

The background of the cover features abstract geometric shapes in shades of gold and yellow. In the top-left corner, there are several overlapping chevron and rectangular shapes. In the bottom-right corner, there are more overlapping geometric shapes, including a large chevron and several rectangles, creating a modern, architectural feel.

TAREA 04

REALIZACIÓN DE ANÁLISIS FORENSES EN IOT

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

Caso práctico

María se enfrenta a uno de sus mayores retos, en la escena de un posible delito encuentran una cámara IP que podría haber almacenado información valiosa sobre lo sucedido.

El problema es que María no sabe qué tipo de sistema operativo o sistema de ficheros usa este dispositivo o que tipo de servicios o conexiones realizar por lo que analiza su firmware para tener más detalles de dónde, qué y cómo buscar.

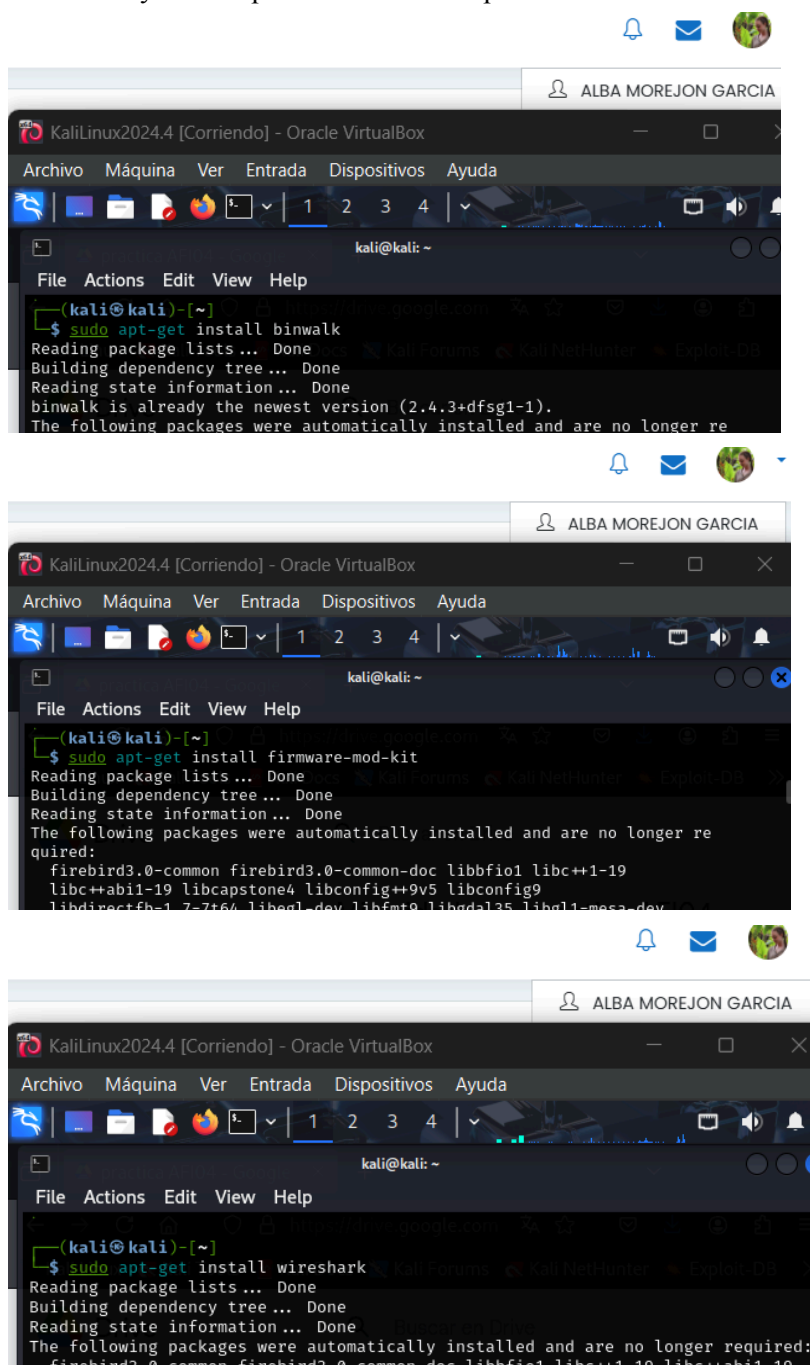
Apartado 1: Análisis de IoT

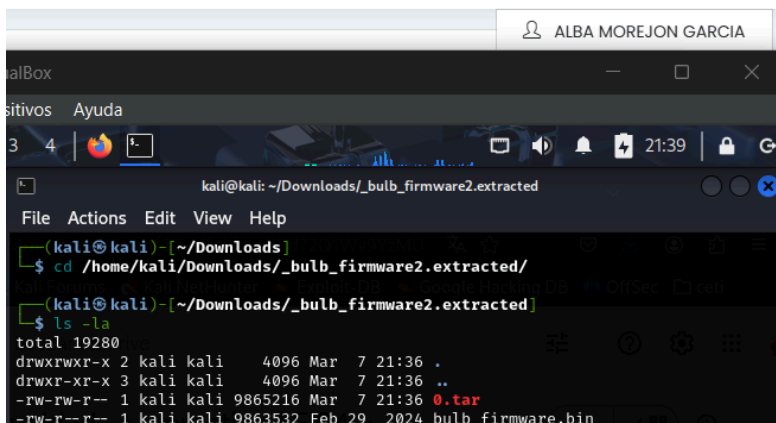
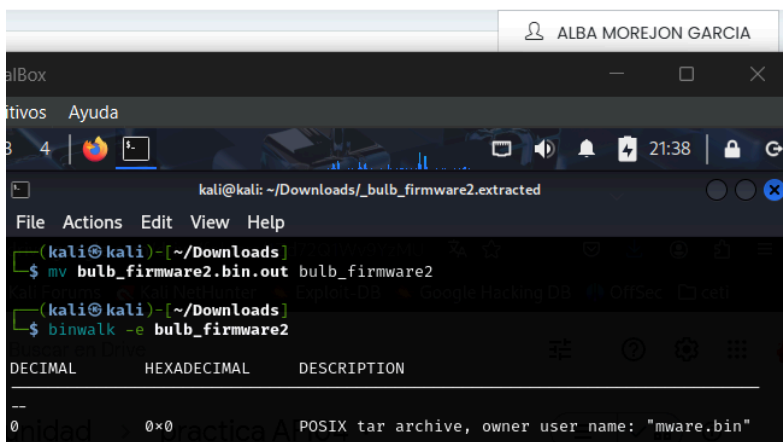
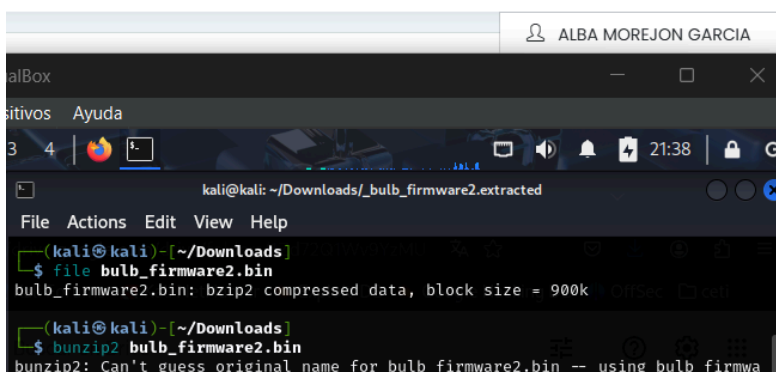
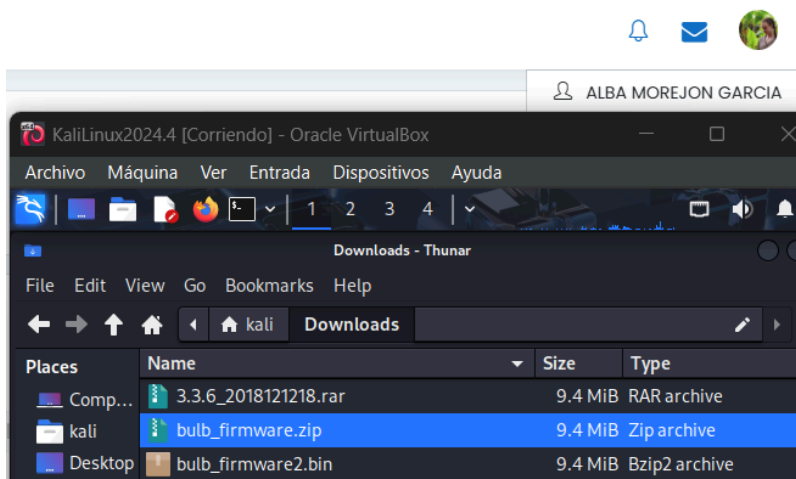
En esta tarea nos enfrentaremos a uno de los principales retos que tenemos cuando tenemos que analizar un dispositivo de IoT que desconocemos su funcionamiento.

PREGUNTA 1: ¿Qué información podemos obtener del firmware de la siguiente de la bombilla (dispositivo IoT)? ¿Por qué sucede esto? ¿Qué supone para el análisis forense esta situación?

[Link firmware](#)

Instalación y descompresión del archivo para ver la información:





ALBA MOREJON GARCIA

Box

Activos Ayuda

4 | [icon] [icon] [icon]

