Long Term Evolution (LTE) Protocol Analyzer

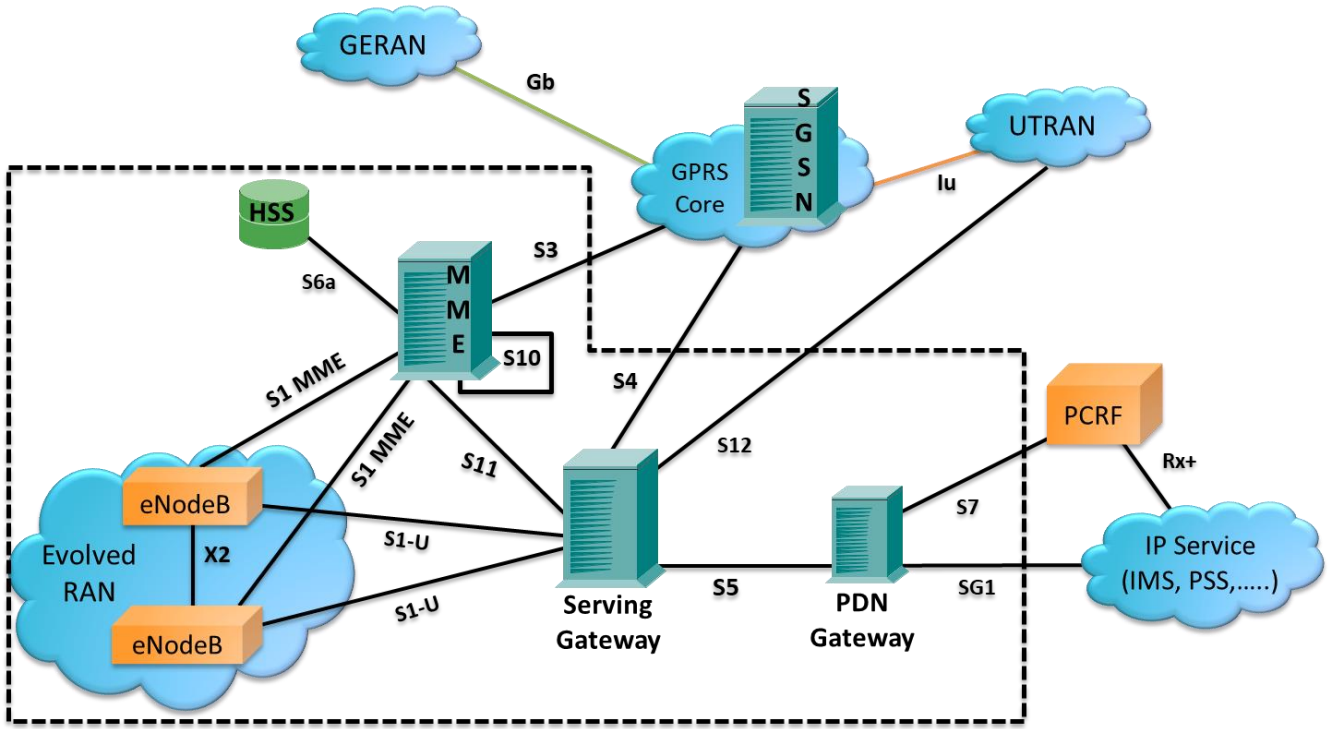
GL Communications Inc.
818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878
Phone: (301) 670-4784 Fax: (301) 670-9187 Email: info@gl.com
Website: https://www.gl.com

Introduction

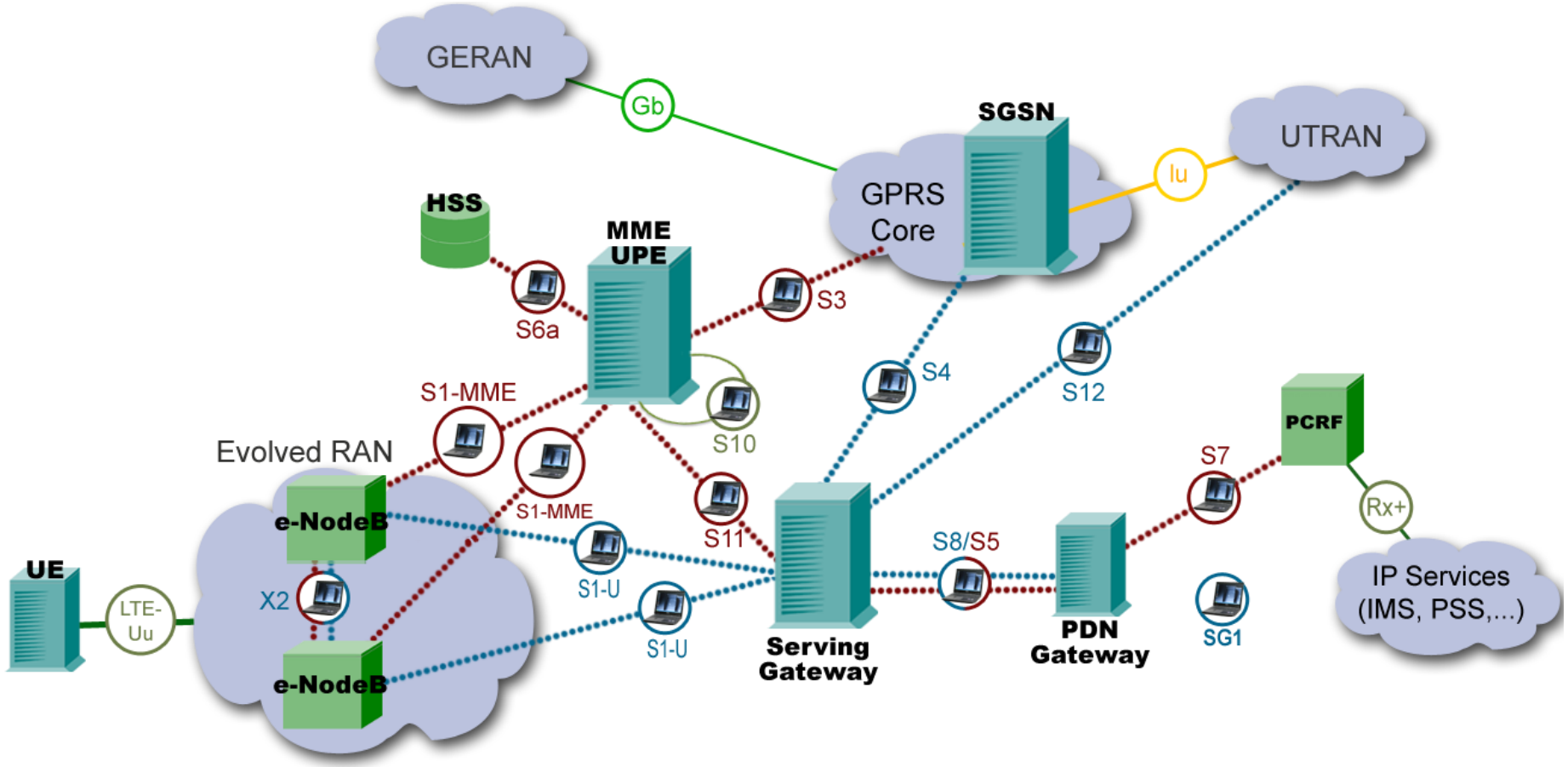
- The LTE (Long Term Evolution) protocol standard was developed as an enhancement to existing Universal Mobile Telecommunications System (UMTS) to provide users enhanced mobile Internet access
- The evolved Universal Mobile Telecommunications Service (UMTS) terrestrial Radio Access Network (RAN), abbreviated 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



