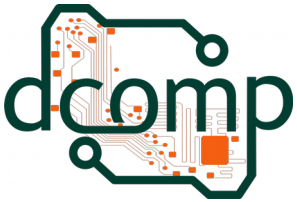
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCA UFES
Departamento de Computação



Investigação Digital

Computação Forense

Site: http://jeiks.net
E-mail: jacsonrcsilva@gmail.com

Tópicos

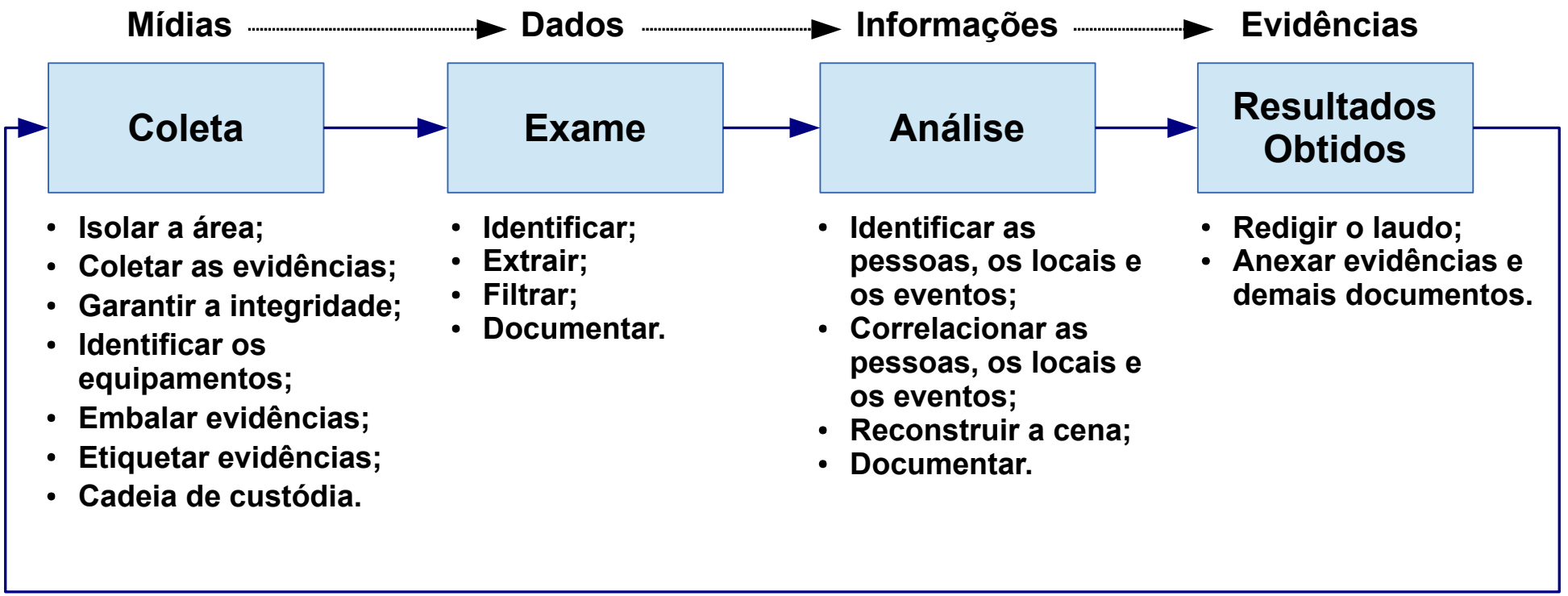
- Processo de investigação Digital:
  - Coleta de Dados;
  - Exame de Dados;
  - Análise das Informações;
  - Interpretação dos resultados;

    Obs.: futuramente esses tópicos serão novamente discutidos, porém com mais detalhes e com casos de estudo.
- Metodologias de Análise Forense:
  - *Live Forensics*;
  - *Post Mortem Forensics*.
- Desenvolvimento de ferramentas para a análise forense.

Processo de Investigação Digital

- Basicamente, possui quatro etapas:
  - Coleta dos dados:
    - Obter os dados mantendo sua integridade. Armazenar de forma segura os dados e os equipamentos coletados e identificá-los.
  - Exame dos dados:
    - Seleção e utilização das ferramentas e técnicas apropriadas para cada tipo de dado coletado.
  - Análise das informações:
    - Analisar os dados filtrados na etapa de Exame, com intuito de obter informações úteis e relevantes para o caso.
  - Interpretação dos resultados:
    - Criação de um relatório com a descrição dos procedimentos realizados e os resultados obtidos.

