Validando a Técnica de Destruição de Dados no Android.

Fernando Colosio[1], Gustavo Rotondo[1], Gustavo Amaral[2], Rodrigo Silva[2], Érico Amaral[1]

[1]Engenharia de Computação – Universidade Federal do Pampa (UNIPAMPA)
Avenida Maria Anunciação Gomes de Godoy, n°1650 – Bagé – RS – Brasil

[2]Análise e Desenvolvimento de Sistemas - Instituto Federal Sul-Rio-Grandense (IFSUL)
Av. Leonel de Moura Brizola, n° 2501 – Bagé – RS – Brasil

fernando.colosio@hotmail.com, gustavo.rotondo@gmail.com,
gustavo.h.amaral@gmail.com, orki2008@gmail.com, ericoamaral@unipampa.edu.br

Abstract. *Mobile devices are widely used by different types of users, from the user who uses it to the corporate environment, to the user who is using the device for leisure. Having this range of profile, each user has a priority of the type of information stored on your device and it is critical that the user has full control over those files, either at the time of exclusion or keep the files. This study shows some techniques for the destruction of data on mobile devices. At the end of the study it was noted that some applications were able to be effective in the information cleaning process.*

Resumo. *Dispositivos móveis são amplamente utilizados para diferentes tarefas por diversos tipos de usuários, do uso pessoal ao corporativo. Baseado nesta gama de perfis e, reconhecendo que cada utilizador tem uma prioridade quanto ao tipo de informação armazenada em seu dispositivo, é de suma importância que o usuário possua um controle total sobre os seus dados, seja no momento da exclusão dos mesmos, ou até durante a manipulação de seu dispositivo. Este estudo aponta algumas técnicas para o controle e destruição de dados em dispositivos móveis. Ao final deste estudo constatou-se a efetividade, de algumas ferramentas, no processo de higienização dos dados em equipamentos com a plataforma Android.*

1. Introdução

Ao longo da evolução computacional, os dispositivos tornaram-se menores, mais pessoais e com maior poder de processamento, devido ao fato da miniaturização dos componentes, porém não só o poder computacional dos diversos aparelhos disponíveis aumentou como também a geração de informações ao longo dos anos. Estima-se que em 2015, foi gerado cerca de 8 zettabytes de dados. COSTA (2012). Muitos destes contendo informações pessoais e sigilosas dentre outros arquivos importantes. Com isso existe o risco de algum arquivo ser deletado de forma intencional. Para contornar esta situação, foram criadas ferramentas capazes de examinar a memória do dispositivo procurando pelos elementos excluídos. Esses utilitários partem do princípio de rastreio de ponteiros que apontavam para os arquivos na memória através de um escaneamento profundo no armazenamento do dispositivo.

Nos sistemas computacionais atuais, ao apagar um arquivo da memória, o dado não é removido completamente e sim ocorre a exclusão do ponteiro, que faz a referência para o local onde estão armazenados os dados. Algumas aplicações possuem a função de destruir as informações reescrevendo várias vezes na memória a ponto de não ser mais possível localizar o

ponteiro que fazia tal referência. O estudo busca apresentar maneiras de sanitarização de disco em dispositivos móveis visando à privacidade do usuário.

2. Referencial teórico

2.1. Sistemas de Arquivos

O sistema de arquivos é a maneira com a qual o computador acessa os arquivos salvos em disco. O tipo de estrutura determina por exemplo, como o arquivo será acessado, os tipos de permissões de cada usuário e o formato de armazenamento. Atualmente o sistema operacional *Android* é proveniente de derivações *Linux*, as quais por consequência façam que estrutura adote a maioria de suas características, inclusive o tipo de gerenciamento de arquivos: *EXT4*. Que trabalha como base o sistema *EXT3* derivado do *EXT2* que utiliza o *journaling* uma técnica que consiste em criar um registro que tem a finalidade de recuperar o sistema em caso de um desligamento não programado. O processo consiste em 3 níveis de implementação: *Journal*: os metadados e os dados dos arquivos são escritos no *journal* antes de serem de fato escritos no sistema de arquivos principal. *Writeback*: as informações são escritas no *journal* mas não o conteúdo dos registros. *Ordered*: é como o *writeback*, mas força que a escrita do conteúdo dos documentos seja feita após a marcação de seus metadados como escritos no *journal*. Esse é considerado um meio-termo aceitável entre confiabilidade e performance, sendo, portanto, o nível padrão TWEEDIE (2000).

