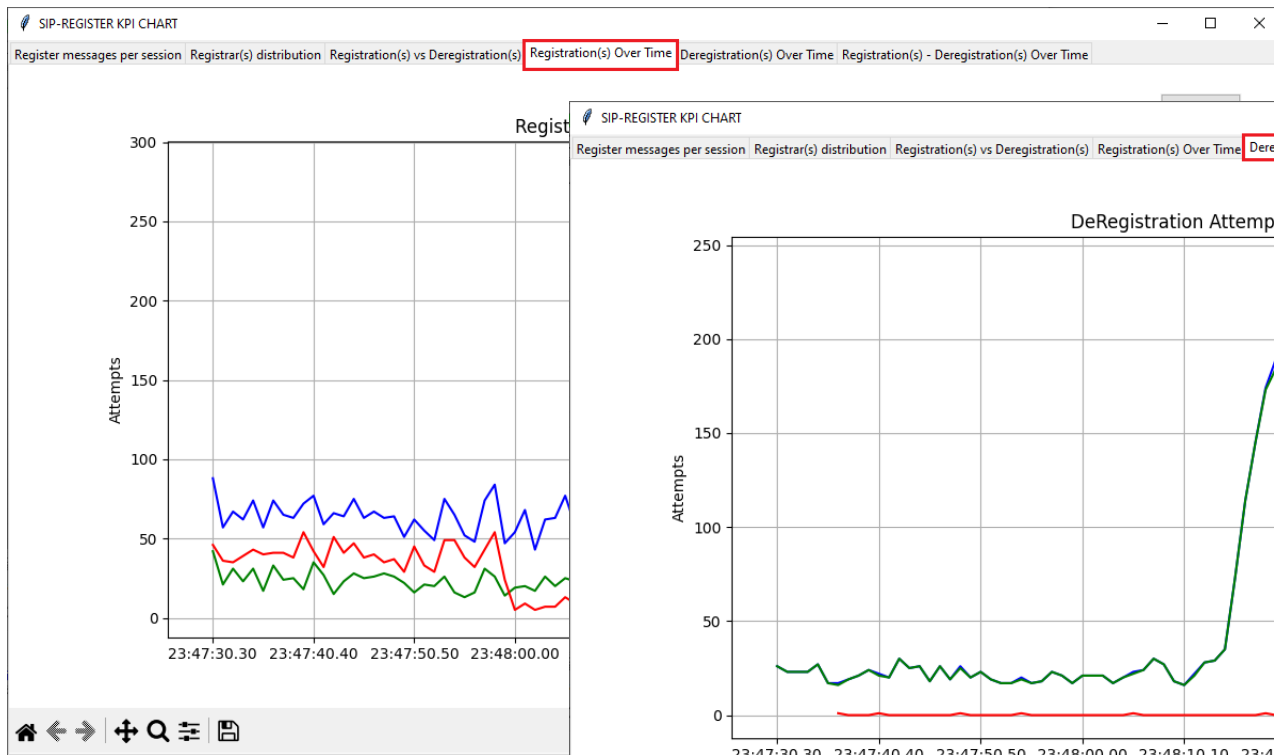
Save as PDF

Distribution of Register vs Deregister

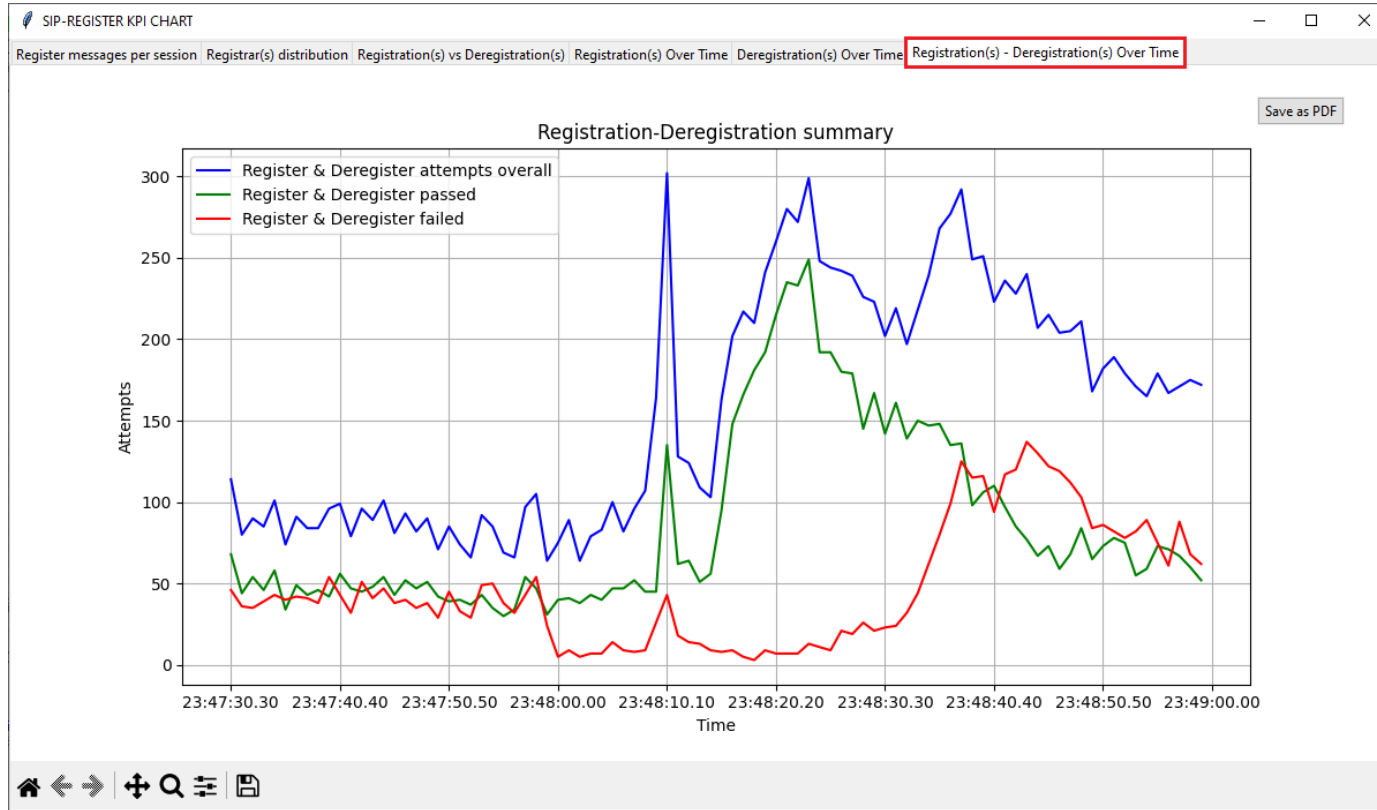