kali@kali: ~/Downloads/_bulb_firmware2.extracted

File Actions Edit View Help

bulb_firmware.bin

```
(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ file bulb_firmware.bin
bulb_firmware.bin: bzip2 compressed data, block size = 900k

(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ bunzip2 bulb_firmware.bin
bunzip2: Can't guess original name for bulb_firmware.bin -- using bulb_firmwar
```

ALBA MOREJON GARCIA

Box

Activos Ayuda

3 4 | [icon] [icon] [icon]

kali@kali: ~/Downloads/_bulb_firmware2.extracted

File Actions Edit View Help

```
(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ ls -la
total 41396
drwxrwxr-x 2 kali kali 4096 Mar 7 21:46 .
drwxr-xr-x 3 kali kali 4096 Mar 7 21:36 ..
-rw-rw-r-- 1 kali kali 9865216 Mar 7 21:36 0.tar
-rw-r--r-- 1 kali kali 16254976 Feb 29 2024 bulb_firmware.bin.out
-rw-r--r-- 1 kali kali 16252932 Dec 12 2018 tf_recovery.img

(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ file tf_recovery.img
tf_recovery.img: u-boot legacy uImage, Linux-3.3.0, Linux/ARM, OS Kernel Image
(Not compressed), 1911456 bytes, Wed Dec 12 10:18:18 2018, Load Address: 0X00
8000, Entry Point: 0X008000, Header CRC: 0X4A67D2CC, Data CRC: 0X9A892BBB
```

ALBA MOREJON GARCIA

Box

Activos Ayuda

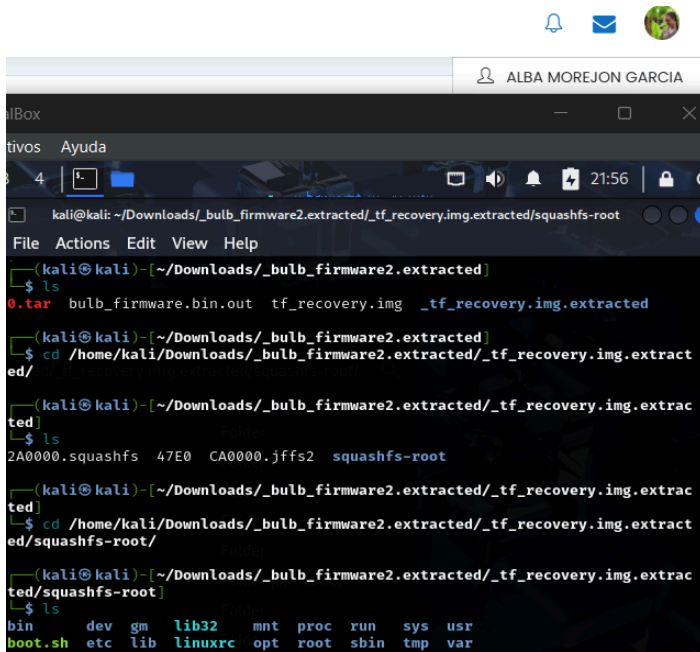
3 4 | [icon] [icon] [icon]

kali@kali: ~/Downloads/_bulb_firmware2.extracted

File Actions Edit View Help

```
(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ sudo apt-get install squashfs-tools
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
squashfs-tools is already the newest version (1:4.6.1-1).
```

