DOI: http://dx.doi.org/10.5769/C2011009

Aquisição de Evidências Digitais em *Smartphones* Android

André Morum de L. Simão1, Fábio Caús Sícoli[1], Laerte Peotta de Melo[2], Flávio Elias de Deus[2], Rafael Timóteo de Sousa Júnior[2]
(1) Departamento de Polícia Federal, MJ
(2) Universidade de Brasília, UnB
(1,2) Brasília, Brasil
(1) {morum.amls, sicoli.fcs}@dpf.gov.br
(2) {peotta, flavioelias, desousa}@unb.br

***Resumo* — Sob a perspectiva pericial, um celular operando o sistema operacional Android é um grande repositório de informações que ficam armazenadas localmente ou dispostas remotamente. Essa plataforma permite ao analista extrair evidências diretamente do aparelho, coletando informações sobre seu proprietário e fatos que estão sob investigação. Desse modo, é possível obter a autoria e materialização de delitos, bem como fornecer informações ao apuratório por meio da análise e correlação desses dados.**

Existem abordagens periciais bem difundidas e documentadas para exames em aparelhos celulares e computadores. Entretanto, não são suficientemente específicas e detalhadas para a realização de exames em dispositivos controlados pelo Android. Essas abordagens não se aplicam em sua totalidade quando associadas a exames em *smartphones*, uma vez que nesses dispositivos, as soluções de hardware e software são minimalistas e o sistema operacional possui suporte à utilização de memórias internas cuja remoção ou espelhamento são procedimentos considerados invasivos e com maior grau de complexidade, devido às dificuldades de acesso direto ao hardware. Além disso, os dispositivos possuem características específicas para cada versão e fabricante do hardware.

Diante desses desafios, este artigo propõe um método para realizar a aquisição dos dados de um *smartphone* utilizando o sistema operacional Android, abstraindo a versão e o fabricante do aparelho. A abordagem proposta utiliza as técnicas periciais adotadas tanto para análise de telefones celulares como para computadores, adaptando-as às características do sistema Android, sua estrutura de armazenamento de dados, seus aplicativos e às condições em que o equipamento tenha sido encaminhado ao analista pericial.

Palavras-chave — perícia forense; aquisição de dados; análise de evidências; telefone celular; smarphone; Android.

Abstract **— From an expert's perspective, an Android phone is a large data repository that can be stored either locally or remotely. Besides, its platform allows analysts to acquire device data and evidence, collecting information about its owner and facts that are under investigation. This way, by means of exploring and cross referencing that rich data source, one can get information related to unlawful acts and its perpetrator.**

There are widespread and well documented approaches to forensic examining mobile devices and computers. Nevertheless, they are not specific nor detailed enough to be carried out on Android cell phones. These approaches are not totally adequate to examine modern smartphones, since these devices have internal memories whose removal or mirroring procedures are considered invasive and complex, due to difficulties in having direct hardware access. Furthermore, specific features of each smartphone platform have to be considered prior to acquiring its data.

In order to deal with those challenges, this paper proposes a method to perform data acquisition of Android smartphones, regardless of version and manufacturer. The proposed approach takes into account existing techniques of computer and cell phone forensic examination, adapting them to specific Android characteristics, its data storage structure, popular applications and the conditions under which the device was sent to the forensic examiner.

Key-words — forensic analisys; data aquisition; evidence analisys;cell phone; smarphone; Android.

1. Introdução

Em 2011, o sistema operacional Android ultrapassou em número de aparelhos vendidos os outros sistemas para *smartphones* [1]. O sistema tem grande aceitação no mercado e conjectura-se que esta aceitação se deve ao código aberto e ao suporte aos mais modernos recursos e aplicativos disponíveis para esse tipo de equipamento móvel. Dada a capacidade de prover um grande número de funcionalidades ao usuário, um *smartphone* com o sistema Android pode armazenar um expressivo volume de informação sobre seu proprietário, configurando-se como uma fonte de provas para fatos que se queira elucidar ou obter informações para subsidiar uma investigação [2].

Algumas das funcionalidades do sistema operacional Android são: navegação na Internet, captura de imagens e vídeos, criação e visualização de documentos, anotações de calendário, gerenciamento de contatos, localização por GPS e navegação por mapas. Do ponto de vista do desenvolvedor de aplicações, o Android possui recursos que facilitam o desenvolvimento, a publicação e instalação dos aplicativos criados, o que enriquece os serviços providos pela plataforma.

Diferentemente da abordagem de aquisição de dados em ambientes computacionais, em que geralmente os dados podem ser extraídos no estado em que foram encontrados e ficam preservados a partir do momento da sua apreensão, a extração de dados de telefones celulares e *smartphones*

normalmente exige a execução de alguma intervenção no dispositivo. Além disso, tendo em vista que utilizam memórias embutidas, cujo acesso, sendo direto ao hardware, é delicado e complexo, é preciso instalar aplicativos ou utilizar ferramentas diretamente no dispositivo para que se proceda à aquisição dos dados armazenados e consequentes evidências. Desta forma, o analista pericial deve ter o conhecimento necessário para realizar os procedimentos periciais no dispositivo da forma menos intrusiva possível, controlando o ambiente de maneira a se evitar a perda, a alteração ou mesmo a contaminação de dados tratados como evidências [3], o que dará maior confiabilidade à perícia.

2. Plataforma Android

A plataforma Android é composta pelo sistema operacional, o SDK (*Software Development Kit*) e suas aplicações. O SDK é um conjunto de ferramentas disponibilizadas pela empresa Google que forma um ambiente de desenvolvimento para a criação de aplicativos Android. Uma das ferramentas é o ADB (*Android Debug Bridge*), que provê uma interface de comunicação com o sistema Android por meio de um computador. Quando conectado por meio dessa interface, o computador é capaz de acessar um interpretador de comandos (*shell*), instalar ou remover aplicativos, ler registros históricos (*logs*), transferir arquivos entre a estação e o dispositivo, dentre outras ações.

