h e g

Haute école de gestion
Genève

Récupération de données à partir d'iOS

De la théorie à un cas pratique

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

par :

Diogo BRANDAO

Conseiller au travail de Bachelor :

David BILLARD

Genève, le 6 octobre 2017

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

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 Bachelor of Science en Informatique de Gestion.

L'étudiant atteste que son travail a été vérifié par un logiciel de détection de plagiat.

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 6 octobre 2017

Diogo BRANDAO

Remerciements

En premier lieu, je souhaite remercier la Haute Ecole de Gestion ainsi que les professeurs m'ayant soutenu durant mon parcours académique.

Je remercie particulièrement Monsieur David Billard qui m'a guidé durant mon travail. Il a su me conseiller et partager ses connaissances afin que je progresse dans la réalisation de ce travail.

Pour finir, je remercie mes proches, ma famille et mes amis, qui ont su me soutenir pendant la réalisation de mon mémoire.

Résumé

Le nombre de smartphones et de tablettes ne cesse de croître d'année en année à tel point qu'ils peuvent remplacer les ordinateurs dans certaines tâches. En effet, la technologie utilisée dans ces appareils évolue rapidement et offre aux utilisateurs de nombreuses fonctionnalités comme l'appareil photo, la messagerie et bien d'autres. De plus, les constructeurs proposent davantage de stockage pour que les consommateurs puissent stocker énormément de données.

Apple a révolutionné le monde en présentant le premier smartphone multi-touch en 2007 et l'iPad en 2012. Depuis, l'entreprise à la pomme a commercialisé plus d'un milliard de téléphones qui s'ajoutent au total des ventes des iPad et des iPod. IOS est le système d'exploitation mobile développé par Apple pour plusieurs tous ses appareils mobile (iPhone, iPad et iPod) et est réputé pour sa sécurité accrue.

Les smartphones et les tablettes sont utilisés au quotidien par les consommateurs. Simples d'utilisation et pratiques, nous l'avons dans notre poche lorsque nous nous rendons au travail ou sur la table de chevet pour une lecture avant de nous coucher. En octobre 2016[1], davantage de personnes dans le monde ont surfé sur l'Internet mobile que depuis un simple poste d'ordinateur. Dès lors, ces produits représentent une énorme source de données. En effet, ces objets contiennent toutes sortes de données personnelles et pouvant être très sensibles tels que l'historique de navigation, la messagerie, les photos, les mots de passe, etc.

Ce travail a pour but de récupérer des données sur les périphériques d'Apple de différentes manières, depuis la sauvegarde effectuée par iTunes, par iCloud et directement depuis l'appareil.

[1] https://www.lesechos.fr/02/11/2016/lesechos.fr/0211453241386_l-internet-mobile-depasse-pour-la-premiere-fois-l-internet-fixe-dans-le-monde.htm

Table des matières

Liste des tableaux

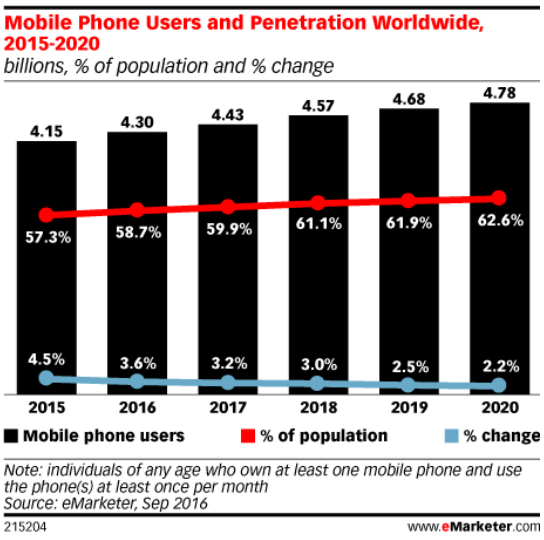
Liste des figures

1. Introduction

Apple a révolutionné le marché de la téléphonie mobile en présentant un mini-ordinateur capable de téléphoner et d'envoyer des messages. Par la suite, il présenta une tablette qui, selon certains spécialistes, aurait pour conséquence de menacer le marché de l'ordinateur portable et cela s'est avéré exact. En effet, depuis le franc succès des smartphones et des tablettes, les ventes d'ordinateurs s'effondrent d'année en année. L'Internet mobile a également aidé à ce succès en proposant une connexion aussi rapide que sur un ordinateur.

De nos jours, il est beaucoup plus simple et pratique d'utiliser un appareil connecté pour effectuer certaines tâches. En quelques gestes, nous pouvons prendre une photo, consulter nos mails, discuter avec un partenaire, utiliser les réseaux sociaux… Nous passons énormément de temps sur nos appareils et le nombre d'utilisateurs ne cesse de grandir.

Figure 1 : Nombre d'utilisateurs



(https://www.emarketer.com/Article/Mobile-Phone-Smartphone-Usage-Varies-Globally/1014738)

La capacité maximale d'un iPhone est de 256go, un espace de stockage important afin de permettre aux utilisateurs de garder en mémoire leurs données personnelles. Cependant, la hantise de tout possesseur de smartphones et/ou de tablettes est de ne pas retrouver ses données ou, au contraire, ces appareils peuvent contenir des preuves utiles pour une enquête judiciaire.

A travers ce travail, je démontrerais les différentes manières de récupérer ces données.

2. Périphérique iOS

Apple a conçu son propre système d'exploitation connu sous le nom d'IOS. Ce système d'exploitation est présent sur l'iPhone, l'iPad et l'iPod. Le dernier IOS en date est la version 11 sortie le 19 septembre 2017.

2.1 iPhone

L'appareil le plus populaire chez Apple est sans doute l'iPhone. Au total, 18 modèles ont été présentés, l'iPhone 8 et 8 Plus ainsi que l'iPhone X ont été dévoilés cette année. Dans le tableau ci-contre, les différents modèles disponibles à la vente.

Tableau 1 : Modèles d'iPhone disponibles à la vente

Modèle	**Date de sortie**	**Stockage**
iPhone 6s / 6s Plus	25 septembre 2015	32 / 128go
iPhone SE	31 mars 2016	32 / 128go
iPhone 7 / 7Plus	16 septembre 2016	32 / 128go
iPhone 8 / 8 Plus	22 septembre 2017	64 / 256go
iPhone X	11 novembre 2017	64 / 256go

(https://www.apple.com/iphone/)

2.2 iPad

Suite au franc succès de l'Iphone, Apple a lancé sur le marché sa première tablette en 2010. L'iPad, comme l'iPhone, fonctionne sous le système d'exploitation IOS. Dans le tableau ci-contre, les différents modèles disponibles à la vente.

Tableau 2 : Modèles d'iPad disponibles à la vente

Modèle	**Date de sortie**	**Stockage**
iPad mini 4	9 septembre 2015	128go
iPad	24 mars 2017	32 / 128go
iPad Pro	31 mars 2016/13 juin 2017	64/256/512

(https://www.apple.com/ipad/)

2.3 iPod Touch

Un autre appareil qu'Apple a lancé est l'iPod Touch. Ce baladeur numérique a été conçu sans les fonctions de téléphonie, mais avec le même système d'exploitation que l'iPhone et l'iPad.

Tableau 3 : Modèle d'iPod disponible à la vente

Modèle	**Date de sortie**	**Stockage**
iPod Touch 6G	15 juillet 2015	8 / 32 / 64go

(https://www.apple.com/ipod-touch/)

2.4 Identifier les appareils

Etant donné qu'Apple propose plusieurs modèles d'iPhone, d'iPad ou d'iPod Touch, il y a différentes manières de les connaître.

2.4.1 Au dos de l'appareil

Premièrement, le numéro de modèle est présent sur chaque périphérique iOS. Il se situe au dos de ce dernier. Ensuite, il suffit de faire une recherche sur Google ou directement sur le site d'Apple. Nous obtenons le modèle ainsi que les différentes caractéristiques de l'appareil.

Figure 3 : Dos d'un iPhone 4

Figure 2 : Caractéristique de l'iPhone 4

iPhone 4

Année de commercialisation : 2010 (modèle GSM), 2011 (modèle CDMA)
Capacité : 8, 16, 32 Go
Couleurs : noir, blanc
Numéro de modèle sur la partie arrière : A1349, A1332

(https://support.apple.com/fr-ch/HT201296)

2.4.2 Depuis iTunes

Si nous possédons le code de déverrouillage du périphérique IOS ou si ce dernier n'en possède pas, il suffit de le connecter à un ordinateur qui contient iTunes. Les informations de l'appareil sont affichées comme sur l'image qui suit :

Figure 4 : Informations de l'appareil sur iTunes

En cliquant sur l'identifiant du modèle, nous obtenons le numéro de série, l'UDID (Unique Device Identifier) ainsi que le numéro ECID (Exclusive Chip ID ou Electronic Chip ID).

2.5 Commande « ideviceinfo »

Pour cette procédure, nous devons installer la bibliothèque « libimobiledevice » ainsi que l'outil « ideviceinstaller ». La bibliothèque contient des protocoles qui permettent de communiquer avec les dispositifs d'Apple. L'outil permet quant à lui de récupérer des informations, effectuer des sauvegardes, synchroniser, etc.

Premièrement, nous devons installer un logiciel de gestion de paquets se nommant Homebrew[2]. Il permet d'installer les outils cités plus haut. Pour cela, il faut ouvrir une boîte de dialogue et taper cette commande :

```
MacBook-Pro-de-Diogo:~ Reguila$ /usr/bin/ruby -e "$(curl -fsSL https://raw.githubuser
content.com/Homebrew/install/master/install)"
```

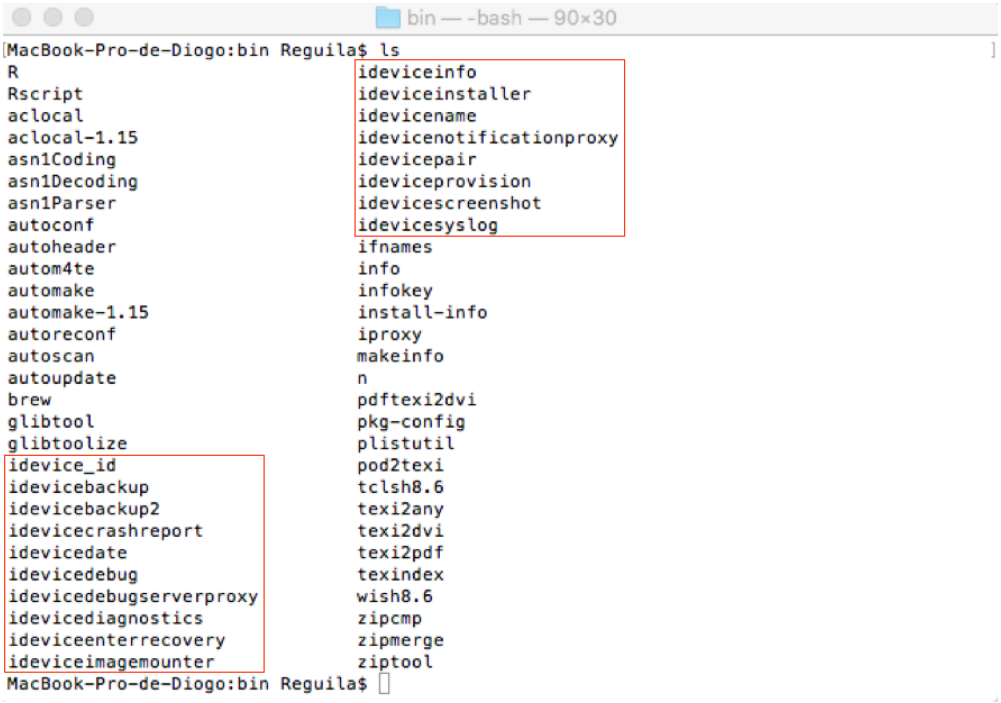
Ensuite, nous faut installer la bibliothèque et l'outil ainsi :

```
MacBook-Pro-de-Diogo:~ Reguila$ brew install --HEAD libimobiledevice -g
```

```
MacBook-Pro-de-Diogo:~ Reguila$ brew install ideviceinstaller -g
```

Pour finir, nous disposons de diverses fonctionnalités présentes dans iTunes. Ces fonctionnalités sont utiles aux utilisateurs Linux afin qu'ils puissent utiliser leurs iDevices[3] sous cet OS. Cette démarche peut être effectuée sur des ordinateurs contenant les systèmes d'exploitation Linux, Mac OS et Windows.

