Forense Computacional

Diego Tavares
(PET-Computação)

diegot@dsc.ufcg.edu.br

Introdução

"A Forense Computacional pode ser definida como a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional."

Introdução

- Ocorrências mais comuns:
  - Calúnia, difamação e injúria via e-mail
  - Roubo de informações confidenciais
  - Remoção de arquivos
- Outros crimes:
  - Pedofilia
  - Fraudes
  - Tráfico de drogas via Internet

Introdução

- **Objetivo da Forense Computacional**: aplicar métodos científicos e sistemáticos, buscando extrair e analisar tipos de dados dos diferentes dispositivos, para que essas informações passem a ser caracterizadas como evidências e, posteriormente, como provas legais de fato.

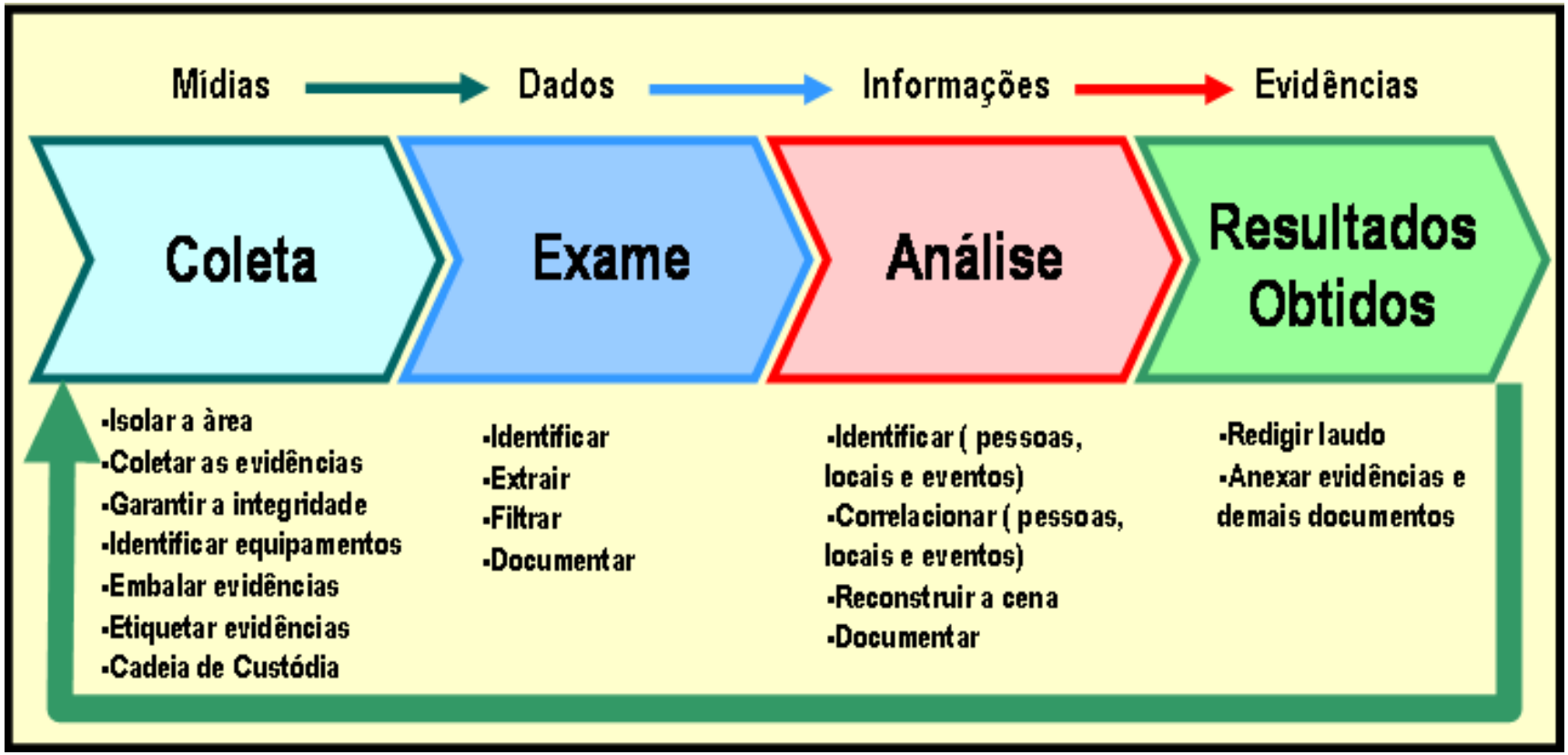
- A forense aplicada à tecnologia é muito recente, porém a ciência forense como um todo existe há muito tempo.
  - No século VII já eram utilizadas impressões digitais para determinar as identidades dos devedores. As impressões digitais dos cidadãos eram anexadas às contas que ficavam em poder dos credores.

