

Forense Digital / Computacional

CIn – UFPE, 2007

Forense Computacional

- Agenda
 - Introdução
 - Ciência Forense
 - O que é Ciência Forense, O que *NÃO É* Ciência Forense
 - Forense Digital / Computacional
 - Etapas de Investigação
 - Coleta, Exame, Análise e Resultados
 - Técnicas Forenses
 - Ferramentas Forenses (etapas da investigação)
 - Técnicas Anti-Forense
 - Conclusão

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.*”

Ciência Forense

- Diz-se da aplicação de campo científico específico à investigação de fatos relacionados a crimes e/ou contendas judiciais.
- Ou simplesmente: A aplicação da Ciência no Direito

The Forensic Science Society

(<http://www.forensic-science-society.org.uk>)

Ciência Forense

- Archimedes (287-212 a.C.)
 - Quantidade real de ouro da Coroa calculada pela teoria do peso específico dos corpos.
- Impressões digitais
 - Utilizadas no *século VII* como comprovação de débito (a impressão digital do devedor era anexada à conta).
- Medicina e Entomologia
 - Referidas no livro “Collected Cases of Injustice Rectified”, de Xi Yuan Ji Lu, em 1247.
 - Foice e moscas, afogamento (pulmão e cartilagens do pescoço), entre outros.

Ciência Forense

- Século XX – A evolução da Ciência Forense
 - Pesquisas que conduziram à identificação do tipo sanguíneo e a análise e interpretação do DNA;
 - Publicação dos principais estudos referentes à aplicação de métodos e técnicas utilizadas na investigação de crimes;
 - Criado o “*The Federal Bureau of Investigation* (FBI)”, uma referência no que tange à investigação de crimes e a utilização de técnicas forenses em diversas áreas.

Ciência Forense

- Atualmente, existem peritos especializados em diversas áreas científicas, entre elas:
 - Análise de documentos (documentoscopia);
 - Criminalística (Balística, Impressões digitais, substâncias controladas);
 - Antropologia (identificação de restos mortais, esqueletos)
 - Arqueologia;
 - Entomologia (insetos, verificação de data, hora e local);
 - Odontologia;
 - Computação (Forense Computacional ou Forense Digital);
 - E outras: Patologia, Psicologia, Toxicologia, Metrologia, ...

O que Ciência Forense
Não é!



Forense Digital/Computacional

- Objetivo:
 - Suprir as necessidades das instituições legais no que se refere à manipulação das *novas formas de evidências eletrônicas*.
 - Ela é 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.
 - Através da utilização de métodos *científicos* e *sistemáticos*, para que essas informações passem a ser caracterizadas como evidências e, posteriormente, como *provas legais* de fato.

“Forense Computacional: Aspectos Legais e Padronização”
(<http://www.ppgia.pucpr.br/~maziero/pesquisa/ceseg/wseg01/14.pdf>)