Figure 5 : Fonctionnalités de l'outil "ideviceinstaller"



[2] https://brew.sh/index_fr.html

[3] Terme utilisé pour nommer un dispositif sous iOS

La fonctionnalité « ideviceinfo » est intéressante essentiellement, car elle permet de connaître plusieurs informations sur l'appareil malgré qu'il soit verrouillé par un mot de passe.

Pour retrouver le modèle du dispositif connecté à l'ordinateur, il suffit de chercher « ProductType » ou « HardwareModel ». Pour le premier, nous obtenons le type d'appareil (iPad, iPhone ou iPod) ainsi que 2 chiffres séparés par une virgule. Les chiffres représentent la génération de l'appareil. Et, le deuxième, un numéro composé de chiffres et de lettres qui correspondent au nom interne utilisé par Apple.

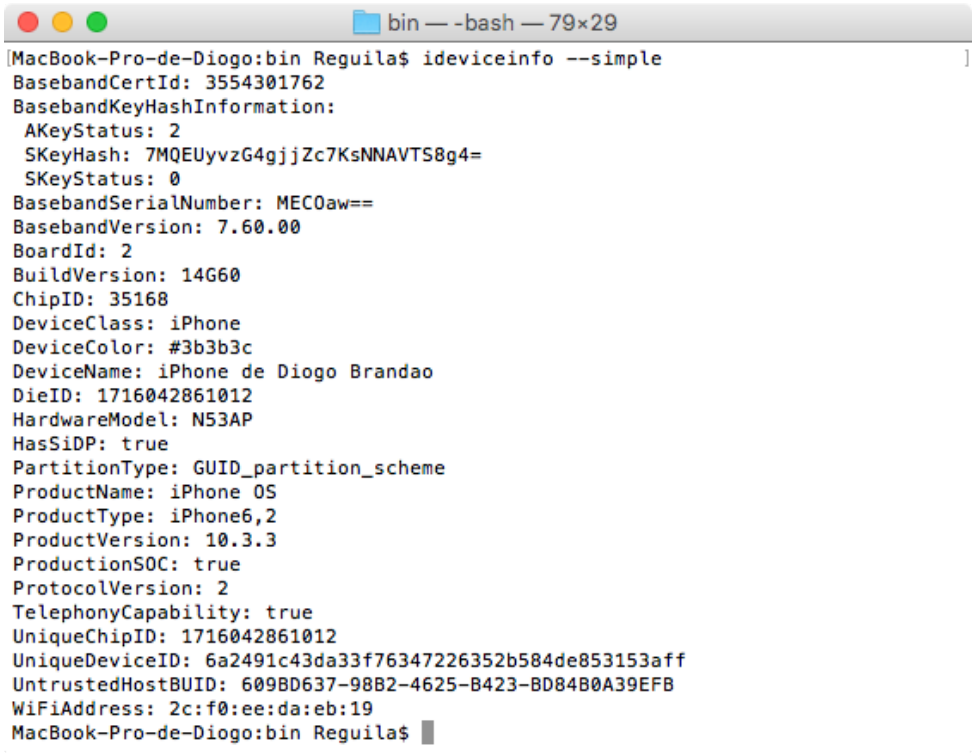
Pour la démonstration de mon travail de Bachelor, deux appareils ont été utilisés.

Tableau 4 : Les modèles des appareils utilisés

Appareil	**ProductType**	**HardwareModel**
iPhone 5s	iPhone6,2	N53AP
iPhone 4	iPhone3,1	N90AP

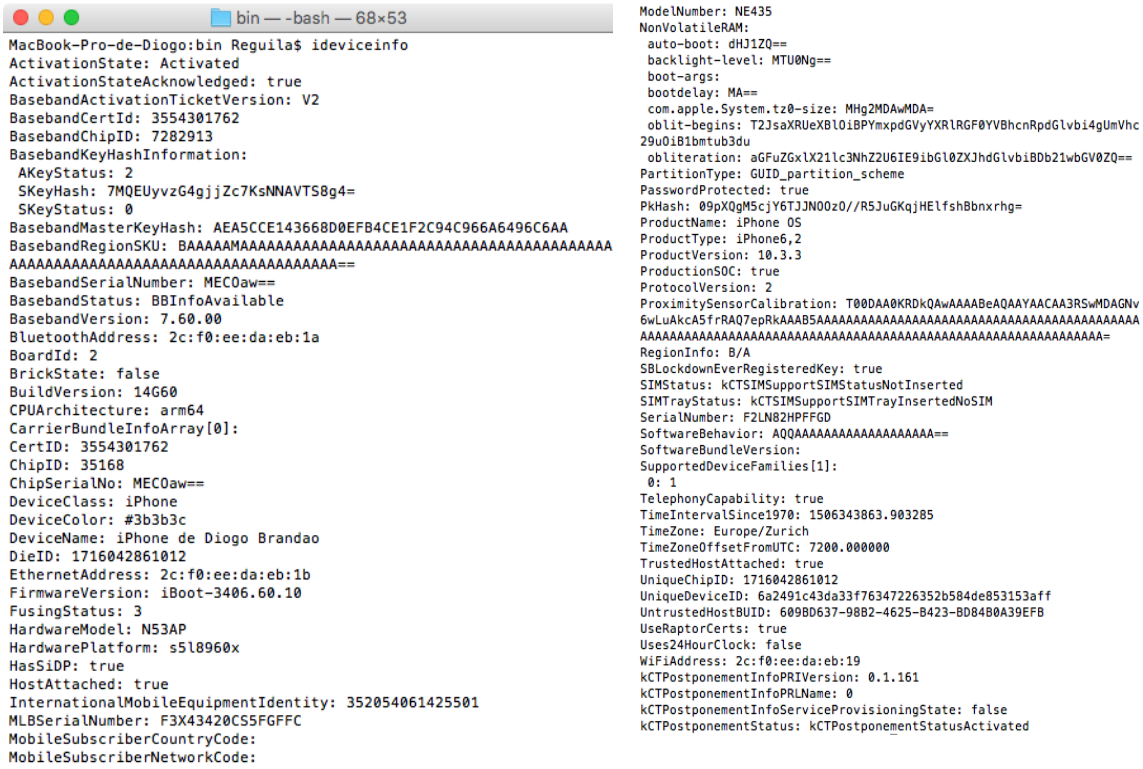
Informations de l'iPhone 5s avant le déverrouillage :

Figure 6 : Informations de l'iPhone 5s



Informations de l'iPhone 5s après le déverrouillage :

Figure 7 : Informations complètes de l'iPhone 5s



```
bin — -bash — 68×53
MacBook-Pro-de-Diogo:bin Reguila$ ideviceinfo
ActivationState: Activated
ActivationStateAcknowledged: true
BasebandActivationTicketVersion: V2
BasebandCertId: 3554301762
BasebandChipID: 7282913
BasebandKeyHashInformation:
 AKeyStatus: 2
 SKeyHash: 7MQEUyvzG4gjjZc7KsNNAVTS8g4=
 SKeyStatus: 0
BasebandMasterKeyHash: AEA5CCE14366BD0EFB4CE1F2C94C966A6496C6AA
BasebandRegionSKU: BAAAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==
BasebandSerialNumber: MECOaw==
BasebandStatus: BBInfoAvailable
BasebandVersion: 7.60.00
BluetoothAddress: 2c:f0:ee:da:eb:1a
BoardId: 2
BrickState: false
BuildVersion: 14G60
CPUArchitecture: arm64
CarrierBundleInfoArray[0]:
CertID: 3554301762
ChipID: 35168
ChipSerialNo: MECOaw==
DeviceClass: iPhone
DeviceColor: #3b3b3c
DeviceName: iPhone de Diogo Brandao
DieID: 1716042861012
EthernetAddress: 2c:f0:ee:da:eb:1b
FirmwareVersion: iBoot-3406.60.10
FusingStatus: 3
HardwareModel: N53AP
HardwarePlatform: s5l8960x
HasSiDP: true
HostAttached: true
InternationalMobileEquipmentIdentity: 352054061425501
MLBSerialNumber: F3X43420CS5FGFFC
MobileSubscriberCountryCode:
MobileSubscriberNetworkCode:
ModelNumber: NE435
NonVolatileRAM:
 auto-boot: dHJ1ZQ==
 backlight-level: MTU0Ng==
 boot-args:
 bootdelay: MA==
 com.apple.System.tz0-size: MHg2MDAwMDA=
 oblit-begins: T2JsaXRUeXBlOiBPYmxpdGVyYXRlRGF0YVBhcnRpdGlvbi4gUmVhc
29uOiB1bmtub3du
 obliteration: aGFuZGxlX21lc3NhZ2U6IE9ibGl0ZXJhdGlvbiBDb21wbGV0ZQ==
PartitionType: GUID_partition_scheme
PasswordProtected: true
PkHash: 09pXQgM5cjY6TJJNOOzO//R5JuGKqjHElfshBbnxrhg=
ProductName: iPhone OS
ProductType: iPhone6,2
ProductVersion: 10.3.3
ProductionSOC: true
ProtocolVersion: 2
ProximitySensorCalibration: T00DAA0KRDkQAwAAAABeAQAAYAACAA3RSwMDAGNv
6wLuAkcA5frRAQ7epRkAAAB5AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
RegionInfo: B/A
SBLockdownEverRegisteredKey: true
SIMStatus: kCTSIMSupportSIMStatusNotInserted
SIMTrayStatus: kCTSIMSupportSIMTrayInsertedNoSIM
SerialNumber: F2LN82HPFFGD
SoftwareBehavior: AQQAAAAAAAAAAAAAAAAA==
SoftwareBundleVersion:
SupportedDeviceFamilies[1]:
 0: 1
TelephonyCapability: true
TimeIntervalSince1970: 1506343863.903285
TimeZone: Europe/Zurich
TimeZoneOffsetFromUTC: 7200.000000
TrustedHostAttached: true
UniqueChipID: 1716042861012
UniqueDeviceID: 6a2491c43da33f76347226352b584de853153aff
UntrustedHostBUID: 609BD637-98B2-4625-B423-BD84B0A39EFB
UseRaptorCerts: true
Uses24HourClock: false
WiFiAddress: 2c:f0:ee:da:eb:19
kCTPostponementInfoPRIVersion: 0.1.161
kCTPostponementInfoPRLName: 0
kCTPostponementInfoServiceProvisioningState: false
kCTPostponementStatus: kCTPostponementStatusActivated
```

3. Système de fichier

Le système de fichier permet de stocker et d'organiser les informations dans des dossier sur une mémoire de masse. Les iDevices embarquent tous le système de fichier AFPS sorti en mars 2017, mais avant celui-ci, c'était le système de fichier HFS+.