O sistema operacional Android utiliza o conceito de *sandbox*, em que os aplicativos, depois de serem instalados, possuem áreas reservadas, isolando o ambiente de execução dos processos e delimitando o acesso aos recursos. Desta forma, as aplicações não podem acessar áreas que não sejam explicitamente permitidas [4]. Entretanto, o acesso a funcionalidades pode ser autorizado por meio de permissões configuradas no arquivo "AndroidManifest.xml". No momento da instalação do aplicativo, tal arquivo informa ao usuário quais recursos disponíveis no *smartphone* serão utilizados. O usuário pode aceitar a instalação do aplicativo, após ter sido informado dos recursos que serão utilizados, ou simplesmente recusar a instalação por não concordar com os tipos de funcionalidades que o aplicativo teria que acessar.

Outra característica do Android é a utilização do banco de dados SQLite, que é de domínio público e código aberto. Trata-se de um banco de dados relacional de simples utilização, que armazena em um único arquivo a estrutura de objetos completa (tabelas, *views*, índices, *triggers*) [5]. Tal banco de dados não necessita de configurações e utiliza as próprias permissões do sistema para controle de acesso aos dados.

Com relação ao sistema de arquivos, atualmente grande parte dos dispositivos com o sistema Android adota o YAFFS2 (*Yet Another Flash File System 2*), que é um sistema de arquivos concebido para memórias *flash* e adaptado às peculiaridades deste tipo de memória. Vale notar que as principais ferramentas forenses disponíveis no mercado não são compatíveis com esse sistema de arquivos, dificultando a montagem de partições do Android e acesso aos dados ali armazenados. Contudo, conforme citado por Andrew Hoog [6], no final de 2010, observou-se que alguns aparelhos Android já utilizavam o sistema de arquivos EXT4 (*Fourth Extended File System*). Há uma tendência de migração para esse sistema de arquivos, tendo em vista o suporte a processadores com núcleos duplos e multiprocessamento, além do emprego de memórias e-MMC (*Embedded MultiMediaCard*), que já trabalham simulando dispositivos de armazenamento em bloco, que são mais robustos, maduros e de maior aceitação comercial.

O acesso às partições do sistema é restrito no sistema operacional Android. Por padrão, os usuários não possuem permissões para acessar áreas reservadas do sistema. O sistema fica blindado, a fim de evitar que aplicativos mal intencionados ou mal desenvolvidos afetem a estabilidade e a confiabilidade do sistema operacional. Contudo, é possível explorar algumas vulnerabilidades do sistema ou do dispositivo de modo a obter permissões de "super usuário" (*root*). Assim, é possível utilizar aplicativos e acessar um interpretador de comandos que tenha permissão de acesso total e irrestrito ao sistema. Consequentemente, um analista pericial pode realizar uma cópia espelho de todas as partições do sistema, bem como acessar arquivos que não seriam possíveis com as credenciais convencionais oferecidas pelo Android. Cabe a ressalva de que as técnicas adequadas variam conforme a versão do Android, assim como também podem depender do fabricante e modelo do aparelho. Além disso, essas técnicas são geralmente invasivas e podem inclusive danificar os dados armazenados no dispositivo.

O sistema operacional possui mecanismos de autenticação com a utilização de senhas ou uso de padrão táctil. Segundo o guia para forense em telefones celulares do NIST [5], há três métodos possíveis para desbloquear um aparelho: método investigativo, método baseado em software ou método baseado por hardware. Essas formas podem ser aplicadas ao equipamento Android dependendo da situação da apreensão, do modelo do aparelho e da versão do sistema.

Dadas as características descritas, para o analista pericial realizar uma extração de dados, além de possuir conhecimento sobre a plataforma Android, ele deve avaliar os procedimentos a serem adotados. Por exemplo, há cenários em que o telefone pode estar desligado ou ligado, ter memória removível ou interna, estar bloqueado ou desbloqueado, estar com acesso via modo de depuração USB ou não, ter algum aplicativo em execução que tenha informações úteis à investigação e ainda pode estar com permissões de "super usuário" habilitadas. Assim, o analista deve avaliar os procedimentos corretos a serem adotados a depender do estado do *smartphone* Android.

3. Método para aquisição de dados de um *smartphone* Android

Considerando as características singulares do Android e os diferentes cenários com que um analista pericial pode se deparar, propõe-se o método para aquisição de dados exibido no *workflow* da Figura 1.

