

---

---

# Long Term Evolution (LTE) Protocol Analyzer

---

---



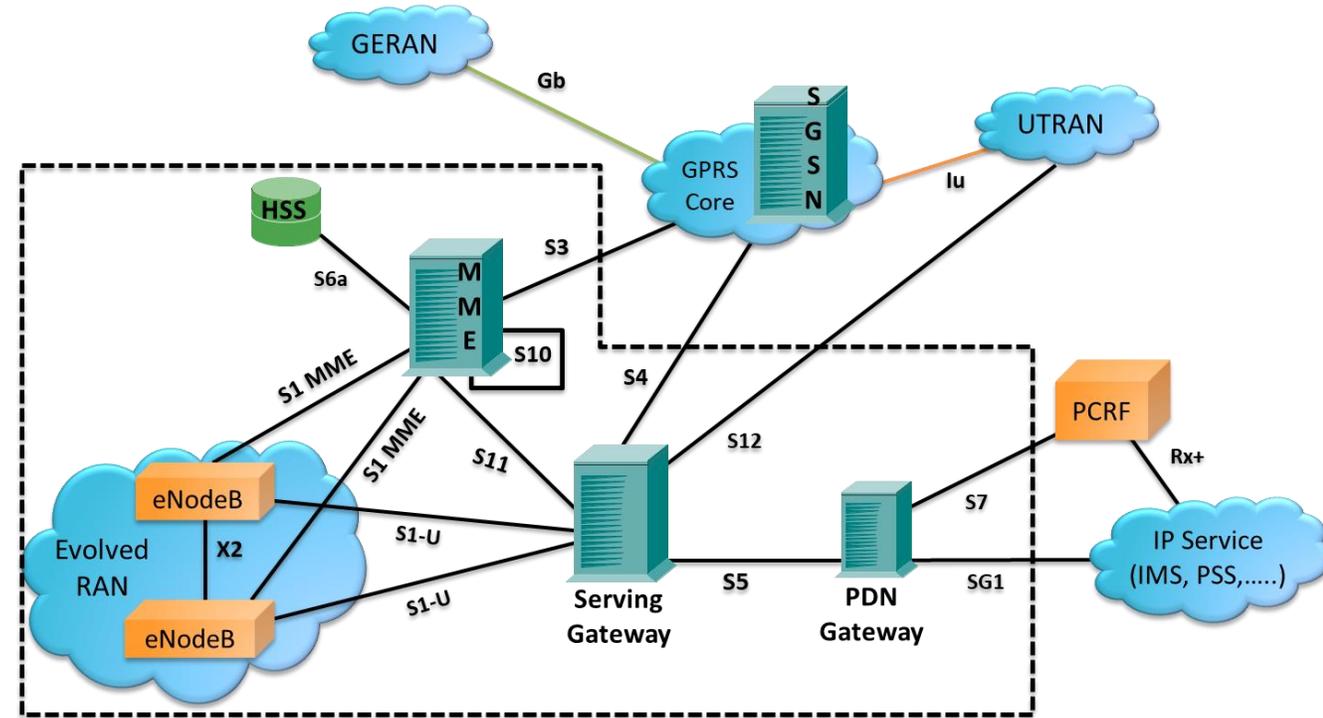
818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878  
Phone: (301) 670-4784 Fax: (301) 670-9187 Email: [info@gl.com](mailto:info@gl.com)  
Website: <https://www.gl.com>

