Dispositivos *Android*

Filipe Henriques
Mestrado de Cibersegurança e Informática Forense
Instituto Politécnico de Leiria
Leiria, Portugal
2180066@my.ipleiria.pt

Jéssica Pedrosa
Mestrado de Cibersegurança e Informática Forense
Instituto Politécnico de Leiria
Leiria, Portugal
2180067@my.ipleiria.pt

Patrícia Silva
Mestrado de Cibersegurança e Informática Forense
Instituto Politécnico de Leiria
Leiria, Portugal
2180068@my.ipleiria.pt

Tiago Martins
Mestrado de Cibersegurança e Informática Forense
Instituto Politécnico de Leiria
Leiria, Portugal
2182716@my.ipleiria.pt

I. Introdução

No âmbito da unidade curricular de Análise Forense Digital II do mestrado Cibersegurança e Informática Forense, da Escola Superior de Tecnologia e Gestão, do Instituto Politécnico de Leiria, foi elaborado o presente artigo sob o tema "Dispositivos *Android*". Este artigo consiste na exploração de certos aspetos da análise forense a dispositivos móveis *Android*, aplicado a um caso prático.

Será explorada a versão 9 do *Android* que, até à data, é a mais recente, sendo feito um estudo à hierarquia de ficheiros do sistema *Android*, assim como aos tipos de sistemas de ficheiros utilizados, e uma exemplificação destes tópicos aplicados num dispositivo *Android*. Serão também explorados os diferentes métodos de aquisição de dados, as diferenças entre cada um destes e será realizada uma aquisição a um equipamento *Android*, recorrendo a um destes métodos. Uma vez que o cenário selecionado para a fase prático-laboratorial do trabalho está relacionado com o *WhatsApp* (uma aplicação de mensagens instantâneas e chamadas de voz), este será previamente alvo de uma análise, de modo a se compreender alguns aspetos bem como o funcionamento do mesmo. Deste modo, o trabalho passará por entender o funcionamento interno do *Android*, perceber o conceito de análise forense em dispositivos móveis e ainda o funcionamento do *WhatsApp* e de outras aplicações de mensagens instantâneas.

Este relatório está dividido em quatro capítulos, sendo que o capítulo dois consiste no estado da arte, onde serão introduzidos os diversos conceitos explorados neste artigo. O capítulo três será o cenário prático-laboratorial e por fim, o quarto capítulo é constituído pela conclusão do trabalho.

II. Estado da Arte

A. *Breve História do Android*

A *Android Inc*. foi fundada por 4 pessoas, nomeadamente, Rich Miner, Nick Sears, Cohris White, e Andy Rubin em 2003 e em 2005 a *Google* adquiriu a companhia. [1] Mais tarde a *Google* juntou-se a várias empresas, sendo formando essas empresas a *Open Handset Alliance* (*OHA*), que desenvolveu o sistema operativo *Android*. [2] A *Google* lançou pela primeira vez, em 2008, o primeiro dispositivo com o sistema *Android*. [1]

Até ao início de 2011, a *Google* já tinha lançado pelo menos 7 versões *Android*, sendo que todas elas tiveram o nome baseado em doces, uma prática que se mantém até hoje, com exceção da primeira versão que foi lançada. [1]

O *Android* é um dos sistemas operativos mais usados em *smartphones*, tanto em Portugal, como no mundo. A Ilustração 1 - Quantidade de sistemas operativos em dispositivos móveis pelo mundo representa a quantidade de sistemas operativos nos *smartphones*, em todo o mundo.

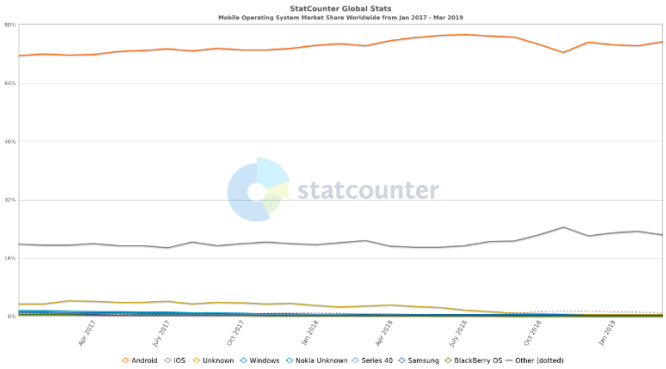

Ilustração 1 - Quantidade de sistemas operativos em dispositivos móveis pelo mundo [3]

A distribuição da quantidade de dispositivos que utilizam as várias versões *Android* está representada na Ilustração 2. Os dados foram recolhidos durante 7 dias em 2018 e todas as versões com menos de 0.1% não irão aparecer.

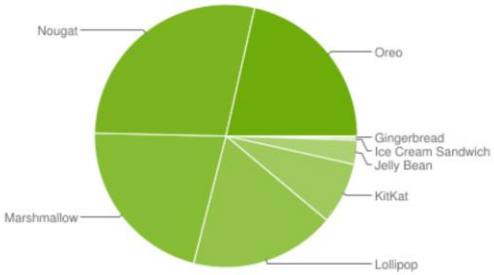

Ilustração 2 - Distribuição das diferentes versões Android nos dispositivos [4]

Como se pode perceber, além do sistema *Android* ser um dos mais utilizados em *smartphones*, as versões que nos dias de hoje são mais populares, são as versões *Nougat*, *Marshmallow*, *Oreo* e *Lollipop*.