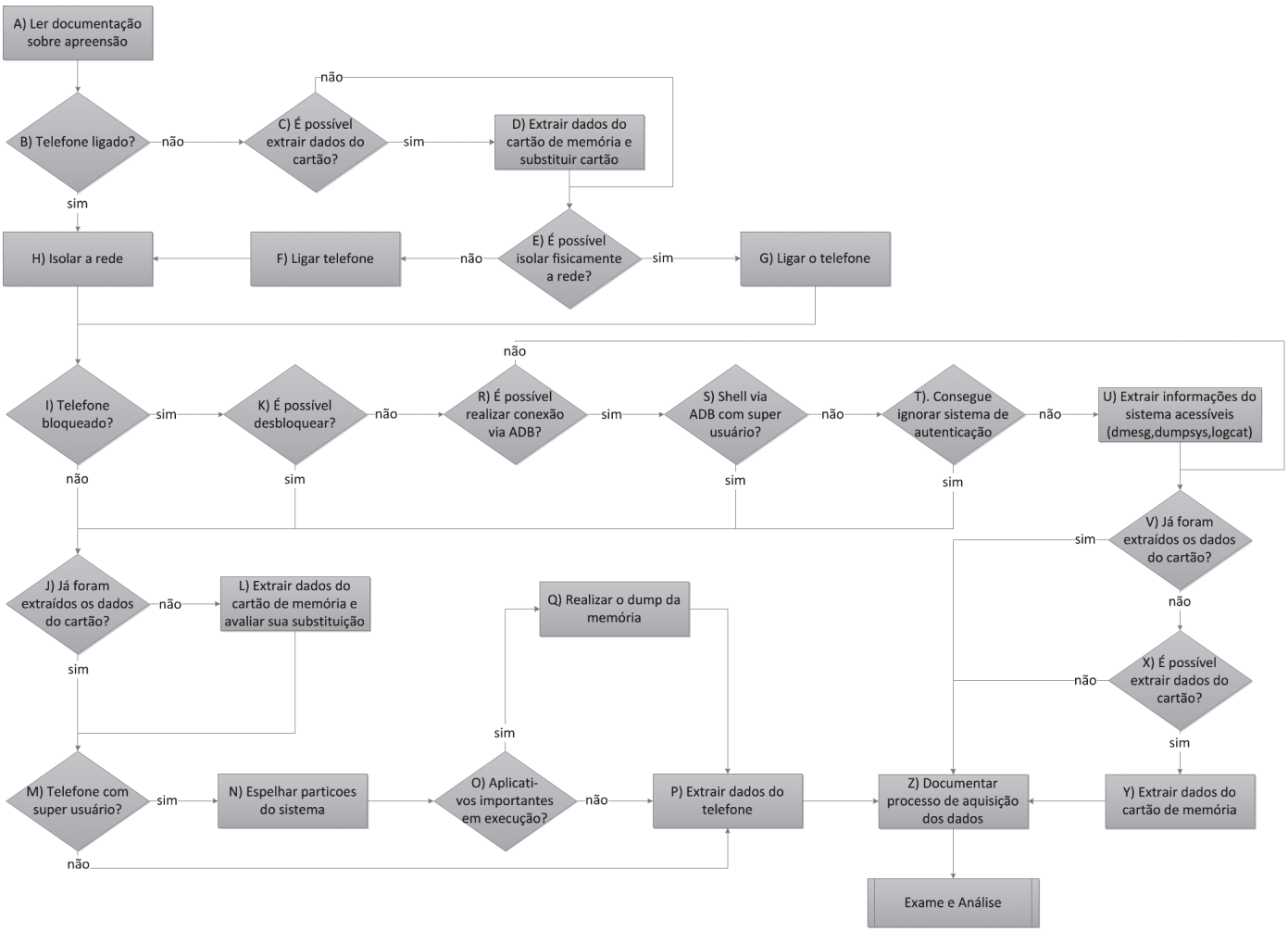

Figura 1. Diagrama do processo de aquisição de dados de um *smartphone* com sistema operacional Android.

Na figura, são apresentados diferentes cenários e os respectivos procedimentos a serem adotados pelo analista. A partir desse método, é possível obter o máximo de informações do dispositivo móvel, de maneira a documentar, resguardar e processar a evidência da forma mais segura e menos intrusiva possível.

A. Procedimentos iniciais para preservação dos dados do smartphone

Ao receber o *smartphone*, o analista pericial deve seguir os procedimentos a fim de preservar os dados armazenados no equipamento apreendido. Assim, deve verificar se o telefone encontra-se ligado ou não. Com o telefone desligado, deve-se avaliar a possibilidade de extrair os dados do cartão de memória. Cabe a ressalva de que alguns modelos de celulares Android possuem cartão de memória interno, não sendo possível sua remoção para a cópia dos dados por meio do uso de um leitor padrão USB. No caso em que é possível retirar o cartão de memória, basta removê-lo e duplicar integralmente os dados para um cartão de memória do analista pericial, a fim de garantir sua preservação. Para copiar os dados do cartão de memória, pode-se utilizar a mesma abordagem utilizada em *pendrives*. Deve-se utilizar ferramentas forenses para a cópia ou até mesmo executar um *disk dump* e gerar o *hash* dos dados duplicados. Ao término do processo, o cartão de memória com a cópia deve ser reinserido no aparelho.

A próxima etapa é isolar o telefone das redes de telefonia e de dados. A situação ideal é utilizar uma sala com isolamento físico de sinais eletromagnéticos. Entretanto, quando não se dispõe de tal infraestrutura, o analista deve colocar o *smartphone* em modo de voo, avião ou *offline*. A partir do momento que o aparelho está ligado, deve-se imediatamente configurá-lo para esses modos sem conexão, evitando assim a transmissão de dados ou recebimento de chamadas ou mensagens SMS (*Short Message Service*) após o momento da apreensão do equipamento. Se porventura até o momento de isolá-lo da rede, o telefone receber uma chamada, mensagem, e-mail ou qualquer outra informação, o analista deverá documentar e relatar o ocorrido em seu relatório final, que será redigido após o processo de exames e análise dos dados extraídos.

Com o *smartphone* isolado das redes de telecomunicação, o analista pericial verificará se o Android foi configurado para prover algum mecanismo de autenticação, seja uma senha ou um padrão táctil. Em seguida, realizará os procedimentos

descritos nas seções a seguir, que dependem do controle de acesso configurado no dispositivo.

B. Smartphone sem controle de acesso

A situação menos complexa com que um examinador pode se deparar é aquela em que o celular não possui bloqueio e está prontamente apto a ter seus dados extraídos. Nessa situação, primeiramente devem-se extrair os dados dos cartões de memória, caso ainda não tenham sido copiados, e no caso de cartões de memórias removíveis, reinstalar no equipamento os cartões que tenham recebido as cópias, preservando os originais.

