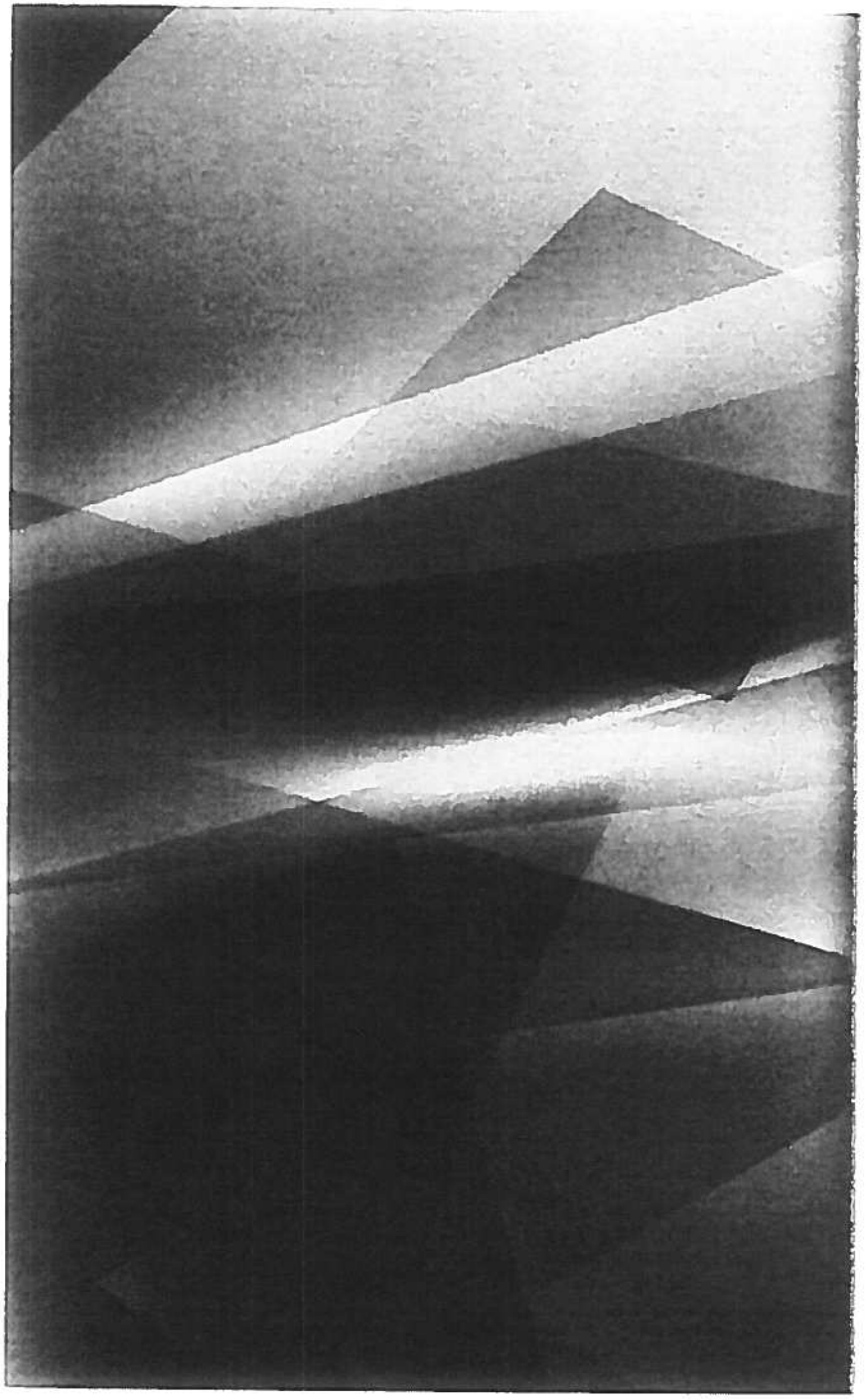
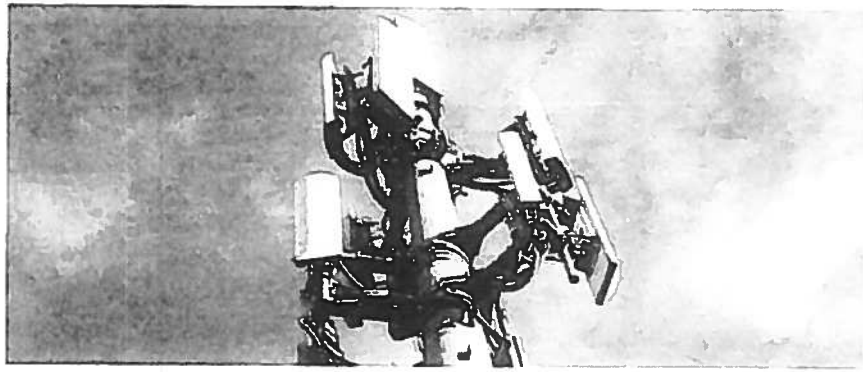


CEPOL

Investigations et téléphonie mobile



Module 1
L'intérêt de la téléphonie mobile

[redacted] – CEPOL 2019

Intérêt de la téléphonie dans le CT

Intérêts de la téléphonie et contre-terrorisme

- Communications terroristes

- Financement terroriste

Communications Terroristes :

- Tout le monde a un téléphone portable
- Surveillance des individus connus
- Identification des correspondants
- Géolocalisation
- Utilisation d'internet
- Applications mobiles de télécommunications

Les fraudes à la téléphonie

On peut difficilement voler 100 000 € à une personne .

On peut facilement voler 1 € à 100 000 personnes.

Financement terroriste :

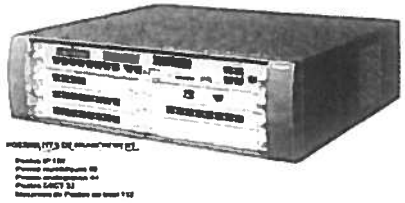
Escroqueries téléphoniques :

- PABX/IPBX
- Utilisation des numéros premium /micro-paiements.
- Les sites remboursements de crédit Tel.
- SexCAM et Virus.
- Ping Call et Call Back
- Sim-swapping

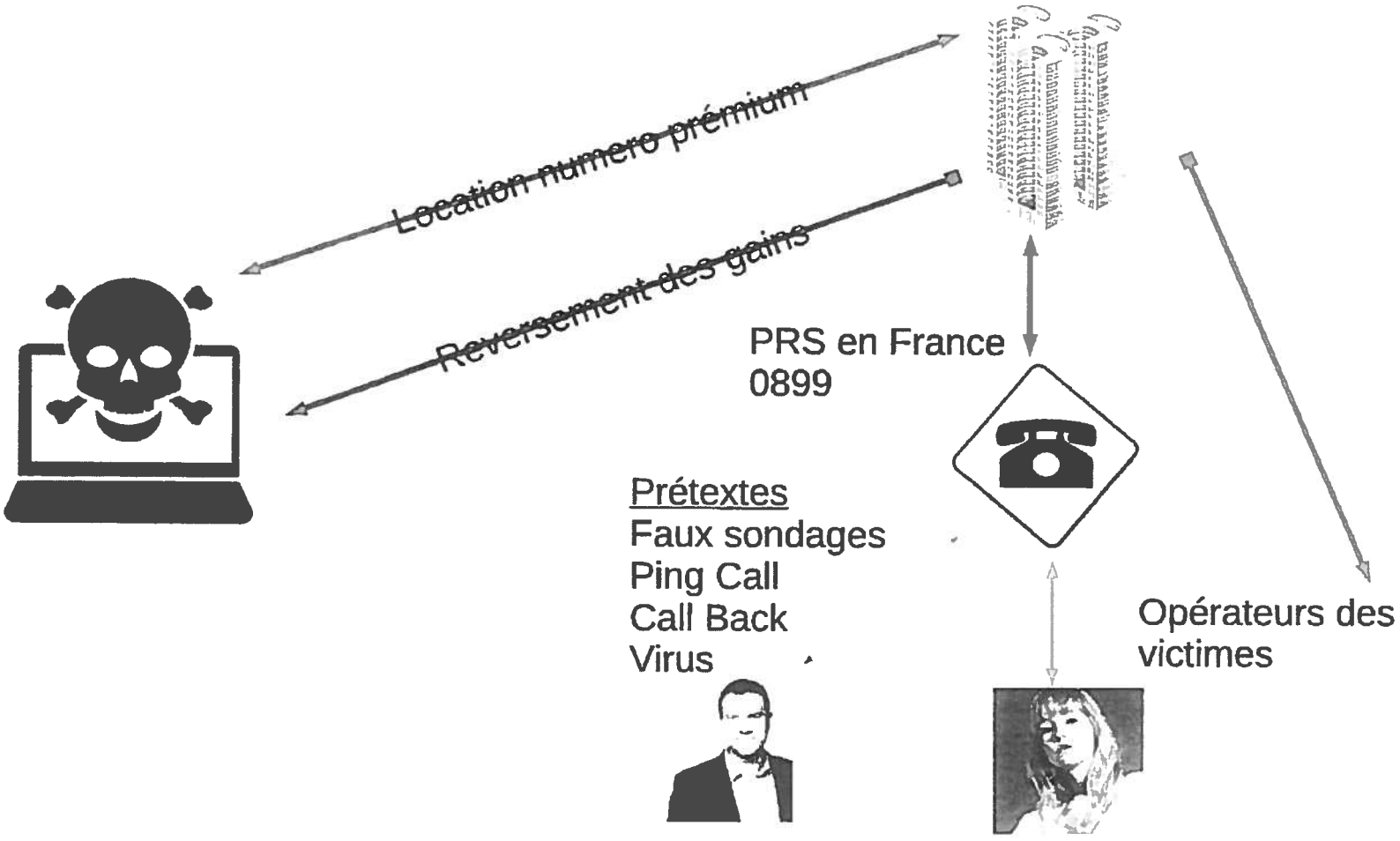
Fraudes aux PABX / IPBX

- Standards téléphoniques des sociétés
- Pirate s'introduit sur l'appareil (code de maintenance)
- Il emet des appels vers des numeros premium ou des pays étrangers.
- Souvent l'attaque provient de l'étranger.

STANDARD TELEPHONIQUE PABX + IPBX



Le circuit des numéros premium



Youpass.com / les sites de remboursements crédits

Remboursements de forfait	Nombre de membres	Seuil de paiement	Paiements declares sur NBR	Statut
				NOUVEAUTÉ
				
				
				
				
				
				

Les virus téléphoniques :

Dylan, le hacker amiénois, condamné à 1 an de prison

Faits divers | 08 novembre 2012, 21h05 |

A A

Son virus avait affecte 17000 smartphones Jeudi, Dylan, un Amiénois de 20 ans, a éte condamne par le tribunal correctionnel d'Amiens à un an d'emprisonnement, dont six mois fermes à purger sous bracelet électronique Son delit ? « Escroquerie et atteinte à un système automatise de donnees ». Le jeune homme encourait une peine allant jusqu'à cinq ans de prison. Les requisitions, elles, se limitaient à douze mois avec sursis

Leur virus de smartphones aurait fait 2 000 victimes

Ile-de-France & Oise > Seine-Saint-Denis > Aubervilliers, 15 février 2012, 21h00 |

A A

On l appelle Foncy. A l'actif de ce logiciel malveillant made in France, vieux d'a peine six mois, plus de 2 000 victimes et un préjudice estime a 100000 €. C'est la première fois en France que des enquêteurs decouvrent un tel « dialer » qui s'attaque aux téléphones Android, ces smartphones qui utilisent un logiciel concurrent d'Apple. Cette enquête, inedite, a valu aux deux auteurs presumés de cette arnaque technologique de rendre des comptes a la justice

Ping Call et Call Back :

- Ping call ou « appel en absence ».
  08 9xxxx ou téléphone rebond.

- Call Back

L'ALSACE.fr

A la Une Actualité

A la Une

ENQUÊTE

Numéros surtaxés, une arnaque à 38 millions d'euros

Quatre salariés de la société de téléphonie Viva Multimedia ont été mis en examen le 31 mai dernier. Ils sont soupçonnés d'avoir empoché 38 millions d'euros grâce à une arnaque aux numéros surtaxés.

Sim swapping

Le fraudeur appelle le service client opérateur mobile de la victime et demande qu'une nouvelle carte SIM soit reliée au numéro de portable ;

- Cette nouvelle carte SIM permet à l'escroc de récupérer le code SMS 3D-Secure.

