Projeto

Mestrado em Engenharia Informática – Computação Móvel

Digital Forensics Procedures For Apple Devices

Fábio António Lavrador Amado Marques

Leiria, *agosto de 2017*

Projeto

Mestrado em Engenharia Informática – Computação Móvel

Digital Forensics Procedures For Apple Devices

Fábio António Lavrador Amado Marques

Projeto de Mestrado realizado sob a orientação do Doutor Miguel Frade, Professor da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Leiria, *Agosto de 2017*

Esta página foi intencionalmente deixada em branco

Em memória de Maria José Gomes Lavrador Miguel

Esta página foi intencionalmente deixada em branco

Agradecimentos

A conclusão do Mestrado de Engenharia Informática – Computação móvel só foi possível com a ajuda e apoio dos que direta ou indiretamente estiveram presentes na minha vida ao nível pessoal e académico durante todo este percurso.

Começo por agradecer ao meu orientador Dr. Miguel Frade pela disponibilidade e pelo apoio prestado ao longo do projeto.

Agradeço do fundo do coração aos meus pais, Ana Paula Lavrador Amado Marques, minha mãe, e António José Pires Marques, meu pai, por todo o esforço que fizeram para me manterem a estudar todos estes anos de percurso académico. À minha Madrinha de batismo, Élia Ribeiro também agradeço por todo o apoio e ajuda prestada e por ter estado sempre presente.

Não posso deixar de agradecer à minha avó, Maria José Gomes Lavrador Miguel que apesar de não estar presente entre nós, desde cedo apoiou à minha ida para o ensino superior e o prosseguimento de estudos e fez com que fosse possível a conclusão de todo este percurso.

Por último, gostaria de agradecer aos amigos e às pessoas mais especiais, Joana Pedrosa, João Santos e Elton Eira, que sempre estiveram presentes para ajudar e apoiar durante todo o percurso.

Esta página foi intencionalmente deixada em branco

Resumo

Os dispositivos móveis estão cada vez mais presentes no dia-a-dia das pessoas. A sua ligação à internet das coisas permite a troca de uma grande quantidade de informação. Dada a sua utilização massiva, estes dispositivos estão cada vez mais envolvidos em crimes e por sua vez em investigações digitais. A ciência digital forense tem como objetivo identificar, obter, preservar, documentar, analisar e apresentar provas digitais obtidas de dispositivos móveis, computadores e redes. A ciência digital forense faz parte das investigações criminais e está relacionada com todo o processo legal de investigação em vários tipos de crimes. As ferramentas forenses utilizadas têm como objetivo obter o máximo de provas digitais, mantendo a sua integridade, para que estes possam ser utilizados em tribunal e legalmente reconhecidas e validadas.

No projeto são apresentados um conjunto de procedimentos forenses para dispositivos móveis Apple e adaptados ao LabCIF (Laboratório de cibersegurança e informática forense). Os procedimentos criados permitem ao analista forense passar pelas várias etapas forenses sabendo quais os passos que deve efetuar aumentando assim a qualidade e rapidez dos processos da análise forense.

Dada a quantidade de aplicações móveis utilizadas no dia-a-dia o projeto apresenta um caso de estudo em que um conjunto de aplicações de chat são testadas e utilizadas em dispositivos móveis Apple. Foram efetuadas várias aquisições forenses com o software forense XRY. Com esse estudo foi possível verificar que dados era possível obter e dessa forma retirar conclusões e indicar quais as localizações dos dados mais importantes de determinadas aplicações.

Palavras-chave: Dispositivos móveis, Ciência digital forense, Provas digitais, Procedimentos forenses, Apple, Aplicações de chat.

Esta página foi intencionalmente deixada em branco

Abstract

Mobile devices are part of people everyday life. These devices are connected to the Internet of Things that allows to exchange a lot of information. Due to massive use of mobile devices, these are even more involved in legal digital investigations.

Digital forensics is a science that pretends to identify, collect, preserve, examine, analyze, document and present digital evidences from mobile devices, computers and networks.

Digital Forensics is part of an investigation and it is related to all legal process of investigation in various types of crimes.

Forensic tools are used with the objective of obtain the maximum digital evidences, maintaining data integrity. That way, digital evidences can be legally recognized and used in a court of law.

This project presents a set of digital forensics procedures for Apple mobile devices adapted to LabCIF(Laboratório de cibersegurança e informática forense) of IPLeiria (Instituto Politécnico de Leiria). Forensics procedures help forensics analysts doing the various forensic phases. This will improve quality and quickness of forensic processes.

There are lots of mobile applications used by people on their everyday life. As so on, this project presents a case study with chat and social applications that were tested and used on Apple mobile devices. Forensics acquisitions were made to these devices with XRY software. With this case study, we could draw some conclusions and indicate the which types of data could be obtained from mobile applications.

Keywords: *Mobile devices, Digital Forensics, Digital Evidence, Forensics Procedures, Apple, Chat applications.*

Esta página foi intencionalmente deixada em branco

Índice

Lista de figuras

Esta página foi intencionalmente deixada em branco

Lista de tabelas

Esta página foi intencionalmente deixada em branco

Lista de siglas

AAFS American Academy of Forensics Sciences

ACL Access Control List

ACPO Association of Chief Police Officers

AD1 AccessData Custom Content Image

AES Advanced Encryption Standard

AFF Advanced Forensics File Format)

AOSP Android Open Source Project

APFS Apple File System

ASCLD/LAB American Society of Crime Laboratory Directors / Laboratory Accreditation Board

ASTM American Society for Testing and Materials

ATF Alcohol, Tobacco, Firearms and Explosives

BSD Berkeley Software Distribution)

CD Compact Disk

CDR Call detail records

CFTT (Computer Forensic Tool Testing Project

CPU Central processing unit

DCO Device configuration overlays

DEA Drug Enforcement Administration

DFU Device Firmware Upgrade

DNS Domain Name Server

DOS Disk Operating System

DVD Digital versatile disk

EAFS European Academy of Forensic Science

EEPROM Electronically Erased Programmable Read Only Memory

EFSA	European Forensic Science Area
ENFSI	European Network of Forensic science institutes
ESTG	Escola Superior de Tecnologia e Gestão
EWF	Expert Witness Disk Image Format
EWGC	Expert Working Group Comitee
exFAT	Extended File Allocation table
EXT	Extended File System
ext2fs	Second version Extended File System
ext3fs	Third Version Extended File System
ext4fs	Fourth Version Extended File System
f2fs	Flash-friendly file system
FAT	File allocation table
FBI	Federal Bureau of Investigation
FSC	Forensic Science Regulator
GB	Gigabyte
GDPs	Gross Domestic product
GPS	Global Positioning Systems
HFS	Hierarchical File System
HPA	Host Protected Area
HTTP	Hypertext Transfer Protocol
IACIS	International Association Of Computer Investigate Specialists
ICCID	Integrated Circuit Card Identifier
IM	Instant Messaging
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
IOCE	International Origanization of Computer Evidence

iOS iPhone Operating System

iOT Internet of things

IP Internet Protocol

IPLeiria Instituto Politécnico de Leiria

IRS-CI Internal Revenue Service, Criminal Investigation

ISO international organization for standardization

JFFS2 Journal Flash File System

JPEG Photographic Expert Group File Format

LabCIF Laboratório de Cibesegurança e Informática Forense

MAC Media Access Control

MBR Master Boot Record

MCC Mobile Country Code

MII Major Industry ID

MLC Multi Level Cell

MMS Multimedia Messaging Service

MNC Mobile network code

MSIN Mobile Subscription Identification Number

MSISDN Mobile Station International Subscriber Directory Number

NAND Not And

NAS National Academy of Sciences

NIC Network Interface Card

NICE National Initiative Cyber Security Education

NIST National institute of standards and technology

NOR Not OR

NTFS The new technology file system

PGR Procuradora Geral da República

PIN Personal Identification Number

PJ Polícia Judiciária

PLIST Property List File

POI Points of interest

PUK PIN Unblock key / Personal unblocking key

QCC Quality & Competence Committee

RAID redundant array of independent disks

RAM Random Access Memory

RPM Rotações por minuto

SGQ Sistemas de gestão da qualidade

SIM subscriber identity module

SLC Single-Level Cells

SMS Short Message Service

SOP Standard Operating Procedures

SSD Solid State drive

SWGDE Scientific Working Group on Digital Evidence

TAC Type Allocation Code

TLD Top Level Domain

UDID Unique Device Identifier

UICC Univesal Integrated Circuit Card

URL Uniform Resource Locator

USB Universal Serial Bus

VFAT virtual file allocation table

VFS Virtual File System

XML eXtensible Markup Language

YAFFS Yet Another Flash File System

Esta página foi intencionalmente deixada em branco

1. Introdução

O projeto "*Digital Forensics Procedures for Apple Devices*" tem como objetivo principal o desenvolvimento de procedimentos forenses para dispositivos Apple assim como o estudo dos tipos de dados importantes e da localização dos mesmos nos dispositivos. Tendo em conta a existência de uma grande quantidade de dispositivos móveis, ao facto de que a classe média, média/alta e alta utilizarem cada vez mais dispositivos Apple e à grande quantidade de dados existentes nos mesmos, o objetivo dos procedimentos é apoiar um examinador forense nas diversas fases de um caso forense relacionado com dispositivos Apple. Desta forma, o examinador, ao seguir os procedimentos, realizará os passos essenciais e saberá as localizações mais importantes dos dados, facilitando todo o processo e garantindo a devida qualidade. Outro dos objetivos principais é a análise de dados obtidos relativamente a aplicações.

Nas partes seguintes são descritos o Laboratório de Cibersegurança e Informática Forense (LabCIF), assim como a estrutura do relatório e os anexos para apoio do projeto.

O Laboratório de Cibersegurança e Informática Forense (LabCIF, foi inaugurado a 28 de maio de 2015. A Figura 1 mostra uma identificação existente no laboratório.

Figura 1 – Identificação do LabCIF Fonte: (Frade, 2016)**.**

O LabCIF resulta de uma cooperação entre o Instituto Politécnico de Leiria (IPLeiria), a Procuradora Geral da República (PGR)e a Polícia Judiciária (PJ) com objetivo principal o combate ao crime informático.

O relatório encontra-se organizado nos seguintes capítulos descritos na Tabela 1.

Tabela 1 – Descrição dos capítulos do relatório.

Nome do capítulo	Descrição
1 – Introdução	A introdução descreve conceitos introdutórios como o conceito de análise forense digital, políticas e procedimentos, a definição de prova digital, os cuidados a ter com as mesmas e um resumo de vários processos forenses.
2 – Enquadramento tecnológico	O Enquadramento tecnológico descreve conceitos importantes para o projeto, como uma introdução às tecnologias, os tipos de memória, a organização dos dados os dispositivos, uma descrição dos dispositivos móveis e capacidades tecnológicas.
3 – Procedimentos Forenses	O capítulo procedimentos forenses contém trabalho relacionado com o tema do projeto como conceitos forenses, software utilizado, tipos de aquisição e os procedimentos forenses.
4 – Caso de estudo	O caso de estudo contém as aplicações utilizadas para teste nos dispositivos moveis Apple, assim como os dados que foram adquiridos nas aquisições forenses e os respetivos resultados obtidos.
5 - Conclusões e trabalho futuro	A conclusão contém um resumo do trabalho efetuado com o desenvolvimento dos procedimentos e com o teste das aplicações de chat.

A Tabela 2 contém todos os anexos do projeto assim como a descrição dos mesmos.

Tabela 2 – Lista de anexos do Projeto e repetia descrição

Nome do anexo	Descrição
Anexo A Guia de aquisição e análise.pdf	Anexo que contém um guia com imagens de aquisição a dois dispositivos Apple usando o software forense XRY. Contém também uma breve explicação de como usar o software XAMN.
Anexo B Tabela de resultados da aquisição Parte 1.pdf	Anexo que contém a tabela com os resultados de aquisições efetuadas aos dispositivos Apple. (Parte 1)
Anexo C Tabela de resultados da aquisição Parte 2.pdf	Anexo que contém a tabela com os resultados de novas aquisições efetuadas aos dispositivos Apple. (Parte 2)
Anexo D Características dos iPhone.pdf	Anexo que contém uma descrição detalhada das características de todos os modelos do smartphone da Apple desde a primeira versão até à atual.
Anexo E Software Forense.pdf	Anexo que contém uma tabela com a descrição das funcionalidades de vários softwares forenses.
Anexo F Device Categories.pdf	Anexo de apoio aos procedimentos que contém um conjunto de dispositivos nas suas diferentes categorias.
Anexo G Device Acronyms.pdf	Anexo de apoio aos procedimentos que contém a lista de acrónimos.

A Tabela 3 apresenta a lista de ficheiros que contém os procedimentos forenses.

Tabela 3 – Lista de ficheiros de procedimentos forenses.

Nome do procedimento	Descrição
Procedure 0 Procedures Index.pdf	Procedimento introdutório a todos os procedimentos.
Procedure 1 Reception.pdf	Procedimento que começa pela assinatura do documento de autorização, receção dos dispositivos móveis, verificações importantes, proteção dos dados e inicio do relatório interno.
Procedure 2 Photographic Cataloging.pdf	Procedimento de catalogação e registo fotográfico (Atribuição de siglas numeradas a cada dispositivo e dispositivos de armazenamento externo, fotografia nas diversas vistas indicadas).
Procedure 2.1 Photographing.pdf	Procedimento de fotografia, para apoio ao procedimento anterior.
Procedure 3 Preservation.pdf	Procedimento de apoio à preservação (Preservação dos dados em todos os procedimentos forenses).
Procedure 4 Acquisition.pdf	Procedimento de aquisição (Aquisição dos dados dos dispositivos com *software* forense).
Procedure 5 Examination.pdf	Procedimento de pesquisa das provas (Pesquisa das provas a partir dos dados da aquisição).
Procedure 6 Analysis.pdf	Procedimento de análise das provas (Análise das provas encontradas, hipóteses e conclusões).
Procedure 7 Final Report.pdf	Procedimento de relatório Final (Indicação de como construir o relatório final a partir de todos os dados obtidos durante os vários procedimentos forenses e escritos no relatório interno.

1.1. Análise Forense Digital

Nesta secção descrevemos a análise forense digital e conceitos importantes associados.

Existem várias formas de definir a ciência digital forense ou análise forense digital, e cada autor tem a sua interpretação.

Segundo o autor (Sammons, 2012) forense é a aplicação de uma ciência computacional e processos de investigação com o propósito legal que envolve a análise de provas digitais (*digial evidence*).

(Kent, Chevalier, Grance, & Dang, 2006) afirma que a ciência digital forense, conhecida como ciência forense de computadores e redes tem várias definições. É considerada a aplicação da ciência para identificação, aquisição, análise de dados, preservando a integridade da informação e mantendo os dados protegidos.

Segundo o autor (B. D. Carrier, 2006), a ciência digital forense é um processo cientifico baseado em formular hipóteses e testar as mesmas. Uma hipótese tenta explicar algo que não foi possível explicar, criando uma história com texto devidamente justificado.

Segundo o autor (Whatson & Jones Andrew, 2013) a ciência digital forense é um campo em crescimento que trata de recolher provas de dispositivos digitais, aplicando processos e procedimentos a tudo o que possa conter provas. Este autor considera que os principais processos digitais forenses são, a preservação das provas (*Preserving the evidence*), a identificação das provas *(identifying the evidence*), a extração das provas (*extracting the evidence*), a documentação das provas obtidas (*documenting the evidence*), a interpretação das provas (*Interpreting the vidence*) e a apresentação das provas (*Presentig the evidence*).

Tendo em conta a informação de vários autores, conseguimos entender o conceito de ciência digital forense e que a maior parte organizações contém um conjunto de etapas forenses, no entanto algumas podem estar mais resumidas ou simplificadas. Dessa forma, criamos um conjunto de etapas forenses adaptadas ao LABCIF. A análise forense consiste em métodos que permitem a receção, catalogação, preservação, registo fotográfico, aquisição, procura das provas, análise, e documentação das provas digitais.

Consideramos também que investigação digital é um processo onde se desenvolvem e se testam hipóteses que respondem a questões já colocadas. Inicialmente são colocadas

questões e ou hipóteses tendo em conta as provas que foram encontradas e depois essas hipóteses são devidamente testadas com uma ou mais provas que possam ser encontradas. O objetivo é provar se determinada hipótese é ou não verdadeira.

1.1.1. A importância da Análise Forense digital

Nesta subsecção identificamos a necessidade da análise forense digital, o conceito, assim como para os efeitos que é usada.

Uma das questões podemos colocar é, "Porque é necessária a análise forense digital?" Alguns anos atrás apenas se falava em ataques a computadores ou redes, em que os dados eram roubados ou alterados, comprometendo os mesmos. Estes acontecimentos violam leis uma vez que a segurança e integridade dos dados é colocada em causa. Devido à facilidade de aceder à internet e com o aparecimento e utilização massiva dos dispositivos móveis, foi aberta uma nova área da investigação digital forense. A análise digital forense envolve não só computadores portáteis e de secretária, mas também dispositivos móveis, redes e os dados em nuvem (*cloud computing*), com todo o tipo de conteúdos (Gogolin, 2012; Sammons, 2012).

Por norma, as ciências digitais forenses envolvem a recuperação de dados perdidos, ocultados ou envolvidos em algum incidente num ou vários dispositivos (Whatson & Jones Andrew, 2013).

Um dos problemas da análise digital forense são as leis, a forma como se investigam os crimes e o incentivo das leis à procura de provas digitais. Os equipamentos digitais utilizados no dia-a-dia tais como telemóveis, tablets, consolas etc. podem conter bastantes provas. O problema passa pela parte em fazer reconhecer essas provas para serem validadas em tribunal. As leis vão sendo adotadas de forma lenta para poder contemplar novas situações envolvendo equipamentos digitais (Sammons, 2012).

Razões para o uso da análise digital forense

Os incidentes que levam ao uso da análise Forense digital podem ser considerados de 3 tipos. De forma acidental, onde não houve intenção de comprometer algo, de forma deliberada (com intenção de comprometer os dados) ou devido a uma ameaça como *malware* ou outro tipo.

Podem ainda ser considerados 3 tipos de crimes, crimes que envolvam litígios civis, inteligência ou terrorismo, questões administrativas relacionadas com empresas entre outro tipo de situações (Sammons, 2012).

Segundo o autor (Whatson & Jones Andrew, 2013) existem um conjunto de crimes dos quais podem dar origem a uma investigação digital forense. Na lista seguinte são apresentados exemplos mais comuns.

- Uso não apropriado de um sistema: usando um dispositivo de processamento de dados contra a lei ou contra uma politica de utilização em que se quebrem políticas de utilização dentro de uma organização ou haja uma fuga de informação;
- Acesso não autorizado: Atacantes internos ou externos que tentam ganhar acesso à informação e aos recursos como: aceder ou copiar informação sem permissões, aceder a redes não seguras, tentar ou forçar um sistema para obter permissões de administrador, tentar obter palavras-passe etc.;
- Ataque de *malware* ou outro tipo de vírus;
- Negação de serviço (*Denial of service*) como por exemplo: Tentativa de mandar um sistema abaixo, tornar uma rede *wireless* inutilizável, estabelecer várias sessões de login para impedir outros utilizadores, criar vários ficheiros para ocupar o espaço do disco, utilização elevada de recursos e ocupação da largura de banda da rede.

Principio de troca de Locard, (*Locard's Exchange Principle)*

O principio de troca de *Locard* diz que, no mundo atual, quando os autores entram ou abandonam um cenário de crime, irão deixar algum vestígio e levar algo com eles. Os exemplos forenses antigos incluíam DNA, impressões digitais, cabelo entre outros. Na ciência digital forense existem também um conjunto de vestígios e registos que podem ser deixados para trás, como por exemplo: ficheiros relativos a registos dos sistemas, metadados e outras informações (Sammons, 2012).

1.1.2. Análise forense de dispositivos móveis

Nesta subsecção vamos descrever de uma forma breve a relação entre os dispositivos móveis e a análise forense.

Mobile forensics é, segundo (Epifani & Stirparo, 2015), o campo da análise forense digital focada em dispositivos móveis, sendo uma área que está em constante crescimento de forma exponencial dado o aumento da utilização destes dispositivos. A grande variedade de dispositivos móveis, de diversos fabricantes, com sistemas operativos diferentes, e a quantidade de aplicações trazem novos desafios para esta área em desenvolvimento.

Existem uma série de desafios com os dispositivos móveis que obrigam que os equipamentos e *software* forense estejam em constante desenvolvimento. Na lista abaixo indicamos alguns factos (Whatson & Jones Andrew, 2013).

- O rápido desenvolvimento da tecnologia que obriga à criação de novas ferramentas, técnicas e procedimentos assim como a necessidade de os mesmos serem validados e testados;
- As provas digitais podem ser difíceis de interpretar para alguém que não entende sobre determinadas tecnologias;
- O sistema dos tribunais assim como o sistema judiciário pode não entender o funcionamento da tecnologia assim como a forma como as provas são obtidas;
- As leis levam algum tempo a serem adaptadas de forma a favorecer a análise forense digital. Sendo que devem ser o mais genéricas possível.

O foco de uma investigação digital.

O foco de uma investigação digital é um ou mais dipositivos que esteve envolvido num incidente ou crime.

Do ponto de vista forense, existe então uma necessidade de descobrir e responder às seguintes perguntas: quem foi, o que aconteceu, onde, quando, e em que consistiu o crime? (Kent et al., 2006).

1.1.3. Politicas e procedimentos

Nesta subsecção vamos identificar o conceito de políticas e procedimentos no contexto forense.

As politicas e procedimentos estão relacionados com os passos que um ou mais analistas forenses do laboratório toma aquando do tratamento de um caso forense, isto é, como trata das provas desde o inicio até ao fim. Todos os passos devem ser tidos em conta com base em politicas e Procedimentos standard SOP (*Standard Operating Procedures*). Os SOP são documentos que detalham como devem ser seguidas todas as fases forenses. Estes procedimentos têm em conta situações que podem ocorrer durante as diversas fases, logo, não podem ser demasiado limitativos ou demasiado amplos de forma a facilitar as tarefas mais fáceis ou mais difíceis que podem ocorrer (Sammons, 2012).

Os procedimentos devem ser mantidos e atualizados constantemente. Devem estar também atualizados tendo em conta as novas tecnologias, novas politicas, e tendo sempre em conta a integridade e confiabilidade dos dados.

1.1.4. Provas digitais

Nesta subsecção identificamos o conceito de prova digital.

As provas digitais (*digital evidence*) são os dados obtidos dos dispositivos que podem ser importantes para a investigação forense de um dado caso uma vez que podem ser úteis.

Os smartphones tem uma grande probabilidade de conter provas digitais dada a utilização diária dada pelos utilizadores. Estes dispositivos são cada vez mais usados em crimes. Podem existir uma grande quantidade de provas que podem ser usadas para recriar todo o acontecimento que envolve o crime ocorrido. O dispositivo móvel contém uma série de registos como chamadas, mensagens, localização via GPS, conteúdos multimédia (imagens e vídeos) e registos de aplicações de mensagens e redes sociais. Enquanto as provas físicas podem muitas vezes ser destruídas, as provas digitais deixam alguns rastos que permitem ajudar na investigação.

Em seguida apresentamos a definição de prova digital segundo vários autores.

A *Scientific Working Group on Digital Evidence* (SWGDE) afirma que "As provas digitais são valores que são guardados ou transmitidos de uma forma digital" (Epifani & Stirparo, 2015).

A *International Origanization of Computer Evidence* (IOCE) afirma que "Uma prova digital é informação guardada ou transmitida em formato binário e que pode vir a ser usada em tribunal"(Epifani & Stirparo, 2015).

A definição de (Carrier, 2006) define uma prova digital como "Dados digitais que contém informação importante e aprovam ou vão contra uma hipótese sobre um acontecimento digital ou o estado dos dados".

Como podem ser as provas validadas em tribunal?

Para serem válidas em tribunal, as provas devem ser obtidas de forma correta e legal. Dessa forma, as politicas e os procedimentos devem ser seguidos de forma correta (Sammons, 2012).

Tudo se deve ao facto de que as provas:

- Podem ser danificadas durante o processo de aquisição;
- Podem ser duplicadas;
- Podem ser alteradas sem deixar qualquer rasto;
- Podem ser alteradas no momento em que são transmitidas;
- Podem não ser possíveis de ler e podem ter que ser fotografadas;
- São difíceis de destruir;
- Podem ser criadas por um dispositivo e não por um ser humano;
- Podem estar encriptadas;
- Podem estar guardados em vários dispositivos ao mesmo tempo;

A seguinte lista apresenta um conjunto de regras que as provas digitais devem seguir para serem corretamente validadas (Sammons, 2012).

- Legalmente obtidas – As provas devem ser obtidas de acordo as regras existentes, principalmente de acordo com as leis existentes. Devem ser também consideradas úteis relativamente ao caso e não devem violar quaisquer regras;
- Relevância – As provas devem ser importantes e ter alguma relevância, confirmando ou não factos que podem ser ou não verdade;
- Completas – As provas devem ser o mais completas possível de forma a que seja possível retirar o máximo de informação possível. Desta forma é importante que possa ser provada tanto a culpa como a inocência;
- Confiança – As provas devem ser as mesmas que foram obtidas, sem modificações de integridade. Seguindo os melhores procedimentos e as melhores práticas consegue-se assegurar a integridade dos dados;
- Precisão – Não devem haver erros na obtenção das provas e os procedimentos devem ser devidamente certificados para que ao serem seguidos possam ajudar a obter as provas que, se corretas, podem ser úteis em tribunal.
- Acreditação – Em tribunal, o Juiz deve ficar convicto relativamente às provas encontradas. Aqui se aplica o termo cadeia de custódia *(chain of custody*) que tem por objetivo preservar todo o cenário de crime para que este possa ser acreditado em tribunal, de forma a provar que todas as etapas foram corretamente efetuadas e os dados não foram manipulados.

Cuidados a ter com os dispositivos e as provas digitais.

Dependendo do tipo de dispositivo, existem uma série de cuidados a ter no manuseamento dos mesmos e das provas.

- Os dispositivos podem ser controlados remotamente se estiverem ligados à rede e toda a informação pode ser apagada;
- As baterias têm uma duração limitada e se não forem tomados cuidados esta pode descarregar, por isso pode ter que ser carregada várias vezes;
- Se o dispositivo for desligado, poderá nunca mais conseguir ser ligado se existirem códigos;
- Palavras-passe incorretas podem originar a perda de todos os dados;
- Deve ser tido cuidado no transporte dos dispositivos que podem conter provas para evitar causar danos.

Cópia de segurança de um caso digital forense

Todo o trabalho forense deve ser devidamente guardado como cópias de segurança. Deve ser efetuada uma cópia das imagens obtidas durante o processo de aquisição para várias localizações de armazenamento de dados. Dessa forma, os dados das aquisições efetuadas estarão sempre guardados. Deve ser também efetuada uma cópia dos dados a serem analisados que foram obtidos depois da aquisição da imagem do dispositivo, neste caso as provas, para evitar que seja perdido todo o trabalho de procura de provas já elaborado.

1.2. Organizações digitais forenses

Nesta secção vamos descrever algumas organizações forenses.

Existem algumas organizações forenses que estão concentradas em estabelecer protocolos, standards, e guias de boas práticas e procedimentos para elevar os níveis de conhecimento e certificação dos examinadores e laboratórios forenses. Os examinadores forenses responsáveis por analisar os casos devem ter conhecimentos sobre estas entidades, os papeis que desempenham e as contribuições que fazem.

Em baixo descrevemos algumas organizações existentes:

SWGDE *(Scientific Working Group on Digital Evidence*)

Criada em 1998 pelo "*Federal Crime Laboratory Directors Group*", SWGDE é constituída por órgãos que tem conhecimento das leis e que e as podem aplicar tendo em conta as ciências digitais forenses e os conteúdos digitais associados. À medida que foram surgindo conteúdos digitais foi surgindo a necessidade de criar uma disciplina forense que envolvesse estes conceitos. Os membros iniciais pertenciam a laboratórios forenses como: ATF (*Alcohol, Tobacco, Firearms and Explosives*), DEA (*Drug Enforcement Administration*), FBI (*Federal Bureau of Investigation*), IRS-CI (Internal Revenue Service, Criminal Investigation), *US Customs*, *US Postal Inspection Serivce*, *US secret Service*, *NASA*, e "*Department Of defence Computer Forensics Laboratory*" Todos os constituintes da SWGDE tem álbuns anos de experiência na área (Sammons, 2012).

Esta organização baseia-se nos standards e nas técnicas que são as bases de uma ciência digital forense exata.

O objetivo da SWGDE é juntar as organizações envolvidas nas áreas digitais forenses e com conteúdos multimédia, de forma a melhorar a comunicação e a partilha de conhecimentos, assegurando qualidade e consistência na comunidade

Forense. Dessa forma, é possível desenvolver boas práticas forenses assim como documentação que pode ser utilizada por outras entidades (SWGDE, 1999)

AAFS (*American Academy of Forensics Sciences)*

Esta organização contém membros que trabalham para a NIST (*National institute of standards and technology*) e para a NAS (National Academy of Sciences). Os membros desta comunidade fazem também parte de vários grupos científicos como a SWGDE. O objetivo desta organização é criar standards para a comunidade forense (Sammons, 2012).

ASCLD/LAB (*American Society of Crime Laboratory Directors / Laboratory Accreditation Board)*

ASCLD/LAB é um dos mais antigos mais conhecidos laboratórios acreditação de crime / forense. Os laboratórios forenses certificados por esta entidade são os melhores no mundo forense. Um laboratório fica certificado quando este utiliza standards e requisitos especificados no manual de acreditação da ASCLD.

O principal objetivo desta organização é apoiar os profissionais da área forense, dar apoio nos laboratórios, desenvolver princípios e técnicas forenses. A comunicação entre várias entidades e responsáveis por laboratórios forenses é também uma das grandes bases que permite adquirir, preservar e divulgar muita informação, mantendo e implementando os melhores standards (American Society of Crime Laboratory Directors, 2017).

NIST (*National Institute of standards and technology)*

A NIST foi criada em 1901. Foi dos primeiros laboratórios de investigação de ciências governamentais. Esta organização está envolvida em projetos forenses digitais como:

- NICE (*National Initiative cyber Security Education*) – Um programa de educação em segurança que ensina conteúdos para melhorar a segurança

-*National Software References Library* – Um conjunto de assinaturas de software que podem ser usadas pelos responsáveis da análise de ficheiros para excluir os ficheiros que não tem valor para a investigação.

-*Computer Forensics Tool testing* – Pretende desenvolver metodologias e standards para software e hardware forense.

O principal objetivo desta organização é efetuar pesquisas e melhorar o standards existentes de forma a que a aplicação das ciências digitais forenses sejam aplicadas de forma correta (National Institute of Standards and Technology, 2017; Sammons, 2012).

ASTM (*American Society for Testing and Materials)*

A ASTM é uma entidade que desenvolve standards usados para melhorar a qualidade dos produtos e facilitar o acesso ao mercado e a confiança do consumidor. Criada em 1998 contém 30 mil membros em 141 comités. A comunidade de ciências forenses, conhecida como E30 está dividida numa série de comités. O comité de evidencias digitais e de multimédia (*Digital and Multimedia evidence subcommittee*) é conhecido como E30.12 ASTM.

Existem uma série de organizações que ajudam a estabelecer standards e as melhores práticas na área forense digital. Organizações como AAFS, SWGDE e ASTM (Sammons, 2012).

ENFSI (*European Network of Forensic science institutes*)

Esta organização foi formada em 1992. O objetivo desta organização é criar e manter uma rede forense em toda a Europa. Contém membros de organizações de 32 países. As organizações devem cumprir com uma série de critérios e demonstrar que utilizam standards para serem membros desta organização. Dessa forma é possível partilhar conhecimentos e experiências no campo das ciências forenses. O maior propósito é assegurar a qualidade dos serviços forenses prestados na Europa em laboratórios forenses. A ENFSI é estruturada numa série de comissões (standing *commitees)* e "*Expert Working Groups*" que se juntam regularmente para verificar se todos os objetivos foram cumpridos. A ENFSI tem uma série de comissões como a EWGC (*Expert Working Group Comité*), a *Quality & Competence Committee* (QCC), European Academy of Forensic Science (EAFS). Nas reuniões efetuadas, são discutidas novas tecnologias forenses, novos standards, entre outras informações importantes, permitindo assim aos *Expert Working Groups* desenvolver manuais de boas práticas e guias para

ajudar a estabelecer e manter os standards dos laboratórios forenses na Europa. São ainda mantidas comunicações com organizações como a ASCLD ("About ENFSI | ENFSI," 2017; Encyclopedia.com, 2017).

1.3. Resumo de processos e Etapas Forenses

Existem um conjunto de processos forenses que são aplicados às investigações forenses digitais. Nesta secção apresentamos as fases do ponto de vista de alguns autores que contém pequenas diferenças nas etapas forenses.

Segundo o autor (Whatson & Jones Andrew, 2013), existem quatro passos forenses que podem ser aplicados a quaisquer investigações forenses digitais, em quaisquer circunstâncias. A lista seguinte apresenta esses 4 passos:

- Aquisição (*Acquire*);
- Análise (*Analyze*);
- Avaliação (*Evaluate*);
- Apresentação(*Present*).

Ainda baseado em (Whatson & Jones Andrew, 2013), complementando a lista anterior, apresentamos a descrição das etapas forenses:

1) Identificação (*Identification*) – Reconhecer que aconteceu num crime e identificar o seu tipo. Esta etapa, é uma etapa inicial na qual o laboratório forense é solicitado para começar a investigar.

2) Preparação (*Preparation*) – Preparação de ferramentas, técnicas e obtenção de autorização para trabalhar com os dados.

3) Estratégia de aproximação (*Approach strategy*) – Criação de uma aproximação baseada na tecnologia e tendo em conta as pessoas que são afetadas. O objetivo é aumentar os dados que se conseguem obter no processo de aquisição.

4) Preservação (*Preservation*) – Isolamento, segurança e preservação do estado dos equipamentos e das provas digitais. Esta etapa pode incluir, por exemplo, a proibição do acesso às provas digitais a determinadas pessoas não autorizadas.

5) Aquisição (*Collection*) - Obtenção dos dados dos dispositivos físicos e duplicação desses dados, baseando-se em procedimentos forenses e com as ferramentas específicas.

6) Examination (*Exame*) – Procura sistemática de provas, procurando identificar e localizar provas importantes tendo em conta os dados que foram obtidos no passo anterior.

7) Análise(*Analysis*) – Através das provas que foram identificadas, juntar várias partes dos dados, relacionar os mesmos para poder tirar conclusões.

8) Avaliação (*Evaluation*) – Determinar a importância das provas que foram recolhidas que pode ser importante para apresentar em tribunal.

9) Apresentação (*Presentation*) - Detalhar e obter conclusões sobre o que foi efetuado. Estas conclusões devem ser escritas segundo (*Layman's Terms*), ou seja, escrita de forma a que uma pessoa fora da área técnica e sem conhecimentos da mesma consiga entender todos os termos e conclusões.

10) Devolução das provas (*Returning evicence*) – Devolver os dispositivos ao dono dos mesmos, caso a lei assim o autorize.

Segundo o autor (B. D. Carrier, 2006), o processo de investigação forense considerado é apresentado na seguinte lista:

- Preparação (*Preparation*) – Preparar os equipamentos e as ferramentas para as tarefas necessárias durante a investigação;
- Aquisição (*Coolection*) – Procurar provas, documentar, fazer a aquisição, e cópias dos dispositivos que contenham provas;
- Exame (*Examination*) – Tornar visível as provas digitais e documentar todas as provas;
- Análise (*Analysis*) – Analisar as provas da fase anterior para tomar conclusões;
- Relatório (*Reporting*) – O relatório documenta todas as fases anteriores, mas também inclui todos os dados obtidos e as devidas conclusões.

Segundo o autor (Kent et al., 2006), o processo da ciência digital forense compreende as seguintes fases:

- Aquisição (*Collection*) – Consiste em identificar (*idenfifying*), catalogar (*Labeling*), guardar (*recording*) e aquisição(*acquisition*) dos dados de

possíveis fontes, seguindo guias e procedimentos e preservando a integridade dos dados.

- Exame (*Examination*) – Esta fase envolve o processamento de uma enorme quantidade de dados obtidos. São usados os dados obtidos durante o processo de aquisição em combinação com técnicas automatizadas ou manuais para aceder aos dados, mantendo sempre a integridade dos mesmos.
- Análise (*Analysis*) – Esta fase consiste em analisar os resultados obtidos do processo anterior, usando termos legais e técnicas que possam responder a questões colocadas durante os dois processos anteriores.
- Relatório (*Reporting*) – A fase final consiste em relatar os resultados da análise que podem incluir todos os processos feitos anteriormente, incluindo os procedimentos utilizados, todas as decisões e ações tomadas e *software* utilizado para contornar determinados problemas.

A Figura 2 apresenta as os processos da análise digital forense segundo o autor.

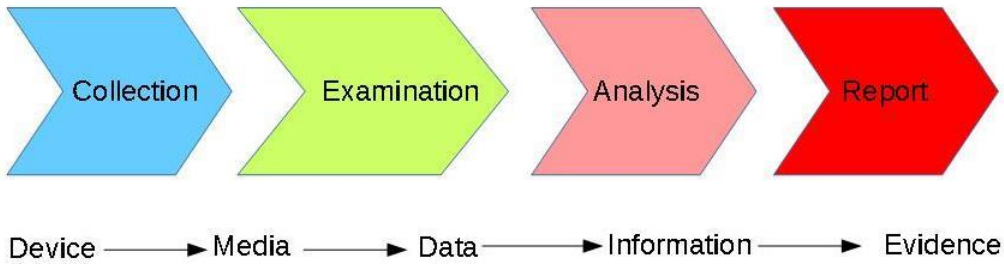


Figura 2 – Fases forenses. Adaptado de (Kent et al., 2006)**.**

A figura começa por identificar os 4 passos forenses segundo o autor.

A fase de aquisição (*collection*) refere-se aos dispositivos (*device*), em seguida a fase de exame (*examination*) refere-se aos dados que são obtidos (*Media* e *Data*), a fase de análise (analysis) refere-se à informação (*information*) que já foi obtida e pode ser visualizada. A última fase, relatório final (*report*) refere-se às provas (*evidence*) que ajudaram a poder tirar conclusões e a criar o relatório.

Segundo o autor (Viriato, 2016), apresentamos as várias fases forenses.

A Figura 3 apresenta os processos da análise digital forense segundo o autor.

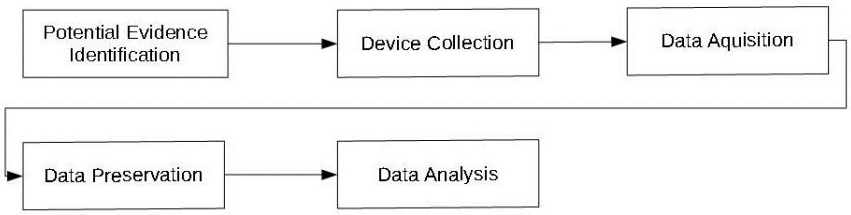


Figura 3 – As várias fases do processo digital forense. Adaptado de (Viriato, 2016)**.**

Na continuação dos processos que foram identificados anteriormente descrevemos as etapas forenses segundo o autor.

Identificação (Potential Evidence *Identification*) - O processo de identificação envolve variadas ações de pesquisa, reconhecimento e registo de dispositivo(s) que possa(m) conter potenciais provas digitais. Deve ser elaborada uma lista de prioridades de acordo com as probabilidades / potencialidades das provas digitais encontradas.

Recolha (Data *Collection*) – A recolha consiste em retirar os dispositivos que podem potenciais provas digitais do local do crime para o laboratório forense que irá efetuar a análise. Este processo deve ser devidamente documentado e os dispositivos devem ser devidamente embalados e protegidos e durante o seu transporte.

Aquisição (Data *Acquisition*) – A aquisição consiste na realização de uma cópia dos dados existentes no dispositivo. A cópia deve ser feita da melhor forma possível e de forma a proteger os dados, mantendo a sua integridade. O ideal será obter os dados de forma igual ao qual estes estavam no dispositivo. Qualquer alteração aos mesmos deve ser devidamente documentada.

Preservação das provas digitais (**Data *Preservation*) -** A preservação pretende proteger as provas digitais de uma possível alteração de integridade, roubo ou adulteração (Viriato, 2016).

Segundo (Viriato, 2016) os dispositivos com possíveis provas digitais podem ser divididos em dois tipos:

- Computadores, dispositivos periféricos e dispositivos de armazenamentos, considerando os computadores equipamentos isolados sem estarem ligados à rede.
- Dispositivos em rede – Todos os dispositivos ligados a uma rede wireless por cabo.

Análise das provas digitais (*Data analysis*)

Segundo (Viriato, 2016), o processo de análise aos dados nos dispositivos recolhidos e aos dados adquiridos ao local do crime deve respeitar a noma de acreditação ISO/IEC 17025:2005. Ainda segundo o mesmo documento, depois das fases de Identificação, recolha, aquisição e preservação devem ser seguidos os processos de Análise de Provas (*Evidence Analysis*) que significa neste caso o processo de extração de informação e preservação das provas (*Evidence Preservation)* e o processo de documentação dos resultados obtidos. Este último, serve como prova e é utilizado para o preenchimento do relatório de todo o processo forense.

1.3.1. Opinião sobre os processos e etapas forenses

Nesta subsecção são abordados todos os processos forenses apresentados na secção anterior em conjunto com uma sugestão para um conjunto de etapas forenses a serem seguidas em procedimentos.

Como primeira etapa forense, consideramos a receção dos equipamentos (*reception*), na qual os equipamentos são devidamente recebidos, são tomados cuidados para proteger o dispositivo de comunicar com a rede e são preenchidos os documentos de autorização. Apenas o autor (Whatson & Jones Andrew, 2013) apresenta os passos 1 e 2 , *Identification* e *Preparation* quase equivalentes ao que foi referido anteriormente.

Como segunda etapa forense, consideramos a catalogação e fotografia (*Photographic Cataloging*), etapa, na qual os dispositivos e os suportes de armazenamento externo cartões de memória, e cartão SIM (*Subscriber Identity Module*) são devidamente

identificados com abreviaturas específicas e depois devidamente fotografados. Relativamente à catalogação, apenas o autor (Kent et al., 2006) faz referência a esta etapa forense. Relativamente ao registo fotográfico apenas o autor aborda esta etapa forense.

Como terceira etapa forense, consideramos a preservação (*preservation*) no qual os dispositivos devem ser isolados e colocados em segurança de forma a que as provas digitais existentes nos mesmos não sejam alteradas. Os autores (Viriato, 2016; Whatson & Jones Andrew, 2013), fazem referência a esta etapa forense.

Como quarta etapa forense consideramos a aquisição (*acquisition*). Esta é a etapa mais importante, na qual são usadas as ferramentas de hardware e software forense para obter os dados dos dispositivos. Todos os autores fazem referência ao processo de aquisição (*acquisition*) ou (*device collection*) ou (*collection*).

Como quinta etapa forense consideramos a procura de provas (*examination*), na qual são usados softwares ou técnicas manuais para a procura das provas nos dados resultantes da aquisição. Os autores (B. D. Carrier, 2006; Kent et al., 2006; Whatson & Jones Andrew, 2013) consideram esta etapa forense.

Como sexta etapa forense consideramos a análise (**analysis**), em que são analisadas as provas recolhidas, relacionar as mesmas e tirar conclusões para que se possam aprovar ou reprovar hipóteses colocadas em causa. Todos os autores consideram esta fase como essencial.

A sétima e última fase forense é o relatório final (*reporting*) em que são documentadas todas as etapas forenses, indicando os dados obtidos, as conclusões tiradas. Os autores fazem referência a esta etapa, nomeadamente (Whatson & Jones Andrew, 2013) com a fase (*presentation*), e (B. D. Carrier, 2006; Kent et al., 2006) (*reporting*).

2. Enquadramento Tecnológico

O capítulo enquadramento tecnológico tem como objetivo a apresentação dos termos tecnológicos e técnicos relacionados com o projeto, a evolução da tecnologia, os tipos de memória dos dispositivos, a organização dos dados, os dispositivos móveis, os sistemas operativos de dispositivos móveis e algumas capacidades tecnológicas como o GPS.

2.1. A evolução dos dados e da tecnologia

Os dados são partes de informação que estão formatados de uma determinada forma e tendo em conta aplicações que possam ler esses dados (Sammons, 2012).

O surgimento da internet que levou ao surgimento do termo internet das coisas *Internet of Things* (IOT), que está relacionado com a grande quantidade de dispositivos ligados à internet e a quantidade / variedade de dados que são trocados. O aumento da utilização dos computadores, seja para uso pessoal, seja para uso profissional, a utilização dos dispositivos móveis e a ligação à internet levou ao aumento do número de aplicações e sucessivamente dos dados gerados por estas. Os dados gerados podem ser guardados ou transferidos por uma série de dispositivos como computadores, dispositivos móveis como smartphones, *smartwatch*, *tablets*, GPS (*Global Positioning Systems*) e câmaras fotográficas. Suportes como CD ou DVD ou dispositivos removíveis como discos rígidos, *pen drives,* cartões de memória e todo tipo de memória *flash*.

Sendo que existe uma grande quantidade de dispositivos, a tendência é para que sejam cada vez mais os dispositivos a poder trocar dados entre si através da internet e que estes tenham mais capacidade de armazenamento.

Enquanto utilizadores de tecnologia deixamos uma pegada digital enorme aquando da utilização de uma grande quantidade de dispositivos. Até mesmo pelos cartões multibanco, pela utilização da internet, os *E-mails*, as mensagens de texto e pelos dados de localização GPS são tudo pegadas digitais deixadas pelos utilizadores (Sammons, 2012).

A Figura 4 apresenta um conjunto de dispositivos, começando pelos cartões de memória (*Memory card*), cartões SIM (*Sim cards*), telefones (*Phones*) ou smartphones, dispositivos vestíveis (*wearables*) como é o caso dos smartWatch, os tablets, os leitores de multimédia (*Media devices*), os GPS e as Camaras.

Figura 4 – Dispositivos móveis e suportes de dados, Fonte: (Frade, 2016)

2.2. Tipos de memória

A memória guarda os dados, que são um dos componentes mais importantes da análise forense e podem servir como provas. Dessa forma é importante destacar os tipos de memória existentes, diferenciando memória de armazenamento, a forma de escrever os dados e a duração que os dados ficam guardados. Esses conceitos irão ser explicados mais abaixo.

Formas de escrever dados

Existem 3 formas principais de escrever dados. Por eletromagnetismo, por transístores microscópios elétricos (flash) e por luzes refletoras (CD, DVD etc.). Em resumo, existem 3 tipos de memória, a memória magnética, a memória flash e a memória ótica dos dispositivos óticos.

2.2.1. Memória Volátil e não volátil

Nesta subsecção será diferenciada a memória volátil de não volátil.

Ao falar sobre memória volátil e não volátil é importante distinguir os conceitos de memória e armazenamento (*Memory / Storage*) uma vez que são dois termos distintos. Memória refere-se à memória de curta duração, enquanto armazenamento se refere a memória de longa duração. Do ponto de vista forense, estes dois termos são bastante distintos e tem uma perspetiva diferente. Por exemplo, no caso dos computadores e dos dispositivos móveis, os dados da memória RAM

(*Random Access Memory*) apenas existem enquanto existe fornecimento de energia. Quando a alimentação é desligada, (i.e., o equipamento é desligado) os dados são apagados. A memória de longa duração, isto é, não volátil mantém os dados guardados mesmo sem alimentação como é o caso dos discos rígidos, da memória flash dos SSD, *pen-drives* ou cartões de memória ou memória interna de dispositivos móveis por exemplo.

A análise digital forense foca-se nos dispositivos de armazenamento como os discos rígidos, Discos SSD, a memória flash de armazenamento interna dos dispositivos que podem conter uma grande quantidade de provas, nos dispositivos de rede entre outros. No caso deste projeto, o foco principal será a memória de armazenamento interna dos dispositivos móveis. Alguns dados são escritos para a memória de curta duração e nesse caso poderá ser importante tentar obter os dados guardados enquanto o dispositivo estiver ligado (Sammons, 2012).

Tendo em conta o que foi dito anteriormente, podemos classificar os dados mais evidentes nos respetivos componentes do mais volátil para o menos volátil. A seguinte lista apresenta a ordem de volatilidade dos dados:

1 CPU, cache, registo;

2 Tabela de encaminhamento, tabela de processos;

3 Memória RAM;

4 Ficheiros temporários em disco / Espaço swap;

5 Dados no disco rígido ou memória flash;

6 Dados de registos;

2.2.2. Tipos de armazenamento de dados

A localização dos dados é importante para a análise forense. Cada dispositivo contém diferentes características, aplicações e capacidades em termos de tamanho *GigaByte* (GB) e de capacidade de leitura ou escrita.

Esta subsecção vai ser focada essencialmente na memória de armazenamento *flash* uma vez que está inteiramente relacionada com dispositivos móveis e com o tema do projeto.

Armazenamento ótico

Este tipo de armazenamento utiliza um laser para ler e escrever dados em material refletivo que está incorporado em discos óticos como *Compact disk* (CD) ou *Digital Versatile Disk* (DVD).

Discos magnéticos

Os discos rígidos magnéticos são usados em computadores. São constituídos por um motor que faz rodar os pratos a determinadas RPM, rotações por minuto, pratos e cabeças agarradas a um braço.

Os dados são guardados como 1's e 0', em espaços denominados de sectores. Os sectores são pequenas partes onde pode ser guardada informação. Cada sector pode guardar até 512bytes, no entanto pode guardar menos ou até mais. Por exemplo, caso tenhamos um ficheiro com 1024 bytes, este vai ocupar 2 setores de 512bytes. Caso o ficheiro seja apagado, este vai ser removido de um índice de ficheiros (Sammons, 2012) .

A Figura 5 ilustra um disco rígido magnético.

Figura 5 – Disco rígido. Fonte: (Irani Elias, 2017)**.**

Dispositivos de gestão de redes

Os dispositivos de gestão de redes que fazem parte da rede de uma empresa, organização ou até de uma habitação pessoal são partilhados por várias pessoas. A seguinte lista anuncia tipos de dispositivos de rede (Whatson & Jones Andrew, 2013):

- Placa de rede, Network Interface Card (NIC);
- Router;
- Bridge;
- Hub;
- Switch;
- Firewall;
- Pontos de acesso wireless (Access Point).

Dispositivos amovíveis (*Removable Media)*

Os dispositivos amovíveis são dispositivos de memória flash que por norma são facilmente removidos de algum dispositivo. Como exemplo podem ser as *pen-drives* e os cartões de memória.

2.2.3. Localização dos dados

A localização dos dados é um ponto importante do ponto de vista forense. Neste projeto incidimos principalmente nos dispositivos móveis.

Os dados, guardados em dispositivos móveis podem estar localizados em 3 localizações diferentes. A maioria dos dados estão guardados na memória interna de um dado dispositivo e no cartão de memória. Apesar da quantidade de armazenamento ser menor, é importante ter em consideração os cartões SIM (*Subscriber Identity Module*) como possível localização dos dados porque podem conter dados importantes.

No caso dos dispositivos da Apple, não existe armazenamento por cartão de memória, dessa forma as únicas localizações possíveis para guardar dados são na memória interna do dispositivo e no cartão SIM. A principal incidência é a memória interna do dispositivo (Frade, 2016; Sammons, 2012).

Considerando a evolução da Internet, podemos considerar também a computação em nuvem (*cloud computing*) como uma forma de armazenamento ou possível localização dos dados. No caso da computação em nuvem, existe uma aplicação intermédia que trata da sincronização dos dados. (Sammons, 2012). Os exemplos são: a Dropbox, a Google Drive, ou outro tipo de solução existente, que guarda os dados na nuvem e a aplicação é usada para os aceder. Nos dispositivos móveis os dados das aplicações de *cloud* ficam visíveis, mas o utilizador escolhe o que quer guardar. No caso dos dispositivos Apple, o serviço que permite guardar os dados em nuvem denomina-se *icloud*.

2.2.4. Memória flash

A memória *flash* é um dos pontos mais importantes neste projeto. Este tipo de memória é usada numa grande quantidade de dispositivos cujo principal objetivo é a portabilidade.

As vantagens deste tipo de memória são a portabilidade, rapidez, a não existência de partes móveis que possam sofrer com os movimentos e o seu baixo consumo de energia (Sammons, 2012).

É um tipo memória não volátil, não necessitando de energia para manter os dados guardados (Fiorillo, 2009). Esta tecnologia está aplicada nas *Pen Drive*, cartões de memória, nos discos SSD (*Solid State Drive*) usados nos computadores e nos dispositivos móveis sendo denominada de memória interna.

A memória *flash* é um tipo de EEPROM (Electronically Erased Programmable Read Only Memory) que pode estar apagada (*erased*) ou não apagada (*non-erased*). Este tipo de memória utiliza atualmente a tecnologia NAND (Not AND) mas chegou a utilizar a tecnologia NOR (NOT OR).

Este tipo de memória guarda os dados como um vetor (*array*) de células. Uma célula é um transístor único que pode estar carregado com uma carga elétrica. Na memória flash mais antiga constituída por single-level cells (SLC), cada célula continha um bit (1 ou 0). De forma a aumentar a densidade e a capacidade da memória NAND, atualmente é utilizada outra tecnologia denominada de *multi-level cell* (MLC). Uma célula MLC consegue guardar 2 bits de dados numa única célula.

Para que seja possível guardar dados na célula, esta deve estar no estado apagada (*erased*). Quando são guardados dados, é aplicada tensão positiva. Para escrever dados sobre uma célula, primeiro a célula tem que ser apagada. A memória flash NAND permite apagar vários blocos de células de uma só vez (Fukami et al., 2017; Sammons, 2012).

Os dispositivos móveis denominados de "*feature phones*" dados chegaram a utilizar a tecnologia NOR para a memória de armazenamento interno. Os primeiros smartphones utilizavam a tecnologia NOR e NAND enquanto que os últimos já só utilizavam a tecnologia NAND (Ayers, Jansen, & Brothers, 2014).

2.2.5. Implicações da memoria flash a nível forense

Nesta subsecção abordamos algumas implicações forenses ao nível da memória *flash*.

Quando se fala deste tipo de armazenamento na análise forense digital anteveem-se alguns desafios dado que existem diferenças na forma de armazenamento dos dados (Sammons, 2012).

Do ponto de vista forense, ao fazer uma aquisição a este tipo de memória *flash*, pode ser feita aquisição via *software* ou caso haja dados danificados e a solução baseada em *software* não for suficiente, devem ser retirados os chips de memória para ser feita uma aquisição física (Fukami et al., 2017).

A seguinte lista apresenta alguns pontos especiais deste tipo de memória que pode trazer problemas do ponto de vista forense (Mary Mack & Pattison, 2017; Regan, 2009):

- O processo chamado de "*self-corrosion*" pode levar a que as provas existentes num dispositivo com este tipo de armazenamento possam ser permanentemente apagadas de uma forma tão rápida que um disco rígido não conseguiria apagar;

- Este tipo de armazenamento guarda os dados de uma forma muito mais complexa que outros tipos de armazenamento o que pode levar a que haja mais dificuldades em recuperar os dados.
- Algumas tecnologias mais antigas tinham um limite de ciclos de leitura e escrita mais baixo por célula o que podia levar à falha do suporte de dados .

2.3. Organização dos dados

Um ficheiro é considerado um conjunto de informação agrupado e referenciado por um nome único, o nome do ficheiro. Um ficheiro pode ser de vários tipos, pode ainda conter texto, uma imagem, um vídeo, ou uma aplicação (Sammons, 2012).

O aparecimento da internet, a maior utilização de dispositivos móveis e aplicações fez aumentar a quantidade e tipos de ficheiros usados para guardar dados. Existem uma série de dispositivos móveis como: PDA, telemóveis, smartphones, câmaras fotográficas, por sua vez estes dados são guardados na memória interna ou em cartões de memória que estendem a memória destes dispositivos.

Esta secção faz referência aos sistemas de ficheiros de dispositivos móveis dos sistemas operativo Android e iOS sendo que incide mais sobre este último uma vez que se relaciona com o tema do projeto.

2.3.1. Volumes e partições

Os dispositivos de armazenamento de dados usados para guardar dados não voláteis estão organizados em volumes. Um volume é um conjunto de localizações para armazenamento nos quais um utilizador pode ler ou escrever. Estes dispositivos são particionados, assim podemos dividir um volume em vários volumes mais pequenos (B. D. Carrier, 2005; Quick, Darren Alzaabi, 2011)

Segundo (B. D. Carrier, 2005), um volume é uma coleção de setores com respetivo endereço, que o sistema operativo ou aplicação conseguem usar para armazenar dados.

Uma partição é um conjunto de setores seguidos num volume. Podemos também considerar uma partição como um volume (B. D. Carrier, 2005).

Segundo o exemplo de (B. D. Carrier, 2005) a Figura 6 apresenta um exemplo para um sistema de ficheiros de um computador com o sistema operativo Windows. O disco rígido é um volume e está particionado em três volumes, cada um contém um sistema de ficheiros. Cada volume contém um nome, C, D e E.

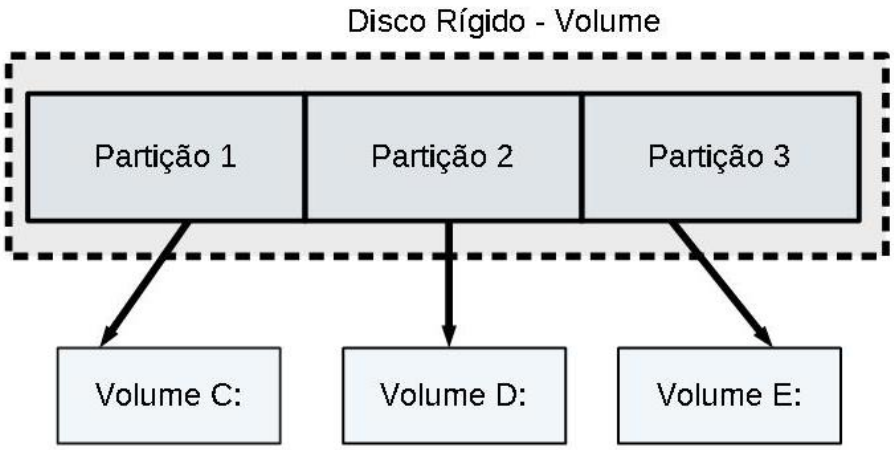


Figura 6 - Partições e volumes. Adaptado de: (B. D. Carrier, 2005)**.**

Segundo (Kent et al., 2006), Os dispositivos usados para guardar dados são particionados e formatados em volumes lógicos. O particionamento divide o dispositivo em partes lógicas que podemos associar como se tratassem de partes fisicamente separadas. Um volume é uma partição, ou conjunto de partições que funcionam como uma única entidade que foi formatada com o sistema de ficheiros. O formato dos volumes é determinado pelo tipo de sistema de ficheiros.

Do ponto de vista dos computadores, existem partições como as partições DOS (*Disk Opearting System*), mais conhecidas como MBR (*Master Boot Record*).

Do ponto de vista dos dispositivos de armazenamento amovíveis como por exemplo os cartões de memória, contém partições do tipo DOS, assim como os discos rígidos externos.

Os dispositivos móveis, como o android e iOS são baseados em Linux. No caso do Android pode estar particionado como no exemplo seguinte. Neste exemplo o sistema android contém 6 partições principais como apresentamos na seguinte lista (Wadhah R. Baiee, 2014):

- /boot;
- /system;
- /recovery
- /data
- /cache
- /misc
- /sdcard (para o cartão de memória)
- /sd-ext (para o cartão de memória)

A Figura 7 representa o exemplo de um sistema de partições android.

Figura 7 – Sistema de partições Android. Adaptado de : (Wadhah R. Baiee, 2014).

As partições dos dispositivos Apple com sistema operativo iOS são baseadas em unix. Estas partições estão descritas numa estrutura de mapa de partições (*partition map strucutre*), que está localizada no início do disco. Cada entrada no mapa de partições define o inicio do setor da partição, o tamanho, o tipo e o nome do volume. A Figura 8 apresenta um exemplo de um disco com sistema operativo iOS e as partições.

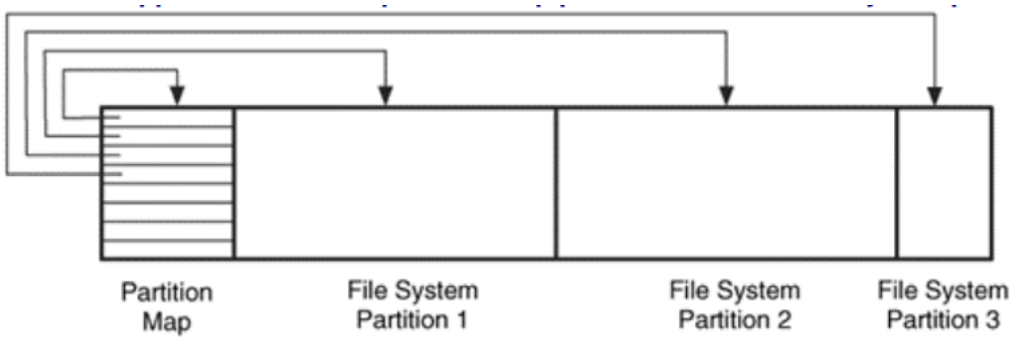


Figura 8 – Disco com sistema de partições de um sistema operativo iOS.

A Tabela 4 contém a informação contida num "*volume header file*".

Tabela 4 – Descrição do ficheiro de cabeçalho de um volume.

Signature	Este campo contém a assinatura do volume que deve ser "H+" se o sistema de ficheiros for HSF+ e "HX" se for HFSX.
Version	Versão do formato. 4 se for HFS Plus e 5 se for HFSX.
Atributes	Este campo contém os atributos do volume (se o "*journaling*" esta ativo).
lastmountedversion	Este campo descreve o sistema operativo instalado.
journalInfoBlock	Este campo contém o bloco de alocação que gere o "*journaling*".
createDate	Este campo contém a data de criação do volume.
modifyDate	Este campo contém a data de modificação do volume.
backupDate	Este campo contém a data de cópia ed segurança do volume.
checkedDate	Este campo contém a última verificação de consistência do volume.

fileCount	Este campo contém o número de ficheiros no volume, sem os ficheiros especiais.
folderCount	Este campo contém o número de pastas no volume, sem a pasta root.
blockSize	Este campo contém o tamanho de alocação dos blocos.
totalBlocks	Este campo contém o número de blocos alocados.
freeBlocks	Este campo contém o numero de blocos de alocação livres.
nextAllocation	Este campo contém o endereço do bloco de alocação seguinte.
rsrcClumpSize	Este campo contém o tamanho do conjunto para um recurso "*rasoure fork*".
dataClumpSize	Este campo contém o tamanho para um "resource fork".
nextCatalogID	Esse campo contém o primeiro "*Catalog ID*" disponível.
writecount	Este campo contém as vezes que o volume foi montado.
encodingsBitmap	Este mapa de bits descreve a codificação utilizada para um ficheiro e pasta.
finderInfo	Este campo contém informação utilizado pelo Mac OS e o processo de arranque de *software*.
allocationFile	Este campo contém a localização e o tamanho do ficheiro de alocação.
extentsFile	Este ficheiro contém a localização e o tamanho do ficheiro "extintos".

catalogFile	Este campo contém a localização e o tamanho do ficheiro de catalogação.
attributesFile	Este campo contém a localização e o tamanho do ficheiro de atributos.
startupFile	Este campo contém a localização e o tamanho do ficheiro de arranque.

O ficheiro de alocação (*catalog file*) é utilizado para manter informação da hierarquia de ficheiros e pastas no sistema de ficheiros HFS+.

Segundo (Epifani & Stirparo, 2015) os dispositivos móveis Apple estão divididos em duas partições, a de sistema (*System or firmware partition)* e a de dados (*data partition*).

A partição de sistema contém o sistema operativo iOS e as aplicações instaladas. O utilizador não tem permissão de escrita nesta partição.

A partição de dados ocupa mais espaço que a partição de sistema. Contém os dados dos utilizadores, dados das aplicações instaladas pelo utilizador e está montada em /private/var.

A Figura 10 mostra o exemplo de uma partição de sistema (*System Partition)* de um iPhone.

A partição de dados foi alterando a sua estrutura ao longo das várias versões de iOS. A Figura 10 apresenta uma partição de dados para o iOS 7.0.4.

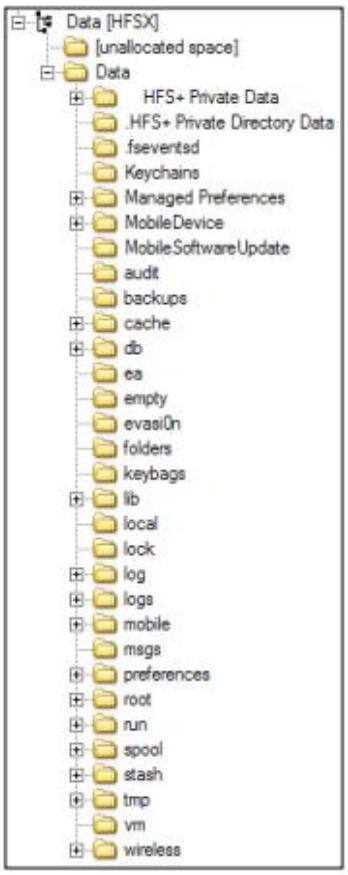


Figura 10 – Partição de dados (Data partition)

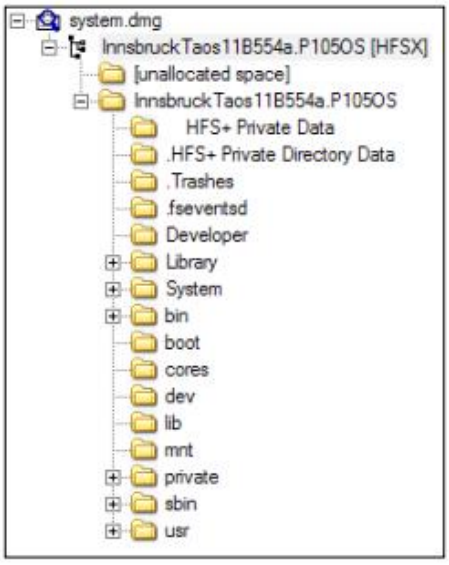


Figura 9 - Partição de sistema (*System partiton*).

2.3.2. Sistemas de Ficheiros

O sistema de ficheiros define a forma como os ficheiros estão nomeados, organizados, armazenados e acedidos em volumes lógicos. O sistema de ficheiros gere o espaço livre, o espaço ocupado assim como a localização de cada ficheiro. Apesar das diferenças dos sistemas de ficheiros, existem conceitos semelhantes entre os mesmo como as pastas e os ficheiros.

Nos computadores existem os seguintes sistemas de ficheiros: FAT (*File allocation table*), NTFS (*The new technology file system*), HFS (*Hierarchical File System*), ext2fs (*Second extended file system*), ext3fs (*third version extended file system*) e ext4fs (*fourth version extended filesystem*).

Os dispositivos móveis com sistema operativo android, são baseados em Linux. Existe uma abstração chamada *Virtual File System* (VFS) que permite gerir todos os sistemas de ficheiros diferentes existentes num dispositivo. Todos os sistemas de ficheiros são implementações do VFS. Os sistemas de ficheiros utilizados são os da seguinte lista (Bill Anderson, 2017):

- exFAT (*Extended file allocation* table) - Sistema de ficheiros proprietário da Microsoft para memória flash, apesar de não fazer parte do kernel do Linux, o android suporta este sistema de ficheiros;
- F2FS (Flash-fiendly file system) - Sistema de ficheiros *open source* introduzido pela Samsung;
- JFFS2(*Journal Flash File System version 2*) - Sistema de ficheiros por defeito para memória flash do *Android Open Source Project* (AOSP) que veio substituir o JFFS, versão antes do JFFS2;
- YAFFS2 (*Yet Another Flash File System version 2*) - Sistema de ficheiros usado até ao *kernel* 2.6.3.2 mas que que atualmente não é suportado.

O android suporta também os seguintes sistemas de ficheiros (Quick, Darren Alzaabi, 2011; Wadhah R. Baiee, 2014):

- MSDOS – Que suporta os sistemas de ficheiros FAT12, FAT16 e FAT32 (*File allocation table*);

- VFAT (*Virtual File Allocation table*) é uma extensão dos sistemas de ficheiros FAT12, FAT16 e FAT32. Alguns cartões de memória podem vir com este formato.
- EXT2 EXT3 e EXT4 (Extended *File System*) – Sistema de ficheiros standard do Linux. Desde 2010 que o EXT4 é usado para substituir o YAFFS2 e o JFFS2 nos dispositivos android;

Segundo (Epifani & Stirparo, 2015), os dispositivos iOS utilizam o sistema de ficheiros HFSX (*Hierarchical File System*) que é baseado no sistema de ficheiros HFS+ e por sua vez uma evolução deste. O sistema de ficheiros HFS+ é uma evolução do HFS, criado em 1996. Foi o sistema de ficheiros inicialmente criado para os computadores Apple.

O HFS+ é uma versão melhorada do HFS, que permite ao utilizador trabalhar com ficheiros que alocam mais espaço, tudo isto graças ao suporte de blocos de 32 bits em vez dos antigos 16 bits do HFS e ao uso de Unicode para os nomes dos ficheiros que permite até 255 caracteres. As permissões dos ficheiros são baseadas em ACL (*Access Control List*).

O sistema de ficheiros HFS+ trabalha com alocação em blocos que pode conter um ou mais setores, tipicamente 512bytes num disco rígido normal. O número de blocos de alocação depende do tamanho do volume. O HFS+ utiliza 32 bits para endereçar os blocos.

Os dados no sistema de ficheiros HFS são organizados segundo um ficheiro de catalogação ou um sistema denominado de B*tree, *balanced tree* (árvore equilibrada). Este esquema em árvore usa um ficheiro de catalogação e são constituídos por vários nós. Estes nós tornam os dados mais fáceis de aceder. Cada ficheiro que é criado contém um número único denominado de "*catalog ID number*" que lhe é atribuído. O número é gerido pelo cabeçalho do volume do sistema de ficheiros (*HFS Volume Header*) (B. D. Carrier, 2005; Epifani & Stirparo, 2015).

A Figura 11 ilustra a estrutura do sistema de ficheiros HFS.

