São Paulo, Brazil
October 29-30, 2018

The Tenth International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2018006 or http://dx.doi.org/10.5769/C2018006

Uma Revisão das Técnicas Forenses Aplicadas aos Dispositivos Móveis

Marjori Naiele Mocelin Klinczak[1]

(1) Paraná Pericias, Email: mnmk.lvseg@gmail.com

Abstract: Forensic science makes use of forensic techniques to provide legal evidence for various investigations without the evidence being contaminated or modified. In this way, and with the great growth of crimes involving computers and cell phones, computer forensics techniques were applied. In this way we wish to present a review of the extraction techniques that are being used in mobile devices, addressing the issue of data preservation and the challenges of this field, as well as presenting a brief state of the art and the architecture of the main operating systems available in the market.

Key words: Digital forensics, Mobile devices, Data extraction.

I. Introdução

A popularização de equipamentos como computadores e celulares fez com que esses dispositivos passassem a fazer parte do dia a dia das pessoas. Porém esse crescimento fez com que também aumentasse o número de práticas ilícitas que podem ser cometidas com o uso desses aparelhos.

Uma pesquisa realizada pela pela Fundação Getúlio Vargas [1] demonstra que o Brasil já tem mais *smartphones* ativos que pessoas, sendo 220 milhões de celulares ativos no país contra 207,6 milhões de habitantes, de acordo com os dados do IBGE. A pesquisa também aponta que em torno de 70% dos aparelhos utilizados para conexão com a internet em nosso país são *smartphones*.

Outro fator que podemos apontar como influenciador do crescimento do uso dos telefones celulares é o crescente número de recursos disponíveis em um mesmo aparelho, que vai desde fazer e receber ligações, até utilizar redes sociais, tirar fotos, ouvir música, GPS, utilizar diversos aplicativos, entre outros.

Porém todo esse crescimento também acaba atraindo pessoas com más intenções e que procuram um novo meio para aplicar golpes, segundo um relatório da Norton Cyber Security [2], em 2017 o Brasil se tornou o segundo país com maior número de casos de crimes cibernéticos, o que afeta 62 milhões de pessoas, ficando atrás somente da China.

Entre os diversos tipos de ataques que podemos citar, os principais, segundo esse relatório são: ter um dispositivo infectado por vírus, ter uma senha pessoal comprometida, fraude em cartão de crédito, acesso não autorizado a emails ou redes sociais, entre diversos outros tipos de problemas.

De acordo com [4], os dados coletados de celulares estão se tornando a primeira fonte de evidências em investigações, e com o crescimento de crimes digitais, foi necessário criar

métodos de coleta que preservem e permitam a análise das evidências, de forma que os autores possam responder pelos seus crimes.

Surgiu então, segundo [3], a Análise Forense em Dispositivos Móveis, que faz uso das técnicas da ciência forense para capturar e analisar evidências legais para investigações relacionadas.

A extração de evidências de celulares também se torna um desafio, devido a diversividade dos dados que podem ser encontrados (fotos, logs do sistema e de aplicativos, áudio, video, arquivos de memória, entre outros) e também devido a facilidade com que evidências podem ser modificadas, onde um programa pode, por exemplo, através de uma conexão wifi deletar todo o conteúdo de um dispositivo, ou então a retirada da bateria do aparelho pode comprometer os registros de data/ hora de ligações e SMS's, além de apagar conteúdos que estão na memória.

Temos então como objetivo desse trabalho discutir as etapas de extração e análise de dados de dispositivos mobile, demonstrando seus desafios frente a técnicas forenses aplicadas em computadores, como também apresentar a evolução dos principais sistemas operacionais, e por fim, apresentar alguns trabalhos relacionados encontrados na literatura.

Na próxima seção abordaremos a evolução dos dois principais sistemas operacionais disponíveis no mercado hoje, Android e iOS e posteriormente, o processo de extração e análise dos dados.

