FORENSE COMPUTACIONAL APLICADA EM RECUPERAÇÃO DE ARQUIVOS EM AMBIENTE WINDOWS, LINUX E MAC OS X

Douglas de Oliveira, Henrique Pachioni Martins, Elvio Gilberto da Silva, Kelton Augusto Pontara da Costa

Instituto de Informática – Universidade Sagrado Coração (USC) Bauru – SP

Centro de Ciências Exatas e Sociais Aplicadas – Universidade Sagrado Coração, USC.

oliveira.douglas@outlook.com, henrique.martins@usc.br, egsilva@usc.br, kelton.costa@usc.br

Abstract. *The data recovery, common or sensitive, it is necessary due to the steady growth of the use of data storage equipment. This procedure is adopted by both common users, who have lost their files by accident as by forensic investigators to search for evidence of crimes, be they digital or not. This paper analyzes data forensic tools in order to establish which tool and which operating system you can get the best file recovery. Were selected two tools for each operating system, as follows: DiskDigger and Recuva for Windows, Mac Data Recovery Free and Disk Drill for Mac OS X; Foremost and Scalpel for Linux. All these tools are available for free, but some of them have proprietary version. Testing tools preselected were performed in order to recover files from a formatted flash drive, each in its operating system. After this battery of tests, have been checking which tool is most effective for recovering deleted files.*

Keywords: Files deleted. Computational Forensics. Data recovery.

Resumo. *A recuperação de dados, comuns ou sigilosos, se faz necessária devido ao crescimento constante do uso de equipamentos de armazenamento de dados. Este procedimento é adotado tanto por usuários comuns, que têm os seus arquivos perdidos por acidente, como por investigadores forenses em busca de evidências de crimes, sejam eles digitais ou não. Este trabalho analisa ferramentas de dados forenses com o objetivo de estabelecer qual ferramenta e em qual sistema operacional é possível se obter a melhor recuperação de arquivos. Foram selecionadas duas ferramentas para cada sistema operacional, sendo: Recuva e DiskDigger para o Windows; Mac Data Recovery Free e Disk Drill para Mac OS X; Foremost e Scalpel para Linux. Todas essas ferramentas são disponíveis gratuitamente, porém, algumas delas possuem versão proprietária. Os testes das ferramentas pré-selecionadas foram realizadas com o intuito de recuperar arquivos formatados de um pendrive, cada qual em seu sistema operacional. Após essa bateria de testes, foi possuir verificar qual ferramenta é mais eficaz para a recuperação de arquivos apagados.*

Palavra chave: Arquivos apagados. Forense Computacional. Recuperação de dados.

Introdução

O avanço constante da informática vem promovendo acesso rápido e prático a rede mundial de computadores, a Internet. Hoje em dia é cada vez mais comum encontrarmos lares com computadores conectados a Internet, fator que evidencia a inclusão digital que se vivencia.

Todavia, tais facilidades promovidas pela Internet abrem espaço para práticas ilícitas e de fundamentação não legal perante a lei, utilizando-se das falhas de segurança de um sistema e da ausência de leis suficientes que definam e tratem de crimes eletrônicos, bem como de tecnologia madura capaz de prover segurança e soluções praticáveis. Assim, aumentam os números de fraudes em transações financeiras pela Rede, invasões de privacidade em organizações, violação de direitos autorais ou destruição de conteúdo privado.

Nesse momento, surge a computação forense – campo da Ciência da Computação responsável pela preservação, identificação, extração e documentação de evidências criminais em sistemas de computador (Marcella e GrennField, 2001). Assim, sua importância é fundamental para toda a sociedade, focando seus esforços em promover um ambiente de informações seguro sob a ótica financeira, além de efetuar um papel investigativo e jurídico, assegurando direitos e punições aos responsáveis de atos ilícitos no âmbito digital.

O processo de análise forense executa uma série de atividades para uma investigação completa. Carrier (2002) cita que, para uma melhor abordagem sobre esse processo, a análise forense computacional pode ser dividida basicamente em três fases: a aquisição, onde são coletadas as evidências, a análise, que examina e analisa as provas adquiridas e a apresentação, que mostra os resultados da investigação.

