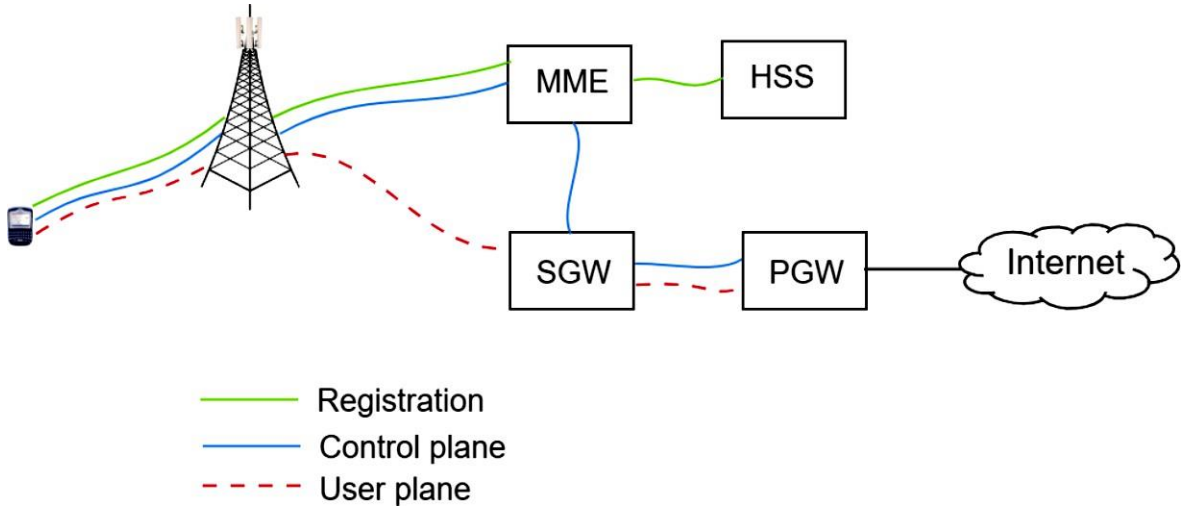
IN LAB

Files Requirement:

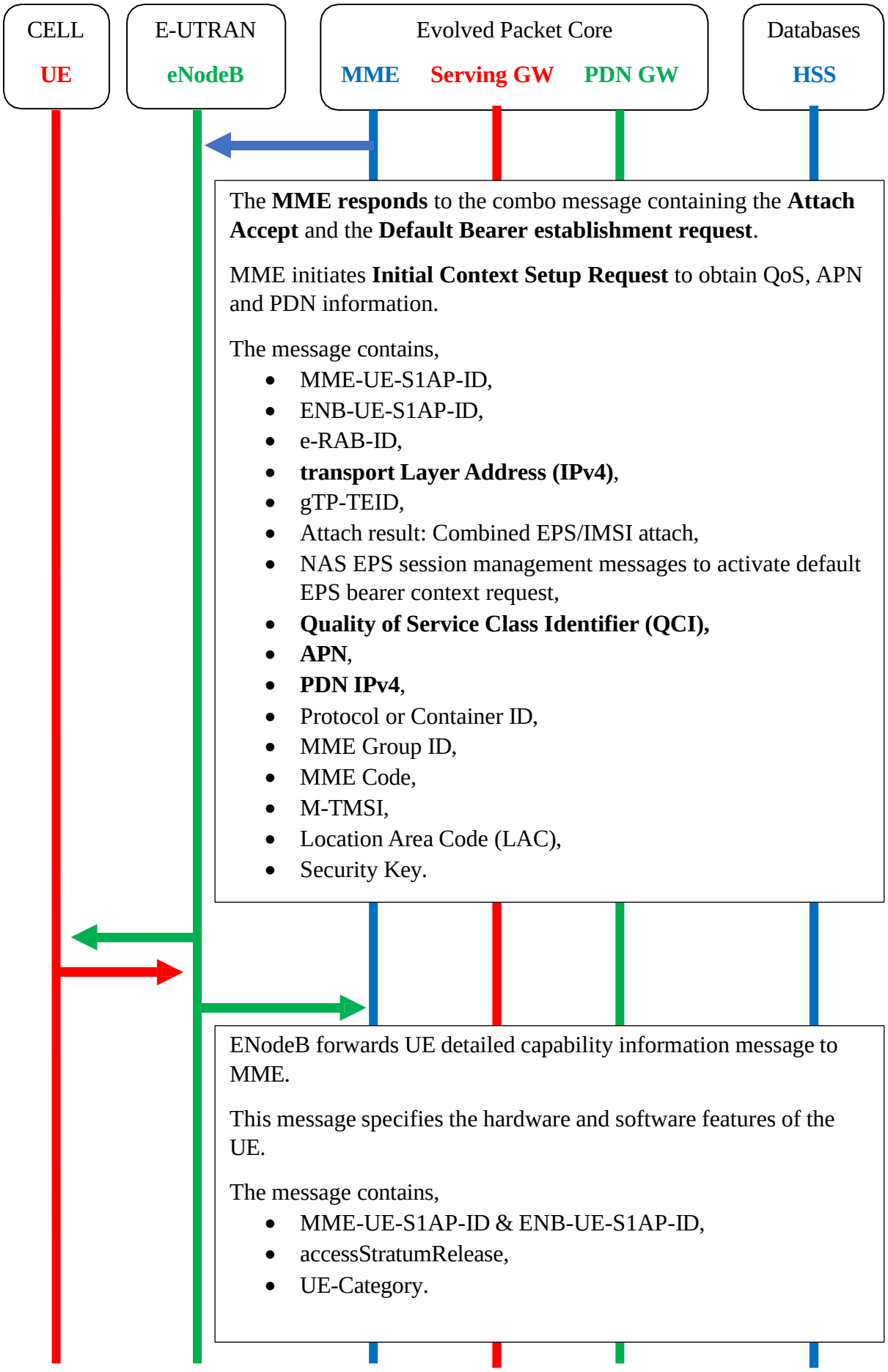
- During Experiment 1, **.pcap** files were generated for CN and eNB in Step 8 and Step 14.
- Experiment 2, Step 1 and 2 from will be informative.