3.1 HFS+

C'est une version améliorée de HFS (Hierarchical File System) qui prend en charge des fichiers plus grands. En effet, HFS+ utilise une valeur de 32 bits pour l'attribution d'adresses de blocs alors que son prédécesseur n'utilisait que 16 bits. Ensuite, pour nommer les éléments, Mac OS Roman a été remplacé par de l'Unicode. Ainsi, HFS+ peut prendre en charge plus de quatre milliards de fichiers (2^{32} = 4 294 967 296). Afin de trier ces nombreux fichiers, Apple utilise une structure de données se nommant « B-tree ».

3.2 AFPS

La première bêta d'IOS 10.3, sortie le 26 janvier 2017, apportait un nouveau système de fichier se prénommant APFS (Apple File System). iOS, macOS, tvOS et watchOS ont migré automatiquement sur ce nouveau système. Seuls les iPhone en 64 bits ont profité de ce changement car la valeur utilisée pour le système de fichiers est de 64 bits. Par conséquent, les iPhone possédant une architecture de 32 bits n'ont pas eu la possibilité de détenir l'Apple File System, cela concerne les appareils sortis avant l'iPhone 5s.

Apple a uniformisé son système afin de faciliter le travail aux développeurs, mais surtout d'offrir de meilleures performances que son précurseur. APFS peut ainsi prendre en charge 9 quintillions de fichiers (ce qui équivaut à 9000000000000000000) grâce à son système de fichiers de 64 bits. Il intègre la même structure de données que l'Hierarchical File System.

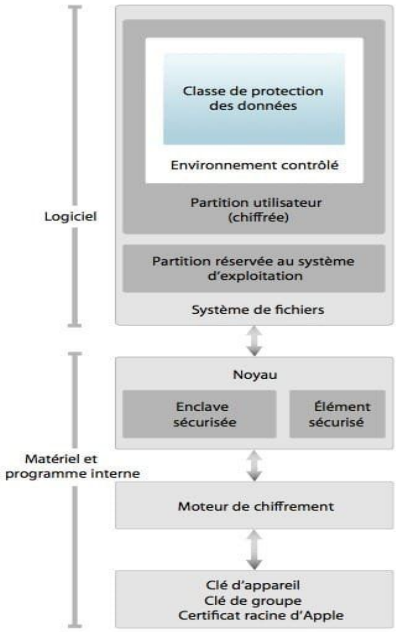
3.3 B-tree

Pour traiter et organiser les données d'une manière simple et triée, la B-tree est utilisée dans les mécanismes de système de fichier et dans les bases de données. Le principe de cette structure de données est d'insérer, de rechercher et de supprimer en temps logarithmique. L'arbre doit être équilibré afin de minimiser le nombre de pas. Pour cela, il croit à partir de la racine et non depuis les feuilles et ainsi, chaque nœud parent peut posséder plus de deux nœuds enfants.

3.4 Partitions

Les dispositifs iOS ont deux types de partitions : la partition de système et la partition de données. Ces dernières sont partitionnées sur le seul disque de montage de l'appareil. La première partition contient les informations relatives au système iOS, comme le système d'exploitation et les applications préinstallées. La dernière comprend toutes les données liées à l'utilisateur.

Figure 8 : Les partitions



(https://iphonesoft.fr/2017/08/18/iphone-5s-securite-firmware-enclave-touch-id-devoile-apple)

3.5 Fichier plist

Une liste de propriétés ou « Proprety list » est une structure de données au format XML. Les applications utilisent ces propriétés pour la gestion de la configuration dans l'OS. Ces fichiers peuvent contenir différentes informations comme une adresse e-mail, des cookies Web, des points GPS… Un simple éditeur de texte permet d'ouvrir ce type de fichier.

3.6 SQLite

Les entrailles d'un dispositif d'Apple regorgent de fichiers SQLite afin d'y stocker des données. Par exemple, l'historique des appels, les SMS et le carnet d'adresses sont enregistrés dans une base de données de type SQLite. Lors de l'extraction de ces fichiers, il est très simple de le parcourir avec un outil adéquat.

4. Sauvegarde

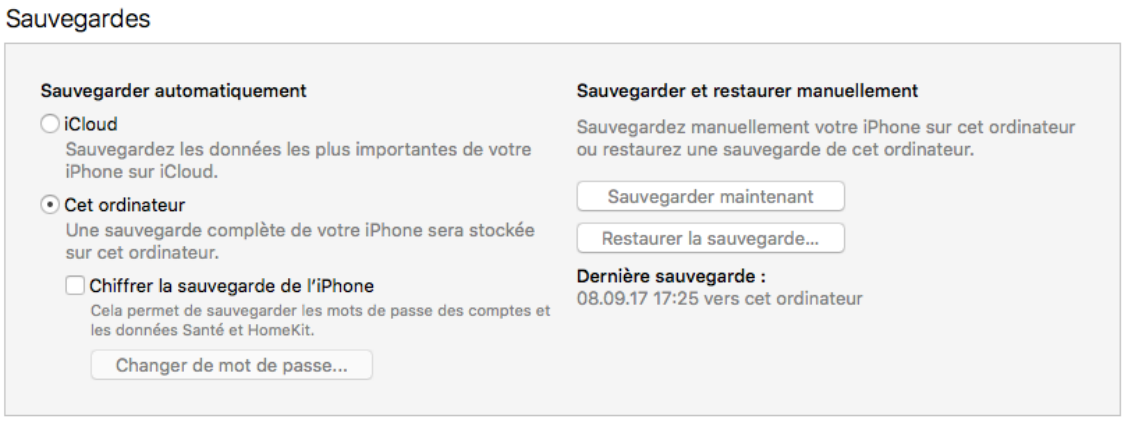
Il existe plusieurs moyens de sauvegarder des données d'un appareil Apple sur un ordinateur ou sur le « cloud ». Une sauvegarde de l'appareil permet d'avoir une copie des données lorsqu'on doit le remplacer ou s'il a subi un problème logiciel. Il se peut qu'il tombe en panne ou, par inadvertance, une suppression a été effectuée. Dès lors, il est possible de récupérer certaines données.

4.1 Par l'intermédiaire d'iTunes

iTunes est un logiciel développé par Apple pour permettre la gestion des photos, vidéos et musiques sur les appareils pommés. Il fait office de lecteur multimédia également. De surcroît, iTunes propose la synchronisation et la sauvegarde des appareils, mais dans le cadre de ce travail, nous analyserons uniquement la sauvegarde. La synchronisation a pour but de transférer les médias choisis par l'utilisateur présents sur l'ordinateur.

Pour effectuer une sauvegarde depuis iTunes, il est indispensable d'installer le logiciel sur MacOs ou sur Windows. Ensuite, le dispositif doit être branché par USB et par défaut, iTunes s'ouvre en affichant les informations de ce dernier. Dans la même fenêtre, Apple propose d'effectuer une sauvegarde soit sur iCloud, soit sur l'ordinateur. Dans cet exemple, le second choix est opté.

Figure 9 : Sauvegarder depuis iTunes



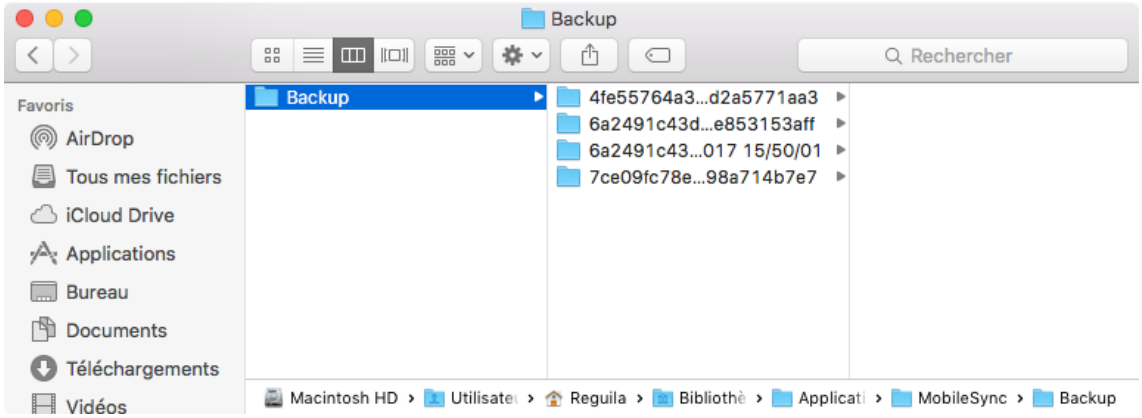
Nous pouvons aussi chiffrer la sauvegarde en cochant la case située en dessous. Cette option est aussi disponible pour iCloud. En chiffrant la sauvegarde par un mot de passe, l'utilisateur augmente la sécurité et rend l'accès plus difficile. Si le mot de passe est oublié ou n'est pas connu, il sera compliqué d'effectuer une restauration.

Selon le système d'exploitation utilisé, le fichier de sauvegarde sera stocké dans :

- **Windows 7, 8 ou 10**
  \Users\(nomd'utilisateur)\AppData\Roaming\AppleComputer\MobileSync\Backup\
- **MacOS**
  ~/Bibliothèque/Application Support/MobileSync/Backup/

Dans les deux cas, les dossiers, AppData et Bibliothèque, sont cachés. Il est essentiel d'activer l'affichage des dossiers et fichiers cachés.

Figure 10 : Emplacement des sauvegardes



4.1.1 La sauvegarde d'iTunes

La sauvegarde créée par iTunes comprend les données de l'utilisateur tels que la photothèque, les contacts, les messages, les mails, le calendrier, les notes, les enregistrements vocaux ainsi que les réglages de l'appareil. Toutefois, les données suivantes ne sont pas sauvegardées :

- Les téléchargements effectués depuis l'iTunes Store, l'App Store et l'iBooks (il est possible de télécharger à nouveau depuis ces applications)
- Les vidéos, les livres et les photos synchronisés depuis iTunes
- La photothèque iCloud ou « Mon flux de photos »[4] s'ils sont présents sur iCloud
- Les informations relatives à l'Apple Pay[5]
- Les données concernant les applications Santé et Activité (pour les enregistrer, il est nécessaire de chiffrer la sauvegarde)
- Les réglages du Touch ID
- Les données liées au trousseau[6] (pour les enregistrer, il est nécessaire de chiffrer la sauvegarde)

4.2 Par l'intermédiaire d'iCloud

Apple offre à ses utilisateurs 5 Go de stockages sur son service de « cloud computing ». Pour profiter de ce service, il faut nous rendre dans les réglages de l'appareil et dans les paramètres d'iCloud, il est nécessaire d'insérer l'identifiant. Dès que la connexion est effectuée, la photothèque, les documents, les messages, etc. seront transférés automatiquement lorsque le dispositif est connecté à un réseau Wifi. Par ailleurs, iCloud réalise un « backup » complet de l'appareil.

