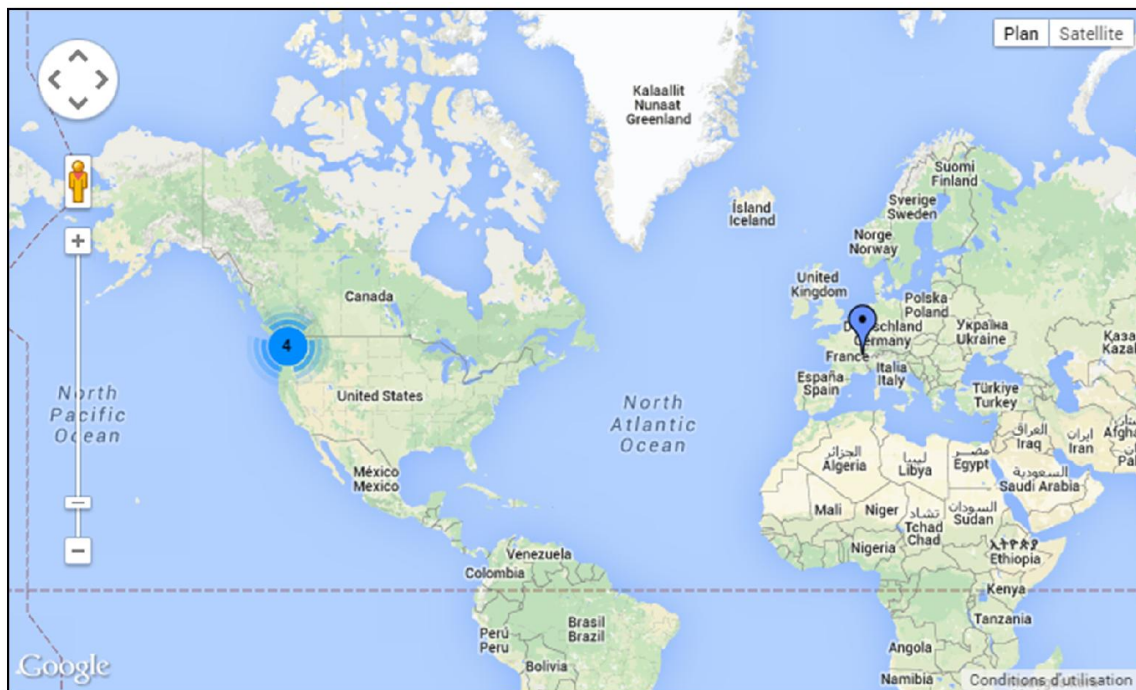


Mise en relation des données de géolocalisation lors de procédures pénales



Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Michael Laranjo

Conseiller au travail de Bachelor :

David BILLARD, Professeur HES

Genève, le 19 décembre 2014

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en Informatique de Gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : http://www.orkund.fr/student_gorsahar.asp.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 25 novembre 2014

Michael Laranjo

Remerciements

Tout d'abord, je tiens à remercier mon conseiller au travail de Bachelor, le professeur David Billard, pour avoir accepté de suivre ce projet et pour les conseils qu'il a pu me donner tout au long de ce travail.

Je remercie Daniel Lamas pour les conseils, les relectures et les corrections apportées à ce document.

Je tiens également à remercier Madame Geneau pour ses conseils concernant la mise en page de ce document.

Enfin, je remercie ma famille pour l'énorme soutien qu'ils m'ont apporté tout au long de ce travail.

Résumé

Ce travail traite le thème de la géolocalisation

La première partie présente ce qu'est la géolocalisation et l'histoire de celle-ci à travers le temps, tout en mettant en avant quelques faits historiquement marquants. Puis, quelques techniques utilisées à des fins de géolocalisation sont détaillées, pour finir avec le Wardriving.

La deuxième partie, quant à elle, parle plus précisément du smartphone et des emplacements internes qui sont susceptibles de contenir des informations de localisation. Le but étant de réussir à extraire des coordonnées GPS depuis plusieurs sources telles que les photos ou encore les fichiers systèmes d'un téléphone intelligent.

La troisième et dernière partie concerne la pratique du projet. Les divers choix technologiques sont abordés, ainsi que la structure de la base de données, tout en passant par les aspects importants de la programmation.

Le but de ce projet est d'une part de sensibiliser le lecteur à la géolocalisation. D'autre part, de fournir un outil capable d'acquérir, stocker et afficher des données d'emplacements géographiques extraits de téléphones intelligents.

Table des matières

Déclaration.....	i
Remerciements	ii
Résumé	iii
Liste des tableaux	vi
Liste des figures.....	vi
1. Introduction.....	1
2. Géolocalisation.....	2
2.1 Histoire	2
2.2 Les techniques utilisées.....	6
2.2.1 GPS	6
2.2.2 GSM.....	7
2.2.2.1 Identification du temps (E-OTD).....	7
2.2.2.2 Triangulation (TOA).....	8
2.2.2.3 Identification de l'antenne cellulaire (Cell ID).....	9
2.2.3 NFC	10
2.2.4 RFID	12
2.2.4.1 Tags actifs	12
2.2.4.2 Tags passifs	13
2.2.4.3 Tags semi-passifs	14
2.2.4.4 Nabaztag	14
2.2.5 Wi-Fi	15
2.3 Le Wardriving.....	16
2.3.1 Les débuts	16
2.3.2 Curiosité.....	17
2.3.3 Conséquences	23
3. Smartphones, où sont les données de géolocalisation ?.....	24
3.1 Le standard Exif	25
3.1.1 Une véritable mine d'informations	25
3.1.1.1 JPEG	25
3.1.2 Tags utilisés dans le cadre du projet	27
3.1.2.1 La date.....	27
3.1.2.2 La localisation.....	28
3.2 Les fichiers système	30
3.2.1 Android	31
3.2.1.1 Root.....	31
3.2.2 iOS.....	32
3.2.2.1 Sauvegardes Apple	32
3.2.2.2 Jailbreak	34
3.2.2.3 Lecture du fichier.....	34
4. Partie pratique	36

4.1	Choix technologiques.....	36
4.2	Base de données.....	37
4.3	Programmation.....	38
4.3.1	Outils.....	38
4.3.1.1	Logiciels.....	38
4.3.1.2	CSS	38
4.3.1.3	JavaScript.....	39
4.3.2	Fonctionnalités principales	39
4.3.2.1	Upload de photos avec coordonnées.....	39
4.3.2.2	GoogleMaps	41
4.3.2.3	Reporting	42
5.	Conclusion	43
	Bibliographie	44
	Annexe 1 : Glossaire.....	46
	Annexe 2 : Modèle physique de données	47
	Annexe 3 : Dictionnaire de données	48
	Annexe 4 : Dictionnaire de données (suite).....	49
	Annexe 5 : Vue graphique d'un fichier JPEG/Exif.....	50
	Annexe 6 : Fonctionnalité GoogleMaps au démarrage.....	51
	Annexe 7 : Fonctionnalité GoogleMaps après requête.....	52
	Annexe 8 : Fonctionnalité Reporting après requête	53
	Annexe 9 : Fonctionnalité Reporting après requête (suite).....	54
	Annexe 10 : Print Screen WinSCP Consolidated.db	55

Liste des tableaux

Tableau 1 : Coordonnées du jet d'eau de Genève	28
Tableau 2 : Programmes utilisés	38
Tableau 3 : Bibliothèques JavaScript utilisées.....	39

Liste des figures

Figure 1 : Boussole	2
Figure 2 : Sinan	2
Figure 3 : Boussole iPhone 3	3
Figure 4 : Représentation d'un radar	3
Figure 5 : Satellite GPS en orbite	4
Figure 6 : Magellan NAV 1000	4
Figure 7 : Benefon Esc!.....	5
Figure 8 : Représentation sommaire du GPS	7
Figure 9 : Schéma E-OTD	8
Figure 10 : Triangulation GSM	8
Figure 11 : Carte OpenCellID – Plaine de Plainpalais	10
Figure 12 : Etiquette NFC au musée	11
Figure 13 : Utilisations possibles du NFC	11
Figure 14 : Péage RFID	12
Figure 15 : Tag actif – Via Verde	13
Figure 16 : Intérieur du tag actif.....	13
Figure 17 : Ouverture/fermeture d'un véhicule Mobility.....	13
Figure 18 : Lapin RFID Nabaztag	14
Figure 19 : Antenne Wi-Fi externe montée sur une voiture.....	16
Figure 20 : Carte WiGLE - Suisse	17
Figure 21 : Légende Map	17
Figure 22 : Carte WiGLE - Genève.....	18
Figure 23 : Carte WiGLE – Mes réseaux	19
Figure 24 : Modem Linksys	20
Figure 25 : Routeur Asus.....	20
Figure 26 : Informations Générales	21
Figure 27 : Statistiques d'encryption Wi-Fi	21
Figure 28 : Réseaux dans la base de données.....	21
Figure 29 : Types d'encryptions.....	22
Figure 30 : Statistiques géographiques	22
Figure 31 : Structure d'un fichier Exif compressé	26
Figure 32 : Détail de la section APP1	26
Figure 33 : Google Maps - Emplacement [-34.866746°, -56.159582°].....	29
Figure 34 : Google Maps - Emplacement [34.866746°, 56.159582°]	29
Figure 35 : cache.cell & cache.wifi	31
Figure 36 : Exemple de contenu des fichiers cache.cell & cache.wifi	32
Figure 37 : Script Kettle	34
Figure 38 : SQLite Manager	35
Figure 39 : Représentation des composants WAMP	36
Figure 40 : Contraintes de clés étrangères	37
Figure 41 : Fenêtre modale – Ajout d'un nouveau marqueur	40
Figure 42 : Ajout d'un marqueur photo	40
Figure 43 : Upload de photos activé	40
Figure 44 : Upload de photos	41

Figure 45 : Exemple filtre < 1 km.....	42
Figure 46 : Exemple aucun marqueur dans l'enquête.....	42
Figure 47 : Exemple un marqueur dans l'enquête	42

1. Introduction

La géolocalisation, qu'est-ce que c'est ?

De mon point de vue, c'est un ensemble de techniques utilisées dans le but de trouver l'emplacement d'un objet. Ceci est possible grâce aux coordonnées géographiques récupérées de plusieurs façons.

La géolocalisation est massivement utilisée dans plusieurs domaines, et de plusieurs façons. C'est là qu'entre en jeu l'aspect technologique de la géolocalisation, dans lequel chaque technique possède ses avantages et ses inconvénients.

L'avènement des nouvelles technologies et notamment du smartphone, a permis une avancée dans ce domaine, car dorénavant tout possesseur d'un téléphone intelligent est dit « connecté », avec tous les avantages et inconvénients que cela implique.

Les applications installées sur les smartphones sont nombreuses à utiliser des données de géolocalisation. Certaines nécessitent de ses données d'une manière évidente, comme c'est le cas d'une application de navigation ou encore de recherche de commerces et restaurants aux alentours. D'autres applications ses données différemment, par exemple à des fins statistiques.

En plus des applications, il y a les systèmes d'exploitation de smartphones qui collectent des données relatives aux emplacements géographiques. Ces données font référence aux emplacements parcourus par toute personne propriétaire de l'un de leurs périphériques.

La Police Scientifique a également recours à ce procédé pour leur permettre d'en savoir plus à propos des personnes suspectes dans une enquête. C'est là que les téléphones des suspects sont analysés dans le but de trouver plus d'indications quant aux emplacements passés. Ce qui leur permet, en cas de réussite, de relier un smartphone à une zone dans laquelle un crime aurait été commis par exemple.

2. Géolocalisation

La géolocalisation est la science qui permet de localiser une personne ou un objet d'après son lieu géographique et de l'instant présent. Avant d'aborder les quelques-unes des techniques utilisées, il faut d'abord passer en revue quelques événements historiques ayant un lien avec la géolocalisation.

2.1 Histoire

Contrairement à ce que l'on pourrait croire, l'envie de l'être humain de calculer des distances et établir des plans date d'il y a fort longtemps. La suite de ce chapitre contient quelques explications à propos des technologies utilisées à travers le temps. Il aborde également quelques faits historiques qui ont changé la géolocalisation telle qu'on l'a connaît actuellement.

En se basant sur l'histoire de l'humanité, il faut remonter à la période de la Grèce antique, soit deux-mille ans en arrière, lorsque les hommes de sciences ont commencé à calculer des distances par triangulation avec les étoiles.

La boussole, outil disposant d'une aiguille magnétisée, sert aussi bien à la navigation maritime que pédestre (voir figure 1). La date de son invention reste controversée, car, bien que la boussole telle qu'on la connaît date du XII^{ème} siècle, les chinois se servaient bien avant d'une sorte de cuillère appelée Sinan et disposée sur un plateau qui indique le sud (voir figure 2).

Figure 1 : Boussole



(Source : Compass. wikipedia.org)

Figure 2 : Sinan



(Source : Boussole. chine-informations.com)

Figure 3 : Boussole iPhone 3



(Source : iPhone 3GS. macworld.com)

De nos jours, il est possible d'utiliser une boussole directement sur un smartphone. Certains d'entre eux disposent d'une application intégrée nativement, comme c'est le cas pour l'iPhone 3GS (voir figure 3).

Bien qu'il soit possible d'installer une application tierce afin de remédier à cette absence, celle-ci ne fonctionnera que si le smartphone dispose de la technologie nécessaire (capteur boussole).

Dans les années 1940, le radar est développé, et depuis, il est utilisé dans plusieurs domaines, tels que la navigation maritime ou sous-marine. Ce système permet le calcul de la distance et de la vitesse d'un objet, c'est donc un objet permettant lui aussi de calculer des emplacements. Le fonctionnement d'un radar nécessite de plusieurs éléments. Ceux-ci sont : un émetteur et un récepteur.

Figure 4 : Représentation d'un radar



(Source : Radar screen. dynastyfootballwarehouse.)

Le calcul d'une distance se fait grossièrement en trois étapes :

- Premièrement, l'émetteur envoie des ondes ;
- Deuxièmement, si les ondes émises entrent en contact avec un objet, elles sont réfléchies et captées par le récepteur ;
- Enfin, la dernière étape consiste à analyser la vitesse et l'angle de l'onde réfléchi afin de déterminer la distance parcourue par celle-ci.

Une fois que les données sont récupérées, il est alors possible de calculer la distance à laquelle l'objet se trouve.