Let's analyze the UE registration messages between eNodeB, MME and HSS to enable LTE session.



Control Plane

In this experiment we will explore the process and communication to establish data service and assign an IP address to the UE as well as QoS parameters.



The **MME responds** to the combo message containing the **Attach Accept** and the **Default Bearer establishment request**.

MME initiates **Initial Context Setup Request** to obtain QoS, APN and PDN information.

The message contains,

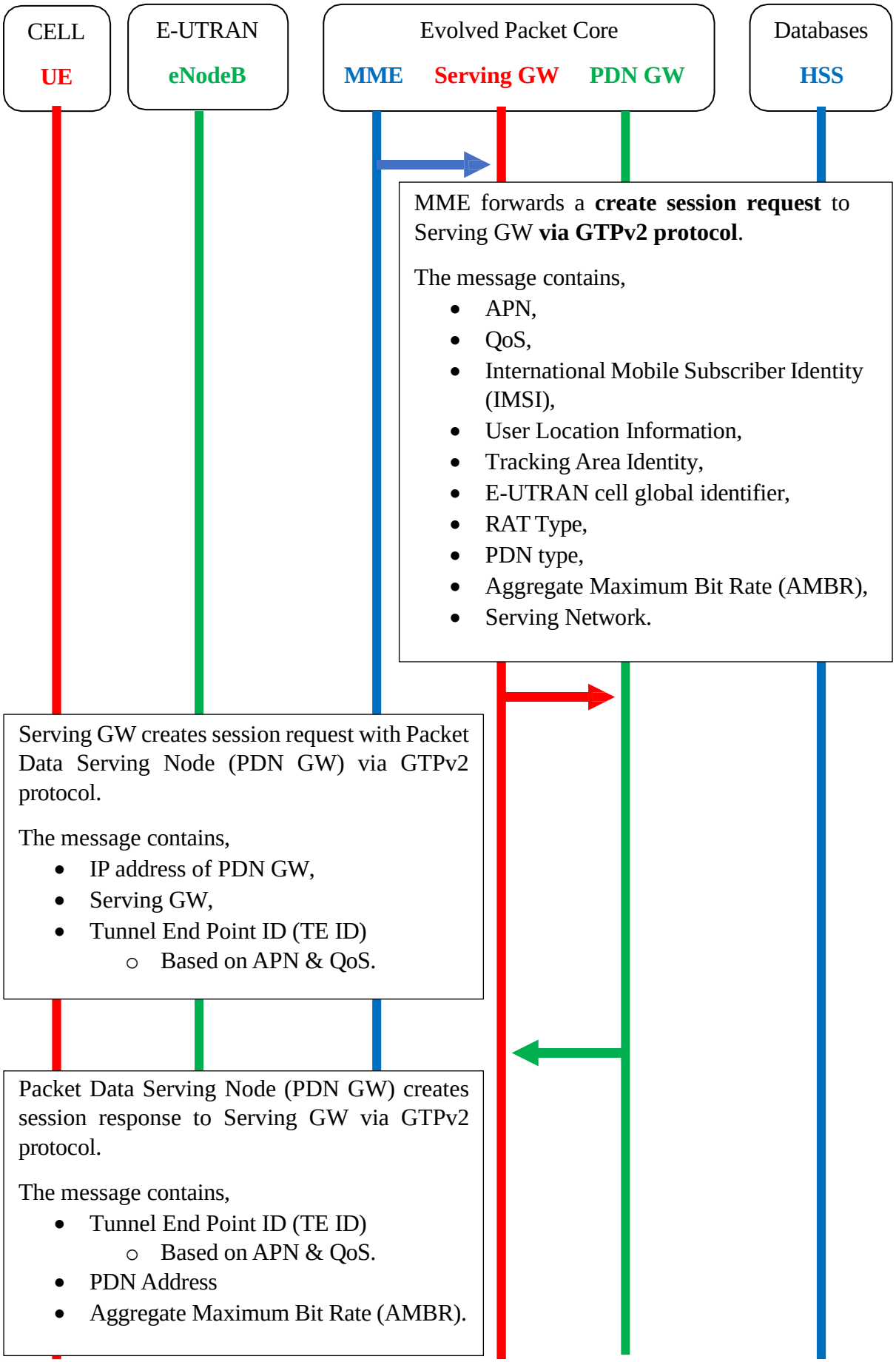
- MME-UE-S1AP-ID,
- ENB-UE-S1AP-ID,
- e-RAB-ID,
- **transport Layer Address (IPv4)**,
- gTP-TEID,
- Attach result: Combined EPS/IMSI attach,
- NAS EPS session management messages to activate default EPS bearer context request,
- **Quality of Service Class Identifier (QCI),**
- **APN**,
- **PDN IPv4**,
- Protocol or Container ID,
- MME Group ID,
- MME Code,
- M-TMSI,
- Location Area Code (LAC),
- Security Key.

