Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos
Curso: Tecnologia em Sistemas para Internet
Disciplina: Segurança e Preservação de Dados

# Atividade Prática em Laboratório (Roteiro) - Computação Forense com Autopsy

Esta é uma prática de fixação para exercitar um dos conteúdos apresentados no tópico 'Computação Forense'. A intenção da atividade é praticar a análise de imagens periciais usando a ferramenta **Autopsy Digital Forensics**.

**01.** Baixe o arquivo pronto (docker-compose.yml) com a indicação da imagem personalizada do Autopsy e as configurações necessárias para executar o contêiner:

```
$ mkdir autopsy
$ cd autopsy
$ wget https://www.segurancaderedes.com.br/spd/pratica10/docker-compose.yml
```

**02.** Execute/ative o contêiner:

```
$ docker compose up -d
```

**03.** Acesse o contêiner:

```
$ docker exec -it autopsy bash
```

**04.** Baixe para dentro do contêiner o arquivo de imagem pericial que será analisado:

```
# cd /home/autopsy/files
# wget https://www.segurancaderedes.com.br/spd/pratica10/imagem_pendrive.tgz
# tar -xvzf imagem_pendrive.tgz
```

**05.** Verifique o endereço IP atribuído ao contêiner (para o acesso a partir do terminal de sua máquina):

```
# hostname -I
```

**06.** Abra outro terminal em seu computador e conecte-se via SSH ao docker (informando o IP descoberto no passo anterior) com o parâmetro '-X' para exportar o display gráfico da ferramenta:

```
$ ssh -X autopsy@IP_DO_CONTÊINER
(exemplo: ssh -X autopsy@172.18.0.2)
```

- Digite '`yes`' para configuração de primeiro acesso SSH
- Informe a senha: **`forensics`**

**07.** Execute o Autopsy no contêiner (a interface gráfica será exportada para fora do docker através da conexão SSH):

```
autopsy@autopsy:~$ autopsy --nosplash
```

- Clique no botão '`OK`' na tela inicial de informações

**08.** Clique em '`New Case`' para iniciar um 'novo caso' no framework:


**09.** Informe um 'nome' para o novo caso (`Case Name`) escolha um diretório onde serão armazenados os dados coletados/analisados (`Base Directory`) e clique no botão '`Next`'.

**10.** Para esta prática não precisa preencher a tela de informações opcionais (`Optional Information`), basta apenas clicar no botão '`Finish`'.

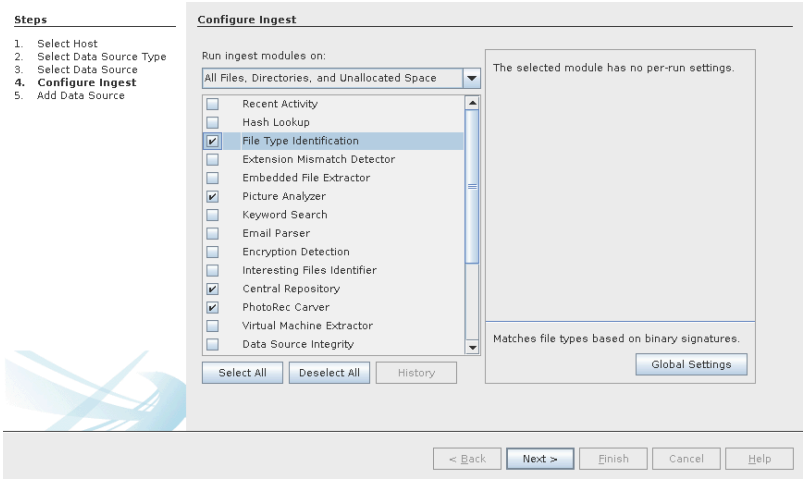
**11.** Clique no botão '`Next`' indicando a criação de um 'novo `Host Name`' para referenciar a imagem forense que será analisada.

**12.** Clique no botão '`Next`' indicando que deseja selecionar como tipo de fonte de dados (`Data Source Type`) uma imagem de disco (`Disk Image or VM File`).

**13.** Informe agora onde está o arquivo de imagem pericial que você quer analisar (`Data Source Type`). Clique no botão '`Browse`' e selecione a imagem do 'pendrive' que baixamos no início da prática e depois de selecionar clique no botão '`Next`'.

**14.** Indique agora quais módulos do Autopsy (`Ingest Modules`) serão aplicados na imagem pericial sob análise. Inicialmente desmarque todos, clicando no botão '`Deselect All`' e selecione (clicando na caixinha ao lado de cada módulo) os seguintes módulos:

- `File Type Identification`
- `Picture Analyzer`
- `Central Repository`
- `PhotoRec Carver`




**15.** Clique no botão '`Next`' para seguir e, em seguida, no botão '`Finish`'.

O arquivo de imagem foi processado, com todos os 'Ingest Modules' selecionados executados para realizar a extração/recuperação/análise da imagem!!!

**16.** Explore agora a ferramenta, fazendo a análise dos resultados. Como a imagem de 'pendrive' utilizada só tinha arquivos de imagens (figuras) neste caso analise as imagens extraídas/recuperadas:

- `File Types` ➡ `By Extension` ➡ `Images` (Veja as imagens extraídas/recuperadas)