Annex 8: CEPOL Morocco

Project funded by the European Union

CEPOL EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

EU/Maroc - Partenariat Contre-Terrorisme

Activité résidentielle

Recueillir les informations dans CT par Internet

DGSN

Hôtel Ibis Agdal Rabat, Maroc

Lundi 10 Juin – Vendredi 14 Juin 2019

Le contenu de ces sessions a été développé dans le respect de la loi et des droits fondamentaux

CEPOL: [redacted]

Experts: [redacted]

Dimanche 9 Juin

Arrivée de la délégation des experts CEPOL, suivant différents itinéraires et horaires.

Lundi 10 juin

9:00 – 9:30	Cérémonie d'ouverture
9:30 – 10:45	Etats des lieux sur la cybercriminalité
10:45 – 11:00	Pause
11:00 – 12:00	Perspective de l'UE sur la collecte d'informations à partir d'Internet
12:00 – 13:00	Déjeuner
13:00 – 14:45	Le renforcement des capacités d'investigation numérique -Définition d'un projet « laboratoire » -objectifs et contraintes -Normes ISO et certification Relations entre acteurs nationaux et internationaux – pyramidage et pilotage Maintien en condition opérationnelle et évolution de domaine de compétence
14:45 - 15:00	Pause
15:00 - 16:00	Présentation et Installation du poste de travail OSINT : Firefox and plugins Tor-Browser Gephi+java Python3 et Twint
16:00	Fin

Mardi – 11 Juin 2019

9:00 – 9:45	Investigations sur Twitter : Utilisation de DMI-TCAT et Gephi Twitter-stream pour le monitoring les tweets en temps réel. Création de clef d'API et paramétrage de l'app
9:45 – 10:45	Exercice cas 1 pratique sur Twitter : Collecte automatisée Extraction et analyse grâce à DMI-TCAT et Gephi, sous forme de graphe Notion de Social network Analysis, intérêt des algorithmes pour l'analyse.
10:45 – 11:00	Pause
11:00 – 12:00	Exercice cas 2 (CT) pratique sur Twitter : Collecte automatisée grâce à Twint. Visualisation et Analyse des données
12:00 – 13:00	Déjeuner
13:00 – 14:45	Formation Télécommunication - Intérêt de la téléphonie dans le CT (appels mais aussi financement) - Généralités sur la téléphonie - Architecture physique d'un réseau GSM
14:45 - 15:00	Pause
15:00 - 16:00	Formation Télécommunication - Les données de l'opérateur (Fadet, bornages, extinction, reboot, portables non communicants) - Le réseau SS7 et le Spoof Id - La navigation internet et les ports de communications - La carte SIM et ses informations - Le telephone portable (IMEI, android Id, Mac address...) - Recherches opensource - Les comptes utilisateurs (android Gmail, Apple id...)
16:00	Fin

Mercredi 12 Juin

9:00 – 9:45	Investigations sur Facebook – Présentation et utilisation avancée du FB-Graph
10:00 – 10:45	Cas pratique Facebook : extraction automatique des liens d'amitié sur un profil. Construction d'une matrice relationnelle sous Libreoffice. Injection des données dans Gephi.
10:45 – 11:00	Pause
11:00 – 11:45	Cas pratique Facebook (part 2) : extraction automatique des liens d'amitié sur un profil. Construction d'une matrice relationnelle sous Libreoffice. Injection des données dans Gephi.
11:45 – 13:00	Déjeuner
13:00 – 13:45	Aller plus loin sur Facebook :

	Reverse imaging Analyse de profil Identification mail et téléphones.
13:45 – 14:45	Formation Télécommunication (4) L'analyse des données opérateurs (excel , ANB, Mercure)
14:45 - 15:00	Pause
15:00 - 16:00	Formation Télécommunication (5) - Précautions à prendre lors d'une saisie de téléphone - L'exploitation des données du telephone - Xry/Ufed
16:00	Fin

Jeudi 13 Juin

9:00 – 9:45	Techniques d'identification de comptes et pseudo sur Internet. Social Hacking.
10:00-10:45	De l'information à la preuve - Les fondamentaux de la preuve numérique - Les acteurs (experts, spécialistes police,…) - La communication de preuve numérique au niveau international (accès, format, transport, projet EU EVIDENCE
10:45 – 11:00	Pause
11:00 – 12:00	De l'information à la preuve - Les données stockées à distance - la collecte (données publiques, données accessibles via réquisition, techniques spéciales d'enquête) - le traitement (croisement de données, données à caractère personnel)
12:00 – 13:00	Déjeuner
13:00 – 13:45	De l'information à la prevue – données continues dans un support numérique - la collecte (perquisitions, saisies, copies, blocage en écriture) - le traitement (problématiques de volume, de chiffrement, de stockage, de croisement de données) - méthodologies de discrimination et analyses par étapes
14:00 – 14:45	De l'information à la preuve – le live forensics - objectifs (capture de RAM, lutte contre le chiffrement, stockage à distance,…) - outils (First, OSTriage, Darwin,..) - méthodologie (discrimination et préservation de l'intégrité de la preuve)
14:45 - 15:00	Pause
15:00 - 16:00	De l'information à la preuve – Le compte rendu d'analyse - Du compte rendu oral au rapport d'expertise - Caractéristiques fondamentales d'un rapport d'exploitation
16:00	Fin

Vendredi 14 Juin

9:00 – 10:30	De l'information à la preuve – Le témoignage du spécialiste numérique au procès pénal -contexte et acteurs du procès - se présenter - défendre une expertise -les attaques courantes
10:30 – 10:45	Pause
10:45 – 11:00	Evaluation
11:00 – 12:00	Remise des certificats
12:30	Fin

Liste des participants

N	Nom et Prénom	Grade	Service/ville
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

Recherches Internet - UE

—

[redacted]

Perspective de l'UE sur la collecte d'informations sur Internet

OSint ou RoSO?

Quelques éléments

Pour savoir de quoi on parle....

- OSIF
- Pas uniquement internet (presse, édition...)
- Information librement accessible
- Pas de stratagème pour l'obtenir

Applications

En matière de terrorisme ou de crimes contre l'humanité...

- Le Mandat d'arrêt CPI Werfalli (Libye) - Bellingcat

- Exemple en juridiction - Dossier Sheddadi.

Difficultés

Il y en a...

- Sécurité (Virus, Manipulation...)
- Juridiques (qques jurisprudences...)
- Technique (ToS, volumétrie des data)
- Ethique (Fichiers, data de tiers...)

Etat des lieux dans l'UE

Régime Juridique

Trois grandes tendances qui cohabitent au sein de l'UE

- Régime totalement contrôlé (ex : Portugal)
- Régime différenciation ponctuel/habituel (ex Belgique)
- Régime "Open-Bar" (France, Finlande, etc...)

Action de l'UE

Rôle normatif et de protection

Deux exemples parmi d'autres....

- RGPD (GDPR)(1016/679)

  Conséquences sur l'OSint (databreach, whois....)

- E-evidence (*Cloud Act EU*)

  Conséquences notamment sur l'accès au contenu des réseaux sociaux...

Rôle Formation et coopération

Trois exemples...

- CEPOL (Formation)
- EUROPOL (Opérationnel)
- ENLETS (Réseau prospective, échanges et bonnes pratiques)

En conclusion...

Contexte important

Internet est notre assistant personnel...

- Accès à la preuve

  Conflits longue distance, temporalité

- Risque de disparition de la preuve

  Transfert de charge des Etats vers les plateformes pour la suppression du contenu

Investigations sur Twitter - Temps réel

—

[redacted]

LinkedIn is for the people you know.
Facebook is for the people you used to know.
Twitter is for people you want to know.

~ Inconnu

Twitter...

Twitter

Quelques chiffres et notions...

- 500 millions de tweets sont publiés chaque jour (5.787t/s)
- 326 millions de personnes utilisent Twitter chaque mois
- Réseau asymétrique
- Terrorisme et désinformation
- "Réseau de l'instant"

Twitter

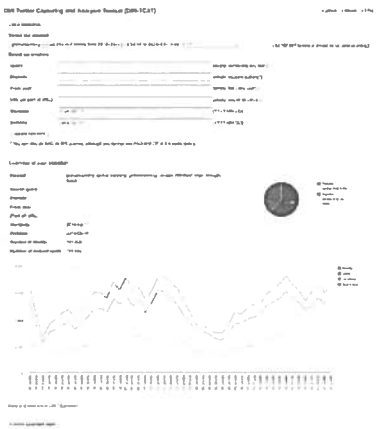
Aspects techniques

- Une API très documentée...
- ... mais avec ses limites...
- Beaucoup d'outils disponibles
- Beaucoup de bibliothèques
- Mon choix : deux outils libres, gratuits et très efficaces pour le monitoring temps réel : DMI-TCAT et Gephi

Monitoring temps réel

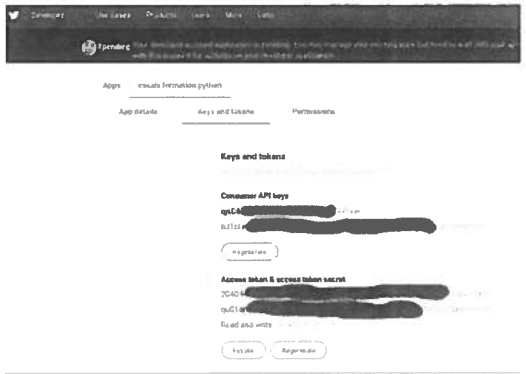
Monitoring en temps réel

1. Possible via l'API de Twitter
2. Pratique si on veut suivre un événement prévu
3. Suivi par hashtag, mot-clefs, utilisateurs
4. Rendu sous forme de base de données et de graphes
5. Attention : ne fait pas le passé!



Etape UN - clef d'API

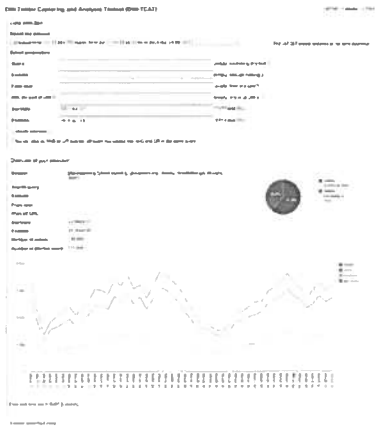
1. Créer un compte développeur Twitter
2. Prévoir un email et un numéro de gsm
3. Récupérer keys et token
4. Attention : Twitter est devenu pénible avec les comptes développeurs pour cause de bot russes...



Installation de DMI-TCAT...

DMI-TCAT

1. Installation en une ligne de commande sous linux
2. Architecture Client/Serveur : Un serveur de collecte, un serveur de requête
3. Suivi par hashtag, mot-clefs, ou utilisateurs
4. Conseils d'utilisation et utilisation



Installation de Twitter Streaming Importer pour Gephi...

Twitter Streaming Importer

1. Un plugin pour Gephi
2. Collecte et analyse en temps réel
3. Suivi par hashtag, mot-clefs, ou utilisateurs
4. Conseils d'utilisation et installation

Intérêt des outils de SNA

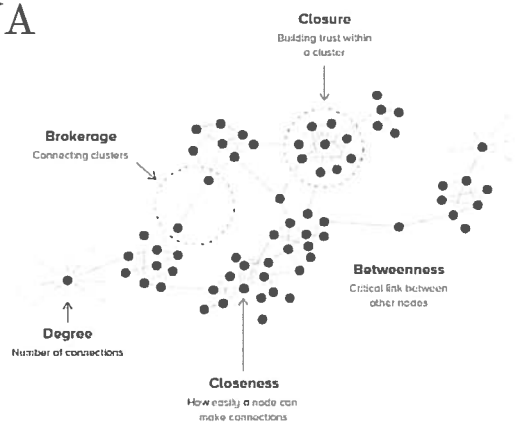
Les unités de mesures quantitatives ne sont pas forcément les plus pertinentes...

L'intérêt d'une analyse est d'identifier rapidement des acteurs-clefs : Auteur initial, influenceurs, etc....

Certains concepts de la SNA sont à connaître et vous seront utiles...

- La modularité
- La centralité intermédiaire

Elles permettent de dégager rapidement des tendances et des éléments marquants.



Conclusion

Le monitoring en temps réel efficace de Twitter est possible gratuitement à l'aide d'outils open-source.

L'Analyse des Réseaux Sociaux (SNA) permet quant à elle de s'affranchir des biais traditionnels de l'approche volumétrique de l'analyse en améliorant la précision des *metrics*.

Le plus difficile reste juste... à obtenir une clef d'API!

Investigations sur Twitter -
Retour vers le futur
—
[redacted]

Comment étudier
le passé sur
Twitter?

L'expérience

Question

Qui est le premier média à avoir donné le nom du terroriste de l'attentat de Nice? Quand et à quelle heure?

- Articles modifiés en temps réel
- Beaucoup de tweets (>17.000)
- Besoin d'archivage
- Besoin d'exhaustivité et de preuve
- Solution : Twint

Twint

Un scraper et une bibliothèque python qui se passe de l'API

- Facile à installer et très rapide
- Pas de limite de temps
- Fonctions de recherche avancées
- Extensible et intégrable
- Archivage

Installation et usage

Installation en une ligne de commande...

pip3 install --upgrade -e git+https://github.com/twintproject/twint.git@origin/master#egg=twint

Usage simple....

- Syntaxe claire
- Export dans divers formats (csv, json, sql...)
- Utilisable via TOR

Exemples d'utilisation

A vous de jouer...

Quelques exemples

Géolocalisés

Chercher des tweets sur l'EI, dans un rayon de 20km autour de Rabat.

Temporalisés

Complexifier la requête en limitant la période à septembre/décembre 2016

Exemple de Nice

Résoudre la question initiale sur Mohamed Lahouej Bouhlel.

Que faire des data?

Conclusion

Twint est un outil indispensable lors d'une enquête judiciaire.

Il permet de :

- S'affranchir des contraintes de temps et des limitations de l'API.
- Préserver et archiver la preuve
- Gagner du temps
- S'ouvrir des possibilités d'analyse statistiques complémentaires.

OSINT - Préparation du poste de travail

—

[redacted]

Objectif : travailler confortablement et efficacement...

Le navigateur

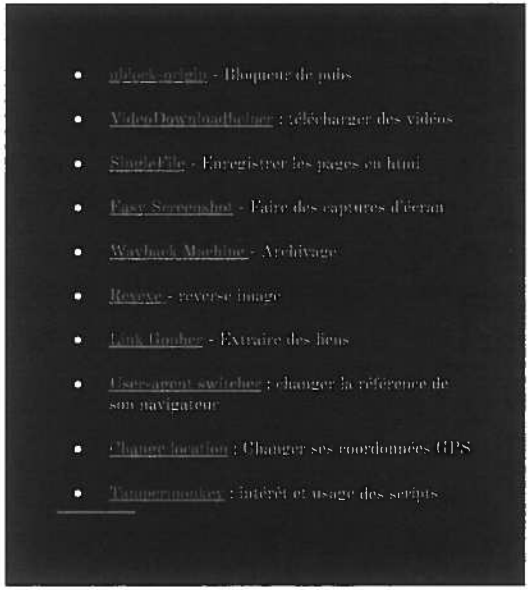
Firefox

Le bon choix de navigateur !

- Libre et gratuit
- Rapide
- Modulaire et extensible
- Mis à jour régulièrement
- Respect de la vie privée

Firefox

Des plugins très utiles...



Autres Outils....

1. GoogleEarth : géolocalisation
2. Hugin : création de panoramas
3. Python3 : langage de programmation
4. TOR Browser : un peu d'anonymat
5. Gephi : analyse de graphes

Cette liste n'est pas exhaustive!...

Les accessoires...
Indispensables!

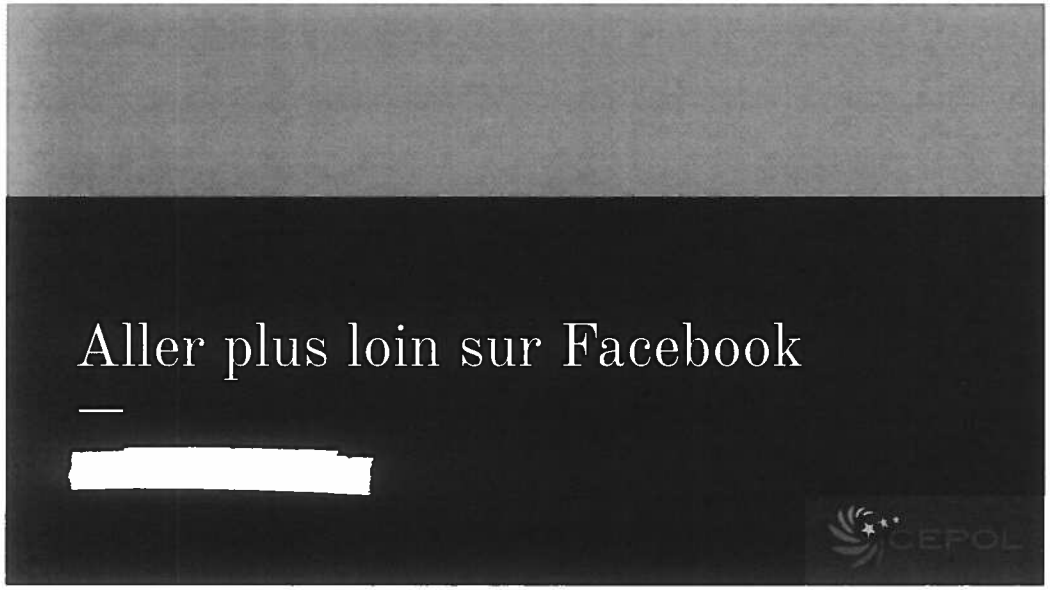
Commencez une
double vie...

Autres Outils....

1. Un ou plusieurs burner-phones
2. Un VPN avec plusieurs points de sortie
3. Des comptes sur les réseaux sociaux
4. Des adresses mails
5. Un bloc-note et des crayons!
6. de la curiosité et de la patience!

Conclusion

- Pas besoin de beaucoup d'argent pour faire de l'OSINT!
- Bien préparer son poste de travail permet de gagner du temps!



Facebook,
helping stalkers
since 2004.

Facebook en chiffres

Facebook

Le premier réseau social.
(Des vieux...)

- 2,234 milliards d'utilisateurs actifs par mois
- 1,49 milliard d'utilisateurs actifs quotidiens
- Un moteur de recherches : le GRAPH
- Population qui vieillit
- Contrôle très fort des publications

Le Graph Facebook

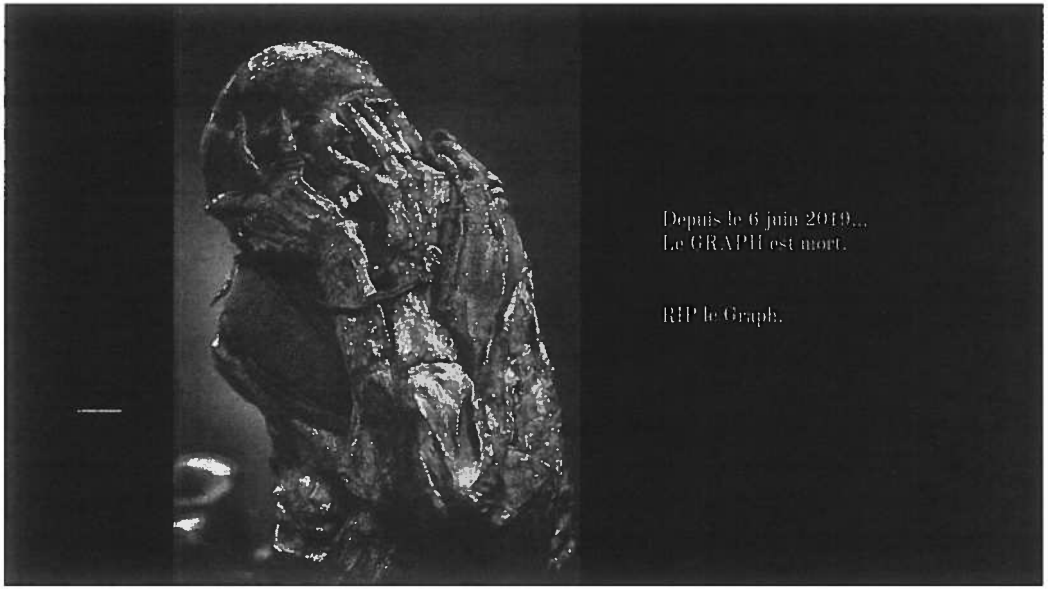
Quelques prérequis...

Un profil fake en anglais...

- Un profil fake est un bien précieux
- Il faut l'entretenir, comme une orchidée
- VPN oui mais tard. TOR? bof.
- Il faut le paramétrer en anglais
- Attention : on travaille en sources ouvertes, on ne devient pas amis avec sa cible.
- On ne travaille pas avec son compte personnel. Jamais.