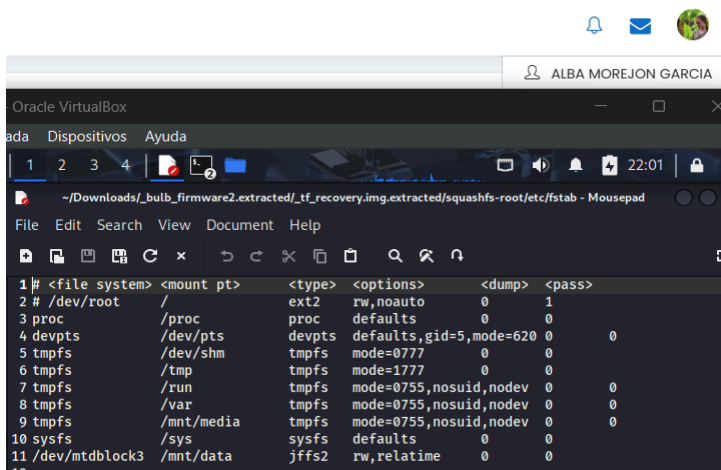
Archivos que tenemos actualmente



```
kali@kali: ~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root
File Actions Edit View Help
(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ ls
0.tar  bulb_firmware.bin.out  tf_recovery.img  _tf_recovery.img.extracted
(kali@kali)~/Downloads/_bulb_firmware2.extracted
$ cd /home/kali/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/
(kali@kali)~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted
$ ls
2A0000.squashfs  47E0  CA0000.jffs2  squashfs-root
(kali@kali)~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted
$ cd /home/kali/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/
(kali@kali)~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root
$ ls
bin      dev  gm  lib32  mnt  proc  run  sys  usr
boot.sh  etc  lib  linuxrc  opt  root  sbin  tmp  var
```

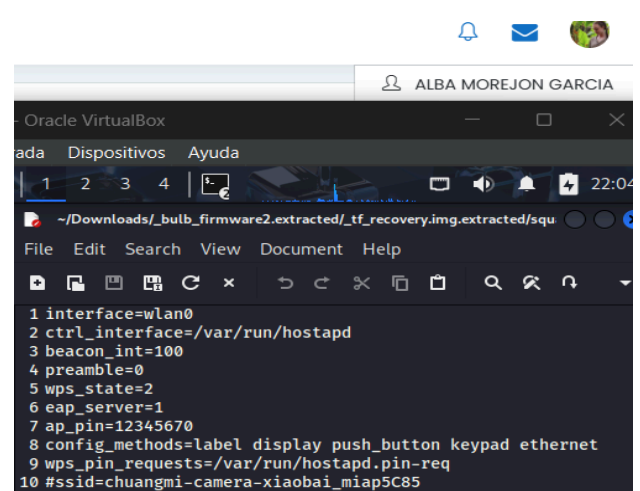
Vemos algunos archivos

fstab:



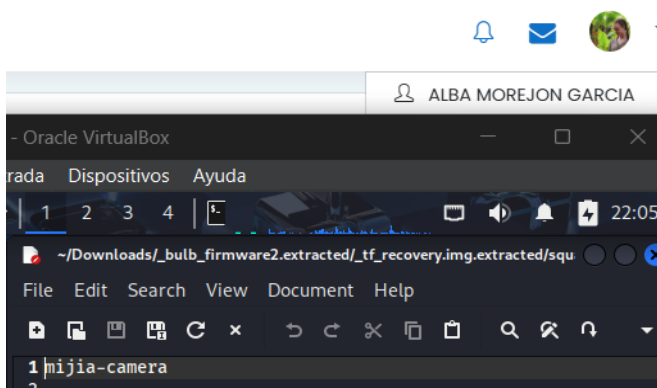
```
1# <file system> <mount pt> <type> <options> <dump> <pass>
2# /dev/root / ext2 rw,noauto 0 1
3 proc /proc proc defaults 0 0
4 devpts /dev/pts devpts defaults,gid=5,mode=620 0
5 tmpfs /dev/shm tmpfs mode=0777 0 0
6 tmpfs /tmp tmpfs mode=1777 0 0
7 tmpfs /run tmpfs mode=0755,nosuid,nodev 0 0
8 tmpfs /var tmpfs mode=0755,nosuid,nodev 0 0
9 tmpfs /mnt/media tmpfs mode=0755,nosuid,nodev 0 0
10 sysfs /sys sysfs defaults 0 0
11 /dev/mtdblock3 /mnt/data jffs2 rw,relatime 0 0
12
```

hostapd.conf:



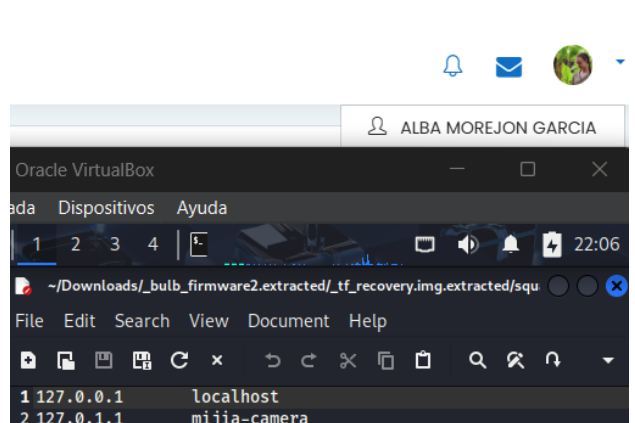
```
1 interface=wlan0
2 ctrl_interface=/var/run/hostapd
3 beacon_int=100
4 preamble=0
5 wps_state=2
6 eap_server=1
7 ap_pin=12345670
8 config_methods=label display push_button keypad ethernet
9 wps_pin_requests=/var/run/hostapd.pin-req
10 #ssid=chuangmi-camera-xiaobai_miap5C85
```

hostname:



```
1 mija-camera
2
```

hosts:



```
1 127.0.0.1 localhost
2 127.0.1.1 mija-camera
```

inittab:

```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc/inittab - Mousepad
File Edit Search View Document Help
16 # Startup the system
17 ::sysinit:/bin/mount -t proc proc /proc
18 ::sysinit:/bin/mount -o remount,rw /
19 ::sysinit:/bin/mkdir -p /dev/pts
20 ::sysinit:/bin/mkdir -p /dev/shm
21 ::sysinit:/bin/mount -a
22 ::sysinit:/bin/mkdir -p /var/run
23 ::sysinit:/bin/mkdir -p /var/lock
24 ::sysinit:/bin/mkdir -p /var/log
25 ::sysinit:/bin/mkdir -p /var/cache
26 ::sysinit:/bin/mkdir -p /var/lib/dbus
27 ::sysinit:/bin/hostname -F /etc/hostname
28 # now run any rc scripts
29 ::sysinit:/etc/init.d/rcS
30
31 # Put a getty on the serial port
32 ttyS0::respawn:/sbin/getty -L ttyS0 115200 vt100 # GENERIC_SERIAL
33 ttyS0::respawn:/bin/sh < /dev/ttyS0 2>&1 > /dev/ttyS0
34
35 # Stuff to do for the 3-finger salute
36 ::ctrlaltdel:/sbin/reboot
```

wpa_supplicant.conf:

```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc/wpa_supplicant.conf - Mousepad
File Edit Search View Document Help
1 ctrl_interface=var/run/wpa_supplicant
2 update_config=1
3
4 # Wi-Fi Protected Setup (WPS) parameters
5
6 # Device Name
7 # User-friendly description of device; up to 32 octets encoded in UTF-8
8 device_name=RTL8192CU
9
10 # Manufacturer
11 # The manufacturer of the device (up to 64 ASCII characters)
12 manufacturer=Realtek
13
14 # Model Name
15 # Model of the device (up to 32 ASCII characters)
16 model_name=RTW_STA
```

Carpeta network:

```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Entrada Dispositivos Ayuda
~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc - Mousepad
File Actions Edit View Help
(kali@kali)~/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc
$ ls -la network
total 16
drwxrwxr-x 3 kali kali 4096 Dec 4 2018 .
drwxrwxr-x 12 kali kali 4096 Mar 7 21:47 ..
drwxrwxr-x 2 kali kali 4096 Dec 4 2018 if-pre-up.d
-rw-rw-r-- 1 kali kali 77 Dec 4 2018 interfaces
```