B. *Estrutura Interna do Android*

1) *Partições do Android*

O Sistema *Android* está organizado em várias partições. Destas partições, apenas algumas são normalmente acedidas pelo utilizador, enquanto as outras são partições utilizadas pelo sistema.

A estrutura, que normalmente se encontra, consiste nas seguintes partições: [5]

- *boot* – Esta partição contém a informação e os ficheiros necessários para que o dispositivo arranque. Nela está contido o *kernel* e o *RAM disk*.
- *system* – Aqui encontram-se vários ficheiros e diretorias referentes ao sistema operativo, como serviços e programas.
- *recovery* – Esta partição foi desenvolvida com o propósito de permitir a recuperação do sistema no caso deste ficar corrompido, tendo um conjunto de ferramentas para o mesmo.
- *data* – Esta partição contem ficheiros relativos à *ROM*, assim como outos dados de configurações do sistema e das aplicações.
- *cache* – Esta partição é utilizada para guardar informação frequentemente acedida pelo sistema, aplicações e outros programas, assim como alguns *logs* para rapidez de acesso sendo assim uma partição muito valiosa em termos de informação no ponto de vista forense.
- *misc* – Nesta partição estão guardadas várias definições diferentes tais como de *hardware*, *USB* entre outras, assim como informações sobre estados do dispositivo.
- *sdcard* – Nesta partição encontram-se os ficheiros dos utilizadores como as fotografias, os vídeos, as músicas, os contactos, os *SMS*, os ficheiros gerados pelas aplicações transferidas, entre outros ficheiros.

Dentro da partição *sdcard*, existem algumas pastas que são comuns às diversas versões do *Android* e assim como as pastas onde a informação pessoal do utilizador está contida. As pastas são as seguintes:

- *Android* – Dentro desta pasta existem mais duas pastas, a *data* e a *obb*. Nestas pastas é onde estão instaladas as aplicações transferidas entre outros dados gerados pelas mesmas.
- *DCIM* – Aqui é onde todas as fotografias tiradas a partir de uma aplicação com a câmara são guardadas, assim como os vídeos.
- *Pictures* – Esta pasta tem imagens que tenham sido guardadas a partir de aplicações como *Facebook* e outras.
- *Download* – Nesta pasta são guardados todos os ficheiros relativos a *downloads*, seja o *download* a partir do *browser* ou outra aplicação que permita fazer também *downloads*.

2) *Sistema de Ficheiros Android*

Sendo o *Android* baseado em *Linux*, os tipos de sistemas de ficheiros suportadados pelo *Android* serão muito semelhantes aos suportados pelo *Linux*. No entanto, existem alguns tipos específicos ao *Android*. Os tipos de sistemas de ficheiros suportados por um dispositivo podem ser obtidos através da uma *adb shell* com o comando '*$ cat /proc/filesystems*'. Na Ilustração 3 é possível observar os tipos suportados pelo dispositivo *Xiaomi Mi 5*.

Os tipos de sistema de ficheiros utilizados estão dependentes do dispositivo, mas no caso do dispositivo que será utilizado para este projeto, o *Xiaomi Mi 5*, é possível

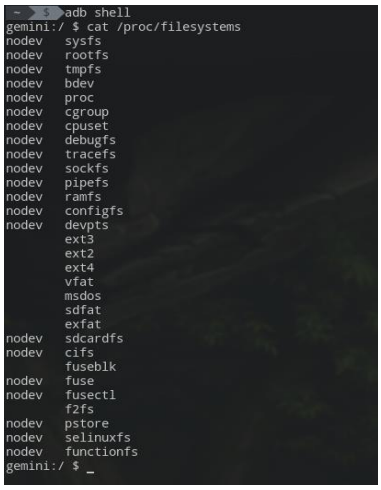

Ilustração 3 - Tipo de ficheiros suportados pelo Xiaomi Mi 5

observar os tipos de sistema de ficheiros utilizados nas diferentes partições através da *adb shell*, com o comando '*$ mount*'. Neste caso, existiam muitos *mountpoints*, mas serão apenas apresentados os que foram considerados fundamentais para o funcionamento básico do *Android*. Na Tabela 1 estão representados alguns dos *mountpoints* e respetivos sistemas de ficheiros e dispositivos. De notar que, a Tabela 1 foi construída através de informações retiradas do *smarthphone Xiaomi Mi 5*.

