DOI: 10.5748/9788599693131-14CONTECSI/PS-4963

A COMPUTATIONAL EXPERT PROCESS FOR ASSESSING PRIVACY PROTECTION IN ANDROID APPLICATIONS

Fábio Calandrelli Ribeiro (Institute for Technological Research of the State of São Paulo, São Paulo, São Paulo, Brasil) - fcalandrelli2016@gmail.com)
Eduardo Takeo Ueda (Institute for Technological Research of the State of São Paulo, São Paulo, Brasil) - edutakeo@usp.br

The execution of forensic expert work in the area of computing requires the gathering of digital proofs with legal validity to qualify an activity as criminal. Through anti-forensic applications installed on electronic devices such as smartphones, criminals can commit illegal acts and still communicate with other individuals for violations, such as pedophilia and invasion of privacy, making it difficult to produce valid digital proofs and accepted by a court. This work presents an expert process for information retrieval in an environment with specific applications that were used for the communication between users and Internet access, with the intention of avoiding the traceability of the actions taken. The process consists of seven activities to perform pre-analysis, acquisition and examination of the data of a smartphone. The results allowed us to conclude that although application manufacturers declare the impossibility of recovering data when hiding or destroying historical data, it was possible to reestablish information, such as the date, time and type of actions performed by a user. We conclude from the analyzed situations that the data recovery can be effected by applying the proposed process, even with the data privacy protection features being used in order to deceive expert work. In addition, we have realized that the techniques of data concealment or destruction of the examined applications still need to be improved by the use of other antiforenses techniques, such as masking of data.

Keywords: Forensic, Expert Process, Privacy, Smartphone, Android.

1. Introdução

A produção de provas que caracterizem uma atividade ilícita ocorre para sustentar a prática de um inquérito policial, civil público ou procedimento administrativo. Muitas vezes, após executar o trâmite jurídico, um perito deve lidar com situações em que existe a necessidade de análise forense de um *smartphone* devido a suspeita do proprietário ter utilizado aplicativos com funcionalidades antiforense, tais como, ocultação e destruição de dados, para comunicação com outros indivíduos e navegação na Internet para execução de ações criminosas. Embora aplicativos com funcionalidades para garantir a privacidade dos usuários não sejam declaradamente utilizados como ferramentas antiforense visando comprometer um trabalho pericial, podem ser aplicadas para este propósito.

Diante dessas condições, os riscos da impossibilidade de recuperação dos dados devido aos procedimentos executados em um dispositivo que podem comprometer o trabalho pericial são inerentes, tornando-se um desafio contornar essas medidas.

Os recursos fornecidos por aparelhos *smartphones* proporcionam a conveniência da comunicação por meio da troca de mensagens de voz, texto, imagens e vídeos; além disso, existe a facilidade de acesso à Internet substituindo os computadores pessoais para tal finalidade. No quarto trimestre de 2016 foram vendidas em torno de 428 milhões de celulares e *smartphones* no mundo (Teleco, 2017). De acordo com a pesquisa anual de uso de Tecnologia da Informação realizada pela Fundação Getúlio Vargas a projeção para o número de *smartphones* no Brasil para 2018 é de aproximadamente 268 milhões de aparelhos (FGV, 2017).

Para o seu funcionamento, um *smartphone*, assim como qualquer computador, necessita de um sistema operacional instalado sendo o que lidera em participação de mercado (81, 2% mundo e 80,4% Brasil) o Android, um sistema Linux de código aberto que se adapta a vários tipos de dispositivos e que tem evoluído no sentido de fornecer cada vez mais funcionalidades aos usuários (Chainho, 2014).

Este trabalho está organizado como descrito a seguir. A Seção 2 relata a metodologia aplicada para o desenvolvimento da pesquisa. Na Seção 3 é apresentada uma revisão de literatura de técnicas antiforenses e trabalhos periciais voltados para *smartphones*. A Seção 4 especifica o procedimento pericial proposto por meio do processo e tecnologias utilizadas para sua aplicação. A Seção 5 descreve detalhes dos experimentos executados para validação da proposta. A Seção 6 discute os resultados alcançados; e por fim, a Seção 7 expõe as considerações finais e trabalhos futuros.

2. Metodologia

A metodologia empregada na elaboração deste trabalho consistiu de quatro etapas principais, conforme ilustrado na Figura 1 a seguir.