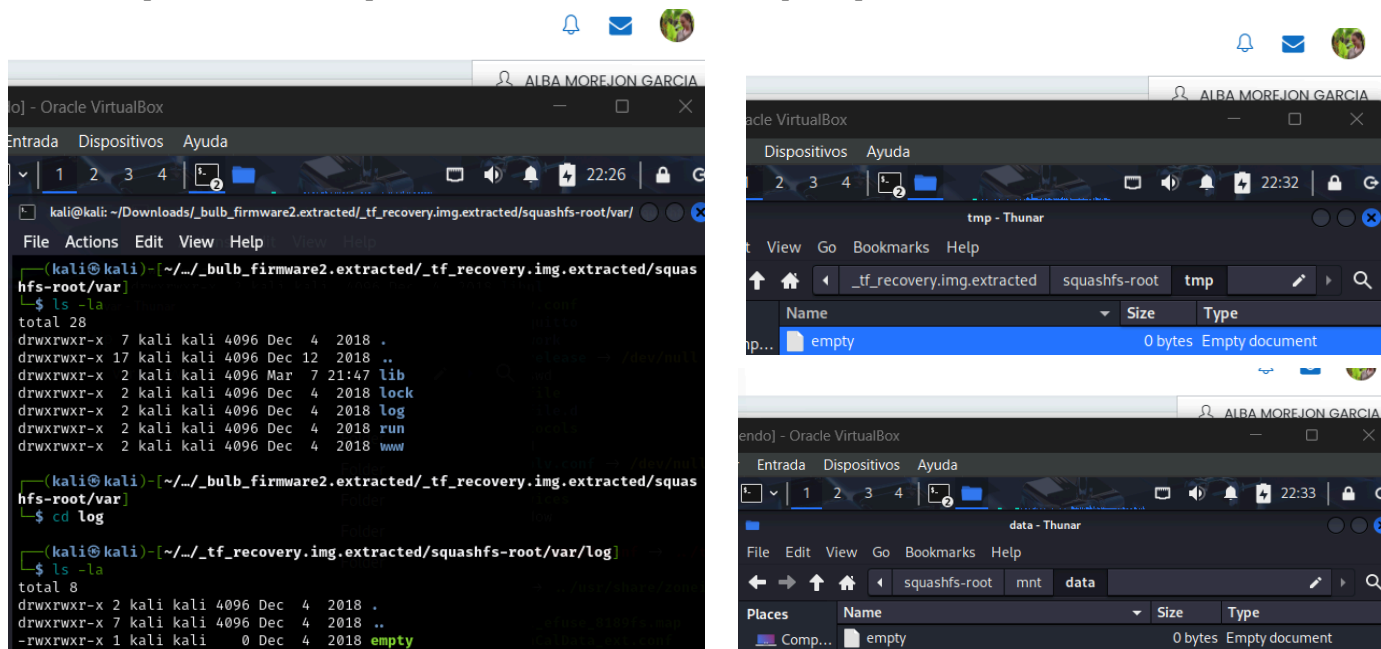
Carpeta init.d:

```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Entrada Dispositivos Ayuda
~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc - Mousepad
File Actions Edit View Help
(kali@kali)~/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc
$ ls -la init.d
total 12
drwxrwxr-x 2 kali kali 4096 Dec 4 2018 .
drwxrwxr-x 12 kali kali 4096 Mar 7 21:47 ..
-rwxrwxr-x 1 kali kali 4096 Dec 4 2018 rcS
```

```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc/network/if-pre-up.d/wait_iface - Mousepad
File Edit Search View Document Help
1 #!/bin/sh
2
3 # In case we have a slow-to-appear interface (e.g. eth-over-USB),
4 # and we need to configure it, wait until it appears, but not too
5 # long either. IF_WAIT_DELAY is in seconds.
6
7 if [ "${IF_WAIT_DELAY}" -a 1 -e "/sys/class/net/${IFACE}" ]; then
8     printf "Waiting for interface %s to appear" "${IFACE}"
9     while [ "${IF_WAIT_DELAY}" -gt 0 ]; do
10         if [ -e "/sys/class/net/${IFACE}" ]; then
11             printf "\n"
12             exit 0
13         fi
14         sleep 1
15         printf "."
16     done
17     printf " timeout\n"
18     exit 1
19 fi
```

```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
~/Downloads/_bulb_firmware2.extracted/_tf_recovery.img.extracted/squashfs-root/etc/init.d/rcS - Mousepad
File Edit Search View Document Help
1 #!/bin/sh
2
3 ft_mode="cat /proc/ft_mode"
4
5 ft_cfg_file=ft_config.ini
6 sd_mountdir=/tmp/sd
7 ft_running_dir=/tmp/ft
8 ft_securekey_file=/mnt/data/ft/prikey.pem
9 ft_decrypt=/mnt/data/ft/rsa_decrypt
10
11 mmc_device=""
12 if [ -b /dev/mmcblkp1 ]; then
13     mmc_device=/dev/mmcblkp1
14 elif [ -b /dev/mmcblk0 ]; then
15     mmc_device=/dev/mmcblk0
16 fi
17
18 if [ "$mmc_device" != "" ]; then
19     if [ "$sd_mountdir" != "" ]; then
20         mount -t vfat $mmc_device $sd_mountdir
21         if [ $? -eq 0 ]; then
22             if [ "$ft_mode" != "1" ]; then
23                 if [ -f $sd_mountdir/$ft_cfg_file ]; then
24                     config_mode=$(cat $sd_mountdir/$ft_cfg_file | sed -n 's/^config_mode=//;s/^$/ /;p')
25                     if [ "$config_mode" = "SA" ]; then
26                         ft_mode="3"
27                     elif [ "$config_mode" = "SA" ]; then
28                         ft_mode="1"
29                     elif [ "$config_mode" = "NTBF" ]; then
30                         ft_mode="4"
31                     else
32                         ft_mode="2"
33                     fi
34                     echo $config_mode > /tmp/ft_sub_mode
35                 fi
36             fi
37         fi
38     fi
```


En otras carpetas como var, tmp o data, no encontramos archivos que se puedan analizar:



Información que podemos obtener del firmware de la bombilla IoT

Configuración de red y seguridad, en los archivos: hostapd.conf, wpa_supplicant.conf, vemos información acerca de las configuraciones de red inalámbrica, SSID, contraseñas y métodos de configuración de seguridad.

Nombre del dispositivo, en el archivo hostname conseguimos el nombre del host (mijia-camera).

Mapeo de direcciones de IP, en el archivo hosts, hay información de mapeo de direcciones IP a nombres de host, útil para entender cómo se comunica el dispositivo en la red.

Configuración de inicialización del sistema, en archivos como: inittab, rcS, tenemos información de comandos y scripts que se ejecutan al inicio, configuraciones de montaje de sistemas de archivos y servicios que se inician automáticamente.

Montaje de sistemas de archivo, en el archivo fstab, hemos visto información acerca de los puntos de montaje y configuración de particiones, incluyendo sistemas de archivos temporales y persistentes.

¿Por qué sucede esto?

El firmware de un dispositivo IoT contiene la configuración y scripts necesarios para que el dispositivo funcione correctamente. Esto incluye configuraciones de red, seguridad, inicialización del sistema...

Analizando el firmware, podemos obtener una visión completa de cómo está configurado y cómo funciona el dispositivo.

¿Qué supone para el análisis forense esta situación?

Identificación de vulnerabilidades, analizar el firmware permite identificar posibles vulnerabilidades en las configuraciones de red y de seguridad que podrían ser explotadas por atacantes.

Recolección de evidencias, la información obtenida del firmware puede ser crucial para entender el comportamiento del dispositivo y recolectar evidencia en investigaciones forenses.