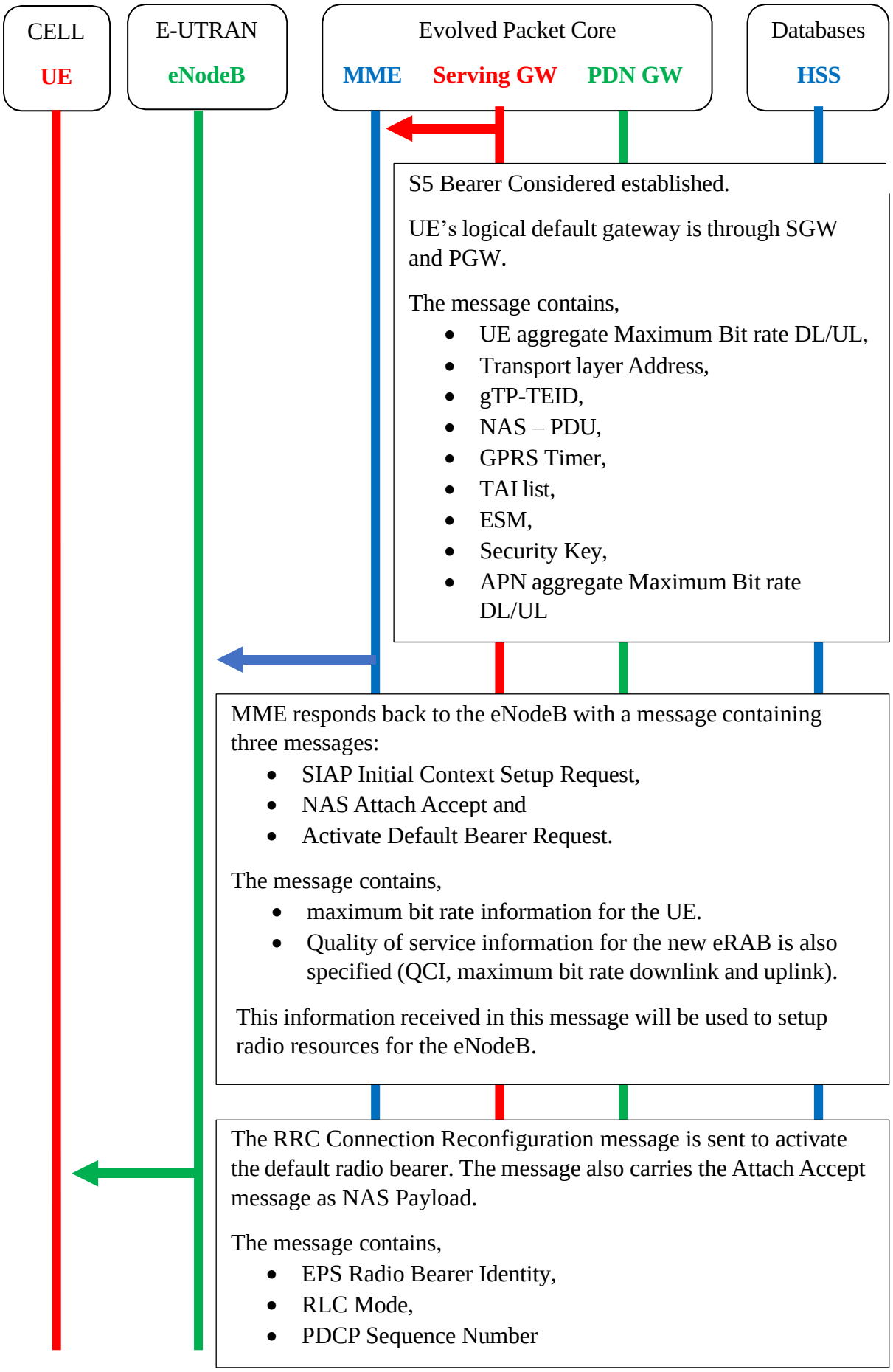
ENodeB forwards UE detailed capability information message to MME.

This message specifies the hardware and software features of the UE.

The message contains,

- MME-UE-S1AP-ID & ENB-UE-S1AP-ID,
- accessStratumRelease,
- UE-Category.

