Computação forense: uma aplicação de softwares livres para recuperação de dados digitais

Bruno De Souza Eduardo[1], Fabrício Augusto Beijo Carvalho[1], André Ricardo Prazeres Rodrigues[1]

[1]Sistemas de Informação – Universidade Geraldo Di Biase (UGB)
27.213-080 – Volta Redonda – RJ – Brasil

bruno_souza_eduardo@hotmail.com, fabricio.carvalho_@hotmail.com, andrepraz@gmail.com

Abstract. *This article studies the application of free software capable of recovering files that have already been deleted from a Hard Disk or Flash Driver. It details the concept of Forensic Computing, along with its applications and solutions in the cyber world, and in which scenarios can be applied. The application of these free software has great importance to keep the data safe, making this data to be backed up, for example, and also to show how it can be recovered after deletion. The application of these free software is safe to the point that before the recovery of data, an image copy of the storage device is performed so that it is not lost in any moment, for example, and also show how it can be recovered after deleted.*

Resumo. *Este artigo estuda a aplicação de softwares livres capazes de recuperar arquivos que já foram deletados de um Hard Disk ou Flash Driver. Detalha o conceito da Computação Forense, juntamente com suas aplicações e soluções no mundo cibernético, e em quais cenários podem ser aplicados. A aplicação destes softwares livres tem grande importância para manter os dados em segurança, fazendo com que esses dados tenham backup, por exemplo, e, mostrar como é possível recuperá-los após deletados. A aplicação desses softwares livres é segura ao ponto de, antes da realização da recuperação de dados, ser realizada uma cópia da imagem do dispositivo de armazenamento para que em nenhum momento seja perdido.*

1. Introdução

A popularização da Internet, que ocorreu nos anos 90, devido à criação do serviço de *World Wide Web* (WWW), permitiu que usuários espalhados pelo mundo pudessem trocar dados e informações em poucos milissegundos, permitindo maior velocidade e rapidez na comunicação entre máquinas e, consequentemente, entre as pessoas (ELEUTÉRIO e MACHADO, 2011).

Atualmente, apenas alguns minutos transcorrem entre conectar-se à Internet e ser atacado por outra máquina – e isso é apenas o ruído de fundo dos ataques sem um alvo

específico. Houve uma época em que um computador poderia funcionar ano após ano sem sofrer ataques (FARMER e VENEMA, 2005).

Cada vez mais pessoas estão tendo acesso a qualquer meio digital, seja um notebook, celular, tablet ou qualquer outro dispositivo. Toda essa evolução traz benefícios tanto para os usuários, que realizam atividades comuns do dia a dia como o acesso as redes sociais, quanto para as empresas, que aproveitam a praticidade das novas tecnologias para automatizar seus processos os deixando mais simples e eficiente. Mas com todo esse crescimento, paralelamente, surgem os crimes digitais, que é onde a perícia forense entra para dar respaldo técnico e permitir solucionar esses crimes.

Segundo QUEIROZ e VARGAS (2010), a forense computacional é um conjunto de procedimentos e metodologias com a função de investigar e armazenar evidências que possam responder se houve ou não um crime, tendo como base de análise equipamentos de processamento de dados (computadores pessoais, laptops, servidores, estações de trabalho ou outras mídias eletrônicas).

É nesse contexto que surge no Brasil o Perito Forense Computacional. Esse profissional deverá ser criterioso com a forma de lidar no ambiente a ser investigado. Sua atenção deverá estar voltada para os equipamentos ligados (em uso) na cena de um crime, deve desliga-los ou não. Atenção também, na verificação, se durante a retirada de equipamentos de um ambiente, estará ou não apagando evidencias de dispositivos por eletromagnetismo. E orientar a forma correta de guardar esses equipamentos (ROCHA, 2018).

Ainda segundo ROCHA (2018), durante uma investigação, o perito deve estar atento quanto as licenças de software e hardware utilizadas na obtenção de provas. Estas provas poderão ser invalidadas caso o perito tenha utilizado em seu laboratório software pirata, ou que tenha sido alterado sem a devida autorização do autor, podendo o seu laudo ser invalidado diante do juiz.

