

Forensics

Experimento 05 – Teoria e Experimento

Não precisamos acionar o Wireshark
para esse experimento

Forensics (Forense)

- A Forense (também conhecida como ciência forense computacional) é um ramo da ciência forense digital pertencente a evidências encontradas em computadores e mídias de armazenamento digital. O objetivo da computação forense é examinar a mídia digital de uma maneira forense, com o objetivo de identificar, preservar, recuperar, analisar e apresentar fatos e opiniões sobre a informação digital.
- Embora seja mais frequentemente associado à investigação de uma ampla variedade de crimes de informática, a computação forense também pode ser usada em processos civis.
- A disciplina envolve técnicas e princípios semelhantes à recuperação de dados, mas com diretrizes e práticas adicionais projetadas para criar uma trilha de auditoria legal.

Forensics (Forense)

- Evidências de investigações forenses computacionais são geralmente submetidas às mesmas diretrizes e práticas de outras evidências digitais. Ele tem sido usado em vários casos importantes e está se tornando amplamente aceito como confiável nos sistemas de tribunais dos EUA e da Europa.
- Kali tem várias ferramentas forenses embutidas em sua caixa de ferramentas. Podemos encontrar essas ferramentas no Kali Linux -> Forensics.
 - Forensics Imaging Tools (imagens de investigação auditáveis)
 - Forensics Carving Tools (Coleta, Identificação e Extração de Dados)
 - Digital Forensics (Análise)

<<https://h11dfs.com/the-best-open-source-digital-forensic-tools/>>

Digital Forensics (Analysis)

- A contestação de técnicas periciais utilizadas (quando provada tecnicamente) pode inviabilizar todo o esforço pericial...
- Na maioria das vezes é mais fácil provar que as técnicas utilizadas foram inadequadas que provar que o acusado é inocente.
- A aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade” (Manual de Patologia Forense do Colégio de Patologistas Americanos, 1990).

Digital Forensics: Conceitos Importantes

- Evidências
 - Não-Voláteis x Voláteis
 - Tipos de Análise:
 - In Loco ou Post mortem
 - Recuperação
 - Extração
- ❖ Principais Etapas: Aquisição, Identificação, Avaliação, Apresentação

Digital Forensics: O que Coletar/Analisar

- Mídias: Hds, pendrives, cds, dvds...
- Dispositivos não convencionais: Câmeras digitais, óculos/relógios/pulseiras (com dispositivos de armazenamento).
- Dados trafegando na rede: Em investigações de tráfego de informações com equipamentos ligados e “trafegando”.
- Dados em memória: Análises com equipamentos ligados

IMPORTANTE (Informações Cronológicas)

Saber quando uma sequencia de eventos ocorreu pode ser mais importante do que saber o que ocorreu. MACtimes - São atributos de tempo de um arquivo (mtime, atime e ctime).

- mtime (Modification time): mostra a ultima data e hora em que o arquivo foi modificado.
- atime (Access time): mostra a ultima data e hora em que um diretorio ou arquivo foi acessado/lido.
- ctime (Creation time): mostra a data e hora em que arquivo foi criado.

Comando touch

- \$ touch -m 0909141940 arquivo
- \$ touch -c -t 20181108140000.15 mem.dump

Coletar (Imaging)

- Se você tem experiência como administrador de sistema ou de rede, provavelmente já fez backups do sistema. Estas são cópias simples do sistema operacional, aplicativos e dados para um disco rígido ou, às vezes, unidades voláteis. Infelizmente, tal cópia não funcionará para nós, o investigador forense.
- O que precisamos é de uma cópia bit-a-bit do disco rígido ou da memória que não altere um único bit de informação.
- Vários softwares que transferem a cópia para essa imagem poderá alterá-la, e não poderemos apresentá-la em um tribunal.

Coletar (Imaging)

Ferramenta dd (ou evolução dela)

- Linux (nativo em todas as principais distribuições)
- Windows (<http://www.chrysocome.net/dd>)

dd if=origem of=destino

Ex.: Geração da Imagem (partição hda1 para arquivo imagem.dd):

```
# dd if=/dev/hda1 of=imagem.dd
```

Importante:

- o dd (e ferramentas semelhantes) fazem a cópia bloco a bloco (e não bitabit). O sistema operacional disponibiliza os dados para as ferramentas em forma de blocos (ou clusters, em sistemas de arquivos Microsoft). Os blocos mais comuns têm 4KB.
- Apesar de ser a maneira mais simples e eficiente de realizar a duplicação, o utilitário dd não oferece algumas funcionalidades importantes;

Comando “dd”

- Historicamente, quase todas as distribuições Linux / UNIX incluíam um comando conhecido como dd (disk-to-disk). Sua finalidade era fazer uma cópia bit-a-bit de qualquer arquivo, unidade ou partição. A sintaxe básica do dd é algo como isto:

`dd if=<source> of=<destination> bs=<byte size>`Por

- Como exemplo, ilustramos:

`dd if=/dev/sda2 of=/dev/sdb2 bs=512`

- Isso criaria uma cópia de bit a bit de sda2 para sdb2 usando um tamanho de byte de 512 bytes. Existem muitas opções para o dd, mas um dos mais usados é o **noerror**. Quando usamos a opção noerror, o dd não terminará quando encontrar erros, então o nosso comando ficaria assim:

`dd if=/dev/sda2 of=/dev/sdb2 bs=512 noerror`

Kali Linux dcfldd

- Embora a maioria das distribuições do Linux inclua `dd`, diversas variações foram desenvolvidas e aprimoradas, o que facilita o processo de aquisição de imagens forenses. Quase toda ferramenta de aquisição de imagens existente, seja para Windows ou Linux, é uma variação do `dd`.
- No Kali Linux, temos uma versão do `dd` que foi desenvolvida pelo Laboratório Forense de Computação Digital do Departamento de Defesa que é `dcfldd` (presumivelmente, computador digital de laboratório forense `dd`).
- O **`dcfldd`** possui um log de toda a operação, faz divisão da imagem (`split`) e permite verificar diretamente a integridade da operação através de vários algoritmos de hash.
- Existe ainda o `dc3dd`, que é uma reescrita do `dcfldd` (ferramenta atualmente mais completa)

Kali Linux dcfldd

Assim, **dcfldd** é uma **versão melhorada do GNU dd** com características úteis para Forense e segurança e tem como características adicionais:

- **Hash On-the-fly** dos dados transmitidos.
- **Barra de progresso** da quantidade de dados que já foram tratados.
- **Wipe** - Limpeza de discos com padrões conhecidos.
- **Check** - Verificação se a copia gerada é idêntica a unidade original, bit por bit.
- **Destino duplo** - Saída simultânea para mais de um arquivo / disco é possível.
- **Split** - A saída pode ser dividido em vários arquivos.

Nota : Na descrição teórica do experimento apresente essas características com mais detalhes.

Kali Linux dcfldd

```
dcfldd if=/dev/sda1 hash=md5,sha256 hashwindow=1G \
md5log=md5.txt sha256log=sha256.txt hashconv=after \
conv=noerror,sysc split=1G splitformat=aa of=image.dd
```

- noerror = não para caso encontre erros
- sysc = se encontrar erro preenche com 0 (zero)
- Tamanho máximo de cada arquivo = 1Gb
- Nomes: image.dd.aa / image.dd.bb / ...

Existe ainda interfaces GUI para isso ...

- Helix 3 Pro, produção de imagens baseado no Adepto 2.1 usando a interface Air

Nota : Na descrição teórica do experimento apresente um conhecimento de 2 parágrafos sobre uma interface gráfica de “imaging”

Análise de memória física

A análise de memória física baseia-se em fazer um dump da memória física e virtual de um sistema.

- O que podemos conseguir através da memória física?
 - ❖ Arquivos com senhas em texto puro;
 - ❖ Arquivos com variáveis de ambiente (\$HISTFILE)
 - ❖ O mapas de todos os serviços que se encontram em execução.
- Aplicações de terminal:
 - ❖ **memdump (posix)**

<<http://www.porcupine.org/forensics/memdump-1.0.tar.gz>>

<<http://www.vivaolinux.com.br/dica/A-importancia-de-rastrearcomandos-com-o-HISTFILE>>

Análise de memória física (usando dd...)

Dump da memória e nome do processo de capturar as informações da memória, e pode ser feito através do comando dd, dcfldd entre outros.

```
# dd < /dev/mem > mem.dump
```

```
# dd < /dev/kmem > kmem.dump
```

- possível realizar buscas por palavras-chave através dos comandos grep e strings

```
# strings -a mem.dump | grep palavra-chave
```

```
Ex. # strings -a mem.dump | grep Firefox
```

```
Ex. # strings -a mem.dump | grep TROJAN
```

Análise de memória física (/proc)

- O diretório /proc é um pseudo-sistema de arquivos usado como uma interface para as estruturas de dados do kernel.
- A memória pode ser acessada pelo pseudo-arquivo /proc/kcore, que representa a memória física do sistema no formato de um core file.
- Buscando processos vinculados ao firefox:

```
# strings -a /proc/kcore | grep firefox > kcore_firefox.dump  
# more kcore_firefox.dump
```

```
# strings -a /proc/kcore | grep TROJAN > kcore_TROJAN.dump  
# more kcore_TROJAN.dump
```


Coleta de dados não voláteis

Criando imagem de disco para disco (clone) pela rede

- A estação Forense será o server ou seja, receberá e gravará os dados vindos da estação suspeita. Para isso, você deve levantar o netcat em modo *listening* (ouvindo), desta forma todos os dados que chegarem a porta definida, serão processados por ele. A estação suspeita por sua vez terá seus dados copiados e enviados a estação Forense. Na estação Forense, que receberá os dados da estação suspeita faça:

\$ nc -v -l 12345 > hd1-caso1.dd

- **nc** --> netcat
- **-v** -->> verbose
- **-l** --> parâmetro informando ao nc que ele será o ouvinte (listening)
- **12345** --> porta tcp na qual o netcat estará aguardando os dados
- **hd1-caso1.dd** --> arquivo que será gerado a partir dos dados recebidos pelo netcat na porta 12345

Coleta de dados não voláteis

Criando imagem de disco para disco (clone) pela rede

- Na estação suspeita e que terá seus dados copiados, faça:

```
sudo dcfldd if=/dev/sdb hash=sha256,sha512  
sha256log=/home/fdtk/evidencias/sha256.txt  
sha512log=/home/fdtk/evidencias/sha512.txt hashconv=after  
conv=noerror,sync bs=128k | nc -vn 10.1.1.10 12345 -q 5
```

- **dcfldd** --> disk dump, copia os dados
- **if=/dev/sdb** --> informa qual a origem dos dados
- **hash256,hash512** --> Calcula um hash256sum + um hash 512 on-the-fly
- **sha256log=/home/fdtk/evidencias/sha256.txt** --> Local e arquivo de hash criado on-the-fly de 256-bits
- **sha512log=/home/fdtk/evidencias/sha512.txt** --> Local e arquivo de hash criado on-the-fly de 512-bits
- **hashconv=after** --> gerar o hash apos a cópia

Coleta de dados não voláteis

- **conv=noerror,sync** --> informa ao dcfldd que não pare a copia caso ocorra algum erro.
- **bs=128k** --> informando ao dcfldd que envie blocos de 128k de dados por vez
- **|** --> pipe = informa que a saída dos dados de um comando serão entrada em outro.
- **nc** --> netcat
- **-vn** --> verbose + ip numérico
- **10.1.1.10** --> ip de destino
- **12345** --> porta de destino
- **-q 5** --> desconectar em 5 segundos após a conclusão da operação

Experimento 5 – Atividade 1

- **Criar um disco pequeno (1Mb) no Virtual Box** no qual será antecipadamente
 - Copiado 4 imagens
 - Copie 3 arquivos textos pequenos. Edite-os, mude algo e salve”
 - Copie 1 imagem jpg ou .png e renomeie para .txt
 - Criado um arquivo texto com uma frase com a palavra TROJAN.
 - Deletada 2 das 4 imagens iniciais.

