TP5 : Les réseaux 4G/LTE

Objectifs :

1. Analyser les trames échangées entre un utilisateur mobile et une station eNB.
2. Récupérer les différent paramètre et identificateur d'un réseau 4G et du mobile.
3. Analyser les étapes de l'attachement du mobile au réseau LTE et Cœur.
4. Analyser l'étape de la récupération d'une adresse IP par un mobile.

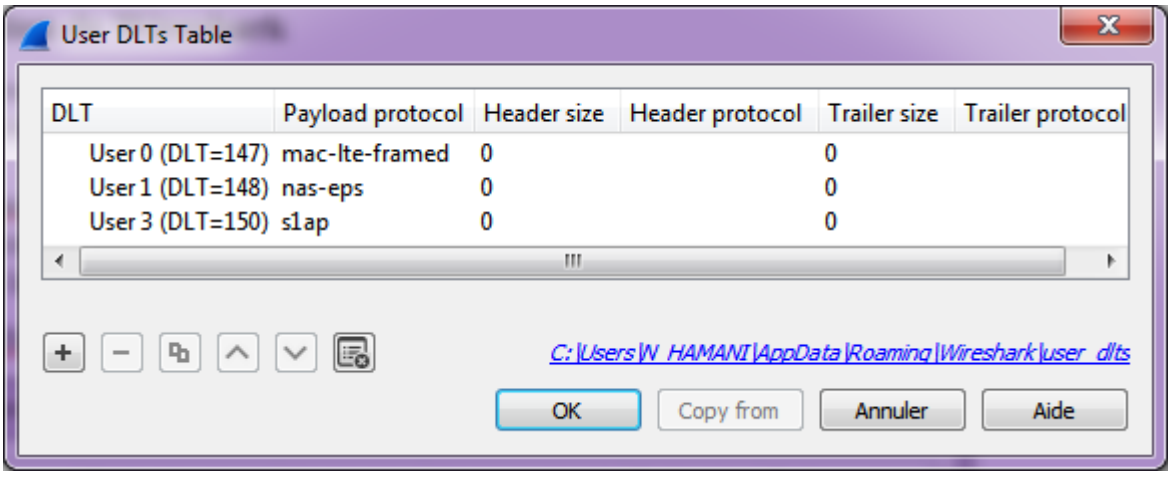
1- Préparation de Wireshark

Nous allons analyser des traces de réseaux cellulaire 4G en utilisant Wireshark. Ouvrir le fichier 4G-LTE.pcap

Wireshark nécessite une configuration pour afficher correctement les traces. Pour pouvoir analyser les traces, veuillez utiliser une version récente de Wireshark et faire les configurations suivantes :

- Preferences □ Protocols □ DLT_USER
- Edit Encapsulation Table
- Ajouter les entrées suivantes (+) :

Pour l'UE et l'eNodeB on rajoute *mac-lte-framed* et *nas-eps* et pour le l'EPC on rajoute *s1ap*.



2- Information sur la station de base

Sélectionner la première trame RRC

1. Quel est le canal utilisé ? Le canal utilisé est : BCCH.
2. Quel est le rôle de ce canal ?

Le BCCH fournit des informations nécessaires pour que la station mobile puisse se synchroniser avec la cellule et établir une connexion.

3. De quel type est cette trame (data ou signaling) ? C'est une trame de signalisation.

La trame est envoyée en plusieurs bloc. Nous allons nous intéresser à la trame concernant « Information System ». Dans LTE, le System Information Blocks, SIB transporte des informations qui permettent à l'UE d'accéder à la cellule. Il existe 13 types.

Les information système sont diffusées en utilisant les Master Information Block (MIB) et une série de System Information Blocks (SIB).

4. Quel est l'identificateur de l'eNB ? L'identificateur de l'eNB est : 144.
5. Quel est l'identificateur de la cellule (Cell ID) ? L'identificateur de la cellule est : 32202.

3- Information sur l'opérateur

Sélectionner la 2ème trame RRC qui vient juste après

1. Naviguer dans les informations de la trame et pointer l'identité du PLMN. Que représente le PLMN ? gsm-MAP
   Public Land Mobile Network, signifie un réseau mobile public présent dans un pays donné.
2. Quelle est la valeur du MCC ? (208).
3. Que représente le MCC ? Le code du pays de l'opérateur.
4. Quelle est la valeur du MNC ? (10).
5. Que représente le MNC ? Le code du réseau auquel est connecté l'opérateur téléphonique.
6. Chercher à quoi correspondent le MCC et le MNC ? La société française du radiotéléphonique (MNC) en France (MCC).
7. Quelle est la valeur de l'identificateur du PLMN ? 208 10.
8. Déduire l'ID globale de l'eNB qui le distingue d'une façon unique dans le monde. [208-10-144].