Puis, vient le GPS, technologie connue de tous. Voici quelques faits historiques importants :

- En 1957, Spoutnik 1 est le premier satellite (voir figure 5) à être lancé en orbite par l'URSS. Cet événement, survenu en pleine période de « guerre froide », est considéré par beaucoup comme le début de l'ère spatiale, mais également ce qui a provoqué le début des recherches concernant le GPS.
- La fin des années 1950 et le début des années 60 marquent le début du guidage par satellite. Du nom « Transit », c'est le projet de l'armée américaine qui consistait à créer le premier système de navigation par satellite pour une utilisation militaire et non civile.
- Suite à une tragédie qui a eu lieu en 1983, pendant laquelle l'URSS avait abattu un avion de ligne coréen qui avait pénétré dans l'espace aérien soviétique, le président américain Ronald Reagan décida alors de rendre accessible le guidage par satellite pour les civiles, dans le but était de rendre plus sûre la navigation par la mer et les airs.

Figure 5 : Satellite GPS en orbite



(Source : GPS-Block-IIF-satellite. robohub.org)

En 1989, alors que les premiers satellites étaient lancés, le constructeur Magellan met à disposition sur le marché grand public le premier GPS autonome : le Magellan NAV 1000 (voir figure 6).

Figure 6 : Magellan NAV 1000



(Source : Commerical GPS Turns 25. mashable.com)

En 1995, le nombre de satellites en orbite s'élevait à 27 et le GPS était déclaré fonctionnel. L'infrastructure en place permettait le fonctionnement permanent du système, il disposait d'une précision d'environ 100 mètres pour un usage civil. Celle-ci était volontairement bridée, favorisant la précision à l'usage militaire.

Le premier téléphone portable muni d'une puce GPS a été lancé en 1999 par le constructeur finlandais Benetton : c'est le Benetton Esc! (voir figure 7).

Figure 7 : Benefon Esc!



(Source : Benefon. theapplecollection.com)

En mai 2000, le GPS connaît un changement important : la dégradation volontaire de la précision lors d'une utilisation civile est levée sous ordre du gouvernement américain. Le signal fourni est amélioré et la précision passe alors de 100 mètres à environ 10-15 mètres, ce qui a profité à diverses industries en plus des civiles. Cette période coïncide également avec celle du lancement de logiciels GPS, tels que Tomtom et Garmin, installés sur PDA.

En février 2005, Google lance Google Maps aux USA, le service de cartographie. Quelques mois plus tard, il a été lancé en Europe. Sa force principale est de mettre à disposition gratuitement des cartes du monde entier.

Le lancement en Europe, plus précisément au Royaume-Uni, correspond avec l'ajout de deux fonctionnalités : l'apparition des itinéraires entre deux adresses et un nouveau mode de vue avec des photos satellites.

Pour terminer ce chapitre historique, il convient de parler du projet Galileo, en route depuis une dizaine d'années. C'est un projet, auquel participent plusieurs pays européens, qui vise à développer un système de navigation par satellites concurrent au GPS, dans le but de devenir indépendants face au système américain. Initialement contre, les Etats-Unis participent à ce projet. La bonne nouvelle est que Galileo fonctionnera en parallèle avec le GPS, ce qui améliorera encore la précision et ne rendra pas obsolètes les périphériques de navigation utilisés actuellement.

2.2 Les techniques utilisées

Plusieurs techniques, basées sur différentes technologies, sont utilisées dans un même but : celui de récupérer des coordonnées géographiques permettant de localiser une personne ou un objet. Bien que plusieurs techniques existent, les plus connues restent le guidage par satellite ou encore la triangulation GSM.

Chaque technologie a des avantages et des inconvénients. C'est pourquoi, il n'est pas impossible que plusieurs de ces techniques soient employées simultanément dans le but d'obtenir un meilleur résultat, du point de vue de la précision ou de la vitesse d'obtention des informations.

2.2.1 GPS

Cette technique, très populaire, permet à un appareil d'utiliser le système de guidage par satellites. Des satellites tournent en orbite autour de la Terre et offrent une couverture dans les quatre coins du globe terrestre (voir figure 8).

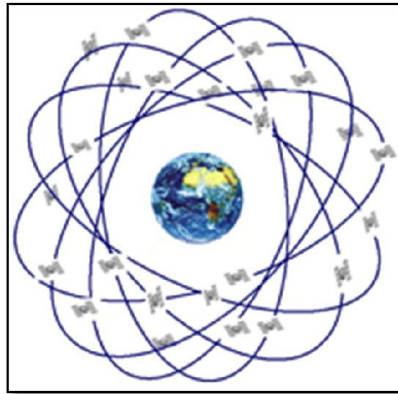
Voici une explication simple du procédé de la localisation par GPS :

- Réception des signaux
Grâce aux signaux envoyés par les satellites, chaque récepteur GPS connaît un certain nombre d'informations qu'il a capté. Plus précisément le temps pendant lequel les ondes ont parcourues la distance du satellite au récepteur.
- Mesure des distances
Le récepteur se sert de cette durée de transmission et utilise la vitesse de la lumière afin de calculer la distance qui le sépare de chaque satellite.
- Calcul de la position
Connaissant la durée de transmission des signaux et la distance qui le sépare de chaque satellite, le récepteur peut alors procéder à de calculs complexes qui auront comme finalité l'obtention de l'emplacement.

Les téléphones qui disposent d'une puce GPS ont la possibilité de connaître leurs emplacements. Celui-ci peut être utile lorsqu'un utilisateur désire utiliser une application de guidage.

D'ailleurs, de nombreuses applications gratuites et payantes existent. Pour les payantes, les plus connues sont Tomtom et Navigon. Alors que des programmes tels que Mappy GPS ou encore celui de Google, appelé Google Navigation, sont gratuits. Certains constructeurs de smartphones intègrent à leurs périphériques une solution maison, comme c'est le cas avec Nokia et son application HERE Maps.

Figure 8 : Représentation sommaire du GPS



(Source : Géolocalisation en HTML5. alsacreations.com)

2.2.2 GSM

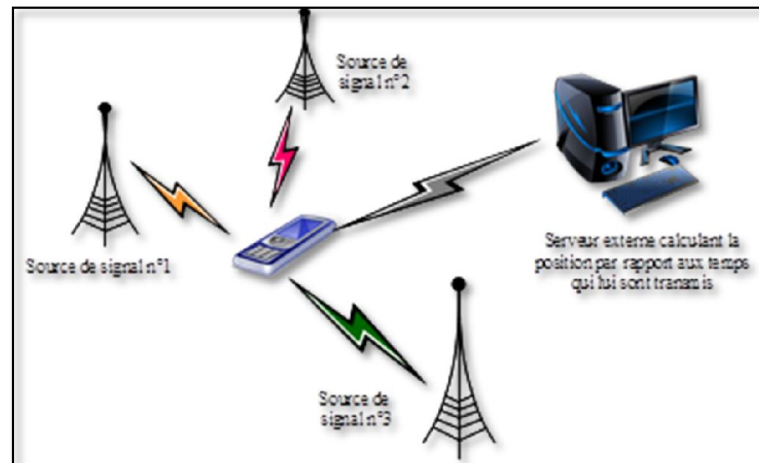
Tous les téléphones portables se connectent au réseau GSM constitué d'antennes cellulaires. Il est donc possible d'obtenir le positionnement approximatif du périphérique à travers plusieurs techniques, mais ont tous une similitude : celle de nécessiter d'un nombre minimum d'antennes dans le voisinage du téléphone.

Avant de passer à la suite, il faut noter que l'efficacité de certains de ces procédés dépend du nombre d'antennes « vues » par le téléphone. Ce qui veut dire que la précision n'est pas la même lorsque le téléphone se trouve en ville entouré d'antennes ou en campagne où les antennes sont moins nombreuses.

2.2.2.1 Identification du temps (E-OTD)

Le principe est d'effectuer le calcul du temps que les ondes mettent pour aller d'un téléphone aux antennes cellulaires voisines. Sachant que c'est la plus proche qui répondra, il est alors possible, à travers un serveur externe, de calculer la position du téléphone portable grâce au laps de temps écoulé entre l'émission et la réception du signal.

Figure 9 : Schéma E-OTD



(Source : Géolocalisation. anr-prodige.com)

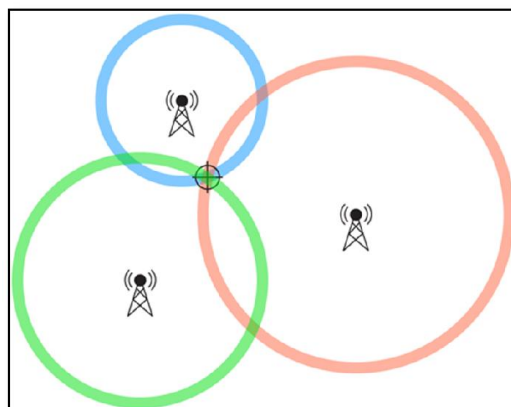
2.2.2.2 Triangulation (TOA)

L'efficacité de cette méthode dépend du nombre d'antennes auquel le téléphone est connecté. Dans le cas de l'utilisation d'une ou de deux antennes, la localisation reste trop approximative, c'est pourquoi il en faut trois.

C'est grâce à la force et à la précision du signal des antennes reçu par le téléphone, qu'il est possible d'établir un cercle autour de chaque antenne cellulaire.

Le résultat est visible sur la figure 6 ci-dessous ; on obtient trois cercles, un autour de chaque antenne. C'est l'intersection de ces cercles qui représente la localisation du téléphone.

Figure 10 : Triangulation GSM



(Source : Mobile Network Geolocation. neilson.co.za)

2.2.2.3 Identification de l'antenne cellulaire (Cell ID)

Appelé Cell ID, cette technique ne requiert aucun matériel. Elle utilise les identifiants uniques de chaque antenne cellulaire, voire des antennes voisines, pour retrouver un emplacement en utilisant une base de données et un service de cartographie. C'est donc cet identifiant de l'antenne à laquelle le téléphone est connecté qui permettra d'accéder à sa position géographique.

Il est possible de trouver sur internet ces bases de données contenant des milliers d'antennes cellulaires et les informations de chacune. Il existe une communauté, appelée OpenCellID, qui recense les informations sur les antennes cellulaires afin de permettre à toute personne d'y avoir accès gratuitement. D'après leur site web¹, la base de données contiendrait plus de 6 millions d'entrées.

On remarque sur la figure 6 ci-dessous, que chaque antenne dispose de plusieurs informations, voici à quoi ils correspondent :

- MCC correspond au pays dans laquelle l'antenne est située ;
- MNC indique l'opérateur ;
- LAC est un nombre qui désigne la zone de localisation du téléphone dans un réseau public GSM ;
- Cell ID est, comme dit plus haut, un identifiant unique de l'antenne ;

Toutes ces informations vont permettre la recherche d'antennes.

¹ Source : What is OpenCellID. http://wiki.opencellid.org/wiki/Main_Page

Figure 11 : Carte OpenCellID – Plaine de Plainpalais



(Source : OpenCellID. opencellid.org)

2.2.3 NFC

Le NFC est une technologie dérivée du RFID, qui est basée sur des hautes fréquences radios. Sa portée est de l'ordre de quelques centimètres. Certains smartphones de dernière génération disposent d'un lecteur NFC et d'une carte à puces NFC, ce qui leur permet de recevoir et d'envoyer des informations à travers cette puce.

Cette technologie tend à se démocratiser de plus en plus, notamment avec l'arrivée du paiement sans fil en Amérique et en Europe. Or, elle a déjà été adoptée dans quelques pays précurseurs comme le Japon où, depuis plusieurs années, des commerces disposent des moyens techniques nécessaires afin que les clients règlent leurs achats en payant avec leur smartphone.

Les utilisations possibles du NFC sont nombreuses. En France, cette technologie aurait été testée dans quelques villes depuis 2012, dans plusieurs lieux et pour des utilités différentes. Par exemple, aux arrêts de bus afin d'avoir accès à diverses informations relatives au réseau de transport. Dans certains stades de football, des puces NFC sont utilisées afin de valider les billets d'entrée, mais également de recevoir des informations

concernant le match en cours telles que les joueurs utilisés. Autre utilisation, il est possible d'utiliser son smartphone en tant que carte de fidélité/adhérent, comme par exemple la Supercard de Coop et la Cumulus de Migros.

Plus récemment, Apple a évoqué que la technologie Apple Pay, disponible dans l'iPhone 6 et l'iPhone 6 Plus, devrait pouvoir évoluer afin de permettre le remplacement des badges d'accès sécurisés dans les immeubles, mais encore de faire office de titres de transport.

Là où l'utilisation du NFC devient intéressante du point de vue de la géolocalisation, est pour le guidage intérieur, là où le GPS a du mal à fonctionner. Il est possible dans certains établissements, tels que les musées (voir figure ci-dessus), d'être guidé à travers les étapes d'une exposition. Cela permet également d'avoir du contenu supplémentaire sous forme audio ou de texte, comme une description ou encore une biographie à propos de l'objet scanné.

Figure 12 : Etiquette NFC au musée



(Source : NFC for Museums Case Study: Museum of London. qfuse.com)

Figure 13 : Utilisations possibles du NFC



(Source : Everything You Need to Know About NFC. techspot.com)

2.2.4 RFID

Le RFID est une technologie basée sur plusieurs fréquences radios. Elle peut être comparée au principe du code-barres, qui permet la lecture d'informations. Celle-ci nécessite de plusieurs composants pour fonctionner :

- Un tag
Appelé également transpondeur ou étiquette, c'est un objet composé d'une puce et d'une antenne. C'est là où se trouvent les informations.
- Un lecteur
C'est le dispositif qui va envoyer et recevoir des ondes radios.
- Un ordinateur
Couplé à un logiciel, c'est le responsable de la gestion des données.

La portée des ondes dépend des éléments tels que la qualité des composants utilisés mais aussi de la fréquence des ondes. Là encore, il est possible de séparer les tags en trois parties, appelée classes.

2.2.4.1 Tags actifs

Les tags actifs émettent des signaux grâce à une batterie intégrée. Ce type de tag permet l'échange d'informations à une distance plus grande que les autres deux types, mais de ce fait coûtent plus cher.

Un de nombreux exemples d'utilisation de ce type de tags est celui de l'entreprise portugaise Via Verde et son système de paiement de péages. Lancé initialement en 1991 et actif dans tout le pays dès 1995, le système mis en place permet aux automobilistes adhérents de circuler sur les autoroutes sans la contrainte de devoir s'arrêter pour payer des péages. Ceci se fait grâce à une sorte de boîtier contenant une étiquette RFID alimentée par batterie (voir figure 16).