SILVA e OLIVEIRA (2014) apresentam um estudo sobre as ferramentas computacionais baseadas em software livre e as principais técnicas disponíveis para uma perícia forense computacional. Para isso foram utilizadas as ferramentas Forense Digital *ToolKit* (FDTK-UbuntuBr) e *Computer Aided Investigative Environment* (CAINE), duas distribuições Linux que possuem um vasto conjunto de ferramentas que atendem aos diversos processos de investigação. Dentre algumas ferramentas apresentadas, foram utilizadas ferramentas para a recuperação de dados de ambas as plataformas (FDTK-UbuntuBr e CAINE), realizando ao final um comparativo entre as ferramentas.

Neste artigo, o objetivo é realizar a recuperação de arquivos já deletados da memória de dispositivos de armazenamento mais comuns, por meio dos principais softwares livres baseados em *LINUX*, assim sendo possível fazer com que provas apagadas de algum dispositivo, por exemplo, sejam novamente coletadas para a montagem de um dossiê de uma investigação criminal.

2. A Computação Forense

Com o avanço tecnológico hoje existem vários dispositivos de armazenamento além do computador, tais como: discos ópticos (*CD-ROM e DVD-ROOM*), *external Hard Disk*, *Pendrive*, cartão de memória, dentre muitos outros. E todos esses dispositivos podem armazenar dados que possam ser evidências de um crime de informática.

A maioria dos aplicativos de computador necessita armazenar e recuperar informações, e boa parte dessas informações necessitam ser guardadas por um bom período. Essas informações podem ser armazenadas em mídias internas ou externas e organizadas em unidades chamados arquivos. O gerenciamento desses arquivos é realizado por uma parte do sistema operacional, normalmente conhecido como sistema de arquivos, o qual deverá prover mecanismos de acesso às informações tais como: criação, alteração, proteção, entre outros (TANENBAUM e WOODHULL, 2000).

Um sistema de arquivos consiste em um conjunto de estruturas lógicas e de rotinas que permitem ao sistema operacional controlar o acesso ao disco rígido. Diferentes sistemas operacionais usam diferentes sistemas de arquivos (MORIMOTO, 2002).

Para FILHO (2012), os sistemas de arquivos relacionam à forma como os dados são armazenados, organizados e acessados em um local de armazenamento digital. É um artificio imposto pelo sistema operacional e não pelo hardware.

O *MS Windows* suporta quatro tipos de sistemas de arquivos: *CDFS, UDF, FAT e NTFS*. Cada sistema determina como os arquivos e diretórios são organizados, o formato dos nomes dos arquivos, desempenho e segurança de acesso aos dados. O *CDFS (CD-ROM File System)* oferece suporte a dispositivos como *CD-ROM* e *DVD's*. O *UDF (Universal Disk Format)* é uma evolução do *CDFS*, e é voltado para *CD's* e *DVD's* (MACHADO e MAIA, 2013).

O crescimento da indústria de recuperação de dados e evidência digital vem acompanhado do forte crescimento do número de ferramentas para forense computacional (MOHAY, ANDERSON, et al., 2003).

A Computação Forense é a ciência que, através de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo (ELEUTÉRIO e MACHADO, 2011).

Muitas situações requerem a recuperação de dados no sistema de arquivos, seja por uma perda acidental ou intencional. Sendo assim foi desenvolvida uma variedade de aplicativos e ferramentas qualificados para essa recuperação de arquivos conhecidas como ferramentas forenses, que podem recuperar dados diretamente de um dispositivo físico ou lógico, como um disco rígido ou uma partição desse disco bem como recuperar dados a partir de uma imagem.

3. Materiais e métodos

O *FDTK (Forense Digital Toolkit)* é uma ferramenta voltada para a prática da Forense Computacional. Foi a primeira ferramenta *open source* voltada para a área de computação forense desenvolvida por brasileiros e totalmente em português. Atualmente, a *FDTK* está na versão 3.0 e conta com a comunidade Linux para implementação de melhorias. Pode ser usado também como *Live CD* ou a partir de um *pendrive* rodando sobre qualquer Sistema Operacional (CAVALCANTI, 2016).