2.2. Técnicas para exclusão segura de dados

Para destruição de dados em um disco, existem diversos métodos, dentre eles destacam-se as técnicas de *Gutmann*, *Degaussing*, *DOD5220.22-M* e *VSITR*.

Degaussing, que consiste basicamente em sobrescrever todas as posições do disco por um único caractere, ocorrendo a seguir a verificação das posições sobrescritas, escrevendo por cima de todas as posições por caráter aleatório, verifica novamente o disco e por fim termina de recapeá-lo antes de sua utilização Ibanez (2009).

Segundo Gutmann (1996), para a eliminação segura dos dados, é necessário sobrescrever um bloco de disco várias vezes com alternância de padrões e em diferentes freqüências. Para ter uma abrangência aceitável de consistência, ele especificou 22 padrões de dados para sobrescrever o disco e usa 35 passos de sobrescrita em cada aglomerado do disco: o *DOD5220.22-M* consiste em três etapas de sobrescrita, na primeira vez o bloco e sobrescrito por zeros, na segunda por ums na terceira e última aleatoriamente, apesar de ter sido criado pelo Departamento de Defesa dos Estados Unidos é um método de exclusão falho pois ferramentas forenses são capazes de recuperar os dados excluídos BARRETO (2009); o método *VSITR* propõe sete sobrescritas do disco, na primeira vez com zeros, na segunda com uns, na terceira com zeros, na quarta com uns, na quinta com zeros, na sexta com uns, na sétima e última com zeros, objetivando desestabilizar qualquer vestígio de dados que possa estar contido na região do disco Barreto(2009).

2.3. Ferramentas de sanitarização para plataforma Android

Sanitarização de disco é a maneira de efetuar uma limpeza segura dos dados armazenados em HDs (discos rígidos) de servidores, estações de trabalho e *notebooks*, dentre outros, evitando assim o vazamento de informações (PRODESP, 2015).

Através do aplicativo *SDelete* foram feitas as exclusões de arquivos no sistema *Android*. Para usá-lo não foi necessário fazer *backup* de dados, ter feito o *root* no dispositivo e nem ter acesso à Internet. Com esse *app* eliminamos qualquer arquivo da memória interna ou do cartão SD do telefone de maneira definitiva. Não é preciso ter permissões especiais para usá-lo no aparelho, reforçamos que com o uso da ferramenta a recuperação dos dados fica impossibilitada de recuperação.

2.4. Trabalhos Correlatos

Concomitante a esta pesquisa, alguns trabalhos correlatos foram investigados, a fim de se verificar o estado da arte relacionado a este estudo, dentre os quais destaca-se o trabalho de Dibb & Hammoudeh (2013). Para estes autores, a área de recuperação de dados em sistemas operacionais móveis é de suma importância na área forense para solução de crimes. As informações armazenadas em um dispositivo móvel tais como: *logs* de ligações, históricos de acesso web, mensagens *SMS*, etc. podem ser provas determinantes em uma investigação criminal. Os pesquisadores fizeram o uso de uma ferramenta específica para realizar a coleta de dados em um aparelho. O utilitário questão possibilitou a recuperação de comunicações e *logs* de aplicações do sistema *Android* tais como: *Google Maps, Facebook, Twitter e Whatsapp.*

3. Metodologia e Implementação

A metodologia adotada neste estudo tem caráter quantitativo, o qual visa apresentar as ferramentas obtiveram melhor êxito na destruição de dados contidos em um dispositivo carregado com a plataforma Android.

A metodologia utilizada para o desenvolvimento desta pesquisa seguiu um conjunto de 3 etapas distintas: A primeira etapa consistiu na identificação da importância do estudo sobre o tema destruição de dados, visto a demanda atual na utilização de dispositivos móveis. O estudo e definição das ferramentas que deveriam ser utilizadas para a execução dos experimentos foram definidas na etapa dois. A terceira e última etapa consistiu na análise dos resultados obtidos.

Para os experimentos realizados nesta pesquisa adotou-se um conjunto de ações técnicas, sobre um dispositivo *Alcatel Hero2C* (*TCL-7055A*), rodando a versão 4.4.2 do sistema operacional *Android*. Para a escolha das aplicações para exclusão de dados foi considerado o nível de maturidade destas, na loja de aplicativos, além da avaliação por parte dos seus usuários.

Para a obtenção dos resultados foram manipulados 2 tipos de dados no *smartphone*: uma imagem (exemplo*.jpg*) e um arquivo de audio (exemplo.*ogg*), ambos armazenados no cartão de memória interno do aparelho. Posteriormente executou-se, individualmente, as aplicações selecionadas. O procedimento para a observação e coleta de dados consistiu em excluir e recuperar, sucessivamente, os arquivos criados para o experimento.