2. Técnicas Forenses Aplicadas aos Dispositivos Móveis

A ideia de um aparelho que pudesse fazer ligações surgiu em 1947, por [6], porém tornou-se apenas um conceito devido a baixa tecnologia da época. Somente em 1973 foi feita a primeira ligação via telefone celular [7] e a Motolola tornou-se a principal fabricante de celulares [8], onde em 1983 começou a vender o modelo DynaTAC 800x por um alto valor.

Com o passar dos anos, a tecnologia se tornou mais acessível e surgiram diversos outros modelos com diversas funcionalidades, sendo que hoje os novos aparelhos possuem diversos tipos de conexão e uma intensa troca de dados [8].

2.1. Sistemas Operacionais Móveis

O sistema operacional é responsável por fazer a ligação entre o hardware e software de um dispositivo, e segundo a Figura 1, temos o Android e iOs como principais sistemas operacionais disponíveis no mercado. Cada um dos sistemas tem particularidades que afetam a forma como será feita sua análise.

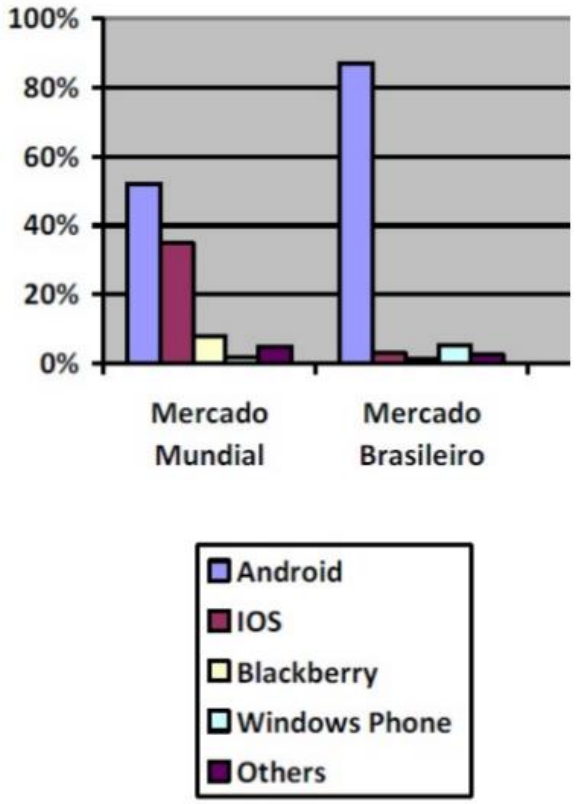

Figura 1: Popularidade dos sistemas mobile a nível Brasil e Mundo [5].

2.1.1. Android

O Android é um sistema operacional baseado em Linux que foi adquirido pela Google em 2005, tendo iniciado em 2003 com a Android Inc., uma empresa de Palo Alto, Califórnia, USA.

Sua principal característica e motivo de sua popularidade é justamente seu núcleo baseado em Linux, pois seu código fonte aberto permite que diversos desenvolvedores e empresas possam criar e corrigir funcionalidades e falhas na plataforma [9].

Na Figura 2 apresentamos a arquitetura do sistema operacional, sendo sua primeira camada a mais abstrata e onde os desenvolvedores vão operar, até mesmo quando criarem aplicações que se relacionem com o hardware, pois o acesso é através de bibliotecas já disponibilizadas. Na segunda camada temos o Framework, que disponibiliza acesso dos serviços ao kernel, como por exemplo para executar chamadas telefônicas, receber notificações, acessar a câmera, entre outros. Na
camada de antecede o núcleo do Android, temos as bibliotecas mencionadas que darão acesso ao kernel as aplicações, como funções e multimídia, e por fim, na última camada temos o kernel, que é responsável pelo gerenciamento do sistema como um todo, incluindo memória, aplicativos, armazenamento, entre outros.

Figura 2: Arquitetura do sistema Android [10].