Identifier les numéros surtaxés français:

- Pour les numéros 08 9xxxx

  http://www.infosva.org/

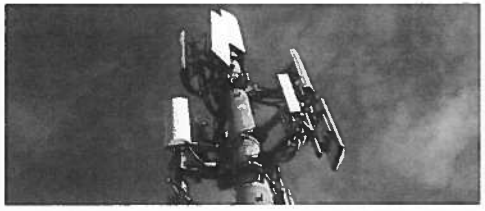
- Pour les SMS+ (5 chiffres)

  https://annuaire.infoconso-multimedia.fr/assistant-infoconso/smsplus

Des questions ?

CEPOL

Investigations et téléphonie mobile



Module 2
Les réseaux GSM

[redacted] CEPOL 2019

Sommaire :

- Généralités sur la téléphonie
- Architectures simplifiées d'un réseau mobile
- La gestion des téléphones sur le réseau

Généralités sur la téléphonie

Les appareils mobiles ?

- **Téléphones portables / tablettes**
- **Clés 3g / 4g**
- **Balises GPS**
- **Objets connectés**

Les acteurs de la téléphonie

L'agence Nationale de Réglementation des Télécommunications (ANRT)

- Missions juridiques
- Missions économiques
- Missions techniques.

Les acteurs de la téléphonie

Opérateurs historiques

- **Propres infrastructures réseaux**
- **Utilisent leurs cartes SIM**
- **Marketing, commercialisation, facturation et services clients.**

Les acteurs de la téléphonie

Les sociétés de commercialisation des services (SCS) :

- **Utilisent les cartes SIM des opérateurs historiques à leurs couleurs.**
- **Commercialisent les offres d'un ou plusieurs opérateurs.**

Les acteurs de la téléphonie

Les opérateurs mobiles virtuels (MVNO) :

- **Utilisent leurs propres cartes SIM**
- **Achètent des minutes en gros aux opérateurs**
- **Créent des offres (tarifs, services)**
- **Utilisent les infrastructures opérateurs historiques.**

L'opérateur virtuel catalan FonYou débarque au Maroc

Différentes prestations de services :

- **Abonnement** : l'utilisateur est identifié auprès de l'opérateur,informations bancaires.
- **Carte pré-payée** : la carte est mise à disposition de l'utilisateur avec un crédit de communication inclus. Possibilité ou non de s'identifier.
- **Recharge pré-payée** : permet le rechargement de crédit (voucher).

Les obligations légales :

Les opérateurs ont des obligations légales envers le client :

- Traitement des données personnelles
- Portabilité des numéros

Les demandes judiciaires :

Les opérateurs ont des obligations légales envers les forces de l'ordre :

- Obligation de conservation des données pour la recherche, constatation et poursuite des infractions pénales.
- Conservation des données techniques (données traitées en vue de l'acheminement d'une communication sur le réseau ou sa facturation).

Architectures simplifiées d'un réseau mobile

Le réseau cellulaire :

Le territoire est segmenté en petites zones appelées « **cellules** »

- Souvent représentées sous forme d'hexagones
- En réalité la forme dépend de la configuration des lieux et du rayonnement des antennes.

Le réseau cellulaire :

On peut distinguer 4 type de « cellules »:

- **La macro cellule** (+dizaines km)
- **La petite cellule** (-10 km)
- **La micro cellule** (-1 km)
- **La pico cellule** (+10 m)

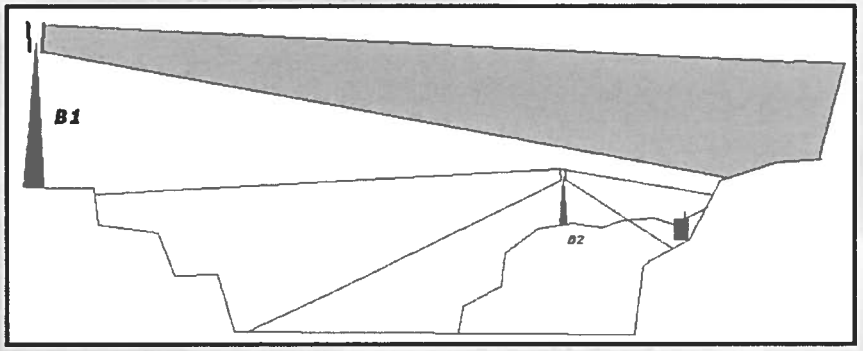
Les antennes relais :

Chaque cellule est couverte par une antenne relais qui peut être :

- Mono-sectorielle (360°)
- Bi-sectorielle (180°)
- Tri-sectorielle (3 x 120 °)
- Quadri-sectorielle (4 x 90°)

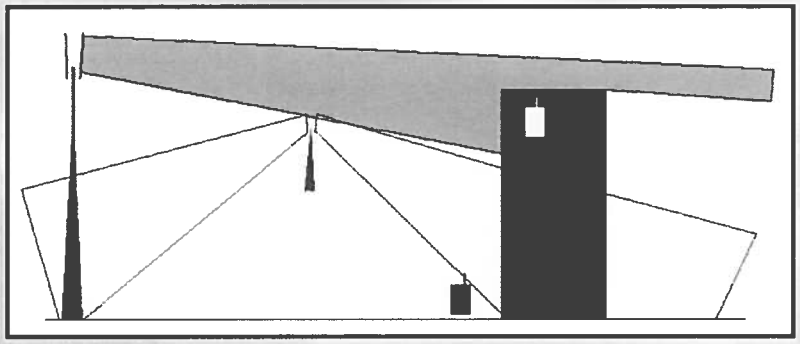
Les antennes relais :

Rayonnement et couverture



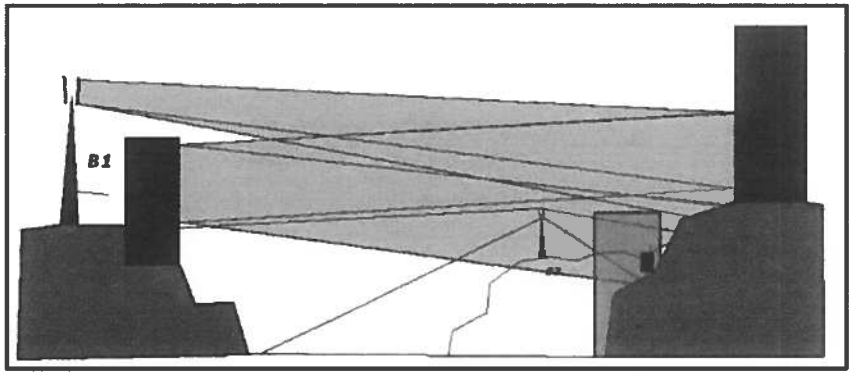
Les antennes relais :

Rayonnement et couverture



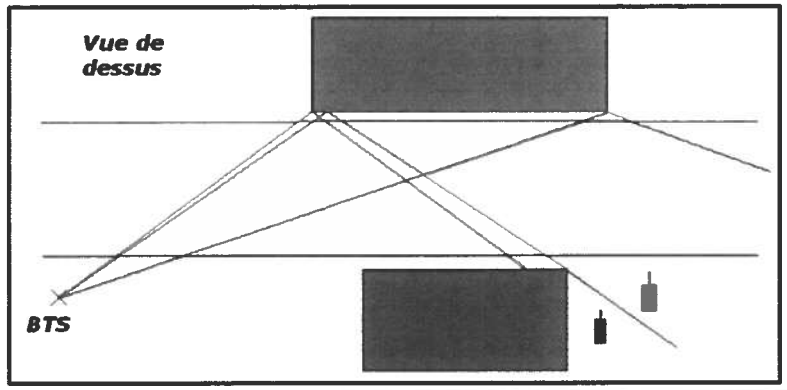
Les antennes relais :

Rayonnement et couverture



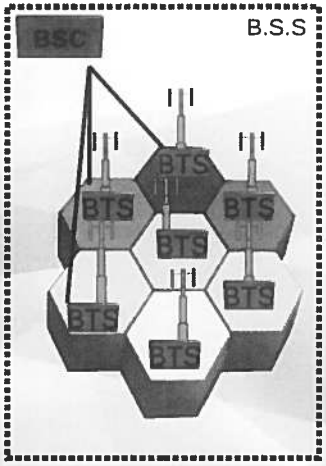
Les antennes relais :

Rayonnement et couverture



Le Base Station Subsystem (BSS) :

Il s'agit de l'ensemble composé :



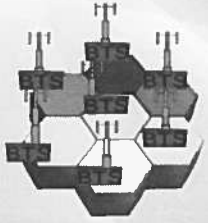
- des antennes
- des BTS
- des BSC

Cette partie est connectée au coeur du réseau télécom le Network SubSystem (N.S.S).

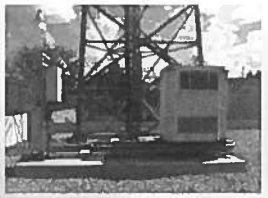
Le réseau cellulaire :

Les antennes sont reliées à des BTS « Base Transceiver Station » / E-nodeB (4G)

Cet élément est chargé principalement d'assurer les liaisons radio avec les téléphones mobiles.

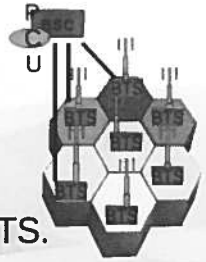


Rôle de la Base Transceiver Station :



- Gestion de la signalisation entre les téléphones et l'infrastructure
- Transmission radio (modulation, démodulation , égalisation..)
- Chiffrement des contenus
- Mesures radio nécessaires de la liaison normale

Rôle de la Base Station Controller :

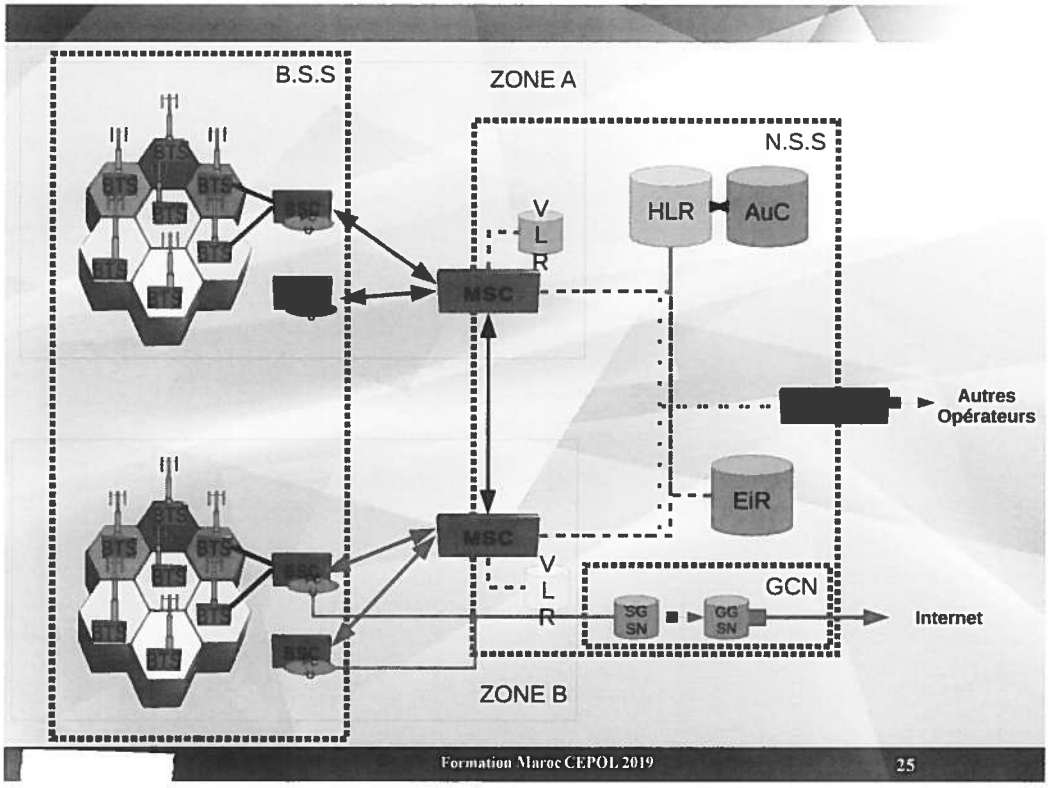


- Les BTS sont reliées à des BSC « Base Station Controller » par un lien.
- Une BSC peut contrôler plusieurs dizaines de BTS.
- Dans le réseau 3G, la BSC est remplacée par le RNC « Radio Network Controller »

- Un Packet Control Unit (PCU) est associé à la BSC pour assurer le trafic GPRS

Rôle de la Base Station Controller :

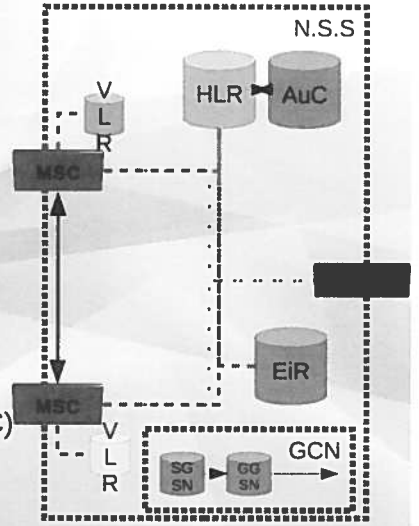
- Partie « intelligente » du réseau BSS
- Peut commander une cinquantaine de BTS.
- Décide la puissance d'émission des BTS.
- Concentre les communications vers une sortie unique.
- Gère les handovers sur les BTS de la zone.