4- La procédure d'attachement

Les échanges entre l'UE et l'eNB sont caractérisés par les mentions : UL (Uplink) de l'UE vers l'eNB ou DL (Downlink) de l'eNB vers l'UE.

1. D'une manière générale, que se passe-t-il quand vous allumez votre téléphone (avant la procédure d'attachement) ?
   Avant de procéder à l'attachement, l'identification et l'authentification sont effectuées. L'UE doit transmettre son IMSI et son IMEI afin d'informer les eNB qui lui sont associées. Ces dernières transmettent ensuite les informations nécessaires à l'UE.

2. Quelle est la 1ère étape de communication l'UE aborde avec l'eNB ?
   L'UE initie une demande de connexion RRC et transmet ses capacités radio.
3. A quel moment le mobile a déclenché cette procédure dans la trace Wireshark ?
   trame 30 ; Time 0.38 ; info RRC Connection Request
4. Quel est l'objectif de la procédure d'attachement ? Établir une connexion avec les eNB afin d'accéder au réseau cœur de l'opérateur, puis à internet.
5. Quel est le canal utilisé le canal CCCH
6. Quelle est la caractéristique principale de ce type de canal ? Transmission de la signalisation si on ne peut pas utiliser un canal dédié
7. Pourquoi L'UE a fait recours à ce type de canal ? Car il est toujours en phase de connexion au réseau et ne dispose donc pas encore d'un canal dédié.
8. Quel est le 1er message de cette procédure ? Connexion RRC Message
9. Qui est l'initiateur du message et justifier ? L'UE est l'entité qui initie la connexion au réseau de l'opérateur.
10. Quelle est l'identité utilisé par l'UE et quelle est sa valeur ? L'UE s'identifie à l'aide du TMSI, dont la valeur est 24203036.
11. Pourquoi c'est le TMSI qui envoyé et n'est pas l'IMSI ? Comme l'IMSI est connu, cela présente un risque de traçage de l'UE. Pour éviter cela, un TMSI lui est attribué immédiatement après l'authentification.
12. Quelle est la raison de l'utilisation de TMSI au lieu de l'IMSI ? La raison est que le TMSI est plus sécurisé, ce qui réduit le risque de piratage.
13. L'identité de la zone est composée du MNC et du code LAC[1] (Location Area Code)[2]. Donner l'identité de la zone actuelle ? 1012102

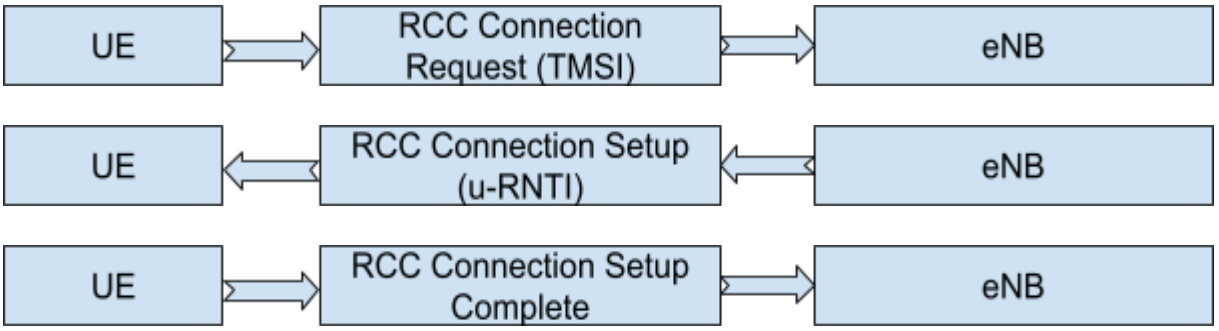
14. Localiser le moment de la réponse d'attachement (instant) ? La Trame 31 : 0:96
15. Il s'agit de quel message ? RCC Connexion Setup
16. Qui est l'origine de la réponse ? eNB
17. Vérifier les données de l'identification de l'UE. Est-ce que ce sont les mêmes que celles du la requête d'attachement ? Oui ce sont les mêmes que celles du la requête d'attachement.
18. L'eNB affecte à l'UE un identificateur unique dans la cellule u-RNTI (UTRAN RNTI) qui est une composition de deux valeurs : SRNC[3] (Serving Radio Network Controller) et S-RNTI (Serving Radio Network Temporary Identifier). Déterminer la valeur de u-RNTI ? 144 34659
19. Dans le même message l'UE envoie également le « ***scrambling code*** » qui est un code qui permet à l'eNB de communiquer avec plusieurs UE. L'eNB reçoit plusieurs ondes radio à la fois de plusieurs UE, en utilisant le scrambling code elle parvient à différencier les ondes. Exemple : remplacer les bit 0 et 1 par d'autre séquence 1□ 00110, 0□11100. Cette opération fait partie de la négociation des paramètres radio.

