



Análisis Forense con Kali Linux

≡ Topic	Unidad V: Seguridad TICs - Análisis Forense con Herramientas de Kali Linux
▼ Module	IT - Cibersecurity
👤 Teacher, -s	Chrystian Ruiz Diaz
👤 Student, -s	Tobías Emanuel González Vera
🎓 Career, -s	Ingeniería en Tecnologías de la Información Empresarial
📅 Date	@July 4, 2024
📅 Wochentage	Donnerstag
📅 Deadline	@July 4, 2024
⚡ Status	Sended
📎 Attached files	<u>Unidad_40_Análisis_Forense.pdf</u>

Parte 1: Análisis de Metadatos con ExifTool

Parte 2: Análisis de Volcado de Memoria con Volatility

Parte 3: Captura y Análisis de Tráfico de Red con Wireshark

Parte 4: Análisis de Sistemas de Archivos con Autopsy

Objetivo: Aprender a utilizar herramientas de análisis forense disponibles en Kali Linux para investigar y extraer información relevante de archivos, sistemas y redes.

Parte 1: Análisis de Metadatos con ExifTool

Instalación

```
sudo apt-get install exiftool
```

```
(kali@kali)-[~]  
$ sudo apt-get install exiftool  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Note, selecting 'libimage-exiftool-perl' instead of 'exiftool'  
libimage-exiftool-perl is already the newest version (12.76+dfsg-1).  
libimage-exiftool-perl set to manually installed.  
The following packages were automatically installed and are no longer required:  
  libdaxctl1 libndctl6 libpmem1  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 472 not upgraded.  
  
(kali@kali)-[~]  
$ ss
```

```
(kali@kali)-[~]  
└─$ sudo apt-get install exiftool  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Note, selecting 'libimage-exiftool-perl' instead of 'exiftool'  
libimage-exiftool-perl is already the newest version (12.76+dfsg-1).  
libimage-exiftool-perl set to manually installed.
```

The following packages were automatically installed and are n
libdaxctl1 libndctl6 libpmem1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 472 not upgrad

Análisis de imagen

```
exiftool /ruta/a/tu/imagen.jpeg
```

```
└─$ exiftool beerbongs.jpeg
ExifTool Version Number      : 12.76
File Name                    : beerbongs.jpeg
Directory                    : .
File Size                    : 14 kB
File Modification Date/Time  : 2024:07:04 13:41:26-04:00
File Access Date/Time       : 2024:07:04 13:42:07-04:00
File Inode Change Date/Time  : 2024:07:04 13:41:26-04:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 228
Image Height                  : 221
Encoding Process              : Baseline DCT, Huffman codin
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:4:4 (1 1)
Image Size                   : 228x221
Megapixels                   : 0.050
```

- **¿Qué información puedes inferir sobre la imagen a partir de los metadatos?**

Según los metadatos proporcionados:

- **File Size:** 14 kB
- **File Modification Date/Time:** 2024-07-04 13:41:26
- **File Type:** JPEG
- **Image Width:** 228 pixels
- **Image Height:** 221 pixels
- **Color Components:** 3 (indicando que la imagen es en color)
- **Encoding Process:** Baseline DCT, Huffman coding

A partir de estos datos, podemos inferir que la imagen es de baja resolución (228×221 píxeles) y tiene un tamaño de archivo relativamente pequeño (14 kB). Además, al ser un JPEG con proceso de codificación Baseline DCT y Huffman, es comúnmente utilizado para fotografías digitales y puede contener información comprimida.

- **¿Cómo podrían estos datos ser útiles en una investigación forense?**

Los metadatos de una imagen, como los obtenidos con `exiftool`, pueden ser extremadamente útiles en investigaciones forenses:

- **Fecha y hora de modificación:** Puede proporcionar pistas sobre cuándo se creó o modificó la imagen, lo cual es crucial para establecer una línea de tiempo en una investigación.
- **Tamaño del archivo:** Puede indicar si la imagen ha sido comprimida o alterada desde su creación original.
- **Resolución y formato:** Ayuda a determinar la calidad de la imagen y el tipo de archivo, lo cual puede ser relevante para establecer la autenticidad de la imagen.
- **Otras informaciones técnicas:** Como el tipo de codificación, pueden revelar detalles adicionales sobre cómo se creó o manipuló la imagen digitalmente.