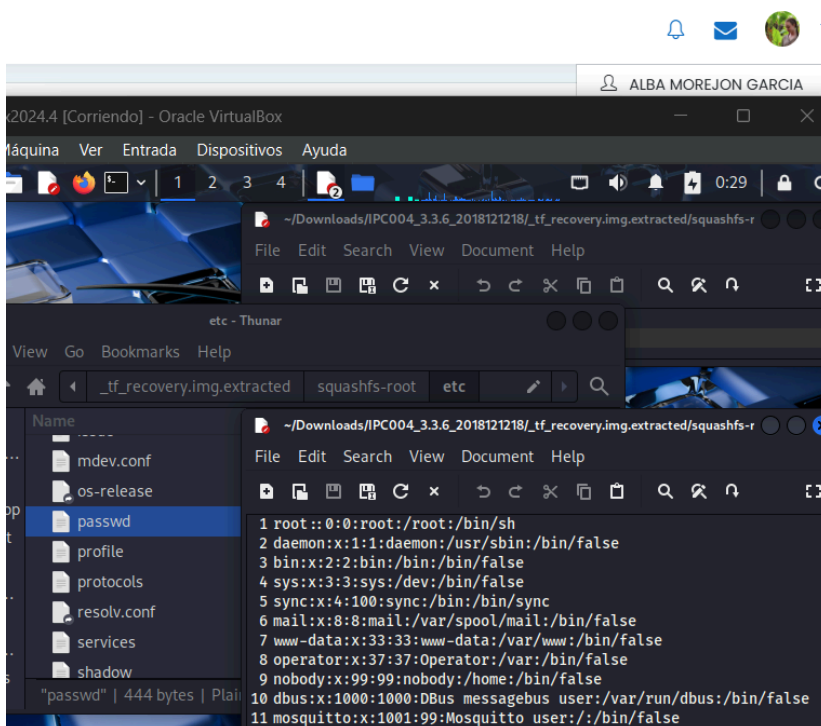
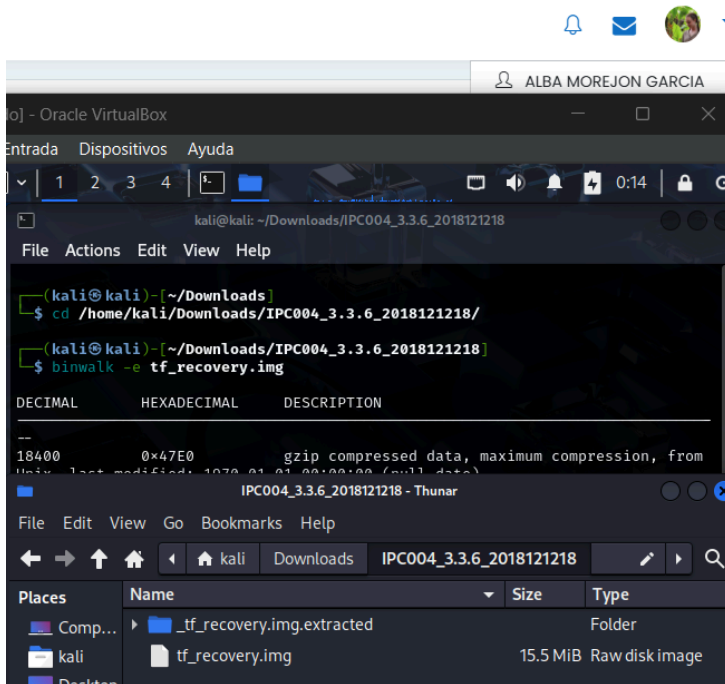
Compresión del funcionamiento del dispositivo, permite una comprensión detallada de cómo el dispositivo se comunica en la red, qué servicios se ejecutan y cómo se manejan las actualizaciones y configuraciones.

Mitigación de riesgos, identificar y corregir configuraciones inseguras puede ayudar a mitigar riesgos y proteger el dispositivo contra ataques futuros.

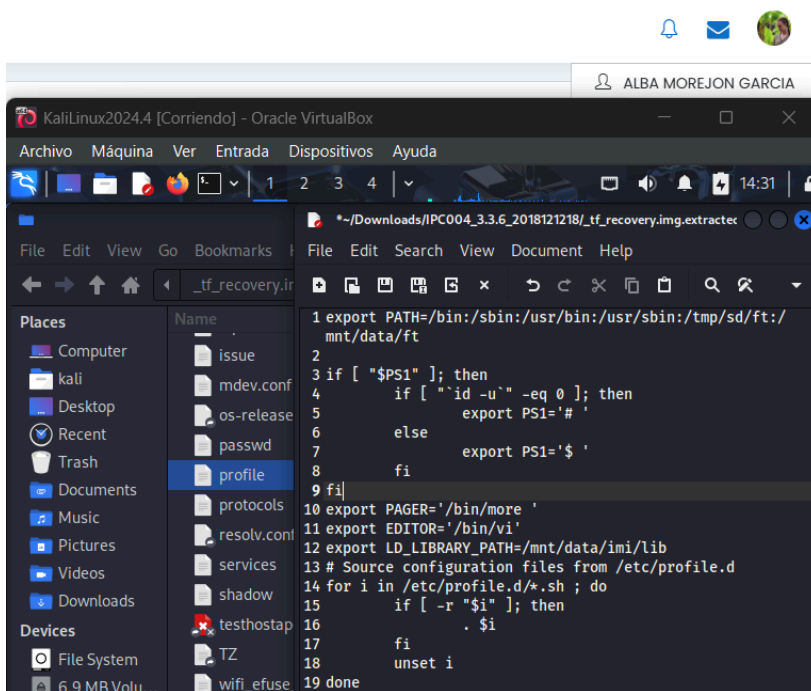
PREGUNTA 2: ¿Qué información podemos obtener del firmware de la cámara XIAOMI IMI Home Security Camera 1080P ? ¿Qué sistema operativo usa? [Link al archivo](#)

Descomprimos el archivo, vamos a analizar los archivos situados en esta ruta:

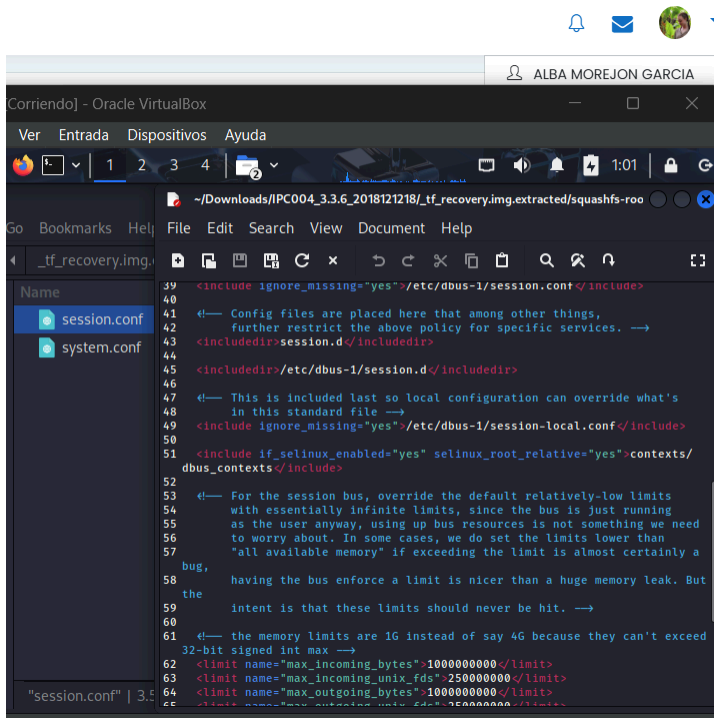
/home/kali/Downloads/IPC004_3.3.6_2018121218/_tf_recovery.img.extracted/squashfs-root/



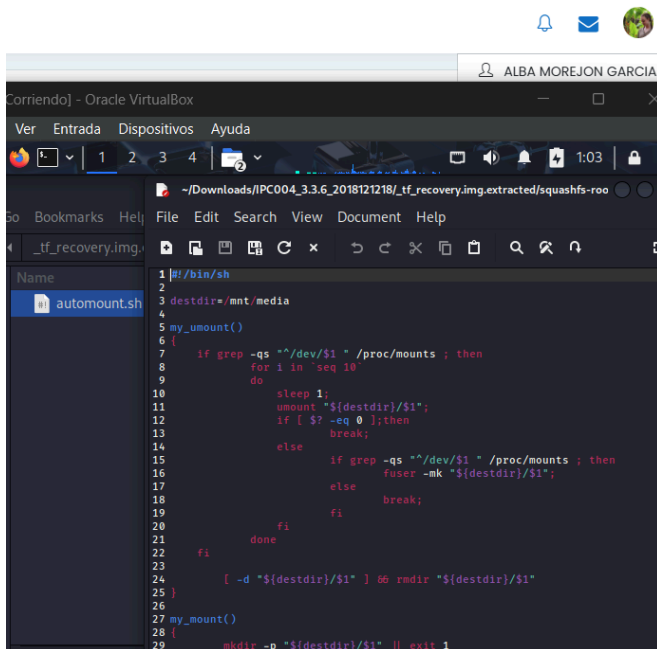
El archivo /etc/passwd, nos muestra los usuarios actuales del dispositivo y la presencia de usuarios como root, daemon, bin y sys, sugiere que el sistema operativo es una variante de Linux.



El archivo profile, es un archivo que establece variables de entorno y contiene rutas como /bin /sbin, /usr/bin... que son típicas de sistemas Linux (además, utiliza vi como editor).



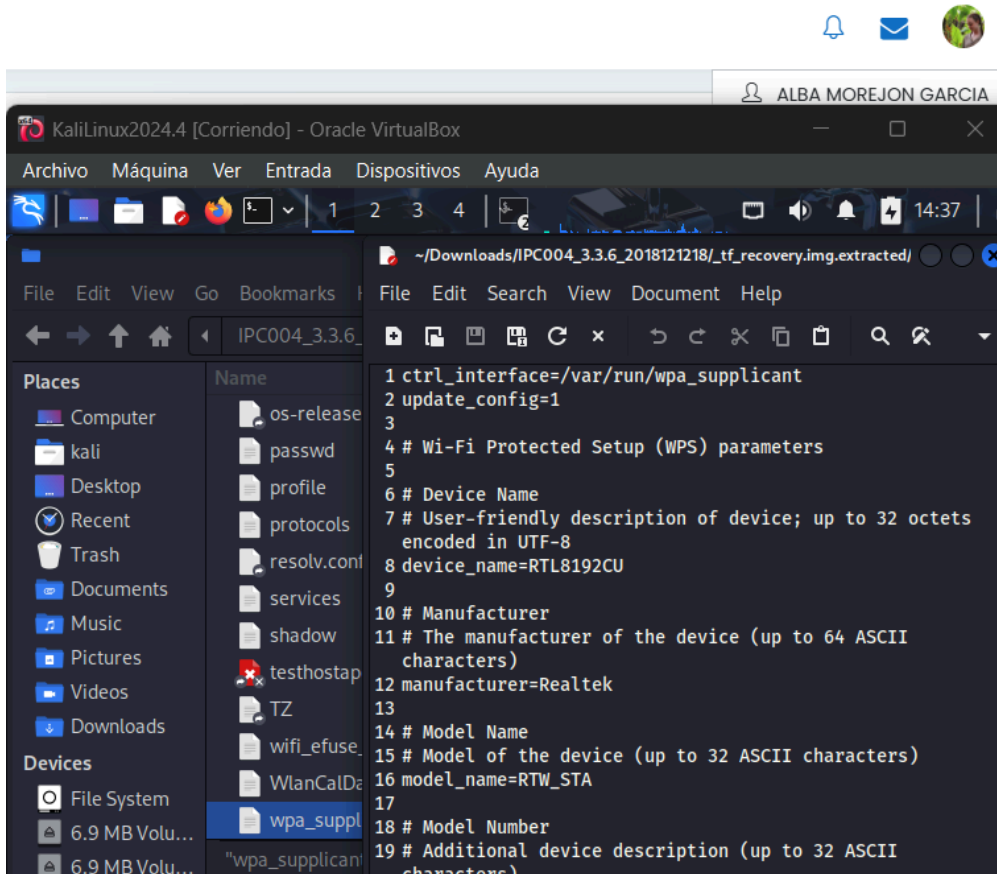
El archivo session.conf, configura D.Bus que es utilizado en sistemas Linux para la comunicación entre procesos.