---

[4] Transfère automatiquement les photos et les vidéos aux dispositifs connectés avec le même Apple ID

[5] Service de paiement développé par Apple

[6] Contient des identifiants et des mots de passe des sites Internet, des cartes bancaires et des réseaux Wi-Fi

4.2.1 La sauvegarde iCloud

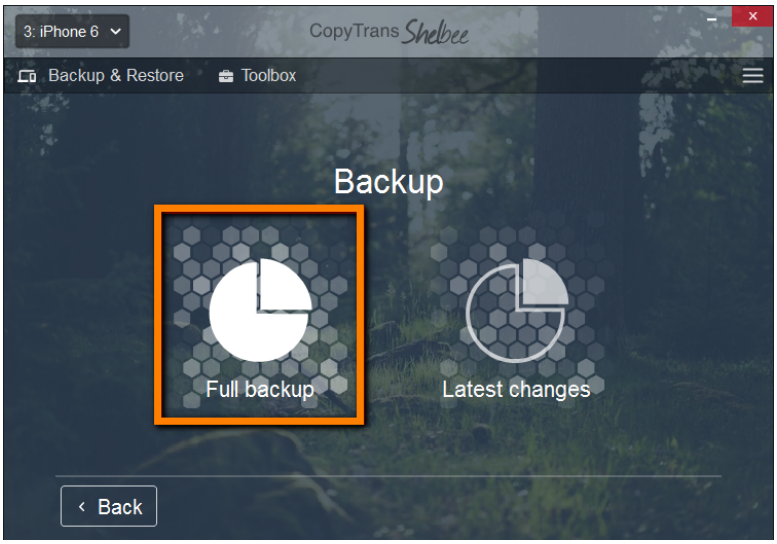
La sauvegarde effectuée par iCloud comprend l'ensemble des données hormis celles déjà enregistrées automatiquement via iCloud. Elle stocke également les réglages du dispositif iOS. Néanmoins, elle n'intègre pas :

- Les informations relatives à Apple Pay
- Les réglages du Touch ID
- Les contenus issus des différents stores d'Apple (App Store, iTunes store et iBooks)
- Les données enregistrées via d'autres services comme Gmail ou Exchange

4.3 Par l'intermédiaire d'une application tierce

Il existe des outils tiers tels que CopyTrans, MobileTrans et beaucoup d'autres pour sauvegarder ou récupérer certaines données. Ces alternatives à iTunes et à iCloud apportent de la simplicité dans la gestion des contenus si nous ne souhaitons pas utiliser le logiciel d'Apple.

Figure 11 : Sauvegarder depuis CopyTrans



(https://www.copytrans.net/support/how-to-backup-and-restore-iphone-without-itunes/)

5. Récupération des données

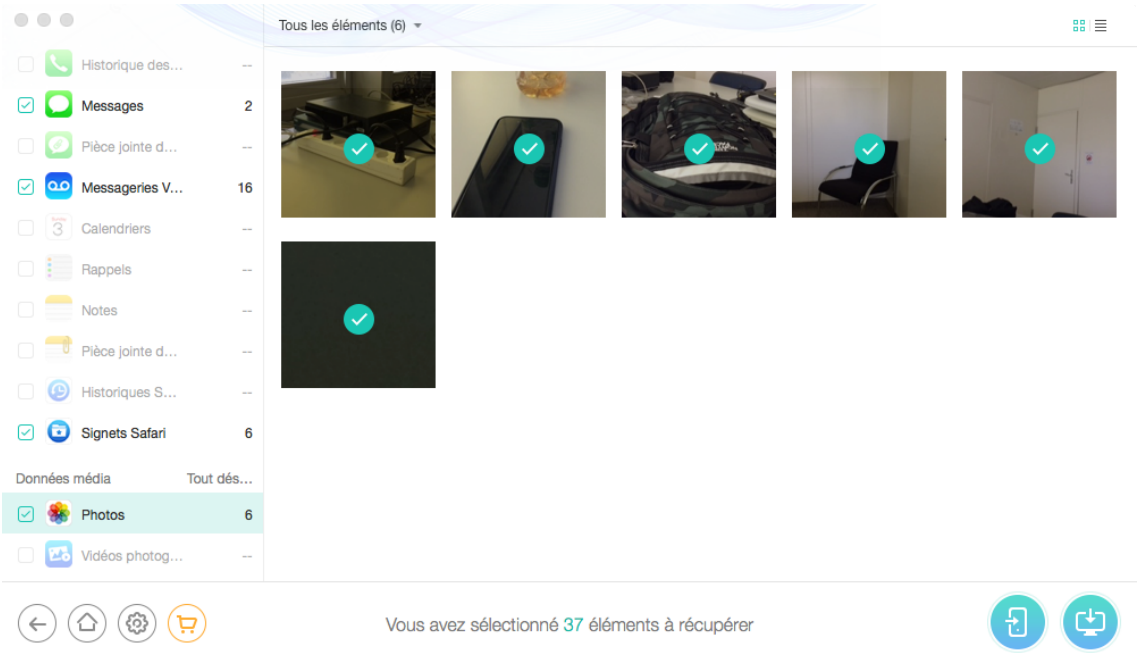
Il existe plusieurs façons de récupérer des données à partir d'iOS. Cependant, nous pouvons rencontrer certaines difficultés comme un smartphone verrouillé par un mot de passe, une sauvegarde cryptée, écran fissuré…

5.1 Depuis l'appareil

Si le dispositif ne dispose pas de code de verrouillage ou si le certificat « lockdown » est connu (traité dans le chapitre 6), il est possible de récupérer très facilement des données. En effet, il suffit de brancher l'iDevice à l'ordinateur et lancer un logiciel tiers comme iFunBox, iExplorer ou PhoneRescue afin de récupérer manuellement les données. Ces logiciels fonctionnent avec la bibliothèque iTunes, il faut au préalable installer celui-ci.

L'exemple ci-dessous est réalisé avec le logiciel PhoneRescue. A gauche de la fenêtre, les différentes applications affichent le nombre de fichiers disponible sur l'appareil. Ensuite, il faut sélcetionner les données à extraire et, pour finir, les télécharger en cliquant sur le bouton en bas à droite de la fenêtre.

Figure 12 : Logiciel PhoneRescue

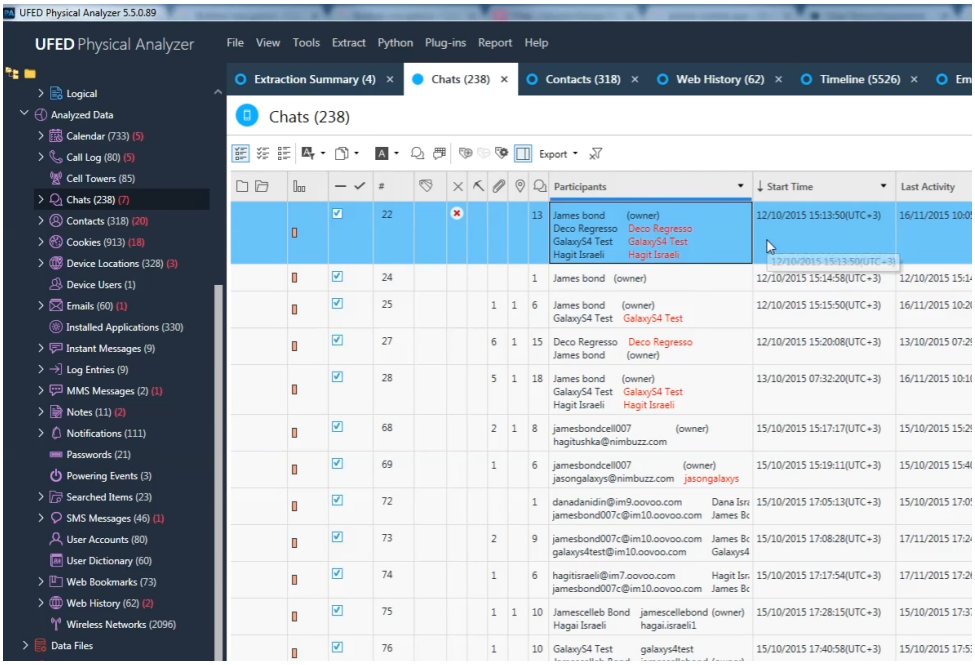


5.2 Logiciel professionnel

Pendant une enquête, certains dispositifs peuvent être utiles pour récolter des preuves. Ce qui complique la tâche des enquêteurs est le verrouillage de l'appareil par un mot de passe ou si la sauvegarde est chiffrée. De ce fait, des entreprises comme Oxygen Forensic, XRY et Cellebrite se sont spécialisées dans ce domaine. Toutefois, ces logiciels sont payants, mais ils offrent des fonctionnalités avancées.

La firme israélienne, Cellebrite, a contribué au déverrouillage de l'iPhone du terroriste de San Bernardino aux Etats-Unis. Dans la figure suivante, nous découvrons une extraction d'un appareil effectué à l'aide d'un des logiciels de l'entreprise.

Figure 13 : UFED Physical Analyzer



(https://www.cyberscoop.com/cellebrite-iphone-6-ufed-samsung-galaxy-facebook-messenger-snapchat/)

5.3 Acquisition physique

L'acquisition physique consiste à faire une copie du périphérique iOS bit par bit et de ce fait, il est possible d'extraire presque toutes les données. Les dispositifs utilisent deux types de mémoire : volatile (RAM) et non volatile (NAND). La première est utilisée par le système d'exploitation ainsi que par des applications. Nous y trouvons des mots de passe, des clés de cryptage, des logins, etc. Il est important d'extraire cette mémoire avant que l'appareil ne soit redémarré, car sinon tout est perdu. En ce qui concerne la NAND, les données sont stockées même si un redémarrage a lieu et, ainsi, des informations importantes peuvent être récupérées.

Cependant, ce procédé nécessite le démontage de l'appareil pour récupérer les deux mémoires. Ensuite, elles sont branchées à un appareil spécial capable d'effectuer une copie minutieuse. Une pratique concernant cette acquistion ne sera pas réalisée dans le cadre de ce travail.

5.3.1 Custom RAM

Une autre méthode plus complexe consiste à modifier la RAM en contournant certaines sécurités de l'appareil. Pour ce faire, il est nécessaire d'installer une RAM personnalisée par l'intermédiaire du mode DFU. Ce mode, Firmware Upagrde Device, permet de mettre à jour l'appareil et est utile pour les diagnostics. Des logiciels de « jailbreak » ont notamment utilisé ce moyen pour avoir accès aux données.

5.4 Via Jailbreak

Cette technique a pour but de supprimer les restrictions imposées par Apple et ainsi étendre les fonctionnalités d'iOS. En utilisant ce moyen, l'utilisateur a accès à toutes les partitions notamment à la racine des fichiers de l'appareil. Dès lors, nous pouvons installer des outils tels que SSH et Terminal par l'intermédiaire de Cydia[7] qui n'est pas proposé par Apple. La dernière version encore exploitable par le « jailbreak » est l'iOS 9.3.3.

Figure 14 : Logiciel Pangu

Pour procéder au déplombage de l'appareil, le logiciel Pangu doit être exécuté et l'appareil connecté à l'aide de la connexion USB. Ensuite, il suffit de suivre les procédures affichées dans la fenêtre du logiciel et attendre que le processus soit terminé. Si le processus s'est achevé correctement, Cydia sera installé sur l'écran d'accueil.

[7] Application non officielle pour iOS qui a été conçue par Jay Ryan Freeman. Permet d'installer des applications non certifiées par Apple

Dès lors, nous pouvons extraire une image du périphérique qui sera ensuite analysée par un logiciel. Pour cela, l'installation du protocole SSH est nécessaire sur l'appareil en question. Après, deux choix s'offrent à nous, soit on utilise le terminal disponible sur les ordinateurs soit nous l'installons sur l'iDevice. Dans cet exemple, nous effectuerons l'installation. Ensuite, nous tapons cette commande :

dd if=/dev/rdisk0 bs=4096 | ssh -C username@computer_IP 'dd of=iphone.img'

L'« username » est remplacé par le nom d'utilisateur de l'ordinateur et « computer_IP » par l'adresse IP de l'ordinateur. La copie de l'image est transférée dès que le processus est terminé, tout dépend de la taille de stockage, et nous obtiendrons un fichier .img (voir figure 15).