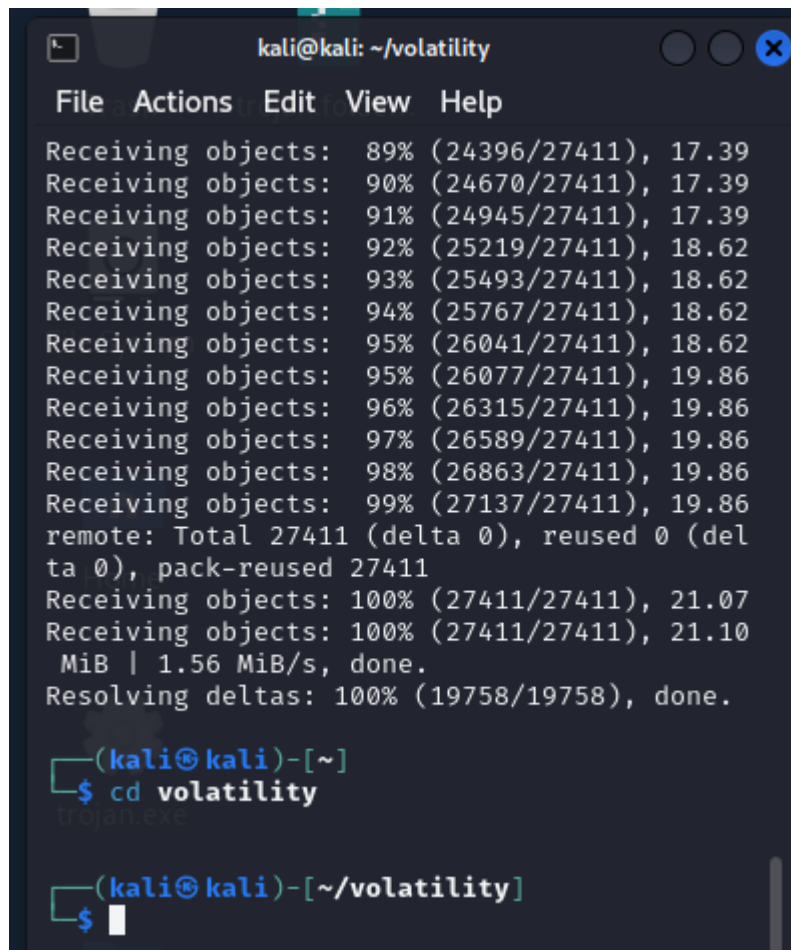
Parte 2: Análisis de Volcado de Memoria con Volatility

Instalación

```
sudo apt-get install volatility
```

Al no funcionar, lo traigo de Github

```
git clone https://github.com/volatilityfoundation/volatility.
```

A screenshot of a terminal window titled 'kali@kali: ~/volatility'. The window shows the output of a git clone command. It displays progress for receiving objects from 89% to 100%, with a final summary of 'remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411'. Below this, it shows the resolution of deltas at 100%. The prompt then changes to '(kali@kali)-[~/volatility]' and a cursor is visible.

```
kali@kali: ~/volatility
File Actions Edit View Help
Receiving objects: 89% (24396/27411), 17.39
Receiving objects: 90% (24670/27411), 17.39
Receiving objects: 91% (24945/27411), 17.39
Receiving objects: 92% (25219/27411), 18.62
Receiving objects: 93% (25493/27411), 18.62
Receiving objects: 94% (25767/27411), 18.62
Receiving objects: 95% (26041/27411), 18.62
Receiving objects: 95% (26077/27411), 19.86
Receiving objects: 96% (26315/27411), 19.86
Receiving objects: 97% (26589/27411), 19.86
Receiving objects: 98% (26863/27411), 19.86
Receiving objects: 99% (27137/27411), 19.86
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Receiving objects: 100% (27411/27411), 21.07
Receiving objects: 100% (27411/27411), 21.10
MiB | 1.56 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
(kali@kali)-[~]
$ cd volatility
(kali@kali)-[~/volatility]
$
```