Introdução

- **A forense computacional é empregada:**
  - para fins legais (ex.: investigar casos de espionagem industrial);
  - em ações disciplinares internas (ex.: uso indevido de recursos da instituição);
- Para serem consideradas provas válidas, é muito importante que o perito realize o processo de investigação de maneira cuidadosa e sistemática.
  - Preservar a integridade das evidências
  - Gerar documentação detalhada

Etapas da investigação

- Fases de um processo de investigação



Coleta dos dados

- Possíveis fontes de dados:
  - Computadores pessoais;
  - Dispositivos de armazenamento em rede;
  - CDs, DVDs;
  - Máquina fotográfica, relógio com comunicação via USB, etc.

Coleta dos dados

- Os dados também podem estar armazenados em locais fora dos domínios físicos da cena investigada
  - Provedores de Internet
  - Servidores FTP (*File Transfer Protocol*)
  - Servidores corporativos
- Nesses casos, a coleta dos dados somente será possível mediante ordem judicial

Coleta dos dados

- **Cópia dos dados**: envolve a utilização de ferramentas adequadas para a duplicação dos dados
- Garantir e preservar a integridade
  - Se não for garantida a integridade, as evidências poderão ser invalidadas como provas perante a justiça
  - A garantia da integridade das evidências consiste na utilização de ferramentas que aplicam algum tipo de algoritmo ***hash***
- Assim como os demais objetos apreendidos na cena do crime, os materiais de informática apreendidos deverão ser relacionados em um documento (cadeia de custódia)

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 053203 **Pag.: 01** **De: 05**

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
00001	HD de Notebook com 80GB de capacidade		
Fabricante:	Modelo:	Num. de serie:	
TOSHIBA	MK4026GAX	85MC7639T	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
20/5/2007 15:30	Paulo A. Neukamp	dcfldd	053203_01.dd	01
Drive:	HASH:			
Disco Completo	d243367072088feae98364977441d736			

CADEIA DE CUSTÓDIA

Seqüência:	Data/Hora:	Origem:	Destino	Motivo:
001	Data: 20/5/2007	Nome/Org.: Sigilo	Nome/Org.: Lab. Perí. Unisinos	Investigação sobre denuncia de Pedofilia
	Hora: 16:00	Assinatura:	Assinatura:	