O estudo consiste em utilizar a ferramenta *FDTK*-Ubuntu que é um software livre baseado em *LINUX*, para fazer a recuperação de arquivos de um dispositivo de armazenamento, depois de ter sido formatado e/ou ter tido seus arquivos deletados. Utilizou-se, mais precisamente, os comandos *dd* (criação da imagem) e *SCALPEL* (recuperação dos arquivos).

Uma das facilidades do *FDTK*-Ubuntu é estar totalmente em Português. Também, tem-se a possibilidade de a instalação ser realizada em um dispositivo de armazenamento comum. Ou então, o sistema operacional pode ser instalado em uma máquina virtual (VM), sendo assim, exigindo alguns requisitos a mais da máquina, como por exemplo, um mínimo de memória temporária disponível para que a VM venha a trabalhar sem problemas.

Para a realização dos testes utilizou-se um *pendrive* de 2Gb formatado no sistema de arquivo *FAT*. Criou-se uma imagem do *pendrive* e a partir dele buscou recuperar os dados. Não há restrição do tamanho do dispositivo de armazenamento em que se queira trabalhar, porém, quanto maior a capacidade de armazenamento, maior a demora para realização da ação, devido a varredura em todos os bits do dispositivo.

4. Resultados

Conforme descrito no material e método, buscou-se simular a perda dos dados do *pendrive* formatando-o. Supondo que um usuário tenha restaurado os padrões do dispositivo, conforme mostrado na (Figura 1).

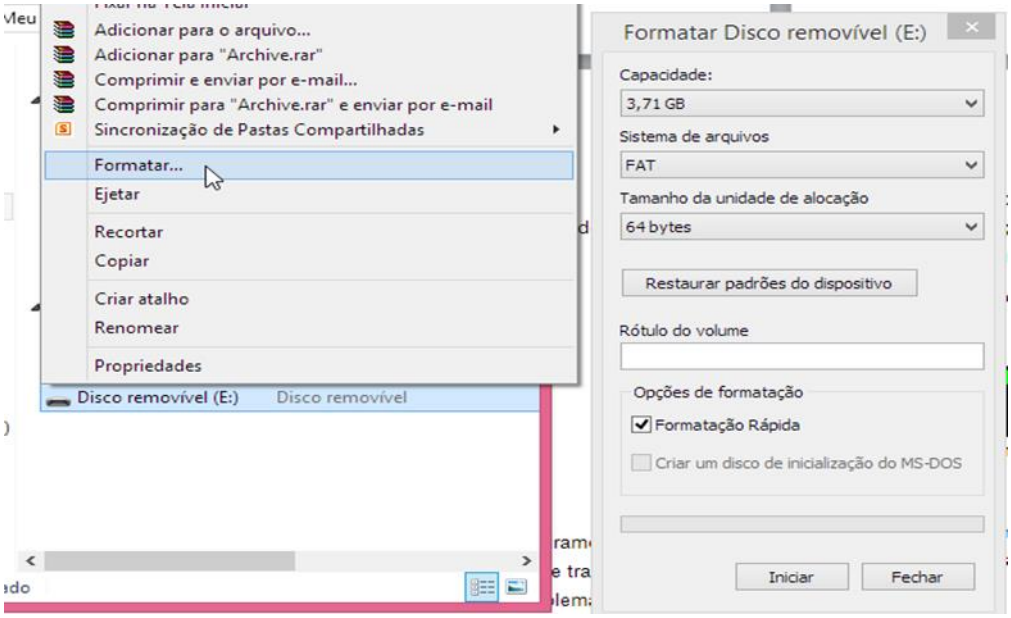

Figura 1: Formatando o dispositivo.

Com isso, todos os arquivos que estavam armazenados no dispositivo foram deletados. A partir desse momento, é possível utilizar a ferramenta estudada para fazer a análise do caso, e então, executar a recuperação dos arquivos.

1º passo: Para a recuperação dos arquivos, cria-se uma imagem do dispositivo, ao qual os arquivos foram apagados. Deve-se trabalhar na cópia do arquivo, e não no próprio dispositivo. Isso evita eventual problema nos arquivos que serão ocasionalmente recuperados, nesse caso. Segue, na (Figura 2), o comando a ser aplicado para criar a imagem, e então, o resultado da criação.