Le Network SubSystem (N.S.S) :

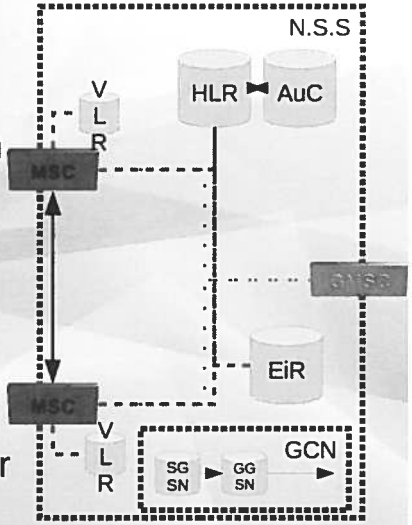
Il s'agit de l'ensemble composé :

- Mobile Switching Center (MSC)
- Visitor Location Register (VLR)
- Home Location Register (HLR)
- l'Authentification Center (AuC)
- l' Equipment Identity Register (EiR)
- Gateway Mobile Switching Center (GMSC)
- Serving GPRS Support Node (SGSN)
- Gateway GPRS Support Node (GGSN)



Le Mobile Switching Center (MSC) :

- Il s'agit d'un dispositif chargé du routage dans le réseau et des interconnexions entre mobile et un autre MSC.
- Concentre les flux en provenance des BSC.
- Contrôle les handovers intra-MSC (BSC) / inter-MSC.
- Dialogue avec le VLR pour assurer la localisation et l'itinérance.

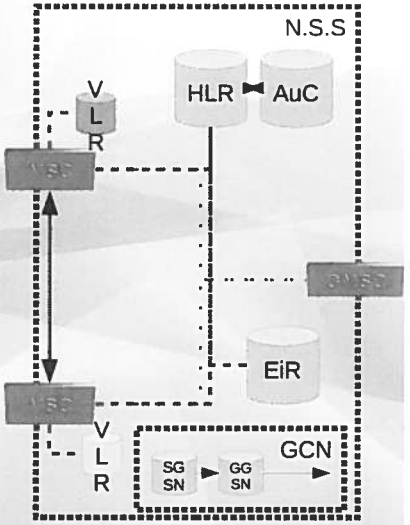


Le Visitor Location Register (VLR) :

Il s'agit d'une base de données temporaire contenant les informations des utilisateurs sur zone.

Exemples :

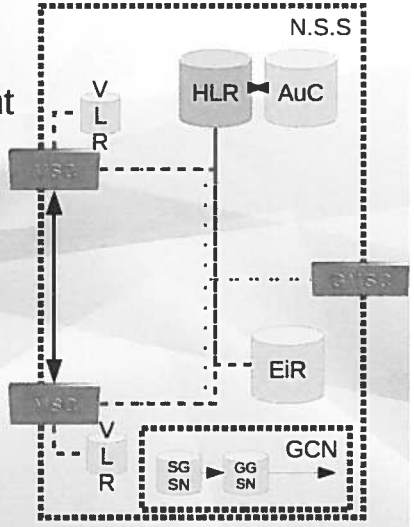
- TMSI dérivé de l'IMSI , LAI, adresse du MSC...
- Assure l'itinerance/roaming



Le Home Location Register (HLR) :

Il s'agit de la base de données centrale d'un opérateur comportant les informations de l'abonné :

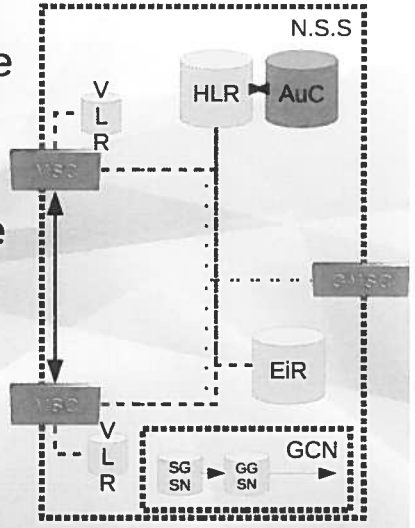
- IMSI,Numéro de l'abonné, IMEI, type d'abonnement, position grossière de l'abonné (le numéro de VLR où il est enregistré)….



L'Authentification Center (AuC) :

S'occupe de la sécurité, vérifie que l'abonné à les droits :

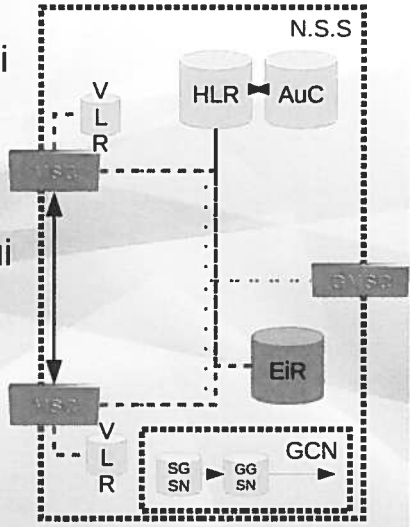
- Authentifie les abonnés par une clé présente dans la carte SIM du téléphone et le centre AuC.
- Grâce à l'authentification, un VLR peut accueillir un téléphone d'un autre réseau.



L'Equipment Identity Register (EiR) :

Il s'agit d'une base de données qui référence les portables (IMEI) sur le réseau.

Si un téléphone est volé, il peut être rentré dans cette base pour lui interdire l'accès au réseau.

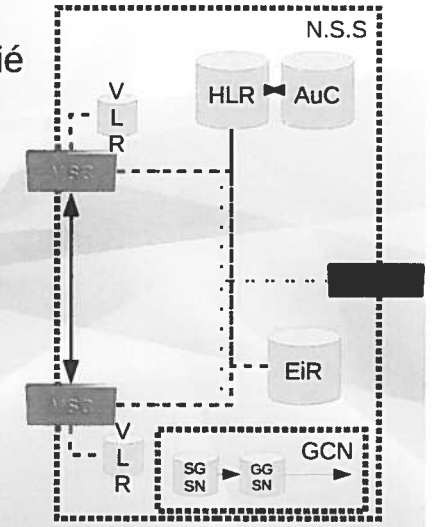


Gateway Mobile Switching Center (GMSC) :

Il s'agit d'un MSC a qui on a confié un rôle de passerelle avec les autres réseaux.

Ils sont souvent placés en périphérie du réseau d'un opérateur pour assurer l'interopérabilité avec les autres opérateurs.

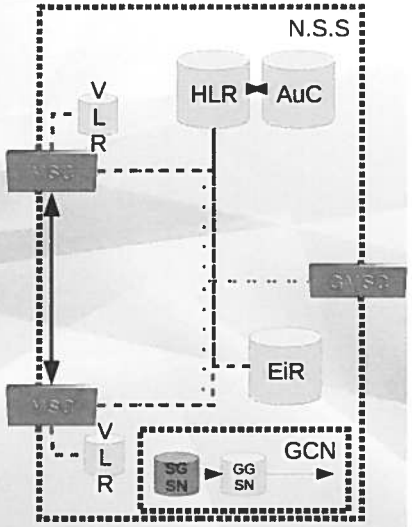
Interroge le HLR lors d'un appel entrant.



Serving GPRS Support Node (SGSN) :

Il s'agit d'une passerelle qui achemine les données dans les réseaux mobiles

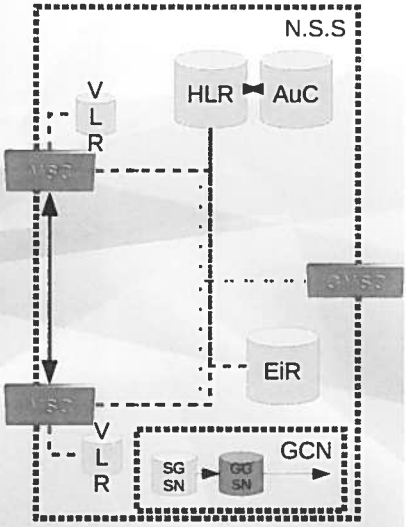
- Même rôle que le MSC (voix)
- Il gère l'interface IP via une autre passerelle le GGSN.