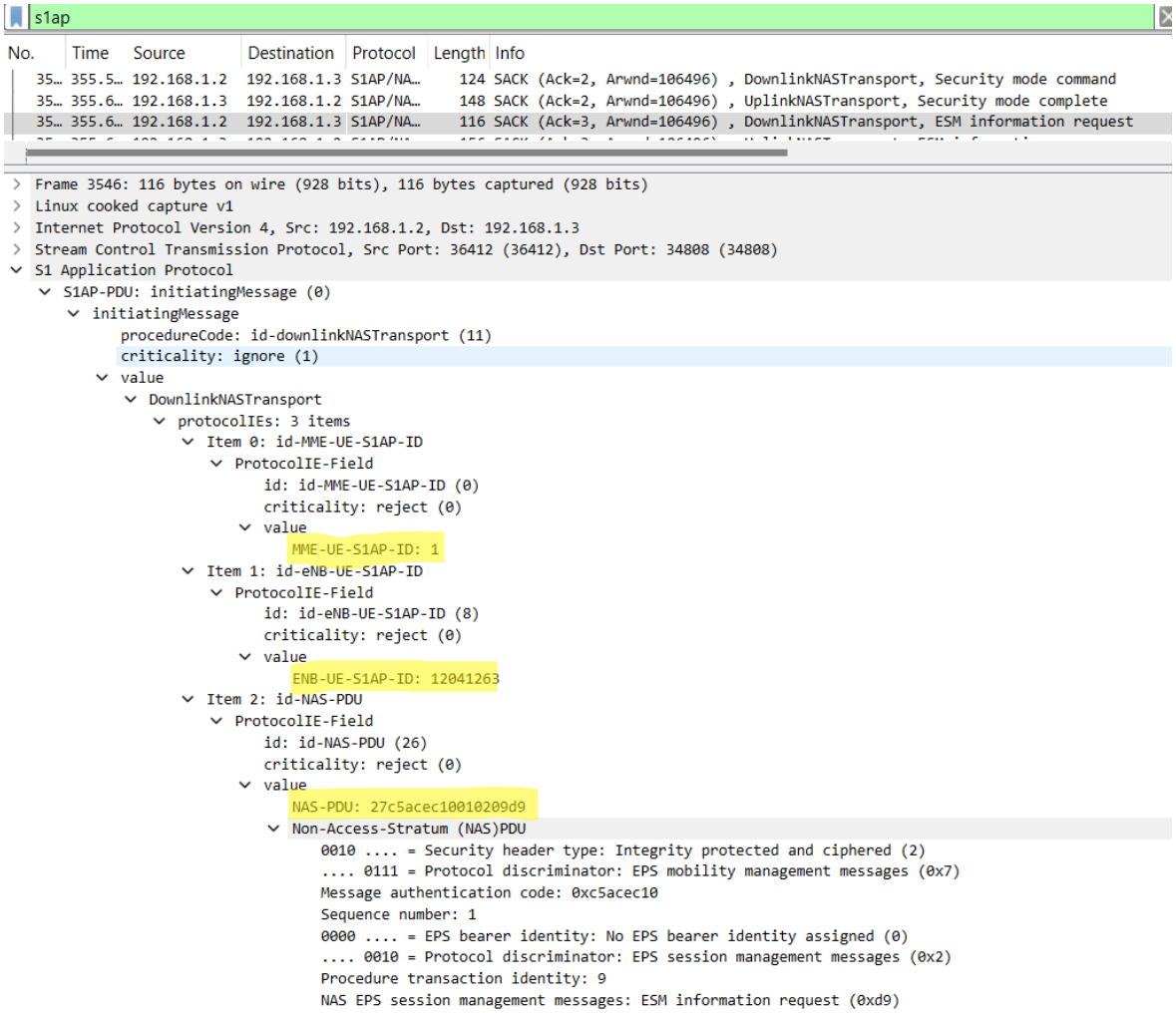

CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
MME forwards a create session request to Serving GW via GTPv2 protocol.
The message contains,
APN,
QoS,
International Mobile Subscriber Identity (IMSI),
User Location Information,
Tracking Area Identity,
E-UTRAN cell global identifier,
RAT Type,
PDN type,
Aggregate Maximum Bit Rate (AMBR),
Serving Network.
Serving GW creates session request with Packet Data Serving Node (PDN GW) via GTPv2 protocol.
The message contains,
IP address of PDN GW,
Serving GW,
Tunnel End Point ID (TE ID)
Based on APN & QoS.
Packet Data Serving Node (PDN GW) creates session response to Serving GW via GTPv2 protocol.
The message contains,
Tunnel End Point ID (TE ID)
Based on APN & QoS.
PDN Address
Aggregate Maximum Bit Rate (AMBR).


CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
S5 Bearer Considered established.
UE's logical default gateway is through SGW and PGW.
The message contains,
UE aggregate Maximum Bit rate DL/UL,
Transport layer Address,
gTP-TEID,
NAS – PDU,
GPRS Timer,
TAI list,
ESM,
Security Key,
APN aggregate Maximum Bit rate DL/UL
MME responds back to the eNodeB with a message containing three messages:
SIAP Initial Context Setup Request,
NAS Attach Accept and
Activate Default Bearer Request.
The message contains,
maximum bit rate information for the UE.
Quality of service information for the new eRAB is also specified (QCI, maximum bit rate downlink and uplink).
This information received in this message will be used to setup radio resources for the eNodeB.
The RRC Connection Reconfiguration message is sent to activate the default radio bearer. The message also carries the Attach Accept message as NAS Payload.
The message contains,
EPS Radio Bearer Identity,
RLC Mode,
PDCP Sequence Number

Open .cpcap file using Wireshark.

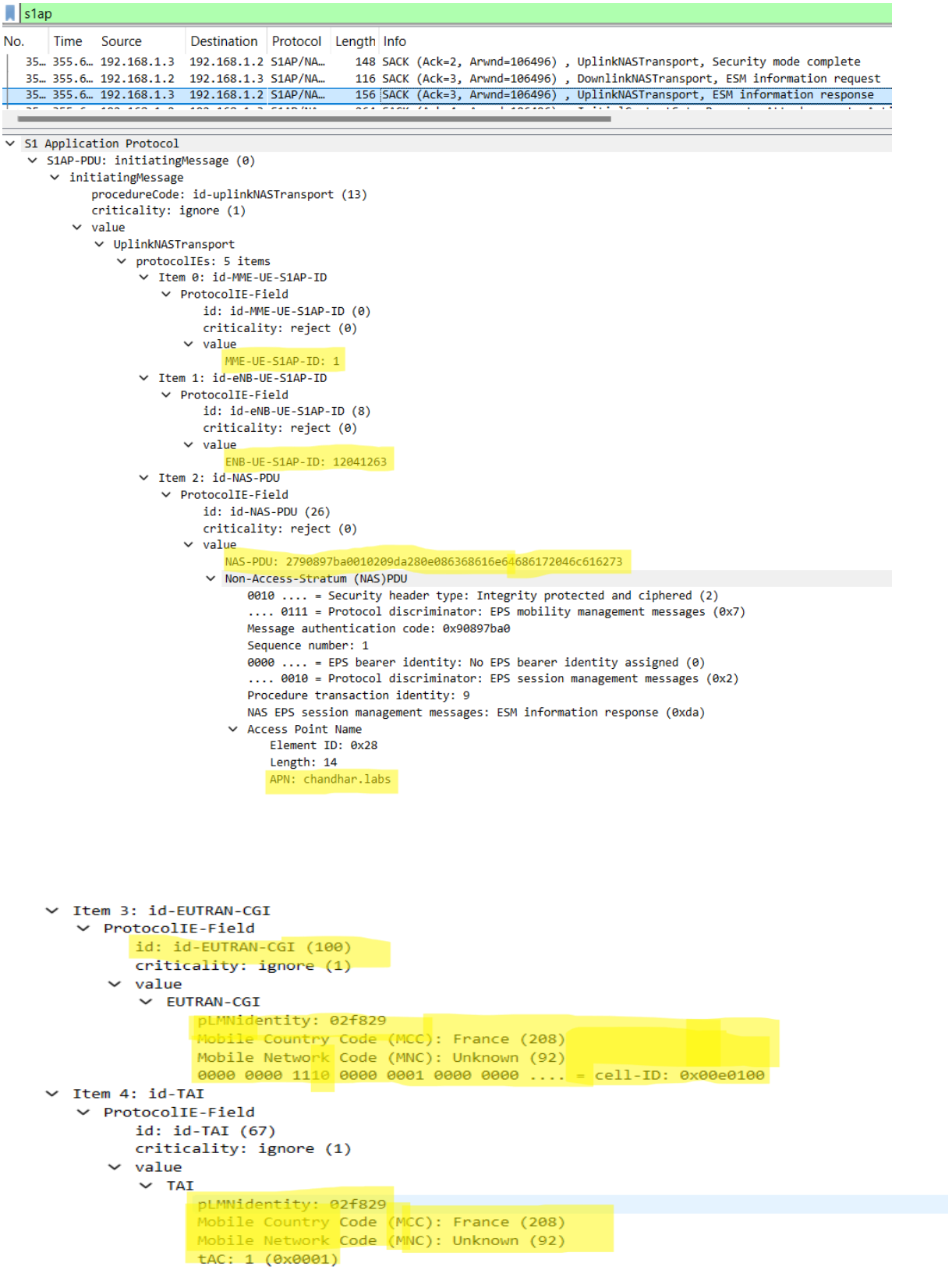
1. **In Wireshark after applying s1ap filter, Downlink NAS Transport to view ESM information request.**