Crie uma imagem desse disco com o “dcfldd” neste momento.

Experimento 5 – Atividade 2

- Reabra o arquivo texto com a palavra “TROJAN” no editor de texto.
- Abra o Firefox em um site qualquer.
- Em outro terminal realize uma "Análise de memória física”.
- Faça também uma "Análise de memória física” do “/proc”

Experimento 5 – Atividade 3

- No uso do “**dcfldd**” vemos o atributo “**hash=**”
- Sabe-se que na criação da imagem forense existe uma tarefa importante de "hashing" sob a imagem gerada.

•

DISCUTA qual a importância do "hashing"? Discuta se a geração de uma chave é suficiente para que possamos “provar em um tribunal que a imagem que usamos para análise não foi adulterada.

Data Carving

- *Data carving* é o processo de extrair uma coleção de dados de um conjunto de dados maior.
- Técnicas de *data carving* ocorrem frequentemente durante uma investigação digital quando o espaço do sistema de arquivos não alocado é analisado para extrair arquivos.
- Os arquivos são "minerados" em áreas não alocados usando valores de cabeçalho e rodapé específicos de tipo de arquivo.
- As estruturas do sistema de arquivos não são usadas durante o processo.

Data Carving: Sistema de Arquivos

- *Sistemas de Arquivos é conjunto de estruturas lógicas e de rotinas, que permitem ao sistema operacional controlar o acesso ao disco rígido*
- *Sistemas de Arquivos padrões Windows: FAT16, FAT32, NTFS*
- *Sistemas de Arquivos padrões Linux/Unix: EXT2, EXT3, EXT4, ReiserFS, XFS, JFS, ...*

Data Carving (ou File Carving) independe de sistema de arquivos

Data Carving: Magic Numbers e File Signatures

- *Funciona como uma assinatura do tipo de arquivo.*
- *São método de identificação de arquivos independente de sistema operacional/sistema de arquivos.*
- *Baseia-se em informações inseridas/coletadas dentro de cada arquivo (cabeçalhos, rodapés, campos específicos)*

DISCUTA Sistemas de arquivos e assinaturas (exemplifique algumas assinaturas – JPEG, ZIP, etc).