Navigation icons: Home, Back, Forward, Zoom, Filter, Save

Registration(s) over Time, Deregistration over Time KPIs

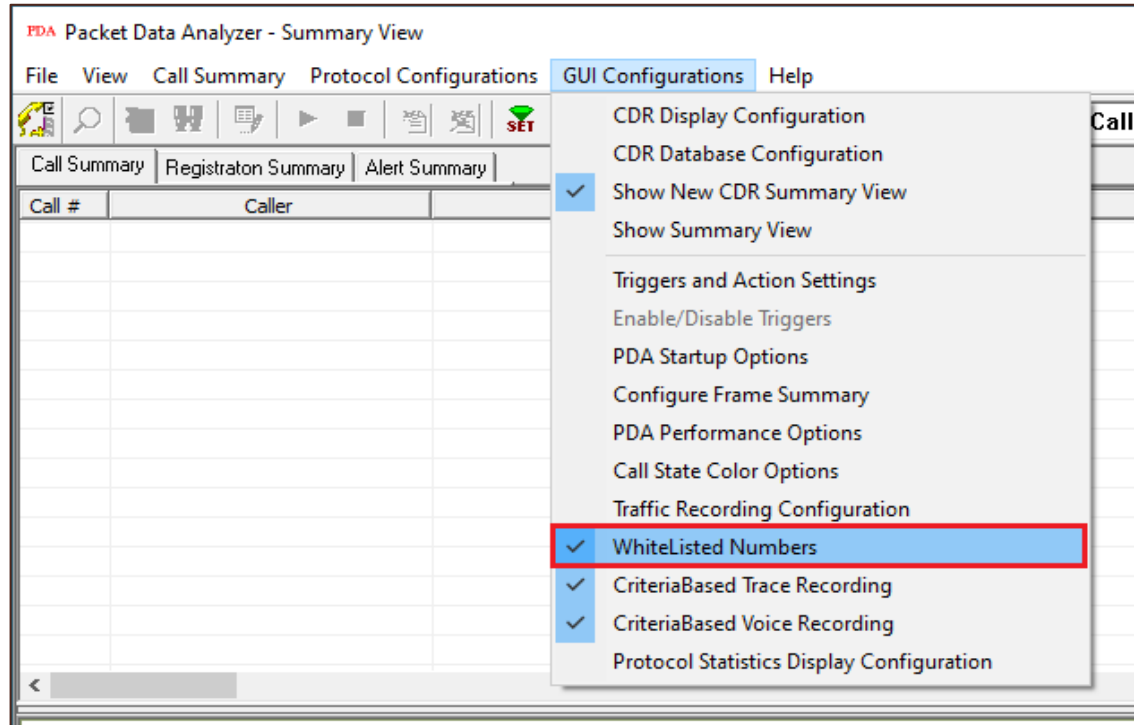