Tabela 1 - Mountpoints e respetivos sistemas de ficheiros e dispositivos

DISPOSITIVO	MOUNTPOINT	SISTEMA DE FICHEIROS
rootfs	/	rootfs
tmpfs	/dev	tmpfs
proc	/proc	proc
sysfs	/sys	sysfs
selinuxfs	/sys/fs/selinux	selinuxfs
tmpfs	/mnt	tmpfs
/dev/block/sda12	/persist	ext4
/dev/block/sde39	/system	ext4
/dev/block/sde38	/vendor	ext4
tmpfs	/system/etc	tmpfs
/dev/block/sda13	/cache	ext4
/dev/block/sda14	/data	ext4
tmpfs	/sbin	tmpfs
tmpfs	/storage	tmpfs
/data/media	/storage/emulated	sdcardfs
/data/media	/mnt/runtime/default/read	sdcardfs
/data/media	/mnt/runtime/default/write	sdcardfs
/data/media	/mnt/runtime/default/emulated	sdcardfs

O *ext4* (*Extended File System 4*) é vulgarmente utilizado em ambientes *linux* como o tipo principal de sistema de ficheiros. [5] O *sdcardfs* é um sistema de ficheiros do estilo *FUSE* (*Filesystem in Userspace*) que basicamente funciona como um sistema de ficheiros virtuais, onde os dados não são guardados em si, mas sim noutros lugares do sistema de armazenamento, servindo então como uma camada tradutora. [6] O *tmpfs*, como se pode deduzir do nome, é um tipo de sistema de ficheiros para armazenamento temporário. [7] O *rootfs* é uma instância especial do *ramdisk*. [8] O *sysfs* é um *pseudo* sistema de ficheiros que exporta informação de vários subsistemas do *kernel*, dispositivos de *hardware* e *drivers* associadas a módulos do *kernel* carregados para o dispositivo. [9] O *selinuxfs* faz parte do *SELinux Module* (*Security-Enhanced Linux*) que é uma das funcionalidades de segurança que podem ser utilizadas no *linux*. [10] O *proc* ou *procfs* tal como o *sysfs*, é um sistema de ficheiros especial que apresenta informações acerca de processos, entre outras. [11]

3) Hierarquia do Sistema de Ficheiros Android

Neste dispositivo em concreto, o Xiaomi Mi 5, através da *adb shell* com o comando 'ls -lah' com o utilizador *root*, obteve-se a seguinte lista que é a hierarquia de ficheiros do dispositivo:

- .
- ..
- acct
- bin -> /system/bin
- bt_firmware -> /vendor/bt_firmware
- bugreports -> /data/user_de/0/com.android.shell/files/bugreports
- cache
- charger -> /sbin/charger
- config
- d -> /sys/kernel/debug
- data
- default.prop -> system/etc/prop.default
- dev
- dsp -> /vendor/dsp
- etc -> /system/etc
- firmware -> /vendor/firmware_mnt
- init
- init.environ.rc
- init.rc
- init.usb.configfs.rc
- init.usb.rc
- init.zygote32.rc
- init.zygote64_32.rc
- mnt
- odm
- oem
- persist
- plat_file_contexts
- plat_hwservice_contexts
- plat_property_contexts
- plat_seapp_contexts
- plat_service_contexts
- proc
- product -> /system/product
- res
- root
- sbin
- sdcard -> /storage/self/primary
- sepolicy
- storage
- sys
- system
- ueventd.rc
- vendor
- vendor_file_contexts
- vendor_hwservice_contexts
- vendor_property_contexts
- vendor_seapp_contexts
- vendor_service_contexts
- vndservice_contexts

De referir que os diretórios com o prefixo *init*, retêm informação acerca do *ramdisk.*

C. Versão Utilizada para o Trabalho

Para este trabalho será feita a análise à versão 9.0 do *Android*, também conhecido como *Android Pie*. Tal como em grande parte das atualizações das versões do *Android*, esta também apresentou alterações ao nível da interface do utilizador. Esta versão apresenta o protocolo de segurança *DNS over TLS* (*DoT*), que permite encriptar os pedidos *DNS*, o que permite evitar ataques *eavesdropping* e *spoofing*. [12] Também apresenta a *Android Dashboard*, que informa o utilizador acerca do tempo que o mesmo passa ao telemóvel. Para além das referidas, possui também outras funcionalidades novas e suporta o *Vulkan 1.1*, que é uma *API* de computação e gráficos. [13] [14]

Algumas caraterísticas de segurança interessantes desta versão passam por os pedidos das aplicações, por omissão, serem feitos em *HTTPS*; os *backups* desta versão serem encriptados; as aplicações em *background* não terem acesso ao microfone e à câmara do dispositivo, mas também existem novas medidas de segurança relacionadas com os outros sensores do telemóvel. [15]

De realçar, que o dispositivo utilizado será o *Xiaomi Mi 5*.

D. Importância da Análise Forense a Dispositivos Móveis

Com o desenvolvimento tecnológico a que se assiste atualmente, é notório que a sociedade tem presente na sua vida a mais variada forma de tecnologia. Nos últimos anos, conceitos como *Internet of Things*, *Cloud Computing*, *Big Data* bem como os *smartphones* são tendências tecnológicas crescentes. Relativamente aos *smartphones*, é significativamente notório que estes, nos últimos anos, são cada vez mais uma presença assídua no dia-a-dia por diversas razões, estando de certo modo presentes em bastantes atividades do quotidiano. No gráfico apresentado (Ilustração 4 - Utilização de telemóveis em comparação com outros dispositivos) é possível verificar a diferença de percentagens de utilização entre *smartphones*, *desktops* e *tablets*. Conclui-se, por análise do gráfico, que, de facto, é crescente a utilização dos *smartphones*, acabando mesmo por existir um destaque significativo em termos de utilização comparativamente com os restantes.