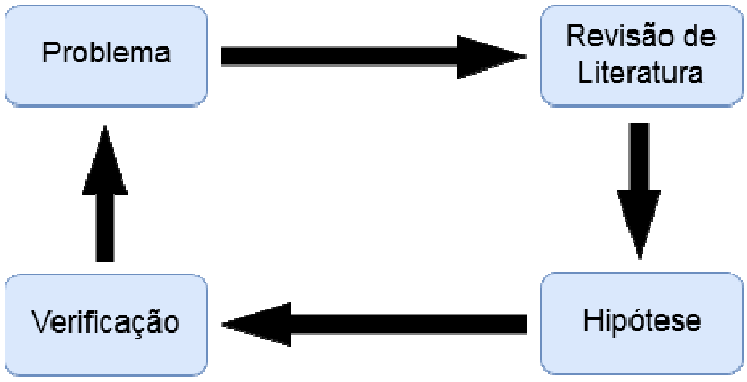

Figura 1 - Metodologia da pesquisa

O problema de pesquisa consiste em propor abordagens que sejam adequadas para realizar perícias computacionais em aparelhos com sistema operacional Android e aplicativos que possuem funcionalidades antiforenses como mecanismos para prover privacidade para usuários. Uma vez definido o problema o passo seguinte consistiu em uma revisão de literatura para identificar as principais técnicas para forense de *smartphones*.

A partir de uma análise crítica dos trabalhos relacionados encontrados na literatura foi possível levantar a hipótese de que um novo procedimento adaptado da proposta de Simão (2011) poderia contribuir como uma nova maneira de tratar o problema de pesquisa. Por fim, com a realização de experimentos práticos como prova de conceito a hipótese pode ser verificada/validada.

3. Trabalhos Relacionados

No domínio computacional a análise forense possui como metas a aquisição, preservação, recuperação e exame de dados que estão em formato digital e armazenados em algum tipo de mídia eletrônica. Tais atividades são executadas visando suprir as necessidades de órgãos legais no que se refere à manipulação de evidências digitais (Guimaraes, 2008).

Na tentativa de comprometer o trabalho pericial, existem técnicas denominadas antiforenses que são definidas como maneiras de modificar ou destruir uma evidência digital (Harris, 2006), e caracteriza-se como uma forma de limitar a identificação, extração, verificação e validação de dados digitais. Harris (2006) detalha ainda a classificação dessas técnicas em quatro tipos: ocultação, destruição, ofuscação de dados e ataque contra as ferramentas utilizadas no trabalho pericial.

Entre as técnicas consideradas nesta pesquisa, a ocultação de dados é definida como a camuflagem de evidência de modo que não seja visualizada ou interpretada como uma prova válida. Um exemplo é a utilização de recursos de aplicativos em modo anônimo que oculta a existência de vestígios de utilização. Por sua vez a destruição de dados, é uma técnica que pode ser aplicada usando ferramentas, ou manualmente, e que destina-se a tornar impraticável a recuperação de arquivos de dados pela subscrição das trilhas do disco de armazenamento ou da exclusão dos arquivos (Harris, 2006).

Por meio de ferramentas antiforenses comerciais disponíveis para *smartphones* Sporea et al. (2012) apresentaram técnicas para efetuar a destruição, ocultação e simulação de dados

aplicadas em aparelhos com Android e iOS. Com a finalidade de testar a eficácia do procedimento de análise forense foram utilizadas duas ferramentas forenses proprietárias e constatou-se que não houve a recuperação dos dados, demonstrando a necessidade de extensão da pesquisa para gerar contramedidas que poderiam impedir a perda ou destruição dessas evidências.

Azadegan et al. (2012) utilizaram as técnicas de destruição (exclusão total, exclusão parcial) e de ofuscação (substituição por dados falsos) em três cenários experimentais e por meio da aplicação de um procedimento de aquisição e exame de dados verificaram que essas técnicas comprometeram a etapa de exame, invalidando as evidências produzidas.

Albano et al. (2011) proporam uma técnica antiforense que foi aplicada em um *smartphone* com Android e que tornou possível editar e excluir dados sem modificar o sistema de arquivos por meio de um aplicativo de sanitização segura. Para verificação de êxito da técnica foi realizada a aquisição por meio da recuperação de dados com duas ferramentas, sendo uma delas comercial e a outra de software livre. Como resultado, essas ferramentas recuperaram os dados, entretanto, como estes dados estavam alterados houve a geração de um falso álibi a um indivíduo.

