STARTUP DAY

Técnicas forenses para a recuperação de arquivos

João Eriberto Mota Filho

Natal, RN, 18 maio 2019

Sumário

- ✔ Discos e memória
- ✔ Formatação e deleção
- ✔ Mais sobre arquivos...
- ✔ Demonstração de recuperação de arquivos
- ✔ Deleção segura de arquivos e discos
- ✔ Conclusão

Sumário

- ✔ Discos e memória
- ✔ Formatação e deleção
- ✔ Mais sobre arquivos...
- ✔ Demonstração de recuperação de arquivos
- ✔ Deleção segura de arquivos e discos
- ✔ Conclusão

Discos e memória

- ✔ Discos são fisicamente organizados por trilhas divididas em setores, que podem ser físicos ou lógicos.
- ✔ Cada setor lógico possui 512 bytes. Há um projeto de migração para 4096, conhecido como advanced format.

Discos e memória

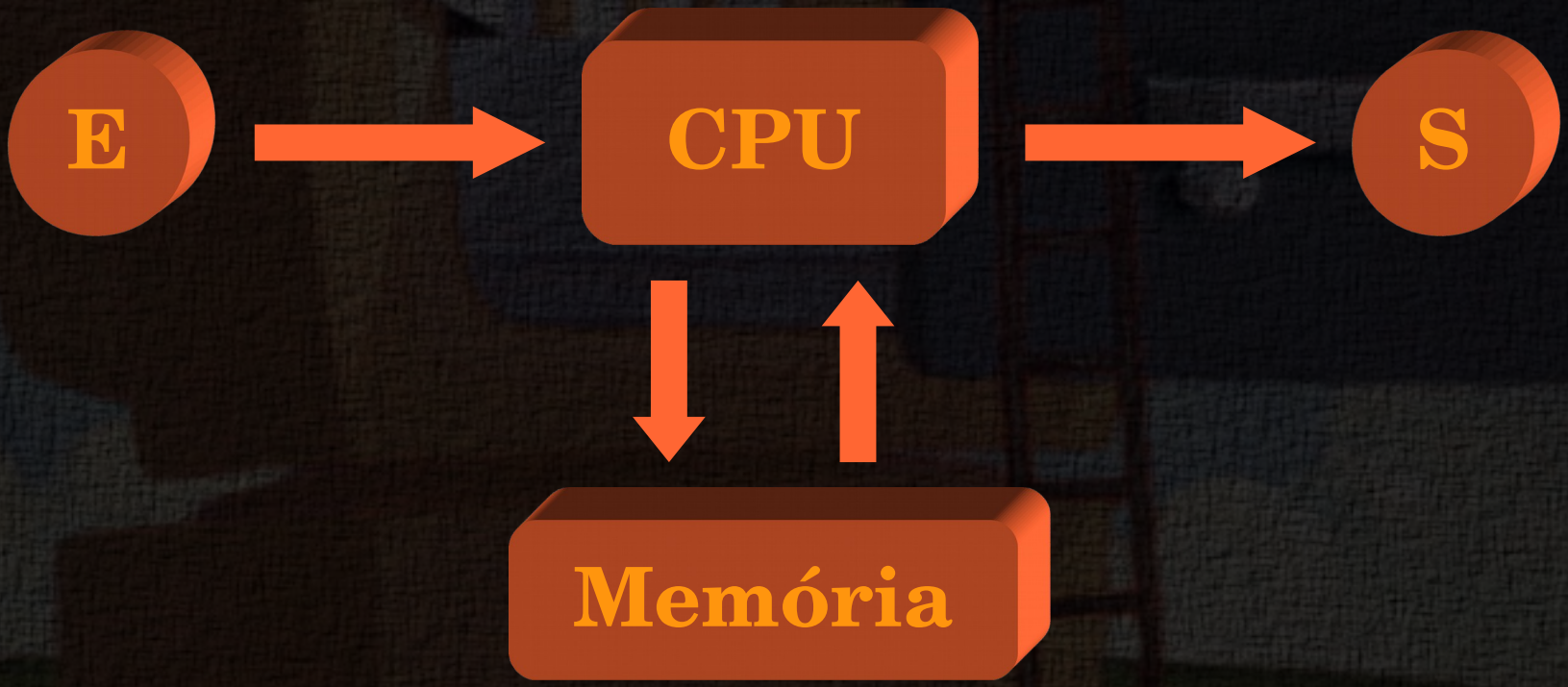
- ✔ As projeções verticais das trilhas nos diversos pratos formam os cilindros.
- ✔ A menor quantidade de dados que uma controladora pode acessar em um disco é um setor físico.
- ✔ Partições de disco precisam ser formatadas logicamente para receberem dados.
- ✔ Formatar logicamente é estabelecer um filesystem.
- ✔ Filesystems são compostos por blocos (agrupamento de setores) e são divididos em área de controle e área de dados.