Figure 14 : Péage RFID



(Source : Via Verde, sistema de portagens eletrónico. oguiadeportugal.com)

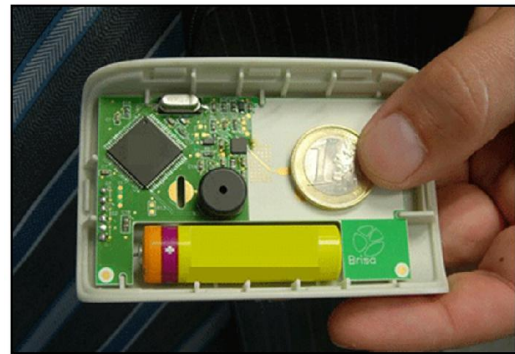
Plus récemment, l'utilisation de ce système a été portée au-delà des autoroutes (voir figure 14) ; il est aujourd'hui possible de payer le plein d'essence dans des stations Galp, le stationnement dans des parkings ou encore les commandes effectuées aux McDrives.

Figure 15 : Tag actif – Via Verde



(Source : Via Verde disponível em 100 parques. lusomotores.com)

Figure 16 : Intérieur du tag actif



(Source : OBU-Identificador. dailywork.pt)

2.2.4.2 Tags passifs

La classe des passifs est la plus répandue de toutes, car c'est aussi la moins coûteuse. Ne nécessitant pas de batterie afin de fonctionner, elle se sert du courant des ondes radios reçues par le lecteur pour retourner les informations de la puce. Comme la portée est liée à la puissance d'émission des ondes du lecteur, ce type de tag fonctionnera sur une distance beaucoup plus faible.

Il y a plusieurs exemples d'utilisation des tags passifs ; à la Haute Ecole de Gestion, des cartes sont utilisées en tant que badges d'accès aux différents bâtiments et également pour effectuer des impressions papier. Mobility, entreprise de partage de véhicules, utilise également cette technologie.

Figure 17 : Ouverture/fermeture d'un véhicule Mobility



(Source : Marche à suivre. mobility.ch)

Chaque abonné dispose d'une carte qui leur permet de fonctionner comme une clé de voiture. Comme on le voit sur la figure ci-dessous, il suffit de passer la carte sur le lecteur, souvent situé sur le coin inférieur droit de la vitre avant, pour actionner le verrouillage central des portes. Bien sûr, il faut au préalable que le client ait effectué la réservation, sinon le véhicule ne s'ouvre pas.

2.2.4.3 Tags semi-passifs

Les tags semi-passifs fonctionnent comme des tags passifs à une différence près, celle de disposer d'une batterie. Semi-passifs, car contrairement aux tags actifs, ils n'émettent pas d'ondes au lecteur, mais le courant de la batterie est utilisée afin d'alimenter tout type de capteurs, par exemple thermique.

2.2.4.4 Nabaztag

Parmi les objets qui utilisent cette technologie, il faut distinguer le Nabaztag : petit lapin connecté qui permettait d'effectuer une multitude d'actions. En plus de disposer d'un lecteur RFID, il pouvait se connecter aux réseaux Wi-Fi domestiques.

De la lecture des emails entrants à l'indication des indices boursiers, en passant par l'annonce des prévisions météo, il était livré avec un certain nombre d'étiquettes RFID. Ces tags pouvaient être programmés par les propriétaires afin d'effectuer des actions bien spécifiques comme par exemple lancer la lecture d'une playlist.

Grâce à ses capteurs et à sa connectivité, il pouvait également être utilisé en tant que système de surveillance, envoyant une alerte à son propriétaire lorsqu'il détectait quelque chose.

Figure 18 : Lapin RFID Nabaztag



(Source : Nabaztag's Violet RFID-Readin' USB Mirror now available. engadget.com)

2.2.5 Wi-Fi

Semblable aux antennes cellulaires, chaque réseau sans fil dispose d'une adresse unique, appelée adresse MAC, en plus d'un nom de réseau, appelé SSID.

Grâce à cet identifiant unique, il est possible de connaître l'emplacement d'un périphérique. Pour cela, il faut avoir accès à des bases de données où ses points d'accès sont référencés, notamment grâce à la technique du wardriving. Celle-ci est détaillée dans le chapitre suivant (cf. [Le Wardriving](#)).

2.3 Le Wardriving

Le wardriving peut être considéré comme une forme de géolocalisation. En effet, c'est une pratique qui consiste à scanner des réseaux Wi-Fi grâce à un appareil électronique, tel qu'un ordinateur portable, un smartphone ou autre, tout en se déplaçant à bord d'un véhicule.

Le périphérique qui effectue le balayage doit absolument être équipé d'une puce Wi-Fi. De plus, pour une meilleure efficacité lors de l'utilisation d'un laptop, il est préférable d'utiliser une carte Wi-Fi externe branchée via le port USB plutôt que celle intégrée. La raison est simple : la carte ajoutée dispose d'une antenne externe qui est facilement déplaçable grâce à l'ajout d'une rallonge (voir figure ci-contre).

Figure 19 : Antenne Wi-Fi externe montée sur une voiture



(Source : Antenna for wardriving. joi.ito.com)

On peut faire un rapprochement avec les véhicules utilisés par Google pour le service StreetView. Ils disposent d'une caméra sur le toit pouvant capturer des images à 360 degrés, le tout en sillonnant les routes du monde entier.

2.3.1 Les débuts

Ce procédé a été inventé entre 1999 et 2000 par Peter Shipley, un expert en sécurité informatique, qui a été le premier à complètement automatiser la procédure de scan et d'analyse des réseaux Wi-Fi.

Un peu plus d'un an avant, alors qu'il faisait des recherches sur la sécurité des systèmes « dial-up », il s'est rendu compte que la sécurité des réseaux Wi-Fi n'était pas quelque chose d'assimilé pour un bon nombre de personnes. C'est alors qu'il a eu l'idée de se lancer dans le wardriving, afin de faire prendre conscience à tout un chacun de l'importance de la sécurité des réseaux sans fil.

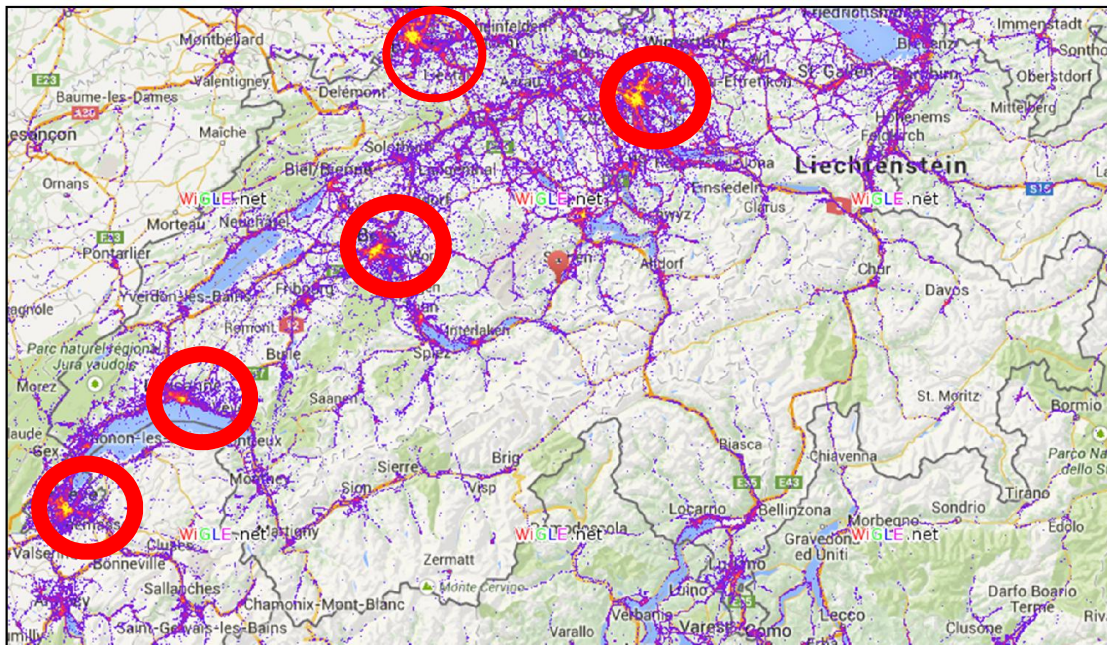
Le wardriving était pratiqué avant lui, mais de façon manuelle. Appelé warjogging ou warwalking, le principe était le même, mais les déplacements se faisaient à pied, avec des appareils pouvant scanner les réseaux sans fil, pour ensuite noter les résultats sur une feuille de papier ou dans un document texte.

2.3.2 Curiosité

Après quelques recherches sur internet, il est facile de trouver des sites web de communautés pratiquant le wardriving. Sans trop m'attarder sur quel site choisir, j'ai accédé au site de la communauté WiGLE. Communauté active depuis 2001, elle a pour but le référencement dans une base de données peuplée de tous les réseaux, cellulaires et Wi-Fi, grâce à l'apport d'informations effectué par ses nombreux membres.

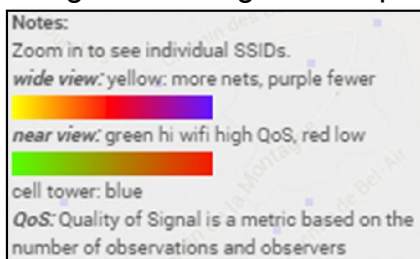
En allant plus loin, on trouve via le menu « View » puis « Map », une page qui permet d'afficher les informations sur une carte. En se positionnant au-dessus de la Suisse, voici ce qu'on obtient :

Figure 20 : Carte WiGLE - Suisse



(Source : WiGLE View Map. wigle.net)

Figure 21 : Légende Map



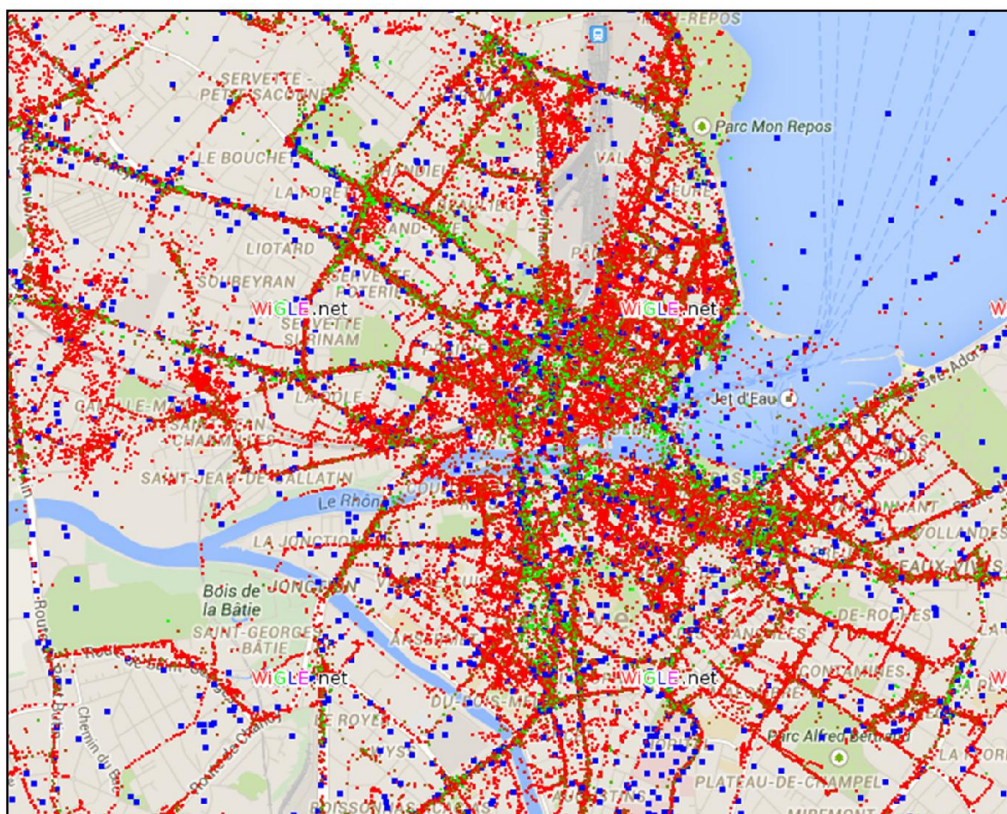
Selon la légende du plan (voir figure ci-contre), la couleur violette indique qu'il y a un faible nombre de réseaux dans la zone, alors que les couleurs rouge et jaune indiquent qu'il y en a un nombre important.

(Source : WiGLE View Map. wigle.net)

Dès lors, on arrive à distinguer cinq villes suisses (voir figure 22) qui disposent d'un grand nombre de réseaux recensés. Ces villes sont : Bâle, Berne, Genève, Lausanne et Zurich.

En effectuant un zoom de façon à voir tout le canton de Genève, on n'y voit que des zones violettes. Cependant, en agrandissant encore un peu la carte, voici ce qu'on obtient :

Figure 22 : Carte WiGLE - Genève



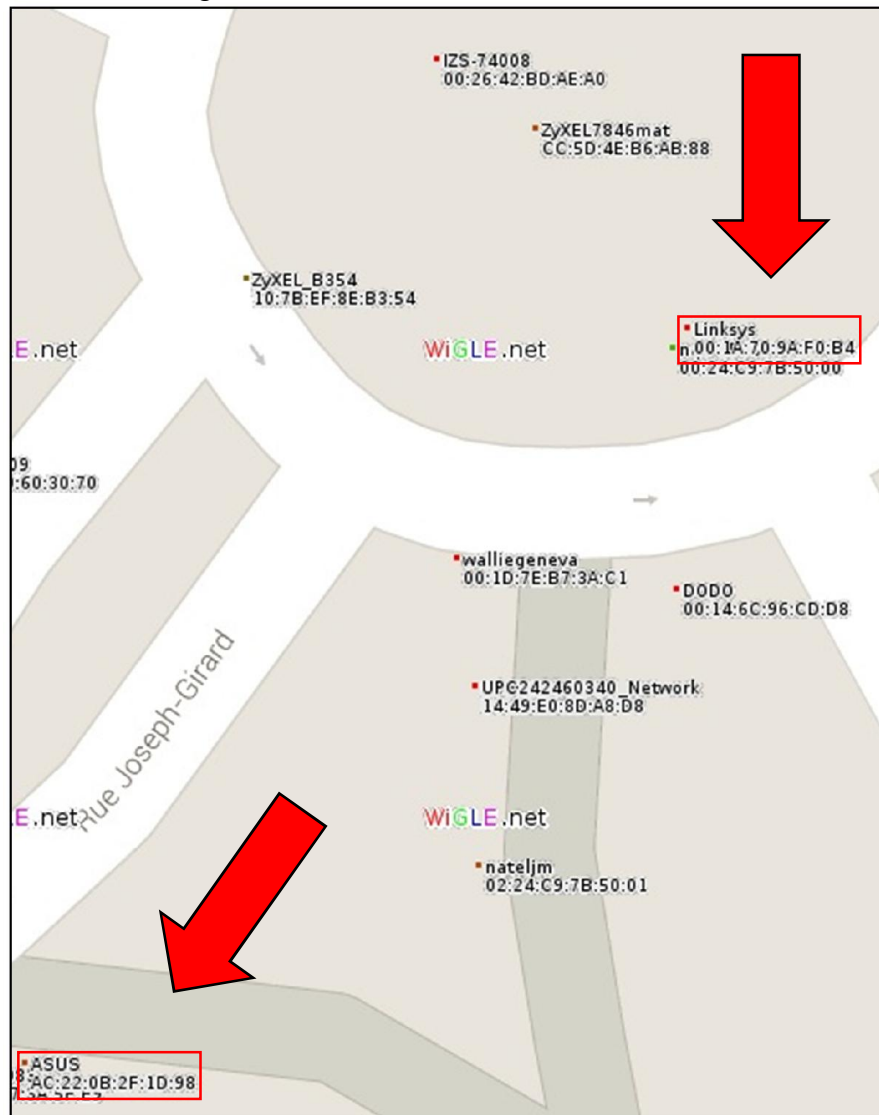
(Source : WiGLE View Map. wagle.net)

Le fait de zoomer apporte de nouveaux éléments à la carte. Lorsque le niveau de zoom est proche, les réseaux Wi-Fi sont représentés par des points verts et rouges.