Para a realização sanitização da memória do dispositivo, foi selecionado o aplicativo *SDelete*[1]. Para a análise da eficiência do aplicativo, posteriormente a execução das ferramentas, e a ferramenta *Disk Digger*[2] para a recuperação de arquivos. Tal ferramenta foi escolhida com base nas avaliações da mesma na *Google Play Store* e estudos realizados sobre recuperação de dados na plataforma *Android*. A mesma é capaz de recuperar através do método de *carving*, cerca de 20 tipos de arquivos diferentes tanto da memória interna ou externa do dispositivo.

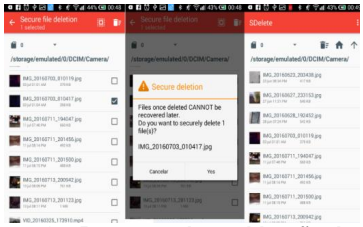

Figura 01. Processo de sanitização de um arquivo de áudio através da ferramenta SDelete

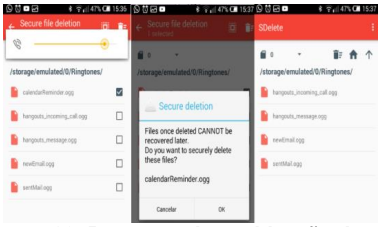

Figura 02. Processo de sanitização de um arquivo *.jpg* através da ferramenta SDelete

A aplicação *SDelete* obteve êxito na sanitização da memória do aparelho. Após a execução da mesma, foi constatada a exclusão dos arquivos selecionados no armazenamento do dispositivo. Posteriormente foi executado a aplicação *DiskDigger* para recuperação de dados a qual não alcançou sucesso em recuperar as informações excluídas com a ferramenta.

4. Conclusões

As aplicações analisadas tiveram desempenhos satisfatórios. A comprovação se deu através de um aplicativo capaz de restaurar os ponteiros da estrutura de arquivos do sistema *Android*, o que torna alta a eficácia de recuperação de dados.

Mesmo após a remoção dos arquivos utilizando as ferramentas analisadas, o *app* de recuperação não foi capaz de fazer a restauração dos arquivos. Foi observado que a aplicação de reciclagem de dados foi capaz de restaurar dados mesmo após uma formatação completa do sistema, porém ao tentar recuperar o dado excluído pela ferramenta *SDelete*, o *app Disk Digger* não foi capaz de traze-lo de volta, comprovando assim a eficácia da sanitarização feita no aparelho.

Como trabalhos futuros, pretende-se desenvolver uma aplicação para a destruição de dados que adote técnicas efetivas para este fim, além de métodos que permitam a validação deste processo.

Referências

BARRETO, G. L. (2009). Utilização de técnicas anti-forenses para garantir a confidencialidade. Curitiba, PUCPR. Disponível em: http://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC. Acessado em 02/06/2015

COSTA, LUIS HENRIQUE MK, et al. (2012). "Grandes Massas de Dados na Nuvem: Desafios e Técnicas para Inovaç ao."

DIBB, P., & HAMMOUHED M**.** (2013). Forense Data Recovery from Android OS Devices: An Open Source Toolkit. Manchester – ING.

DIBB, P. & HAMMOUHED, M. (2013, August). Forensic Data Recovery from Android OS Devices: An Open Source Toolkit. In Intelligence and Security Informatics Conference (EISIC), 2013 European (pp. 226-226). IEEE.

PRODESP (2015). Sanitarização de disco. Disponível em <http://www.prodesp.sp.gov.br/servicos/servicos_pdfs/sanitarizacao.pdf> Acessado em 03/09/2016

TWEEDIE, Stephen C. EXT3. Journaling File System. olstrans. sourceforge. net/release/OLS2000-ext3/OLS2000-ext3. html, 2000.

GUGIK, G. (2009). A História dos computadores e da computação Disponivel em: http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-dacomputacao.htm. Acessado em 02/06/2015

GUTMANN, P. (1996, July). Secure deletion of data from magnetic and solid-state memory. In Proceedings of the Sixth USENIX Security Symposium, San Jose, CA (Vol. 14).

HABERLAND, JURI. Linux EXT3 FAQ. Disponivel em: http://batleth.sapienti-sat.org/projects/FAQs/ext3-faq.html. Acessado em 06/05/2016

IBANEZ MAMANI, R. A. (2009). Métodos de Limpieza (Degaussing y Gutmann). Revista de Información, Tecnología y Sociedad, 15.