Mahajan et al. (2013) produziram um estudo comparativo dos resultados de aquisição de dados em nível lógico por meio de duas ferramentas comerciais e o posterior exame dos dados coletados. Em cinco modelos de *smartphones* foram simuladas a troca de mensagens de texto, compartilhamento de vídeos, imagens e áudio por meio dos aplicativos de comunicação WhatsApp e Viber. Embora a simulação tenha sido feita sem a utilização de técnicas antiforenses, foi possível identificar a data e horário dos arquivos e mensagens enviadas e recebidas, arquivos trocados, porém sem determinar a localização dos arquivos. Al-Hadadi (2013) em sua pesquisa apresentaram um procedimento de recuperação de dados no qual um indivíduo utilizou em um *smartphone* aplicativos para a troca de mensagens de texto, áudio e vídeo, e-mails e navegação web como suporte para cometimento de um crime. A partir deste aparelho, foi realizada a aquisição, exame e análise de dados com ferramentas comerciais em níveis de *dumping* e lógico, e efetuada uma comparação quantitativa entre essas ferramentas de arquivos, mensagens de textos e de contatos que foram recuperados.

No trabalho de Barghouthy (2014) foi proposta uma estratégia de aquisição e exame de dados em um *smartphone* com o Android instalado no qual foi simulado o acesso a um *site* de conteúdo de rede social, em um navegador web que não deixa rastro dos *sites* acessados. Foi considerada a aplicação em dois cenários, sendo que no primeiro cenário, a ferramenta de aquisição de dados obteve êxito, mas o rastreamento das atividades não foi possível. Os autores atribuíram o resultado a falta de privilégios de administrador no *smartphone*. No segundo cenário, com os privilégios de administrador houve a verificação dos *sites* acessados, com exceção da senha de acesso ao *site* da rede social.

Na pesquisa de Mehrotra (2013) o principal propósito do estudo foi a realização de investigação pericial forense para a recuperação de dados em dois *smartphones*, após a comunicação por mensagens de texto, áudio e vídeo com a utilização de um aplicativo antiforense denominado “Wickr”. Tal aplicativo emprega a técnica de autodestruição em um determinado período de tempo evitando que seja possível a rastreabilidade do histórico de utilização. Mesmo com os autores realizando o procedimento em um dispositivo com

privilégios de superusuário habilitado, da adaptação das etapas de aquisição, exame e análise de dados do método (NIST, 2014), não foi possível a recuperação de dados.

Dentro do contexto apresentado nesta seção, as técnicas antiforense utilizadas como funcionalidades de apoio à privacidade em aplicativos surgem como impeditivos para que atividades ilícitas efetuadas por um proprietário de *smartphone* sejam identificadas. O procedimento proposto e descrito em nosso trabalho permite um perito contornar este tipo de complicação no decorrer da aquisição de dados e consequentemente aprimorar o exame e análise para eficaz reestabelecimento de elementos que compõe um fato ocorrido e a produção de provas válidas.

4. Procedimento Pericial Proposto

Esta seção divide-se em duas subseções que apresentam respectivamente o detalhamento das atividades realizadas e as tecnologias aplicadas para a implementação do procedimento deste trabalho.

4.1. Processo

O procedimento executado consistiu de sete macro atividades baseadas na proposta de Simão (2011) e aderente ao padrão elaborado e revisado pelo NIST em 2014, contendo as diretrizes para realização da análise forense em dispositivos móveis, tais como, *tablets* e *smartphones*. Cada parte é detalhada a seguir considerando as recomendações fornecidas pelo NIST de análise forense:

1. Isolamento do dispositivo: O isolamento do dispositivo deve preservá-lo tanto em nível físico quanto da troca de sinais eletromagnéticos, entretanto, não tendo tal infraestrutura deve-se colocá-lo em modo avião ou *off-line* evitando que qualquer transmissão de dados possa efetivar alguma modificação no aparelho.

2. Aplicação de rastreabilidade: Esta atividade permite ao perito documentar as atividades que foram efetuadas no *smartphone*, inclusive para demonstrar que não houve nenhum procedimento realizado que invalidasse a produção das provas comprovando em caso de necessidade o que foi efetuado no aparelho.

3. Obtenção do estado de funcionamento: Por meio de intervenção no dispositivo, o perito necessita obter informações, tais como, processos em execução, usuários ativados, estado da bateria, configurações do aparelho, aplicativos com funcionalidades antiforenses instalados, bloqueio do *smarpthone* e se o mesmo possui o privilégio de superusuário ativado.