Buscar vestígios digitais e caracterizá-los como evidências e provas de crime são atividades fundamentais da perícia forense computacional, que requerem cuidados e conhecimentos específicos. É preciso saber onde pesquisar por vestígios, que tipos de vestígios buscarem, dispor de conhecimento técnico para coletar e preservar esses vestígios, e observar a minimização dos riscos de sua deterioração ou invalidação como prova.

Todos nós já passamos por situações desesperadoras ao perceber que havia perdido algum arquivo ou documento de muita importância do nosso computador, mas o que muitos não sabem é que quando esses arquivos são “perdidos” ou apagados acidentalmente, eles não são removidos completamente do sistema, e sim, perdem apenas a referência que indica o local de armazenamento daquele arquivo na mídia.

Portanto, através de softwares específicos e técnicas de recuperação de dados, é possível restaurar quase sempre esses dados apagados.

A recuperação de dados é a ciência que procura reconstruir o sistema de arquivos para que se possam acessar os arquivos apagados. Cada sistema operacional tem um

sistema de arquivos, que é um método único de indexar e monitorizar os arquivos. O avanço constante da informática vem promovendo acesso rápido e prático a rede mundial de computadores, a Internet. Hoje em dia é cada vez mais comum encontrarmos lares com computadores conectados a Internet, fator que evidencia a inclusão digital que se vivencia.

Todavia, tais facilidades promovidas pela Internet abrem espaço para práticas ilícitas e de fundamentação não legal perante a lei, utilizando-se das falhas de segurança de um sistema e da ausência de leis suficientes que definam e tratem de crimes eletrônicos, bem como de tecnologia madura capaz de prover segurança e soluções praticáveis. Assim, aumentam os números de fraudes em transações financeiras pela Rede, invasões de privacidade em organizações, violação de direitos autorais ou destruição de conteúdo privado.

Nesse momento, surge a computação forense – campo da Ciência da Computação responsável pela preservação, identificação, extração e documentação de evidências criminais em sistemas de computador (Marcella e GrennField, 2001). Assim, sua importância é fundamental para toda a sociedade, focando seus esforços em promover um ambiente de informações seguro sob a ótica financeira, além de efetuar um papel investigativo e jurídico, assegurando direitos e punições aos responsáveis de atos ilícitos no âmbito digital.

O processo de análise forense executa uma série de atividades para uma investigação completa. Carrier (2002) cita que, para uma melhor abordagem sobre esse processo, a análise forense computacional pode ser dividida basicamente em três fases: a aquisição, onde são coletadas as evidências, a análise, que examina e analisa as provas adquiridas e a apresentação, que mostra os resultados da investigação.

Buscar vestígios digitais e caracterizá-los como evidências e provas de crime são atividades fundamentais da perícia forense computacional, que requerem cuidados e conhecimentos específicos. É preciso saber onde pesquisar por vestígios, que tipos de vestígios buscarem, dispor de conhecimento técnico para coletar e preservar esses vestígios, e observar a minimização dos riscos de sua deterioração ou invalidação como prova.

Todos nós já passamos por situações desesperadoras ao perceber que havia perdido algum arquivo ou documento de muita importância do nosso computador, mas o que muitos não sabem é que quando esses arquivos são “perdidos” ou apagados acidentalmente, eles não são removidos completamente do sistema, e sim, perdem apenas a referência que indica o local de armazenamento daquele arquivo na mídia.

Portanto, através de softwares específicos e técnicas de recuperação de dados, é possível restaurar quase sempre esses dados apagados.

A recuperação de dados é a ciência que procura reconstruir o sistema de arquivos para que se possam acessar os arquivos apagados. Cada sistema operacional tem um sistema de arquivos, que é um método único de indexar e monitorizar os arquivos. Infelizmente para os que perdem dados, os sistemas de arquivos podem ser muito complexos, razão pela qual pode ser muito difícil localizar arquivos apagados. Por exemplo, os sistemas de arquivos utilizados em meios empresariais requerem detalhes de segurança e dados de operações de acesso. Um bom exemplo disso é um sistema de

arquivos baseado em operações, ou um livro-diário, cujo objetivo consiste em registar quando se acessa, modifica ou grava cada arquivo, sendo assim um sistema mais complicado e mais difícil de reconstruir (NÓBREGA, 2010).