Registration(s)-Deregistration(s) over Time KPI



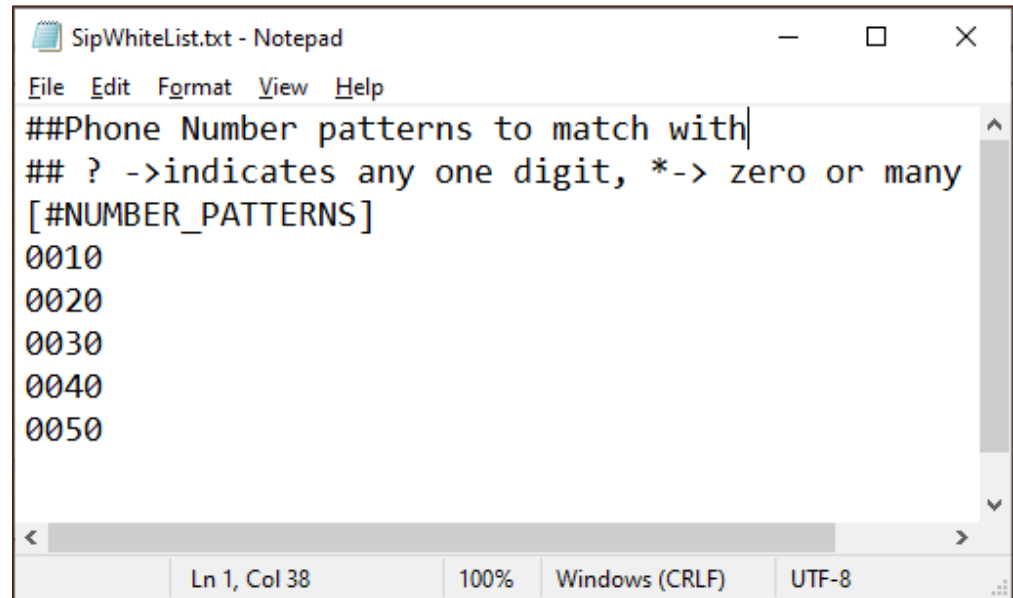
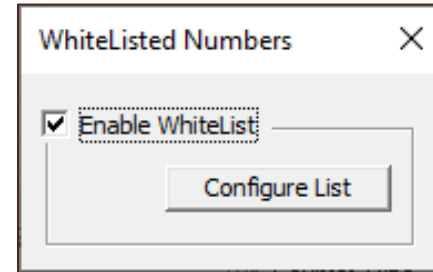
Whitelist Configuration