Com os dados dos cartões de memória extraídos e devidamente preservados, o examinador deve verificar se o Android possui permissões de "super usuário" habilitadas. O aplicativo denominado "Superuser" pode estar instalado para prover acesso com tais permissões. A partir do momento em que o analista se depara com um *smartphone* Android com permissões de "super usuário", pode-se obter acesso a todos os dados armazenados no dispositivo sem qualquer restrição. Utilizando a ferramenta de depuração ADB (*Android Debug Bridge*), presente no SDK do Android, é possível realizar uma conexão ao dispositivo, acessar um interpretador de comandos (*shell*) com permissões de "super usuário" e realizar a cópia espelho das partições do sistema armazenadas em sua memória interna, conforme ilustrado no Quadro 1.

Quadro 1 - Comandos para listar os dispositivos conectados, obter informações das partições e gerar o arquivo de *dump* de partições.

```
C:\Android\android-sdk\platform-tools>adb devices
List of devices attached
040140611301E014        device

C:\Android\android-sdk\platform-tools>adb -s 040140611301E014 shell
$ su -
su –
# mount | grep mtd
mount | grep mtd
/dev/block/mtdblock6 /system yaffs2 ro,relatime 0 0
/dev/block/mtdblock8 /data yaffs2 rw,nosuid,nodev,relatime 0 0
/dev/block/mtdblock7 /cache yaffs2 rw,nosuid,nodev,relatime 0 0
/dev/block/mtdblock5 /cdrom yaffs2 rw,relatime 0 0
/dev/block/mtdblock0 /pds yaffs2 rw,nosuid,nodev,relatime 0 0# cat /proc/mtd
cat /proc/mtd
dev:   size   erasesize  name
mtd0: 00180000 00020000 "pds"
mtd1: 00060000 00020000 "cid"
mtd2: 00060000 00020000 "misc"
mtd3: 00380000 00020000 "boot"
mtd4: 00480000 00020000 "recovery"
mtd5: 008c0000 00020000 "cdrom"
mtd6: 0afa0000 00020000 "system"
mtd7: 06a00000 00020000 "cache"
mtd8: 0c520000 00020000 "userdata"
mtd9: 00180000 00020000 "cust"
mtd10: 00200000 00020000 "kpanic"
# ls /dev/mtd/mtd*
ls /dev/mtd/mtd*
…
/dev/mtd/mtd6
/dev/mtd/mtd6ro
/dev/mtd/mtd7
/dev/mtd/mtd7ro
/dev/mtd/mtd8
/dev/mtd/mtd8ro
…
# dd if=/dev/mtd/mtd6ro of=/mnt/sdcard/PERICIA/mtd6ro_system.dd bs=4096
dd if=/dev/mtd/mtd6ro of=/mnt/sdcard/PERICIA/mtd6ro_system.dd bs=4096
44960+0 records in
44960+0 records out
184156160 bytes transferred in 73.803 secs (2495239 bytes/sec)
# dd if=/dev/mtd/mtd7ro of=/mnt/sdcard/PERICIA/mtd7ro_cache.dd bs=4096
dd if=/dev/mtd/mtd7ro of=/mnt/sdcard/PERICIA/mtd7ro_cache.dd bs=4096
27136+0 records in
27136+0 records out
111149056 bytes transferred in 41.924 secs (2651203 bytes/sec)
# dd if=/dev/mtd/mtd8ro of=/mnt/sdcard/_PERICIA/mtd8ro_userdata.dd bs=4096
dd if=/dev/mtd/mtd8ro of=/mnt/sdcard/_PERICIA/mtd8ro_userdata.dd bs=4096
50464+0 records in
50464+0 records out
206700544 bytes transferred in 74.452 secs (2776292 bytes/sec)
# ls /mnt/sdcard/PERICIA
ls /mnt/sdcard/PERICIA
mtd6ro_system.dd
mtd7ro_cache.dd

mtd8ro_userdata.dd
```

Cabe esclarecer que, com a realização do procedimento descrito no Quadro 1, as imagens das partições espelhadas serão gravadas no cartão de memória instalado no dispositivo. Em algumas situações, pode não ser possível realizar a substituição do cartão de memória original por outro do analista pericial. Entretanto, independente da sua substituição, os dados da mídia removível devem ter sido espelhados antes de ser realizado o procedimento de espelhamento e cópia das imagens do sistema. Assim, os dados contidos no cartão de memória original, apreendido junto com o *smartphone*, são preservados, com o perito registrando as devidas ressalvas no relatório a ser redigido ao final da análise dos dados extraídos.

Após a realização do espelhamento das partições, é importante observar os processos que estão em execução no sistema e avaliar a real necessidade de se obter os dados de tempo de execução, que se encontram carregados na memória do dispositivo. Assim, é possível extrair os dados da memória utilizados pelos aplicativos que se encontram em execução para ter acesso a informações sensíveis, como senhas e chaves criptográficas. A partir da chamada de um interpretador de comandos com credenciais de "super usuário", altera-se a permissão do diretório "/data/misc", e se interrompe abruptamente processos em execução no sistema, o que gerará um arquivo de *dump* de memória para cada processo terminado [6]. O Quadro 2 apresenta a demonstração da aplicação da técnica descrita por Thomas Cannon [6].