Si l'on se réfère à la légende (voir figure 21), le vert représente un réseau doté d'une bonne performance générale (QoS) et le rouge indique l'inverse. Les carrés bleus visibles correspondent aux antennes cellulaires.

Vu le grand nombre de réseaux référencés à Genève, je suis parti à la recherche de mon réseau domestique. On peut voir dans la figure suivante que dès que le zoom est encore plus important que précédemment, les points colorés disparaissent pour laisser place à des inscriptions sous forme de texte.

Figure 23 : Carte WiGLE – Mes réseaux



(Source : WiGLE Map View. wigle.net)

En cherchant l'adresse de mon domicile, je me suis rendu compte que mon réseau Wi-Fi actuel était présent, ainsi que celui que j'avais avant d'avoir remplacé mon point d'accès.

On constate qu'en comparant les adresses MAC des réseaux « Asus » et « Linksys » de la figure ci-dessus, à celles des périphériques des figures suivantes, les adresses concordent.

Figure 24 : Modem Linksys



(Photo de Michael Laranjo)

Figure 25 : Routeur Asus



(Photo de Michael Laranjo)

En plus de tutoriels, ils conseillent les outils à utiliser et font même des statistiques. D'ailleurs, en allant dans le menu « Stats », on accède à une page où sont montrées toutes sortes de statistiques. On a accès à beaucoup d'informations grâce à ces statistiques, toutes, elles, scannées par les nombreux membres de la communauté. En regardant un peu plus en détail, on y voit qu'en date du 1^{er} décembre 2014 :

Figure 26 : Informations Générales

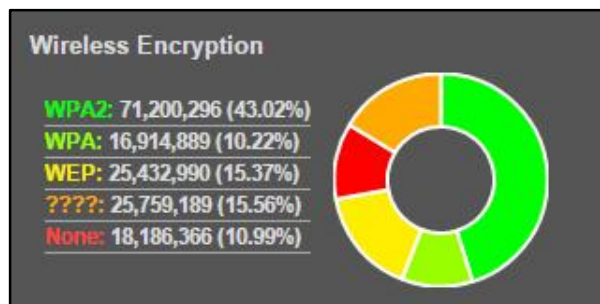
- Un peu plus de 165 millions de SSID sont recensés dans leur base de données ;

Unique WiFi networks in DB:	165,494,443
Unique networks w/ location:	163,639,139
Unique WiFi locations in DB:	2,147,483,647
Unique Cell towers in DB:	4,154,539
Unique Cells w/ location:	4,129,622
Registered Users:	162,161

(Source : WiGLE stats general. wigle.net)

Figure 27 : Statistiques d'encryption Wi-Fi

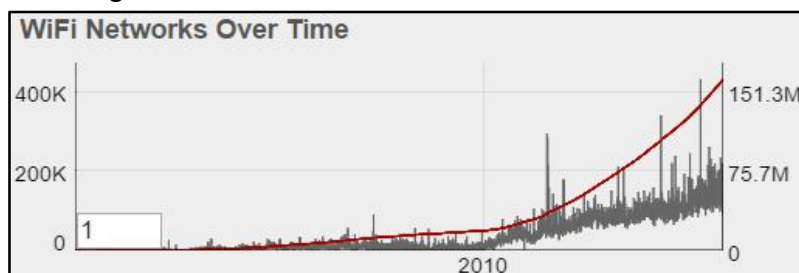
- On remarque qu'environ 11%, soit près de 18 millions des réseaux ne présentent aucune forme de protection;



(Source : WiGLE stats general. wigle.net)

- Le nombre des réseaux Wi-Fi scannés est en forte augmentation depuis 2010;

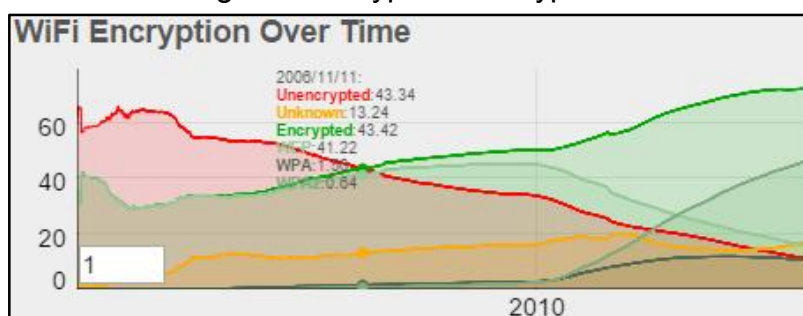
Figure 28 : Réseaux dans la base de données



(Source : WiGLE stats general. wigle.net)

- Qu'à la fin de l'année 2008, le nombre de réseaux protégés est devenu majoritaire par rapport au nombre de réseaux non-protégés.

Figure 29 : Types d'encryptions



(Source : WiGLE stats general. wige.net)

En s'intéressant de plus près à l'onglet « Geographic », on a accès à la liste de pays classés par le nombre de réseaux. En regardant de plus près la Suisse (voir figure ci-dessous), on constate que parmi localités ayant le plus de réseaux, se trouve le code postal 1201 avec un peu plus de 12'000 antennes. De plus, on voit que même si la plupart des réseaux Wi-Fi suisses sont protégés, près de 83'000 ne disposent d'aucune protection.

Figure 30 : Statistiques géographiques

Country	Count	Region	Count	Postal Code	Count	Encryption	Count
US	53,491,544	Zu00fcrich	163,504	1201	12,587		539,818
DE	8,856,309	Bern - Berne	155,585	3011	11,245		269,898
GB	7,891,812	Basel-Stadt	112,135	3007	9,527		161,173
NL	6,051,334	Zürich	107,559	4058	9,007		96,387
CA	5,198,488	Vaud	94,783	8050	7,836		83,082
FR	3,370,726	Genu00e8ve	69,464	3014	7,782		
JP	2,837,254	Luzern	62,148	8005	7,082		
RU	2,499,233	Aargau	57,654	8004	7,019		
AU	2,079,888	Basel-Landschaft	42,959	3006	6,472		
PL	1,939,211	Genève	39,555	4056	6,445		
ES	1,897,154	St. Gallen	37,422	1004	6,345		
BE	1,679,765	Ticino	35,484	3008	6,122		
SE	1,519,415	Zug	24,485	3013	5,997		
DK	1,491,799	Thurgau	24,427	1205	5,826		
IT	1,426,888	Solothurn	23,785	1204	5,790		
CH	1,150,358	Schwyz	21,859	8037	5,689		

(Source : WiGLE stats geographic. wige.net)

2.3.3 Conséquences

Bien que l'idée première était de jouer la carte de la prévention, on imagine que certaines personnes notamment des hackers, ont exploité cette technique et continuent de le faire dans des buts malveillants. Le but, pour les personnes malveillantes qui pratiquent cette activité, est simple lorsque l'on sait qu'un réseau dit ouvert correspond à une connexion internet sans coûts et anonyme, pour toute personne extérieure se connectant à ce réseau.

En Suisse, le fait de se connecter à un réseau Wi-Fi n'est pas illégal à condition qu'il ne soit pas protégé. La loi suisse concernant l'accès aux systèmes informatiques dit ceci :

« Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. »

(Code pénal suisse, art. 143^{bis} al. 1)

Donc, pour les personnes qui cherchent à surfer sur internet de façon normale, c'est-à-dire sans commettre d'actes illicites, cela ne pose pas de problèmes dès lors qu'aucune infraction n'ait été commise.

En revanche, dans le cas des personnes malveillantes, elles savent qu'un réseau ouvert est une porte à l'anonymat et à la liberté ; elles ont moins de chances d'être attrapées. Les hackers n'auront pas trop à se soucier des conséquences liées à d'éventuels actes de piratage, tels que le vol de données confidentielles, ou bien tout autre acte illégal effectué sur internet.

Le fait que le propriétaire d'un accès internet n'ait pas protégé son point d'accès correctement peut lui causer des problèmes. En effet, si de tels actes venaient à se produire, les autorités remonteraient naturellement à son domicile, car c'est depuis son réseau que les actes illégaux ont été commis. En plus, il pourrait se faire voler des données partagées dans son réseau. Pour s'innocenter, il devra alors prouver que ce n'est pas lui le coupable des faits et que le périphérique utilisé ne fait pas partie des siens.

Après quelques recherches, je remarque qu'il n'existe aucun texte de loi suisse concernant le wardriving. Cependant, bien que cette pratique ne soit pas illégale, c'est son utilisation qui déterminera si la personne intruse peut être ou non accusée de piratage. L'un des inconvénients présent, même lorsque rien d'illégal ne se passe, est qu'un ralentissement de vitesse de navigation peut se faire ressentir, baissant ainsi le confort de l'utilisation d'internet du propriétaire de la borne Wi-Fi.

3. Smartphones, où sont les données de géolocalisation ?

Les informations de localisation sont précieuses pour la police scientifique, car elles permettent, dans le cadre de procédures pénales, de lier des personnes à des lieux dans lesquels des crimes ont pu avoir lieu.

Les téléphones intelligents regorgent de nouvelles fonctionnalités censées apporter, à tout possesseur de ces terminaux, une meilleure expérience utilisateur. Pourtant, certains constructeurs ont longtemps caché le fait qu'ils enregistraient les déplacements de leurs smartphones. Certes, connaître l'emplacement d'un individu permet aujourd'hui aux développeurs de proposer de la publicité ciblée, ou dans le cas de Facebook d'indiquer les amis à proximité, mais cette pratique est souvent considérée par certains comme une intrusion à la vie privée.

Laissant de côté cet aspect juridique pour traiter l'aspect technique, la question que je me suis posée était de savoir où ses données étaient stockées à l'intérieur des smartphones. Après quelques recherches, il s'avère qu'en 2011 il y a eu polémique après qu'un expert en sécurité ait découvert qu'Apple stockait et envoyait de manière intermittente l'historique des déplacements de chaque téléphone.

Ensuite, d'autres experts se sont penchés vers Android et ont indiqué que Google le faisait également, mais que les informations stockées, du point de vue de la période de la collecte, est beaucoup plus limitée que dans iOS.

Pour sa part, Microsoft, a déclaré recueillir des informations de localisation depuis leur OS mobile Windows Phone. La récolte d'informations est faite de manière anonyme afin de remplir leur base de données constituée de points d'accès Wi-Fi et d'antennes cellulaires. Microsoft indique que ceci est fait dans le but de servir l'utilisateur, lorsque celui-ci désire utiliser une application qui nécessite l'emplacement actuel. C'est à ce moment que la base de données est utilisée afin de comparer les réseaux visibles par le smartphone et les entrées de la base de données.

En plus de certains fichiers qui contiennent l'historique des déplacements, il est également possible de trouver des informations de géolocalisation dans les photos prises. La plupart des smartphones permettent d'enregistrer l'emplacement auquel les photos sont prises. On peut penser que l'utilité première d'utiliser l'emplacement des photos est de constituer des albums de vacances classés par dates ou bien par emplacements.

3.1 Le standard Exif

Exif est un standard créé au milieu des années 1990 par l'association « Japan Electronics and Information Technology Industries Association ». De façon générale, ce format permet l'inclusion de métadonnées qui sont enregistrées par un appareil numérique lors de la prise d'une photo ou d'un enregistrement audio.

On peut remarquer le fait que la période de création du standard coïncide avec celui de l'avènement de l'appareil photo numérique. On parle d'appareils numériques au sens général, car cela englobe tout appareil pouvant enregistrer des fichiers audio ou des images. Tout smartphone ou tablette possédant un appareil photo numérique intégré en fait donc partie.

3.1.1 Une véritable mine d'informations

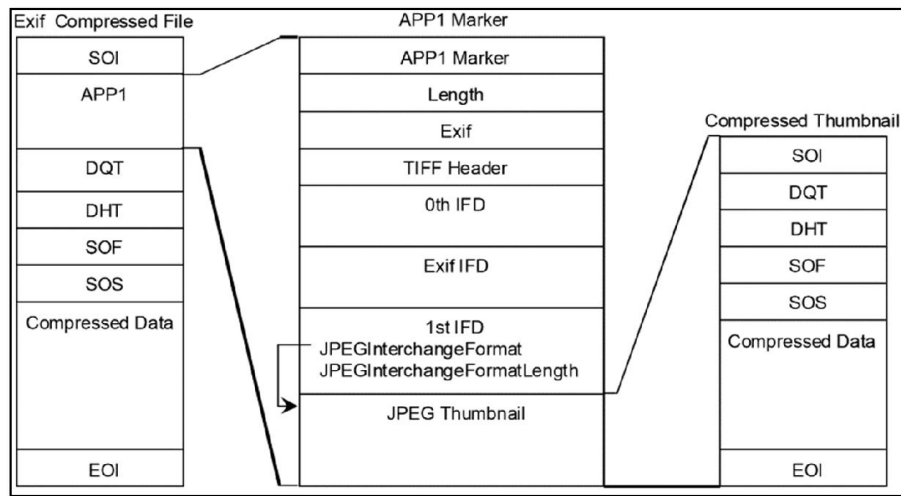
Le format d'enregistrement Exif permet de stocker dans les fichiers images ou audio un nombre impressionnant d'informations, mais cela ne fonctionne pas avec toutes les sortes de fichiers. En effet, le standard Exif prend en charge les fichiers WAV et les images TIFF et JPEG ; le format JPEG pour les fichiers compressés et le format TIFF pour les fichiers non-compressés.