2.1.1. iOS

O iOs foi lançado em 2007 pela Apple, sendo um sistema que foi desenvolvido para o Iphone e que até o lançamento não tinha um novo, dessa forma foi chamado de iPhone Operating System (iOS) [13]. O sistema foi baseado no então já existente Mac OX X, que se tornou o principal sistema da empresa, sendo utilizado em todos os produtos [11].

A arquitetura do iOs é de certa forma similar a do Android, pois também trabalha com 4 camadas e não permite o acesso direto do desenvolvedor ao hardware, sendo que isso é feito através de bibliotecas que estão na terceira camada.

As camadas são apresentadas na Figura 3, na primeira dá-se a interação com os desenvolvedores, na segunda temos as mídias em geral, como áudio, imagens e video. Na terceira camada temos as bibliotecas que permitem acesso aos mais diversos serviços, e por fim, na última camada temos o núcleo do sistema que faz todo o gerenciamento da energia, aplicativos, armazenamento, entre outros.

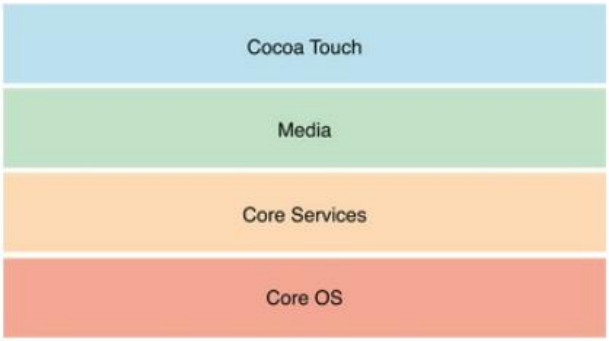

Figura 3: Arquitetura do sistema iOs [12].

2.2. Perícia Forense em Dispositivos Móveis

A ciência forense consiste no uso de técnicas forenses para providenciar evidências que possam ser aceitas como provas válidas no meio jurídico [3]. Dessa forma a análise forense em dispositivos móveis é a ciência que visa a recuperação de evidências digitais de um celular [14], de forma a preservar e não contaminar os dados digitais [4].

O forense digital tem crescido muito nos últimos anos [15] devido a popularização dos aparelhos, e tem aplicação dos mais diversos casos, desde disputas domésticas até em análises de acidentes de carro, pois o log do sistema pode mostrar se o motorista estava utilizando o aparelho no momento do acidente ou não [14].

Os principais desafios consistem no grande volume de armazenamento de dados que

cada vez aumentam mais, e também na diversidade de dados (desde histórico de navegação da internet, logs de sistema, registros de chamadas, dados de aplicativos, entre outros) [4] e [14]. Outro desafio consiste que a evidência não pode ser modificada, o que se tratando de telefones celulares é mais complexo que em um computador.

A Figura 4 apresentamos um quadro dividindo as etapas que envolve uma pericia em mobile.

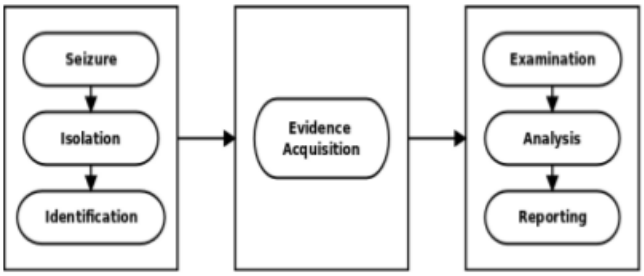

Figura 4. Etapas na investigação forense em dispositivos mobile [4].

2.2.1. Preservação dos Dados

Antes de iniciar a coleta de evidências temos que nos certificar que a preservação dos dados será feita, temos então os seguintes detalhes relacionados ao isolamento do aparelho de interferências externas [14] e [4]:

• Um aparelho ligado deve ser mantido ligado, de forma a não perder registros que estão na memória;

• O aparelho deve ser desconectado de qualquer wifi para não ocorra acesso remoto e o dispositivo seja formatado ou então para que informações não sejam apagadas;

• O aparelho deve ser isolado de qualquer telecomunicação (3G, 4G, GSM, entre outros) e do GPS;

• A bateria deve ser mantida carregada;

• O aparelho deve ser protegido de influências externas, tal como o recebimento de mensagens ou ligações;

• Em caso do aparelho estar desligado, sua bateria não pode ser retirada, pois pode alterar a hora e data do sistema, e dessa forma comprometer as evidências, o mesmo para o cartão SIM, que não deve ser retirado;

• Todos os cabos e cartões devem ser coletados.