Quadro 2 - Mostra os comandos para modificar permissões da pasta, terminar processos de forma abrupta para geração de arquivos de *dump* de memória de processos e copiar o *dump* de memória para a estação pericial.

```
# chmod 777 /data/misc
chmod 777 /data/misc
# kill -10 6440
kill -10 6440
# kill -10 6379
kill -10 6379
# kill -10 6199
kill -10 6199
# kill -10 5797
kill -10 5797
# ls /data/misc | grep dump
ls /data/misc | grep dump
heap-dump-tm1303909649-pid5797.hprof
heap-dump-tm1303909632-pid6199.hprof
heap-dump-tm1303909626-pid6379.hprof
heap-dump-tm1303909585-pid6440.hprof
#
…
C:\android-sdk\platform-tools>adb -s 040140611301E014 pull /data/misc/heap-dump-
tm1303909649-pid5797.hprof
2206 KB/s (2773648 bytes in 1.227s)
C:\android-sdk\platform-tools>adb -s 040140611301E014 pull /data/misc/heap-dump-
tm1303909632-pid6199.hprof
2236 KB/s (3548142 bytes in 1.549s)
```

```
C:\android-sdk\platform-tools>adb -s 040140611301E014 pull /data/misc/heap-dump-
tm1303909626-pid6379.hprof
1973 KB/s (3596506 bytes in 1.779s)
C:\android-sdk\platform-tools>adb -s 040140611301E014 pull /data/misc/heap-dump-
tm1303909585-pid6440.hprof
1968 KB/s (2892848 bytes in 1.435s)
```

A extração dos dados de um telefone com credenciais de "super usuário" habilitadas pode ser finalizada neste momento.

Ressalta-se que, para a inspeção posterior dos dados extraídos, o analista pericial deve ter um ambiente de exames com ferramentas para montar imagens com suporte ao sistema de arquivos utilizado no dispositivo, geralmente o YAFFS2. Pode-se utilizar a técnica descrita por Andrew Hoog para análise deste sistema de arquivos [4]. Entretanto, é recomendável que seja feita uma cópia lógica dos arquivos do sistema diretamente para a estação pericial, como mostrado no Quadro 3.

Quadro 3 – Cópia dos arquivos lógicos armazenados no diretório "/data" do dispositivo para o diretório "pericia" da estação de trabalho.

```
C:\android-sdk\platform-tools> adb pull /data pericia/
Pull: building file list…
…
684 files pulled. 0 files skipped
857 KB/s (194876514 bytes in 226.941s)
```

Os dados armazenados no diretório "/data", por exemplo, contêm informações a respeito dos aplicativos instalados, bancos de dados, informações sobre configurações do sistema, dentre outras. A cópia lógica de arquivos criará uma redundância que poderá ser útil no momento dos exames, principalmente em situações em que não seja necessário aprofundar a análise das partições do sistema. Ademais, alguns aplicativos podem estar ativos no sistema, sendo que uma simples inspeção visual pode prover informações que seriam de difícil acesso por meio da análise da imagem gerada. Adicionalmente, pode ser avaliada a utilização de ferramentas forenses de extração para auxiliar a interpretação das informações armazenadas.

Em situações em que o *smartphone* Android não apresente permissões de "super usuário", a extração dos dados armazenados na memória interna deve ser realizada por meio de inspeção visual direta na interface gráfica do aparelho. Alternativamente, ferramentas e aplicativos forenses podem ser utilizados para auxiliar o analista a extrair os dados do dispositivo. No entanto, é importante realizar a conferência das informações obtidas por tais ferramentas, já que o sistema Android possui diferentes versões e customizações realizadas pelas operadoras de telefonia e fabricantes de celulares, que podem interferir no funcionamento adequado das ferramentas para extração automatizada. Há diversos aplicativos que podem armazenar informações relevantes para investigação e análise, cuja extração de dados não são suportadas por ferramentas periciais. Torna-se evidente a necessidade de o analista pericial ter conhecimento sobre o Android e seus aplicativos, uma vez que a extração de informações relevantes deve ser feita da forma mais completa possível.

Alguns modelos de *smartphones* Android permitem realizar a cópia da memória interna utilizando vulnerabilidades do *bootloader* do aparelho, sem a necessidade de se possuir as credenciais de "super usuário" no sistema. Cabe ao analista avaliar se é possível e viável a aplicação dessa técnica para aquele tipo de dispositivo. É sugerido que seja discutida com a equipe de investigação a necessidade de aplicação da técnica, e que seus riscos e impactos para os resultados dos exames sejam de conhecimento do responsável pela investigação.

Quanto a ferramentas periciais disponíveis atualmente, cabe citar que a empresa viaForensics desenvolveu um aplicativo disponível gratuitamente para agentes da lei denominado "Android Forensic Logical Application" (AFLogical) [7], cujo objetivo é a extração de informações de *smartphones* Android. Além disso, recentemente foi disponibilizada a ferramenta comercial viaExtract que, segundo a viaForensics, possui funcionalidades mais consistentes e relevantes, como, por exemplo, a geração de relatórios. Outra ferramenta de grande utilidade é o "Cellebrite UFED", cuja versão 1.1.7.5, lançada em julho de 2011, realiza a extração física de dados de alguns modelos sem a necessidade de o sistema estar com as permissões de "super usuário" habilitadas. A mesma ferramenta também possui um *plugin* para visualizar bancos de dados no formato SQLite do Android e tem suporte a aplicativos instalados por padrão no sistema, a exemplo do Gmail, SMS, MMS e contatos.

C. Smartphone com controle de acesso

Caso o celular Android possua o controle de acesso ativado, seja por padrão táctil ou senha, ainda assim é possível ao analista aplicar técnicas para obter acesso ao dispositivo.