Pour le projet, la priorité était d'extraire des informations de géolocalisation des photos prises par des smartphones. De ce fait, je me suis tourné vers les spécifications concernant les fichiers JPEG.

3.1.1.1 JPEG

Comme nous le montre la figure ci-dessous, la structure d'un fichier Exif au format JPEG est complexe. On constate qu'un fichier de ce type est constitué de plusieurs sections, chacune contenant diverses informations. La section qui contient les données Exif est la section APP1, c'est donc à l'intérieur de celle-ci qu'il faut chercher afin de trouver les données d'une photo.

Figure 31 : Structure d'un fichier Exif compressé



(Source : Standard Exif version 2.3, p.24)

Au début de celle-ci, on retrouve des informations d'identification, un en-tête TIFF, puis les structures IFD qui contiennent les données Exif. Afin d'en savoir plus, il a fallu parcourir le standard afin de savoir à quoi elles correspondent.

Lorsque l'on regarde le détail de la section APP1 (figure détail), on aperçoit où sont stockées les informations pertinentes dans le cadre du projet. Chaque section de couleur verte représente les données relatives à chaque photo.

Figure 32 : Détail de la section APP1

	Length	Value
APP1 Section	2	APP1 Marker (0xFF, 0xE1)
	2	APP1 Length Including the size of the length field
	6	Exif Identifier (0x45, 0x78, 0x69, 0x66, 0x00, 0x00) ('E', 'x', 'I', 'f', NULL, NULL)
	8	TIFF Header
	var.	0th IFD
	var.	Exif IFD
	var.	Interoperability IFD
	var.	GPS IFD
var.	1st IFD	

(Source : ExifLibrary for .NET. codeproject.com)

Cependant, il est important de signaler que la section « GPS IFD » n'est pas toujours présente. En effet, elle n'apparaît pas dans la structure du fichier lorsqu'il n'y a pas de données à l'intérieur. Ce cas de figure peut se présenter lorsque l'appareil numérique qui capture la photo ne possède pas de puce GPS, ou lorsque la fonction qui permet d'enregistrer l'endroit de la prise de la photo est désactivée.

3.1.2 Tags utilisés dans le cadre du projet

On a pu voir que ce format intègre un nombre impressionnant de données, allant du constructeur et du modèle de l'appareil, au temps d'exposition ou encore de la longueur focale. C'est pourquoi, uniquement une partie de ces tags ont été retenus

Pour la partie pratique du projet, il fallait extraire les informations GPS et la date et heure de la prise de la photo. En parcourant les spécifications du standard, on remarque que plusieurs tags concernant la date sont présents et que c'est aussi le cas pour les tags relatifs aux données GPS.

3.1.2.1 La date

Comme dit précédemment, on retrouve plusieurs tags concernant des dates dans la structure d'un fichier Exif. En parcourant le document de la norme Exif version 2.2, sept tags contenant des informations de dates ont retenu mon attention.

- DateTime ;
- DateTimeOriginal ;
- DateTimeDigitized ;
- SubsecTime ;
- SubsecTimeOriginal ;
- SubsecTimeDigitized ;
- GPSTimeStamp.

En analysant la description de chacun des tags, on remarque que GPSTimeStamp n'est pas intéressant dans le cadre du projet, car le tag retourne uniquement la date au format « YYYY:MM:DD », sans la moindre indication horaire. Les six autres tags contiennent non seulement des dates, mais également les heures. Celles-ci sont stockées avec des formats différents, mais représentent les mêmes éléments ; chacun des trois tags ayant comme format « YYYY:MM:DD HH:MM:SS » ont leur équivalent en timestamp.

Dans la partie pratique du travail, comme on ne cherche pas à faire de calculs avec ces dates, j'ai donc retenu les tags suivants : DateTime, DateTimeOriginal et DateTimeDigitized. Toutefois, il est nécessaire d'apporter un peu plus d'explications à propos de ces tags.

Les valeurs de ces trois dates peuvent être les mêmes sur certaines photos, alors qu'elles correspondent à trois événements distincts :

- DateTime correspond non seulement à la date et l'heure de création du fichier, mais aussi la date et l'heure de la dernière modification de celui-ci ;

- DateTimeOriginal indique le moment où le bouton déclencheur de l'appareil photo a été appuyé et que les données Exif ont été générées ;
- DateTimeDigitized fait référence au moment où la photo est enregistrée sous forme numérique.

Dans le cas du tag DateTime, cela veut dire que lorsque l'image recevra un traitement quelconque dans un logiciel de retouche, ce tag indiquera une nouvelle date et heure. Ce n'est donc pas le tag à utiliser. De ce fait, on privilégiera les tags DateTimeOriginal et DateTimeDigitized pour l'extraction de la date et l'heure.

3.1.2.2 La localisation

En ce qui concerne les tags de localisation, ils sont bien plus nombreux. Après une brève recherche, on trouve 31 tags dans la section « GPS IFD », mais voici ceux qui contiennent les informations relatives aux coordonnées GPS :

- GPSLatitudeRef ;
- GPSLatitude ;
- GPSLongitudeRef ;
- GPSLongitude.

Les tags GPSLatitudeRef et GPSLongitudeRef correspondent respectivement à l'indication d'une latitude N pour Nord et S pour Sud, et d'une longitude E pour Est et W pour Ouest.

GPSLatitude et GPSLongitude contiennent des coordonnées GPS. Celles-ci sont écrites au format sexagésimal, en « Degrés Minutes Secondes ». Bien que cette notation soit facile à comprendre, il a fallu, dans le cadre du projet, les convertir au format décimal afin de pouvoir faire des calculs avec les coordonnées extraites des photos. Dans le tableau 1 ci-dessous, il est possible de voir quelles sont les différences entre ces deux notations.

Tableau 1 : Coordonnées du jet d'eau de Genève

	Latitude	Longitude
Degrés Minutes Secondes	46° 12' 26" N	6° 9' 22" E
Décimales	46.207222°	6.156111°

(Source : Wikimedia Tool Labs. tools.wmflabs.org)

La conversion n'est pas compliquée à réaliser. Cependant, il faut tenir compte de deux choses importantes ; la première, que la latitude correspond à des angles allant de moins

90 degrés à plus 90 degrés. La deuxième, que la longitude s'étale, elle, entre moins 180 degrés à plus 180 degrés. Ce qui a pour conséquence l'ajout du signe moins devant la latitude ou la longitude lorsque :

- la latitude indique le sud (tag GPSPLatitudeRef égal à « S ») ;
- la longitude indique l'ouest (tag GPSLongitudeRef égal à « W »).

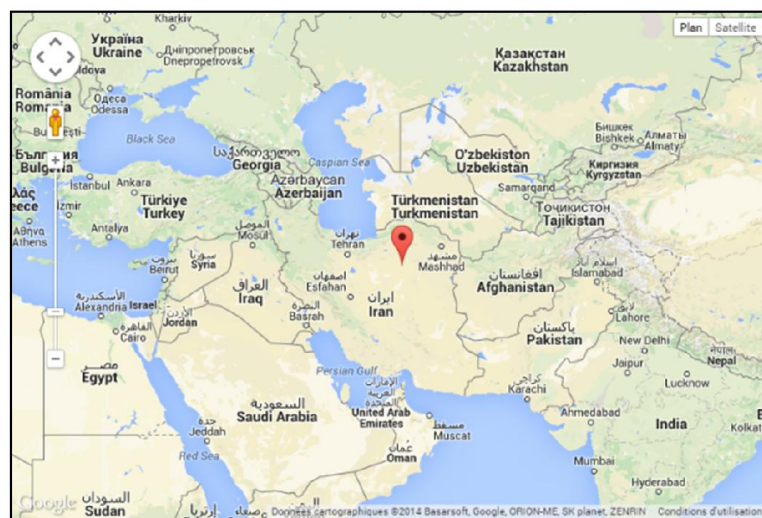
Par exemple, les coordonnées suivantes [-34.866746°, -56.159582°] pointent sur l'Uruguay. En les rendant positives, elles indiquent un emplacement totalement différent, quelque part en Iran (voir figures 33 et 34).

Figure 33 : Google Maps - Emplacement [-34.866746°, -56.159582°]



(Source : Coordonnées GPS. coordonnees-gps.fr)

Figure 34 : Google Maps - Emplacement [34.866746°, 56.159582°]



(Source : Coordonnées GPS. coordonnees-gps.fr)

3.2 Les fichiers système

Il faut savoir que dans nos smartphones, qu'ils aient comme système d'exploitation iOS d'Apple ou bien Android de Google, l'historique de nos déplacements est enregistré. Ils contiennent des informations telles que les antennes cellulaires et des points d'accès Wi-Fi auxquels le smartphone a été connecté et même ceux à proximité.

Ces informations sont enregistrées dans des fichiers qui se trouvent dans la mémoire interne des téléphones. Toutefois, ils ne sont pas dans la partie « visible », partie à laquelle tout un chacun a accès. D'ailleurs, en explorant l'arborescence d'un smartphone à l'aide d'un explorateur de fichiers, on constate que les emplacements contenant ces fichiers ne sont pas accessibles.

Afin de remédier à cette situation, il faut pour cela « débloquer » le smartphone concerné. Cette procédure est appelée Jailbreak pour le système d'Apple et Root pour le système Android. Les deux systèmes d'exploitation mobiles ne sont pas semblables du point de vue de la liberté utilisateur. Afin de les différencier d'avantage que par leur système d'exploitation respectif, il faut préciser que le déblocage n'effectue pas les mêmes opérations sur chaque OS :

- Le jailbreak permet l'ajout de fonctionnalités qui ne sont pas incluses dans le système de base ;
- Le root consiste à obtenir les permissions maximales dans le système.

Le jailbreak libère d'une certaine façon l'utilisateur des restrictions d'iOS. Une fois l'appareil « jailbreaké », l'utilisateur peut ainsi installer des applications sans passer par l'App Store. La différence fondamentale est que sur Android, l'installation d'applications hors du Play Store est possible sans accès root.

Parfois, des applications spécifiques ont besoin de ses droits afin d'avoir accès aux entrailles du terminal, comme par exemple une application sous Android qui permet d'augmenter la cadence de fonctionnement du processeur.

3.2.1 Android

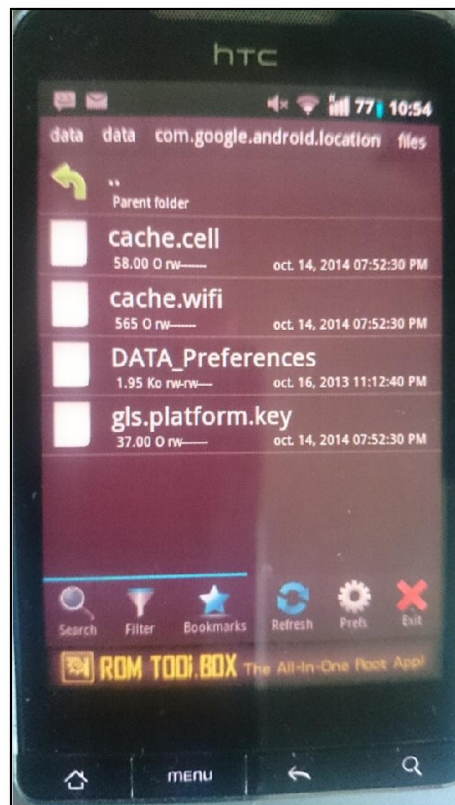
Comme vu précédemment, le root est un accès total au système donnant le contrôle total à l'utilisateur. Dans le cadre du projet, ce déblocage est impératif pour réussir à accéder aux fichiers qui enregistrent l'historique des emplacements. Ces deux fichiers sont : cache.cell et cache.wifi.

3.2.1.1 Root

L'extension de chaque fichier donne ici un indice quant à son contenu. Voici l'emplacement auquel les fichiers se trouvent:

« /data/data/com.google.android.location/files »

Figure 35 : cache.cell & cache.wifi



(Photo de Michael Laranjo)

Ces fichiers sont des fichiers binaires. Ce qui veut dire que lecture de ses fichiers est particulière. Cependant, d'après ce site², il est possible grâce à du code Python de décoder les fichiers.

² <http://forensics.spreitzenbarth.de/2011/10/28/decoding-cache-cell-and-cache-wifi-files/>

Voici le type de contenu enregistré dans ses fichiers :

Figure 36 : Exemple de contenu des fichiers cache.cell & cache.wifi

```
$ ./parse.py cache.wifi
db version: 1
total:      47

key          accuracy  conf.  latitude  longitude  time
50:63:13:57:42:7e    80      92    57.689354  11.994763  04/11/11 10:03:51 +0200
e0:cb:4e:7e:cc:53    75      92    57.689340  11.994495  04/11/11 10:03:51 +0200
4c:54:99:14:47:68    57      92    57.708979  11.916581  04/11/11 01:14:53 +0200
00:26:18:0a:ad:cb    60      92    57.709699  11.917637  04/13/11 08:40:36 +0200
00:22:15:28:3f:7a    60      92    57.699467  11.979340  04/13/11 11:52:16 +0200
00:22:3f:a7:d9:fd    65      92    57.699442  11.979343  04/13/11 11:52:16 +0200

$ ./parse.py cache.cell
db version: 1
total:      41

key          accuracy  conf.  latitude  longitude  time
240:5:15:983885      1186    75    57.704031  11.910801  04/11/11 20:03:14 +0200
240:5:15:983882      883     75    57.706322  11.911692  04/13/11 01:41:29 +0200
240:5:75:4915956     678     75    57.700175  11.976824  04/13/11 11:52:16 +0200
240:5:75:4915953     678     75    57.700064  11.976629  04/13/11 11:53:09 +0200
240:7:61954:58929    1406    75    57.710205  11.921849  04/15/11 19:46:31 +0200
240:7:15:58929       -1      0     0.000000   0.000000  04/15/11 19:46:32 +0200
240:5:75:4915832     831     75    57.690024  11.998419  04/15/11 16:13:53 +0200
```

(Source : android-locdump. github.com)

3.2.2 iOS

Sur iOS, le fichier contenant toutes les informations de géolocalisation est le fichier « consolidated.db ». De par son extension, on constate que c'est une base de données SQLite.

Avant de regarder son contenu, il faut récupérer ledit fichier dans l'arborescence du terminal Apple. Après quelques recherches, il s'avère qu'il est possible d'accéder à ce fichier sans être obligé de débloquent son smartphone. C'est ce que l'on va voir dans le prochain chapitre.

3.2.2.1 Sauvegardes Apple

Bien que dans mon idée première il était indispensable d'effectuer le jailbreak, il s'est avéré, après de nombreuses recherches, que le fichier recherché pouvait être récupéré à travers les sauvegardes effectuées. Celles-ci sont faites grâce au logiciel iTunes et permet, lorsque le téléphone à un problème, de restaurer ses données sauvées au préalable.