Processo de Investigação Digital



Coleta dos Dados

- Identificar as possíveis fontes de dados, como:
  - Computadores pessoais;
  - Laptops;
  - Celulares;
  - Dispositivos de armazenamento em geral.
- O armazenamento também pode ser externo:
  - Servidores FTP;
  - Servidores de E-mail;
  - Servidores corporativos;
  - Servidores de armazenamento de dados (Dropbox).
- O acesso aos dados deve ser realizado sob ordem judicial.

Coleta dos Dados

- Após identificar, deve-se adquirir os dados.
- As etapas da aquisição dos dados:
    1. Prioridade da coleta dos dados:
        - Volatilidade: tomar cuidado com a preservação dos dados mediante seu meio de armazenamento, como dados de rede e da memória virtual.
        - Esforço: verificar a dificuldade de coletar dados e também o tempo necessário, o custo do equipamento e serviços de terceiros, se necessários.
        - Valor estimado: estimar um valor relativo para os dados que podem ser encontrados em cada provável fonte de dados.

Coleta dos Dados

- As etapas da aquisição dos dados:

  2. Copiar dados:
     - Utilizar as ferramentas adequadas para obter e duplicar os dados da mídia de armazenamento, tanto voláteis quanto não-voláteis.
  3. Garantir e preservar a integridade dos dados:
     - Após a coleta dos dados, deve-se preservar a integridade dos mesmos.
     - A integridade de um dado permite que o mesmo seja utilizado perante a justiça.
     - Para garantir em um laudo a integridade dos dados, pode-se realizar um *hash* sobre os arquivos ou mídias obtidas na investigação.

Trabalhando com *hashes*...

Exame dos Dados

- Tem como finalidade analisar e extrair informações relevantes à investigação:
  - Analisar os arquivos e seu conteúdo para encontrar as evidências do evento.


```
grep -n conteúdo arquivos
strings arquivo
hexdump -C arquivo
wxHexEditor
```

- Filtrar as informações dentre os dados coletados:
  - Tentativas de invasão em um arquivo de *log*;
  - Arquivos apagados em um sistema de arquivos;
  - Imagens com conteúdos implícitos;
  - etc.
- Ideal utilizar ferramentas que permitam a pesquisa por termos chave e por determinados tipos de arquivos.

Obs.: tipos de arquivos

- Determinados por extensões:
  - exe, arj, doc, rar, zip, …
- Determinados por Assinaturas:
  - Chamado de *File Signatures*, mais especificamente:

    "*Magic Numbers*"
  - São os primeiros bytes de um arquivo, podendo variar de 1 a 4 bytes;
  - Um banco de dados de assinaturas conhecidas encontra-se em: <http://www.filesignatures.net>


```
file -Lks arquivo
python3 -c "print( open('arquivo', 'rb').read(4).hex() )"
```

Análise das Informações

- Momento de analisar as informações:
  - Identificar pessoas, locais e eventos relacionados à investigação;
- Alguns exemplos:
  - IP do invasor;
  - Imagem da cena do crime;
  - E-mails apagados;
  - Softwares piratas instalados/removidos; …

- Dependem da experiência e do conhecimento do perito, pois não existem ferramentas para isso.
- Demandam então muito tempo.

Interpretação dos Resultados

- Etapa conclusiva da investigação;
- Momento da construção do Laudo pericial, que deve:
  - Ser claro e de fácil interpretação por **qualquer** pessoa;
  - Pode ser jurídico ou técnico;
  - Deve ser organizado em seções, como: introdução; objetivos; metodologia; evidências analisadas e detalhes; conclusão; e anexos.
  - Se necessário, adicione referências.
  - Lembre-se de responder tudo que foi pedido de forma direta e clara.

Interpretação dos Resultados

- O Laudo deve apresentar uma conclusão **imparcial** e **final** sobre a investigação.
- Qualquer item escrito que possa causar dúvidas ou não ser claro, servirá para atrasar o tempo do processo e para você não ser mais nomeado como perito.
- Cite tudo que foi realizado para encontrar as evidências:
  - Metodologia e técnicas utilizadas;
  - Ferramentas e *softwares* utilizados;
  - Qual a licença do software utilizado;
  - TUDO necessário para que as fases de investigação possam ser reproduzidas.