# Introduction

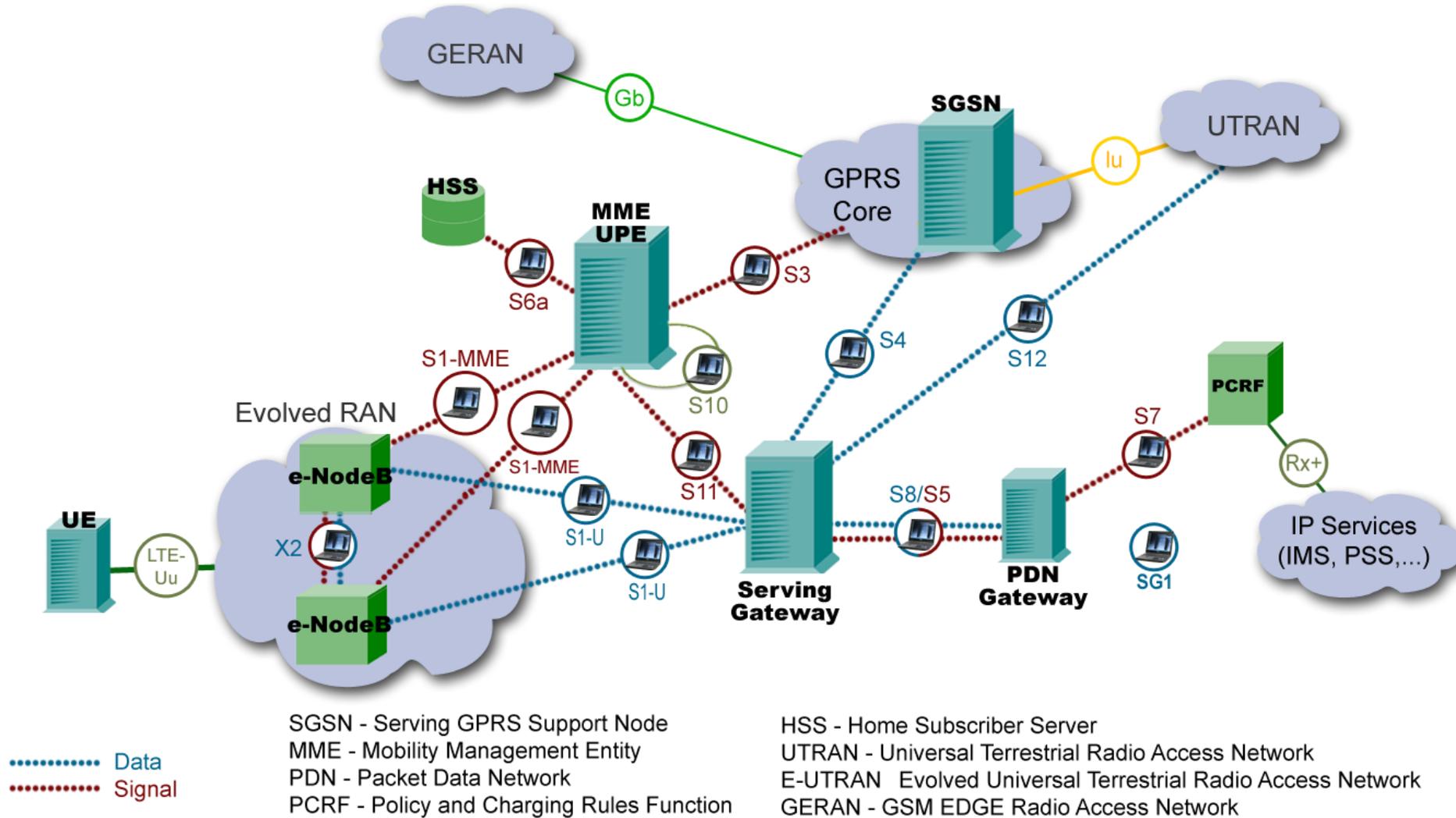
- The LTE (Long Term Evolution) protocol standard was developed as an enhancement to existing Universal Mobile Telecommunications System (UMTS) to provide users enhanced mobile Internet access
- The evolved Universal Mobile Telecommunications Service (UMTS) terrestrial Radio Access Network (RAN), abbreviated as E-UTRAN, is also known as LTE
- Although an evolution of UMTS (UMTS uses wideband code-division multiple access (WCDMA) for transmitting signals), the LTE air interface is a completely new system based on orthogonal frequency-division multiple access (OFDMA) in the downlink and single-carrier frequency-division multiple access (SC-FDMA) (DFTS-FDMA) in the uplink that efficiently supports multi-antenna technologies (MIMO)
- This robust feature is useful when handling the varying propagation conditions seen in mobile radio. In MIMO techniques, either multiple antennas can transmit the same data stream to improve data-transmission reliability or different antennas can transmit different data streams simultaneously to increase throughput
- Another significant feature of LTE is its high bandwidth—up to 20 MHz. Because the usable bandwidth is scalable, LTE can also operate in the existing 5-MHz UMTS frequency bands, or in even smaller bands

# LTE Network Diagram

- LTE standard is progressing as a part of 3rd Generation Partnership Project (3GPP)
- The Evolved Packet System (EPS) standardized by 3GPP is divided into a radio access network known as the E-UTRAN and a core network known as the Evolved Packet Core (EPC)
- The E-UTRAN consists of eNodeBs, which provide the radio interface toward the user equipment
- The eNodeBs are interconnected with each other via the IP-based X2 interface and toward the Evolved Packet Core (EPC) via the IP-based S1 interfaces