NOTE: At Step 1, take a screenshot and attach it.
Highlight the initial message fields



2. **In Wireshark after applying s1ap filter, Uplink NAS Transport to view ESM information response.**

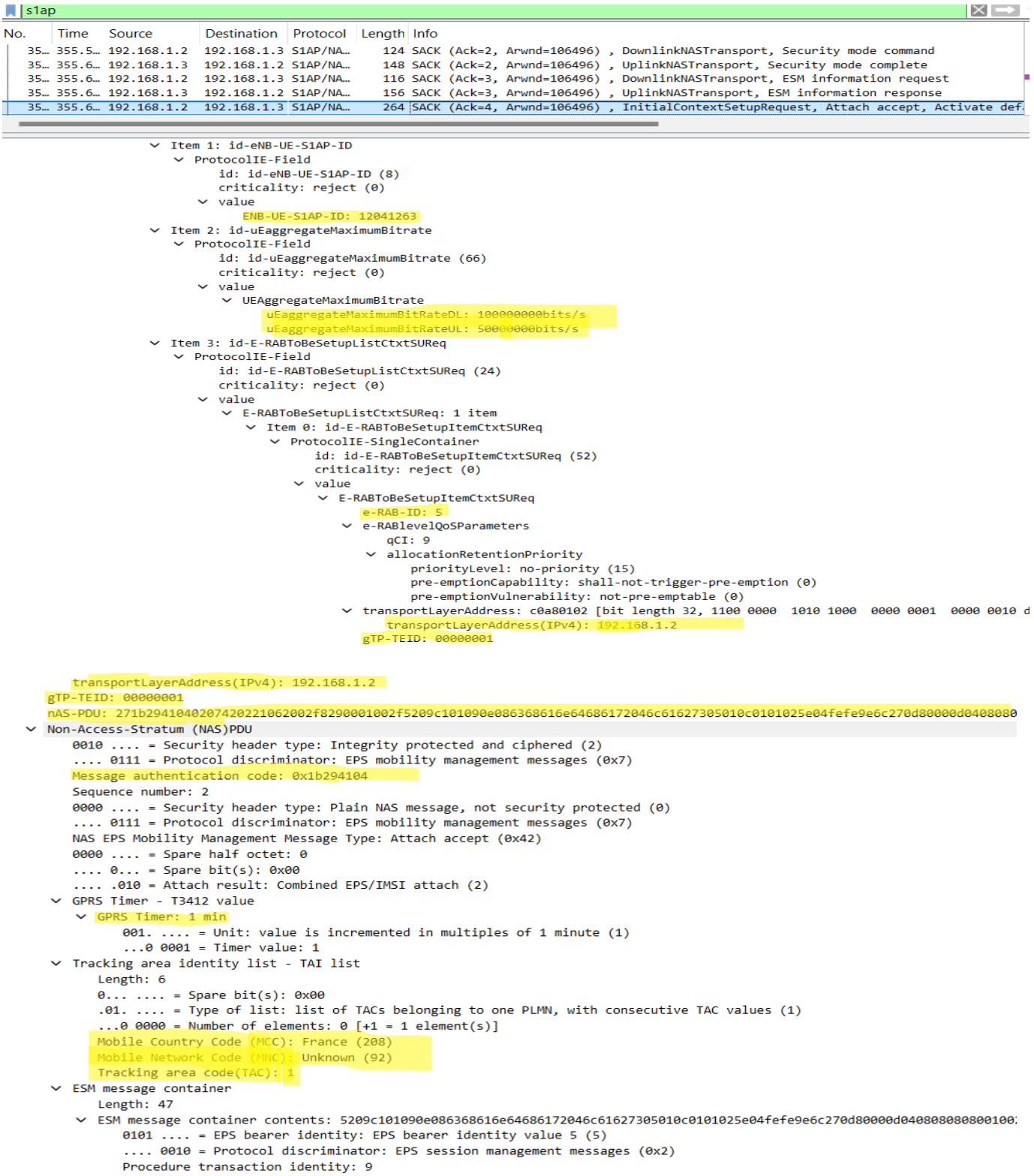
NOTE: At Step 2, take a screenshot and attach it.
Highlight the initial message fields



3. In Wireshark view the message details of Initial Context Setup Request, Attach accept, Activate default EPS bearer context request communicated via s1ap protocol.

NOTE: At Step 3, take a screenshot and attach it.
Identify the IP address of mobile. *6 MARKS*
Highlight the initial message fields