Coleta de dados

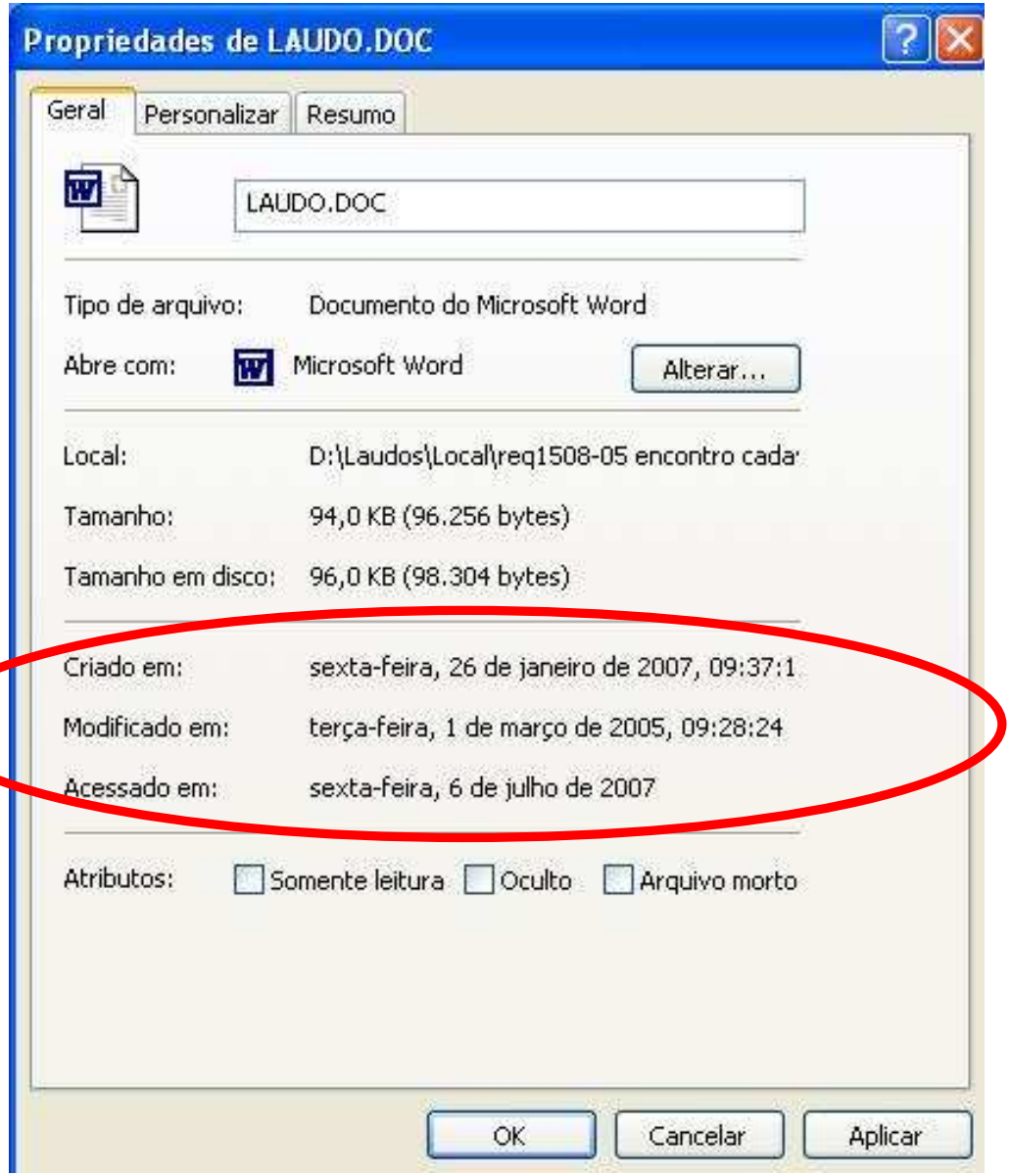
- **Cópia lógica (Backup):** as cópias lógicas gravam o conteúdo dos diretórios e os arquivos de um volume lógico. Não capturam outros dados:
  - arquivos excluídos;
  - fragmentos de dados armazenados nos espaços não utilizados, mas alocados por arquivos.
- **Imagem:** imagem do disco ou cópia *bit-a-bit* inclui os espaços livres e os espaços não utilizados:
  - mais espaço de armazenamento, consomem muito mais tempo;
  - permitem a recuperação de arquivos excluídos e dados não alocados pelo sistema de arquivos. Exemplo: setor de 4KB, arquivo com 9KB (3 setores ocupados)

Parte utilizada pelo arquivo

Parte não utilizada pelo arquivo

Coleta de dados

- Durante a aquisição dos dados é muito importante manter a integridade dos atributos de tempo *mtime* (*modification time*), *atime* (*access time*) e *ctime* (*creation time*) – MAC *Times*.
  - **Modificação:** registro da data e hora em que ocorreu a última alteração no arquivo;
  - **Acesso:** registro da data e hora em que ocorreu o último acesso ao arquivo;
  - **Criação:** registro da data e hora em que o arquivo foi criado.