Forense Digital/Computacional

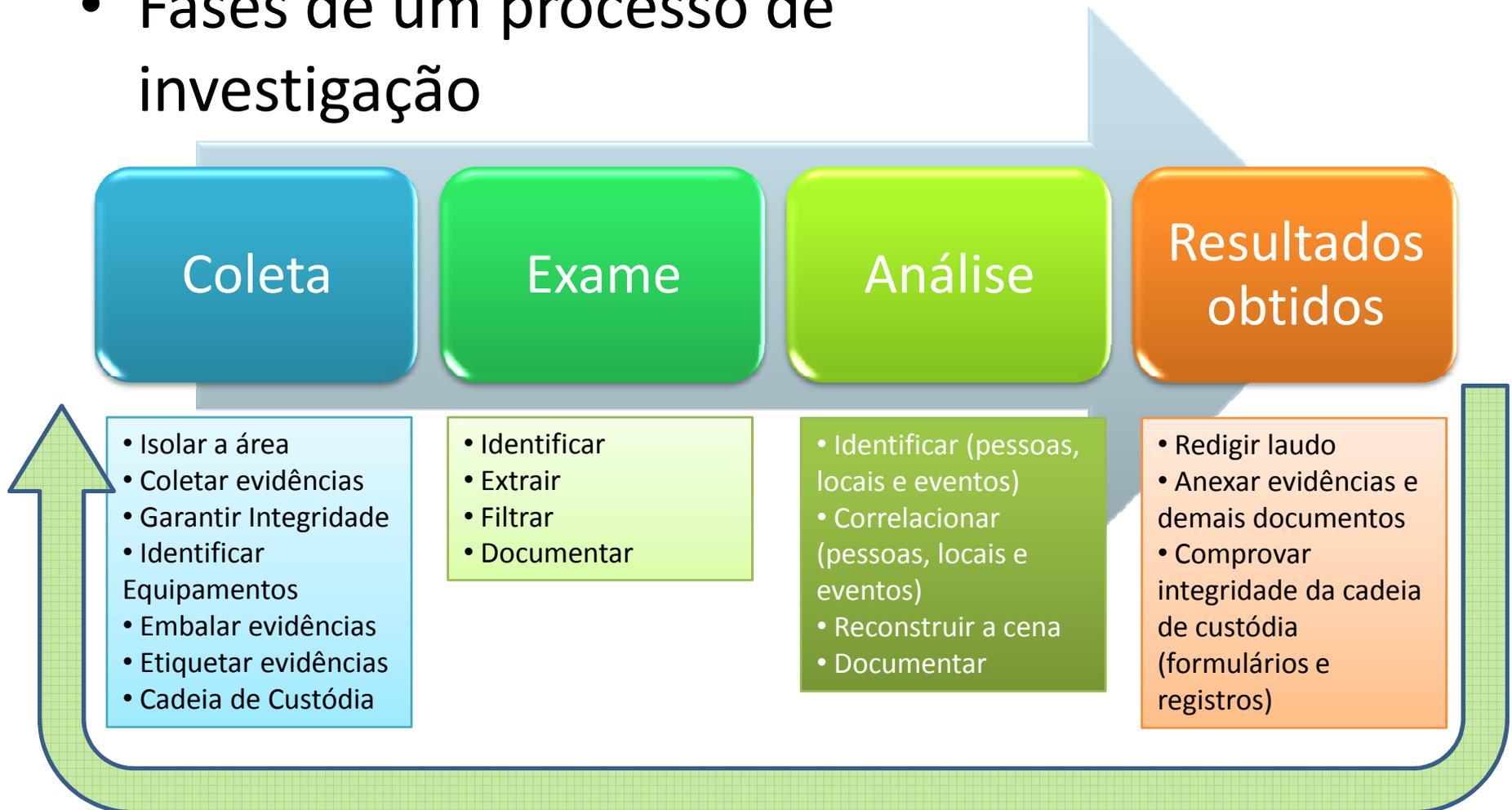
- É utilizada com fins:
 - Legais
 - ex.: investigação de casos de espionagem industrial, roubo de identidade, extorsão ou ameaças.
 - Ações disciplinares internas
 - ex.: uso indevido de recursos da instituição, ou eventos onde não se deseja chamar a atenção externa

Forense Digital/Computacional

- Ocorrências mais comuns:
 - Calúnia, difamação e injúria via e-mail ou web
 - Roubo de informações confidenciais
 - Remoção de arquivos
- Outros crimes:
 - Pedofilia
 - Fraudes
 - Auxílio ao tráfico de drogas e intorpecentes

Etapas da investigação

- Fases de um processo de investigação



Coleta de Dados

- Identificação de possíveis fontes de dados:
 - Computadores pessoais, laptops;
 - Dispositivos de armazenamento em rede;
 - CDs, DVDs;
 - Portas de comunicação: USB, Firewire, Flash card e PCMCIA;
 - Máquina fotográfica, relógio com comunicação via USB, etc.