Instalación de los headers del kernel para LiME

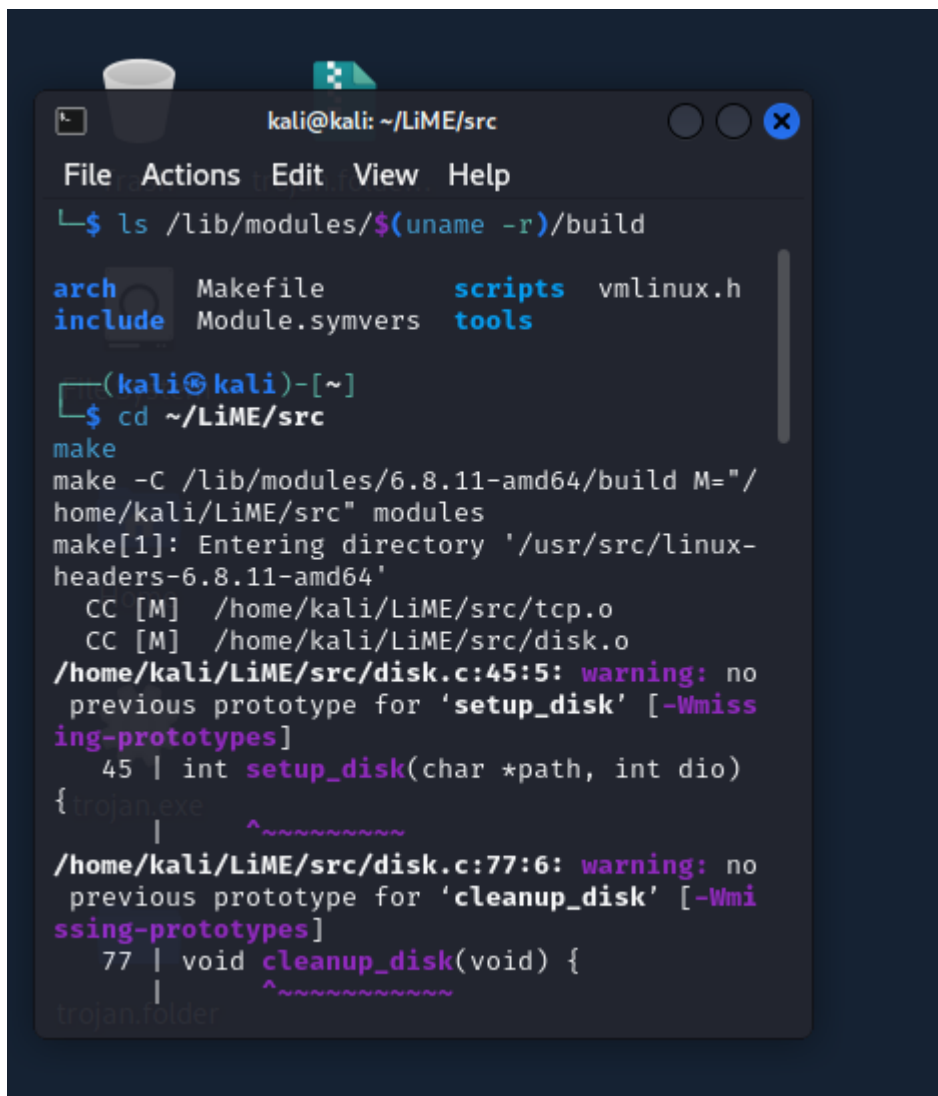
```
sudo apt-get install linux-headers-amd64
```

Instalación de LiME

```
git clone https://github.com/504ensicsLabs/LiME.git
cd LiME/src
make
```