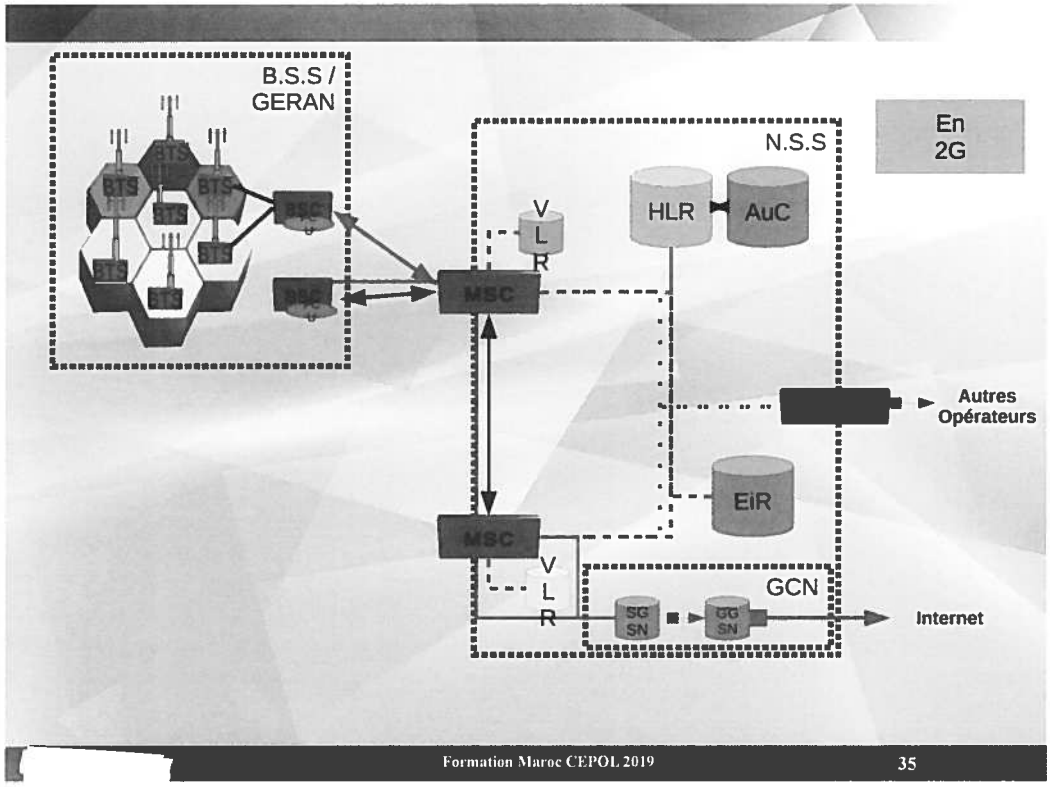


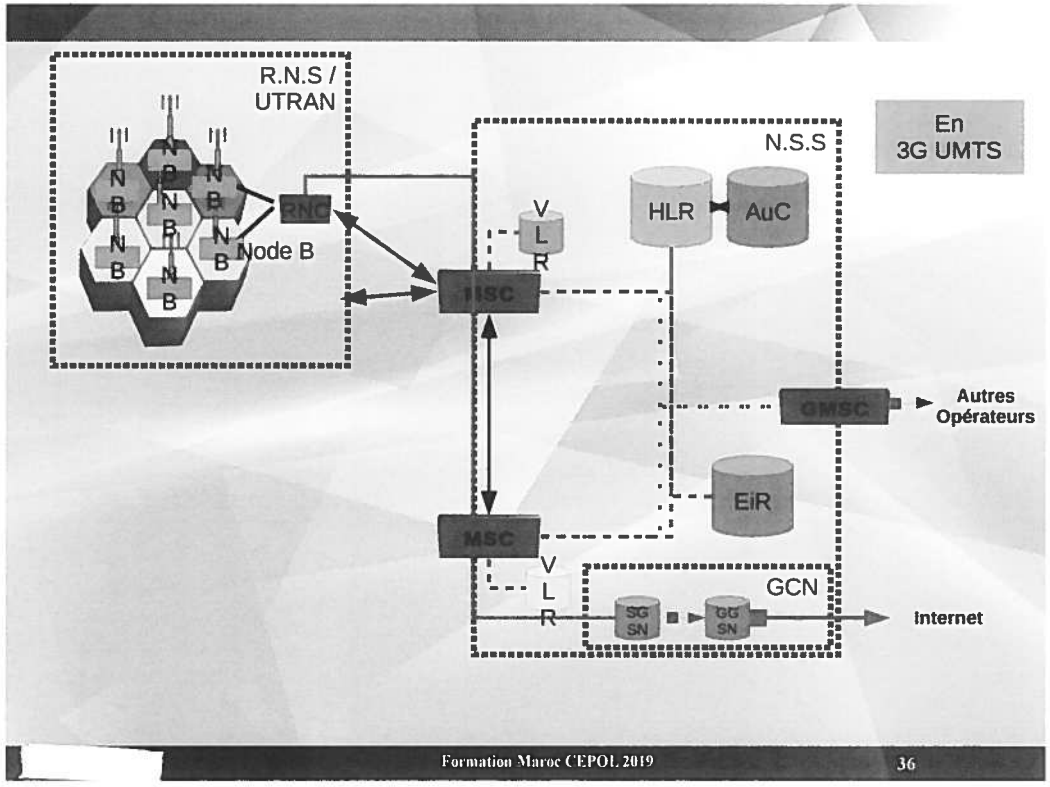
Gateway GPRS Support Node (GGSN) :

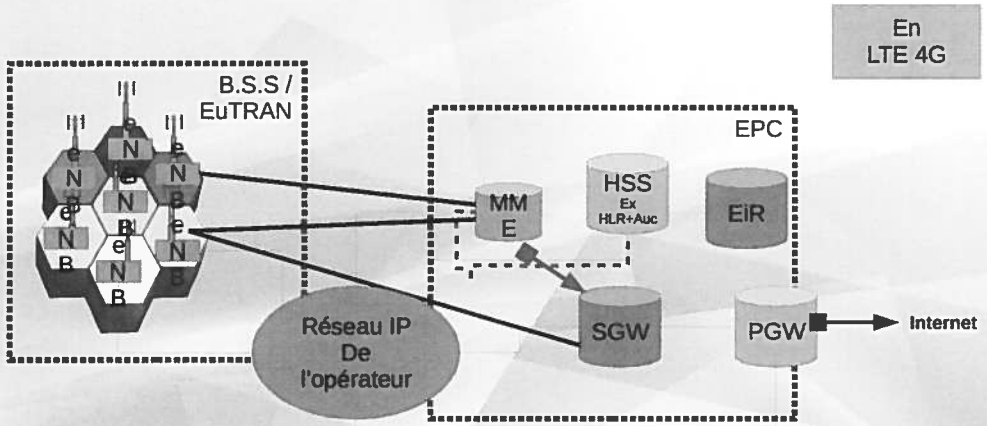
Passerelle réalisant l'interface entre réseau GPRS et internet.

- Transmet le trafic au SGSN utilisé par le téléphone.
- Assure le routage des informations.
- Assure la mobilité lors du déplacement de l'abonné (avec le PDP Packet Data Protocol).
- Fait office de parefeu.




B.S.S / GERAN
BTS
BSC
MSC
V L R
N.S.S
HLR
AuC
En 2G
Autres Opérateurs
EiR
MSC
V L R
GCN
SG SN
GG SN
Internet

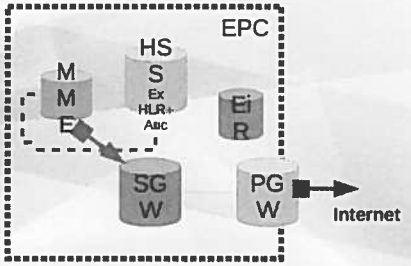

R.N.S / UTRAN
N B
RNC
Node B
MSC
V L R
N.S.S
HLR
AuC
En 3G UMTS
GMSC
Autres Opérateurs
EiR
MSC
V L R
GCN
SG SN
GG SN
Internet



L'architecture 4G :

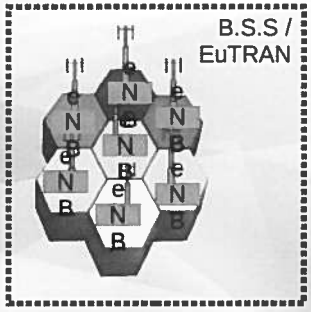
Il s'agit de l'ensemble composé :

- des EnB
- Des MME
- Du HSS
- SGW
- PGW
- Eir



Les Enodes B :

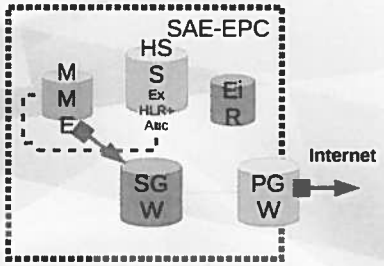
- Equivalent du NodeB de l'UMTS.
- Connectés au coeur de réseau EPC par réseau Backhaul (fibre).
- Trient voix et données. Les données sont envoyées en IP dans le coeur de réseau.
- Intégrent les fonctions de contrôle des RNC.



Les Mobility Management Entity (MME) :

Equipement qui gère la signalisation entre les téléphones et le coeur de réseau (attachements, localisation)…

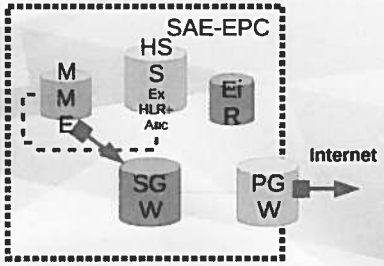
- Gère les handovers, l'itinérance
- Dialogue avec le HSS pour consulter les profils des mobiles.
- Selection du SGW



Le Home Subscriber Server (HSS) :

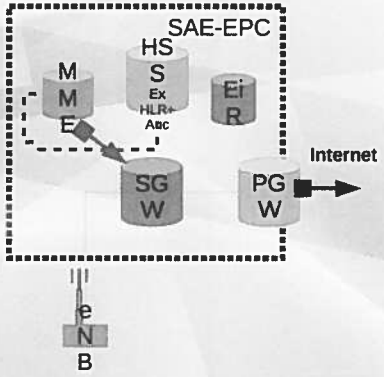
Equivalent du HLR (mais peut être utilisé sur 2g,3g,4g du même opérateur)

- Possède les mêmes fonctions d'authentification que l'AuC.



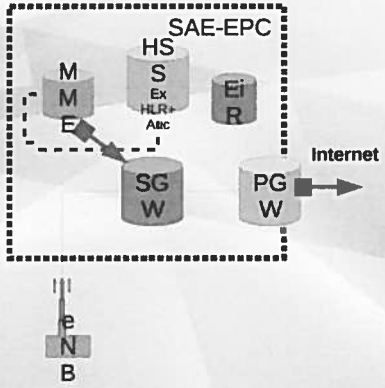
Le Serving Gateway (SGW) :

- Achemine les données et voix.
- Passerelle régionale reliée au PGW.
- Routage des paquets sortants au PGW et les paquets entrants vers le EnodeB de l'abonné en cas de mobilité du terminal.

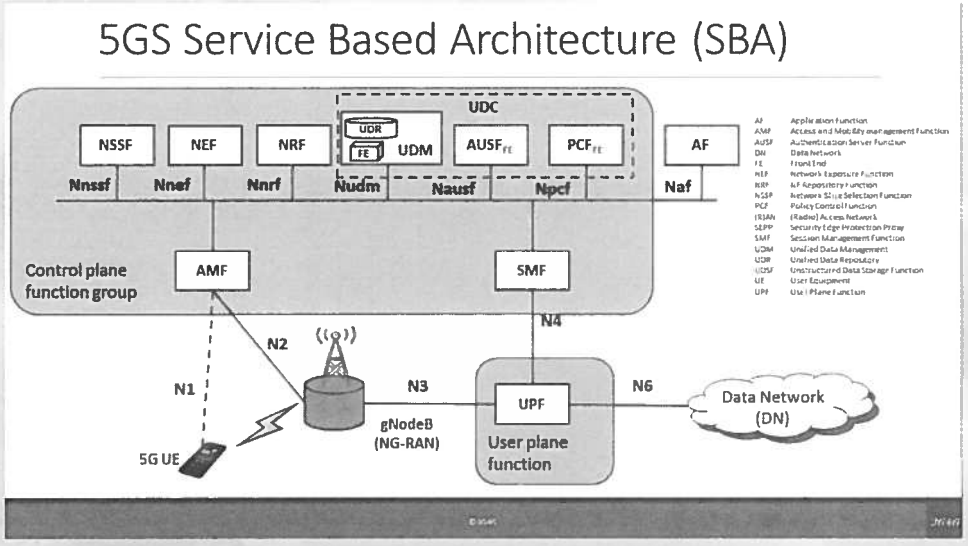


Le Packet Data Network Gateway (PGW) :

- Interface vers les réseaux externes.
- Routages des paquets IP vers le EnodeB de l'abonné
- Assure l'interface IP v4 et v6.



La prochaine étape : la 5 G :



La gestion des téléphones sur le réseau Télécom

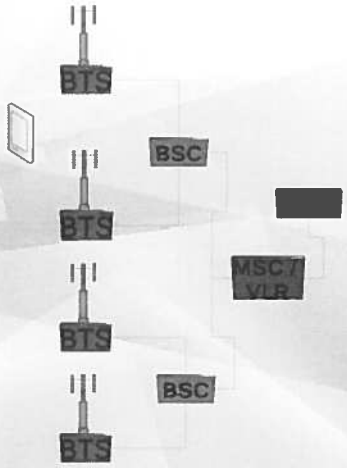
La voie balise :

- Chaque station de base diffuse régulièrement un signal qui informe de son existence et donne les caractéristique du réseau (Ex : Nom opérateur)

- On parle de « voie balise » ou « Beacon Channel ».

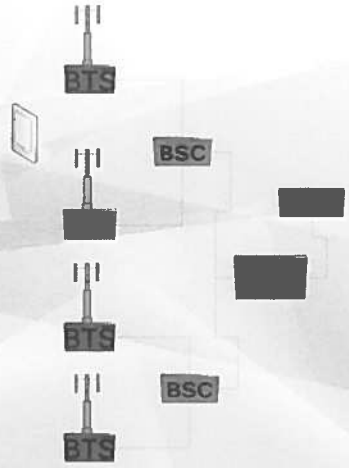
Mise sous tension du téléphone :

- Le mobile se signale au réseau (attachement réseau ou IMSI attach)
- Authentification du mobile : le VLR demande au HLR
- Le VLR informe que l'IMSI se trouve dans le VLR concerné
- Transfert du profil abonné du HLR au VLR.
- Attribution d'un TMSI par le VLR en fin de procédure



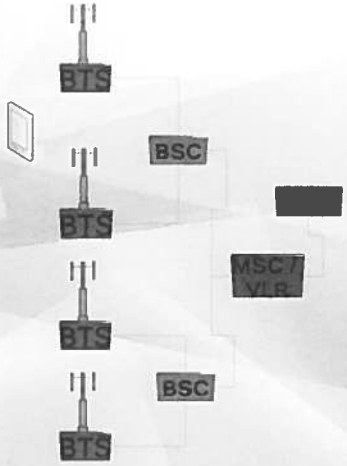
Appel sortant :

- Le mobile transmet son TMSI
- Le VLR vérifie les droits de l'abonné
- Création d'un canal de transmission
- Lors que le correspondant décroche, la connexion se réalise.