2 MARKS



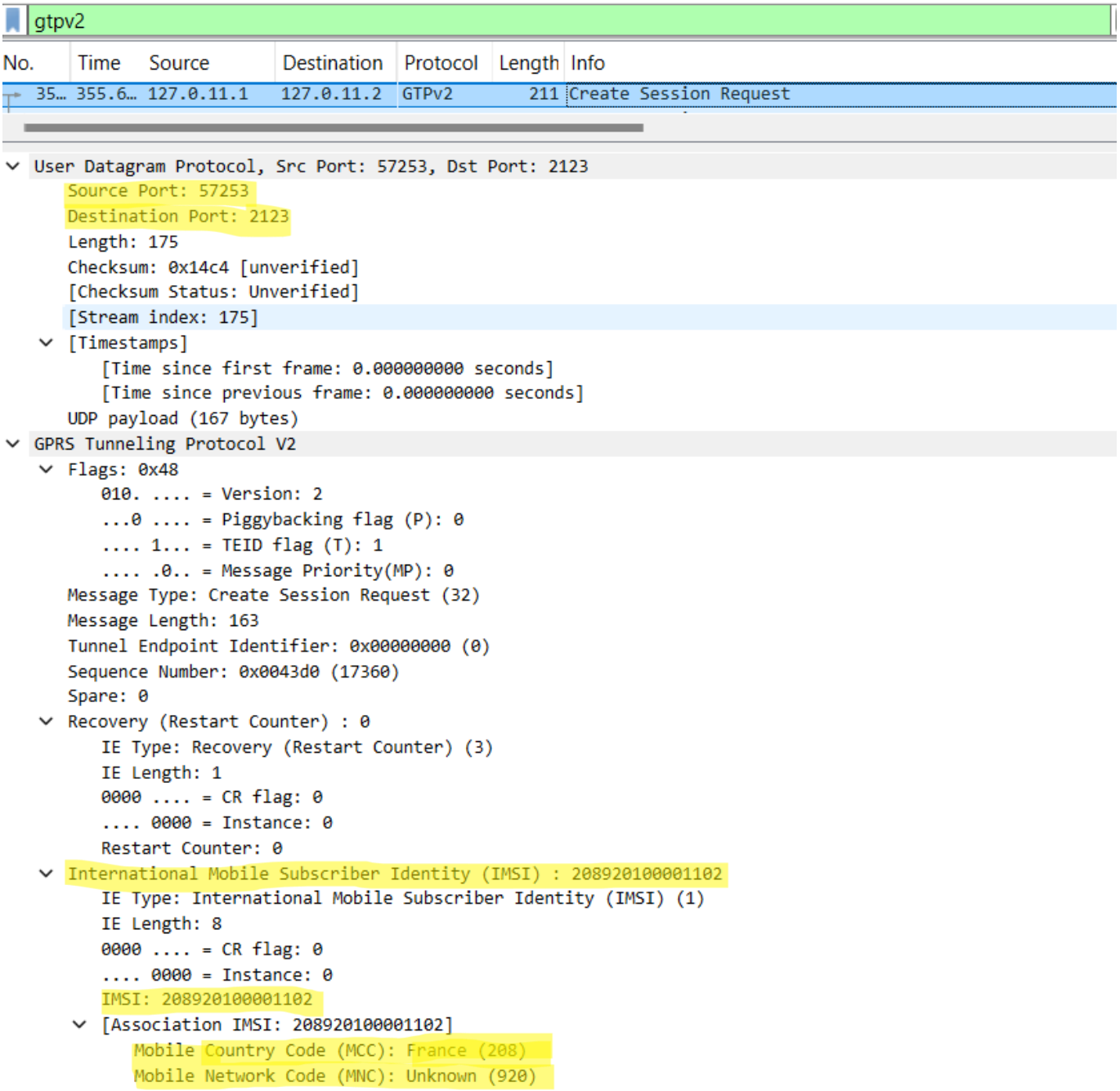
```
Procedure transaction identity: 9
NAS EPS session management messages: Activate default EPS bearer context request (0xc1)
v EPS quality of service
    Length: 1
    Quality of Service Class Identifier (QCI): QCI 9 (9)
v Access Point Name
    Length: 14
    APN: chandhar.labs
v PDN address
    Length: 5
    0000 0... = Spare bit(s): 0x00
    PDN type: IPv4 (1)
    PDN IPv4: 12.1.1.2
v APN aggregate maximum bit rate
    Element ID: 0x5e
    Length: 4
    APN-AMBR for downlink: 8640 kbps
    APN-AMBR for uplink: 8640 kbps
    APN-AMBR for downlink (extended): 100 Mbps
    Total APN-AMBR for downlink: 100.000 Mbps
    APN-AMBR for uplink (extended): 50 Mbps
    Total APN-AMBR for uplink: 50.000 Mbps
v Protocol Configuration Options
    Element ID: 0x27
    Length: 13
    [Link direction: Network to MS (1)]
    1... .... = Extension: True
    .... .000 = Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
  v Protocol or Container ID: DNS Server IPv4 Address (0x000d)
      Length: 0x04 (4)
      IPv4: 8.8.8.8
  v Protocol or Container ID: IPv4 Link MTU (0x0010)
      Length: 0x02 (2)
      IPv4 link MTU size: 1500 octets
```

```
35… 355.6… 192.168.1.3  192.168.1.2  S1AP/NA…   156 SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, ESM information response
35… 355.6… 192.168.1.2  192.168.1.3  S1AP/NA…   264 SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, Attach accept, Activate def…
```

```
                                        v Protocol or Container ID: IPv4 Link MTU (0x0010)
                                            Length: 0x02 (2)
                                            IPv4 link MTU size: 1500 octets
                                    v EPS mobile identity - GUTI
                                        Element ID: 0x50
                                        Length: 11
                                        .... 0... = Odd/even indication: Even number of identity digits
                                        .... .110 = Type of identity: GUTI (6)
                                        Mobile Country Code (MCC): France (208)
                                        Mobile Network Code (MNC): Unknown (92)
                                        MME Group ID: 4
                                        MME Code: 1
                                        M-TMSI: 1 (0x00000001)
            v Item 4: id-UESecurityCapabilities
              v ProtocolIE-Field
                    id: id-UESecurityCapabilities (107)
                    criticality: reject (0)
                  v value
                    v UESecurityCapabilities
                      v encryptionAlgorithms: e000 [bit length 16, 1110 0000  0000 0000 decimal value 57344]
                            1... .... .... .... = 128-EEA1: Supported
                            .1.. .... .... .... = 128-EEA2: Supported
                            ..1. .... .... .... = 128-EEA3: Supported
                            ...0 0000 0000 0000 = Reserved: 0x0000
                      v integrityProtectionAlgorithms: e000 [bit length 16, 1110 0000  0000 0000 decimal value 57344]
                            1... .... .... .... = 128-EIA1: Supported
                            .1.. .... .... .... = 128-EIA2: Supported
                            ..1. .... .... .... = 128-EIA3: Supported
                            .... ..0. .... .... = EIA7: Not supported
                            ...0 00.0 0000 0000 = Reserved: 0x0000
            v Item 5: id-SecurityKey
              v ProtocolIE-Field
                    id: id-SecurityKey (73)
                    criticality: reject (0)
                  v value
                      SecurityKey: 3508ee9d1d95a9ca9f3d49c945e0aa8984846310e425354b8bc0dfbc08a9ea65 [bit length 256]
```

4. **In Wireshark view the message details of Create Session Request via GTPv2 protocol.**