Propriedades de LAUDO.DOC
Geral
Personalizar
Resumo
LAUDO.DOC
Tipo de arquivo: Documento do Microsoft Word
Abre com: Microsoft Word
Alterar...
Local: D:\Laudos\Local\req1508-05 encontro cada
Tamanho: 94,0 KB (96.256 bytes)
Tamanho em disco: 96,0 KB (98.304 bytes)
Criado em: sexta-feira, 26 de janeiro de 2007, 09:37:1
Modificado em: terça-feira, 1 de março de 2005, 09:28:24
Acessado em: sexta-feira, 6 de julho de 2007
Atributos: Somente leitura Oculto Arquivo morto
OK
Cancelar
Aplicar

Exame dos dados

- Finalidade: localizar, filtrar e extrair somente as informações relevantes à investigação → tarefa trabalhosa!
  - Capacidade de armazenamento dos dispositivos atuais
  - Quantidade de diferentes formatos de arquivos existentes (imagens, áudio, arquivos criptografados e compactados)
  - Muitos formatos de arquivos possibilitam o uso de esteganografia para ocultar dados, o que exige que o perito esteja atento e apto a identificar e recuperar esses dados
- Em meio aos dados recuperados podem estar informações irrelevantes e que devem ser filtradas.
  - Ex.: o arquivo de log do sistema de um servidor pode conter milhares de entradas, sendo que somente algumas delas podem interessar à investigação

Exame dos dados

- Após a restauração da cópia dos dados, o perito faz uma avaliação dos dados encontrados:
  - arquivos que haviam sido removidos e foram recuperados;
  - arquivos ocultos;
  - fragmentos de arquivos encontrados nas áreas não alocadas;
  - fragmentos de arquivos encontrados em setores alocados, porém não utilizados pelo arquivo.

Análise das informações

- Após a extração dos dados considerados relevantes, o perito deve concentrar suas habilidades e conhecimentos na etapa de análise e interpretação das informações.
- Finalidade: identificar pessoas, locais e eventos; determinar como esses elementos estão inter-relacionados.
- Normalmente é necessário correlacionar informações de várias fontes de dados
  - Exemplo de correlação: um indivíduo tenta realizar um acesso não autorizado a um determinado servidor
    - É possível identificar por meio da análise dos eventos registrados nos arquivos de log o endereço IP de onde foi originada a requisição de acesso
    - Registros gerados por firewalls, sistemas de detecção de intrusão e demais mecanismos de proteção

Resultados

- A interpretação dos resultados obtidos é a etapa conclusiva da investigação.
- O perito elabora um laudo pericial que deve ser escrito de forma clara e concisa, listando todas as evidências localizadas e analisadas.
- O laudo pericial deve apresentar uma conclusão imparcial e final a respeito da investigação.

Resultados

- Para que o laudo pericial torne-se um documento de fácil interpretação, é indicado que o mesmo seja organizado em seções:
  - Finalidade da investigação
  - Autor do laudo
  - Resumo do incidente
  - Relação de evidências analisadas e seus detalhes
  - Conclusão
  - Anexos
  - Glossário (ou rodapés)

Resultados

- Também devem constar no laudo pericial:
  - Metodologia
  - Técnicas
  - *Softwares* e equipamentos empregados
- Com um laudo bem escrito torna-se mais fácil a reprodução das fases da investigação, caso necessário.

Técnicas Forenses

- Boas práticas que antecedem a coleta dos dados:
  - Limpar todas as mídias que serão utilizadas ou usar mídias novas a cada investigação
  - Certificar-se de que todas as ferramentas (*softwares*) que serão utilizadas estão devidamente licenciadas e prontas para utilização
  - Verificar se todos os equipamentos e materiais necessários (por exemplo, a estação forense, as mídias para coleta dos dados, etc.) estão à disposição
  - Quando chegar ao local da investigação, o perito deve providenciar para que nada seja tocado sem o seu consentimento, com o objetivo de proteger e coletar todos os tipos de evidências
  - Os investigadores devem filmar ou fotografar o ambiente e registrar detalhes sobre os equipamentos como: marca, modelo, números de série, componentes internos, periféricos, etc.
  - Manter a cadeia de custódia.