4. Definição das ferramentas técnicas a serem utilizadas na aquisição de dados: Com base na obtenção do estado de funcionamento, o perito deve prosseguir com o trabalho pericial selecionando o tipo de aquisição e exame de dados a serem realizados, as ferramentas necessárias e qual o escopo das informações a serem obtidas.

5. Coleta de dados: Software para extração de imagem da memória não volátil deve ser utilizado, mas deve-se ponderar o modelo do aparelho e versão do sistema operacional Android. Caso o *smartphone* ainda não esteja isolado ou habilitado em modo avião, é crucial que o profissional responsável pelo trabalho pericial forense

efetue esta atividade antes de prosseguir.

6. Aplicação de integridade: Os dados extraídos de um *smartphone* devem ser armazenados com proteção de integridade, por meio da aplicação de um algoritmo de *hash*, para garantir a possibilidade de comprovação de que a informação utilizada no âmbito judicial é a mesma gerada no recolhimento de provas durante o trabalho pericial.

7. Documentação do procedimento realizado: Todo o procedimento de aquisição de dados deve ser efetuado considerando a documentação do que foi realizado e o registro visando garantir a integridade e confidencialidade dos dados.

4.2. Tecnologias

As tecnologias que foram utilizadas para a implementação da técnica de análise forense computacional foram as seguintes:

- Máquina virtual: Contendo a instalação da distribuição Santoku baseada na versão Ubuntu do Linux e voltada para a realização de trabalhos periciais em dispositivos móveis (Now Secure, 2017).

- Android SDK Manager: Parte integrante da distribuição Santoku que fornece as bibliotecas de API e as ferramentas necessárias para desenvolver, realizar testes e depurações de aplicações (Now Secure, 2017). Deve ser carregada conforme a versão do sistema operacional do dispositivo periciado.

- Android Debug Bridge: Conforme o Android Developers (2017), esta ferramenta é parte integrante do Android SDK Manager e permite a comunicação de uma instância com um smartphone.

- Dalvik Debug Monitor Server (DDMS): Utilitário do Android SDK Studio, possui a funcionalidade associada a depuração de código fonte, captura telas e processos em execução em um dispositivo móvel (Now Secure, 2017). Evidencia as atividades realizadas em um *smartphone* bem como os aplicativos em execução. Permite ainda a obtenção do estado de funcionamento do aparelho, por exemplo, aplicativos instalados.

- Aplicativo Kingroot: Desenvolvido e mantido por um grupo de desenvolvedores chineses que visa a otimização do sistema operacional Android e pode ser baixada do próprio site deste grupo (Kingroot, 2017). Esta ferramenta possui êxito em 60% das vezes, aproximadamente, o que é considerado um nível alto dentre a variedade de modelos e de sistemas operacionais (Kingroot, 2017).

- Autopsy Forensic Browser: Ferramenta de aplicação gráfica fornecida na

distribuição Santoku que faz uso de um conjunto de funcionalidades de extração de dados de arquivos de imagem de partição. Por agrupamento, permite que tipos de dados sejam recuperados, tais como, bancos de dados, arquivos em formato texto, vídeo, imagens, mensagens de texto e contatos telefônicos (Now Secure, 2017).

- SHA512SUM: Disponível para ser utilizado na distribuição Santoku, implementa a autenticidade dos dados coletados por código de proteção que preserva a integridade dos arquivos de imagem gerados.

Em cada cenário dos experimentos descritos na próxima seção, foi efetuada a conexão remota entre a estação de trabalho forense e o *smartphone* periciado para a coleta de dados por meio de espelhamento da partição "/data". Por meio de comandos ADB foi efetuada a leitura dos dispositivos em cada cenário. De modo complementar no cenário 3, houve a necessidade de instalação do aplicativo Kingroot e obtenção do privilégio superusuário. Após a execução dos procedimentos mencionados acima, por meio do comando "mount" as partições do dispositivo foram montadas e com o comando dd (programa que efetua a cópia origem e destino de dados bit a bit) os dados da partição "/data" foram enviados para um cartão SD armazenado no dispositivo.

5. Experimentos

O procedimento de aquisição de dados ocorreu após 5 horas da simulação efetuada nos aplicativos. No decorrer deste período houve a utilização dos *smartphones* para outras atividades em que não foram aplicadas técnicas antiforenses.

Os dados do cartão SD foram copiados para a estação de trabalho forense e importados na ferramenta Autopsy para o exame por meio de análise manual dos dados. Uma busca por palavras chave (exemplo: nome dos aplicativos utilizados) foi efetuada na estrutura de pastas partição "/data". Caso fosse identificada alguma pasta ou arquivo, era realizado o detalhamento e exploração do conteúdo visando identificar artefatos que pudessem comprovar as atividades efetuadas pelo proprietário do dispositivo.