SGSN - Serving GPRS Support Node
MME - Mobility Management Entity
PDN - Packet Data Network
PCRF - Policy and Charging Rules Function

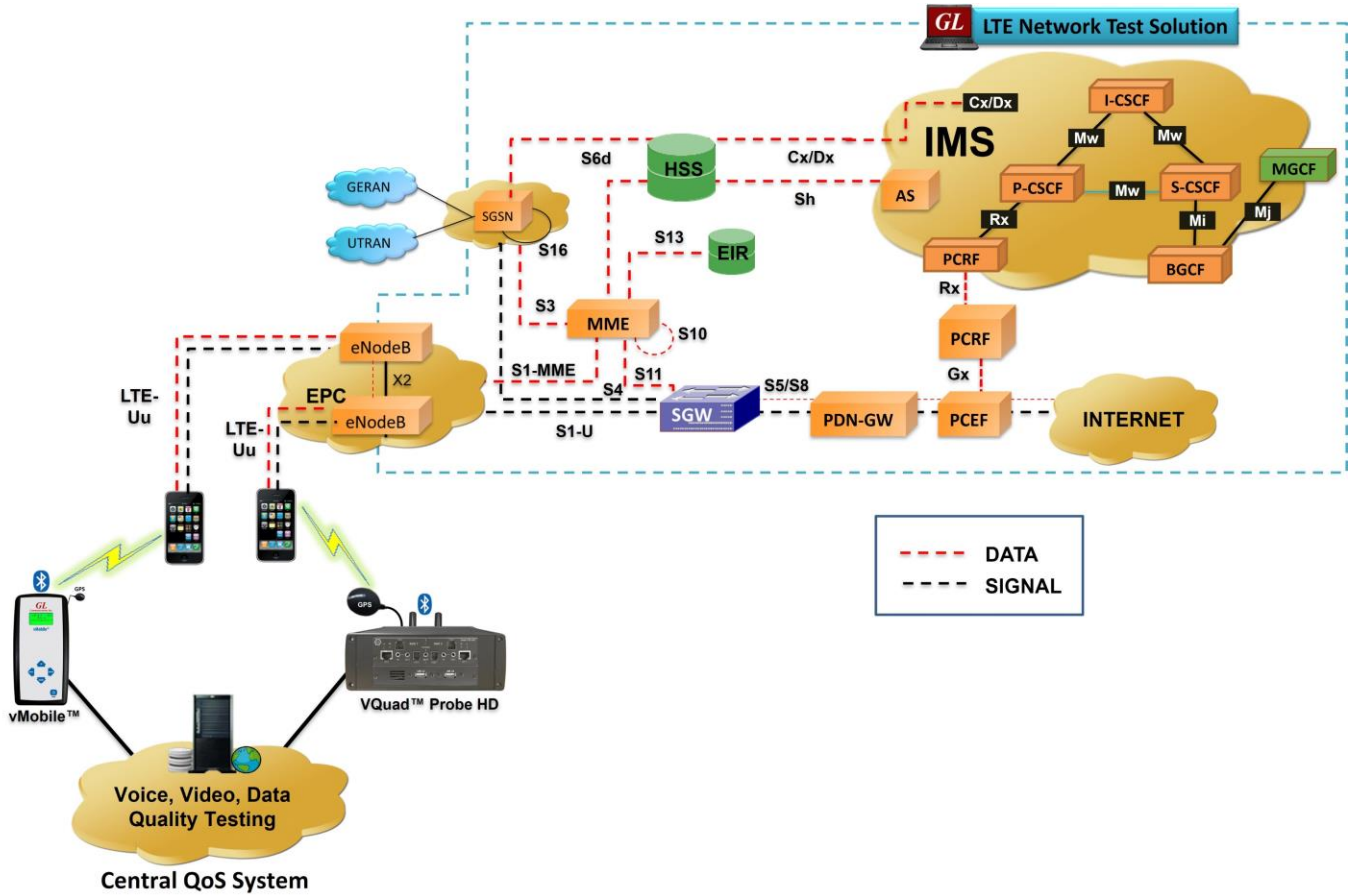
HSS - Home Subscriber Server
UTRAN - Universal Terrestrial Radio Access Network
E-UTRAN Evolved Universal Terrestrial Radio Access Network
GERAN - GSM EDGE Radio Access Network

GL Communications

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.