Segundo o NIST [5], há três formas de obter acesso aos dados de dispositivos bloqueados. A primeira forma é o método investigativo, por meio do qual o investigador busca no local onde o *smartphone* foi apreendido possíveis senhas ou ainda realiza uma entrevista com o suposto proprietário do aparelho para que ele coopere fornecendo a senha espontaneamente. Outra forma é a de obtenção de acesso por hardware, em que o analista realiza uma pesquisa sobre o modelo em questão para saber se há possibilidade de executar algum procedimento não destrutivo a fim de acessar os dados do aparelho. Para isso, pode ser solicitado apoio dos fabricantes e de assistências técnicas autorizadas. Finalmente, há métodos de acesso por software que, embora dependam do modelo do aparelho e da versão do Android, geralmente são a forma mais simples e que podem ser aplicadas no próprio ambiente de exames do analista pericial.

Para se ter acesso ao sistema, o analista deve fazê-lo da forma menos intrusiva possível, a fim de evitar o comprometimento das evidências. Caso a senha ou o padrão táctil tenha sido obtido no momento da apreensão do dispositivo, esses devem ser prontamente testados. Alternativamente, pode-se usar a técnica para descoberta do padrão táctil por meio de resíduos deixados na tela do próprio dispositivo [8], antes de se tentar qualquer outra forma de ultrapassar o controle de acesso, evitando a contaminação da tela.

Caso o analista não tenha sucesso, ele verifica se o Android está configurado para aceitar conexões de depuração USB por meio da ferramenta disponível no SDK, o ADB. Em tendo sucesso, tenta obter o acesso com credenciais de "super usuário" para retomar o processo de aquisição, da forma que seria executada nos casos em que o dispositivo móvel não estivesse bloqueado, pois com tais permissões, podem-se obter todos os dados armazenados no aparelho, conforme descrito na seção anterior.

Ainda que não se tenha acesso de "super usuário" ao dispositivo, é possível ao analista instalar aplicativos por meio da ferramenta ADB a fim de superar o controle de acesso do sistema. A técnica descrita por Thomas Cannon [9] consiste em instalar o aplicativo "Screen Lock Bypass", disponível no *Android Market*. Nesta técnica, é necessário que a senha da conta Google esteja cadastrada no dispositivo Android, assim como habilitado o acesso à Internet, o que se considera desaconselhável. Desta forma, recomenda-se obter o aplicativo a partir de outro dispositivo Android e instalá-lo via ADB no dispositivo móvel examinado. Assim, é possível realizar o desbloqueio da tela usando a técnica de Cannon sem a necessidade de se ter a senha da conta Google do dispositivo ou tampouco conectá-lo à grande rede. O Quadro 4 demonstra a instalação via ADB do aplicativo desenvolvido por Cannon, assim como sua ativação, que depende da instalação de um segundo aplicativo qualquer, para realizar o desbloqueio do controle de acesso.

Quadro 4 – Conexão via ADB, verificação do acesso *root* e instalação do aplicativo para ignorar o controle de acesso.

```
C:\android-sdk\platform-tools>adb -s 040140611301E014 shell
$ su -
su -
Permission denied
$ exit
...

C:\android-sdk\platform-tools>adb -s 040140611301E014 install screenlockbypass.apk
224 KB/s (22797 bytes in 0.100s)
      pkg: /data/local/tmp/screenlockbypass.apk
Success

C:\android-sdk\platform-tools>adb -s 040140611301E014 install AndroidForensics.apk
716 KB/s (31558 bytes in 0.046s)
      pkg: /data/local/tmp/AndroidForensics.apk
Success
```

Em situações em que não seja possível ignorar o sistema de autenticação ou não se tenha o acesso de depuração USB ativado, resta ao analista realizar a cópia dos dados contidos em um cartão de memória removível eventualmente instalado. Nestas situações, é de grande importância documentar o fato da impossibilidade de acesso ao dispositivo com os procedimentos utilizados. Complementarmente, caso haja outra técnica possível de ser aplicada, seja ela mais invasiva ou complexa, isso deve ser informado a quem solicitou os exames. Desta forma, pode-se discutir as implicações de se aplicar tais técnicas, descrevendo os riscos inerentes a situação, a exemplo de possíveis danos definitivos ao *smartphone* examinado.

D. Documentação da aquisição

Recomenda-se que em todas as técnicas e procedimentos utilizados o analista documente o processo, a fim de subsidiar a etapa de exame e análise dos dados extraídos. Independente do fluxo seguido pelo especialista no *workflow* ilustrado na Figura 1, o processo deve ser registrado, permitindo auditabilidade e confiabilidade dos procedimentos realizados pelo analista pericial.

O analista deve atentar-se de registrar os códigos de integridade dos dados gerados e extraídos no processo de aquisição, assim como informar em seu relatório qualquer ressalva que considere importante para a condução da etapa de exame e análise, a exemplo de um e-mail ou SMS recebido antes de se isolar o *smartphone* das redes de telecomunicação ou até mesmo a existência de aplicativos que contenham informações armazenadas em servidores na Internet, como de computação em nuvem.

O analista pericial, na execução de suas atividades, deve considerar que quanto mais bem descrito o processo de aquisição dos dados, maior confiabilidade será dada ao resultado do exame. O fato de o processo ser bem documentado é o primeiro passo para a realização de uma análise dos dados extraídos de forma imparcial, clara e objetiva.

4. Validação do método de aquisição proposto

O método proposto foi testado com a utilização de uma amostra de seis *smartphones* com o sistema operacional Android instalado. Dentre esses aparelhos, foi possível

TABELA I. Cenários utilizados para validar o método proposto.