Pour accéder à l'emplacement des sauvegardes, il suffit d'utiliser un explorateur de fichiers et aller à cet emplacement³ :

Sur Mac OS X

/Users/NomUtilisateur/Library/Application Support/MobileSync/Backup/

Sur Windows⁴

C:\Users\NomUtilisateur\AppData\AppleComputer\MobileSync\Backup

A l'intérieur du dossier « Backup », chaque dossier trouvé correspond à une sauvegarde effectuée.

Le dossier qui contient le fichier que l'on cherche est encodé, c'est-à-dire que l'arborescence du backup ne contient pas les mêmes noms que lorsque l'on parcourt l'intérieur d'un iPhone en SSH. Voici le nom du dossier :

« 4096c9ec676f2847dc283405900e284a7c815836 »

³ Pour les systèmes d'exploitation Windows, il faut activer la vue des fichiers et dossiers cachés.

⁴ Sur Windows XP : C:\Documents and Settings\NomUtilisateur\Application Data\MobileSync\Backup\

3.2.2.2 Jailbreak

L'opération est simple à effectuer⁵, avant de lancer l'application, il faut enlever tout mot de passe de déblocage d'écran ainsi que désactiver la fonction d'iCloud « Localiser mon iPhone ». Pour éviter les pertes de données, il est conseillé de faire une sauvegarde du téléphone.

Une fois ces deux choses faites, il suffit connecter son iPhone et cliquer à deux trois reprises. Une fois le terminal Apple « jailbreaké », il faut se certifier qu'il soit accessible par SSH. En utilisant un logiciel adapté tel que WinSCP, il faudra se connecter à l'appareil en utilisant :

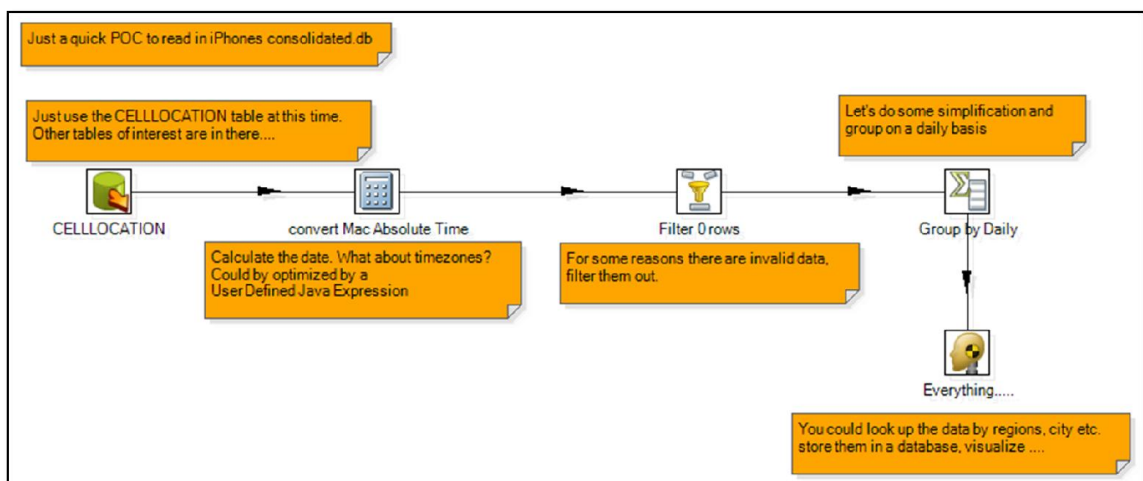
- Son adresse IP ;
- Le nom d'utilisateur SSH ;
- Le mot de passe SSH.

Pour l'adresse IP, il faut que l'iPhone et l'ordinateur soient connectés au même réseau. Le nom d'utilisateur et le mot de passe SSH pour les appareils de la marque Apple sont : « root » et « alpine ». Pour plus de sécurité, il est conseillé de changer de mot de passe lors de l'utilisation d'un appareil débloqué.

3.2.2.3 Lecture du fichier

Il y a plusieurs moyens de parvenir à lire le fichier consolidated.db, que voici :

Figure 37 : Script Kettle



(Source : iPhone Tracking: How to read the consolidated.db with Kettle. Kettle.bleuel.com)

⁵ Testé sur un iPhone 5 iOS 8.1.2 avec l'utilitaire TaiG V1.2.0

Figure 38 : SQLite Manager

The screenshot shows the SQLite Manager interface with a table named 'WifLocation' selected. The table contains 87451 rows of data. The columns are: rowid, MAC, Timestamp, Latitude, Longitude, HorizontalAccuracy, Altitude, VerticalAccuracy, Speed, Course, and Confidence. The data is displayed in a grid format with alternating row colors.

rowid	MAC	Timestamp	Latitude	Longitude	HorizontalAccuracy	Altitude	VerticalAccuracy	Speed	Course	Confidence
420	0:22:75:7...	32779881...	46.7342627	-117.0223...	226	0	-1	-1	-1	50
537	c0:3f:e6:2...	32779881...	46.7347781	-117.0211...	123	0	-1	-1	-1	50
823	0:12:e:89:f...	32779881...	46.73404...	-117.0287...	128	0	-1	-1	-1	50
826	0:b:6c:bd:...	32779881...	46.73406...	-117.0287...	89	0	-1	-1	-1	50
827	40:fc:89:b...	32779881...	46.73399...	-117.0287...	68	0	-1	-1	-1	50
836	c:d5:2:56:...	32779881...	46.734079	-117.0285...	128	0	-1	-1	-1	50
845	0:1:c:e:25:...	32779881...	46.73364...	-117.0291...	79	0	-1	-1	-1	50
883	0:23:69:fe...	32779881...	46.73415...	-117.0251...	282	0	-1	-1	-1	50
884	0:26:c7:84...	32779881...	46.7332856	-117.0323...	51	0	-1	-1	-1	50
902	0:14:c1:b...	32779881...	46.73403...	-117.0231...	298	0	-1	-1	-1	50
904	0:14:70:56...	32779881...	46.73451...	-117.0231...	297	0	-1	-1	-1	50
908	0:23:69:5f...	32779881...	46.7346491	-117.0227...	135	0	-1	-1	-1	50
910	0:25:9c:ea...	32779881...	46.73435...	-117.0226...	286	0	-1	-1	-1	50
916	0:23:69:ae...	32779881...	46.73387...	-117.0284...	106	0	-1	-1	-1	50
927	0:24:1:78...	32779881...	46.7340936	-117.0224...	136	0	-1	-1	-1	50
929	c0:c1:c0:9...	32779881...	46.73471...	-117.0225...	228	0	-1	-1	-1	50
933	c0:3f:e6:3...	32779881...	46.73413...	-117.0224...	185	0	-1	-1	-1	50
936	94:44:52:...	32779881...	46.73456...	-117.0224...	100	0	-1	-1	-1	50
940	0:22:3f:a3...	32779881...	46.73459...	-117.0223...	95	0	-1	-1	-1	50
954	0:27:19:d...	32779881...	46.73485...	-117.0220...	70	0	-1	-1	-1	50
959	68:7f:74:a...	32779881...	46.73493...	-117.0218...	90	0	-1	-1	-1	50
960	68:7f:74:c...	32779881...	46.73580...	-117.0221...	117	0	-1	-1	-1	50
966	5c:da:d4:5...	32779881...	46.73623...	-117.0223...	57	0	-1	-1	-1	50
973	0:24:b2:7e...	32779881...	46.73605...	-117.0221...	145	0	-1	-1	-1	50
981	68:7f:74:c...	32779881...	46.73588...	-117.0219...	141	0	-1	-1	-1	50
982	0:22:3f:d8...	32779881...	46.73544...	-117.0216...	145	0	-1	-1	-1	50
990	0:23:69:fb...	32779881...	46.73486...	-117.0213...	102	0	-1	-1	-1	50
995	c:d5:2:34:...	32779881...	46.7352035	-117.0214...	110	0	-1	-1	-1	50
996	0:1d:7e:5c...	32779881...	46.73525...	-117.0214...	149	0	-1	-1	-1	50
1001	0:23:69:6...	32779881...	46.73578...	-117.0215...	221	0	-1	-1	-1	50
1005	0:1:c:10:27...	32779881...	46.73751...	-117.0345...	50	0	-1	-1	-1	50
1009	0:1:e:5:1:...	32779881...	46.73536...	-117.0213...	107	0	-1	-1	-1	50
1014	68:7f:74:9...	32779881...	46.73475...	-117.0211...	77	0	-1	-1	-1	50
1024	c0:3f:e6:2...	32779881...	46.73476...	-117.0210...	158	0	-1	-1	-1	50
1025	c0:c1:c0:9...	32779881...	46.73601...	-117.0360...	233	0	-1	-1	-1	50
1030	0:22:69:1...	32779881...	46.7356224	-117.0313...	245	0	-1	-1	-1	50

(Source : Hack Your Phone | Map Your Phone. Lib.uidaho.edu)

4. Partie pratique

Le but du projet était de développer un logiciel ayant les fonctionnalités suivantes :

- Acquérir des coordonnées GPS;
 - En analysant des photos pour vérifier les informations Exif
- Afficher les emplacements sur une carte ;
- Analyser les distances entre les emplacements ;

4.1 Choix technologiques

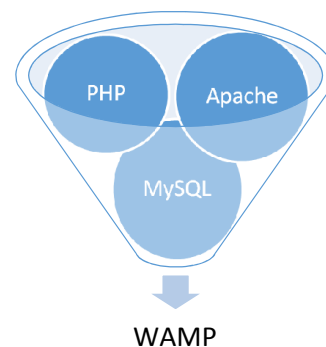
Avant de partir tête baissée dans l'implémentation, j'ai dû analyser et sélectionner les éléments dont j'allais avoir besoin, tels que le langage de programmation ou encore le type de base de données.

Pour le choix du service de cartographie, trois d'entre eux sont sortis du lot lors de mes recherches, bien qu'il en existe d'autres moins connus. Ces trois services sont : Bing Maps, OpenStreetMap et Google Maps. Face à ses plusieurs choix possibles, j'ai alors ciblé mes recherches dans le but de trouver lequel serait plus aisé à manipuler du point de vue programmation et de la documentation disponible sur internet. Les divers tutoriaux trouvés ainsi que les nombreux forums d'entraide m'ont poussé à choisir le service Google Maps, qui est également le plus connu de tous.

Les langages de programmations retenus initialement étaient JAVA et PHP. Le premier apporte un avantage non négligeable par rapport au second, qui est la portabilité entre systèmes. Le choix du langage a été influencé par celui du service de cartographie, car la plupart des pages trouvées, lors de mes recherches, indiquaient l'utilisation de l'API JavaScript de Google Maps. Je me suis donc tourné vers PHP.

Dans le cadre du développement d'une application web, il est nécessaire d'avoir un environnement de programmation propice. Pour cela, de nombreux logiciels WAMP existent sur Windows. Ils ont l'avantage d'intégrer plusieurs éléments (voir figure 39) nécessaires au développement, tels qu'un serveur web, un serveur de base de données et un interpréteur de scripts PHP. Après avoir effectué quelques tests avec deux logiciels de ce type, EasyPHP et WampServer, j'ai opté pour WampServer, car EasyPHP fonctionnait de manière plus lente.

Figure 39 : Représentation des composants WAMP



SQL est donc le type de base de données utilisé dans cette application et sa prise en main n'est que plus aisée grâce à phpMyAdmin, intégré à WampServer.

4.2 Base de données

Pour cette application, l'utilisation d'une base de données est indispensable afin de pouvoir y lire, stocker, modifier et supprimer les informations utilisées. Les données qui doivent pouvoir être stockées concernent les objets suivants : les enquêtes, les marqueurs et les téléphones.

- La table des enquêtes contient les données des enquêtes.
- La table des téléphones contient les informations de chaque téléphone portable.
- La table des marqueurs est la table centrale, car elle doit faire référence à une enquête et à un téléphone. On doit pouvoir relier tout emplacement au téléphone à qui il correspond et également à l'enquête dont il fait partie. De ce fait, cette table contient deux clés étrangères en plus de sa clé primaire.

Etant donné que la base de données contient une table dans laquelle se trouve deux clés étrangères, il faut faire attention au choix du moteur de base de données. Par défaut, MySQL utilise le moteur MyISAM, or celui ne prend pas en charge les clés étrangères. De ce fait, lors de la création de chaque table, Il fallait sélectionner le moteur InnoDB.

L'ordre de création des table a une certaine importance, car pour ajouter des contraintes de clés étrangères, il faut que les tables auxquelles elles font référence soient déjà créées. Dans le projet, les contraintes ont été faites de sorte à ce que si un élément « parent » est supprimé, les entrées concernées le seront aussi. Pareil lors de la mise à jour d'un élément « parent », l'élément « enfant » sera modifié automatiquement.

Figure 40 : Contraintes de clés étrangères

Colonne	Contrainte de clé étrangère (INNODB)		
mar_id	geocoding		
mar_date	Aucun index n'est défini ! Créez-en un dans le dialogue plus bas		
mar_nom	Aucun index n'est défini ! Créez-en un dans le dialogue plus bas		
mar_adresse	Aucun index n'est défini ! Créez-en un dans le dialogue plus bas		
mar_latitude	Aucun index n'est défini ! Créez-en un dans le dialogue plus bas		
mar_longitude	Aucun index n'est défini ! Créez-en un dans le dialogue plus bas		
mar_enq_id	geocoding	enquete	enq_id
	Nom de la contrainte: marqueur_ibfk_1		
	ON DELETE	CASCADE	
	ON UPDATE	CASCADE	
mar_tel_id	geocoding	telephone	tel_id
	Nom de la contrainte: marqueur_ibfk_2		
	ON DELETE	CASCADE	
	ON UPDATE	CASCADE	

4.3 Programmation

4.3.1 Outils

Plusieurs outils ont été utilisés dans ce projet. C'est pourquoi je trouve nécessaire le fait d'aborder brièvement chacun d'entre eux.

4.3.1.1 Logiciels

Tableau 2 : Programmes utilisés

Nom	Fonction
Notepad++ 6.6.9	Editeur de texte
WampServer 2.5	Apache MySQL PHP
Google Chrome	Navigateur Internet

4.3.1.2 CSS

Après énormément de réflexion et de temps passé à rechercher un template, j'ai opté pour partir de zéro. Il existe plusieurs templates de type « DashBoard », mais ils étaient soit payants, soit pas adaptés au projet.

C'est pourquoi j'ai opté pour le framework Bootstrap.