Une syntaxe particulière...

- en Anglais simplifié
- via des opérateurs
- un guide important : Paul Myers
- Des applications pour vous aider :
  - Stalkscan
  - Whopostedwhat
  - PeopleFind Thor
  - Facebook Matrix



Quelques prérequis...

Un profil fake en anglais...

- Un profil fake est un bien précieux
- Il faut l'entretenir, comme une orchidée
- VPN oui mais tard. TOR? bof.
- Il faut le paramétrer en anglais
- Attention : on travaille en sources ouvertes, on ne devient pas amis avec sa cible.
- On ne travaille pas avec son compte personnel. Jamais.

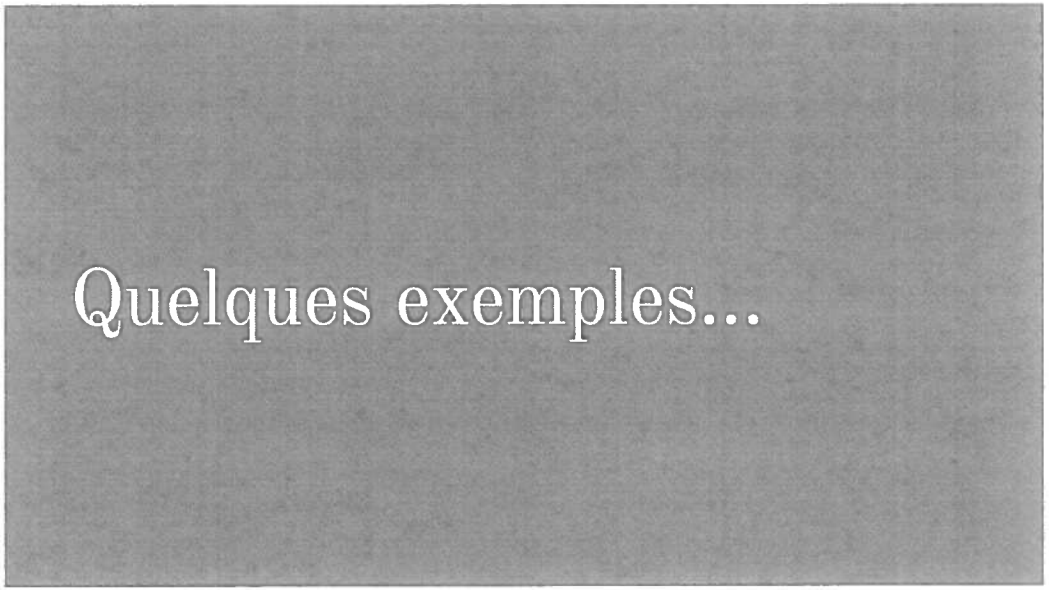
Une syntaxe particulière depuis juin 2019

- en Anglais simplifié
- via des opérateurs
- https://whopostedwhat.com/
- https://sowdust.github.io/fb-search/
- https://mtg-bi.com/content/facebook-graph-search-workaround
- (Facebook Matrix)

Fake profile

Un profil fake en anglais...

- Un profil fake est un bien précieux
- Une adresse mail et un numéro de téléphone.
- Pas de “nouveau mobile”, préférer un smartphone déjà utilisé
- Pas de VPN les premiers temps
- Ajouter des amis de temps en temps
- Poster des liens (youtube)
- Adopter un comportement “normal”.



Transposition à Instagram

Instagram a été racheté par Facebook.

La fusion des objets et entités est en cours.

Exemple sur les lieux :

Hotel Ibis Agdal 231797643558338 -> Sur Instagram

Espace Hassan à Rabat -> Sur Instagram

Conclusion

Le Graph est un moteur de recherches très puissant.

Sa syntaxe est complexe, il est régulièrement mis à jour dans le plus grand secret par Facebook.

Le suivi régulier de quelques spécialistes permet toutefois de se tenir à jour de ces évolutions.

Le Graph est une source primordiale d'information en ligne.

Facebook - Graphes relationnels

—

[redacted]

Introduction :
Construire un graphe simple

—

Un graphe

Quelques notions simples sur les graphes

- Les noeuds et arêtes (nodes & edges)
- LibreOffice ou Excel
- Gephi

Un graphe dans Gephi

Comment symboliser une relation

- Relation entre A et B
- Notion de sens de la relation
- Comment le symboliser dans Excel
- Colonnes Source, Target, Type et commentaire

Hypothèse Facebook 1 : la liste d'amis est publique

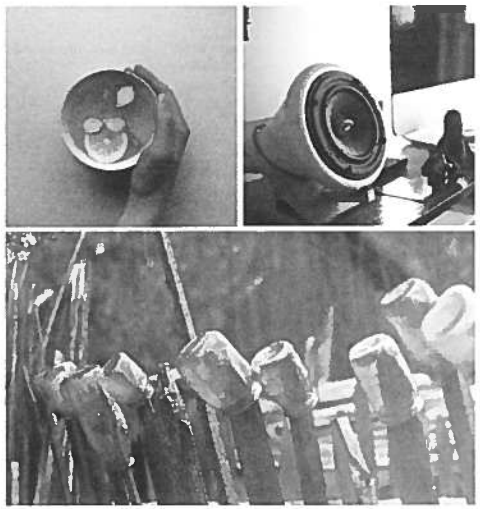
Matériel

Trouvé sur notre bureau !

- Un compte Facebook
- Linkgopher
- LibreOffice ou Excel
- Gephi

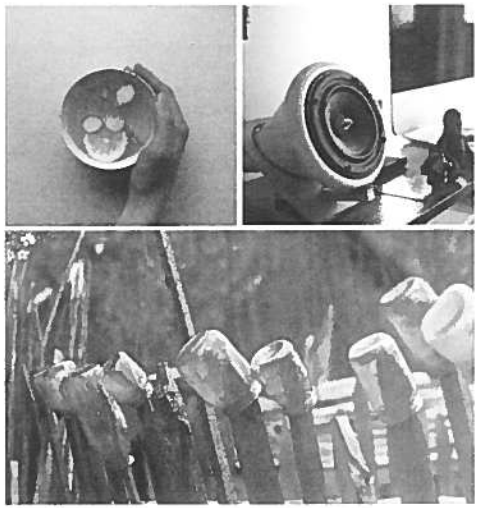
Procédure 1

1. Afficher la liste d'amis de la cible et scroller jusqu'au dernier
2. A l'aide de LinkGopher, récupérer les liens d'amitiés (pb&hc_location=friends_tab)
3. Copier/coller les liens dans une feuille de calcul, dans une colonne "Target"
4. Ajouter une colonne "Source" avec l'ID de votre cible.
5. Ajouter une colonne "Type" avec pour valeur "Undirected"

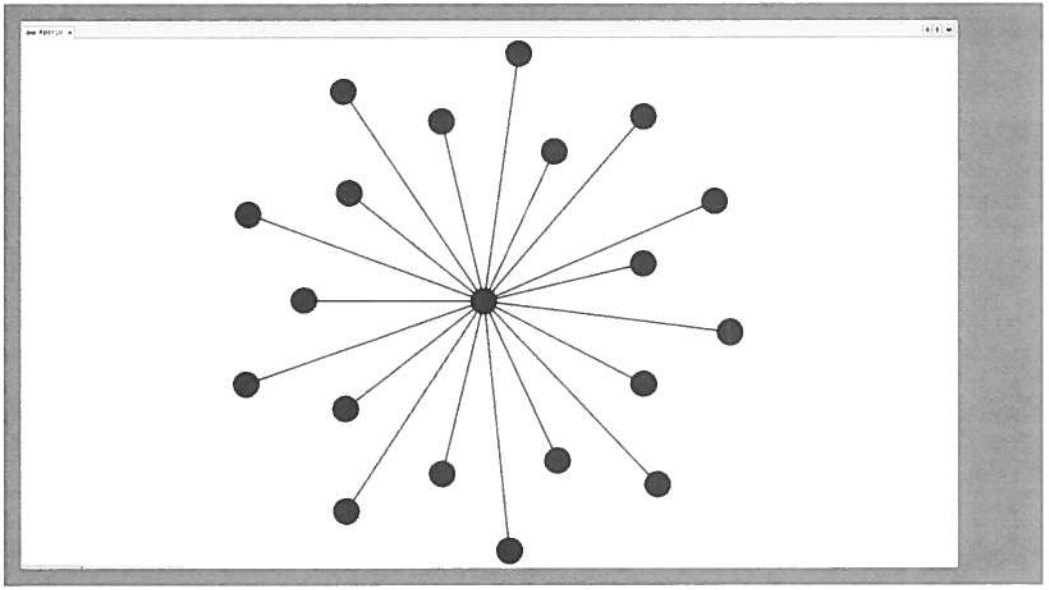


Procédure 2

1. Pour chaque amis, récupérer l'ID via lookup-id. compléter le tableau
2. La colonne Source doit contenir l'ID ou le pseudo de votre cible
3. La colonne Target doit contenir l'ID ou le pseudo de ses amis.
4. Enregistrer le fichier au format csv.
5. Importer ce fichier dans Gephi.



Un premier résultat



C'est un premier graphe, allons plus loin....

Une illustration des liens d'amitiés à faible valeur ajoutée...

Certes, notre cible est liée à ses amis...

https://www.facebook.com/profile.php?id=100009332073971

Mais il manque une information essentielle pour comprendre ce réseau, les liens entre les amis.

A est ami avec B et C. Est-ce que B et C sont amis?

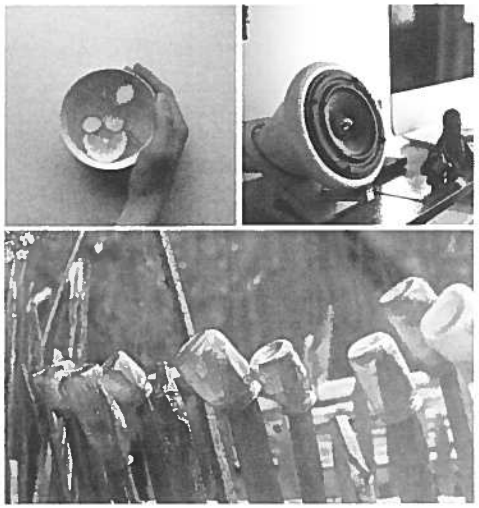
Sur Facebook, il est possible d'obtenir facilement cette information.

https://www.facebook.com/browse/mutual_friends/?uid=ID_Cible&node=ID_Target

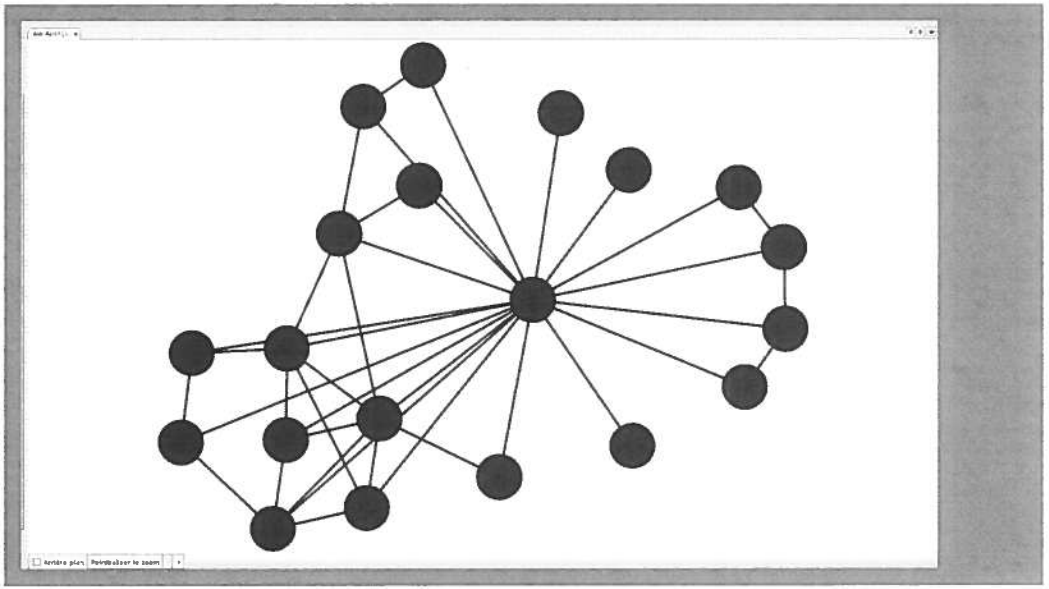
Limite : si les deux amis masquent leurs amis, il n'y a pas de résultats.

Procédure

1. Composer une URL avec l'id de votre cible et son premier ami
2. Les amis communs apparaissent alors à l'écran
3. Compléter le tableau avec en "Target", les profils obtenus, et en "Source" le nom du premier ami.
4. Faire de même pour les amis suivants



Un résultat plus précis

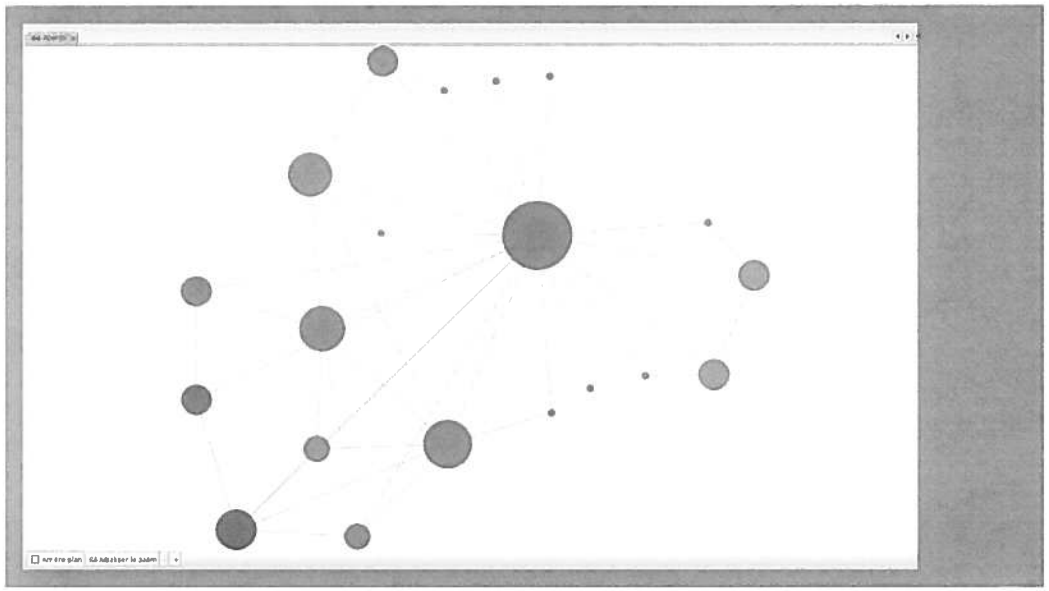


Affinons le résultat

Social Network Analysis

Calculons quelques valeurs !

- Les sous-communautés par Modularité.
- Les influenceurs par la centralité Betweenness
- Forme et taille des noeuds
- Spatialisation



Accélérer le processus

C'est un peu lent, en effet....

- Facebook n'aime pas l'automatisation
- Mais le processus peut être automatisé
- Seule technique à ce jour, le scraping.

Hypothèse Facebook 2 : la liste d'amis est privée

Idée : Si tu likes mes publications, tu es mon ami.

Vérifions cette idée...

- Ouvrir les publications publiques
- Afficher les likes et commentaires
- Récupérer leurs liens
- Construire une première liste d'amis potentiels
- Tester les amis communs
- Réitérer

Exemple : Farid

Transposition : Réseau Social VK et automate

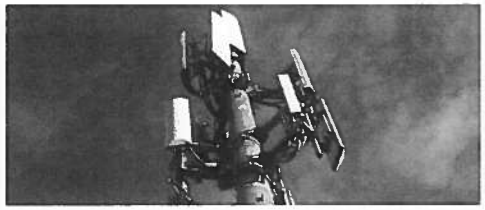
Conclusion

Nous avons vu comment créer un graphe relationnel des amis d'une cible sur Facebook.

A l'aide de Gephi, il est possible de donner du sens à ce graphe et de dégager des pistes de travail, beaucoup plus facilement que par une simple lecture du profil.

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)

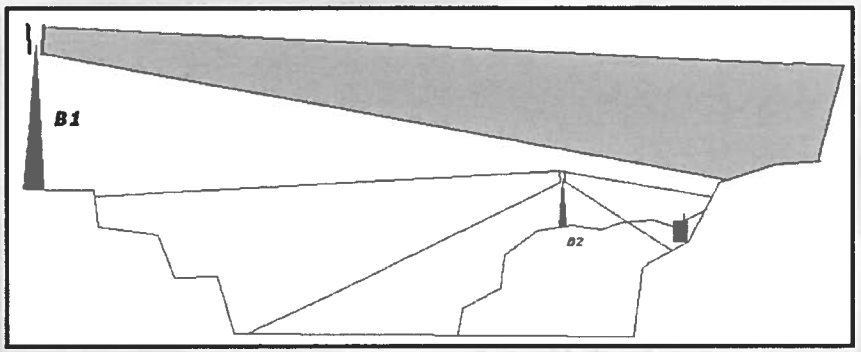
Les antennes relais :

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°)

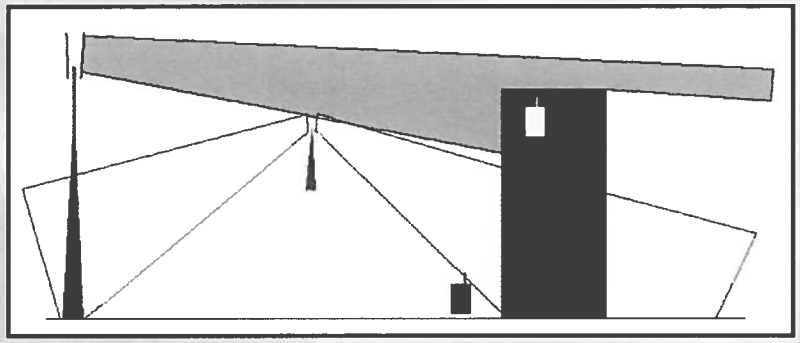
Les antennes relais :

Rayonnement et couverture



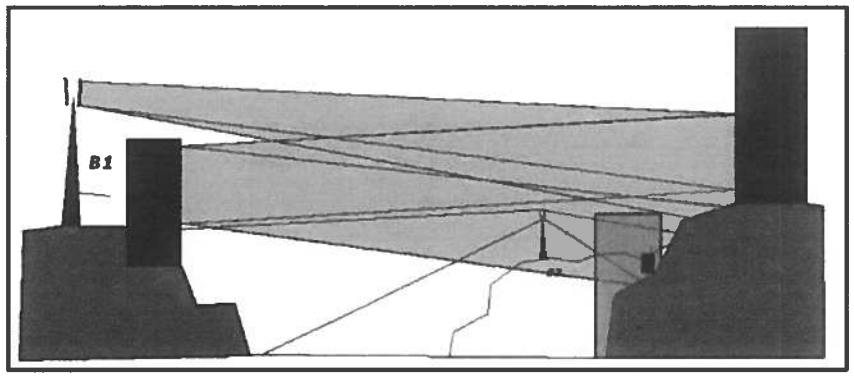
Les antennes relais :

Rayonnement et couverture



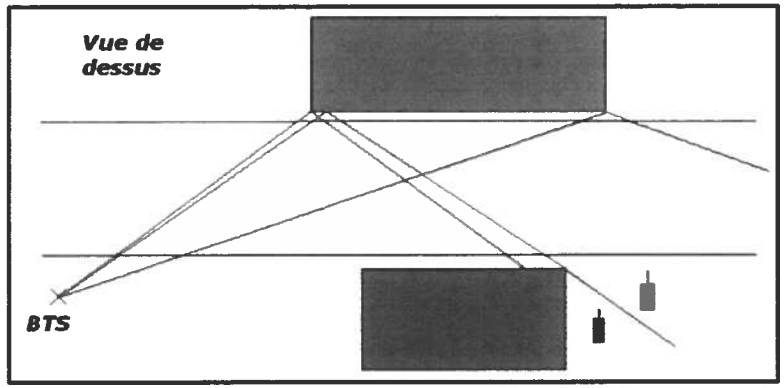
Les antennes relais :

Rayonnement et couverture



Les antennes relais :

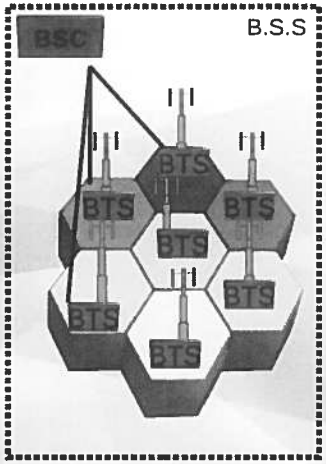
Rayonnement et couverture



Le Base Station Subsystem (BSS) :

Il s'agit de l'ensemble composé :

- des antennes
- des BTS
- des BSC

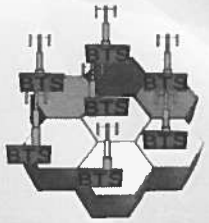


Cette partie est connectée au coeur du réseau télécom le Network SubSystem (N.S.S).