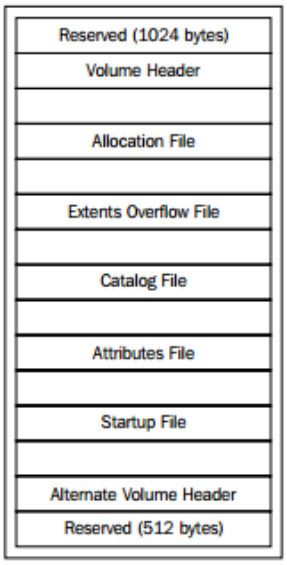


Figura 11 - Estrutura do Sistema de ficheiros HFS. Retirado de:(Epifani & Stirparo, 2015; Morrissey, 2010)**.**

A seguinte lista caracteriza um volume do sistema de ficheiros HFS+ e descreve a Figura 11.

- Os primeiros 1024 bytes são reservados para blocos de arranque (*boot blocks*);
- (*Volume header*) Ficheiro de Cabeçalho do volume – Constituído por 1024 bytes define a estrutura do volume, o tamanho de cada bloco alocado, o número de blocos usados e blocos livres e o tamanho/posição de outros ficheiros especiais;
- (*Allocation File*) Ficheiro de alocação – Este ficheiro inclui um mapa com os blocos usados e os blocos livres de cada volume;
- (*Extents overflow file*) - Este ficheiro contém ponteiros para extensões adicionais, para ficheiros que requerem mais do que 8 blocos de alocação;
- (*Catalog File*) Ficheiro de catalogação – Este ficheiro define a estrutura das pastas no sistema de ficheiros e é usado para identificar a localização de um ficheiro ou pasta. É guardado também o número único atribuído a cada ficheiro;
- (*Attributes file*) Ficheiro de atributos – Este ficheiro contém os atributos configuráveis para um ficheiro;

- (*Startup file*) Ficheiro de arranque – Este ficheiro contém informação importante para o arranque;
- (*Alternate volume header*) – Contém uma cópia co cabeçalho do volume usada para reparar o disco;
- Os últimos 512 bytes são reservados.

Todos os dispositivos móveis Apple utilizam o HFSX como sistema de ficheiros. O HFSX é uma variação do HFS+ e contém uma diferença importante, é sensível a letras maiúsculas e minúsculas (*Case sensitive*). O que significa que podem haver ficheiros com o mesmo nome, mas com diferenças nas letras do nome em termos de maiúsculas e minúsculas.

As partições existentes são essencialmente duas, a partição de sistema operativo (*os* partition) e a partição para os dados (*data partition*). A Figura 12 ilustra as duas partições de um iPhone (Epifani & Stirparo, 2015; Morrissey, 2010).

Figura 12 – Esquema de partições do iOS. Adaptado de: (Morrissey, 2010)**.**

A linha de comandos "Hdiutil" permite ver a estrutura de partições do iPhone.

A partição do sistema operativo (*os partition*) é um volume que apenas permite leitura. Acendo a /private/etc/fstab através de um editor de texto, podemos visualizar a informação da Figura 13.

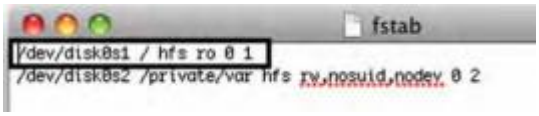


Figura 13 – Partições do iPhone e respetivas informações. Retirado de: (Morrissey, 2010)**.**

Segundo a Figura 13,o armazenamento do iPhone está identificado como "Disk0", sendo que a partição do sistema operativo está identificada como "Disk0s1" e a partição de dados identificada como "Disk0s2". A informação começa por mostrar o caminho para a partição, /dev/disk01s e /dev/disk02s respetivamente, depois está identificado o ponto de montagem / e /private/var respetivamente, o sistema de ficheiros "hfs" e as permissões de leitura e escrita. Neste caso "ro" significa *read-only* (permissões de leitura) e "rw" significa *read-write* (permissões de leitura e escrita).

Na partição do sistema operativo, os dados não estão visíveis dado que a partição é apenas de leitura a não ser que o dispositivo esteja desbloqueado (*jailbreak*). Caso a partição de sistema operativo apresente a informação "rw" significa que o dispositivo está desbloqueado.

A Figura 14 apresenta o exemplo da estrutura de uma partição de sistema operativo do iOS de um iPhone. Por norma o conteúdo desta partição não está visível.

Figura 14 -Partição de sistema do iOS. Retirado de: (Quick, Darren Alzaabi, 2011)

A Tabela 5 descreve a partição do sistema operativo (*iOS System partition*).

Tabela 5 – Descrição das pastas da partição de sistema do iOS. Baseado em: (Morrissey, 2010)**.**

Pasta	Descrição
Applications	Atalho (link simbólico) que aponta para a pasta /var/stacsh que contém as aplicações.
Etc	Atalho (link simbólico) que aponta para a pasta /private/etc Contém ficheiros fstab, master.passwd e ficheiros passwd. private/etc/passwd é o ficheiro de palavras-passe do sistema operativo.
Tmp	Atalho (link simbólico) que aponta para a pasta tmp.
User	Atalho (link simbólico) que aponta para a pasta user.
Var	Atalho (link simbólico) que aponta para /private/var.
Cores	Pasta Vazia
Dev	Pasta Vazia
Developer	Pasta Vazia
Library	Contém os plug-ins de sistema e algumas configurações de sistema.
private	Contém as pastas etc e var.
sbin	Contém binários da linha de comandos.
System	Contém configurações e preferências de sistema. Contém o ficheiro SystemVersion.plist que contém a versão de *Firmware*.

Usr	Contém binários da linha de comandos e a data e hora.

Partição de dados do iOS

A partição de dados tem sofrido alterações dado a evolução do iOS. É possível verificar essas diferenças nas aquisições lógicas que são efetuadas. Os dados possíveis de obter vêm desta partição que tem permissões de leitura e escrita como referido anteriormente.

A Figura 15 apresenta a estrutura de uma partição de dados do iOS de um iPhone.

Figura 15 – Estrutura da partição de dados.

A Tabela 6 descreve as pastas mais importantes existentes na partição Data.

Tabela 6 – Descrição de parte das pastas existentes na partição de dados.

Dhcpclient	Contém um ficheiro .plist que contém o endereço IP e informação de rotas para o dispositivo.
Keychains	Contém ficheiros como keychain.db com palavras-passe de várias aplicações.
Logs	Contém registos com a versão de sistema operativo e número de série, entre outros dados.
Mobile	Contém dados dos utilizadores
Preferences	Configuração do dispositivo e dados de rede
Root	Pasta caches – Com dados de GPS
Run	Registos do sistema

Segundo (RENE RITCHIE, 2017) o APFS (*Apple File System*) é um sistema de ficheiros, anunciado em 2016, que tem por objetivo substituir o HFS+ para todos os dispositivos Apple. O HFS já existe desde 1985 e o HFS+ desde 1998. Surgiu a necessidade de fazer melhorias. O HFS+ corre em todos os dispositivos Apple, mas existem diferenças na implementação dos mesmos. O APFS tem por objetivo funcionar de forma mais consistente em todas as plataformas Apple, trazer novas funcionalidades e estar otimizado para o hardware existente.

Segundo (Elizabeth Jones, 2017), este sistema de ficheiros pode ser encontrado no iOS 10.3. Segundo o autor apresentamos algumas vantagens do novo sistema de ficheiros na seguinte lista:

- Otimização para a memória flash usada em todos os dispositivos Apple;
- Melhor gestão do espaço utilizado;
- Aplicações com mais eficiência na abertura e fecho;

- Melhor eficiência na cópia de ficheiros;
- Uniformidade na implementação entre todos os dispositivos Apple;
- Encriptação dos dados.

Data persistence

Os dados guardados num dispositivo de armazenamento podem ser considerados persistentes e pode não ser fácil apagar os mesmos. Os dados apagados podem continuar a existir até serem substituídos, até o dispositivo escrever dados na localização dos antigos, o que pode levar bastante tempo. O sistema de ficheiros é considerado como um índice, sabendo a localização de todos os ficheiros. Ao apagar um ficheiro seria como apagar esse ficheiro do índice de ficheiros, no entanto o ficheiro pode continuar a existir no dispositivo de armazenamento. Os ficheiros que são sobrepostos, podem ser considerados perdidos, no entanto existem algumas exceções, como por exemplo, caso, ao escrever, o novo ficheiro não ocupe todo o espaço do antigo ficheiro, podem ficar ainda partes do ficheiro antigo que podem ser recuperadas. Este espaço não ocupado pelo novo ficheiro e que ainda contem "restos" do antigo ficheiro é denominado de *Slack Space*.

2.3.3. Representação dos dados

O conhecimento da representação dos dados é importante para a análise digital forense. Dessa forma é possível obter melhores resultados e uma melhor análise das provas para alcançar conclusões precisas. A memória e o armazenamento são os componentes mais importantes deste tipo de análises.

Os dados são representados como 1s e 0s. A linguagem usada é chamada de binária. Nesta linguagem apenas existem duas saídas possíveis, 1 ou 0. Cada 1 ou 0 é chamado de bit em termos matemáticos. Em comparação por norma usamos o sistema numérico de base 10, denominado de decimal que usa números de 0 a 9. Para melhorar as capacidades os dispositivos trabalham com grandes quantidades de bits. Estes grandes blocos de dados são chamados de bytes. Um byte é constituído por 8 bits.

Como é possível os bytes representarem letras e números? Cada letra, número, espaço e caracter especial é representado por um único byte. Por exemplo, usando a representação ASCII o conjunto de caracteres 01000001 é representado pela letra "A" maiúscula, enquanto o conjunto de caracteres 01100001 representa a letra "a" minúscula.

File Carving

Na ciência digital forense, os examinadores podem ter que analisar os dados "bit a bit" ou "byte a byte" para encontrarem informação relevante e poder extrair e analisar provas. File carving é um procedimento usado para localizar e descobrir ficheiros que podem estar mais ocultos, tais como o espaço não alocado. O ficheiro é, por norma, identificado pelo seu cabeçalho caso este cabeçalho exista. Quando o final do ficheiro é encontrado, os dados podem ser extraídos e copiados para outra localização. Um ficheiro fragmentado é mais difícil de recuperar. Este processo só é possível se houver capacidade para interpretar ficheiros binários e hexadecimais (Sammons, 2012).

Extensões de ficheiros e assinaturas dos mesmos

Essencialmente, os ficheiros são constituídos por carateres, ou sequências de bits e bytes. Identificar um ficheiro pode ser feito de diversas formas. Por norma os ficheiros têm extensões. As extensões dos ficheiros são sufixos acrescentados ao final do nome do ficheiro, indicando o seu formato. Exemplos de duas extensões num dispositivo móvel podem ser ".jpg" e ".db", correspondentes a uma imagem e a um ficheiro de base de dados respetivamente.

Os utilizadores identificam os tipos de ficheiros pelas suas extensões caso o sistema esteja bem configurado, mas a interpretação do sistema operativo pode não corresponder ao conteúdo do ficheiro se este tiver a sua extensão alterada.

Do ponto de vista das ciências digitais forenses, as extensões de ficheiros não são as melhores formas de identificar um ficheiro uma vez que as extensões podem ser mudadas facilmente. Dessa forma é possível ocultar dados que estão à vista do utilizador. Algumas ferramentas forenses podem dar a volta a este problema, baseando-se nos cabeçalhos dos ficheiros e não na sua extensão, identificando assim os ficheiros com extensão modificada por exemplo. Este género de comparação é chamado de "*file signature analysis*" Análise da assinatura digital do ficheiro. A Figura 16 e Figura 17 mostram exemplos de uma extensão de ficheiro original e alterada respetivamente, num computador (Sammons, 2012).

Figura 16 - Ficheiro original em formato Microsoft Word

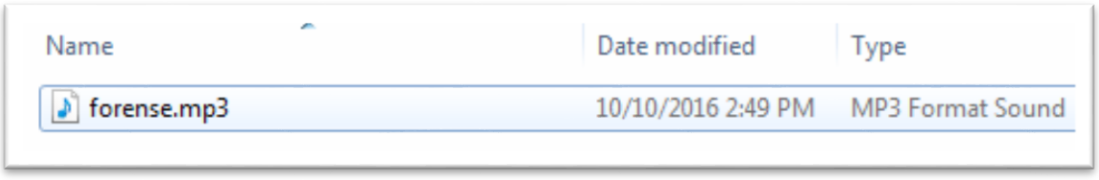


Figura 17 - Ficheiro com extensão modificada

Como podemos verificar na Figura 16 e na Figura 17 foi possível modificar a extensão do ficheiro de extensão .docx correspondente a um ficheiro Microsoft office word, para extensão .mp3 correspondente a um ficheiro de música. O sistema operativo

interpretou o ficheiro dada a sua nova extensão, no entanto o conteúdo continua o mesmo.

A Figura 18 apresenta 4 ficheiros, forense.mp3 e forense 1.jpeg cujas extensões foram alteradas com base no ficheiro forense 2 em formato "word document". O ficheiro de imagem "Photo" encontra-se sem alteração de extensão.

Figura 18 – Ficheiros com extensão alterada em iPhone.

Dessa forma e como apresentado na Figura 18 foi também possível copiar ficheiros com a extensão alterada para o iPhone.

Utilizando *software* que interpreta o ficheiro com extensão alterada podemos verificar que tipo é o ficheiro. Na Figura 19 podemos ver um exemplo de ficheiro que está identificado como "word/document.xml".

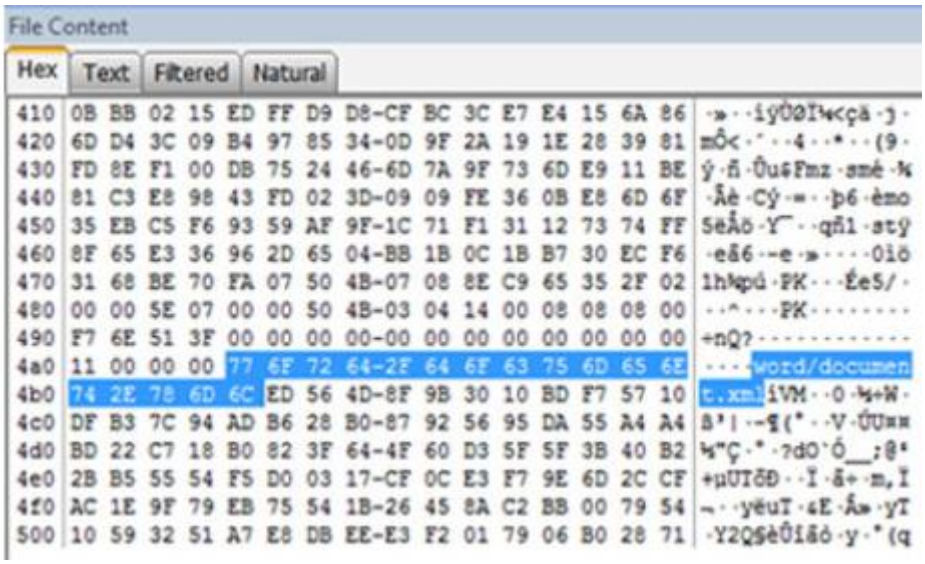


Figura 19 - Leitura de um ficheiro com extensão alterada para detetar o seu tipo. Retirado de (Sammons, 2012)**.**

2.3.4. Metadados

Os metadados são informações associadas a um dado ficheiro que podem ser obtidas pelo utilizador. Podem incluir uma série informações. Segundo (Whatson & Jones Andrew, 2013) podem conter os dados da Tabela 7:

Tabela 7 - Conjunto de dados possíveis de existir nos metadados.

• Atributos; • Autor; • Categoria; • Quantidade de carateres; • Comentários; • Entidade / Empresa; • Data de criação; • Data a que foi acedido; • Data de modificação;	• Última vez que foi gravado; • Tipo de ficheiro; • Nome do ficheiro; • Localização; • Data que foi imprimido; • Chave criptográfica MD5 ou SHA; • Número de páginas; • Versão;

2.4. Dispositivos Móveis e suas características

No mundo atual, existe uma enorme quantidade e variedade de dispositivos móveis. Desde os telemóveis simples (*feature phone*), aos smartphones, tablets, GPS, câmaras fotográficas, os chamados "*wearables*" (Pulseiras, *smartwatch*), entre outros. Além da variedade existem uma série de fabricantes diferentes. Um smartphone por exemplo tem uma série de características e pode ser aproveitado com um conjunto de aplicações que aproveitam as características dos mesmos.

Em seguida apresentamos a relação entre os dispositivos móveis e análise forense, códigos identificadores dos dispositivos, diferentes tipos de sistemas operativos e algumas características e capacidades dos dispositivos móveis.

2.4.1. Dispositivos Móveis e a Análise Forense

A análise forense de dispositivos móveis estuda a parte dos dispositivos móveis envolvidos em crimes. Segundo (Lin, Chao, & Peng, 2011) a NIST definiu análise forense de smartphones como a necessidade do uso de métodos apropriados para obter provas digitais de dispositivos móveis como é o caso do smartphone.

Esta área tem evoluído bastante nos últimos tempos e continua em rápida evolução, fazendo com que os responsáveis tenham de se atualizar constantemente dado que saem constantemente novos equipamentos todos os anos. O que diferencia a análise forense de dispositivos móveis em comparação com os computadores é que na primeira um dispositivo móvel pertence apenas a uma pessoa enquanto que um computador pode ser utilizado por várias. Sendo assim um dispositivo móvel é provável que tenha mais dados pessoais.

Os dispositivos móveis são um novo desafio do ponto de vista da análise forense uma vez que cada vez existem mais modelos de dispositivos móveis, nomeadamente *smartphones*. Com a grande quantidade de equipamentos é impossível haver uma solução ou até ferramentas que permitam analisar todos estes dispositivos do ponto de vista forense (Sammons, 2012).

As aplicações, que quando instaladas, permitem aumentar as funcionalidades destes dispositivos, estão disponíveis nas lojas online e são cada vez em maior quantidade. Passando pelos clientes de troca de mensagens, IM (*Instant Messaging*), *browsers* para acesso à internet, redes sociais, aplicações para navegação em mapas, jogos entre outros. A sincronização entre o telemóvel e o computador ou *cloud* tornou-se também uma funcionalidade comum nos tempos atuais.

Para além da diversidade de equipamentos existe também uma grande quantidade de sistemas operativos como o iOS da Apple, o Android da Google, o Blackbery OS da Blackiberry, o Windows Phone da Microsoft e ainda alguns sistemas operativos mais antigos utilizados por telemóveis descontinuados.

Atualmente, os smartphones conseguem ser utilizados mesmo sem cartão SIM (*subscriber identity module*) (Sammons, 2012).

Numa análise a um smartphone podemos encontrar mensagens de texto (SMS), mensagens multimédia (MMS), imagens, vídeos, aplicações instaladas, e-mails, dados de localização, dados recebidos por Bluetooth, dados relativos ao histórico da internet ou a redes a que o utilizador esteve ligado, dados relativos a chamadas entre outros.

2.4.2. Identificadores dos dispositivos

Os dispositivos contêm uma série de códigos. Nesta subsecção identificamos os códigos mais importantes.

Todos equipamentos contém o IMEI ("*International Mobile Equipment Identifier*"). Este código de 15 dígitos identifica o dispositivo unicamente, assim como na rede. Este identificador, por norma, está localizado detrás da bateria. Este código pode também ser acedido pelo código "*#06#" no dispositivo. Na Figura 20 podemos ver a divisão do IMEI em vários códigos.

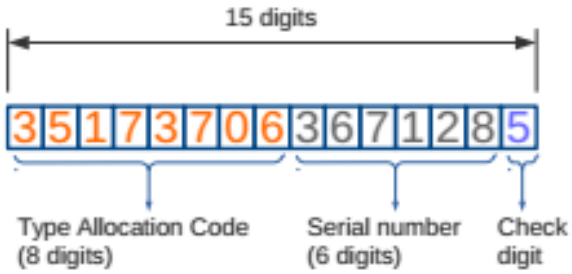


Figura 20 – Composição do código que inclui o IMEI Fonte: (Frade, 2016).

Da esquerda para a direita, o código designado por TAC (*Type Allocation Code*), o número de série (*Serial number*) e um digito de verificação (*Check Digit*). O TAC é um código de 8 dígitos, parte inicial do IMEI e é utilizado para identificar dispositivos com *Wi-Fi* (Epifani & Stirparo, 2015; Frade, 2016).

UDID (*Unique Device Identifier*)

Cada dispositivo Apple é constituído por um UDID (*Unique Device ID*) que o identifica. Este código resulta num conjunto de 59 ou 60 caracteres descritos na seguinte lista (Epifani & Stirparo, 2015; Sammons, 2012).

- Um número de série constituído por 11 ou 12 caracteres nos novos dispositivos;
- O IMEI (*International Mobile Equipment Identity*), constituído por 15 caracteres ou 13 caracteres ECID (*Eletronic Chip ID*) em decimal;
- O endereço físico, denominado "*MAC Address*" da placa Wi-Fi, constituído por 17 caracteres,
- O Endereço físico, denominado "*MAC Address*" da placa Bluetooth constituído por 17 caracteres.

2.4.3. Sistemas Operativos

Existe uma grande quantidade de sistemas operativos em dispositivos móveis. Alguns sistemas operativos mais conhecidos são o Android da Google, o IOS da Apple, o Windows mobile da Microsoft, o Blackberry OS e o Symbian da nokia. No projeto irá ser focado o sistema operativo IOS. A Figura 21 mostra alguns exemplos.

Figura 21 – Sistemas Operativos de dispositivos móveis, Fonte: (Epifani & Stirparo, 2015)

Android

O Android foi comprado pela Google em 2005. Mais tarde, em 2007 foi formada a Open Handset Alliance. Esta empresa era constituída por 84 empresas de tecnologia móvel que procuravam melhorar a qualidade a e experiência dos utilizadores. Alguns membros são a T-Mobile, a LG Eletronics, a Asus Motorola, a Google entre outros. O sistema operativo Android passou a ser instalado numa série de equipamentos móveis e atualmente vai na versão 7.0 (Sammons, 2012).

iOS

O iOS (iPhone Operating System) é o sistema operativo da Apple desenvolvido para os seus dispositivos móveis como o iPhone, iPad, iPod e IWatch. Este sistema operativo foi apresentado em janeiro de 2007. É baseado no sistema operativo MAC OS X que é utilizado nos computadores portáteis e de secretária da Apple que por sua vez deriva do BSD (*Berkeley Software Distribution)* unix e com kernel do Darwin OS (Epifani & Stirparo, 2015).

A Tabela 8 apresenta algumas versões do sistema operativo iOS, o nome de código e a respetiva data de lançamento.

Tabela 8 – Algumas versões do sistema operativo iOS e respetivos nomes de código e datas de lançamento Adaptado de:(Hotz, 2017b; Ritchie, 2017) **.**

Versão de sistema operativo iOS	Nome de código	Data de lançamento
1.1.1	Little Bear	Setembro de 2007
2.2.1	Timberline	Janeiro de 2009
3.1.3	Northstar	Fevereiro de 2010
4.2.1	Jasper	Novembro de 2010
5.1.1	Hoodoo	Maio de 2012
6.1.6	Brighton	Fevereiro de 2014
7.1.2	Sochi	Junho de 2014
8.4.1	Copper	Agosto de 2015
9.3.5	Eagle	Agosto de 2016
10.3.3	Erie	Julho de 2017
11 Beta	Tigris	Agosto de 2017

No âmbito deste projeto são utilizados dispositivos Apple, IPhone, que usam o sistema operativo iOS.

2.4.4. Cartão SIM

O cartão SIM, (*Subscriber Identity Module)* ou também denominado de UICC (*Univesal Integrated Circuit Card*) que é a parte física do cartão, permite aos dispositivos estabelecerem uma ligação à rede móvel para dessa forma a efetuarem comunicações. Estes cartões contêm dois componentes importantes: O processador e o armazenamento. O armazenamento pode ir desde 16 a 64 KB, mas existem casos com 1GB.

Quando se trata de análise forense de dispositivos móveis é importante analisar os cartões SIM, uma vez que podem conter provas importantes que podem ser recolhidas e analisadas. De notar que existem muitos dispositivos com capacidade para dois cartões SIM (Epifani & Stirparo, 2015).

O cartão SIM existe nos seguintes formatos como mostra a Tabela 9.

Tabela 9 - Lista com os tipos de cartões SIM Fonte: (Frade, 2016)**.**

Tipo de cartão	Data de lançamento	Medidas
1FF	1991	85.6x53.98
2FF	1996	25.0 x 15.0
3FF	2003	15.0x12.0
4FF	2012	12.3x 8.8

A Figura 22 complementa a informação da Tabela 9 com as dimensões dos cartões SIM.

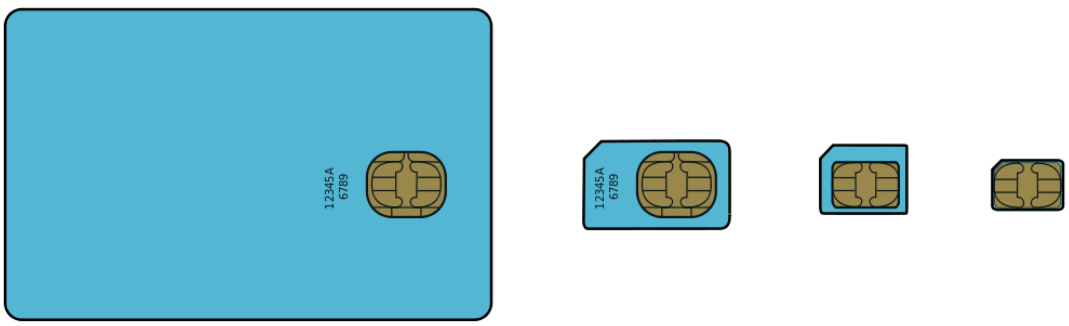


Figura 22 - Dimensões dos cartões SIM, Fonte: (Frade, 2016)

O cartão SIM contém um conjunto de códigos, o ICC-ID (*Integrated circuit Card Identifier*), o IMSI (*International Mobile Subscriber Identity*) e o MSISDN (*Mobile Station International Subscriber Directory Number)* que são devidamente identificados em seguida.

ICC-ID

O ICC-ID é o número de série do cartão SIM. É um código não editável, constituído por 19 ou 20 dígitos que identifica o cartão sim internacionalmente. Este código identifica também o operador da rede e o país em questão. O código pode estar impresso no cartão, assim como registado digitalmente dentro do mesmo (Frade, 2016; Sammons, 2012).

O ICCID é constituído pelos seguintes 5 códigos apresentados também na Figura 23:

- (MII) *Major Industry ID*– Identificador da indústria de telecomunicações;
- *Country code* – Código do Pais;
- *Provider ID* - Identificador do fornecedor do serviço;
- *Individual account ID* – Identificador da conta de utilizador;
- *Luhn check digit* – Digito final de verificação.

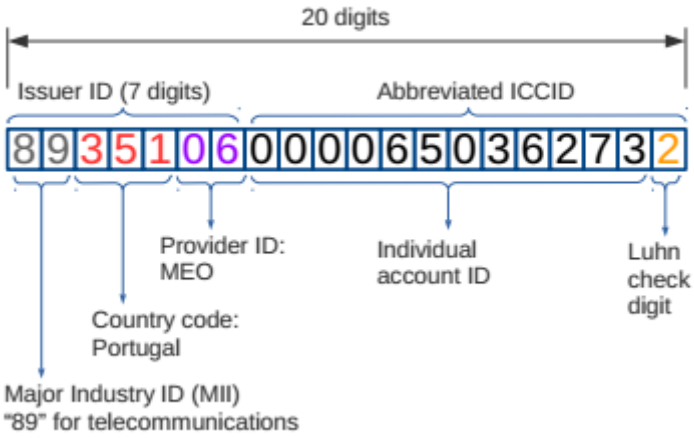


Figura 23 – Constituição do código ICCID, Fonte: (Frade, 2016).

IMSI

O IMSI é um código não editável que contém 15 dígitos e identifica o utilizador na rede móvel a que está ligado. Este código está registado digitalmente no cartão (Frade, 2016).

O código IMSI é constituído por 3 códigos:

- MCC (*Mobile Country Code*) – Código de identificação do país (268 corresponde a Portugal);
- MNC (*Mobile network code*) - corresponde ao código da rede móvel (MNC 01 Vodafone, 03 Nos e 06 à MEO);
- MSIN (*Mobile Subscription Identification Number*) código que identifica a subscrição do utilizador (Frade, 2016).

A Figura 24 Ilustra a composição deste código.

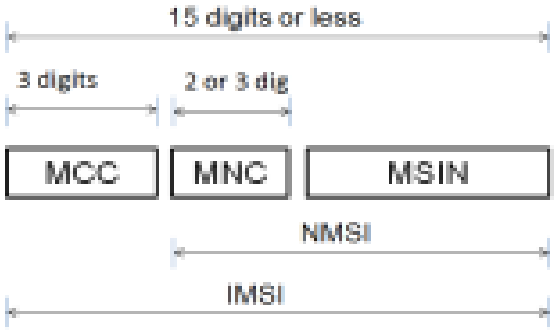


Figura 24 – Composição do código IMSI, Fonte: (Frade, 2016)**.**

MSISDN

O MSISDN (*Mobile Station International Subscriber Directory Number*) É o número de telemóvel associado ao cartão. Os cartões SIM podem guardar um ou mais números de telemóvel. Sendo que este número pode ser alterado no cartão (Frade, 2016).

Segurança dos cartões SIM

Do ponto de vista da segurança, os cartões SIM utilizam uma chave de autenticação (*Authentication key*) para se identificarem e ligarem à rede. Esta chave é atribuída pelo operador durante o processo de fabrico, não pode ser alterada e é também guardada do lado da operadora. A cada cartão está associado a uma conta do lado da operadora para controlo de custos.

Os dispositivos são protegidos pelos códigos PIN (Personal Identification Number) e PUK (Personal Unlock Key).

O PIN serve para o utilizador se autenticar. Caso seja inserido incorretamente três vezes é necessário o código PUK para o desbloquear. Este código pode ser alterado.

O código PUK é impossível de alterar e está limitado a 10 tentativas. Para situações em que seja necessário a análise do cartão SIM, os operadores de rede são obrigados a fornecer o código PUK. Se as 10 tentativas forem ultrapassadas o cartão fica completamente inutilizável (Sammons, 2012).

Em resumo, o cartão sim contém duas funções importantes:

- Autenticação: A rede móvel usa mecanismos de segurança para permitir o aceso à rede.
- Conta: O cartão SIM contem uma referência única que identifica o cartão SIM na operadora.

Cartão SIM do ponto de vista forense

Do ponto de vista forense os cartões SIM podem guardar informação importante, nomeadamente texto, mensagens, contactos, e dados de localização (onde estiveram ligados) que podem servir como provas.

É importante ler o cartão SIM, uma vez que este pode conter dados do utilizador associados a vários dispositivos, e também guardar os códigos ICCID e IMSI.

É importante referir que alguns dispositivos, se detetarem uma troca de cartão SIM, podem apagar todos os registos que tem.

A maior parte dos smartphones funciona sem um cartão SIM instalado, e alguns usam apenas o cartão para guardar contactos ou efetuar a ligação à rede (Frade, 2016; Sammons, 2012).

2.4.5. Serviço de Mensagens

Os telemóveis suportam dois tipos de mensagens, SMS (*Short Message Service*) e MMS (Multimedia *Messaging Service*), que podem ser trocadas entre dispositivos ligados à rede móvel.

As SMS são conhecidas como as tradicionais mensagens de texto. Estas mensagens tem um limite de 160 caracteres e podem ser divididas em várias quando são enviadas. Antes da utilização da internet era esta a forma de comunicação mais usada.

As mensagens MMS permitem que sejam enviadas mensagens de maior tamanho que as SMS e anexos multimédia como som, imagem ou vídeo.

2.4.6. GPS

O GPS (*Global Positioning Systems*) permite que os dispositivos sejam localizados, a navegação por mapas assim como agregar dados de localização a outros tipos de dados como por exemplo as imagens. Os dispositivos, nomeadamente smartphones, tem a capacidade de agregar dados de localização a determinados ficheiros, nomeadamente fotografias. Do ponto de vista forense. os dados de GPS podem trazer inúmeras provas que podem vir a ser úteis.

Os dados de GPS podem ser divididos em duas categorias. Dados do sistema e dados do utilizador. Os dados do sistema guardam pontos de localização assim como um possível registo dos locais onde passou determinado utilizador (*Track Points*). Estes pontos de utilização são automaticamente criados pelo sistema. Como dados do utilizador podemos considerar os (*WayPoints*), dados criados pelo utilizador ou os pontos de interesse, POI (*Points of interest*). Neste caso, estes pontos de localização podem indicar localizações que o utilizador pesquisou numa determinada aplicação (Sammons, 2012).

Apesar dos sinais de GPS nos fornecerem a localização, temos de considerar que o GPS é sensível a determinados fatores como edifícios, determinados materiais que refletem os sinais e até mesmo às condições atmosféricas. Por vezes os GPS podem dar erros na localização (Frade, 2016).

A latitude e a longitude são o sistema de coordenadas mais utilizadas para localizar objetos (McNamara, 2004).

As coordenadas de latitude e longitude podem ser escritas das seguintes formas:

Graus, minutos e segundos: DDDº MM' SS. s"

Este formato é usado maioritariamente para marcar os mapas. É o formato de coordenada mais complexo.

Exemplo:43º 23' 24,34" N 125º 25' 32,11" W

Graus e minutos decimais: DDDºMM.MMM'

Os segundos são colocados de parte e a parte decimal dos minutos é usada com os graus.

Este formato é mais utilizado nos equipamentos de navegação.

Exemplo: 65º 17.432' N 122º 43.221' W

Graus: DDD.DDDDDº

Neste formato apenas são contemplados os graus. É usado em todos os mapas utilizados em dispositivos digitais, nomeadamente computadores.

Exemplo: 32.3456321º N 21.2376321º W

2.5. Dispositivos móveis Apple

Nesta secção são apresentados os dispositivos móveis da Apple.

Os dispositivos móveis da Apple utilizam o sistema operativo iOS. Existe uma gama de dispositivos móveis, desde o iPhone, o iPad, o iPadMini e o iPod. O dispositivo que irá ser utilizado no projeto é o iPhone (Epifani & Stirparo, 2015).

Em baixo, na Figura 25 estão apresentados 3 tipos de dispositivos móveis Apple. Da esquerda para a direita um iPod, um iPhone, um iPad na Figura 26 um iWatch.

Figura 25 – Dispositivos móveis Apple. Fonte: http://www.datarescuelabs.com/data-security/iphone-data-recovery/

Figura 26 iWatch Fonte: https://www.apple.com/shop/buy-watch/apple-watch.

iPhone

O iPhone é o smartphone da Apple que corre o sistema operativo iOS. O primeiro iPhone foi lançado em junho de 2007 e está neste momento na sua versão 7 lançada em setembro de 2016.

O iPhone, é identificado pelos seguintes 5 códigos (Epifani & Stirparo, 2015):

- Número de série;
- Identificador do dispositivo (*Device iD*);
- IMEI;
- Identificadores de rede;
- Endereço Físico (*Mac-Address*) da Placa Wi-Fi;
- Endereço físico da placa Bluetooth.

O anexo "Anexo D – Características dos iPhone" descreve algumas características dos vários modelos do smartphone da Apple (Epifani & Stirparo, 2015; Hotz, 2017.).

Modo de arranque

Do ponto de vista forense é importante saber a forma como os dispositivos Apple arrancam e como estes funcionam. Desta forma a seguinte lista mostra as 3 diferentes formas de funcionamento destes dispositivos (Epifani & Stirparo, 2015).

- Normal – O dispositivo arranca com a interface por defeito para o utilizador
- Recovery – Este modo é utilizado para fazer alterações como ativações ou atualizações ao dispositivo. Este modo pode ser ativado pressionando o botão "*home*" enquanto o dispositivo está ligado ao computador.
- Modo DFU (*Device Firmware Upgrade*) – Este modo é usado para fazer atualizações ou quando um dos processos de arranque falha.

Os modos "*Recovery*" e "*DFU*" são úteis para fazer aquisições físicas aos dispositivos.

3. Conceitos e Procedimentos forenses

O capítulo conceitos e procedimentos forenses tem como objetivo a descrição de conceitos importantes para a análise forense digital. Começa por definir um conjunto de princípios forenses, algumas normas forenses existentes, como funciona um laboratório forense, uma breve análise a vários softwares forense, apresenta a distinção entre vários tipos de aquisição e por fim o conjunto de procedimentos forenses estudados ao longo do projeto.

3.1. Princípios Forenses

Nesta secção são abordados um conjunto de princípios forenses importantes.

Existem uma série de princípios forenses a serem adotados. Cada organização tem definidos um conjunto de princípios forenses.

Os seguintes princípios são de organizações distintas e foram adaptados de: (Whatson & Jones Andrew, 2013).

A ACPO (Association of Chief Police Officers) de Inglaterra define boas práticas de como tratar provas digitais. Em seguida apresentamos alguns princípios.

- Principio 1 – Nenhum dos órgãos de aplicação de leis deve tomar ações que modifiquem a integridade dos dados em qualquer dispositivo;
- Principio 2 – Quando é necessário aceder aos dados de um dispositivo ou suporte de dados, essa pessoa deve ser competente para efetuar as tarefas necessárias e explicar tudo o que foi feito;
- Principio 3 – Todas as etapas efetuadas e todos os processos aplicados a dispositivos eletrónicos devem ser criadas, registadas e preservadas para que uma terceira entidade consiga entender os resultados;
- Principio 4 - A pessoa que leva a cargo a investigação é responsável por verificar que a lei e todos os princípios estão a ser aplicados.

A NIST, (National Institute Of Standards And Technology), requer que as ferramentas para aquisição de dados sigam uma série de critérios:

- A ferramenta deve fazer uma cópia duplicada ou uma imagem do disco ou partição;
- A ferramenta não deve alterar os dados existentes no suporte de dados;
- A ferramenta deve poder verificar a integridade de uma imagem de um suporte de dados;
- A ferramenta deve copiar os dados para um suporte de dados que seja maior que o original;
- A ferramenta deve avisar caso o suporte de dados de destino seja mais pequeno.

3.1.1. Cadeia de custódia (*Chain of custody*)

Nesta subsecção será apresentado o conceito de cadeia de custódia.

Antes de qualquer dispositivo ou prova ser levado a tribunal, deve passar por uma série de processos legais. Um desses processos é o chamado (*Chain of custody*), cadeia de custódia. No caso de um telemóvel ou qualquer outro dispositivo, passa por um conjunto de etapas forenses e por uma ou mais pessoas. Cada uma das etapas é devidamente registada, todos os passos, decisões, pessoas responsáveis, quem foi responsável por cada etapa e por manusear casa dispositivo, assim como os resultados obtidos para que seja devidamente validado num tribunal. Desta forma, é possível manter um registo no qual o dispositivo passou, por quem passou e o que foi feito, provando assim que nas provas não foram alteradas (Epifani & Stirparo, 2015).

Segundo (Whatson & Jones Andrew, 2013), o termo *chain of custody* é um processo utilizado pelos especialistas forenses para preservar o cenário de crime. O que inclui a preservação de dados armazenados em computadores, dispositivos de armazenamento, dispositivos móveis, ou até na rede. Cada etapa deve ser ainda bem documentada, identificadas todas a ferramentas utilizadas, processos e procedimentos para que o relatório possa ser levado a tribunal e provar que os dados não foram alterados durante a investigação.. Dessa forma, a cadeia de custódia permitiu manter o registo de todos os passos efetuados.

3.2. Normas Forenses Existentes

Nesta secção apresentamos um conjunto de normas forenses criadas por entidades específicas.

A realização de inspeções forenses por diversas entidades, são em alguns países, observadas por entidades superiores que obrigam que os laboratórios forenses sejam certificados e cumpram normas ISO (*International Organization for Standardization*), regulando assim o mercado de prestação de serviços de perícias forenses. Por exemplo, no Reino Unido existe a FSR (*Forensic Science Regulator*) que garante que as entidades de serviços forenses estejam sujeitas a regras de qualidade. A nível Europeu, existe intenção por parte do Conselho da União Europeia, de até 2020, criar uma área Europeia de Ciência Forense European Forensic Science Area (EFSA) cujos principais objetivos são a acreditação dos laboratórios forenses, as boas práticas, o seguimento de regras e de padrões de qualidade, a certificação dos peritos entre outras situações importantes. Atualmente existe cada vez mais necessidade de sistemas de gestão de qualidade (SGQ) para garantia a melhor qualidade nos serviços. Este assunto é ainda recente e está em desenvolvimento. Em Portugal ainda há muito por fazer (Viriato, 2016) .

Em seguida apresentamos um conjunto de normas.

Norma ISO/IEC 17020:2013 – Requisitos para o funcionamento de diferentes tipos de organismos de inspeção.

Esta norma especifica os requisitos para as entidades competentes que realizam inspeções e também com a recolha e a preservação de provas (Viriato, 2016).

Norma NP ISSO/IEC 17025:2005 - Requisitos de Competência de Laboratórios de Ensaio e Calibração

Esta norma contém os requisitos para acreditação de laboratórios das entidades que pretendem realizar análises forenses a informação digital contida em dispositivos recolhidos num caso de um crime. Esta norma, apesar de poder ser aplicável a outro tipo de laboratórios, também é aplicável a laboratórios forenses (MULLER & DINIZ, 2005).

Esta norma contém informações que descrevem que devem ser mantidos registos e descrição do estado, forma e condições físicas de quaisquer dispositivos apreendidos. A clausula 5.4.2 indica também que o prestador de serviços forenses deve ter em conta a redundância de hardware e software de modo a que não haja perdas dade dados (Viriato, 2016).

ISO/IEC 27037 – Tecnologia de informação – Técnicas de Segurança - Guias para identificação, recolha, aquisição e preservação de provas digitais.

Esta norma é específica para atividades relacionadas com o tratamento de provas digitais, nomeadamente identificação, obtenção, aquisição e preservação de potenciais provas digitais A norma suporta o tratamento de provas digitais, assim como os procedimentos utilizados pelas diversas entidades. Os dispositivos móveis assim como vários tipos de suporte de armazenamento de dados fazem também parte desta norma. Esta norma não substitui as normas de acreditação ISO/IEC 17020:2013 e ou a ISO/IEC 17025:2005 (ISO, 2012).

ISO/IEC 27042 – Tecnologia de informação – Técnicas de Segurança – Guias para análise e interpretação de provas digitais.

Esta norma pretende ajudar na análise e interpretação de provas digitais. Existem uma série de processos equivalentes que podem ser aplicados numa investigação digital. Esta norma ISO pretende unificar a forma como são analisadas e interpretadas as provas digitais (ISO, 2015a).

ISO/IEC27043 – Tecnologia de Informação - Técnicas de segurança – Princípios e processos de investigação digital.

Esta norma dispõe de guias e modelos para investigação de vários tipos de crimes contendo provas digitais. Passando pela preparação da investigação, até à conclusão da mesma. Os vários guias, processos e princípios desta norma são aplicáveis a vários tipos de investigações como acesso não autorizado, corrupção de dados, fugas de informação e qualquer outro tipo de investigação digital (ISO, 2015b).

3.3. Os laboratórios Forenses e segurança da informação.

Esta secção apresenta uma breve abordagem sobre os laboratórios forenses e a segurança da informação nos mesmos.

Os laboratórios forenses podem apresentar diferentes características a nível de *software* e *hardware* assim como as ferramentas disponíveis. Os procedimentos (*Standard Operating procedures*) e a segurança dos dados "*quality assurance*" são também dois componentes importantes de um laboratório forense.

Segurança dos laboratórios Forenses

A segurança de um laboratório forense é um ponto importante. Deve ser mantida a integridade de todas as provas que existam no laboratório forense.

Podem ocorrer acidentes de forma deliberada, isto é, com intenção de comprometer algo, assim como um acidente natural (incêndio ou inundação) ou até um ataque por vírus ou *malware*. Dessa forma, o acesso a todos os equipamentos assim como aos dados / provas deve ser restritivo. Apenas pessoas autorizadas devem ter acesso às áreas mais criticas como os locais onde se efetuam as aquisições, à localização dos dados e provas recolhidas. Tendo em conta as ligações à rede, os equipamentos utilizados para efetuar e aquisição de dados assim como os equipamentos que podem conter provas não devem estar ligados à internet, evitando assim acessos não autorizados, algum tipo de ataque ou até problemas relacionados com algum tipo de vírus. As limitações digitais poderão não ser suficientes, é importante implementar barreiras físicas, i.e., com portas, e controlos de acesso com cartões e ou códigos (Sammons, 2012).

3.4. Software forense

Nesta secção são abordados alguns tipos de software forense existente, as suas capacidades, assim como o software forense utilizado no projeto.

O *Software* forense faz parte dos processos da análise forense, nomeadamente para as fases de aquisição, procura de provas e análise das mesmas. Existem uma série de soluções para analisar e fazer aquisições de um dispositivo móvel. Estas ferramentas podem ser acompanhadas de hardware ou *software* ou ambas. Devido a uma grande variedade de dispositivos móveis, nem todas as ferramentas possuem as mesmas capacidades, podem suportar apenas determinados dispositivos. Podem haver ferramentas com resultados de aquisição diferentes, o que está relacionado com o suporte que a ferramenta tem para determinados dispositivos e ou sistemas operativos.

Existem soluções pagas, soluções *opensouree* e soluções "*freeware*".

Como são validadas as ferramentas forenses?

Como existe uma grande quantidade de ferramentas forenses no mercado, estas devem ser devidamente validadas, de forma a que os profissionais que efetuem as várias tarefas forenses possam ter os melhores resultados mantendo a sua integridade. Por exemplo, a NIST é uma das organizações que valida as ferramentas forenses. Contém uma ferramenta denominada CFTT (*Computer Forensic Tool Testing Project*) que contém metodologias para testar as ferramentas forenses.

O software forense enfrenta cada vez mais novos desafios no que toca à capacidade de extração de dados dos dispositivos. Estes tendem a ser cada vez mais difíceis de extrair uma vez que os sistemas operativos são cada vez mais fechados e os suportes de armazenamento de dados são cada vez mais cifrados.

No caso da Apple, segundo (Fukami et al., 2017; Sheldon, 2013) desde o iPhone 3GS que existe encriptação implementada por defeito.

Segundo (Apple Inc., 2017; Teufl, Zefferer, Stromberger, & Hechenblaikner, 2013), no iOS 10 os dados encontram-se cifrados devido a uma encriptação de hardware localizada entre a memória de armazenamento flash e a memória do sistema. O algoritmo de cifra

utilizado é o AES 256 (*Advanced Encryption Standard*). Cada dispositivo contém uma chave AES (*AES Key*). Este nível de proteção assegura um alto nível de encriptação para as aplicações, mensagens, e-mail, calendário, contactos, fotos entre outros. A encriptação do sistema de ficheiros está implementada para uma proteção básica e para a funcionalidade (*remote wipe*), que permite apagar os dados à distância.

Existem uma série de empresas que tem soluções forenses para as entidades que tratam os casos forenses. No caso deste projeto foi utilizado software da empresa MSAB, detentora do XRY e XAMN *viewer*. Num laboratório forense, além das ferramentas forenses para fazer aquisição e análise dos dados, é importante que hajam ferramentas para interpretar o cabeçalho dos ficheiros, para abrir ficheiros de base de dados, ficheiros do tipo ".plist" no caso de dispositivos Apple, ficheiros com localização gps integrada, entre outros.

Os websites (DFIR Training, 2017; NIST, 2016) contém uma serie de software e ferramentas forenses importantes.

Na **Tabela 10** apresentamos uma lista de software forense.

O "Anexo E Software Forense.pdf" contem informação mais detalhada acerca do software apresentado na Tabela 10**.**

O Objetivo do anexo é apresentar diferenças entre várias soluções de software forense assim como as capacidades das mesmas.

Tabela 10 - Software forense breve descrição do mesmo.

Software	Breve descrição
XRY	Aquisição lógica e física. Suporta iPhone. Contém kit de cabos específicos.
Cellebrite ufed touch ultimate	Dispositivo portátil que suporta todos os tipos de aquisição e análise de dados. Suporta iPhone.
Oxygen forensics extractor (Oxygen, 2017)	Aquisição física e lógica. Suporta iPhone.
Paraben U3 Universal(Paraben, 2017)	Aquisição lógica e física. Apresenta maior suporte a dispositivos Android.
AccessData mobile phone Examiner plus (AccessData, 2014)	Aquisição física e lógica. Oferece uma versão de demonstração por 20 dias. Suporta iPhone.

Elcomsoft Mobile Forensics Bundle	Apenas suporta iPhone. Com suporte especial para contas google e aplicação WhatsApp.
Backlight (BlackBag, 2017)	Apenas suporta aquisição lógica. Suporta iPhone.
Lantern (Katana Forensics, 2017)	Apenas pode ser instalado em computadores Apple. Suporta aquisição lógica e física. Suporta iPhone.
Molbiledit forensics express (Compelson Labs, 2017)	Suporta aquisição lógica e física. Suporta iPhone.
Magnet IEF (Magnet forensics inc., 2017)	Apenas suporta análise dos dados. Suporta iPhone.
Autopsy(B. Carrier, 2017)	Software opensource. Apenas suporta análise dos dados. Suporte especial para Android.
XAMN Viewer	Apenas suporta análise dos dados. Suporta iPhone.
FTK Imager	Software opensource que apenas suporta análise dos dados. Não tem suporte específico para dispositivos móveis.

Por questões legais apenas conseguimos testar o software XRY, XAMN viewer, autopsy e FTK Imager. Os outros softwares indicados apresentam custos elevados o que não nos permitiu adquirir mais nenhum para teste.

3.5. Hardware Forense

Esta secção pretende abordar um pouco sobre o hardware forense.

Existem várias ferramentas de hardware forense especificas para as várias etapas forenses. Como por exemplo: ferramentas para clonagem de cartões SIM, ferramentas para aquisição de dispositivos móveis e respetivos cabos, bloqueadores de escrita, e adaptadores.

A seguinte lista apresenta algum hardware necessário para um laboratório forense (Whatson & Jones Andrew, 2013) :

- Computadores forenses com capacidade de processamento;
- Equipamento específico para laboratórios forenses como (bloqueadores de escrita, kit's específicos para telemóveis com respetivos cabos, hub's usb (*Universal Serial Bus*) entre outros equipamentos.

Apesar da tendência levar a que todos os dispositivos móveis utilizem os mesmos standards para os conectores como é o caso do micro usb e do usb Type-C, que irá ser cada vez mais implementado, ainda existem conectores proprietários como é o caso do Apple Lighning. A Figura 27 mostra o exemplo de 3 tipos de conectores, Micro-usb, Lightning e Type-C.

Figura 27 – Connectores Micro usb, lightning da Apple e type-C. Fonte: (haileehaas, 2015)**.**

Os dispositivos mais antigos utilizam conectores proprietários e dessa forma é importante que o laboratório disponha de um conjunto de cabos e acessórios. A Figura 28 mostra um exemplo de uma mala que faz parte de um kit da empresa msab, detentora do XRY.

Figura 28 – Conjunto de cabos para dispositivos móveis. Fonte: msab.com.

3.6. Tipos de aquisição

Nesta secção são distinguidos os tipos de aquisição, aquisição lógica e aquisição física.

Do ponto de vista forense é muito importante obter os dados armazenados nos dispositivos pois podem servir como provas.

Para obter o máximo de dados é importante examinar e obter os dados de tudo o que está ao alcance e questionar sempre se pode existir informação adicional e mais algum dispositivo ou suporte de dados.

A aquisição depende de algumas variáveis como apresentadas na seguinte lista:

- Modelo do dispositivo;
- Versão de iOS;
- Da existência ou não de palavra passe;
- Existência de uma palavra-passe secundária;
- Se o dispositivo está desbloqueado "jailbreak";

Os dados de um dispositivo móvel podem ser obtidos de duas formas diferentes, por aquisição física ou por aquisição lógica.

Aquisição Lógica

A aquisição lógica possibilita extrair parte da informação do sistema de ficheiros. Esse tipo de cópia não inclui ficheiros como e-mails, registos de localização, ficheiros temporários das aplicações ou ficheiros apagados. Pode ainda ser usado software na memória do dispositivo para usar a sua API (aquisição lógica completa) (Epifani & Stirparo, 2015; Scientific Working Group on Digital Evidence, 2013).

Podemos dividir a aquisição lógica em duas partes:

- Aquisição completa – Quando é feita através de uma aplicação que faz de agente;
- Um backup do dispositivo;

No caso dos dispositivos Apple o *backup*, pode ser conhecida como "*iTunes Backup*", ou seja, cópia de segurança via iTunes.

Aquisição Física

A aquisição física obtém todos os dados no dispositivo móvel, nomeadamente no sistema de ficheiros. Este tipo de aquisição funciona como um "*clone*" bit-a-bit do armazenamento do dispositivo. Este tipo de aquisição captura também os dados apagados.

Aquisição Forçada:

No caso dos dispositivos Apple, podemos considerar a existência de um terceiro tipo de aquisição, a aquisição forçada. Este tipo de aquisição é uma aquisição física na qual é feito um *jailbreak* de forma a desbloquear o dispositivo. Dessa forma é possível fazer uma boa aquisição de dados uma vez que foram desbloqueados os acessos e é possível fazer uma aquisição física.

3.6.1. Live e Dead Analysis

Nesta subsecção são distinguidas duas formas de aquisição de dados, "*live acquisition*", com o dispositivo ligado e "*dead acquisition*" ou *posmorten memory analysis*, com o dispositivo desligado.

Live acquisition (Aquisição com dispositivo ligado)

Neste tipo de aquisição, o dispositivo encontra-se ligado o que permite capturar os dados da memória RAM e efetuar uma aquisição lógica ou física aos dados da memória de armazenamento do dispositivo. Este tipo de aquisição é por norma, efetuada nos dispositivos móveis.

Dead acquisition ou *Posmorten memory analysis*.

Este tipo de aquisição implica que o dispositivo esteja desligado, não havendo interação com o equipamento. Desta forma existe uma vantagem, menos probabilidade de alterações nos dados de forma remota por exemplo. Este tipo de abordagem, é por norma, aplicada nos computadores.

Nos dispositivos móveis não é possível fazer aquisição à memória interna do dispositivo com o mesmo desligado. Com o dispositivo desligado apenas é possível fazer uma aquisição ao cartão de memória (caso haja), no caso da Apple não utiliza cartões de memória e ao cartão sim. Por outro lado, se o dispositivo estiver protegido com algum código, poderemos não conseguir voltar a ligar o mesmo.

3.7. Tipos de dados Importantes para a análise Forense

Nesta secção são identificados os tipos de dados importantes para a análise forense. Neste caso será dada importância aos dispositivos móveis uma vez que se enquadra no tema do projeto.

No enquadramento da análise forense digital, os dados importantes são tratados como provas digitais (*digital evidence*). Existe uma grande quantidade de provas possíveis de serem encontradas nos dispositivos móveis. A Tabela 11 apresenta tipos de provas e a respetiva descrição (Frade, 2016; Sammons, 2012; Whatson & Jones Andrew, 2013).

Tabela 11 – Tipos de provas e respetiva descrição

Tipo de Prova	Descrição
Dados do cartão SIM	O cartão SIM pode conter: Códigos como IMSI e ICC-ID. Informações sobre o operador, localização do dispositivo, contactos guardados, mensagens de texto SMS existentes e apagadas.
Informação do dispositivo	Informações como: IMEI, número de série, marca e modelo do dispositivo.
Contactos	Contactos do dispositivo e de aplicações existentes.
Mensagens SMS e MMS	Mensagens enviadas, recebidas e apagadas.
Registo de Chamadas	Chamadas efetuadas, recebidas e não atendidas. Autor da chamada, duração, localização da chamada.
Mensagens de Chat	Mensagens trocadas em aplicações de mensagens instantâneas.
Dicionário de Palavras	Palavras e ou abreviaturas que foram guardadas para facilitar a escrita.
Contas de utilizador	Contas de utilizador para as aplicações.
Anexos trocados	Anexos (Fotografias e vídeos) trocados entre aplicações.
Fotografias	Fotografias, trocadas entre mensagens, e com base em aplicações. As fotografias podem ainda conter metadados como: bits por pixel, data e hora da fotografia, versão de exif, flash, exposição, Informações de localização, Fabricante,

	modelo, versão de software, Tipo de compressão, resolução e nome da fotografia.
Vídeos	vídeos da câmara, trocados entre mensagens, e com base em aplicações.
Dados de GPS	Dados de localização como: Localização agregada a um elemento como fotografia ou vídeo, Destinos favoritos e pontos guardados no mapa, localização da casa, registos de viagens.
Dados Wi-fi	Redes wi-fi registadas e dados importantes como palavras-passe.
Bases de dados	Bases de dados resultantes de aplicações instaladas.
Histórico Web	Histórico web das páginas visitadas, download de ficheiros de uma aplicação para acesso à internet. Registo de websites favoritos.
Palavras-passe	Palavras-passe de aplicações e de acesso a websites.
Calendário e eventos	Dados do calendário, eventos e tarefas registadas.
E-mails	Contas de e-mail registadas e e-mails guardados e apagados.
Gravação de voz	Gravação de voz gravada no dispositivo ou por parte de aplicações.
Documentos	Documentos escritos em formato de texto com ou sem anexos
Aplicações Instaladas	Aplicações instaladas no dispositivo.
Sistema de ficheiros	Sistema de ficheiros do dispositivo móvel que contém a estrutura de pastas, programas e dados do utilizador.
Ficheiros Apagados	Ficheiros apagados que possam ser recuperados podem conter provas importantes.
Metadados de ficheiros	Os metadados dos ficheiros podem conter informações relevantes acerca dos mesmos.

3.8. Formatos de aquisição de dados

Nesta secção são identificados alguns formatos de dados resultantes das aquisições forenses.

O resultado da extração dos dados é uma imagem forense. O formato desta imagem pode ser diferente consoante o software utilizado. De relembrar que existem formatos *opensource* e formatos proprietários. A Tabela 12 apresenta alguns formatos de aquisição de dados (Frade, 2016; Vandeven & Filkins, 2014).

Tabela 12 – Descrição de formatos de imagens forenses.

Extensão	Descrição
.E01 (*EnCase* EWF) (Expert Witness Disk image format)	Formato proprietário gerado pelo *software* EnCase.
.Ex01 (EnCase 7 EWF)	Formato proprietário gerado pela versão 7 *software* EnCase.
.L01 (Encase Logical EWF)	Formato proprietário gerado pelo *software* EnCase.
.LX01 (Encase 7 Logical EWF)	Formato proprietário gerado pela versão 7 *software* EnCase.
.001 (*Raw dd*)	Formato *opensource.*
.AD1 (*AccessData Custom Content Image*)	Formato proprietário da empresa AccessData.
.XRY	Formato proprietário Gerado pelo software XRY.
.AFF (Advanced Forensics File Format)	Formato *opensource.*
.AFF4 (Advanced Forensics File Format 4)	Formato opensource, melhoria do anterior AFF.

A Figura 29 apresenta dois exemplos de ficheiros do formato proprietário do XRY.

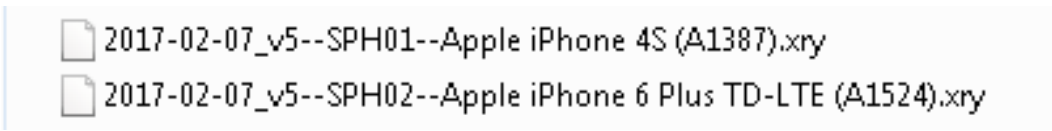


Figura 29 – Formatos de ficheiros do software XRY.

3.9. Procedimentos forenses

Esta secção apresenta uma introdução aos procedimentos forenses apresentados nas seguintes subsecções.

Os *Standard Operating Procedures* (SOP) são documentos que detalham como devem ser seguidas todas as fases forenses. Para que as provas possam ser usadas em tribunal, os procedimentos forenses devem ser devidamente seguidos, de forma a tomar as melhores decisões, desde quando se identificam os dispositivos até à parte final em que se elabora o relatório.

Um dos problemas relativo aos dispositivos móveis é o facto de estes estarem constantemente a trocar dados através da rede, seja pela rede móvel, por *Wi-Fi*, ou por *Bluetooth* e nesse sentido deve haver alguns cuidados para preservar e manter a integridade dos dados.

Uma vez que a documentação deve ser começada desde o inicio do caso forense, é recomendado ler o capítulo 3.9.7 Relatório final (*Final report*) e ler o Procedimento 7 – Relatório Final.

Os procedimentos abordados nas seguintes subsecções são os da seguinte lista:

- Procedimento 1 – (Receção) Assinatura do documento de autorização, receção dos dispositivos móveis, verificações importantes, proteção dos dados e inicio do relatório interno.
- Procedimento 2 – (Catalogação e registo fotográfico) Atribuição de siglas numeradas a cada dispositivo e dispositivos de armazenamento externo, fotografia nas diversas vistas indicadas.
- Procedimento 3 – (Preservação) Preservação dos dados em todos os procedimentos forenses para manter a integridade dos mesmos.
- Procedimento 4 – (Aquisição) Aquisição dos dados dos dispositivos com *software* forense e criação de cópias de segurança dos dados.
- Procedimento 5 – (Pesquisa das provas) Pesquisa das provas a partir dos dados da aquisição com base em Software e técnicas manuais.
- Procedimento 6 – (Análise das provas) Análise das provas encontradas, hipóteses e conclusões.

- Procedimento 7 – (Relatório Final) Indicação de como construir o relatório final a partir de todos os dados obtidos durante os vários procedimentos forenses e escritos no relatório interno.

3.9.1. Procedimento 1 Receção dos equipamentos (*Reception*)

Nesta subsecção será apresentado o procedimento de receção dos equipamentos (*reception*).

Este procedimento trata da receção dos equipamentos quando estes chegam ao laboratório forense pela primeira vez para um dado caso forense.

O preenchimento de documentos de autorização é efetuado logo no inicio desta fase, nomeadamente um documento (*request*) que indica o tipo de análise forense a ser efetuado a um dado caso, a autorização para usar os dispositivos e poder trabalhar com os dados, uma possível indicação dos riscos que podem ocorrer e a identidade legal que pede para efetuar a análise forense.

Uma vez que os dispositivos são recebidos, devem-se efetuar algumas verificações que podem ser importantes para os seguintes casos forenses. Deve ser verificado se existe algum cabo de alimentação, verificar se o dispositivo está ligado ou desligado, ligar o monitor do dispositivo e verificar o que está a acontecer, se existe algum código, o nível da bateria e colocar o dispositivo em modo de avião para evitar comunicação com a rede móvel, rede Wi-Fi e Bluetooth. Se necessário alimentar o dispositivo para evitar que este desligue. Alguns destes passos fazem parte da preservação de dados.

O relatório interno é começado nesta etapa forense, começando por inserir a informação disponível para os dispositivos e os responsáveis forenses. Também a cadeia de custódia deve ser começada a partir desta etapa.

O procedimento de Receção (*Reception*) encontra-se no ficheiro "Procedure 1 Reception" e deve ser seguido na realização desta etapa forense.

3.9.2. Procedimento 2 Catalogação e Registo fotográfico (*Photographic Cataloging*)

Nesta subsecção será apresentado o procedimento de catalogação e registo fotográfico (*Photographic Cataloging*).

O procedimento 2, Catalogação e Registo fotográfico (*photographic cataloging*) é o procedimento no qual os dispositivos envolvidos no processo forense são devidamente identificados e fotografados. Nesse sentido, os dispositivos e respetivos suportes de armazenamento externo como 1 ou mais cartões de memória, e 1 ou mais cartões SIM (*Subscriber Identity Module*) são devidamente identificados com abreviaturas específicas e devidamente fotografados. Com apoio de uma régua e de um dispositivo para tirar fotografias, estas devem incidir sobre as vistas mais importantes, o estado em que se encontra o dispositivo e devem identificar informações como números de série, possíveis partes danificadas, portas de IO (*Input/Output)*. Desta forma será mais fácil reconstituir todo o cenário e utilizar as fotografias na documentação (Sammons, 2012).

A catalogação contribuir para que as provas sejam devidamente identificadas para serem distinguidas uma vez que podem haver dispositivos iguais. Por exemplo, no caso de um crime numa empresa, podem existir uma série de dispositivos móveis iguais.

O procedimento de Catalogação e registo fotográfico (*Photographic Cataloging*) encontra-se no ficheiro "Procedure 2 Photographic Cataloging" e deve ser seguido na realização desta etapa forense. Contém ainda um anexo com um resumo das vistas para fotografar os diversos dispositivos. O ficheiro "Procedure 2.1 Photographing" é um subprocedimento de apoio. Contém um conjunto de notas de ajuda, a posição de cada dispositivo e as vistas mais importantes a fotografar.

3.9.3. Procedimento 3 - Preservação das provas (*Preservation*)

Nesta subsecção será apresentado o procedimento de preservação das provas (*preservação*).

A fase de preservação das provas consiste em preservar o estado das mesmas assim como dos dispositivos. As ações tomadas nesta etapa podem variar consoante os requisitos da investigação. O objetivo desta fase é garantir que os dados não são modificados nem acrescentados assim como garantir que os dados ficam devidamente guardados para futuras análises (B. D. Carrier, 2005).

A seguinte lista mostra cuidados a ter durante a fase de preservação (Whatson & Jones Andrew, 2013):

- Usar bloqueadores de escrita;
- Criar cópias dos dados para evitar perdas dos dados de todo o processo forense;
- Criar a cadeia de custodia, criando um processo detalhado para as provas;
- Assegurar que apenas pessoas certificadas e de confiança tratam das provas;
- Assegurar que os dispositivos móveis aprendidos não são usados;
- Usar algoritmos criptográficos como o SHA256 para calcular uma chave criptográfica dos dados (provas).
- A catalogação de cada dispositivo como efetuada no Procedimento 2 Catalogação e registo fotográfico.
- Manter a integridade dos dados obtidos da aquisição, pesquisa de provas e análise dos mesmos.

O isolamento dos dispositivos da rede é também considerado parte da preservação das provas digitais. Tal como noutro tipo de dispositivos, os dados devem ser mantidos intactos, mantendo a sua integridade. Os dispositivos móveis Apple podem ser apagados ou bloqueados remotamente por parte dos donos de forma a proteger os dados. Neste caso são perdidos todos os dados, o que é um ponto negativo do ponto de vista forense em que se procura obter o maior número de provas possível (Sammons, 2012).

Soluções de isolamento

Em seguida apresentamos algumas soluções de isolamento. De notar que todas as soluções têm vantagens e desvantagens.

- Desligar o dispositivo - Evita que o dispositivo deixe de comunicar com a rede, não gastando bateria. No entanto podemos não conseguir ligar mais o dispositivo uma vez que pode conter uma palavra-passe ou podemos não saber o código PIN o cartão SIM.
- Modo de avião (*Airplane mode*) – Este talvez seja um dos métodos com mais vantagens uma vez que o dispositivo não comunica com nenhuma rede e não gasta mais bateria por isso. É fácil de ativar o modo de avião uma vez que a partir do iOS 7, mesmo que o dispositivo esteja protegido por palavra-passe, pode ser feito a partir do menu.
- Remover o cartão SIM – Esta técnica irá evitar que o dispositivo comunique com a rede móvel. No entanto podemos não saber o código do cartão SIM e as ligações às redes Wi-Fi e Bluetooth necessitam de ser desligadas à parte. Nos iPhone não é necessário tirar a bateria para retirar o cartão SIM.
- Saca de Faraday (*faraday bag*) (ver Figura 30) - Esta saca é constituída por materiais que repelem os sinais das redes, protege o dispositivo dos sinais da rede. Evitando assim de receber mensagens, chamadas, ou até ser controlado remotamente. No entanto como desvantagem a carga da bateria desce mais rapidamente por este estar à procura de rede constantemente.

Figura 30 – Saca de Faraday.

A solução mais vantajosa será a do modo de avião uma vez que é fácil de aceder, não faz descarregar a bateria rapidamente e não coremos o risco de necessitar do código do cartão SIM caso não o tenhamos.

Relativamente aos acessórios e cabos, é também importante que existam os cabos apropriados para fornecer energia ao dispositivo, evitado assim que o mesmo se desligue e não o consigamos ligar por causa de algum código.

O procedimento de preservação das provas (*preservation*) encontra-se no ficheiro "Procedure 3 Preservation" e deve ser seguido na realização desta etapa forense.

3.9.4. Procedimento 4 - Aquisição de dados (*Acquisition*)

Nesta subsecção será apresentado o procedimento de aquisição de provas (*acquisition*).

A aquisição de dados, pode ser denominada de várias formas, "*data collection*", "*data extraction*", "*evidence acquisition*" ou "*evidence extraction*". A aquisição permite obter uma imagem forense de um determinado dispositivo móvel que pode conter um conjunto de provas que vão ser úteis para o caso forense. A aquisição de dados é feita com um software forense que reconhece o dispositivo móvel ligado ao computador ou a um dispositivo proprietário.

Identificar as principais fontes de dados

Antes de se iniciar o processo de aquisição de dados é importante identificar as potenciais fontes de dados. Se estivermos a tratar de dispositivos móveis Apple podemos considerar a sua memória interna, o cartão SIM e até os dados na *cloud*. Apple não utiliza cartões de memória nos seus dispositivos.

Segundo o autor (Kent et al., 2006) a aquisição de dados deve ser efetuada segundo 3 passos como apresenta a seguinte lista:

- Planear a aquisição de dados – É importante uma vez que podem haver vários dispositivos e cada um pode ter uma prioridade diferente consoante o seu estado.
    - Depende da experiência do analista forense, da violabilidade dos dados e do esforço que tem de ser feito para fazer a aquisição.
- Aquisição de dados – Após identificadas as fontes de dados, passamos à parte em que é feita a aquisição de dados do dispositivo. A aquisição é efetuada com base em ferramentas forenses constituídas por *software* e ou *hardware*.
- Verificar a integridade dos dados – É importante manter a integridade dos dados e evitar que estes fiquem corrompidos. Gerando uma chave criptográfica com os dados originais e gerando outra com os dados depois da cópia, o valor da chave teria de ser exatamente igual, provando a sua integridade, ou seja, que não foi efetuada qualquer alteração aos mesmos.

Estado do dispositivo (Ligado e desligado) versus aquisição lógica ou física

Um dispositivo móvel pode ser encontrado em dois estados, ligado ou desligado. Pode conter ou não um código de proteção. Com o dispositivo ligado e sem código (ou sendo o código conhecido) é possível efetuar uma aquisição lógica. Se o dispositivo estiver protegido por um código desconhecido não nos é possível efetuar uma aquisição a não ser que esse código fosse obtido com algum software de desbloqueio. Com o dispositivo desligado apenas é possível fazer uma aquisição física, em alguns casos, com desbloqueio via *jailbreak.* Neste caso apenas vamos considerar os dispositivos se encontram ligados e sem código e que são feitas aquisições lógicas.

