

Recuperação de Dados em Pen-Drive Utilizando as Ferramentas Autopsy e Foremost: Fases para o Processamento de Evidências

Ligia M. O. Campos, Everaldo Gomes, Henrique P. Martins

Faculdade de Tecnologia de Bauru – Redes de Computadores (FATEC-Bauru)
CEP 17.015-171 – Bauru, SP – Brasil

ligia.maira@hotmail.com, {everaldogoms,henmartins}@gmail.com

***Abstract.** This research aims to describe the phases and the proper procedures for recovering storage device data, analyzing the computational forensics tools: Autopsy Forensic Browser and Foremost, used for information retrieval, review the evidence and give it probative value before a jury. Check which of the tools used is the best performer, stressing the runtime and the performance of these tools.*

***Resumo.** Esta pesquisa tem como objetivo descrever as fases e os procedimentos adequados para a recuperação de dados em dispositivo de armazenamento, analisando as ferramentas de análise forense computacional: Autopsy Forensic Browser e Foremost, usadas para recuperação das informações, avaliar as provas e atribuir valor probatório perante um júri. Verificar qual das ferramentas utilizadas possui a melhor performance, salientando o tempo de execução e o desempenho dessas ferramentas.*

1. Introdução

Dados são frequentemente excluídos de dispositivos de armazenamento, através do simples processo de exclusão ou pelo processo de formatação, e esses dados podem colaborar com a solução de crimes. Para a recuperação de dados em pen-drive é necessário o cumprimento de fases e procedimentos técnicos específicos. A computação forense possui ferramentas capazes de recuperar informações excluídas, para a recuperação serão utilizadas ferramentas de acesso gratuito, proporcionando fácil acesso às ferramentas e será descrito como cada ferramenta funciona, facilitando sua utilização.

Eleutério e Machado (2010) relatam que a análise pericial mais solicitada na computação forense é o exame em dispositivos de armazenamento, esse exame é formado de quatro fases: preservação, extração, análise e formalização, as fases iniciam-se no recebimento dos dispositivos e concluem-se com a entrega do laudo pericial. Para a análise serão utilizadas algumas técnicas, entre elas a recuperação de arquivos apagados.

Precauções são necessárias para evitar a perda de informações e a fragilidade do dispositivo de armazenamento não deve ser negligenciada, sendo necessários cuidados especiais contra descarga eletrostática, poeira, excesso de umidade e calor.

Conforme Eleutério e Machado (2010) o profissional deve utilizar ferramentas e softwares forenses para garantir que os dados não sofram alterações. Destaca que toda a

análise forense deve ser efetuada na cópia fiel criada a partir do dispositivo original. Recomenda ainda que seja feito o registro com o conteúdo dos dados do dispositivo, o profissional pode utilizar o cálculo do *hash* (cálculo utilizado sobre os arquivos de dados e sequências de texto ou informação de forma a permitir e verificar alterações no conteúdo dos arquivos) de partes ou do seu conteúdo total. Enfatiza que após esta fase o dispositivo será lacrado e mantido em local seguro.

Para Farmer e Venema (2007) os dados originais devem ser protegidos e ficar em seu estado puro, todos os procedimentos serão efetuados na cópia dos dados, enfatiza que em cada camada que faz parte da hierarquia das abstrações que compõem os sistemas de computador, após ser excluída a informação permanece congelada, mesmo que as informações se tornem ambíguas conforme descemos para camadas mais baixas, essas informações tornam-se mais resistentes.

Segundo Farmer e Venema (2007) uma análise absoluta abrange a coleta e o processamento das informações, quanto mais exatos e completos os dados, melhor e mais interessante será a avaliação. Relata ainda que existem três atributos que podem auxiliar o perito em sua análise, o *atime*, que demonstra a última data/hora de acesso do arquivo ou pasta, o *mtime* que se altera quando ocorre uma modificação no conteúdo de um arquivo, e o *ctime* faz o controle da mudança de conteúdo ou das metainformações do arquivo. O atributo *ctime* também nos dá a percepção de quando o arquivo foi excluído.

Eleutério e Machado (2010) a última fase é a formalização que consiste na elaboração de um laudo pericial, indicando o resultado, apresentando todas as evidências encontradas no material analisado, e todas as técnicas utilizadas para a preservação, extração e análise, também devem ser incluídas no documento.

Este trabalho dispõe-se a auxiliar no aprimoramento do profissional que atua na área de Perícia Forense Computacional, objetivando demonstrar as fases e os procedimentos adequados para a recuperação de dados em dispositivo de armazenamento, analisar as ferramentas, Autopsy Forensic Browser e Foremost utilizadas para a recuperação de informações e verificar qual das ferramentas utilizadas apresenta os melhores resultados, enfatizando o tempo de execução e o desempenho.