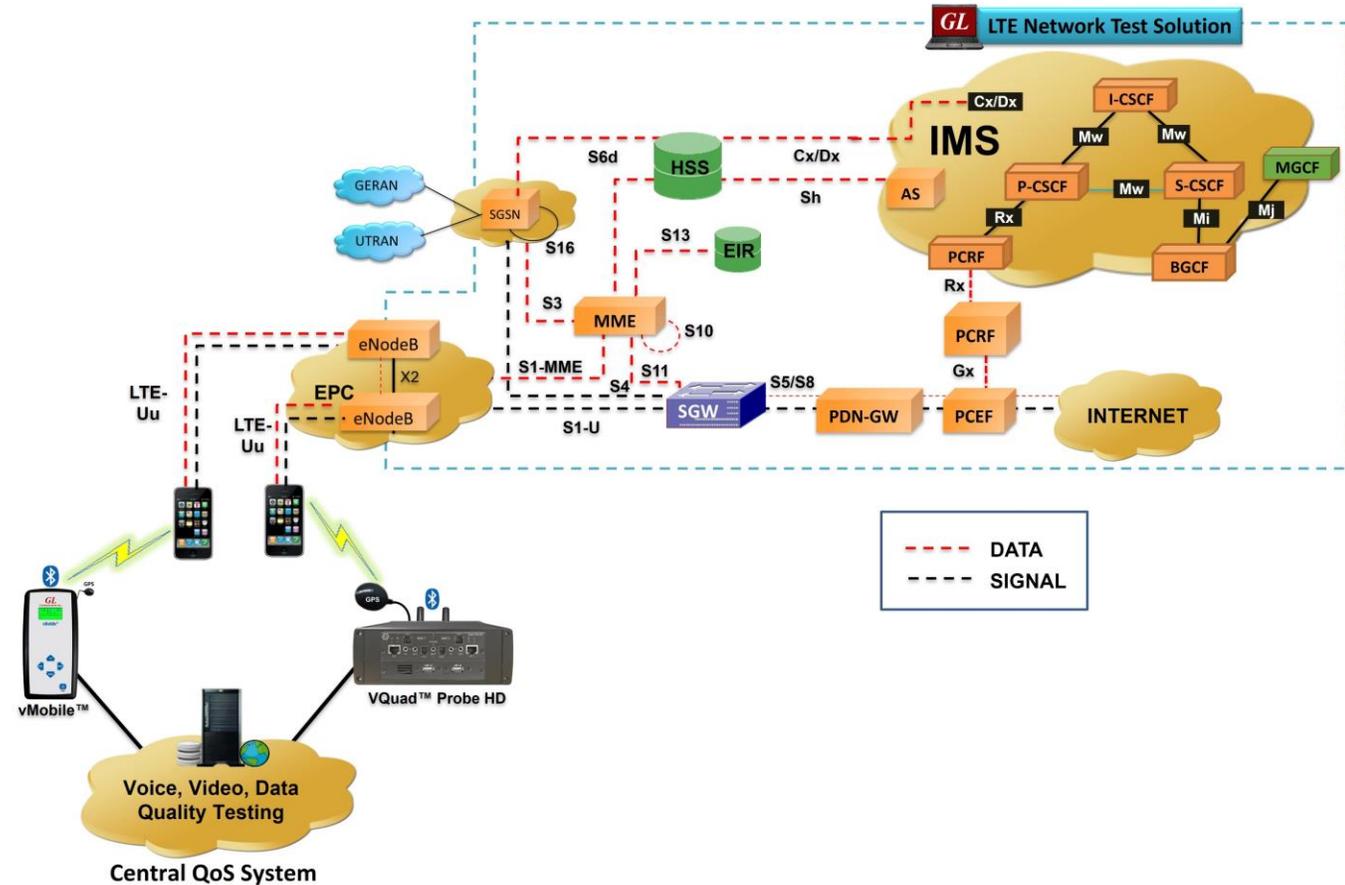
# GL's LTE Analyzer



# Automated Testing solutions for LTE, VoLTE, and IMS networks

The representation of LTE-IMS network indicates the support of most of the interfaces by GL's test tools.

- End-to-end voice, video, and data quality testing (vMobile™ and VQuad™) with speech metrics such as PESQ, and POLQA
- This solution combined with other metrics such as delay, packet loss, drops, and more, the true performance of VoLTE can be realized
- All elements within LTE-IMS wireless infrastructure can be tested with GL's protocol simulation - MAPS™ framework, which supports simulation of various interfaces of LTE (S1-u, S1-MME, X2, S3, S4, S5/S8, S6a, S10, S11, S13, S16) and IMS (Cx/Dx, Rx, Gx, Gm, SGi, Mw, Mi, Mj) interfaces using MAPS™ LTE S1, LTE eGTP, Diameter, and IMS simulators
- With these, one can simulate VoLTE calls in lab, and study the network behaviour



# Main Features

Following are some of the main features of LTE Analyzer.

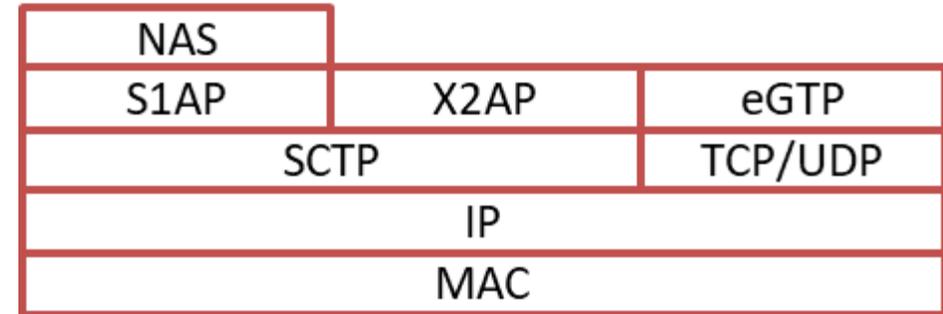
- Supported Interfaces - S1, S3, S4, S5 (or S8), S6a, S10, S11, S13 and X2 interfaces
- Supports capturing, decoding and performing various test measurements
- Displays summary, detail, hex-dump, summary and statistics views
- Detail View displays decodes of a user-selected frame from the Summary View
- Statistics View displays statistics based on frame count, byte count, frames/sec, bytes/sec etc. for the entire captured data
- Hex dump View displays raw data as a hexadecimal and ASCII octet dump
- Search and filtering capabilities

# Main Features (Contd.)

- Exports Summary View information to a comma delimited file for subsequent import into a database or spreadsheet
- Capability to export detailed decode information to an ASCII file
- Remote monitoring capability using GL's Network Surveillance System
- Additional features supported by Offline LTE Analyzer
  - Trace files for analysis can be loaded through simple command-line arguments
  - Multiple trace files can be loaded simultaneously with different GUI instances for offline analysis

# Protocol Stack

- Decode and analyze full LTE protocol stack
- Test eNodeB or UE over S1, S3, S4, S5 (or S8), S6a, S10, S11, S13 and X2 interfaces of the LTE network
- The protocols supported for decoding across all these interfaces are NAS, S1AP, X2AP, eGTP, GTP-U, Diameter, SCTP, UDP, TCP, and IP



Supported Protocols	Standard / Specification Used
SCTP	RFC 2960
S1AP	3GPP TS 36.413 V9.0.0
X2AP	3GPP TS 36.423 V9.0.0
eGTP	3GPP TS 29.274 V8.0.0
NAS	3GPP TS 24.301 V9.0.0