O procedimento de aquisição encontra-se no ficheiro “Procedure 4 Acquisition” e deve ser seguido na realização desta etapa forense. O procedimento apenas se aplica a aquisições lógicas com os dispositivos ligados.

3.9.5. Procedimento 5 Pesquisa das provas (*Examination)*

Nesta subsecção será apresentado o procedimento de pesquisa de provas (*examination*).

Na fase de aquisição (*acquisition*) obtivemos uma imagem forense do dispositivo móvel. Nesta fase vamos procurar provas digitais que possam existir nessas imagens forenses e que podem conter centenas de ficheiros. É importante que sejam escolhidos os ficheiros mais importantes que contenham informação relevante (Kent et al., 2006).

Que métodos ou ferramentas devem ser usadas para pesquisa das provas digitais?

O processo de procura das provas digitais pode ser automático, sendo ajudado por *software* ou determinadas ferramentas que organizam os dados em categorias por exemplo, ou de forma manual procurando os dados com base em determinados métodos. Não existem métodos ou ferramentas específicas para todos os casos forenses, uma vez que cada caso é um caso. Devem usados métodos e ferramentas específicas para o que se pretende procurar, tendo em conta o caso forense em questão.

Alguns *softwares* ajudam a procurar determinados ficheiros conhecidos ou determinados dados de forma automática, organizando os mesmos por categorias. Esses dados são os dados que mais se procuram na análise forense digital (Registos de histórico da Internet, e-mails, mensagens, dados trocados entre aplicações, chamadas, fotografias, entre outros). A Figura 31 apresenta um exemplo de *software* com vários tipos de dados organizados.

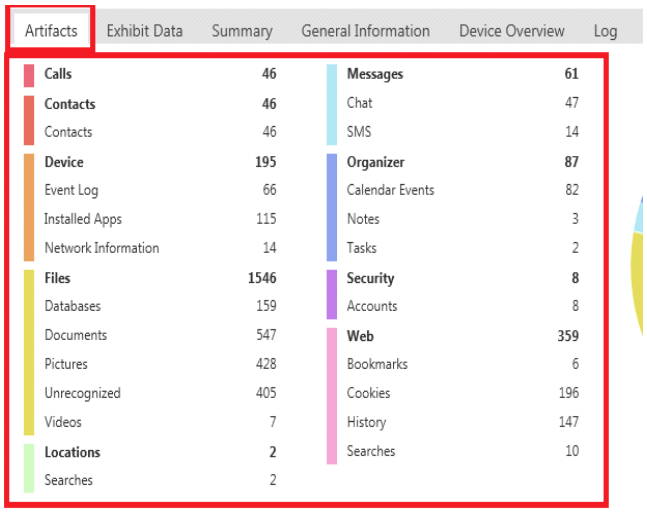


Figura 31 – Software que organiza os dados por categorias e tipos.

Processos manuais de pesquisa de provas

Um dos processos manuais é extrair os ficheiros da imagem forense que foi criada para que possamos abrir o ficheiro manualmente. No caso da imagem gerada pelo *software* ”XRY” utilizamos o software “XAMN Viewer” para abrir as imagens geradas e assim poder extrair os ficheiros que nos interessam.

Pesquisa por texto

Tendo por base o que pretendemos encontrar podemos utilizar pesquisas por texto tentando procurar ficheiros pelo seu nome ou até mesmo pelo conteúdo que o ficheiro possa conter. Podem também ser usadas ferramentas específicas para verificar o conteúdo de texto do ficheiro. Um dos exemplos é o comando “strings” que pode ser utilizado na linha de comandos de um sistema operativo com base em Linux.

Pesquisa por tipo de ficheiro

Um ficheiro pode ser procurado pelo seu tipo, nomeadamente pela sua extensão associados ao seu conteúdo, se se trata de um ficheiro de texto, música, uma imagem, um ficheiro comprimido, um ficheiro de base de dados ou outro tipo. Caso a extensão do ficheiro seja modificada pode ser confirmado pelo cabeçalho do ficheiro.

A localização das provas mais importantes vai depender de caso para caso. Por exemplo, se for um dispositivo do mesmo fabricante ou com o mesmo sistema operativo, o sistema de ficheiros pode ser parcial ou totalmente igual, havendo mais facilidade em encontrar determinadas provas. Esse é o caso do iPhone.

Tal como será indicado no procedimento, será necessário procurar dados como: configurações, dados do cartão SIM, contactos, mensagens SMS e MMS, registo de chamadas, contas de utilizador, aplicações instaladas, anexos trocados entre aplicações, fotos e vídeos, dados de GPS e ficheiros com localização GPS agregada, dados Wi-Fi e palavras-passe, bases de dados, texto trocado entre contactos de aplicações de chat, histórico da internet, calendário, eventos e notas, e-mails e sistema de ficheiros.

Como resultado da pesquisa das provas, deve ser tudo registado, dessa forma, assim como descrito em (Whatson & Jones Andrew, 2013) devem ser tidos em conta os pontos da seguinte lista:

- Atualizar o relatório interno com tudo o que foi feito;
- Colocar todos os ficheiros que foram obtidos da imagem para análise;
- Colocar o conteúdo de alguns ficheiros mais importantes;
- Deve ser colocada uma estrutura do sistema de ficheiros;
- Para cada ficheiro, colocar o nome do mesmo, a diretoria onde se encontrava, a aplicação relacionada e que tipo de dados obtidos;
- Gerar uma chave criptográfica para mais tarde comprovar que os ficheiros não foram modificados;

Pode ser necessário efetuar novas pesquisas ou até utilizar outro software (*dual tool verification*) dado as razões da seguinte lista (Whatson & Jones Andrew, 2013):

- Uma prova pode não ser útil para justificar alguma informação;
- Pode ser preciso procurar mais provas;

O procedimento de pesquisa de provas (*Examination*) encontra-se no ficheiro “Procedure 5 Examination” e deve ser seguido na realização desta etapa forense.

3.9.6. Procedimento 6 - Análise das provas (Analysis)

Nesta subsecção será apresentado o procedimento de análise das provas (*analysis*).

As provas digitais foram extraídas na fase de pesquisa de provas, nesse sentido é necessário que as mesmas sejam analisadas. Na fase de pesquisa de provas o analista forense já tem uma noção dos dados que está a visualizar, no entanto estes devem ser devidamente analisados, comparados e relacionados. É importante tirar o máximo de conclusões, relacionar os dados com pessoas, lugares, como foram feitas as trocas de dados, determinar como todos estes elementos podem estar relacionados uns com os outros de forma a poder obter conclusões finais. Para tal acontecer, é preciso correlacionar múltiplos ficheiros das provas obtidas (Kent et al., 2006).

Os dados extraídos devem ser considerados e analisados analisado uma série de informações como os dados temporais (*timestamps*), os metadados (data de criação, modificação, autor etc.), o conteúdo de cada ficheiro extraído na fase anterior, os requisitos do caso forense e considerar se são úteis para o caso forense.

Com base nas hipóteses colocadas, as provas digitais são usadas para aprovar ou não aprovar essas hipóteses, podendo assim ser possível tirar conclusões sobre o caso forense e a utilidade das provas digitais.

O procedimento de análise (*Analysis*) encontra-se no ficheiro “Procedure 6 Analysis” e deve ser seguido na realização desta etapa forense.

3.9.7. Procedimento 7 Relatório Final (*Final Report)*

Nesta subsecção são apresentadas as diferenças entre relatório interno e relatório final ou externo, assim como o procedimento para elaborar o relatório Final.

A documentação é um ponto importante de todo o processo forense, a partir do momento em que os dispositivos chegam às mãos dos analistas forenses até à análise dos dados obtidos. Dessa forma, podemos considerar que o relatório forense é começado desde o inicio do processo, denominado de relatório interno e tudo o que acontecer durante o processo deve ser anotado. Tal como diz a expressão "If you didn't write it down, it didin't happen" Tudo o que aconteceu deve ser anotado (Sammons, 2012). Tendo por base a cadeia de custódia (chain of custody), todos os passos e pessoas responsáveis são devidamente registados, o que permitirá completar o relatório final.

Relatório Interno e relatório Final ou externo

O procedimento 1 Receção (*Reception*), faz referência ao relatório interno, documento que deve ser escrito desde inicio da investigação digital forense. O procedimento 7, relatório final (*Final Report*) aborda o relatório final Alguns autores como (Sammons, 2012; Whatson & Jones Andrew, 2013) consideram ser o relatório externo.

O relatório final contem toda a informação do relatório interno e tudo o que foi feito durante todos os processos forenses até ao procedimento 6 análise inclusive, de forma a preparar e apresentar toda a informação.

Antes de passarmos ao procedimento vamos abordar os dois tipos de relatório, interno e relatório final.

Relatório Interno

O relatório interno, que é começado desde o inicio do caso forense permite aos responsáveis entender o caso e determinar se uma dada prova obtida e analisada aprova ou reprova hipóteses que foram colocadas ou os requisitos da investigação.

Segundo o autor (Whatson & Jones Andrew, 2013), apresentamos um exemplo de tópicos que o relatório interno deve conter.

- Informação básica do caso;
- Dispositivos a serem analisados;
- Provas procuradas;
- Provas encontradas;
- Anexos.

Um dispositivo pode ser descrito pelo seu tipo, fabricante, modelo, número de série, IMEI e outras informações. É importante anotar se o dispositivo está ou não ligado, se está interligado a outro tipo de dispositivo ou até a uma rede (Bluetooth, Wi-Fi ou rede móvel). Parte do processo de documentação é iniciado no procedimento 1 – Receção.

Durante os processos forenses devem ser tiradas o máximo de notas possíveis sobre todas as decisões tomadas assim como a pessoa responsável por uma dada ação (Sammons, 2012).

Relatório Final

O relatório final contém toda a informação de todo o processo forense. É importante que o relatório final seja escrito de uma forma explicativa, de forma a que todos o possam entender. Deve incluir um resumo explicativo de todos passos efetuados começando pelo cenário de crime e acabando nas conclusões tiradas com base nas provas encontradas. Dessa forma é mais fácil de ser lido e interpretado por pessoas que não tenham formação na área em questão como por exemplo os advogados e os juízes. É importante que estas pessoas consigam ler e compreender a informação existente no relatório.

Segundo (Kent et al., 2006) existem alguns fatores que são importantes para o relatório forense tais como: os da seguinte lista:

- Se um dado acontecimento tiver mais do que uma explicação, devem ser devidamente justificadas no relatório;
- Considerar quem vai ler a informação – As informações e os dados vão ser lidos por uma ou mais pessoas das quais se deve ter em consideração. Vão também ser utilizadas leis em conjunto com todas as informações obtidas e podem ser ainda pedidas cópias dos dados obtidos para serem visualizados;

- Informação com valor elevado – O relatório deve conter informação a partir da que foi obtida, que leva a poder obter ainda mais informações ou chegar a determinadas concussões sobre futuras informações a serem obtidas.
- O relatório final pode ainda indicar correções a serem efetuadas aos guias e procedimentos forenses.

O processo de catalogação de todos os dispositivos e suportes de armazenamento deve ser devidamente anotada nas tabelas respetivas assim como colocadas algumas fotos. Este processo decorre durante o Procedimento 2 Catalogação e Registo fotográfico

Depois da preservação das provas, Procedimento 3 Preservação das provas (*preservation*), quando todos os dispositivos estiverem devidamente identificados e fotografados, passa-se para a aquisição das provas, Procedimento 4 Aquisição (*Acquisition*). Na fase de aquisição devemos ter em conta que são necessários outros recursos importantes, que precisam de ser identificados caso sejam necessários de obter, e que mais uma vez devem ser também documentados. Na fase de Pesquisa de dados (*examination*) procura-se as provas e anotam-se as mesmas, anunciando o seu conteúdo. Na fase de análise dos dados, Procedimento 6 (*Analysis*) é feito um resumo de todas as provas encontradas para todos os dispositivos e essas provas são utilizadas para aprovar ou não determinadas hipóteses.

O procedimento de elaboração do relatório final (*Final Report*) encontra-se no ficheiro "Procedure 7 Final Report" e deve ser seguido na realização desta etapa forense.

4. Caso de Estudo

Neste capitulo será apresentado o caso de estudo desenvolvido tendo em conta toda a documentação existente e todo o *software* e *hardware* existente no LabCIF.

O objetivo do caso de estudo foi utilizar dispositivos móveis da marca Apple e instalar aplicações que são mais usadas pelas pessoas no seu dia-a-dia. Os dispositivos foram utilizados regularmente com objetivo de gerar o máximo de dados possíveis.

À medida que foram utilizados, foram sendo feitas aquisições forenses aos mesmos com objetivo de poder ter uma noção do que era possível obter e obter o máximo de dados possíveis para posterior análise.

Os dispositivos que foram utilizados encontram-se indicados na Tabela 13. O iPhone 4s e o iPhone 6s foram utilizados apenas para o caso de estudo. O iPhone 6plus tinha sido utilizado por estudantes de Erasmus que deixaram o dispositivo com dados. Ao instalarmos as aplicações geramos ainda mais dados. Com as aquisições forenses verificamos que existiam uma grande quantidade de provas além daquelas que nós próprios geramos para o caso de estudo.

Dado que as versões de iOS são diferentes tentamos obter as diferenças entre as mesmas. Apesar de os dispositivos serem diferentes em termos de *hardware,* a versão do sistema operativo faz prevalecer muitas semelhanças.

Nota: se os dispositivos estivessem desbloqueados, denominado de *jailbreak*, poderíamos ter obtido ainda mais dados nas aquisições que foram efetuadas.

Foram usados os seguintes dispositivos apresentados na Tabela 13. Esta tabela contém observações relativamente às versões de iOS que estavam instaladas nos dispositivos aquando das aquisições forenses.

Tabela 13 – Lista de dispositivos e respetivas versões de iOS.

Dispositivo	Observações
iPhone 4s (A1387)	As primeiras duas aquisições foram efetuadas com a versão 9.2.1. Foi feita uma atualização para a o iOS 9.3.5 e foram efetuadas mais 3 aquisições.
iPhone 6s (A1586)	As aquisições foram efetuadas com o iOS 9.2
iPhone 6Plus (A1524)	As aquisições foram efetuadas com o iOS 10.2.1

4.1. Realização de aquisições forenses no LabCIF

O LabCIF contém *software* e *hardware* necessário para efetuar aquisições forenses. Foram efetuadas uma série de aquisições forenses aos vários dispositivos.

A Figura 32 apresenta dois dispositivos ligados ao hub usb xry para efetuar uma aquisição, em conjunto com a chave de software. Este dispositivo permite ligar no máximo 3 dispositivos em simultâneo.

Figura 32 – Dispositivos ligados para efetuar uma aquisição.

4.2. Aplicações Utilizadas para o estudo

Nesta secção são apresentadas as aplicações utilizadas no caso de estudo.

Os avanços tecnológicos mudaram alguns hábitos na vida das pessoas, que procuram estar sempre em contacto com outras pessoas. As aplicações de mensagens instantâneas (*Instant Messanging)* permitem que as pessoas utilizem a Internet como meio de comunicação, usando estas aplicações para trocar texto e imagens.

Do ponto de vista das aplicações, é guardada informação nos dispositivos uma vez que são trocados anexos e texto, mas não apenas isso, são também feitas cópias de segurança dos dados. O objetivo está em descobrir se os dados guardados pelas aplicações estão devidamente encriptados e seguros e o seu formato, para que em caso de um ataque ou na ocorrência de um crime, consigamos obter a maior quantidade de dados possível de uma determinada aplicação.

Utilizamos a loja de aplicações da Apple, o *itunes*, como fonte para obter a lista de aplicações mais usadas. Nesse sentido efetuamos uma pesquisa sobre as aplicações que consideramos mais importantes e as mais usadas pelo público em geral, tendo em conta a popularidade na loja itunes.

Segundo uma pesquisa no *itunes*, na lista de aplicações grátis mais usadas verificamos que a maior parte das aplicações usadas para troca de texto e "chat" são classificadas como (*Social Networking).* Apesar de estarem classificadas nessa categoria, o objetivo não é testar as aplicações de redes sociais como o "*Facebook"*, o "*Instagram"*, ou o "*Twitter"* por exemplo. O objetivo é estudar as aplicações de troca de mensagens de texto e anexos, por isso foram apenas consideradas aplicações que se enquadram no objetivo do projeto.

De notar que a lista das aplicações mais usadas tem em conta o país onde nos encontramos, que neste caso é Portugal como podemos ver na Figura 33 no canto inferior direito.

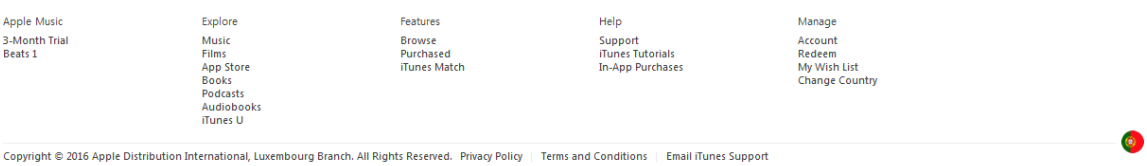


Figura 33 – Identificação de Portugal na aplicação iTunes. Fonte: iTunes.

A Figura 34 mostra a lista de aplicações grátis (*Free)* mais utilizadas em Portugal. Foram selecionadas as aplicações de troca de texto e anexos que mais se enquadravam no contexto do projeto.

Figura 34 – Lista do topo de aplicações grátis mais usadas, segundo a loja de aplicações iTunes. Fonte: iTunes, Data da consulta: 21-11-2016, País a que se aplica: Portugal.

Como se pode observar na Figura 34, a aplicação "WhatsApp" na 1ª posição, "Messenger" na 2ª posição, "Skype" na 5ª posição e "Viber" na 9ª posição, encontram-se nas listas das mais usadas. As outras aplicações foram consideradas por serem conhecidas ou existir feedback positivo sobre a segurança das mesmas.

Consideramos também a aplicação "Gmail" uma vez que se trata de uma aplicação para troca de e-mails muito usada e do ponto de vista forense interessa obter também informações.

Uma outra pesquisa efetuada nas aplicações grátis na categoria (*All Categories*) que contém todas as aplicações mostra-nos o resultado da Figura 35.

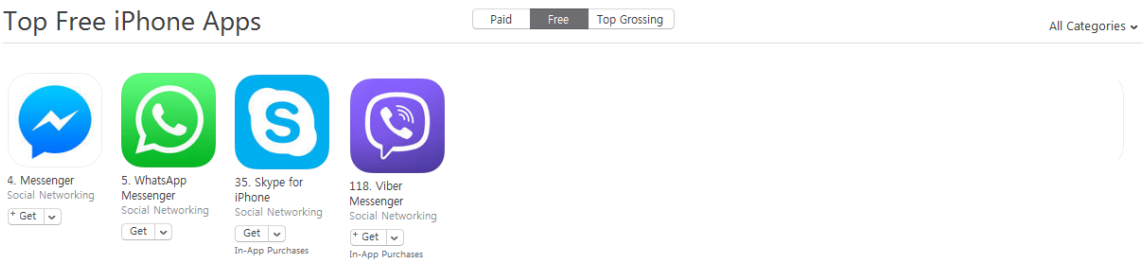


Figura 35 – Lista de aplicações de troca de mensagens e anexo mais utilizadas na categoria "*All Categories*". Fonte: iTunes, Data da consulta: 7-12-2016, País a que se aplica: Portugal

Como podemos verificar, as aplicações mais usadas no geral são o "Messenger", "WhatsApp", "Skype" e "Viber".

Foi efetuada uma pesquisa no website www.appannie.com. Conseguimos obter as aplicações grátis da categoria "*Social Networking*" mais usadas em iOS como mostra a Figura 36.

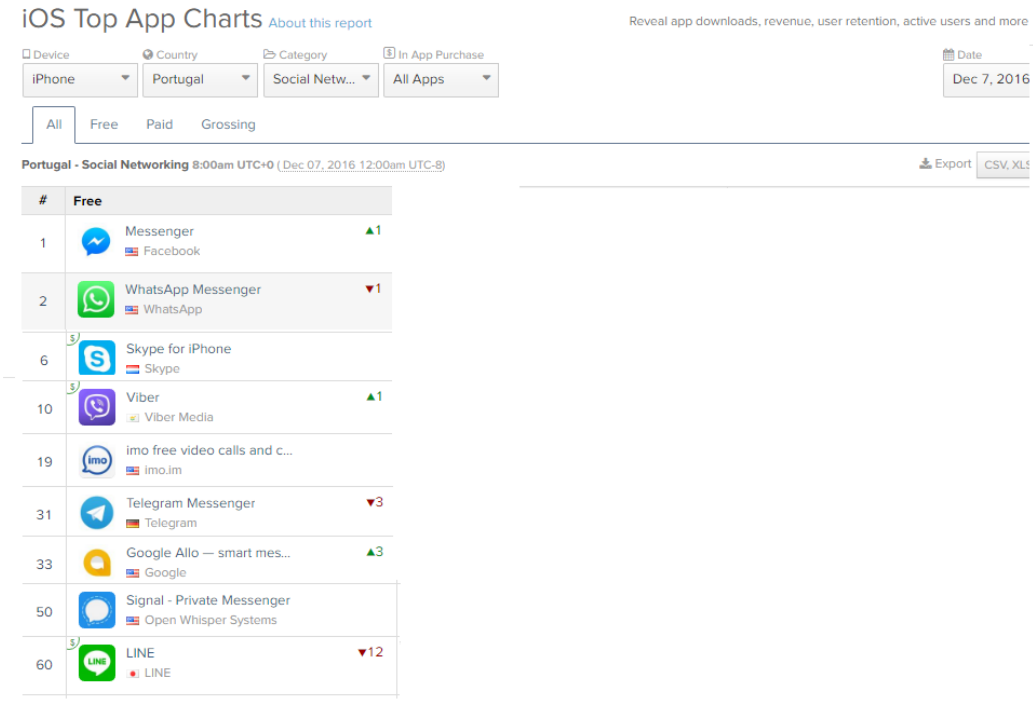


Figura 36 – Aplicações mais utilizadas da categoria "social networking" Fonte: (App Annie, 2016) **Data da consulta: 7-12-2016.**

Como podemos observar na Figura 36, as aplicações Messenger, WhatsApp, Skype e Viber são das mais usadas, o que vem comprovar as figuras anteriores. De notar que a bandeira que se encontra em cada aplicação é referente ao país que dá suporte à mesma. O país a que se aplica é Portugal.

Foi efetuada uma pesquisa no website https://www.apptweak.com conseguimos obter as aplicações grátis da categoria "*Social Networking*" mais usadas em iOS como mostra a Figura 37.

Figura 37 – Aplicações mais usadas da categoria "*social networking*". Fonte:(TechSnoops LLC, 2016) **Data da consulta: 7-12-2016.**

Como pudemos observar na Figura 37, as aplicações "Messenger", "WhatsApp", "Skype", "Viber" e "imo" são das mais usadas, o que vem comprovar as figuras anteriores.

4.3. Software utilizado

Nesta secção apresentamos o *software* utilizado durante a realização do caso de estudo. Na Tabela 14 está apresentada a lista de *software* está incluído *software* forense e ferramentas de análise.

Tabela 14 – Software utilizado no projeto.

Software utilizado	Objetivo
XRY	*Software* forense que permite aquisição de dados nos dispositivos móveis.
XAMN	*Software* forense que permite a leitura das imagens geradas pelo XRY para análise e exportação dos dados adquiridos dos dispositivos.
Autopsy	*Software* forense que permitiu a análise dos dados adquiridos dos dispositivos através dos ficheiros exportados pelo XRY.
Vmware Workstation Player	Software de virtualização utilizado para virtualizar o sistema operativo Ubuntu com objetivo de analisar os dados de determinados formatos através de ferramentas linha de comandos.
SQLite Browser	Ferramenta para abertura de ficheiros de base de dados com extensão “.db”, “.sqlite”, “.sqlitedb” entre outros utilizada para análise manual dos ficheiros.
Plist Viewer	Software para abrir ficheiros de formato. plist. E poder analisar os dados
GeoSetter	Software utilizado para obtenção de dados das fotografias, nomeadamente a localização GPS.

4.4. Ferramentas para aquisição de dados

Nesta secção identificamos ferramentas, assim como hardware forense específico utilizado no projeto. A Tabela 15 apresenta essa informação.

Tabela 15 – Ferramentas e hardware forense utilizado.

Ferramenta / Hardware	Objetivo
Comando file	O comando file permitiu identificar os tipos de ficheiros.
Comando Strings	O comando permitiu extrair palavras (*strings*) de um determinado ficheiro (ascii, utf-8, ou utf-16).
Exiftool	Ferramenta / comando que permitiu obter os dados de gps de fotografias.
Bloqueador de escrita XRY	*Hardware* Forense utilizado para aquisição de dados dos dispositivos sem que houvesse alteração da integridade dos dados.

4.5. Ficheiros importantes

Foram encontrados diversos tipos de ficheiros nas aquisições e análise efetuadas. Nesta secção identificamos os vários tipos de ficheiros importantes. A Tabela 16 é um resumo desses tipos de ficheiros importantes encontrados (Channels & Social, 2012).

Extensão do ficheiro	Descrição
.plist	Formato proprietário da Apple, (*property list file*).
.sqlite , .sqlitedb, .db , .data e .storedata	Formato de ficheiro de base de dados.
.supp	Formato de aplicações iOS.
.blog	Ficheiro do tipo Blog File Extension.
.binarycookies	Ficheiro do tipo "persistent Cookies".
.jpg	Ficheiro do tipo "Photographic Expert Group File Format" que contém uma imagem.
.thumb	Ficheiro do tipo " Thumbnail Image", miniatura de imagem.

Tabela 16 - Tipos de ficheiros importantes encontrados durante a fase de análise.

De seguida são descritos alguns tipos de ficheiros mais importantes referidos na Tabela 16, nomeadamente os ficheiros ".plist", ".sqlite", ".jpg", ".thumb" e ficheiros com localização gps agregada.

4.5.1. Ficheiros “.pllist”

Os ficheiros com extensão. plist, são denominados de (*property list files)* são que guardam configurações do sistema operativo e de algumas aplicações (metadados, propriedades, e atributos de aplicações do equipamento ou dos ficheiros, inclusive chaves de autenticação). Estes ficheiros são codificados na codificação UTF-8 são baseados em texto e podem estar formatados em XML (eXtensible Markup Language). Na maior parte das vezes os ficheiros “.plist” contém caracteres (string) , valores boleanos (verdadeiro ou falso), caracteres em binário e informações importantes do ponto de vista forense (Altheide & Carvey, 2011; Carpene, 2011; Morrissey, 2010).

Segundo (Apple, 2017), o nó “*root*” é um dicionário com um conjunto de chaves e valores. O sistema utiliza estas chaves e valores para obter informação sobre a configuração de uma dada aplicação. Por norma, um ficheiro deste formato com informações é denominado “Info.plist”.

As Figuras Figura 38, Figura 39 e Figura 40 mostram exemplos de ficheiros “.plist”

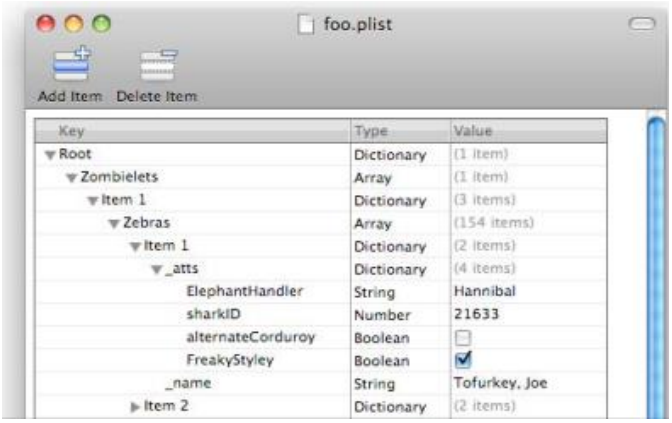


Figura 38 - Ficheiro ".plist" Retirado de: (Epifani & Stirparo, 2015)**.**

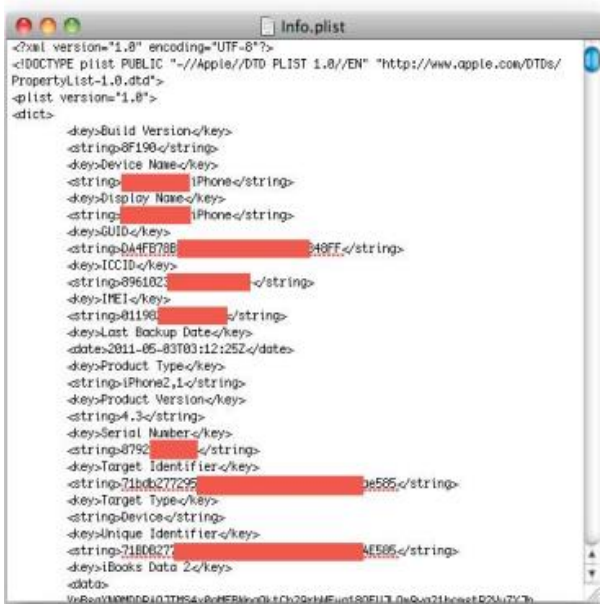


Figura 39 – Ficheiro ".plist" Retirado de: (Epifani & Stirparo, 2015)**.**

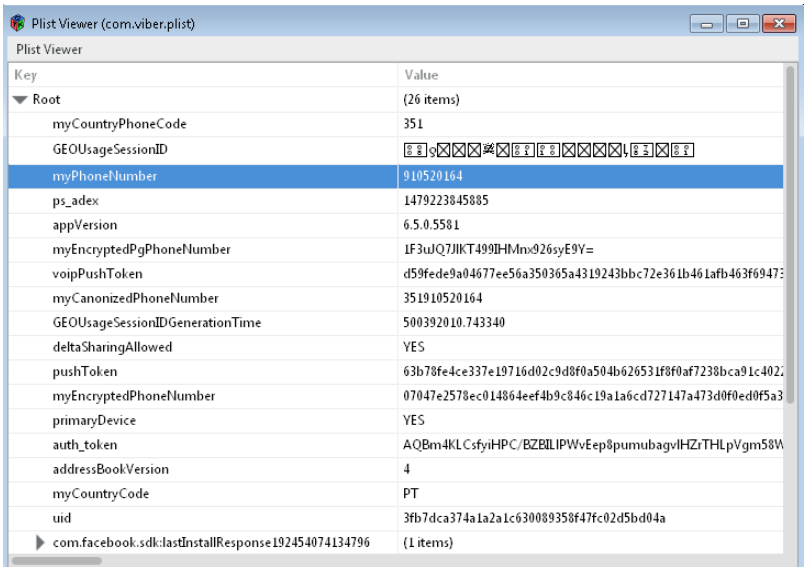


Figura 40 – Ficheiro ".plist" obtido de um iPhone 6.

No que toca a ficheiros de cópias de segurança a Apple guarda também informação em ficheiros de extensão ".plist" como mostra a Tabela 17, descrevendo 3 ficheiros importantes.

Tabela 17 - Ficheiros ".plist" importantes. Baseado em : (Epifani, 2013; Morrissey, 2010)**.**

Nome do ficheiro	Descrição
Info.plist	Ficheiro que contém informação sobre o *iPhone* como o nome, o modelo, a versão de *firmware*, e identificadores do dispositivo.
Manifest.plist	Ficheiro que contém uma lista de aplicações do dispositivo.
Status.plist	Ficheiro que contém informações sobre as cópias de segurança do dispositivo.

Do ponto de vista forense é importante ter *software* apropriado para ler ficheiros ".plist", como o software (*plist viewer*) para analisar todos os ficheiros deste tipo. Este software irá mostrar os dados de uma forma mais ordenada.

4.5.2. Ficheiros de base de dados

O iOS existe um conjunto de ficheiros de base de dados. São esses os ficheiros de extensão ".sqlite", ". sqlitedb", ".db", ".data" e ". storedata".

Ficheiros ".SQLite"

Os dispositivos móveis como o iPhone utilizam as bases de dados SQLite para guardar informação (Morrissey, 2010) .

SQLite é um software de base de dados *open source* com um formato leve para o sistema para que possa ser fácil e rápido de aceder aos dados. Os ficheiros desta extensão são pequenas bases de dados, tratando-se de uma base de dados local. O aumento da utilização de dispositivos móveis e por sua vez a crescente quantidade de aplicações fez com que este tipo de ficheiros fosse cada vez mais adotado. Dessa forma, as aplicações beneficiam do facto destas base de dados ocuparem pouco espaço e serem fáceis de aceder (Lee, Jeon, Bang, & Byun, 2012).

Do ponto de vista forense, estas bases de dados contém bastantes provas.(Lee,2012).

Uma aquisição forense realizada a um iPhone irá obter um número considerável de ficheiros de bases de dados SQLite. O sistema operativo utiliza também estas bases de dados para passar informação entre as mesmas e disponibilizar informação na interface gráfica. Existem essencialmente três bases de dados com informação relevante, contactos, mensagens SMS e registo de chamadas.

A Figura 41 apresenta o resultado da linha de comandos com o comando file para diversos ficheiros de base de dados com as extensões ".sqlitedb", ".storedata", ".data", ".sqlite" e ".db".O comando file interpreta todos os ficheiros como sendo de base de dados sqlite, "SQLite 3.x database".

```
fabio@ubuntu:~/Desktop/db$ file Calendar.sqlitedb
Calendar.sqlitedb: SQLite 3.x database
fabio@ubuntu:~/Desktop/db$ file CallHistory.storedata
CallHistory.storedata: SQLite 3.x database
fabio@ubuntu:~/Desktop/db$ file Contacts.data
Contacts.data: SQLite 3.x database
fabio@ubuntu:~/Desktop/db$ file Photos.sqlite
Photos.sqlite: SQLite 3.x database
fabio@ubuntu:~/Desktop/db$ file Recordings.db
Recordings.db: SQLite 3.x database
fabio@ubuntu:~/Desktop/db$
```

Figura 41 – Resultado do comando file para diversos ficheiros de base de dados.

4.5.3. Ficheiros ".jpg" e ".thumb"

Um ficheiro JPG contém uma imagem guardada num formato standard de imagem comprimido. Este standard foi criado pela JPEG (*Photographic Experts Group*). É comum encontrar ficheiros deste tipo numa série de dispositivos, inclusive os iPhone analisados neste projeto utilizam este formato de imagem. A Figura 42 apresenta o resultado do comando file para um ficheiro com extensão ".jpg".

```
fabio@ubuntu:~/Desktop$ file FotografiaComCoordenadas.jpg
FotografiaComCoordenadas: jpg: JPEG image data, Exif standard: [TIFF image data,
big-endian, direntries=11, manufacturer=Apple, model=iPhone 6 Plus, orientation=
upper-right, xresolution=166, yresolution=174, resolutionunit=2, software=10.1.1
, datetime=2017:01:25 13:04:56, GPS-Data], baseline, precision 8, 3264x2448, fra
```

Figura 42 – Resultado do comando file para um ficheiro de imagem .jpg.

Os ficheiros ".thumb" são do tipo *JAlbum Thumbnail File*. São pequenas miniaturas geradas a partir das imagens originais, que ocupam pouco espaço, para que seja possível visualizar várias fotos ao mesmo tempo de uma forma rápida.

4.5.4. Ficheiros com localização GPS

Tendo em conta as informações estudadas anteriormente, existem determinados ficheiros com dados de localização de GPS, nomeadamente fotografias. Foram utilizadas 3 ferramentas distintas para provar a existência de dados de localização. Um website, um software e a linha de comandos do ubuntu.

A Figura 43 apresenta uma fotografia que foi carregada para o website http://www.geoimgr.com/en/tool que por sua vez continha dados de localização que são apresentados.

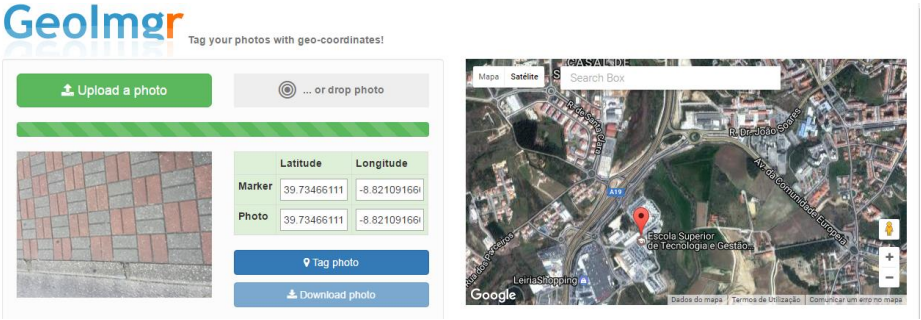


Figura 43- Fotografia com dados de localização interpretada através do website http://www.geoimgr.com/en/tool.

A Figura 44 apresenta a utilização da aplicação GeoSetter para obter os dados de localização de uma fotografia.

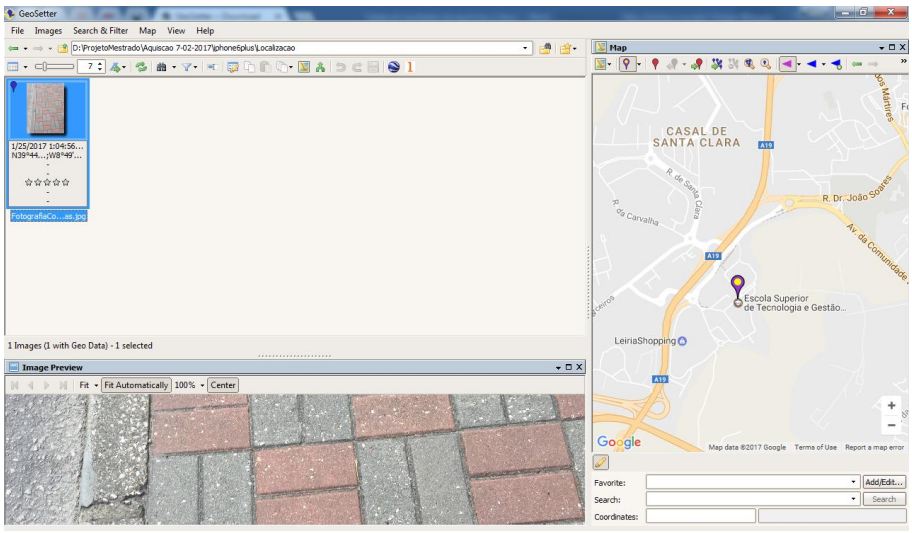


Figura 44 – Utilização da aplicação GeoSetter para obter os dados de localização de uma fotografia.

A Figura 45 apresenta o resultado do comando "exiftool" para uma imagem com dados de localização.

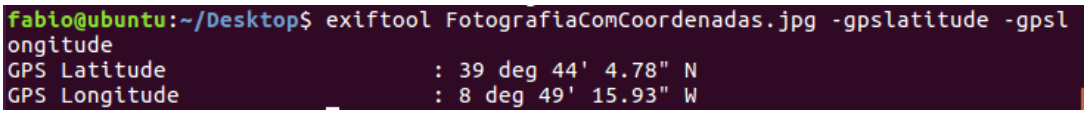


Figura 45 – Resultado do comando exiftool para uma imagem com dados de localização.

4.6. Resultados da aquisição de dados

O foco do caso de estudo está na aquisição e análise dos dados. Nas secções seguintes vão ser apresentados os resultados das aquisições forenses realizadas aos dispositivos, incidindo nas aplicações estudadas. Foram efetuadas várias aquisições, das quais foram criados os seguintes anexos da Tabela 18.

Tabela 18 – Lista de anexos resultantes da aquisição e análise efetuada no projeto.

Nome do ficheiro	Data das aquisições
Tabela de resultados da aquisição Parte 1.pdf	7-11-2016 22-11-2016
Tabela de resultados da aquisição Parte 2.pdf	25-01-2017 31-01-2017 07-02-2017

Nota importante:

As diferenças encontradas nas aquisições diferem tanto das atualizações dos sistemas operativos dos dispositivos móveis, assim como da atualização de software que foi feita ao XRY, que capacita o software de maiores capacidades de encontrar dados.

A Tabela 19 apresenta as funcionalidades mais importantes das aplicações testadas.

Tabela 19 – Funcionalidades das aplicações.

Aplicação	Empresa Associada	Mensagem de texto	Chamada de Vídeo	Chamada de Voz	Anexos
Google Alo	Google	SIM			SIM
Cyphr	Golden Frog	SIM		SIM	SIM
Imo	imo.im	SIM	SIM	SIM	SIM
Line	Line Corporation	SIM	SIM	SIM	SIM
Messenger	Facebook	SIM	SIM	SIM	SIM
Signal	whispersystems	SIM	SIM (1)	SIM	SIM
Skype	Microsoft	SIM	SIM	SIM	SIM
Telegram	Telegram Messenger LLP	SIM			SIM
Viber	Viber Media SARL	SIM	SIM	SIM	SIM
Whatsapp	Facebook	SIM	SIM	SIM	SIM
iMessage	Apple	SIM			

(1) – Já é possível, devido a uma atualização recente.

Em baixo, na Tabela 20 apresentamos o resultado para as aplicações estudadas. De notar que podem existir diferenças nos resultados da aquisição para os diversos sistemas operativos, tendo em conta as diferentes versões do mesmo e as versões do software XRY que foram utilizadas.

Tabela 20 – Dados obtidos das aplicações.

	Número do cartão	Contas de utilizador	Contactos	Mensagens de texto	Anexos trocados	Registo de Chamadas	Fotos perfil	Chave privada	Endereços IP
Google Alo	✓								
Cyphr		✓		✓	✓			✓	
Imo	✓	✓	✓	✓	✓				
Line	✓	✓	✓	✓	✓	✓			
Messenger	✓	✓	✓					✓	
Signal									✓
Skype	✓	✓							✓
Telegram	✓		✓				✓		
Viber	✓	✓	✓	✓	✓		✓		
Whatsapp	✓	✓	✓	✓	✓	✓	✓		✓
iMessage				✓					

A Tabela 21 apresenta parte dos dados encontrados e respetivos ficheiros dos dispositivos móveis Apple relativamente às mensagens, número do cartão SIM, registo de chamadas, contas de utilizador, histórico web, websites favoritos, fotografias de aplicações e da câmara, redes wi-fi, lista de contactos, registos de gps e eventos / registos de calendário. Algumas informações foram obtidas através da pesquisa e análise manual de cada ficheiro. Foi também consultada informação nos artigos (Morrissey, 2010; Satish B, 2011).

Tabela 21 – Dados obtidos e localização dos mesmos.

Dados	Localização do ficheiro ou pasta
Localização principal dos dados das aplicações	/private/var/mobile/Containers/Data/Application/ ou /private/var/mobile/Containers/Shared/AppGroup/
Localização principal de fotografias e imagens	/private/var/mobile/Media/
Fotografias da camara	/private/var/mobile/Media/DCIM/100APPLE/
Mensagens do dispositivo	/private/var/mobile/Library/SMS/sms.db
Número de telemóvel do cartão SIM inserido no dispositivo	/private/var/wireless/Library/Databases/CellularUsage.db
Histórico de Chamadas do dispositivo	/private/var/mobile/Library/CallHistoryDB/ CallHistory.storedata
Contas de utilizador no dispositivo	/private/var/mobile/Library/Accounts/Accounts3.sqlite
Histórico web da aplicação Safari	/private/var/mobile/Containers/Data/Application/ com.apple.mobilesafari/Library/Safari/History.db
Base de dados de fotografias	/private/var/mobile/Media/PhotoData/Photos.sqlite
Conta de utilizador gmail	/private/var/mobile/Containers/Data/ Application/com.google.Gmail/Library/Preferences/ com.google.Gmail.plist
Contas de utilizador de e-mail para os quais foram enviados e-mails.	/private/var/mobile/Containers/Shared/AppGroup/ group.com.google.Gmail/ Library/Preferences/group.com.google.Gmail.plist

Redes Wi-fi a que o dispositivo esteve ligado ou foram detetadas.	/private/var/preferences/SystemConfiguration/ com.apple.wifi.plist
Lista de contactos	/private/var/mobile/Library/AddressBook/ AddressBook.sqlitedb
Imagens dos contactos do dispositivo e dados dos contactos	/private/var/mobile/Library/AddressBook/ AddressBookImages.sqlitedb
Chamadas dos dispositivos	/private/var/wireless/Library/CallHistory/call_history.db
Websites favoritos que foram guardados.	/private/var/mobile/Library/Safari/Bookmarks.db
Registos de GPS	/private/var/root/Library/Caches/locationd/consolidated.db
Eventos de calendário e notas	/private/var/mobile/Library/Calendar/Calendar.sqlitedb
Nome do dispositivo e configurações de rede relativamente ao cartão SIM	/private/var/preferences/SystemConfiguration/preferences.plist

A Tabela 22 apresenta os tipos de dados encontrados e respetivos ficheiros relativamente às aplicações testadas.

Tabela 22 - Tabela com tipos de dados e ficheiros com provas importantes relativos às aplicações estudadas.

Dados	Localização do ficheiro
Google Alo – Número de telemóvel do cartão SIM	/private/var/mobile/Containers/Data/ Application/com.google.fireball/Library/ Preferences/ com.google.fireball.plist
Cyphr - Chave privada, registo de conversas entre contactos, nomes dos contactos e contas de utilizador com quem se trocou texto e anexos	/private/var/mobile/Containers/ Data/Application/com.goldenfrog. cyphr.mobile/Documents/ Cyphr.sqlite
Cyphr – Pasta com anexos trocados durante conversas	/private/var/mobile/Containers/Data/ Application/com.goldenfrog.cyphr.mobile/ Documents/cyphr/
Imo - Número de telemóvel relativo ao cartão instalado no dispositivo e nome da conta de utilizador da aplicação	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/Preferences/ group.im.imo.plist
Imo - Número de telemóvel de um dos contactos com quem se trocou texto e imagens.	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/Preferences/ ioimiphone.plist
Imo - Número de telemóvel da conta da aplicação e número de telemóvel de um contacto com quem se trocou texto e imagens.	/private/var/mobile/Containers/ Data/Application/imoimiphone/Documents/ imo_state.dat
Line - Número de telemóvel relativo ao cartão instalado no dispositivo e nome da conta de utilizador da aplicação.	/private/var/mobile/Containers/Data/ Application/jp.naver.line/Library/Preferences/ jp.naver.line.plist

Line - Lista de contactos da aplicação com nome e número de telemóvel e mensagens trocadas entre os contactos e respetivos números de telemóvel. Registo de chamadas efetuadas.	/private/var/mobile/Containers/ Shared/AppGroup/group.com.linecorp.line/ Library/ ApplicationSupport/PrivateStore /P_u8b9ad4ec8bc4325393881a1 d47a96ec8/Messages/Line.sqlite
Line - informação de uma chamada de vídeo recebida e o nome do contacto.	/private/var/mobile/Library/SpringBoard /PushStore/ jp.naver.line.pushstore.plist
Line – pasta de anexos trocados.	\private\var\mobile\Library\Application Support\PrivateStore\ P_u8b9ad4ec8bc4325393881a1d47a96ec8\Message Attachments
Messenger - Chave privada e nome de utilizador da aplicação.	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/ com.facebook.Messenger.plist
Messenger - informação dos contactos da aplicação Messenger e respetivos nomes.	/private/var/mobile/Library/SpringBoard /ApplicationShortcuts/ com.facebook.Messenger.plist
Signal - Informação de uma chamada recebida e do respetivo contacto.	/private/var/mobile/Containers/Data/ Application/org.whispersystems.signal/ Library/Preferences/private/var/ mobile/Library/SpringBoard/PushStore/
Skype - informação da conta de utilizador do utilizador da aplicação.	/private/var/mobile/Containers/Data/ Application/ com.skype.skype/Library/Preferences/ com.skype.skype.plist
Skype - informação de um dos contactos com os quais foram trocados texto e anexos.	/private/var/mobile/Library/SpringBoard/ PushStore/ com.skype.skype.pushstore.plist

Telegram – Informação sobre os contactos com quem se trocou texto e anexos	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/ ph.telegra.Telegraph.plist
Telegram - informação de um dos contactos, nomeadamente o nome da conta.	/private/var/mobile/Library/ SpringBoard/PushStore/ ph.telegra.Telegraph.pushstore
Viber - informação relativa ao número de telemóvel associado à conta de utilizador.	/private/var/mobile/Containers/Data/Application/ com.viber/Library/Preferences/com.viber.plist
Viber - Fotografia do perfil de utilizador da conta local.	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/avatar.jpg
Viber - informação relativa aos contactos com que se trocou informações	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/ Shared.data
Viber – Pasta com anexos trocados durante as conversas entre contactos.	/private/var/mobile/Containers/ Data/Application/com.viber/ /Documents/Attachments
Viber - Miniaturas das fotos de perfil da conta de utilizador.	/private/var/mobile/Containers/ Data/Application/com.viber/ Documents/ViberIcons
Viber - mensagens trocadas contactos da aplicação, números de telemóvel, registo de anexos trocados, registos de chamadas feitas e recebidas	/private/var/mobile/Containers/ Data/Application/com.viber/ Documents/contacts.data
Viber - número de telemóvel associado à aplicação	/private/var/mobile/Containers/ Data/Application/com.viber/Documents/ Settings.data
WhatsApp – Contactos bloqueados	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/ blockedcontacts.dat.plist
WhatsApp - registos de Chamadas com duração entre outros dados e os respetivos nomes de utilizador e números de telemóvel e registo dos contactos com quem se efetuou chamadas	/private/var/mobile/Containers/Data/ Application/ net.whatsapp.WhatsApp/Documents/ calls.backup.log.plist
WhatsApp - registos de Chamadas e os respetivos nomes de utilizador e números de	/private/var/mobile/Containers/Data/ Application/

telemóvel e registo dos contactos com quem se efetuou chamadas	net.whatsapp.WhatsApp/Documents/ calls.log.plist
WhatsApp – Pasta com ficheiros ".log" com registos de números de telemóvel associados às contas de utilizador dos contactos e do utilizador local, nome da operadora associada ao cartão SIM e registos de chamadas.	/private/var/mobile/Containers/ Data/Application/net.whatsapp. WhatsApp/Library/Logs/
WhatsApp – Pasta com anexos trocados durante o chat.	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Library /Media
WhatsApp - números de telemóvel associados às contas de utilizador com quem o utilizador trocou mensagens no chat.	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/ Library/Preferences/UITextInput ContextIdentifiers.plist
WhatsApp - Contém, para cada contacto do chat o registo de texto trocado nas conversas	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/ ChatSearch.sqlite
WhatsApp - contactos com quem se trocou mensagens no chat, índice de anexos trocados nas mensagens e texto trocado entre as conversas e os respetivos contactos	private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/ChatStorage.sqlite
WhatsApp - contactos do telemóvel	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/Contacts.sqlite
WhatsApp - Número de telemóvel associado à conta de utilizador do whatsapp	/private/var/mobile/ Containers/Shared/AppGroup/ group.net.whatsapp.WhatsApp.shared/ Library/Preferences/ group.net. whatsapp. WhatsApp.shared.plist

WhatsApp – Pasta com foto de perfil do utilizador local e contactos.	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/ Media/Profile/
iMessage - mensagens SMS do dispositivo com o texto trocado e os respetivos números que enviaram as mensagens	/private/var/mobile/Library/SMS/sms.db

4.7. Aplicação Google Allo

A aplicação google allo apenas permitiu a troca de mensagens de texto e ficheiros como imagens ou vídeo. Não permitiu efetuar chamadas de voz ou vídeo.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As versões de iOS eram as 9.2 e 9.2.1.

- Número de telemóvel do cartão SIM e à qual está configurada a aplicação – Ver Figura 46.

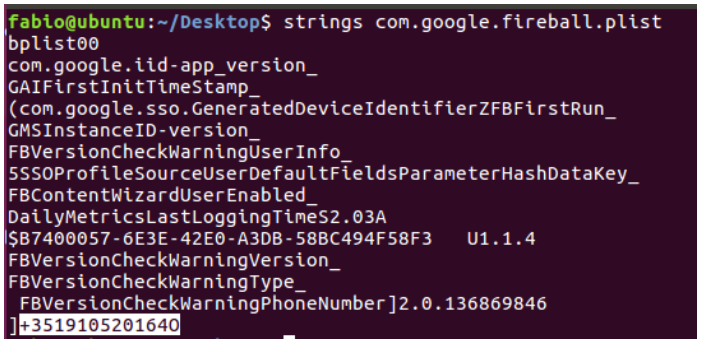


Figura 46 – Número a que está associada a conta allo deste dispositivo.

No iOS 9.3.5 e 10.2.1 foram obtidos ficheiros do tipo sqlite no entanto não foram obtidos mais dados.

Com base na informação analisada depois da aquisição podemos afirmar que do ponto de vista do utilizador, a aplicação Google allo é segura, pois não conseguimos encontrar muita informação, apenas o número de telemóvel. Do ponto de vista forense é uma aplicação da qual conseguimos obter poucos dados, o que pode ser considerado um problema em caso de investigação forense.

4.8. Aplicação Cyphr

A aplicação Cyphr apenas permitiu a troca de mensagens de texto, chamadas de voz e ficheiros como imagens ou vídeo. Não permitiu efetuar chamadas de vídeo.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As versões de iOS eram as 9.3.5 e 10.2.1.

- Chave privada – Ver Figura 47;
- Chaves públicas - Ver Figura 48;
- Mensagem de texto trocada entre os contactos– Ver Figura 49;
- Contas de utilizador utilizadas na aplicação – Ver Figura 50;
- Anexos, imagens trocadas entre utilizadores – Ver Figura 51.

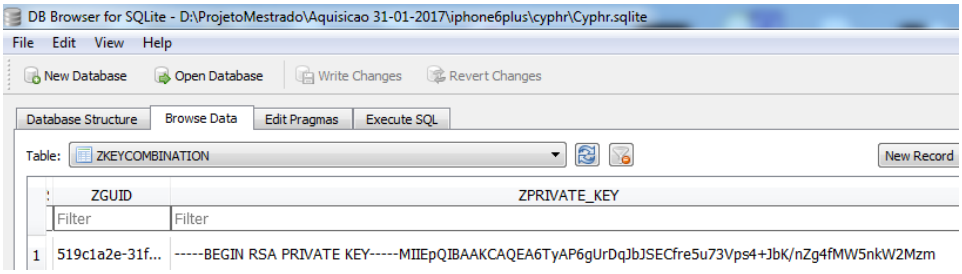


Figura 47 – Chave privada encontrada num dos ficheiros de base de dados, "Cyphr.sqlite"

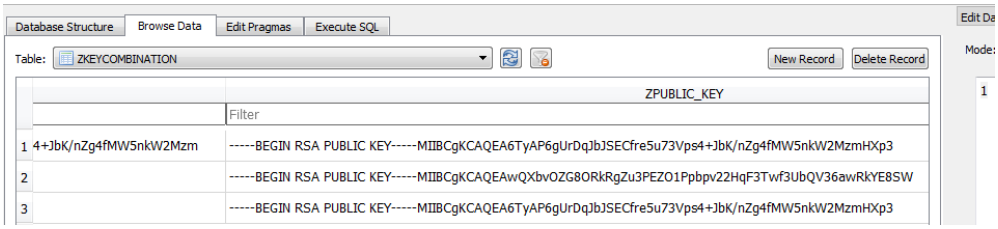


Figura 48 – Chaves públicas encontradas no ficheiro "Cyphr.sqlite"

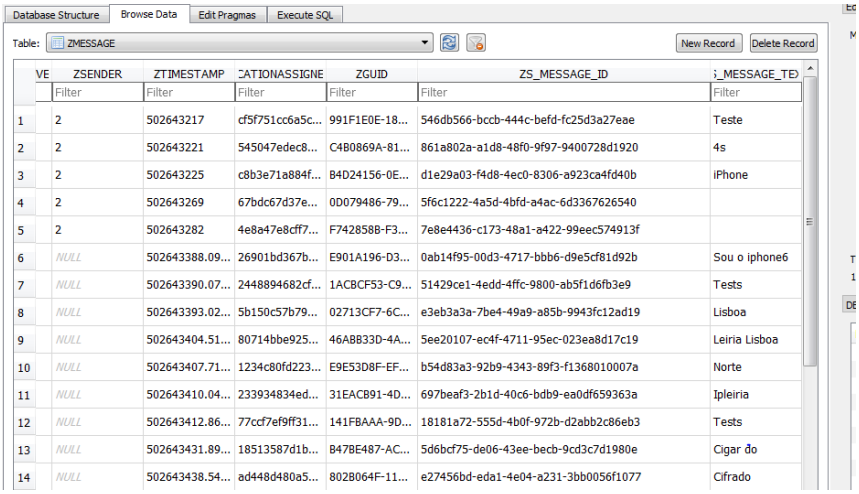


Figura 49 – Mensagens Encontradas no ficheiro "cyphr.sqlite"

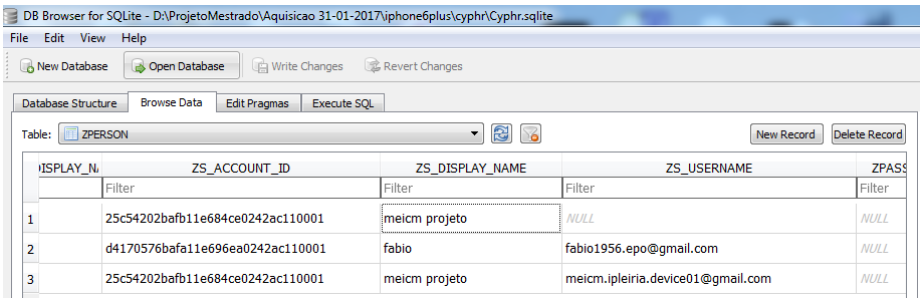


Figura 50 – Contas de utilizador registadas na aplicação.

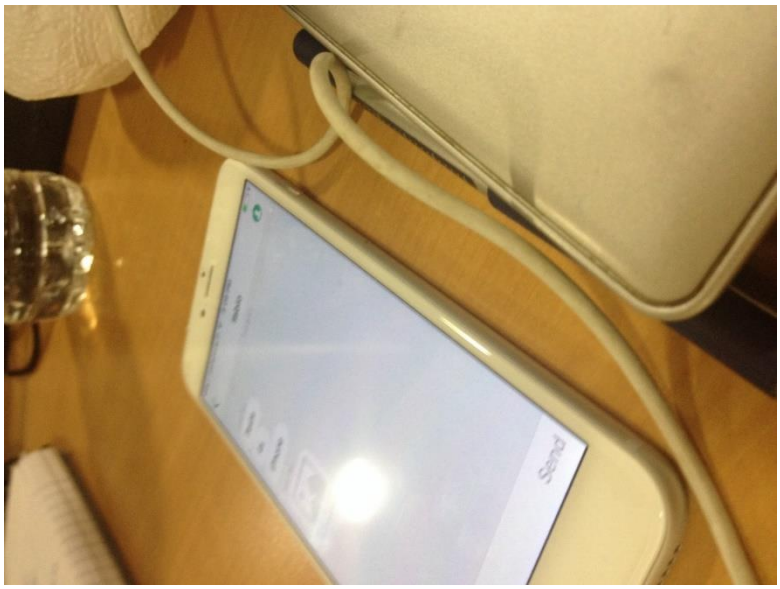


Figura 51 – Anexo trocado durante conversa entre utilizadores da aplicação.

Com base na informação analisada depois da aquisição podemos afirmar que do ponto de vista do utilizador, a aplicação Cyphr não é segura, pois não tem a sua informação devidamente cifrada e protegida. Conseguimos obter uma chave privada assim como uma grande quantidade de dados relativos à aplicação e aos utilizadores da mesma. Do ponto de vista forense é uma aplicação da qual, conseguimos obter alguns dados que podem ser úteis para uma investigação forense.

4.9. Aplicação imo

A aplicação imo permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz e vídeo.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As provas foram obtidas dos dispositivos com iOS 9.2 e 9.2.1

- Número de telemóvel relativo ao cartão SIM instalado no dispositivo – Ver Figura 52;
- Contas de utilizador utilizadas na aplicação- Ver Figura 52 e Figura 53.

Key	Value
Root	(9 items)
verification_time	12268
getstarted_time_start	1479743952626
sends_server_sms	NO
verification_time_start	1479743940141
show_rate_imo	NO
name_age_time	17234
getstarted_time	100655
my_profile_json_key	{"display_name":"Meicm Device","phone_cc":"pt","phone":"+351963155223","uid":"1019320374292917","primitive":"offline"}
name_age_time_start	1479743952441

Figura 52 – Número de telemóvel associado ao cartão SIM e nome de utilizador da conta da aplicação.

Figura 53 – Conta de utilizador da aplicação

No iOS 9.3.5 e 10.2.1 foram encontradas mais provas como apresentadas na seguinte lista:

- Número de telemóvel de um dos contactos – Ver Figura 54 e Figura 55;
- Mensagem de texto trocada entre os contactos – Ver Figura 56.

Figura 54 – Número de telemóvel de um dos contactos da aplicação.

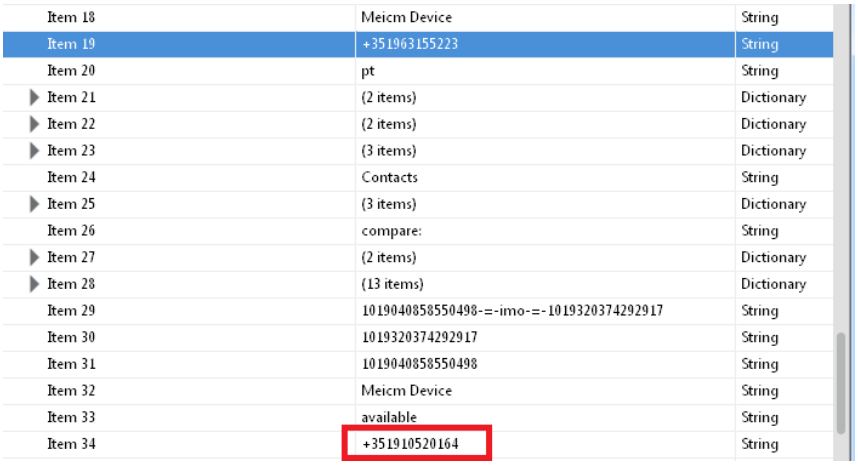


Figura 55 - Número de telemóvel de um dos contactos da aplicação.

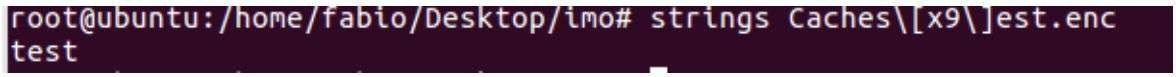


Figura 56 – Parte de mensagem trocada entre utilizadores da aplicação.

Com base na informação analisada depois da aquisição podemos afirmar que do ponto de vista do utilizador a aplicação não é segura uma vez que foi possível obter os números de telemóvel dos contactos, as contas de utilizador e ainda uma pequena parte de uma mensagem. Do ponto de vista forense é uma aplicação da qual, conseguimos obter alguns dados que podem ser úteis para uma investigação forense.

4.10. Aplicação Line

A aplicação line permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz e vídeo.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As versões de IOS eram as 9.2 e 9.2..

- Número de telemóvel relativo ao cartão SIM instalado no dispositivo- Ver Figura 57;
- Nome da conta de utilizador da aplicação;
- Contactos da aplicação - ver Figura 58;
- Número de telemóvel dos contactos da aplicação -ver Figura 58 ;
- Mensagem de texto trocada entre os contactos – ver Figura 59;
- Informação de chamada recebida – Ver Figura 60.

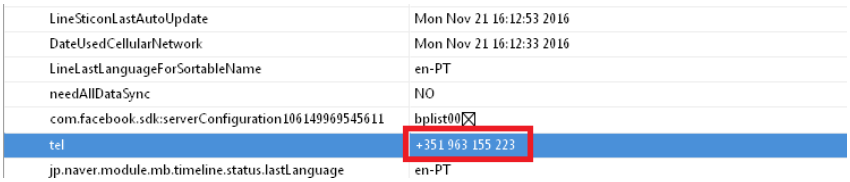


Figura 57 – Número de telemóvel associado ao cartão sim e à aplicação.

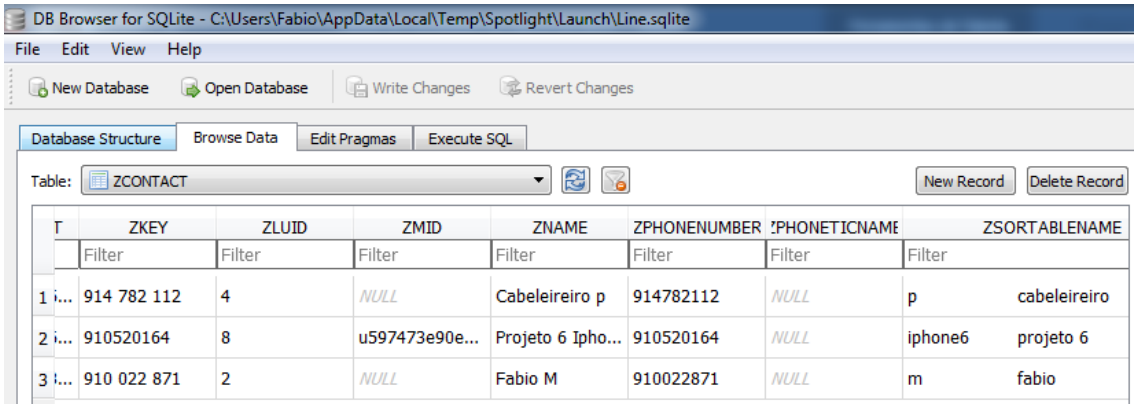


Figura 58 – Contactos da aplicação.

	ZCHAT	ZSENDER	ZLATITUDE	ZLONGITUDE	ZID	ZMESSAGETYPE	ZTEXT	ONTENTME
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	NULL	0.0	0.0	5239185404497	NULL	Call History : ...	BLOB
2	1	1	0.0	0.0	5239188024615	NULL	NULL	BLOB
3	1	1	0.0	0.0	5239188611896	NULL	Teste	NULL
4	1	1	0.0	0.0	5239188771016	NULL	Leiria	NULL
5	1	1	287.0	384.0	5239189229501	NULL	Projeto 6 Ipho...	BLOB
6	1	NULL	0.0	0.0	5239189755934	NULL	Ola	NULL
7	1	NULL	0.0	0.0	5239189862701	NULL	Teste	NULL
8	1	NULL	0.0	0.0	5239190028255	NULL	LisboA	NULL
9	1	NULL	0.0	0.0	5239190261711	NULL	Iphone4s	NULL
10	1	NULL	430.0	572.0	5239190768525	NULL	You sent a ph...	BLOB

Figura 59 – Mensagens de texto trocadas entre os contactos

Item 13	Resposta	String
Item 14	AppNotificationRemote	String
Item 15	Chamada recebida de Meicm device 2	String

Figura 60 – Informação de chamada recebida

Nas versões de iOS 9.3.5 e 10.2.1. foram encontrados os seguintes dados diferentes: Anexos, imagens trocadas entre utilizadores – Ver Figura 61.

Figura 61 – Anexo trocado durante a conversa entre os utilizadores.

Com base na informação analisada depois da aquisição, do ponto de vista do utilizador, podemos afirmar que a aplicação Line não é segura uma vez que foi possível obter os contactos, os números de telemóvel dos contactos, as contas de utilizador, mensagens e ainda alguns anexos. Do ponto de vista forense conseguimos obter alguns dados que podem ser úteis para uma investigação forense.

4.11. Aplicação Messenger (Facebook)

A aplicação messenger permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz e vídeo.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As versões de IOS eram as 9.2 e 9.2.1.

- Certificado SSL – Ver Figura 62;
- Contactos da aplicação – Ver Figura 64;
- Nome da conta de utilizador da aplicação Figura 63 ;
- Facebook Login UUID – ver Figura 65 .

Figura 62 – Certificado SSL encontrado.

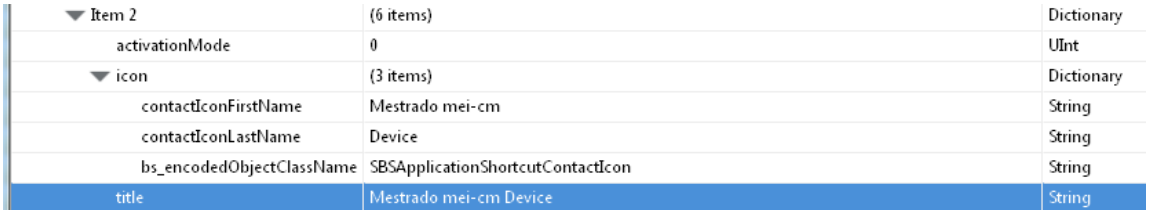


Figura 63 – Nome de utilizador da aplicação

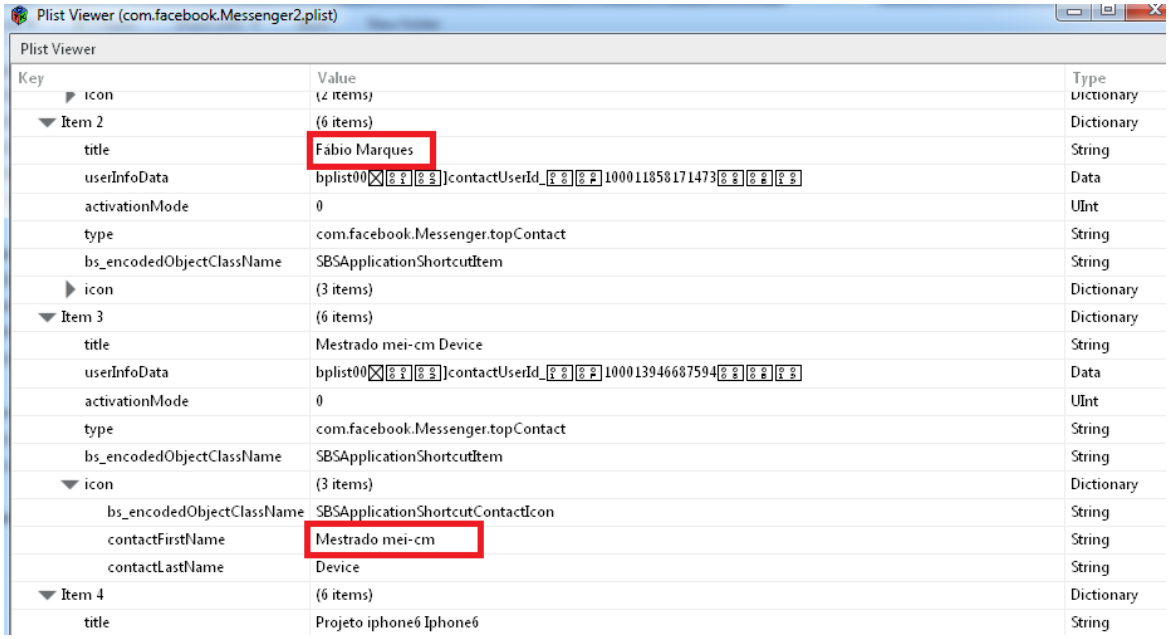


Figura 64 – Contactos da aplicação.