[1] Location Area Code, also learned from the SIBs
[2] https://www.cellmapper.net/
[3] https://rncmobile.net

Quel est le scramblig code attribué par l'eNB[4] ? 1117851

20. Quel est le dernier message d'attachement envoyé ? RRCConnectionSetupComplete
21. Quel est le canal utilisé ? DCCH
22. Pourquoi le type du canal de communication utilisé a changé ? Après l'établissement de la connexion RRC, l'UE reçoit un canal dédié qu'elle utilise pour la signalisation.
23. Globalement, quelles sont les informations envoyées par l'UE dans ce message ?
    les informations envoyées par l'UE dans ce message
    - Les capacités radio
    - L'algorithme de chiffrement
    - Le GUTI
    - L'identité de domaine

24. Donner le diagramme résumé de la procédure d'attachement capturée et les principaux paramètres échangé entre l'UE et l'eNB.



Les **capacités réseau**, les **données de sécurité** et le **GUTI** sont des paramètres échangés entre le **UE** et l'**eNB**. Le bearer établi est le **Signaling Radio Bearer (SRB)**

5- Echange de données

Analysons le message à l'instant 0.60 « InitialDIrectTransfer ». Le mot Direct veut dire que l'UE envoi une donnée directement vers le réseau EPC (Evolved Packet Core). Il est appelé NAS (Non-Access Stratum)" payload.

1. Que veut dire la mention nas-Message ? Le message est échangé entre l'UE et Le coeur du réseau
2. Il est de quelle direction ? UpLink
3. Quelles sont les principales informations échangées pour assurer cette opération ?
   Les informations échangées sont :