Infelizmente para os que perdem dados, os sistemas de arquivos podem ser muito complexos, razão pela qual pode ser muito difícil localizar arquivos apagados. Por exemplo, os sistemas de arquivos utilizados em meios empresariais requerem detalhes de segurança e dados de operações de acesso. Um bom exemplo disso é um sistema de arquivos baseado em operações, ou um livro-diário, cujo objetivo consiste em registar quando se acessa, modifica ou grava cada arquivo, sendo assim um sistema mais complicado e mais difícil de reconstruir (NÓBREGA, 2010).

Metodologia

Para Dencker (2002), o início da pesquisa é marcado pela pesquisa bibliográfica por meio de livros, monografias, teses de mestrado e/ou doutorado, e da internet. Através de trabalhos que se adequam ao tema em estudo, a pesquisa se torna mais contundente e rica, pois são diversas opiniões e teorias que entram em conflito para se obter uma ideia em comum.

A princípio foi realizada uma pesquisa e estudo abordando todo o conceito de forense computacional, sobre o que abrange essa área e onde as técnicas forenses se fazem necessárias.

Com relação à perícia forense, o trabalho relata quais os procedimentos que um perito forense deve tomar, quais são os tipos de perícias existentes, métodos para coletas de evidências e também a fase onde o perito gera o laudo, cujo qual deve conter todas as informações obtidas durante a fase de coleta de evidências.

Já em relação à recuperação de arquivos, foi realizada uma rápida pesquisa para verificar quais as ferramentas comumente utilizadas nos três sistemas operacionais, para que depois pudesse ser feita a fase de estudo de caso.

No estudo de caso, foram instalados os softwares, cada qual em seu sistema operacional e também foi selecionado um pendrive qualquer para a realização dos testes.

No pendrive, foram colocados alguns arquivos de formatos variados e em seguida esses arquivos foram apagados e o pendrive foi formatado, mantendo seu sistema de arquivos padrão do Windows (NTFS). Com o pendrive preparado, iniciaram-se os testes em busca dos arquivos apagados do pendrive com os softwares pré-selecionados nos três diferentes sistemas operacionais.

Os resultados obtidos durante a fase de testes foram tabulados com o auxílio do Excell, colocando o nome do software e a quantia de arquivos recuperados de acordo com seu tipo (música, áudio, vídeo ou texto), para que no fim do trabalho esses resultados pudessem ser comparados, revelando com qual programa e em qual sistema operacional era possível se obter o melhor percentual de restauração dos arquivos apagados.

Resultados

Ao término de todos os testes, pôde-se montar um quadro comparando os resultados entre cada software em cada sistema operacional, exibindo especificamente o número de arquivos recuperados, conforme mostrado no Quadro 1. Lembrando que o número de arquivos contidos no pendrive foram 35, divididos entre músicas, imagens, vídeos e textos.

Quadro 1 - Dados coletados

Software	Recuva	DiskDigger	Disk Drill	Mac Data Recovery Free	Foremost	Scalpel
imagens	10	10	8	8	6	3
videos	5	5	4	0	2	0
músicas	7	10	5	10	6	7
textos	10	10	10	0	0	10
	Windows		**Mac OS X**		**Linux**	

Fonte: Elaborado pelo autor

Com os dados devidamente coletados e tabulados, foi possível gerar um gráfico (Gráfico 1) que facilitasse a visualização da quantidade de arquivos recuperados entre as diferentes ferramentas utilizadas.