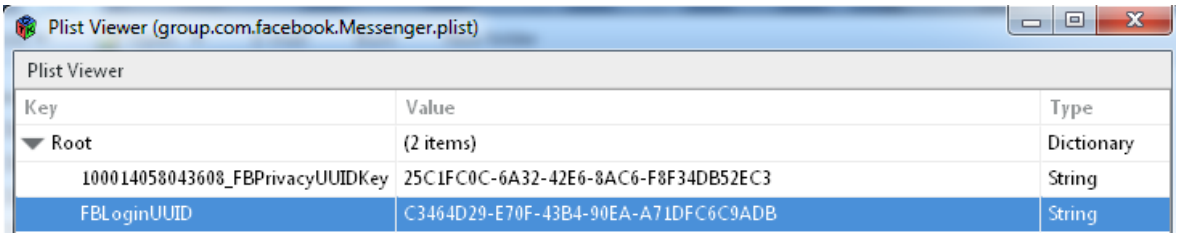


Figura 65 – Facebook login UUID

No iOS 9.3.5 e 10.2.1 foram encontrados mais ficheiros do tipo ".plist" e ".sqlite" entre outros dados como apresenta a seguinte lista:

- Chave privada – Ver Figura 66;
- Chave Privada SSL – Ver Figura 67 ;
- Registo de chamadas da aplicação – ver Figura 68;
- Número de telemóvel relativo ao cartão SIM instalado no dispositivo – Ver Figura 69 .

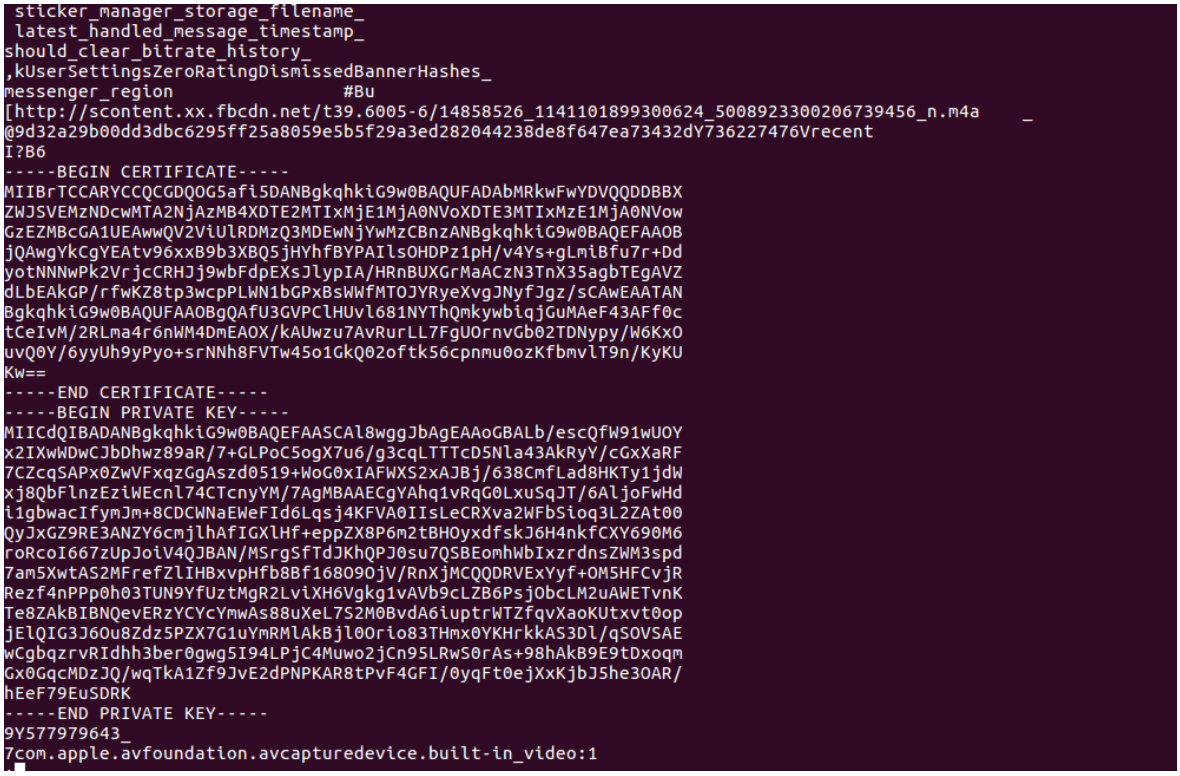


Figura 66 – Chave privada encontrada num dos ficheiros.

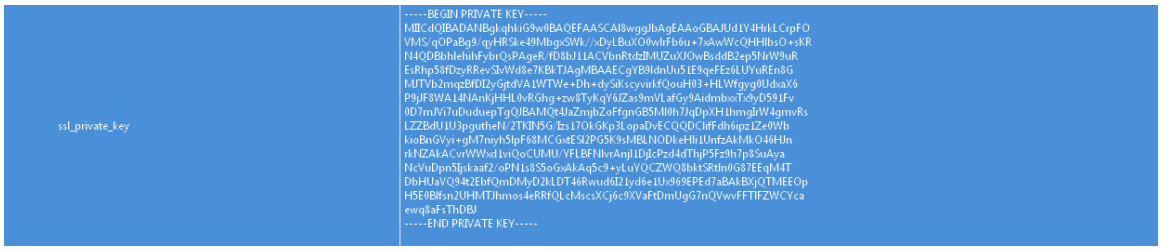


Figura 67 – Chave privada SSL encontrada.

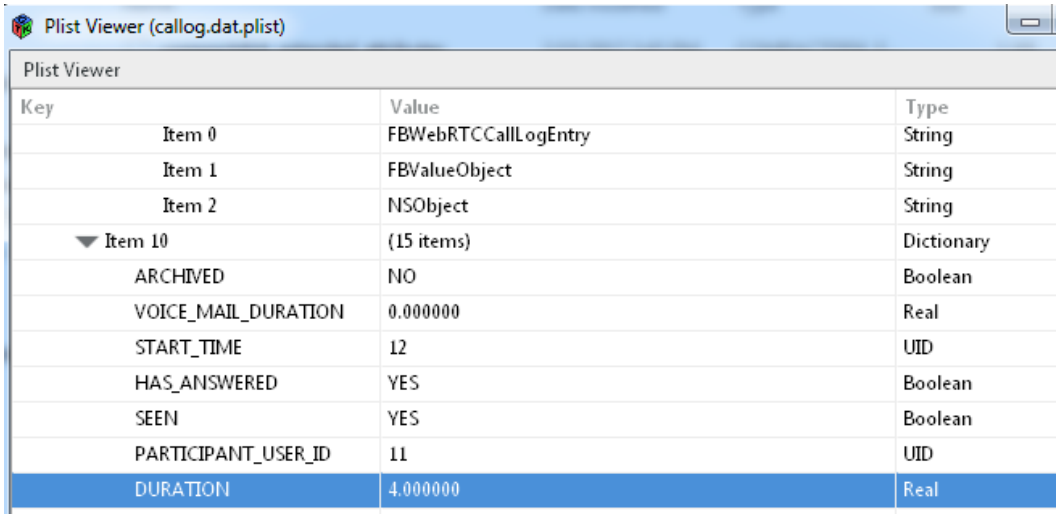


Figura 68 – Registo de chamadas da aplicação

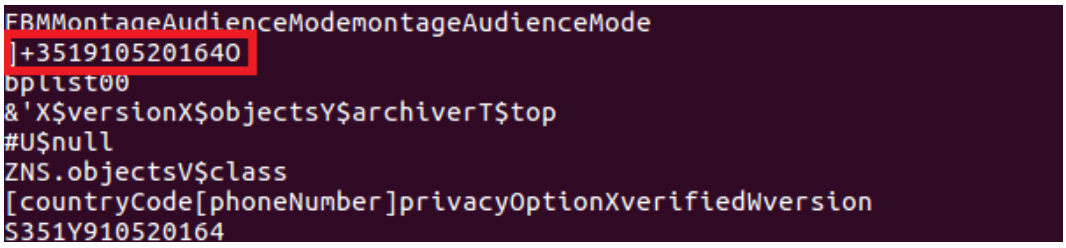


Figura 69 – Número de telemóvel do cartão SIM associado à aplicação.

Com base na informação analisada depois da aquisição podemos afirmar que do ponto de vista do utilizador, aplicação Messenger não é segura nem contém todos os seus dados seguros uma vez que foi possível obter uma chave privada, os contactos da aplicação, certificados SSL, nome da conta de utilizador, o registo de chamadas e um número de telemóvel associado ao cartão sim. Do ponto de vista forense é uma aplicação da qual, conseguimos obter alguns dados que podem ser úteis para uma investigação forense.

4.12. Aplicação Signal

A aplicação Signal permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As provas foram obtidas dos dispositivos com iOS 9.2 e 9.2.1

- Data de instalação da aplicação- Ver Figura 70;
- Hash MD5 – Ver Figura 71;

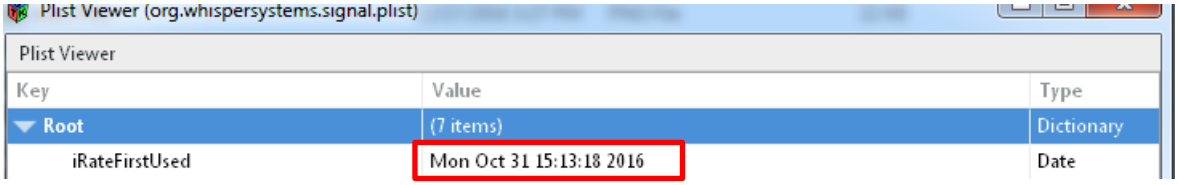


Figura 70 – Data de instalação da aplicação

```
#Bundle id: org.whispersystems.signal
#Old bundle version: 2.6.2.0 2.6.2
#New bundle version: 26315 2.6.3
#Old IPA hash (md5): 03dc7e93a99f6c9b555a9ef9fbf5f437
#New IPA hash (md5): 35b9f1e2ed821c46436945482 98ef2ab
```

Figura 71 - Hash MD5 Encontrada

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As provas foram obtidas dos dispositivos com IOS iOS 9.3.5 e 10.2.1.

- Chamada recebida e do respetivo contacto

Com base na informação analisada depois da aquisição e tendo em conta as aplicações analisadas anteriormente podemos afirmar que do ponto de vista do utilizador, a aplicação Signal é segura uma vez que não foram encontrados dados relevantes. Do ponto de vista forense, torna-se um ponto negativo o facto de não se conseguirem obter dados da aplicação que podiam ser úteis para uma investigação forense.

4.13. Aplicação Skype

A aplicação Skype permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz e vídeo.

Na seguinte lista vamos apresentar as provas que foram encontradas nos dados da aquisição. As versões de IOS eram as 9.2 e 9.2.1.

- Endereços IP e portos – Ver Figura 72e Figura 73 ;
- Nome da conta de utilizador da aplicação - .Ver Figura 74.

```
(Value not set)
ECS_ADSP_DisableSilenceSuppresionFor1To1Calls
ECS_ADSP_EnableSilkSWB
(Value not set)
ECS_ADSP_EnableSilkSWB
f6Qw
        29796a34-706a-4175-822a-c2dcd105ecfd
        <NULL>
        29796a34-706a-4175-822a-c2dcd105ecfd
13.107.8.50
MediaMgrBlob="MrDnsE=13.107.8.50,MrResE=1,MrErrE=0,MrBgnE=36881246551772828,MrEn
dE=36881246551808668,MrDnsCacheReadAttempt=0,BlobVer=1"
        13.107.8.50
        13.107.8.50
        13.107.8.50
        13.107.8.50
```

Figura 72 – Endereços IP encontrados

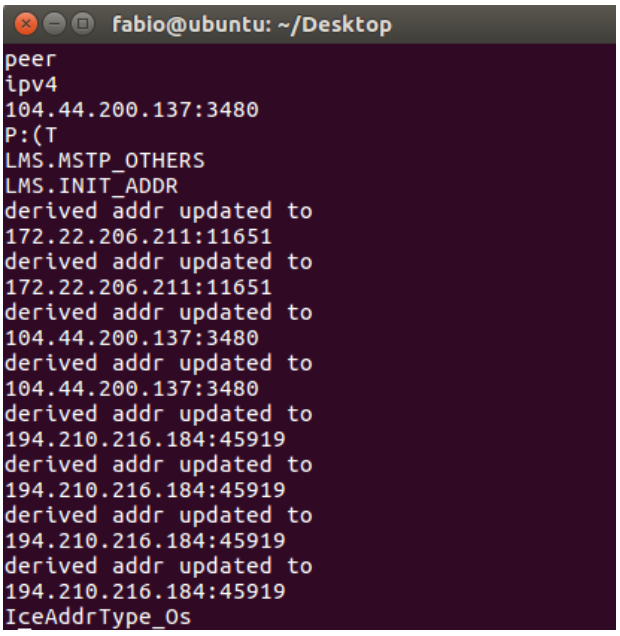


Figura 73 – Endereços IP e portos encontrados.

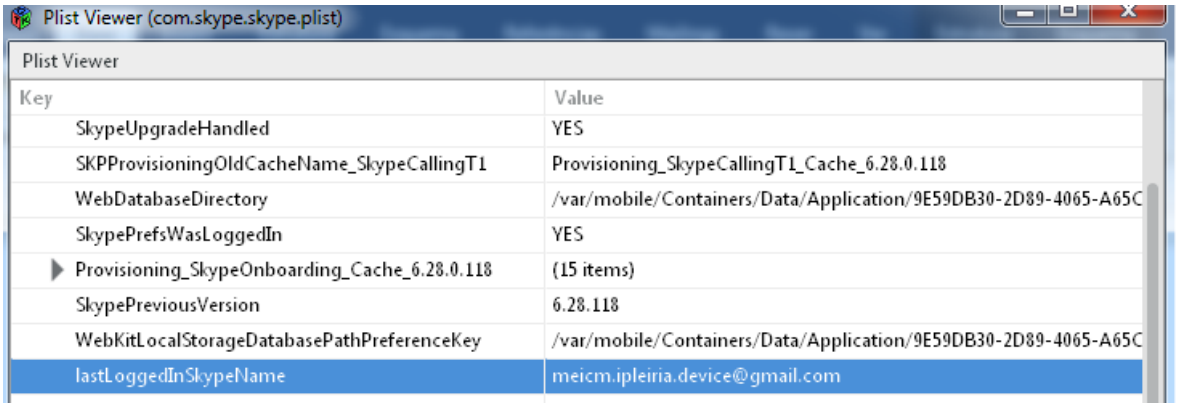


Figura 74 – Nome de utilizador da aplicação

No iOS 9.3.5 e 10.2.1 foram encontrados mais ficheiros do tipo ".plist" e ".sqlite" entre outros dados como apresenta a seguinte lista:

- Número de telemóvel relativo ao cartão SIM instalado no dispositivo

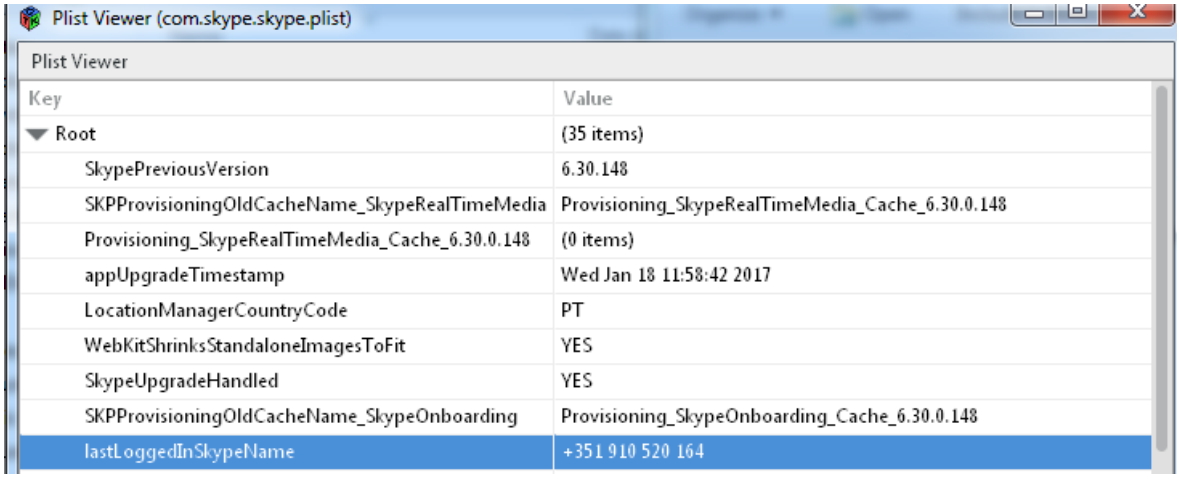


Figura 75 – Número de telemóvel do cartão SIM associado.

Com base na informação analisada e do ponto de vista do utilizador, podemos afirmar que a aplicação Skype não é totalmente segura apesar dos poucos dados que foram adquiridos. Do ponto de vista forense, é uma aplicação que não disponibiliza muita informação, o que pode ser um ponto negativo.

4.14. Aplicação Telegram

A aplicação Signal permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo.

Nas versões de IOS 9.2 e 9.2.1 não foram encontrados dados.

No iOS 9.3.5 e 10.2.1 foram encontrados dados como apresenta a seguinte lista:

- Nome de utilizador dos contactos da aplicação – Ver Figura 76 e Figura 77;
- Anexos trocados durante conversas – Ver Figura 78;

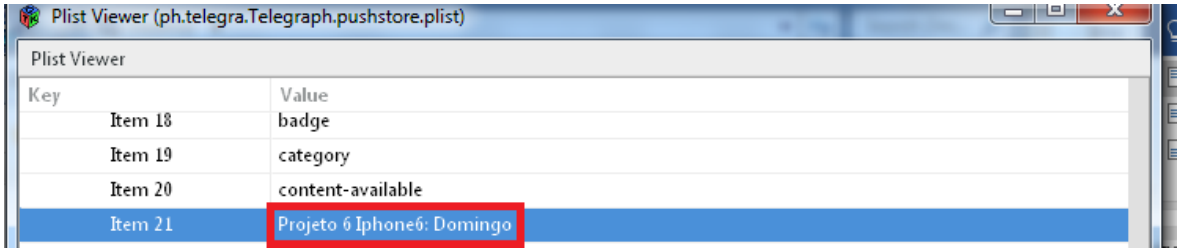


Figura 76 – Um dos contactos da aplicação

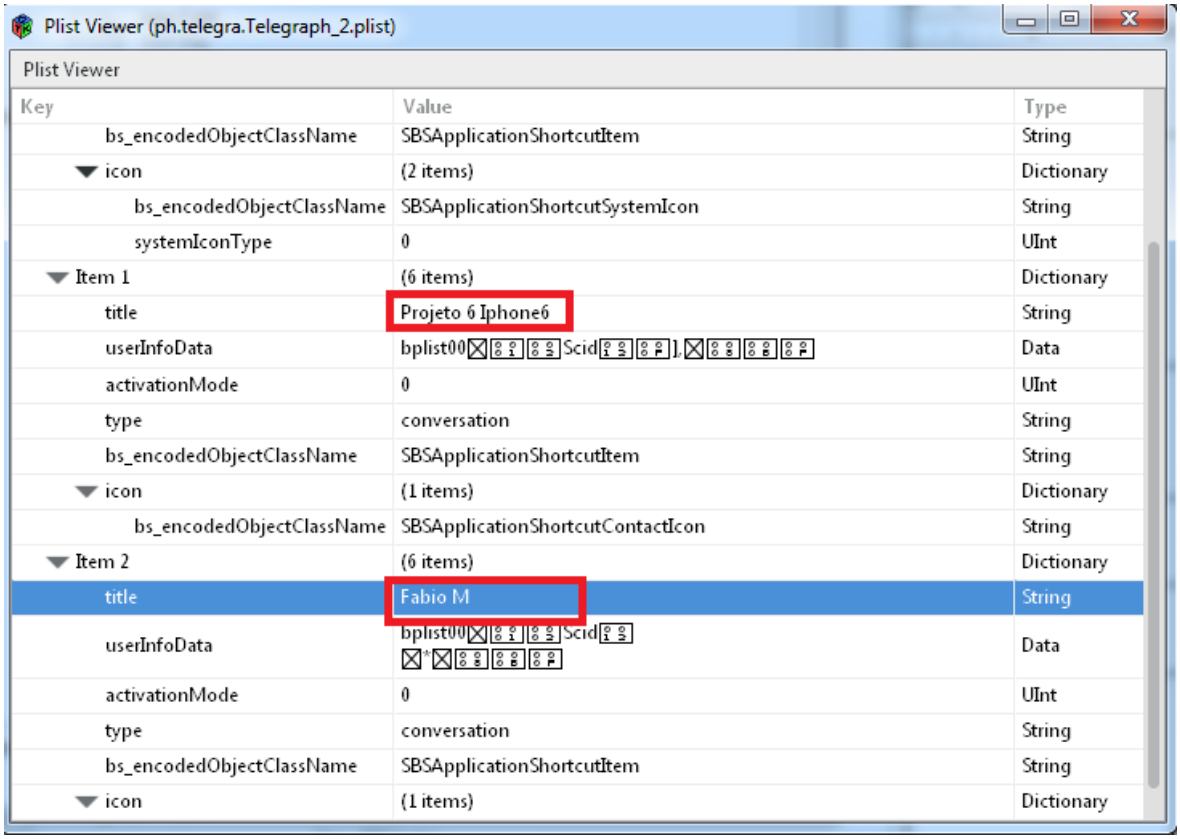


Figura 77 - Um dos contactos da aplicação

Figura 78- Um anexo trocado durante a conversa.

Com base na informação analisada e do ponto de vista forense, podemos afirmar que a aplicação Telegram não contém muitas informações que podem ser obtidas, o que pode ser um ponto negativo do lado forense. Do ponto de vista de utilizador e apesar de mostrar os nomes de utilizador de outras contas podemos considerar a aplicação segura.

4.15. Aplicação Viber

A aplicação Viber permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz e ou vídeo.

Nas versões de IOS 9.2 e 9.2. foram encontrados os dados da seguinte lista:

- Número de telemóvel relativo ao cartão SIM instalado no dispositivo – Ver Figura 79.
- Nome da conta de utilizador da aplicação – Ver Figura 80;
- Fotografia do perfil do utilizador local da aplicação -Figura 81;
- Nome da conta de utilizador dos contactos da aplicação – Ver Figura 82;
- Número de telemóvel dos contactos da aplicação – Ver Figura 82;
- Mensagem de texto trocada entre os contactos - Ver Figura 83;
- Hash MD5 – Ver Figura 84.

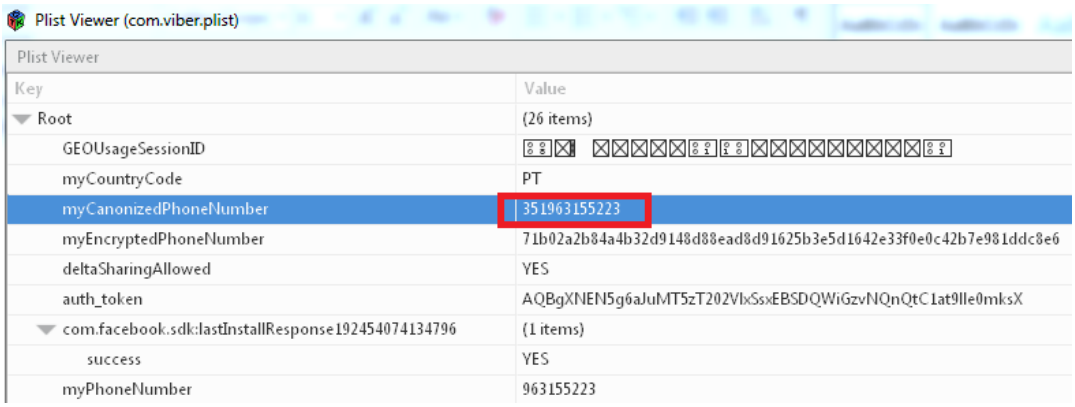


Figura 79 - Número de telemóvel relativo ao cartão SIM instalado no dispositivo.

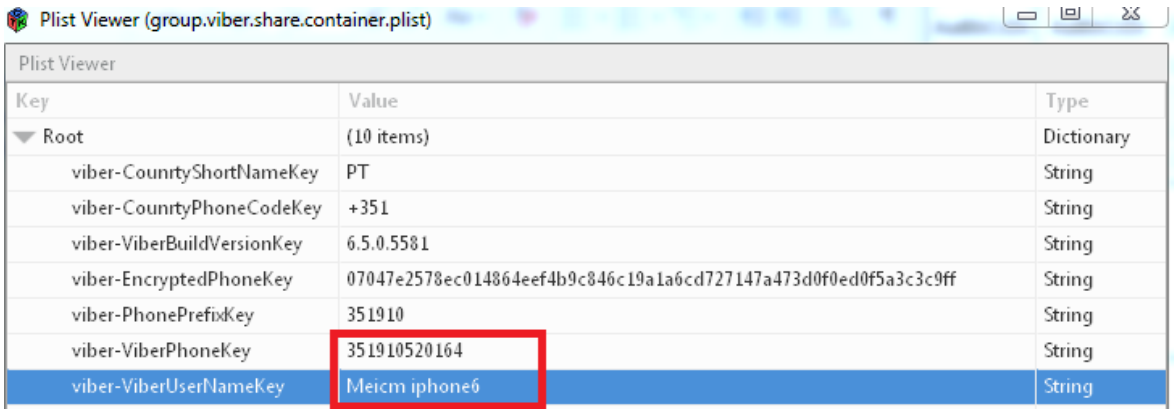
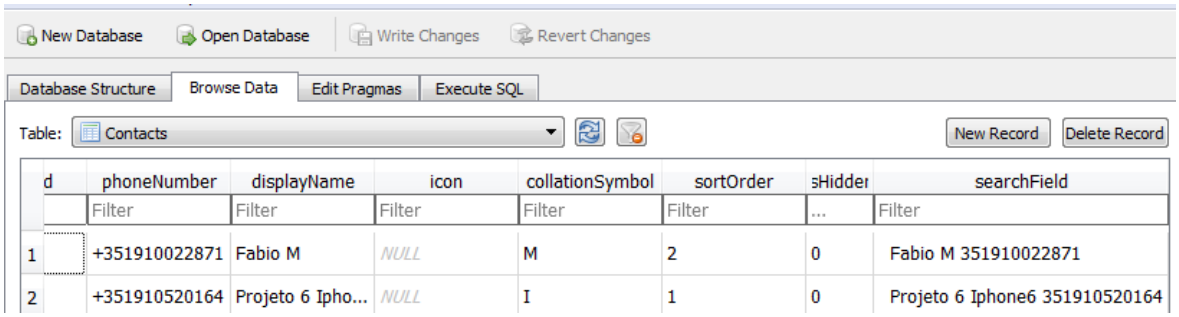


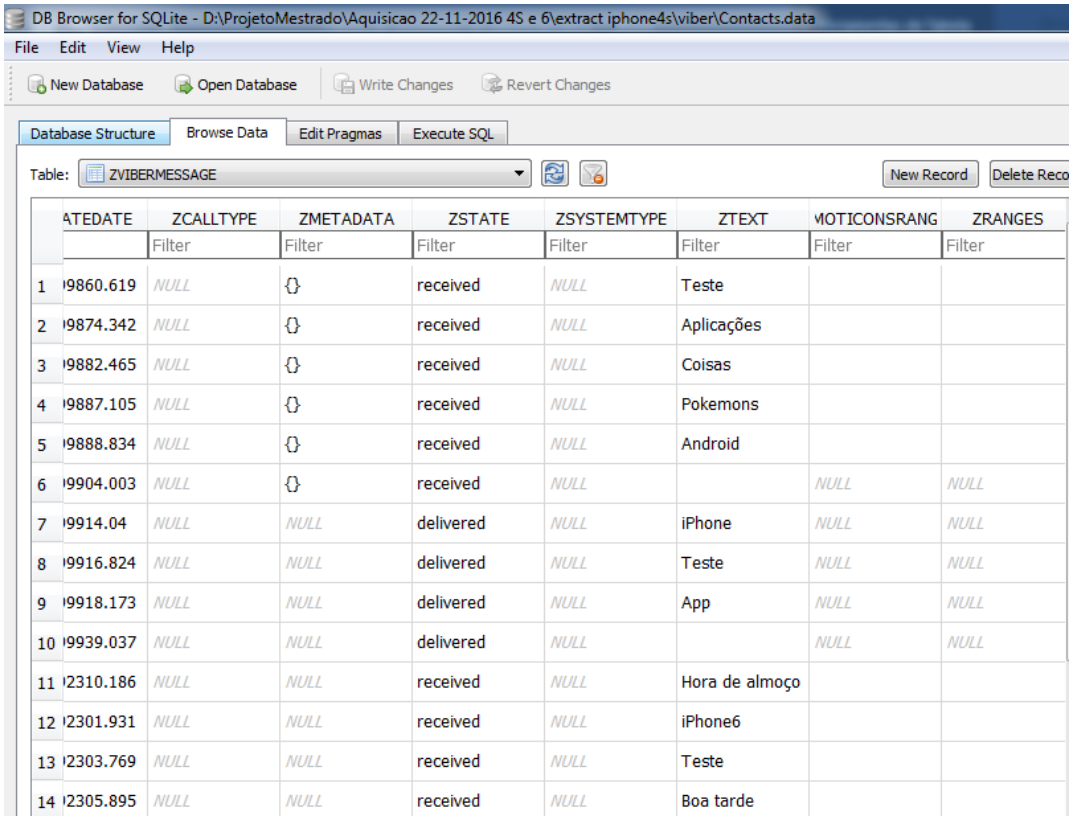
Figura 80 - Nome da conta de utilizador da aplicação e respetivo número de telemóvel.

Figura 81 - Fotografia do perfil do utilizador local da aplicação.



	d	phoneNumber	displayName	icon	collationSymbol	sortOrder	sHidder	searchField
		Filter	Filter	Filter	Filter	Filter	...	Filter
1		+351910022871	Fabio M	NULL	M	2	0	Fabio M 351910022871
2		+351910520164	Projeto 6 Ipho...	NULL	I	1	0	Projeto 6 Iphone6 351910520164

Figura 82 – Contactos da aplicação e respetivos números de telemóvel.



	ATEDATE	ZCALLTYPE	ZMETADATA	ZSTATE	ZSYSTEMTYPE	ZTEXT	MOTICONSRANG	ZRANGES
		Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	9860.619	NULL	{}	received	NULL	Teste		
2	9874.342	NULL	{}	received	NULL	Aplicações		
3	9882.465	NULL	{}	received	NULL	Coisas		
4	9887.105	NULL	{}	received	NULL	Pokemons		
5	9888.834	NULL	{}	received	NULL	Android		
6	9904.003	NULL	{}	received	NULL		NULL	NULL
7	9914.04	NULL	NULL	delivered	NULL	iPhone	NULL	NULL
8	9916.824	NULL	NULL	delivered	NULL	Teste	NULL	NULL
9	9918.173	NULL	NULL	delivered	NULL	App	NULL	NULL
10	9939.037	NULL	NULL	delivered	NULL		NULL	NULL
11	2310.186	NULL	NULL	received	NULL	Hora de almoço		
12	2301.931	NULL	NULL	received	NULL	iPhone6		
13	2303.769	NULL	NULL	received	NULL	Teste		
14	2305.895	NULL	NULL	received	NULL	Boa tarde		

Figura 83 - Mensagem de texto trocada entre os contactos

```
#Bundle id: com.viber
#Old bundle version: 6.3.4.81 6.3.4
#New bundle version: 6.5.0.5581 6.5.0
#Old IPA hash (md5): 32f4857d09b2c94998e76fe3c8b6a91d
#New IPA hash (md5): 09bb4ead8def9eb907cf43773091369a
```

Figura 84 – Hash MD5

No iOS 9.3.5 e 10.2.1 foram encontrados dados como apresenta a seguinte lista:

- Pasta "Attachments" – Contém os anexos trocados durante as conversas com os contactos da aplicação – Ver Figura 85;
- Pasta "ViberIcons" – Contém miniaturas das fotos de perfil dos contactos da aplicação – Ver Figura 86;
- Chave pública – Ver Figura 87;
- Registo dos anexos trocados – Ver Figura 88;
- Registo de chamadas da aplicação – Ver Figura 89.

Figura 85 - anexos trocados durante as conversas com os contactos da aplicação.

Figura 86 – Miniaturas das fotos de perfil dos contactos da aplicação

20	PUBLIC_ACCOUNT_CALL_AFTER_KEY_TIME	1485189345413	PUBLIC
21	PUBLIC_ACCOUNT_CALL_KEY_MSG	iQA+fbV+pRg0q4hTAd0ZqvbcsO8A8PL1TQBcJgUHAAIAMQARAExvY2FsIEJ1c2luZXNzZ...	PUBLIC

Figura 87 – Chave pública encontrada.

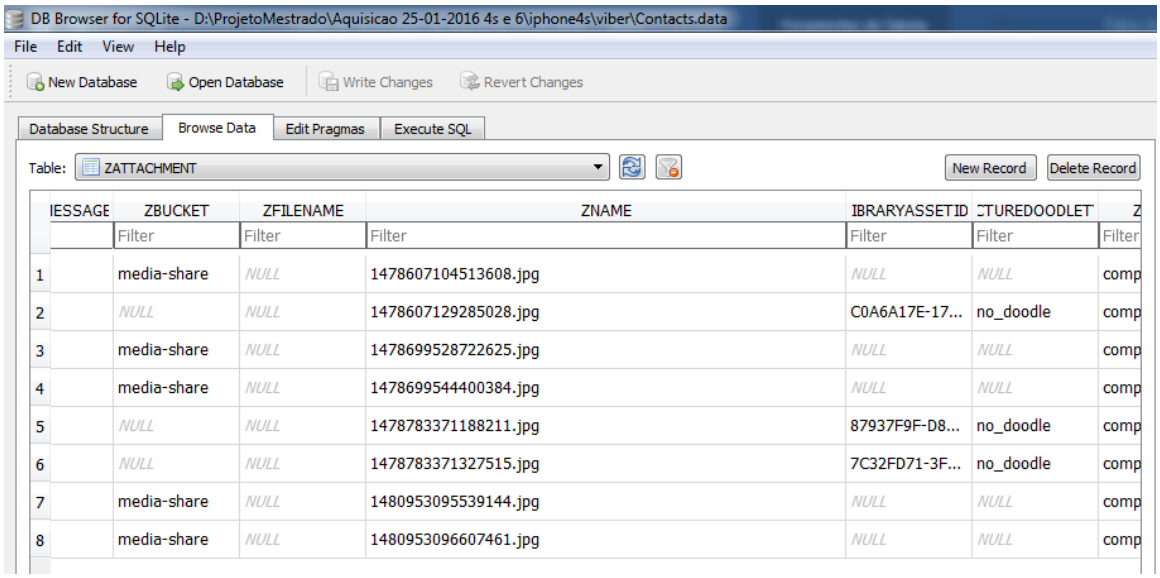


Figura 88 – Anexos trocados com os contactos da aplicação.

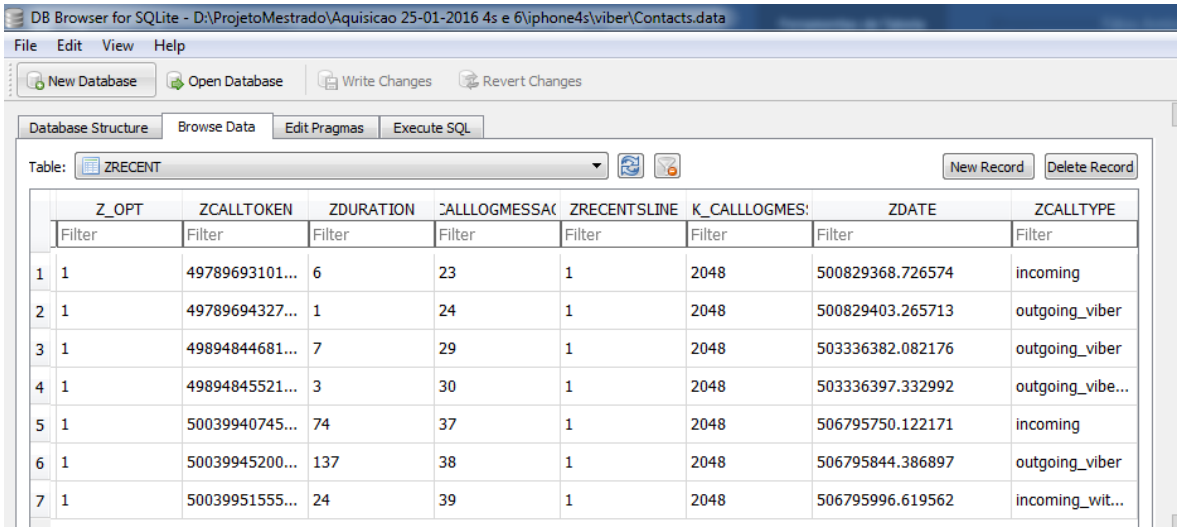


Figura 89 – Registo de chamadas da aplicação

Com base na informação analisada e do ponto de vista forense, podemos afirmar que a aplicação Viber contém uma série de informações importantes que conseguiram ser obtidas o que é um aspeto positivo do ponto de vista forense. Já do ponto de vista de utilizador, a aplicação é insegura uma vez que não guarda de forma segura os dados.

Do ponto de vista das versões dos sistemas operativos, podemos concluir que encontramos algumas diferenças no que toca aos dados adquiridos.

4.16. WhatsApp

A aplicação WhatsApp foi instalada com objetivo de fazer uma aquisição lógica, utilizando a aplicação XRY.

A aplicação foi utilizada em ambos os dipositivos, para trocar texto, anexos (Imagens) e para efetuar chamas de voz e vídeo.

Do ponto de vista da aquisição, era de esperar que fosse possível obter alguns dados tais como, mensagens, anexos trocados, os contactos e registos de chamadas. Para isso, depois da aquisição lógica efetuada pelo software "XRY" foram procurados todos os ficheiros existentes nas pastas correspondentes à aplicação.

Para a análise dos dados obtidos, utilizando a imagem gerada pelo XRY, foi utilizada a aplicação "XAMN"

A aplicação WhatsApp permitiu a troca de mensagens de texto, e ficheiros como imagens ou vídeo, assim como efetuar chamadas de voz e ou vídeo.

Nas versões de IOS 9.2 e 9.2. foram encontrados os dados da seguinte lista:

- Registo de chamadas da aplicação com números de telemóvel dos contactos - Ver Figura 90;
- Registo de chamadas da aplicação com nome da conta de utilizador da aplicação – Ver Figura 91;
- Número de telemóvel de um dos contactos com quem se trocou mensagens - Ver Figura 92e Figura 93 ;
- Nome da conta de utilizador da aplicação – Ver Figura 95;
- Endereços IP – Ver Figura 94;
- Anexos, imagens trocadas entre utilizadores – Ver Figura 96;
- Pasta Media – Contém uma pasta por cada contacto, com um conjunto de anexos trocados pelos contactos – Ver Figura 97 e Figura 98 ;
- Índice de anexos trocados – Ver Figura 99.
- Mensagens de texto trocada entre os contactos – Ver Figura 100;
- Contactos da aplicação – Ver Figura 101;

- Pasta Profile – Foto de perfil e miniatura do utilizador da aplicação – Ver Figura 102;

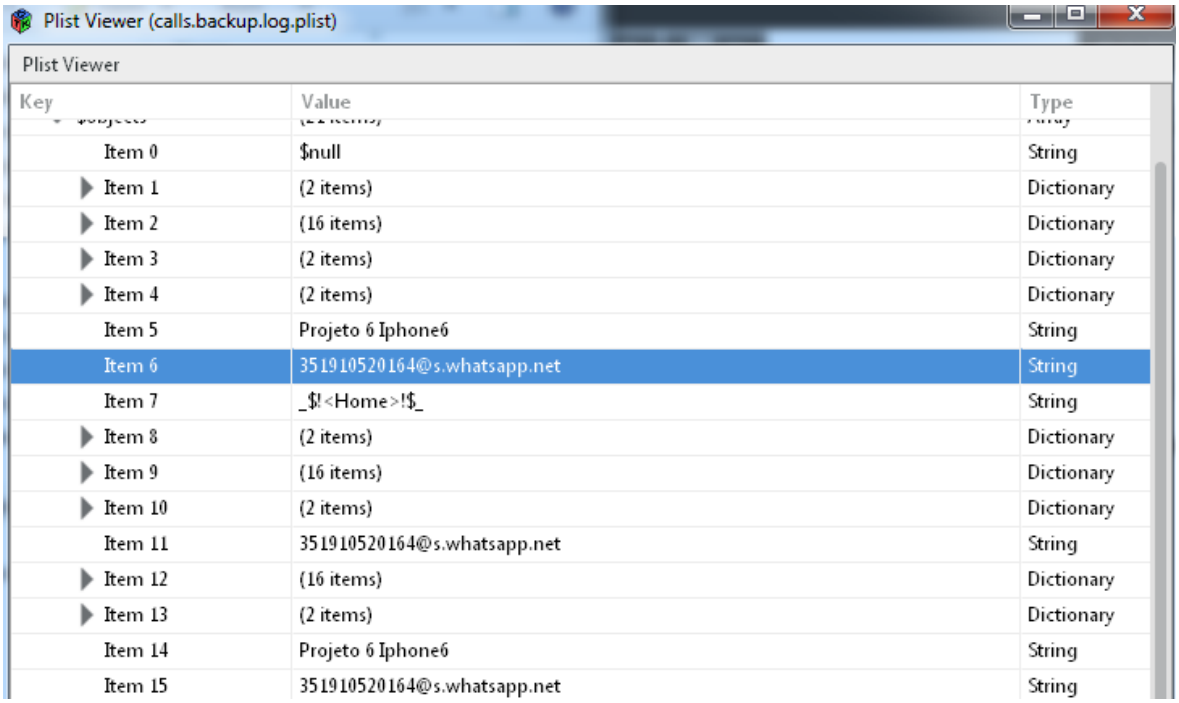


Figura 90 – Registo de chamadas da aplicação com número de telemóvel dos contactos.

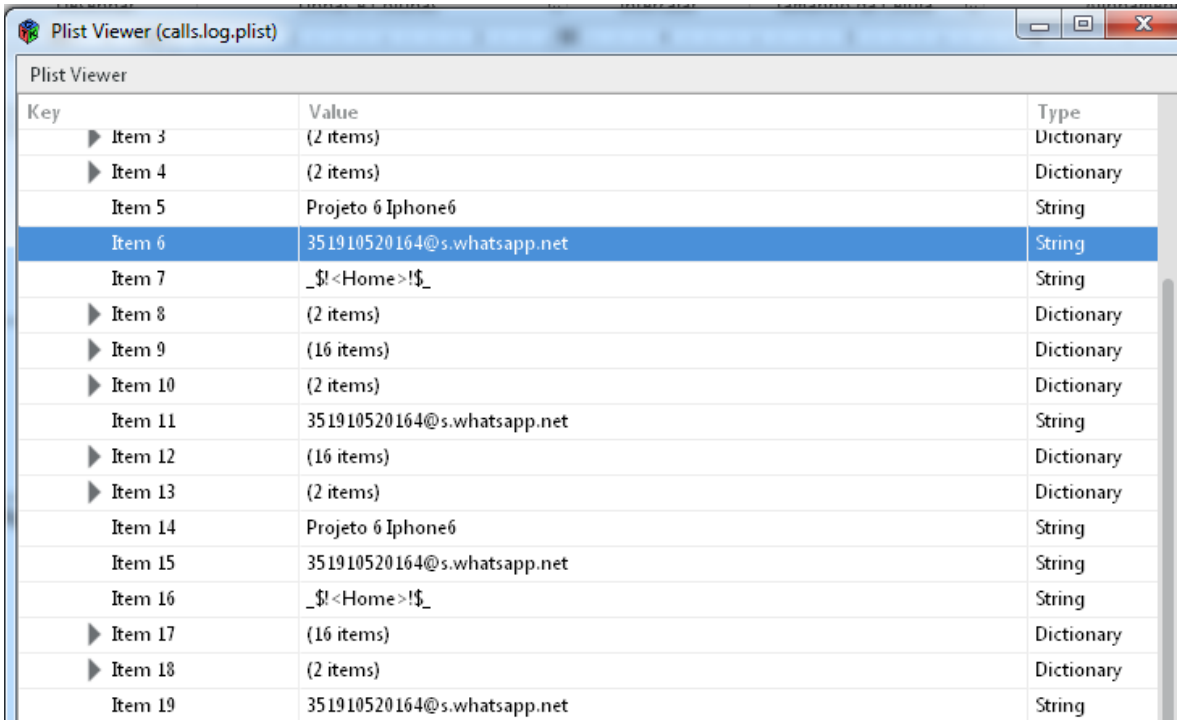


Figura 91 – Registo de chamadas com nome da conta de utilizador da aplicação dos contactos.

```
2016-11-20 22:27:30.566 [ 315111] [xmpp          ] [F] LL_A  connection/state/changed: 3 -> 4
2016-11-20 22:27:30.585 [ 315111] [xmpp          ] [F] LL_N  > send > [presence/available]
2016-11-20 22:27:30.591 [ 315111] [xmpp          ] [F] LL_N  > send > [presence/subscribe t=351910520164@s.whatsapp.net]
```

Figura 92 - Número de telemóvel de um dos contactos

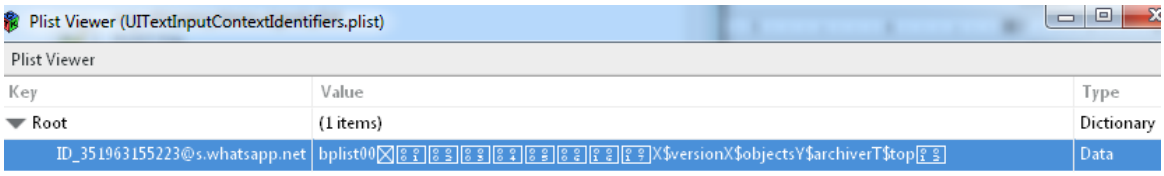


Figura 93 – Número de telemóvel de um dos contactos com quem se trocou mensagens de texto.

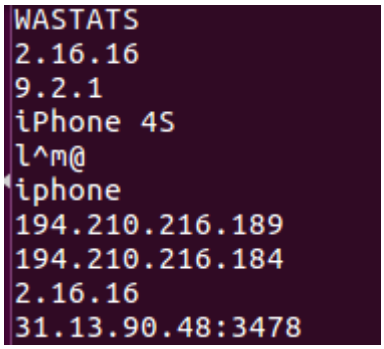


Figura 94 – Endereços IP e portos encontrados

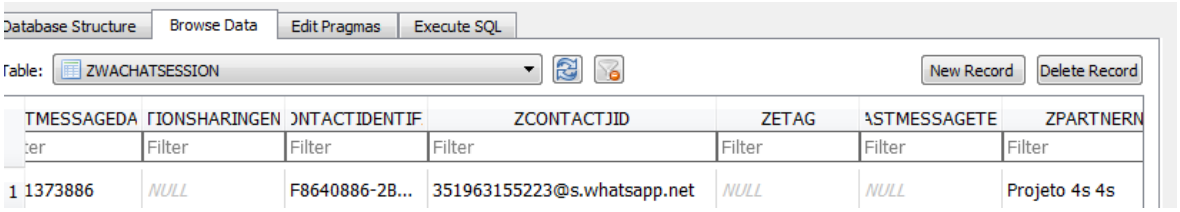


Figura 95 – Nome de utilizador de um contacto da aplicação e respetivo número de telemóvel.

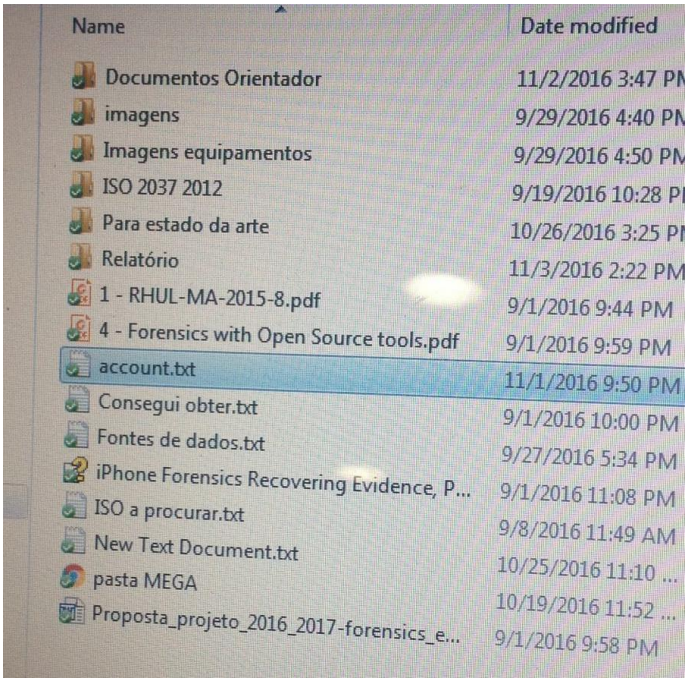


Figura 96 – Anexo trocado entre os contactos

351910022871@s.whatsapp.net	1/31/2017 12:54 PM	File folder
351910520164@s.whatsapp.net	1/31/2017 12:54 PM	File folder

Figura 97 - Conteúdo da Pasta Media

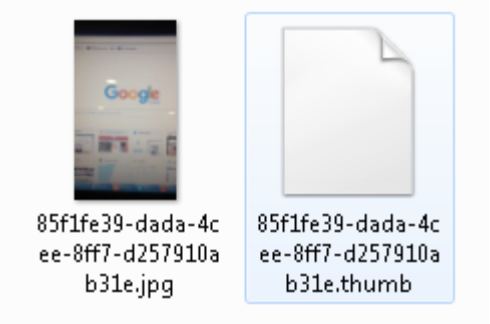


Figura 98 – Conteúdo de uma das pastas dos utilizadores da pasta Media.

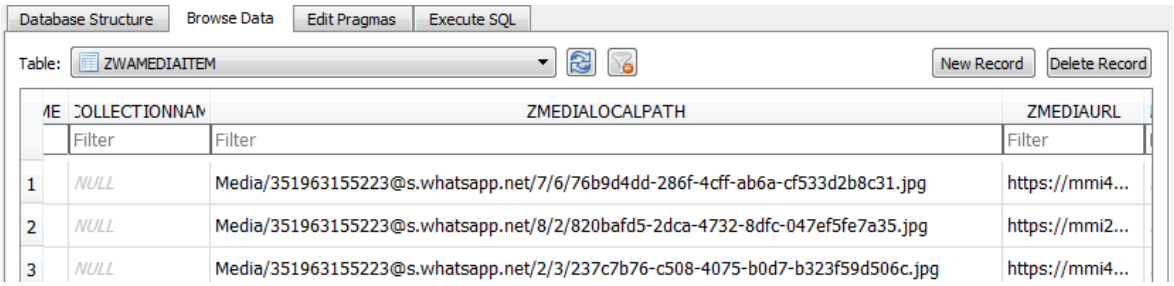

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ZWAMEDIAITEM — New Record — Delete Record

	ME	COLLECTIONNAM	ZMEDIALOCALPATH	ZMEDIAURL
	Filter	Filter	Filter	Filter
1		NULL	Media/351963155223@s.whatsapp.net/7/6/76b9d4dd-286f-4cff-ab6a-cf533d2b8c31.jpg	https://mmi4...
2		NULL	Media/351963155223@s.whatsapp.net/8/2/820bafd5-2dca-4732-8dfc-047ef5fe7a35.jpg	https://mmi2...
3		NULL	Media/351963155223@s.whatsapp.net/2/3/237c7b76-c508-4075-b0d7-b323f59d506c.jpg	https://mmi4...

Figura 99 – Índice de anexos trocados entre os contactos.

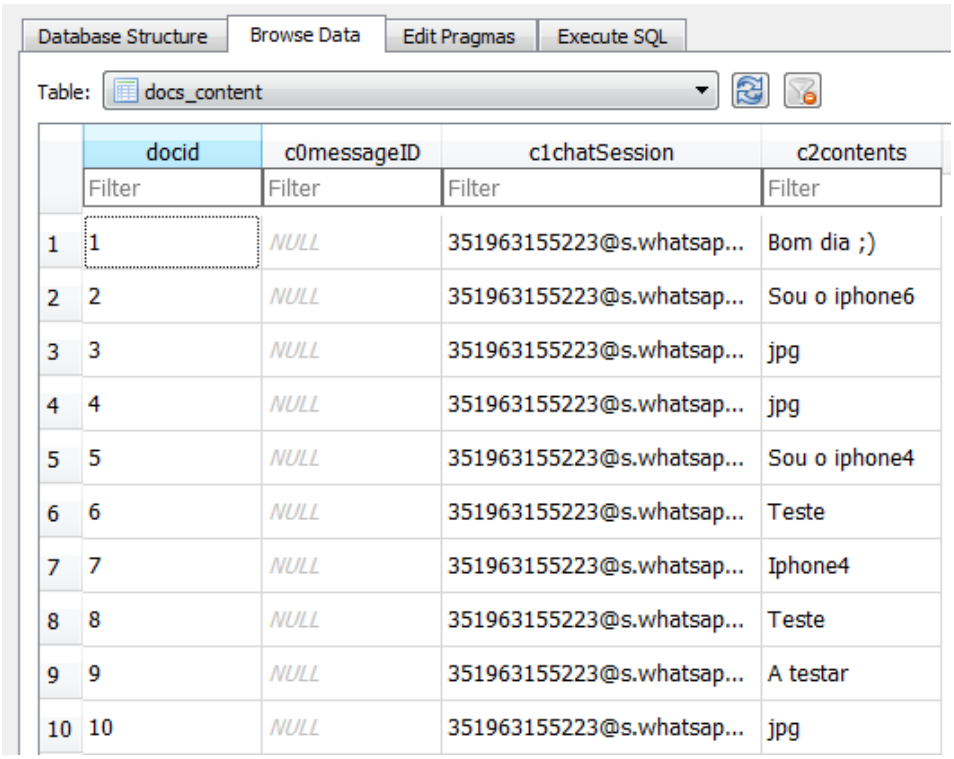

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: docs_content

	docid	c0messageID	c1chatSession	c2contents
	Filter	Filter	Filter	Filter
1	1	NULL	351963155223@s.whatsap...	Bom dia ;)
2	2	NULL	351963155223@s.whatsap...	Sou o iphone6
3	3	NULL	351963155223@s.whatsap...	jpg
4	4	NULL	351963155223@s.whatsap...	jpg
5	5	NULL	351963155223@s.whatsap...	Sou o iphone4
6	6	NULL	351963155223@s.whatsap...	Teste
7	7	NULL	351963155223@s.whatsap...	Iphone4
8	8	NULL	351963155223@s.whatsap...	Teste
9	9	NULL	351963155223@s.whatsap...	A testar
10	10	NULL	351963155223@s.whatsap...	jpg

Figura 100 - Mensagem de texto trocada entre os contactos com respetivos números de telemóvel.

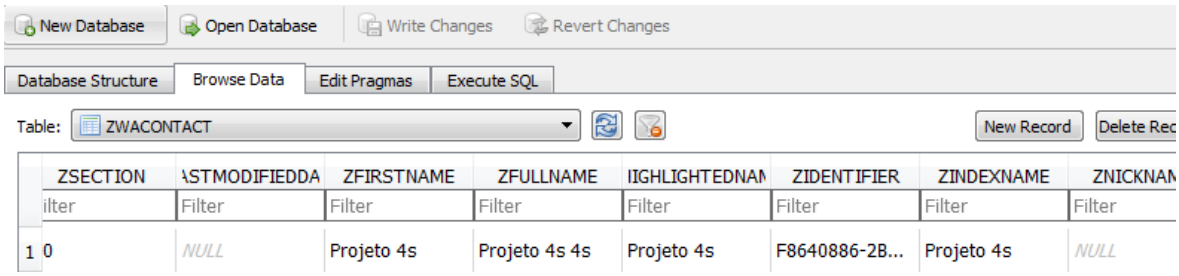


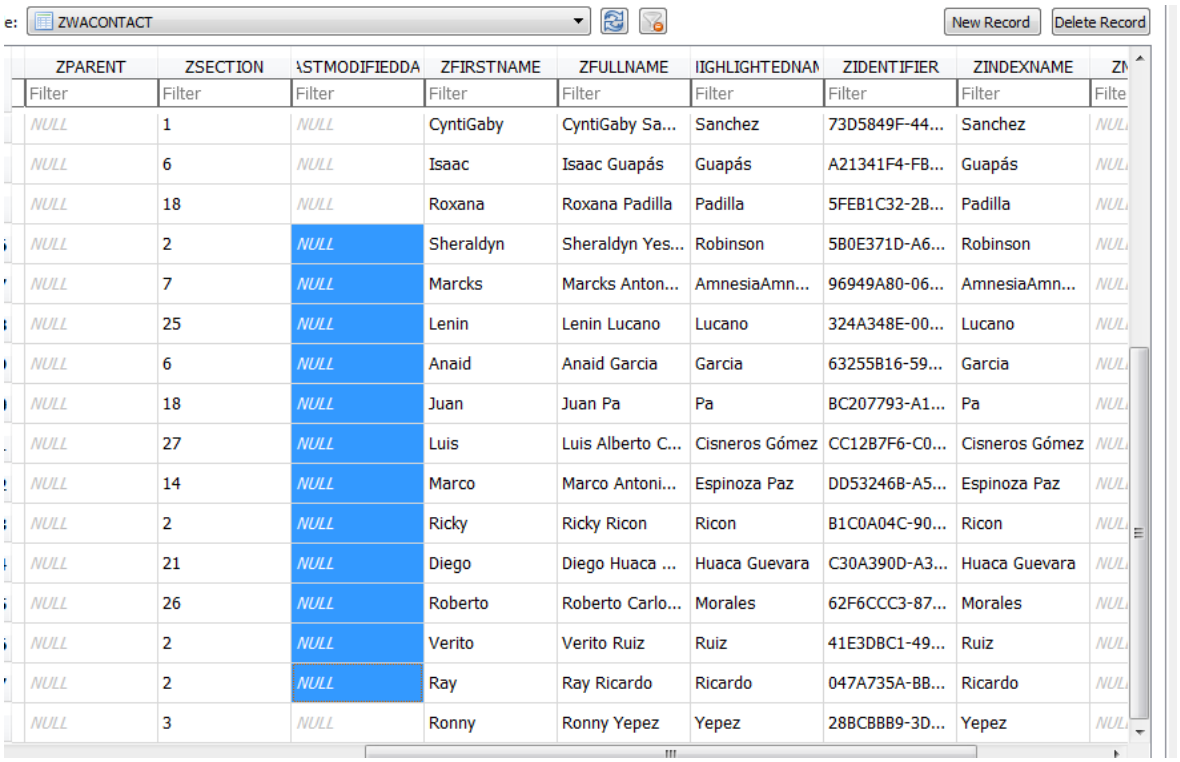
Figura 101 – Contactos da aplicação.

Figura 102 - Conteúdo da Pasta Profile

No iOS 9.3.5 e 10.2.1 foram encontrados dados como apresenta a seguinte lista:

- Registo de chamadas da aplicação com respetiva descrição – Ver Figura 103;
- Todos os contactos existentes na aplicação – Ver Figura 104;

Figura 103 - Registo de chamadas da aplicação com respetiva descrição



ZPARENT	ZSECTION	ASTMODIFIEDDA	ZFIRSTNAME	ZFULLNAME	IIGHLIGHTEDNAM	ZIDENTIFIER	ZINDEXNAME	ZN
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filte
NULL	1	NULL	CyntiGaby	CyntiGaby Sa...	Sanchez	73D5849F-44...	Sanchez	NUL
NULL	6	NULL	Isaac	Isaac Guapás	Guapás	A21341F4-FB...	Guapás	NUL
NULL	18	NULL	Roxana	Roxana Padilla	Padilla	5FEB1C32-2B...	Padilla	NUL
NULL	2	NULL	Sheraldyn	Sheraldyn Yes...	Robinson	5B0E371D-A6...	Robinson	NUL
NULL	7	NULL	Marcks	Marcks Anton...	AmnesiaAmn...	96949A80-06...	AmnesiaAmn...	NUL
NULL	25	NULL	Lenin	Lenin Lucano	Lucano	324A348E-00...	Lucano	NUL
NULL	6	NULL	Anaid	Anaid Garcia	Garcia	63255B16-59...	Garcia	NUL
NULL	18	NULL	Juan	Juan Pa	Pa	BC207793-A1...	Pa	NUL
NULL	27	NULL	Luis	Luis Alberto C...	Cisneros Gómez	CC12B7F6-C0...	Cisneros Gómez	NUL
NULL	14	NULL	Marco	Marco Antoni...	Espinoza Paz	DD53246B-A5...	Espinoza Paz	NUL
NULL	2	NULL	Ricky	Ricky Ricon	Ricon	B1C0A04C-90...	Ricon	NUL
NULL	21	NULL	Diego	Diego Huaca ...	Huaca Guevara	C30A390D-A3...	Huaca Guevara	NUL
NULL	26	NULL	Roberto	Roberto Carlo...	Morales	62F6CCC3-87...	Morales	NUL
NULL	2	NULL	Verito	Verito Ruiz	Ruiz	41E3DBC1-49...	Ruiz	NUL
NULL	2	NULL	Ray	Ray Ricardo	Ricardo	047A735A-BB...	Ricardo	NUL
NULL	3	NULL	Ronny	Ronny Yepez	Yepez	28BCBBB9-3D...	Yepez	NUL

Figura 104 – Todos os contactos da aplicação.

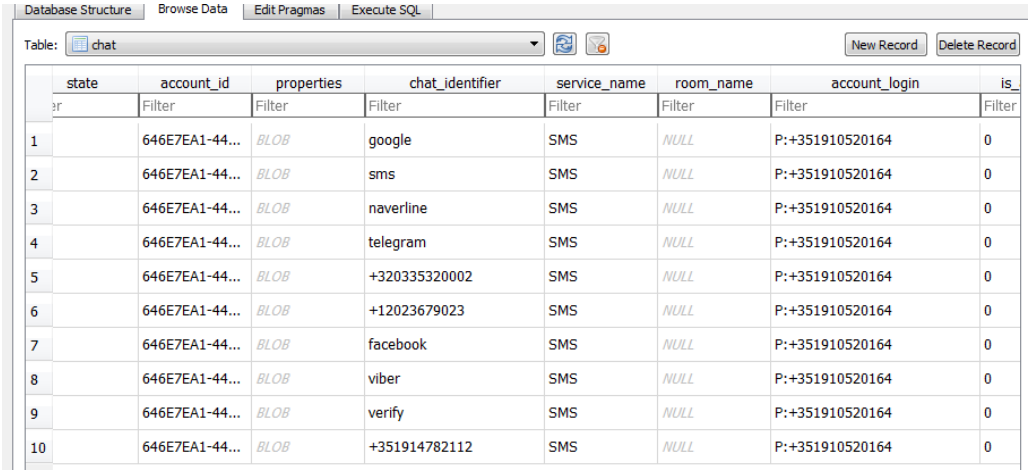
Com base na informação analisada e do ponto de vista forense, podemos afirmar que a aplicação WhatsApp contém uma série de informações importantes que podem ser obtidas, o que é um ponto importante pois conseguem ser obtidos vários tipos de provas digitais. Do ponto de vista do utilizador a aplicação WhatsApp é insegura pois não guarda de forma segura os seus dados, estes conseguem ser facilmente obtidos.

4.17. Aplicação iMessage

A aplicação iMessage é a aplicação nativa do iPhone para envio e receção de mensagens, permitindo assim a troca de mensagens de texto.

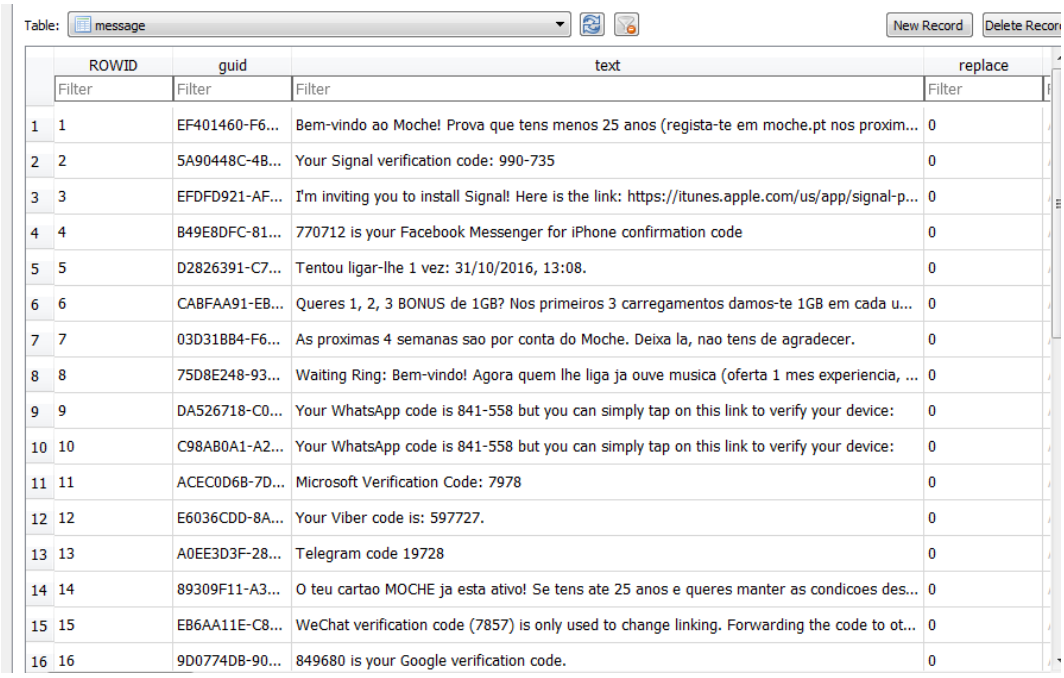
Nas versões de IOS 9.2 e 9.2, 9.3.5 e 10.2.1 foram obtidos os mesmos dados para esta aplicação, como apresenta a seguinte lista:

- Número de telemóvel do cartão SIM de um contacto - Ver Figura 105;
- Conteúdo das mensagens de texto - Ver Figura 106;



	state	account_id	properties	chat_identifier	service_name	room_name	account_login	is_
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1		646E7EA1-44...	BLOB	google	SMS	NULL	P:+351910520164	0
2		646E7EA1-44...	BLOB	sms	SMS	NULL	P:+351910520164	0
3		646E7EA1-44...	BLOB	naverline	SMS	NULL	P:+351910520164	0
4		646E7EA1-44...	BLOB	telegram	SMS	NULL	P:+351910520164	0
5		646E7EA1-44...	BLOB	+320335320002	SMS	NULL	P:+351910520164	0
6		646E7EA1-44...	BLOB	+12023679023	SMS	NULL	P:+351910520164	0
7		646E7EA1-44...	BLOB	facebook	SMS	NULL	P:+351910520164	0
8		646E7EA1-44...	BLOB	viber	SMS	NULL	P:+351910520164	0
9		646E7EA1-44...	BLOB	verify	SMS	NULL	P:+351910520164	0
10		646E7EA1-44...	BLOB	+351914782112	SMS	NULL	P:+351910520164	0

Figura 105 – Números de telemóvel e indentificação de algumas entidades que enviaram mensagens de texto SMS.



	ROWID	guid	text	replace
	Filter	Filter	Filter	Filter
1	1	EF401460-F6...	Bem-vindo ao Moche! Prova que tens menos 25 anos (regista-te em moche.pt nos proxim...	0
2	2	5A90448C-4B...	Your Signal verification code: 990-735	0
3	3	EFDFD921-AF...	I'm inviting you to install Signal! Here is the link: https://itunes.apple.com/us/app/signal-p...	0
4	4	B49E8DFC-81...	770712 is your Facebook Messenger for iPhone confirmation code	0
5	5	D2826391-C7...	Tentou ligar-lhe 1 vez: 31/10/2016, 13:08.	0
6	6	CABFAA91-EB...	Queres 1, 2, 3 BONUS de 1GB? Nos primeiros 3 carregamentos damos-te 1GB em cada u...	0
7	7	03D31BB4-F6...	As proximas 4 semanas sao por conta do Moche. Deixa la, nao tens de agradecer.	0
8	8	75D8E248-93...	Waiting Ring: Bem-vindo! Agora quem lhe liga ja ouve musica (oferta 1 mes experiencia, ...	0
9	9	DA526718-C0...	Your WhatsApp code is 841-558 but you can simply tap on this link to verify your device:	0
10	10	C98AB0A1-A2...	Your WhatsApp code is 841-558 but you can simply tap on this link to verify your device:	0
11	11	ACEC0D6B-7D...	Microsoft Verification Code: 7978	0
12	12	E6036CDD-8A...	Your Viber code is: 597727.	0
13	13	A0EE3D3F-28...	Telegram code 19728	0
14	14	89309F11-A3...	O teu cartao MOCHE ja esta ativo! Se tens ate 25 anos e queres manter as condicoes des...	0
15	15	EB6AA11E-C8...	WeChat verification code (7857) is only used to change linking. Forwarding the code to ot...	0
16	16	9D0774DB-90...	849680 is your Google verification code.	0

Figura 106 – Mensagens de texto enviadas e recebidas

Com base na informação analisada e do ponto de vista forense, podemos afirmar que a aplicação iMessage contém os dados necessários a uma investigação forense, pois as mensagens, o conteúdo das mesmas e a entidade ou pessoa que as envia estão devidamente identificadas. Do ponto de vista do utilizador, não é uma aplicação segura pois facilmente conseguimos obter os dados.

5. Conclusões e trabalho futuro

Neste capítulo são apresentadas as conclusões resultantes do projeto, nomeadamente relativamente aos procedimentos forenses e às aplicações de "*Instant Messanging*" que foram instaladas nos dispositivos Apple para depois serem testados alguns dos procedimentos.