<http://www.krollontrack.com.br>



Coleta de 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*) – ex. [Formulário de Cadeia de Custódia](#)

Coleta de Dados

- Após a identificação das possíveis origens dos dados, o perito necessita *adquiri-los*.
- Para a aquisição dos dados, é utilizado um processo composto por *três etapas*:
 - Identificação de prioridade;
 - Cópia dos dados;
 - Garantia e preservação de integridade.

Coleta de Dados:

Identificação de Prioridade

- Identificar a prioridade da coleta: o perito deve estabelecer a ordem (*prioridade*) na qual os dados devem ser coletados
 - *Volatilidade: dados voláteis* devem ser *imediatamente coletados* pelo perito.
 - Ex.: o estado das conexões de rede e o conteúdo da memória
 - *Esforço*: envolve não somente o *tempo gasto* pelo perito, mas também o *custo* dos equipamentos e serviços *de terceiros*, caso sejam necessários.
 - Ex.: dados de um roteador da rede local x dados de um provedor de Internet
 - *Valor estimado*: o perito deve *estimar um valor relativo* para cada provável fonte de dados, para *definir a seqüência* na qual as fontes de dados serão investigadas

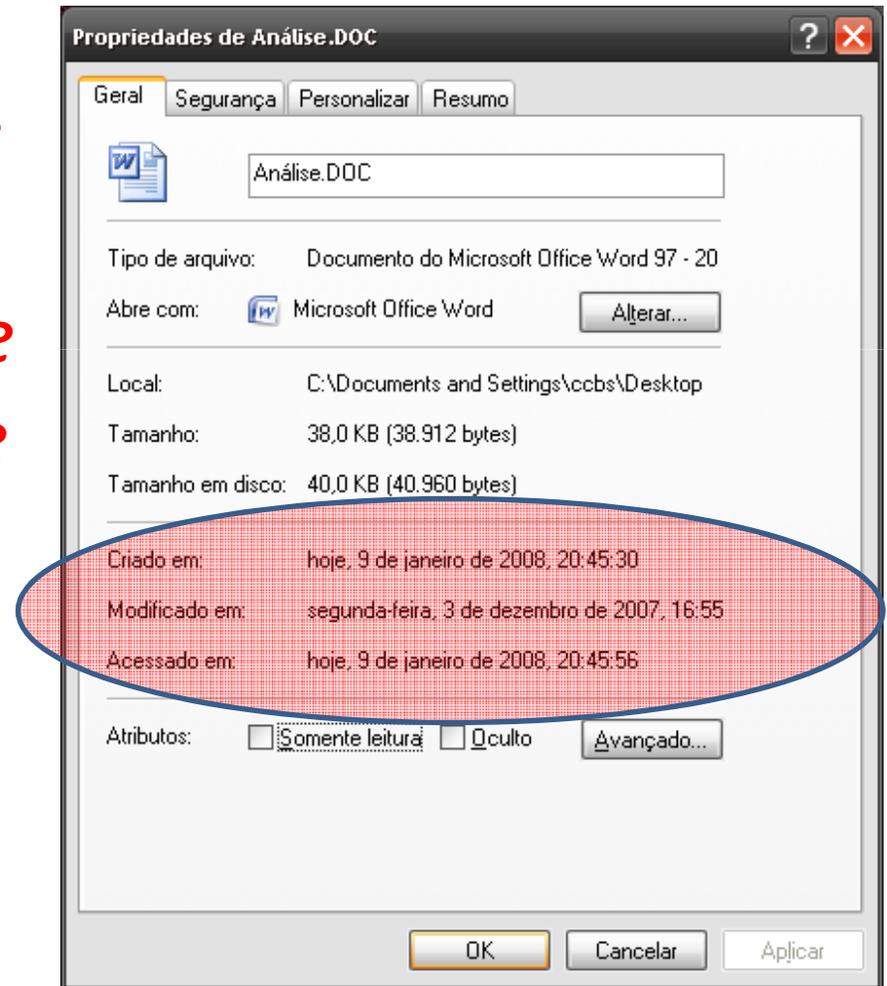
Coleta de Dados: *Cópia dos dados*

- *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)



Coleta de Dados: *Garantia e preservação de integridade*

- 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*.