No momento de execução de um trabalho pericial voltado para dispositivos móveis, o perito pode se deparar com uma enorme diversidade de cenários em que é necessária a análise forense para a produção de provas válidas. Aparelhos com acesso de root ativado ou não, de fabricantes distintos e diferentes versões do sistema operacional Android são algumas delas.

Neste trabalho foram abordados três cenários que estão detalhados na Tabela 1 considerando diferentes características de hardware, versão do sistema operacional dos *smartphones* e tipo de restrição de acesso aos dados.

Todo o tráfego de dados ocorreu em uma rede local sem fio (WLAN) baseada no padrão IEEE 802.11 e não em redes de operadoras de telefonia, pelo fato da análise em redes de operadoras dificultar o trabalho pericial e aumentar a dependência da recuperação dos dados no próprio aparelho.

Tabela 1 - Cenários e características dos dispositivos

Descrição	Dispositivo	Cenário
Aparelho ligado, sem tela de bloqueio, com acesso de depuração restrito (ADB), e com permissões de superusuário.	LG, modelo G2 mini D618 Dual Chip, Android 5.0.2	Cenário 1
Aparelho ligado, com tela de bloqueio e sem permissões de superusuário.	Samsung, modelo Galaxy Pocket Neo S5310B, Android 4.1.2	Cenário 2
Aparelho ligado, sem bloqueio e com reset de fábrica aplicado.	Jixin, modelo J1000, Android 4.0.3	Cenário 3

Para validar o procedimento proposto, em cada cenário foram instalados cinco aplicativos, sendo três de comunicação entre usuários pela troca de arquivos em mensagens instantâneas e dois navegadores de acesso à Internet. Os aplicativos foram selecionados com base na quantidade de *downloads* efetuada na loja oficial da Google Play, no caso do Wickr. A escolha ocorreu pela possibilidade de avanços na recuperação de dados considerando os resultados obtidos por (Mehrotra, 2013). As funcionalidades antiforenses dos aplicativos analisados neste artigo são voltadas para a ocultação ou destruição de dados e podem ser nativas ou implementadas manualmente pelo usuário.

Conforme apresentado na Tabela 2, foram realizadas atividades de envio e recebimento de mensagens contendo arquivos de áudio, vídeo e imagem (entre os dispositivos de cada cenário) e acesso a *sites* que podem potencialmente ser utilizados para cometimento de atividades ilícitas, tais como, redes sociais, bate papo, instituição financeira, repositório de imagens e vídeos.

Tabela 2 – Simulação em cada dispositivo de troca de mensagens/acesso a sites

Tipo de troca de mensagens/ *Sites* Acessados (Quantidade)	Tipo de Operação (Técnica antiforense)	Aplicativo
Arquivo de Áudio/ Arquivo de Imagem/ Arquivo de Vídeo (5 arquivos trocados de cada tipo)	Bate-papo (Autodestruição – nativa)	Wickr
Arquivo de Áudio/ Arquivo de Imagem/ Arquivo de Vídeo (5 arquivos trocados de cada tipo)	Bate-papo (Autodestruição – implementada pelo usuário)	Telegram
Arquivo de Imagem/ Arquivo de Vídeo (10 arquivos trocados de cada tipo)	Bate-papo (Autodestruição – nativa)	Snapchat
Acesso a *sites* com a permanência por cinco minutos na página em modo anônimo e executada uma atividade (evento)	Navegação (Ocultação – implementada pelo usuário)	Firefox
- www.facebook.com (acesso a página da rede social) - www.twitter.com (acesso a página da rede social) - www.bb.com.br (acesso ao extrato de conta corrente) - www.uol.com.br/batepapo (acesso a uma sala de bate-papo) - www.youtube.com (visualização de um vídeo) (5 *sites* acessados)	Navegação (Ocultação – implementada pelo usuário)	Dolphin

No decorrer da execução das atividades, nos cenários 1 e 3 houve a ativação da depuração nos dois dispositivos periciados por meio da intervenção manual, ao acessar o item "Opções do Desenvolvedor" e "Depuração Android". Com a depuração ativada, foi efetuada a conexão dos dispositivos com a estação de trabalho forense por meio de comunicação USB. Entretanto, no cenário 2, constatou-se que o dispositivo encontrava-se bloqueado e com a necessidade de verificação de que seria possível prosseguir com as demais atividades com uma intervenção manual. Neste cenário, identificou-se que a depuração estava ativada pelo comando "adb devices".