4.3.1.3 JavaScript

Tableau 3 : Bibliothèques JavaScript utilisées

Nom	Utilité
Google Maps JavaScript API v3	Affichage d'une carte et de marqueurs
Bootstrap	Utilisation de composants (fenêtres modales)
jQuery	Interaction des éléments HTML
jQueryUI <ul style="list-style-type: none">• Datepicker• Slider	Utilisation lors de l'insertion des dates afin de faciliter l'utilisateur dans la saisie.
markerClusterer	Lorsqu'il y a trop de marqueurs dans une zone, crée un cluster contenant un nombre qui indique combien de marqueurs sont dans la zone.
Dropzone	Utilisé pour l'upload des photos.
Timepicker	Ajout de l'heure dans le plugin Datepicker de jQuery UI.

4.3.2 Fonctionnalités principales

4.3.2.1 Upload de photos avec coordonnées

Lors de l'ajout de marqueurs, il est possible de sélectionner une ou plusieurs photos à examiner.

Il faut préciser qu'il y a plusieurs restrictions lors de l'upload de photos pour des questions de performances. Leur taille ne doit pas dépasser les 10Mo et l'upload est limité à vingt photos simultanément.

Pour ce faire il faut cliquer sur le menu « Marqueurs ». Il sera possible de voir tous les marqueurs présents dans la base de données.

Puis il faut cliquer sur le bouton « Ajouter marqueur » et une fenêtre modale apparaîtra, laissant le choix à l'utilisateur d'ajouter un marqueur de façon manuelle ou bien avec des photos.

Figure 41 : Fenêtre modale – Ajout d'un nouveau marqueur



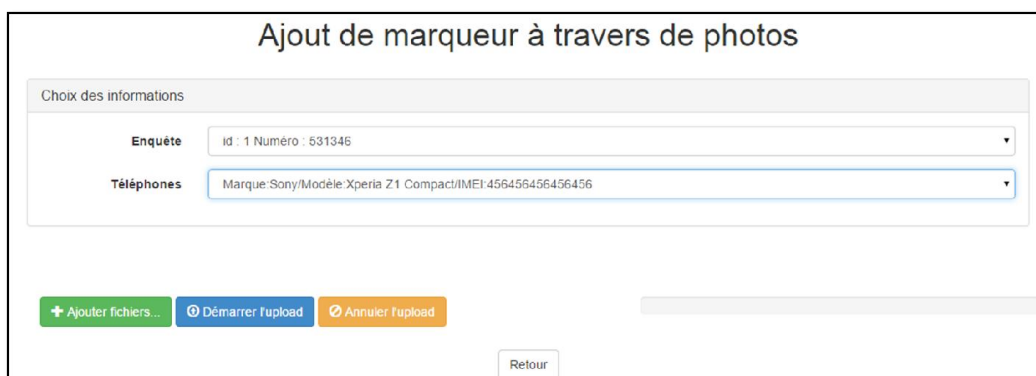
Arrivé à ce stade, il faut cliquer sur le bouton « Photos Exif », puis on arrivera sur une autre page.

Figure 42 : Ajout d'un marqueur photo



Pour afficher les boutons qui permettent d'uploader des fichiers, il faut pour cela choisir l'enquête concernée et le téléphone depuis lequel les photos ont été prises.

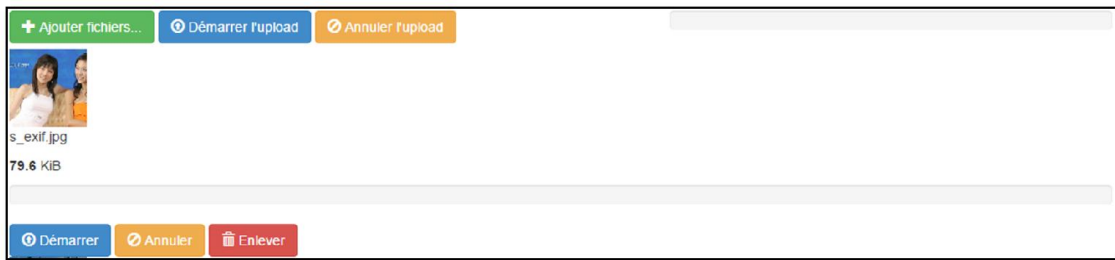
Figure 43 : Upload de photos activé



En cliquant sur le bouton vert « Ajouter fichiers », une boîte de dialogue s'ouvre. C'est là qu'il faut sélectionner la ou les photos. Une fois fait, la miniature de celle-ci apparaîtra avec son nom et sa taille.

Comme on peut le voir sur l'image ci-dessous, il est tout à fait possible d'uploader les photos une par une, ou bien de stopper l'upload.

Figure 44 : Upload de photos



Une fois l'upload démarré, elle sera transmise du côté serveur pour l'analyse d'informations Exif. Si la photo contient les informations des tags (GPS et date/heure) que l'on désire récupérer, le système va alors les récupérer et insérer une nouvelle entrée dans la base de données. L'id du marqueur inséré est alors récupéré et utilisé pour renommer la photo. Elle est ensuite placée dans le dossier « Photos », à l'intérieur du dossier « Marqueur ».

4.3.2.2 GoogleMaps

Cette fonctionnalité permet d'afficher des marqueurs sur une carte. Pour ce faire, il faut d'abord sélectionner une enquête parmi la liste. Puis la liste des téléphones concernés se chargera. Il faut sélectionner au moins deux téléphones afin de lancer l'affichage des points (voir annexe 6).

Une fois fait et le bouton « Afficher » appuyé, les marqueurs s'affichent sur la carte de deux couleurs, chacune correspondant à un téléphone (voir annexe 7). On aperçoit un cluster formé de quatre marqueurs, ce qui veut dire que quatre emplacements sont proches les uns des autres.

Il est tout à fait possible de changer d'enquête et simplement de téléphones en faisant la même manipulation. De plus, il est possible de filtrer les marqueurs par date. La date minimale correspond au marqueur le plus ancien. Et la date maximale à l'emplacement le plus récent.

4.3.2.3 Reporting

Cette fonctionnalité permet d'afficher les distances entre tous les marqueurs d'une même enquête. C'est d'une utilité remarquable, car en un coup d'œil, on peut voir les marqueurs voisins.

Une fois l'enquête sélectionnée, une liste de tous les marqueurs s'affiche dans un encadré bleu comme dans l'image de l'annexe 8.

Plus bas dans la page (voir annexe 9), se trouve un encadré vert dans lequel on trouve un tableau par marqueur, dans lequel il est comparé à tous les autres afin de calculer la distance entre les deux emplacements.

Il est possible de filtrer les résultats grâce à la liste « Distance maximum », qui permet de choisir les valeurs suivantes :

- < 1 kilomètre
- < 5 kilomètres
- < 10 kilomètres

S'il n'y a pas d'emplacements voisins une fois le filtre appliqué le message d'erreur suivant s'affiche entre l'encadré bleu et l'encadré vert :

Figure 45 : Exemple filtre < 1 km



Bien sûr, si l'enquête sélectionnée ne contient pas de marqueurs, un message s'affiche dans le même encadré rouge. Idem lorsqu'une enquête ne contient qu'un marqueur.

Figure 46 : Exemple aucun marqueur dans l'enquête



Figure 47 : Exemple un marqueur dans l'enquête

Choisir une enquête : id : 3 Numéro : 923878 Date de début : 01/01/2001 Date de fin : 10/10/2010

Distance maximum : Aucun filtre

Liste des marqueurs de l'enquête id 3

id	Date	Nom	Adresse	Latitude	Longitude	Marque	Modèle	IMEI
15	2014-12-08 12:12:34	Test	Test	46.181290	6.100191	HTC	Legend	333333333333444

Aucun marqueur à comparer !
Marqueur id 15

5. Conclusion

Après de nombreuses recherches dans le domaine de la géolocalisation, on s'aperçoit que c'est utilisé à très grande échelle. L'envie et le besoin de savoir où l'on se trouve et même où les autres se trouvent remonte à loin dans l'histoire.

La combinaison des technologies permet de pallier aux désavantages de certaines d'entre elles, comme par exemple l'utilisation du Wi-Fi et des réseaux GSM afin de trouver une localisation. Certes, c'est plus rapide, mais l'emplacement reste très approximatif comparé au GPS.

Les informations à l'intérieur des smartphones existent vraiment. De plus, comme on l'a vu, il est possible de trouver des coordonnées GPS à l'intérieur des photos. Les fichiers systèmes sont également riches en informations de localisation. Cependant, l'accès à ses fichiers reste quelque peu laborieux pour une personne pas à l'aise avec la technique.

La partie pratique du projet a permis de voir qu'il était possible d'extraire des coordonnées GPS de fichiers JPEG/Exif. Le fait de prendre en main l'API de Google Maps a été une grande aventure pour moi, autant que le framework Bootstrap et l'upload de photos.

En conclusion, je trouve qu'il est important de savoir que la géolocalisation est quelque chose de présent dans notre quotidien. Qu'on le veuille ou non, les diverses techniques permettent aux autorités, mais également à des hackers, de profiter des possibilités qu'elles offrent. Ce qui amène à réfléchir à propos à l'atteinte à la sphère privée de toutes ces technologies.

Les avancées technologiques dans ce domaine connaîtront-elles une limite un jour ?

Bibliographie

- <http://www.neilson.co.za/mobile-network-geolocation-obtaining-the-cell-ids-the-signal-strength-of-surrounding-towers-from-a-gsm-modem/>
- <http://technowizz.wordpress.com/2010/01/03/lbs-technologies-part-1/>
- <http://anr-prodige.com/index.php?n=Technologies.Geolocalisation>
- <http://ressources.univ-lemans.fr/AccesLibre/UM/Pedago/physique/02/divers/gps1.html>
- http://ec.europa.eu/enterprise/policies/satnav/galileo/why/index_en.htm
- <http://www.google.com/about/company/history/#2004>
- <http://www.techhive.com/article/2000276/a-brief-history-of-gps.html>
- <http://www.mio.com/technology-history-of-gps.htm>
- http://en.wikipedia.org/wiki/Global_Positioning_System
- <http://www.nfctags.com/nfc-success-stories>
- <http://www.tomsguide.fr/article/nfc-smartphone.2-78-9.html>
- <http://www.idownloadblog.com/2014/10/27/iphone-6-nfc-new-uses/>
- <http://blog.atlasrfidstore.com/rfid-vs-nfc>
- <http://fr.scribd.com/doc/2951650/Via-verde-o-mito-portugues#scribd>
- <http://www.oguiadeportugal.com/2013/06/via-verde-sistema-de-portagens.html>
- <http://www.cnil.fr/linstitution/actualite/article/article/geolocalisation-et-collecte-dinformations-issues-des-points-daces-wi-fi-le-pas-en-avant-de-mi/>
- <http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/la-geolocalisation-a-partir-des-points-daces-wi-fi/>
- http://www.astel.be/La-geolocalisation-des-GSM_585
- <http://www.over-blog.com/La-localisation-de-Gsm-comment-ca-marche-1095203942-art142861.html>
- <http://resources.infosecinstitute.com/sim-card-forensics-introduction/>
- <http://www.theguardian.com/technology/2010/may/21/google-street-view-uk-data>
- <http://www.cnet.com/news/microsoft-collects-locations-of-windows-phone-users/>
- <http://www.theguardian.com/technology/blog/2011/apr/26/windows-phone-location-data>
- <http://www.rembrandtvc.com/news/story/431/is-it-tracking-your-location-via-smartphone>
- <http://www.01net.com/editorial/531977/comme-liphone-android-possederait-un-mouchard/>
- <http://www.awaresystems.be/index.html>
- http://en.wikipedia.org/wiki/Exchangeable_image_file_format
- http://en.wikipedia.org/wiki/Near_field_communication
- http://en.wikipedia.org/wiki/Radio-frequency_identification
- <http://www.photometadata.org/meta-resources-metadata-types-standards-exif>
- http://www.cipa.jp/std/std-sec/jcia-std_e.html
- <http://www.dis.org/shiopley/>

<http://www.starkrealities.com/shiplely.html>
<http://www.admin.ch/opc/fr/classified-compilation/19370083/index.html#a143bis>
http://www.chine-informations.com/guide/boussole_2964.html
<http://mashable.com/2014/05/25/commercial-gps-25-anniversary/>
<http://www.centrenational-rfid.com/fonctionnement-dun-systeme-rfid-article-17-fr-ruid-17.html>
<http://anr-prodige.com/index.php?n=Technologies.Geolocalisation>
<http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid>
<http://news.thomasnet.com/imt/2014/03/04/passive-vs-semi-passive-vs-active-tags-in-rfid>
<http://getbootstrap.com/examples/theme/#>
<https://developers.google.com/maps/documentation/business/geolocation/>
<http://trentrichardson.com/examples/timepicker>
<http://openclassrooms.com/courses/prenez-en-main-bootstrap/mise-en-route-8>
<http://getbootstrap.com/examples/theme/#>
<http://blueimp.github.io/jQuery-File-Upload/index.html>
<http://openclassrooms.com/courses/exif-lire-les-infos-d-une-image>
<http://www.movable-type.co.uk/scripts/latlong-vincenty.html>

Annexe 1 : Glossaire

E-OTD : Enhanced Observed Time Difference est un standard utilisé pour localiser des téléphones portables.

Exif : Exchangeable image file format est un standard qui apporte des informations supplémentaires à des images et des vidéos sous forme de tags.

GPS : Le Global Positioning System désigne le système de navigation par satellite.

GSM : Global System for Mobile Communications est la norme utilisé par les téléphones portables lors de télécommunications.

IFD : Image File Directory correspond aux structures contenant des données Exif.

MAC : C'est un identifiant unique qui est présent dans tous les périphériques pouvant communiquer à travers le réseau internet.

NFC : Near Field Communication est une technologie de communication sans-fil de courte portée, basée sur le RFID.

OS : Operating System désigne le software installé dans les périphériques électroniques.

PDA : Personal Digital Assistant - Pocket PC.

QoS : Le Quality of Service est la mesure de performance globale d'un réseau d'ordinateurs ou d'un réseau téléphonique.