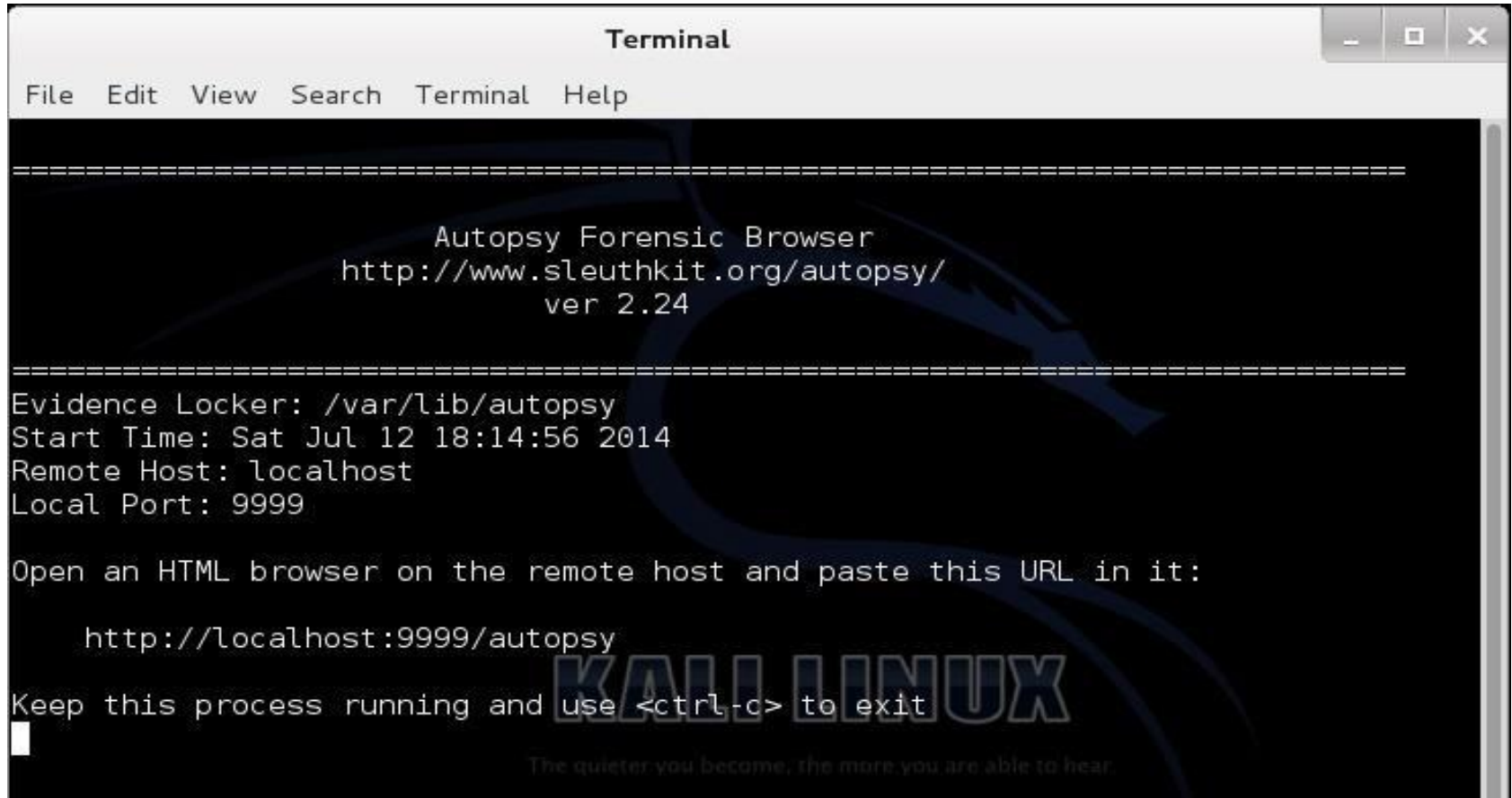
Data Carving: Recuperação

- Executar aplicativo com parametros especificos
magicrescue -d diretorio_destino -r base_tipos imagem
 - _destino: Diretorio onde sera gravado o resultado
 - base_tipos: Base com padrao do tipo de arquivo buscado (/usr/share/magicrescue/recipes)
 - imagem: imagem do dispositivo analisado

Exemplo:

```
magicrescue -d /home/forense/analisar  
-r /usr/share/magicrescue/recipes/avi  
pendrive.dd
```

Autopsy



A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help) and standard window controls. The terminal output shows the Autopsy Forensic Browser version 2.24, the installation path /var/lib/autopsy, the start time (Sat Jul 12 18:14:56 2014), the remote host (localhost), and the local port (9999). It instructs the user to open an HTML browser on the remote host and paste the URL http://localhost:9999/autopsy. It also tells the user to keep the process running and use <ctrl-c> to exit. A "KALI LINUX" watermark is visible in the background.

```
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: Sat Jul 12 18:14:56 2014
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
█
```

- **<http://localhost:9999/autopsy>**

Autopsy (Início do Experimento Autopsy)

- Abra o Firefox em <http://localhost:9999/autopsy>
- Quando for instando a derfinicao de “New case” use sua <matricula. Clique no link “New Case”



Autopsy

- *Preencha e ... Next*

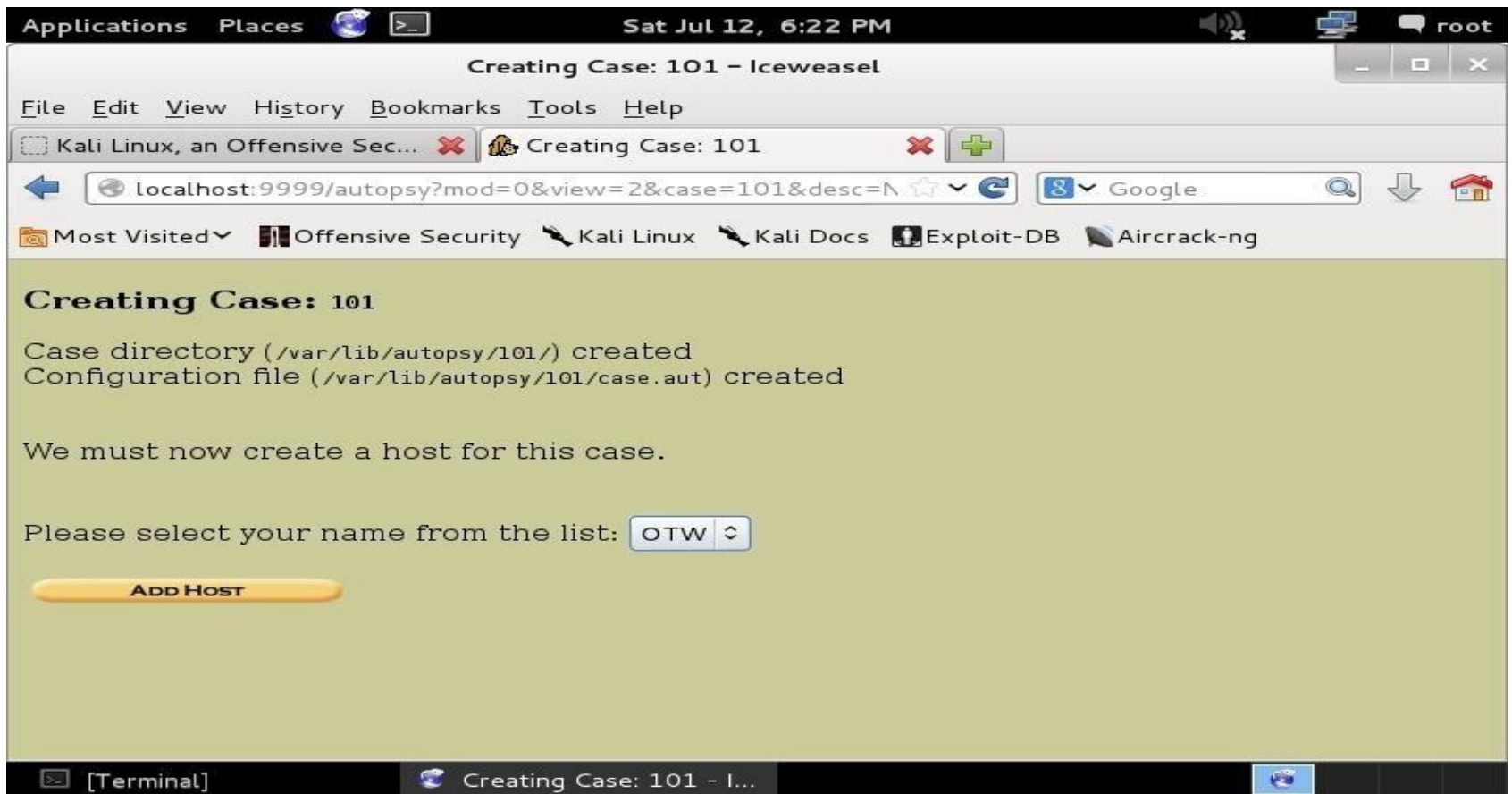
The screenshot shows a web browser window titled "Create A New Case - Iceweasel". The address bar shows a URL with "&view=1&x=111&y=10". The browser's bookmarks bar includes "Kali Linux, an Offensive Security Project", "Offensive Security", "Kali Linux", "Kali Docs", "Exploit-DB", and "Aircrack-ng". The main content area is titled "CREATE A NEW CASE" and contains three sections for form input:

- 1. Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
- 2. Description:** An optional, one line description of this case.
- 3. Investigator Names:** The optional names (with no spaces) of the investigators for this case.
a.
b.
c.
d.
e.
f.

The browser's status bar at the bottom shows "[Terminal]" and "Create A New Case - I...".

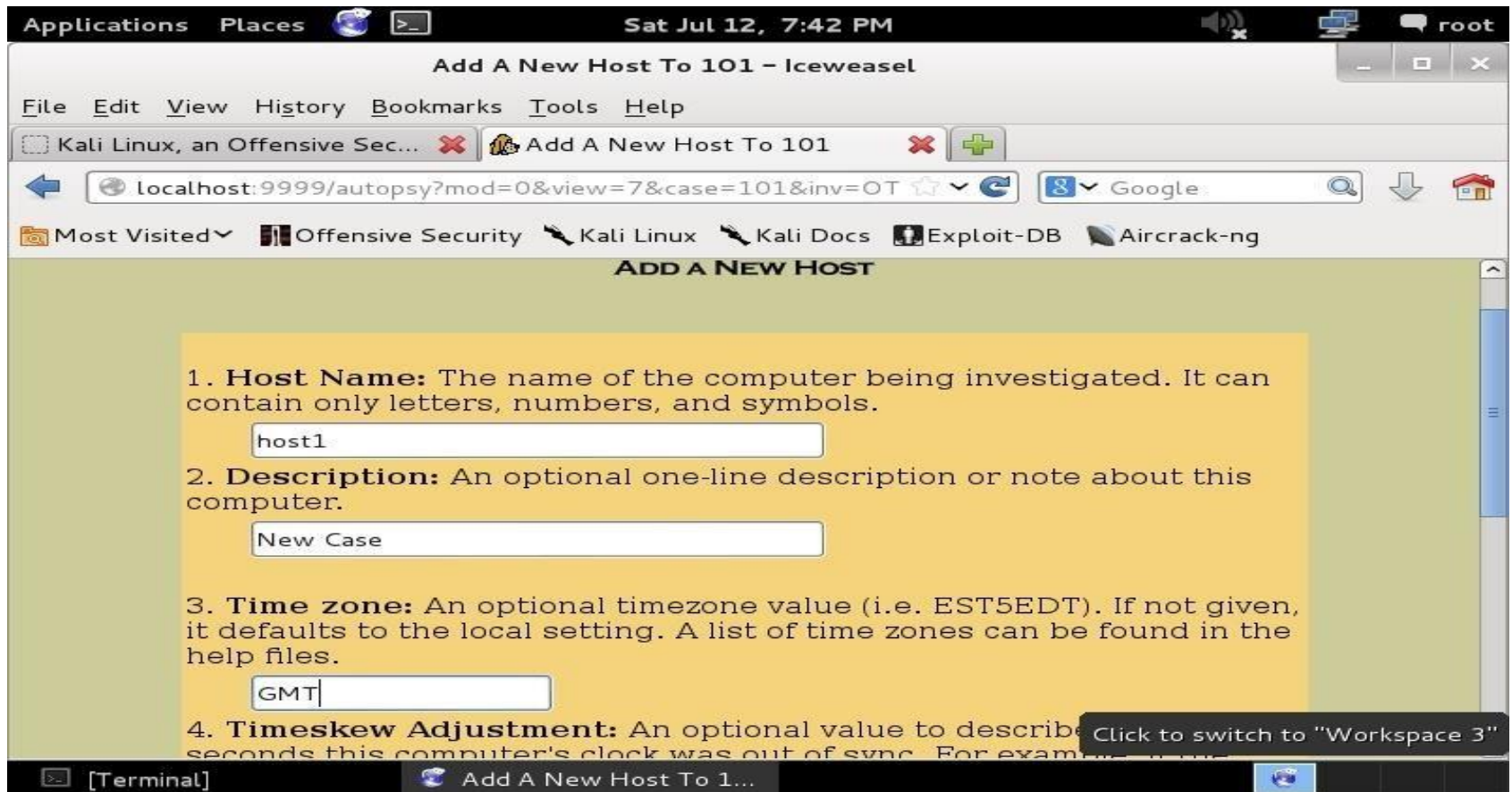
Autopsy

- Anote o diretório (os resultados vão para lá ...)