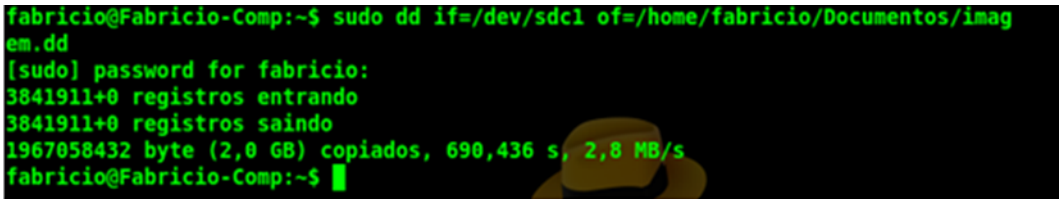

Figura 2: Criação de Imagem Forense.

2º passo: Deve se abrir o *SCALPEL* em um editor de texto, para então, se definir qual a extensão de arquivo se deseja ser recuperado. Exemplo: *.png, .jpeg, .pdf, .docx, .jpg* entre outros. O teste do artigo foi realizado com arquivos extensão *.jpg*.

Com o editor de texto aberto para edição, conforme a (Figura 3) deve-se apagar o símbolo "#" da frente da extensão. Depois dessa modificação, toda a recuperação dos arquivos será sob essa extensão definida.

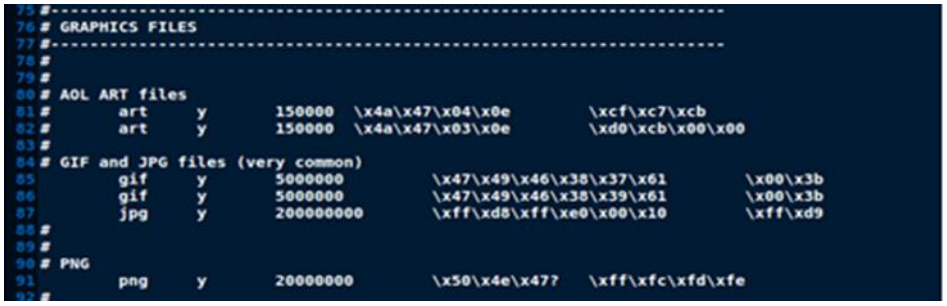

Figura 3: Exibição do editor de texto.

Por último, como mostrado na (Figura 4), aplica-se o comando para a recuperação dos arquivos, ao qual foi selecionado a extensão no editor de texto do *SCALPEL*.

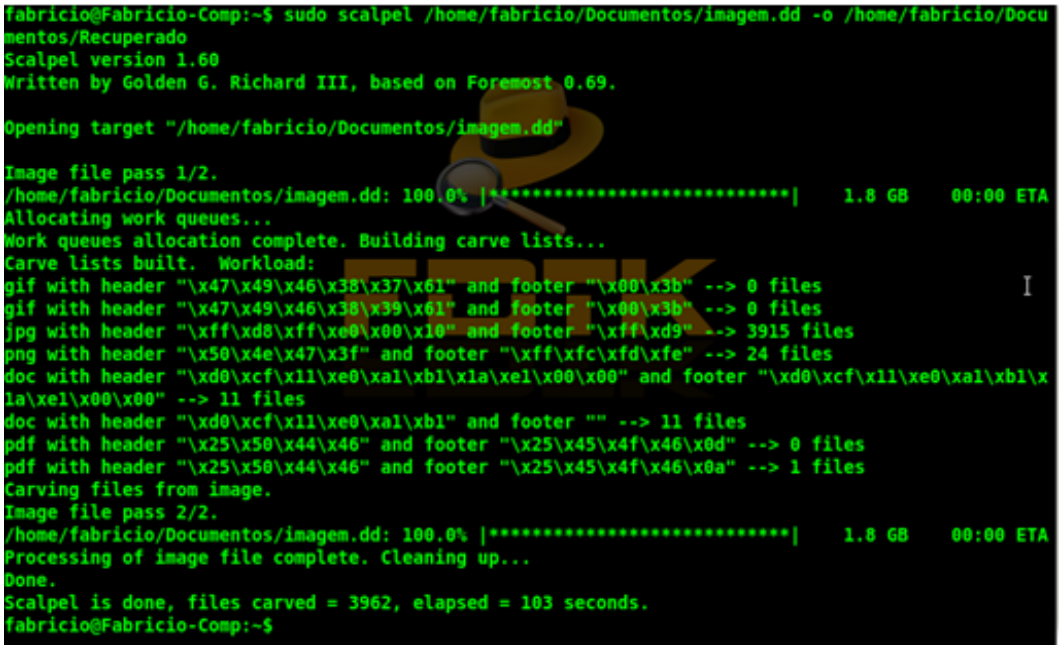

Figura 4: Recuperação dos arquivos.