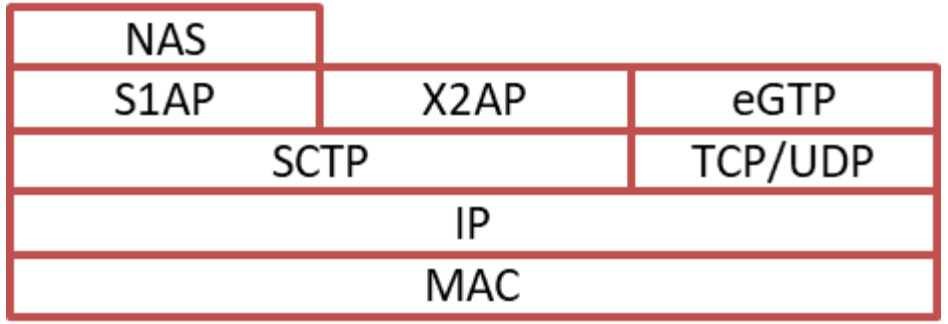
- Supported Interfaces - S1, S3, S4, S5 (or S8), S6a, S10, S11, S13 and X2 interfaces
- Supports capturing, decoding and performing various test measurements
- Displays summary, detail, hex-dump, summary and statistics views
- Detail View displays decodes of a user-selected frame from the Summary View
- 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

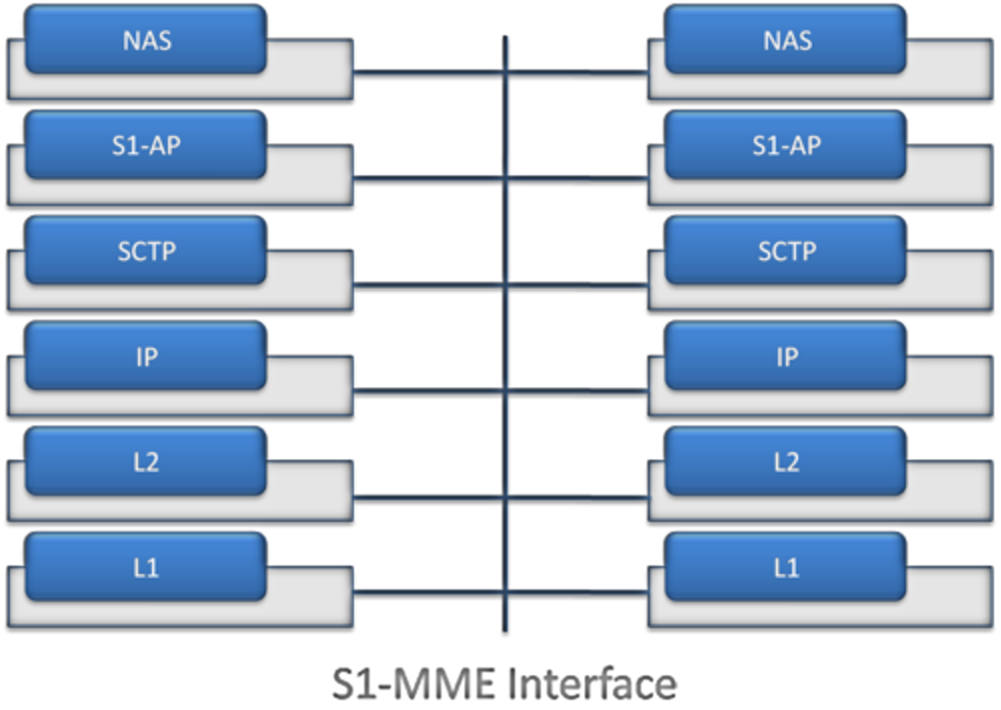
- S1 Interface
- S3 Interface
- S4 Interface
- S5 Interface
- S8 Interface
- S10 Interface
- S11 Interface
- S6a Interface
- S13 Interface
- X2 Interface