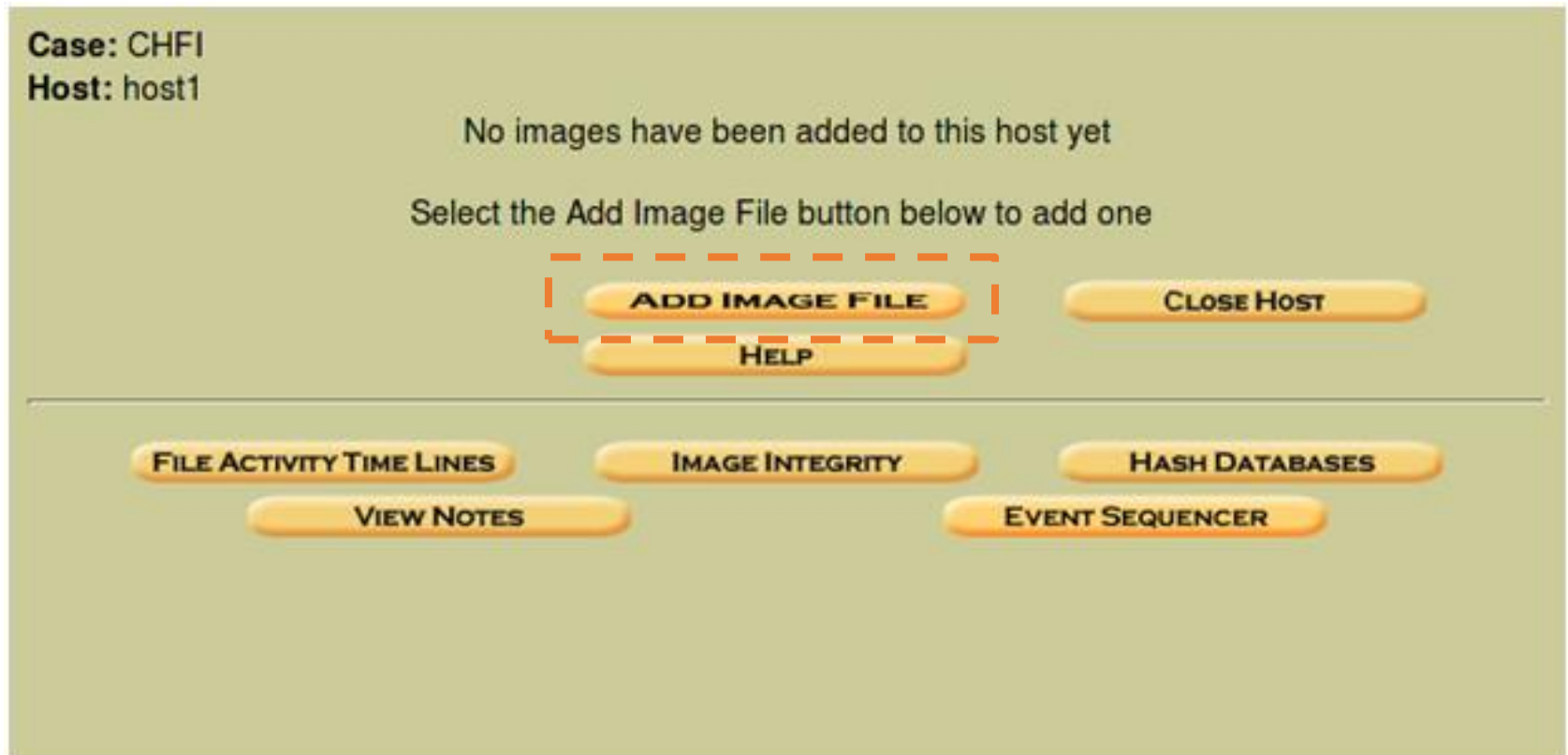
Autopsy

- Adicione o *Host* (sua máquina)



Autopsy

- Adicione a imagem usada no início do experimento.



Autopsy

- Adicione a imagem usada no início do experimento.

Case: CHFI
Host: host1

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter "" for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

☒ Disk ☐ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☒ Symlink ☐ Copy ☐ Move

NEXT

CANCEL **HELP**

Autopsy

- A imagem tem hash ...

