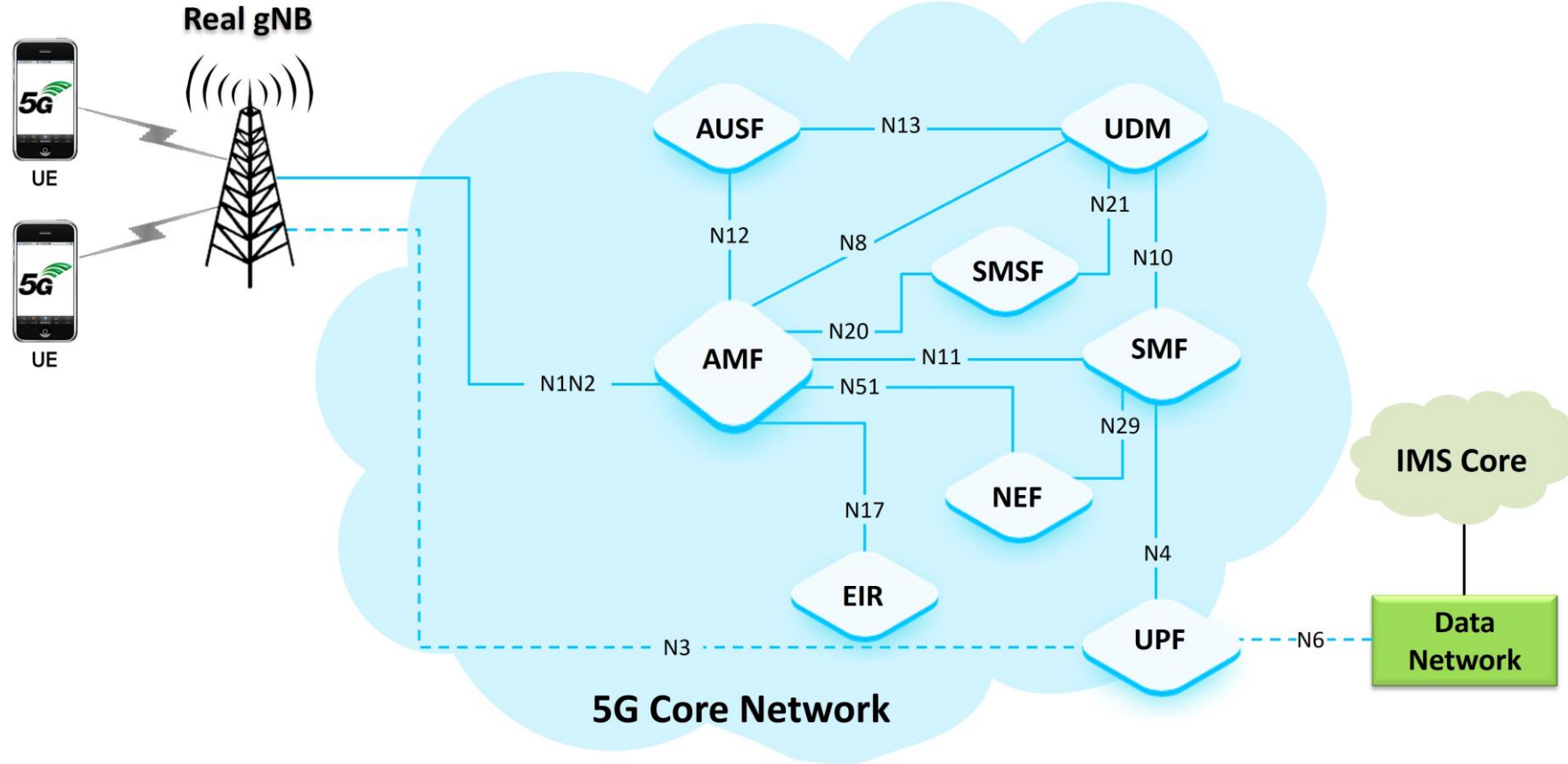

PacketScan™ 5G Protocol Analyzer



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>

Introduction

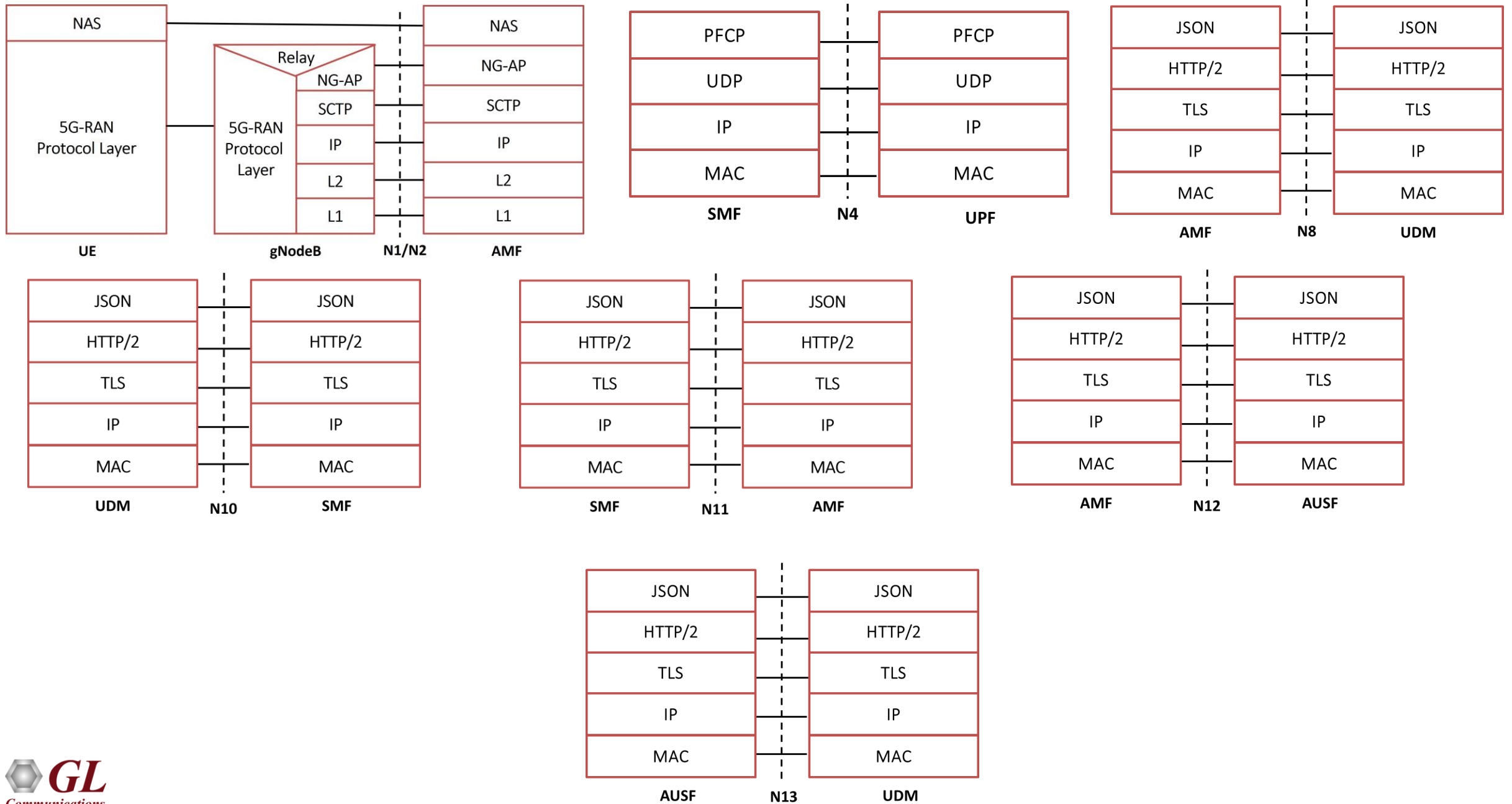


- PacketScan™ 5G protocol analyzer supports monitoring of 5G networks
- Captures, segregates, monitors and collects statistics on all calls over N1N2, N4, N8, N10, N11, N12, and N13 interfaces of the 5G network

Main Features

- Capture, decode, and analyze calls in the 5G Network
- Supported protocols include Non-Access Stratum (NAS), Next Generation Application Protocol (NGAP), Packet Forwarding Control Protocol (PFCP)
- Supported interfaces:
 - N1N2 Interface - gNodeB (also called Next Generation RAN), and AMF (Access and Mobility Management Function) nodes
 - N4 Interface - Session Management Function (SMF) and User Plane Function (UPF) elements
 - N8 Interface - Unified Data Management (UDM) and Access and Mobility Management Function (AMF)
 - N10 Interface - Unified Data Management (UDM) and Session Management Function (SMF)
 - N11 Interface - Mobility Management Function (AMF) and Session Management Function (SMF)
 - N12 Interface - Authentication Server Function (AUSF) and Access and Mobility Management Function (AMF)
 - N13 Interface - Authentication Server Function (AUSF) and User Data Management (UDM)
- Provides VoNR call statistics such as caller, callee, MOS scores, discarded packets and voice storage
- Save calls to PCAP (Wireshark® format) and in HDL (GL Proprietary format)
- Packet Data Analyzer feature in Packetscan™ provide a complete call flow of a 5G session
- Displays Summary, Detail, Hex dump, Statistics, and Call Detail Views