Ejecución

```
cd ~/LiME/src
make
```



```
kali@kali: ~/LiME/src
File Actions Edit View Help
└─$ ls /lib/modules/$(uname -r)/build
arch      Makefile      scripts      vmlinux.h
include   Module.symvers tools
(kali@kali)-[~]
└─$ cd ~/LiME/src
make
make -C /lib/modules/6.8.11-amd64/build M="/home/kali/LiME/src" modules
make[1]: Entering directory '/usr/src/linux-headers-6.8.11-amd64'
  CC [M]  /home/kali/LiME/src/tcp.o
  CC [M]  /home/kali/LiME/src/disk.o
/home/kali/LiME/src/disk.c:45:5: warning: no previous prototype for 'setup_disk' [-Wmissing-prototypes]
   45 | int setup_disk(char *path, int dio)
      | ^~~~~~
/home/kali/LiME/src/disk.c:77:6: warning: no previous prototype for 'cleanup_disk' [-Wmissing-prototypes]
   77 | void cleanup_disk(void) {
      | ^~~~~~
trojan.exe
trojan.folder
```

```
(kali@kali)-[~]
└─$ cd ~/LiME/src
make
make -C /lib/modules/6.8.11-amd64/build M="/home/kali/LiME/src" modules
make[1]: Entering directory '/usr/src/linux-headers-6.8.11-amd64'
  CC [M]  /home/kali/LiME/src/tcp.o
  CC [M]  /home/kali/LiME/src/disk.o
/home/kali/LiME/src/disk.c:45:5: warning: no previous prototype for 'setup_disk' [-Wmissing-prototypes]
```

```

45 | int setup_disk(char *path, int dio) {
    | ^~~~~~
/home/kali/LiME/src/disk.c:77:6: warning: no previous prototy
77 | void cleanup_disk(void) {
    | ^~~~~~
CC [M] /home/kali/LiME/src/main.o
CC [M] /home/kali/LiME/src/hash.o
/home/kali/LiME/src/hash.c:53:5: warning: no previous prototy
53 | int ldigest_init(void) {
    | ^~~~~~
/home/kali/LiME/src/hash.c:97:5: warning: no previous prototy
97 | int ldigest_update(void *v, size_t is) {
    | ^~~~~~
/home/kali/LiME/src/hash.c:142:5: warning: no previous prototy
142 | int ldigest_final(void) {
    | ^~~~~~
/home/kali/LiME/src/hash.c:172:5: warning: no previous prototy
172 | int ldigest_write_tcp(void) {
    | ^~~~~~
/home/kali/LiME/src/hash.c:189:5: warning: no previous prototy
189 | int ldigest_write_disk(void) {
    | ^~~~~~
/home/kali/LiME/src/hash.c:215:6: warning: no previous prototy
215 | void ldigest_clean(void) {
    | ^~~~~~
CC [M] /home/kali/LiME/src/deflate.o
/home/kali/LiME/src/deflate.c:38:12: warning: no previous pro
38 | extern int deflate_begin_stream(void *out, size_t out
    | ^~~~~~
/home/kali/LiME/src/deflate.c:65:5: warning: no previous prot
65 | int deflate_end_stream(void)
    | ^~~~~~
/home/kali/LiME/src/deflate.c:72:9: warning: no previous prot
72 | ssize_t deflate(const void *in, size_t inlen)
    | ^~~~~~
LD [M] /home/kali/LiME/src/lime.o
/home/kali/LiME/src/lime.o: warning: objtool: init_module():
/home/kali/LiME/src/lime.o: warning: objtool: cleanup_module(

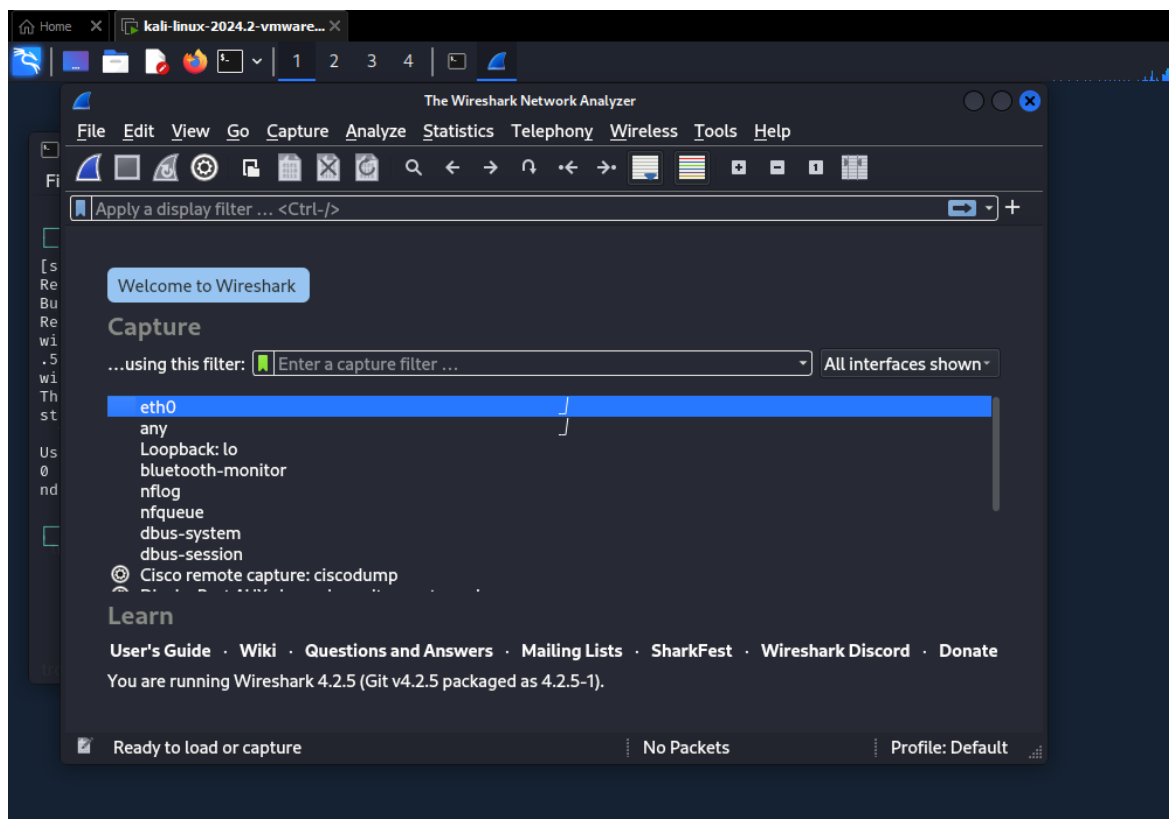
```