2. Material e Método

Para realização desta pesquisa foi inicialmente realizada uma revisão de literatura a fim de estudar e compreender os conceitos necessários, em seguida foram realizados os procedimentos práticos, estes procedimentos foram feitos em um notebook com processador Intel core i3-2328M CPU 2.20 Ghz, com 8G de RAM, com um disco rígido de 500G e com o sistema operacional (S.O.) Linux Mint 17. Utilizando o software VirtualBox 4.3.6, instalou-se uma máquina virtual com o S.O. Deft 7, com 1G de RAM, e com um disco rígido de 16G. Na máquina virtual foram utilizadas as ferramentas Autopsy Forensic Browser 2.24 e a ferramenta Foremost 1.5.7. Ambas as ferramentas são livres e open source e são nativas do S.O. Deft. Para os testes de recuperação foi utilizado um pen-drive Kingston de 2G de Memória.

Todas as fases e etapas forenses foram respeitadas durante a análise. E para atingir os objetivos houve a necessidade de se efetuar quatro tipos de testes, para o primeiro teste foram excluídos os arquivos, no segundo teste foi efetuada a formatação rápida do dispositivo, já no terceiro teste foi efetuada a formatação completa do dispositivo, no quarto teste foi efetuada a formatação física do dispositivo. Para efetuar esses testes foi salvo no pen-drive alguns arquivos conforme demonstrado na Figura 1. Vale ressaltar que a escolha dos arquivos foi feita de forma aleatória.






| Nome | Data de modificaç... | Tipo | Tamanho |
|---|----------------------|----------------------|----------|
|  AUTOVELL | 29/03/2015 22:32 | Documento do Mi... | 48 KB |
|  Segunda Avaliação de Serviço em Redes | 23/05/2015 08:31 | Foxit Reader PDF ... | 284 KB |
|  npp.6.7.8.2.Installer | 26/05/2015 10:21 | Aplicativo | 6.782 KB |
|  20150509_204709 | 21/05/2015 19:37 | Arquivo JPG | 1.646 KB |
|  kali_dragon_by_humanlly-d61ax9j | 16/03/2015 19:22 | Arquivo PNG | 173 KB |

Figura 1. Pen-drive com vários arquivos

Para cada teste o pen-drive foi montado no S.O. Deft como somente leitura e foi utilizando o comando “dd” (ex: # dd if=/dev/sdb1 of=/home/everaldo/Deletados/imagem.img) para gerar uma imagem do pen-drive, todos os testes foram realizados na imagem, que foi submetida às ferramentas de recuperação Autopsy Forensic Browser e Foremost com o intuito de recuperar os arquivos.

Para a recuperação utilizando a ferramenta Autopsy Forensic Browser (Figura 2) foi necessário seguir os seguintes passos: 1- Foi necessário entrar no menu iniciar do Deft iniciar/ferramentas forenses, em seguida foi clicado em Autopsy, e foi solicitado a senha de super usuário, onde foi informada; 2- Foi aberto o browser, e foi necessário clicar em New Case; 3- Foram inseridos um nome do caso e o nome do investigador, e depois foi clicado em New Case; 4- Em seguida foi necessário clicar em Add Host e foi inserido o Host Name, e por fim foi clicado Add Host; 5- Depois foi necessário clicar em Add Imagem; para em seguida clicar em Add Imagem File, depois foi solicitado inserir o Location (localização da imagem), o type (Disk ou Partition) e o Import Method (Symlink) e depois clicado em next; 6- Em seguida foi necessário clicar na opção Calculate: para calcular o hash value, e inserido o Mount Point ex: C: e File System Type ex: FAT32 e depois clicado em Add; 7- Em seguida foi solicitado para confirmar os dados e clicado em OK; 8- a página mostrou o caso montado, e foi clicado em Analyze; 9- Por fim é só aguardar que o Autopsy faça a varredura e mostre na tela do browser os arquivos recuperados.



Figura 2. Ferramenta Autopsy Forensic Browser

Para a recuperação utilizando a ferramenta Foremost (Figura 3) foi necessário seguir os seguintes passos: 1- foi necessário entrar no terminal do DefT e digitar o comando # foremost -Q nome_da_imagem.img; 2- a ferramenta gerou um arquivo log.txt e uma pasta chamada output; 3- em seguida foi aberta a pasta chamada output e listado os arquivos da pasta; 4- essa pasta contém os arquivos recuperados e um arquivo chamado audit.txt, onde no seu conteúdo mostrou tudo que o Foremost encontrou durante sua varredura.



Figura 3. Ferramenta Foremost

Foram realizados quatro testes, no primeiro teste foram excluídos os arquivos, em seguida foi executado o comando “dd” e a imagem submetida às ferramentas.