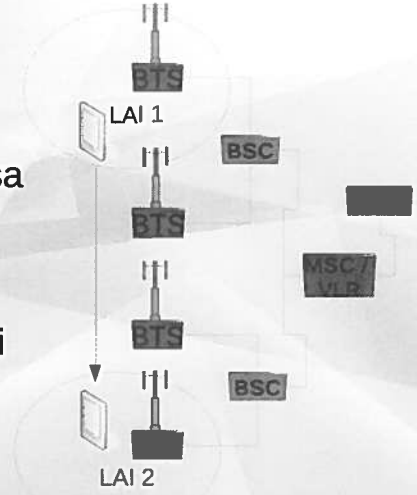
Appel entrant :

- Le correspondant compose le numéro.
- Passage par la GMSC de l'abonné
- Consultation des informations dans le HLR
- Identification du VLR où se trouve l'abonné par IMSI
- Notification de l'abonné par TMSI (paging)
- Création du canal de conversation.



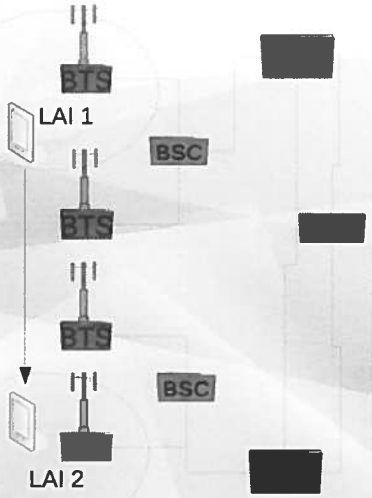
Changement de zone et même VLR :

- Location Area Identity
- Envoi par le mobile au VLR de sa nouvelle localisation
- La mise à jour est fait par l'envoi de son TMSI



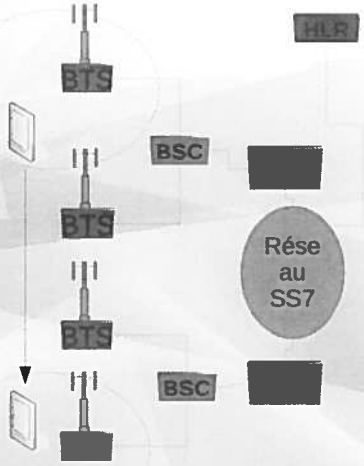
Changement de zone et de VLR :

- Le TMSI est alloué à l'ancien VLR
- Le mobile envoi l'ancien LAI au nouveau VLR2
- LAI+TMSI unique au monde
- Le nouveau VLR demande à l'ancien VLR l'IMSI du mobile
- Récupération des infos de profil dans le HLR
- Attribution d'un nouveau TMSI sur le VLR2



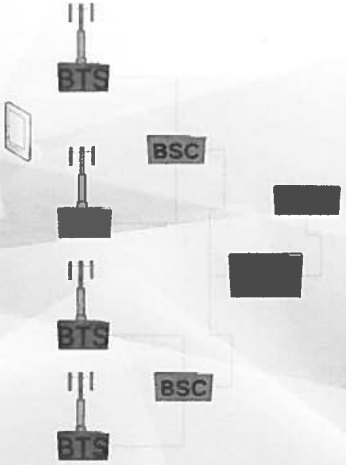
Changement de pays et de réseau :

- Les MSC/VLR et HLR sont connectés au niveau international par le réseau SS7.
- Souvent, le nouveau réseau ne peut déterminer l'ancien VLR à partir de l'ancienne localisation
- Le mobile indique donc son IMSI



Extinction du téléphone :

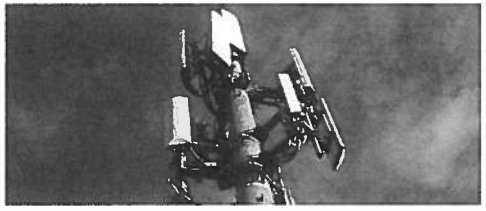
- Procédure de détachement avant l'arrêt
- Transmission au HLR de l'état du téléphone
- Abonné non joignable
- Orientation vers messagerie.



Des questions ?

CEPOL

Investigations et téléphonie mobile



Module 3
Les données opérateurs

[redacted] – CEPOL 2019

Sommaire :

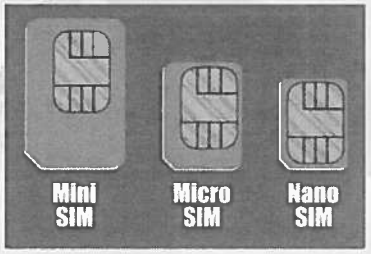
- La carte SIM et ses informations
- Le téléphone portable
- Les données opérateurs
- La navigation internet mobile
- Le réseau SS7 et le Spoof ID

La carte SIM et ses données

La carte SIM et ses données

Différents formats de cartes Subscriber Identity Module (SIM) :

- **Mini**
- **Micro**
- **Nano**
- **e-sim**



La carte SIM et ses données

- Identification de l'opérateur (logo ou nom)
- Présence d'un numéro de carte
- Ses informations sont parfois grattées par les utilisateurs.

La carte SIM et ses données

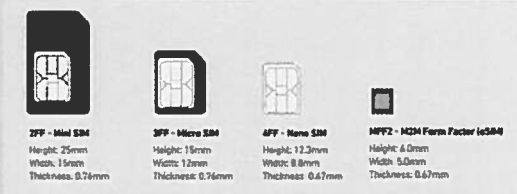
- La carte SIM est sécurisée par un code PIN (Personal Idenfication Code)
- Peut être débloquée avec le code PUK (Personal Unlock Code)

La carte SIM et ses données

- Carte SIM (2 G / 3G)
- Carte USIM (Universal Subscriber Identity Module) – 3G / 4G
- Il s'agit en fait d'une application stockée sur la puce qui authentifie l'utilisateur par son IMSI (International Mobile Subscriber Identity).

La carte SIM et ses données

- Arrivée de la e-sim : une carte SIM virtuelle qui est installée sur le téléphone (puce)
- Le Google Pixel 2 est un de premiers téléphone à l'utiliser.



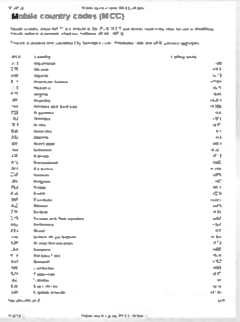
La carte SIM et ses données

- International Mobile Subscriber Identity (IMSI)
- Numéro d'authentification stocké sur la carte SIM et non connu de l'utilisateur.
- Composé de 15 chiffres

La carte SIM et ses données

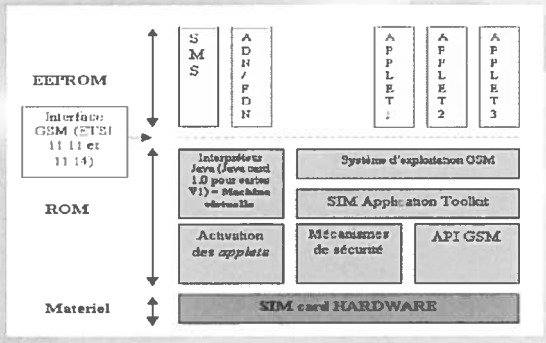
- International Mobile Subscriber Identity
- 3 chiffres : MCC (Mobile Country Code)
- 2 ou 3 chiffres : MNC (Mobile Network Code)
- 10 chiffres : MSIN (Mobile Subscriber Identification Number)

https://fr.wikipedia.org/wiki/Mobile_Network_Code
https://fr.wikipedia.org/wiki/Mobile_country_code


Mobile country codes (MCC)

La carte SIM et ses données

- L'architecture interne d'une carte SIM



Le téléphone portable

Le téléphone portable

- Différents constructeurs
- Un élément d'identification l'IMEI
- International Mobile Equipment Identity

- 14 chiffres + 1 chiffre

Le téléphone portable

- International Mobile Equipment Identity (IMEI)
- 15 chiffres
- 8 chiffres TAC (Type Allocation Code)
- 6 chiffres SNR (Serial Number)

Https://imei.info

- Https://www.numberingplans.com

Le téléphone portable

- L'IMEI permet de bloquer un portable volé sur le réseau d'un opérateur (EiR)
- Intéresse l'enquêteur pour déterminer le type de téléphone utilisé.
- Il existe des solutions pour reprogrammer l'IMEI d'un téléphone (MTK Tools).

Le téléphone portable

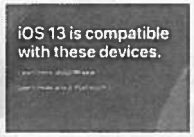
Les adresses de connexions sans fil :

- MAC Adresse

  Journal de connexions cybercafe - Macvendors.com
- Bluetooth Adresse
- Peuvent intéresser l'enquêteur en cas de connexions sur un hotspot/appairage périphérique (exemple log de hotspot).

Le téléphone portable

- Chaque téléphone est doté d'un système d'exploitation :
- Apple iOS
- Google Android



Le téléphone portable

Les comptes utilisateurs :

- Apple iD
- Compte Android

- Peuvent intéresser l'enquêteur pour identifier le téléphone associé à une adresse mail / applications achetées / différents appareils associés...

Le téléphone portable

L'exemple de Google Account

https://myaccount.google.com

Le téléphone portable

Sans oublier les informations GPS !

L'exemple de Periscope

- https://www.periscope.tv/w/1YpKkvALAbVxj?channel=travel-world-new
- https://api.periscope.tv/api/v2/getBroadcastPublic?token=1YpKkvALAbVxj

Le téléphone portable

Sans oublier les informations GPS !

Onemilliontweetmap.com

Les données opérateurs

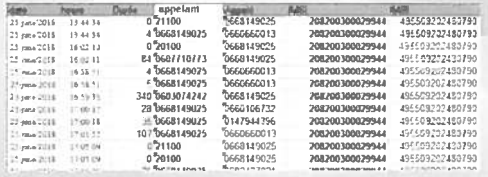
Les données opérateurs

En France, existence d'un référentiel « telecom » :

- Des prestations pour les services généraux
- Des prestations particulières pour les services spécialisés

Les données opérateurs

- Les informations clients « identité, moyens paiement, coordonnées »…
- Les données techniques : FADET ; Bornages, Fadet de Bornes, extinctions des portables, reboot, portables non communiquants sur zone…
- Présentation du référentiel



date	heure	Durée	appelant	Numéro	IMEI	IMSI
23 janv 2018	13 44 34		0 21100	0668149025	208200300029944	495509223480790
23 janv 2018	13 44 34		4 0668149025	0660660013	208200300029944	495509223480790
23 janv 2018	16 02 13		0 20100	0668149025	208200300029944	495509223480790
25 mars 2018	16 02 11		84 0687710773	0668149025	208200300029944	495509223480790
25 mars 2018	16 55 41		4 0668149025	0660660013	208200300029944	495509223480790
25 janv 2018	16 58 51		4 0668149025	0660660013	208200300029944	495509223480790
23 janv 2018	16 59 35		340 0603074242	0668149025	208200300029944	495509223480790
23 janv 2018	17 00 17		28 0668149025	0660106732	208200300029944	495509223480790
23 janv 2018	17 00 18		35 0668149025	0147544796	208200300029944	495509223480790
25 mars 2018	17 01 55		107 0668149025	0660660013	208200300029944	495509223480790
25 janv 2018	17 07 09		0 21100	0668149025	208200300029944	495509223480790
25 janv 2018	17 07 09		0 20100	0668149025	208200300029944	495509223480790

Les données opérateurs

	Prestations concernant les Mobiles et les Abonnés	
MA01	Identification instantanée, en masse, d'abonnés à partir de leur numéro d'appel.	Auto
MA02	Identification instantanée, à l'unité, d'un abonné à partir de son numéro d'appel.	Auto → Man
MA03	Identification instantanée avec coordonnées bancaires, en masse, d'abonnés à partir de leur numéro d'appel.	Auto
MA04	Identification instantanée avec coordonnées bancaires, à l'unité, d'un abonné à partir de son numéro d'appel.	Auto → Man
MA05	Identification instantanée, en masse, d'abonnés à partir de leur numéro de carte SIM.	Man
MA06	Identification instantanée, à l'unité, d'un abonné à partir de son numéro de carte SIM.	Man
MA07	Identification instantanée avec coordonnées bancaires, en masse, d'abonnés à partir de leur numéro de carte SIM.	Man
MA08	Identification instantanée avec coordonnées bancaires, à l'unité, d'un abonné à partir de son numéro de carte SIM.	Man
MA10	Identification instantanée, à l'unité, d'un abonné à partir de son numéro IMSI.	Auto → Man
MA21	Historique d'attribution, ou identification à une date donnée, d'un numéro d'appel.	Man
MA22	Historique d'attribution, ou identification à une date donnée, d'un numéro de carte SIM.	Man
MA23	Historique d'attribution, ou identification à une date donnée, d'un numéro IMSI.	Man
MA30	Identification d'un abonné à partir du nom, prénom ou de la raison sociale.	Man
MA31	Identification d'un abonné à partir du nom, prénom ou de la raison sociale et filtre sur d'autres critères (adresse, date de naissance).	Man

Les données opérateurs

Code	Prestation
MA40	Identification des numéros d'appel et des abonnés associés à partir des moyens de paiement utilisés.
MA41	Identification d'un abonné et de ses moyens de paiement à partir d'un numéro d'appel.
MA42	Identification d'un abonné et de ses moyens de paiement à partir d'un numéro de carte SIM.
MA50	Recherche de numéros d'appel ou identification d'un abonné à partir d'un numéro IMEI.
MA51	Recherche d'identifiants de téléphone mobile et identification d'abonné à partir d'un numéro d'appel.
MA52	Recherche d'identifiants de téléphone mobile et identification d'abonné à partir d'un numéro de carte SIM.
MA60	Identification d'un point de vente à partir d'un numéro d'appel.
MA61	Identification d'un point de vente à partir d'un numéro de carte SIM.
MA62	Identification d'un point de vente à partir d'un numéro IMSI.
MA63	Identification d'un point de vente à partir d'un numéro IMEI.
MA70	Recherche du code PUK à partir du numéro d'appel.
MA71	Recherche du code PUK à partir du numéro de carte SIM.
MA72	Identification d'un numéro court à partir de son numéro d'appel.