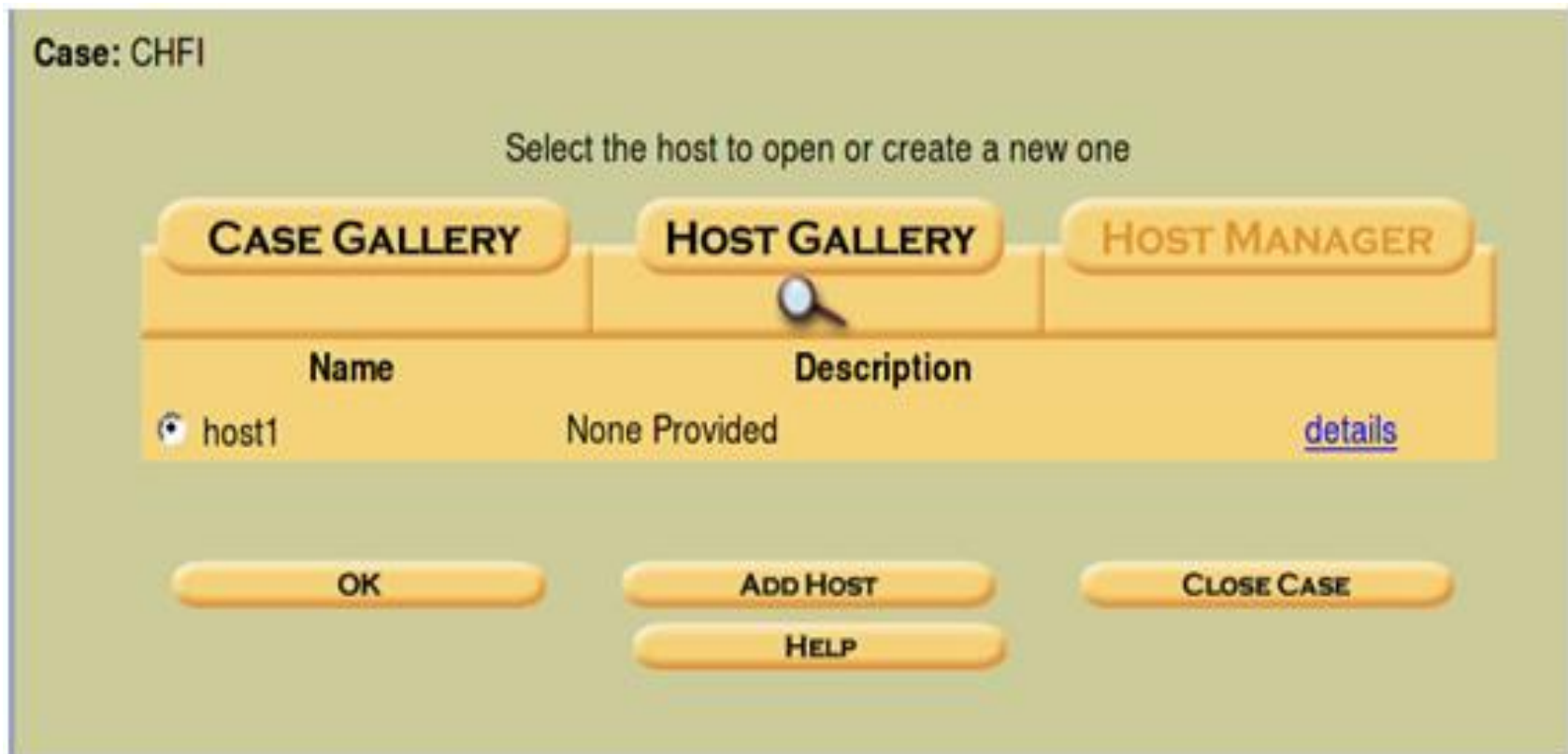
The screenshot shows the 'Image File Details' dialog box in the Autopsy application. The dialog has a yellow background and a title bar. It contains the following elements:

- Image File Details** (Section Header)
- Local Name:** images/nullbyte
- Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
- Three radio buttons for hash handling:
 - ☒ Ignore the hash value for this image.
 - ☐ Calculate the hash value for this image.
 - ☐ Add the following MD5 hash value for this image:
 - A text input field for the MD5 hash value.
- ☐ Verify hash after importing?
- File System Details** (Section Header)
- Analysis of the image file shows the following partitions:
- Three buttons at the bottom: **ADD**, **CANCEL**, and **HELP**.

For your reference, the `nmmls` output was the following:

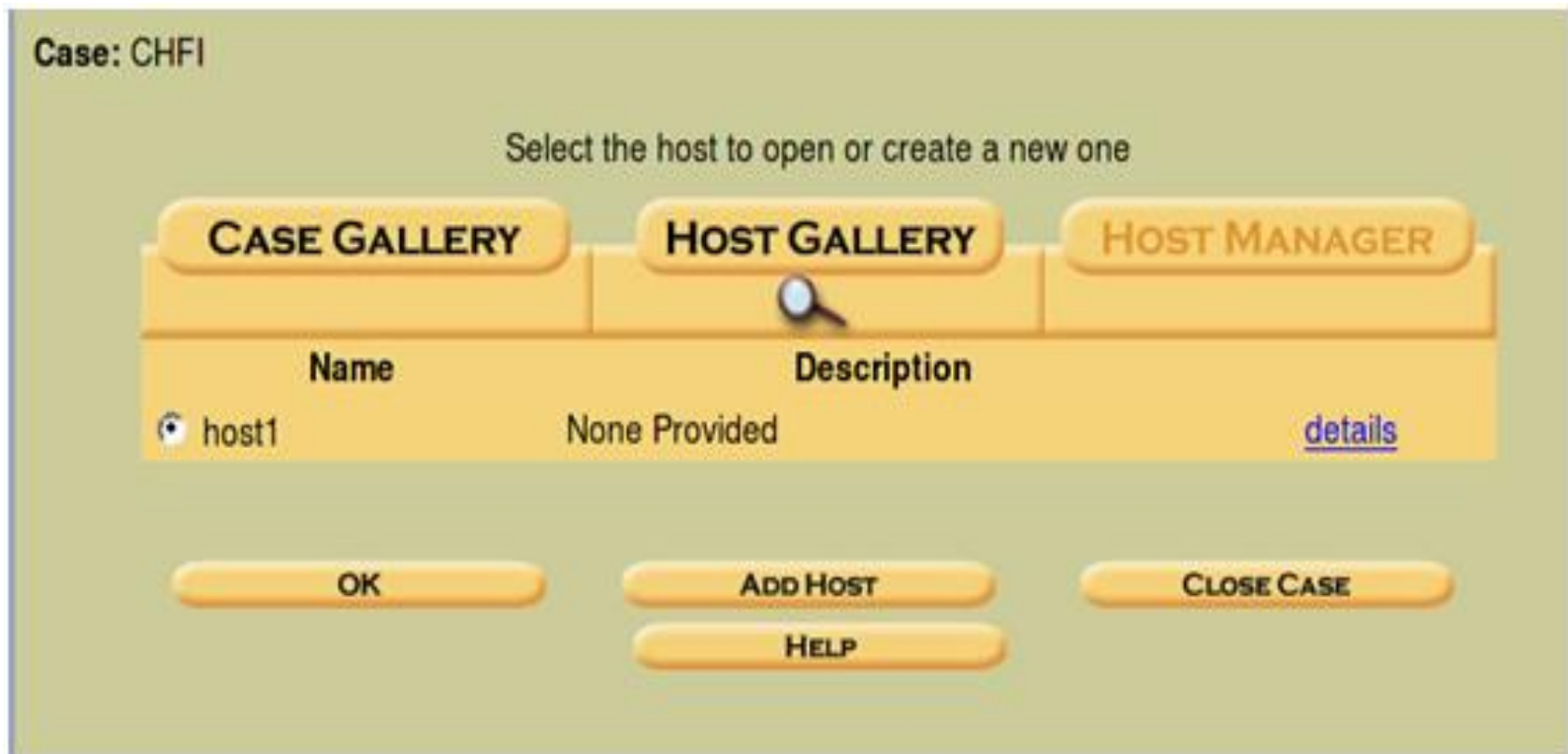
Autopsy

- Selezione para o experimento



Autopsy

- Selezione para o experimento



Experimento 5 – Atividade 4

- **Recupere as informações**
- File Listing: Analise os arquivos e diretórios, incluindo os nomes de arquivos e arquivos excluídos com nomes baseados em Unicode.
- File Content: O conteúdo dos arquivos pode ser visualizado em raw, hexa strings ASCII, e podem ser extraídas. Quando os dados são interpretados no Autopsy, higienize-o para evitar danos ao sistema de análise local. **Ilustre alguns conteúdos.**
- File Type Sorting: Classifique os arquivos com base em suas assinaturas internas para identificar arquivos de um tipo conhecido. O Autopsy também pode extrair apenas imagens gráficas (incluindo miniaturas). **A extensão do arquivo também será comparada ao tipo de arquivo para identificar arquivos que podem ter sua extensão alterada para ocultá-los.**

Experimento 5 – Atividade 4

- **Recupere as informações**

- Timeline of File Activity: Uma linha do tempo de atividade de arquivo pode ajudar a identificar áreas de um sistema de arquivos que podem conter evidências. O Autopsy pode criar linhas do tempo que contêm entradas para os tempos Modificado, Acesso e Alteração (MAC) de arquivos alocados e não alocados.
- Keyword Search: As pesquisas por palavra-chave da imagem do sistema de arquivos podem ser executadas usando strings ASCII e expressões regulares com o grep. **As pesquisas podem ser executadas sobre a imagem completa do sistema de arquivos ou apenas no espaço não alocado (FAÇA)**. Um arquivo de índice pode ser criado para pesquisas mais rápidas. As cadeias de caracteres que são pesquisadas com frequência podem ser facilmente configuradas no Autopsy para pesquisas automatizadas.

Experimento 5 – Atividade 5

- **Recupere as informações**
- Data Unit Analysis: Unidades de dados são aonde o conteúdo do arquivo é armazenado. O autópsia permite visualizar o conteúdo de qualquer unidade de dados em vários formatos, incluindo ASCII, hexdump e strings. O tipo de arquivo também é fornecido pelo Autopsy, que pesquisará as estruturas de metadados para identificar qual alocou a unidade de dados.
- Image Details: Os detalhes do sistema de arquivos podem ser visualizados, incluindo layout no disco e os horários de atividade. Essa opção fornece informações úteis durante a recuperação de dados.
- **PRINCIPALMENTE, recupere e informe dados dos arquivos deletados e informe os dados de integridade da imagem.**

Experimento 5 – Atividade 6

- **Veja o p0f (que será apresentado a seguir) e execute em sua máquina virtual e no servidor de sala de aula.**
- **Recupere dados do sistema operacional.**
- **Em uma situação de tráfego, use o p0f para observar a impressão digital do TCP. Explique.**

p0f

- p0f é uma ferramenta que pode identificar o sistema operacional de um host de destino simplesmente examinando os pacotes capturados, mesmo quando o dispositivo em questão está por trás de um firewall de pacote.
- p0f não gera tráfego de rede adicional, direto ou indireto; sem pesquisas de nome; nenhuma sondagem misteriosa; sem consultas ARIN; ou outro tráfego.
- Nas mãos de usuários avançados, o p0f pode detectar a presença do firewall, o uso do NAT e a existência de balanceadores de carga.

```
p0f -i eth0 -p -o ~/p0f.log
```

p0f

- **Step 1: Em um terminal, digite o seguinte comando para iniciar a escuta p0f e deixar o comando em execução:**

```
$ sudo p0f -A
```

```
[sudo] password for user:
```

p0f - passive os fingerprinting utility, version 2.0.8

(C) M. Zalewski , W. Stearns

p0f: listening (SYN+ACK) on 'eth0', 61 sigs (1 generic, cksum B253FA88),
rule: 'all'.

- **Step 2: Em outra janela, navegue até um site como um exemplo de destino. A saída irá parecer com a seguinte.**
- **Observe que muitos resultados são “UNKNOWN” porque este projeto foi infelizmente abandonado.**
- **No entanto, você pode usar os dados fornecidos como informações reunidas para a impressão digital TCP.**

173.230.156.66:80 - UNKNOWN [S10:64:1:48:M1460,N,N,S:ZA:?:?]

-> 98.126.63.202:3037 (link: ethernet/modem)

206.12.19.7:80 - UNKNOWN [5792:55:1:60:M1460,S,T,N,W7:ZAT:?:?] (up: 4395 hrs)

-> 173.230.156.66:32928 (link: ethernet/modem)

128.31.0.51:80 - UNKNOWN [5792:52:1:60:M1460,S,T,N,W6:ZAT:?:?] (up: 1559 hrs)

-> 173.230.156.66:58958 (link: ethernet/modem)

173.230.156.66:80 - UNKNOWN [14480:64:1:60:M1460,S,T,N,W4:ZAT:?:?] (up: 5906 hrs)

-> 151.63.225.212:34013 (link: ethernet/modem)

...