GL Communications

S1-MME Interface

S1 Interface

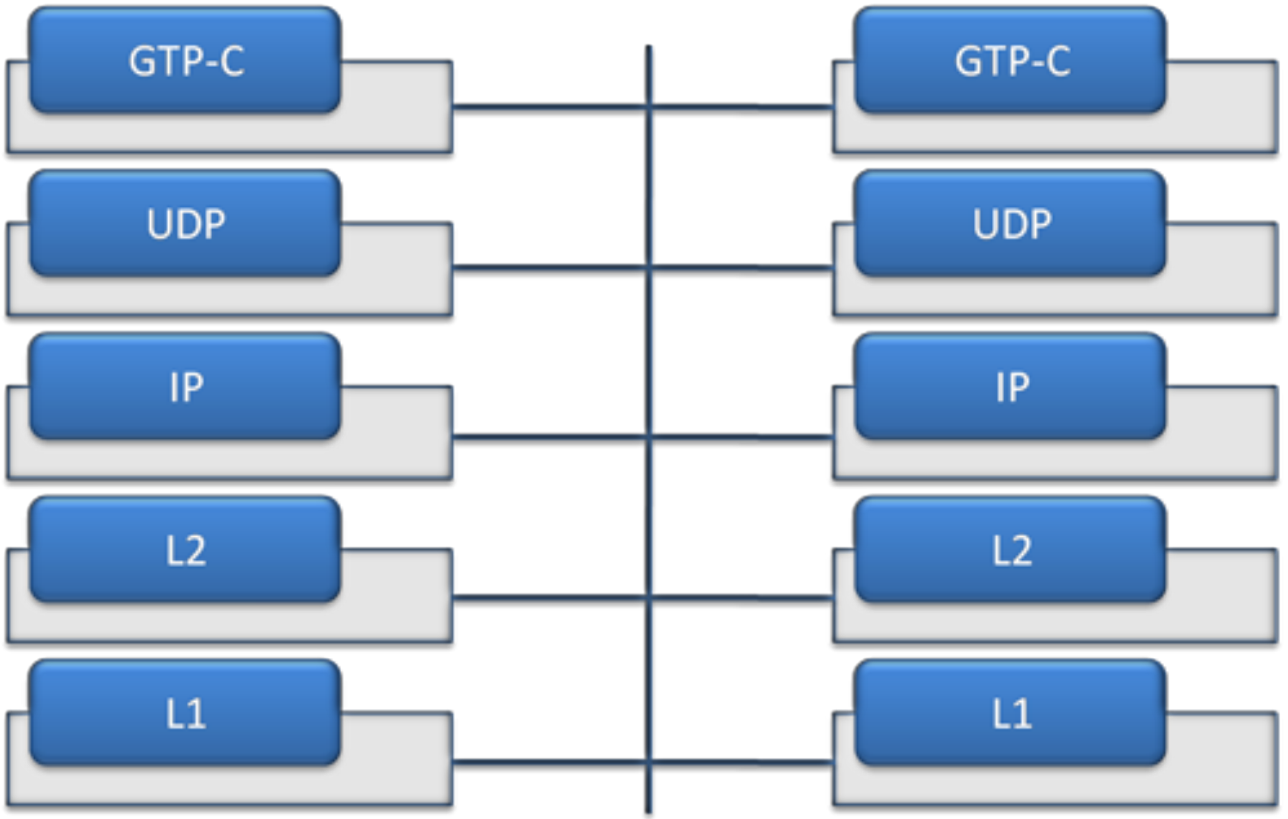
- S1-U - Reference point between E-UTRAN and Serving GW for the per bearer user plane tunnelling and inter eNodeB path switching during handover.
- S1-MME - Reference point for the control plane protocol between E-UTRAN and Mobility Management Entity (MME). The MME is responsible for authentication and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



S1-MME Interface

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

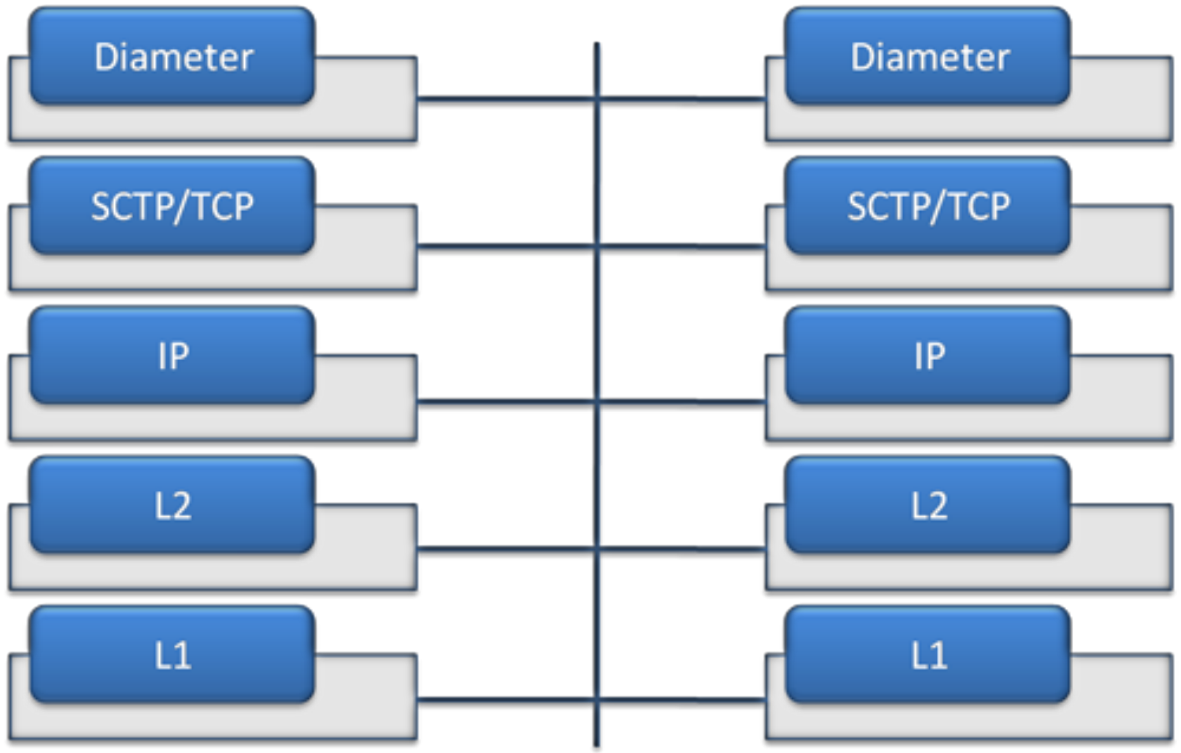
- **S3 Interface**
  - It enables user and bearer information exchange for inter 3GPP access network mobility in idle and/or active state
- **S4 Interface**
  - It provides related control and mobility support between GPRS Core and the 3GPP Anchor function of Serving GW. In addition, if Direct Tunnel 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