Protocol Stack



Protocol Specifications

Supported Protocols	Standard / Specification
System Architecture for the 5G	3GPP TS 23.501
NG Application Protocol (NGAP)	3GPP TS 38.413
Non-Access-Stratum (NAS)	3GPP TS 24.501
GPRS Tunneling Protocol for User Plane (GTP-U)	3GPP TS 29.281
NR and NG-RAN Overall Description	3GPP TS 28.300
Packet Forwarding Control Protocol (PFCP)	3GPP TS 29.244
UDP	IETF RFC 768
IPv4	IETF RFC 791 [5]
IPv6	IETF RFC 2460 [6]
JavaScript Object Notation (JSON)	IETF RFC 8259
HTTP/2	IETF RFC 7231 IETF RFC 7540/RFC 7541
TLS	IETF RFC 8446
TCP	IETF RFC 793

Configuration Editor Settings

The screenshot shows a window titled "Configuration Editor of PacketScan Settings. C:\Program Files\GL Communications Inc\Pa...". The window contains a tree view on the left with the following items: TCAP, CNAM, TCP and/or UDP, SCTP, PDA, PDA Performance Log, LTE, UMTS, IMS, and 5G. The 5G item is selected and expanded, showing a table of settings:

NgAP Protocol Version:	Release 15 V.2
NAS-5G Protocol Version:	Release 15 V.2
MISCELLANEOUS	
IMSI MNC Digits Length	2
Enable/Disable LTE signalling processing:	<input checked="" type="checkbox"/>
Number of protocol decoder to be created:	1
Point Code Notation:	DOT
Number of frames to be processed per second in offline:	0
Enable/Disable luPS signalling processing:	<input type="checkbox"/>
Enable/Disable GB signalling processing:	<input type="checkbox"/>
Active call timer:	360

Below the table, there is a section titled "5G Settings." and a row of buttons: Apply, Default, Expand, Collapse, and Exit.

Real-time Analysis

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

The screenshot displays the PacketScan 64-bit application window. The top menu includes File, View, Capture, Statistics, Database, Call Detail Records, Configure, and Help. Below the menu is a toolbar with various icons and a 'GoTo' field. The main window is divided into two panes. The upper pane 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 Address IPv4. The lower pane shows a detailed protocol tree for the selected packet (Frame #61), highlighting the NGAP Layer. The protocol tree includes fields such as NGAP-PDU, Extensibility Marker, Choice Index, InitiatingMessage, ProcedureCode, Contents, procedureCriticality, Value, Length, InitialUEMessage, Extensibility Marker, ProtocolIE-Container, Iteration Count, ProtocolIE-Container, ProtocolIE-Field, ProtocolIE-ID, Contents, procedureCriticality, Value, Length, RAN-UE-NGAP-ID, Length Determinant, Contents, ProtocolIE-Container, ProtocolIE-Field, ProtocolIE-ID, Contents, procedureCriticality, Value, Length, NAS PDU, and NAS-PDU.

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4
✓ 0	54	00:00:04.071183000	60		ARP			
✓ 0	55	00:00:04.078905000	60		ARP			
✓ 0	56	00:00:04.530010000	217		Internet IP(IPv4)		192.168.12.10	239.255.255.250
✓ 0	57	00:00:04.530250000	217		Internet IP(IPv4)		192.168.12.11	239.255.255.250
✓ 0	58	00:00:04.679183000	158		Internet IP(IPv4)		192.168.13.101	192.168.13.106
✓ 0	59	00:00:04.756884000	60		ARP			
✓ 0	60	00:00:04.769177000	130		Internet IP(IPv4)		192.168.13.106	192.168.13.101
✓ 0	61	00:00:04.779202000	126		Internet IP(IPv4)		192.168.13.101	192.168.13.106

```

0030 Length = 112 (x0070)
0032 TSN = 448 (x000001C0)
0036 Stream Identifier = 0 (x0000)
0038 Stream Sequence Number = 448 (x01C0)
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 = 36
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 = SEQUENCE
NAS-PDU = OCTET STRING
    
```

At the bottom of the window, the status bar shows: Capture Rate : 0.02 Mbps, C:\Program Files\GL Communications Inc\Packe Captured 10 242 frames, Missed Frames : 0.