Cenários	Ligado	Cartão Removível	Bloqueado	Desbloqueável	Super usuário
Cenário 1 (Sony Ericson Xperia X10 miniPro)	Sim	Não	Não	Não se aplica	Não
Cenário 2 (Motorola Milestone II A953)	Não	Sim	Sim	Sim	Não
Cenário 3 (Samsung Galaxy S 9000[a]) (Motorola Defy)	Não	Sim	Não	Não se aplica	Sim
Cenário 4 (Motorola Milestone A853) (Motorola I1)	Não	Sim	Não	Não se aplica	Não

[a] Além do cartão microSD removível, o celular em questão possui um cartão de memória embutido não removível.

identificar quatro cenários diferentes, resumidos e apresentados na Tabela 1.

No Cenário 1, o smartphone não se encontrava bloqueado e foi colocado em modo de voo a fim de isolá-lo da rede. O modelo do aparelho deste cenário possuía um cartão de memória que não era removível. Os dados do cartão foram espelhados (copiados integralmente), sendo a própria memória utilizada para extração das informações do aparelho por meio do software forense de extração "Android Logical Forensics Application" [7]. Também foi realizada inspeção visual dos dados.

No segundo cenário, como o aparelho encontrava-se desligado, primeiramente seu cartão de memória removível foi retirado e espelhado. Em seguida, reinseriu-se um cartão de memória com a cópia do original. Posteriormente, o *smartphone* foi ligado e colocado imediatamente em modo de voo. Observou-se que o celular encontrava-se bloqueado, mas com acesso de depuração USB ativado. A partir da ferramenta ADB, obteve-se um interpretador de comandos e verificou-se que não havia permissões de "super usuário" disponíveis, o que impossibilitou o espelhamento das partições do sistema. Entretanto, a partir do ADB, foi possível instalar os aplicativos "Screen Lock Bypass" [9], que foi utilizado para desbloquear o equipamento, e o "Android Logical Forensics Application", utilizado para extração dos dados do telefone. Procedeu-se à extração dos dados do aparelho do mesmo modo que foi realizado no cenário anterior.

Da mesma forma que foi realizada no cenário 2, no terceiro cenário, o cartão de memória foi removido, espelhado e substituído, uma vez que o aparelho se encontrava desligado. Em um segundo momento, o *smartphone* foi ligado e imediatamente colocado em modo de voo. Observou-se que o celular encontrava-se desbloqueado, assim como também possuía um segundo cartão de memória embutido. Procedeu-se a realização da cópia espelho deste segundo cartão de memória. O *smartphone* possuía o aplicativo "Superuser", que fornece credenciais de super usuário. Desta forma, habilitou-se o modo de depuração USB, realizou-se uma conexão ADB, obtendo um interpretador de comandos com permissões de "super usuário" para realização do espelho das partições do sistema. Não foi realizada a cópia dos dados em memória RAM, pois o celular encontrava-se desligado e os analistas não julgaram necessário a realização do procedimento. Depois, foi utilizada a ferramenta pericial para extração de dados do telefone Cellebrite UFED System 1.1.7, seguida da inspeção visual para complementação dos dados extraídos pela ferramenta.

Finalmente, no último cenário, o cartão de memória foi removido, espelhado e substituído ainda com o aparelho desligado. Em seguida, o celular foi ligado e imediatamente colocado em modo de voo. Verificou-se que o celular se encontrava desbloqueado. Assim, foi utilizada a ferramenta pericial para extração de dados do telefone Cellebrite UFED System 1.1.7, com posterior inspeção visual para complementação dos dados extraídos.

Os procedimentos citados no método puderam ser diretamente traduzidos para ações desempenhadas nos aparelhos examinados. Desta forma, foi possível realizar a aquisição de dados de todos os celulares inteligentes testados, demonstrando a adequabilidade e validade do método proposto para os diferentes cenários encontrados.

5. Conclusão

A Plataforma Android para *smartphones* já é o mais presente entre esses dispositivos de comunicação móvel. No entanto, as abordagens periciais para exames em aparelhos celulares e computadores não se adequam completamente às peculiaridades dessa classe de dispositivos. Ademais, os modelos atualmente propostos de análise forense em telefones celulares não consideram as peculiaridades de cada plataforma.

Foi proposto então um método específico que direciona as ações do analista pericial para aquisição de dados de aparelhos que utilizam a Plataforma Android, levando em consideração características do sistema operacional, seus aplicativos mais populares e recursos de hardware de seus dispositivos.

A partir da especificação de um método de aquisição de dados do sistema Android, foi possível antever as dificuldades com que os analistas periciais podem se deparar, preparando-os para realizar uma aquisição completa da evidência, dada a situação em que o dispositivo móvel foi encaminhado, evitando imprevistos no processo de extração dos dados e perda de provas periciais.

O método foi definido de maneira abrangente, de forma que as técnicas, procedimentos e ferramentas específicas escolhidas pelo analista no decorrer do *workflow* não interferem em sua aplicação. Assim, havendo novas técnicas com abordagens diferentes para a realização de alguma atividade, seja para desbloqueio de acesso, espelhamento de partições ou até mesmo acesso ao sistema, elas serão abrangidas pelo método proposto, que tem o foco no resultado que a atividade produz.

O método proposto foi validado por meio de sua aplicação no exame de seis *smartphones* Android, que foram enquadrados em quatro cenários, que abordavam diferentes situações que um analista pode se deparar.

Para trabalhos futuros, propõe-se que o método seja validado para o Android 3, avaliando sua eficácia no sistema da Google voltado para dispositivos do tipo Tablet, realizando as adaptações que o novo sistema porventura requeira. Outro trabalho de interesse a ser desenvolvido seria a criação de uma ferramenta forense com suporte ao sistema de arquivos YAFFS2, voltada para memórias flash NAND, facilitando a extração de dados, o acesso e a montagem de imagens das mídias de armazenamento.