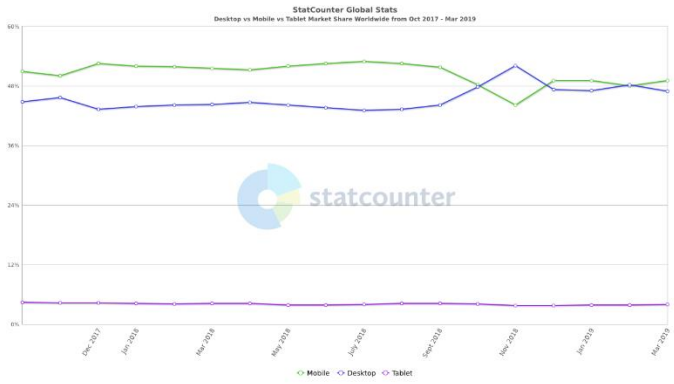

Ilustração 4 - Utilização de telemóveis em comparação com outros dispositivos [16]

Como resultado desta utilização tão frequente, nos dias de hoje, os *smartphones* apresentam uma quantidade de informação considerável, diversificada e valiosa - acerca não só do dispositivo em si, mas também do utilizador do mesmo. Isto leva a que, atualmente, os *smartphones* sejam um elemento relevante a ser alvo de análise no âmbito de investigações digitais, designando-se o referido por análise forense a dispositivos móveis. Segundo a *National Institute of Standards and Technology* (*NIST*), análise forense a dispositivos móveis "(…) é a ciência da recuperação de provas digitais de um dispositivo móvel em condições forenses, utilizando métodos aceites" [17].

O processo de análise forense a dispositivos móveis apresenta um conjunto de fases. A primeira etapa, a apreensão do dispositivo, consiste principalmente em se proceder ao isolamento do dispositivo em relação à rede. De seguida, ocorre a aquisição que consiste na identificação e extração de dados e, por fim, ocorre a fase de examinação e análise dos mesmos. De uma forma geral, com a aquisição de dados presentes em *smartphones*, poderá ser possível ter acesso a fotografias, conversas recentes, dados de localização, histórico de chamadas (recebidas, efetuadas e não atendidas), histórico de navegação na Internet, cookies, listas de tarefas, dados apagados, informações acerca da conexão *wifi*, entre outros. [18]

Tal como já foi mencionado anteriormente, um dos primeiros passos a se concretizar no processo de análise forense a dispositivos móveis é a realização do isolamento do dispositivo em relação à rede de modo a evitar-se alterações nos dados existentes no dispositivo bem como evitar *remote locks* ou *wipes*. O processo de isolamento pode ser efetuado de dois modos distintos. A primeira forma, que é mais objetiva e simples, passa por colocar-se o *smartphone* em modo avião. Já outras formas alternativas consistem em remover o cartão *SIM* e desligar a conexão *wifi*, usar uma faraday *cage* e ainda usar os *signal jammers*. [19]

Relativamente à aquisição de dados em *smartphones*, há três métodos, nomeadamente o método físico, o lógico e ainda o manual. Na análise forense a dispositivos móveis, o método físico consiste em se criar uma cópia exata *bit-a-bit* do sistema de ficheiros, adquirindo-se informações do dispositivo através do acesso direto à memória *flash* – memória não volátil que é utilizada, por exemplo, em cartões de memória e *pens USB*. Os dados extraídos com este método normalmente estão na forma de dados brutos o que faz com que não sejam legíveis ao olho humano de imediato. É de referir que para a utilização deste método de extração, geralmente recorre-se ao método *JTAG* (*Joint Action Test Group*) que permite efetuar uma aquisição física de forma não invasiva. [20] Um dos grandes benefícios deste tipo de aquisição passa precisamente pelo facto de esta permitir adquirir todos os dados presentes no dispositivo – incluindo tanto os que tenham sido apagados previamente bem como a informação presente em espaço não alocado. Já o método de aquisição lógica passa por sincronizar o conteúdo de um *smartphone* com um computador, através das *APIs* do fabricante do equipamento. Através deste método serão extraídos os ficheiros existentes num armazenamento lógico, como por exemplo, de uma partição do sistema de ficheiros. Neste método é relevante que o investigador tenha em atenção se, por alguma razão, o *smartphone* é modificado durante o processo de aquisição. Este tipo de aquisição é geralmente efetuado através da *adb shell*. É de mencionar que a quantidade de dados recolhidos está diretamente dependente do *smartphone* ter ou não permissões *root*. [21] Poder-se-á obter dados como mensagens de texto, histórico de chamadas, lista das aplicações instaladas (com versão), detalhes de localização (dados do *GPS*) ou imagens; é de ter em conta que os dados existentes em espaço não alocado não são recuperados. [5] [22]

Quando de facto não há outra forma possível de adquirir informação do *smartphone* ou quando a informação que se pretende obter/verificar é reduzida, poder-se-á recorrer ao método de aquisição manual. Este consiste em visualizar o conteúdo do *smartphone* em causa e, geralmente, implica o uso dos botões, do teclado ou do *touchscreen*, sendo que as ações executadas podem ser gravadas com uma câmara externa. [17] Não se poderá ainda ignorar o facto de este ser um método de aquisição muito dispendioso em termos de tempo e que o mais pequeno erro poderá levar à perda de dados cruciais à investigação.

