SISTEMAS DE ARQUIVOS
e
Análise Forense
para ambientes NTFS

Aluna: Jussara Reis
Disciplina: Sistemas Operacionais
Professor: Adonai Medrado

Valença – Ba, 27 de nov. 2010

O que é Sistema de arquivos?

E a parte do sistema responsável pela gerência dos arquivo, e é responsável pelas manipulações, como por exemplos: identificar, organizar, compartilhar, definir métodos de acesso, proteger e realizar operações de entrada e saída.

- A organização do arquivo pode ser definida pelo criador do arquivo no momento da criação.

- Os métodos de acesso dependem de qual forma o arquivo está organizado, estes acessos podem ser *seqüencial, direto e indexado.*
- Os atributos de um arquivo são as informações de controle que este possui, tais atributos variam a depender do sistema de arquivo, mas algumas informações como, por exemplo: tamanho do arquivo e identificação do criador, são encontradas na maioria dos sistemas.
- O sistema de arquivo utiliza os diretórios, que são estruturas de dados que contém informações das referência do arquivo, para facilitar a organização dos arquivos contidos nos discos.

- A gerencia de alocação do disco é quem controla quais áreas do disco os arquivos serão alocados, as principais técnicas usadas para alocação são:

- **Alocação Contígua** - armazena um arquivo em blocos sequencialmente disposto no disco.
  - First-fit
  - Best-fit
  - Worst-fit
- **Alocação Encadeada** - é organizado como um conjunto de blocos ligados logicamente ao disco.
- **Alocação Indexada –** permite o acesso direto aos blocos de arquivos.

Sistemas de arquivos no windows

Os sistemas de arquivos reconhecidos pelo sistema operacional Windows que são sistemas baseados em DOS são:

- **FAT12** – utilizado em disquete e nas primeiras versões do MS-Dos, com end de 12 bits e partições de 16 MB.
- **FAT16** – compatível com todos os sistemas operacionais e dispositivos como: câmeras, mp3 e pendrive. Usa end. de 16 bits e partições de 2GB.
- **FAT32** – lançado com o Win 95,para diminuir o desperdicio de espaço em disco. Com uso de end de 32 bits e partições até 2TB.
- **NTFS** – desenvolvido na decada de 90 com o Win NT, possui muitas vantagens em relação ao FAT, mas por possui grande número de clusters necessidade de grande processamento para encontrar os dados desejados.

Analise forense para ambiente NTFS

- Segundo THORTON (1997), a ciência forense é exercida em favor da lei para uma resolução correta de um conflito, baseada em procedimentos científicos para obtenção de informações que possam ser utilizadas durante uma disputa judicial.

- De acordo com OLIVEIRA (2001), a forense computacional serve para identificar e entender as relações de causa e efeito de todas as ações ocorridas dentro do sistema, através da manipulação e análise de evidências digitais. Para que se tenha um bom sucesso nas análises é necessário o raciocínio lógico e uma mente aberta para o entendimento das causas e efeito.

Alguns procedimentos para manipulação de sistemas de arquivos são gerais, pode-se citar como exemplos:

- **Análise sobre cópias:** As analises devem ser feitas a partir de cópias dos dados originais, de preferência bit a bit, ou seja, por imagem.
- **Assinaturas digitais:** As assinaturas digitais é uma maneira de assegurar a confiabilidade que os dados recolhidos para analise são iguais aos originais.
- **Sem Permissão de escrita e execução:** A desabilitação da função de escrita e execução do sistema na imagem feita dos dados originais evita a alteração das informações a ser analisadas.
- **MACTimes:** É um termo usado para fazer referencia aos três atributos (mtime, atime e ctime) de tempo presente em todos os arquivos e diretórios da maioria dos SO´s.
- **Arquivos excluídos:** a utilização de um mecanismo de recuperação de arquivos excluídos auxilia na eficiência da analise forense.

- A análise forense no sistema operacional Windows NT, pode-se dizer que é bastante complexo, pois se trata da utilização de um sistema operacional com pouca documentação e sistema fechado.

- *Alternate Streams* é um mecanismo utilizado para embutir um arquivo dentro do outro, sem que seu conteúdo seja alterado. No sistema NTFS este mecanismo é um dos pontos importantes na análise forense, pois pode-se dizer que todos os arquivos NTFS possui um outro arquivo sem nome embutido.

- Existem diversas ferramentas para efetuar uma análise, por exemplo: o TASK, é um conjunto de ferramentas de código aberto para analise forense com suporte ao sistema de arquivo NTFS, desenvolvida por Brian Carrier.

Referências

- MACHADO, Francis B.; MAIA, Luiz P.. **Arquitetura de Sistemas Operacionais**. 4ª Ed. Rio de Janeiro: LTC, 2007. Pg 213-229.
- VILLELA, Anderson. **Sistema de Arquivos do Windows XP.** Disponível em: http://www.OFICINADANET.com.br/artigo/298/sistema_de_arquivos_do_windows_xp. Acessado em: 19 nov. 2010.
- MORIMOTO, Carlos E. **Hardware, o Guia Definitivo.** Disponível em: http://www.gdhpress.com.br/hardware Acessado em: 18 nov 2010.
- TORRES, Gabriel. **Sistema de arquivos.** Disponível em: http://www.clubedohardware.com.br/artigos/313 Acessado em: 19 nov 2010.
- ALECRIM, Emerson. **Sistemas de Arquivos NTFS**. Disponível em: http://www.infowester.com/ntfs.php Acessado em: 19 nov 2010.

- THORTON, J.; **The general assumptions and rationale of forensic identification**. Modern Scientific Evidence: The Law and Science of Expert Testimony; West Publishing Co.; Volume 2; 1997;
- OLIVEIRA, Flávio. **Metodologias de análise forense para ambientes baseados em NTFS.** Disponível em: http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-flavio.oliveira-forense.ntfs.pdf. Acessado em: 25 nov. de 2010.
- HOLPERIN, Marco; LEOBONS, Rodrigo. **Análise Forense.** Disponível em: http://www.gta.ufrj.br/grad/07_1/forense/task.html Acessado em: 26 nov 2010.