Les données opérateurs

Code	Prestation	Orange
	Prestations concernant les Mobiles et les Trafics	
MT10	Détail des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro d'appel.	Auto
MT11	Détail des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro de carte SIM.	Man
MT12	Détail des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro IMSI.	Auto
MT13	Détail des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro d'appel étranger en itinérance.	Auto
MT14	Détail des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro IMEI.	Auto
MT20	Détail géolocalisé des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro d'appel.	Auto
MT21	Détail géolocalisé des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro de carte SIM.	Man
MT22	Détail géolocalisé des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro IMSI.	Auto
MT23	Détail géolocalisé des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro d'appel étranger en itinérance.	Auto
MT24	Détail géolocalisé des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro IMEI.	Auto
MT30	Détail des trafics vers un numéro d'abonné étranger sur une période indivisible d'un mois.	Auto
MT40	Détail des trafics écoulés dans un relais téléphonique (cellule) sur une période de 4 heures au cours des douze derniers mois.	Auto
MT41	Détail des trafics écoulés dans un relais téléphonique (cellule) avec identification des abonnés sur une période de 4 heures au cours des douze derniers mois.	NC

Les données opérateurs

	Prestations concernant les Mobiles et les Equipements (cellules)	
ME50	Localisation d'une cellule à partir de son numéro d'identification	Auto
ME51	Carte de couverture optimale d'une cellule	Man
ME52	Carte de couverture secondaire d'une cellule	NC
ME53	Recherche de cellule à partir d'un lieu géographique (couverture optimale théorique)	Man
ME54	Recherche de cellule à partir d'un lieu géographique (couverture secondaire théorique)	NC
	Prestations concernant les Mobiles et les Documents	
MD10	Copie du contrat d'abonnement	Man
MD11	Copie des documents annexés au contrat d'abonnement	Man
MD12	Copie de factures	Man
	Prestations concernant les Fixes et les Abonnés	
FA01	Identification en nombre d'abonnés à partir de leur numéro d'appel.	Man
FA02	Identification d'un abonné à partir de son numéro d'appel.	Man
FA03	Identification en nombre d'abonnés à partir de leur numéro d'appel, avec coordonnées bancaires.	NC
FA04	Identification d'un abonné à partir de son numéro d'appel, avec coordonnées bancaires.	Man

Les données opérateurs

Code	Prestation	Orange
FA05	Recherche et identification d'un abonné appelant derrière une tête de ligne ou un serveur.	Man
FA07	Historique d'attribution d'un numéro.	Man
FA10	Identification d'un abonné à partir du nom, prénom ou de la raison sociale.	Man
FA11	Identification d'un abonné à partir du nom et prénom ou de la raison sociale et filtre sur d'autres critères (adresse, date de naissance).	Man
FA20	Identification d'un abonné à partir de l'adresse de son installation téléphonique.	Man
FA21	Identification des publiphones implantés dans une zone géographique donnée.	Man
FA30	Identification d'un point de vente à partir d'une carte prépayée.	Man
FA31	Identification d'une carte prépayée et d'un numéro appelé	Man
FA40	Recherche de numéros d'appel et identification d'un abonné à partir d'un moyen de paiement.	Man
FA41	Identification d'un abonné et de ses moyens de paiement à partir d'un numéro d'appel.	Man
FA50	Recherche d'un opérateur tiers à partir de son numéro de faisceau	Man
FA51	Identification d'un abonné ADSL et de son fournisseur d'accès internet.	Man
	Prestations concernant les Fixes et les Eléments techniques d'une ligne	
FE10	Détail des caractéristiques techniques de la ligne en vue d'une interception, demande copiable sous forme électronique	Man

Les données opérateurs

Code	Prestation	Orange
	Prestations concernant les Fixes et les Trafics	
FT10	Détail des trafics d'un abonné sur une période indivisible d'un mois, à partir/vers un numéro d'appel.	Auto
FT20	Détail des trafics en relation avec un abonné d'un opérateur étranger.	Man
FT21	Détail des données relatives au trafic d'un abonné avec un serveur.	NC
FT30	Détail des trafics d'une interception sans HI2	Man
FT40	Détail des données relatives au trafic d'une carte prépayée.	Man
	Prestations concernant les Fixes et les Documents	
FD10	Copie du contrat d'abonnement	Man
FD11	Copie des documents annexés au contrat d'abonnement	Man
FD12	Copie de factures	Man
	Prestations concernant le Web (internet) et les Abonnés	
WA01	Identification d'abonné internet à partir d'une adresse IP	Man
WA07	Identification d'abonné internet à partir de caractéristiques de compte	Man
WA08	Identification d'abonné internet à partir d'une adresse courriel	Man
WA09	Identification d'abonné internet à partir d'une URL de site visité	Man

Les données opérateurs

Code	Prestation	Orange
	Prestations concernant le Web (internet) et les Documents	
WD10	Copie du contrat d'abonnement internet	Man
WD11	Copie des documents annexés au contrat d'abonnement internet	Man
WD12	Copie de factures d'abonnement internet	Man
	Prestations concernant les Mobiles et les Interceptions	
MI20	Interception des communications d'un abonné téléphonie mobile et IRI	Man
	Prestations concernant les Fixes et les Interceptions	
FI20	Interception des communications d'un abonné téléphonie fixe	Estimation
	Prestations concernant le Web (internet) et les Interceptions	
WI01	Interception du trafic DATA/IP émis et à destination de l'accès internet	Man
	Prestations concernant les Fixes (TOIP) et les Interceptions	
FI23	Interception des communications de téléphonie sur IP d'un abonné et IRI	Man
	Prestations concernant les Fixes internationaux et les Interceptions	
FI27	Interception internationale	Man

Les données opérateurs

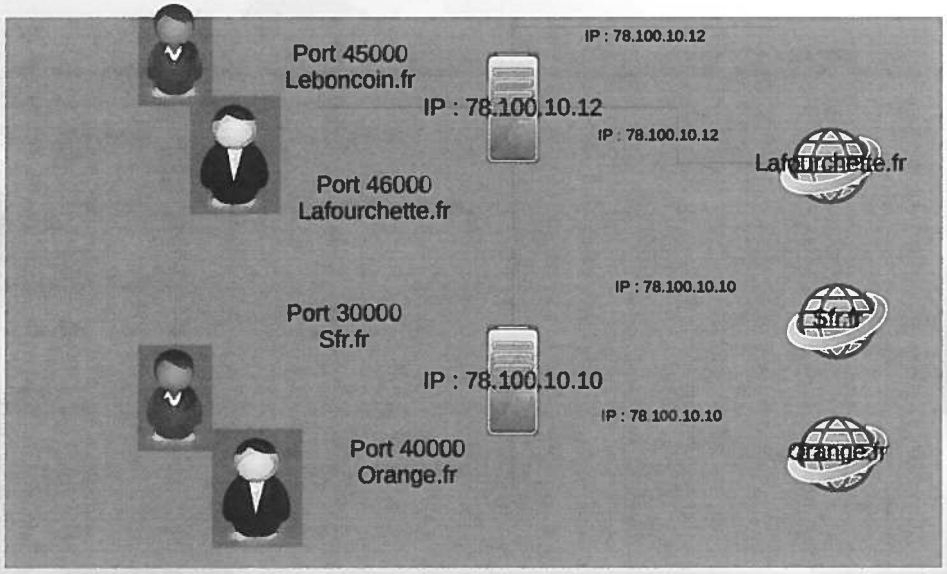
Code	Prestation
	Prestations autres
ARRET	Arrêt anticipé d'une interception
REPORT	Prolongation d'une interception
HREF	Prestation Hors REFérentiel

La navigation internet mobile

La navigation internet

- Les opérateurs utilisent des passerelles de sortie internet avec des adresses IP spécifiques.
- Tout le trafic « clients » passe par plusieurs passerelles IP des différents opérateurs.
- Chaque client se voit attribuer un port pour le transfert des données (65535 ports)

La navigation internet

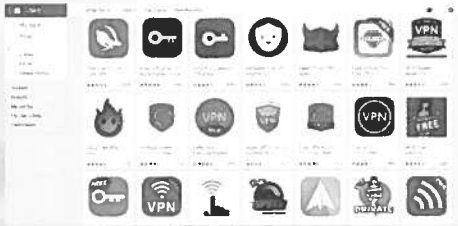


La navigation internet

- Pour identifier un client « internet » il est donc important pour l'opérateur de connaître le port attribué à l'usager
- Possibilité sinon de fournir les données d'une période, à charge pour l'enquêteur de trouver l'identité du client.

La navigation internet

- Attention aux VPN



- Les utilisateurs peuvent également se servir de ORBOT

  Vidéo démo orbot/telegram

Le réseau SS7 et le spoof-iD

Le réseau SS7

- Signalisation Sémaphore 7
- Permet de faire transiter les communications et la signalisation de façon séparée.
- Date des années 80, sécurisation faible, serait utilisé par la NSA pour la géolocalisation

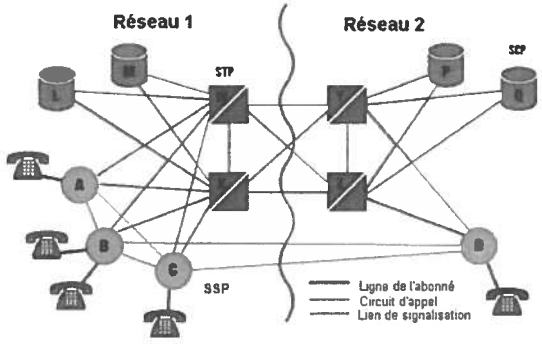
Le réseau SS7

- Chaque opérateur possède son propre réseau SS7 auquel sont reliés des commutateurs téléphoniques et des bases de données.
- Un réseau SS7 international interconnecte les différents opérateurs par l'intermédiaire de passerelles.

Le réseau SS7

SCP : Service Control Point
STP : Signal Transfert Point

Architecture SS7



Le réseau SS7

- Un rapport du Departement of Homeland Security américain prévient que le réseau SS7 est vulnérable (avril 2017).
- À l'écoute électronique (voix, messages)
- Géolocalisation
- Déni de service
- Fraudes

Le réseau SS7

- Selon le homeland security, ces failles peuvent être exploitées par des criminels, des terroristes ou des états étrangers.

Le spoof-ID

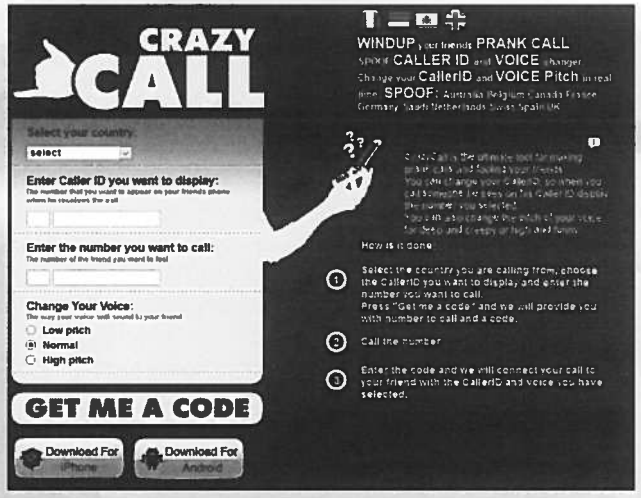
- Le « Spoof-id » ou l'usurpation d'identité.
- Une technique qui peut compliquer les investigations policières.
- Permet d'afficher le numéro qu'on désire au destinataire (Swatting).