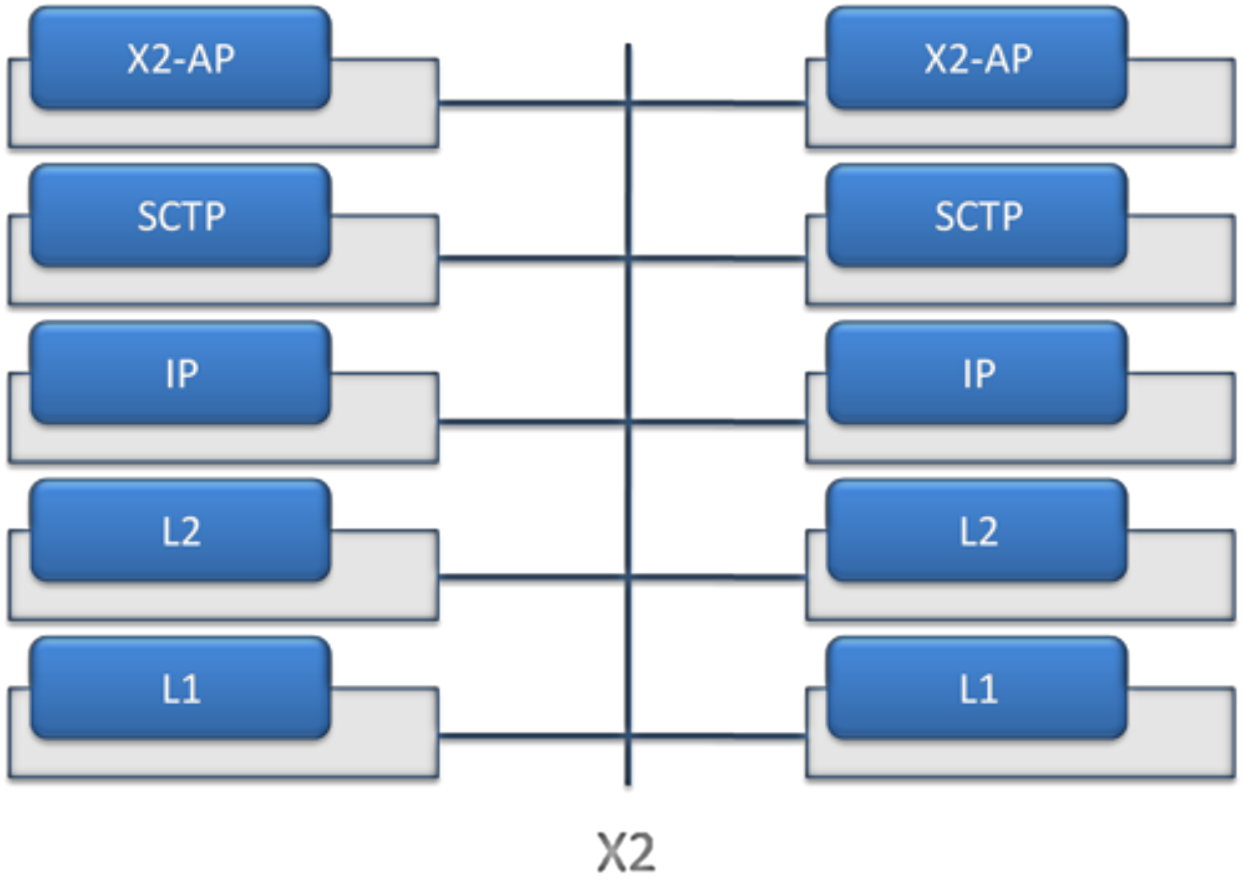
- S6a Interface
  - ➢ It enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between MME and HSS.
- S13 Interface
  - ➢ It enables UE identity check procedure between MME and EIR