Exame dos Dados

- *Finalidade*: localizar, filtrar e extrair somente as informações relevantes à investigação.
 - Devemos considerar:
 - Capacidade de armazenamento dos dispositivos atuais
 - Quantidade de diferentes formatos de arquivos existentes
 - Ex.: 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 dos Dados

- 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 e apresentação 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 *filmар 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 !!!*

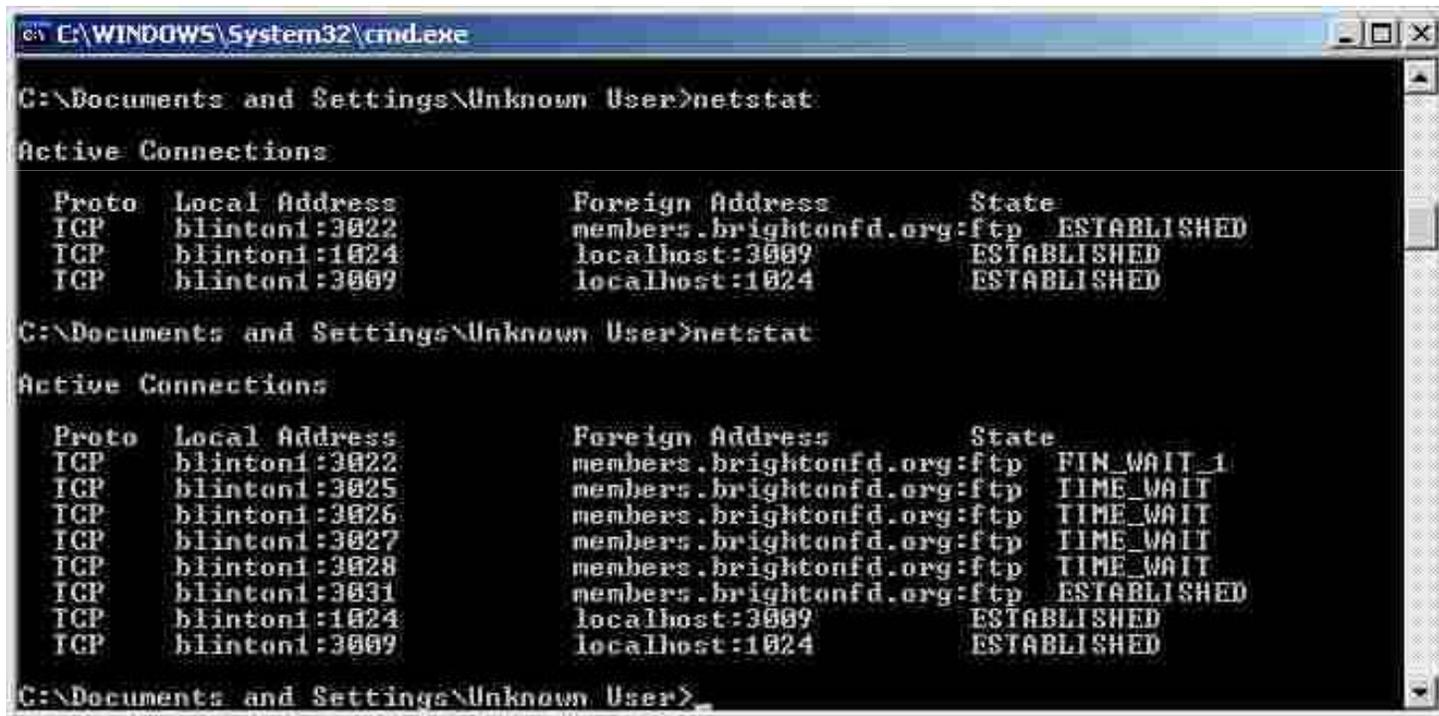
Ferramentas Forenses

- Algumas ferramentas forenses comumente utilizadas nas etapas:
 - Coleta dos dados
 - Avaliar: Live Forensics ou Post-Mortem
 - Exame dos dados
 - Análise dos dados