Por muito que já sejam efetuadas atualmente análises forenses a dispositivos, esta é uma área que ainda enfrenta alguns desafios como por exemplo a necessidade de possuir o material/*hardware* (como conectores) adequado para cada *smartphone*. [23]

E. Processo Geral de Instalação de uma ROM Customizada

Para dispositivos relativamente recentes, o processo inicia-se por conseguir obter permissões *root* no dispositivo. Dependendo de o dispositivo ser suportado ou não (*https://twrp.me/Devices/*), o próximo passo passa por instalar a aplicação do *TWRP* (*https://twrp.me/app/*), que até ao momento, encontra-se na *Google Play Store*. A partir da aplicação, é possível instalar uma *recovery* customizada, que irá permitir a instalação da *ROM* customizada. Dependendo da versão *Android* do dispositivo, poderá ser necessário instalar a última versão da *ROM* do fabricante antes de instalar a *ROM* customizada pretendida. Para *ROMs* customizadas, a mais popular e com atualizações frequentes é a *Lineage OS*. Para instalar uma *ROM* baseada em *Lineage OS*, no caso de o dispositivo ser suportado, basta ir ao site oficial do *Lineage* na parte de *downloads* (*https://download.lineageos.org*), selecionar o dispositivo e fazer *download* da última versão. Uma particularidade das *ROMs* baseadas em *Lineage OS*, é que não vêm com os serviços da *Google Play Store* nem com aplicações da *Google*. Para contornar isto, é possível instalar um pacote com os serviços da *Google Play* e outras aplicações

da *Google*, que não estejam disponíveis na *Google Play Store*. Existem várias implementações deste método, no entanto, a mais popular é o projeto *OpenGapps* (*https://opengapps.org/*). No site do *OpenGapps* seleciona-se a arquitetura do processador, seguido da versão *Android* da *ROM* a instalar, e o pacote em si. Existem vários pacotes desde o "*pico*" que apenas contêm o mínimo para os serviços da *Google Play* ficarem funcionais, até ao "*Aroma*", que é um instalador gráfico que permite selecionar entre todas as aplicações disponíveis pelo projeto *OpenGapps*. Poderá também ser instalado um *root manager* de modo a ter permissões *root* no telemóvel para assim desbloquear funcionalidades adicionais. Um dos *root* managers mais populares é o *Magisk Manager* (*https://magiskmanager.com*), e é relativamente suportado pela maior parte dos dispositivos/versões *Android* recentes. O *Magisk Manager* consiste numa aplicação normal *Android* onde se pode gerir o acesso a permissões *root* a determinadas aplicações que as requeiram, assim como outras funcionalidades adicionais. No entanto, para o *Magisk Manager* funcionar, é necessário ter o *Magisk Framework* instalado, em que o processo da instalação deste é semelhante à de instalação de uma *ROM* customizada. [24]

F. Aplicações de Mensagens Instantâneas

1) WhatsApp

O *WhatsApp* é uma aplicação *freeware* de partilha de mensagens entre diversos tipos de plataformas, e tem como metodologia de comunicação, *VoIP*. Esta aplicação foi criada pela empresa *WhatsApp Inc.* fundada por antigos trabalhadores do *Yahoo*, Jan Koum e Brian Acton em 2009, mais recentemente em 2014, o *WhatsApp Inc.* foi adquirida pelo *Facebook*. [25] [26] O *WhatsApp* para além de disponibilizar a funcionalidade de *SMS* básica, esta também apresenta funcionalidades para elaborar conversas em grupo, manter estas conversas sincronizadas entre diversos dispositivos, efetuar chamadas de voz ou de vídeo, partilhar ficheiros multimédia como imagens, vídeos, gravações de voz, ou documentos com tamanho não superior a 100 *MB*. E, em cima de todas estas funcionalidades, o *WhatsApp* fornece segurança na forma de encriptação de ponto-a-ponto assim que é instalada a aplicação. Todas estas funcionalidades tiram partido da *internet* sempre que possível, pelo que tornam estas funcionalidades gratuitas, caso um utilizador queria usar a aplicação sem internet este poderá ter de pagar taxas pelo serviço, isto dependendo da operadora. [27] [28]