S6a & S13 Interfaces

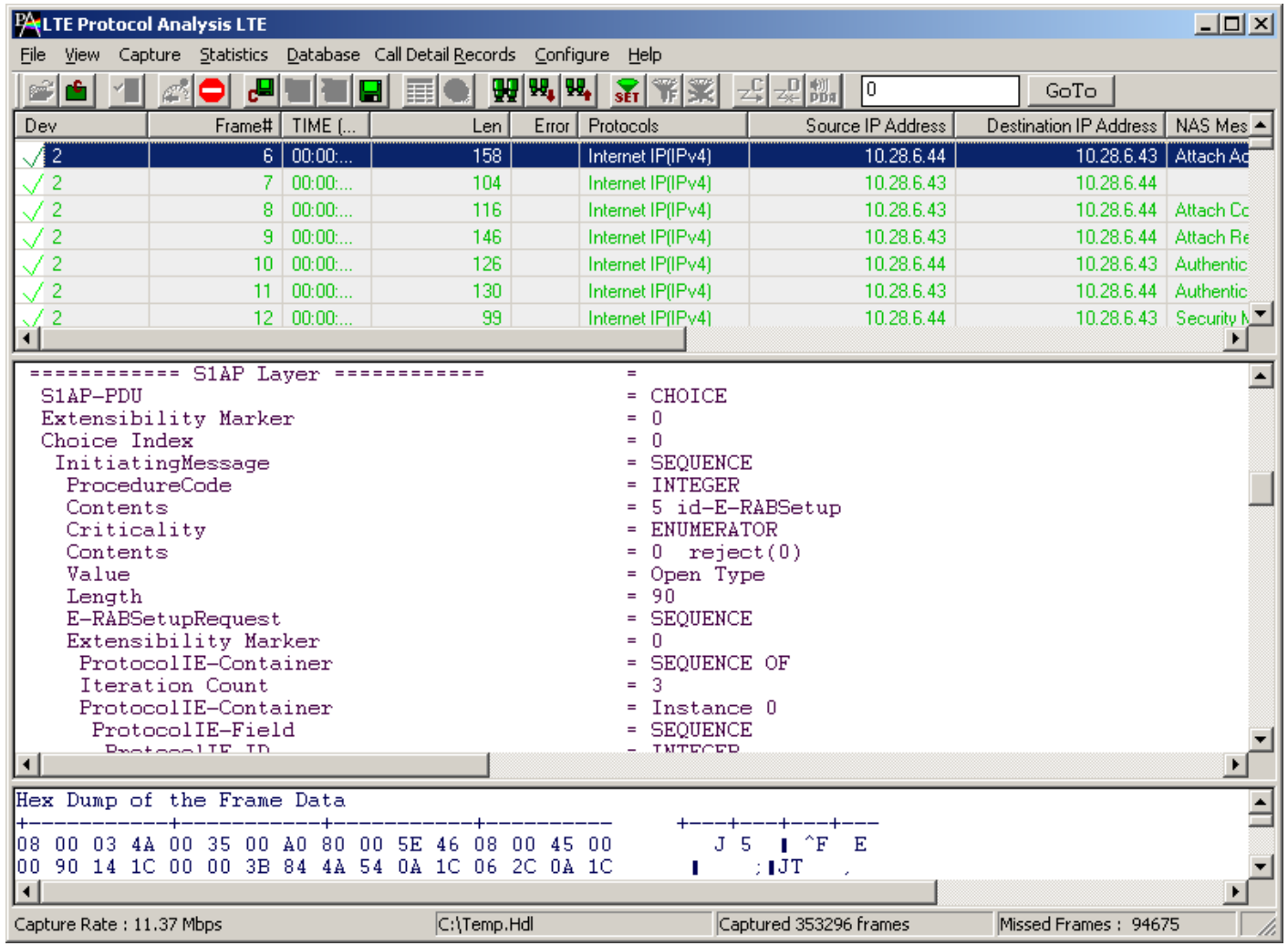
X2 Interface

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

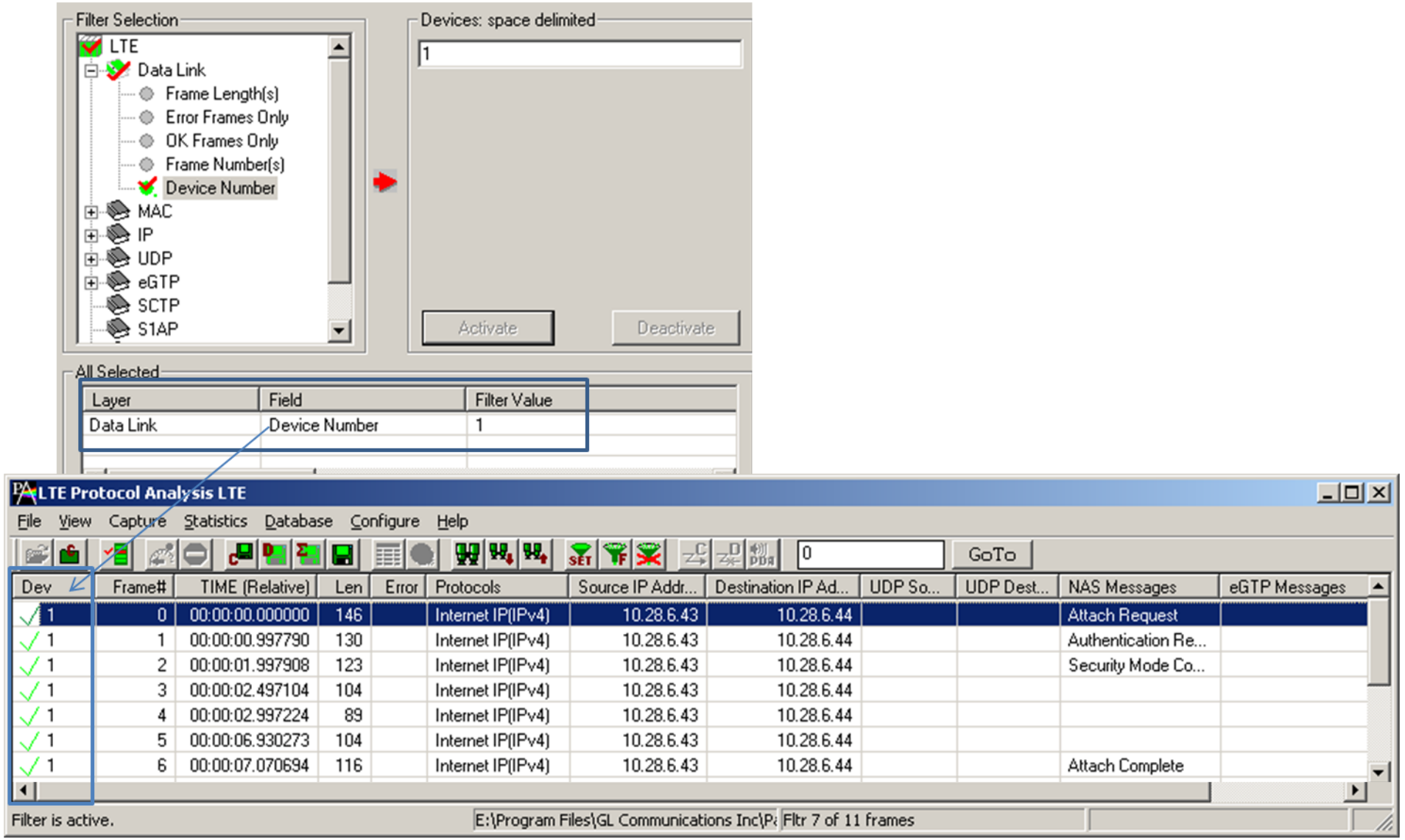


Real-time Analysis

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



Real-time Capture Filter



Decode View of LTE Protocol

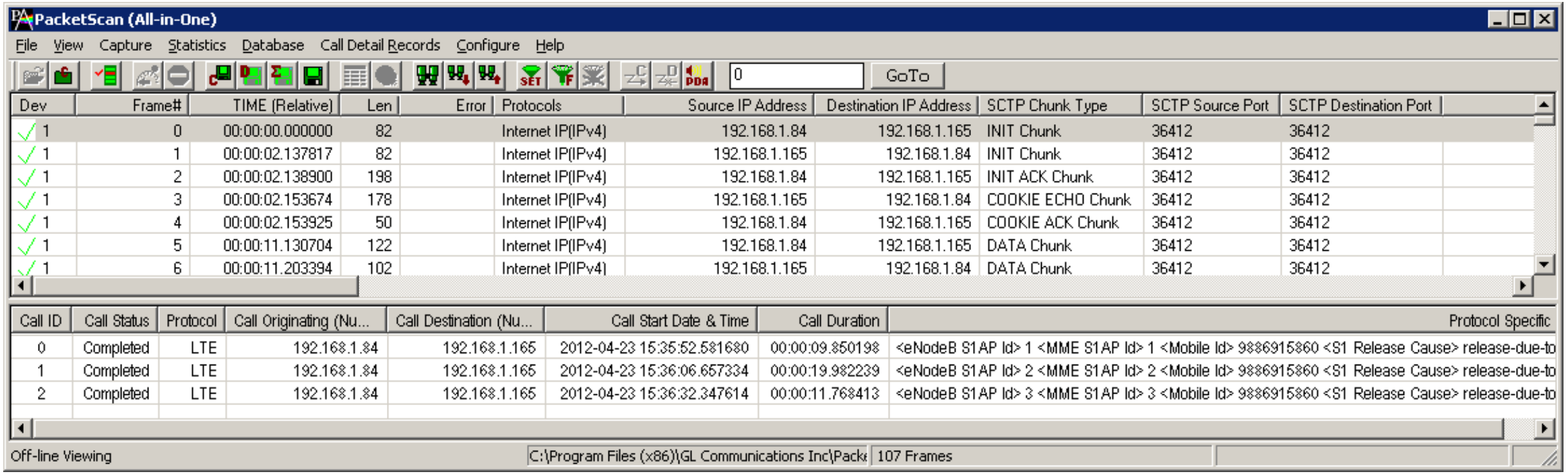
The detail decode view of LTE call displays the following:

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