# Supported Interfaces and Protocols

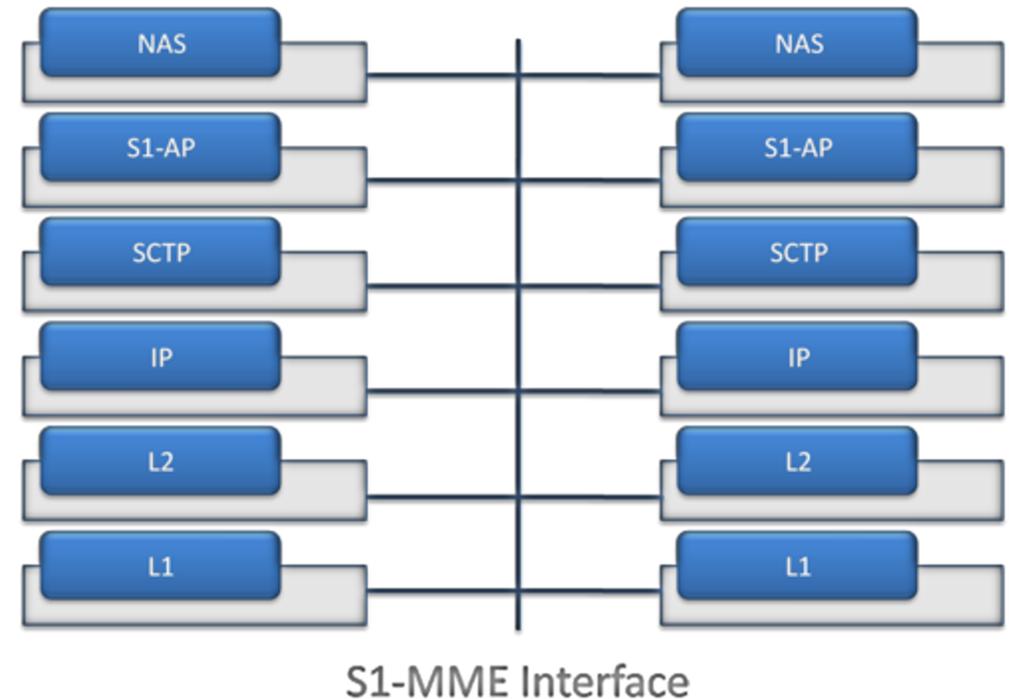
- GL's LTE analyzer can capture and decoding various interfaces i.e., S1, S3, S4, S5 (or S8), S6a, S10, S11, S13 and X2 interfaces of the LTE network. The protocols supported for decoding across all these interfaces are NAS, S1AP, X2AP, eGTP, Diameter, SCTP, UDP, TCP, IP

- S1 Interface
- S3 Interface
- S4 Interface
- S5 Interface
- S8 Interface
- S10 Interface
- S11 Interface
- S6a Interface
- S13 Interface
- X2 Interface

# S1-MME Interface

## S1 Interface

- S1-U - Reference point between E-UTRAN and Serving GW for the per bearer user plane tunnelling and inter eNodeB path switching during handover.
- S1-MME - Reference point for the control plane protocol between E-UTRAN and Mobility Management Entity (MME). The MME is responsible for authentication and critical management for mobile devices



# S3, S4, S5 (or S10), and S11 Interfaces

- **S3 Interface**

- It enables user and bearer information exchange for inter 3GPP access network mobility in idle and/or active state

- **S4 Interface**

- It provides related control and mobility support between GPRS Core and the 3GPP Anchor function of Serving GW. In addition, if Direct Tunnel is not established, it provides the user plane tunneling

- **S5 Interface**

- It provides user plane tunneling and tunnel management between Serving GW and PDN GW
- It is used for Serving GW relocation due to UE mobility and if the Serving GW needs to connect to a non-collocated PDN GW for the required PDN connectivity

- **S8 Interface**

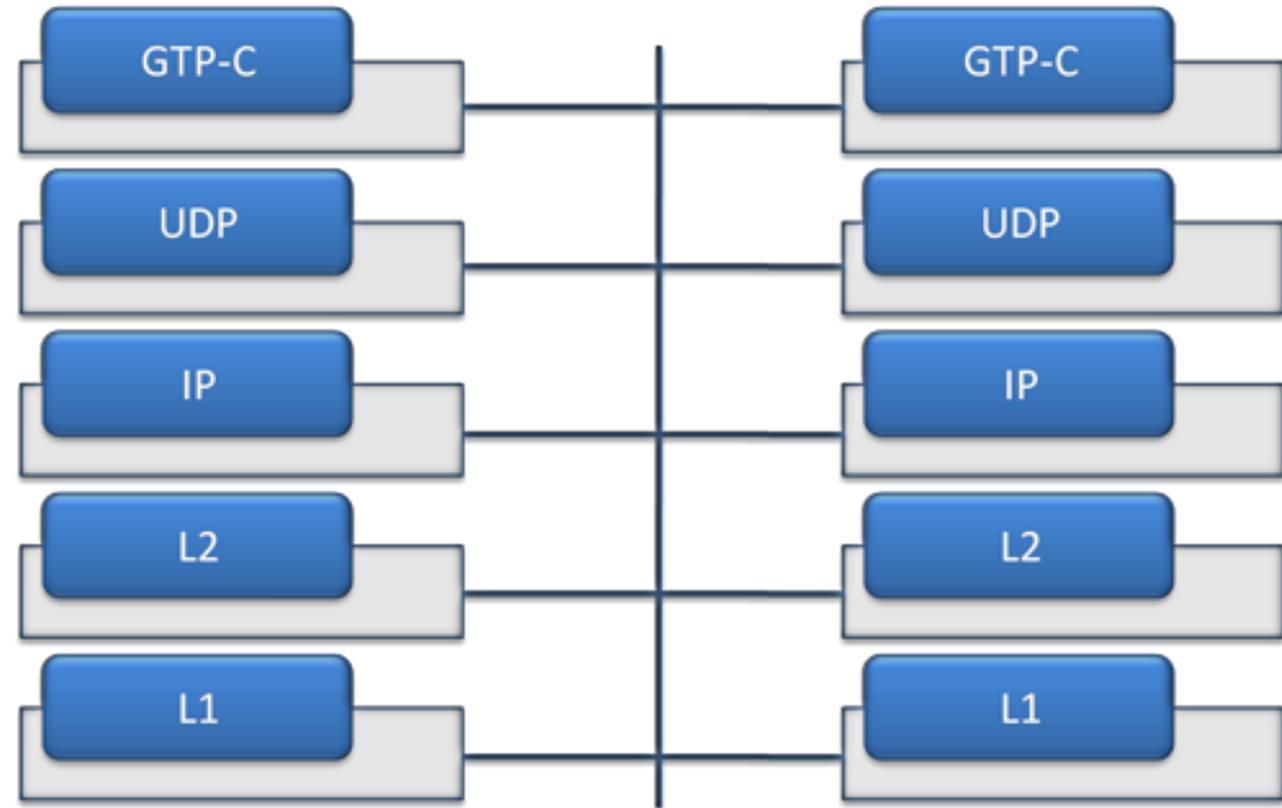
- Inter-PLMN reference point providing user and control plane between the Serving GW in the VPLMN and the PDN GW in the HPLMN. S8 is the inter PLMN variant of S5