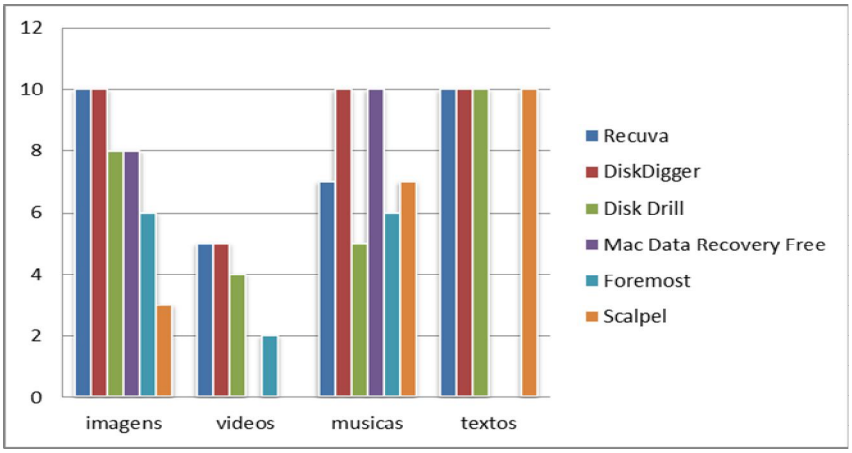

Gráfico 1 - Comparativo dos resultados entre os softwares.
Fonte: Elaborado pelo autor

Portanto, percebeu-se com os resultados obtidos que a ferramenta mais eficaz para a recuperação de arquivos apagados em um sistema de arquivos do tipo NTFS é o DiskDigger, utilizado no ambiente Windows. O fator “tempo” não foi comparado pois ele pode variar de acordo com o computador em que está sendo realizado a recuperação, quanto o tamanho dos arquivos que se deseja recuperar.

Considerações Finais

Como a facilidade na locomoção de dados através de unidades móveis como pendrives e cartões de memória, e os valores dos mesmos cada vez mais acessíveis, a probabilidade de perda de arquivos armazenados nessas mídias se torna cada vez mais comum. Pelo mesmo motivo, os crimes usando estes equipamentos também aumentam na mesma proporção.

Levando isso em consideração, muitas ferramentas são desenvolvidas com o intuito de recuperar esses arquivos, tanto para uso pessoal, em busca de restaurar arquivos perdidos acidentalmente ou mesmo dados importantes, como no uso profissional, no caso de uma perícia forense em busca de vestígios criminais.

Neste trabalho foram usadas algumas dessas ferramentas, todas em sua versão disponibilizadas gratuitamente, e feito o teste nos três sistemas operacionais mais utilizados hoje em dia, sendo Windows, Mac OS X e Linux.

Cada ferramenta, utilizada cada qual em seu sistema operacional, mostraram-se com comportamento diferente quando utilizadas para a recuperação de arquivos de um pendrive formatado, sendo que apenas uma delas mostrou-se totalmente eficaz na recuperação dos arquivos apagados, o DiskDigger. Mas o Recuva também não deixou a desejar, ficando na segunda posição por uma diferença de apenas três arquivos em relação ao DiskDigger.

No caso, as ferramentas utilizadas no ambiente Windows se saíram melhor do que as demais ferramentas de outros sistemas operacionais. Talvez isso se deve ao fato do pendrive utilizados nos testes ter seu sistema de arquivos sendo NTFS, um sistema de arquivos utilizados pelo Windows. Sendo assim, fica uma sugestão de trabalhos futuros para analisar a recuperação de arquivos levando em consideração cada sistema de arquivos utilizados e não apenas as ferramentas diferenciadas pelos sistemas operacionais.

Outra conclusão que pode ser retirada é a dificuldade em remover por completo algum arquivo, tornando seu acesso ou recuperação praticamente impossível até mesmo por profissionais neste quesito, pois existem cada vez mais ferramentas sofisticadas para tal finalidade. Portanto, fica outra sugestão de trabalho futuro, sendo que ao invés de mostrar as técnicas utilizadas na recuperação, mostrar o processo realizado para evitar a recuperação dos arquivos apagados e inviabilizar seu acesso de uma vez por todas.

Referências

CARRIER, B. Open source digital forensics tools. 2002. Disponível em: <http://www.digital-evidence.org/papers/opensrc_legal.pdf>. Acesso em: 10 mar. 2012.

DENCKER, Ada de Freitas Maneti. Pesquisa e interdisciplinaridade no Ensino Superior: uma experiência no Curso de Turismo. São Paulo: Aleph, 2002. 111p.

MARCELLA, A. J.; GRENNFIELD, R. S., (ed.). Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. [s. l.] 2001.: Auerbach Publications..

NÓBREGA, J. Como funciona a recuperação de dados. 2010. Disponível em: <http://www.computerworld.com.pt/2010/06/17/como-funciona-a-recuperacao-de-dados/>. Acesso em: 15 out. 2012