Para o segundo teste foi efetuada a formatação rápida do dispositivo. Esse teste foi dividido em duas partes que utilizaram os sistemas de arquivos FAT32 (*File Allocation Table* ou Tabela de Alocação de Arquivos) e NTFS (*New Technology File System*), para cada etapa foi executado o comando “dd” e as imagens submetidas às ferramentas.

Já no terceiro teste foi efetuada a formatação completa do dispositivo. Esse teste também foi dividido em duas partes que utilizaram os sistemas de arquivos FAT32 e NTFS, para cada etapa foi executado o comando “dd” e as imagens submetidas às ferramentas.

No quarto teste foi efetuada a formatação física, em seguida executado o comando “dd” e a imagem submetida às ferramentas.

Após a realização dos testes foi efetuada a comparação dos resultados obtidos de cada ferramenta de recuperação, para demonstrar qual ferramenta foi a mais indicada à recuperação das informações, após a tentativa de apagá-las utilizando os métodos de exclusão, formatação rápida, formatação completa ou formatação física. Foi avaliado também o tempo de execução de cada teste e comparados se há diferenças significativas entre as ferramentas Autopsy Forensic Browser e Foremost.

3. Resultados e Discussões

Através da imagem gerada a partir do pen-drive, foram efetuados quatro tipos de testes com o propósito de recuperar arquivos que foram excluídos, ou que o dispositivo de armazenamento passou pelo processo de formatação rápida, completa, ou física, as imagens foram submetidas às ferramentas Autopsy Forensic Browser e Foremost para a recuperação de arquivos que o usuário pretendia apagar. Durante os testes determinou-se o tempo de execução e o desempenho das ferramentas. A Tabela 1 apresenta os resultados obtidos nos testes, correlacionando o tipo de formatação com a ferramenta de recuperação e seu respectivo tempo de execução lembrando que foram inseridos 5 arquivos no dispositivo para que os testes fossem realizados. Ainda na Tabela I, pode-se perceber que quando os arquivos foram somente excluídos, pode-se recuperar 100% dos arquivos.

Tabela 1. Resultados dos testes

| | Arq. rec. Autopsy | Tempo Autopsy | Arq. rec. Foremost | Tempo Foremost |
|---------------------------|-------------------|---------------|--------------------|----------------|
| Excluídos | 5 | 10 seg. | 5 | 100 seg. |
| Formatação Rápida FAT32 | 0 | 10 seg. | 5 | 100 seg. |
| Formatação Completa FAT32 | 0 | 10 seg. | 0 | 70 seg. |
| Formatação Rápida NTFS | 0 | 10 seg. | 5 | 100 seg. |
| Formatação Completa NTFS | 0 | 10 seg. | 0 | 70 seg. |
| Formatação Física | 0 | 10 seg. | 0 | 70 seg. |

A Tabela 2 apresenta os tipos de formatação utilizados e o tempo que se levou para conclusão de cada tipo de formatação, percebe-se que a formatação física levou 10 minutos.

Tabela 2. Relação entre tipo de formatação e o tempo

| Tipos de Formatação | Rápida | Completa | Física |
|---------------------|---------|----------|---------|
| Tempo de execução | 20 seg. | 03 min. | 10 min. |

4. Conclusões

Com os resultados obtidos nos testes e com a comparação entre eles pode-se concluir que a ferramenta Autopsy Forensic Browser é executada em 10% do tempo de execução da ferramenta Foremost quando a varredura encontra arquivos e em 14,3% do tempo de execução da ferramenta Foremost quando a varredura não encontra arquivos, obtendo

100% de recuperação dos arquivos excluídos, mas a ferramenta Autopsy Forensic Browser não foi eficaz quando o dispositivo de armazenamento passou por processos de formatação.

A ferramenta Foremost tem o tempo de execução maior, porém, ela obteve melhor desempenho que a ferramenta Autopsy Forensic Browser uma vez que obteve 100% dos arquivos recuperados quando excluídos e 100% dos arquivos recuperados quando o dispositivo passou pelo processo de formatação rápida.

As ferramentas são ineficazes para a recuperação de arquivos quando o dispositivo passou pelo processo de formatação completa ou física.

Para que os dados sejam irrecuperáveis pelas ferramentas avaliadas, foi necessário formatar o dispositivo de forma completa ou física, e foi verificado que a formatação completa é mais eficaz devido a apagar 100% dos arquivos em 33% do tempo de execução da formatação física.

Pode-se concluir que as ferramentas são de fácil usabilidade, e as duas ferramentas podem ser utilizadas por profissionais da computação forenses, a fim de buscar por evidências em dispositivos de armazenamento.

Referências

- Eleutério, P. M. da S.; Machado, M. P. (2010), *Desvendando a Computação Forense*, Novatec, São Paulo.
- Farmer, D.; Venema, W. (2007), *Perícia Forense Computacional: Teoria e Prática Aplicada*, Pearson Prentice Hall, São Paulo.