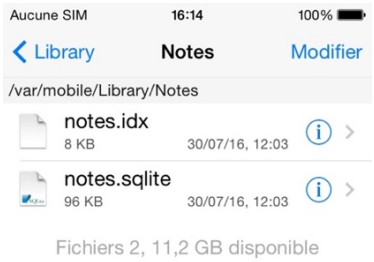
Figure 15 : Copies au format .img

Le logiciel tel qu'Elcomsoft iOS Forensic Toolkit permet l'analyse de l'image et ainsi récupérer les données.

5.4.1 iFile

iFile est un tweak[8] disponible sur Cydia qui permet d'accéder aux fichiers dans les entrailles de l'appareil. De cette façon, nous pouvons nous rendre dans les chemins contenant les bases de données SQLlite, les fichiers plist… Par exemple, dans la prochain figure, l'emplacement indiqué est l'endroit où sont stockées les notes.

Figure 16 : iFile



[8] Application téléchargeable depuis Cydia

5.5 Depuis une sauvegarde iOS

Comme cité précédemment, les sauvegardes sont stockées sur l'ordinateur ou sur le cloud d'Apple. A partir de ces sauvegardes, nous pouvons récupérer des données en restaurant l'iPhone ou en les extrayant à l'aide de logiciel.

5.5.1 Restauration d'un dispositif iOS

5.5.1.1 Depuis iTunes

Nous devons ouvrir iTunes, brancher l'appareil à l'ordinateur et sélectionner « Restaurer la sauvegarde… ». A ce moment, iTunes proposera la sauvegarde la plus récente. A la fin de l'opération, il se peut qu'un mot de passe soit demandé si la sauvegarde est chiffrée. Si nous ne le possédons pas, certains logiciels permettent de décrypter le mot de passe.

5.5.1.2 Depuis iCloud

Nous pouvons effectuer l'opération par l'intermédiaire du périphérique iOS ou par iTunes. Pour ce dernier, le procédé est identique au précédent.

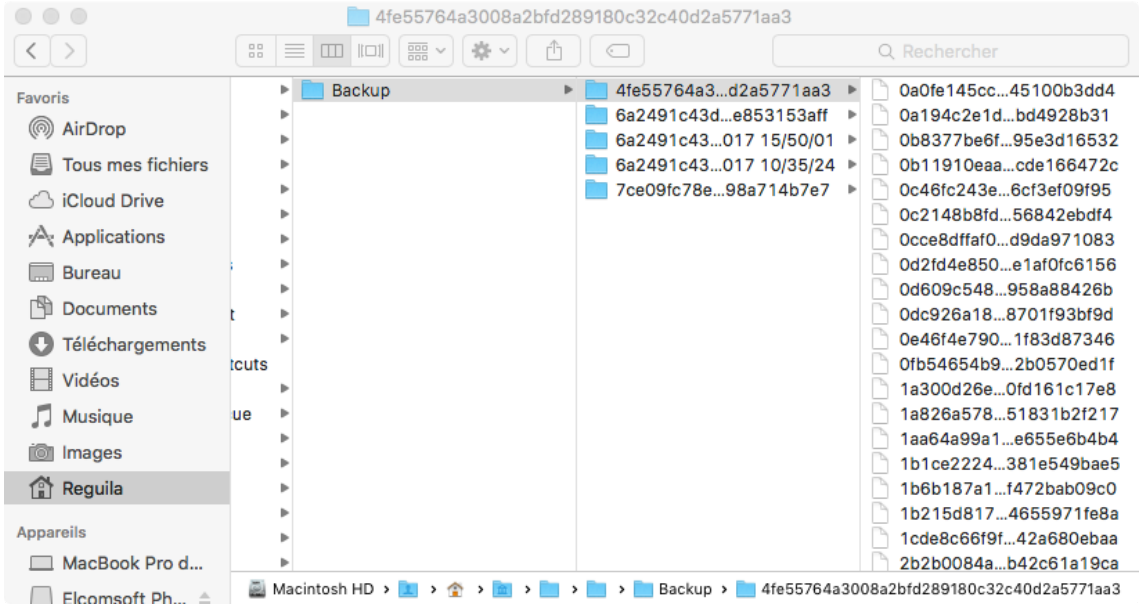
Par contre, il faut effacer le contenu de l'appareil pour restaurer depuis iTunes. Pour cela, nous devons nous rendre dans les réglages du dispositif iOS et dans les paramètres généraux, une option pour réinitialiser est disponible. Le processus peut prendre quelques minutes avant que celui-ci ne redémarre l'appareil. Ensuite, il y a la possibilité de restaurer le dispositif à partir d'iCloud. Un identifiant Apple est demandé, il suffit alors de le rentrer. Si ce dernier n'est pas connu, une méthode de connexion par l'intermédiaire d'un jeton d'authentification est réalisable.

5.5.2 Applications tierces

Les sauvegardes enregistrées sur l'ordinateur sont lisibles à l'aide de logiciel comme iPhoneAnalyzer, iBackupViewer, iBackupbot… En effet, le fichier de sauvegarde est composé de plusieurs fichiers représentés par des chiffres et des lettres. Ces 40 caractères dans le titre représentent la valeur d'hachage SHA1 du chemin.

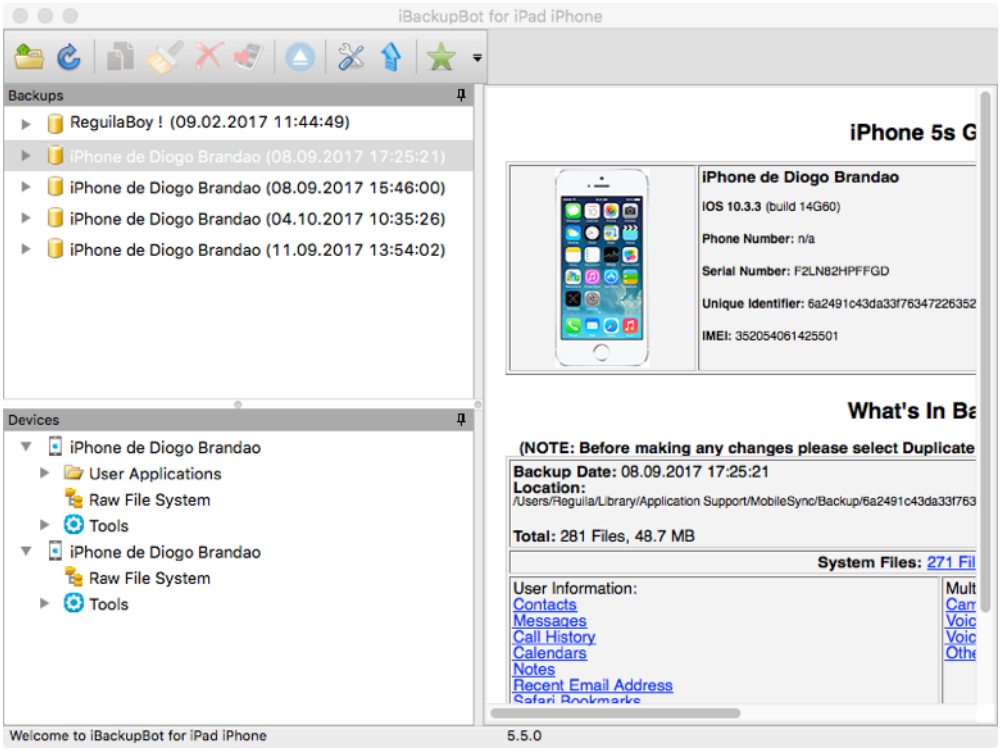
Dans le dossier Backup, se trouve les différentes sauvegardes des appareils réalisés sur l'ordinateur.

Figure 17 : Les sauvegardes



Lors de l'ouverture d'une de ces sauvegardes à l'aide des logiciels adéquats, ils proposent en premier lieu les sauvegardes disponibles sur l'ordinateur.

Figure 18 : iBackupBot



Nous choisissons la sauvegarde qui nous intéresse et ensuite, l'accès aux différentes données est possible et l'extraction également.

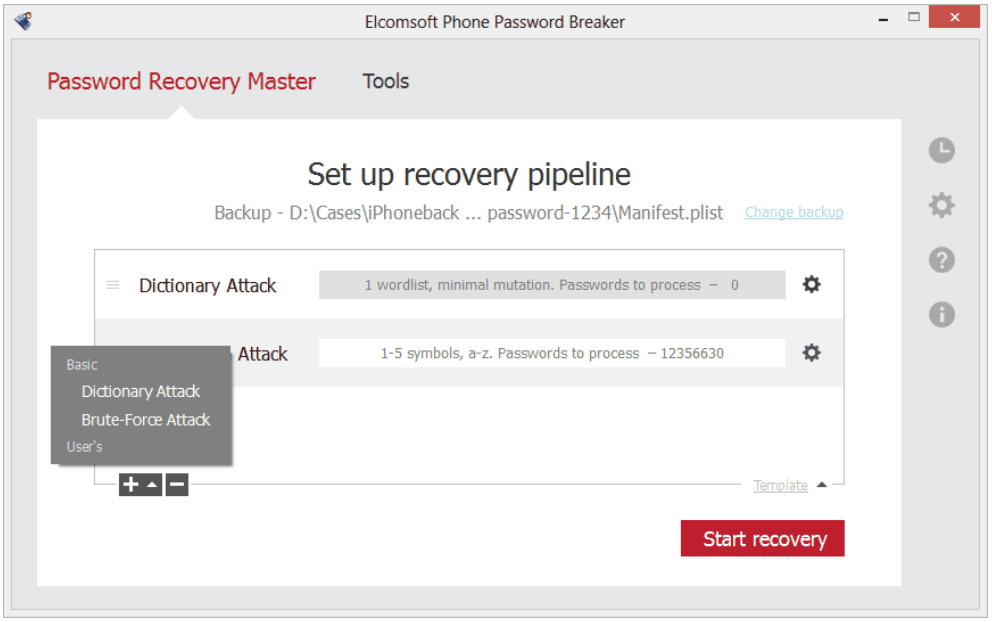
Figure 19 : iBackupBot

5.5.3 Sauvegarde cryptée

iTunes propose de chiffrer les backups afin d'offrir plus de sécurité. Par contre, cela rend la tâche plus complexe pour accéder aux informations. Dès lors, il faut connaître le mot de passe pour déchiffrer la sauvegarde. Toutefois, des logiciels sont capables de déchiffrer le mot de passe.

Par exemple, Elcomsoft Phone Breaker utilise l'attaque par brute-force, ce type d'attaque consiste à tester plusieurs combinaisons ainsi qu'une liste des mots de passe les plus utilisés. Le temps nécessaire pour découvrir le mot de passe dépend de la complexité de celui-ci.

Figure 20 : Décryptage d'une sauvegarde



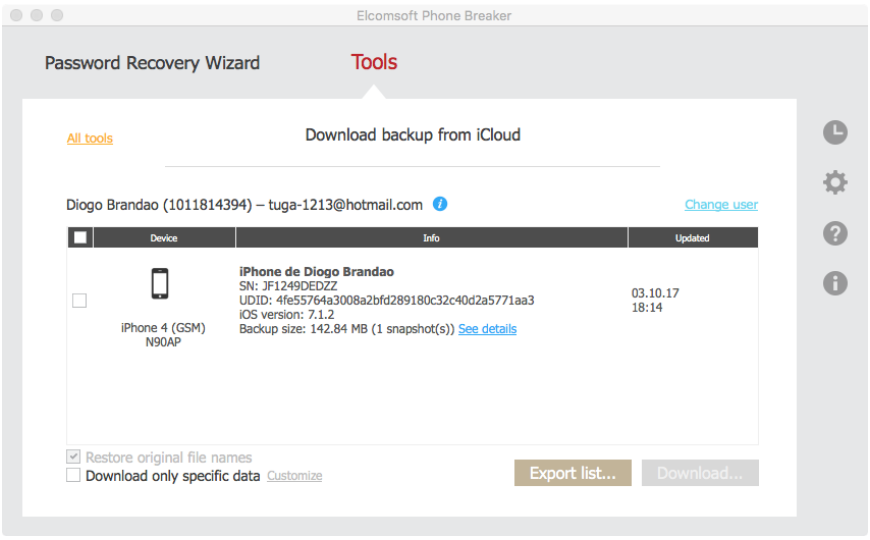
Etant donné qu'il s'agit d'un logiciel commercial, nous ne connaissons pas entièrement le mot de passe trouvé.