Em geral, caso o aparelho esteja ligado pode-se colocar o aparelho em modo avião, de forma a desligar as telecomunicações e wifi. Mas também pode-se pedir o cancelamento ou bloqueio do número de telefone na operadora ou então utilizar uma caixa de Faraday, porém esses métodos não desligam a wifi, por exemplo.

2.2.2. Aquisição dos Dados

A etapa de aquisição pode ser feita de 3 formas, manual, por aquisição lógica ou física, explicaremos as 3 formas adiante.

2.2.2.1. Aquisição Manual

Esse tipo de aquisição geralmente é feita quando o aparelho não é compatível com nenhuma ferramenta forense [14], e consiste na navegação do dispositivo e coleta manual de dados tais como fotos e ligações. Não possibilita uma análise aprofundada pois não permite acesso ao log do dispositivo, nem a dados que já foram excluídos.

Geralmente é utilizado apenas para que o perito tenha ideia do tipo de conteúdo que tem no aparelho, tais como pastas, aplicativos, entre outros.

2.2.2.2. Aquisição Física

Esse tipo de aquisição copia bit-a-bit os dados, de forma a fazer uma cópia idêntica para que o perito possa trabalhar sem se preocupar em comprometer a evidência.

Esse tipo de extração também é capaz de copiar falhas no equipamento original e binários, que são responsáveis por registrar dados excluídos, por exemplo.

O ideal é que seja utilizado um hardware específico para fazer a cópia. Para a extração dos dados de um cartão SIM é necessário um hardware específico também [4].

2.2.2.3. Aquisição Lógica

Nesse tipo de aquisição o aparelho é sincronizado com o computador, para o Android é utilizado o ADB, disponível no SDK da Google para fazer a conexão e para que sejam acessadas as informações do dispositivo. Para o iOs temos a ferramenta *libimobile device*.

Pode-se por exemplo extrair todo o histórico de mensagens, ligações e também pode-

se copiar as bases de dados de aplicativos em específico, para posterior análise.

2.2.3. Exame e Análise

A última etapa consiste em analisar as informações coletadas, para isso existem diversas ferramentas que podem auxiliar. Cada análise depende do problema e dos quesitos que o perito necessita responder, e por fim ele deve elaborar o laudo respondendo todas as indagações que lhe foram feitas.

A cópia dos dados também deve ser mantida.

3. Trabalhos Relacionados

Apesar do tema ainda ser recente, já encontramos uma considerável literatura a respeito do assunto, demonstrando sua importância. Abaixo iremos apresentar algumas pesquisas encontradas.

A autora [17] apresenta a arquitetura de 5 sistemas operacionais, Android, iOs, Blackberry, Windows Phone e Symbiam. Ela também apresenta algumas ferramentas forenses e suas características, entre elas: EnCase, FTK, Oxygen Forensic Suite, entre outros.

Os autores [16] apresentaram a forma de extração de dados no sistema operacional Android, descrevendo não apenas a forma de coleta de evidências mas também como proceder no caso dos aparelhos com e sem bloqueio. Por fim finalizaram através da demonstração de 4 estudos de caso baseados em diferentes características, como por exemplo: possuir ou não acesso root, aparelhos ligados e desligados e com e sem cartão de memória, do qual, em todos os casos conseguiram obter os dados como registro de ligações, mensagens, imagens, entre outros.