- **S10 Interface**

- Reference point between MMEs for MME relocation and MME to MME information transfer

- **S11 Interface**

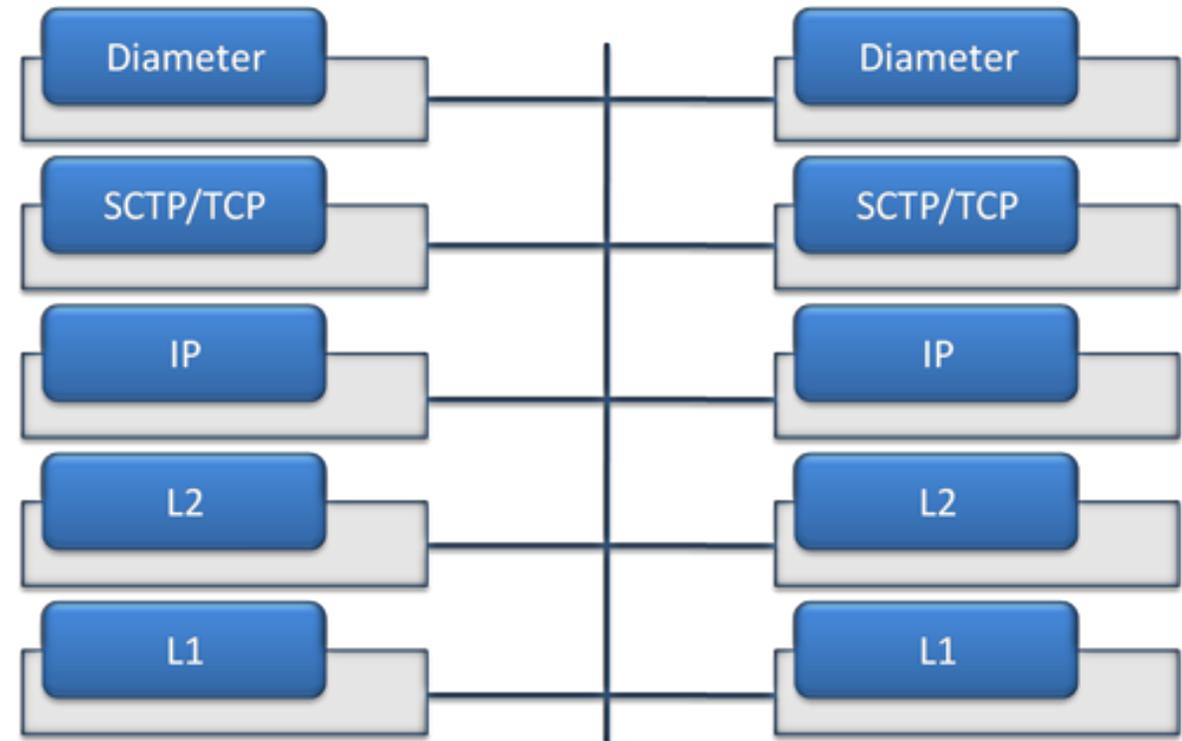
- Reference point between MME and Serving GW



S3, S4, S5 (or S8), S10, AND S11 Interfaces

# S6a and S13 Interfaces

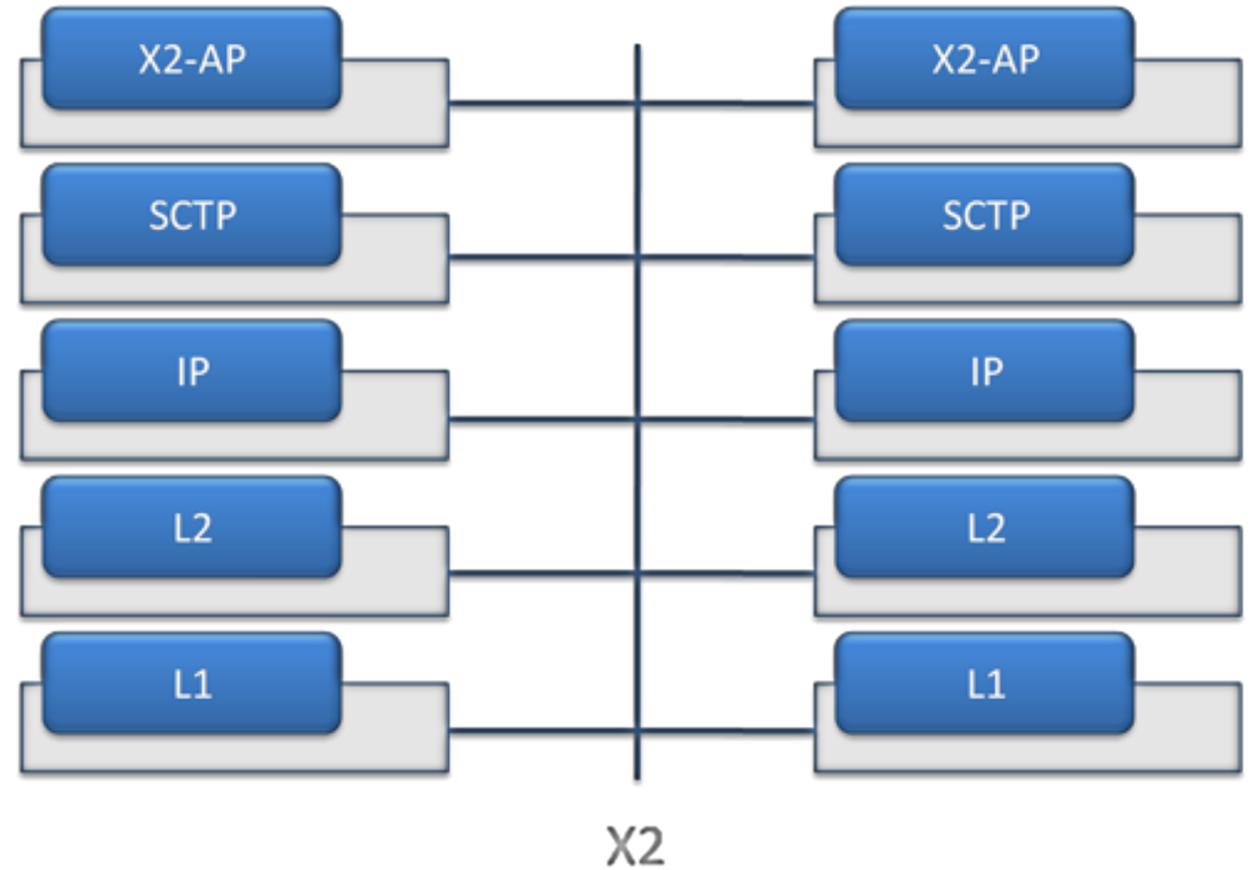
- S6a Interface
  - It enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between MME and HSS.
- S13 Interface
  - It enables UE identity check procedure between MME and EIR