Detail View of 5G NAS Layer

The detail decode view of NAS Layer displays the following:

- MAC Layer
- IPv4 Layer
- SCTP Layer
- NGAP Layer
- NAS Layer

The screenshot shows the PacketScan 64-bit interface. The top part is a table of captured packets:

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type	Packet Type	Source IP Address	Destination IP Address
✓	0	00:00:04.071183000	60		ARP			
✓	0	00:00:04.078905000	60		ARP			
✓	0	00:00:04.530010000	217		Internet IP(IPv4)		192.168.12.10	239.255.255.250
✓	0	00:00:04.530250000	217		Internet IP(IPv4)		192.168.12.11	239.255.255.250
✓	0	00:00:04.679183000	158		Internet IP(IPv4)		192.168.13.101	192.168.13.106
✓	0	00:00:04.756884000	60		ARP			
✓	0	00:00:04.769177000	130		Internet IP(IPv4)		192.168.13.106	192.168.13.101
✓	0	00:00:04.779202000	126		Internet IP(IPv4)		192.168.13.101	192.168.13.106

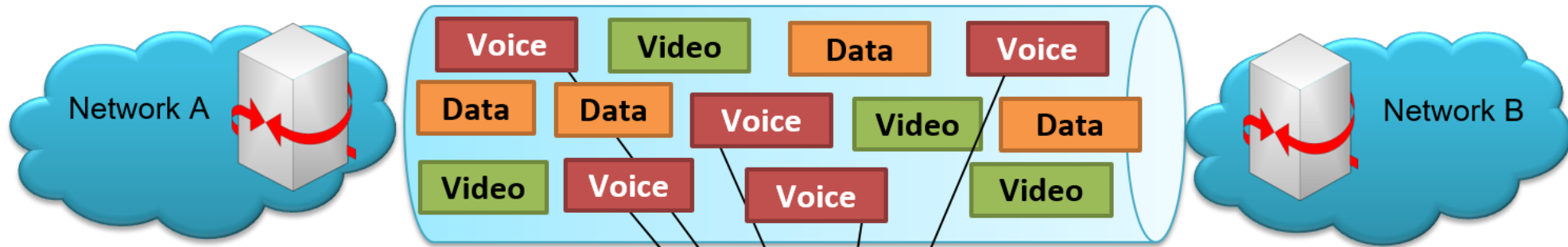
The bottom part shows the detailed decode view of the selected packet (Frame 0):

```

Contents = 0 reject(0)
Value = Open Type
Length = 1
UEContextRequest = ENUMERATOR
Extensibility Marker = 0
Contents = 0 requested(0)
===== 5G NAS Layer =====
0050 Extended Protocol Discriminator = 01111110 SGS Mobility Management Messages
0051 Security Header Type = ....0000 Plain NAS message, not security protected
0052 Message Type = 01000001 Registration Request
      5GS Registration Type and NAS Key Set Identifier =
0053 Registration Type = ....0001 Initial Registration
0053 Follow-On Request = ....0... No follow-on Request Pending
0053 NAS Key Set Identifier = .111.... (7)
0053 Type of Security Context Flag (TSC) = 0..... Native security context (for KSIAMF)
      5GS Mobile Identity =
0054 Length = 13 (x000D)
0056 Type of Identity = ....0001 SUCI
0056 SUPI Format = .000.... IMSI
0057 MCC = 001
0058 MNC = 01
005A Routing Indicator Digit = 0000
005C Protection Scheme Identifier = ....0000 Null scheme
005D Home Network Public Key Identifier = 0 (x00)
      Scheme output = 3012041631
      5GMM Capability =
0063 Information Element Id = 00010000 5GMM Capability
0064 Length = 1 (x01)
0065 S1 Mode = .....0 Not Supported
0065 HO Attach = .....0. Handover request to transfer PDU session from N1 mode to S1 mode not supported
0065 LTE Positioning Protocol (LPP) Capability = .....0... LPP in N1 mode not supported
      UE Security Capability =
0066 Information Element Id = 00101110 UE Security Capability
0067 Length = 2 (x02)
0068 5GS Encryption Algorithm 5G-EA7 = .....0 Not Supported
0068 5GS Encryption Algorithm 5G-EA6 = .....0. Not Supported
0068 5GS Encryption Algorithm 5G-EA5 = .....0... Not Supported
0068 5GS Encryption Algorithm 5G-EA4 = ....0... Not Supported
0068 5GS Encryption Algorithm 128-5G-EA3 = ..0.... Not Supported
0068 5GS Encryption Algorithm 128-5G-EA2 = .0..... Not Supported
0068 5GS Encryption Algorithm 128-5G-EA1 = .1..... Supported
  
```

At the bottom of the window, the status bar shows: Capture Rate: 0.02 Mbps, C:\Program Files\GL Communications Inc\Packe Captured 11 586 frames, Missed Frames: 0.