NOTE: At Step 4, take a screenshot and attach it.
Highlight the initial message fields *2 MARKS*



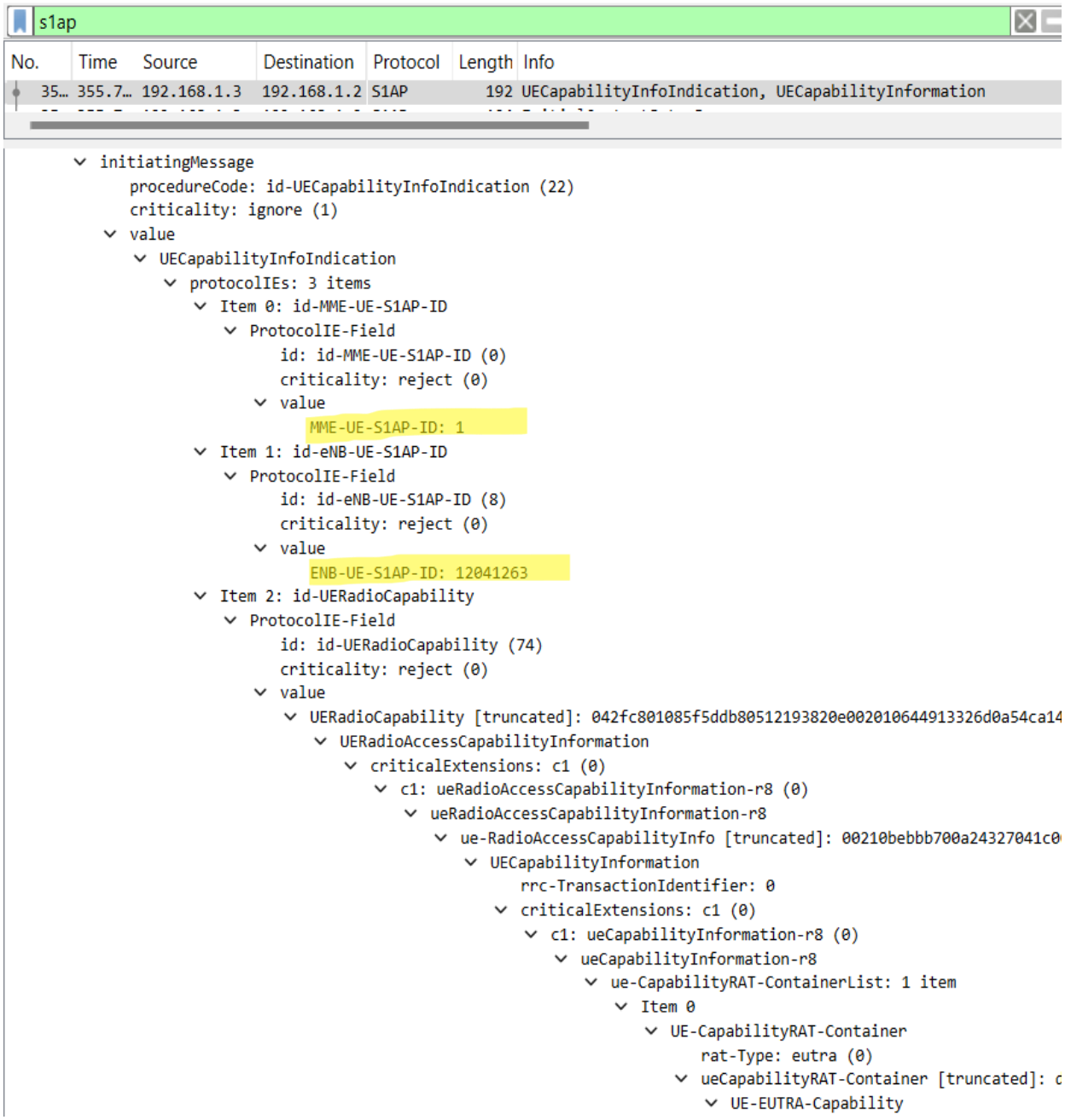
```
User Location Info (ULI) : TAI ECGI
    IE Type: User Location Info (ULI) (86)
    IE Length: 13
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
  ULI Flags: 0x18, ECGI Present, TAI Present
      0... .... = Extended Macro eNodeB ID Present: False
      .0.. .... = Macro eNodeB ID Present: False
      ..0. .... = LAI Present: False
      ...1 .... = ECGI Present: True
      .... 1... = TAI Present: True
      .... .0.. = RAI Present: False
      .... ..0. = SAI Present: False
      .... ...0 = CGI Present: False
  Tracking Area Identity (TAI)
      Mobile Country Code (MCC): France (208)
      Mobile Network Code (MNC): Unknown (92)
      Tracking Area Code: 0x0001 (1)
  E-UTRAN Cell Global Identifier (ECGI)
      Mobile Country Code (MCC): France (208)
      Mobile Network Code (MNC): Unknown (92)
      Spare: 0
    ECI (E-UTRAN Cell Identifier): 917760
        .... 0000 0000 1110 0000 0001 .... .... = eNodeB Id: 3585
        .... .... .... .... .... .... 0000 0000 = CellId: 0
RAT Type : EUTRAN (6)
    IE Type: RAT Type (82)
    IE Length: 1
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    RAT Type: EUTRAN (6)
PDN Type : IPv4
    IE Type: PDN Type (99)
    IE Length: 1
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    0000 0... = Spare bit(s): 0
    .... .001 = PDN Type: IPv4 (1)

PDN Address Allocation (PAA) : IPv4 0.0.0.0
    IE Type: PDN Address Allocation (PAA) (79)
    IE Length: 5
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    .... .001 = PDN Type: IPv4 (1)
    PDN Address and Prefix(IPv4): 0.0.0.0
APN Restriction : No Existing Contexts or Restriction (0)
    IE Type: APN Restriction (127)
    IE Length: 1
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    APN Restriction: No Existing Contexts or Restriction (0)
Aggregate Maximum Bit Rate (AMBR) :
    IE Type: Aggregate Maximum Bit Rate (AMBR) (72)
    IE Length: 8
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    AMBR Uplink (Aggregate Maximum Bit Rate for Uplink): 50000
    AMBR Downlink(Aggregate Maximum Bit Rate for Downlink): 100000
```

```
Fully Qualified Tunnel Endpoi..  er  ..er (F-TEID) : S11 MME GTP-C interface, TEID/GRE Key: 0x00000001, IPv4 127
   IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
   IE Length: 9
   0000 .... = CR flag: 0
   .... 0000 = Instance: 0
   1... .... = V4: IPv4 address present
   .0.. .... = V6: IPv6 address not present
   ..00 1010 = Interface Type: S11 MME GTP-C interface (10)
   TEID/GRE Key: 0x00000001 (1)
   F-TEID IPv4: 127.0.11.1
Access Point Name (APN) : chandhar.labs
   IE Type: Access Point Name (APN) (71)
   IE Length: 14
   0000 .... = CR flag: 0
   .... 0000 = Instance: 0
   APN (Access Point Name): chandhar.labs
Selection Mode : MS or network provided APN, subscribed verified
   IE Type: Selection Mode (128)
   IE Length: 1
   0000 .... = CR flag: 0
   .... 0000 = Instance: 0
   .... ..00 = Selection Mode: MS or network provided APN, subscribed verified (0)
Serving Network : MCC 208 France, MNC 92
   IE Type: Serving Network (83)
   IE Length: 3
   0000 .... = CR flag: 0
   .... 0000 = Instance: 0
   Mobile Country Code (MCC): France (208)
   Mobile Network Code (MNC): Unknown (92)
Bearer Context : [Grouped IE]
   IE Type: Bearer Context (93)
   IE Length: 31
   0000 .... = CR flag: 0
   .... 0000 = Instance: 0
```

