Márcio Fernandes Justino

Fragmentação de Arquivos em File Carving em Sistemas de Arquivos NTFS

São Paulo – SP

Maio / 2013

Márcio Fernandes Justino

Fragmentação de Arquivos em File Carving em Sistemas de Arquivos NTFS

Projeto de pesquisa apresentado como requisito parcial para a aprovação na disciplina Metodologia do Trabalho Científico do Curso de Computação Forense da Universidade Presbiteriana Mackenzie.

Orientadora:
Ivete Irene dos Santos

UNIVERSIDADE PRESBITERIANA MACKENZIE
INSTITUTO DE COMPUTAÇÃO
PÓS GRADUAÇÃO EM COMPUTAÇÃO FORENSE

São Paulo – SP

Maio / 2013

Dedico a meus pais, cujo exemplo
de honestidade e trabalho tem marcado
minha vida, à minha esposa que me apoiou
nesta caminhada e à minha filha que
acompanhou todo este trabalho
ainda no ventre da mãe.

Resumo

A proposta desta pesquisa é explanar e determinar uma melhor forma de localização de fragmentos de arquivos não alocados durante o processo de file carving em uma perícia forense digital abordando o conceito da metodologia de identificação de fragmentos de arquivos e os benefícios que o mesmo proporciona para a análise em uma investigação de uma imagem digital quando possível localizar suas partes, permitindo assim sua identificação.

Palavras-chave: NTFS, fragmentação, carving, identificação, partes, arquivos.

Sumário

1 Introdução

Juntamente com o avanço da tecnologia computacional e da internet veio o aumento do número de pessoas conectadas trocando informações, seja em nível pessoal ou organizacional. Nesse meio, existem usuários que promovem o cybercrime[1] ou atividades ilegais na rede[2]. As informações computacionais são armazenadas em discos rígidos[3] usando apropriados sistemas de arquivos que são suportados pelo sistema operacional instalado no computador. Existem diversos sistemas de arquivos para armazenamento de arquivos no mercado, e um dos mais comuns atualmente é o NTFS. (MAHANT, 2012)

A técnica de Data Carving é frequentemente utilizada durante investigações digitais quando o espaço não alocado de um sistema de arquivos é analisado para extração de arquivos. Quando um arquivo está disposto no espaço não alocado de um disco o mesmo pode ser sobrescrito ou ter partes de sua estrutura sobrescritas por outros arquivos determinados pelo sistema operacional na reutilização de espaço não mais alocado. Essa operação trás um enorme desafio para o processo de file carving que precisa assim identificar as partes do arquivo muitas vezes fragmentados pelo sistema de arquivos para identificar seu conteúdo ou seus metadados.

"In forensic practice, file carving can recover files that have been deleted and have had their directory entries reallocated to other files, but for which the data sectors themselves have not yet been overwritten." (GARFINKEL, 2007)

1.1 Justificativa

O processo de "File Carving"é de suma importância para a investigação forense computacional e envolve a identificação de arquivos perdidos (deletados ou apagados) do equipamento investigado. A dispersão desses arquivos não mais indexados pela tabela de alocação de arqui-

[1] crimes cibernéticos tendo sistemas informatizados como meio de ação

[2] o termo rede será usado ao longo deste texto podendo representar a internet como um todo ou a ligação de mais de computadores entre si.

[3] unidade física de armazenamento de dados em um computador

vos do sistema de arquivos NTFS torna o processo de identificação dos arquivos um desafio para a investigação e identificação de ilícitos.

> During a digital forensic investigation many diferent pieces of data are preserved for investigation, of which bit-copy images of hard drives are the most common. These images contain the data allocated to files as well as the unallocated data. The unallocated data may still contain information that is relevant to an investigation, in the form of (parts of) intentionally deleted les or automatically removed temporary files. Unfortunately, this data is not always easily accessible: a string search on the raw data might recover (parts of) interesting text documents, but it won't help to get to information present in for example images or compressed files. Besides that, the exact strings to look for may not be known beforehand. To get to this information, the deleted files have to be recovered. (KLOET, 2007)

1.2 Problema de Pesquisa

Como identificar fragmentos de arquivos em file carving em sistemas de arquivos NTFS?

1.3 Hipótese(s)

Análise dos metadados de um arquivo quanto ao seu início e fim (cabeçalho e rodapé do arquivo), informações que determinam onde os dados de um determinado arquivo começam e onde eles terminam. Identificar um padrão de dados para localização dos fragmentados de forma consistente, reduzindo assim os falsos positivos comumente apresentados no processo de file carving e permitindo a identificação máxima do conteúdo do arquivo no processo de investigação.

1.4 Objetivo Geral

Determinar uma melhor metodologia de localização de fragmentos de arquivos no processo de file carving em sistemas de arquivos NTFS.

1.5 Objetivo Específico

Para chegar ao objetivo principal e determinar uma melhor metodologia de localização de fragmentos de arquivos é necessário entender primeiramente e de forma mais detalhada alguns

items específicos:

- Verificar como são identificados os arquivos no sistema de arquivo NTFS;
- Verificar como um arquivo fragmentado é armazenado em um sistema NTFS;
- Levantar uma padronização entre os fragmentos de arquivos para melhor localização;
- Identificar formas de localização de fragmentos dos arquivos não alocados;

Verificar assim a forma como os arquivos são registrados nos sistemas de arquivos NTFS, o processo de diferenciação de tipos de arquivos para determinar o início e o fim de um arquivo (área de cabeçalho, área de dados, de metadados e ponto de fim de arquivo), podendo então encontrar certos padrões que possam permitir a identificação de partes de um arquivo fragmentado no sistema de arquivos.

1.6 Metodologia

...em desenvolvimento...

2 Levantamento Bibliográfico

...em desenvolvimento...

2.1 Capítulo 1 - xxxx

...

2.2 Capítulo n - xxxx

...

3 Considerações Finais

...em desenvolvimento...

4 Apêndice

...

5 Anexos

...

Referências Bibliográficas

GARFINKEL, S. L. Carving contiguous and fragmented files with fast object validation. *ELSEVIER*, v. 4S, p. S2–S12, 2007.

KLOET, S. *Measuring and Improving the Quality of File Carving Methods*. Dissertação (Mestrado) — Eindhoven University of Technology, 10 2007.

MAHANT, B. S. H. Ntfs deleted files recovery - forensics view. *IRACST - International Journal of Computer Science and Information Technology and Security (IJCSITS)*, v. 2, n. 3, p. 491–497, 2012.