5.1. Aplicações Testadas e dados obtidos

As aplicações de troca de mensagens instaladas tiveram como objetivo a criação de dados para que pudéssemos efetuar aquisições forenses, verificar quais as aplicações mais inseguras e testar alguns procedimentos. Assim sendo, foram testadas as aplicações Google Allo, Cyphr, Imo, Line, Messenger, Signal, Skype, Telegram, Viber, WhatsApp e iMessage. Foram também utilizadas todas as funcionalidades dos dispositivos móveis como as chamadas, mensagens de texto, o browser para acesso à internet, o calendário, a câmara entre outras funcionalidades.

Podemos concluir através dos dados obtidos que o software XRY conseguiu obter uma grande quantidade de dados destas aplicações e das funcionalidades dos dispositivos. Conseguimos demonstrar que apesar de terem sido efetuadas aquisições lógicas, foi possível obter registos de conversas das aplicações, chamadas, fotografias, fotos de perfil de utilizadores, contactos entre outros dados. No caso de uma investigação digital forense no mundo real estes dados seriam bastante úteis, servindo como provas digitais em tribunal.

No aspeto das aplicações de chat, foi demonstrado que a aplicação WhatsApp não é uma aplicação segura do ponto de vista do utilizador uma vez que foi possível obter todo o tipo de registos desta aplicação. Já a aplicação Signal demonstrou ser bastante segura do ponto de vista do utilizador uma vez que não foi possível obter dados. Já do ponto de vista forense não será um ponto positivo uma vez que se ocorrerem crimes e forem trocadas informações através da aplicação Signal, os analistas forenses irão ter dificuldades em obter provas digitais. Podemos também justificar que o software XRY pode não ter suporte a todas as aplicações e dessa forma não consegue obter dados dessas aplicações uma vez que este tipo de software está em constante adaptação às tecnologias existentes.

Apesar da encriptação que a Apple aplica nos seus dispositivos é ainda possível obter uma grande quantidade de dados dos mesmos, o que prova que os Softwares forenses conseguem ler grande parte do sistema de ficheiros.

5.2. Procedimentos forenses

Os procedimentos forenses foram elaborados com objetivo de simplificar o trabalho do analista forense e apoiar o LabCIF. Através de informação bibliográfica e das aquisições que foram sendo efetuadas. O dispositivo Apple contém algumas particularidades, nomeadamente a não utilização de cartão de memória e o facto de não ser possível copiar dados para a memória destes de forma tão fácil como os dispositivos Android por exemplo. Dessa forma, os procedimentos foram adaptados a estes dispositivos.

Com base no que consideramos importante para o analista forense consideramos 7 procedimentos diferentes, nomeadamente, Receção, Catalogação e Registo fotográfico, Preservação, Aquisição, Pesquisa, Análise e Relatório Final. O procedimento de receção é importante uma vez que existem uma quantidade de tarefas que devem ser efetuadas quando os dispositivos chegam às mãos dos analistas forenses pela primeira vez, uma delas a colocação em modo de voo para evitar comunicações com a rede e proteger os dados. A catalogação e o registo fotográfico são outro ponto importante uma vez que os dispositivos e respetivos dispositivos de armazenamento ficam devidamente identificados, como uma forma de organizar todo o conjunto de peças do caso forense. As fotografias são importantes uma vez que mostram os dispositivos no estado atual e alguns códigos ou informações. A preservação é um ponto muito importante se queremos que as provas sejam mantidas intactas e possam ser validadas em tribunal. A aquisição é o ponto mais importante uma vez que são obtidos os dados do sistema de ficheiros do dispositivo móvel. A pesquisa e a análise são pontos que apesar de separados tem bastante em comum uma vez que ao efetuar uma pesquisa das provas que existem estamos já a ver que tipos de provas existem e se estas são ou não valiosas para o caso forense. Na pesquisa utilizamos uma série de técnicas para procurar provas e depois organizar estas em tabelas. Na análise vamos verificar realmente se estas provas são importantes ou não para o caso forense e se podem ser relacionadas com outras. O relatório final, e como descrito nos procedimentos é um relatório que começa a ser escrito

desde o primeiro procedimento, nomeadamente o relatório interno. Todas as etapas contêm informações muito importantes que devem ser escritas em relatório. No final, estas informações devem ser passadas para o relatório final, de uma forma mais cuidada e fácil de entender uma vez que este relatório irá ser usado em tribunal.

Devido à falta de tempo não nos foi possível testar todos os procedimentos. Os procedimentos que foram testados foram os de Receção, Aquisição, Pesquisa de provas, análise e parte do relatório final. Os dados obtidos através da pesquisa de provas e análise foram colocados no relatório e em anexos.

Bibliografia

About ENFSI | ENFSI. (2017). Retrieved May 9, 2017, from http://enfsi.eu/about-enfsi/

AccessData. (2014). Mobile Phone Examiner Plus release notes. Retrieved from https://ad-pdf.s3.amazonaws.com/MPE 5.5.3 RN with Velocitor.pdf

Altheide, C., & Carvey, H. a. (2011). *Digital forensics with open source tools using open source platform tools for performing computer forensics on target systems: Windows, Mac, Linux, UNIX, etc.* https://doi.org/http://0-dx.doi.org.wam.seals.ac.za/10.1016/B978-1-59749-586-8.00001-7

American Society of Crime Laboratory Directors. (2017). Our History | ASCLD. Retrieved July 21, 2017, from http://www.ascld.org/about-us/our-history/

App Annie. (2016). iOS Top App Charts. Retrieved July 12, 2016, from https://www.appannie.com/apps/ios/top-chart/portugal/social-networking/

Apple. (2017). About Information Property List Files. Retrieved August 9, 2017, from https://developer.apple.com/library/content/documentation/General/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

Apple Inc. (2017). iOS Security iOS 10. Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Ayers, R., Jansen, W., & Brothers, S. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). *NIST Special Publication*, *1*(1), 85. https://doi.org/10.6028/NIST.SP.800-101r1

Bill Anderson. (2017). Understanding the Android File Hierarchy | Android News for Costa Rica. Retrieved July 11, 2017, from http://www.all-things-android.com/content/understanding-android-file-hierarchy

BlackBag. (2017). BlackLight | Native Mac, Windows, Android, iPad and iPhone Forensic Analysis Software by BlackBag Technologies. Retrieved August 15, 2017, from https://www.blackbagtech.com/software-products/blacklight-7/blacklight.html#Features

Carpene, C. (2011). Looking to iPhone backup files for evidence extraction, (December), 5–7. https://doi.org/10.4225/75/57b2b9e540ce9

Carrier, B. (2017). Autopsy. Retrieved August 15, 2017, from https://www.sleuthkit.org/autopsy/

Carrier, B. D. (2005). *File System Forensics Analysis*.

Carrier, B. D. (2006). Hypothesis-Based Approach To Digital Forensic Investiga Ations, 190.

Channels, C., & Social, O. (2012). N S T I T U T E U T H O R R E T a I N S F U L L R I G. *Forensic Analysis on iOS Devices*.

Compelson Labs. (2017). Forensic Express — MOBILedit. Retrieved August 15, 2017, from http://www.mobiledit.com/forensic-express

DFIR Training. (2017). Elcomsoft Mobile Forensic Bundle. Retrieved August 15, 2017, from https://www.dfir.training/index.php/tools/mobile-device-forensics/281-elcomsoft-mobile-forensic-bundle

Elizabeth Jones. (2017). Apple File System (APFS), the BIG iOS 10.3 Feature You've Never Heard Of - AppleToolBox. Retrieved July 27, 2017, from http://appletoolbox.com/2017/03/apple-file-system-apfsthe-big-ios-10-3-feature-youve-never-heard/

Encyclopedia.com. (2017). European Network of Forensic Science Institutes - Dictionary definition of European Network of Forensic Science Institutes | Encyclopedia.com: FREE online dictionary. Retrieved May 9, 2017, from http://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/european-network-forensic-science-institutes

Epifani, M. (2013). Acquisition and Analysis of Ios Devices. *SANS Digital Forensics and Incident Response Blog*, (October). Retrieved from https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Epifani, M., & Stirparo, P. (2015). *Learning iOS Forensics*. (M. Frade, Ed.). Retrieved from https://books.google.com/books?id=mUsZBwAAQBAJ&pgis=1

Fiorillo, S. (2009). Theory and practice of flash memory mobile forensics. *7 Th Australian Digital Forensics Conference*. https://doi.org/10.4225/75/57b2893340cd0

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Fukami, A., Ghose, S., Luo, Y., Cai, Y., & Mutlu, O. (2017). Improving the reliability of

chip-off forensic analysis of NAND flash memory devices. *Digital Investigation*, *14*, S1–S11. https://doi.org/10.1016/j.diin.2017.01.011

Gogolin, G. (2012). *Digital Forensics Explained - Greg Gogolin - Google Livros*. Retrieved from https://books.google.pt/books?id=0FTNBQAAQBAJ&pg=PA66&lpg=PA66&dq=digital+forensic+acronyms+smartphones&source=bl&ots=WmFf5X-gu-&sig=XZ5j3wXFzyHcGPIkgzq__WjTX9I&hl=pt-PT&sa=X&ved=0ahUKEwiMi4G__uTSAhXC6iYKHXeXBN8Q6AEIPTAF#v=onepage&q=digital forensic a

haileehaas. (2015). What is USB Type-C? | ShowMeCables Blog. Retrieved August 17, 2017, from http://blog.showmecables.com/what-is-usb-type-c/

Hotz, G. (2017a). List of iPhones - The iPhone Wiki. Retrieved August 10, 2017, from https://www.theiphonewiki.com/wiki/List_of_iPhones

Hotz, G. (2017b). The iPhone Wiki. Retrieved August 8, 2017, from https://www.theiphonewiki.com/wiki/Timeline

Irani Elias. (2017). curso de manutencao de micro - parte 5 - disco rigido - Curso de manutenção de... Retrieved July 24, 2017, from http://www.ebah.com.br/content/ABAAAfzcQAI/curso-manutencao-micro-parte-5-disco-rigido

ISO. (2012). ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved August 18, 2017, from https://www.iso.org/standard/44381.html

ISO. (2015a). ISO/IEC 27042:2015 - Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence. Retrieved August 18, 2017, from https://www.iso.org/standard/44406.html

ISO. (2015b). ISO/IEC 27043:2015 - Information technology -- Security techniques -- Incident investigation principles and processes. Retrieved August 18, 2017, from https://www.iso.org/standard/44407.html

Katana Forensics. (2017). Katana Forensics – Lantern 4. Retrieved August 14, 2017, from https://katanaforensics.com/products/lantern/

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic

techniques into incident response. *NIST Special Publication*, (August), 800–886. https://doi.org/10.6028/NIST.SP.800-86

Lee, S., Jeon, S., Bang, J., & Byun, K. (2012). A recovery method of deleted record for SQLite database, 707–715. https://doi.org/10.1007/s00779-011-0428-7

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, 386–391. https://doi.org/10.1109/BWCCA.2011.63

Magnet forensics inc. (2017). Magnet IEF. Retrieved August 17, 2017, from https://www.magnetforensics.com/magnet-ief/

Mary Mack, E., & Pattison, S. (2017). *Electronic Evidence Management* (Vol. 9). https://doi.org/10.14296/517.9781911507079

McNamara, J. (2004). *GPS for dummies*. Wiley Pub. Retrieved from http://www.dummies.com/store/product/GPS-For-Dummies.productCd-0764569333.html

Morrissey, S. (2010). *iOS Forensic Analysis for iPhone, iPad and iPod touch*. Retrieved from https://sensperiodit.files.wordpress.com/2011/04/ios-forensic-analysis-for-iphone-ipad-and-ipod-touch.pdf

MULLER, G., & DINIZ, A. C. G. . (2005). Entendendo a norma ABNT ISO/IEC 17025: 2005. *Anais Do XIV Congresso Nacional de Estudantes de …*. Retrieved from http://www.abcm.org.br/pt/wp-content/anais/creem/2007/PDF/0181.PDF

National Institute of Standards and Technology. (2017). About NIST | NIST. Retrieved July 21, 2017, from https://www.nist.gov/about-nist

NIST. (2016). Computer Forensics Tool Catalog - Tool Search. Retrieved August 14, 2017, from https://toolcatalog.nist.gov/populated_taxonomy/index.php?all_tools=refine&ff_id=5&1%5B%5D=any&4%5B%5D=any&8%5B%5D=any&9%5B%5D=any&2%5B%5D=any&3%5B%5D=any&5%5B%5D=any&6%5B%5D=any&7%5B%5D=any

Oxygen. (2017). Oxygen Forensics - Oxygen Forensic® Extractor. Retrieved August 14, 2017, from https://www.oxygen-forensic.com/en/products/oxygen-forensic-extractor

Paraben. (2017). E3:UNIVERSAL Feature Chart. Retrieved from www.paraben.com

Quick, Darren Alzaabi, M. (2011). Forensic analysis of the android file system YAFFS2. *Digital Investigation*, *8*(2), 101–109. https://doi.org/10.4225/75/57b2c23a40cf1

Regan, J. E. (2009). THE FORENSIC POTENTIAL OF FLASH MEMORY. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a509258.pdf

RENE RITCHIE. (2017). Apple File System (APFS): What you need to know! | iMore. Retrieved July 12, 2017, from https://www.imore.com/apfs

Ritchie, R. (2017). iOS version code names | iMore. Retrieved August 8, 2017, from https://www.imore.com/ios-version-codenames

Sammons, J. (2012). *Introduction*. *The Basics of Digital Forensics*. https://doi.org/10.1016/B978-1-59749-661-2.00001-2

Satish B. (2011). Forensic Analysis of iPhone Backups, 20.

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

Sheldon, R. (2013). How Apple iOS encryption and data protection work. Retrieved August 17, 2017, from http://searchmobilecomputing.techtarget.com/tip/How-iOS-encryption-and-data-protection-work

SWGDE. (1999). History of SWGDE, 1999–2001.

TechSnoops LLC. (2016). Top Free iPhone Apps for Social Networking - App Charts | iOSnoops. Retrieved December 7, 2016, from http://www.iosnoops.com/apps-charts/iphone/social-networking/free/

Teufl, P., Zefferer, T., Stromberger, C., & Hechenblaikner, C. (2013). IOS encryption systems: Deploying iOS devices in security-critical environments. *ICETE 2013 - 10th International Joint Conference on E-Business and Telecommunications; SECRYPT 2013 - 10th International Conference on Security and Cryptography, Proceedings*, 170–182.

Vandeven, S., & Filkins, B. (2014). Forensic Images: For Your Viewing Pleasure GIAC (GCFA) Gold Certification. Retrieved from https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447

Viriato, L. M. (2016). *Gestão da qualidade e acreditação em informática forense.* Instituto Politécnico de Leiria.

Wadhah R. Baiee. (2014). Android File System. Retrieved from http://www.uobabylon.edu.iq/eprints/publication_4_13681_1356.pdf

Whatson, D., & Jones Andrew. (2013). *Digital Forensics Processing and Procedures*. Elsevier.

Esta página foi intencionalmente deixada em branco

Glossário

No glossário apresentamos alguma nomenclatura importante para o projeto em questão Fontes: (Sammons, 2012; Whatson & Jones Andrew, 2013).

- Caso (*case*) – Uma investigação levada a cabo pelo laboratório forense que usa processos das ciências digitais forenses.
- Examinador Forense (*Forensic Analyst*) – Pessoa responsável por efetuar todo o trabalho forense no laboratório.
- Equipa Forense (*Forensic Team*) – A equipa forense envolvida num dado caso.
- Gestor de Incidentes (*Incident Manager*) – A pessoa responsável por um dado incidente que se está a tratar.
- Gestor de laboratório Forense (*Laboratory Manager*) – A pessoa responsável pelo laboratório forense.
- Terceiros (*Third Party*) – Uma entidade, podendo ser uma organização ou uma pessoa que não está diretamente envolvida, mas pode ser útil no caso.
- Telemóvel (*Cell* ou *Mobile Phone)* – Dispositivo sem fios que é alimentado por uma bateria que é carregada quando este for ligado a uma fonte de energia.
- Smartphone – Telemóvel com a capacidade de correr aplicações e ter acesso à internet
- Telefone sem fios (*cordless*) – Um dispositivo sem fios associado a uma base que é alimentado por uma bateria que é carregada quando este está na base.
- Global Positioning System (GPS) – Dispositivo que permite o utilizador navegar entre localizações utilizando os sinais de rádio para indicar a posição e as direções para um determinado destino

Esta página foi intencionalmente deixada em branco

Projeto

Mestrado de Engenharia Informática – Computação Móvel

Digital Forensics procedures for Apple Devices

Anexo A – Guia de Aquisição e análise

Fábio António Lavrador Amado Marques

O anexo “Guia de Aquisição Lógica utilizando o software XRY” apresenta os passos realizados para a realização de uma aquisição lógica a dois dispositivos Apple, nomeadamente um iPhone 4 e um iPhone 6. Depois da aquisição foi utilizado o *software* forense XAMN para abrir uma das imagens forenses e apresentar a organização do *software* assim como a forma como se pode explorar e exportar os dados para futura analise dos mesmos.

Todas as imagens utilizadas neste anexo foram obtidas com base em capturas de ecrã efetuadas ao software utilizado.

A) Aquisição lógica com o software forense XRY

Foi feita uma aquisição lógica a dois dispositivos, um iPhone 4 e um iPhone 6.

Os dispositivos tinham sido utilizados de forma a conseguir gerar a maior quantidade de dados possível.

1) Tendo em conta as práticas forenses, os dispositivos foram colocados em modo de voo, assim como foi tirada uma fotografia do ecrã de cada um dos mesmos. A Figura 1 identifica o iPhone 4 e a Figura 2 identifica o iPhone6.

Figura 1 – iPhone 4 em modo de voo.

Figura 2 - iPhone 6 em modo de voo.

2) Os dispositivos foram corretamente identificados tendo em conta o seu modelo que está gravado na parte traseira do mesmo. A Figura 3 identifica os dois dispositivos. Do lado esquerdo o iPhone6 e do lado direito o iPhone4.

Figura 3 – Iphone6 e iPhone 4 respetivamente com a identificação do modelo na parte traseira.

3) Tendo em conta que estamos a utilizar equipamento da empresa MSAB, nomeadamente o *software* XRY, os dispositivos foram ligados ao "Hub" do XRY pelos respetivos cabos. A Figura 4 mostra o "Hub" do XRY, o dispositivo que centraliza todas as ligações e que suporta até 3 dispositivos assim como uma chave de *hardware*.

Figura 4 – Hub XRY com os dispositivos móveis ligados.

O dispositivo denominado "Hub XRY" da Figura 4 permite fazer até 3 extrações forenses em simultâneo nomeadamente de dispositivos móveis, cartões de memória e cartões SIM.

4) A Figura 5 apresenta a página de apresentação inicial do software XRY utilizado para fazer a aquisição.

Tendo em conta os passos anteriores e que os dispositivos se encontram corretamente ligados, para começar a extração de um dos dispositivos basta escolher a opção "Create New Extraction Case"

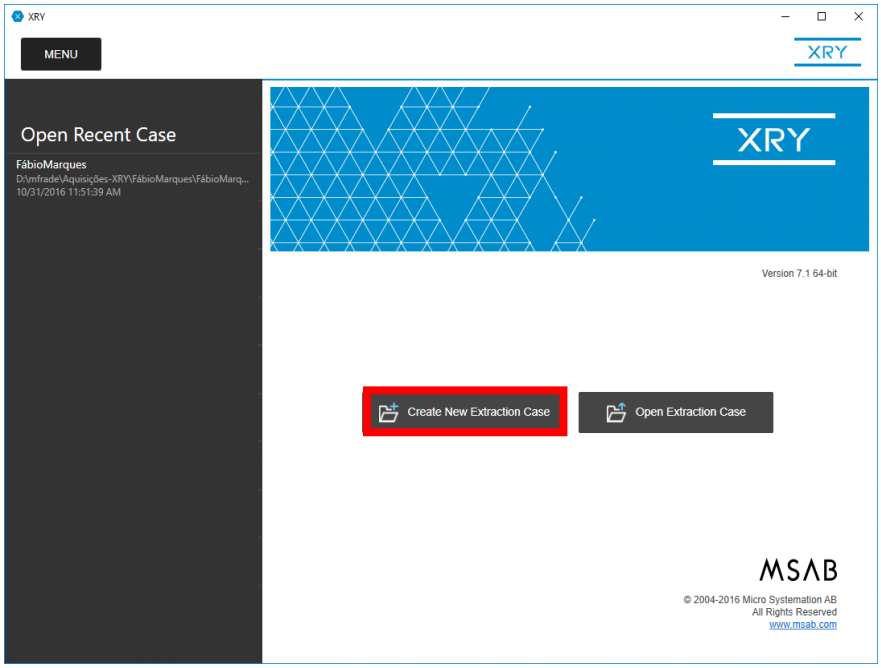


Figura 5 - Apresentação inicial do software XRY.

5) O software detetou que se encontravam dois dispositivos iOS ligados. A Figura 6 confirma que se encontram dois dispositivos ligados no separador "Connected devices".

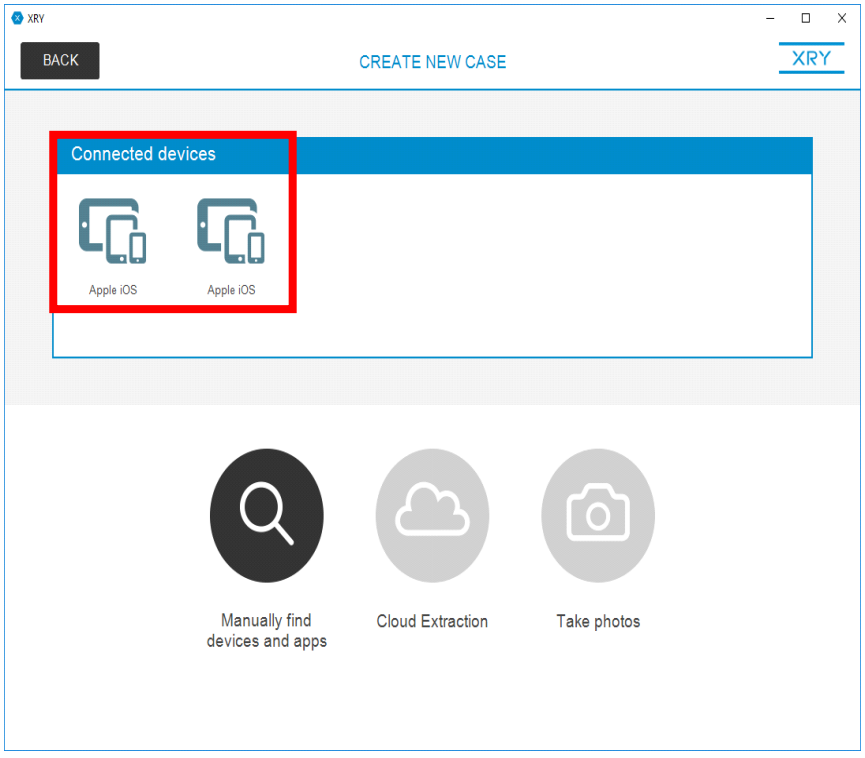


Figura 6 – Software indica os dispositivos ligados

6) Ao escolhermos um dos dispositivos é nos solicitado para escolher qual o modelo em questão como mostra a Figura 7. Sendo assim, e tendo em conta o modelo do iPhone que está na sua parte traseira como foi visto no passo 2) escolhemos a opção correspondente.

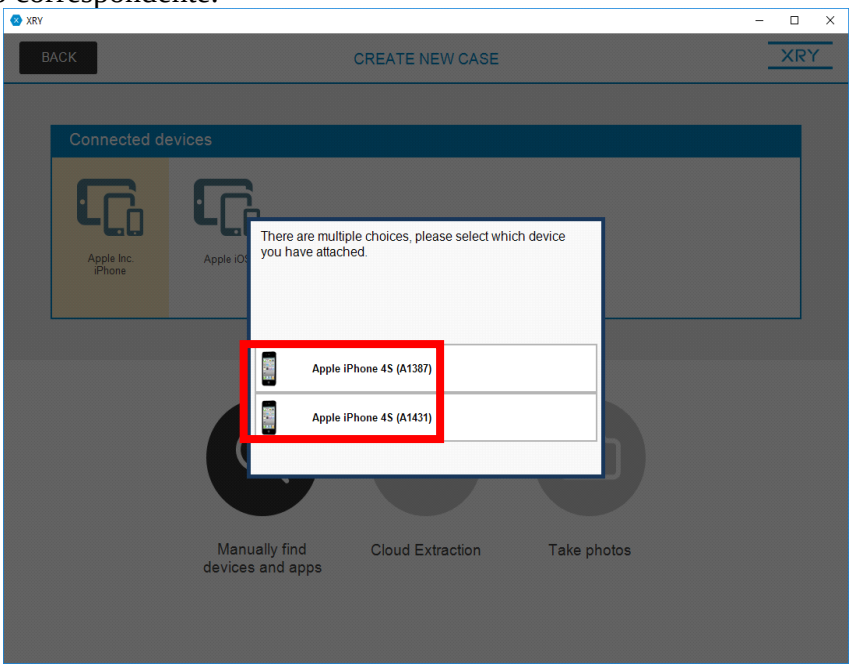


Figura 7 – Escolha do modelo do iPhone.

7) Após escolher o dispositivo são nos apresentadas diversas informações relativamente ao mesmo e o que é possível obter do mesmo tal como mostra a Figura 8. Tudo o que está identificado com um "certo" de cor verde é possível de obter. Tudo o que está identificado com um "x" de cor vermelha não é possível obter. Depois é escolhida a opção "Logical (Full Read)" para se iniciar o processo de aquisição. De notar que esta figura apresenta dados o iPhone 4s.

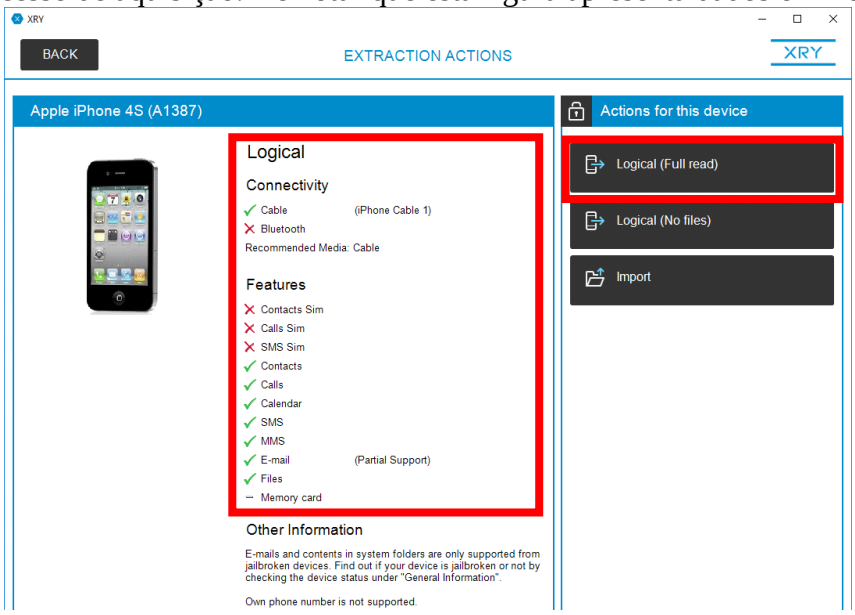


Figura 8 – Informações sobre o dispositivo, o que é possível ou não obter.

A Figura 9 mostra o mesmo passo para o iPhone6.

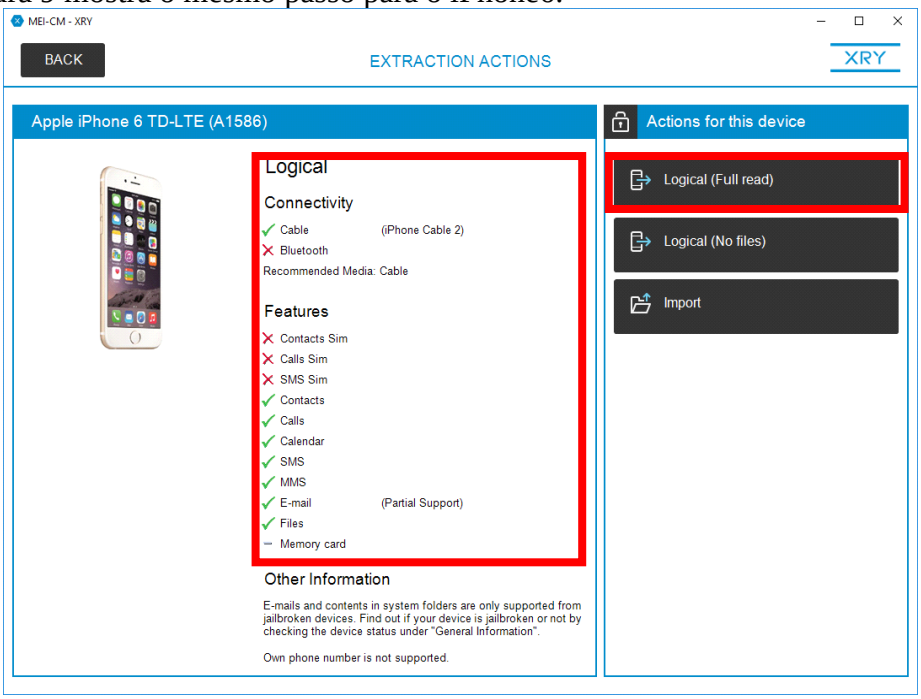


Figura 9 - Informações sobre o dispositivo, o que é possível ou não obter.

8) A Figura 10 mostra um formulário que deve ser corretamente preenchido. Os dados são preenchidos consoante a identificação do caso, do dispositivo, o nome da pessoa responsável pela aquisição e o nome do ficheiro. O ficheiro a ser gerado pode depois ser aberto com um software especifico da MSAB, denominado "XAMN" que permite analisar os dados obtidos. Depois é selecionada a opção "Begin Extraction". Podíamos ainda proteger o ficheiro com uma palavra-passe selecionando a opção "Protect with password"

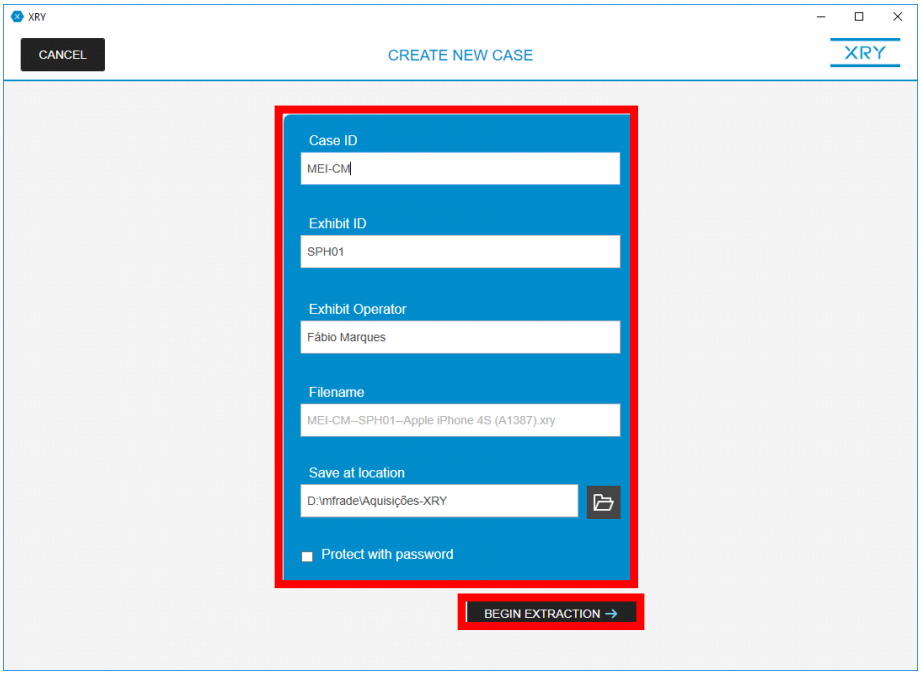


Figura 10 – Preenchimento de formulário para inicio da aquisição.

9) O software apresenta uma mensagem que nos avisa que devemos selecionar a opção “Trust this computer” que nos aparece no dispositivo a ser analisado. A Figura 11 informa o que deve ser feito no dispositivo. Dessa forma devemos desbloquear o dispositivo e escolher a opção indicada. Só assim será possível fazer a aquisição dos dados. Em seguida inicia-se o processo de aquisição.

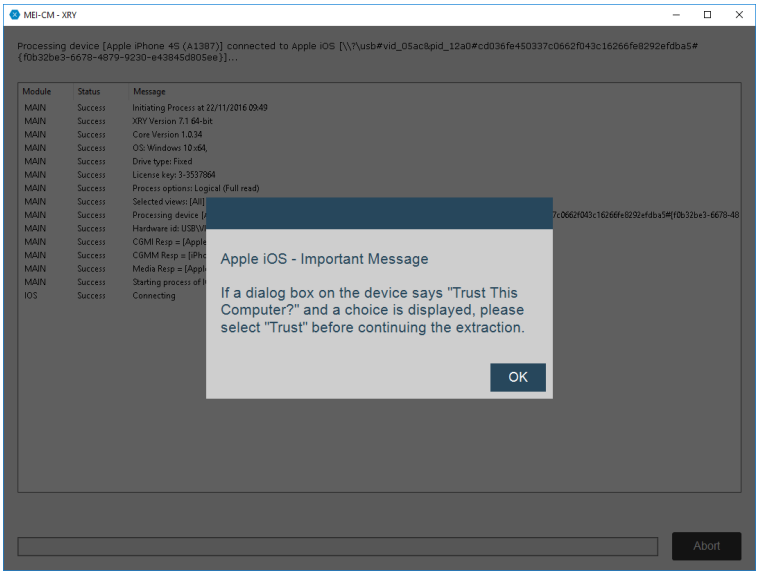


Figura 11 – Aviso do software para escolher a opção “Trust this computer” no dispositivo móvel.

A Figura 12 apresenta a mensagem apresentada no dispositivo.

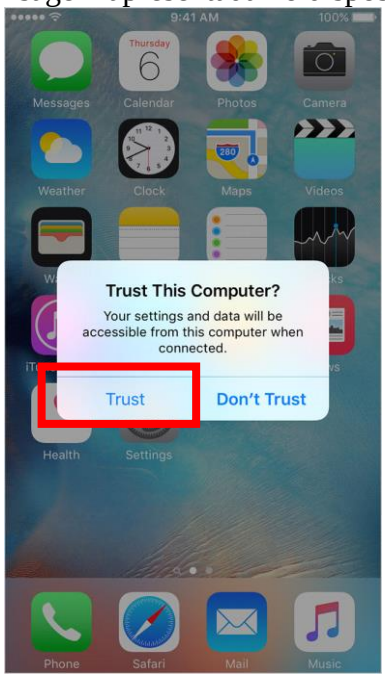


Figura 12 – Mensagem apresentada para permitir o acesso.

10) Na Figura 13 podemos ver o processo de aquisição a ser iniciado. Em que o software se tenta ligar ao dispositivo como podemos ver na mensagem “Connect to device”.

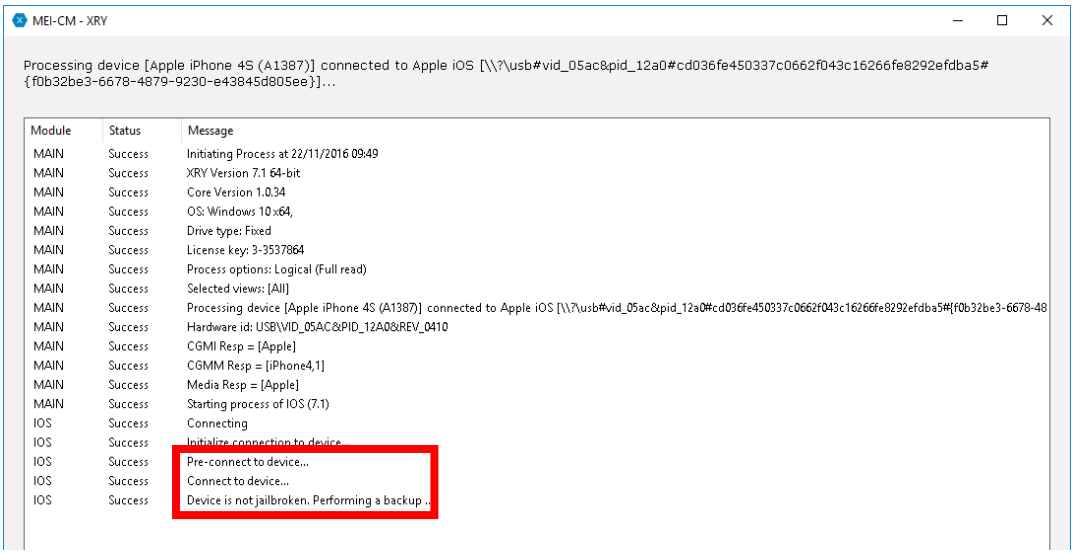


Figura 13 – Software XRY a ligar-se ao dispositivo móvel.

11) Na Figura 14 podemos ver o processo de aquisição em que são mostradas algumas informações do processo, identificado por “a receber dados das aplicações do utilizador, (Retrieving user app data…) com a identificação de uma aplicação instalada. Neste caso o software de aquisição está a recolher o máximo de dados possíveis. De notar que sendo uma aplicação forense apenas vai ler o conteúdo existente sem efetuar alterações na integridade dos dados do dispositivo.

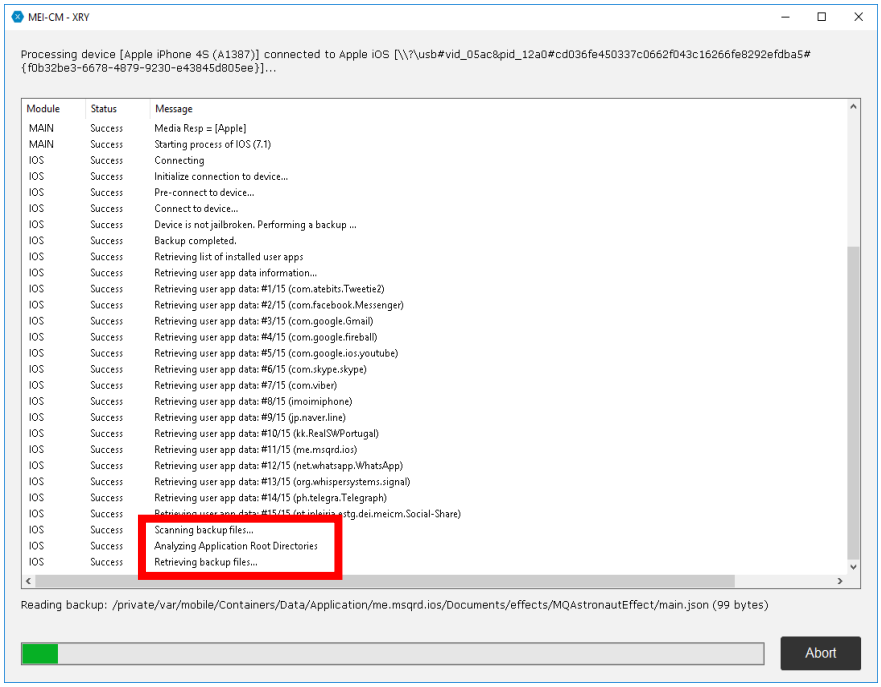


Figura 14 – Processo de aquisição ao dispositivo.

12) No final da aquisição é mostrada uma mensagem “Extraction finished successfully” como mostra a Figura 15. Para finalizar basta escolher a opção “Finish”.

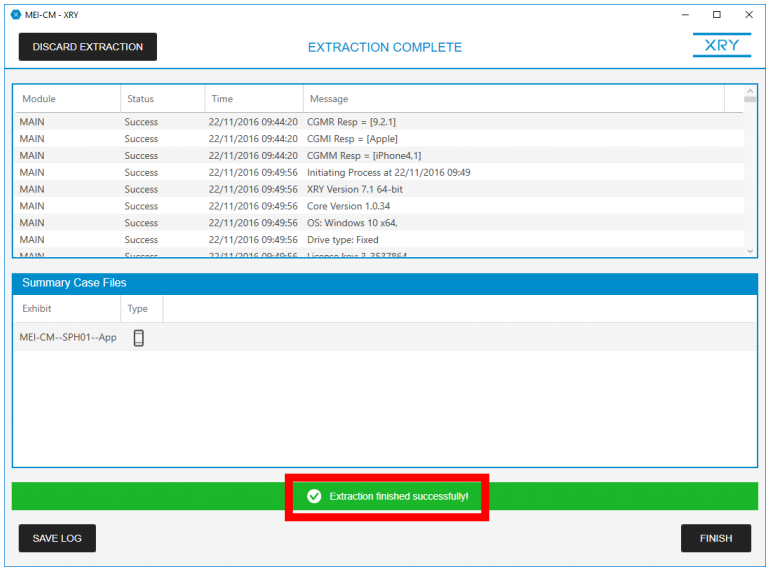


Figura 15 – Finalização do processo de aquisição.

13) Quando o processo de aquisição é finalizado é nos mostrada a janela seguinte da Figura 16 com alguma informação do dispositivo e a informação “Completed” indicando que a aquisição está feita.

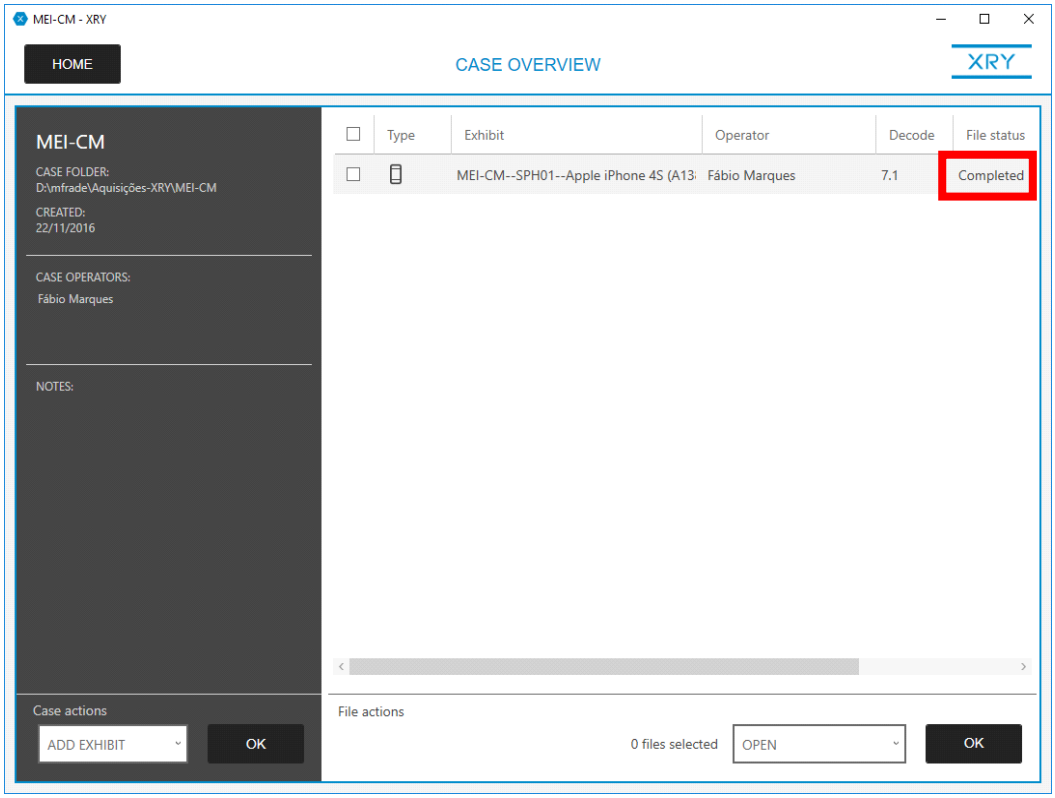


Figura 16 - Finalização do processo de aquisição.

A Figura 17 mostra o processo completo, “Completed” para ambos dispositivos, iPhone 4s e iPhone 6.

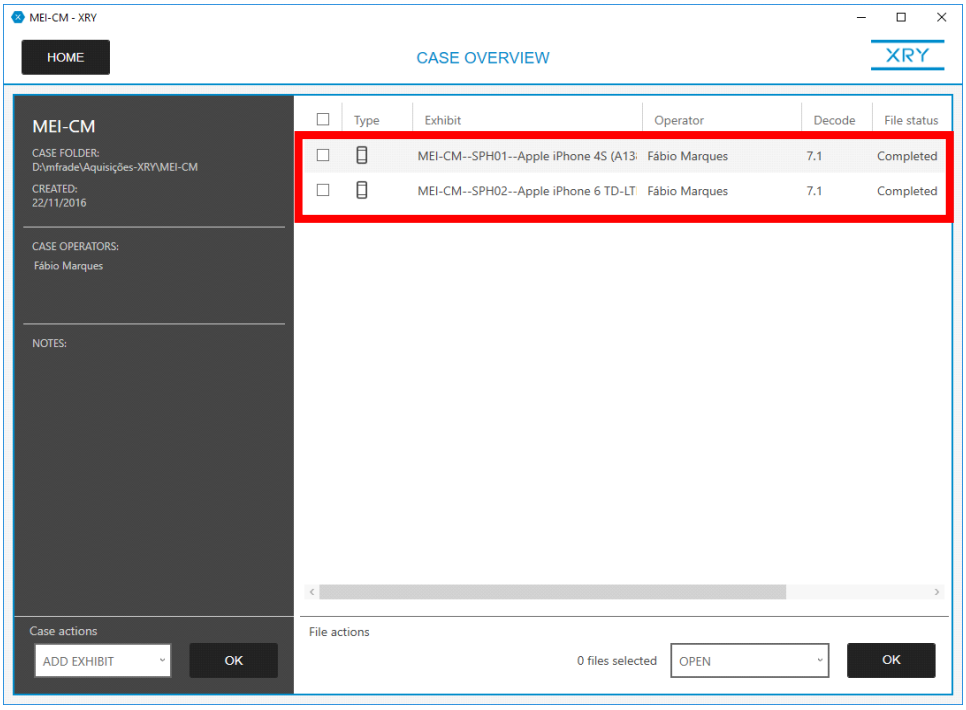


Figura 17 – Processo complete para os dois dispositivos.

A Figura 18 mostra os ficheiros resultantes da extração do iPhone4s e do iPhone6.

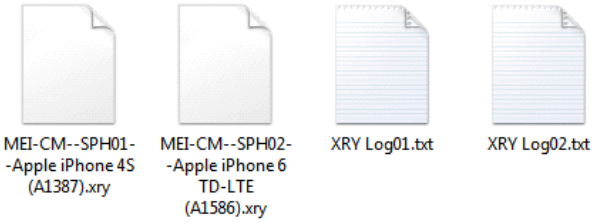


Figura 18 – Ficheiros de imagem em formato XRY resultantes da extração.

Processo de procura dos dados obtidos durante a aquisição.

Após a recolha dos dados que ficaram guardados nos respetivos ficheiros passa-se ao processo de procura dos ficheiros recolhidos no processo de aquisição.

Foi utilizado o software "XAMN" da MSAB para a análise dos dados obtidos da aquisição. Este software, sendo de licença Freeware, permite abrir os ficheiros gerados pelo XRY. A Figura 19 mostra o software que foi referido. Escolhendo a opção "Open" Podemos abrir um ficheiro resultante da aquisição do XRY. Do lado esquerdo encontram-se ficheiros de imagens de aquisições recentemente abertos.

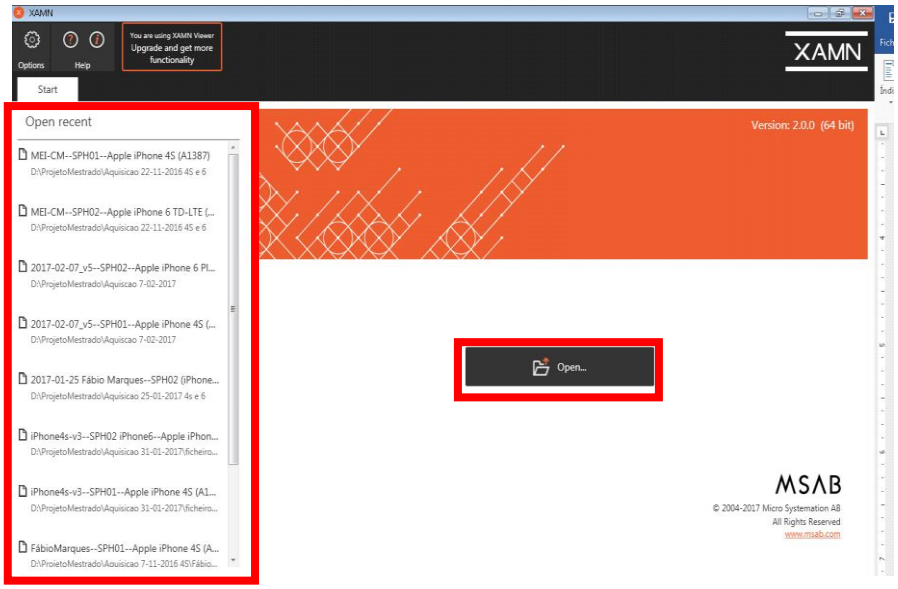


Figura 19 – Interface principal do Software XAMN.

Se for a primeira vez que se utiliza este software ou estamos a abrir novos ficheiros, devemos ir à procura dos ficheiros da aquisição. A Figura 20 apresenta a escolha do ficheiro para dar inicio ao processo de procura.

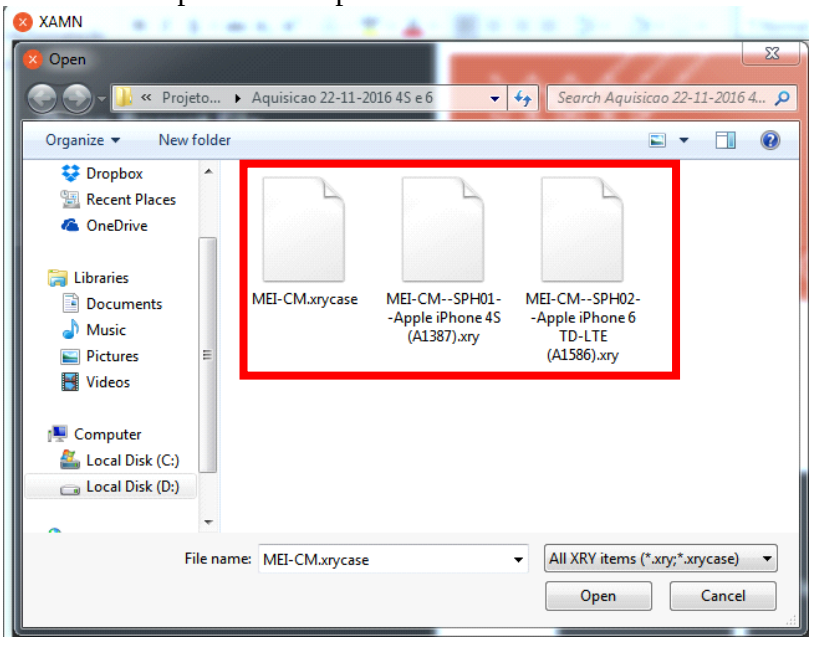


Figura 20 – Escolha manual de ficheiros de imagem XRY para abrir com o software XRY.

Caso já tenhamos efetuado análises, os ficheiros XRY abertos recentemente ficam guardados nesta barra lateral de forma a que futuramente possam ser novamente abertos como mostra a Figura 21.

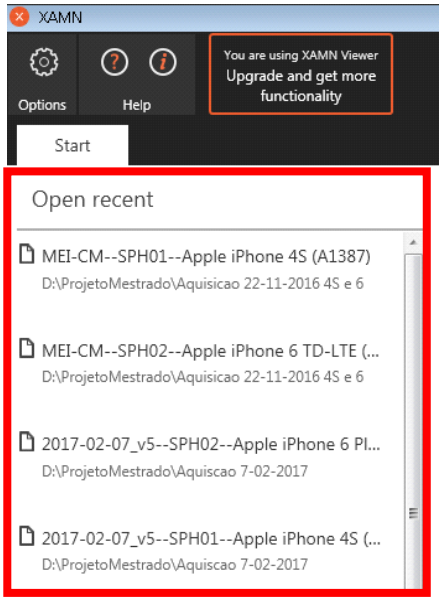


Figura 21 – Lista de ficheiros de imagem forense recentemente abertos.

Depois da abertura do ficheiro, o XAMN apresenta uma lista de informações como podemos ver na Figura 22. O separador aberto é o "artifacts" que contém um resumo de dados de chamadas encontradas, contactos, aplicações, mensagens, calendário, dados de localização, dados web, imagens, vídeos entre outras informações.

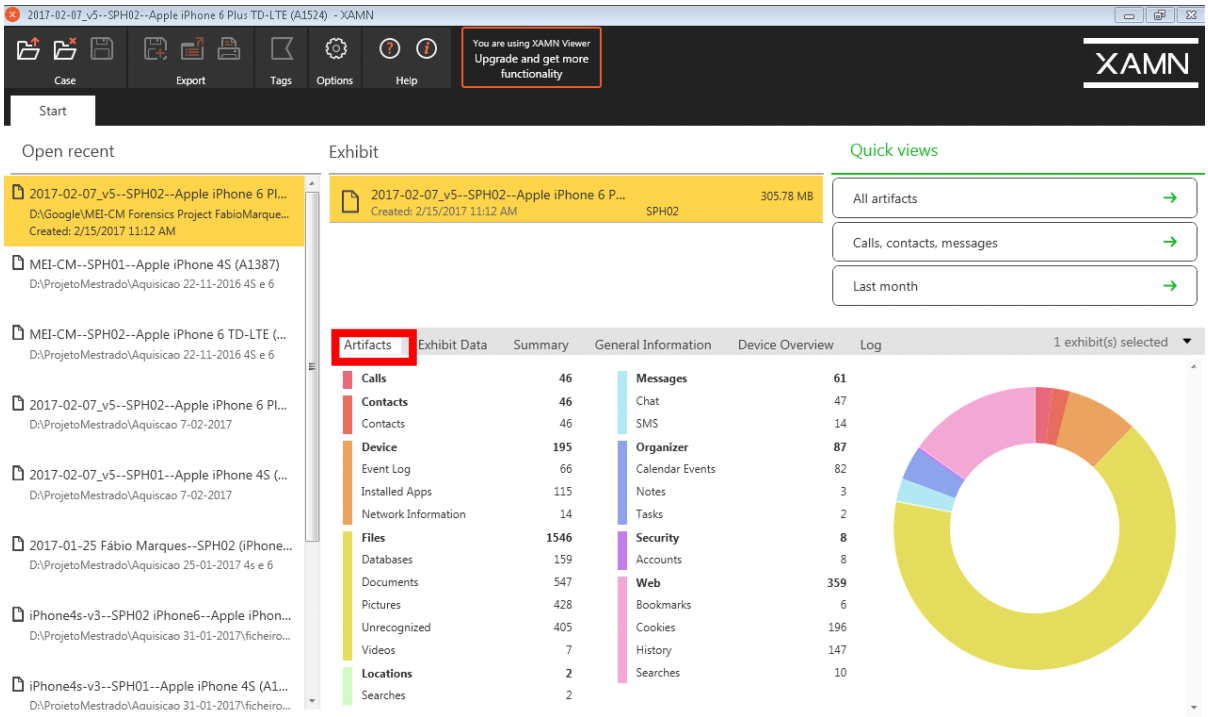


Figura 22 – Resumo de alguns dados recolhidos do dispositivo

A Figura 23 apresenta o separador “Exhibit Data” que contém dados sobre o caso, e o responsável pela aquisição.

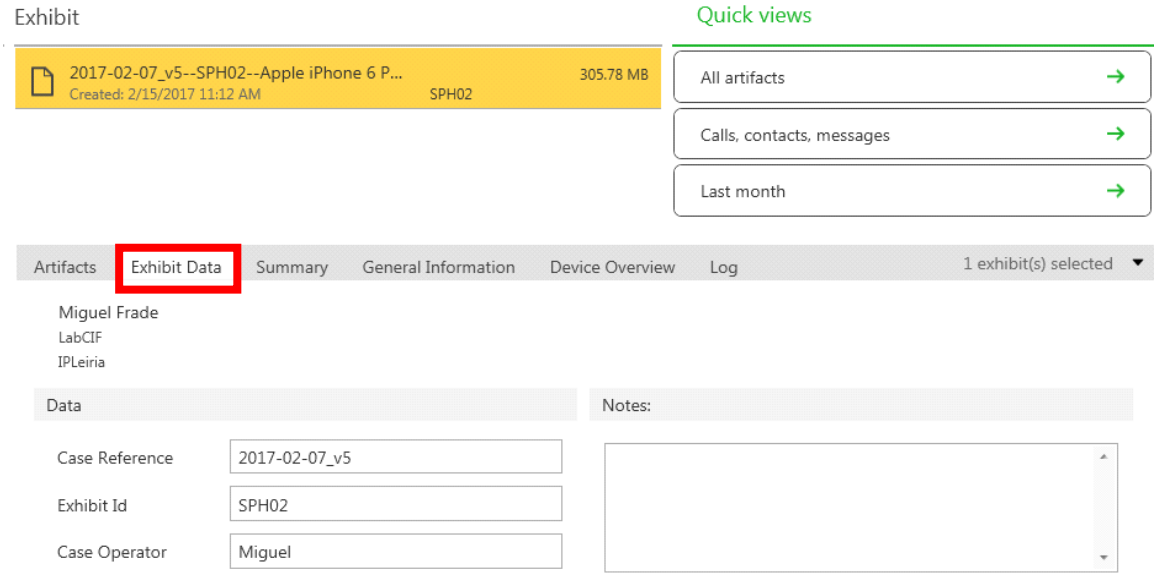


Figura 23 – Separador “Exhibit data”

No separador “Summary” apresenta a data de criação da imagem forense, a versão de software XRY como mostra a Figura 24.

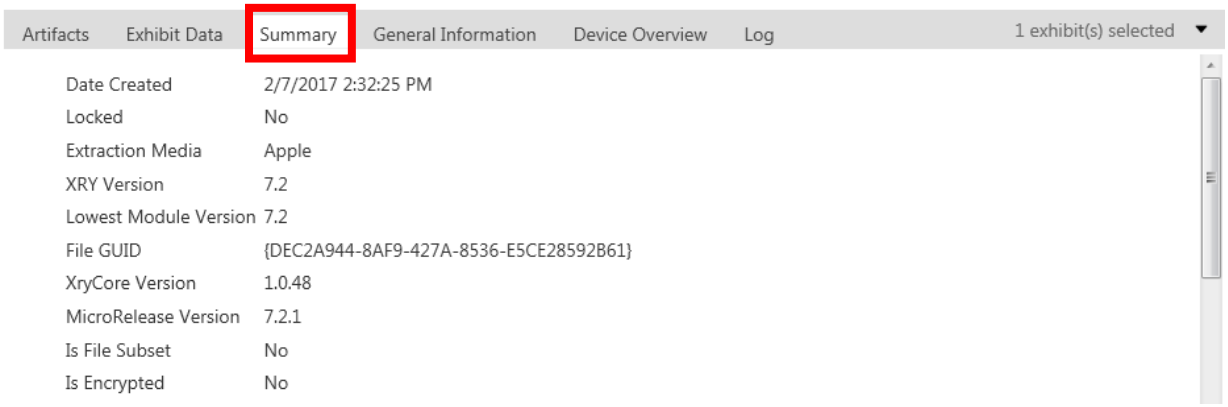


Figura 24 – Separador “Summary”.

E ainda no separador “Summary” podemos encontrar algumas estatísticas de dados encontrados como mostra a Figura 25.

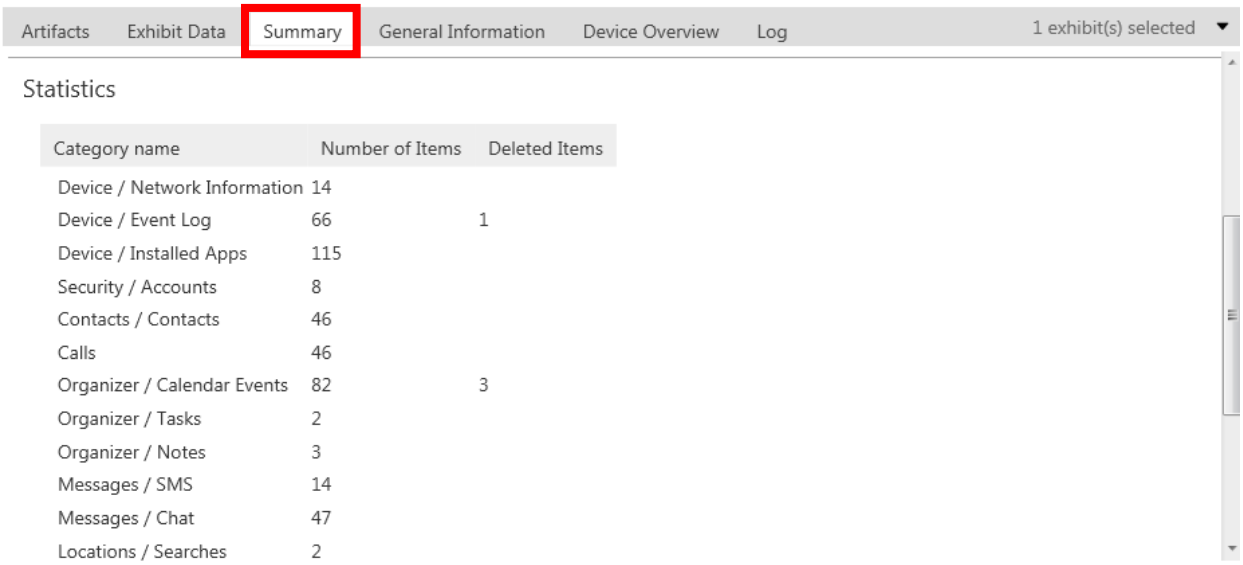


Figura 25 – Separador “Summary”.

No separador “General Information” são apresentados detalhes técnicos sobre o dispositivo como podemos ver na Figura 26 e Figura 27.

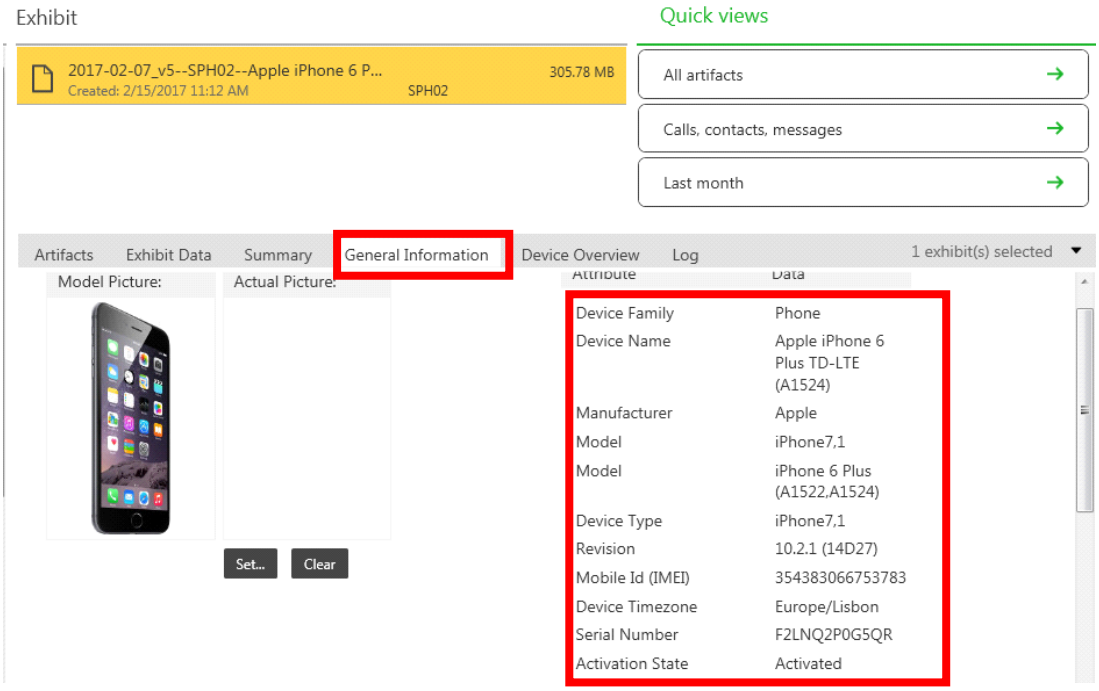


Figura 26 – Informações do dispositivo no separador “General Information”

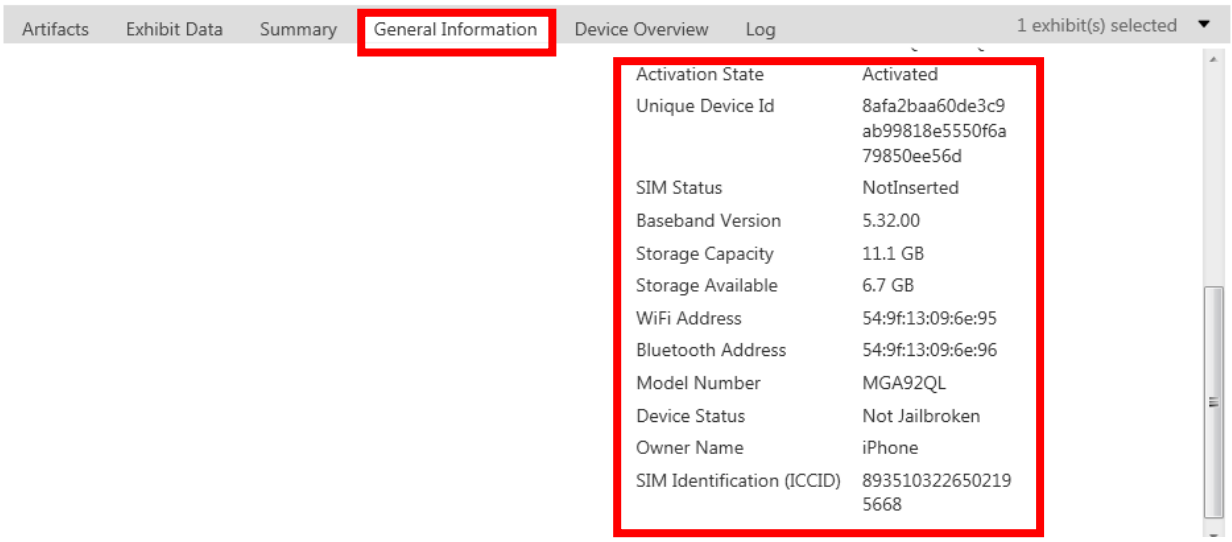


Figura 27 – Informações do dispositivo no separador "General Information"

Dos dados da figura anterior destacam-se os seguintes da Figura 28:
O IMEI, o identificador ICCID relativamente ao SIM, o número de serie do dispositivo, o identificador único do dispositivo, o endereço físico da placa Wi-Fi e Bluetooth.

Attribute	Data
Device Family	Phone
Device Name	Apple iPhone 4S (A1387)
Manufacturer	Apple
Model	iPhone4,1
Model	iPhone 4s (A1387,A1431)
Device Type	iPhone4,1
Revision	9.2.1 (13D15)
Mobile Id (IMEI)	013176002988379
Device Timezone	Europe/Lisbon
SIM Identification (ICCID)	89351060000676253089
Serial Number	DNPJ231FDTD7
Activation State	Activated
Unique Device Id	cd036fe450337c0662f043c16266fe8292efdba5
SIM Status	Ready
Baseband Version	6.0.00
Storage Capacity	27.2 GB
Storage Available	24.5 GB
WiFi Address	84:85:06:29:a1:23
Bluetooth Address	84:85:06:29:a4:30
Model Number	MD242IP
Device Status	Not Jailbroken
Owner Name	Luis's iPhone

Figura 28 – Dados importantes do dispositivo.

O separador “Device Overview” Apresenta também uma pequena descrição do dispositivo, da rede, sistema operativo, da forma como está ligado e de dados suportados pela aquisição. A Figura 29 apresenta essa informação.

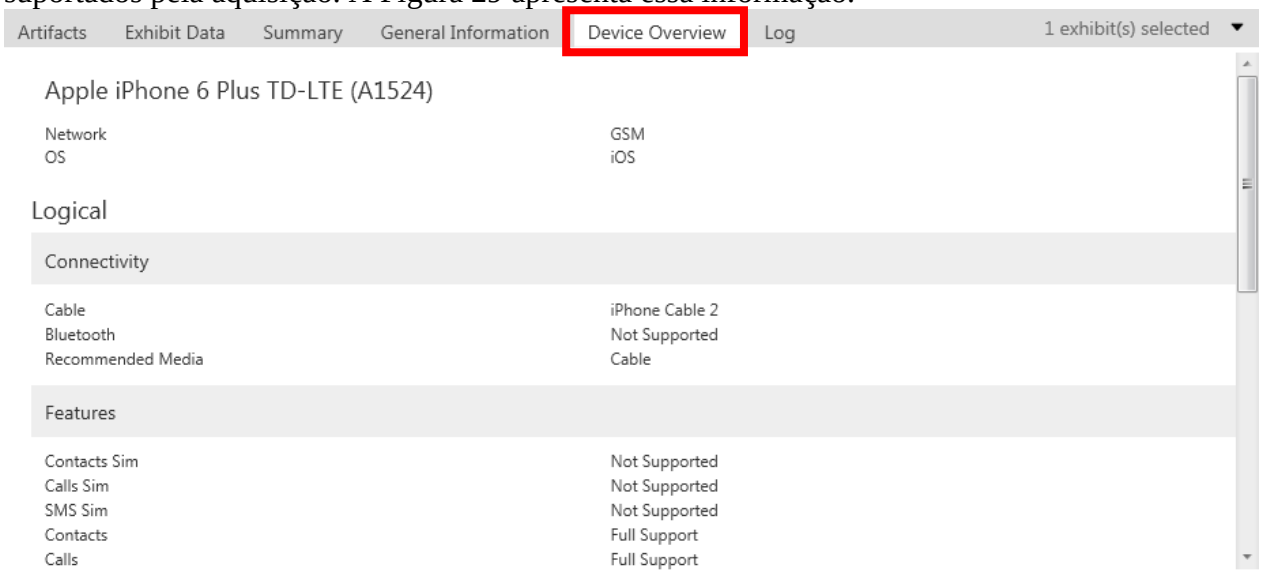


Figura 29 – Separador “Device Overview”

O separador “Log” apresenta o registo dos dados que foram obtidos dos dispositivos como mostra a Figura 30.