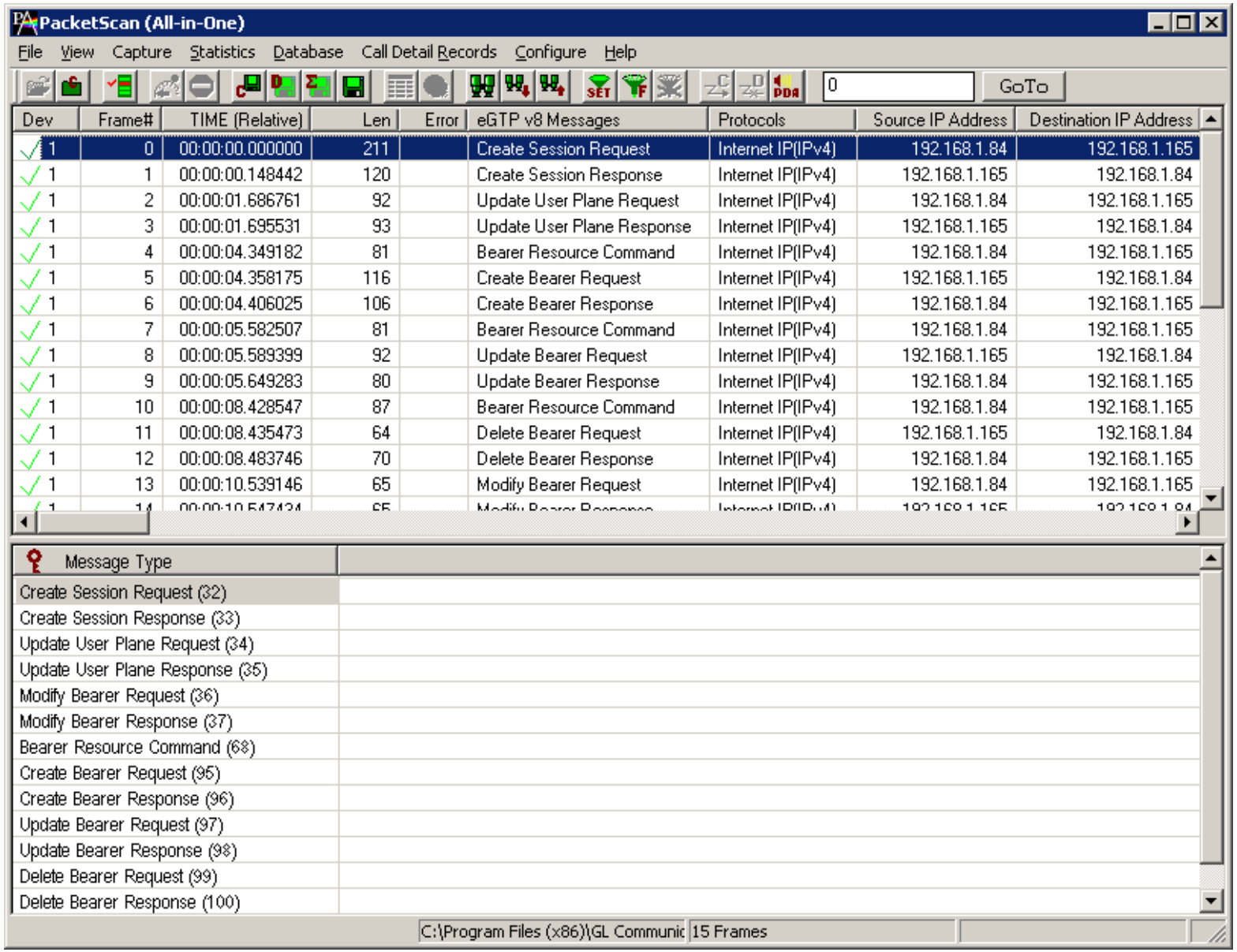
```
000F  Delay                                          = ...0.... Normal Delay
000F  Throughput                                     = ....0... Normal Throughput
000F  Reliability                                    = .....0.. Normal Reliability
000F  Reserved for Future Use                        = ......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 (...00000 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
```