6. Agradecimentos

O presente trabalho foi desenvolvido com o apoio institucional do Departamento de Polícia Federal – DPF e com

recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça. Os estudos foram realizados sob a supervisão da equipe de Professores do Departamento de Engenharia Elétrica da Universidade de Brasília, que contribuiu para o direcionamento e produção de conhecimento científico em alto nível.

Referências

[1] Canalys. "Android takes almost 50% share of worldwide smartphone market". Sítio da internet da Empresa Canalys, 1/8/2011. Disponivel em: <http://www.canalys.com/newsroom/android-takes-almost-50-share-worldwide-smart-phone-market>. Acesso em: 3 agosto 2011.

[2] Rossi, M. "Internal Forensic Acquisition for Mobile Equipments", n. 978-1-4244-1694-3. IEEE, 2008.

[3] Association of Chief Police Officers. "Good Practice Guide for Computer-Based Electronic Evidence". Versão 4.0. [S.l.]. 2008.

[4] Google Inc. "Android Fundamentals". Android Developers, 2011. Disponivel em: <http://developer.android.com/guide/topics/fundamentals.html>. Acesso em: 17 março 2011.

[5] SQLite. "About SQLite". SQLite, 2011. Disponivel em: <http://www.sqlite.org/about.html>. Acesso em: 5 abril 2011.

[6] Hoog, A. "Android Forensics - Investigation, Analisys and Mobile Security for Google Android". 1a. ed. [S.l.]: Syngress, 2011.

[7] Jansen, W.; Ayers, R. "Guidelines on Cell Phone Forensics - Recomendations of the National Institute of Standards and Technology". [S.l.]. 2007.

[8] Cannon, T. "Android Reverse Engineering". Thomas Cannon, 2010. Disponivel em: <http://thomascannon.net/projects/android-reversing/>. Acesso em: 23 março 2011.

[9] ViaForensics. "Android Forensics Logical Application (LE Restricted)". Sítio da viaForensics, 2011. Disponivel em: <http://viaforensics.com/android-forensics/android-forensics-logical-application-le-restricted.html>. Acesso em: 03 agosto 2011.

[10] Aviv, A. J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; Smith, Jonathan M. "Smudge Attacks on *Smartphone* Touch Screens". 4th Workshop on Offensive Technologies. Washington, DC: [s.n.]. 2010.

[11] Cannon, T. "Android Lock Screen Bypass". Thomas Cannon, 2011. Disponivel em: <http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/>. Acesso em: 23 março 2011.

André Morum de Lima Simão é Bacharel em Ciência da Computação pela Universidade Católica de Brasília (2000) e Especialista em Gestão da Segurança da Informação pela Universidade de Brasília (2002). Entrou para o quadro de Peritos Criminais Federais do Departamento de Polícia Federal em 2005, onde vem exercendo atividades periciais na sua área de formação. Atualmente é Mestrando em Informática Forense e Segurança da Informação do Departamento de Engenharia Elétrica da Universidade de Brasília.

Fábio Caús Sícoli é Bacharel em Ciência da Computação pela Universidade de Brasília (2004) e Especialista em Criptografia e Segurança em Redes pela Universidade Federal Fluminense (2010). Além disso, é Mestrando em Informática Forense e Segurança da Informação do Departamento de Engenharia Elétrica da Universidade de Brasília e trabalha há seis anos como Perito Criminal Federal no Departamento de Polícia Federal.

Laerte Peotta de Melo possui graduação em Elétrica com ênfase em Eletrônica pela Universidade Presbiteriana Mackenzie-SP (1996), especialização em segurança de redes de computadores pela Universidade Católica de Brasília (2004), perito forense computacional pela Universidade Federal do Ceará (2007), Mestrado em Engenharia Elétrica pela Universidade de Brasília (2008), Doutorando em engenharia elétrica pela Universidade de Brasília. Atualmente é Doutorando Pesquisador pelo Banco do Brasil, trabalhando na área de segurança da informação. Professor em cursos de pós graduação em Brasília. Instrutor da Escola Superior de Redes – RNP, atuando nos cursos Tratamento de incidentes de segurança e Auditoria e Análise forense. Tem experiência na área de Engenharia Elétrica, com ênfase em Sistemas de Telecomunicações, atuando principalmente nos seguintes temas: Segurança da informação, segurança de redes, combate ao crime digital, governança em TI, confiança computacional e software livre.

Flávio Elias de Deus possui graduação em Engenharia Elétrica pela Universidade Federal de Goiás (1998), mestrado em Engenharia Elétrica pela Universidade de Brasília (2001) e Doutorado pela Universidade de Brasília (2006) com Doutorado Sandwich na University of Pittsburgh (2005). Atualmente é Professor Adjunto no Departamento de Engenharia Elétrica-UnB. Tem experiência na área de Redes de Comunicação, atuando principalmente nos seguintes temas: Tecnologia da Informação, Wireless Local Area Network (WLAN), Mobile ad-hoc Networks (MANET) entre outros topicos correlatos.

Rafael Timóteo de Sousa Jr possui graduação em Curso de Engenharia Elétrica pela Universidade Federal da Paraíba, Campina Grande (1984), mestrado (DEA) em Telemática e Sistemas de Informação pela Ecole Supérieure d'Electricité - SUPELEC (1985) e doutorado em Processamento de Sinais e Telecomunicações pela Université de Rennes I (França, 1988). Fez pós-doutorado na Ecole Supérieure d'Electricité - SUPELEC (2006-2007). Atualmente é professor adjunto da Universidade de Brasília, curso de Engenharia de Redes de Comunicação. Tem experiência em Engenharia de Software e Engenharia de Redes de Comunicação, atuando principalmente nos seguintes temas: segurança da informação e confiança computacional, gerência de redes, mobile ad-hoc networks (manet), computação distribuída na Internet.