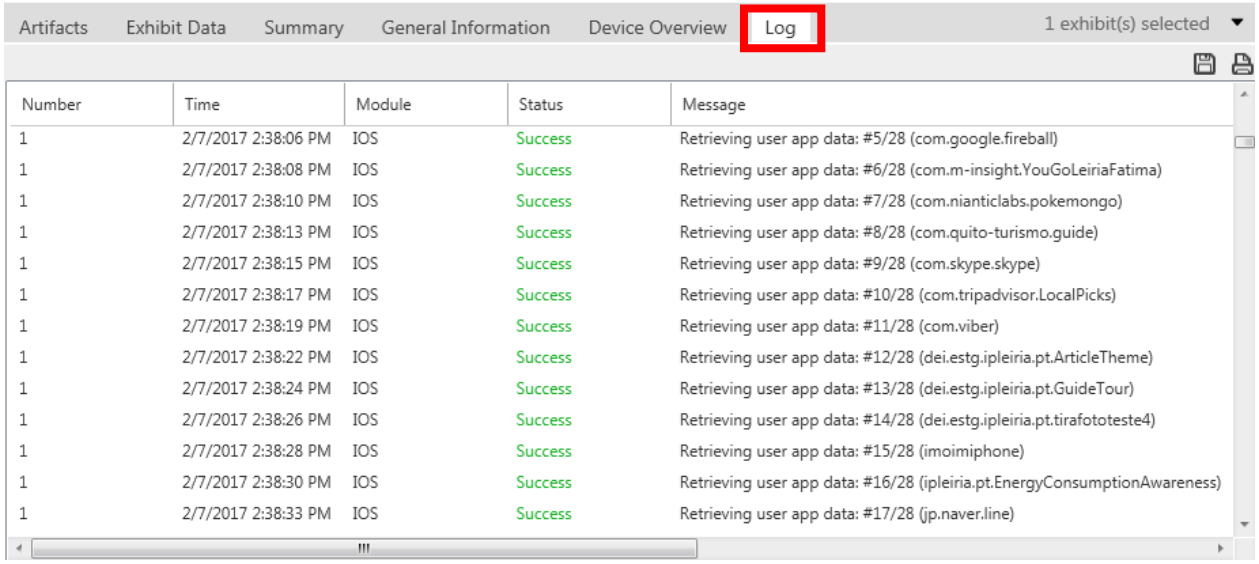


Figura 30 – Separador “Log”

Processo de procura de dados com auxílio do software XAMN.

O objetivo depois da aquisição é efetuar a procura de dados para posteriormente serem analisados. Dessa forma, nos seguintes passos iremos mostrar como se procuram determinados tipos de dados e como os podemos exportar.

A Figura 31 apresenta duas formas essenciais de aceder aos dados. Em cima no separador verde "Quick Views" podemos escolher "All Artifacts" e iremos aceder a todos os dados obtidos, separados por separadores. Como outra opção podemos escolher "Calls, contacts, messages" que nos leva a uma página com estas opções escolhidas. A opção "Last Month" iria levar-nos às ultimas procuras de dados efetuadas no mês passado.
Em baixo, no separador "Artifacts" contemos uma série de dados organizados por categorias que podemos escolher para visualizar mais rapidamente. Por exemplo, se queremos ver apenas bases de dados iriamos escolher "Databases".

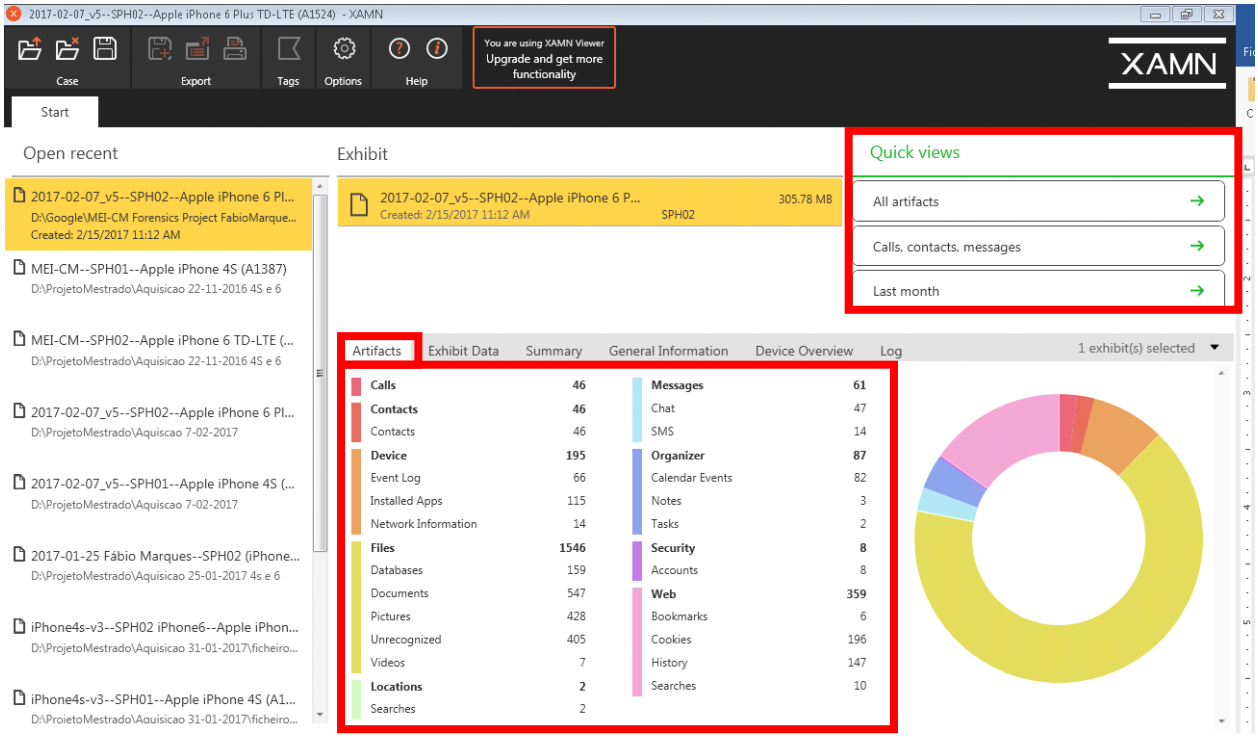


Figura 31 – Página do software com diversas formas organizadas de aceder aos dados.

De uma forma mais concreta iremos exemplificar ambas as formas de visualizar os dados.

Se optarmos pela opção “All Artifacts” na opção de “Quick Views” como mostra a Figura 32 e quisermos procurar manualmente somos levados a uma página como mostra a Figura 33.

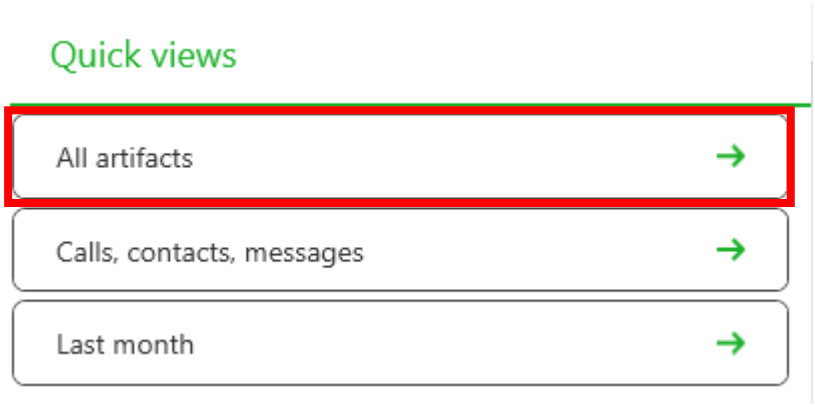


Figura 32 – Opções do separador “Quick Views”

A Figura 33 e a Figura 34 contém uma numeração para diversas funcionalidades legendadas mais abaixo.

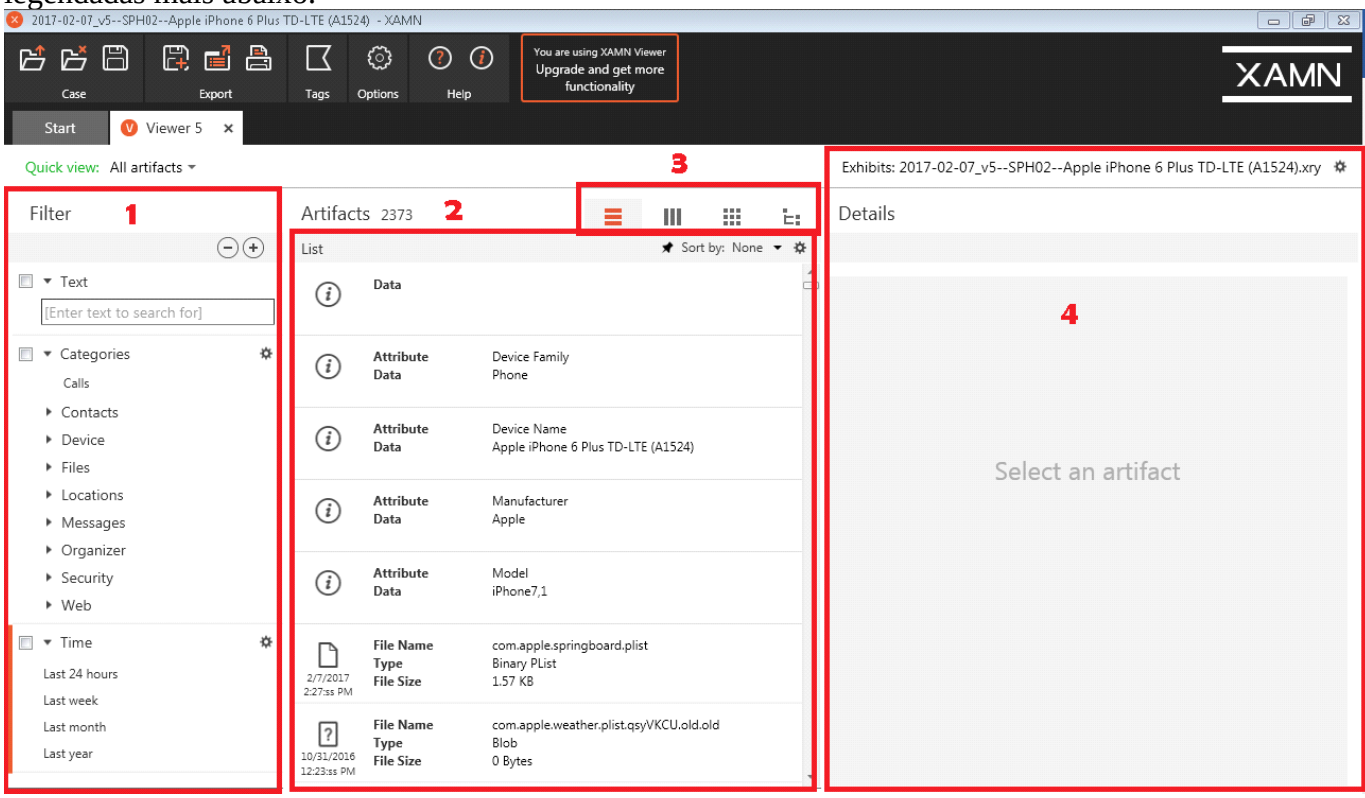


Figura 33 – Página do software XAMN para procura de dados.

1 (Filtros) – Nesta coluna é possível filtrar e selecionar os dados que queremos visualizar.

2 (Detalhes dos ficheiros) – Detalhes dos ficheiros por linhas dependendo da vista escolhida em 3.

3 (Formas de visualização) – Formas de visualização dos ficheiros e ou das suas informações e detalhes.

4 (Detalhes específicos, pré-visualização ou opções para os ficheiros) – Detalhes específicos sobre um determinado ficheiro ou pré-visualização. Um exemplo de detalhes está representado na Figura 36. A Figura 39 apresenta a legenda dos botões que permitem guardar os ficheiros individualmente entre outras opções.

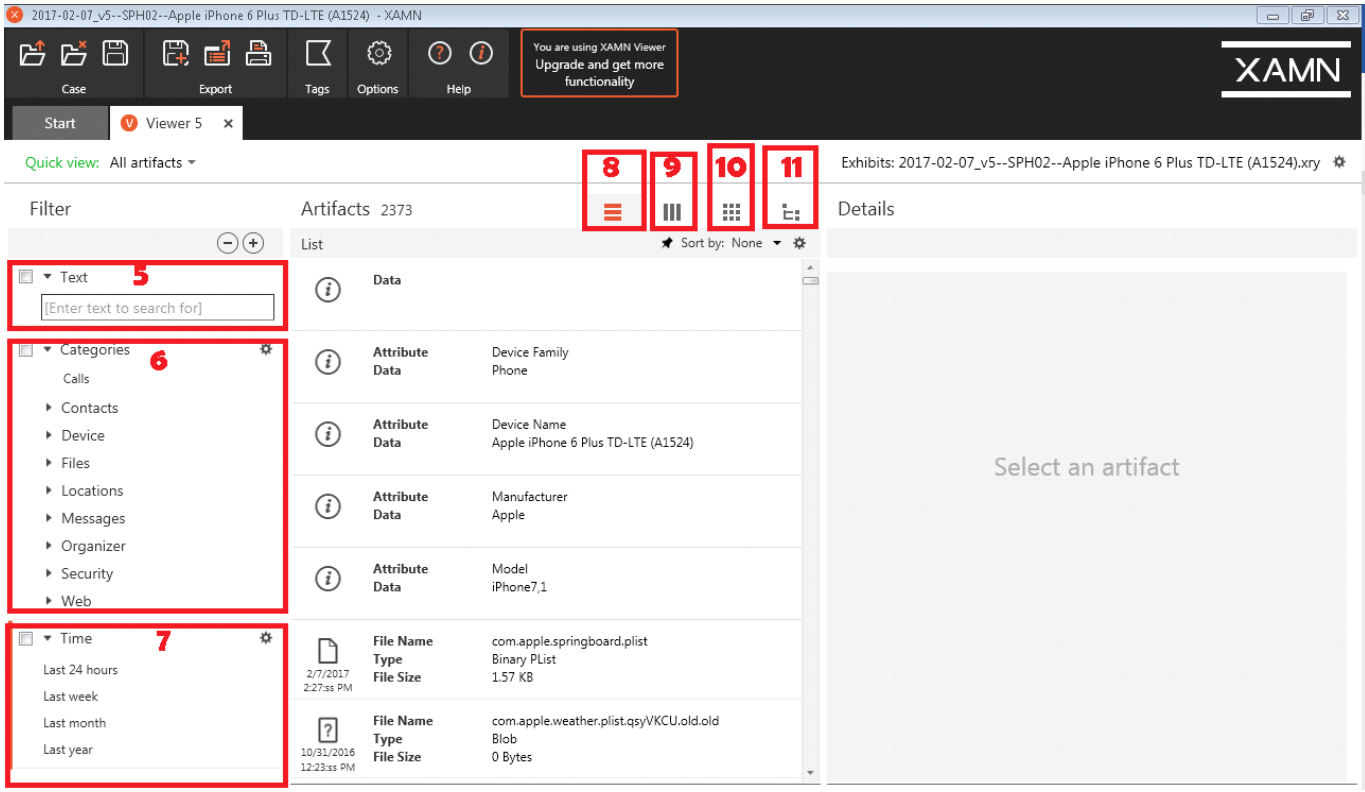


Figura 34 - Página do software XAMN para procura de dados.

5 (Pesquisa por texto) – Nesta caixa de texto é possível colocar texto e efetuar uma pesquisa sobre um determinado nome conhecido de um ficheiro ou extensão de ficheiro. Na Figura 35 podemos comprovar uma pesquisa por texto.

6 (Pesquisa por categorias ordenadas) – Nesta opção existem uma série de menus com categorias de dados ordenados que o software reconheceu e organizou. É possível efetuar uma seleção do tipo de dados que pretendemos procurar em concreto, poupando assim algum tempo. Na Figura 36 podemos verificar uma pesquisa por categoria em que selecionamos a categoria contactos e um dos contactos.

7 (Pesquisa por data) – Nesta opção podemos procurar determinados ficheiros que tenham sido criados numa determinada data dependendo das opções disponíveis. Na Figura 37 podemos verificar uma pesquisa por data,

8 (Vista em forma de lista) – Nesta vista é possível ver os ficheiros ou dados em forma de lista na coluna abaixo. A Figura 38 contém um exemplo desta vista.

9 (Vista em forma de coluna com mais detalhes) – Nesta vista é possível ver cada ficheiro por linha mas com colunas com uma série de detalhes diferentes. A Figura 38 contém um exemplo desta vista.

10 (Vista de galeria) – Na Vista de galeria é possível ver uma pré-visualização de imagens existentes na lista de ficheiros. A Figura 38 contém um exemplo desta vista.
11 (Vista de hierarquia de pastas e ficheiros) – Nesta vista é possível navegar pelas pastas e ficheiros. A Figura 38 contém um exemplo desta vista.

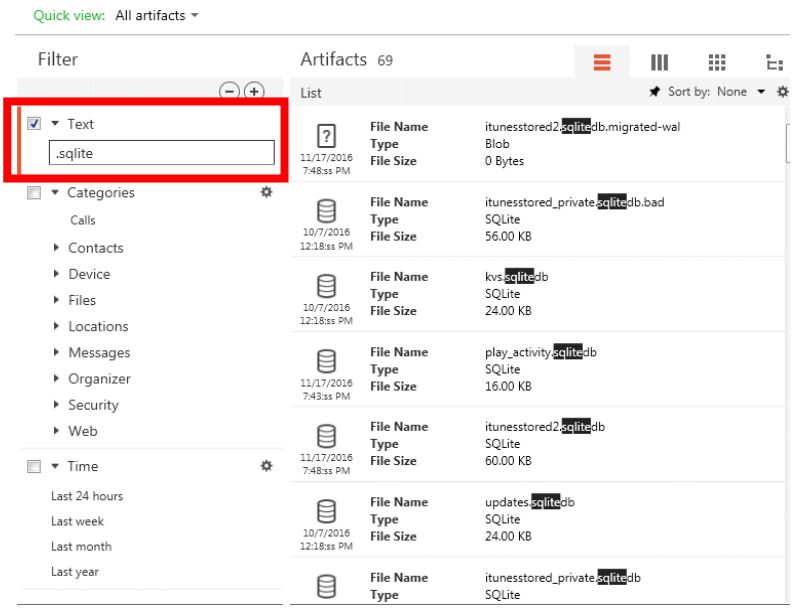


Figura 35 – Filtro – Pesquisa por texto.

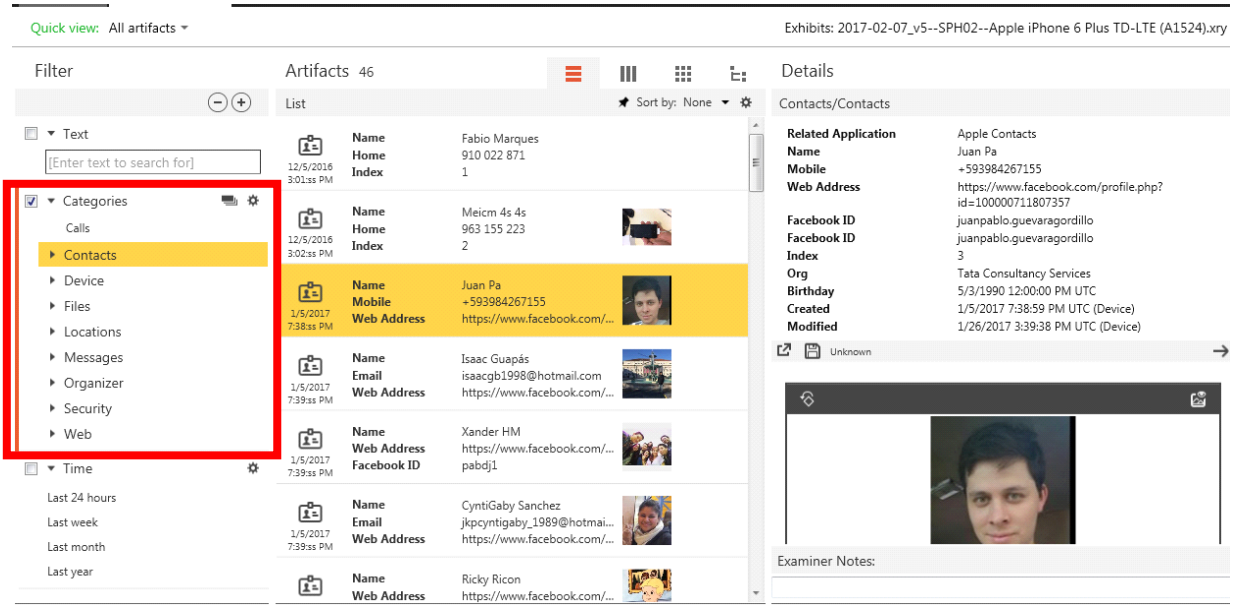


Figura 36 – Pesquisa por categorias.

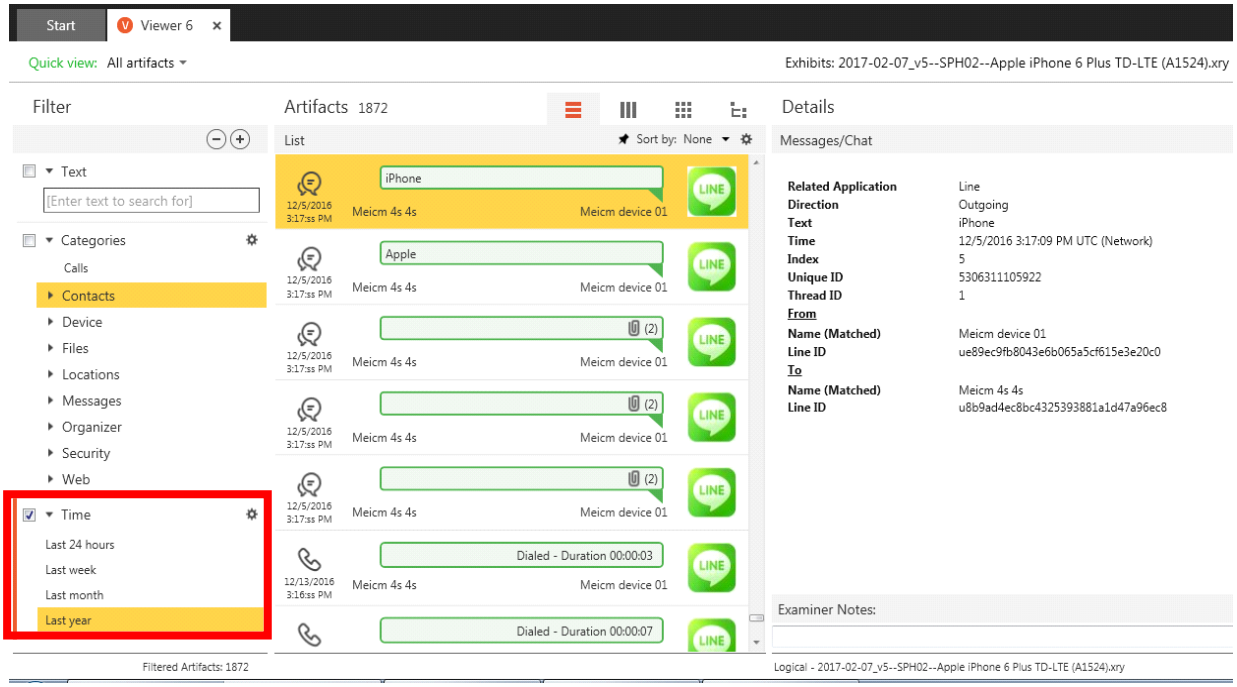


Figura 37 – Pesquisa por data.

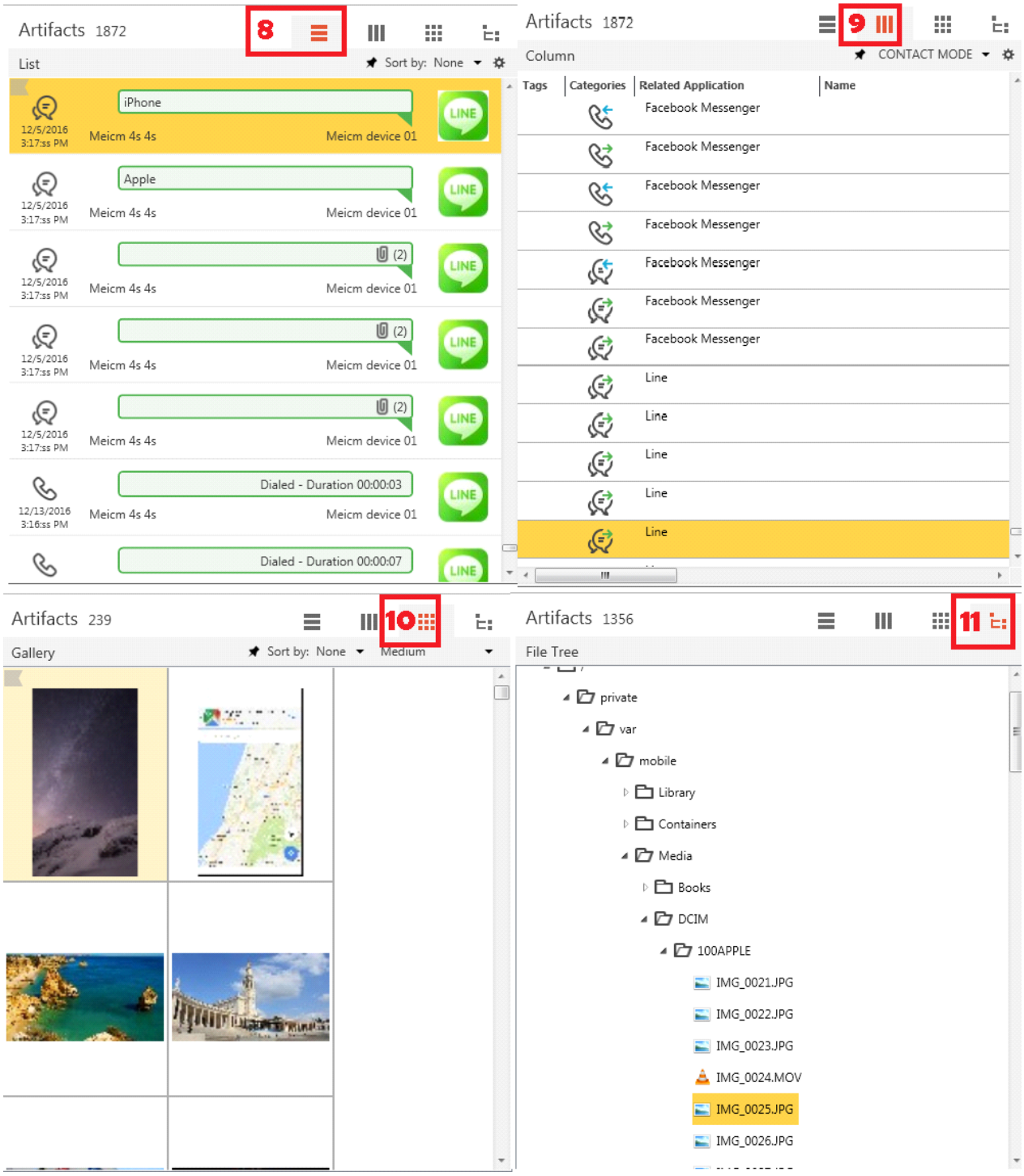


Figura 38 – Legenda das vistas de lista (8), coluna com detalhes (9), galeria (10) e hierarquia de pastas e ficheiros (11).

A Figura 39 apresenta a complementação do número 4 da Figura 33 em que é possível ver detalhes de um determinado ficheiro em conjunto com a pré-visualização do mesmo. Em baixo apresentamos a legenda dos números 12, 13 14 e 15.

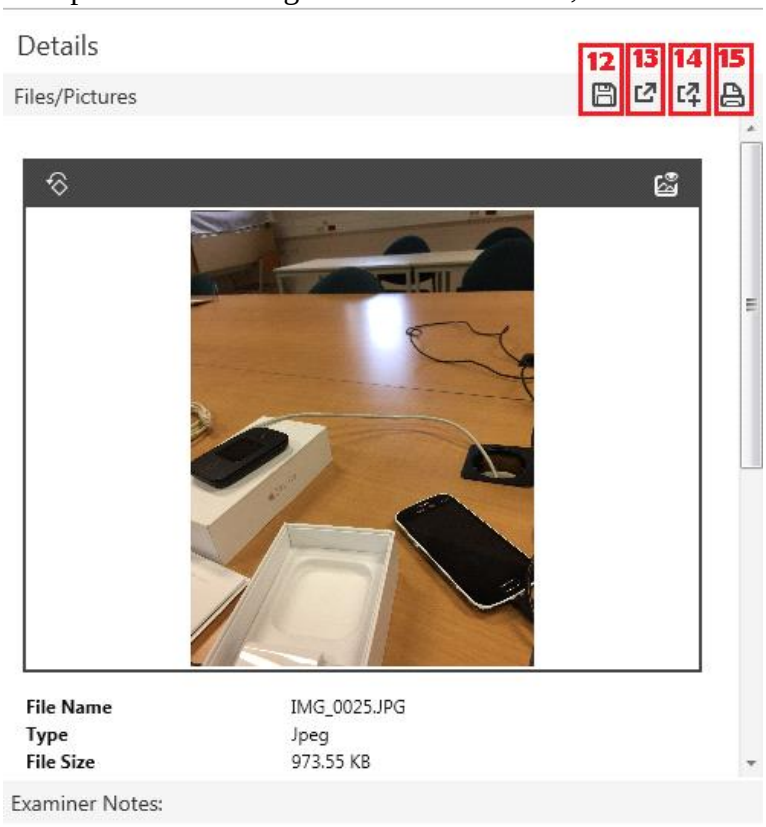


Figura 39 – Detalhes de um determinado ficheiro e opções.

12 (Exportar ficheiro) – Esta opção permite exportar um dado ficheiro numa localização à escolha para futura analise.

13 (Abrir o ficheiro na aplicação por defeito) – Esta opção permite abrir o ficheiro na aplicação por omissão, caso exista aplicação para o efeito instalada no computador.

14 (Escolher que aplicação pode abrir este ficheiro) - Esta opção permite escolher a aplicação do computador para abrir determinado ficheiro.

15 (Vista para impressão) – Esta opção permite gerar uma página com a pré-visualização e alguns detalhes para futura impressão. – Ver Figura 40.

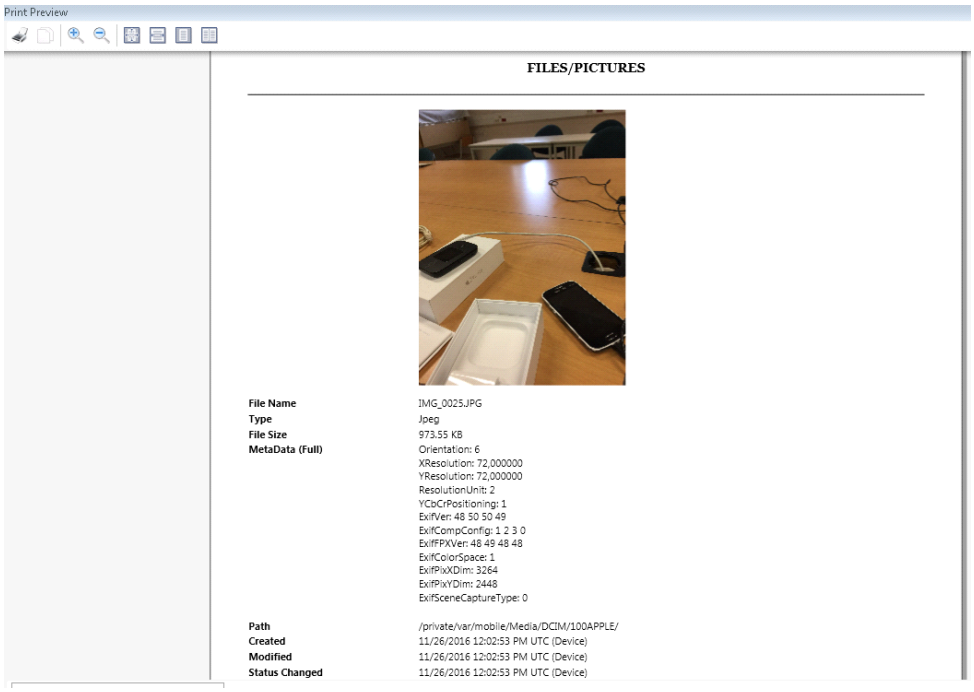


Figura 40 – Opção de pré-visualização para impressão.

Escolhendo uma categoria do separador "Artifacts" podemos chegar mais rápido a um tipo de dados. A Figura 41 vem em complementação do que foi referido anteriormente na Figura 31,

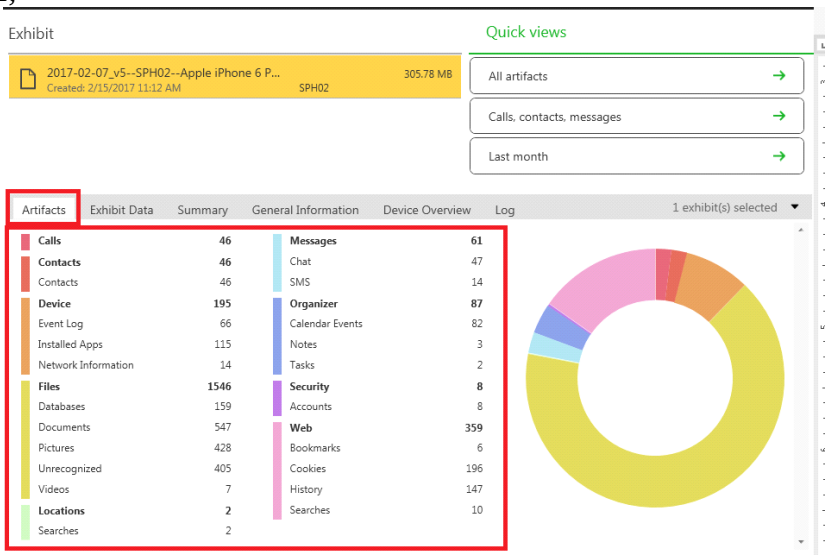


Figura 41 – Separador "Artifacts" com um conjunto de categorias de dados organizados.

Se optarmos por escolher um tipo de dados do separador “Artifacts” somos direcionados para uma página igual à da Figura 34 referida anteriormente, mas com o tipo de dados selecionado. A Figura 42 apresenta um exemplo.

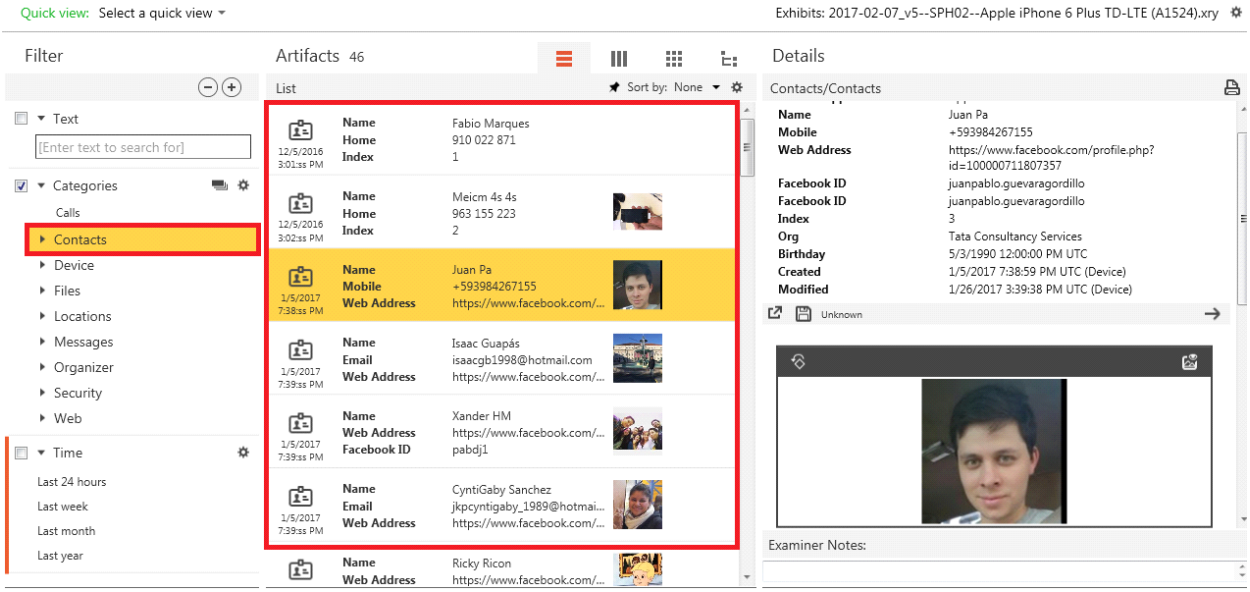


Figura 42 – Resultado da escolha de um tipo de dados no separador “Artifacts”

Chegamos ao fim deste guia.

Os dados obtidos através da procura e extração dos mesmos com base no software XAMN são depois analisados para poder tirar conclusões acerca das provas recolhidas.

Projeto

Mestrado de Engenharia Informática – Computação Móvel

Digital Forensics procedures for Apple Devices

Anexo B – Tabela de resultados da aquisição Parte 1

Fábio António Lavrador Amado Marques

O anexo “Tabela de resultados da aquisição parte 1” contempla os resultados da aquisição e pesquisa de ficheiros através do software XRY. Os ficheiros contidos nas tabelas foram alvo de uma análise com várias ferramentas para poder determinar o conteúdo desses mesmos ficheiros.

Este anexo contempla o resultado das aquisições forenses efetuadas nas seguintes datas:

07-11-2016 e 22-11-2016

Os dispositivos à qual foram feitas aquisições foram os seguintes da Tabela 1. São também apresentadas as versões do sistema operativo iOS.

Tabela 1 - Dispositivos utilizados e respetivas versões de sistema operativo iOS.

Dispositivos	Versão de iOS
Iphone 4s (A1387)	9.2.1
Iphone 6S (A1586)	9.2

As aplicações testadas foram as seguintes:

- Google Allo;
- Cyphr;
- Imo;
- Line;
- Facebook Messenger;
- Signal;
- Skype;
- Telegram;
- Viber;
- WhasApp;
- iMessage.

Além das aplicações testadas, foi tido em consideração dados que pudessem conter dados de aplicações internas do dispositivo tais como: Mensagens SMS, Chamadas de voz, e-mail, fotografias com ou sem localização, vídeos, eventos de calendário, notas, registos de acesso à rede *wi-fi* entre outros dados.

A Tabela 2 apresenta os tipos de teste feitos às aplicações tendo em conta que nem todas as aplicações possuem todas as funcionalidades.

Tabela 2 - Tipos de testes efetuados às aplicações

Teste	Descrição
A	Troca de mensagens, ficheiros, chamada de voz e vídeo.
B	Troca de mensagens, ficheiros e chamada de voz.
C	Troca de mensagens e ficheiros.
D	Troca de mensagens

A Tabela 3 apresenta os tipos de teste feitos às aplicações tendo em conta que nem todas as aplicações possuem todas as funcionalidades.

Tabela 3 - Aplicações e tipos de testes efetuados às mesmas.

Aplicação	Tipo de teste
Gogle Alo	C
Cyphr	B
Imo	A
Line	A
Messenger	A
Signal	B
Skype	A
Telegram	C
Viber	A
WhatsApp	A
iMessage	D

A Tabela 4 apesenta o código de cores consoante a importância dos ficheiros e das provas encontradas.

Tabela 4 – Esquema de cores consoante a informação dos ficheiros.

Relevância de ficheiro	Código de cor
Ficheiro com informação mais relevante	
Ficheiro com informação menos relevante	
Ficheiro sem informação	

A Tabela 5 apresenta os resultados de aquisição de dados do IPhone 4s.

Tabela 5 - Tabela de aquisição de dados do Iphone 4s

Aplicação	Ficheiro	Localização do ficheiro	Dados obtidos
Allo (Google)	com.google.fireball.plist	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém o número de telemóvel do dispositivo e que está associado à aplicação
	com.google.fireball.pushstore	/private/var/mobile/Library/SpringBoard/ PushStore/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados.
Cyphr	Sem testes uma vez que esta aplicação não estava instalada		
imo	group.im.imo.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/Preferences/	-Ficheiro de formato ".plist" -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação imo
line	jp.naver.line.plist	/private/var/mobile/Containers/Data/ Application/jp.naver.line/Library/Preferences/	-Ficheiro de formato ".plist" -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação imo
	Line.sqlite	/private/var/mobile/Containers/Shared /AppGroup/ group.com.linecorp.line/Library/Application Support/PrivateStore /P_u8b9ad4ec8bc4325393881a 1d47a96ec8/Messages/	-Ficheiro de formato ".sqlite" -Lista de contactos da aplicação com nome e número de telemóvel. -Mensagens trocadas entre

			os contactos e respetivos números de telemóvel -Registo de chamadas efetuadas
	group.com.linecorp.line.plist	/private/var/mobile/Containers/Shared /AppGroup/ group.com.linecorp.line/Library/Preferences/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados.
	jp.naver.line.pushstore.plist	/private/var/mobile/Library/SpringBoard /PushStore/	-Ficheiro de formato ".plist" -Com informação de uma chamada de vídeo recebida e o nome do contacto.
Messenger	com.facebook.Messenger.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados. - Com certificados SSL
	group.com.facebook. Messenger.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados.
	com.facebook.Messenger.plist	/private/var/mobile/Library/SpringBoard /ApplicationShortcuts/	-Ficheiro de formato ".plist" -Com informação dos contactos da aplicação Messenger e respetivos nomes.
Signal	org.whispersystems.signal.plist	/private/var/mobile/Containers/Data/Application/ org.whispersystems.signal/Library/Preferences/	-Ficheiro de formato ".plist" -Com a data da instalação da aplicação.
	com.apple.deltainstallcommands. org.whispersystems.signal	/private/var/mobile/Media/Downloads/- 5095741372043912297/-8484332955277915849/	-Ficheiro do tipo texto -Com bibliotecas
	Signal	/private/var/mobile/Media/Downloads/- 5095741372043912297/-	-Ficheiro executável -Sem dados possíveis de

		8484332955277915849/Payload/Signal.app/	serem interpretados.
	com.apple.deltainstallcommands.org.whispersystems.signal	/private/var/mobile/Media/Downloads/95609824770112569 1/-6178039652087907965/	-Ficheiro do tipo texto -Sem dados possíveis de serem interpretados. -Bibliotecas
	Signal.supp	/private/var/mobile/Media/Downloads/95609824770112569 1/-6178039652087907965/Payload/Signal.app/SC_Info/	-Ficheiro com dados de texto - Sem dados possíveis de serem interpretados. -Ficheiro do tipo “Data”
	Signal2	/private/var/mobile/Media/Downloads/95609824770112569 1/-6178039652087907965/Payload/Signal.app/	-Ficheiro executável -Sem dados possíveis de serem interpretados.
Skype	MediaStackETW.etl	/private/var/mobile/Containers/Data/Application/com.skype.skype/Documents/	-Ficheiro “Microsoft Event Trace Log File” -Contém registos de eventos se aberto com o gestor de eventos do Windows.
	Skype.blog	/private/var/mobile/Containers/Data/Application/com.skype.skype/Documents/	-Ficheiro de extensão “.blog” -Contém endereços IP e portos.
	Skype-1.blog	/private/var/mobile/Containers/Data/Application/com.skype.skype/Documents/	-Ficheiro de extensão “.blog” -Contém endereços IP e portos.
	Skype-2.blog	/private/var/mobile/Containers/Data/Application/com.skype.skype/Documents/	-Ficheiro de extensão “.blog” -Sem dados possíveis de

			serem interpretados.
	Cookies.binarycookies	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Library/Cookies/	-Ficheiro de extensão ".binarycookies" Persistent cookies. -Contém a versão de Skype instalada
	com.skype.skype.plist	/private/var/mobile/Containers/Data/Application/ com.skype.skype/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação da conta de utilizador do utilizador da aplicação.
	authentication.archive.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.skype.skype/interapp/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	com.skype.skype.pushstore.plist	/private/var/mobile/Library/SpringBoard/ PushStore/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
Telegram	ph.telegra.Telegraph.plist	/private/var/mobile/Containers/ Data/Application/ph.telegra.Telegraph/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém configurações da aplicação.
Viber	com.viber.plist	/private/var/mobile/Containers/Data/Application/ com.viber/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação relativa ao número de telemóvel associado à conta de utilizador.
	avatar.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro de extensão ".jpg" .Fotografia do perfil de utilizador da conta local.

	group.viber.share.container.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/ Library/Preferences/	-Ficheiro de extensão “.plist” -Com informação relativa ao número de telemóvel associado à conta de utilizador.
	SecureStorage.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo ”Sqlite Database”. -Sem dados possíveis de serem interpretados.
	Shared.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo ”Sqlite Database”. -Com informação relativa aos contactos com que se trocou informações -Contém números de telemóveis relativos às contas dos contactos.
	com.apple.deltainstallcommands.com.viber	/private/var/mobile/Media/ Downloads/8162430225171061633/-4373835475155680820/	-Ficheiro “ASCII Text” -Contém a versão do programa -Contém hash md5
	Viber	/private/var/mobile/Media/ Downloads/8162430225171061633/-4373835475155680820/Payload/Viber.app/	-Ficheiro executável -Sem dados possíveis de serem interpretados.
	Contacts.data	/private/var/mobile/Containers/Data /Application/com.viber/Documents/	-Ficheiro do tipo ”Sqlite Database”. -Contém os contactos com que se estabeleceu conversa na aplicação -Contém conversas de texto

			trocadas entre utilizadores.
WhatsApp	blockedcontacts.dat.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	calls.backup.log.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas e os respetivos nomes de utilizador e números de telemóvel.
	calls.log.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas e os respetivos nomes de utilizador e números de telemóvel.
	StatusMessages.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp /Documents/	-Ficheiro de extensão ".plist" -Contém algumas mensagens de texto predefinidas.
	SyncHistory.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém uma data sobre a ultima sincronização e cópia das conversas.
	fieldstats.active	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Library/ FieldStats/	-Contém endereços IP -Contém a versão do dispositivo
	whatsapp-2016-11-20-	/private/var/mobile/Containers/	-Ficheiro "UTF8 unicode

	22-27-26-049-WhatsApp-18.log	Data/Application/net.whatsapp.WhatsApp/ Library/Logs/	text” -Contém números de telemóvel associados às contas de utilizador dos contactos e do utilizador local. -Contém o nome da operadora associada ao cartão SIM.
	7acdbda6-b478-431d-ab1b-03e91d3173ff.jpg	/private/var/mobile/Containers/ Data/Application/net.whatsapp.WhatsApp /Library/Media/ 351910022871@s.whatsapp.net/7/a/	-Ficheiro de extensão “.jpg” -Fotografia enviada durante uma conversa.
	7acdbda6-b478-431d-ab1b-03e91d3173ff.thumb	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Library /Media/351910022871@s.whatsapp.net/7/a/	-Ficheiro de extensão “.thumb” -Miniatura de fotografia envidada durante uma conversa.
	Media (Pasta)	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Library /Media	-Contém uma pasta por cada contacto que se estabeleceu uma conversa. -Existem subpastas com anexos trocados, nomeadamente imagens
	net.whatsapp.WhatsApp.plist	/private/var/mobile/Containers/ Data/Application/net.whatsapp.WhatsApp/ Library/Preferences/	-Ficheiro de extensão “.plist” -Contém o número de telemóvel de um dos contactos.
	UITextInput ContextIdentifiers.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/	-Ficheiro de extensão “.plist”

		Library/Preferences/	-Contém os números de telemóvel associados às contas de utilizador com quem o utilizador trocou mensagens no chat.
	Biz.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/Biz/	-Ficheiro do tipo ”Sqlite Database”. -Sem dados possíveis de serem interpretados
	ChatSearch.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém, para cada contacto do chat o registo de texto trocado nas conversas
	ChatStorage.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém os contactos com quem se trocou mensagens no chat -Contém o índice de anexos trocados nas mensagens -Contém texto trocado entre as conversas e os respetivos contactos
	Contacts.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém os contactos do telemóvel na aplicação whatsapp

	Jobs.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Sem dados possíveis de serem interpretados
	group.net. whatsapp. WhatsApp.shared.plist	/private/var/mobile/ Containers/Shared/AppGroup/ group.net.whatsapp.WhatsApp.shared/ Library/Preferences/	-Ficheiro de extensão “.plist” -Contém o numero de telemóvel associado à conta de utilizador do whatsapp
	Pasta (Profile)	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/ Media/Profile/	-Contém a foto de perfil e a miniatura do utilizador da conta da aplicação local.
	net.whatsapp.WhatsApp2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	Ficheiro de extensão “.plist”. -Sem dados possíveis de serem interpretados
	WhatsApp	/private/var/mobile/Media/ Downloads/-8986121162958679320/ 2469026049518789349/Payload/ WhatsApp.app/	-Ficheiro executável
iMessage	Sms.db	/private/var/mobile/Library/SMS/	-Ficheiro do tipo ”Sqlite Database” -Contém as mensagens SMS do dispositivo com o texto trocado e números de telemóvel.

A Tabela 6 representa ficheiros encontrados que estão relacionados com funcionalidades do dispositivo.

Tabela 6 - Outros ficheiros encontrados relacionados com funcionalidades do dispositivo.

Ficheiro	Localização do Ficheiro	Descrição / Aplicação relacionada	Dados obtidos
CellularUsage.db	/private/var/wireless/Library/Databases/		-Ficheiro do tipo ”Sqlite Database”. -Contém número de telemóvel do cartão inserido no dispositivo
CallHistory.storedata	/private/var/mobile/Library/CallHistoryDB/	Histórico de Chamadas do dispositivo	-Ficheiro do tipo ”Sqlite Database” -Contém os números de telemóvel relacionados com chamadas do dispositivo.
Accounts3.sqlite	/private/var/mobile/Library/Accounts/	Contas de utilizador no dispositivo	-Ficheiro do tipo ”Sqlite Database”. -Contém para cada aplicação, os tipos de autenticação utilizados -Nome de utilizador de algumas aplicações
History.db	/private/var/mobile/Containers/ Data/Application/ com.apple.mobilesafari/Library/Safari/	Histórico da aplicação Safari	-Ficheiro do tipo ”Sqlite Database”. -Contém o histórico do browser safari.
downloads.28.sqlitedb	/private/var/mobile/Media/Downloads/	Histórico de download de aplicações	-Ficheiro do tipo ”Sqlite Database”. -Contém algumas aplicações que foram instaladas no dispositivo a partir da appstore.

Photos.sqlite	/private/var/mobile/Media/PhotoData/	Base de dados de fotografias	-Ficheiro do tipo ”Sqlite Database”. -Contém uma base de dados com uma lista de imagens do dispositivo.
com.google.Gmail.plist	/private/var/mobile/Containers/Data/ Application/com.google.Gmail/Library/ Preferences/	Gmail	-Ficheiro de extensão “.plist”. -Contém a conta de e email do utilizador
group.com.google.Gmail.plist	/private/var/mobile/Containers/ Shared/AppGroup/group.com.google.Gmail/ Library/Preferences/	Gmail	-Ficheiro de extensão “.plist” -Contém a conta de utilizador local de e-mail -Contém e-mails de outros utilizadores com quem se trocou e-mails
group.com.apple.notes.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.com.apple.notes/Library/ Preferences/	Notas	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados
com.apple.wifi.plist	/private/var/preferences/ SystemConfiguration/	Redes Wi-Fi	-Ficheiro de extensão “.plist” -Contém as redes Wi-Fi a que o dispositivo estve ligado.

A Tabela 7 contém outros dados obtidos do iphone 4s a partir dos resumos de informação do software XAMN. Os ficheiros com as imagens encontram-se em anexo. .

Tabela 7 - Tabela de aquisição de outros dados do Iphone 4s

Tipo de dados / Categoria	Descrição dos dados	Imagem
Contactos do dispositivo	Todos os contactos existentes no dispositivo, contendo número de telemóvel e nome	Contactos.png
Chamadas telefónicas	Todas as chamadas telefónicas efetuadas e recebias contendo o número de telemóvel, nome do contacto e a data/hora da chamada	Chamadas.png
Mensagens	Mensagens trocadas via sms, facebook, Line, viber e WhatsApp	Mensagens.png MensagensFacebook.png MensagensViber.png MensagensWhatApp.png MensagensLine.png
Localização	Dados de localização com respetivas coordenadas GPS em Graus e fotografia do mapa	localizacao.png
Histórico WEB	Histórico web da aplicação Safari, contendo o website visitado e ou a pesquisa efetuada	Historicoweb.png
Redes Wi-Fi	Redes Wi-Fi a que o dispositivo esteve ligado	Wifi.png
Fotografia	Fotografia tirada com localização por coordenadas GPS	FotografiaComCoordenadas.png

A Tabela 8 apresenta os resultados de aquisição de dados do Iphone6 S.

Tabela 8 - Tabela de aquisição de dados do Iphone 6Ss

Aplicação	Ficheiro	Localização do ficheiro	Dados obtidos
Allo (Google)	com.google.fireball.plist	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/Preferences/	-Ficheiro de formato “.plist” -Contém o número de telemóvel do dispositivo e

			que está associado à aplicação
	com.google.fireball.pushstore	/private/var/mobile/Library/SpringBoard/ PushStore/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados.
Cyphr	Sem testes uma vez que ainda não tinha instalado esta aplicação.		
imo	group.im.imo.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/Preferences/	-Ficheiro de formato ".plist" -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação imo
line	jp.naver.line.plist	/private/var/mobile/Containers/Data/ Application/jp.naver.line/Library/Preferences/	-Ficheiro de formato ".plist" -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação line
	Line.sqlite	/private/var/mobile/Containers/Shared /AppGroup/ group.com.linecorp.line/Library/Application Support/PrivateStore /P_u8b9ad4ec8bc4325393881a 1d47a96ec8/Messages/	-Ficheiro do tipo "Sqlite Database". -Lista de contactos da aplicação com nome e número de telemóvel. -Mensagens trocadas entre os contactos e respetivos números de telemóvel -Registo de chamadas efetuadas
	group.com.linecorp.line.plist	/private/var/mobile/Containers/Shared /AppGroup/ group.com.linecorp.line/Library/Preferences/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados.

	jp.naver.line.pushstore.plist	/private/var/mobile/Library/SpringBoard /PushStore/	-Ficheiro de formato ".plist" -Com informação de uma chamada de vídeo recebida e o nome do contacto. -Com informação de uma notificação
Messenger	com.facebook.Messenger.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém o nome de utilizador associado à aplicação - Com certificados SSL -Com uma chave privada SSL
	group.com.facebook. Messenger.plist	/private/var/mobile/Containers/ Shared/AppGroup/ group.com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém o UUID do facebook
	com.facebook.Messenger.plist guardado como com.facebook.Messenger2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	-Ficheiro de formato ".plist" -Com o nome da conta de utilizador local da aplicação.
Signal	org.whispersystems.signal.plist	/private/var/mobile/Containers/ Data/Application/org.whispersystems.signal/ Library/Preferences/	-Ficheiro de formato ".plist" -Com a data da instalação da aplicação.
Skype	MediaStackETW.etl	/private/var/mobile/Containers/ Data/Application/ com.skype.skype/Documents/	-Ficheiro "Microsoft Event Trace Log File" -Contém registos de eventos se aberto com o gestor de eventos do Windows.
	Skype.blog	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro de extensão ".blog" -Contém endereços IP e portos.

	Skype-1.blog	/private/var/mobile/Containers/Data/ Application/ com.skype.skype/Documents/	-Ficheiro de extensão ".blog" -Sem dados possíveis de serem interpretados.
	Skype-2.blog	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro de extensão ".blog" -Sem dados possíveis de serem interpretados.
	Cookies.binarycookies	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Library/Cookies/	-Ficheiro de extensão ".binarycookies" Persistent cookies. -Contém a versão de Skype instalada
	com.skype.skype.plist	/private/var/mobile/Containers/Data /Application/ com.skype.skype/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação da conta de utilizador do utilizador da aplicação.
	authentication.archive.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.skype.skype/interapp/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	com.skype.skype.pushstore.plist	/private/var/mobile/Library/ SpringBoard/PushStore/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
Telegram	ph.telegra.Telegraph.plist	/private/var/mobile/ Containers/Data/Application/ ph.telegra.Telegraph/Library/ Preferences/	-Ficheiro de formato ".plist" -Contém configurações da aplicação.
Viber	com.viber.plist	/private/var/mobile/Containers/Data/ Application/com.viber/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação relativa ao número de telemóvel associado à conta de

			utilizador.
	group.viber.share.container.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/ Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação relativa ao número de telemóvel associado à conta de utilizador. -Com o nome da conta de utilizador da conta da aplicação.
	SecureStorage.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo "Sqlite Database". -Sem dados possíveis de serem interpretados.
	Shared.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo "Sqlite Database". -Com informação relativa aos contactos com que se trocou informações -Contém números de telemóveis relativos às contas dos contactos.
WhatsApp	blockedcontacts.dat.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	calls.backup.log.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas e os respetivos nomes de utilizador e

			números de telemóvel.
	calls.log.plist	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas e os respetivos nomes de utilizador e números de telemóvel.
	StatusMessages.plist.xml	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".xml" -Contém algumas mensagens de texto predefinidas.
	SyncHistory.plist.xml	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".xml" -Contém uma data sobre a ultima sincronização.
	fieldstats.active	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/FieldStats/	-Contém endereços IP -Contém a versão do dispositivo
	whatsapp-2016-11-20-22-27-26-049-WhatsApp-18.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro "UTF8 unicode text" -Contém números de telemóvel associados às contas de utilizador dos contactos e do utilizador local. -Contém o nome da operadora associada ao cartão SIM. -Contém o tipo de dispositivo
	237c7b76-c508-4075-b0d7-b323f59d506c.jpg		-Ficheiro de extensão ".jpg" -Fotografia enviada durante uma conversa.
	Media (Pasta)	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Media	-Contém uma pasta por cada contacto que se estabeleceu uma conversa.

			-Existem subpastas com anexos trocados, nomeadamente imagens
	net.whatsapp.WhatsApp.plist	/private/var/mobile/Containers/ Data/Application/net.whatsapp.WhatsApp/ Library/Preferences/	-Ficheiro de extensão ".plist" -Contém o número de telemóvel de um dos contactos.
	UITextInput ContextIdentifiers.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/ Library/Preferences/	-Ficheiro de extensão ".plist" -Contém os números de telemóvel associados às contas de utilizador com quem o utilizador trocou mensagens no chat.
	Biz.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/Biz/	-Ficheiro do tipo "Sqlite Database". -Sem dados possíveis de serem interpretados
	ChatSearch.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro de extensão ".sqlite" -Contém, para cada contacto do chat o registo de texto trocado nas conversas
	ChatStorage.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo "Sqlite Database". -Contém os contactos com quem se trocou mensagens no chat -Contém o índice de anexos trocados nas mensagens -Contém texto trocado entre as conversas e os respetivos

			contactos
	Contacts.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém os contactos do telemóvel na aplicação whatsapp
	Jobs.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Sem dados possíveis de serem interpretados.
	group.net. whatsapp. WhatsApp.shared.plist	/private/var/mobile/ Containers/Shared/AppGroup/ group.net.whatsapp.WhatsApp.shared/ Library/Preferences/	-Ficheiro de extensão “.plist” -Contém o numero de telemóvel associado à conta de utilizador do whatsapp
	Pasta (Profile)	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/ Media/Profile/	-Contém a foto de perfil e a miniatura do utilizador da conta da aplicação local.
	net.whatsapp.WhatsApp2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados.
iMessage	sms.db	/private/var/mobile/Library/SMS/	Mensagens SMS -Ficheiro do tipo ”Sqlite Database”. -Contém as mensagens SMS do dispositivo com o texto trocado e números de telemóvel.

Tabela 9 representa ficheiros encontrados que estão relacionados com funcionalidades do dispositivo.

Tabela 9 - Outros ficheiros encontrados relacionados com funcionalidades do dispositivo.

Ficheiro	Localização do Ficheiro	Descrição / Aplicação relacionada	Dados obtidos
CellularUsage.db	/private/var/wireless/Library/ Databases/		-Ficheiro do tipo ”Sqlite Database”. -Número de telemóvel do cartão inserido no dispositivo
com.apple.ids.service. com.apple.private.alloy.sms.plist	/private/var/mobile/Library/ Preferences/	Mensagens SMS	-Ficheiro de extensão “.plist” -Contém o número de telemóvel do cartão SIM do dispositivo
com.apple.ids.service.com.apple. private.alloy.sms.watch.plist	/private/var/mobile/Library/ Preferences/	Mensagens SMS	- Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados
com.apple.MobileSMS.plist	/private/var/mobile/Library/ Preferences/	Mensagens SMS	- Ficheiro de extensão “.plist” -Contém um número de telemóvel com quem se trocou mensagens
com.apple.imservice.SMS.plist	/private/var/mobile/Library/ Preferences/	Mensagens SMS	- Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados
CallHistory.storedata	/private/var/mobile/Library/ CallHistoryDB/	Histórico de Chamadas do dispositivo	-Ficheiro do tipo ”Sqlite Database”. -Contém os números de telemóvel relacionados com chamadas do dispositivo.

Accounts3.sqlite	/private/var/mobile/Library/ Accounts/	Contas de utilizador no dispositivo	-Ficheiro do tipo ”Sqlite Database”. -Contém para cada aplicação, os tipos de autenticação utilizados -Nome de utilizador de algumas aplicações
History.db	/private/var/mobile/Containers/ Data/Application/ com.apple.mobilesafari/Library /Safari/	Histórico da aplicação Safari	-Ficheiro do tipo ”Sqlite Database”. -Contém o registo dos sites visitados.
downloads.28.sqlitedb	/private/var/mobile/Media/ Downloads/	Histórico de download de aplicações	-Ficheiro do tipo ”Sqlite Database”. -Contém algumas aplicações que foram instaladas no dispositivo a partir da appstore.
Photos.sqlite	/private/var/mobile/Media/ PhotoData/	Base de dados de fotografias	-Ficheiro do tipo ”Sqlite Database”. -Contém uma base de dados com uma lista de imagens do dispositivo, mas não as fotos tiradas
Photos.sqlite-shm	/private/var/mobile/Media/ PhotoData/	Base de dados de fotografias	-Sem dados.
Photos.sqlite-wal	/private/var/mobile/Media/ PhotoData/	Base de dados de fotografias	Ficheiro do tipo “SQLite Write-Ahead Log” -Contém uma lista de nomes de ficheiros de fotografias -Com dados de localização de fotografias

com.google.Gmail.plist	/private/var/mobile/Containers/Data/ Application/com.google.Gmail/Library/ Preferences/	Gmail	-Ficheiro de extensão ".sqlite" -Contém a conta de e-mail do utilizador
group.com.google.Gmail.plist	/private/var/mobile/Containers/ Shared/AppGroup/ group.com.google.Gmail/ Library/Preferences/	Gmail	-Ficheiro de extensão ".sqlite" -Contém a conta de utilizador local de e-mail -Contém e-mails de outros utilizadores com quem se trocou e-mails
com.apple.wifi.plist	/private/var/preferences/ SystemConfiguration/	Redes Wi-Fi	-Ficheiro de extensão ".sqlite" -Contém as redes Wi-Fi a que o dispositivo estve ligado.
com.apple.ids.service.com.apple. private.alloy.wifi.networksync.plist	com.apple.ids.service.com.apple. private.alloy.wifi.networksync.plist	Redes Wi-Fi	-Ficheiro do tipo "Sqlite Database". -Sem dados
Calendar.sqlitedb	/private/var/mobile/Library/ Calendar/	Calendário / Eventos de calendário	-Ficheiro do tipo "Sqlite Database". -Contém dados sobre alguns feriados e outros eventos do calendário

A Tabela 10 contém outros dados obtidos do iPhone 6S a partir dos resumos de informação do software XAMN. Os ficheiros com as imagens encontram-se em anexo.

Tabela 10 - Tabela de aquisição de outros dados do Iphone 6S

Tipo de dados / Categoria	Descrição dos dados	Imagem
Contactos do dispositivo	Todos os contactos existentes no dispositivo, contendo número de telemóvel e nome	Contactos.png

Chamadas telefónicas	Todas as chamadas telefónicas efetuadas e recebias contendo o número de telemóvel, nome do contacto e a data/hora da chamada	Chamadas.png
Calendário	Dados sobre eventos do calendário, incluindo eventos agendados pelo utilizador	Calendário.png
Mensagens	Mensagens trocadas via sms, facebook, Line, viber e WhatsApp	Mensagens.png MensagensFacebook.png MensagensViber.png MensagensWhatApp.png MensagensLine.png
Histórico WEB	Histórico web da aplicação Safari, contendo o website visitado e ou a pesquisa efetuada	Historicoweb.png

Projeto

Mestrado de Engenharia Informática – Computação Móvel

Digital Forensics procedures for Apple Devices

Anexo C - Tabela de resultados da aquisição Parte 2

Fábio António Lavrador Amado Marques

O anexo “Tabela de resultados da aquisição parte 2” contempla os resultados da aquisição e pesquisa de ficheiros através do software XRY. Os ficheiros contidos nas tabelas foram alvo de uma análise com várias ferramentas para poder determinar o conteúdo desses mesmos ficheiros.

Este anexo contempla o resultado das aquisições efetuadas nas seguintes datas:

25-01-2017

31-01-2017

07-02-2017

Os dispositivos à qual foram feitas aquisições foram os seguintes da Tabela 1. São também apresentadas as versões do sistema operativo iOS.

Tabela 1 – Dispositivos utilizados e respetivas versões de sistema operativo iOS.

Dispositivos	Versão de iOS
Iphone 4s (A1387)	9.3.5
Iphone 6 plus (A1524)	10.2.1

As aplicações testadas foram as seguintes:

- Google Allo;
- Cyphr;
- Imo;
- Line;
- Facebook Messenger;
- Signal;

- Skype;
- Telegram;
- Viber;
- WhasApp;
- iMessage;

Além das aplicações testadas, foi tido em consideração dados que pudessem conter dados de aplicações internas do dispositivo tais como: Mensagens SMS, Chamadas de voz, e-mail, fotografias com ou sem localização, vídeos, eventos de calendário, notas, registos de acesso à rede *wi-fi* entre outros dados.

A Tabela 2 apresenta os tipos de teste feitos às aplicações tendo em conta que nem todas as aplicações possuem todas as funcionalidades.

Tabela 2 – Tipos de testes efetuados às aplicações

Teste	Descrição
A	Troca de mensagens, ficheiros, chamada de voz e vídeo.
B	Troca de mensagens, ficheiros e chamada de voz.
C	Troca de mensagens e ficheiros.
D	Troca de mensagens

A Tabela 3 apresenta os tipos de teste feitos às aplicações tendo em conta que nem todas as aplicações possuem todas as funcionalidades.

Tabela 3 – Aplicações e tipos de testes efetuados às mesmas.

Aplicação	Tipo de teste
Gogle Alo	C
Cyphr	B
Imo	A
Line	A
Messenger	A
Signal	B
Skype	A
Telegram	C
Viber	A
WhatsApp	A
iMessage	D

A Tabela 4 apesenta o código de cores consoante a importância dos ficheiros e das provas encontradas.

Tabela 4- Esquema de cores consoante a informação dos ficheiros.

Relevância de ficheiro	Código de cor
Ficheiro com informação mais relevante	
Ficheiro com informação menos relevante	
Ficheiro sem informação	

A Tabela 5 apresenta os resultados de aquisição de dados do iPhone 4s.

Tabela 5 - Tabela de aquisição de dados do Iphone 4s

Aplicação	Ficheiro	Localização do ficheiro	Dados obtidos
Allo (Google) (Fireball)	com.google.fireball.plist	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém o número de telemóvel do dispositivo e que está associado à aplicação
	google_tagmanager.db	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	googleanalytics-aux-v4.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados.
	googleanalytics-v2.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	googleanalytics-v3.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	GTM.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados.
	gtm_img_unrepeatable	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Documents/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados
	Na aplicação "allo" apenas encontramos o número de telemóvel relativo ao cartão sim instalado no dispositivo relacionado com a conta de utilizador.		
Cyphr	Cyphr.sqlite	/private/var/mobile/Containers/	-Ficheiro do tipo "Sqlite Database"

		Data/Application/com.goldenfrog. cyphr.mobile/Documents/	-Contém uma chave privada -Contém 3 chaves públicas -Registo de conversas entre contactos -Nomes dos contactos e contas de utilizador com quem se trocou texto e anexos
	5088E971-147F-4F7B-9BCA-3A3922F9752C	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	B79B21C5-E06F-4C33-B087-E32F4F747628	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	C54049C8-7CD0-48BA-B087-7C4993F9028C	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	CD202FB8-F6B1-4F63-9C95-DA5F1EE31981	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	F8E5334D-906D-4AB1-B528-DBC63B57D917	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	FF4C4BDF-738F-49AF-843E-253A6C35F660	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	CLSUserDefaults.plist	/private/var/mobile/Containers/ Data/Application/com.goldenfrog. cyphr.mobile/Library/Application Support/com.crashlytics/	-Ficheiro de formato “.plist” -Contém a data relativa à ultima atualização da aplicação. -Contém informação relativa ao tipo de dispositivo
	com.goldenfrog.cyphr.mobile.plist	/private/var/mobile/Containers	-Ficheiro de formato “.plist

		/Data/Application/com.goldenfrog.cyphr.mobile/Library/Preferences/	-Sem dados possíveis de serem interpretados
	Na aplicação “Cyphr” encontramos uma chave privada e várias chaves públicas, dados relativos aos contactos com quem se estabeleceu troca de texto e imagens e anexos		
imo	group.im.imo.plist	/private/var/mobile/Containers/Shared/AppGroup/group.im.imo/Library/Preferences/	-Ficheiro de formato “.plist” -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação imo.
	imoimiphone.plist	/private/var/mobile/Containers/Shared/AppGroup/group.im.imo/Library/Preferences/	-Ficheiro de formato “.plist” -Contém o número de telemóvel de um dos contactos com quem se trocou texto e imagens.
	Caches[x9]est.enc	/private/var/mobile/Containers/Shared/AppGroup/group.im.imo/Library	-Ficheiro do tipo “ASCII Text” -Contém o registo de uma mensagem de texto trocada
	Cookies.binarycookies	/private/var/mobile/Containers/Shared/AppGroup/group.im.imo/Library/cookies	-Sem dados possíveis de serem interpretados
	iat.dat	/private/var/mobile/Containers/Data/Application/imoimiphone/Documents/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados
	imo_state.dat	/private/var/mobile/Containers/Data/Application/imoimiphone/Documents/	-Ficheiro de formato “.plist” -Contém o número de telemóvel da conta da aplicação -Contém o número de telemóvel de um contacto com quem se trocou texto e imagens.
	PendingIMAndPhotoModel1.sqlite	/private/var/mobile/Containers/Data/Application/imoimiphone/Documents/	-Ficheiro do tipo “Sqlite database” -Sem dados possíveis de serem interpretados.
	rmq2.sqlite	/private/var/mobile/Containers/	-Ficheiro do tipo “Sqlite database”

		Data/Application/imoimiphone/Documents/	-Sem dados possíveis de serem interpretados.
	Na aplicação “imo” encontramos dados relativos à conta de utilizador e número de telemóvel.		
line	jp.naver.line.plist	/private/var/mobile/Containers/Data/Application/jp.naver.line/Library/Preferences/	-Ficheiro de formato “.plist” -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação line
	Line.sqlite	/private/var/mobile/Containers/Shared/AppGroup/group.com.linecorp.line/ Library/Application Support/PrivateStore/ P_u8b9ad4ec8bc4325393881a1d47a96ec8/Messages/	-Ficheiro de formato “.sqlite database” -Lista de contactos da aplicação com nome e número de telemóvel. -Mensagens trocadas entre os contactos e respetivos números de telemóvel -Registo de chamadas efetuadas.
	group.com.linecorp.line.plist	/private/var/mobile/Containers/Shared/AppGroup/ group.com.linecorp.line/Library/Preferences/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados.
	jp.naver.line.pushstore.plist	/private/var/mobile/Library/SpringBoard/PushStore/	-Ficheiro de formato “.plist” -Com informação de uma chamada de vídeo recebida e o nome do contacto.
	5239190768525	\private\var\mobile\Library\Application Support\PrivateStore\ P_u8b9ad4ec8bc4325393881a1d47a96ec8\ Message Attachments	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	Cookies.binarycookies	\private\var\mobile\Library\Cookies	-Sem dados possíveis de serem interpretados .