5.5.4 iCloud

En utilisant le logiciel Elcomsoft Phone Breaker, nous pouvons extraire ou télécharger des fichiers spécifiques. Il suffit de lancer le logiciel et de sélectionner « Download from iCloud », nous devons connaître au préalable l'Apple ID. Dès la connexion établie, les sauvegardes disponibles sont affichées.

Pour finir, il suffit de sélectionner la sauvegarde désirée et la télécharger.

Figure 21 : Sauvegarde iCloud

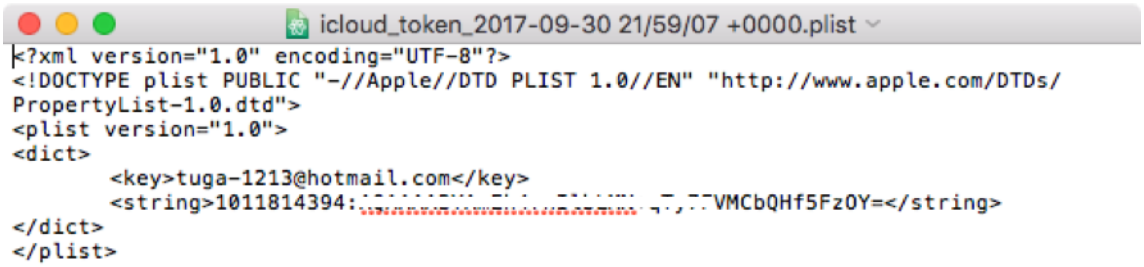


Si nous ne possédons pas l'Apple ID, nous pouvons nous connecter à l'aide d'un jeton d'authentification (authentication token). Ce jeton est un fichier généré lors d'une connexion avec iCloud, il permet à l'utilisateur d'être connecté afin que la synchronisation se fasse automatiquement. De ce fait, il est possible de le récupérer sur l'ordinateur de la personne qui s'est connecté à iCloud.

5.5.4.1 Sur MacOs

L'entreprise Elcomsoft propose l'outil Elcomsoft Token Extractor pour les utilisateurs de MacOS. Simple d'utilisation, le logiciel recherche une authentification et extrait un fichier plist. Par défaut, le fichier est enregistré dans */Users/(nom d'utilisateur)/* et nous l'ouvrons avec un simple éditeur de texte. Le fichier contient l'Apple ID et le jeton d'authentification.

Figure 22 : Code XML d'un jeton d'authentification



A l'aide du programme Elcomsoft Phone Breaker et du jeton, la connexion à iCloud peut être établie en suivant les étapes de la section 5.5.4.

5.5.4.2 Sur Windows

Elcomsoft Phone Braker offre la possibilité d'extraire le jeton sur Windows par l'outil de ligne de commande, atex.exe. Cet outil recherche dans l'ordinateur une authentification et crée un fichier texte dans lequel sont contenus l'Apple ID et le jeton d'authentification. Le fichier est enregistré dans le dossier du logiciel.

6. Récupération d'une sauvegarde

Depuis l'arrivée de l'iPhone 4s, Apple a augmenté la sécurité d'iOS. Dans les récentes versions, il est difficile de contourner les différentes couches de protection notamment lorsque l'appareil est verrouillé. Des méthodes pour déverrouiller les dispositifs d'Apple existent. C'est le cas de l'IP-Box qui utilise un script python afin d'effectuer une attaque brute-force. Toutefois, plus le code de déverrouillage est complexe et plus il sera difficile de l'obtenir. De plus, si plusieurs tentatives échouent, l'appareil est bloqué par Apple.

La technique, que nous étudierons, consiste à récupérer une sauvegarde malgré un verrouillage du dispositif grâce à l'appairage avec un poste de travail. Premièrement, il faut être certains que l'appareil n'a pas été redémarré ou éteint après l'appairage sinon la technique est compromise. Après, il faut récupérer un fichier contenu dans le dossier « lockdown » pour l'utiliser sur un poste de travail différent. Finalement, la sauvegarde de l'appareil sera possible.

Tout d'abord, il est essentiel de comprendre le fonctionnement d'un fichier « lockdown ». Lorsqu'un utilisateur branche son dispositif à un ordinateur muni d'iTunes, une relation d'appariement est établie entre les deux périphériques ce qui permet la synchronisation des données. Au moment de ce jumelage, les deux appareils échangent des clés cryptographiques ainsi, l'ordinateur bénéficie d'un accès au dispositif iOS quoiqu'il soit verrouillé.

Pour ce faire, l'appareil doit être débloqué par le code d'accès ou l'empreinte digitale (Touch ID) et nous devons autoriser l'accès « Se fier » à l'appareil et sur l'ordinateur comme suit :

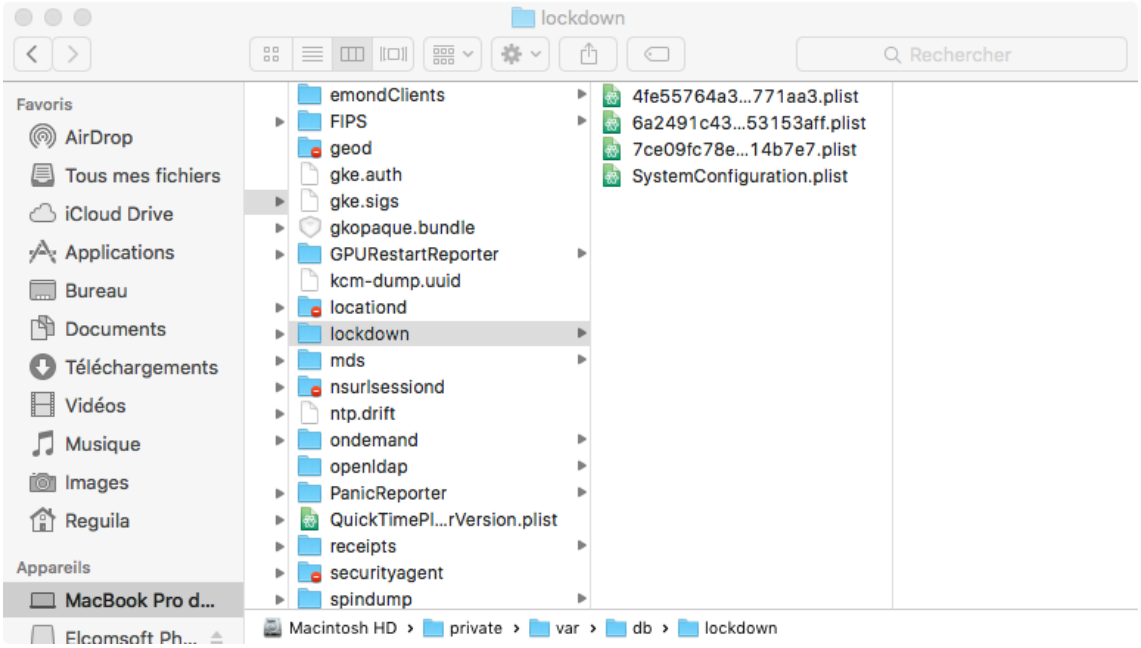
Figure 23 : Autorisation d'accès

A cet instant, un enregistrement « lockdown » est créé avec les clés cryptographiques. Ce fichier est stocké aux emplacements suivants :

- **MacOs :**
  /var/db/lockdown/
- **Windows**
  C: \ProgramData\Apple\Lockdown

Dans ces dossiers, nous trouvons des fichiers plist qui correspondent aux appareils jumelés. Leurs noms représentent les identifiants UDID (Unique Device Identifier).

Figure 24 : Emplacement des fichiers "lockdown"



En récupérant le fichier de l'appareil désiré, il est possible de le copier sur un autre PC et de l'enregistrer dans le même dossier. Le logiciel d'Apple, iTunes, reconnaîtra le dispositif et la sauvegarde peut être effectuée. Pour finir, il suffira de suivre les étapes du chapitre 5.

Nous devrons prendre en compte plusieurs détails. D'une part, le périphérique iOS nécessite d'être sous tension et qu'aucun redémarrage n'a eu lieu, car depuis la version 8 d'iOS, le fichier « lockdown » est modifié à chaque démarrage. Donc, il est essentiel que l'appareil reste allumé pour tenter une extraction de données avec le fichier.

Par contre, si l'appareil n'a pas été déverrouillé une seule fois, il sera difficile d'effectuer une sauvegarde en effectuant ces étapes.

7. Les répertoires intéressants

Il est important de comprendre comment les données de notre téléphone sont stockées. La plupart des données de l'utilisateur sont stockées dans :

/private/var/mobile/ ou /User/

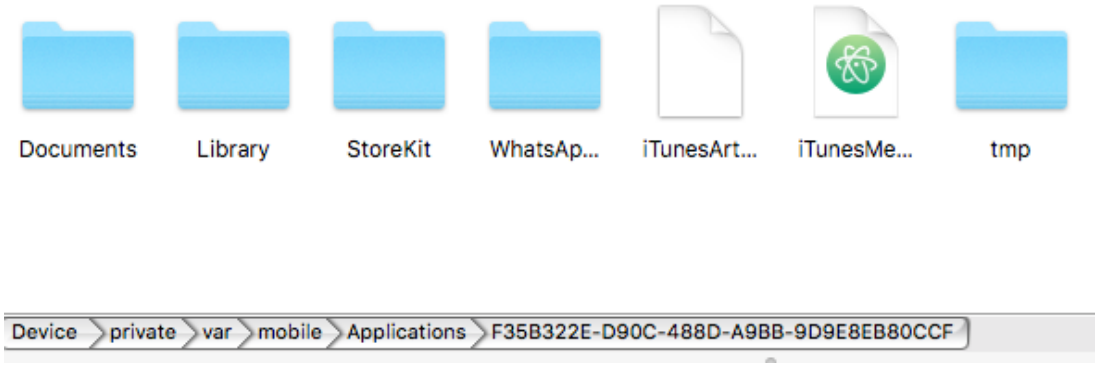
7.1 Chemin des applications

Les applications installées sur les appareils iOS se trouvent dans le répertoire suivant :

/private/var/mobile/Application ou /User/Application/

Les applications sont représentées par leur UDID et des sous-dossiers y sont présents comme :

Figure 25 : Chemin d'accès à WhatsApp



/AppName.app/ est le package de l'application.

/Documents/ contient des données relatives à l'application.

/Library/ contient des fichiers spécifiques à l'application.

/tmp/ permet de stocker les fichiers temporaires.

Une liste avec les applications installées est disponible dans */private/var/mobile/Library/Caches/com.apple.mobile.installation.plist*. Elle indique également le chemin pour parvenir à leur dossier.

7.2 Fichiers de configurations

Voici une liste de fichiers de configurations qui sont intéressantes pour une analyse profonde :

/private/var/root/Library/Lockdown/data_ark.plist - Ce fichier comporte des informations de l'appareil ainsi que le compte utilisé.

private/var/mobile/Library/Accounts/Accounts3.sqlite – Ici, nous avons une base de données SQL dans laquelle toutes les informations du compte sont stockées.