Dando continuidade a aplicação da rastreabilidade, foi executada o aplicativo Dalvik Debug Monitor Server (DDMS) na estação de trabalho forense. Com isso foi ativada a leitura e a rastreabilidade das atividades no *smartphone* pela inicialização dos registros em

tempo real por modo promíscuo (verbose). Esses registros permitiram comprovar as atividades executadas no aparelho. Durante a intervenção no *smartphone*, os registros foram gravados periodicamente em disco da estação de trabalho forense em ordem cronológica visando corroborar as atividades efetuadas em caso de necessidade.

Como foi possível a leitura do aparelho por meio do DDMS, os dados de hardware e software dos dispositivos associados aos três cenários foram colhidos na memória volátil (DDMS >> Device >>Dump App State e Dump Device State). Ambas as opções coletaram informações sobre processos em execução, usuários ativados, conta do gmail habilitada no dispositivo, estado da bateria e configurações do aparelho.

Além disso, devido a identificação do privilégio de superusuário ativo ou com a possibilidade de ser habilitado, foi escolhido o processo realizado por Faheem (2014) para a aquisição de dados. Após os procedimentos executados, foi criado um arquivo de imagem com a extensão .dd, gerado em um cartão de dados inserido no dispositivo periciado. Neste arquivo foi aplicada a proteção de integridade dos dados pelo comando sha512sum gerando um código *hash*.

Os experimentos foram conduzidos tendo como premissa a recuperação de elementos que permitem reconstruir as circunstâncias de um fato (Del-Campo, 2009). Para a troca de arquivos esses elementos foram considerados a data, horário, conteúdo do tipo de mensagem trafegada (se áudio, imagem ou vídeo), remetente e destinatário. Quanto a *sites* acessados foram a data, horário, endereço eletrônico e tipo de evento realizado (exemplo: se autenticação, visualização de vídeo, sala bate papo).

Os dados do cartão SD foram copiados para a estação de trabalho forense e importados na ferramenta Autopsy com o objetivo de serem examinados por meio de análise manual de conteúdo. Uma busca por estrutura de diretórios dos aplicativos listados nos cenários contidos neste artigo foi efetuada na estrutura de pastas partição “/data”. Caso fosse identificada alguma pasta ou arquivo, era realizado o detalhamento e exploração do conteúdo para identificar artefatos que pudessem comprovar as atividades efetuadas.

Com o utilitário SHA512SUM, foi aplicado código de checagem de integridade dos arquivos gerados no decorrer da aplicação do procedimento. Este código permite que em caso de necessidade haja a verificação de que o arquivo coletado nos experimentos não sofreu modificações.

6. Análise dos Resultados

Nesta seção são discutidos os resultados provenientes dos experimentos executados em cada cenário, após a simulação de troca de mensagens e acesso a *sites* da Internet. Foi utilizada a estratégia de Xenakis et al. (2014), cujo percentual de recuperação de dados é calculado considerando o total de elementos passíveis de recuperação versus o que efetivamente foi recuperado.

Os valores apresentados na Tabela 3 demonstram que existe uma variação dos elementos recuperáveis por cenário, aplicativos e tipos de arquivos trafegados, porém o maior percentual de recuperação foi identificado no cenário 1 (53%). No detalhamento por aplicativos e tipos de arquivos, observa-se que a maioria dos elementos recuperados está

relacionada a mensagens contendo arquivos em formato de imagem e vídeo do aplicativo Snapchat.

Por outro lado, nos demais aplicativos não foi possível a identificação do destinatário das mensagens. Cabe ressaltar que dos três cenários, a técnica antiforense voltada para a preservação de privacidade do aplicativo Wickr demonstrou ser a mais eficiente, pela menor quantidade de elementos recuperados em relação aos demais aplicativos analisados (em torno de 40). Apesar disso, houve um avanço de 18% na recuperação de dados diante dos resultados do trabalho de (Mehrotra, 2013). Pela recuperação parcial dos elementos das mensagens trafegadas por meio dos aplicativos Snapchat e Telegram, é possível estabelecer que a funcionalidade de destruição dos dados não funciona em sua totalidade.