Discos e memória

- ✔ Os blocos de um filesystem podem ter tamanho pré-definido.
- ✔ Geralmente, os blocos possuem um tamanho default de 4 KB.
- ✔ Os blocos compõem tanto a área de controle quanto a área de dados.
- ✔ Os blocos da área de controle são denominados inodes.

Discos e memória

✔ Modelo von Neumman: tudo passa pela memória!



Discos e memória

- ✔ A memória RAM é composta por páginas, que são similares aos blocos em filesystems. Há área de controle e área de dados.
- ✔ O tamanho da página é ditado pela arquitetura de hardware. Exemplo: 4 KB para x86 e x86-64.
- ✔ Como tudo passa pela memória, é possível a recuperação de vários tipos de dados, como textos, senhas, processos em execução etc.
- ✔ A volatilidade da memória...
- ✔ Aquisição e análise de memória em diversos SO: lime-forensics, dumpit, volatility etc.

Sumário

- ✔ Discos e memória
- ✔ **Formatação e deleção**
- ✔ Mais sobre arquivos...
- ✔ Demonstração de recuperação de arquivos
- ✔ Deleção segura de arquivos e discos
- ✔ Conclusão

Formatação e deleção

- ✔ Escrita em disco x deleção de dados.

Formatação e deleção

- ✔ Escrita em disco x deleção de dados.
- ✔ Deletar não apaga a área de dados!
- ✔ Apagar de verdade significa escrever por cima (wipe e zerofill). Isso não é comum, pois representaria um esforço computacional imenso.
- ✔ Formatar, geralmente, não altera a área de dados. Apenas é refeita a área de controle.
- ✔ Na memória também não é comum ocorrer uma real deleção de algo. As áreas são declaradas livres para poderem ser superpostas.

Sumário

- ✔ Discos e memória
- ✔ Formatação e deleção
- ✔ **Mais sobre arquivos...**
- ✔ Demonstração de recuperação de arquivos
- ✔ Deleção segura de arquivos e discos
- ✔ Conclusão

Mais sobre arquivos...

- ✔ Arquivos ocupam blocos e, ao serem apagados, na verdade, apenas estarão passíveis de superposição.
- ✔ Escrever parcialmente em um bloco significa preservar partes anteriores de um arquivo. Isso gera os slack spaces.
- ✔ A maioria dos arquivos possui patterns, que são padrões que os identificam.
- ✔ Exemplo de pattern: todo JPG inicia com 0xFFD8FF.

Sumário

- ✔ Discos e memória
- ✔ Formatação e deleção
- ✔ Mais sobre arquivos...
- ✔ **Demonstração de recuperação de arquivos**
- ✔ Deleção segura de arquivos e discos
- ✔ Conclusão

Demonstração de recuperação de arquivos

- ✔ Demonstração de uma deleção.
- ✔ Demonstração de uma formatação.
- ✔ Recuperação via inode.
- ✔ Recuperação via pattern.
- ✔ Recuperação com dd ou dcfldd.
- ✔ Recuperação de fragmentos com strings.
- ✔ Obs.: há guias de comandos e exercícios (casos) disponíveis em http://eriberto.pro.br/forense.

Sumário

- ✔ Discos e memória
- ✔ Formatação e deleção
- ✔ Mais sobre arquivos...
- ✔ Demonstração de recuperação de arquivos
- ✔ **Deleção segura de arquivos e discos**
- ✔ Conclusão

Deleção segura de arquivos e discos

- ✔ Wipe e derivados (eraser no Windows) apagam somente os dados, quando aplicados em arquivos. Os inodes permanecem!!! Áreas prévias também permanecerão.
- ✔ Wipe e dd (dcfldd) podem ser aplicados em dispositivos inteiros. Ex: # dcfldd if=/dev/zero of=/dev/sda. Esta última ação chama-se zerofill.
- ✔ Com dd ou dcfldd, pode-se criar um arquivo com conteúdo não significativo que preencha toda a área livre de um filesystem. Ex: # dcfldd if=/dev/zero of=/teste.txt
- ✔ Com o procedimento anterior, os slack spaces de blocos ocupados permanecem!!!
- ✔ O pacote secure-delete (# apt-get install secure-delete) possui executáveis para limpar (wipe) memória, swap etc.

Sumário

- ✔ Discos e memória
- ✔ Formatação e deleção
- ✔ Mais sobre arquivos...
- ✔ Demonstração de recuperação de arquivos
- ✔ Deleção segura de arquivos e discos
- ✔ Conclusão

Conclusão

- ✔ Apagar dados, na ampla concepção da ideia, não é uma ação natural.
- ✔ Formatar um disco é, na verdade, reestabelecer a área de controle.
- ✔ Há boas possibilidades de arquivos apagados ou discos formatados acidentalmente serem recuperados. Isso dependerá de técnica e de paciência.
- ✔ Fragmentos ou arquivos completos apagados poderão ser preservados por anos, principalmente em HDs grandes.

Esta palestra está disponível em:

http://eriberto.pro.br

Siga-me no Twitter @eribertomota

Eriberto - maio 2019