Esta aplicação usa uma versão customizada do *Extensible Messaging and Precense Protocol*, XMPP, que é uma norma aberta ao público. É através deste protocolo que o WhatsApp efetua as comunicações *VoIP*. [29] Todas as chaves são geradas no lado do servidor por forma a evitar a criação de par de chaves inseguras. Estas chaves são por sua vez usadas no sistema de encriptação ponto-a-ponto, este sistema é essencialmente o protocolo *Signal* criado pelo *Open Whisper Systems*. [30]

Os servidores do *WhatsApp* evitam guardar dados relativos aos conteúdos das conversas na aplicação cliente, desta forma ele segue um mecanismo de "*store and forward*" para a troca de mensagens entre utilizadores. A utilidade deste mecanismo é a de possibilitar conversas continuas e de forma privada entre dispositivos, mesmo se estes não estiverem disponíveis, por exemplo, quando um utilizador envia uma mensagem, esta segue primeiro para os servidores do *WhatsApp* onde fica guardada temporariamente, assim que é possível enviar a mensagem para o destinatário o servidor envia e depois elimina essa mensagem do servidor. Caso o servidor não consiga enviar a mensagem dentro de 30 dias, o servidor eliminará a mensagem. Desta forma, todos os dados do *WhatsApp* são apenas armazenados de forma permanente no dispositivo cliente, mais concretamente na pasta "*Android/data/data/com.whatsapp/*" do armazenamento interno *Android*. Por estes motivos quando um utilizador necessitar de restaurar o histórico do seu *chat*, o *WhatsApp* oferece opções para exportar e importar esses dados. [31] [32] Em termos de conteúdo multimédia, conteúdo que tenha um tamanho máximo de 100 *MB* será enviado de forma normal, caso o tamanho ultrapasse o valor máximo, o *WhatsApp* oferece uma lista de outras aplicações recomendadas, como o *Dropbox* ou o *Google Drive*, pela qual será enviado o conteúdo multimédia. Tudo isto significa que o conteúdo da aplicação relativo às conversas na aplicação será guardado no dispositivo cliente. [33] Mas, do ponto de vista forense, o *WhatsApp* e outras as aplicações de partilha de mensagens como o *Skype*, o *Viber*, e o *Tango* produzem artefactos como a data de instalação, os dados de tráfego, os dados de conteúdo, os dados do perfil de utilizador, os dados de autenticação de utilizador, os ficheiros partilhados, a base de dados de contactos, e os dados de localização, que têm valor numa análise forense digital. [17]

2) Facebook Messenger

O *Facebook Messenger*, ou simplesmente *Messenger*, é uma aplicação *freeware* de mensagens e foi desenvolvida pelo *Facebook* em 2008. Tal como o *WhatsApp*, o *Messenger* usava também uma versão personalizada do protocolo XMPP para as suas comunicações, mas atualmente este usa na sua versão móvel o protocolo MQTT, e HTTP na versão para *browser*. [34] [35] Atualmente esta aplicação apresenta duas versões, o *Messenger* e o *Messenger Lite*, sendo que a principal diferença entre elas está no seu tamanho e no número de funcionalidades que cada uma oferece. A versão *Messenger* pode ser considerada como a versão principal por esta apresentar todas as funcionalidades existentes, nomeadamente: partilhar mensagens de texto, vídeos, fotos, mensagens de voz, *stickers*, e GIFs; efetuar chamadas de voz e vídeo; aplicar filtros, máscaras e efeitos nas chamadas de vídeo; entrar em contacto com pessoas com ou sem conta do *Facebook*; visualizar quando pessoas estão online, e ver quando uma mensagem foi lida; criar *Stories* e ver outras; personalizar os chats; participar em jogos com amigos; efetuar pagamentos ao adicionar um cartão de débito ou conta de *Paypal*; e partilhar a localização do dispositivo cliente. [36] [37]

Existe também uma funcionalidade opcional para efetuar mensagens em modo confidencial, "*Secret Conversations*". Aqui os utilizadores podem estabelecer uma comunicação encriptada de ponto-a-ponto utilizando o protocolo *Signal* para tal. [38]

Ao contrário do *WhatsApp*, o *Facebook Messenger* guarda o histórico das conversas tanto nos servidores do *Facebook* como nos dispositivos-cliente. Segundo a política de dados do *Facebook*, e na qual esta aplica-se tanto ao *Facebook*, como ao *Instagram* e ao *Messenger*, todos os dados recolhidos nestas aplicações são armazenados nos servidores e tratados de acordo com o Regulamento Geral da Proteção de Dados. [39] Todos os dados nesta aplicação podem ser encontrados

na pasta "*Android/data/data/com.facebook.orca*" nos dispositivos *Android*.

3) WhatsApp versus Facebook Messenger

Em termos de popularidade mundial, o *WhatsApp* apresenta ser a aplicação no topo destacando-se com um número de utilizadores de cerca de 1500 milhões, estando depois em segundo lugar o *Facebook Messenger* com o número perto de 1300 milhões (ver Ilustração 5 -).