Le spoof-ID

- La principale technique est d'utiliser la VoiP/SIP.
- Impact sur les FADETS opérateurs.
- Impact sur les répondeurs téléphoniques.

Le spoof-ID

- Exemple de site



Le spoof-ID

- Un cas français : Gregory CHELLI Aka ULCAN
- Spécialiste du « viol vocal »
- Diffuse sur youtube ses exploits

- Contacte les services de police pour demander des infos en usurpant d'autres numéros de services.

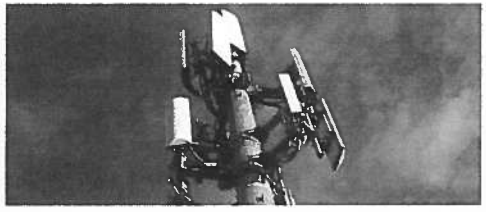
Le spoof-ID

- En cas de doute, il faut faire les FADETS des deux numéros.
- Difficile souvent de déterminer le site utilisé pour le Spoof-id.
- Ces sites sont souvent payants « Follow the money ».

Des questions ?

CEPOL

Investigations et téléphonie mobile



Module 4
L'analyse des données opérateurs

CEPOL 2019

Sommaire :

- Tableurs (Excel, Calc)
- Logiciel d'analyse générique (ANB)
- Logiciel d'analyse dédié Mercure v4

Les tableurs (Excel, Calc)

Les tableurs (Excel et Calc)

L'exploitation des données téléphoniques des opérateurs est une activité particulière.

- Il n'y a pas de logiciel gratuit purement destiné à cet effet.
- Les concepteurs de logiciels n'ont pas accès aux données des opérateurs.

Les tableurs (Excel et Calc)

Il est tout à fait possible de faire de l'exploitation de FADET à l'aide de logiciels bureautiques de type « tableurs » :

- Microsoft Excel
- LibreOffice Calc

- Ou d'utiliser des logiciels de gestion de bases de données (Access, SQL...)

Les tableurs (Excel et Calc)

Avantages :

Gratuit

Formation bureautique

Inconvenients :

Peu flexible

multi-traitements plus difficiles

Les tableurs (Excel et Calc)

tableau dynamique - calc

	A	B	C	D
1	abonné	Type appel	Correspondant	Compter - dat
2	0622256741	Emis	0139397187	1
3			0171660510	1
4			0610301950	1
5			0617073736	1
6			0617927572	2
7			0624254968	6
8			0627632472	3
9			0664502374	1
10			0666890099	2
11			0671933287	2
12			0672299121	3
13			0698921350	1
14			0699068328	2
15			2162106754	1
16		Message ecrit emis	0624254968	1
17				1
18		Message ecrit reçu		10
19		Rappel automatique		8
20		Reçu	0240595140	1
21			0615364858	2
22			0616957865	1
23			0617073736	1
24			0624254968	2
25			0666890099	6
26			0671933287	5
27			0673925289	1
28			0699068328	1
29		Répondeur		18
30	Total Resultat			87

Un logiciel d'analyse générique (ANB)

Un logiciel d'analyse générique (ANB)

- Analyst NoteBook est un logiciel commercial de la société IBM.
- Il permet d'effectuer des recoupements avec n'importe quel type de données : financières, téléphoniques, informatiques.

Analyst Notebook

Avantages :

Puissance du logiciel

capacités de traitement (personne, telephone, argent)

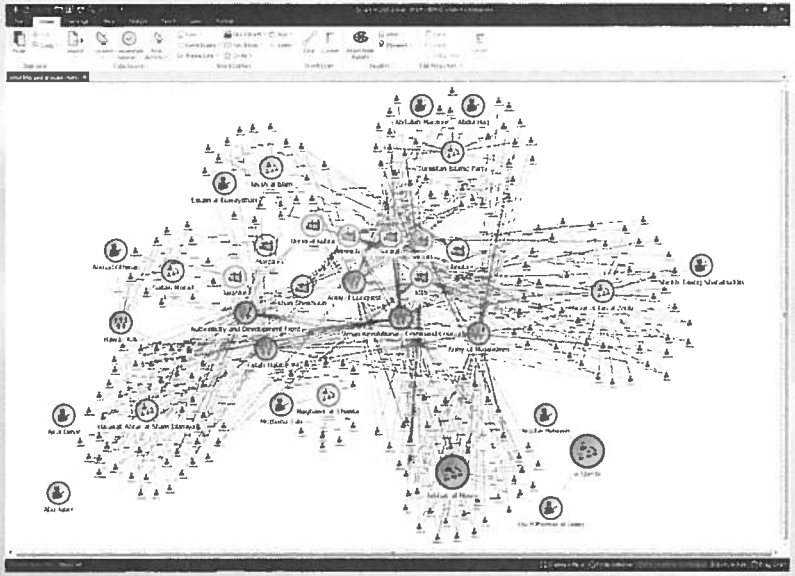
Inconvenients :

Payant

Formation longue durée

Doit être manié par un analyste expérimenté

Un logiciel d'analyse générique (ANB)



Un logiciel d'analyse dédié (Mercure v4)

Logiciel d'analyse dédié (Mercure v4)

- Logiciel payant de la société Ockham
- Spécifiquement dédié à la gestion des données des opérateurs de téléphonie.

Mercure V4

Avantages :

capacités de traitement dédié à la téléphonie

Formation de courte durée 2 niveaux

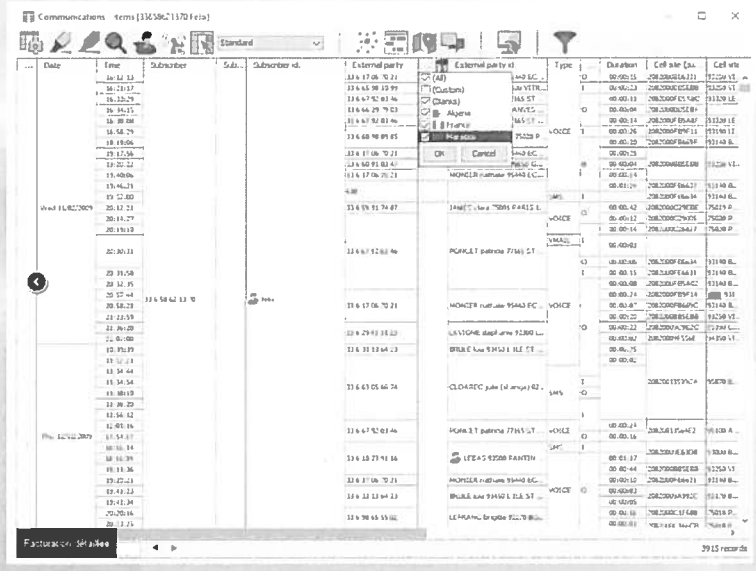
accessible pour les enquêteurs

Peut être utilisé en mono-poste ou réseau

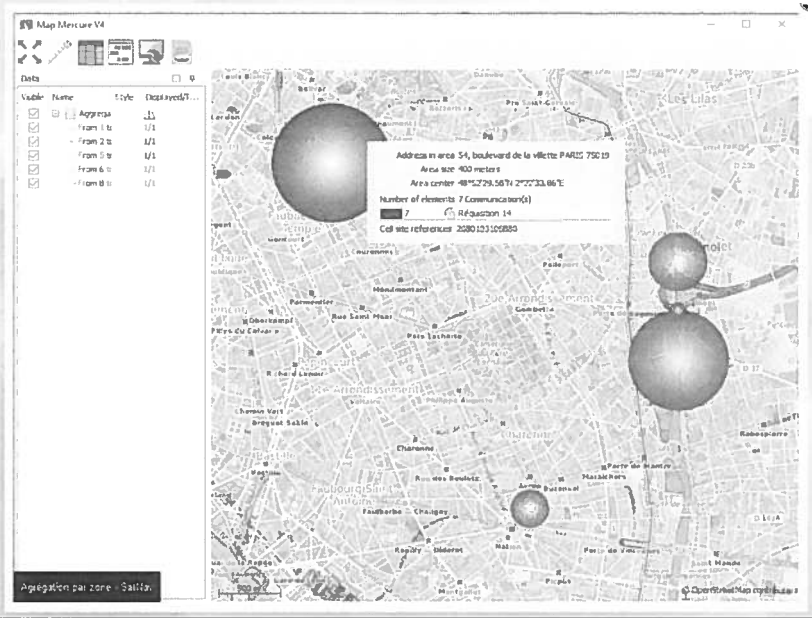
Inconvenients :

Payant

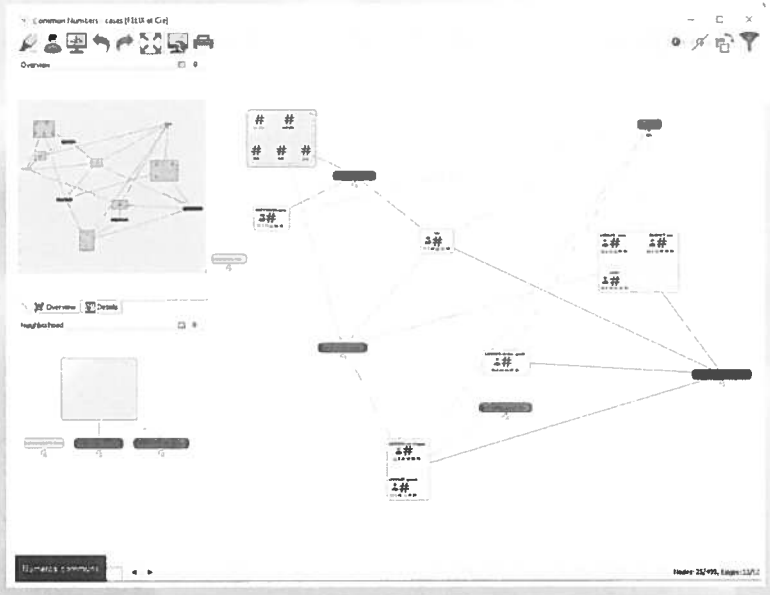
Logiciel d'analyse dédié (Mercure v4)



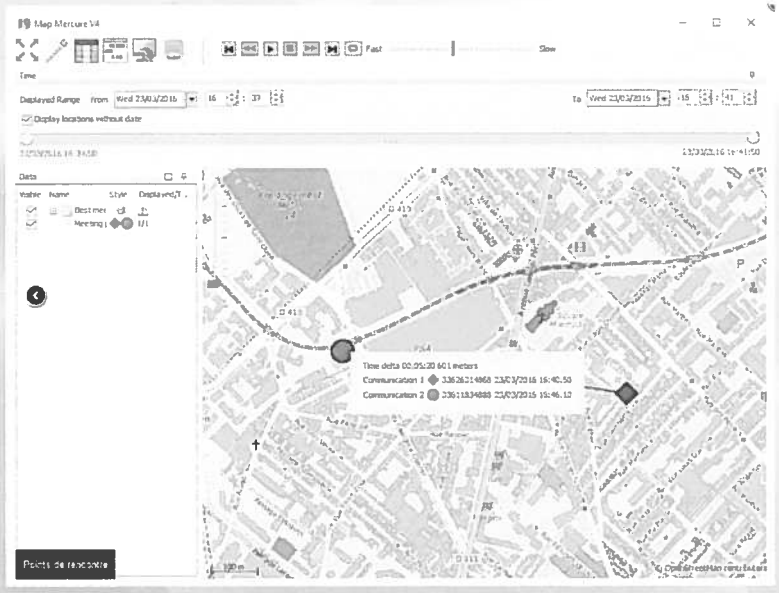
Logiciel d'analyse dédié (Mercure v4)