- On the **PDA** main window, click on **GUI Configurations** → **WhiteListed Numbers** to configure Whitelist number

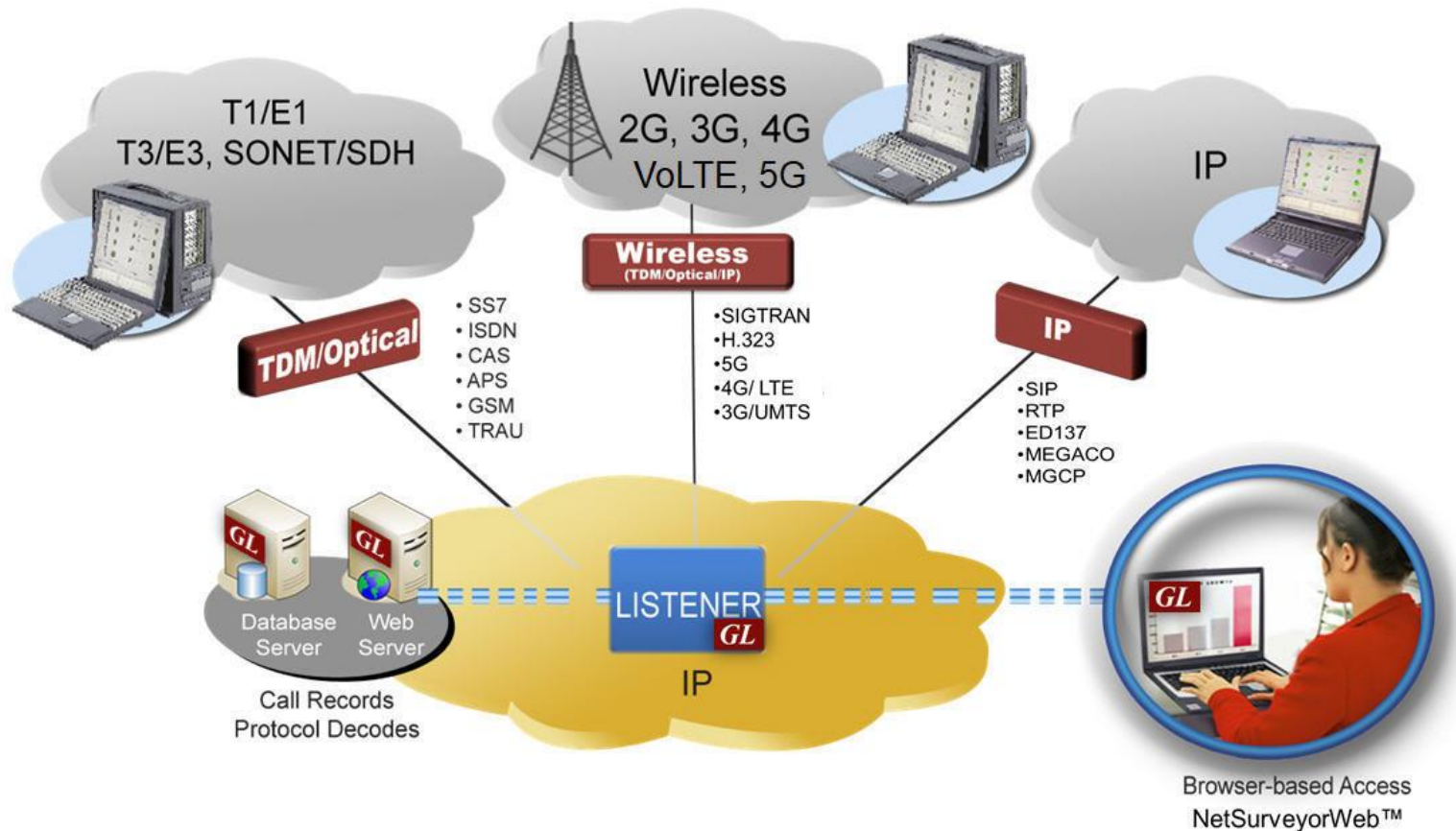


Whitelist Configuration (Contd.)