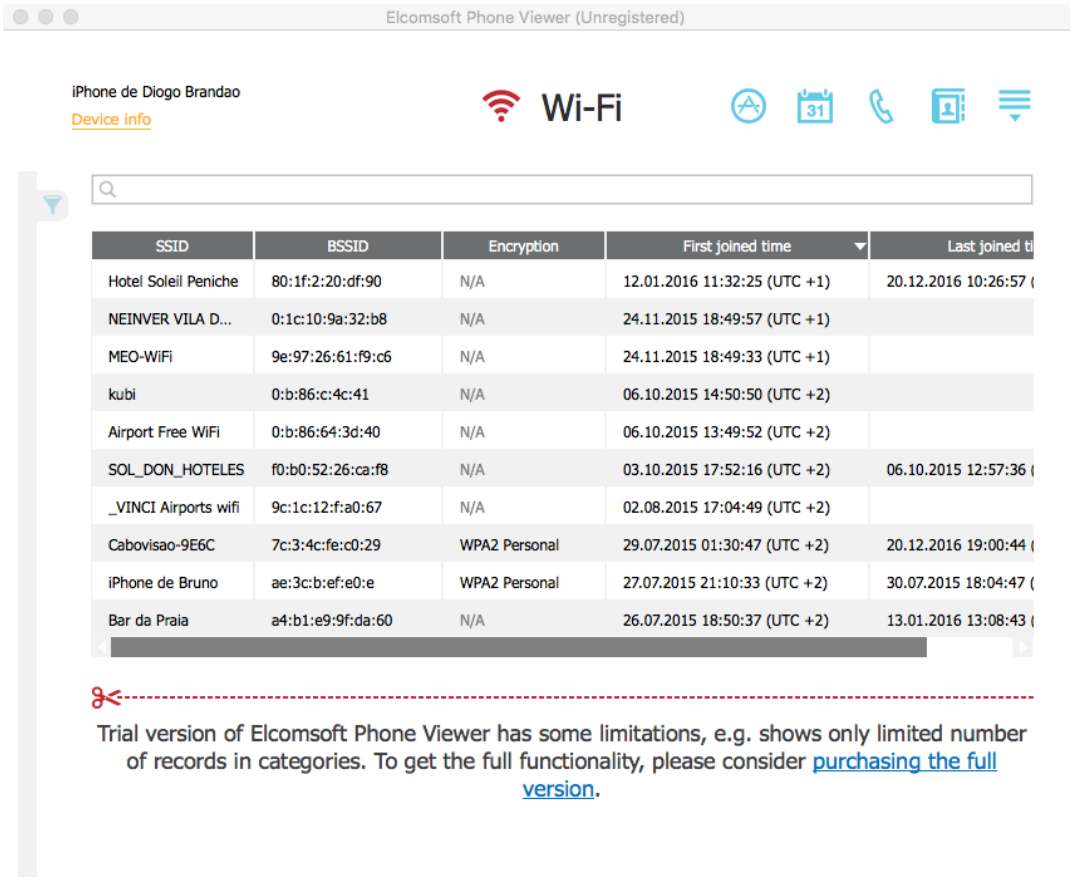
/private/var/mobile/Library/DataAccess/AccountInformation.plist - Ce fichier contient toutes les informations concernant le compte Apple utilisé pour paramétrer les applications.

path/private/var/root/Library/Lockdown/Pair_records/ - Lors du jumelage avec un ordinateur, un fichier plist est enregistré dans ce dossier afin de connaître les postes de travail autorisés à communiquer avec le dispositif.

/private/var/wireless/Library/Preferences/com.apple.commcenter.plist – Toutes les informations concernant la carte SIM (Suscriber Identify Module) sont disponibles dans ce fichier plist. L'ICCID est le numéro de la carte et l'IMSI qui est un numéro attribué par l'opérateur afin d'identifier l'utilisateur.

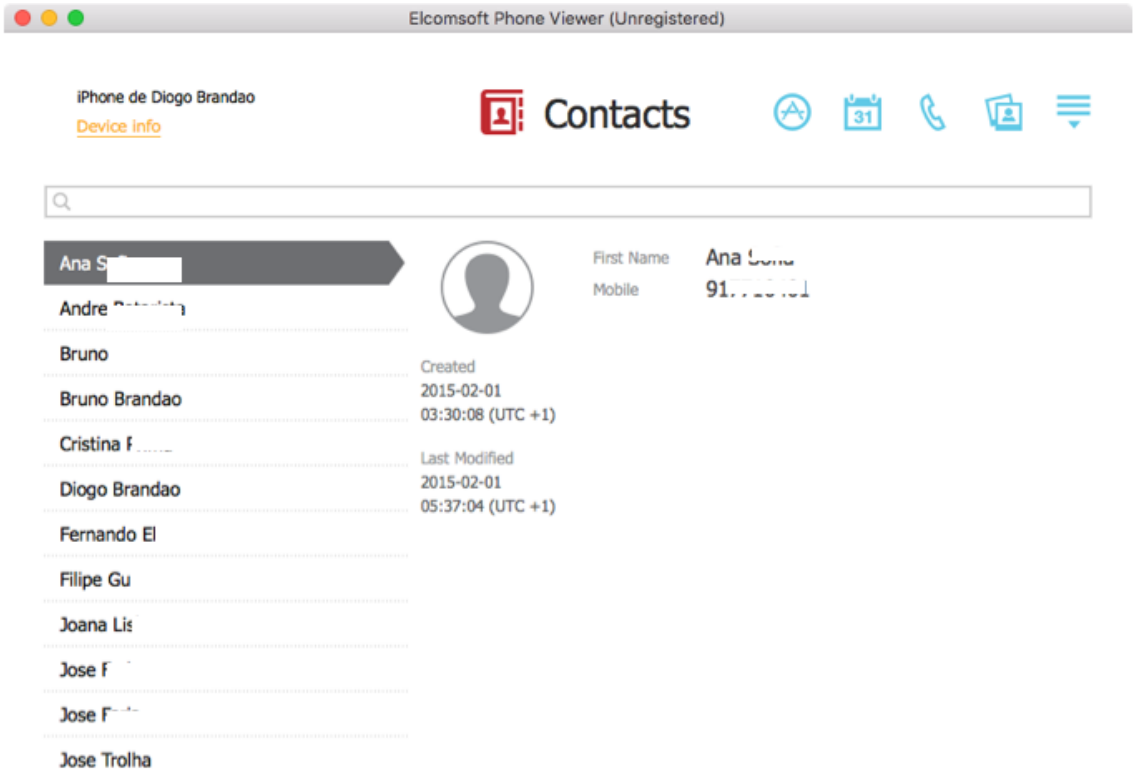
/private/var/preferences/ SystemConfiguration/com.apple.wifi.plist – Les réseaux Wi-Fi auxquels nous nous sommes connectés ainsi que la date et l'heure de notre dernière connexion sont enregistrés dans ce fichier.

Figure 26 : Les réseaux Wi-Fi enregistrés



/private/var/mobile/library/AddressBook/ - Dans ce dossier, nous avons plusieurs fichiers concernant les contacts. Notamment les deux bases de données : AddressBook.sqlitedb et AddressBookImages.sqlitedb. Dans la première, il y a les informations du contact et dans la deuxième, les photos de ces derniers.

Figure 27 : Contacts enregistrés



/private/var/mobile/Media/Recordings/ – Les enregistrements, effectués par l'application dictaphone, sont enregistrés dans ce dossier.

/private/var/mobile/Library/Calendar/Calendar.sqlitedb – Cette base de données possède l'intégralité des évènements ajoutés sur le Calendrier du dispositif iOS.

/private/var/wireless/Library/CallHistory/Call_History.db – L'historique des appels se situe dans cette base de données.

/private/var/mobile/Library/Mail/ – Chaque compte mail possède son propre dossier accompagné des e-mails ainsi que les pièces jointes.

/private/var/mobile/Media/ - Cet emplacement renferme toute la photothèque de l'utilisateur. Dans le dossier DCIM, se trouvent les photos et les vidéos prises à l'aide de l'appareil photo ou télécharger par l'intermédiaire des applications.

Dans PhotoData, il y a les albums synchronisés par iCloud ou l'ordinateur et en sous-dossier, nous avons les vignettes des images enregistrées dans le dossier Thumbnails. Quant aux métadonnées, elles sont ajoutées dans le fichier Photos.sqlite.

/private/var/mobile/Library/Preferences/com.apple.Maps.plist – Les dernières recherches faites dans l'application de géolocalisation d'Apple sont inscrites dans ce fichier. Ainsi que la longitude et la latitude des lieux. Tandis que dans le dossier principal de Maps, qui se situe dans */private/Library/Maps*, nous avons les endroits enregistrés et toutes les recherches.

/private/var/mobile/Library/Notes/notes.sqlite – Toutes les notes inscrites dans l'appareil se retrouvent dans ce fichier SQLite.

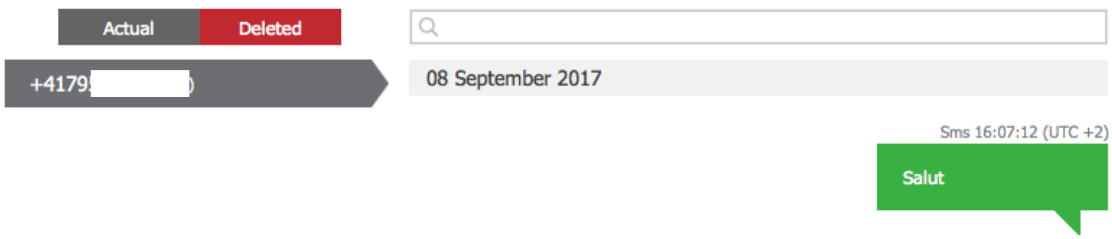
/private/var/mobile/Library/Safari/ et */private/var/mobile/Library/* - Ces deux destinations sont essentielles au stockage pour l'application Safari. En se rendant dans */Library/Safari/Bookmarks.db*, il y a une base de données contenant les signets.

L'historique du navigateur est disponible dans un fichier plist disponible en se rendant dans *Library/Safari/History.plist*. Cependant, lorsque l'utilisateur supprime l'historique, tout est perdu. Par contre, l'historique des recherches reste intact dans *Library/Preferences/com.apple.mobilesafari.plist*.

Dans */Library/Cookies/Cookies.binarycookies,* les cookies y sont stockés. Alors que dans *Library/Caches/Safari/Recentsearches.plist* se trouve les dernières recherches. Et les différents téléchargements réalisés depuis Safari se retrouvent dans *Library/Caches/com.apple.mobilesafari/Cache.db*.

/private/var/mobile/Library/SMS/sms.db – L'emplacement des SMS, MMS et iMessages reçus et envoyés depuis l'appareil. Les pièces jointes sont enregistrées dans le dossier */Library/SMS/Attachments/.*

Figure 28 : SMS supprimé



/private/var/mobile/Library/Voicemail/ - Contient les fichiers audio ainsi que la base de données voicemail.db contenant les informations des messages vocaux.

/private/var/mobile/Library/caches/com.apple.UIKit.pboard – Le presse-papiers contient des données comme des mots de passe, les copier/couper/coller, ou d'autres textes.

/private/var/root/Library/Caches/locations/consolidated.db – Les localisations liées à chaque point d'accès Wi-Fi et aux antennes téléphoniques sont inscrites dans cette base de données. Les appareils plus récents ont une deuxième base de données dans laquelle est enregistré la localisation des Access-points Wi-Fi.