Wireshark Filtering



Wireshark lossless capture and filter

- Filtering can be based on the following:

- Pattern match
- Protocol information
- Frame size

- Checksum errors

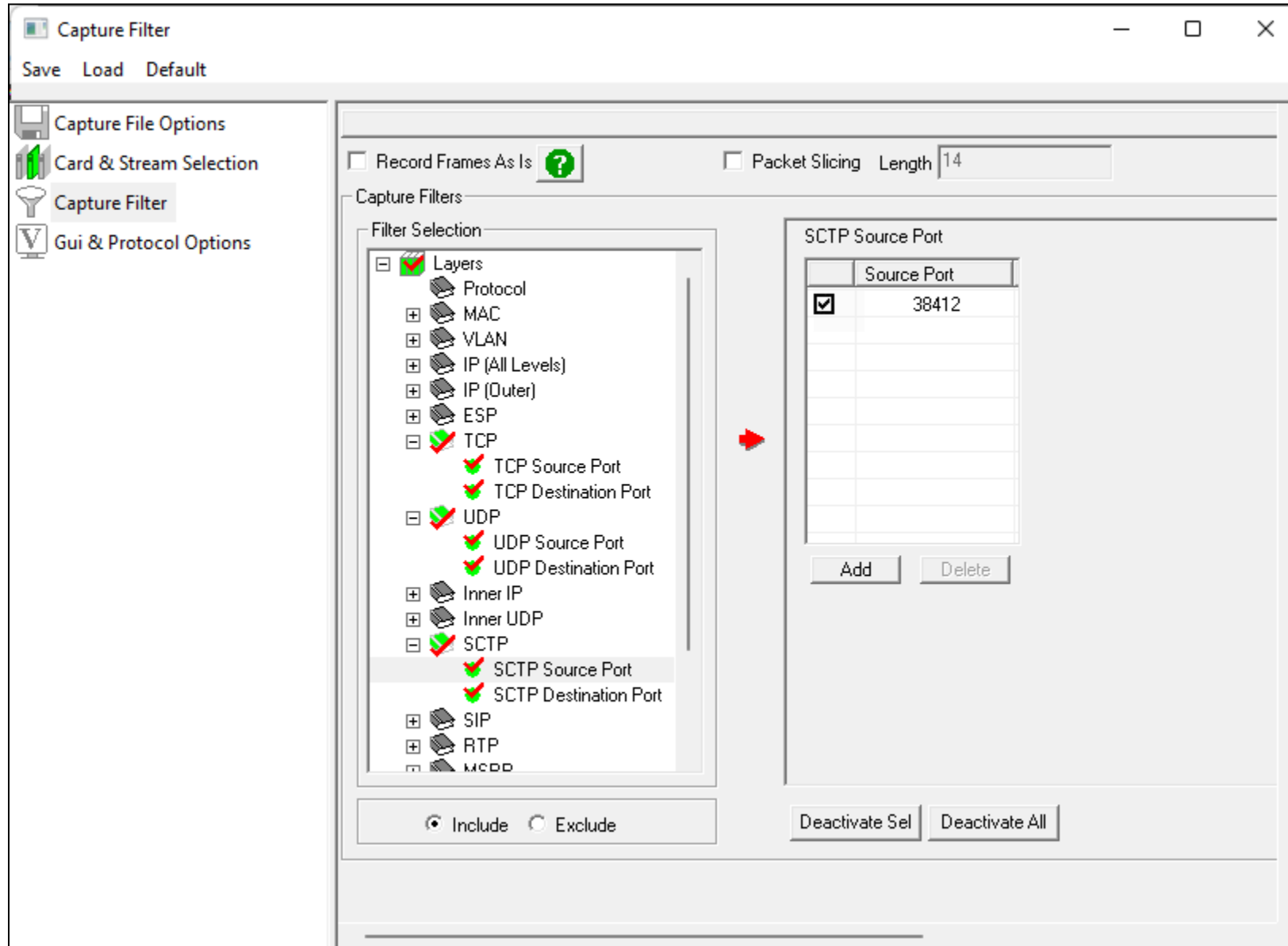
- Port number

- IP address and address ranges

Voice



Real-time Capture Filter



Packet Data Analyzer (PDA) – 5G N1N2 Call Graph

- Displays the message sequences of captured 5G calls
- Decodes of the selected N1N2 message is displayed on the right pane