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.

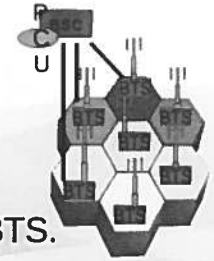


Rôle de la Base Transceiver Station :

- 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.

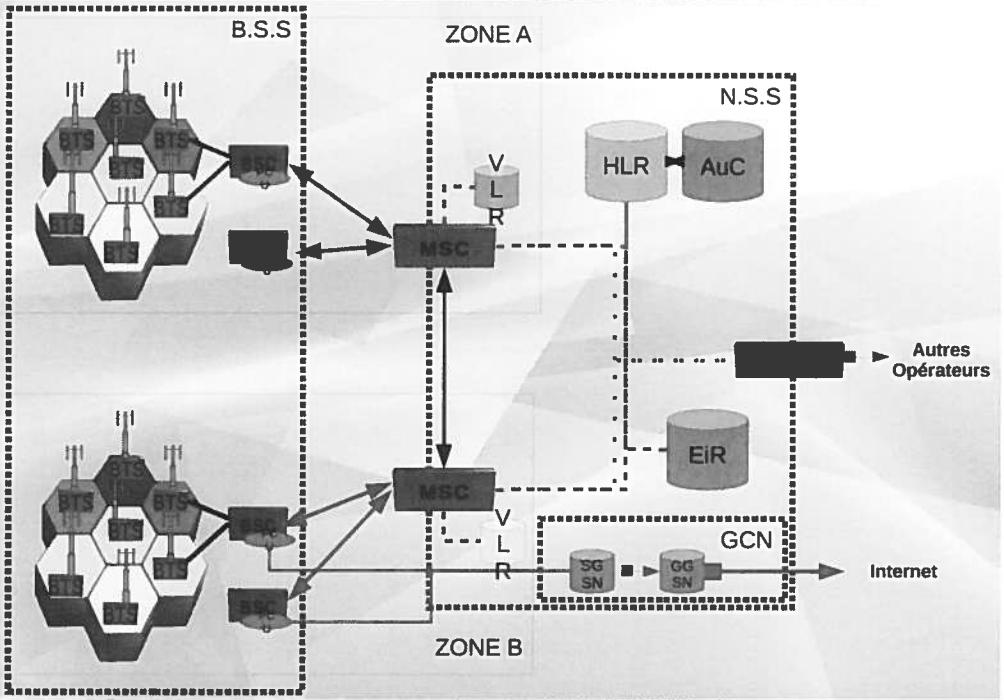


- Une BSC peut contrôler plusieurs dizaines de BTS.
- Dans le réseau 3G, la BSC est remplacée par le RNC « Radio Network Controller »

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

Rôle de la Base Station Controller :

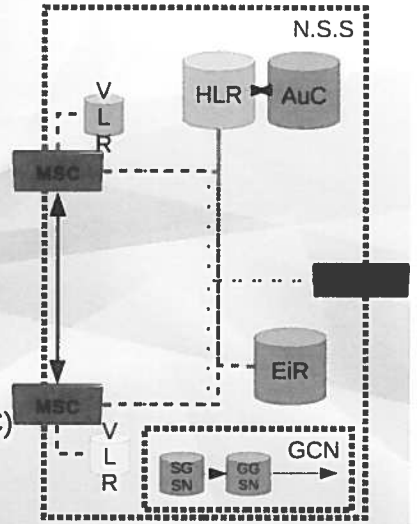
- Partie « intelligente » du réseau BSS
- Peut commander une cinquantaine de BTS.
- Décide la puissance d'émission des BTS.
- Concentre les communications vers une sortie unique.
- Gère les handovers sur les BTS de la zone.



Le Network SubSystem (N.S.S) :

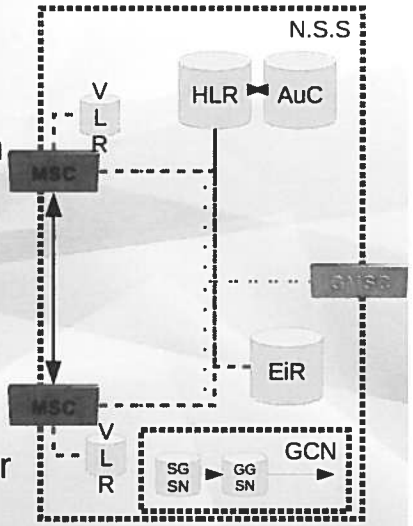
Il s'agit de l'ensemble composé :

- 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.

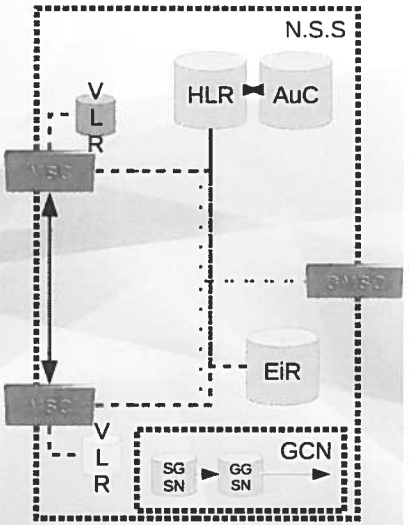


Le Visitor Location Register (VLR) :

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

Exemples :

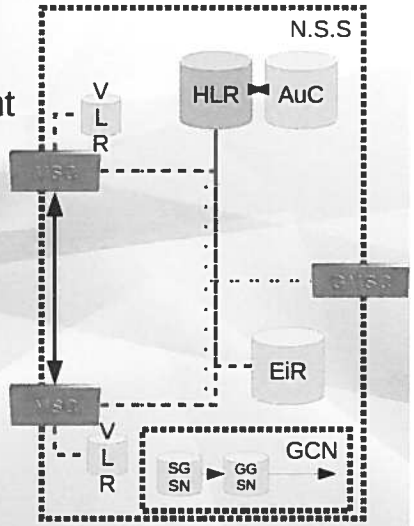
- TMSI dérivé de l'IMSI , LAI, adresse du MSC...
- Assure l'itinerance/roaming



Le Home Location Register (HLR) :

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

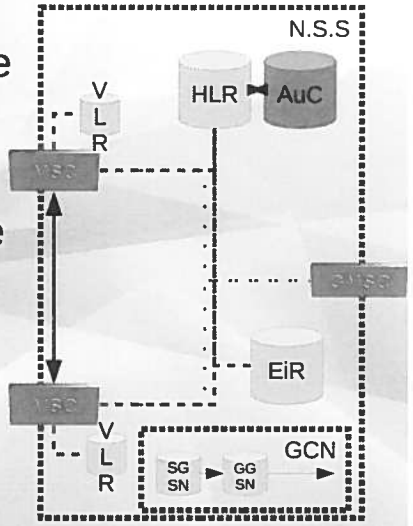
- IMSI,Numéro de l'abonné, IMEI, type d'abonnement, position grossière de l'abonné (le numéro de VLR où il est enregistré)….



L'Authentification Center (AuC) :

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

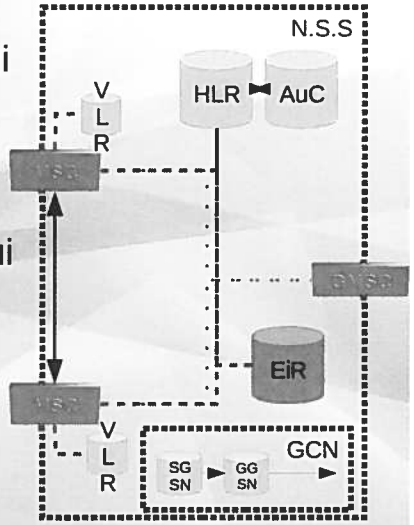
- Authentifie les abonnés par une clé présente dans la carte SIM du téléphone et le centre AuC.
- Grâce à l'authentification, un VLR peut accueillir un téléphone d'un autre réseau.



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.

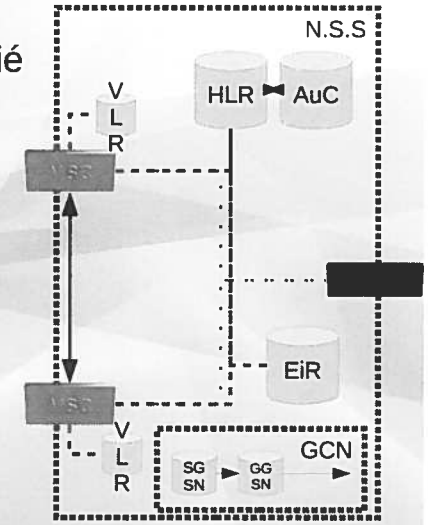


Gateway Mobile Switching Center (GMSC) :

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.

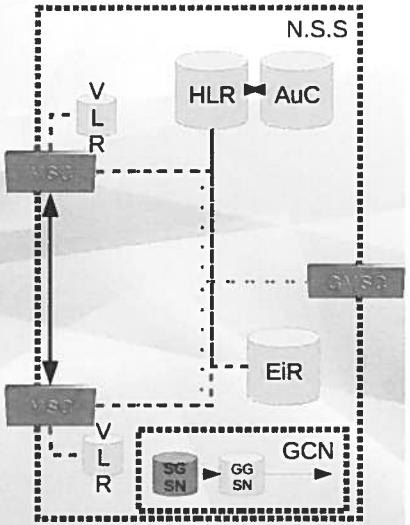
Interroge le HLR lors d'un appel entrant.



Serving GPRS Support Node (SGSN) :

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

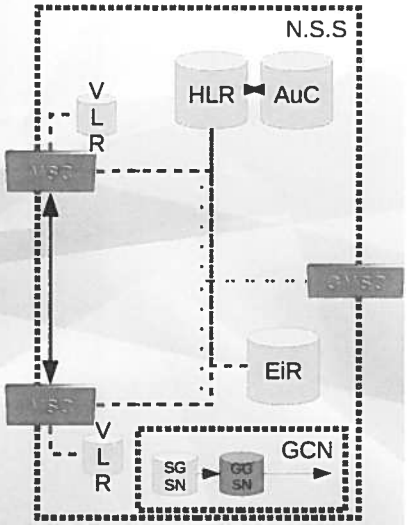
- Même rôle que le MSC (voix)
- Il gère l'interface IP via une autre passerelle le GGSN.

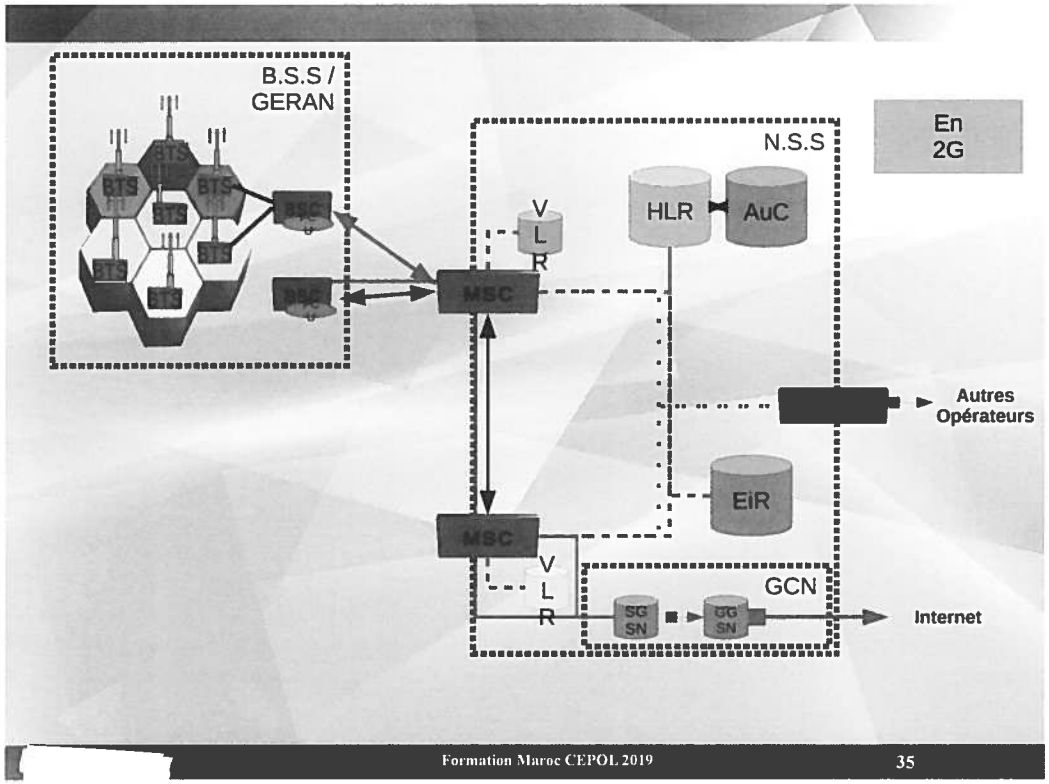


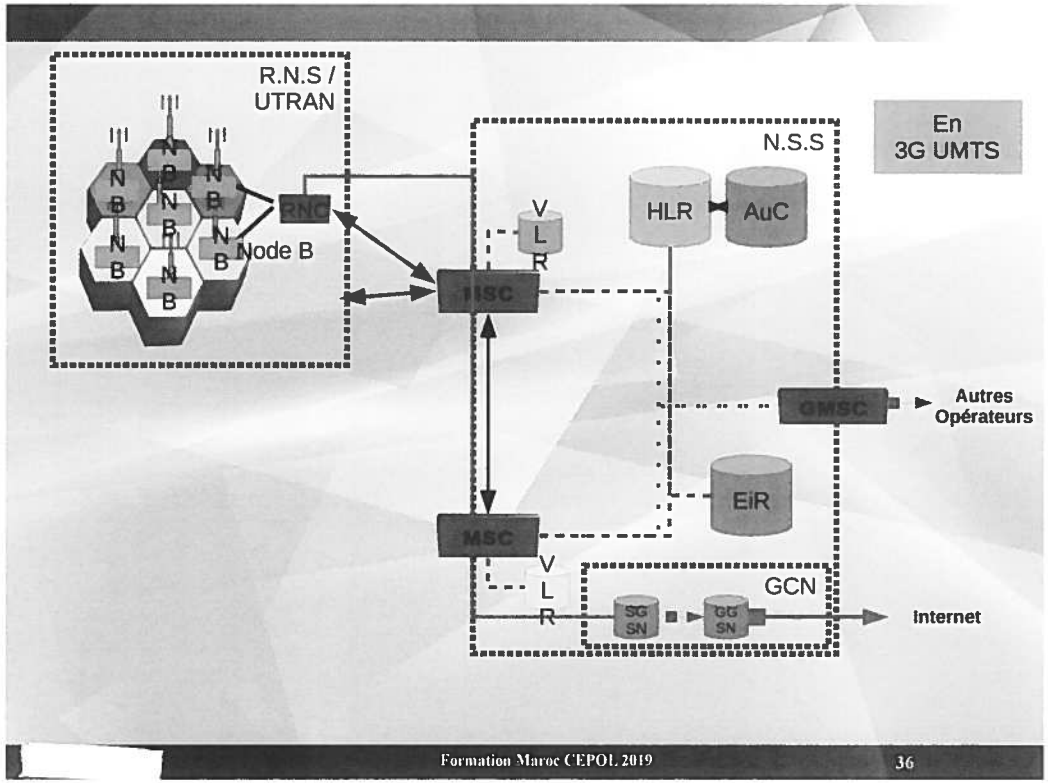
Gateway GPRS Support Node (GGSN) :

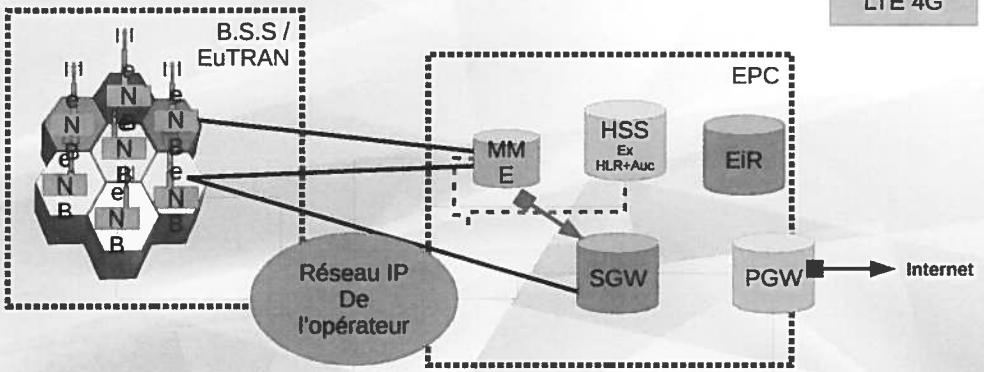
Passerelle réalisant l'interface entre réseau GPRS et internet.

- 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
EiR
En
2G
Autres
Opérateurs
GCN
SG
SN
GG
SN
Internet

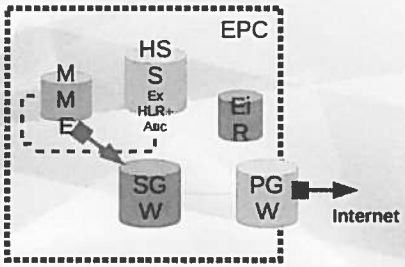

R.N.S /
UTRAN
N
B
RNC
Node B
MSC
V
L
R
N.S.S
HLR
AuC
EiR
En
3G UMTS
GMSC
Autres
Opérateurs
GCN
SG
SN
GG
SN
Internet



L'architecture 4G :

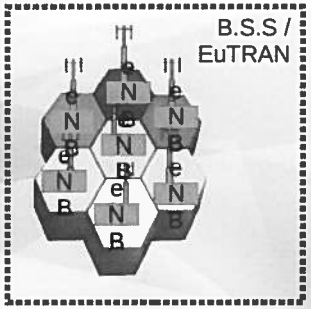
Il s'agit de l'ensemble composé :

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



Les Enodes B :

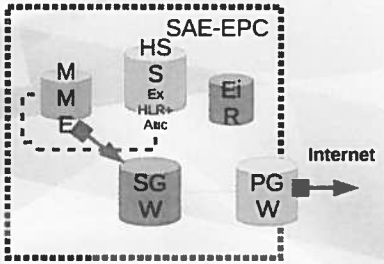
- Equivalent du NodeB de l'UMTS.
- Connectés au coeur de réseau EPC par réseau Backhaul (fibre).
- Trient voix et données. Les données sont envoyées en IP dans le coeur de réseau.
- Intégrent les fonctions de contrôle des RNC.



Les Mobility Management Entity (MME) :

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

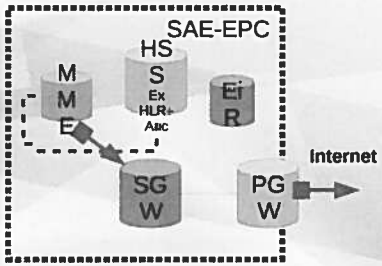
- Gère les handovers, l'itinérance
- Dialogue avec le HSS pour consulter les profils des mobiles.
- Selection du SGW



Le Home Subscriber Server (HSS) :

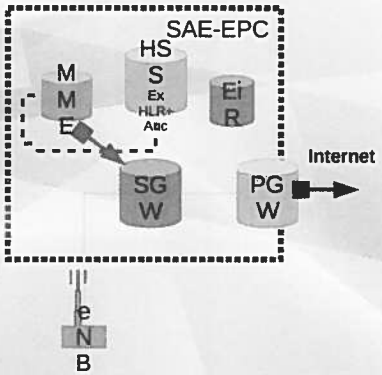
Equivalent du HLR (mais peut être utilisé sur 2g,3g,4g du même opérateur)

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



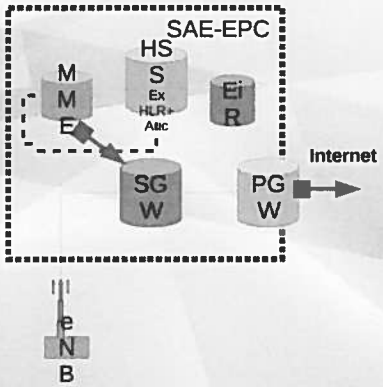
Le Serving Gateway (SGW) :

- 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.