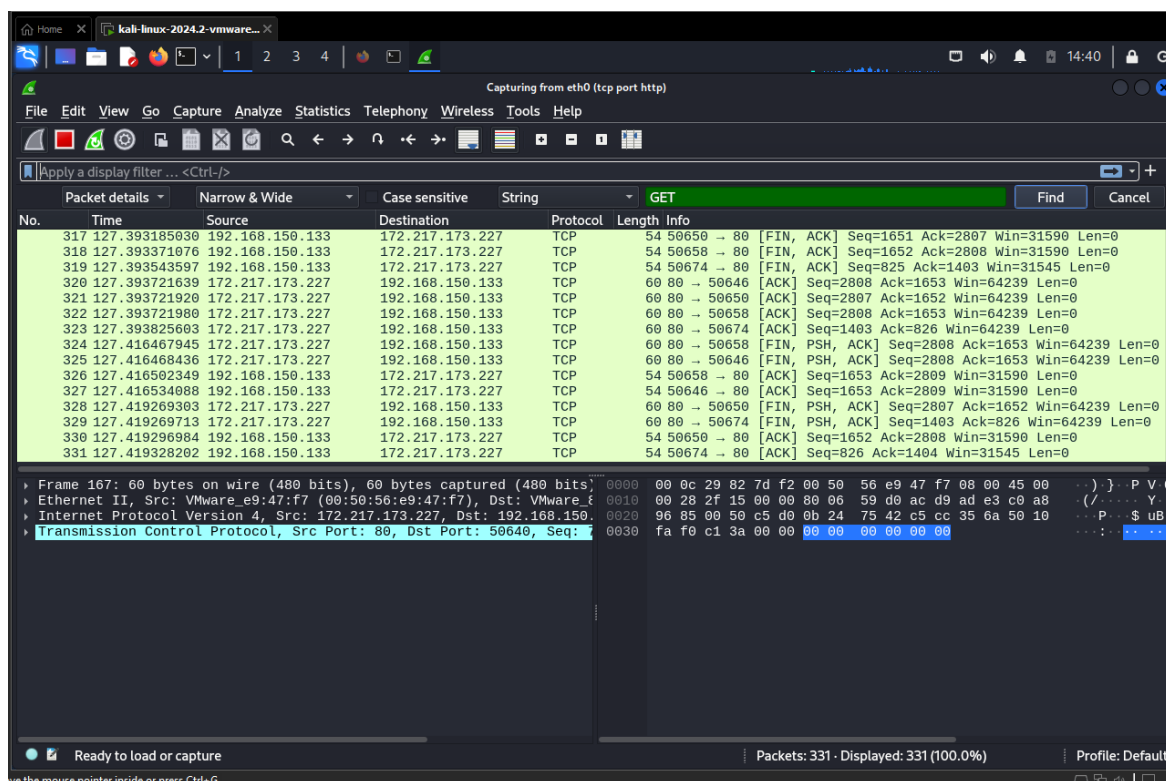
```
MODPOST /home/kali/LiME/src/Module.symvers
CC [M] /home/kali/LiME/src/lime.mod.o
LD [M] /home/kali/LiME/src/lime.ko
BTF [M] /home/kali/LiME/src/lime.ko
Skipping BTF generation for /home/kali/LiME/src/lime.ko due to
make[1]: Leaving directory '/usr/src/linux-headers-6.8.11-amd64'
strip --strip-unneeded lime.ko
mv lime.ko lime-6.8.11-amd64.ko
```