PDA Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

5G N1N2 Interface Show All Calls

Call Summary | Registrar Summary | Alert Summary

Call #	StartTime	AmfUeNgapId	RrcEstablishmentCause	NrCellIdentity	Tac	AmfSetID	AmfRegionID	Amfpointer	Mcc	Mnc	RegistrationType	EndTime	RegistrationResult
1	2023-01-25 11:28:33.449	76	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.854	ACCEPTED
2	2023-01-25 11:28:37.052	77	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.654	ACCEPTED
3	2023-01-25 11:28:37.752	78	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.954	ACCEPTED
4	2023-01-25 11:28:41.453	81	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.854	ACCEPTED
5	2023-01-25 11:28:41.453	80	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.854	ACCEPTED
6	2023-01-25 11:28:41.453	83	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.854	ACCEPTED
7	2023-01-25 11:28:41.453	79	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.954	ACCEPTED
8	2023-01-25 11:28:41.453	82	mo-Signalling	1	1	1			001	01	Initial Registration	2023-01-25 11:28:41.553	REJECTED
9	2023-01-25 11:28:41.453	84	mo-Signalling	1	1	1			001	01	Initial Registration	2023-01-25 11:28:41.541	REJECTED
10	2023-01-25 11:28:41.453	85	mo-Signalling	1	1	1	2	63	001	01	Initial Registration	2023-01-25 11:28:47.754	ACCEPTED

Column Width Absolute Timing Show Latest

Time	Frame#	192.168.13.101	192.168.13.106
00.00.000	24	38412	38412
		InitialUEMessage - Registration Request	
00.00.088	25	38412	38412
		DownlinkNASTransport - Authentication Request	
00.00.100	26	38412	38412
		UplinkNASTransport - Authentication Response	
00.00.188	28	38412	38412
		DownlinkNASTransport - Security Mode Command	
00.00.200	30	38412	38412
		UplinkNASTransport - Security Mode Complete	
00.00.288	31	38412	38412
		InitialContextSetup - Registration Accept	
00.00.300	33	38412	38412
		InitialContextSetupRes	
00.00.300	34	38412	38412
		UplinkNASTransport - Registration Complete	
00.00.400	37	38412	38412
		UplinkNASTransport - UL NAS Transport - Session Establishment	
00.00.488	39	38412	38412
		PDUSessionResourceSetup - DL NAS Transport - Session Establishment	
00.00.500	40	38412	38412
		PDUSessionResourceSetupRes	
00.00.600	44	38412	38412
		UplinkNASTransport - UL NAS Transport - Session Establishment	
00.00.688	48	38412	38412
		PDUSessionResourceSetup - DL NAS Transport - Session Establishment	
00.00.800	53	38412	38412
		PDUSessionResourceSetupRes	
00.10.302	179	38412	38412
		UplinkNASTransport - UL NAS Transport - Session Release	
00.10.391	187	38412	38412
		PDUSessionResourceRelease - DL NAS Transport - Session Release	
00.10.401	194	38412	38412
		PDUSessionResourceReleaseRes	
00.10.401	199	38412	38412
		UplinkNASTransport - UL NAS Transport - Session Release Complete	

Find Complete Stack

```

===== NGAP Layer =====
NGAP-PDU = CHOICE
Extensibility Marker = 0
Choice Index = 0
InitiatingMessage = SEQUENCE
ProcedureCode = INTEGER
Contents = 16 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 = 79
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 = SEQUENCE
NAS-PDU = OCTET STRING
Length Determinant = 43
Contents = x7E004101000D0100F110000000003214061C
ProtocolIE-Container = Instance 2
ProtocolIE-Field = SEQUENCE
ProtocolIE-ID = INTEGER
    
```

Active Calls Graph Call Graph Call Summary



Packet Data Analyzer (PDA) – 5G N4 Call Graph

- Decodes of the selected N4 message is displayed on the right pane

PDA Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

5G N4 (smf-upf) Show All Calls

Call Summary Registraton Summary Alert Summary

Call #	SmfNodeId	NetworkInstance	QFI	GnbTeid	GnbTunIPv4	GnbTunIPv6	UpfTeid	UpfTunIPv4	UpfTunIPv6
1	192.168.13.183	ims	1	3	192.168.13.181		2	192.168.13.185	
2	192.168.13.183	internet	1	5	192.168.31.53		4	192.168.13.185	
3	192.168.13.183	ims	1	3	192.168.13.181		2	192.168.13.185	
4	192.168.13.183	internet	1	5	192.168.31.53		4	192.168.13.185	

Column Width Absolute Timing Show Latest

Time	Frame#	192.168.13.183	192.168.13.185
00.00.000	2905	8805	8805
00.00.000	2911	8805	8805
00.00.003	2959	8805	8805
00.00.004	2966	8805	8805
00.00.008	3026	8805	8805
00.00.009	3027	8805	8805

Find Complete Stack

```

===== PFCP Layer =====
S
Message Priority:
Version
Message Type
Length
Session Endpoint Identifier
Sequence Number
Message Priority
Node ID
Information Element Id
Length
Node ID Type
IPv4 Address
CP F-SEID
Information Element Id
Length
V6
V4
SEID
IPv4 Address
    
```