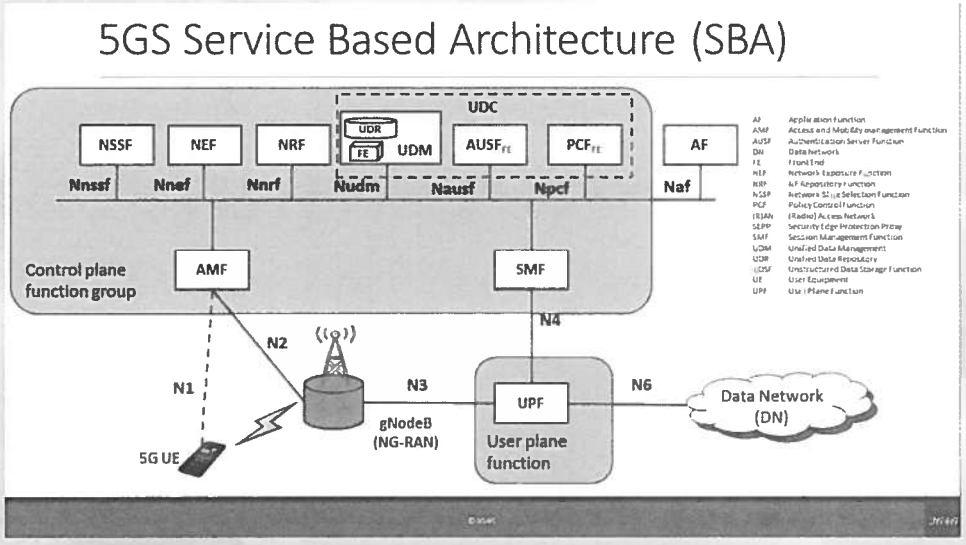


Le Packet Data Network Gateway (PGW) :

- 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 :



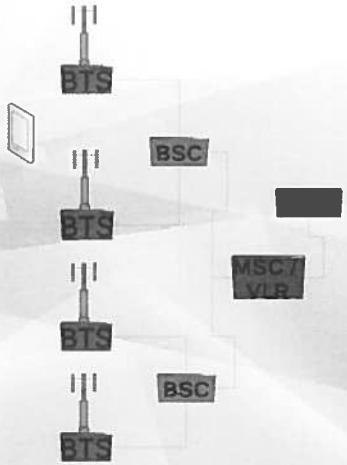
La gestion des téléphones sur le réseau Télécom

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 ».

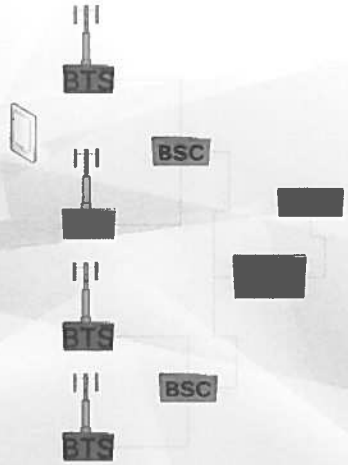
Mise sous tension du téléphone :

- 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



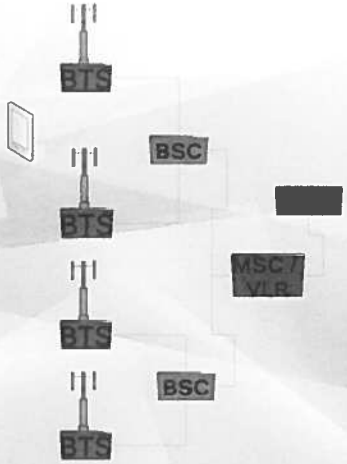
Appel sortant :

- 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.



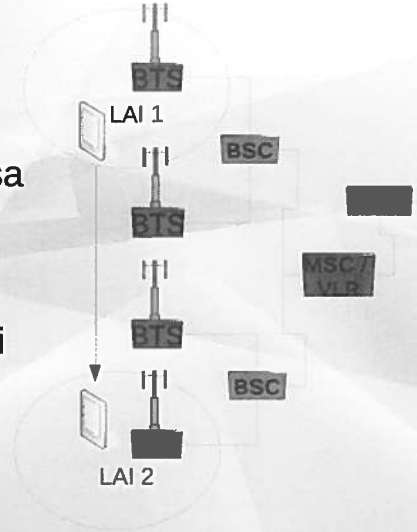
Appel entrant :

- 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.



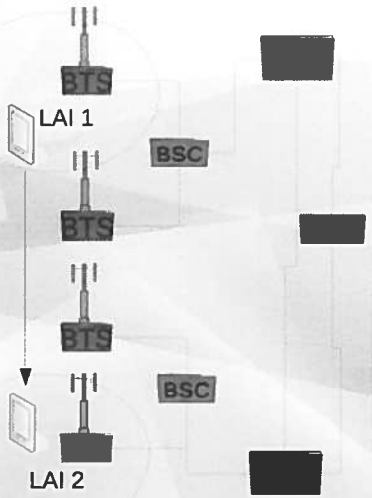
Changement de zone et même VLR :

- 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



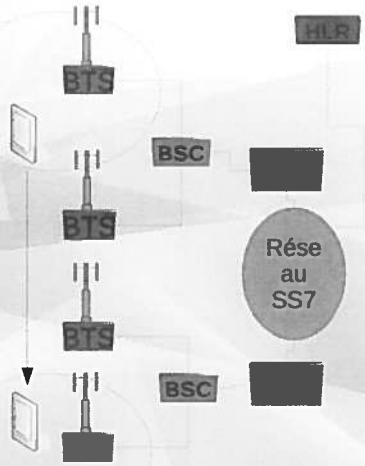
Changement de zone et de VLR :

- 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



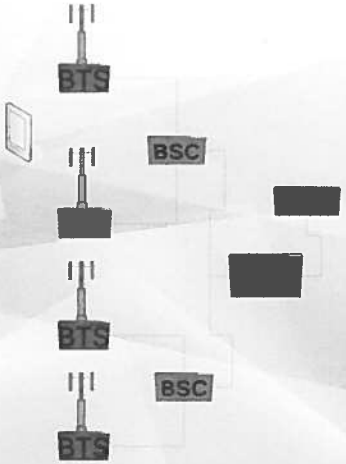
Changement de pays et de réseau :

- 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 :

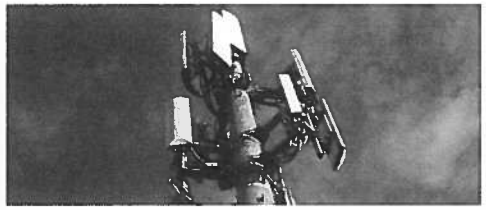
- Procédure de détachement avant l'arrêt
- Transmission au HLR de l'état du téléphone
- Abonné non joignable
- Orientation vers messagerie.



Des questions ?

CEPOL

Investigations et téléphonie mobile



Module 3
Les données opérateurs

[redacted] – CEPOL 2019

Sommaire :

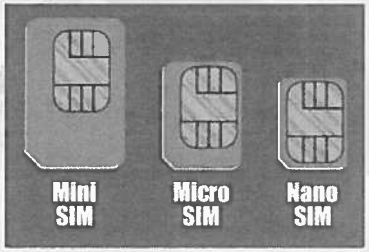
- La carte SIM et ses informations
- Le téléphone portable
- Les données opérateurs
- La navigation internet mobile
- Le réseau SS7 et le Spoof ID

La carte SIM et ses données

La carte SIM et ses données

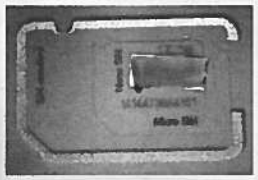
Différents formats de cartes Subscriber Identity Module (SIM) :

- **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

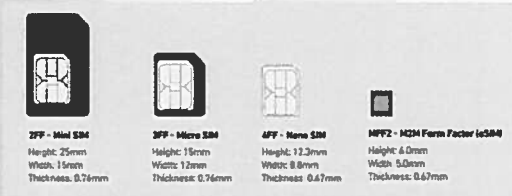
- La carte SIM est sécurisée par un code PIN (Personal Idenfication Code)
- Peut être débloquée avec le code PUK (Personal Unlock Code)

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.



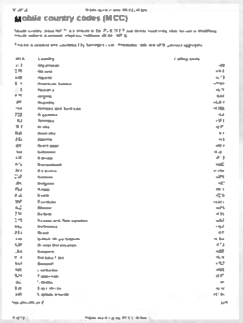
La carte SIM et ses données

- 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

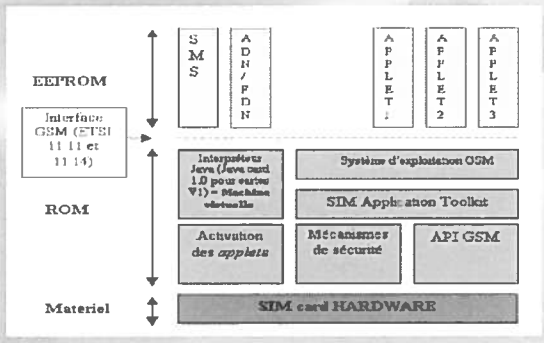
- International Mobile Subscriber Identity
- 3 chiffres : MCC (Mobile Country Code)
- 2 ou 3 chiffres : MNC (Mobile Network Code)
- 10 chiffres : MSIN (Mobile Subscriber Identification Number)

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 :

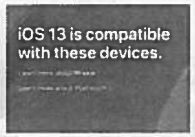
- MAC Adresse

  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

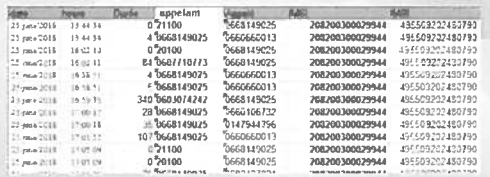
Les données opérateurs

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	Appelé	IMEI	IMSI
21 janv 2018	19 44 34	0	21100	0668149025	208200300029944	495509202480790
21 janv 2018	19 44 34	4	0668149025	0660660013	208200300029944	495509202480790
23 janv 2018	16 02 13	0	20100	0668149025	208200300029944	495509202480790
25 janv 2018	16 02 11	84	0687710773	0668149025	208200300029944	495509202480790
25 janv 2018	16 55 11	4	0668149025	0660660013	208200300029944	495509202480790
25 janv 2018	16 58 51	4	0668149025	0660660013	208200300029944	495509202480790
25 janv 2018	16 59 35	340	0603074242	0668149025	208200300029944	495509202480790
25 janv 2018	17 00 17	28	0668149025	0660106732	208200300029944	495509202480790
25 janv 2018	17 00 18	26	0668149025	0147544796	208200300029944	495509202480790
25 janv 2018	17 01 55	107	0668149025	0660660013	208200300029944	495509202480790
25 janv 2018	17 07 04	0	21100	0668149025	208200300029944	495509202480790
25 janv 2018	17 07 09	0	20100	0668149025	208200300029944	495509202480790

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 electronique	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

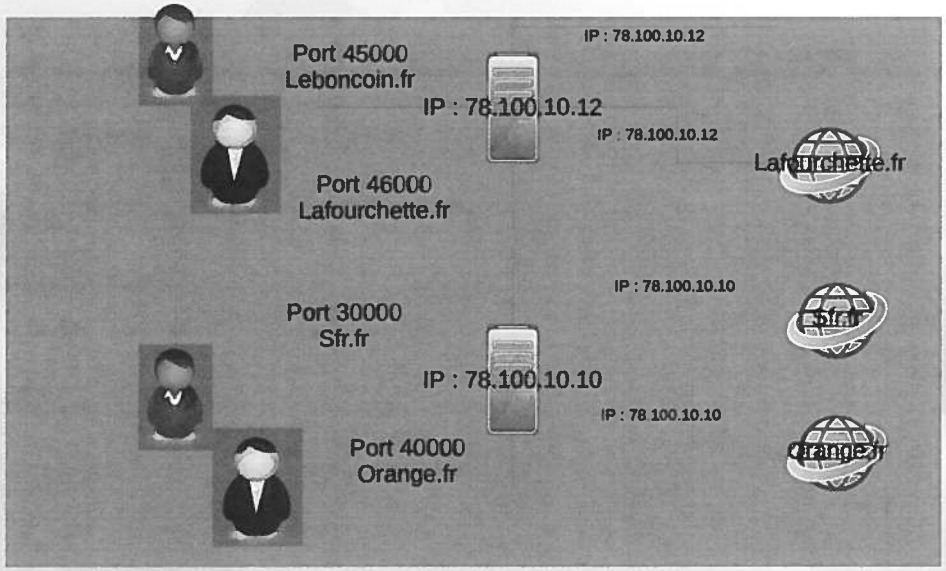
Code	Prestation
	Prestations autres
ARRET	Arrêt anticipé d'une interception
REPORT	Prolongation d'une interception
HREF	Prestation Hors REFérentiel

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

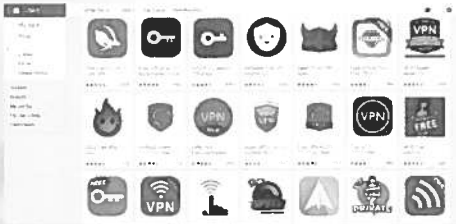


La navigation internet

- 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

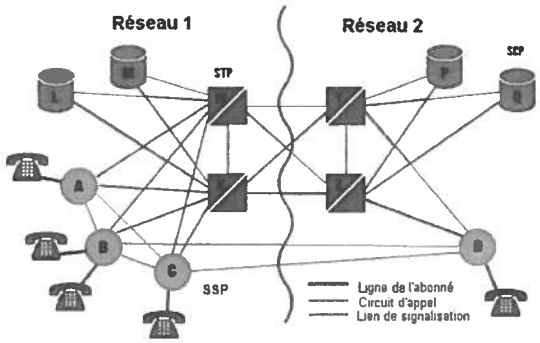
Le réseau SS7

- 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

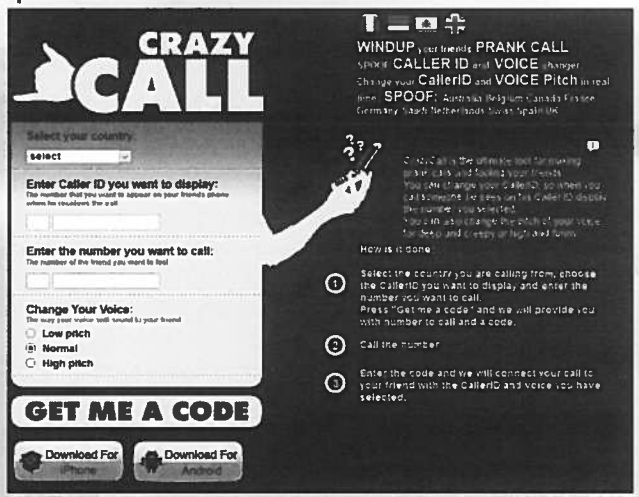
- Le « Spoof-id » ou l'usurpation d'identité.
- Une technique qui peut compliquer les investigations policières.
- Permet d'afficher le numéro qu'on désire au destinataire (Swatting).

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.

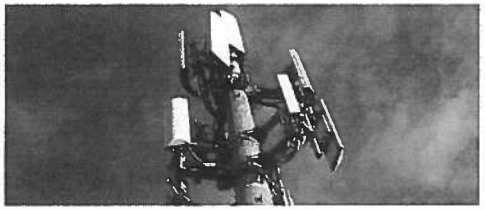
Le spoof-ID

- 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	num correspondant	Compter - durée
2	3622256741	Emis	0139397187	1
3			0171060510	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			0698921380	1
14			0699068328	2
15			216210067S4	1
16		Message ecrit emis	0624254968	1
17				1
18		Message ecrit reçu		12
19		Rappel automatique		8
20		Reçu	0210395140	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)

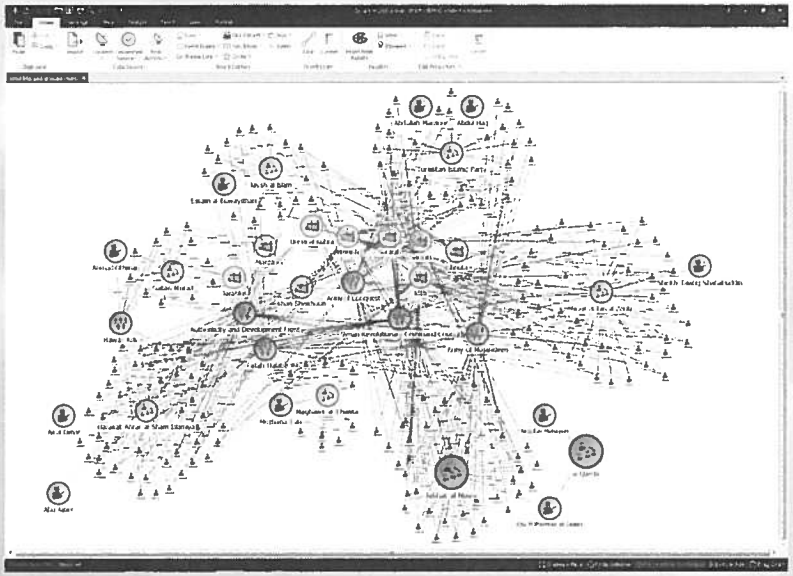
Inconvenients :

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

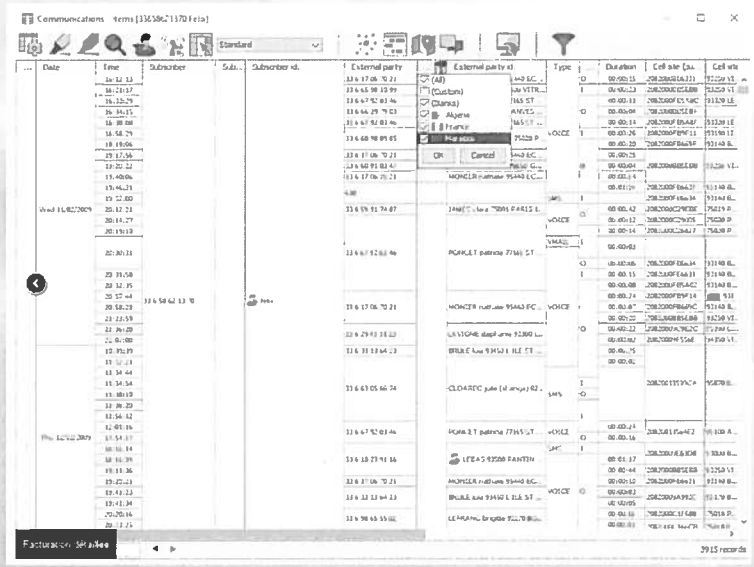
accessible pour les enquêteurs

Peut être utilisé en mono-poste ou réseau

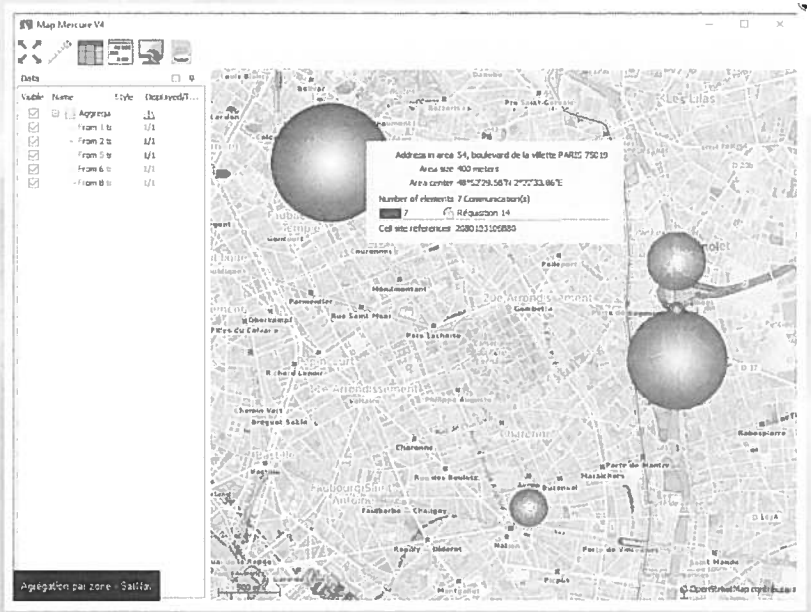
Inconvenients :

Payant

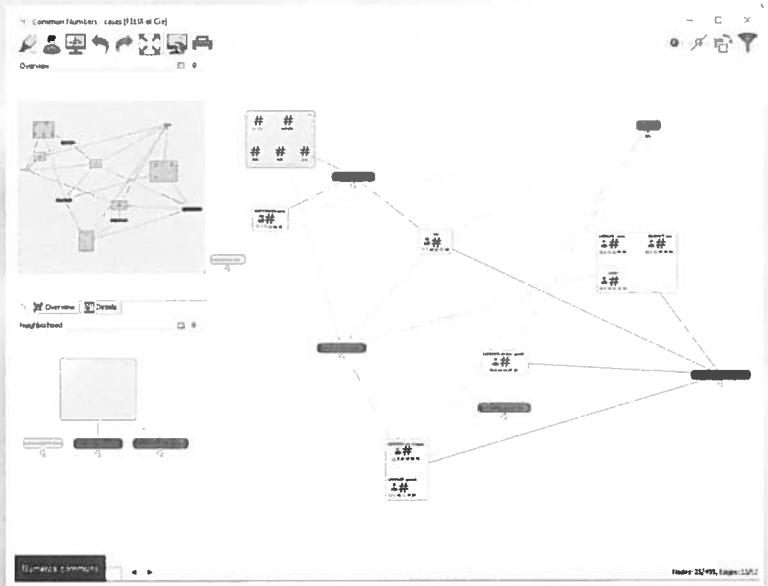
Logiciel d'analyse dédié (Mercure v4)