Mão na Massa

Supondo que você seja um perito e que deva investigar por contratos realizados entre a empresa EMP e o cliente José. Faça:

1. Descreva como seriam suas ações no trabalho de perito.

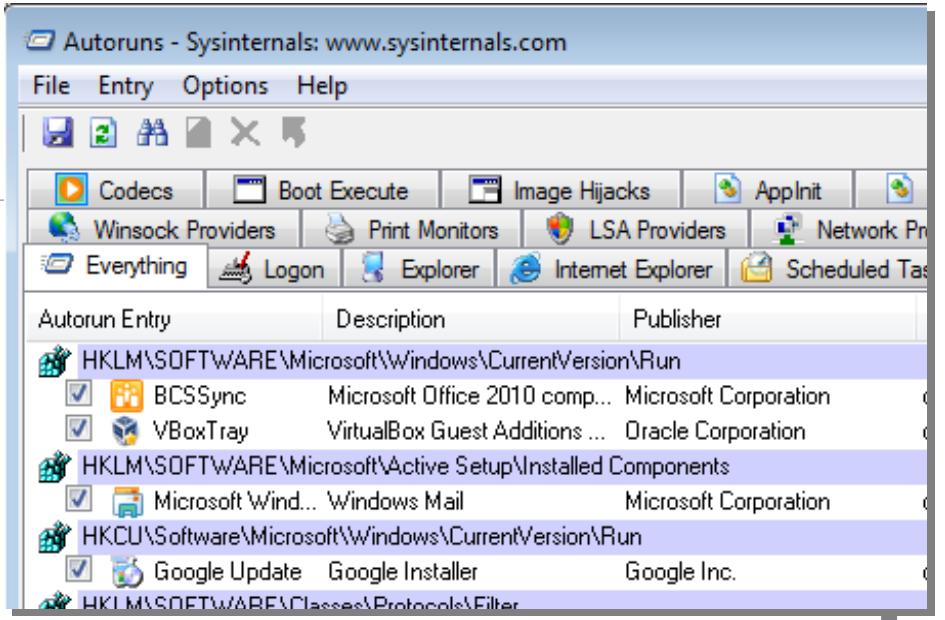
2. Descreva como seria seu Laudo.

Metodologias de Análise Forense

- *Live Forensics*:
  - Investigação do equipamento ainda em funcionamento (antes de ser desligado).
- *Post Mortem Forensics*:
  - Investigação do equipamento após o desligamento do equipamento.

Live Forensics

- Caracteriza-se pela investigação do equipamento ainda em funcionamento.
- Único método que permite a aquisição de informações voláteis, como por exemplo:
  - processos que estão executando no computador;
  - tabelas de roteamento;
  - conexões estabelecidas entre conexões de rede;
  - arquivos temporários;
  - dados da memória principal;
  - etc.
- É necessário cuidado para não atrapalhar as evidências com as ferramentas forenses utilizadas.
- Os dados nessa análise são voláteis e podem ser corrompidos ou perdidos facilmente.



Windows:

- CTRL+ALT+DEL

- tasklist /svc (no cmd)

- Programa Autoruns da Microsoft:

https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx

- Despejo de memória:

Configurar em:

Computador->Propriedades->Avançado->Despejo de memória...

Pressionar: CTRL + SCROOL LOCK + SCROOL LOCK

http://support.microsoft.com/kb/927069/pt-br

GNU/Linux:

- ps fax, pidof e /proc

- /dev/mem

- strings -a

- hexdump

Post Mortem Forensics

- Caracteriza-se pela investigação realizada após o desligamento do equipamento.
- Deve-se verificar se o equipamento não perderá informações ao ser desligado.
- Nunca inicie o sistema do investigado (dê boot no HD dele) após desligar o equipamento. Utilize um sistema secundário para a análise.
- É recomendado:
  - Criar uma cópia fiel (duplicação forense) do material questionado para uma posterior análise;
  - Efetuar um *hash* da cópia criada e da cópia original e colher assinaturas dos responsáveis.
    - Isso garantirá que a imagem entregue a justiça era a original;
    - Isso garantirá que ninguém questione sobre a cópia de trabalho do perito.

No Linux:
Insira um pendrive no seu computador.
Após isso, crie uma imagem do mesmo com a ferramenta: dcfldd
Exemplo:

```
mkdir copia && cd copia
dmesg | tail
dcfldd if=/dev/sdb of=sdb.dd hash=md5,sha256   \
            md5log=sda.dd.md5 sha256log=sda.dd.sha256
```

Na máquina virtual:
Inicie os *Lives Forenses* e verifique quais são as ferramentas que podem ser utilizadas nos tópicos da aula de hoje.
Crie sua lista de ferramentas para possíveis investigações futuras.

Como desenvolver ferramentas para análise forense?

Desenvolvendo ferramentas forenses

- Necessário:
  - Conhecer como os dados são armazenados em mídias de armazenamento;
  - Compreender o funcionamento do dispositivo;
  - Conhecer os sistemas de arquivos.
  - Dominar uma linguagem de programação rápida e eficaz para trabalhar *bit a bit*;
  - Dominar o trabalho com arquivos e operações entre diferentes bases;
  - Dominar a tabela de codificação ASCII e UNICODE;