- Check the **Enable WhiteList** option and click on **Configure List**. This will invoke **SIPWhiteList.txt** in the Notepad application
- Enter the **SIP Caller** or **Callee** Number
- The following numbers should be added in the **SipWhiteList.txt** file
 - 0010
 - 0020
 - 0030
 - 0040
 - 0050
- **Save** and **Close** the file

A screenshot of a Notepad window titled "SipWhiteList.txt - Notepad". The text content is: ##Phone Number patterns to match with, ## ? ->indicates any one digit, *-> zero or many, [#NUMBER_PATTERNS], 0010, 0020, 0030, 0040, 0050. The status bar at the bottom shows "Ln 1, Col 38", "100%", "Windows (CRLF)", and "UTF-8".

NetSurveyorWeb™ - Network Surveillance System



NetSurveyorWeb™ Main GUI

The screenshot displays the NetSurveyorWeb main GUI. The top header shows 'GL NetSurveyorWeb' on the left, a 'Refresh' button in the center, and 'Protocol Type: VOIP (SIP & H323)' on the right. Below the header, there's a navigation menu on the left with options like 'Quick CDR', 'All Calls', 'Failed Calls', etc. The main content area shows a 'Quick CDR \ All Calls' section with a date filter set to '2018-07-05' and a time range from '00:00:00' to '23:59:59'. Below this, there's a search bar with 'Trafficsumid' entered and a table of call records. The table has columns for SIno, Calling Number, Called Number, Starttime, Duration, Call Success, Failure Cause, Listening Mos1, Listening Mos2, and Payload1. The table contains 12 rows of call data.

SIno	Calling Number	Called Number	Starttime	Duration	Call Success	Failure Cause	Listening Mos1	Listening Mos2	Payload1
1	0159@192.168.12.163	0159@192.168.12.164	2018-07-05 12:12:47.134	00:01:00.024	1	0	3.02	3.02	SPEEX/8000
2	0160@192.168.12.163	0160@192.168.12.164	2018-07-05 12:12:47.134	00:01:00.024	1	0	3.02	3.02	SPEEX/8000
3	0161@192.168.12.163	0161@192.168.12.164	2018-07-05 12:12:47.134	00:01:00.024	1	0	4.16	4.16	SPEEX/8000
4	0158@192.168.12.163	0158@192.168.12.164	2018-07-05 12:12:47.104	00:01:00.024	1	0	4.16	4.16	SPEEX/8000
5	0157@192.168.12.163	0157@192.168.12.164	2018-07-05 12:12:47.094	00:01:00.024	1	0	4.16	4.16	SPEEX/8000
6	0156@192.168.12.163	0156@192.168.12.164	2018-07-05 12:12:47.094	00:01:00.024	1	0	3.02	3.02	SPEEX/8000
7	0155@192.168.12.163	0155@192.168.12.164	2018-07-05 12:12:47.064	00:01:00.024	1	0	4.16	4.16	SPEEX/8000
8	0153@192.168.12.163	0153@192.168.12.164	2018-07-05 12:12:47.044	00:01:00.024	1	0	4.01	4.01	iLBC_15_2/8000
9	0154@192.168.12.163	0154@192.168.12.164	2018-07-05 12:12:47.044	00:01:00.024	1	0	3.95	3.95	iLBC_13_33/8000
10	0152@192.168.12.163	0152@192.168.12.164	2018-07-05 12:12:47.034	00:01:00.024	1	0	3.98	3.98	EVRCB/8000
11	0151@192.168.12.163	0151@192.168.12.164	2018-07-05 12:12:47.024	00:01:00.024	1	0	3.98	3.98	EVRCB/8000
12	0150@192.168.12.163	0150@192.168.12.164	2018-07-05 12:12:47.014	00:01:00.024	1	0	3.77	3.77	EVRCB/8000

- Multiple PacketScan™ probes can be used for network monitoring, with call detail reports exported to a central data base
- Results can be accessed remotely using NetSurveyorWeb™, a simple web browser based application

Thank you