S6a & S13 Interfaces

# X2 Interface

- X2 Interface
  - Interface between eNodeBs supports load management and handover coordination between eNodeBs.



# 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 LTE Protocol Analysis LTE software interface. The top pane shows a list of captured frames with columns for Dev, Frame#, TIME, Len, Error, Protocols, Source IP Address, Destination IP Address, and NAS Mes. The bottom pane shows the protocol details for the selected frame, including S1AP-PDU, Extensibility Marker, Choice Index, InitiatingMessage, ProcedureCode, Contents, Criticality, Value, Length, E-RABSetupRequest, Extensibility Marker, ProtocolIE-Container, Iteration Count, ProtocolIE-Container, ProtocolIE-Field, and ProtocolIE ID. The bottom status bar shows the capture rate (11.37 Mbps), file path (C:\Temp.Hdl), number of captured frames (353296), and missed frames (94675).

Dev	Frame#	TIME [...]	Len	Error	Protocols	Source IP Address	Destination IP Address	NAS Mes
✓ 2	6	00:00:...	158		Internet IP(IPv4)	10.28.6.44	10.28.6.43	Attach Ac
✓ 2	7	00:00:...	104		Internet IP(IPv4)	10.28.6.43	10.28.6.44	
✓ 2	8	00:00:...	116		Internet IP(IPv4)	10.28.6.43	10.28.6.44	Attach Cc
✓ 2	9	00:00:...	146		Internet IP(IPv4)	10.28.6.43	10.28.6.44	Attach Re
✓ 2	10	00:00:...	126		Internet IP(IPv4)	10.28.6.44	10.28.6.43	Authentic
✓ 2	11	00:00:...	130		Internet IP(IPv4)	10.28.6.43	10.28.6.44	Authentic
✓ 2	12	00:00:...	99		Internet IP(IPv4)	10.28.6.44	10.28.6.43	Security M

```
===== S1AP Layer =====
S1AP-PDU                               = CHOICE
Extensibility Marker                    = 0
Choice Index                            = 0
InitiatingMessage                       = SEQUENCE
ProcedureCode                           = INTEGER
Contents                                 = 5 id-E-RABSetup
Criticality                              = ENUMERATOR
Contents                                 = 0 reject(0)
Value                                    = Open Type
Length                                   = 90
E-RABSetupRequest                       = SEQUENCE
Extensibility Marker                    = 0
ProtocolIE-Container                    = SEQUENCE OF
Iteration Count                          = 3
ProtocolIE-Container                    = Instance 0
ProtocolIE-Field                        = SEQUENCE
ProtocolIE ID                            = INTEGER
```

Hex Dump of the Frame Data

```
+-----+-----+-----+-----+-----+-----+-----+-----+
08 00 03 4A 00 35 00 A0 80 00 5E 46 08 00 45 00      J 5 | ^F E
00 90 14 1C 00 00 3B 84 4A 54 0A 1C 06 2C 0A 1C      | ;JT ,
```

Capture Rate : 11.37 Mbps | C:\Temp.Hdl | Captured 353296 frames | Missed Frames : 94675

# Real-time Capture Filter

Filter Selection

- LTE
  - Data Link
    - Frame Length(s)
    - Error Frames Only
    - OK Frames Only
    - Frame Number(s)
    - Device Number
  - MAC
  - IP
  - UDP
  - eGTP
  - SCTP
  - S1AP

Devices: space delimited

1

Activate Deactivate

All Selected

Layer	Field	Filter Value
Data Link	Device Number	1

LTE Protocol Analysis LTE

File View Capture Statistics Database Configure Help

0 GoTo

Dev	Frame#	TIME (Relative)	Len	Error	Protocols	Source IP Addr...	Destination IP Ad...	UDP So...	UDP Dest...	NAS Messages	eGTP Messages
✓ 1	0	00:00:00.000000	146		Internet IP(IPv4)	10.28.6.43	10.28.6.44			Attach Request	
✓ 1	1	00:00:00.997790	130		Internet IP(IPv4)	10.28.6.43	10.28.6.44			Authentication Re...	
✓ 1	2	00:00:01.997908	123		Internet IP(IPv4)	10.28.6.43	10.28.6.44			Security Mode Co...	
✓ 1	3	00:00:02.497104	104		Internet IP(IPv4)	10.28.6.43	10.28.6.44				
✓ 1	4	00:00:02.997224	89		Internet IP(IPv4)	10.28.6.43	10.28.6.44				
✓ 1	5	00:00:06.930273	104		Internet IP(IPv4)	10.28.6.43	10.28.6.44				
✓ 1	6	00:00:07.070694	116		Internet IP(IPv4)	10.28.6.43	10.28.6.44			Attach Complete	