Técnicas Forenses

Coleta de dados voláteis

- Sempre que possível e relevante a investigação:
 - *Conexões de rede (netstat)*



```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\Unknown User>netstat
Active Connections
Proto Local Address          Foreign Address         State
TCP    blinton1:3022          members.brightonfd.org:ftp ESTABLISHED
TCP    blinton1:1024         localhost:3009          ESTABLISHED
TCP    blinton1:3009         localhost:1024          ESTABLISHED
C:\Documents and Settings\Unknown User>netstat
Active Connections
Proto Local Address          Foreign Address         State
TCP    blinton1:3022          members.brightonfd.org:ftp FIN_WAIT_1
TCP    blinton1:3025          members.brightonfd.org:ftp TIME_WAIT
TCP    blinton1:3026          members.brightonfd.org:ftp TIME_WAIT
TCP    blinton1:3027          members.brightonfd.org:ftp TIME_WAIT
TCP    blinton1:3028          members.brightonfd.org:ftp TIME_WAIT
TCP    blinton1:3031          members.brightonfd.org:ftp ESTABLISHED
TCP    blinton1:1024         localhost:3009          ESTABLISHED
TCP    blinton1:3009         localhost:1024          ESTABLISHED
C:\Documents and Settings\Unknown User>
```

Técnicas Forenses

Coleta de dados voláteis

- *Sessões de Login (EventViewer / who -u)*
 - dos usuários;
 - das ações realizadas;
- *Conteúdo da memória (WinHEX / dump)*
- *Processos em execução (ProcessXP / ps)*
- *Arquivos abertos*
- *Configuração de rede*
- *Data e hora do sistema operacional*

Ferramentas Forenses

Coleta de dados não voláteis

- *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

Ferramentas Forenses

Coleta de dados não voláteis



Ferramentas Forenses

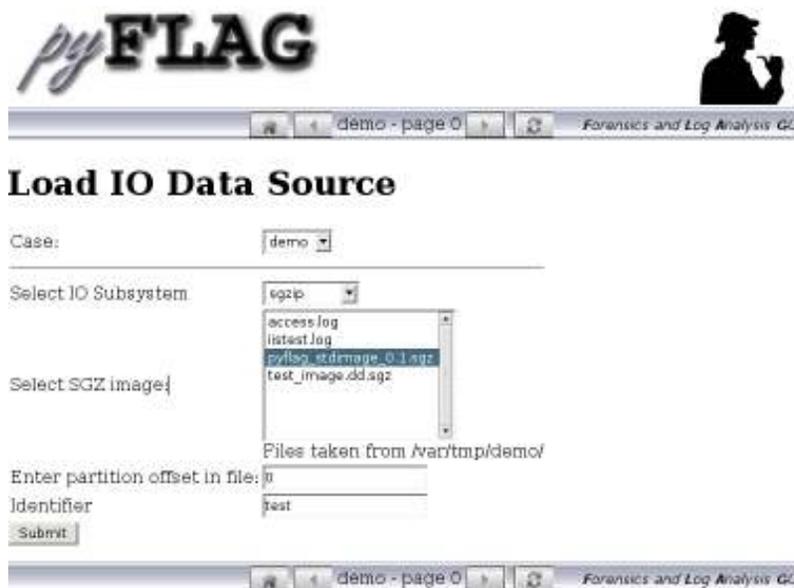
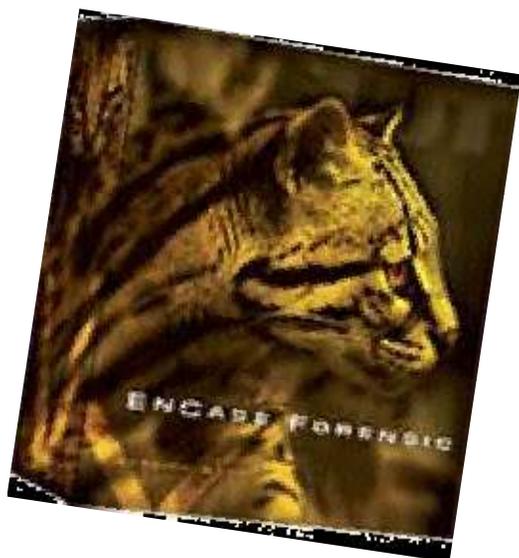
Exame dos dados