Tabela 3 - Elementos Recuperados em Mensagens Instantâneas nos Três Cenários

Cenários	Aplicativo	Tipo	Detalhamento					Total	(%) Recuperado	(%) Médio por Cenário
			Data	Horário	Remetente	Destinatário	Conteúdo			
Cenário 1	Wickr	Áudio	2	2	0	0	2	6/25	24%	53%
		Vídeo	2	2	0	0	2	6/25	24%	
		Imagem	1	1	1	0	1	4/25	16%	
	Telegram	Áudio	3	3	0	0	3	9/25	36%	
		Vídeo	4	4	4	0	4	16/25	64%	
		Imagem	5	5	5	0	5	20/25	80%	
	Snapchat	Vídeo	5	5	5	5	2	22/25	88%	
		Imagem	5	5	5	5	2	22/25	88%	
Cenário 2	Wickr	Áudio	1	1	0	0	1	3/25	12%	40%
		Vídeo	1	1	0	0	1	3/25	12%	
		Imagem	2	2	2	0	2	8/25	32%	
	Telegram	Áudio	1	1	0	0	1	3/25	12%	
		Vídeo	3	3	3	0	3	12/25	48%	
		Imagem	3	3	3	0	3	12/25	48%	
	Snapchat	Vídeo	5	5	4	4	1	19/25	76%	
		Imagem	5	5	4	4	1	19/25	76%	
Cenário 3	Wickr	Áudio	1	1	0	0	1	3/25	12%	41%
		Vídeo	1	1	0	0	1	3/25	12%	
		Imagem	1	1	1	0	1	4/25	16%	
	Telegram	Áudio	2	2	0	0	2	6/25	24%	
		Vídeo	3	3	3	0	3	12/25	48%	
		Imagem	3	3	3	0	3	12/25	48%	
	Snapchat	Vídeo	5	5	5	5	1	21/25	84%	
		Imagem	5	5	5	5	1	21/25	84%	

Por sua vez, a Tabela 4 apresenta os resultados de recuperação de dados obtidos considerando o acesso a 10 endereços eletrônicos em que 20 elementos são passíveis de recuperação no decorrer da navegação. São descritos os aplicativos, data, horário, site acessado e evento realizado. Nota-se que nos três cenários é possível identificar a maioria das ações do usuário em ambos os navegadores, mesmo que a utilização tenha ocorrido em modo anônimo.

Tabela 4 - Elementos Recuperados em Browsers nos Três Cenários

Cenários	Aplicativo	Data	Horário	Site	Evento	Total	(%) Recuperado
Cenário 1	Firefox	5	5	5	3	18/20	90%
	Dolphin	5	5	5	3	18/20	90%
Cenário 2	Firefox	5	5	5	0	15/20	75%
	Dolphin	5	5	5	0	15/20	75%
Cenário 3	Firefox	5	5	5	2	17/20	85%
	Dolphin	5	5	5	2	17/20	85%

Embora os aplicativos do escopo deste trabalho possuam funcionalidades antiforenses ativadas nativamente ou pelo proprietário do *smartphone*, os resultados indicam que pela implementação do procedimento proposto, ainda assim é possível a recuperação dos dados. O aumento nos percentuais de recuperação de dados alcançados na ferramenta Wickr permitiu avançar quanto aos resultados da pesquisa de Mehrotra (2013). Além disso, é possível corroborar o trabalho de Barghouthy (2014) e de Mahajan et al. (2013) em que a obtenção de privilégios de superusuário é necessária para a realização do trabalho pericial.

7. Conclusão e Trabalhos Futuros

O procedimento apresentado neste trabalho analisou aplicativos com funcionalidades de proteção da privacidade de usuários, que apesar de serem necessários podem comprometer a recuperação de dados em um trabalho pericial.

Constatamos que mesmo com a utilização de funcionalidades de ocultação e destruição de dados em aplicativos utilizados em *smartphones* foi possível identificar elementos que permitem comprovar a ação de comunicação por meio de troca de arquivos ou acesso a *sites* na Internet. Com base nessas informações, um perito pode comprovar uma atividade ilícita realizada por um usuário, por exemplo. Em comparação com os diversos trabalhos encontrados na literatura, existe a contribuição relativa a comprovação das atividades efetuadas em situações em que um perito pode utilizar este procedimento em sua totalidade ou parcialmente para executar a análise forense.

Com os resultados obtidos na realização deste trabalho, assim como o conhecimento adquirido no desenvolvimento no decorrer desta pesquisa, sugerimos as seguintes possibilidades de continuidade:

(a) Aplicação deste mesmo processo em cenários diferentes dos abordados neste artigo abrangendo hardware (modelos e fabricantes diferente de *smartphones*, *tablets* entre outros dispositivos móveis), *software* (outras versões do sistema operacional Android ou aplicativos com funcionalidades e técnicas antiforenses, tal como, ocultação por criptografia ou contra ataque para tentativa de acesso a dados).