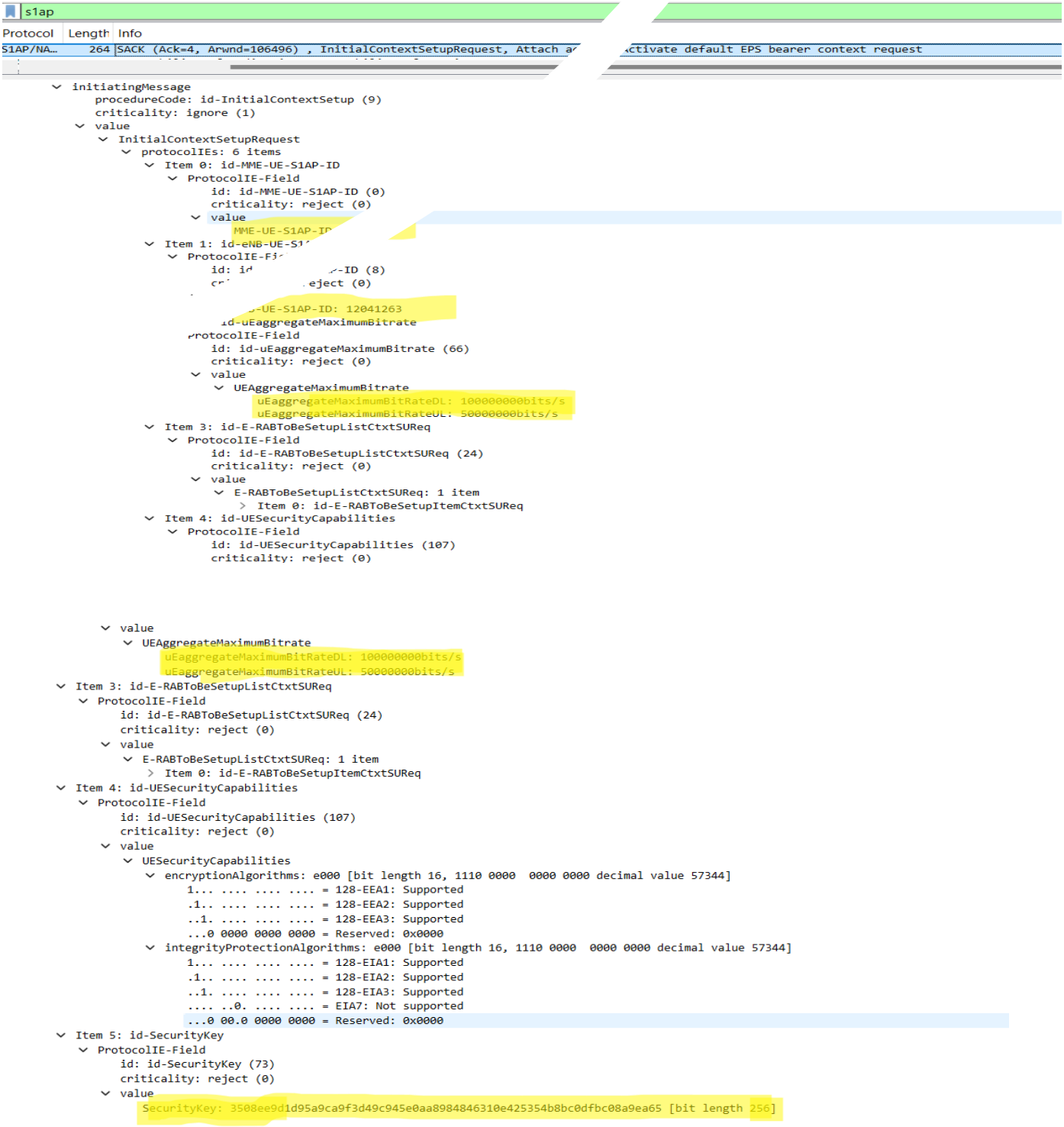
5. In Wireshark view the message details of UE Capability Info Indication and Information communicated via s1ap protocol.

NOTE: At Step 5, take a screenshot and attach it.
Highlight the initial message fields *2 MARKS*



6. **In Wireshark view the message details of Initial Context Setup R onse, Attach complete and the activation of default EPS bearer context accept r municated via s1ap protocol.**

NOTE: At Step 6, take a screenshot and attach it.
Highlight the initial message fields



INFERENCE & ANALYSIS

From the above inlab, illustrate the 4G LTE cellular system IP allocation sequence. Map the modules using a pictorial illustration.