Parte 3: Captura y Análisis de Tráfico de Red con Wireshark

Instalación

```
sudo apt-get install wireshark
```



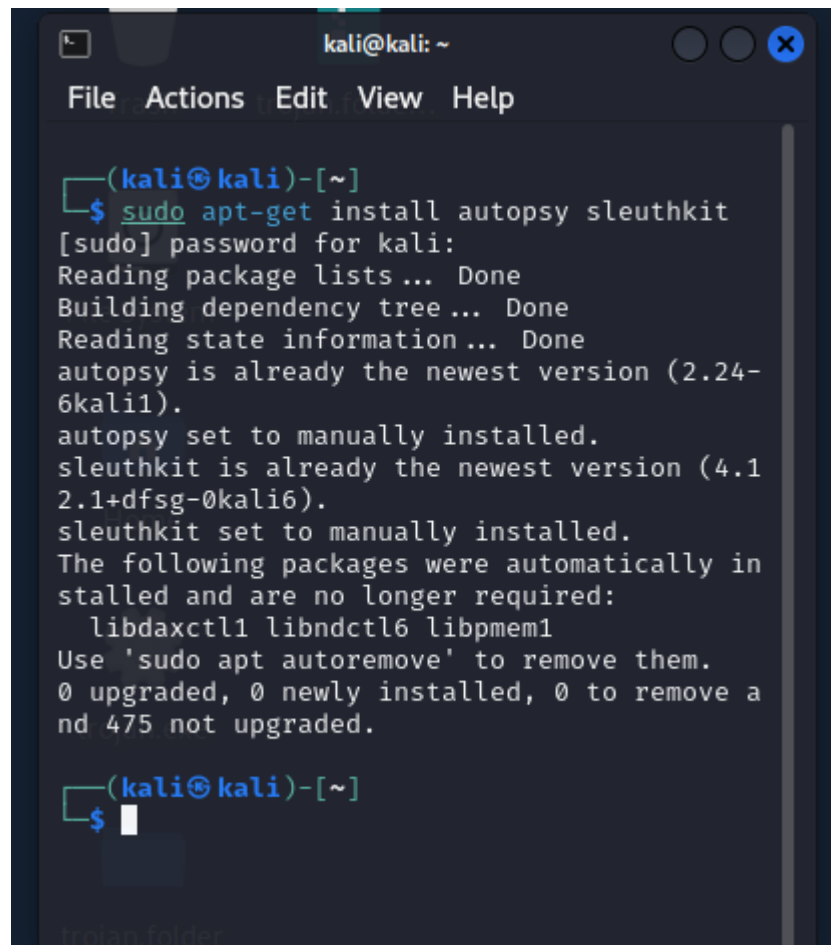


- **¿Qué tipos de datos sensibles puedes identificar en el tráfico capturado?**
 - Credenciales de inicio de sesión sin cifrar.
 - Información personal identificable (PII) como nombres de usuario, direcciones de correo electrónico y números de teléfono.
 - Contenido confidencial como datos financieros o médicos si se transmite sin cifrar.
- **¿Cómo podrías proteger esta información en un entorno real?**
 - Utilizando HTTPS para cifrar la comunicación entre el navegador y el servidor.
 - Implementando políticas que prohíban el acceso a sitios no seguros desde la red corporativa.
 - Complementando con medidas de seguridad en capas como firewalls, IDS/IPS y sistemas de monitoreo de seguridad de red.
 - Manteniendo actualizados los sistemas y software relacionado con la seguridad para mitigar vulnerabilidades conocidas.