Filter is active. E:\Program Files\GL Communications Inc\Pe\Filtr 7 of 11 frames

# Decode View of LTE Protocol

The detail decode view of LTE call displays the following:

- MAC Layer
- IP Layer
- UDP Layer
- eGTP Layer
- S1AP Layer

```
000F Delay = ...0... Normal Delay
000F Throughput = ...0... Normal Throughput
000F Reliability = ...0... Normal Reliability
000F Reserved for Future Use = ...00 (0)
0010 Total Length = 67 (x0043)
0012 Identification = 35445 (x8A75)
0014 Reserved = 0... (0)
0014 DF = 0... May Fragment
0014 MF = 0... Last Fragment
0014 Fragment Offset = 0 (...000000 00000000)
0016 Time To Live = 128 (x80)
0017 Protocol = 00010001 User Datagram
0018 Header Check Sum = x2BEB
001A Source IP Address = 192.168.1.84 (xC0A80154)
001E Destination IP Address = 192.168.1.165 (xC0A801A5)
===== UDP Layer =====
0022 Source Port = 2124 (x084C)
0024 Destination Port = 2123 (x084B)
0026 Length (Header + Data) = 47 (x002F)
0028 Checksum = 9289 (x2449)
===== eGTP R8 Layer =====
002A TEID = ...1... TEID Present
002A Piggybacking (P) = ...0... No piggybacked message
002A Version = 010... GTP-C
002B Message Type = 01000000 Modify Bearer Command
002C Length = 35 (x0023)
002E Tunnel Endpoint Identifier = 1 (x00000001)
0032 Sequence Number = 0 (x0000)
APN-Aggregate Maximum Bit Rate (APN-AMBR) =
0036 Information Element Id = 01001000 Aggregate Maximum Bit Rate (AMBR)
0037 Length = 8 (x0008)
0039 Instance = ...0000 (0)
0039 Comprehension Required (CR) = 000... (0)
Aggregate Maximum Bit Rate-Down Link = 0 (x00)
Aggregate Maximum Bit Rate-Up Link = 0 (x00)
Aggregate Maximum Bit Rate-Down Link (Extended) = 0 (x00)
Aggregate Maximum Bit Rate-Up Link (Extended) = 0 (x00)
Aggregate Maximum Bit Rate-Down Link (Extended-2) = 0 (x00)
Aggregate Maximum Bit Rate-Up Link (Extended-2) = 0 (x00)
AMBR-Specific Data = x0000
```

# Call Detail View

**PacketScan (All-in-One)**

File View Capture Statistics Database Call Detail Records Configure Help

0 GoTo

Dev	Frame#	TIME (Relative)	Len	Error	Protocols	Source IP Address	Destination IP Address	SCTP Chunk Type	SCTP Source Port	SCTP Destination Port
✓ 1	0	00:00:00.000000	82		Internet IP(IPv4)	192.168.1.84	192.168.1.165	INIT Chunk	36412	36412
✓ 1	1	00:00:02.137817	82		Internet IP(IPv4)	192.168.1.165	192.168.1.84	INIT Chunk	36412	36412
✓ 1	2	00:00:02.138900	198		Internet IP(IPv4)	192.168.1.84	192.168.1.165	INIT ACK Chunk	36412	36412
✓ 1	3	00:00:02.153674	178		Internet IP(IPv4)	192.168.1.165	192.168.1.84	COOKIE ECHO Chunk	36412	36412
✓ 1	4	00:00:02.153925	50		Internet IP(IPv4)	192.168.1.84	192.168.1.165	COOKIE ACK Chunk	36412	36412
✓ 1	5	00:00:11.130704	122		Internet IP(IPv4)	192.168.1.84	192.168.1.165	DATA Chunk	36412	36412
✓ 1	6	00:00:11.203394	102		Internet IP(IPv4)	192.168.1.165	192.168.1.84	DATA Chunk	36412	36412

Call ID	Call Status	Protocol	Call Originating (Nu...	Call Destination (Nu...	Call Start Date & Time	Call Duration	Protocol Specific
0	Completed	LTE	192.168.1.84	192.168.1.165	2012-04-23 15:35:52.581680	00:00:09.850198	<eNodeB S1AP Id> 1 <MME S1AP Id> 1 <Mobile Id> 9886915860 <S1 Release Cause> release-due-to
1	Completed	LTE	192.168.1.84	192.168.1.165	2012-04-23 15:36:06.657334	00:00:19.982239	<eNodeB S1AP Id> 2 <MME S1AP Id> 2 <Mobile Id> 9886915860 <S1 Release Cause> release-due-to
2	Completed	LTE	192.168.1.84	192.168.1.165	2012-04-23 15:36:32.347614	00:00:11.768413	<eNodeB S1AP Id> 3 <MME S1AP Id> 3 <Mobile Id> 9886915860 <S1 Release Cause> release-due-to