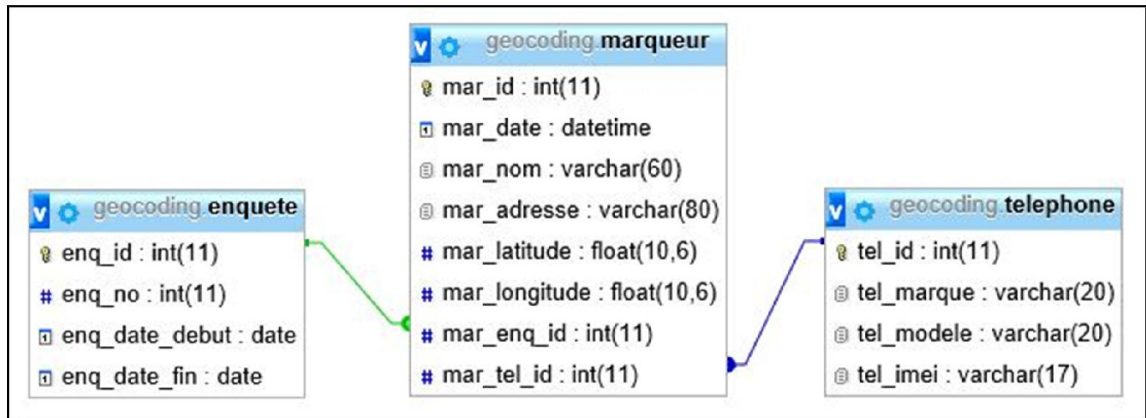
RFID : Radio-frequency identification est une technologie de communication sans-fil.

SSH : Secure Shell est un protocole réseau de communication sécurisé.

SSID : Service set identification est le nom qui identifie un réseau sans-fil.

TOA : Time of Arrival correspond à la méthode de la triangulation des réseaux GSM. L'élément mesuré est le temps que les ondes mettent à parcourir du téléphone portable à l'antenne cellulaire.

Annexe 2 : Modèle physique de données



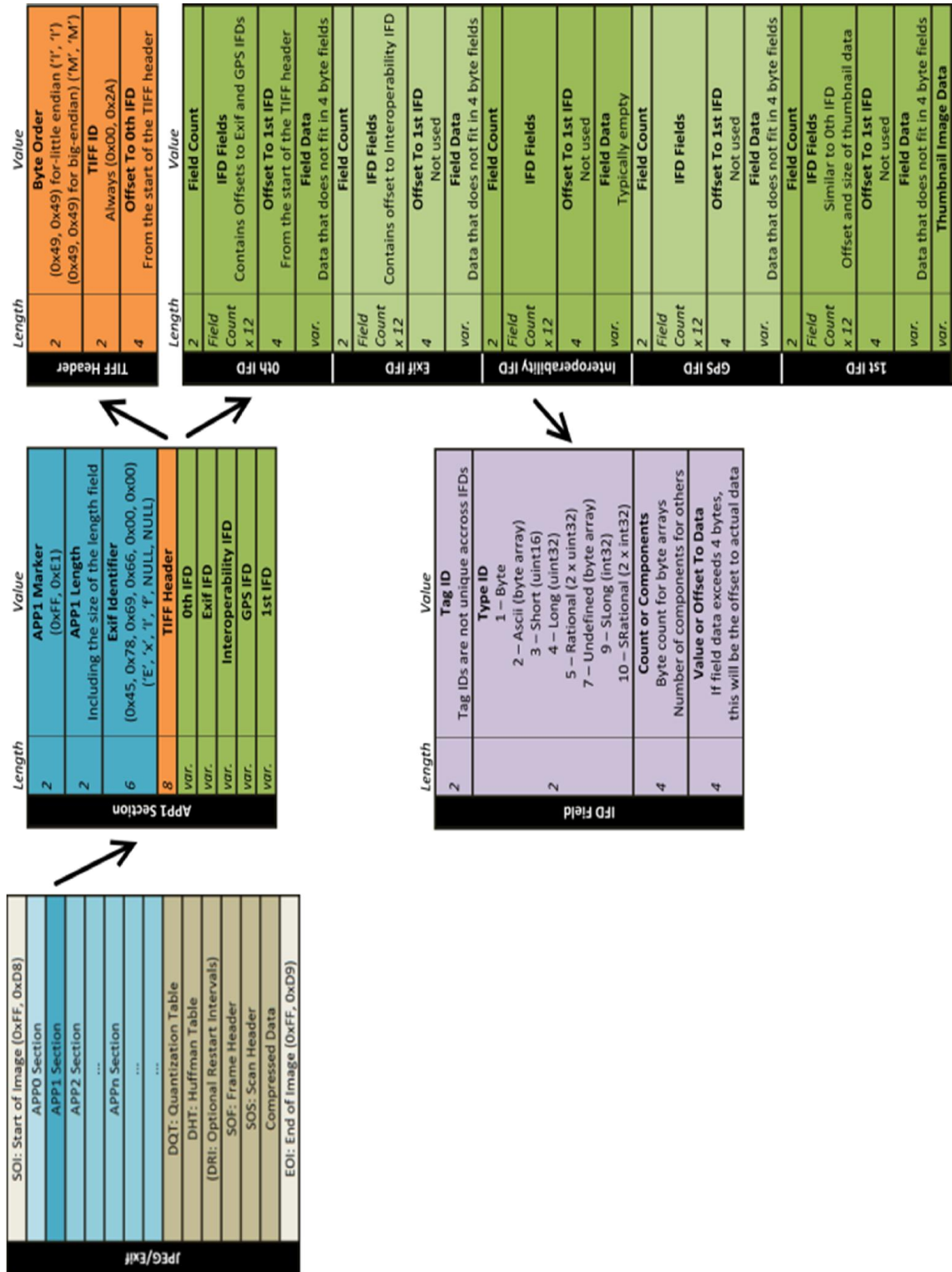
Annexe 3 : Dictionnaire de données

enquete								
Colonne	Type	Null	Défaut	Commentaires				
enq_id	int(11)	Non						
enq_no	int(11)	Non						
enq_date_debut	date	Non						
enq_date_fin	date	Oui	NULL					
Index								
Nom de l'index	Type	Unique	Compressé	Colonne	Cardinalité	Interclassement	Null	Commentaire
PRIMARY	BTREE	Oui	Non	enq_id	8	A	Non	
enq_id	BTREE	Non	Non	enq_id	8	A	Non	
marqueur								
Colonne	Type	Null	Défaut	Commentaires				
mar_id	int(11)	Non						
mar_date	datetime	Non						
mar_nom	varchar(60)	Oui	NULL					
mar_adresse	varchar(80)	Oui	NULL					
mar_latitude	float(10,6)	Non						
mar_longitude	float(10,6)	Non						
mar_enq_id	int(11)	Non						
mar_tel_id	int(11)	Non						
Index								
Nom de l'index	Type	Unique	Compressé	Colonne	Cardinalité	Interclassement	Null	Commentaire
PRIMARY	BTREE	Oui	Non	mar_id	21	A	Non	
mar_enq_id	BTREE	Non	Non	mar_enq_id	10	A	Non	
mar_tel_id	BTREE	Non	Non	mar_tel_id	21	A	Non	
telephone								
Colonne	Type	Null	Défaut	Commentaires				
tel_id	int(11)	Non						
tel_marque	varchar(20)	Non						
tel_modele	varchar(20)	Non						
tel_imei	varchar(17)	Non						

Annexe 4 : Dictionnaire de données (suite)

Index								
Nom de l'index	Type	Unique	Compressé	Colonne	Cardinalité	Interclassement	Null	Commentaire
PRIMARY	BTREE	Oui	Non	tel_id	24	A	Non	
tel_id	BTREE	Non	Non	tel_id	24	A	Non	

Annexe 5 : Vue graphique d'un fichier JPEG/Exif



(Source : ExifLibrary for .NET. codeproject.com)

Annexe 6 : Fonctionnalité GoogleMaps au démarrage

Choix des informations

Enquête: -- Enquêtes --

Téléphones: Choisir deux téléphones

Afficher

Détail des téléphones

Téléphone	Téléphone

Détail des emplacements

Plus ancien	Plus récent

Filter la plage horaire

Nb. marqueurs:

Date minimale:

Date maximale:

Filter **Réinitialiser**

Carte

Annexe 7 : Fonctionnalité GoogleMaps après requête

GEOCODING

Choix des informations

Enquête
Id : 1 Numéro : 531346

Téléphones

Marque: Sony/Modèle: Xperia Z1 Compact/IMEI: 456456456456456
 Marque: Samsung/Modèle: Galaxy Alpha/IMEI: 345654321768543
 Marque: HTC/Modèle: Legend/IMEI: 33333333333333444
 Marque: Apple/Modèle: iPhone 6/IMEI: 83746352867356743

[Attacher](#)

Détail des téléphones

Marque	Téléphone	Téléphone
Samsung	Sony	
Galaxy Alpha	Xperia Z1 Compact	
IMEI: 345654321768543	IMEI: 456456456456456	

3

Détail des emplacements

Plus ancien	Plus récent
14/08/2013 10:27	13/08/2014 10:08

5

Filter la plage horaire

Nb. marqueurs: 5

Date minimale: 14/08/2013 10:27

Date maximale: 13/08/2014 10:08

[Filtrer](#) [Réinitialiser](#)

Carte

Annexe 8 : Fonctionnalité Reporting après requête

GEOCODING GoogleMaps Reporting Enquêtes Marqueurs Téléphones

Choisir une enquête
 id : 1 Numéro : 531346 Date de début : 07/01/2014 Date de fin : 10/10/2014

Distance maximum
 Aucun filtre

Liste des marqueurs de l'enquête id 1

id	Date	Nom	Adresse	Latitude	Longitude	Marque	Modèle	IMEI
1	2014-08-13 10:08:22	Sans nom	Sans adresse	47.612823	-122.340363	Sony	Xperia Z1 Compact	456456456456456
2	2013-08-14 10:27:26	Café du Lys	Rue de l'Ecole-de-Médecine 7, 1205 Genève, CH	46.197231	6.138412	Samsung	Galaxy Alpha	345654321768543
5	2014-11-02 17:58:59	Pan Africa Market	1521 1st Ave, Seattle, WA	47.608940	-122.340141	HTC	Legend	333333333333333444
6	2014-07-16 12:20:10	Buddha Thai & Bar	2222 2nd Ave, Seattle, WA	47.613590	-122.344391	Apple	Iphone 6	83746352867356743
7	2014-02-13 13:23:46	The Melting Pot	14 Mercer St, Seattle, WA	47.624561	-122.356445	Samsung	Galaxy Alpha	345654321768543
12	2014-05-12 07:52:29	Wingdome	1416 E Olive Way, Seattle, WA	47.617214	-122.326584	Samsung	Galaxy Alpha	345654321768543
13	2014-01-15 10:15:15	Piroshky Piroshky	1908 Pike pl, Seattle, WA	47.610126	-122.342834	Sony	Xperia Z1 Compact	456456456456456
14	2014-11-30 05:32:00	Sans nom	Sans adresse	47.613605	-122.350395	Apple	Iphone 6	83746352867356743
16	2003-11-23 18:07:37	Photo	Aucune adresse	39.915558	116.390831	Apple	Iphone 6	83746352867356743
17	2014-10-29 16:34:33	Photo	Aucune adresse	46.181973	6.144631	Apple	Iphone 6	83746352867356743
18	2002-07-13 15:58:28	Photo	Aucune adresse	54.389666	-1.914167	Apple	Iphone 6	83746352867356743

Annexe 9 : Fonctionnalité Reporting après requête (suite)

Résultats			
Détails du marqueur id 1			
id	Latitude	Longitude	Distance entre les emplacements
2	46.197231	6.138412	8445.52 Kilomètres
5	47.608940	-122.340141	432 mètres
6	47.613590	-122.344391	314 mètres
7	47.624561	-122.356445	1.78 kilomètre
12	47.617214	-122.326584	1.14 kilomètre
13	47.610126	-122.342834	352 mètres
14	47.613605	-122.350395	757 mètres
16	39.915558	116.390831	8688.57 Kilomètres
17	46.181973	6.144631	8447.21 Kilomètres
18	54.989666	-1.914167	7322.49 Kilomètres
Détails du marqueur id 2			
id	Latitude	Longitude	Distance entre les emplacements
1	47.612823	-122.340363	8445.52 Kilomètres
5	47.608940	-122.340141	8445.87 Kilomètres
6	47.613590	-122.344391	8445.62 Kilomètres
7	47.624561	-122.356445	8445.11 Kilomètres
12	47.617214	-122.326584	8444.54 Kilomètres
13	47.610126	-122.342834	8445.88 Kilomètres
14	47.613605	-122.350395	8445.87 Kilomètres
16	39.915558	116.390831	8203.94 Kilomètres
17	46.181973	6.144631	1.76 kilomètre
18	54.989666	-1.914167	1129.24 Kilomètres

Annexe 10 : Print Screen WinSCP Consolidated.db

/private/var/root/Library/Caches/locationd					
Name	Ext	Size	Changed	Rights	Owner
..			10.12.2014 23:30:06	rwX-----	root
adsf			01.01.1970 01:43:09	rwX-----	root
ephemeris			01.01.1970 01:43:09	rwX-----	root
indoor_tiles			19.12.2014 07:06:35	rwX-----	root
tiles			19.12.2014 07:06:35	rwX-----	root
tiles_app_v2			19.12.2014 07:06:36	rwX-----	root
tiles_cell			01.01.1970 01:43:09	rwX-----	root
.dat0031.05a		4 571 B	10.12.2014 16:42:02	rw-r--r--	root
.dat003f.063		15 510 B	10.11.2014 02:14:08	rw-r--r--	root
.dat003f.064		762 B	10.11.2014 02:14:08	rw-r--r--	root
.dat003f.11b		0 B	18.11.2014 07:12:17	rw-r--r--	root
.dat003f.2b4		15 470 B	21.10.2014 16:56:48	rw-r--r--	root
.dat0040.0a7		0 B	10.12.2014 15:51:25	rw-r--r--	root
.dat0069.02e		762 B	10.12.2014 16:45:11	rw-r--r--	root
cache.plist		762 B	19.12.2014 07:07:13	rw-r--r--	root
cache_encryptedA.db		468 KiB	19.12.2014 07:06:35	rw-r--r--	root
cache_encryptedC.db		28 672 B	10.12.2014 07:30:06	rw-r--r--	root
clients.plist		5 347 B	19.12.2014 07:07:16	rw-r--r--	root
consolidated.db		36 864 B	10.12.2014 19:37:59	rw-r--r--	root
gyroCal.db		28 672 B	15.12.2014 22:12:40	rw-r--r--	root
lockCache_encrypted...		196 KiB	19.12.2014 05:58:46	rw-r--r--	root
network.plist		106 B	19.12.2014 07:07:14	rw-r--r--	root
significant.plist		42 B	10.11.2014 17:06:37	rw-r--r--	root
significantVisitAuth.p...		42 B	10.11.2014 17:04:18	rw-r--r--	root
significantVisitInteres...		42 B	19.10.2014 06:41:30	rw-r--r--	root
stats.plist		77 B	19.12.2014 07:07:16	rw-r--r--	root
WMM.dat		4 650 B	10.12.2014 07:30:07	rw-r--r--	root