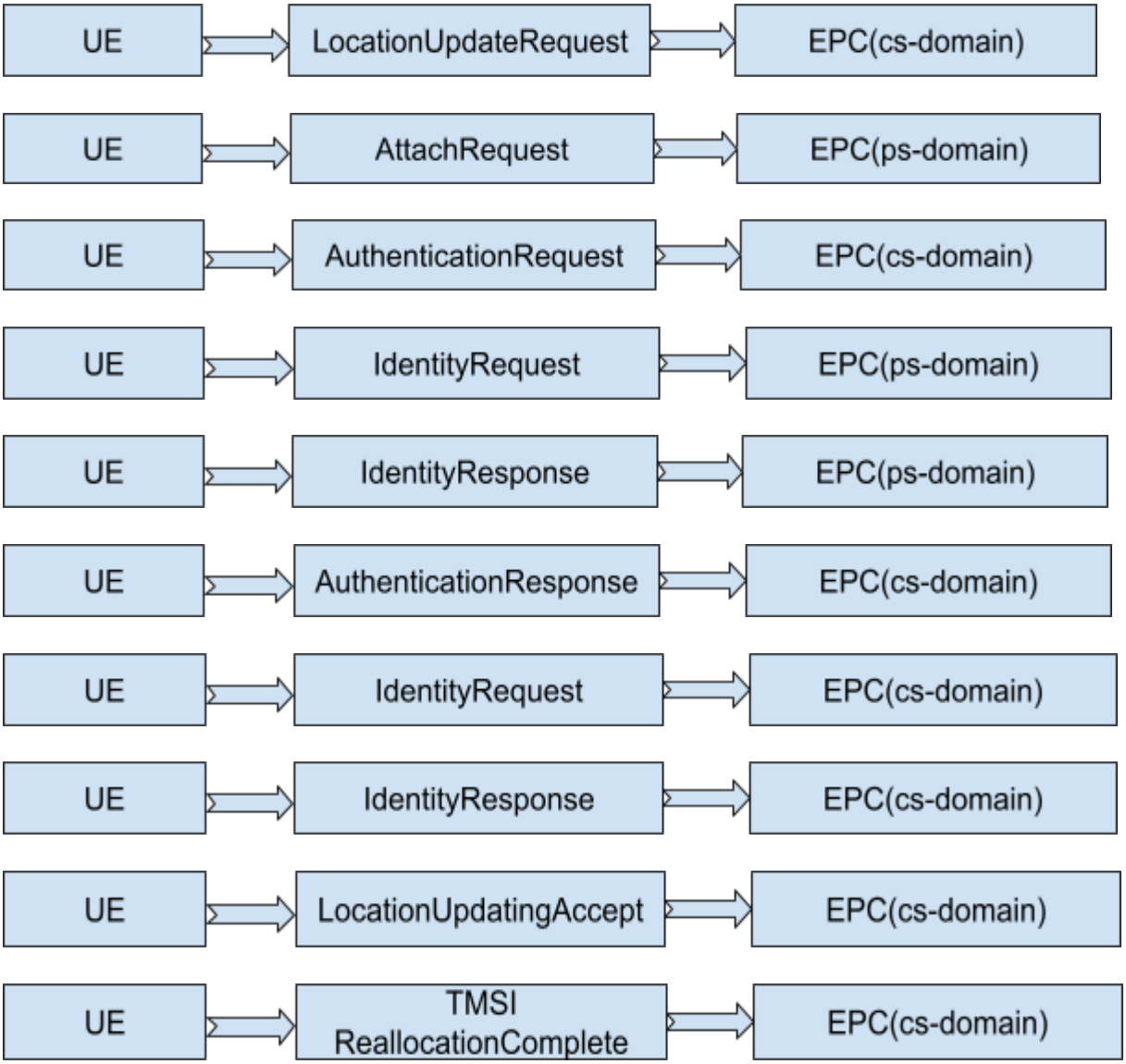
   - Le TMSI

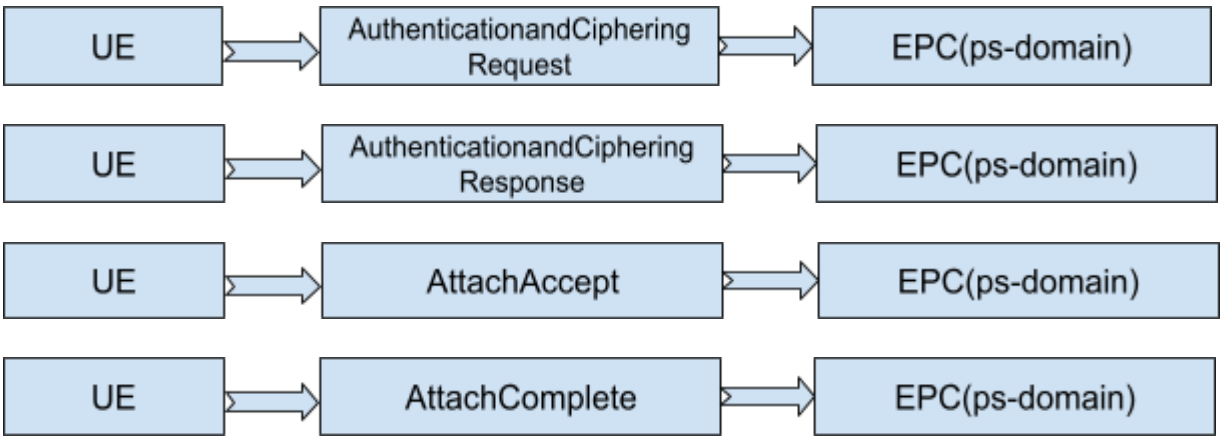
   - Les données liées à la sécurité, telles que le protocole de chiffrement

[4] Chercher dans le dernier item du message envoyé par l'eNB dans la partie FDD (Frequency Division Duplex)

- Les capacités d'accès au réseau

4. Quand l'UE répond à la demande de l'identité quelle information il inclut et quelle est sa valeur ?
   Il contient les éléments permettant son identification, notamment l'IMSI, qui a la valeur suivante : 208109876543120.
5. Dans la réponse à la 2ème demande d'identité quelle information l'UE inclut au message est quelle est sa valeur ?
   IMEISV (IMEI) de valeur 395770595785664
6. A quoi sert cet identifiant ? identifier de manière unique l'UE et l'utiliser lors de l'authentification.
7. Etablir un diagramme d'échange entre l'UE et le NAS à partir des messages avec l'EPC (les message portant la mention DTAP) jusqu'à l'instant 1.624.





6- Accès internet

Aller sur le message de la ligne 37.71 (6.49). Le message service request indique que l'UE demande un accès internet. Dans ce cas il doit demander auprès une adresse IP. Utiliser le filtre suivant :

```
(gsmtap.rrc_sub_type==0||gsmtap.rrc_sub_type==1)&&!(rrc.message==8)
```

Le message Activate PDP Context consiste à échanger les paramètres de connexion.

Inspecter la réponse de l'EPC et déterminer les paramètre IP du mobile lui permettant d'accéder à internet.

Adresse IPv4 : 10.175.144.168

Adresse Primary DNS: 172.20.2.39

Adresse Secondary DNS: 172.20.2.10