Para o comando aplicado, temos o arquivo de imagem em que se deve fazer a recuperação, e para a origem da recuperação, foi criada uma pasta “Recuperado”, para todos os arquivos recuperados serem armazenados.

Foram utilizados um total de 1130 itens, totalizando 37,8 MB. Para o ambiente de teste, foi realizado o procedimento conforme descrito acima, e então, dos 1130 itens, 1129 foram recuperados. Na (Tabela 1) foi mostrado o total de arquivos recuperados. “Recuperado” corresponde a primeira realização do procedimento, e “Recuperado1” corresponde a segunda realização do procedimento. Ambos os resultados foram iguais.

Tabela 1 – Comparativo dos testes para recuperação dos arquivos

Taxa de recuperação: Tabela de resultados		
#	Total Arquivo	Total MB
Recuperado	1119	34,7
Recuperado1	1119	34,7

5. Considerações Finais

Neste artigo foi abordado o conceito sobre a computação forense, sua metodologia e como ela vem a ser útil em diversas ocasiões, como na recuperação de arquivos de dispositivos de armazenamento por meio de softwares livres.

Embora exista diversos dispositivos de armazenamento e uma variação de técnicas de recuperação de dados, utilizou-se um *pendrive* e a distribuição *FDTK*-Ubuntu em Português.

Pela observação dos aspectos analisados, conclui-se que a ferramenta forense *FDTK*-Ubuntu com sua aplicação *SCALPEL* possibilita fazer a recuperação de arquivos no dispositivo de armazenamento *pendrive*, que tenha sido formatado, ou então, que seus arquivos tivessem sido apagados.

Recomenda-se fazer o estudo em outros dispositivos de armazenamentos, bem como na quantidade de dados e no tempo em que os dados levaram para serem recuperados.

6. Referências

CAVALCANTI, B. B. Crimes digitais: A fragilidade da legislação brasileira no Direito Digital e demonstração de perícia forense, Rio De Janeiro, 2016.

ELEUTÉRIO, P. M. D. S.; MACHADO, M. P. Desvendando a Computação Forense. São Paulo: Novatec, 2011.

FARMER, D.; VENEMA, W. Perícia Forense Computacional - Teoria e prática aplicada. São Paulo: Pearson Prentice Hall, 2005.

FILHO, J. E. M. Descobrindo o Linux: Entenda o Sistema Operacional GNU/Linux. 3. ed. São Paulo: Novatec, 2012.

MACHADO, F. B.; MAIA, L. P. Arquitetura de Sistemas Operacionais. 5. ed. Rio De Janeiro: LTC, 2013.

MOHAY, G. et al. Computer and Intrusion Forensics. [S.l.]: Artech House, 2003.

MORIMOTO, C. E. Hardware Manual Completo. 3. ed. [S.l.]: [s.n.], 2002.

QUEIROZ, C.; VARGAS, R. Investigação e perícia forense computacional: certificações, leis processuais e estudos de caso. Rio de Janeiro: Brasport, 2010.

ROCHA, M. F. ATUAÇÃO DO PERITO FOSENSE COMPUTACIONAL NO BRASIL. Unisul, Uberaba, 2018.

SILVA, V. A.; OLIVEIRA, C. H. D. Análise De Ferramentas Livres Para Perícia Forense Computacional. Caderno de Estudos Tecnológicos - Faculdade de Tecnologia de Ourinhos, São Paulo, 2014.

TANENBAUM, A. S.; WOODHULL, A. S. Sistemas Operacionais: Projeto e Implementação. 2. ed. Porto Alegre: Bookman, 2000.