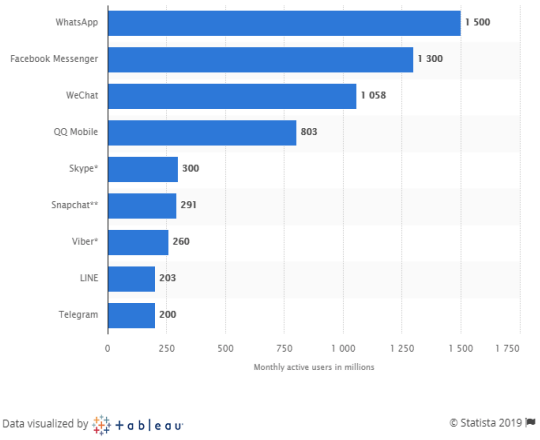

Ilustração 5 - Ranking das aplicações de mensagens mais utilizadas [40]

Em termos de funcionalidades o *Messenger* apresenta mais funcionalidades ao comparar com o *WhatsApp*, e apesar disto não é o *Messenger* que apresenta ter mais utilizadores. Existem vários motivos que elevaram a popularidade do *WhatsApp* acima do *Messenger*, nomeadamente: o suporte do *WhatsApp* para várias plataformas; o facto de as chamadas de voz utilizando sinais fracos de *Wi-Fi* funcionavam melhor no *WhatsApp* do que no *Messenger*; e outros aspetos que o *Messenger* não tinha mas, que o *WhatsApp* tinha anteriormente, como o facto de não ser necessário a criação de uma conta de utilizador. [41] Mas, o que diferencia o *WhatsApp* do *Messenger* pode ser resumido em dois motivos: o facto do *WhatsApp* mostrar ser uma aplicação mais amigável a utilizadores novos, por exemplo para usar o *WhatsApp* não é necessário criar uma conta de utilizador; e a segurança e confidencialidade nas comunicações é estabelecido com a encriptação de ponto-a-ponto de forma não opcional. O facto da privacidade dos dados no *WhatsApp* também é um fator importante, ao contrário do *Messenger*, o *WhatsApp* não guarda nenhum histórico das conversas de forma permanente. [42]

III. Referências

[1] J. Callaham, "The history of Android OS: its name, origin and more," 3 julho 2018. [Online]. Available: https://www.androidauthority.com/history-android-os-name-789433/.

[2] G. C. K. Jeff Lessard, "Android Forensics: Simplifying Cell Phone Examinations," *Small Scale Digital Device Forensic Journal*, pp. 1-12, 2010.

[3] "Mobile Operating System Market Share Worldwide - March 2019," StatCounter GlobarStats, [Online]. Available: http://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201701-201903. [Acedido em 3 abril 2019].

[4] "Distribution dashboard," [Online]. Available: https://developer.android.com/about/dashboards?fbclid=IwAR3Ewcja2d80p77_okz_gD4G3OnTFkLG1kV39-q40JnC3wEhQZjYb997HlQ.

[5] H. Mahalik, S. Bommisetty e R. Tamma, Practical Mobile Forensics, Packt Publishing Ltd, 2016.

[6] M. Rahman, "Diving into SDCardFS: How Google's FUSE Replacement Will Reduce I/O Overhead," 17 janeiro 2017. [Online]. Available: https://www.xda-developers.com/diving-into-sdcardfs-how-googles-fuse-replacement-will-reduce-io-overhead/.

[7] "tmpfs," [Online]. Available: https://en.wikipedia.org/wiki/Tmpfs.

[8] "rootfs," 27 dezembro 2010. [Online]. Available: https://wiki.debian.org/rootfs.

[9] "sysfs," [Online]. Available: https://en.wikipedia.org/wiki/Sysfs) .

[10] "NB LSM," [Online]. Available: http://selinuxproject.org/page/NB_LSM.

[11] "procfs," [Online]. Available: https://en.wikipedia.org/wiki/Procfs.

[12] "DNS-over-TLS," 9 janeiro 2019. [Online]. Available: https://developers.google.com/speed/public-dns/docs/dns-over-tls.

[13] "Vulkan," [Online]. Available: https://www.khronos.org/vulkan/.

[14] "Android version history," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Android_version_history. [Acedido em 3 abril 2019].

[15] J. Knight, "12 Important Privacy & Security Features Google Added to Android 9.0 Pie," 30 agosto 2019. [Online]. Available: https://android.gadgethacks.com/news/12-important-privacy-security-features-google-added-android-9-0-pie-0184332/.

[16] "Desktop vs Mobile vs Tablet Market Share Worldwide - March 2019," StatCounter GlobarStats, [Online]. Available: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide/#monthly-201710-201903. [Acedido em 3 abril 2019].

[17] N. D. W. Cahyani, N. H. A. Rahman, W. B. Glisson e K.-K. R. Choo, "The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Storage Service and Communication Apps," Springer Science + Business Media New York, 2016.

[18] D. Kostadinov, "Introduction: Importance of Mobile Forensics," INFOSEC, 11 janeiro 2019. [Online]. Available: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/?fbclid=IwAR2JYKoO45b5gu7ocGVpAMNM

sBuMX-nfbIXnDSlJ2SKKRmrDVeWzgoNP6hY. [Acedido em março 2019].

[19] M. Frade e B. Rodrigues, "Mobile Devices (MCIF - Digital Forensic Analysis 2)," Leiria (Insituto Politécnico de Leiria), 2019.