Active Calls Graph Call Graph Call Summary

Packet Data Analyzer (PDA) – 5G N8 Call Graph

- Decodes of the selected N8 message is displayed on the right pane

The screenshot displays the Packet Data Analyzer (PDA) interface. The main window is titled "PDA Packet Data Analyzer - Summary View". The menu bar includes "File", "View", "Call Summary", "Protocol Configurations", "GUI Configurations", and "Help". The toolbar contains various icons for search, refresh, and other functions. The main display area is divided into several sections:

- Call Summary:** A table showing call details. The first call is selected, showing details for AmfInstanceId, Nssai_sst, ServiceName, DNN, APIRoot, and Method.
- Message Details:** A table showing message details. The first message is selected, showing details for Time, Frame#, and other parameters.
- Message Content:** A text area displaying the decoded message content, including headers and a JSON body.

The Call Summary table is as follows:

Call #	AmfInstanceId	Nssai_sst	ServiceName	DNN	APIRoot	Method
1	5f8466cd-8e0b-4f49-9e69-17533b...		nudm-uecm		http://192.168.13.188:6666	PUT
2		1	nudm-udm		http://192.168.13.188:6666	GET

The Message Details table is as follows:

Time	Frame#	192.168.13.184	192.168.13.188
00.00.000	2791	33233	6666
00.00.000	2797	33233	6666

The Message Content is as follows:

```
method: PUT
path: /nudm-uecm/v1/imsi-001013012042632/registrations/amf-3gpp-access
scheme: http
authority: 192.168.13.188:6666
content-type: application/json
accept: application/json, application/problem+json
content-length: 317

-----JSON-----
{"amfInstanceId": "5f8466cd-8e0b-4f49-9e69-17533b984a86"
"deregCallbackUri": "http://192.168.13.184:6666/nudm-uecm/v1/imsi-001013012042632/registrations/amf-3gpp-access"
"guami": {"amfId": "2163"
"plmnId": {"mcc": "001"
"mnc": "01"}}
"imsVoPs": "HOMOGENEOUS_SUPPORT"
"initialRegistrationInd": true
"ratType": "NR"}
```

Packet Data Analyzer (PDA) – 5G N10 Call Graph

- Decodes the selected N10 message is displayed on the right pane

The screenshot shows the Packet Data Analyzer (PDA) interface. The title bar reads "PDA Packet Data Analyzer - Summary View". The menu bar includes "File", "View", "Call Summary", "Protocol Configurations", "GUI Configurations", and "Help". The toolbar contains various icons for search, zoom, and other functions. The main window is divided into several sections:

- Call Summary:** A table showing call details. The first call is highlighted.
- Packet List:** A table showing packet details. The first packet is highlighted.
- Packet Detail View:** A detailed view of the selected packet, showing the method (PUT), path, scheme, authority, content-type, accept, and content-length. The JSON body is also displayed.

Call #	SMFInstanceId	DeregCallbackUri	SUPI	APIRoot	Method	OperationId
1	2f8cde07-3a87-4934-9d66-83a40...	http://192.168.13.183:6667/nudm...	imsi-001013012042632	http://192.168.13.188:6666	PUT	GetSmfRegistra
2			imsi-001013012042632	http://192.168.13.188:6666	GET	GetSmData

Time	Frame#	192.168.13.183	192.168.13.188
00.00.000	2880	44233	6666
00.00.000	2885	44233	6666

```
method: PUT
path: /nudm-uecm/v1/imsi-001013012042632/registrations/smf-regis
scheme: http
authority: 192.168.13.188:6666
content-type: application/json
accept: application/json, application/problem+json
content-length: 282

-----JSON-----
{"deregCallbackUri": "http://192.168.13.183:6667/nudm-uecm/v1/ims
"dnn": "ims"
"pduSessionId": 5
"plmnId": {"mcc": "001"
"mnc": "01"}
"singleNssai": {"sd": "01"
"sst": 1}
"smfInstanceId": "2f8cde07-3a87-4934-9d66-83a40d24dd2b"}
```

Packet Data Analyzer (PDA) – 5G N11 Call Graph

- Decodes the selected N11 message is displayed on the right pane

The screenshot displays the Packet Data Analyzer (PDA) interface. At the top, the title bar reads "PDA Packet Data Analyzer - Summary View". Below the title bar is a menu bar with "File", "View", "Call Summary", "Protocol Configurations", "GUI Configurations", and "Help". A toolbar contains various icons, including a search icon, a play icon, and a "5G" dropdown menu. The main window is divided into several sections:

- Call Summary:** A table with columns: Call #, SUPI, MCC, MNC, sNssai-sd, sNssai-sst, ServingNfID, PDUSessionID, PDUSessionType, SSC-Mode, and SmfServiceInstanceID. Two rows are visible, both with SUPI "imsi-001013012042632".
- Column Width:** A slider and checkboxes for "Absolute Timing" and "Show Latest".
- Call Graph:** A timeline view showing two frames. Frame 2875 (Time 00.00.000) is a POST request to "/nsmf-pdusession/v1/sm-contexts" with length 6666. Frame 2908 (Time 00.00.002) is a "201 Created" response with length 6666. Arrows indicate the flow from the request to the response.
- Decoded Message:** A text area showing the details of the POST request, including headers like "method: POST", "path: /nsmf-pdusession/v1/sm-contexts", "scheme: http", "authority: 192.168.13.183:6666", "accept: application/json, application/vnd.3gpp.ngap, application/problem+json", "content-type: multipart/related; boundary='9a942FF552dd471Fc301'", "mime-version: 1.0", and "content-length: 655". Below the headers is a JSON body containing fields like "anType", "dnn", "gpsi", "nlSmMsg", "pduSessionId", "pei", "ratType", "requestType", "sNssai", "sst", "servingNetwork", "mnc", "servingNfId", "smContextStatusUri", and "supi".

At the bottom, there are tabs for "Active Calls Graph", "Call Graph", and "Call Summary".

Packet Data Analyzer (PDA) – 5G N12 Call Graph

- Decodes of the selected N12 message is displayed on the right pane

The screenshot displays the Packet Data Analyzer (PDA) Summary View interface. The window title is "PDA Packet Data Analyzer - Summary View". The menu bar includes File, View, Call Summary, Protocol Configurations, GUI Configurations, and Help. The toolbar shows various icons and a dropdown menu set to "5G". The main view is divided into several sections:

- Call Summary:** A table listing call details.
- Message Details:** A section showing the decoded message details for a selected call.
- Call Graph:** A section showing the call graph with time, frame numbers, and IP addresses.

Call #	SUCI	ResStar	AuthResult	Kseaf	APIRoot	Method
3	suci-0-001-01-0000-0-0-3012042632				http://192.168.13.191:6668	POST
4	suci-0-001-01-0000-0-0-3012042632	7D4B6F026D2AC77CA1851F41D9...	AUTHENTICATION SUCCESS	6F0532F04F0F04E3DFA59621EF2...	http://192.168.13.191:6668	PUT

Message Details:

```
method: POST
path: /nausf-auth/v1/ue-authentications
scheme: http
authority: 192.168.13.191:6668
content-type: application/json
accept: application/3gppHal+json, application/problem+json
content-length: 106
```

JSON:

```
{ "servingNetworkName": "5G:mnc001.mcc001.3gppnetwork.org"
"supiOrSuci": "suci-0-001-01-0000-0-0-3012042632" }
```

Call Graph:

Time	Frame#	192.168.13.184	192.168.13.191
00.00.000	9128	33231	6668
00.00.059	9144	33231	6668

Active Calls Graph | **Call Graph** | Call Summary

Packet Data Analyzer (PDA) – 5G N13 Call Graph

- Decodes of the selected N13 message is displayed on the right pane

The screenshot displays the Packet Data Analyzer (PDA) interface in Summary View. The window title is "PDA Packet Data Analyzer - Summary View". The menu bar includes File, View, Call Summary, Protocol Configurations, GUI Configurations, and Help. The toolbar shows various icons for search, refresh, and settings, along with a "5G" filter and "N13 [ausf-udm]" protocol selection. The "Show All Calls" dropdown is set to "Show All Calls".

The Call Summary table shows the following data:

Call #	SUPI	AuthEventSuccess	AuthEventTimestamp	AuthEventId	APIRoot	Method
2	imsi-001013012042632	true	2023-04-05T08:58:19+05:30	authEventId-001013012042632-4...	http://192.168.13.188:6666	POST
3	imsi-001013012042632				http://192.168.13.188:6666	POST

Below the table, there are options for "Column Width", "Absolute Timing", and "Show Latest". The Call Graph shows a sequence of frames between IP addresses 192.168.13.191 and 192.168.13.188. Frame 2776 (Time 00.00.000) is a POST request to "/nudm-ueau/v1/imsi-001013012042632/auth-events" with a status of 201 Created. Frame 2781 (Time 00.00.000) is a response with a status of 6666. The right pane displays the decoded message details:

```
:method: POST
:path: /nudm-ueau/v1/imsi-001013012042632/auth-events
:scheme: http
<unknown>:
<unknown>:
<unknown>:
content-length: 186
```

At the bottom, there are tabs for "Active Calls Graph", "Call Graph", and "Call Summary".

Thank you