(b) Realização de correlação de dados recuperados dos aplicativos com funcionalidades antiforenses e outros coletados no *smartphone* , tais como, contatos, chamadas telefônicas, mensagens SMS, arquivos armazenados ou configurações.

(c) Diante da criticidade sobre a necessidade do acesso privilegiado de superusuário para a aquisição de dados em dispositivos móveis com o sistema operacional Android, caberia o desenvolvimento de uma técnica universal e menos invasiva, na qual seja possível detalhar a vulnerabilidade explorada neste sistema para todas as versões.

Referências

Albano, P. et al. A Novel Anti-Forensics Technique for the Android OS. In: International Conference on Broadband and Wireless Computing, Communication and Applications, Barcelona, Espanha. 2011.

Al-Hadadi, M.; Alshidani, A. Smartphone Forensics Analysis: A Case Study. International Journal of Computer and Electrical Engineering, Singapura, v.5, n.6, p.576-580, 2013.

Azadegan, S et al. Novel Anti-forensics Approaches for Smart Phones. Hawaii In: Annual International Conference on System Sciences, 45. 2012, Havaí, EUA.

Barghouthy, N. B. A.; Marrignton, A. A Comparison of Forensic Acquisition Techniques for Android Devices: A case study investigation of Orweb browsing sessions. In: New Technologies, Mobility and Security (NTMS), International Conference on, 6.,2014, Dubai (Emirados Árabes).

Chainho, F. N. G. Plataforma Parametrizável para Análise Forense de Dispositivos Móveis. Beja, 2014. 154 f. Dissertação (Mestrado em Engenharia de Segurança Informática) - Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Beja, Beja (Portugal), 2014.

Del-Campo, E. R. A. Exame e levantamento técnico pericial de locais de interesse à Justiça Criminal: abordagem descritiva e crítica. São Paulo, 2008. 274 f. Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

Faheem, M et al. Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool. In: Journal of Information Security, Dublin, v.5, p.83-90, jul. 2014.

Fundação Getúlio Vargas. 27ª Edição da Pesquisa Sobre o Uso de TI - 2016. Disponível em: <http://goo.gl/8bmpPw >. Acesso em: 20/02/2017.

Guimarães, C. C et al. Artigo: Forense Computacional: Aspectos Legais e Padronização. Campinas – SP. Instituto de Computação – UNICAMP, 2008. Disponível em: <http://goo.gl/um6gII>. Acesso em: 20/02/2017.

Harris, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. The International Journal of Digital Forensics & Incident Response, v.3, p. 44-49, aug. 2006.

Kingoroot. Consulta geral a home page. Disponível em:< http://goo.gl/Tmcrzd >. Acesso em: 20/02/2017.

Mahajan, A. et al. Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications, Gujarat (Índia), v.68, n.8, p.38-44, 2013.

Mehrotra, T.; Mehtre, B. M. Forensic Analysis of Wickr Application on Android Devices.

In: Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference, 12., 2013, Enanthi (India). Disponível em: <http://goo.gl/PEFTmo>. Acesso em: 20/02/2017.

NIST. National Institute of Standards and Technology. Guidelines on mobile device forensics. NIST.SP.800-101r1. 2014. 76p.

Now Secure. Consulta geral a home page. Disponível em:< http://goo.gl/g9ePml>. Acesso em: 20/02/2017.

Simão, A. M. L. Proposta de Método para Análise Pericial em *Smartphone* com Sistema Operacional Android. Brasília, 2011. 96 f. Dissertação (Mestrado Profissional em Engenharia Elétrica) - Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, 2011.

Sporea, I. et al. On the Availability of Anti-Forensic Tools for Smartphones. International Journal of Security (IJS), Volume (6): Issue (4) : 2012, Kuala Lumpur (Malásia), v.6, n.4, p.58-64, 2012.

Teleco. Seção: Celular & Smartphone. Disponível em: <http://goo.gl/4prm2>. Acesso em 20/02/2017.

Xenakis, C. et al. Evaluating the privacy of Android mobile applications under forensic analysis. In: Computers and Security Journal (Elsevier), Piraeus, Grécia, v.42, p.66-76, mai. 2014. Disponível em: <http://goo.gl/m3VWTD>. Acesso em 20/02/2017.