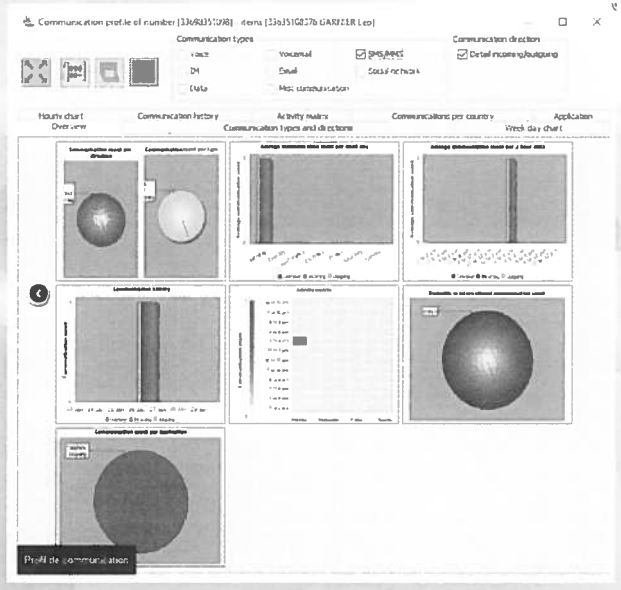
Logiciel d'analyse dédié (Mercure v4)



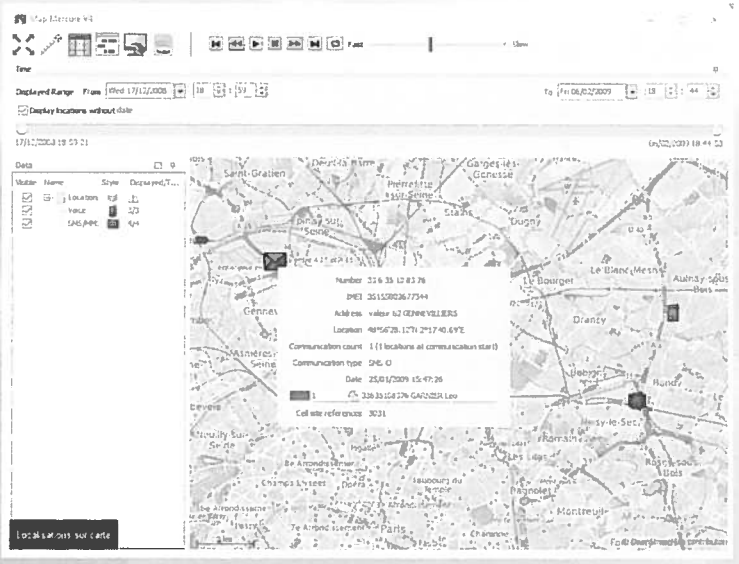
Logiciel d'analyse dédié (Mercure v4)



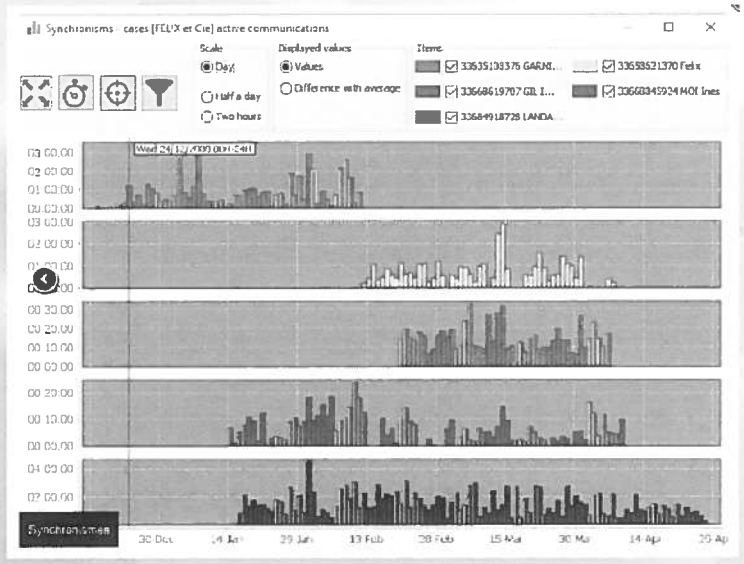
Logiciel d'analyse dédié (Mercure v4)



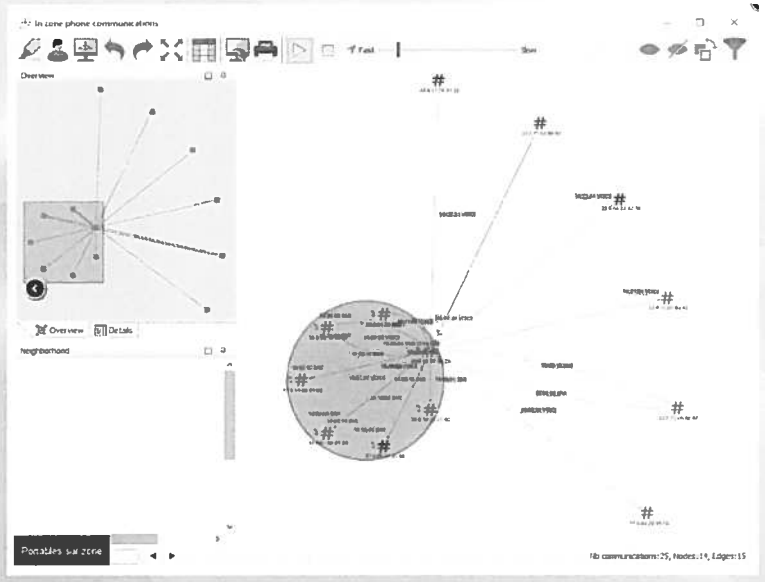
Logiciel d'analyse dédié (Mercure v4)



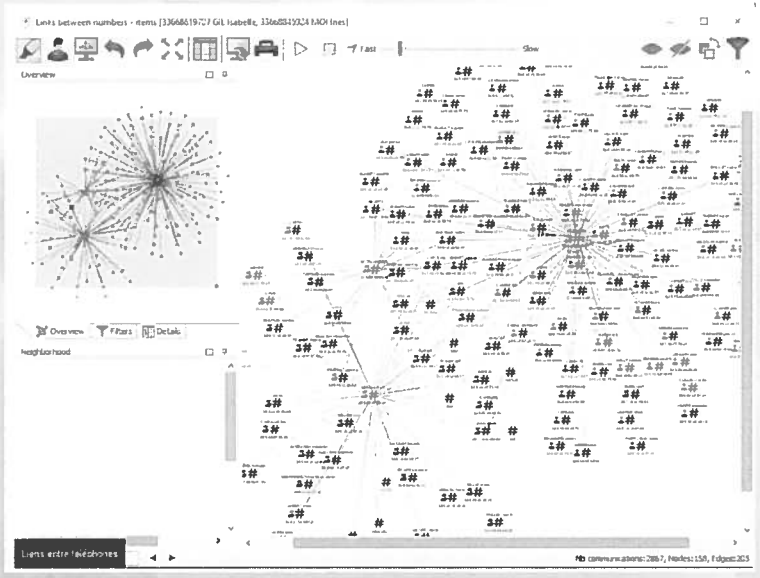
Logiciel d'analyse dédié (Mercure v4)



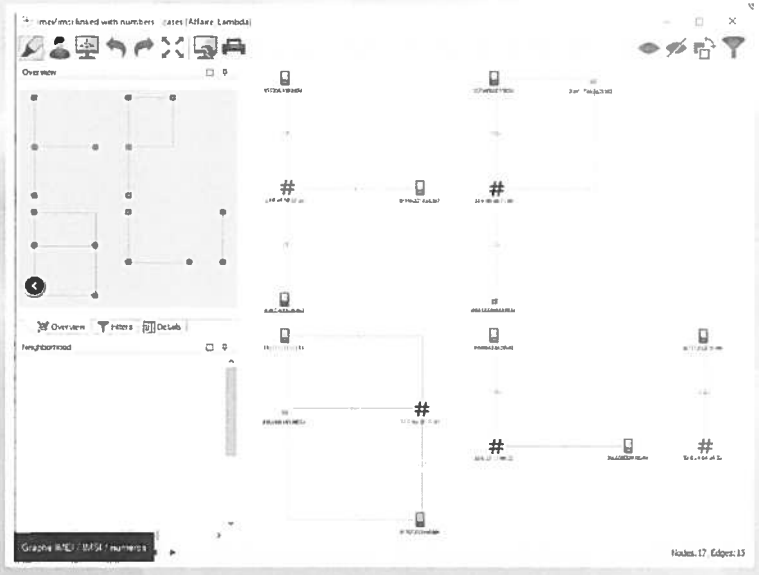
Logiciel d'analyse dédié (Mercure v4)



Logiciel d'analyse dédié (Mercure v4)

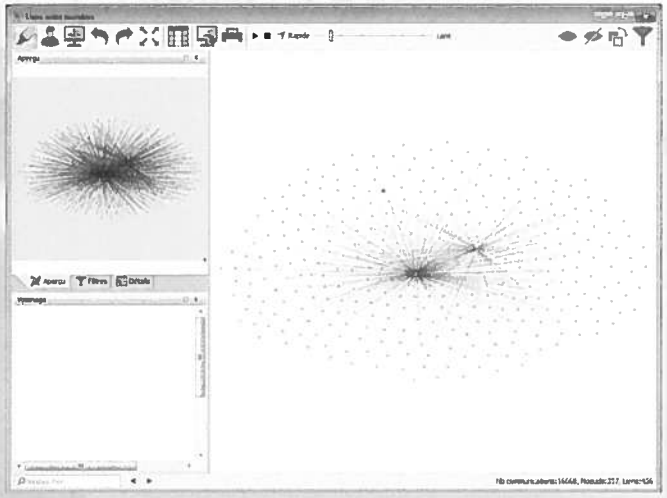


Logiciel d'analyse dédié (Mercure v4)



Logiciel d'analyse dédié (Mercure v4)

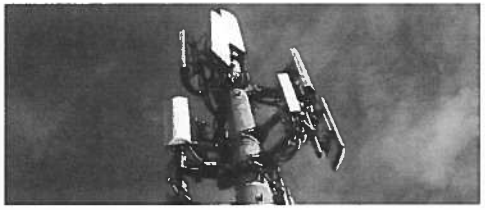
Démonstration Mercure V4



Des questions ?

CEPOL

Investigations et téléphonie mobile



Module 5
L'exploitation des téléphones

[redacted] CEPOL 2019

Sommaire :

- Les exploitations technico-légales
- Les saisies sur site
- L'extraction des données

Les exploitations technico-légales

Les exploitations technico-légales

- « Digital Forensics » : identifier, collecter, examiner et analyser les données en préservant l'intégrité.
- « Mobile Forensics » (téléphones, montres, drones, autos)...

Les exploitations technico-légales

- Désormais un téléphone est plus qu'un simple outil.
- Masse de données : appels, contacts, SMS, photos, historique internet, notes, calendrier, mots de passe, géolocalisation, données des applications, messages systèmes, journaux applications et tous les éléments effacés...

Les exploitations technico-légales

- Le succès de l'opération tient aux bonnes pratiques d'examen.
- La saisie d'un appareil est prévue par les lois nationales ou les procédures policières.
- L'examen d'un appareil mobile demande de la préparation (formations) et du matériel.

Les saisies sur site

Les saisies sur site

- Avant de procéder aux saisies, il faut s'assurer d'avoir le droit de saisir les preuves (CR…)
- La scène de crime doit être sécurisée
- L'équipement de protection adapté est utilisé

Les saisies sur site

- Reconnaitre, identifier, saisir et sécuriser les éléments numériques de la scène.
- Documenter et spécifier les emplacements de découvertes des appareils.
- Collecter, étiqueter et préserver les preuves.
- Emballer et transporter les éléments de manière sûre (sacs faraday, cartons).

Les saisies sur site

- Respecter la « chain of custody »
- Il s'agit du traçage qui indique qui détient la preuve, qui a été en charge de son exploitation et quelles actions ont été entreprises.

Les saisies sur site

- Lors de la saisie d'un téléphone, il est possible de le mettre en mode avion pour éviter les disparitions de preuves (cloud, effacement à distance).

- Cette manœuvre doit être documentée dans le process.

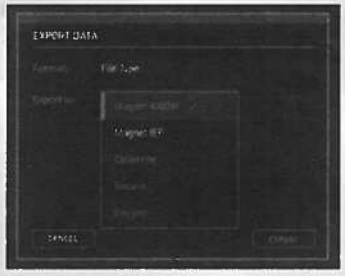
L'extraction des données

L'extraction des données

- Peut être réalisée avec des outils comme Magnet Acquire

  https://www.magnetforensics.com

- Limite de l'extraction



L'extraction des données

- Pour extraire les données d'un téléphone portable, il est possible d'utiliser des équipements spécifiques :

- UFED de Cellebrite / Xry de Msab

L'extraction des données

Démonstration Reader (on ne nous dit pas tout)

Des questions ?