Parte 4: Análisis de Sistemas de Archivos con Autopsy

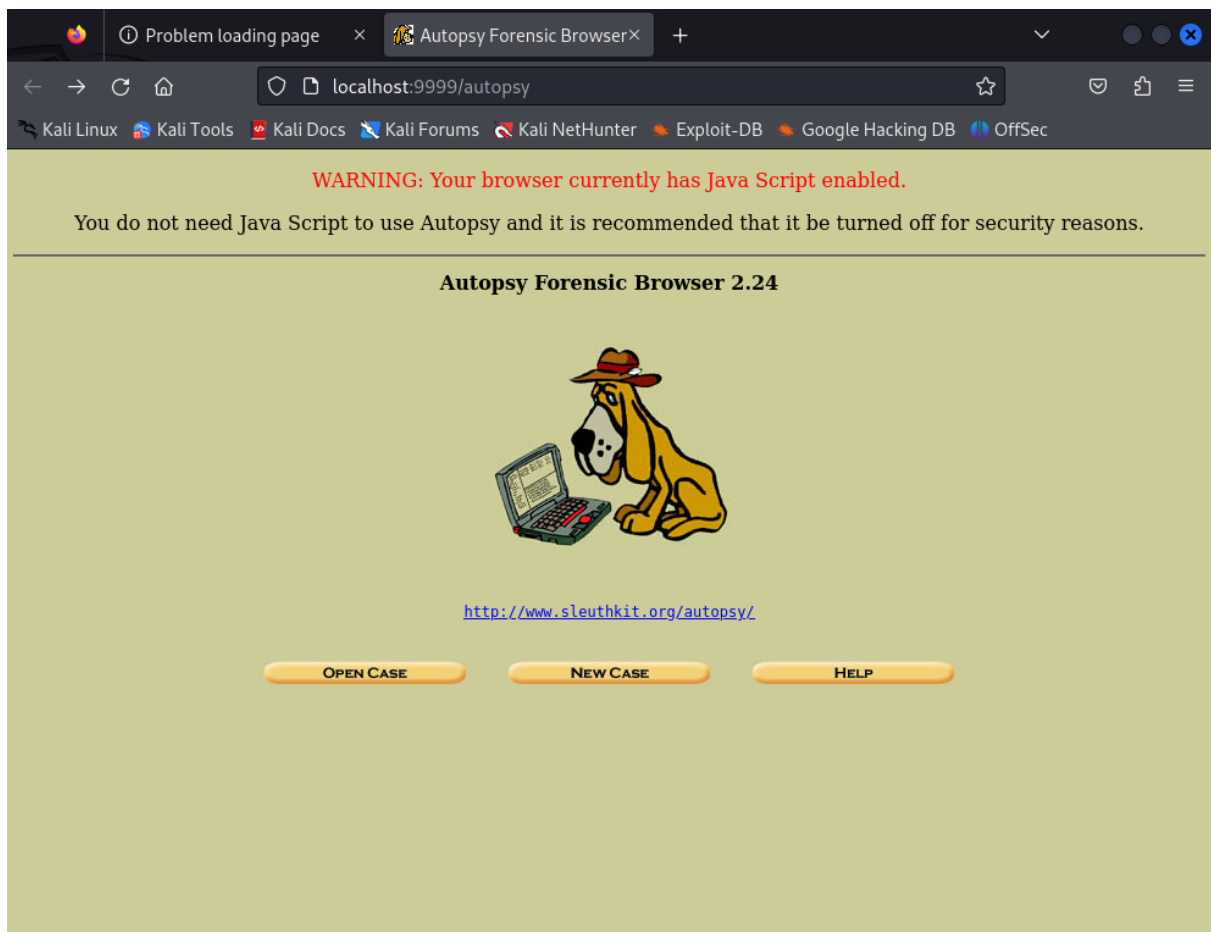
Instalación

```
sudo apt-get install autopsy sleuthkit
```



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo apt-get install autopsy sleuthkit  
[sudo] password for kali:  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
autopsy is already the newest version (2.24-6kali1).  
autopsy set to manually installed.  
sleuthkit is already the newest version (4.12.1+dfsg-0kali6).  
sleuthkit set to manually installed.  
The following packages were automatically installed and are no longer required:  
  libdaxctl1 libndctl6 libpmem1  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 475 not upgraded.  
  
(kali@kali)-[~]  
$
```

Utilizando la interfaz en el navegador



Autopsy se destaca como una herramienta robusta para el análisis forense digital en Kali Linux, facilitando la creación y gestión de casos forenses. A través de su interfaz web, permite añadir diversas fuentes de datos, como imágenes de disco, y realizar un análisis exhaustivo de sistemas de archivos. Sus funcionalidades avanzadas permiten la recuperación de archivos borrados, el análisis de registros de actividad y la generación de líneas de tiempo detalladas, proporcionando a los investigadores una solución completa para la recolección y documentación de evidencia digital.