Quatre points de géolocalisation extraits avec le logiciel iPhone Backup Extractor et transcris au format CSV (comma-seperated values) :

Figure 29 : Localisation GPS

	A
1	Timestamp,"Latitude","Longitude","Source"
2	2016-12-22 13:20:48,46.2570762634277,6.11032247543335,WhatsApp
3	2016-12-31 22:08:48,53.3514747619629,-6.2548394203186,WhatsApp
4	2013-02-01 18:20:17,7.477355,80.62378,Photos
5	2013-02-01 18:20:17,7.477355,80.62378,Photos
6	

Par exemple, la deuxième coordonnée pointe sur une rue à Dublin.

Figure 30 : Google Maps

<Application_Home>/Library/Preferences/com.facebook.plist – Les informations concernant le compte d'utilisateur se trouvent dans ce dossier, tels que la date de la dernière connexion et l'e-mail lié au compte Facebook. Les amis dans Facebook sont eux dans *<Application_Home>/Library/Caches/FbStore.db*.

8. Logiciels

Tout au long de ce travail, plusieurs logiciels ont été utilisés et quelques-uns ont été utiles au développement de ce projet.

Le tableau ci-dessous contient les logiciels ainsi qu'une petite description et les prix respectifs.

Tableau 5 : Tableau des logiciels utilisés

Nom	**Description**	**Prix**
iTunes	Gestionnaire de bibliothèque multimédia développé par Apple	Gratuit
CopyTrans	Transfert de données	Essai gratuit
MobileTrans	Transfert de données	Visualisation gratuite
iFunBox	Parcourir et transfert de données	Gratuit
iExplorer	Parcourir et transfert de données	Visualisation gratuite Extraction limitée
PhoneRescue	Outil de récupération des données	Visualisation gratuite Extraction limitée
Elcomsoft Token Extractor	Extraction du jeton d'authentification	Gratuit
Elcomsoft Phone Viewer	Outil de récupération des données, messages supprimés visibles	Visualisation gratuite Extraction payante

Nom	Description	Prix
iPhone Backup Extractor	Outil de récupération des données	Visualisation gratuite Extraction limitée
iBackupBoot	Visualisation d'une sauvegarde et extraction	Gratuit
iBackup Viewer	Visualisation d'une sauvegarde et extraction	Gratuit
Elcomsoft Phone Breaker	Plusieurs fonctions telles que le déchiffrage d'une sauvegarde cryptée, connexion à iCloud avec un jeton d'authentification, récupération des sauvegardes, etc.	Certaines fonctions sont gratuites
Pangu	Jailbreak les dispositifs iOS jusqu'à la version 9.3.3	Gratuit

9. Tableau récapitulatif des logiciels

Tableau 6 : Tableau récapitulatif des logiciels

Nom	Visualisation depuis l'appareil	Visualisation depuis une sauvegarde	Extraction	Sauvegarde	Déchiffrage	Récupération du jeton d'authentification
iTunes	✗	✗	✗	✓	✗	✗
CopyTrans	✓	✓	✓	✓	✗	✗
MobileTrans	✓	✗	✓	✓	✗	✗
iFunBox	✓	✗	✓	✗	✗	✗
iExplorer	✓	✓	✓	✓	✗	✗
PhoneRescue	✓	✓	✓	✗	✗	✗
Elcomsoft Token Extractor	✗	✗	✗	✗	✗	✓
Elcomsoft Phone Viewer	✗	✓	✓	✗	✗	✗
Elcomsoft Phone Breaker	✗	✗	✓	✗	✓	✗
iBackupBot / iBackup Viewer	✗	✓	✓	✗	✗	✗

10. Conclusion

Les moyens pour effectuer une récupération des données sont variés. Toutefois, certaines techniques nécessitent du matériel spécial pour déverrouiller l'appareil ou faire des modifications dans le hardware. Par ailleurs, des logiciels existent afin qu'une sauvegarde soit lisible pour extraire des données spécifiques. La plupart d'entre eux sont payants, mais ils offrent la possibilité de visualiser et d'extraire une partie des informations.

Nos appareils multimédias sont une source importante de données. En effet, ces dernières peuvent être volées par des gens malhonnêtes ou utilisées pendant une enquête judiciaire. Les appareils d'Apple ont une sécurité très élevée, mais il existe souvent des moyens de les contourner. Certaines personnes sont spécialisées dans la découverte des failles et ces dernières peuvent être vendues à des escrocs. C'est pourquoi, il est essentiel de mettre un code de verrouillage dans chaque dispositif ainsi que dans les sauvegardes enregistrées sur les ordinateurs. D'autres entreprises utilisent les failles pour aider les enquêteurs à trouver des preuves.

Ce travail a été très passionnant et enrichissant pour moi, car auparavant, j'ai rencontré des problèmes avec mes données et je n'ai pas réussi à les retrouver. En effectuant ces techniques, j'aurais pu les récupérer. Dorénavant, j'effectuerai une sauvegarde de l'appareil à l'aide des différents logiciels et si une mésaventure survient, j'utiliserai un logiciel de récupération.

La plus grande difficulté que j'ai rencontrée fut le manque de renseignement en français. En effet, le sujet est souvent traité en anglais dans des livres ou des sites. Mon anglais n'étant pas ma langue maternelle, il a été difficile pour moi de comprendre certains processus.

Finalement, je suis satisfait de ce que j'ai accompli malgré mes difficultés en anglais et j'espère, ainsi, apporter des explications claires à ce sujet.

Bibliographie

Elsa Bembaron, 2013. Le Figaro, Le marché des PC s'effondre face aux smartphones et aux tablettes. [Consulté le 26 juillet 2017] Disponible à l'adresse :

http://www.lefigaro.fr/societes/2013/04/11/20005-20130411ARTFIG00684-le-marche-des-pc-s-effondre-faceaux-smartphones-et-aux-tablettes.php

eMarketer, 2016. Mobile Phone, Smartphone Usage Varies Globally. [Consulté le 26 juillet 2017] Disponible à l'adresse :

https://www.emarketer.com/Article/Mobile-Phone-Smartphone-Usage-Varies-Globally/1014738

Krypted, 2016. Use libimobiledevice To View iOS Logs. [Consulté le 7 août 2017] Disponible à l'adresse :

http://krypted.com/mac-os-x/use-libimobiledevice-to-view-ios-logs/

Mickaël Bazoge, 2017. MacGeneration, APFS : le futur système de fichiers d'Apple qui va changer votre vie. [Consulté le 10 août 2017] Disponible à l'adresse :

https://www.macg.co/os-x/2017/01/apfs-le-futur-systeme-de-fichiers-dapple-qui-va-changer-votre-vie-94735

Wikipédia – Proprety List [Consulté le 12 août 2017] Disponible à l'adresse :

https://en.wikipedia.org/wiki/Property_list

SQLite – Format de fichier SQLite [Consulté le 12 août 2017] Disponible à l'adresse :

http://sqlite.org/fileformat2.html

Apple – Comment sauvegarder les données de votre iPhone, iPad et Ipod touch [Consulté le 13 août 2017] Disponible à l'adresse :

https://support.apple.com/fr-fr/ht203977

CopyTrans – How to back up and restore iPhone without iTunes ? [Consulté le 13 août 2017] Disponible à l'adresse :

https://www.copytrans.net/support/how-to-backup-and-restore-iphone-without-itunes/

Apple – Restaurer votre iPhone, iPad et Ipod touch à partir d'une sauvegarde [Consulté le 17 août 2017] Disponible à l'adresse :

https://support.apple.com/fr-ch/HT204184

iExplorer – iExplorer un logiciel incroyable pour bidouiller dans son iPhone ou iPad [Consulté le 23 août 2017] Disponible à l'adresse :

http://www.sosiphone.com/blogiphone/2013/02/11/iexplorer-un-logiciel-incroyable-pour-bidouiller-dans-son-iphone-ou-ipad-62452/

Vicky, 2017. iFunBox – Browse iPhone File System with Easily. [Consulté le 23 août 2017] Disponible à l'adresse :

https://www.imobie.com/support/ifunbox.htm

MacGeneration, 2017, PhoneRescue : pour ne plus perdre de données avec son iPhone. [Consulté le 25 août 2017] Disponible à l'adresse :

https://www.macg.co/publicite/2017/06/phonerescue-pour-ne-plus-perdre-de-donnees-avec-son-iphone-partenaire-98896

Patrick Howell O'Neil, 2017. Cellebrite can now unlock iPhone 6 and 6+, also extract data from array of popular apps. [Consulté le 26 août 2017] Disponible à l'adresse :

https://www.cyberscoop.com/cellebrite-iphone-6-ufed-samsung-galaxy-facebook-messenger-snapchat/

Pratical Mobile Forensics - Heather Mahalik, Rohit Tamma, Satish Bommisetty [Consulté le 1 septembre 2017] Disponible à l'adresse :

https://books.google.ch/books?id=SNFtDQAAQBAJ&lpg=PA96&ots=I7cmVAsNNn&dq=physical acquisition ram iphone&hl=fr&pg=PP1 - v=onepage&q=physical acquisition ram iphone&f=false

Pangu – FAQ and Help [Consulté le 2 septembre 2017] Disponible à l'adresse :

http://en.9.pangu.io/

CGSecurity – Recover data from an iPhone [Consulté le 5 septembre 2017] Disponible à l'adresse :

http://www.cgsecurity.org/wiki/Recover_data_from_an_iPhone

Bohemian Boomer – How To Browse, View, Export, And Modify iTunes Backup Files with iBackupBot [Consulté le 8 septembre 2017] Disponible à l'adresse :

http://bohemianboomer.com/2013/09/how-to-browse-view-export-and-modify-itunes-backup-files-with-ibackupbot/

Heather Mahalik, 2016. Solutions for iOS 10 – Encrypted backup files, cracking passwords and data acquisition. [Consulté le 9 septembre 2017] Disponible à l'adresse :

http://smarterforensics.com/2016/09/update-ios10-solutions-for-encrypted-backup-files-cracking-passwords-and-data-acquisition/

Elcomsoft – Extracting token on live Windows OS [Consulté le 9 septembre 2017] Disponible à l'adresse :

https://www.elcomsoft.com/help/en/eppb/index.html?extracting_authentication_win.html

SCAR, 2016. Forensic Implications of iOS Lockdown (Pairing) Records [Consulté le 10 septembre 2017] Disponible à l'adresse :

https://articles.forensicfocus.com/2016/11/14/forensic-implications-of-ios-lockdown-pairing-records/

Elcomsoft – Elcomsoft Phone viewer [Consulté le 12 septembre 2017] Disponible à l'adresse :

https://www.elcomsoft.com/epv.html

The iPhone Wiki – Filesystem [Consulté le 13 septembre 2017] Disponible à l'adresse :

https://www.theiphonewiki.com/

Learning iOS Forensics – Mattia Epifani, Pasquale Stirparo [Consulté le 20 septembre 2017] Disponible à l'adresse :

https://books.google.ch/books?id=HodcDgAAQBAJ&lpg=PA16&ots=AxHcyWiN3n&dq=logical acquisition jailbreak&hl=fr&pg=PA15 - v=onepage&q=logical acquisition jailbreak&f=false

Apple – A propos des sauvegardes des appareils iOS [Consulté le 30 septembre 2017] Disponible à l'adresse :

https://support.apple.com/fr-fr/ht204136

Wazzapmigrator – Tutoriel iBackup Viewer [Consulté le 30 septembre 2017] Disponible à l'adresse :

https://www.wazzapmigrator.chttps//www.wazzapmigrator.com/fr/tutoriel-ibackup-viewerom/fr/tutoriel-ibackup-viewer