- Utilizando assinaturas de arquivos comuns, a quantidade de arquivos a ser analisada pode ser reduzida significativamente
 - Ex.: projeto *National Software Reference Library* (NSRL)
 - <http://www.nsrl.nist.gov/Downloads.htm#isos>
 - Total de 43.103.492 arquivos, distribuídos em 4 “discos”

Ferramentas Forenses

Exame dos dados

- Diversas ferramentas já permitem a utilização dos bancos de dados citados, por exemplo:
 - EnCase
 - Autopsy & SleuthKit
 - PyFLAG



Ferramentas Forenses

Exame dos dados

- EnCase
 - Padronização de laudo;
 - Recuperação de dados, banco de dados de evidências;
 - Análise de hardwares e logs.



- 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* (Componente do *SleuthKit*)
- Utilitários de navegação em arquivos da estrutura do Sistema Operacional Windows
 - *Pasco* - <http://www.opensourceforensics.org>
 - Analisa os índices dos arquivos do Internet Explorer
 - *Galleta (Cookie em espanhol)* – *FoundStone.com*
 - *analisa os cookies existentes em uma máquina e separa as informações úteis*

Ferramentas Anti-forense

Destruir/Ocultar dados

- **Objetivo:** destruir, ocultar ou modificar as evidências existentes em um sistema a fim de dificultar o trabalho realizado pelos investigadores
 - Também podem ser utilizadas antes de venda ou doação de mídias a outras pessoas (evita recuperação de dados)
- **Destruição dos Dados:** para impedir ou pelo menos dificultar a recuperação dos dados, são utilizadas ferramentas conhecidas como **wiping tools** para a remoção dos dados
 - *Wipe*
 - *Secure-delete*
 - *PGP/GPG wipe*
 - *The Defiler's Toolkit*
 - *Darik's Boot and Nuke*

Ferramentas Anti-forense

Destruir/Ocultar dados

- *Ocultar Dados*

- Criptografia e esteganografia podem ser aplicados em arquivos, tornando-se uma barreira difícil de ser superada.

- Utilizar ferramentas de *esteganoanálise* em uma mídia de 80GB requer muito tempo e na prática nem sempre é algo viável de se realizar
- O mesmo ocorre quando se trata de arquivos criptografados

- Ex.:

- TrueCrypt, PGP/GPG, Steganos , Hide and Seek, ...

Ferramentas Anti-forense

Destruir/Ocultar dados

- *Outras finalidades*

- Principalmente focado em dificultar ou impedir o trabalho do perito forense, algumas ferramentas têm como objetivo impedir uma das etapas da investigação:

- *Metasploit Anti-Forensic Investigation Arsenal (MAFIA)*
 - *Windows Memory Forensic Toolkit*

Conclusões

- Forense Digital/Computacional é um dos aspectos de Segurança de Informações que chama bastante atenção tanto de corporações quanto da comunidade científica
- Apesar das diversas ferramentas disponíveis que facilitam sobremaneira a ação do perito, a conclusão final ainda paira sobre a experiência, competência e integridade do profissional que conduziu a investigação

Algumas Referências

- 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