	History.db	\private\var\mobile\Library\NCVoIP\ u8b9ad4ec8bc4325393881a1d47a96ec8	-Ficheiro do tipo “data” -Sem dados possíveis de serem interpretados.
	Na aplicação “line” encontramos o número de telemóvel associado à conta de utilizador, o nome de utilizador, a lista de contactos, as mensagens trocadas e registos de chamadas.		
Messenger	com.facebook.Messenger.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados. - Com certificados SSL
	group.com.facebook. Messenger.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados.
	com.facebook.Messenger.plist	/private/var/mobile/Library/SpringBoard /ApplicationShortcuts/	-Ficheiro de formato “.plist” -Com informação dos contactos da aplicação Messenger e respetivos nomes.
	Cookies.binarycookies	/private/var/mobile/Containers/Shared /AppGroup/group.com.facebook.Messenger/ Library/cookies	-Sem dados possíveis de serem interpretados
	UITextInputContextIdentifiers.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados
	https_m.facebook.com_0 .localstorage	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library \WebKit\WebsiteData\LocalStorage	-Ficheiro de formato “.sqlite database” -Sem dados possíveis de serem interpretados
	StorageTracker.db	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/	-Ficheiro de formato “.sqlite database”

		Library \WebKit\WebsiteData\LocalStorage	-Sem dados possíveis de serem interpretados
	.compactdisk_extended_attributes	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Documents/ _sessionlessStore/messenger_secure_ messages.v1	-Ficheiro do tipo “ascii text” -Sem dados possíveis de serem interpretados
	rtc_storage	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Documents/ /facebook/messenger	-Ficheiro de formato “data” -Sem dados possíveis de serem interpretados
	Na aplicação “messenger” encontramos os contactos da aplicação com que foram efetuadas trocas de texto e anexos.		
Signal	org.whispersystems.signal.plist	/private/var/mobile/Containers/Data/Appli cation/ org.whispersystems.signal/Library/Prefere nces/	-Ficheiro de formato “.plist” -Com a data da instalação da aplicação.
	org.whispersystems.signal. pushstore.plist	/private/var/mobile/Library/ SpringBoard/PushStore/	-Ficheiro de formato “.plist” -Contém informação de uma chamada recebida e do respetivo contacto
	com.apple.deltainstallcommands. org.whispersystems.signal	/private/var/mobile/Media/Downloads/ 956098247701125691/ -6178039652087907965/	FIcheiro “ASCII Text” -Contém duas hash md5
	signal	/private/var/mobile/Media/Downloads/ 956098247701125691/- 6178039652087907965/ Payload/Signal.app/	-Ficheiro executável -Sem dados possíveis de serem interpretados
	Signal.supp	/private/var/mobile/Media/Downloads/ 956098247701125691/- 6178039652087907965/Payload/ Signal.app/SC_Info/	-Sem dados possíveis de serem interpretados

	Na aplicação “signal” encontramos registos de uma chamada recebida de um dos contactos com o respetivo número bem como duas hash md5.		
Skype	MediaStackETW.etl	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro “Microsoft Event Trace Log File” -Contém registos de eventos se aberto com o gestor de eventos do Windows.
	Skype.blog	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro de extensão “.blog” -Contém endereços IP e portos relativos à rede a que está ligado.
	Skype-1.blog	/private/var/mobile/Containers/Data/Application/ com.skype.skype/Documents/	-Ficheiro de extensão “.blog” -Sem dados possíveis de serem interpretados
	Skype-2.blog	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro de extensão “.blog” -Sem dados possíveis de serem interpretados.
	Cookies.binarycookies	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Library/Cookies/	-Ficheiro de extensão “.binarycookies” Persistent cookies. -Contém a versão de Skype instalada
	com.skype.skype.plist	/private/var/mobile/Containers/Data/ Application/ com.skype.skype/Library/Preferences/	-Ficheiro de extensão “.plist” -Com informação da conta de utilizador do utilizador da aplicação.
	authentication.archive.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.skype.skype/interapp/	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados.
	com.skype.skype.pushstore.plist	/private/var/mobile/Library/SpringBoard/ PushStore/	-Ficheiro de extensão “.plist” -Com informação de um dos contactos com os quais foram trocados texto e anexos.
	Na aplicação “Skype” encontramos endereços IP, Portos, informação sobre o utilizador da conta local, contactos e texto		

	trocado entre os contactos.		
Telegram	ph.telegra.Telegraph.plist	/private/var/mobile/Containers/ Data/Application/ph.telegra.Telegraph/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém configurações da aplicação.
	ph.telegra.Telegraph_2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	- Ficheiro de formato ".plist" -Contém Informação sobre os contactos com quem se trocou texto e anexos
	ph.telegra.Telegraph.pushstore	/private/var/mobile/Library/ SpringBoard/PushStore/	- Ficheiro de formato ".plist" -Contém informação de um dos contactos, nomeadamente o nome da conta.
	Na aplicação "Telegram" encontramos informação sobre os contactos com quem se trocou texto e anexos, informação sobre os contactos e pequenas partes de texto.		
Viber	com.viber.plist	/private/var/mobile/Containers/Data/Appli cation/ com.viber/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação relativa ao número de telemóvel associado à conta de utilizador.
	avatar.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro de extensão ".jpg" .Fotografia do perfil de utilizador da conta local.
	com.viber.pushstore	/private/var/mobile/Library/ SpringBoard/PushStore/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	SecureStorage.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo "Sqlite Database". -Contém a chave pública.
	Shared.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo "Sqlite Database". -Com informação relativa aos contactos com que se trocou

			informações -Contém números de telemóveis relativos às contas dos contactos.
	com.apple.deltainstallcommands.com.viber	/private/var/mobile/Media/Downloads/8162430225171061633/-4373835475155680820/	-Ficheiro “ASCII Text” -Contém a versão do programa -Contém hash md5
	Viber.app	/private/var/mobile/Media/Downloads/8162430225171061633/-4373835475155680820/Payload/Viber.app/	-Ficheiro executável -Sem dados possíveis de serem interpretados.
	Attachments (Pasta)	/private/var/mobile/Containers/Data/Application/com.viber//Documents/Attachments	-Contém anexos trocados durante as conversas entre contactos.
	ViberIcons	/private/var/mobile/Containers/Data/Application/com.viber/Documents/ViberIcons	-Contém as miniaturas das fotos de perfil da conta de utilizador.
	Contacts.data	/private/var/mobile/Containers/Data/Application/com.viber/Documents	-Ficheiro “Sqlite Database” -Contém mensagens trocadas -Contém os contactos da aplicação -Contém números de telemóvel. -Contém registo de anexos trocados -Contém registos de chamadas feitas e recebidas
	Settings.data	/private/var/mobile/Containers/Data/Application/com.viber/Documents	- Ficheiro “Sqlite Database” -Contém o número de telemóvel associado à aplicação -Contém configurações da aplicação
	Na aplicação “Viber” encontramos o número de telemóvel associado à conta de utilizador, foto de perfil e anexos trocados, uma chave pública, registos de chamadas e texto trocados entre os contactos.		
WhatsApp	blockedcontacts.dat.plist	/private/var/mobile/Containers/Data/Application/	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem

		net.whatsapp.WhatsApp/Documents/	interpretados. -Pode conter possíveis contactos bloqueados
	calls.backup.log.plist	/private/var/mobile/Containers/Data/ Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas com duração entre outros dados e os respetivos nomes de utilizador e números de telemóvel. -Contém registo dos contactos com quem se efetuou chamadas
	calls.log.plist	/private/var/mobile/Containers/Data/ Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas e os respetivos nomes de utilizador e números de telemóvel. -Contém registo dos contactos com quem se efetuou chamadas
	StatusMessages.plist.xml	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp /Documents/	-Ficheiro de extensão ".plist" -Contém algumas mensagens de texto predefinidas.
	SyncHistory.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/ Documents/	-Ficheiro de extensão ".plist" -Contém uma data sobre a ultima sincronização.
	fieldstats.active	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/ Library/ FieldStats/	-Contém endereços IP -Contém a versão do dispositivo (iphone4)

	whatsapp-2017-01-22-21-43-42-671-WhatsApp-26.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro “UTF8 unicode text” -Contém números de telemóvel associados às contas de utilizador dos contactos e do utilizador local. -Contém o nome da operadora associada ao cartão SIM. -Contém uma serie de registos relacionados com ficheiros. -Contém registos de chamadas. -Contém endereços IP
	whatsapp-2017-01-22-22-08-14-581-WhatsApp-27.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro “UTF8 unicode text” -Equivalente ao ficheiro anterior
	Media (Pasta)	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library /Media	-Contém uma pasta por cada contacto que se estabeleceu uma conversa. -Existem subpastas com anexos trocados, nomeadamente imagens
	net.whatsapp.WhatsApp.plist	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/ Library/Preferences/	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados
	UITextInput ContextIdentifiers.plist	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Preferences/	-Ficheiro de extensão “.plist” -Contém os números de telemóvel associados às contas de utilizador com quem o utilizador trocou mensagens no chat.
	Biz.sqlite	/private/var/mobile/Containers/Shared/AppGroup/group.net.whatsapp.WhatsApp.shared/Biz/	-Ficheiro do tipo ”Sqlite Database”. -Sem dados possíveis de serem interpretados

	ChatSearch.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém, para cada contacto do chat o registo de texto trocado nas conversas
	ChatStorage.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém os contactos com quem se trocou mensagens no chat -Contém o índice de anexos trocados nas mensagens -Contém texto trocado entre as conversas e os respetivos contactos
	Contacts.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Contém os contactos do telemóvel na aplicação whatsapp
	Jobs.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo ”Sqlite Database”. -Sem dados possíveis de serem interpretados
	group.net. whatsapp. WhatsApp.shared.plist	/private/var/mobile/ Containers/Shared/AppGroup/ group.net.whatsapp.WhatsApp.shared/ Library/Preferences/	-Ficheiro de extensão “.plist” -Contém o numero de telemóvel associado à conta de utilizador do whatsapp -Contém endereços IP
	Pasta (Profile)	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/ Media/Profile/	-Contém a foto de perfil e a miniatura do utilizador da conta da aplicação local.
	net.whatsapp.WhatsApp2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	Ficheiro de extensão “.plist”. -Sem dados possíveis de serem interpretados
	351910022871- 1483054648.thumb.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.net.whatsapp.	-Ficheiro de formato “.jpg” -Foto de perfil de um dos contactos

		WhatsApp.shared/Media/Profile/	
	351910520164-1478699870.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.net.whatsapp. WhatsApp.shared/Media/Profile/	-Ficheiro de formato “.jpg” -Foto de perfil de um dos contactos
	Photo.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.net.whatsapp. WhatsApp.shared/Media/Profile/	-Ficheiro de formato “.jpg” -Foto de perfil de um dos contactos
Imessage	Sms.db	/private/var/mobile/Library/SMS/	-Ficheiro do tipo ”Sqlite Database” -Contém as mensagens SMS do dispositivo com o texto trocado e os respetivos números que enviaram as mensagens

A Tabela 6 representa ficheiros encontrados que estão relacionados com funcionalidades do dispositivo.

Tabela 6 – Outros ficheiros encontrados relacionados com funcionalidades do dispositivo.

Ficheiro	Localização do Ficheiro	Descrição / Aplicação relacionada	Dados obtidos
CellularUsage.db	/private/var/wireless/Library/Databases/		-Ficheiro do tipo ”Sqlite Database”. -Contém número de telemóvel do cartão inserido no dispositivo
CallHistory.storedata	/private/var/mobile/Library/CallHistoryDB/	Histórico de Chamadas do dispositivo	-Ficheiro do tipo ”Sqlite Database” -Contém os números de telemóvel relacionados com chamadas do dispositivo.
Accounts3.sqlite	/private/var/mobile/Library/Accounts/	Contas de utilizador no dispositivo	-Ficheiro do tipo ”Sqlite Database”. -Contém para cada aplicação, os tipos de autenticação utilizados -Nome de utilizador de algumas aplicações
History.db	/private/var/mobile/Containers/ Data/Application/ com.apple.mobilesafari/Library/Safari/	Histórico da aplicação Safari	-Ficheiro do tipo ”Sqlite Database”. -A base de dados não contém dados.
downloads.28.sqlitedb	/private/var/mobile/Media/Downloads/	Histórico de download de aplicações	-Ficheiro do tipo ”Sqlite Database”. -Contém algumas

			aplicações que foram instaladas no dispositivo a partir da appstore.
Photos.sqlite	/private/var/mobile/Media/PhotoData/	Base de dados de fotografias	-Ficheiro do tipo ”Sqlite Database”. -Contém uma base de dados com uma lista de imagens do dispositivo, mas não as fotos tiradas
com.google.Gmail.plist	/private/var/mobile/Containers/Data/ Application/com.google.Gmail/Library/Preferences/	Gmail	-Ficheiro de extensão “.plist”. -Contém a conta de e email do utilizador
group.com.google.Gmail.plist	/private/var/mobile/Containers/ Shared/AppGroup/group.com.google.Gmail/ Library/Preferences/	Gmail	-Ficheiro de extensão “.plist” -Contém a conta de utilizador local de e-mail -Contém e-mails de outros utilizadores com quem se trocou e-mails
group.com.apple.notes.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.com.apple.notes/Library/ Preferences/	Notas	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados
com.apple.wifi.plist	/private/var/preferences/SystemConfiguration/	Redes Wi-Fi	-Ficheiro de extensão “.plist” -Contém as redes Wi-Fi a que o dispositivo esteve ligado.

preferences.plist	/private/var/preferences/SystemConfiguration/	Pequenas configurações do dispositivo	-Ficheiro de extensão ".plist" -Contém o nome do dispositivo -Contém configurações da rede relativos ao cartão SIM
com.apple.mobilemail.plist	/private/var/mobile/Library/SpringBoard/ ApplicationShortcuts/	E-mail native do iOS	-Ficheiro de extensão ".plist" -Contém informação sobre o número de e-mails por ler que aparece no ícone da aplicação
AddressBook.sqlitedb	/private/var/mobile/Library/AddressBook/	Contactos do dispositivo Baseado em (1)	-Ficheiro de extensão ".plist" -Contém os contactos do dispositivo -Contém dados relativos aos contactos
AddressBookImages.sqlitedb	/private/var/mobile/Library/AddressBook/	Contactos do dispositivo Baseado em (1)	-Ficheiro do tipo "Sqlite Database". -Contém imagens dos contactos do dispositivo
Calendar.sqlitedb	/private/var/mobile/Library/Calendar/	Dados sobre o calendário e eventos. Baseado em (1)	-Ficheiro do tipo "Sqlite Database". -Contém informação sobre algumas pessoas e respetivos endereços de "Facebook"

			-Contém dados de localização acerca dos eventos de calendário
call_history.db	/private/var/wireless/Library/CallHistory/	Dados de chamadas Baseado em (1)	-Ficheiro do tipo ”Sqlite Database”. -Contém informação sobre chamadas
Bookmarks.db	/private/var/mobile/Library/Safari/	Websites guardados no Safari Baseado em (1)	-Ficheiro do tipo ”Sqlite Database”. -Contém os sites favoritos que foram guardados.
consolidated.db	/private/var/root/Library/Caches/locationd/	Dados de GPS Baseado em (1)	-Ficheiro do tipo ”Sqlite Database”. -Contém registos de gps e configurações
Pasta “Media”	/private/var/mobile/Media/	Contém diversas pastas com fotografias de diversas aplicações	-Fotografias diversas
Pasta “100APPLE”	/private/var/mobile/Media/DCIM/100APPLE/	Contém fotografias da Camara	-Fotografias diversas da camara.

A Tabela 7 contém outros dados obtidos do iphone 4s a partir dos resumos de informação do software XAMN. Os ficheiros com as imagens encontram-se em anexo.

Tabela 7 - Tabela de aquisição de outros dados do Iphone 4s

Tipo de dados / Categoria	Descrição dos dados	Imagem
Contactos do dispositivo	Todos os contactos existentes no dispositivo, contendo número de telemóvel e nome	Contactos.png
Chamadas telefónicas	Todas as chamadas telefónicas efetuadas e recebias contendo o número de telemóvel, nome do contacto e a data/hora da chamada (Dispositivo, Line, Viber, WhatsApp)	Chamadas.png
Mensagens	Mensagens trocadas via (SMS facebook, Line, viber e WhatsApp)	Mensagens.png MensagensFacebook.png MensagensViber.png MensagensWhatApp.png MensagensLine.png
Eventos de Calendário	Eventos do calendário (Feriados, Tarefas etc)	Calendário.png
Localização	Dados de localização com respetivas coordenadas GPS em Graus e fotografia do mapa de pesquisas do google Maps	LocalizacaoPesquisaMap.png
Histórico WEB	Histórico web da aplicação Safari, contendo o website visitado e ou a pesquisa efetuada	Historicoweb.png
Fotografia	Fotografia tirada com localização por coordenadas GPS	FotografiaComCoordenadas.png
Dados de localização (Calendário)	Evento no calendário que guardou a localização	localizacaoCalendario.png
Fotografia com localização	Imagem tirada pela camara do dispositivo com dados de localização	IMG_0073.jpg
Miniaturas de Fotografias	Miniatura de fotografia tirada pela camara e nas aplicações de chat	Miniaturas.png

Contas de utilizador	Contas de utilizador de aplicações do dispositivo (Apple, Facebook, google, line , viber, WhatsApp)	ContasUtilizador.png

A Tabela 8 apresenta os resultados de aquisição de dados do Iphone6 plus.

Tabela 8 - Tabela de aquisição de dados do Iphone 6 plus

App	Ficheiro	Localização do ficheiro	Dados obtidos
Allo (Google) (Fireball)	com.google.fireball.plist	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém o número de telemóvel do dispositivo e que está associado à aplicação
	google_tagmanager.db	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	googleanalytics-aux-v4.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	googleanalytics-v2.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	googleanalytics-v3.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	GTM.sql	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Library/	-Ficheiro do tipo "Sqlite Database" -Sem dados possíveis de serem interpretados
	gtm_img_unrepeatable	/private/var/mobile/Containers/ Data/Application/com.google.fireball/ Documents/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados

	Na aplicação “allo” apenas encontramos o número de telemóvel relativo ao cartão sim instalado no dispositivo relacionado com a conta de utilizador.		
Cyphr	Cyphr.sqlite	/private/var/mobile/Containers/ Data/Application/com.goldenfrog. cyphr.mobile/Documents/	-Ficheiro do tipo “Sqlite Database” -Contém uma chave privada -Contém 3 chaves públicas -Registo de conversas entre contactos -Nomes dos contactos e contas de utilizador com quem se trocou texto e anexos
	43A2F749-8C31-49CC-A179-4A6EA6434AF7	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	46A3DF4A-142D-4B36-8A83-2B6667178E26	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	CA3BA5DE-4AD1-4F3C-8A89-1AE7FA599C10	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	CD202FB8-F6B1-4F63-9C95-DA5F1EE31981	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	CA5FA14A-9ADF-4576-85D6-97704A099861	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	D6541128-1B94-4279-B4E1-0D946273708E	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.
	F72D7135-7AD5-4DFA-984E-4A0C5F216B93	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Documents/cyphr/	-Ficheiro do tipo “JPEG Image data” -Anexo (Imagem) trocada durante a conversa.

	CLSUserDefaults.plist	/private/var/mobile/Containers/ Data/Application/com.goldenfrog. cyphr.mobile/Library/Application Support/com.crashlytics/	-Ficheiro de formato ".plist" -Contém a data relativa à ultima atualização da aplicação. -Contém informação relativa ao tipo de dispositivo
	com.goldenfrog.cyphr.mobile.plist	/private/var/mobile/Containers /Data/Application/com.goldenfrog.cyphr. mobile/Library/Preferences/	-Ficheiro de formato ".plist -Sem dados possíveis de serem interpretados.
	Na aplicação "Cyphr" encontramos uma chave privada e várias chaves públicas, dados relativos aos contactos com quem se estabeleceu troca de texto e imagens e anexos		
imo	group.im.imo.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/Preferences/	-Ficheiro de formato ".plist" -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação imo.
	imoimiphone.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/Preferences/	-Ficheiro de formato ".plist" -Contém o número de telemóvel de um dos contactos com quem se trocou texto e imagens.
	Caches[x9]est.enc	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library	-Ficheiro do tipo "ASCII Text" -Sem dados.
	Cookies.binarycookies	/private/var/mobile/Containers/Shared/ AppGroup/group.im.imo/Library/cookies	-Sem dados possíveis de serem interpretados
	iat.dat	/private/var/mobile/Containers/ Data/Application/imoimiphone/Documents/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados
	imo_state.dat	/private/var/mobile/Containers/ Data/Application/imoimiphone/Documents/	-Ficheiro de formato ".plist" -Contém o número de telemóvel da conta da aplicação -Contém o número de telemóvel de um contacto com quem se trocou

			texto e imagens.
	PendingIMAndPhoto Model1.sqlite	/private/var/mobile/Containers/ Data/Application/imoimiphone/Documents/	-Ficheiro do tipo “Sqlite database” -Sem dados possíveis de serem interpretados.
	rmq2.sqlite	/private/var/mobile/Containers/ Data/Application/imoimiphone/Documents/	-Ficheiro do tipo “Sqlite database” -Sem dados possíveis de serem interpretados.
	Na aplicação “imo” encontramos dados relativos à conta de utilizador e número de telemóvel.		
line	jp.naver.line.plist	/private/var/mobile/Containers/Data/ Application/jp.naver.line/Library/Preferences/	-Ficheiro de formato “.plist” -Número de telemóvel relativo ao cartão instalado no dispositivo. -Nome da conta de utilizador da aplicação imo
	Line.sqlite	/private/var/mobile/Containers/Shared/ AppGroup/group.com.linecorp.line/ Library/Application Support/PrivateStore/ P_ue89ec9fb8043e6b065 a5cf615e3e20c0/Messages/	-Ficheiro de formato “.sqlite database” -Lista de contactos da aplicação com nome e número de telemóvel. -Mensagens trocadas entre os contactos e respetivos números de telemóvel -Encontrados vários utilizadores que utilizaram a aplicação. -Registo de chamadas efetuadas
	group.com.linecorp.line.plist	/private/var/mobile/Containers/Shared /AppGroup/ group.com.linecorp.line/Library/Preferences/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados
	3	/private/var/mobile/Containers/ Data/Application/jp.naver.line/ Library/Application Support/ PublicStore/Analytics/	-Ficheiro do tipo “ASCII TEXT” -Sem dados possíveis de serem interpretados

	4	/private/var/mobile/Containers/ Data/Application/jp.naver.line/ Library/Application Support/ PublicStore/Analytics/	-Ficheiro do tipo “ASCII TEXT” -Sem dados possíveis de serem interpretados
	Pasta “Message Attachments”	/private/var/mobile/Containers/Data/ Application/ jp.naver.line/Library/Application Support/PrivateStore/P_ue89ec9fb8043e6b 065a5cf615e3e20c0/Message Attachments/	-Contém os anexos trocados nas conversas entre os contactos.
	5306312780800.jpg	/private/var/mobile/Containers/Data/ Application/ jp.naver.line/Library/Application Support/PrivateStore/ P_ue89ec9fb8043e6b065a5 cf615e3e20c0/Message Attachments/u8b9ad4ec8bc4 325393881a1d47a96ec8/	-Ficheiro do tipo “JPG” -Imagem trocada durante uma conversa entre contactos.
	5306312945031.jpg	/private/var/mobile/Containers/Data/ Application/ jp.naver.line/Library/Application Support/PrivateStore/ P_ue89ec9fb8043e6b065a5 cf615e3e20c0/Message Attachments/u8b9ad4ec8bc4 325393881a1d47a96ec8/	-Ficheiro do tipo “JPG” -Imagem trocada durante uma conversa entre contactos.

	5306313155594.jpg	/private/var/mobile/Containers/Data/ Application/ jp.naver.line/Library/Application Support/PrivateStore/ P_ue89ec9fb8043e6b065a5 cf615e3e20c0/Message Attachments/u8b9ad4ec8bc4 325393881a1d47a96ec8/	-Ficheiro do tipo “JPG” -Imagem trocada durante uma conversa entre contactos.
	Cookies.binarycookies	\private\var\mobile\Library\Cookies	-Sem dados possíveis de serem interpretados
	History.db	/private/var/mobile/Containers/Data/ Application/jp.naver.line/Library/NCVoIP/ ue89ec9fb8043e6b065a5cf615e3e20c0/	-Ficheiro do tipo “data” -Sem dados possíveis de serem interpretados
	E2EEData.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.com.linecorp.line/ Library/Application Support/PrivateStore/P_ue89ec9fb8043e 6b065a5cf615e3e20c0/Messages/	-Ficheiro do tipo “Sqlite database” -Sem dados possíveis de serem interpretados.
	Na aplicação “line” encontramos o número de telemóvel associado à conta de utilizador, o nome de utilizador, a lista de contactos, as mensagens trocadas e registos de chamadas. Foram encontrados registos que indicam os utilizadores que utilizaram a aplicação.		
Messenger	com.facebook.Messenger.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato “.plist” - Com certificados SSL **-Contém chave privada…**
	group.com.facebook. Messenger.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados.

	com.facebook.Messenger_2.plist	/private/var/mobile/Library/SpringBoard /ApplicationShortcuts/	-Ficheiro de formato ".plist" -Com informação de contactos da aplicação Messenger e respetivos nomes.
	Cookies.binarycookies	/private/var/mobile/Containers/Shared /AppGroup/group.com.facebook.Messenger/ Library/cookies	-Ficheiro do tipo "Data" -Sem dados possíveis de serem interpretados.
	UITextInputContextIdentifiers. plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library/Preferences/	-Ficheiro de formato ".plist" -Sem dados possíveis de serem interpretados
	https_m.facebook.com_0 .localstorage	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library \WebKit\WebsiteData\LocalStorage	-Ficheiro de formato ".sqlite database" -Sem dados
	StorageTracker.db	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Library \WebKit\WebsiteData\LocalStorage	-Ficheiro de formato ".sqlite database" -Sem dados possíveis de serem interpretados
	.compactdisk_extended_attributes	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Documents/ _sessionlessStore/messenger_secure_ messages.v1	-Ficheiro do tipo "ascii text" -Sem dados possíveis de serem interpretados
	callog.dat.plist	/private/var/mobile/Containers/Data /Application/com.facebook.Messenger/ Documents/_store_92D5F217-CDEC-49C1-B386-A53FD92779EF/rtc_call_log.v1/	-Ficheiro de formato ".plist" -Contém possíveis dados de chamadas, mas sem números de telemóvel.
	.compactdisk_extended_attributes	/private/var/mobile/Containers/Data /Application/com.facebook.Messenger/ Documents/_store_92D5F217-CDEC-49C1-B386-	.compactdisk_extended_attributes Sem dados possíveis de serem interpretados.

		A53FD92779EF/rtc_call_log.v1/	
	rtc_storage	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Documents/ /facebook/messenger	-Ficheiro de formato “data” -Sem dados possíveis de serem interpretados.
	app_state_logs.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Documents/_sessionlessStore /application_status_pkvs.v1/	-Ficheiro do tipo “.plist” -Sem dados possíveis de serem interpretados.
	manifest_v1.sqlite	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger/ Documents/_sessionlessStore/ application_status_pkvs.v1/	-Ficheiro do tipo”sqlite database” -Com possível data de acesso à aplicação.
	Snapshot.plist	/private/var/mobile/Containers/Data/ Application/com.facebook.Messenger /Documents/_sessionlessStore/ application_status_pkvs.v1/	-Ficheiro do tipo “.plist” -Sem dados possíveis de serem interpretados.
	100014442430752.session.plist	/private/var/mobile/Containers/Data /Application/com.facebook.Messenger/ Documents/_sessionlessStore/preferences.v1/	-Ficheiro do tipo “.plist” -Contém o número de telemóvel do dispositivo associado à aplicação.
	proxy_video_watching_time _tracker.plist	/private/var/mobile/Containers/ Data/Application/com.facebook. Messenger/Documents/	- Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados.
	proxy_video_data_usage.stats.plist	/private/var/mobile/Containers/ Data/Application/com.facebook. Messenger/Documents/	- Ficheiro de formato “.plist” -Sem dados possíveis de serem interpretados.
	configuration.conf	/private/var/mobile/Containers/ Data/Application/com.facebook.Messenger /Documents/analytics/loom/config/	-Ficheiro de formato “.conf” -Sem dados possíveis de serem interpretados.
	Na aplicação “messenger” encontramos os contactos da aplicação com que foram efetuadas trocas de texto e anexos. Foram encontradas chaves públicas e privadas		

Signal	org.whispersystems.signal.plist	/private/var/mobile/Containers/ Data/Application/ org.whispersystems.signal/Library/Preferences/	-Ficheiro de formato ".plist" -Com informação relativa à versão da aplicação instalada.
	Na aplicação "signal" apenas encontramos um ficheiro com informação relativa à versão da aplicação.		
Skype	Skype.blog	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro de extensão ".blog" -Sem dados possíveis de serem interpretados.
	Skype-1.blog	/private/var/mobile/Containers/Data/Application/ com.skype.skype/Documents/	-Ficheiro de extensão ".blog" -Contém endereços IP e portos.
	Skype-2.blog	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Documents/	-Ficheiro de extensão ".blog" -Contém endereços IP e portos.
	Cookies.binarycookies	/private/var/mobile/Containers/Data/ Application/com.skype.skype/Library/Cookies/	-Ficheiro de extensão ".binarycookies" Persistent cookies. -Contém a versão de Skype instalada
	com.skype.skype.plist	/private/var/mobile/Containers/Data/ Application/ com.skype.skype/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação da conta de utilizador do utilizador da aplicação.
	authentication.archive.plist	/private/var/mobile/Containers/Shared /AppGroup/group.com.skype.skype/interapp/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	com.skype.skype.pushstore.plist	/private/var/mobile/Library/SpringBoard/ PushStore/	-Ficheiro de extensão ".plist" - Sem dados possíveis de serem interpretados.
	Na aplicação "Skype" encontramos apenas informação sobre endereços IP, Portos.		
Telegram	ph.telegra.Telegraph.plist	/private/var/mobile/Containers/ Data/Application/ph.telegra.Telegraph/ Library/Preferences/	-Ficheiro de formato ".plist" -Contém configurações da aplicação.

	ph.telegra.Telegraph_2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	- Ficheiro de formato ".plist" -Contém Informação sobre os contactos com quem se trocou texto e anexos
	Pasta "Caches"	/private/var/mobile/Containers/ Shared/AppGroup/ group.ph.telegra.Telegraph/ Caches/	-Pasta com anexos trocados durante as conversas entre os contactos.
	f3a52f50d954b a3ff9e6d636a71ac67e	/private/var/mobile/Containers/ Shared/AppGroup/ group.ph.telegra.Telegraph/ Caches/	-Ficheiro do tipo "JPG" -Anexo trocado durante as conversas entre os contactos.
	Na aplicação "Telegram" encontramos informação sobre os contactos com quem se trocou texto e anexos, e uma pasta contendo anexos.		
Viber	com.viber.plist	/private/var/mobile/Containers/Data/Application/ com.viber/Library/Preferences/	-Ficheiro de extensão ".plist" -Com informação relativa ao número de telemóvel associado à conta de utilizador.
	Cookies.binarycookies	/private/var/mobile/Containers/ Data/Application/com.viber/Library/ Cookies/	-Ficheiro do tipo "Data" -Sem dados possíveis de serem interpretados.
	com.viber.pushstore	/private/var/mobile/Library/ SpringBoard/PushStore/	-Ficheiro de extensão ".plist" -Sem dados possíveis de serem interpretados.
	SecureStorage.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo "Sqlite Database". -Contém a chave pública.

	Shared.data	/private/var/mobile/Containers/Shared/ AppGroup/group.viber.share.container/	-Ficheiro do tipo ”Sqlite Database”. -Com informação relativa aos contactos com que se trocou informações -Contém números de telemóveis relativos às contas dos contactos.
	group.viber.share. container.plist CLSUserDefaults.plist	/private/var/mobile/Containers/ Shared/AppGroup/ group.viber.share.container/ Library/Preferences/	-FIcheiro do tipo “.plist” -Contém o número de telemóvel associado à conta de aplicação e o nome da conta de utilizador.
	SecondaryStorage.data	/private/var/mobile/Containers/ Data/Application/com.viber/Documents/	- Ficheiro “Sqlite Database” -Sem dados possíveis de serem interpretados.
	Contacts.data	/private/var/mobile/Containers/ Data/Application/com.viber/ Documents	-Ficheiro “Sqlite Database” -Contém mensagens trocadas -Contém os contactos da aplicação -Contém números de telemóvel. -Contém registo de anexos trocados -Contém registos de chamadas feitas e recebidas
	Settings.data	/private/var/mobile/Containers/ Data/Application/com.viber/Documents	- Ficheiro “Sqlite Database” -Contém o número de telemóvel associado à aplicação -Contém o nome de utilizador associado à aplicação. -Contém configurações da aplicação
	Pasta “BigAttachmentsPreview”	/private/var/mobile/Containers/ Data/Application/com.viber/Documents/	-Contém anexos trocados durante as conversas

		BigAttachmentsPreview/	
	Pasta “ContactIcons”	/private/var/mobile/Containers/ Data/Application/com.viber/Documents/ ContactIcons/	-Contém as fotos de perfil de vários utilizadores com quem se estabeleceu contacto -Fotos de perfil de uma conta de utilizador anteriormente configurada que foi mais tarde apagada.
	Pasta “Icons”	/private/var/mobile/Containers/ Data/Application/com.viber/ Documents/icons	-Contém possíveis anexos trocados durante conversas.
	Pasta “ViberIcons”	/private/var/mobile/Containers/ Data/Application/com.viber/ Documents/ ViberIcons	-Contém as miniaturas das fotos de perfil da conta de utilizador.
	46bbaf977d9efd9ba9f4ca d3d7857a328bb5ab93e 26e966398f8f83135ada8b7	/private/var/mobile/Containers/ Data/Application/com.viber/ Documents/ViberIcons/	-Possivel foto de perfil de uma conta de utilizador da aplicação
	Na aplicação “Viber” encontramos o número de telemóvel associado à conta de utilizador, foto de perfil e anexos trocados, uma chave pública, registos de chamadas e texto trocados entre os contactos.		
WhatsApp	blockedcontacts.dat.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados. -Pode conter possíveis contactos bloqueados
	calls.backup.log.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão “.plist” -Contém registos de Chamadas com duração entre outros dados e os respetivos nomes de utilizador e números de telemóvel. -Contém registo dos contactos com

			quem se efetuou chamadas
	calls.log.plist	/private/var/mobile/Containers/Data/Application/ net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém registos de Chamadas e os respetivos nomes de utilizador e números de telemóvel. -Contém registo dos contactos com quem se efetuou chamadas
	StatusMessages.plist.xml	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp /Documents/	-Ficheiro de extensão ".plist" -Contém algumas mensagens de texto predefinidas.
	SyncHistory.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Documents/	-Ficheiro de extensão ".plist" -Contém uma data sobre a ultima sincronização.
	fieldstats.active	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/Library/ FieldStats/	-Contém endereços IP -Contém a versão do dispositivo (iphone6)
	whatsapp-2017-01-07-13-45-54-208-WhatsApp-5.log	/private/var/mobile/Containers/ Data/Application/net.whatsapp. WhatsApp/Library/Logs/	-Ficheiro "UTF8 unicode text" -Contém diversos registos. -Contém números de telemóvel associados às contas de utilizador dos contactos e do utilizador local. -Contém uma serie de registos relacionados com ficheiros.
	whatsapp-2017-01-07-15-16-28-978-WhatsApp-6.log	/private/var/mobile/Containers/ Data/Application/net.whatsapp. WhatsApp/Library/Logs/	-Ficheiro "UTF8 unicode text" -Contem configurações, informações da aplicação mas sem dados relevantes
	whatsapp-2017-01-18-11-51-33-283-WhatsApp-7.log	/private/var/mobile/Containers/ Data/Application/net.whatsapp. WhatsApp/Library/Logs/	-Ficheiro "UTF8 unicode text" -Contém informações relevantes ao número de telemóvel registado na

			aplicação. -Contém números de telemóvel dos contactos com quem se estabeleceu contacto.
	whatsapp-2017-01-22-21-43-34-694-WhatsApp-8.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro “UTF8 unicode text” -Contém números de telemóvel dos contactos com quem se estabeleceu contacto. -Contém registos de chamadas -Contém endereços IP
	whatsapp-2017-01-22-22-08-01-316-WhatsApp-9.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro “UTF8 unicode text” -Contém registos do número de telemóvel associado à conta de utilizador. -Contém informações da operadora de telecomunicações.
	whatsapp-2017-02-06-22-33-22-550-WhatsApp-10.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro “UTF8 unicode text” -Contém números de telemóvel dos contactos com quem se estabeleceu contacto. -Contém informações da operadora de telecomunicações.
	whatsapp-2017-02-06-23-35-20-149-WhatsApp-11.log	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library/Logs/	-Ficheiro “UTF8 unicode text” -Contém números de telemóvel dos contactos com quem se estabeleceu contacto. -Contém informações da operadora de telecomunicações.
	Media (Pasta)	/private/var/mobile/Containers/Data/Application/net.whatsapp.WhatsApp/Library	-Contém uma pasta por cada contacto que se estabeleceu uma

		/Media	conversa. -Existem subpastas com anexos trocados, nomeadamente imagens
	net.whatsapp.WhatsApp.plist	/private/var/mobile/Containers/ Data/Application/net.whatsapp.WhatsApp/ Library/Preferences/	-Ficheiro de extensão ".plist" -Contém endereços IP.
	UITextInput ContextIdentifiers.plist	/private/var/mobile/Containers/Data/ Application/net.whatsapp.WhatsApp/ Library/Preferences/	-Ficheiro de extensão ".plist" -Contém os números de telemóvel associados às contas de utilizador com quem o utilizador trocou mensagens no chat.
	Biz.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/Biz/	-Ficheiro do tipo "Sqlite Database". -Sem dados possíveis de serem interpretados.
	ChatSearch.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo "Sqlite Database". -Contém, para cada contacto do chat o registo de texto trocado nas conversas
	ChatStorage.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo "Sqlite Database". -Contém os contactos com quem se trocou mensagens no chat -Contém o índice de anexos trocados nas mensagens -Contém texto trocado entre as conversas e os respetivos contactos
	Contacts.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net.whatsapp. WhatsApp.shared/	-Ficheiro do tipo "Sqlite Database". -Contém os contactos do telemóvel na aplicação whatsapp
	Jobs.sqlite	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/	-Ficheiro do tipo "Sqlite Database". -Sem dados possíveis de serem interpretados.

	group.net. whatsapp. WhatsApp.shared.plist	/private/var/mobile/ Containers/Shared/AppGroup/ group.net.whatsapp.WhatsApp.shared/ Library/Preferences/	-Ficheiro de extensão ".plist" -Contém o numero de telemóvel associado à conta de utilizador do whatsapp -Contém endereços IP
	Pasta (Profile)	/private/var/mobile/Containers/ Shared/AppGroup/group.net. whatsapp.WhatsApp.shared/ Media/Profile/	-Contém a foto de perfil e a miniatura do utilizador da conta da aplicação local.
	net.whatsapp.WhatsApp2.plist	/private/var/mobile/Library/ SpringBoard/ApplicationShortcuts/	Ficheiro de extensão ".plist". -Sem dados possíveis de serem interpretados.
	351963155223-1477927875.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.net.whatsapp. WhatsApp.shared/Media/Profile/	-Ficheiro de formato ".jpg" -Foto de perfil de um dos contactos
	Photo.jpg	/private/var/mobile/Containers/Shared/ AppGroup/group.net.whatsapp. WhatsApp.shared/Media/Profile/	-Ficheiro de formato ".jpg" -Foto de perfil de um dos contactos
iMessage	Sms.db	/private/var/mobile/Library/SMS/	-Ficheiro do tipo "Sqlite Database" -Contém as mensagens SMS do dispositivo com o texto trocado e os respetivos números que enviaram as mensagens

A Tabela 9 representa ficheiros encontrados que estão relacionados com funcionalidades do dispositivo.

Tabela 9 - Outros ficheiros encontrados relacionados com funcionalidades do dispositivo.

Ficheiro	Localização do Ficheiro	Descrição / Aplicação relacionada	Dados obtidos
CellularUsage.db	/private/var/wireless/Library/Databases/		-Ficheiro do tipo ”Sqlite Database”. -Contém número de telemóvel do cartão inserido no dispositivo
CallHistory.storedata	/private/var/mobile/Library/CallHistoryDB/	Histórico de Chamadas do dispositivo	-Ficheiro do tipo ”Sqlite Database” -Contém os números de telemóvel relacionados com chamadas do dispositivo.
Accounts3.sqlite	/private/var/mobile/Library/Accounts/	Contas de utilizador no dispositivo	-Ficheiro do tipo ”Sqlite Database”. -Contém para cada aplicação, os tipos de autenticação utilizados -Nome de utilizador de algumas aplicações
History.db	/private/var/mobile/Containers/ Data/Application/ com.apple.mobilesafari/Library/Safari/	Histórico da aplicação Safari	-Ficheiro do tipo ”Sqlite Database”. -Contém registos de pesquisas e sites visitados no safari
downloads.28.sqlitedb	/private/var/mobile/Media/Downloads/	Histórico de download de aplicações	-Ficheiro do tipo ”Sqlite Database”. -Contém alguns possíveis dados que foram obtidos

			através de download.
Photos.sqlite	/private/var/mobile/Media/PhotoData/	Base de dados de fotografias	-Ficheiro do tipo ”Sqlite Database”. -Contém uma base de dados com uma lista de imagens do dispositivo.
com.google.Gmail.plist	/private/var/mobile/Containers/Data/ Application/com.google.Gmail/Library/ Preferences/	Gmail	-Ficheiro de extensão “.plist”. -Contém a conta de e email do utilizador
group.com.google.Gmail.plist	/private/var/mobile/Containers/ Shared/AppGroup/group.com.google.Gmail / Library/Preferences/	Gmail	-Ficheiro de extensão “.plist” -Contém a conta de utilizador local de e-mail -Contém e-mails de outros utilizadores com quem se trocou e-mails
group.com.apple.notes.plist	/private/var/mobile/Containers/Shared/ AppGroup/group.com.apple.notes/Library/ Preferences/	Notas	-Ficheiro de extensão “.plist” -Sem dados possíveis de serem interpretados.
com.apple.wifi.plist	/private/var/preferences/SystemConfiguration/	Redes Wi-Fi	-Ficheiro de extensão “.plist” -Contém as redes Wi-Fi a que o dispositivo esteve ligado.
preferences.plist	/private/var/preferences/SystemConfiguration/	Pequenas configurações do dispositivo	-Ficheiro de extensão “.plist” -Contém algumas configurações de rede do dispositivo.

com.apple.mobilemail.plist	/private/var/mobile/Library/SpringBoard/ ApplicationShortcuts/	E-mail native do iOS	-Ficheiro de extensão ".plist" -Contém informação sobre o número de e-mails por ler que aparece no ícone da aplicação
AddressBook.sqlitedb	/private/var/mobile/Library/AddressBook/	Contactos do dispositivo Baseado em (1)	-Ficheiro de extensão ".plist" -Contém os contactos do dispositivo -Contém dados relativos aos contactos
AddressBookImages.sqlitedb	/private/var/mobile/Library/AddressBook/	Contactos do dispositivo Baseado em (1)	-Ficheiro do tipo "Sqlite Database". -Contém os contactos do dispositivo. -Contém imagens dos contactos do dispositivo
Calendar.sqlitedb	/private/var/mobile/Library/Calendar/	Dados sobre o calendário e eventos. Baseado em (1)	-Ficheiro do tipo "Sqlite Database". -Contém informação sobre algumas pessoas e respetivos endereços de "Facebook" -Contém dados de localização acerca dos eventos de calendário
Bookmarks.db	/private/var/mobile/Library/Safari/	Websites guardados no Safari Baseado em (1)	-Ficheiro do tipo "Sqlite Database". -Contém os sites favoritos que foram guardados.

consolidated.db	/private/var/root/Library/Caches/locationd/	Dados de GPS Baseado em (1)	-Ficheiro do tipo ”Sqlite Database”. -Contém registos de gps e configurações
Pasta “Media”	/private/var/mobile/Media/	Contém diversas pastas com fotografias de diversas aplicações	-Fotografias diversas
Pasta “100APPLE”	/private/var/mobile/Media/DCIM/100APPLE/	Contém fotografias da Camara	-Fotografias diversas da camara.

A Tabela 10 contém outros dados obtidos do iphone 6 a partir dos resumos de informação do software XAMN. Os ficheiros com as imagens encontram-se em anexo.

Tabela 10 - Tabela de aquisição de outros dados do Iphone 6 plus.

Tipo de dados / Categoria	Descrição dos dados	Imagem
Contactos do dispositivo	Todos os contactos existentes no dispositivo, contendo número de telemóvel, nome e fotografia de perfil Contactos de aplicações (Line, Viber, WhatsApp) A aplicação Line etc já tiveram outros utilizadores e contas	Contactos e Calendario/ Contactos.png ContactosLine.png ContactosViber.png ContactosWhatsApp.png
Chamadas telefónicas	Todas as chamadas telefónicas efetuadas e recebias contendo o número de telemóvel, nome do contacto e a data/hora da chamada (Dispositivo, Line, Viber, WhatsApp)	Chamadas.png
Mensagens	Mensagens trocadas via (SMS facebook, Line, viber e WhatsApp)	Mensagens.png MensagensFacebook.png MensagensViber.png MensagensWhatApp.png MensagensLine.png
Eventos de Calendário	Eventos do calendário (Feriados, Tarefas etc)	Calendário.png
Localização	Dados de localização com respetivas coordenadas GPS em Graus e fotografia do mapa de pesquisas do google Maps	LocalizacaoPesquisaMap.png
Histórico WEB	Histórico web da aplicação Safari, contendo o website visitado e ou a pesquisa efetuada	Historicoweb.png
Fotografia	Fotografia tirada com localização por coordenadas GPS	FotografiaComCoordenadas.jpg
Dados de localização (Calendário)	Evento no calendário que guardou a localização	localizacaoCalendario.png
Contas de utilizador	Contas de utilizador de aplicações do dispositivo (Apple, Facebook, line , viber, WhatsApp)	ContasUtilizador.png

Redes Wifi	Dados de redes Wi-Fi a que o dispositivo esteve ligado	RedesWifi.png

Projeto

Mestrado de Engenharia Informática – Computação Móvel

Digital Forensics procedures for Apple Devices

Anexo D – Características dos iPhone

Fábio António Lavrador Amado Marques

O anexo D “Características dos iPhone” apresenta algumas características dos iPhone, desde a primeira versão até à ultima que foi lançada, nomeadamente o iPhone 7. A Tabela 1 apresenta essa informação.

Tabela 1 – Descrição das características dos vários modelos de iPhone.

iPhone	Número do modelo	Sistema operativo original	Último Sistema operativo	Processador	Memória RAM	Rede Wi-Fi Bluetooth	GPS	Diferenças do ponto de vista forense
iPhone 2G	A1203	iOS 1.0	iOS 3.1.3	S5l8900 ARM 620MHz	128MB	GSM/GPRS/EDGE 802.11b/g 2.0 + EDR	NÂO	
iPhone 3G	A1241	iOS 2.0	iOS 4.2.1	S5l8900 ARM 620MHz	128MB	3G UMTS / HSDPA 802.11b/g 2.0 + EDR	SIM	
iPhone 3GS	A1303	iOS 3.0	iOS 6.1.6	S5L8920 ARM 600 MHz	256MB	GSM HSDPA 802.11b/g 2.0 + EDR	SIM	Fotografias guardam localização GPS
iPhone 4	A1332 (GSM) ou A1349 (CDMA)	iOS 4.0	iOS 7.1.2	A4 S5L8930 800 MHz	512MB	HSDPA+ HSUPA (3G) 802.11b/g/n 2.1 + EDR	SIM	
iPhone 4S	A1431 e A1387	iOS 5.0	iOS 9.3.5	A5S5L8940 800 MHz	512MB	HSPA+ HSUPA (3G) 802.11b/g/n 4.0	SIM	
iPhone 5	A1428 GSM, A1429 GSM/CDMA	iOS 6.0	iOS 10.3.3	A6 S5L8950 1.3 GHz	1GB	LTE (4G) 802.11b/g/n 4.0	SIM	
iPhone 5C	A1507	iOS 7.0	iOS 10.3.3	A6 S5L8950 1.3 GHz	1GB	LTE (4G) 802.11b/g/n 4.0	SIM	

iPhone 5S	A1457	iOS 7.0	iOS 10.3.3	Apple A7 S5L8960 1.3 GHz	1GB	LTE (4G) 802.11b/g/n 4.0	SIM	
iPhone 6	A1586	iOS 8.0	iOS 10.3.3	Apple A8 APL1011 1.38 GHz	1GB	LTE (4G) 802.11b/g/n/ac 4.0	SIM	
iPhone 6 Plus	A1524	iOS 8.0	iOS 10.3.3	Apple A8 APL1011 1,38GHz	1GB	LTE (4G) 802.11b/g/n/ac 4.0	SIM	
iPhone 6 S	A1688	iOS 9.0	iOS 10.3.3	Apple A9 APL1022 1.85GHz	2GB	LTE (4G) 802.11b/g/n/ac + MIMO 4.2	SIM	
iPhone 6s Plus	A1687	iOS 9.0	iOS 10.3.3	Apple A9 APL0898 1.85GHz	2GB	LTE (4G) 802.11b/g/n/ac + MIMO 4.2	SIM	
iPhone SE	A1662	iOS 9.3	iOS 10.3.3	Apple A9 APL0898 1.85GHz	2GB	LTE (4G) 802.11b/g/n/ac 4.2	SIM	
iPhone7	A1778	iOS 10.0	iOS 10.3.3	Apple A10 APL1W24´ 2.34GHZ	2GB	LTE (4G) 802.11b/g/n/ac + MIMO 4.2	SIM	
iPhone 7 Plus	A1784	iOS 10.0	iOS 10.3.3	Apple A10 APL1W24´ 2.24GHz	3GB	LTE (4G) 802.11b/g/n/ac + MIMO 4.2	SIM	

Projeto

Mestrado de Engenharia Informática – Computação Móvel

Digital Forensics procedures for Apple Devices

Anexo E – Software Forense

Fábio António Lavrador Amado Marques

O anexo E, “Software Forense” apresenta um conjunto de softwares forenses. A Tabela 1 apresenta essa informação. A respetiva legenda de cores e abreviaturas é apresentada na Tabela 2. As notas adicionais encontram-se no final do documento.

Tabela 1 – Descrição das características de um conjunto de software Forense.

Nome do Software ou ferramenta	Empresa Website da empresa	Tipo de Licença	Preço	Forense?	Aquisição Lógica	Aquisição Física	Análise	iPhone	Android	Dados Cartão SIM	Info. Dispositivo	Contactos	SMS e MMS	Registo chamadas	Contas utilizador	Anexos Trocados	Fotografia e vídeo	Sistema Ficheiros	Dados GPS	Dados Wi-fi	Bases de dados	Histórico WEB	Calendário	E-mails	App instaladas	Notas adicionais
XRY (MSAB Office)	MSAB Link	P	6772.76€	S	S	S	N	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	1)
Cellebrite UFED touch ultimate	Cellebrite Link	P	14630.39€	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	2)
Oxygen Forensics extractor	Oxygen Link	P	10154.90€	S	S	S	N	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
Paraben E3 Universal	Paraben Link	P	3385.89€	S	S	S	S	S	S	S	S	S	S	S			S	S	S	S	S	S	S	S	3)

Nome do Software ou ferramenta	Empresa Website da empresa	Tipo de Licença	Preço	Forense?	Aquisição Lógica	Aquisição Física	Análise	iPhone	Android	Dados Cartão SIM	Info. Dispositivo	Contactos	SMS e MMS	Registo chamadas	Contas utilizador	Anexos Trocados	Fotografia e vídeo	Sistema Ficheiros	Dados GPS	Dados Wi-fi	Bases de dados	Histórico WEB	Calendário	E-mails	App instaladas	Notas adicionais
AccessData Mobile Phone Examiner Plus	AccessData LINK	P	2495€	S	S	S	S	S	S	S	S	S	S	S	S		S	S		S	S	S	S	S	S	4)
Elcomsoft Mobile forensics bundle	Elcosoft 2995€ Link	P	2995€	S	S	S	S	S	N		S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	5)
Backlight	BlackBag Tecnnologies Link	P	2895.41€	S	S	N	S	S	S			S	S		S		S	S	S			S		S	S	
Lantern	Katana Forensics Link	P	716.16€	S	S	S	S	S	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	6)
MOBILedit forensic express	Compelson Labs Link	P	1276.27€	S	S	S	N	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	

Nome do Software ou ferramenta	Empresa Website da empresa	Tipo de Licença	Preço	Forense?	Aquisição Lógica	Aquisição Física	Análise	iPhone	Android	Dados Cartão SIM	Info. Dispositivo	Contactos	SMS e MMS	Registo chamadas	Contas utilizador	Anexos Trocados	Fotografia e vídeo	Sistema Ficheiros	Dados GPS	Dados Wi-fi	Bases de dados	Histórico WEB	Calendário	E-mails	App instaladas	Notas adicionais
Magnet IEF Internet Evidence Finder	Magnet Forensics Link	P	1275.42€	S	N	N	S	S	S								S					S		S	S	
Autopsy	SleuthKit Link	O		S	N	N	S		S		N		S	S				S				S		S		7)
XAMN Viwer	MSAB Link	F		S	N	N	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	8)
FTK Imager	AccessData Link	O		S	N	N	S	N	N	N	N	N	N	N	N	N	N	S	N	N	N	S	N	N	N	9)

Tabela 2 – Legenda de abreviaturas e coes

Abreviatura / Cor	Singnificado
P	Licença Paga
O	Licença Opensource
F	Licença Freeware
S	Funcionalidade suportada
N	Funcionalidade não suportada
	Sem certeza ou sem informação

A Tabela 1 apresenta uma parte do software forense existente do mercado. Começa por descrever o tipo de licença, que pode ser paga (P), *opensource* (O), ou free (F). Apresenta uma estimativa de preço para as aplicações que pode variar no marcado que é vendido. Para cada aplicação é distinguida se é ou não forense, o tipo de aquisição que suporta e ainda se suporta análise de ficheiros. Como existem aplicações mais focas em Android e outras em IOS decidimos fazer essa distinção. As partes seguintes caracterizam os tipos de dados que podem ser obtidos, que as aplicações suportam. Por último apresentam-se algumas notas adicionais para algumas aplicações.

Notas adicionais:

1) O conjunto MSAB office, além do software, contém também mala com um conjunto de cabos, acessórios para diversos tipos de dispositivos móveis, um dispositivo para clonar cartões e um bloqueador de escrita.

2) A solução da Cellebrite inclui um dispositivo portátil que substitui o computador. Este dispositivo contém um ecrã de toque que permite efetuar uma série de tarefas forenses.

3) O paraben u3 universal apresenta uma maior capacidade de suporte de aquisição física para dispositivos Android. Tem ainda suporte especial para bases de dados de aplicações de chat.

4) A solução da AccessData contém uma versão de demonstração por 20 dias depois é necessário adquirir licença. Suporte adicional a dispositivos android.

5) O Elconsoft apresenta Suporte especial para contas Google e iCloud. Aquisição física nos iPhones 4s, 5 e 5c. Contém uma ferramenta especifica para descodificar ficheiros da aplicação WhatsApp. Esta aplicação só suporta dispositivos Apple.

6) O Lantern apenas é compatível com computadores Apple com sistema operativo OSX 10.12+.

7) O autopsy analisa formatos forenses como o E01, pastas ou localizações de ficheiros, imagens de discos rígidos ou máquinas virtuais. O software apresenta suporte para Android, nomeadamente para SMS, chamadas, registos, contactos etc.

8) O XAMN é a aplicação da MSAB utilizada para ler os ficheiros gerados pelo XRY que suporte a aquisição. Com o XAMN é possível fazer a respetiva análise dos dados e exportação de ficheiros. Mais informação consultar o anexo “Anexo A Guia de Aquisição e analise.pdf”.

9) O FTK Imager é um software que contém uma licença BSD *opensource*. Não é especializado em dispositivos móveis. Apenas permite analisar dados obtidos através de imagens forenses de formatos como o “E01” pastas ou localizações de ficheiros, imagens de discos rígidos ou máquinas virtuais.

Project

Master in computer Engineering – Mobile Computing

Digital Forensics procedures for Apple Devices

Appendix F – Device categories

Fábio António Lavrador Amado Marques

This appendix presents a list of devices in their categories: Computing devices, Storage, Peripherals, Networks and Virtualization.

Digital Forensics Purpose: We are mainly interested on devices that are able to store information.

Computing Devices

Computers

Desktop

Laptop

Server

Mobile

Smart phone

Smart watch

Digital Photographic Camera

Feature phone

GPS

Tablet

IoT

Energy Monitors

IP web cams

Trackers

Health

Pace maker

Storage

Internal mass storage device

HDD

SDD

EMMC (Embedded Multi-Media Controller)

Integrated storage

Integrated disk on computer motherboard

External mass storage device

CD /DVD/ BlueRay

Memory card

External disks

Pen drive

NAS

Criptographyc Devices

Floppy disks

Legacy

SIM CARD

TPM

Peripherals

- Monitors / All in one computer
- Printers
- Scanners

Networks

- Modem
- Routers
- Switches
- Voip Phone

Virtualization

- Virtual Machine

Project

Master in computer Engineering – Mobile Computing

Digital Forensics procedures for Apple Devices

Appendix G – Device acronyms

Fábio António Lavrador Amado Marques

This appendix presents a list of acronyms.

Table 1 - List of acronyms and description

Acronym	Description
A a Z	Target identification (Different people in the same process)
xx	Numbers, for example. 01 (All numbers must have two places)
Computing Devices - Computers	
PCxx	Desktop Computer
LAPxx	Laptop Computer
SRVxx	Specific Hardware from Server (Example: Rack)
Computing Devices - Mobile	
BPHxx	Feature Phone (Only SMS and calls)
SPHxx	Smart Phone (Wi-fi, GPS, ...)
SMWxx	Smart Watch
TBLxx	Tablet
CAMxx	Digital Camera
GPSxx	GPS Equipment (Example: Tom Tom or Garmin)
Computing Devices - IOT	
IOTxx	Energy monitors Trackers, IP Cameras
Computing Devices - Health	
HTHxx	Pace Maker
Storage - Internal Mass Storage Device	
HDDxx	Magnetic Disk
SSDxx	Flash Disk
EMCxx	eMMC memory (Embedded Multi-Media Controller)
Storage - External Mass Storage Device	
CDxx	CD-ROM or CD-R
BLUxx	Blue Ray Disk
DVDxx	DVD Disk
MCxx	All Types of memory Card
USBxx	USB External Disks
PENxx	USB Pen drive

NASxx	Network Attached Storage
Storage - Cryptographic Devices	
SIMxx	SIM Card for Phones
TPMxx	Other TPM cards (Cryptographic chips for authentication. Example: Citizen card or U2F (Used in google)
Storage - Legacy Devices	
FDxx	Floppy Disk
Peripherals	
MONxx	Monitor / All in one
PRNxx	Printer
SCNxx	Scanner
Networks	
MDMxx	Modem
RTRxx	Router
SWTxx	Switch
VOIxx	Voip Phone
Virtualization	
VMxx	Virtual Machine

Next we are going to present some examples of device acronyms.

All IDs must be used hierarchically, separated by points.

Some ID examples:
A # is the identification of the criminal.

1 desktop computer with two disks (HDD and SSD):
- A.PC01 # the computer
- A.PC01.HDD01 # desktop with magnetic disk
- A.PC01.SSD01 # desktop with SSD disk

1 smartphone with 2 SIM cards and a memory card
- A.SPH01 # The smartphone
- A.SPH01.SIM01 # Smartphone and the main SIM card
- A.SPH01.SIM02 # Smartphone and secondary SIM card
- A.SPH01.MC01 # Smartphone and memory card.

1 Portable hard disk:
- A.USB.HDD01 # The USB term is to distinguish disks that can be loose from portable disks.

1 internal loose hard disk, that isn't inside any computer:
- A.HDD01

1 server with various virtual machines (VMs):
- A.SRV01 # the server
- A.SRV01.VM01 # server and virtual machine 1
- A.SRV01.VM02 # server and virtual machine 2
- A.SRV01.VM03 # server and virtual machine 3

Introduction:

This document is an index for forensics procedures.

Follow the next 7 procedures when in a forensic case.

Procedure 1 Reception – This Procedure supports the first steps of a forensics case. Starting by the sign of the authorization request, mobile device reception, important verifications, data protection and the start of the internal report.

Procedure 2 Photographic Cataloging - This procedure supports the device and data storage devices catalogation and Photogaphing devices in the most important views.

Procedure 3 Preservation – This procedure supports data preservation for all procedures, so that data integrity can be mantained.

Procedure 4 Acquisition – This procedure supports on data acquisition with forensics software. Backup data creation.

Procedure 5 Examination- This procedure supports the search for evidences on data obtained from the acquisition with the use of software and manual techniques.

Procedure 6 Analysis - This procedure supports data analyse, comparing data, and relating evidences with hypothesis.

Procedure 7 Final Report – This procedure supports the creation of the final report based on the internal report and all with data and notes taken from all the procedures.

References

Whatson, D., & Jones Andrew. (2013). *Digital Forensics Processing and Procedures*. Elsevier.

Daniels, D. J., & Hart, S. V. (2004). Forensic Examination of Digital Evidence : A Guide for Law Enforcement. *U.S. Department of Justice Office of Justice Programs National Institute of Justice Special*, *44*(2), 634–111. https://doi.org/10.3408/jafst.7.95

Procedure Name: Reception
STO Version: 20170828

Subject:
The purpose of this procedure is the reception of mobile devices.

Scope:
This procedure should be followed when the reception of mobile devices at the begin of a forensics case. This is the first procedure to be followed.

Responsible Authority: LabCIF Quality Manager

Required equipment:
- Mobile devices

Required Documents:
- Request and authorization document.

Procedure detail
This is the first procedure to be followed when in a forensics case.
Read the Procedure 7 – Final Report to start writing the internal report since the beginning of the case.

1. Sign the request and authorization document.
2. Verify the existing devices of the case.
3. For each device verify the device status.
   - 3.1. Verify the device connector.
   - 3.2. Verify if there is any power cord.
   - 3.3. Verify if the device is on or off.
   - 3.4. If possible turn on the device screen and see what's happening.
   - 3.5. Verify the existence of any screen lock code or pin code.
   - 3.6. Verify if the battery level.
     - 3.6.1. If necessary connect a power cord.
   - 3.7. Verify if the device is connected to the mobile network, Wi-Fi network and with a Bluetooth connection.
   - 3.8. **Very Important:** Put the device on airplane mode to disconnect from any network.
   - 3.9. Verify the device model on the back side.
4. Verify if there is a SIM card on the device. (iPhone doesn't have memory SD card).
5. Create the chain of custody since the beginning.
6. Create a document named "Internal report" with case information.
   - 6.1. Insert some basic information about the forensics case
   - 6.2. Create a table with devices information like device type, manufacturer, model, device state and responsible forensics analyst **(view devices table example on appendices).**
   - 6.3. Fill the table with the available information. Red rows will be fulfilled with information from the next procedures.

Appendices

Devices Table

Information	Mobile Devices	
	Mobile device 1	Mobile Device n...
Device type	Smartphone	
Manufacturer	Apple	
Model	Iphone 4S A1234	
IMEI	[redacted]	[redacted]
Serial Number	[redacted]	[redacted]
State (On or OFF)	On	
Network Connected? (Mobile network, Wi-FI, Bluetooth	Mobile network and WiFi	
Device ID (label)	[redacted]	[redacted]
Responsible forensics analyst	Fabio Marques	
SIM CARD 1 and label	[redacted]	[redacted]
SIM CARD 2 and label	[redacted]	[redacted]
Memory Card	[redacted]	[redacted]
Conditions	working	
Observations	Battery in good state	
Photo	[redacted]	[redacted]

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October, 17*.

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

MURPHY, D. (2011). Cellular Phone Evidence Data Extraction and Documentation. Retrieved from http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2010/07/Cell-Phone-Evidence-Extraction-Process-Development-1.8.pdf

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices FOrensics*.

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history
20170512 – first version
20170530 – Procedure structure
20170602 - Procedure structure
20170820 - Improvement on procedure text.
20170822 - Improvement on procedure text.
20170827 - Improvement on procedure text.

Procedure Name: Photographic Cataloging
STO Version: 20170927

Subject:
The purpose of this procedure is the cataloging of the devices and their condition. Description of device positioning for: naming view sides; mandatory sides by device type and photographs

Scope:
This procedure should be followed when we have all equipments related to a case that need to be cataloged and photographed. The steps for Cataloging and Photographic are specified in the request.

Responsible Authority: LabCIF Quality Manager

Required equipment:
- Device to be cataloged
- Photographic Camera
- Memory Card
- Ruler
- Sticky Labels and pen
- Tools to open devices if required

Required Documents:
- Internal report

Possible Limitations
- Some devices cannot be opened.

Procedure detail

1. Take a photo to each received device from the legal authority;
2. Place device on a flat surface well lighted;
3. Take a look searching for damaged parts;
4. View if the device has any external mass storage device (Memory Card or SIM CARD), it can have more than one;
   4.1. If necessary use specific tools;
   4.2. Identify the external mass storage devices like SIM cards;
5. Label the devices , following the attachment “Anexo G Device acronyms” and put a sticker on the device and data supports.
   5.1. Leters (A, B, C, D) Identify the owners of the devices.
   5.2. Acronyms identify devices (SPHxx, Mcxx etc).
   5.3. Labels are in the format ownerID.deviceID
      5.3.1. Read examples to better understand.
6. Place a ruler near the device after taking photos;
7. Take a photo to the device according to the sub procedure “Procedure 2.1 Photographing” on the most important views and damaged sides (if they exist like searched on step 3);
   7.1. Name photos as the format TagID-view_name.jpg

7.1.1. Read examples to better understand.

8. Replace device covers and SIM Card.
9. Continue the internal report started in Procedure 1 - Reception with more information.
   9.1. Fill the **devices table** with more information like the label name, storage devices and photos.
   9.2. Green rows are information from Reception procedure.
   9.3. Red rows is information to be obtained from next procedures.
   9.4. Other rows can be filled with information from this procedure, including photos
   9.5. Highlight photos with damaged parts.