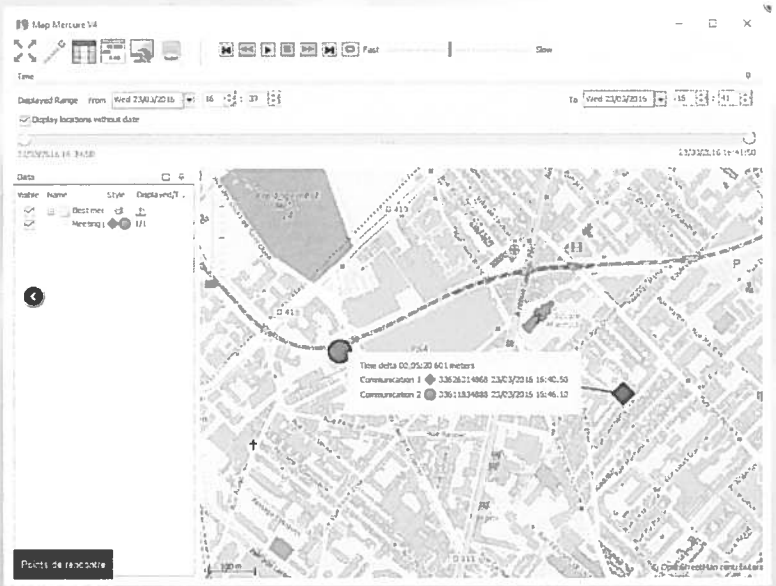
Logiciel d'analyse dédié (Mercure v4)



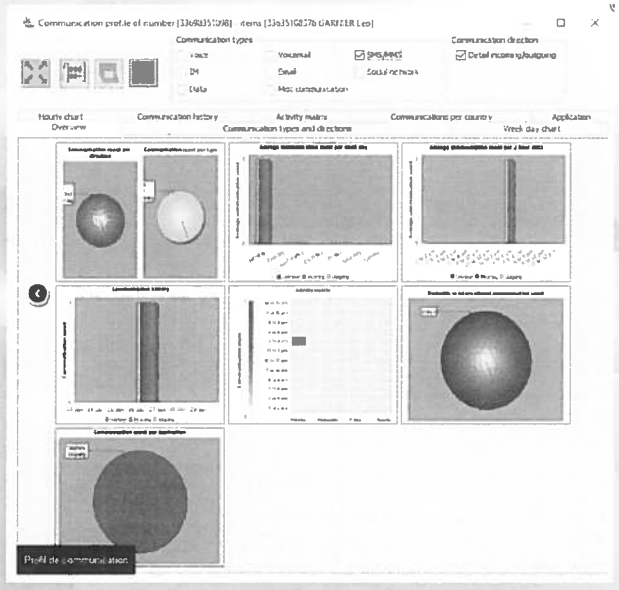
Logiciel d'analyse dédié (Mercure v4)



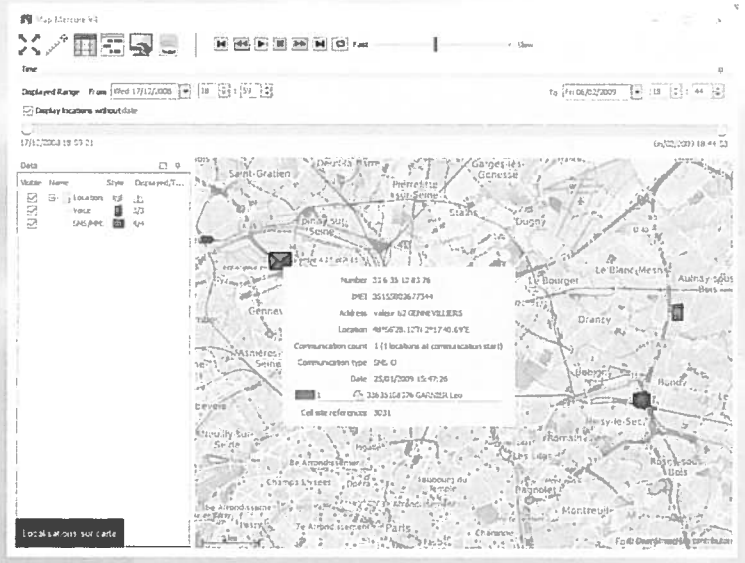
Logiciel d'analyse dédié (Mercure v4)



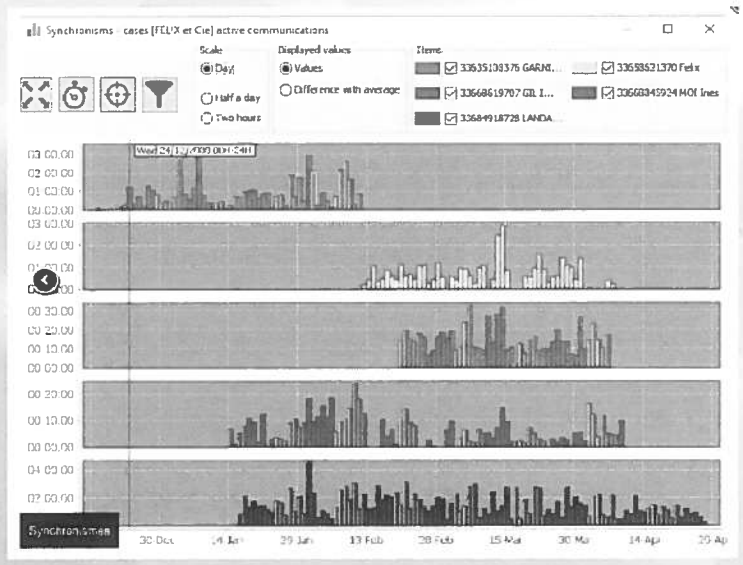
Logiciel d'analyse dédié (Mercure v4)



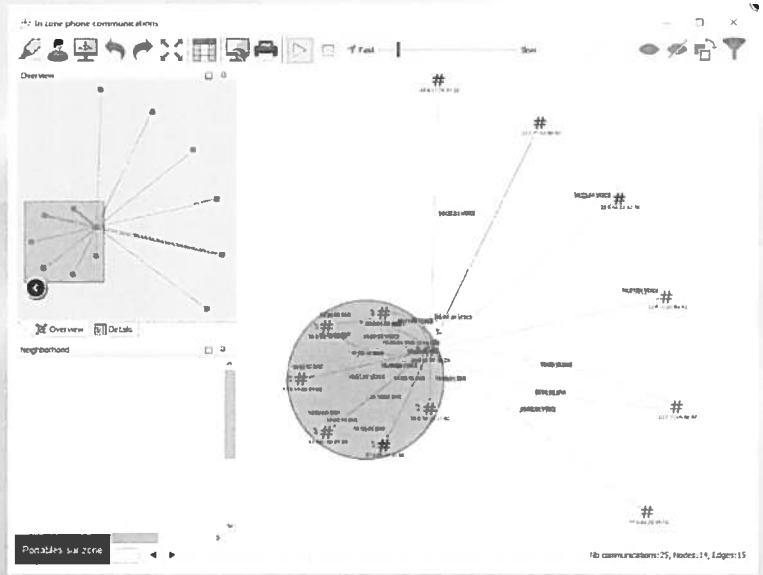
Logiciel d'analyse dédié (Mercure v4)



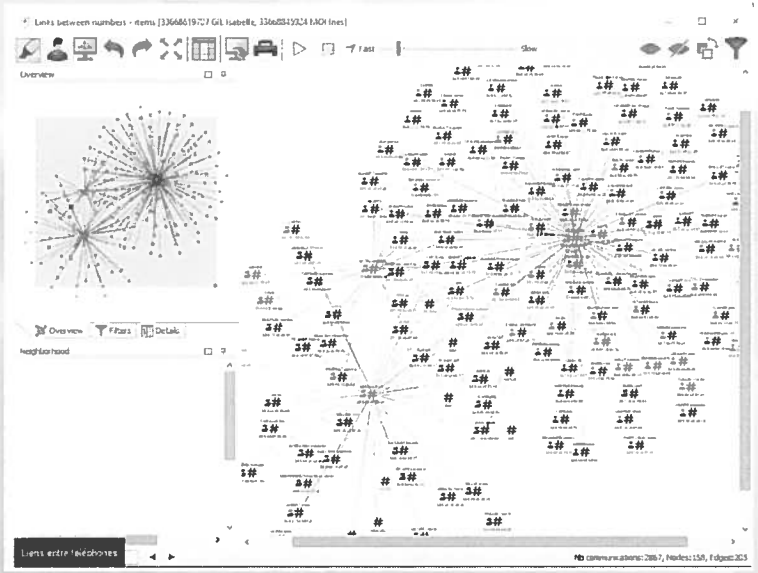
Logiciel d'analyse dédié (Mercure v4)



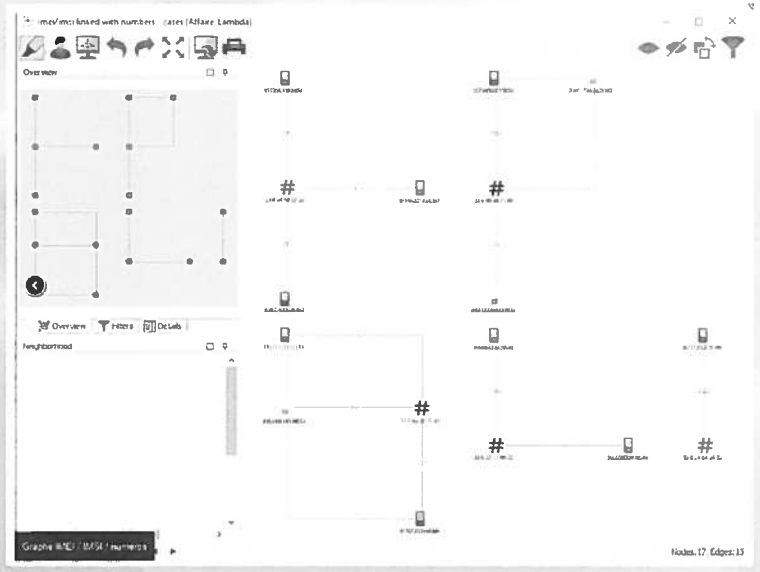
Logiciel d'analyse dédié (Mercure v4)



Logiciel d'analyse dédié (Mercure v4)

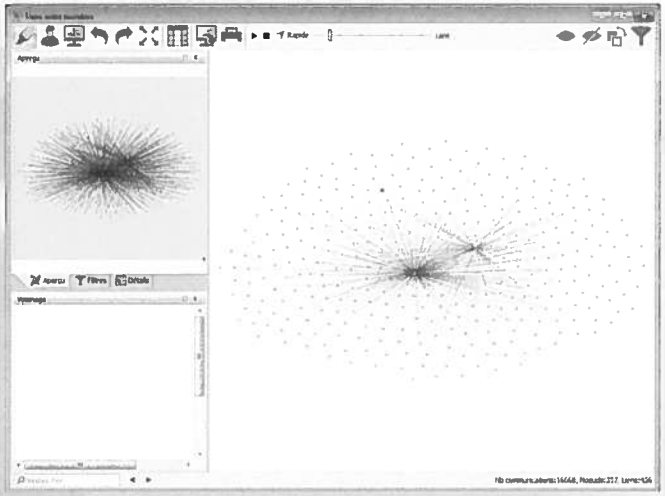


Logiciel d'analyse dédié (Mercure v4)



Logiciel d'analyse dédié (Mercure v4)

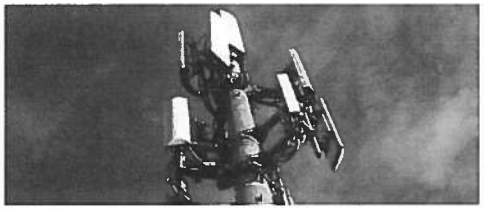
Démonstration Mercure V4



Des questions ?

CEPOL

Investigations et téléphonie mobile



Module 5
L'exploitation des téléphones

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.

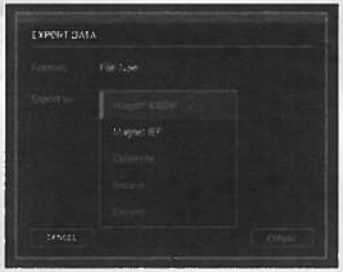
L'extraction des données

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

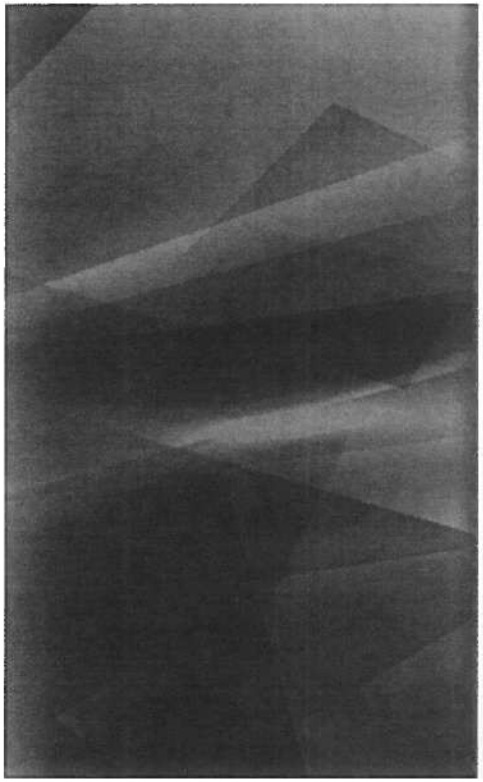
- Pour extraire les données d'un téléphone portable, il est possible d'utiliser des équipements spécifiques :

- UFED de Cellebrite / Xry de Msab

L'extraction des données

Démonstration Reader (on ne nous dit pas tout)

Des questions ?



Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 1 : la preuve numérique, principes fondamentaux

CEPOL

[redacted] – Maroc - 2019

« Finalement, ce que preuves matérielle et immatérielle ont en en commun, c'est bien la confiance. Quelle confiance accorder à la preuve immatérielle ? Comment accorder sa confiance à une preuve immatérielle ? A quel acteur du processus de réalisation d'une preuve matérielle accorder ou ne pas accorder sa confiance ? »

Yves Repiquet, bâtonnier de l'ordre des avocats, 21/11/2007 « La Justice à l'épreuve de la preuve immatérielle», débats à la maison du Barreau de Paris.

1) Information, preuve et vérité
2) Le principe de liberté de la preuve
3) Outils, méthodes et normes
4) Les acteurs de la preuve

Information, preuve et vérité

Donnée et information

- « *Ce qui est connu ou admis comme tel, sur lequel on peut fonder un raisonnement, qui sert de point de départ pour une recherche* » (Larousse)
- « *L'information est une indication, un renseignement, une précision que l'on donne ou que l'on obtient sur quelqu'un ou quelque chose* » (Larousse)
- Un fait ? Une vérité ?
  - Fiabilité (source, intégrité, ...)
  - Validité (crédibilité, légalité, ...)
  - Pertinence (intelligibilité, contexte, ...)

Un policier voleur

Un CRS surpris en train de voler un maillot de foot sur les Champs-Élysées ! (Vidéo)

Publié par [redacted] sur 17 Mars 2019, 10:46am

CRS, Paris, Gilets Jaunes

Gilets jaunes : un policier filmé rangeant des maillots du PSG dans un sac, l'IGPN saisie

ACTUALITÉS

L'IGPN saisie après une vidéo où un policier récupère des maillots du PSG sur les Champs-Élysées

franceinfo:

LADEPECHE.fr

Le Parisien

HUFFPOST

Acte XVIII à Paris : un CRS a-t-il profité de la manifestation pour piller la boutique du PSG ?

Un policier voleur, suite

facebook

[redacted] a partagé une publication
10 h
Incroyable !!!!
Afficher la pièce jointe

[redacted] Scandaleux hormiant putains de force de l'ordre me répugne pourquoi ils agissent ainsi... Mr Macron et castaner ont ils une réponse???
J'aime Répondre 2 j

[redacted] a partagé une publication
3 h
Bravo messieurs, et après on met sur le dos des gilets jaunes Tout les moyens sont bons

largement partagées accusent le premier policier d'avoir volé ces produits du PSG, et le second, auteur du coup de matraque, d'avoir voulu le couvrir.

Revoir la vidéo

La Plume Libre

Contactée par *CheckNews*, une source policière fait état d'images *«embarrassantes»*. La préfecture de police de Paris n'a pas fait de commentaire, indiquant seulement que l'inspection générale de la police

twitter

Un policier voleur, suite

Sollicitée par nos confrères de France Info la préfecture de police de Paris indique que l'Inspection générale de la police nationale (IGPN) a été saisie pour enquêter sur cette affaire. Alors que la CGT Police Ile-de-France ne souhaite pas polémiquer et dément formellement l'hypothèse d'un vol « il s'agit d'une procédure classique de collecte de pièces à conviction ».

"La situation sur place était chaotique. A tout moment ça pouvait dégénérer. Alors dans ces cas-là, on ramasse les objets comme on peut pour matérialiser l'infraction."

— Axel Ronde, secrétaire général VIGI Ile-de-France
à franceinfo

❌ FAKE NEWS / Durant l'#Acte18 des #GiletsJaunes, ce membre des #FDO 👮‍♂️ ne vole pas des maillots d'un magasin du #PSG :
👉 Il met dans un sac des vêtements volés par des casseurs qui ont été interpellés aux alentours & dans la boutique.
facebook.com/brutofficiel/v...

Un policier voleur, suite

LCI

Selon nos informations, le policier mis en cause a rédigé un procès-verbal d'interpellation après cette scène. Dans ce PV, le policier indique avoir procédé à l'interpellation d'un individu qui tentait de s'échapper d'une boutique vandalisée sur les Champs-Elysées. Interpellation pour "vol en réunion avec dégradations", précise le policier, indiquant que cet homme, âgé d'une vingtaine d'années, avait les bras chargés de vêtements.

Au verso du procès-verbal, qui a été versé à l'enquête menée au commissariat du 10e arrondissement, l'agent interpellateur prend le soin de faire l'inventaire de toute la liste des objets ramassés et laissés échappés par le pilleur pendant l'interpellation. Le sac que l'on voit dans la vidéo est d'ailleurs un sac du PSG lui aussi volé. Selon nos informations, 18 articles sont décrits très précisément par le policier, avec à chaque fois la valeur de l'objet. Le préjudice est estimé à 2 004 €.

"Le sac et les affaires consignés ont ensuite été remis à l'officier de police judiciaire. C'est l'OPJ qui a pris ensuite le relais", souligne une source proche de l'enquête. Une enquête de l'IGPN a été ouverte. Selon nos informations, le policier n'aurait pas encore été entendu.

De la preuve à l'information ?

- « *La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation* » , dictionnaire juridique de Serge Braudo
- « La preuve est un *élément matériel qui démontre, établit, prouve la vérité ou la réalité d'une situation de fait ou de droit* », Larousse
- « La preuve est un *fait ou raisonnement propre à établir solidement la vérité* », Wikipédia
- « *Pour qu'elle soit crédible, la preuve doit résister à la discussion* », Patrick Matet, Magistrat à la Cour d'appel de Paris

Preuve et vérité

- La preuve vise t'elle la vérité ?
- « *utile à la manifestation de la vérité* », « *en vue de la manifestation de la vérité* » (code civil, code de procédure pénal, ...)
- La vérité absolue n'existe pas, c'est la croyance à cette vérité qui importe
- La notion de faisceau d'indice : la vérité judiciaire est une construction, pas une donnée
- Cette recherche de la vérité doit composer avec le respect des valeurs fondamentales (vie privée, dignité humaine, ...)

Le principe de liberté de la preuve

Le principe de liberté de la preuve

- ***Article 1358 du code civil***

« Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen. »

- ***Article 1366 du code civil***

« L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

- **Article 427 du code pénal**

« Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.

Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui. »

Les principes fondamentaux

- « *La procédure pénale doit être équitable et contradictoire et préserver l'équilibre des parties* », article préliminaire al 1, code de procédure pénale
- Le principe de légalité
  - Respect de droits de la défense
  - Interdiction des modes de preuve contraires à la dignité humaine
  - Interdictions des moyens déloyaux
- L'exception majeure : le recours à des preuve déloyales voire illégales par une partie
- Le principe de nécessité
- Le principe de proportionnalité des moyens
- Le principe du contradictoire

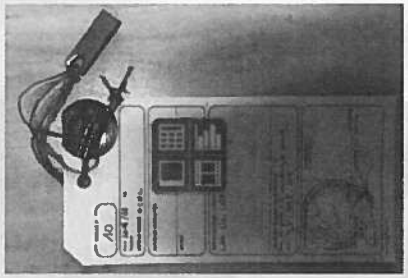
Les principes fondamentaux (suite)

- L'authenticité de la preuve
  - L'origine de la preuve (chain of custody)
  - L'intégrité de la preuve (absence d'altération et répétibilité)
- Existe t'il une hiérarchie des preuves ?
  - De la simple carte postale à l'acte notarié, du témoignage au rapport d'expertise
  - Tout acte de procédure n'a que valeur d'information pour le juge
  - L'intime conviction est humaine
    - Ce qui semble avoir de la valeur
    - Un diplôme, le respect d'une méthodologie connue, une jolie présentation, ...

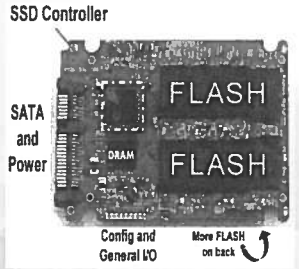
La vulnérabilité de la donnée numérique

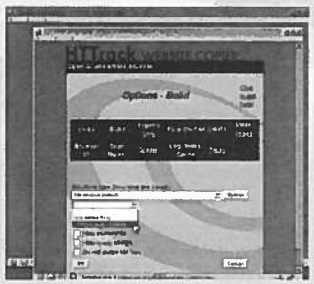
- Toutes les preuves sont falsifiables et fragiles... mais...
- La donnée numérique est très fragile
  - Volatilité de la donnée
  - Évolutivité des technologies
- La donnée numérique est très malléable
  - Facilement copiable (reproduction de preuve)
  - Facilement modifiable (falsification de preuve)
  - Facilement effaçable (destruction de preuve)
- La donnée numérique est incompréhensible au non initié
  - Qui comprend l'hexadécimal ?
  - Existe t'il un expert couvrant tous les domaines de l'investigation numérique ?

La donnée est-elle protégée ?

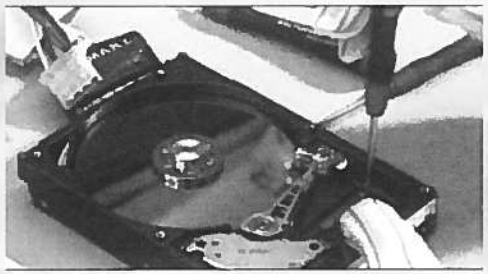


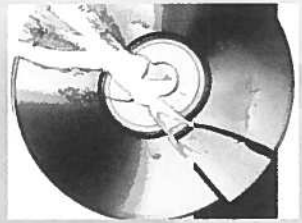
La donnée est-elle protégée ?



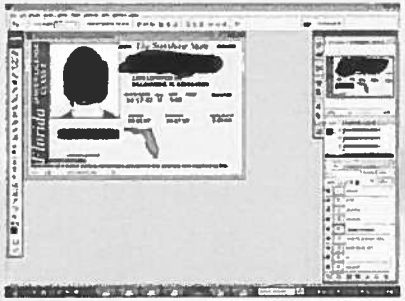


La donnée est-elle toujours accessible ?

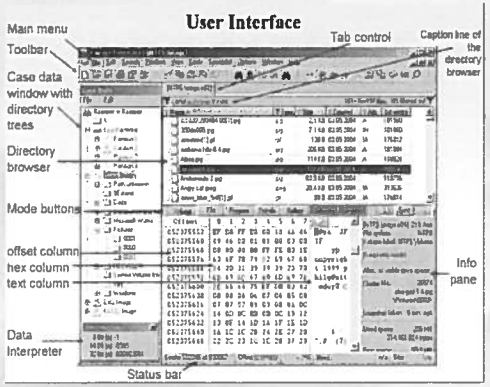


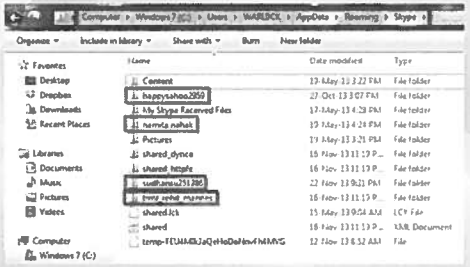


La donnée est-elle fiable ?



La donnée est-elle compréhensible ?





Outils, méthodes, normes

Les outils sont-ils fiables ?

- Outils gratuits et outils payants ?
- Outils à tout faire et outils dédiés ?
- Outils pour experts et outils « facilités »
- Outils « fait maison »
- Comment tester un outil ?

Trouver un outil d'analyse numérique ?

https://toolcatalog.nist.gov/index.php

https://www.dftools catalogue.eu/dftc. home.php

Les outils sont-ils fiables ?

Popular Computer Forensics Top 21 Tools [Updated for 2019]

Tool	Rank
Digital Forensics Framework	1
Open Computer Forensics	2
CAINE	3
XWAYS Forensics	4
Encase	5
Registry Recon	6
The Sleuth Kit	7
Llibforensics	8
Volatility	9
WindowsSCOPE	10
etc...	11

https://resources.infosecinstitute.com/computer-forensics-tools/#gref

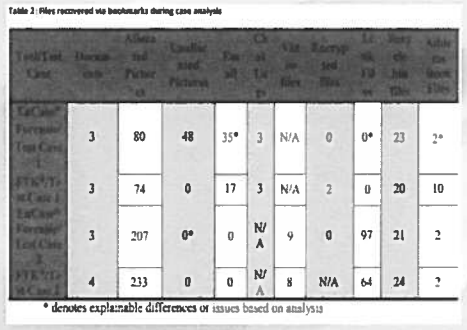
7 Best Computer Forensics Tools [Updated 2019]

Tool	Rank
SANS SIFT	1
Pro Discover Forensic	2
Volatility Framework	3
The Sleuth Kit (+Autopsy)	4
CAINE	5
Xplico	6
Xways Forensics	7
Etc...	8

https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref

Les outils sont-ils fiables ?

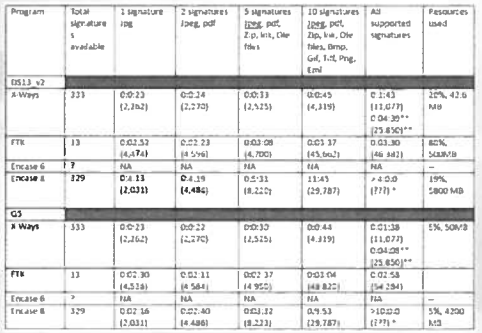
Quelques tests de récupération de données



3	80	48	35*	3	N/A	0	0*	23	2*
3	74	0	17	3	N/A	2	0	20	10
3	207	0*	0	N/A	9	0	97	21	2
4	233	0	0	N/A	8	N/A	64	24	2

* denotes explainable differences or issues based on analysis

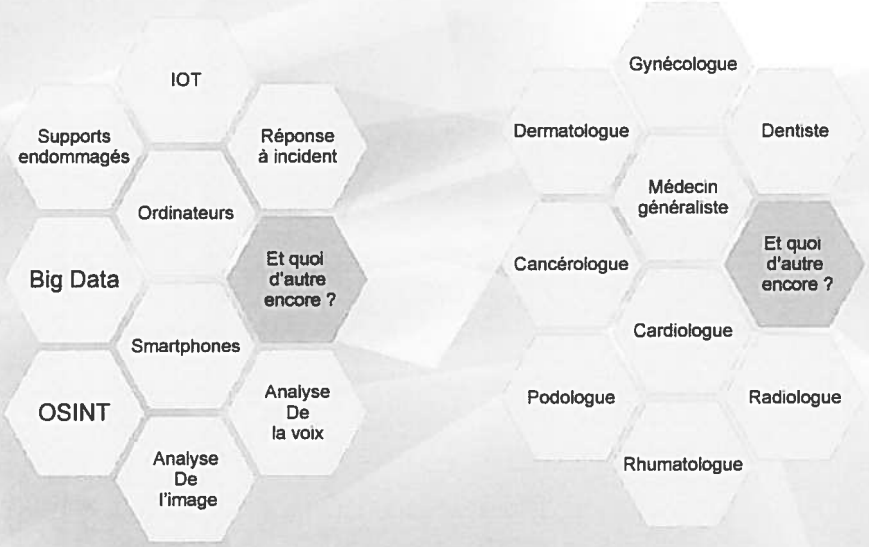
https://www.marshall.edu/forensics/files/CERVELLONEADAM_FinalResearchPaper-8-7-2015_-1.pdf



Program	Total signatures available	1 signature jpg	2 signatures jpeg, pdf	5 signatures jpeg, pdf, Zip, lnk, Ole files	10 signatures jpeg, pdf, Zip, lnk, Ole files, Bmp, Gif, Txt, Png, Eml	All supported signatures	Resources used
DS1.3_v2							
X-Ways	333	0:0:23 (2,262)	0:0:24 (2,270)	0:0:33 (2,525)	0:0:45 (4,319)	0:1:43 (11,077) 0:04:39** (25,850)**	25%, 42.6 MB
FTK	13	0:02:32 (4,474)	0:02:23 (4,596)	0:03:08 (4,700)	0:03:37 (45,662)	0:03:30 (46,842)	80%, 500MB
Encase 6	?	NA	NA	NA	NA	NA	--
Encase 8	329	0:0:13 (2,031)	0:0:19 (4,486)	0:0:31 (8,220)	0:1:43 (29,787)	> 4:0:0 (777) *	19%, 5800 MB
G5							
X-Ways	333	0:0:23 (2,262)	0:0:22 (2,270)	0:0:30 (2,525)	0:0:44 (4,319)	0:01:38 (11,077) 0:04:08** (25,850)**	5%, 50MB
FTK	13	0:02:30 (4,536)	0:02:31 (4,584)	0:02:37 (4,950)	0:03:04 (48,822)	0:02:58 (54,284)	--
Encase 6	?	NA	NA	NA	NA	NA	--
Encase 8	329	0:02:16 (2,031)	0:02:40 (4,486)	0:03:32 (8,223)	0:9:53 (29,787)	>10:0:0 (777) *	5%, 4200 MB

https://binaryforay.blogspot.com/2016/09/let-benchmarks-hit-floor-autopsy-vs.html

Les domaines de l'investigation numérique



Diplômes et certifications

Job board search results (in alphabetical order, by certification)*

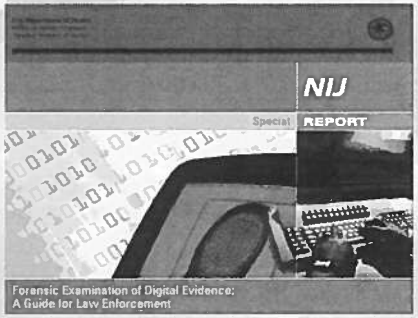
	SimplyHired	Indeed	LinkedIn Jobs	LinkUp	Total
Vendor neutral					
CFCE (IACIS)	65	82	117	46	308
CHFI (EC-Council)	106	140	255	68	567
GCFA (SANS GIAC)	477	489	857	294	2,062
GCFE (SANS GIAC)	203	226	433	143	1,005
Vendor specific					
ACE (AccessData)	25	29	31	12	97
EnCE (EnCase)	110	154	237	114	615

https://www.businessnewsdaily.com/10755-best-digital-forensics-certifications.html

- Quel prix ?
- Quelle notoriété ?
- Quelle durée de validité ?
- Couvrant quel domaine de compétence ?
- Formations métier ou formations outil ?
- La place donnée à l'expérience ?

Les guides méthodologiques

Digital Forensics Laboratory
Management and Procedures Guide



Les normes ISO/IEC

- ISO : norme définie par l'Organisation Internationale de Normalisation
- Standards et certification
- Réévaluation tous les 5 ans
- Quels impacts et à quels coûts ?
- ISO/CEI 17025 : laboratoires d'étalonnage et d'essai
- ISO/CEI 27k : 70 normes relatives à la sécurité des systèmes d'information (https://www.iso27001security.com/html/iso27000.html)
- ISO /CEI 27037 (2015) : Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques.
- Certification, coût et opposabilité… quels risques ?

Les acteurs de la preuve

Expert ou policier ?

Expert ou policier ?

- **57-1 CPP, extrait :**

  «... Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial... »

- **60 CPP, extrait :**

  « ...S'il y a lieu de procéder à des constatations ou à des examens techniques ou scientifiques, l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire a recours à toutes personnes qualifiées... »

- ***Article 156 CPP, extrait :***

  « Toute juridiction d'instruction ou de jugement, dans le cas où se pose une question d'ordre technique, peut, soit à la demande du ministère public, soit d'office, ou à la demande des parties, ordonner une expertise... »

Le policier expert

- *L'expert est celui qui a acquis une grande habilité par l'expérience, par la pratique* (Larousse)
- *L'expert est un spécialiste habilité auprès d'un tribunal ou d'une instance quelconque à émettre un avis sur une question exigeant des connaissances spéciales.* (Larousse)
- Il doit s'agir d'une activité accessoire, l'exercice d'une activité principale étant la base du niveau de compétence de l'expert.
- Article 156 et suiv du CPP et la loi n° 71-498 du 29 juin 1971
- *Toute juridiction d'instruction ou de jugement peut désigner un expert. Celui-ci est choisi sur sur la liste nationale dressée par la Cour de cassation ou sur une des listes dressées par les cours d'appel dans les conditions prévues par la loi précitée. A titre exceptionnel et sur décision motivée, un expert non inscrit peut être choisi. Il devra alors prêter serment d'accomplir ses mission, de faire son rapport et de donner son avis en son honneur et conscience.*
- L'expertise ne peut porter que sur l'examen de questions d'ordre technique.

Le policier expert (suite)

- L'expert doit notamment :
  - être indépendant (Civ. 1re, 6 juill. 2000, n°97-21.404), sous peine de nullité (Crim. 8 juin 2006, 06-81.359).
  - justifier de compétences reconnues pour exercer ou avoir exercé pendant un temps suffisant une profession ou une activité en rapport avec sa spécialité, et dans des conditions coférant une qualification suffisante (article 2 du Décret n°2004-1463 du 23 décembre 2004).
  - à l'issue de son travail rédiger un rapport contenant la description des opérations ainsi que ses conclusions.
- L'expert est habilité notamment à :
  - ouvrir et à reconstituer un scellé
  - travailler hors la présence du propriétaire du support numérique visé par l'expertise

Le policier expert (suite)

- L'expert doit notamment :
  - être indépendant (Civ. 1re, 6 juill. 2000, n°97-21.404), sous peine de nullité (Crim. 8 juin 2006, 06-81.359).
  - justifier de compétences reconnues pour exercer ou avoir exercé pendant un temps suffisant une profession ou une activité en rapport avec sa spécialité, et dans des conditions coférant une qualification suffisante (article 2 du Décret n°2004-1463 du 23 décembre 2004).
  - à l'issue de son travail rédiger un rapport contenant la description des opérations ainsi que ses conclusions.
- L'expert est habilité notamment à :
  - ouvrir et à reconstituer un scellé
  - travailler hors la présence du propriétaire du support numérique visé par l'expertise

Le policier expert (suite)

- Note DCPJ 9685 du 30 avril 2008 : les ESCI/ICC n'ont en général pas vocation à réaliser des expertises, missions réservées aux services centraux mais que celles-ci demeurent pourtant possible à titre exceptionnel si elles respectent les règles suivantes :

  (extrait)

  - l'expertise est un acte de service
  - la demande d'expertise doit être présentée au chef de service qui en apprécie le bien fondé.
  - le chef de service indique au magistrat le nom du fonctionnaire à même de remplir la mission **après s'être assuré que celui-ci n'a participé en amont, en aucune façon, à l'enquête dans laquelle l'expertise trouve son origine**
  - le rapport est signé du seul expert, et ne doit pas être établi sur papier à en-ête du service
  - le transmission du rapport est assurée par le chef de service et ne saurait intervenir sous couvert de la voie hiérarchique

Le policier personne qualifiée

- Base légale : la personne qualifiée est visée aux articles 60, 60-3, 77-1, 77-1-3 et 99-5 du code de procédure pénale. Elle peut, sur réquisition d'un officier de police judiciaire, procéder :
  - à des examens techniques ou scientifiques (60, 77-1 CPP)
  - et/ou à une copie de données dont le support a été placé sous scellé (60-3, 77-1-3 et 99-5 CPP)
- La personne qualifiée doit :
  - Si elle n'est pas inscrite sur les listes d'expert (157 CPP), prêter serment par écrit, d'apporter son concours à la justice en son honneur et sa conscience.
  - dresser l'invetaire du contenu du scellé
  - dresser un rapport de ces opérations
- La personne qualifiée peut :
  - agir hors présence du propriétaire du support numérique.
  - briser un scellé et le reconstituer le scellé à l'issue
  - Communiquer oralement ses conclusions aux enquêteurs en cas d'urgence

Le policier personne qualifiée

- Jurisprudence :
  - Crim 14/09/2005 : *les missions techniques confiées à une personne qualifiées sont de même nature que celles qui peuvent être confiées à un expert.*
  - Crim 04/11/1987 : *les mesures techniques qui ont pour objet la recherche et la constatation ne présente pas le caractère d'une expertise, d'où le cantonnement à des questions d'intérprétations technique.*
- *Le policier ICC personne qualifiée :*
  - *Est titulaire de la qualification ESCI ou ICC*
  - *Est compétence uniquement pour ce qui relève de sa formation*
  - *Est indépendant au regard de la procédure et donc n'avoir participé en amont, en aucune façon, à l'enquête dans laquelle la réquisition trouve son origine.*
  - *doit prêter serment par écrit, d'apporter son concours à la justice en son honneur et sa conscience.*

Des questions ?

Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 2 : preuve numérique et support numérique

[redacted] – Maroc - 2019

FBI Computer Analysis and Response Team (CART)

1) Quels supports ?

2) Les phases de l'exploitation

3) Focus sur la collecte (hash, copie, original)

4) L'analyse ?

Quels supports ?

Quels supports numériques ?

- Systèmes de stockage numériques utilisés dans les ordinateurs tels que les disques durs, clés USB, disquettes, disques optiques, etc.
- Supports mobiles tels que les téléphones, smartphones, tablettes tactiles, cartes mémoire, etc.
- Systèmes de navigation de type GPS
- Systèmes numériques de photographies et de vidéo
- Ordinateurs classiques avec connexion réseau
- Systèmes de réseau et appareils associés
- Objets connectés tels que véhicules connectés, appareils de domotique connectés, etc.

Support et donnée

- Tout système de stockage contenant de la donnée numérique et accessible physiquement au spécialiste
- 57-1 CPP extrait : *« ...accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système... »*
- Par opposition aux données contenues dans des systèmes de stockage non accessibles physiquement au spécialiste autrement que par un réseau
- 57-1 CPP extrait : *«...données intéressant l'enquête en cours et stockées ...dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial… »*

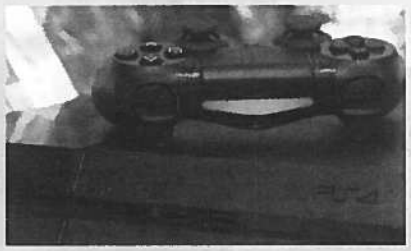
Les phases de l'exploitation

Les phases de l'exploitation

Prise en comte de la mission

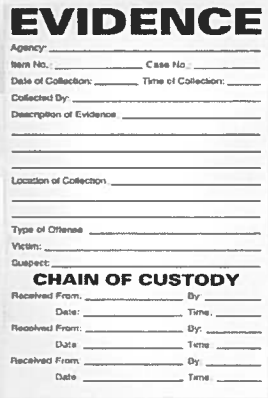
- Quelques pistes pour prendre en compte une mission :
  - Le bon interlocuteur
  - Le contexte du dossier
  - Le cadre juridique
  - L'objet de la mission
  - La préparation (matériel, briefing, ...)
- La présence du primo intervenant ou du spécialiste dans la phase d'identification est-elle nécessaire ?
  - L'importance du numérique dans la mission ?
  - Du support facilement identifiable aux supports dissimulés ou maquillés
  - Ah bon, ça aussi cela contient de la donnée ?

Identification



Identification et attribution

- A qui appartient le support original ?
- Quel sera le parcours du scellé, depuis sa saisie jusqu'à sa présentation au procès pénal
- La chaîne de la preuve (chain of custody)
- Et si le scellé n'est pas intègre quand il arrive à l'expert ?
- Et si l'objet est endommagé ?
- Et si l'examen des données démontre un accès postérieur à la saisie et non référencé en procédure?