GL Communications

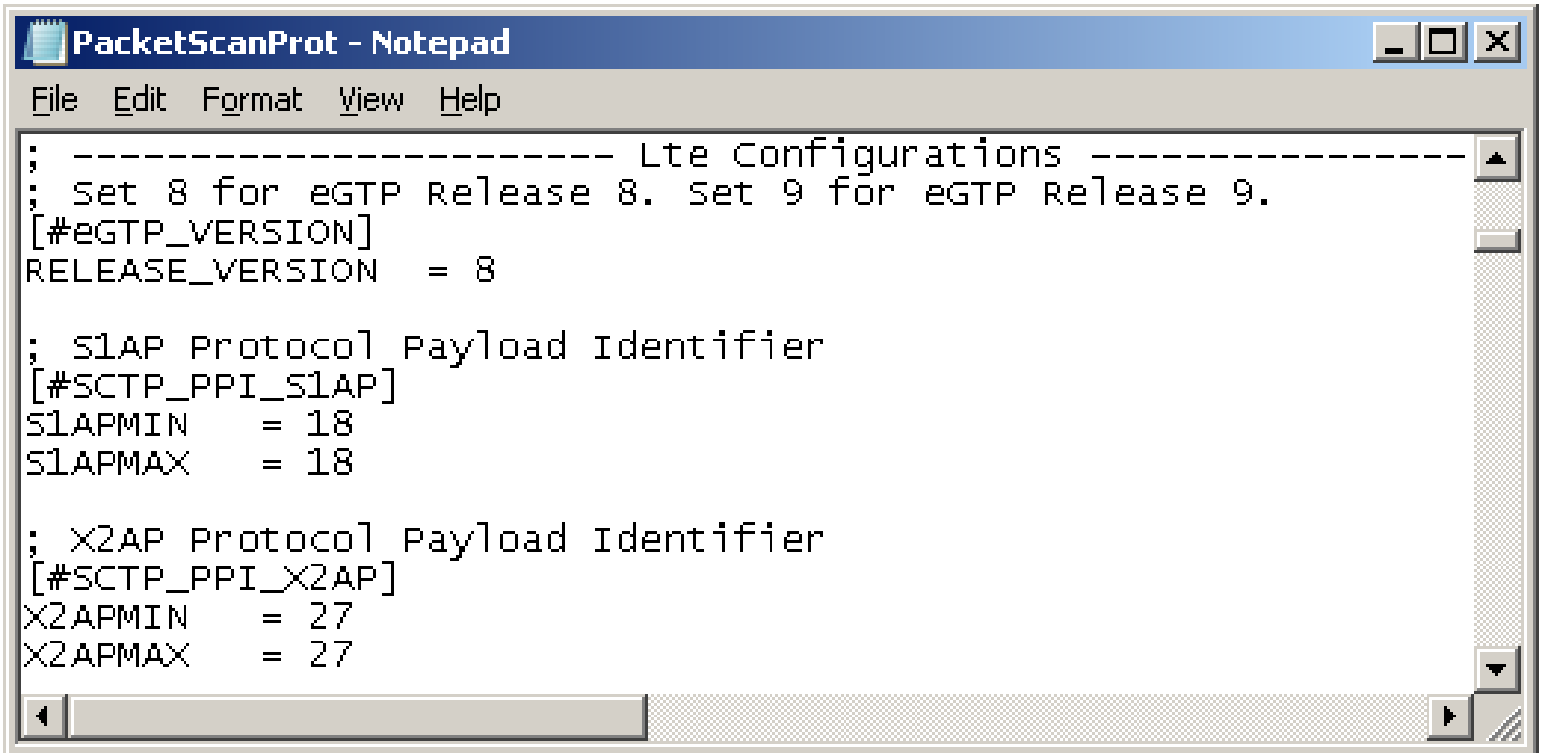
Call Detail View



Statistics View



INI Decode Options



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

Thank you