No trabalho de [18], os autores procuraram examinar o conteúdo de redes sociais (Facebook, Twitter, MySpace) em 3 diferentes modelos de celulares (Blackberry, Android e Iphone 4). A metodologia empregada consistiu em instalar as redes sociais em cada um dos aparelhos, utilizar as mesmas como se fosse um usuário comum, e após isso começaram com a análise forense, primeiro fazendo uma imagem de cada um dos dispositivos e depois, através do uso da ferramenta EnCase procuraram analisar a memória interna de forma a avaliar que dados conseguiriam encontrar. Apenas nos celulares modelo Blackberry não foi possível encontrar dados, enquanto que no Iphone 4 e Android eles encontraram uma vasta quantidade de dados, conforme apresentamos na Figura 5.

Smartphone	Application	Description
BlackBerry	Facebook	Not found
BlackBerry	Twitter	Not found
BlackBerry	MySpace	Not found
iPhone	Facebook	User and friend data incl. contact details and profile picture URLs Photo uploads Comments posted Timestamps All previously logged in users Friends with active chat sessions
iPhone	Twitter	For user and people followed: User names Profile picture URLs Tweets posted Timestamps
iPhone	MySpace	User name/Password Posted comments Timestamps
Android	Facebook	User and friend data incl. contact details and profile Photo uploads Created albums Pictures viewed with app Mailbox/Chat messages
Android	Twitter	For user and people followed: User names Posted tweets and photos Other activity information (e.g., device used to tweet)
Android	MySpace	User name/Password Cookies & cache files

Figura 5. Dados de redes sociais encontrados em dispositivos móveis [18].

O autor [8] faz uma revisão desde o inicio dos sistemas operacionais para dispositivos móveis, descrevendo a arquitetura do Android, iOs e Windows Phone de forma mais completa, mas também abordando alguns outros sistemas operacionais como o Symbian e o Blackberry. O autor foca na questão de segurança da informação, apresentando formas de ataques passivos e ativos contra um dispositivo móvel, tal como vírus, malwares, trojans e também roubo de informações via aplicativos de troca de mensagens.

No trabalho de [19], os pesquisadores fazem uma revisão da literatura sobre as técnicas forenses aplicadas na extração e análise de dados

de dispositivos móveis que estão na nuvem. Eles abordam a questão de logs, arquivos de sistema e banco de dados, e também algumas ferramentas.

Os autores de [15] apresentarem um trabalho descritivo abordando principalmente as formas de extração de evidências de dispositivos, descrevendo algumas ferramentas existentes, tal como: Tableau, Solo4, Cellebriti UFED, entre outras. De forma similar, [4] também apresentam um descritivo da forma de extração de dados, bem como algum quesitos que devem ser considerados na hora de analisar as evidências e montar o laudo.

4. Conclusões e Trabalhos Futuros

Nesse trabalho apresentamos as características e arquitetura dos dois principais sistemas operacionais móveis disponíveis no mercado, Android e iOs, respectivamente. Apresentamos também as etapas de análise forense que são realizadas em dispositivos móveis e suas particularidades.

A extração de dados em aparelhos móveis tem se mostrado mais complexa que em computadores, devido a quantidade de fatores que podem influenciar, alterar ou então destruir os dados com que se está trabalhando, sendo necessário uma série de procedimentos para evitar que isso aconteça.

Na revisão da literatura encontramos uma quantidade considerável de trabalhos, porém ainda pequena se comparada com outras áreas. Um ponto a destacar é que a maior parte das pesquisas focam no sistema operacional Android e na sua extração de dados em diversos cenários. Isso deve-se a facilidade de se trabalhar com o mesmo, que como descrito possui código aberto, e também baixo custo de aquisição, se comparado com o iOS. Também encontramos algumas pesquisas na literatura com o objetivo de extrair dados de aplicativos específicos, como o caso de [18] que desejava extrair dados de redes sociais.

Por fim, concluímos que ainda há um grande campo de pesquisa em aberto, e como forma de contribuir para a área temos o seguinte objetivo de pesquisa futuro:

• analisar em um dispositivo Android se os dados de geolocalização ficam armazenados na memória do aparelho;
• em caso positivo, desejamos montar um mapa de locais por onde o usuário passou, de forma a responder, por exemplo, se o usuário esteve em determinado horário em determinado local.