EVIDENCE

Agency: _____

Item No.: _____ Case No.: _____

Date of Collection: _____ Time of Collection: _____

Collected By: _____

Description of Evidence: _____

Location of Collection: _____

Type of Offense: _____

Victim: _____

Suspect: _____

CHAIN OF CUSTODY

Received From: _____ By: _____

Date: _____ Time: _____

Received From: _____ By: _____

Date: _____ Time: _____

Received From: _____ By: _____

Date: _____ Time: _____

Préservation

- De la protection de la scène de crime à la protection de la preuve numérique
- Le scellé : inviolabilité, inaltérabilité
- Le scellé numérique
  - Plus aucun accès possible à la donnée physiquement
  - Plus aucun accès possible à la donnée via un réseau
  - Les supports magnétiques et les risques de destruction
- Maintien en tension et méthodes de déverrouillage
- Documenter, documenter, documenter…

Focus sur la collecte (hash, copie, original)

Collecte

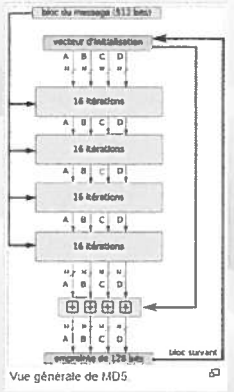
- La répétabilité : Un investigateur doté du savoir-faire requis doit être en mesure d'obtenir le même résultat qu'un autre investigateur doté d'un savoir-faire similaire, travaillant dans des conditions similaires
- La sacro sainte copie
  - Copie physique
    - Format brut ou sans compression (raw, dd, dmg)
      - Taille
      - Altérabilité
    - « expert witness format » (E01, AFF4,...)
      - Compression
      - Log de hash inclu
  - Copie logique
    - Altérabilité

La fonction de hachage

- Fonction de hachage, calcul de hash, somme d'intégrité, condensat, ...
- Calculer une empreinte numérique à partir d'une donnée

$$\forall (x,y) \in S^2, r_o(x,y) \Rightarrow r_o(f(x), f(y))$$

- Au moindre changement de la donnée, le hash sera différent
- S'applique à :
  - Une suite de caractère comme un mot
  - Un fichier
  - Une partition
  - Un volume de stockage complet



Vue générale de MD5

Fonction de hachage (suite)

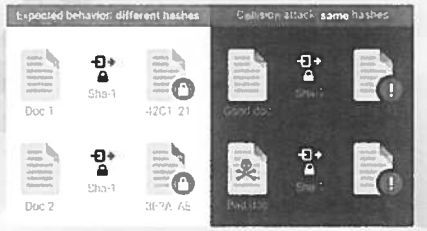
- Formats multiples

Message original	MD4	MD5	SHA-1
Zeste de savoir	7096e36e73cf1a30cd28b603bfb88226	2c598f7a0d3f68686e417ee1ff8aa152	b90f6190fa742e60e93971ee9c4a0764b9de9b8f
Zeste de savoire	52d43d8cf1b544ba65b3fd5d7db2907a	734ad14eea9d911ba6cf2a34f020b8da	b78d3b92624f0cb684474cb8b8511403dace4b79
Roger le tavernier	4ef1e80cfa57834cc856b9787970ce7e	ff9e99da9c27f04e07d9298a7547885f	26d352c29085348a163728def59253d63ba449ce

- A quoi ça sert ?
  - Vérifier un fichier téléchargé
  - Vérifier si un fichier est présent au milieu de 100 000 autres ?
  - Vérification de mot de passe sans tous les stocker en clair
  - Vérifier si la copie est identique à l'original
  - Etc.
- Combien de temps ?

Fonction de hachage (suite)

- La gestion des erreurs
  - Si le support physique est défectueux à l'origine ?
  - Si la panne ou le crash d'un bloc intervient entre deux phases de vérification ?
  - Le hash par bloc ?
- Les collisions
  - La fonction de résistance à la collision
  - La probabilité de collision
  - MD5 : 1ère collision en 1996
  - SHA1 : collision officielle en 2017, mais suspicions depuis 2011
  - Associer deux calculs de hash en vérification de copie ?



Copie et SSD

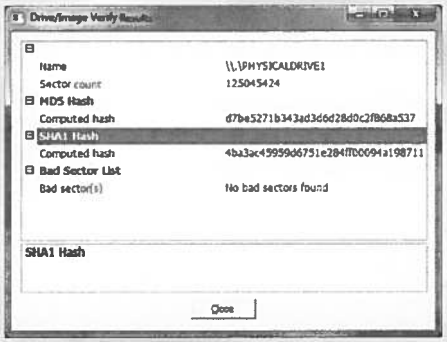
- Plus rapide, plus résistant, moins encombrant
- La mémoire flash
  - Je n'écris pas si ce n'est pas propre, donc je nettoie dès que j'ai un moment de libre (fonction TRIM)
  - J'utilise prioritairement les blocs vides et les moins utilisés car mes cellules ont une fin de vie (le garbage collector)
- La fin de la récupération de données effacées ?
- La fin de la vérification par calcul de hash ?

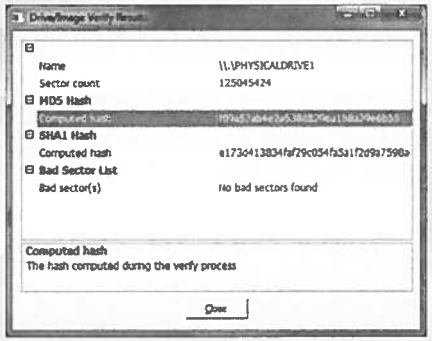
Copie et SSD

- Plus rapide, plus résistant, moins encombrant
- La mémoire flash
  - Je n'écris pas si ce n'est pas propre, donc je nettoie dès que j'ai un moment de libre (fonction TRIM)
  - J'utilise prioritairement les blocs vides et les moins utilisés car mes cellules ont une fin de vie (le garbage collector)
- La fin de la récupération de données effacées ?
- La fin de la vérification par calcul de hash ?

Copie et SSD

Deux hash générés sur un même support, à une heure d'intervalle





Copie, mémoires soudée et chiffrement

- Les mémoires soudées :
  - Développement des portes ultra transportables
  - Copie logicielle (Paladin, Darwin, ...)

- Le chiffrement
  - Bitlocker, Filevault, ...
  - Mac : fusion drive, chip t2, ... (avant les solutions)

- Quid si le spécialiste forensics n'a pas le bon équipement à l'instant T ?

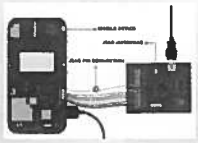
Copie et support mobile

- Exit les règles sacrées de l'analyse numérique ?
- L'impossibilité d'accéder à la donnée d'une manière forensique
  - Copie logique
  - Back up
  - Méthode agent
  - Downgrade apk
  - Etc.
- Des outils automatisés
- Les logs d'activité
- Cip off et JTAG

MSAB XRY XAMN

OXYGEN FORENSICS

Belkasoft



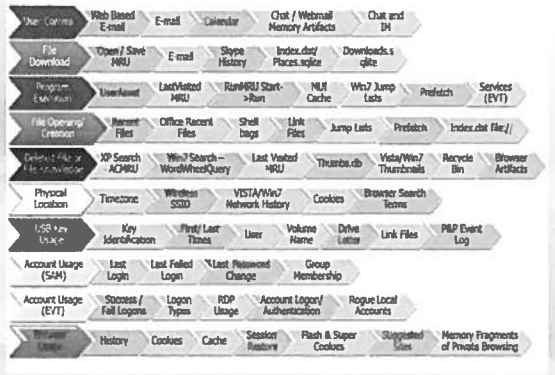
Travailler sur l'original

- C'est mal…
- Les bloqueurs en écriture
  - Logiciels ou matériels ?
  - Différentes connectiques
  - Accès externe ou interne (shadow3)
  - Oui mais les SSD alors ?
  - Oui mais les supports mobiles ?
- C'est mal… mais on le fait… et souvent !

L'analyse ?

L'analyse

- Données présentes
  - Accessibles ?
  - Humainement intelligibles ?
  - Méta données
  - Données système
- Données effacées
  - Complètes
  - Incomplètes
  - Corrompues

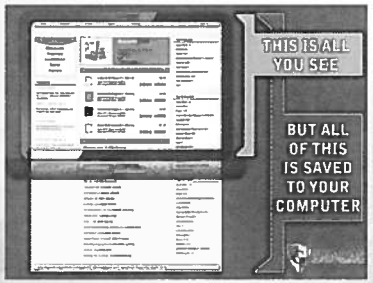


https://digital-forensics.sans.org/blog/2012/01/25/digital-forensic-sifting-colorized-super-timeline-template-for-log2timeline-output-files/

- Données bien documentées et données complexes

L'analyse

- Le problème, c'est :
  - La masse d'information
  - Le temps
  - Savoir ce que l'on cherche
  - Ne pas passer à côté…



- Le meilleur expert du monde peut toujours passer à côté d'une donnée
- Discrimination, analyse rapide et expertise
- *Rendez-vous au module « Compte rendu d'analyse » pour aller plus loin…*

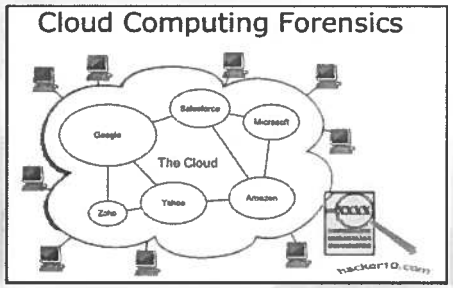
Des questions ?

Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 3 : preuve numérique et données stockées à distance

[redacted] · Maroc - 2019



1) Législation

2) Cloud et forensique

3) Focus sur un outils automatisé

La législation

Opérateurs privés et données de trafic

- L'accès le plus simple à la donnée stockée à distance : requérir l'opérateur qui la détient
- Convention de Budapest, article 18 – Injonction de produire
- France, 60-1, 77-1-1 et 99-3 CPP (accès aux documents) et 60-2 al1, 77-1-2, 99-4 al1 CPP (communication d'information)
- Jurisprudence : arrêt du 6 novembre 2013 dit Ciprelli (Crim., 6 novembre 2013, n° 12-87.130)
  - *communication, sans recours à un moyen coercitif,*
  - *hors le contenu des correspondances échangées,*
  - applicable aux sociétés étrangères : « *ladite société restant, dans ce cas, libre de ne pas y répondre* »

Opérateurs privés et données de contenu

- Réquisitions aux fin de préservation du contenu, articles 60-2 alinéa 2 (enquête de flagrance), 77-1-2 alinéa 2 (enquête préliminaire) et 99-4 alinéa 2 (information judiciaire)
- Production du contenu sur autorisation du juge des libertés et de la détention requis par le Procureur de la République, ou sur autorisation du juge d'instruction
- Ce régime s'explique par le caractère attentatoire à la vie privée de cette réquisition.
- Hors cas de menace imminente grave sur l'intégrité physique d'une personne, les données avancées et les données de contenu ne peuvent être obtenues que sur la base d'une demande d'entraide.

Interception des données

- Données de trafic : Convention de Budapest, article 20 - Collecte en temps réel des données relatives au trafic
- Données de contenu : Convention de Budapest, article 21 – Interception de données relatives au contenu
- Interception de correspondance en France : criminalité organisée et terrorisme, articles 706-95 et 74-2 du code de procédure pénale (flagrance et préliminaire), et articles 100 à 100-7 et 80-4 (commission rogatoire)
- Conversations émises depuis la France vers l'étranger ou depuis l'étranger et entrant en France (Crim., 1er février 2011, n° 10-83.523).
- Interception à l'étranger sur demande d'entraide internationale uniquement (Crim., 27 juin 2001, n° 01-81865).

Les correspondances stockées

- Criminalité organisée et terrorisme, sur autorisation du juge des libertés et de la détention (article 706-95-1 CPP)
- *« ...accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique... »*
- Obtention préalable d'un couple identifiant/mot de passe

USA, le Cloud Act

- Le *Stored Communications Act* de 1986
  - Obligation d'une demande d'entraide judiciaire internationale, fondée sur des traités bilatéraux (MLAT)
  - Issu des suggestions de la Convention de Budapest sur les traités bilatéraux
- Modifié par le *Cloud Act* du 23 mars 2018
  - FBI vs Microsoft, compte Outlook stockée en Irlande
  - Communication des *"contenus de communications électroniques et tout enregistrement ou autre information relatifs à un client ou abonné, ...* [qu'ils] *soient localisés à l'intérieur ou à l'extérieur des Etats-Unis".*
  - Sans que la personne "ciblée" ou que le pays où sont stockées ces données n'en soient informés.

Europe, le règlement « E-evidence »

- Texte proposé par la Commission Européenne le 17 avril 2018
- Une riposte au Cloud act ?
- L'injonction européenne de production :
  - permettre à une autorité judiciaire d'un Etat membre de demander des preuves électroniques directement auprès d'un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre, indépendamment de la localisation des données
  - délai de 10 jours, et dans les 6 heures en cas d'urgence (contre 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire)
- L'injonction européenne de conservation
- Obliger les sociétés proposant un service dans l'Union à avoir un représentant légal dans l'Union

Données publiques

- Donnée publique ou privée ?
  - Accessible à tous, sans condition
  - A l'exclusion de tout espace de discussion nécessitant une inscription ?
    - Forum sur Internet
    - Conversation ou fil de discussion (Telegram par exemple)
- Préserver l'intégrité de la preuve, Cour de cassation, 8 janvier 2019, N° de pourvoi: 18-80748
  - *« le constat d'huissier sur internet doit répondre à des règles techniques garantissant sa fiabilité et sa force probatoire, afin d'éviter que le matériel utilisé ne vienne interférer avec le contenu du site internet sur lequel il est effectué »*

Données publiques

- Vider le cache du navigateur de l'ordinateur afin d'éviter qu'un site qui aurait été préalablement visité ne conserve dans l'ordinateur de constatations des images ou données qui auraient été changées par la suite.
- Supprimer l'ensemble des cookies, les fichiers temporaires et l'historique de navigation avant les constatations.
- Horodater son intervention (pour assurer le suivi ultérieur des actions de l'enquêteur).
- Sauvegarder la page internet où sont réalisées les constatations
  - au format html
  - avec des copies d'écran
  - « outil capture » intégré à Windows depuis 7
  - Utiliser un outil dédié ? (Forensic Acquisition of Websites, Single file sous Firefox, HTTrack,...)

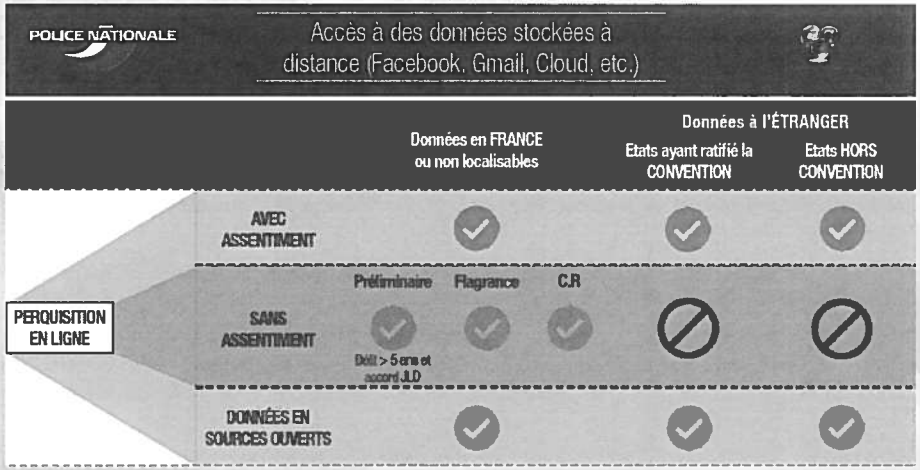
Enquête sous pseudonyme

- France : l'extension du régime avec l'article 230-46 créé par la loi du 23 mars 2019
- Infractions visées : les crimes ou délits punis d'une peine d'emprisonnement et commis par voir de communication électronique
- Enquêteurs habilités et affectés dans des services spécialisés
- Actes autorisés :
  - *Participer à des échanges électroniques, y compris avec les personnes susceptibles d'être les auteurs de ces infractions ;*
  - *Extraire ou conserver par ce moyen les données sur les personnes susceptibles d'être les auteurs de ces infractions et tout élément de preuve*
  - *Après autorisation du procureur de la République ou du juge d'instruction saisi des faits, acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite, ou transmettre en réponse à une demande expresse des contenus illicites.*

Données stockées à distance et supports numérique

- France : 57-1 CPP
  - Pendant la perquisition, accès aux données accessibles depuis le système initial
  - De retour au service, dans le respect des règles de la perquisition, accès accessibles depuis le système initial
  - S'il est avéré que les données sont stockées à l'étranger, respect des règles internationales.
- Europe : Convention de Budapest, article 32
  - Accès aux données stockées dans un autre Etat partie, avec le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Synthèse



Cloud et forensique

Cloud et règles forensiques

- Le stockage est différent
  - pas d'accès direct à la donnée, pas de container physique exploitable, de localisation classique forensique avec offset ou 1er secteur.
  - Uniquement des containers logiques qui sont téléchargés
  - accès uniquement via les API et le scraping
- La méthodologie est différente
  - pas de comparaison possible entre l'original et la copie quand on fait un backup de type Google takeout
  - les données peuvent varier en fonction du mode de copie/extraction (taille d'une image via une capture écran ou un backup)
  - pas de contrôle total de la procédure de copie extraction quand elle est proposée par le cloud service

Cloud et règles forensiques

- les fichiers n'ont pas toujours de métadonnées complètes (auteur, appareil de prise de vue, etc.)
- certains horodatages disparaissent (mactime) ou sont modifiés (par défaut, l'horodatage d'une donnée est fourni en local time)
- difficultés d'attribution : synchronisation de certains services sur plusieurs appareils. Comment déterminer quel appareil a réalisé l'action ? (ex. Chrome)

- Le consentement ?
  - accord librement consenti par une victime, un témoin
  - accord libre et légal d'un usager suspect d'être l'auteur de l'infraction
  - autorisation du juge (en fonction du cadre légal)

Cloud et règles forensiques

- A qui appartient la donnée ?
  - Le fournisseur de service ? Ou l'usager ?
  - Ex des résiliations unilatérales de compte sur violation des CGU (Google, Facebook, ...)
  - Qu'est ce qu'un ayant droit sur la donnée ?
    - Usager ? Fournisseur de service ? L'Etat de résidence de l'usager, du fournisseur de service ?
- Accès à la donnée ?
  - identifiants et mots de passe données par le suspect
  - identifiants et mots de passe découverts par l'enquêteur mais sans accord de l'intéressé
  - token (jeton) d'activation disponible sur un support numérique (ordinateur, téléphone...)