Examples:

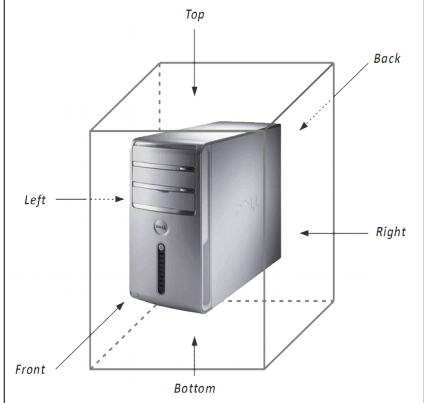
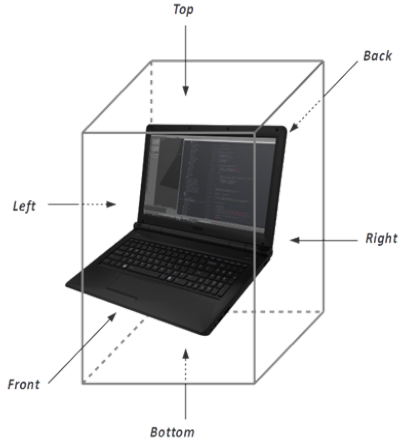
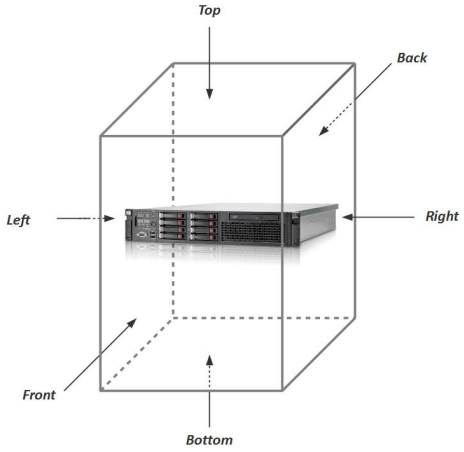
Ownwer: A
Smartphone: SPH01
SDCard: SD01

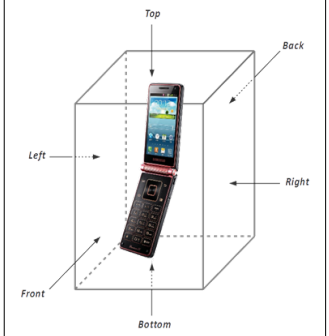
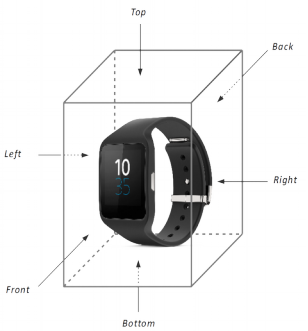
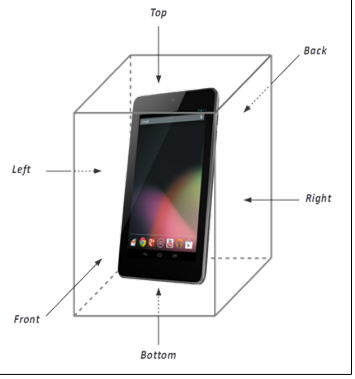
Complete label
A.SPH01.SD01

File Name for photo with sdcard for top view
A-SPH01-SD01-TOP.jpg

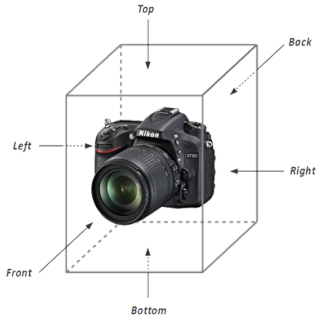
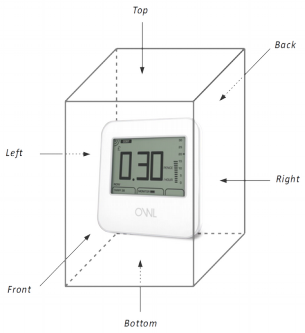
Appendices

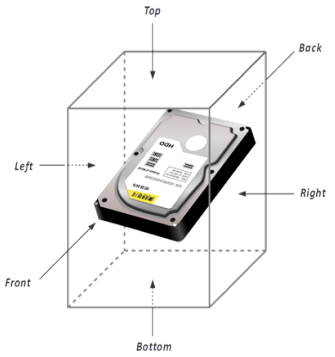
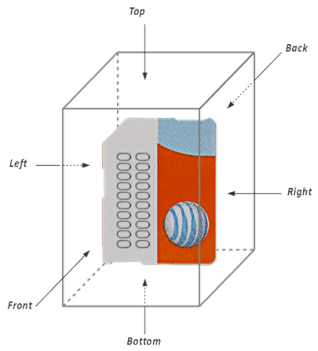
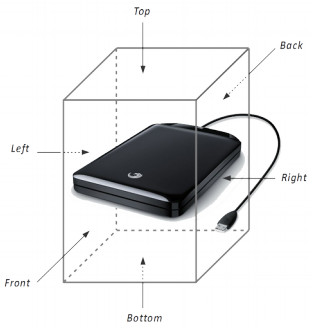
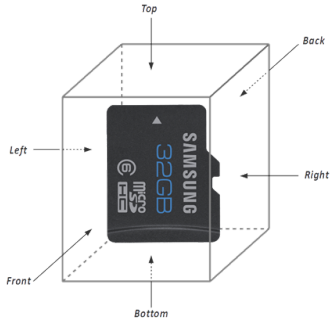
Table of digital equipments and view positioning

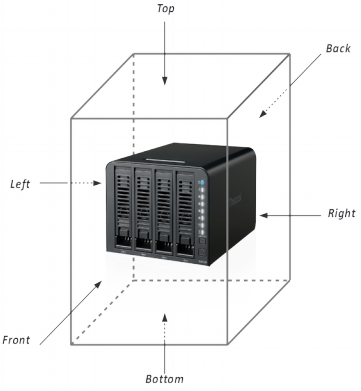
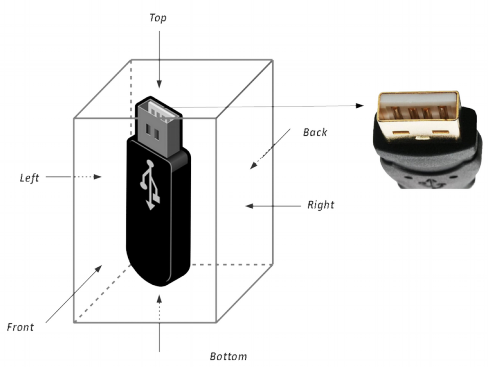
Computing Devices		
Computers		
Desktop Computer	Laptop Computer	Server
		

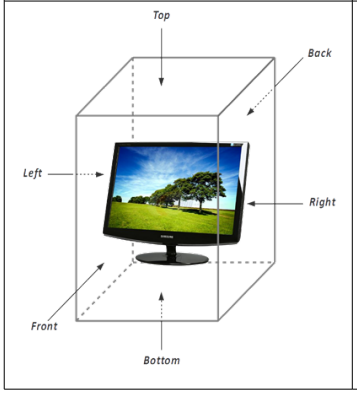
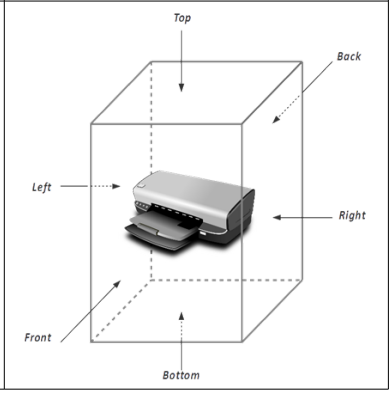
Computing Devices			
Mobile			
Feature Phone	Smartphone	SmartWatch	Tablet
			

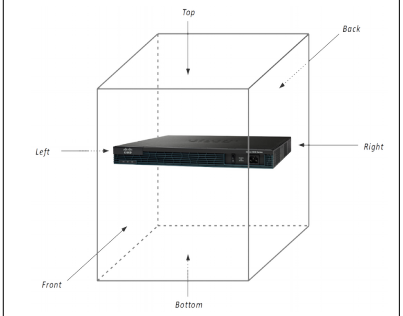
Computing Devices

Mobile	IOT
Camera	Energy Monitors
	

Storage			
Internal mass storage device		External Mass Storage Device	
HDD / SSD	SIM Card	External Disks	Memory Card
			

Storage	
External Mass Storage Device	
NAS	Pen Drive
	

Pheriperals	
Monitor / All-in-one computer	Printer
	

Networks	
Voip Phone	Router
	

Devices Table

Information	Mobile Devices	
	Mobile device 1	Mobile Device n...
Device type	Smartphone	
Manufacturer	Apple	
Model	Iphone 4S A1234	
IMEI		
Serial Number		
State (On or OFF)	On	
Network Connected? (Mobile network, Wi-FI, Bluetooth	Mobile network and WiFi	
Device ID (label)	SPH01.SIM01.SIM02.MC02	
Responsible forensics analyst	Fabio Marques	
SIM CARD 1 and label	SIM01	
SIM CARD 2 and label	SIM02	
Memory Card	MC01	
Conditions	Working	
Observations	Battery in good state	
Photos	A-SPH01-SIM01-SIM02-MC02-TOP	

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Documenting Computer Forensic Procedures. (n.d.). Retrieved March 10, 2017, from http://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Whatson, D., & Jones Andrew. (2013). *Digital Forensics Processing and Procedures*. Elsevier.

I. L. Lin, H. C. Chao and S. H. Peng, "Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone," *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*, Barcelona, 2011, pp. 386-391. doi: 10.1109/BWCCA.2011.63

I. L. Lin, Y. S. Yen and A. Chang, "A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime," *2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Seoul, 2011, pp. 543-548. doi: 10.1109/IMIS.2011.58

ISO. (2017). ISO Templates. Retrieved from https://www.iso.org/iso-templates.html

Sammons, J. (2012). *Introduction*. *The Basics of Digital Forensics*. https://doi.org/10.1016/B978-1-59749-661-2.00001-2

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October*, *17*.

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history
20170307 - First version
20170312 - Table of devices
20170313 - Table of devices / Procedure structure
20170314 - Procedure structure
20170321 - Procedure structure
20170530 - Procedure structure
20170815 - Procedure structure
20170822 - Improvement on procedure text.
20170927 - Improvement on procedure text.

This attachment is important to follow when taking photos in a forensics case.

General Notes:

1. Use a ruler to place near the devices when taking photos.
2. If applicable remove covers or caps in order to:
   - 2.1. Locate and identify internal storage devices;
   - 2.2. Check serial numbers;
   - 2.3. Check Brand and models;
   - 2.4. Check storage capacity;
   - 2.5. Take Photos to all ID’s found;
   - 2.6. If Damaged, take additional photos to show the device conditions when it was received.

Category: Computing Devices | Computers

Desktop

Important Notes:

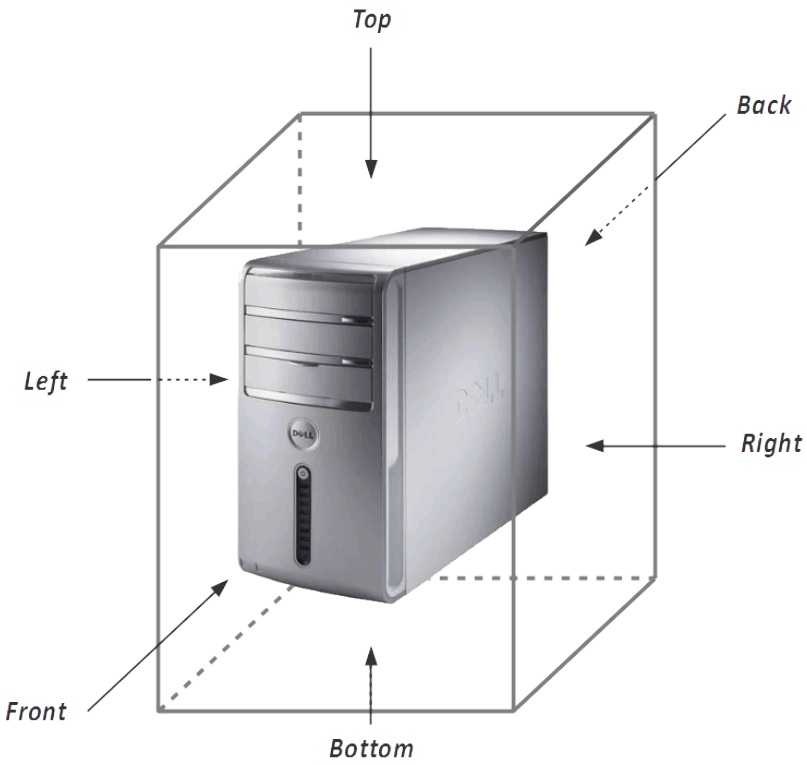
The photos must pick up codes, inputs and data supports;

When possible take photos to the hardware inside of the tower;

The codes can be located on Top, or Bottom, Righ or back view.

Object Position:

Power cable and other connectivity interfaces should be facing the back view (see image bellow).



Mandatory Views:

Back;

Front;

Inside with storage device in place;

Readable photo of any ID numbers.

Category: Computing Devices | Computers

Laptop Computer

Important Notes:

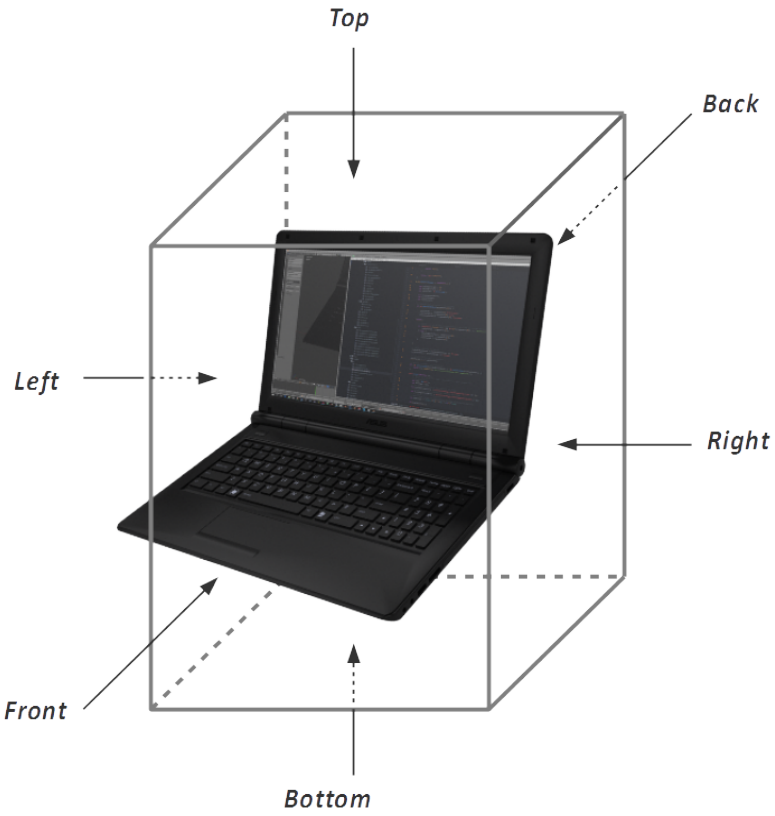
The photos must pick up any codes (serial numbers, model, etc), inputs and data supports;

If possible take photos to the hardware inside of the computer.

Object Position:

The screen of the computer must be open to the maximum allowed angle up to 180º in relation to the keyboard;

Top View: Keyboard with open screen.



Mandatory Views:

Top;

Bottom;

All sides with connections;

Inside with storage device in place;

Readable photo of any ID numbers.

Category: Computing Devices | Computers

Server

Important Notes:

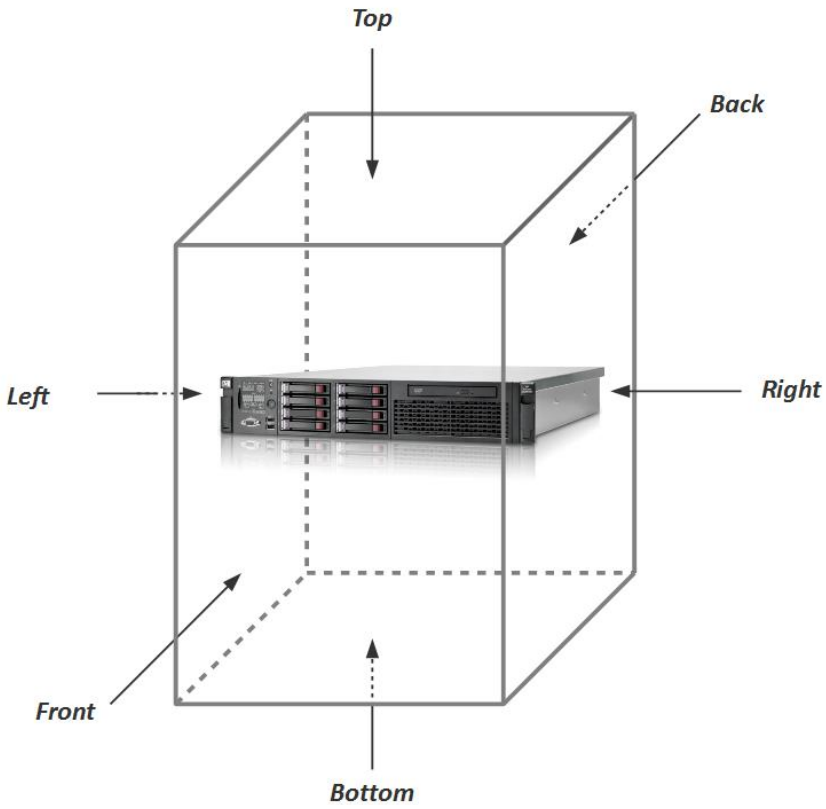
The photos must pick up codes, inputs and storage devices;

If possible take photos to the hardware inside of the towe;r

The codes can be located on Top, or Bottom, Righ or back view.

Object Position:

Power cable facing the back view.



Mandatory Views:

Back;

Front;

Inside with storage device in place;

Readable photo of any ID numbers;

Category: Computing Devices | Mobile

Feature Phone

Important Notes:

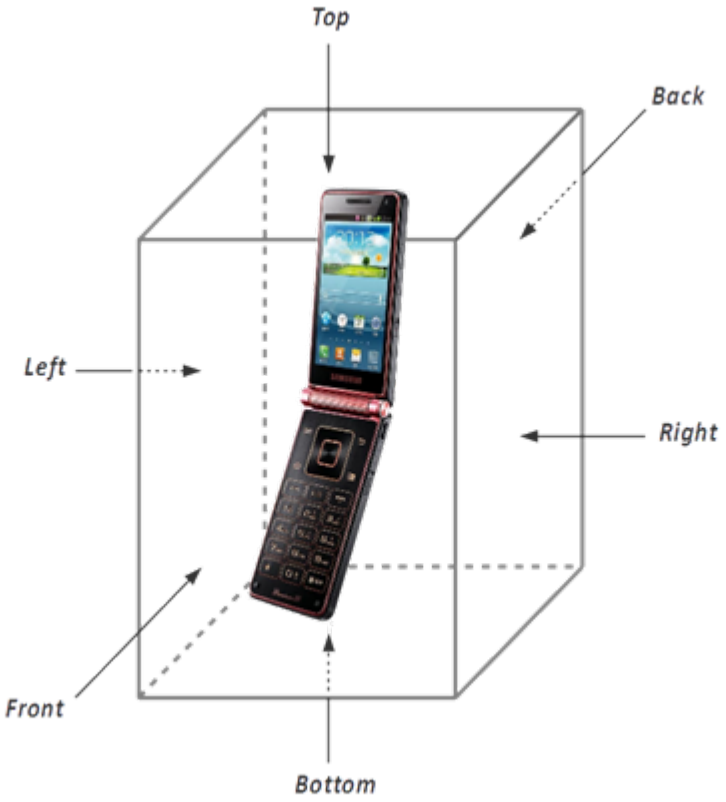
The photos must pick up codes, inputs and data supports without cover and battery;

The IMEI must be visible in one of the photos (it may be located in the battery compartment or, in the SIM card tray).

Object Position:

The phone must be opened;

Front view: Screen.



Mandatory Views:

Front;

Back;

Inside battery compartment if applicable;

Readable photo of any ID numbers.

Category: Computing Devices | Mobile

Smartphone

Important Notes:

The IMEI must be visible in one of the photos.

Object Position:

Front view: Screen.

Mandatory Views:

Front;

Back;

Inside battery compartment if applicable;

Readable photo of any ID numbers.

Category: Computing Devices | Mobile

SmartWatch

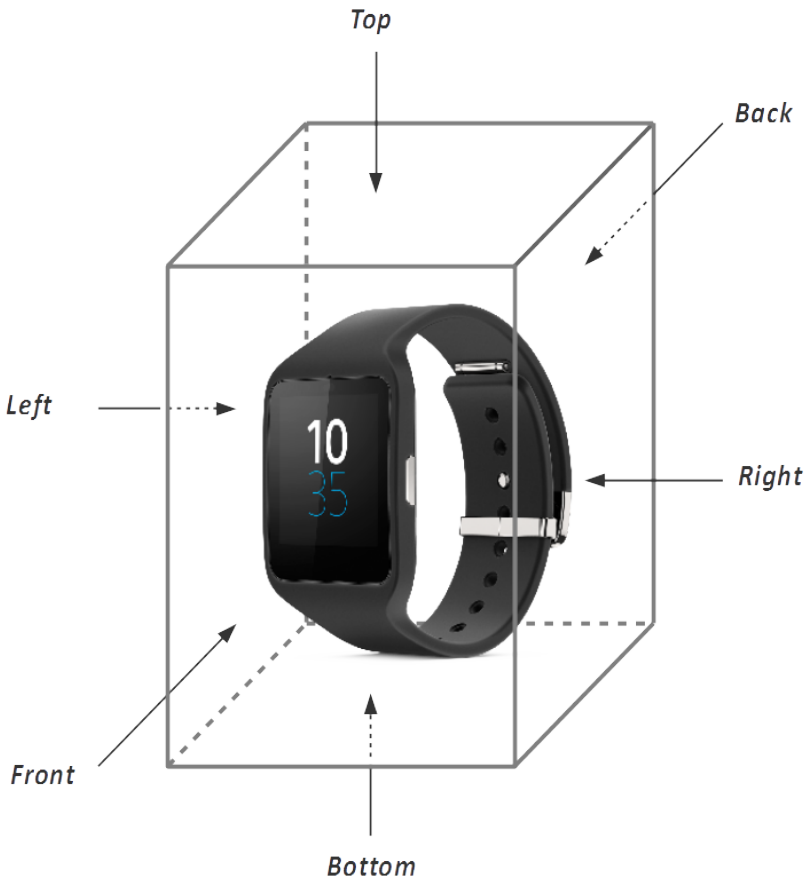
Important Notes:

The photos must pick up codes, inputs and data supports without cover and battery;

The IMEI must be visible in one of the photos.

Object Position:

Front view: Screen.



Mandatory Views:

Front;

Back;

Readable photo of any ID numbers.

Category: Computing Devices | Mobile

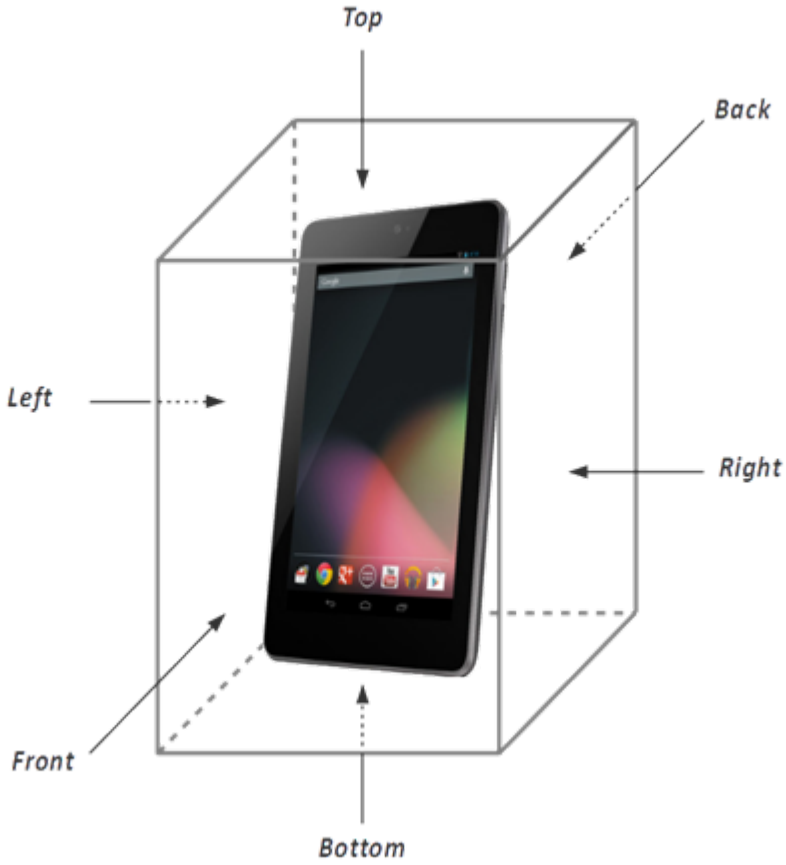
Tablet

Important Notes:

The photos must pick up codes, inputs and data supports;

Object Position:

Front view: Screen facing the user.



Mandatory Views:

Front;

Back;

Inside battery compartment if applicable;

Readable photo of any ID numbers.

Category: Computing Devices | Mobile

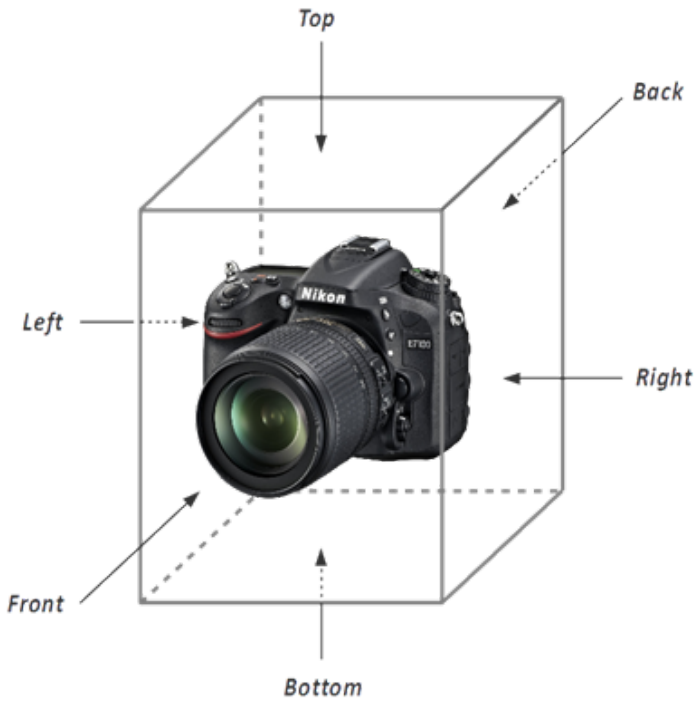
Camera

Important Notes:

The photos must pick up codes, inputs and data supports;

Object Position:

Front view : Lens facing the user.



Mandatory Views:

Front;

Back;

Readable photo of any ID numbers;

Side with memory card door.

Category: Computing Devices | IoT

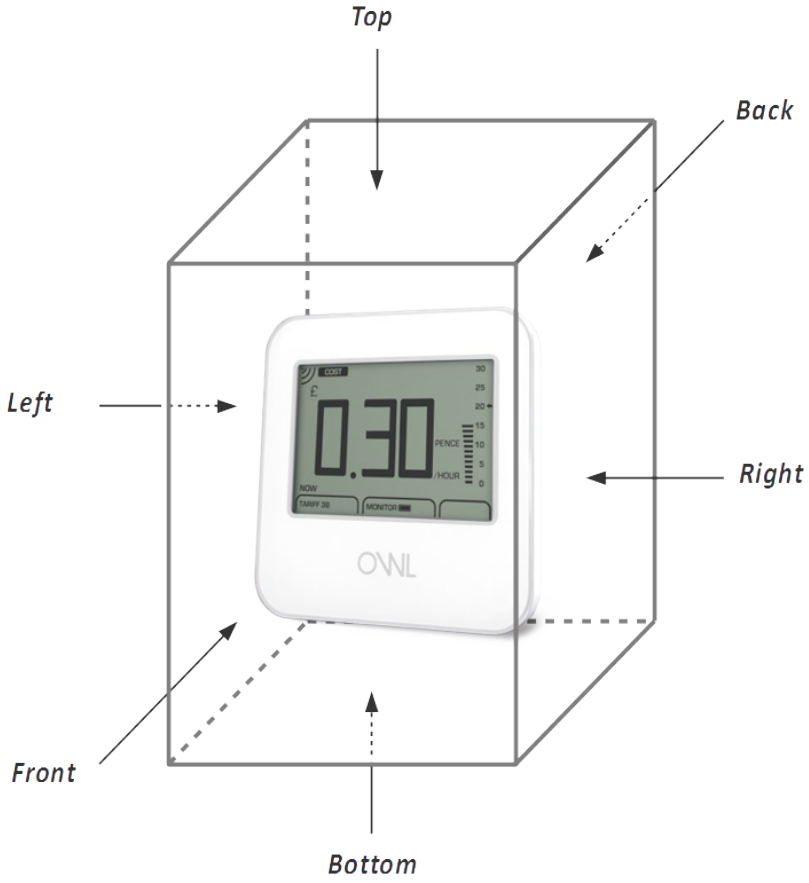
Energy Monitors

Important Notes:

The photos must pick up codes, inputs and data supports.

Object Position:

Front view : screen.



Mandatory Views:

Front;

Back;

Readable photo of any ID numbers.

Category: Storage | Internal Mass Storage Device

HDD or SSD

Important Notes:

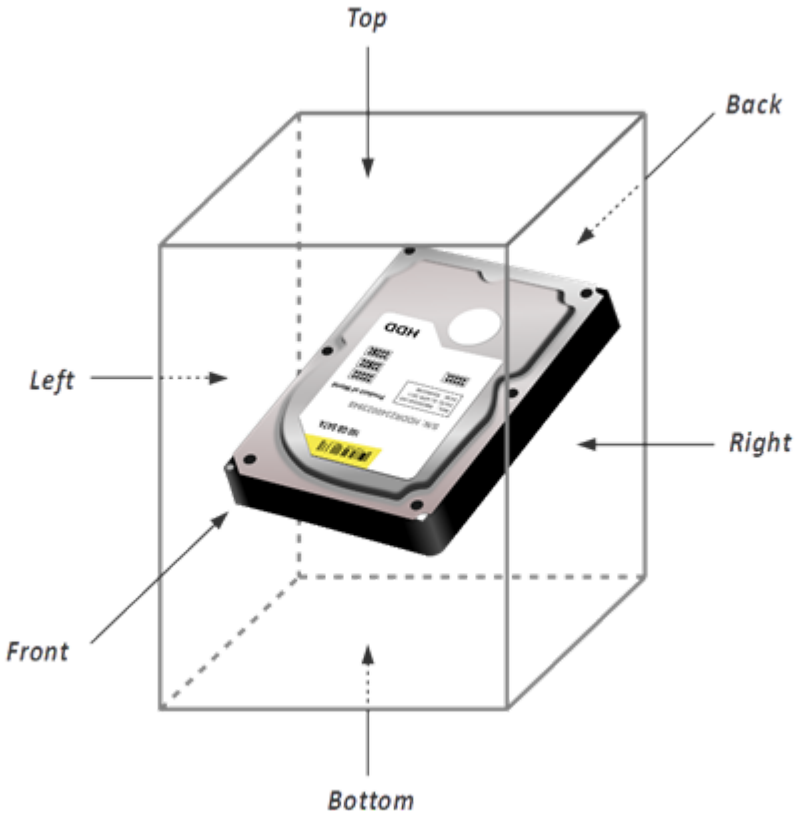
The photos must pick up codes and all ports;

If it is damaged, take additional photos.

Object Position:

Top view: Disk cover and brand label;

Back view: Power and interfaces.



Mandatory Views:

Top;

Bottom;

Readable photo of any ID numbers.

Category: Storage | Internal Mass Storage Device

SIM Card

Important Notes:

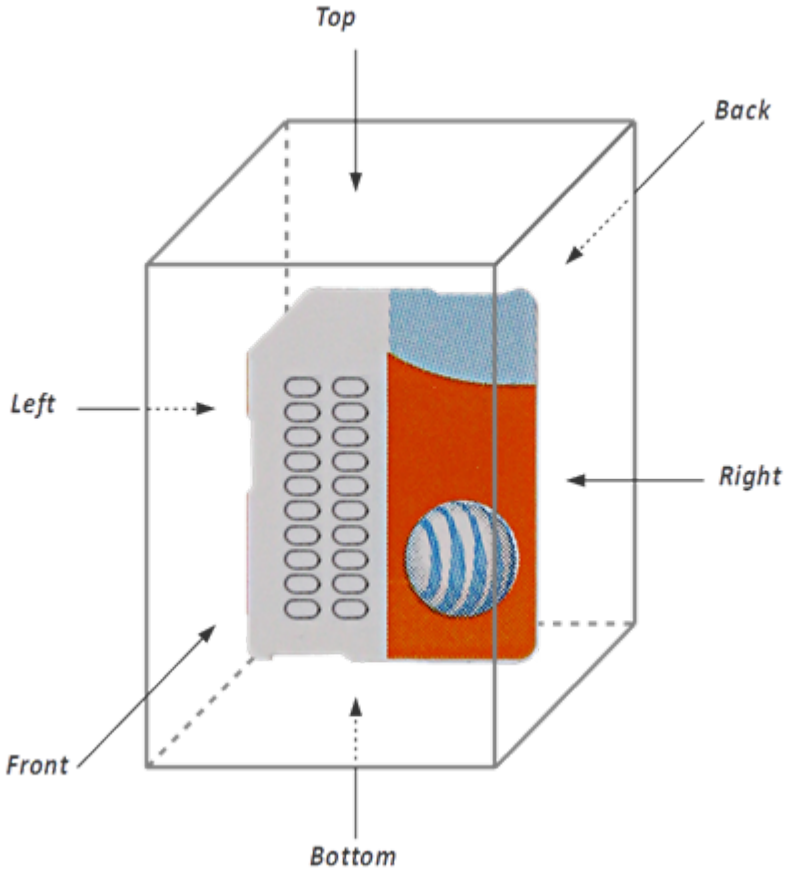
The photos must pick up codes and connections.

Object Position:

Front View: Codes;

Corner to the top;

Back view: electric contacts.



Mandatory Views:

Front;

Back;

Readable photo of any ID numbers.

Category: Storage | External Mass Storage Device

External disks

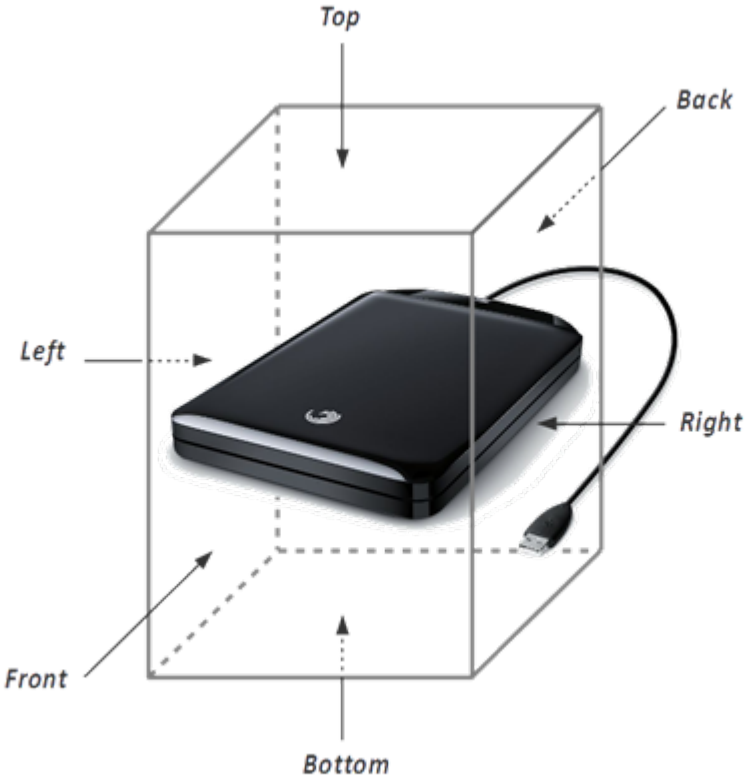
Important Notes:

The photos must pick up codes and inputs;

If it is damaged, take additional photos.

Object Position:

Back view: Data cable connector.



Mandatory Views:

Back;

Top;

Bottom;

Readable photo of any ID numbers.

Category: Storage | External Mass Storage Device

Memory Card

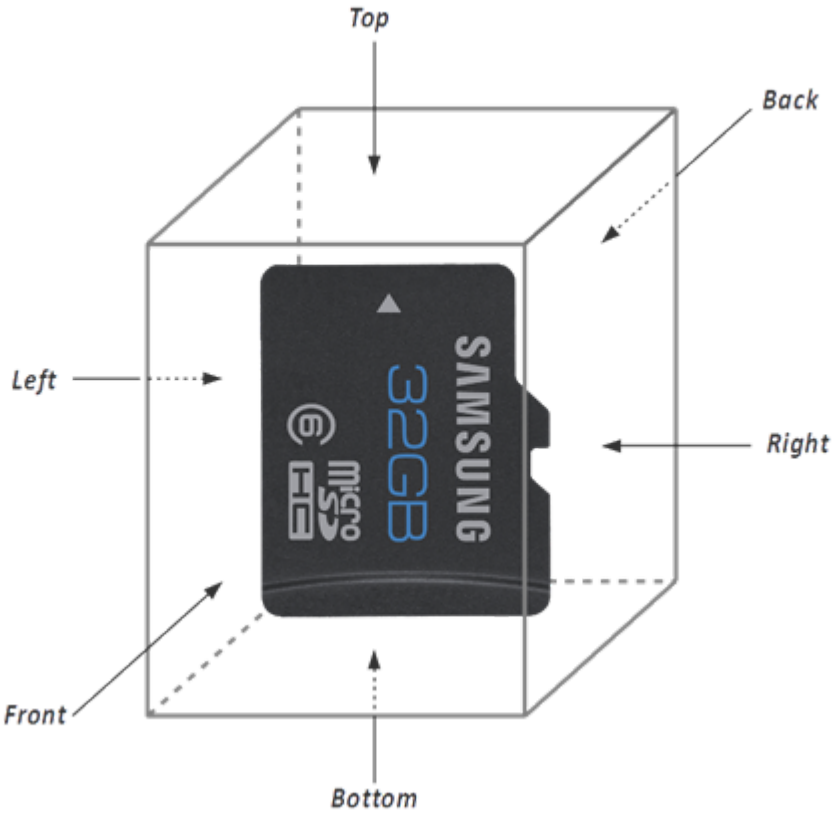
Important Notes:

The photos must pick up codes and electronic contacts.

Object Position:

Back View: Electric contacts;

Bottom view: Side with the protrusion to remove the card.



Mandatory Views:

Front;

Readable photo of any ID numbers.

Category: Storage | External Mass Storage Device

NAS

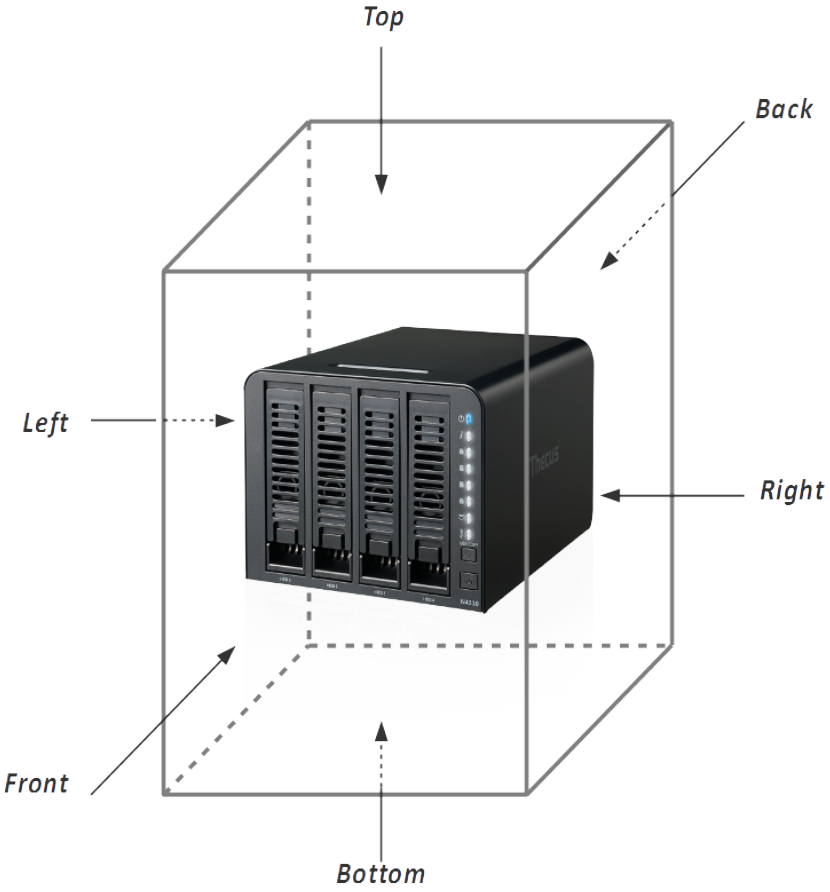
Important Notes:

The photos must pick up codes and inputs.

If it is damaged, take additional photos;

Object Position:

Back view: Interface connectors.



Mandatory Views:

Front;

Back;

Inside with storage devices in place;

Readable photo of any ID numbers.

Category: Storage | External Mass Storage Device

Pen Drive

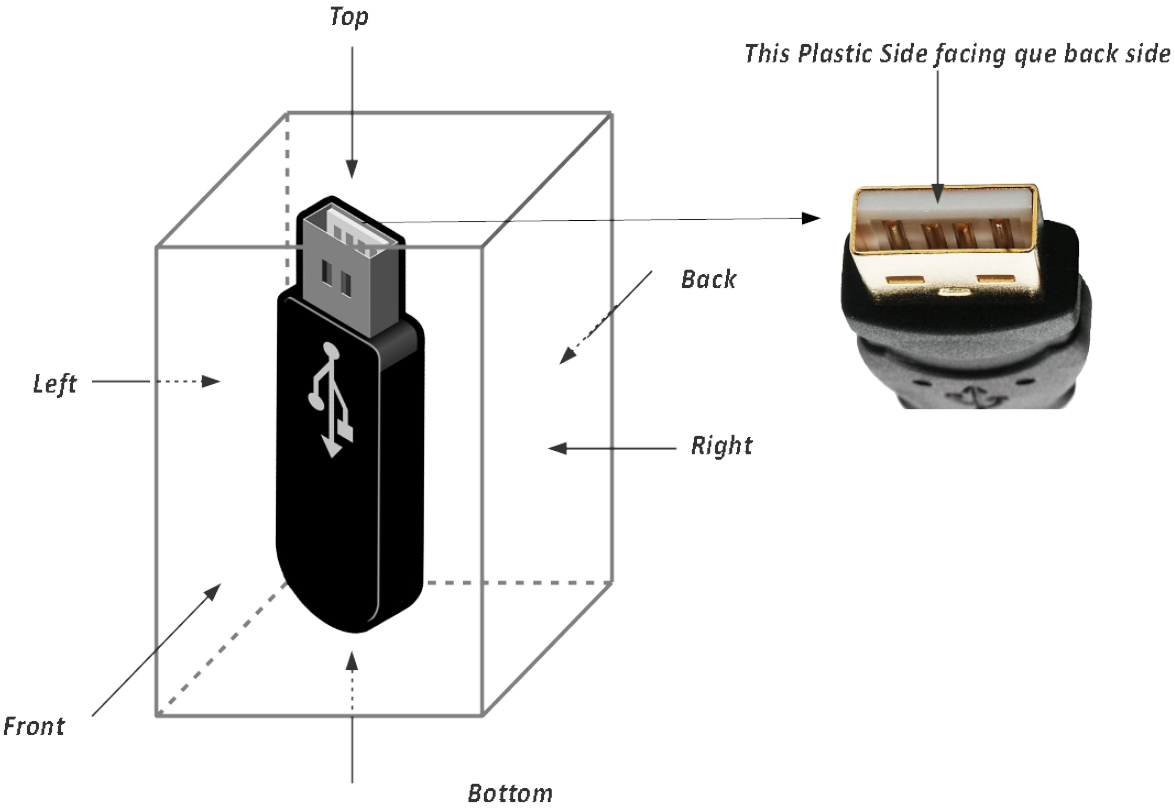
Important Notes:

The photos must pick up codes and connections.

Object Position:

Top view: USB Interface;

Front view: USB inside connectors on the back side.



Mandatory Views:

Front;

Back;

Readable photo of any ID numbers.

Category: Pheriperals

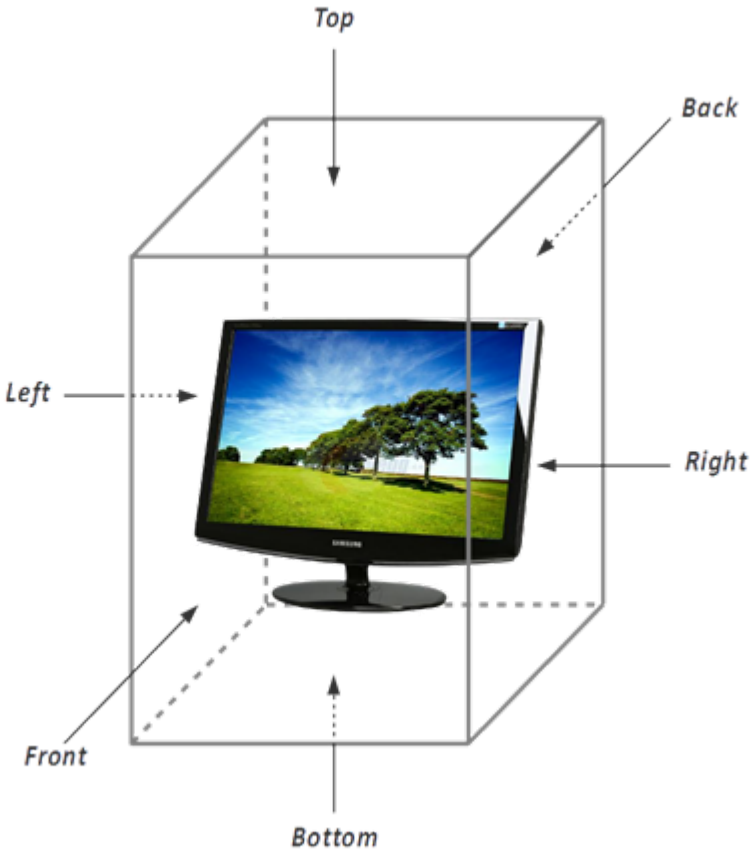
Monitor Or All-in-one computer

Important Notes:

The photos must pick up codes and all ports.

Object Position:

Front view: screen facing the user.



Mandatory Views:

Front;

Back;

Sides with connection interfaces;

Readable photo of any ID numbers.

Category: Pheriperals

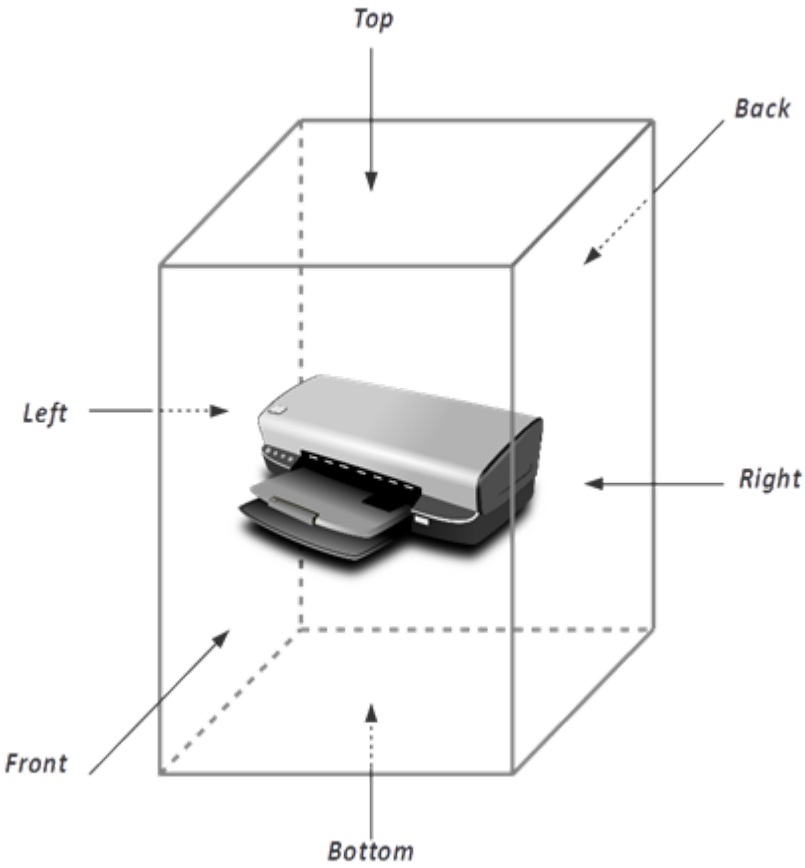
Printer

Important Notes:

The photos must pick up codes and connections.

Object Position:

Front view: printer interface facing the user.



Mandatory Views:

Front;

Readable photo of any ID numbers;

If applicable inside with storage device in place.

Category: Networks

Voip Phone

Important Notes:

The photos must pick up codes and connections.

Object Position:

The phone must be on the normal position with the numbers on the correct read position.

Mandatory Views:

Front;

Top;

Bottom;

Readable photo of any ID numbers.

Category: Networks

Router

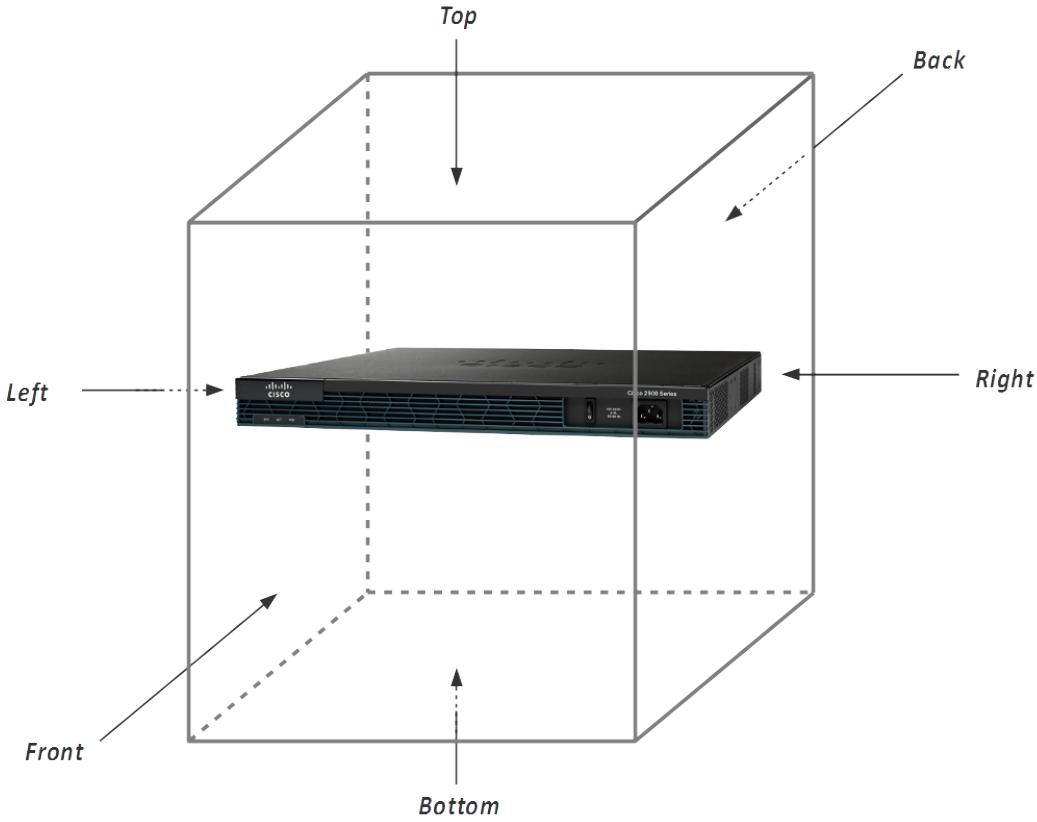
Important Notes:

The photos must pick up codes and connections;

If it is damaged, take additional photos.

Object Position:

Front: Side with lights indicating the connections and equipment state.



Mandatory Views:

Front;

Top;

Back;

Readable photo of any ID numbers.

References:

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Sammons, J. (2012). *Introduction*. *The Basics of Digital Forensics*. https://doi.org/10.1016/B978-1-59749-661-2.00001-2

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Version history

20170309 – first version
20170310 - Procedure structure.
20170313 - Improvement on procedure text.
20170315 - New devices added
20170628 - Improvement on procedure text.
20170629 - Improvement on procedure text.
20170812 - Improvement on procedure text.
20170822 - Improvement on procedure text.
20170828 - Improvement on procedure text.

Procedure Name: Preservation
STO Version: 20170828

Subject:
The purpose of this procedure is to enumerate the main steps when preserving data on a digital forensics case.

Scope:
This procedure should be followed when preserving data from mobile devices.

Responsible Authority: LabCIF Quality Manager

Required equipment:
- RF Shielding (e.g. Faraday Bag)
- Power cable for mobile device
- Special Tools if necessary to remove the SIM card

Possible Limitations
- Low battery power and lack of power cord may cause the device turn off.
- Turning off the device can be a problem because if it has any unknown code we cannot turn it on.
- Unknown SIM card PIN code can be a problem if the SIM card is removed.
- The use of the Faraday bag can cause the battery to drain faster.

Procedure detail

1. Verify the existing devices of the case.
2. Create the chain of custody.
3. For each device verify the device status.
   - 3.1. Ensure that device is integrity
   - 3.2. Verify if the battery level.
     - 3.2.1. If necessary connect a power cord.
   - 3.3. Put the device on airplane mode to disconnect from any network and avoid data integrity problems.
4. Ensure that only authorized forensics analyst use the devices.
5. If it is necessary to do a forensics acquisition to the SIM card in procedure 4 Acquisition, use a write blocker.
6. Create a backup of data obtained from the acquisition phase.
   - 6.1. Ensure that forensic images are stored in adequate devices.
7. Create a backup of data extracted during the examination phase.
   - 7.1. Ensure that evidences are stored in adequate devices.
8. Generate a hash key using SHA256 algorithm from forensics data to ensure data integrity.
9. Insert notes on the internal report related to the steps done on this procedure.

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Carrier, B. D. (2006). Hypothesis-Based Approach To Digital Forensic Investiga Ations, 190.

Sammons, J. (2012). *Introduction*. *The Basics of Digital Forensics*. https://doi.org/10.1016/B978-1-59749-661-2.00001-2

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, 386–391. https://doi.org/10.1109/BWCCA.2011.63

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October*, *17*.

Fukami, A., Ghose, S., Luo, Y., Cai, Y., & Mutlu, O. (2017). Improving the reliability of chip-off forensic analysis of NAND flash memory devices. *Digital Investigation*, *14*, S1–S11. https://doi.org/10.1016/j.diin.2017.01.011

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

MURPHY, D. (2011). Cellular Phone Evidence Data Extraction and Documentation. Retrieved from http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2010/07/Cell-Phone-Evidence-Extraction-Process-Development-1.8.pdf

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history
20170327 – first version
20170418 - Revision
20170610 - Procedure structure
20170612 - Improvement on procedure text.
20170701 - Procedure structure
20170715 - Improvement on procedure text.
20170828 - Improvement on procedure text.

Procedure Name: Acquisition
STO Version: 20170828

Subject:
The purpose of this procedure is to extract data from mobile devices in a crime scenario.

Scope:
This procedure should be followed when doing a logical acquisition from a mobile device that has possible evidences and needs to be analyzed.

Responsible Authority: LabCIF Quality Manager

Required equipment

- Forensics Computer
- Forensics acquisition Software
- Hardware and Software Write Blockers
- Sim Card reader
- Forensics kit with all cables
- Mass storage device to save data from the acquition

Software

- Forensics software

Document

- Internal report

Possible Limitations

- If the device is turned off or it has any code it is not possible to do a logical acquisition.

Procedure detail
This procedure only applies to a logical acquisition.
There must be used write protection mechanisms complementing hardware with software write protection to maintain data integrity.

1. Prepare Hardware and cables on a flat surface table;
   1.1. Use a write blocker on the need to do acquisition to a sim card, to prevent data contamination.
   1.2. Choose the right cables to connect to the mobile device.
2. Prepare forensics software to do the acquisition.
3. identify data sources of information.
   3.1. On iPhone there are no memory cards. There is only the internal memory and the SIM card.
   3.2. Prepare the devices.
4. Connect the devices to the computer or proprietary device.
5. Open forensics software and choose device.
   5.1. Choose to do a logical acquisition.
   5.2. Take attention to the information given by acquisition software during the

acquisition.

5.2.1. If necessary take notes for the internal report.

6. Save the forensics acquisition image file(s) in more than a secure data storage device.
7. If necessary to do an acquisition to the SIM Card, retire the sim card.

7.1.1. Connect it to a write blocker.

8. Generate a Hash MD5 Value of the data after doing the acquisition;

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, (August), 800–886. https://doi.org/10.6028/NIST.SP.800-86

Viriato, L. M. (2016). *Gestão da qualidade e acreditação em informática forense.* Instituto Politécnico de Leiria.

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, 386–391. https://doi.org/10.1109/BWCCA.2011.63

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October, 17*.

Daniels, D. J., & Hart, S. V. (2004). Forensic Examination of Digital Evidence : A Guide for Law Enforcement. *U.S. Department of Justice Office of Justice Programs National Institute of Justice Special*, *44*(2), 634–111. https://doi.org/10.3408/jafst.7.95

Fukami, A., Ghose, S., Luo, Y., Cai, Y., & Mutlu, O. (2017). Improving the reliability of chip-off forensic analysis of NAND flash memory devices. *Digital Investigation*, *14*, S1–S11. https://doi.org/10.1016/j.diin.2017.01.011

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history
20170327 – first version
20170410 - Improvement on procedure text.
20170412 - Procedure structure.
20170415 - Improvement on procedure text.
20170810 - Improvement on procedure text.
20170812 - Procedure structure.
20170828 - Improvement on procedure text.

Procedure Name: Examination
STO Version: 20170827

Subject:
The purpose of this procedure is the examination of extracted data obtained on the acquisition phase from any mobile device involved in an incident or crime.

Scope:
This procedure should be followed when we have original or duplicated data from a forensics acquisition. The steps and techniques used during the examination are specified in the request.

Responsible Authority: LabCIF Quality Manager

Required equipment:
Hardware
- Forensics Computer

Software
- Forensics Software (XAMN Viewer or other)
- Sqlite browser
- Plist Viewer
- GeoSetter or other software to view GPS data.

Command line tools
- File command line tool
- Strings command line tool
- Exiftool

Possible Limitations
- Tool capabilities can limit obtained results

Procedure detail
All steps done in examination process should be well documented as the point 8 of Procedure 7.

1. Read the forensics request and see which important information must be searched.
2. Identify forensics data image from the extraction.
   2.1. Use duplicated data, do not work with original data.
   2.2. Use the appropriate software to open forensics image.
3. Create the Examination table for the internal report that will be used on the final report. **(view Examination table example on appendices)**.
   3.1. Fill the table with files and evidences found.
4. Start Searching data according to the type of crime, by using software automatic features to organize data types in categories.
   4.1. If software supports file preview see if it has important information.
   4.2. Extract files that may contain important information.
   4.3. Take screenshots from important information that cannot be extracted.
   4.4. Note what are the most common file extensions.
   4.5. Indicate software used to search data.

4.5.1. Search for device info (Type, Model, Operating System version, IMEI, serial number, configurations etc).
4.5.2. Search for SIM card data (If software supports.
4.5.3. Search for contacts.
4.5.4. Search for SMS and MMS.
4.5.5. Search for Call Registry.
4.5.6. Search for user accounts.
4.5.7. Search for applications installed.
4.5.8. Search for exchanged attachments between applications and contacts.
4.5.9. Search for Photos and videos.
4.5.10. Search for GPS Data.
4.5.11. Search for Wi-Fi data and passwords.
4.5.12. Search for databases.
4.5.13. Search for Web History, bookmarks and others.
4.5.14. Search for Calendar events and notes.
4.5.15. Search for e-mails.
4.5.16. See file system structure.
4.5.17. Search for deleted files (if possible, depends on the type of acquisition).
4.5.18. Search for backup files.
4.5.19. Search for other types of data important to the forensics case.

5. Use manual search techniques to search more evidences.
   5.1. Use keywords, strings, or regular expression to search data on Software.
   5.2. Extract files that may contain important information.
   5.3. Take screenshots from important information that cannot be extracted
   5.4. Indicate which manual techniques were used.
      5.4.1. Search for data types that are not categorized.
      5.4.2. Search for well kwnow file extensions (.plist, .sqlite, .sqlitedb, .db, .data, storedata, .jpg etc).
   5.5. Use tools to search data inside files.
      5.5.1. file command to see the file type.
      5.5.2. strings command to search text inside files.
      5.5.3. exiftool to search for location data.
6. Fill the examination table with evidences found.
7. Save all extracted files in a folder.
   7.1. Use an encryption algorithm like SHA256 to generate an hash key of all data to maintain it’s integrity.

Appendices

Examination table

Device ID(label)	SPH01.SIM01.MC01		
File Name	File Location	Related Application	Obtained Data
Line.sqlite	/private/var/mobile/ Library/SpringBoard /PushStore/	Line	List of contacts Messages exchanged
Application n...			

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Whatson, D., & Jones Andrew. (2013). *Digital Forensics Processing and Procedures*. Elsevier.

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, 386–391. https://doi.org/10.1109/BWCCA.2011.63

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October*, *17*.

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history

20170328 - first version.
20170412 - Procedure structure.
20170719 - Improvement on procedure text.
20170822 - Improvement on procedure text.
20170827 - Improvement on procedure text.

Procedure Name: Analysis
STO Version: 20170828

Subject:
The purpose of this procedure is the analysis of extracted data or recovery from any mobile device involved in an incident or crime.

Scope:
This procedure should be followed when we have evidences extracted and they need to be analyzed to know which are the most important for the forensics case, relate data, approve or not approve hypothesis and get conclusions.
The steps used for analysis are specified in the request.

Responsible Authority: LabCIF Quality Manager

Required equipment:
Hardware
- Forensics Computer

Software
- Forensics Software (XAMN Viewer or other)
- Sqlite browser
- Plist Viewer
- GeoSetter or other software to view GPS data.

Possible Limitations
- Tool capabilities can limit obtained results

Procedure detail
All steps done in examination process should be well documented to allow another forensics examiner of the same area to analyse and identify all steps done.

1. Create the analysis table for the internal report that will be used on the final report.**(view analysis table example on appendices)**.
2. Create the analysis Hypothesis table for the internal report that will be used on the final report.**(view analysis hypothesis table example on appendices)**.
3. Identify the objectives of forensics case.
4. Analyze and identify data types extracted on the Examination phase.
   - 4.1. Identify all imported files extracted.
     - 4.1.1. Analyze file string content.
     - 4.1.2. Analyze data from SIM Card.
     - 4.1.3. Analyze contacts data.
     - 4.1.4. Analyze SMS and MMS data.
     - 4.1.5. Analyze Call registry data.
     - 4.1.6. Analyze user accounts data.
     - 4.1.7. Analyze application files.

4.1.8. Analyze application attachments.
4.1.9. Analyze photos and videos.
4.1.10. Analyze GPS data.
4.1.11. Analyze Wi-Fi data and passwords.
4.1.12. Analyze databases and their tables.
4.1.13. Analyze web history, bookmarks and others.
4.1.14. Analyze calendar events and notes data.
4.1.15. Analyze e-mail data.
4.1.16. Analyze file system structure.
4.1.17. Analyze deleted files (if they exist).
4.1.18. Analyze backup data.
4.1.19. Analyze other types of data important for the forensics case.
4.2. Identify the ownership of the devices.
4.3. Identify metadata, time stamps and other information.
4.4. Identify if digital evidence has value for the forensics case.
4.5. Relate digital evidences to obtain more conclusions.
4.5.1. Relate files and Applications. Example: Attachments.

5. Fill the analysis table with types of digital evidences found for each device, that can be useful for the forensics case.
6. Fill the analysis hypothesis table with hypothesis and evidences .
6.1. Verify if evidences approve or not approve hypothesis.

Appendices

Analysis table

Devices Device ID (Label)	Data types																	
	SIM card data	Device info	Contacts	SMS and MMS	Call Registry	User accounts	Application Appendices	Photos and videos	File System	GPS Data	Wi-Fi Data	Bluetooth Data	Databases	Web History	Documents	Calendar	E-mails	Installed Applications
iPhone 4S SPH01.SIM01. MC01	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	WhatsApp Line Skype Signal ...
Device 2																		

Analysis Hypothesis table

Hypothesis	Approved / Not Approved	Evidence 1	Evidence n...
John send a smartphone photo to Maria thought WhatsApp	Approved	Maria’s Smartphone had a smartphone photo in WhatsApp image folder	

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Whatson, D., & Jones Andrew. (2013). *Digital Forensics Processing and Procedures*. Elsevier.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, (August), 800–886. https://doi.org/10.6028/NIST.SP.800-86

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, 386–391. https://doi.org/10.1109/BWCCA.2011.63

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October*, *17*.

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history
20170328 – first version
20170401 – Procedure structure
20170716 - Improvement on procedure text.
20170720 - Improvement on procedure text.
20170810 - Procedure structure.
20170816 - Improvement on procedure text.
20170828 - Improvement on procedure text.

Procedure Name: Final Report
STO Version: 20170828

Subject:
The purpose of this procedure is to write the final forensics report.

Scope:
This procedure should be followed when writing the final forensics reporting with all information related to the forensics case.
The steps used for creating the Final Report are specified in the request.

Responsible Authority: LabCIF Quality Manager

Required equipment:
Hardware
- Forensics Computer

Software
- Forensics Software
- Text Processor software

Required Documents
- Internal forensics report with all data related to the forensics case since the reception procedure to the analysis procedure.

Required Data
- Data files from the forensics case.

Procedure detail

1. Create a document named Final Report.
2. Create a chapter named Introduction.
   2.1. Insert the process or case number and report date.
   2.2. Insert information about the requested and what was requested to do on the forensics case.
   2.3. Insert the suspect names and tags.
   2.4. Insert data of the reception of the devices.
   2.5. Use **devices table** created on the internal report.
      2.5.1. Table must contain all devices, device id, related information, and responsible forensics analyst. **(view devices table example on appendices).**
3. Create a chapter per device with all steps and decisions from the forensics procedures.
   3.1. Create a table to have the device info with information from **devices table.**
   3.2. Fill the document with information taken from the chain of custody.
   3.3. Identify steps done on the reception procedure.
   3.4. Identify steps done on Photographic Cataloging procedure.
      3.4.1. Insert photos of the device and storage devices with respective ID (tag).
   3.5. Identify steps done on preservation procedure.
   3.6. Identify steps done on the acquisition phase.
      3.6.1. Use **acquisition table** created on the internal report **(view acquisition table example on appendices).**

3.6.2. Table must contain device manufacturer and model, device ID, case number, software used, type of acquisition (Logical or physical) and data storage devices (SIM card or Memory card).
3.6.3. Indicate witch type of memory was acquired on the acquisition.
3.7. Identify steps done on the Examination phase.
3.7.1. Detail how was done the search of evidences, witch techniques and steps done to search evidences.
3.7.2. Indicate which software was used to search for evidences.
3.7.3. Indicate which manual techniques were used to search evidences.
3.7.4. Use **Examination table** created on the internal report which has the files, related application and obtained data. **(view examination table example on appendices).**
3.8. Identify steps done on the analysis Phase.
3.8.1. Indicate which software was used to analyze data.
3.8.2. Use **analysis table** created on the internal report with data types obtained **(view analysis table example on appendices)**.
3.8.3. Indicate and detail all evidences found.
3.8.4. Use the hypothesis and evidences table created on the internal report **(view Analysis Hypothesis table example on appendices).**
3.8.4.1. Indicate if evidences approve or not hypothesis.
3.8.4.2. True hypothesis should be well justified with one ore more evidences.
3.8.4.3. Indicate one or more explications about something.
3.9. Include the output of tools.
3.10. Verify all forensics steps, hypothesis and evidences.
3.10.1. Verify if all forensics steps were well done.
3.10.2. Verify the results fore more than one time.
3.10.3. Verify if there are repeated data.
3.10.4. To verify possible mistakes, ask another forensics analyst to repeat some steps.

4. Create a conclusions chapter.
4.1. Create a summary with the list of evidences found
4.2. Construct a timeline with all information.
4.3. For each evidences found use images that prove these evidences.
4.4. Explain evidences importance for the process.
4.5. Identify ownership and possession.
4.5.1. Join information about the individuals involved.
4.6. Indicate conclusions about hypothesis and evidences found.
4.7. Indicate if there were any errors on forensics procedures.

Appendices
Note: All tables are filled with data examples.

Devices Table

Information	Mobile Devices	
	Mobile device 1	Mobile Device n...
Device type	Smartphone	
Manufacturer	Apple	
Model	Iphone 4S A1234	
IMEI	11352066060926230	
Serial Number	123456	
State (On or OFF)	On	
Network Connected? (Mobile network, Wi-FI, Bluetooth	Mobile network and WiFi	
Device ID (label)	SPH01.SIM01.MC01	
Responsible forensics analyst	Fabio Marques	
SIM CARD 1 and label	SIM01	
SIM CARD 2 and label		
Memory Card	MC01	
Conditions	working	
Observations	Battery in good state	
Photos	SPH01.SIM01.MC01-TOP	

Acquisition Table

Device manufacturer and model.	Device ID (label)	Case Number	Forensics Software used	Type of acquisition (Logical of Physical)	Data storage devices?	Type of memory acquired
Apple Iphone 4S A1234	SPH01	A	XRY	Logical	1 SIM card 1 Memory card	Internal and mass storage device memory card

Examination table

Device ID(label)	SPH01.SIM01.MC01		
File Name	File Location	Related Application	Obtained Data
Line.sqlite	/private/var/mobile/ Library/SpringBoard /PushStore/	Line	List of contacts Messages exchanged
Application n...			

Analysis table

Devices Device ID (Label)	Data types																	
	SIM card data	Device info	Contacts	SMS and MMS	Call Registry	User accounts	Application Appendices	Photos and videos	File System	GPS Data	Wi-Fi Data	Bluetooth Data	Databases	Web History	Documents	Calendar	E-mails	Installed Applications
iPhone 4S SPH01.SIM01. MC01	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	WhatsApp Line Skype Signal

																		...

Analysis Hypothesis table

Hypothesis	Approved / Not Approved	Evidence 1	Evidence n...
John send a smartphone photo to Maria thought WhatsApp	Approved	Maria's Smartphone had a smartphone photo in WhatsApp image folder	

References

SWGDE. (2012). Model Standard Operation Procedures for Computer, *0*, 1–41.

Whatson, D., & Jones Andrew. (2013). *Digital Forensics Processing and Procedures*. Elsevier.

Formulation, P. (1994). Guide to Writing Policy and Procedure Documents. *October*, *17*.

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, 386–391. https://doi.org/10.1109/BWCCA.2011.63

Fukami, A., Ghose, S., Luo, Y., Cai, Y., & Mutlu, O. (2017). Improving the reliability of chip-off forensic analysis of NAND flash memory devices. *Digital Investigation*, *14*, S1–S11. https://doi.org/10.1016/j.diin.2017.01.011

Scientific Working Group on Digital Evidence. (2013). SWGDE Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

MURPHY, D. (2011). Cellular Phone Evidence Data Extraction and Documentation. Retrieved from http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2010/07/Cell-Phone-Evidence-Extraction-Process-Development-1.8.pdf

Frade, M. (2016). Mobile Devices Forensics. In *Mobile Devices Forensics*.

Barbara, J. (2007). Documenting Computer Forensic Procedures. Retrieved August 28, 2017, from https://www.forensicmag.com/article/2007/10/documenting-computer-forensic-procedures

Version history
20170512 – first version
20170530 – Procedure structure
20170602 - Procedure structure
20170720 - Improvement on procedure text.
20170820 - Procedure structure
20170822 - Improvement on procedure text.
20170828 - Improvement on procedure text.