Ferramentas Forenses

- Algumas ferramentas forenses serão mostradas nas etapas:
  - Coleta dos dados
  - Exame dos dados
  - Análise dos dados

Ferramentas Forenses – Coleta dos dados

- dd (*Disk Definition*)
- dcfldd (*Department of Defense Computer Forensics Lab Disk Definition*): versão aprimorada do *dd*, com mais funcionalidades:
  - geração do *hash* dos dados durante a cópia dos mesmos
  - visualização do processo de geração da imagem
  - divisão de uma imagem em partes
- *Automated Image & Restore* (AIR): interface gráfica para os comandos dd/dcfldd
  - gera e compara automaticamente *hashes* MD5 ou SHA
  - produz um relatório contendo todos os comandos utilizados durante a sua execução
  - elimina o risco da utilização de parâmetros errados por usuários menos capacitados


AIR 1.2.8 - Automated Image & Restore - 09/19/2005
File Source Dest Help
Source device/file:
Destination device/file:
Source Block Size: 512
Custom Block Size:
Dest. Block Size: 8192
Custom Block Size:
Options
Compression: None
Hash: md5
Verify: Yes
Use DCFLDD
Split image
Size: 2047 MBytes
Cryptcat
Key:
DD Count:
Skip (Input): 0
Seek (Output): 0
Conv: noerror
Connected devices
HDC
SDA
ZERO
NULL
NET
Start Stop Exit Show Status Window...
Enter values and click 'Start' to begin

Ferramentas Forenses – Exame dos dados

- Diversas ferramentas já permitem a utilização dos bancos de dados citados, por exemplo:
  - Autopsy
  - pyFlag
  - EnCase:
    - Padronização de laudo;
    - Recuperação de dados, banco de dados de evidências;
    - Análise de hardwares e logs.

Como funciona o EnCase

1. Create image copies of suspect media
2. Authenticate image copies via MD5
3. Analyze content of suspect media
4. Document findings

Ferramentas Forenses – Análise dos dados

- Utilitários para construção da linha de tempo dos eventos
  - ***Mactime:*** permite que a partir das informações contidas nos metadados dos arquivos e diretórios, uma visão cronológica dos acontecimentos seja mostrada
- Muitos arquivos importantes que fazem parte dos sistemas operacionais da família Windows não possuem uma clara explicação de suas estruturas
  - ***Pasco:*** analisa os índices dos arquivos do Internet Explorer (index.dat), exportando os resultados em um formato de texto padrão, inteligível por humanos e que utiliza como delimitador de campos o caractere “|”
  - ***Galleta:*** analisa os *cookies* existentes em uma máquina e separa as informações úteis em campos para que possam ser manipuladas por outros programas

Considerações Finais

- Forense computacional é um tema bastante atual e que tem recebido atenção significativa tanto da comunidade científica quanto da indústria.
- Muitas vezes a investigação não pode prosseguir sem a verificação de computadores de suspeitos → necessidade de pessoal qualificado.
- O surgimento de legislação e padrões a serem aplicados (Brasil) referentes à forense computacional tornariam menor a chance de laudos serem inutilizados por falta de experiência dos peritos.

Referências Bibliográficas

- Neukamp, Paulo A. Forense Computacional: Fundamentos e Desafios Atuais. 11 Junho de 2007. Universidade do Vale do Rio dos Sinos (UNISINOS). 06 Nov. 2007.
- http://www.imasters.com.br/artigo/4175/forense/introducao_a_computacao_forense/
- http://www.guidancesoftware.com/pt/products/ee_index.asp

Dúvidas?

Obrigado!