Cloud et règles forensiques

- Problématique d'accès
  - Authentification avec multi facteurs (vérification par un autre mail, un SMS, etc.)
  - Avertissement au titulaire du compte
  - Variation des techniques d'accès en fonction du service et de sa version

Les outils spécialisés

- Multiplicité d'outils : UFED Cloud Analyzer, XRY Cloud, AXIOM Cloud, ...
- Les services pris en charge varient d'un outil à l'autre mais on retrouve les classiques Facebook, Twitter,Gmail, Google, Dropbox, Instagram, What's App, iCloud, Snapchat, ...
- Quelles possibilités ?
  - acquisition sélective de la donnée (par artefact, par date, etc.)
  - récupération automatisée de token
  - Utilisation d'un mot de passe renseigné manuellement
  - Sécurisation de l'extraction (pas d'effacement des données originales, logs d'audit,...)
  - Traitement facilité pour l'enquêteur (interprétation des données visuelle, corrélation entre les données, ...)
- Une plus value AXIOM : partenariat avec Grayshift et récupération de keychain sur IOS

Focus sur un outil à titre d'exemple

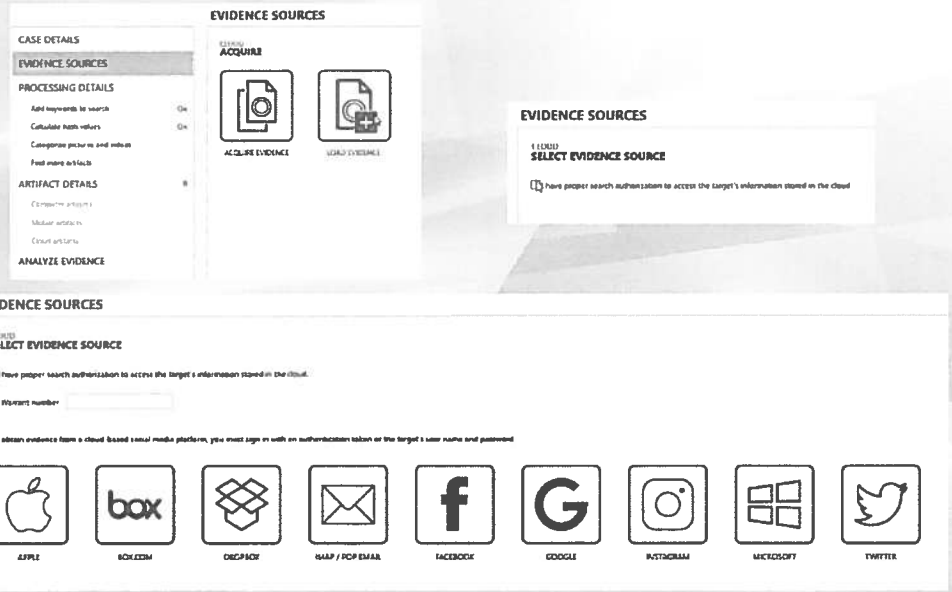
Un exemple, AXIOM

- Organisation : Dashboard / Artefacts / Connexions / File system / Registry / Timeline
- Visualisation : Gallerie / Colonne / Conversation / etc.
- Association de plusieurs sources de données (ordinateur, capture de RAM, Cloud, …)
- AXIOM ressource :

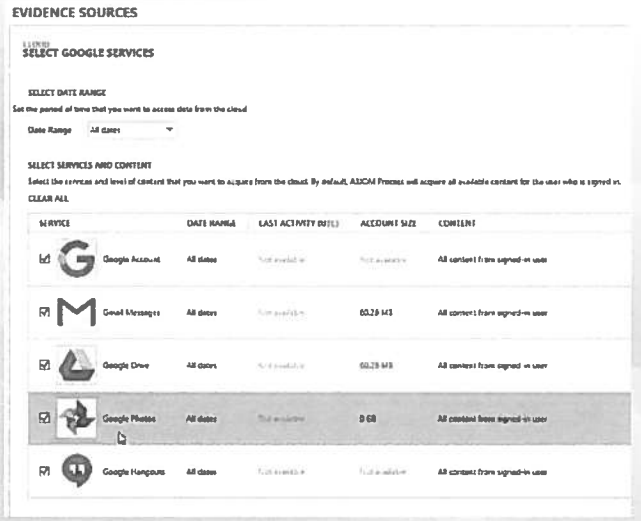
  https://www.magnetforensics.com/resources/

  https://www.magnetforensics.com/resources/getting-started-magnet-axiom/

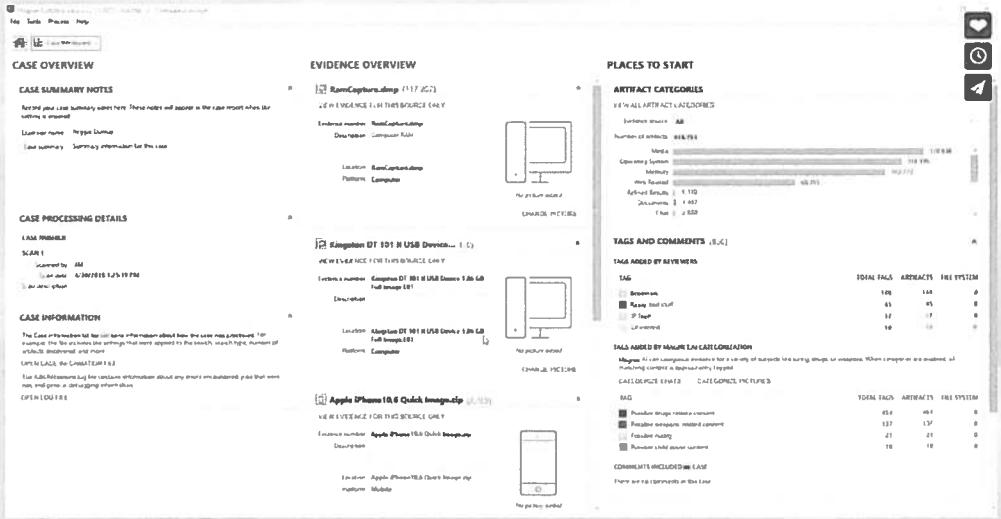
Un exemple, AXIOM



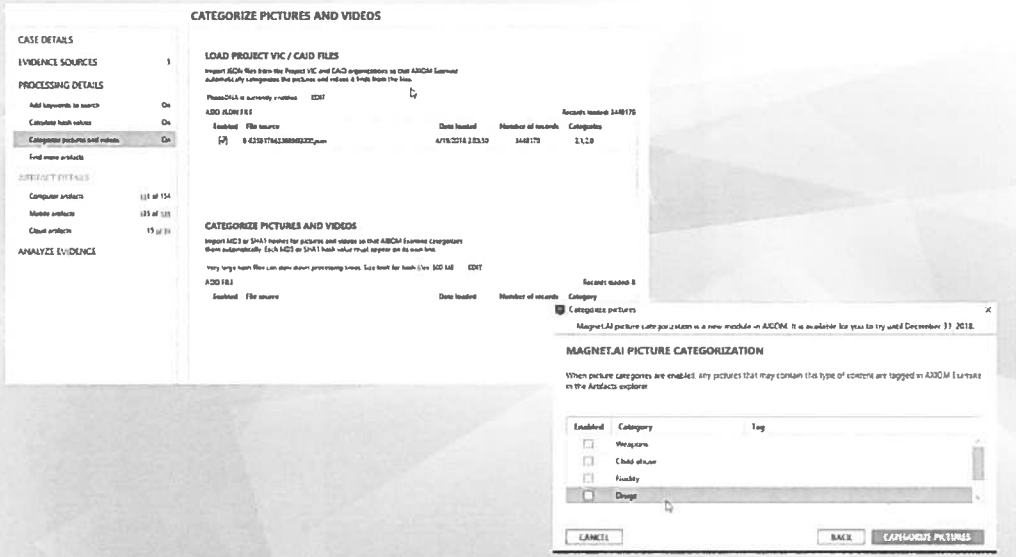
Un exemple, AXIOM



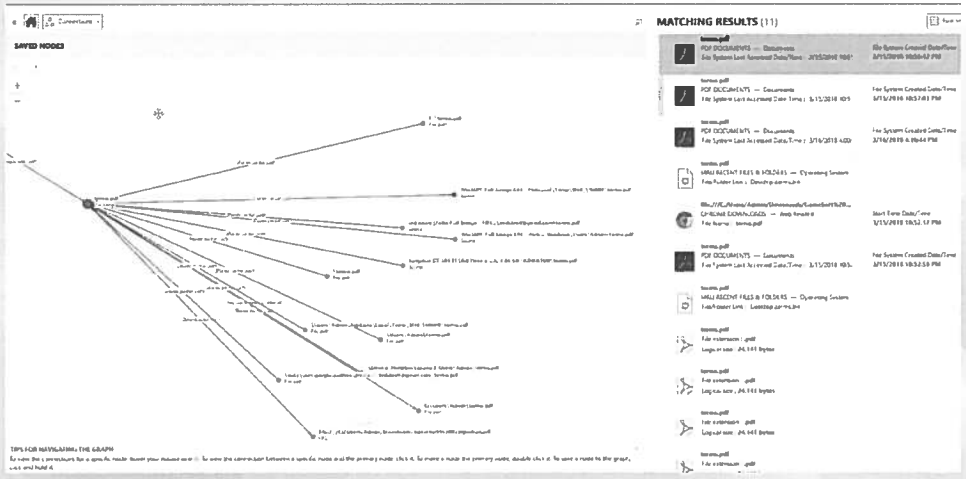
Un exemple, AXIOM



Un exemple, AXIOM



Un exemple, AXIOM



Des questions ?

Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 4 : Anti forensic, live forensic et méthodes de discrimination

· Maroc - 2019

1) Ce qui gêne l'accès à l'information

2) Le live forensics

3) Vers des méthodes de discrimination ?

Ce qui gêne l'accès à l'information

Anti forensic, l'anonymisation

- Nous laissons trop de trace sur Internet
  - http://www.anonymat.org/vostraces/index.php
  - https://myshadow.org/fr/trace-my-shadow
  - https://addons.mozilla.org/fr/firefox/addon/lightbeam/
  - Back up Facebook ou Google...
- Si c'est gratuit, c'est vous le produit
- Une volonté légitime de préserver sa vie privée

1. Créer des mots de passe solides.
2. Prévenir l'usurpation d'identité
3. Demander le déréférencement d'un contenu vous concernant.
4. Distinguer sphère privée/publique.
5. Faire attention aux publications sensibles.
6. Effacer ses données de navigation.

20 juil. 2017

Protéger sa vie privée en 6 étapes | CNIL
https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes

Anonymisation et cyber café

- Les cyber cafés sont soumis aux règles de conservation de données des fournisseurs d'accès Internet, en France, 1 an
- Des logs de connexion... euh, oui ?
- La vidéo surveillance, ah, en panne...
- La comptabilité, vous savez, on paye beaucoup en liquide ici
- Les ordinateurs, on les ghost toutes les semaines, pour éviter les virus
- Un cas concret, le dossier Sophie LETAN, disparue le 7 septembre 2019

Anonymisation et hot spot

- Wardriving : https://wigle.net/
- https://www.aircrack-ng.org/
- Octobre 2018, publication d'une faille WPA2
  (https://www.lesnumeriques.com/informatique/decouverte-d-methode-simple-pour-craquer-wi-fi-wpa2-n79795.html)
- Dossier Nantes, 2018. Et si les hot spots devenaient une source d'information ?

Anti forensic, anonymisation

- Proxy
  - Logiciel ou service
  - Interface origine/cible
- VPN
  - Logiciel ou service
  - Tunnel sécurisé
- TOR, et les autres
  - Réseau indépendant
  - Anonymisation et sites onion
- Navigation privée

Anti forensic, chiffrement

- Chiffrement et code de verrouillage
- 434-15-2 Code pénal, le refus de remise d'une clé de chiffrement
- Conseil Constitutionnel, décision n° 2018-696 QPC du 30 mars 2018
- Tribunal de Nice, 16 mai 2019
  - Le code de verrouillage du téléphone n'est pas un moyen de cryptologie
  - Aucun élément de l'enquête n'indiquait que le téléphone visé contenait des données utilisées pour préparer ou faciliter un délit
  - La demande du code par un policier n'est pas une demande de l'autorité judiciaire (magistrat, institution de jugement)
- Tribunal de Belfort, 5 juin 2019
  - Il refuse de donner son code de verrouillage et est condamné à 3 mois de prison

Anti forensic, effacer ses traces

- *Logiciels de nettoyage (Ccleaner, Bleachbit, Privazer, …)*
- *Wipe (HDShredder, Dban, HDDerase, …)*
- *Destruction de matériel*
- *Deux dossiers sur le Darnet*
  - *Black Hand*
  - *French Deep Web*

Le live forensics

Le live forensics, pourquoi ?

- La généralisation du chiffrement (bitlocker, truecrypt, filevault 1 ou 2, veracrypt, pgp ….)
  - Filevault et bitlocker peuvent se désactiver si la session est active
  - Il est possible d'exporter la clé de mise au clair
  - Il est toujours possible de faire une copie logique des données
- L'augmentation de la taille de la mémoire vive
  - Quelques précisions
    - Pour accélérer le temps de traitement de l'information, et améliorer l'expérience de l'utilisateur, le système n'écrit pas toutes les données utiles et en stocke une partie dans la mémoire vive (RAM)
    - Celle-ci se vide quand elle n'est plus alimentée en électricité

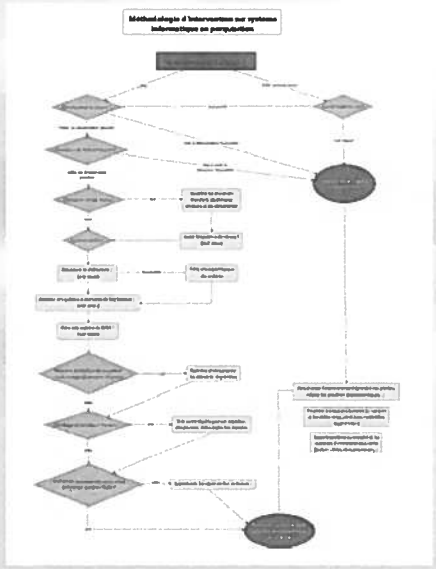
Le live forensics, pourquoi ?

  - La mémoire vive peut contenir :
    - Des mots de passe
    - Des documents en cours d'écriture mais non encore enregistrés
    - Des éléments relatifs aux programmes en cours
    - Etc.
- L'importance croissante du stockage de données à distance
  - Réseaux sociaux
  - Stockage à distance
  - Services externalisés
  - Etc.

Le live forensics, pourquoi ?

- La multiplication des supports numériques et de leur taille
  - De 1956 (5mo) à 2019 (6to), la taille moyenne d'un support a été multipliée par 1200
  - En perquisition, de 1 à 2 supports par foyer à 10 en moyenne
- Certains supports ne s'exploitent qu'en live forensics
  - Box internet (disques souvent chiffrés nativement, données dépendantes de la connexion du domicile)
  - Consoles de jeux (disques nativement chiffrés, systèmes de fichier atypiques)
  - Smart TV (démontage très complexe, navigation facilitée par télécommande utilisateur)

Proposition de méthodologie



Vers des méthodes de discrimination ?

Discrimination, pourquoi ?

- Parce que :
  - Toutes les enquêtes ne nécessitent pas des expertises
  - Tous les mis en cause n'ont pas la même importance dans une enquête
  - Tous les supports numériques ne sont pas susceptibles d'apporter des éléments utiles à l'enquête
  - Le délai disponible pour l'analyse numérique est insuffisant
  - Le nombre de spécialistes n'est pas toujours suffisant
  - Le matériel forensic disponible n'est pas toujours suffisant
- S'adapter, une obligation des services de police
- Et parce que tout dépend des besoins réels de l'enquêteur

Tout prendre ou pas ?

- L'intérêt d'un support dépend d'abord du dossier
  - Il y a t'il des dossiers pour lesquels le numérique est inutile ?
  - Les éléments déjà présents en enquête sont-ils suffisants ?
  - Ces éléments sont-ils incontestables ?
  - Tous les aspects de contexte sont-ils explorés ?
  - Etc.
- Sélectionner les supports
  - En fonction de leur nature ?
  - En fonction de leur dernière date d'utilisation présumée ?
- Il y a t'il des dossiers pour lesquels ont ne peut pas se permettre d'écarter quoi que ce soit ?

Traiter pendant la perquisition

- La perquisition permet :
  - De saisir les supports en vue d'un traitement ultérieur
  - De copier les données en vue d'un traitement ultérieur
  - De traiter les données sur place
- Une obligation, s'adapter au contexte :
  - Les données non exploitées seront-elles accessibles après la perquisition ?
  - Est-il possible de prolonger la perquisition ?
  - Le gain de temps en perquisition est-il utile ?
- Que peut-on dire en quelques minutes ?
  - Vérifier si le support est est exploitable ou HS
  - Dater sa dernière utilisation
  - Déterminer son utilisation générale et corréler cette information au contexte de l'enquête

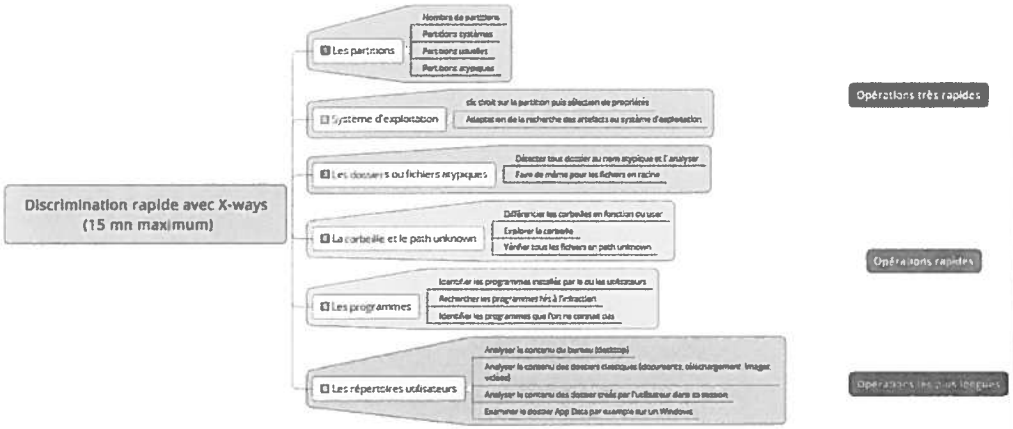
Priorisation

- Le dialogue entre l'expert et l'enquêteur
  - Comprendre les besoins de l'enquêteur
  - Proposer les actes techniques susceptibles de correspondre
  - Evaluer la durée probable de réalisation de ces actes
- Hiérarchiser l'ordre de traitement des supports en fonction des besoins de l'enquêteur
- Limiter les axes de recherche en fonction du type de dossier et du besoin de l'enquêteur
- Ne rien figer et garder une souplesse en fonction :
  - Des éléments découverts
  - De l'arrivée de nouveaux supports au fur et à mesure de la mission
- Les contraintes légales (ex de la copie obligatoire en commission rogatoire)
- Les contraintes techniques (ex de l'extraction sur supports mobiles)

Objectifs

- A l'issue de la discrimination, l'analyse sera en mesure
  - d'exposer tous les axes de recherche qu'il a traité,
  - à quel niveau de profondeur,
  - de préciser ce qu'il n'a pas fait en raison de la demande, du temps imparti, etc.
  - de conclure avec une des options suivantes
    - expliquer si le support analysé contient des éléments pertinents pour l'enquête, lesquels et de les présenter de manière exploitable pour l'enquêteur.
    - expliquer si l'exploitation n'a pas permis la découverte d'éléments pertinents dans le temps imparti
    - informer l'enquêteur que le délai prévu nécessite une nouvelle évaluation de sa part en raison de la découverte d'une complexité technique, de beaucoup d'informations pertinentes, etc.

Méthodologie



Le parcours visuel

- Délai : 15 à 30 mn
- Objectif : "prendre la température" d'un support
- Contraintes : toujours garder une trace de tout élément pertinent découvert
  - Association de table de rapport (Xways)
  - bookmark (Xways, IEF, UFED ou XRY reader)
  - Une simple une prise de note
- **Examen des partitions**
  - Identifier les partitions actives
  - Identifier la partition contenant le système d'exploitation (s'il y en a un)
  - Identifier la ou les partitions de données
  - Différencier les partitions en fonction du nombre de fichiers qu'elles contiennent, de leurs dates de création et d'accès.

Méthodologie de discrimination

- **Système d'exploitation**
  - Orienter l'analyse en fonction des artefacts et localisations propres à chaque système d'exploitation
  - Clic droit > propriété sur la partition sous Xways
- **Les dossiers ou fichiers atypiques**
  - Identifier un fichier atypique en raison de sa taille (les fichiers de machine virtuelle ou de container chiffrés sont en général volumineux ou ont une taille fixée précisément)
  - Identifier les dossiers ou fichiers dont les noms ont un lien potentiel avec l'enquête.
  - Explorer le répertoire racine en premier lieu, puis l'arborescence en recherchant tout nom de dossier ou de fichier inhabituel et/ou en lien avec l'enquête

Méthodologie de discrimination

- **La corbeille et les chemins inconnus**
  - Différencier les corbeilles en fonction de l'utilisateur
  - Rechercher tout élément en lien avec l'enquête
  - Rechercher tout fichier dont le nom est susceptible d'intéresser l'enquête
  - Passer en mode gallerie pour visualiser les images
- **Les programmes**
  - Orienter l'analyse en fonction des artefacts associés ou des fonctions spécifiques de certains programmes
  - Identifier tout programme permettant de découvrir de l'information (messagerie instantanée, mail, etc.)
  - Identifier tout programme susceptible de cacher ou d'effacer de l'information (chiffrement, nettoyeur, etc.)

Méthodologie de discrimination

- **Les répertoires utilisateurs**
  - Concentrer le parcours visuel sur les localisations les plus classiques de stockage d'information
  - Analyser tout le contenu du bureau (Desktop)
  - Analyser le contenu des dossier de stockage dédiés (documents, téléchargement, images, vidéo, etc.)
  - Analyser le contenu des dossiers créés et nommés par l'utilisateur
  - Examiner les dossiers de stockage de données habituels des programmes (App Data sur Windows, Library sur Linux, etc.)

Les tâches automatisées

- Adapter les tâches automatisées à la puissance de la machine
  - création du rapport de base de registre pour les systèmes Windows
  - fonction quick search d'Internet Evidence Finder
  - fonction refine volume snapshot de Xways ou Case processor avec Encase
    - sur un volume système, en discrimination, il est préconisé de le lancer sur le répertoire utilisateur pour une analyse rapide

La copie « enquêteur »

- Souvent, la mission de l'expert vise uniquement à faire une copie exploitable par l'enquêteur
  - Par manque de temps
  - Parce que l'enquêteur est celui qui connaît le mieux le dossier
  - Parce que l'enquêteur a les capacités techniques pour l'exploiter
  - Parce qu'il a de toute façon plus de temps que l'expert
- Outils dédiés : UFED, XRY, IEF/AXIOM
- Manuellement ?

Des questions ?