References

[1] FGV. Disponível em < https://eaesp.fgv.br/ensinoeconhecimento/ centros/cia/pesquisa>. Acesso em 25 de agosto de 2018.

[2] Norton Cyber Security. Norton Cyber Security Insights Report 2017. Disponível em <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>. Acesso em 25 de agosto de 2018.

[3] Jansen, W. Delaitre, A. Moenner, L. Overcoming Impediments to Cell Phone Forensics. Proceedings of the 41 st Annual Hawaii International Conference on System Sciences. 2008.

[4] Joseph, Asha Singh, K. John. A Study on Digital Forensic in Mobile Devices. International Journal Of Electrical, Electronics And Data Communication, Volume-5, Issue-12. 2017

[5] Almeida, Mário de Souza. Elaboração de Projeto, TCC, Dissertação e Tese. 2. ed. São Paulo: Atlas, 2014.

[6] Nicolai B. B., De Oliveira D. M., Moraes N., e Da Silva W. L. Google android - a plataforma, seus componentes e suas versões. Disponiıvel em <http://www.williamluis.com.br/wp-content/uploads/2013/10/TCC-Google-Android-Final.pdf>. Acessado em 8 de maio de 2018.2012.

[7] Morimoto C. E. (2009). Smartphones: Guia Pratico. Porto Alegre: GDH Press e Sul Editores, p. 432.

[8] Bine, Jamilson Kuk, Josiel Neumann. Estudo de Segurança em Dispositivos Móveis. Revista Científica Semana Acadêmica Unicentro – PR. Ed.96, vol.1. 2016.

[9] Lecheta, Ricardo. Google Android: “Aprenda a criar aplicacoes para dispositivos moveis com o Android SDK”. Sao Paulo, Novatec Editora, 2017.

[10] Android. Android interfaces. Disponıvel em <https://source.android.com/devices/>. Acesso em 4 de maio de 2018. 2015.

[11] Milani A. Programando para iPhone e iPad - Aprenda a construir aplicativos para o iOS. São Paulo: Novatec Editora. 2012.

[12] Apple. About theios technologies. Disponıvel em <https://developer.apple.com/library/prerelease/ios/navigation/>. Acesso em 2 de julho de 2018. 2015.

[13] Garcia M. A. P. Filtros de imagens para ios. Disponıvel em: <http://www.tcc-computacao.tiagodemelo.info/monografias/2013/tcc-mario-angel.pdf>. Acessado em: 22 de abril de 2015. 2013.

[14] Curran, Kevin Robinson, Andrew Peacocke, Stephen Cassidy, Sean. Mobile Phone Forensic Analysis. International Journal of Digital Crime and Forensic. Vol. 2, no 2. 2010.

[15] Schmitz, Kiulyn Fernandes Taborda SCHMITZ Melo, João Eduardo Branco de MELO Cardoso, Vanilson. O uso da informática na perícia criminal e suas ferramentas. Revista Espacios, vol. 38 (51). 2017.

[16] Simão, André Morum de L. Sícoli, Fábio Caús Sícoli Melo, Laerte Peotta de Melo Deus, Flávio Elias de Deus Júnior, Rafael Timóteo de Sousa. Acquisition and Analysis of Digital Evidence in Android Smartphones. The International Journal of Forensic Computer Science. 2011.

[17] Yates, Maynard. Practical Investigations of Digital Forensics Tools for Mobile Devices. Infosec. 2010.

[18] Mutawa, Noora Al Baggili, Ibrahim Marrington, Andrew. Forensic analysis of social networking applications on mobile devices. Elsevier, vol.9. 2012.

[19] Kechadi, Tahar Faheem, Muhammad Le-Khac, Nhien-An. The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends. International Journal of Digital Crime and Forensics, 7 (2): 1-19. 2015.