[20] "What is JTAG?," Corelis, [Online]. Available: https://www.corelis.com/education/tutorials/jtag-tutorial/what-is-jtag/. [Acedido em 5 abril 2019].

[21] "Android Debug Bridge," Android Developers, [Online]. Available: https://developer.android.com/studio/command-line/adb. [Acedido em 5 abril 2019].

[22] R. Tamma e D. Tindall, Learning Android Forensics, Packt Publishing Ltd, 2015.

[23] T3K-Forensics, "10 CHALLENGES IN MOBILE FORENSICS," [Online]. Available: http://www.t3k-forensics.com/allgemein-en/10-main-challenges-in-mobile-forensics2/. [Acedido em abril 2019].

[24] "Install LineageOS on gemini," The LineageOS Project, 27 março 2019. [Online]. Available: https://wiki.lineageos.org/devices/gemini/install. [Acedido em 5 abril 2019].

[25] WhatsApp Inc., "About WhatsApp," [Online]. Available: https://www.whatsapp.com/about/. [Acedido em 6 3 2019].

[26] P. Olsen, "Exclusive: The Rags-To-Riches Tale Of How Jan Koum Built WhatsApp Into Facebook's New $19 Billion Baby," 2 2 2014. [Online]. Available: https://www.forbes.com/sites/parmyolson/2014/02/19/exclusive-inside-story-how-jan-koum-built-whatsapp-into-facebooks-new-19-billion-baby/#61ff24032fa1. [Acedido em 6 3 2019].

[27] WhatsApp Inc., "Making voice calls," [Online]. Available: https://faq.whatsapp.com/en/android/28000016/?category=5245237. [Acedido em 6 3 2019].

[28] WhatsApp Inc., "WhatsApp Features," [Online]. Available: https://www.whatsapp.com/features/. [Acedido em 6 3 2019].

[29] A. Jagtap, "What is the protocol used by WhatsApp?," Quora, [Online]. Available: https://www.quora.com/What-is-the-protocol-used-by-WhatsApp. [Acedido em 6 3 2019].

[30] WhatsApp, "WhatsApp Encryption Overview," 19 12 2017. [Online]. Available: https://www.whatsapp.com/security/. [Acedido em 6 3 2019].

[31] WhatsApp Inc., "Saving your chat history," [Online]. Available: https://faq.whatsapp.com/en/android/23756533/?category=5245251. [Acedido em 6 3 2019].

[32] G. Rathee, "Explore WhatsApp Clock Sign, Single Tick, Double Tick," 25 7 2015. [Online]. Available: http://digitalperiod.com/explore-whatsapp-clock-sign-and-tick/. [Acedido em 6 3 2019].

[33] WhatsApp Inc., "Sending media, documents, location and contacts," [Online]. Available: https://faq.whatsapp.com/en/android/23112542/?category=5245251. [Acedido em 6 3 2019].

[34] V. Loh, "Which protocol does Facebook use for its messages?," Quora, [Online]. Available: https://www.quora.com/Which-protocol-does-Facebook-use-for-its-messages. [Acedido em 27 3 2019].

[35] knolleary, "MQTT used by Facebook Messenger," MQTT.org, 12 8 2011. [Online]. Available: https://mqtt.org/2011/08/mqtt-used-by-facebook-messenger. [Acedido em 27 3 2019].

[36] Facebook Messenger, "Conversations come to life on Messenger," Facebook, [Online]. Available: https://www.messenger.com/features. [Acedido em 27 3 2019].

[37] M. Hendrickson, "Facebook Chat Launches, For Some," TechCrunch, [Online]. Available: https://techcrunch.com/2008/04/06/facebook-chat-enters-pre-release-beta/?guccounter=1&guce_referrer_us=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_cs=bBJKWAn7G4q-MztZfc6oYQ. [Acedido em 27 3 2019].

[38] A. Greenberg, ""You Can All Finally Encrypt Facebook Messenger, So Do It," Wired, 4 10 2016. [Online]. Available: https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/. [Acedido em 27 3 2019].

[39] Facebook, "Política de Dados," Facebook, [Online]. Available: https://www.facebook.com/policy.php. [Acedido em 28 3 2019].

[40] M. Iqbal, "WhatsApp Revenue and Usage Statistics (2019)," BusinessofApps, [Online]. Available: http://www.businessofapps.com/data/whatsapp-statistics/. [Acedido em 8 3 2019].

[41] Quora, "Why are people choosing WhatsApp Messenger over Facebook Messenger? What can WhatsApp offer that Facebook Messenger does not?," Quora, [Online]. Available: https://www.quora.com/Why-are-people-choosing-WhatsApp-Messenger-over-Facebook-Messenger-What-can-WhatsApp-offer-that-Facebook-Messenger-does-not. [Acedido em 29 3 2019].

[42] S. Hill, "The best text messaging apps for Android and iOS," Digital Trends, [Online]. Available: https://www.digitaltrends.com/mobile/best-text-messaging-apps/. [Acedido em 8 3 2019].