Off-line Viewing C:\Program Files (x86)\GL Communications Inc\Packr 107 Frames

# Statistics View

**PacketScan (All-in-One)**

File View Capture Statistics Database Call Detail Records Configure Help

0 GoTo

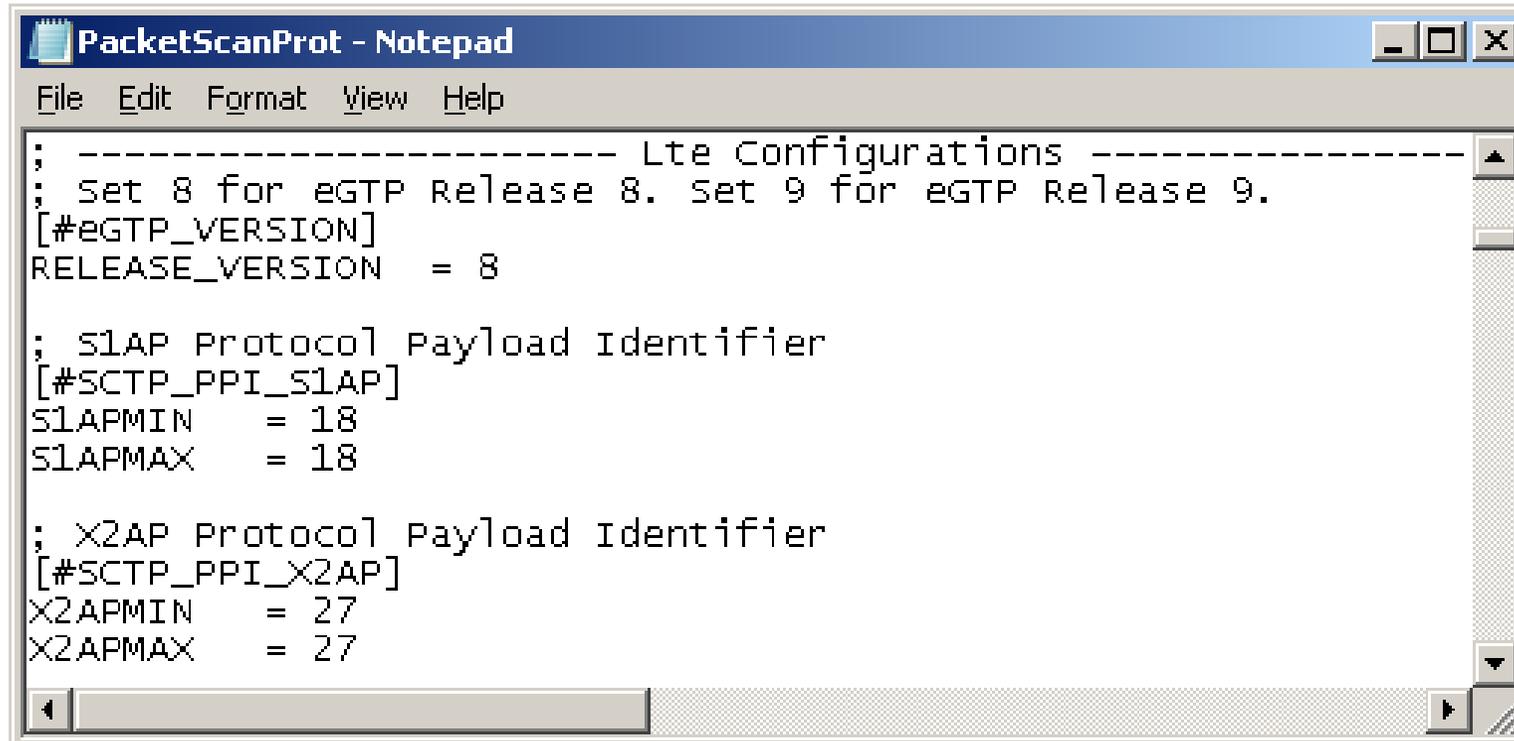
Dev	Frame#	TIME (Relative)	Len	Error	eGTP v8 Messages	Protocols	Source IP Address	Destination IP Address
✓ 1	0	00:00:00.000000	211		Create Session Request	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	1	00:00:00.148442	120		Create Session Response	Internet IP(IPv4)	192.168.1.165	192.168.1.84
✓ 1	2	00:00:01.686761	92		Update User Plane Request	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	3	00:00:01.695531	93		Update User Plane Response	Internet IP(IPv4)	192.168.1.165	192.168.1.84
✓ 1	4	00:00:04.349182	81		Bearer Resource Command	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	5	00:00:04.358175	116		Create Bearer Request	Internet IP(IPv4)	192.168.1.165	192.168.1.84
✓ 1	6	00:00:04.406025	106		Create Bearer Response	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	7	00:00:05.582507	81		Bearer Resource Command	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	8	00:00:05.589399	92		Update Bearer Request	Internet IP(IPv4)	192.168.1.165	192.168.1.84
✓ 1	9	00:00:05.649283	80		Update Bearer Response	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	10	00:00:08.428547	87		Bearer Resource Command	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	11	00:00:08.435473	64		Delete Bearer Request	Internet IP(IPv4)	192.168.1.165	192.168.1.84
✓ 1	12	00:00:08.483746	70		Delete Bearer Response	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	13	00:00:10.539146	65		Modify Bearer Request	Internet IP(IPv4)	192.168.1.84	192.168.1.165
✓ 1	14	00:00:10.547424	65		Modify Bearer Response	Internet IP(IPv4)	192.168.1.165	192.168.1.84

Message Type

- Create Session Request (32)
- Create Session Response (33)
- Update User Plane Request (34)
- Update User Plane Response (35)
- Modify Bearer Request (36)
- Modify Bearer Response (37)
- Bearer Resource Command (68)
- Create Bearer Request (95)
- Create Bearer Response (96)
- Update Bearer Request (97)
- Update Bearer Response (98)
- Delete Bearer Request (99)
- Delete Bearer Response (100)

C:\Program Files (x86)\GL Communic 15 Frames

# INI Decode Options



```
PacketScanProt - Notepad
File Edit Format View Help
; ----- Lte Configurations -----
; set 8 for eGTP Release 8. set 9 for eGTP Release 9.
[#eGTP_VERSION]
RELEASE_VERSION = 8

; S1AP Protocol Payload Identifier
[#SCTP_PPI_S1AP]
S1APMIN = 18
S1APMAX = 18

; X2AP Protocol Payload Identifier
[#SCTP_PPI_X2AP]
X2APMIN = 27
X2APMAX = 27
```

- Provides options to select eGTP Release 8 or eGTP Release 9
- Identifies the SCTP protocol payload identifier for S1AP, and X2AP

**Thank you**