The screenshot shows a terminal window titled "Corriendo] - Oracle VirtualBox" with the user "ALBA MOREJON GARCIA". The terminal displays the content of a script named "automount.sh". The script is a shell script that defines a function "my_mount()" and a loop that iterates over a list of devices. The script is as follows:

```
1#!/bin/sh
2
3destdir=/mnt/media
4
5my_mount()
6{
7    if grep -qs "^/dev/$1 " /proc/mounts ; then
8        for i in `seq 10`
9        do
10            sleep 1;
11            mount "${destdir}/${1}";
12            if [ $? -eq 0 ];then
13                break;
14            else
15                if grep -qs "^/dev/$1 " /proc/mounts ; then
16                    fuser -mk "${destdir}/${1}";
17                    break;
18                fi
19            fi
20        done
21    fi
22}
23
24[ -d "${destdir}/${1}" ] && rmdir "${destdir}/${1}"
25}
26
27my_mount()
28{
29    mkdir -p "${destdir}/${1}" || exit 1
```

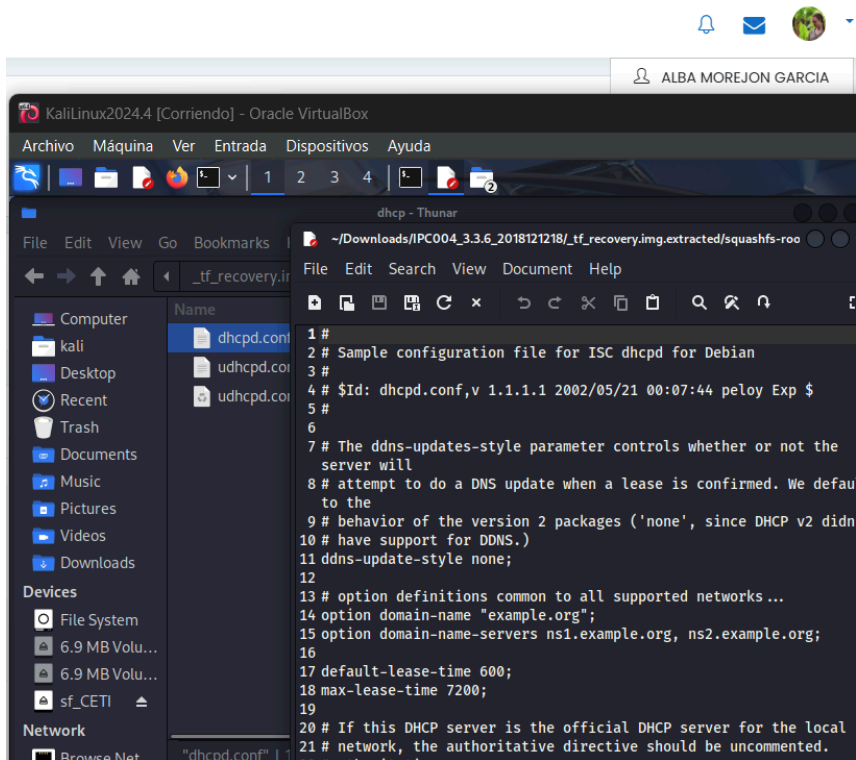
El script llamado automount.sh es un script de shell que comienza con #!/bin/sh, es común en sistemas Unix/Linux, maneja el montaje y desmontaje de dispositivos.



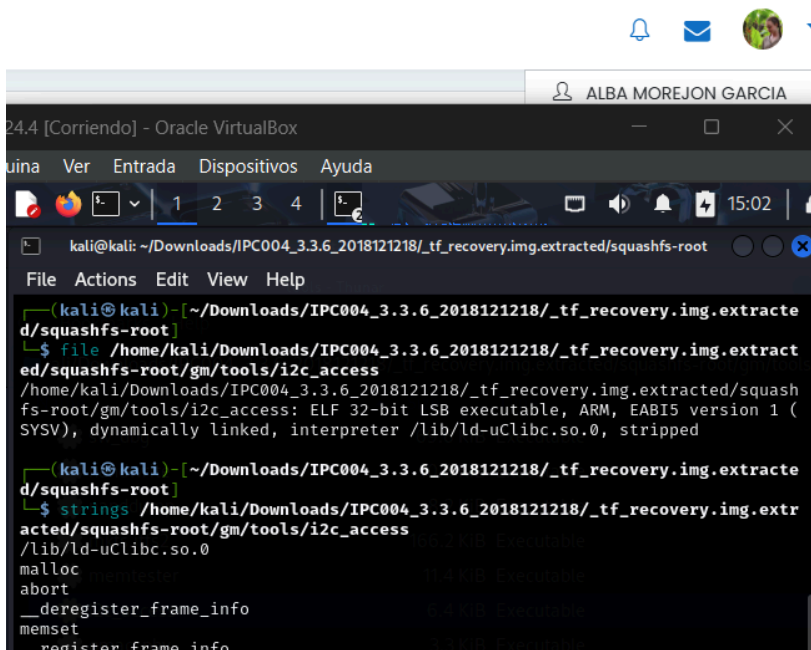
The screenshot shows a terminal window titled "KaliLinux2024.4 [Corriendo] - Oracle VirtualBox" with the user "ALBA MOREJON GARCIA". The terminal displays the content of a file named "wpa_supplicant.conf". The file is a configuration file for the wpa_supplicant daemon. The file is as follows:

```
1ctrl_interface=/var/run/wpa_supplicant
2update_config=1
3
4# Wi-Fi Protected Setup (WPS) parameters
5
6# Device Name
7# User-friendly description of device; up to 32 octets
8# encoded in UTF-8
9device_name=RTL8192CU
10
11# Manufacturer
12# The manufacturer of the device (up to 64 ASCII
13# characters)
14manufacturer=Realtek
15
16# Model Name
17# Model of the device (up to 32 ASCII characters)
18model_name=RTW_STA
19
20# Model Number
21# Additional device description (up to 32 ASCII
22# characters)
```

El archivo wpa_supplicant.conf, es una aplicación de espacio de usuario que maneja la autenticación WPA/WPA2.



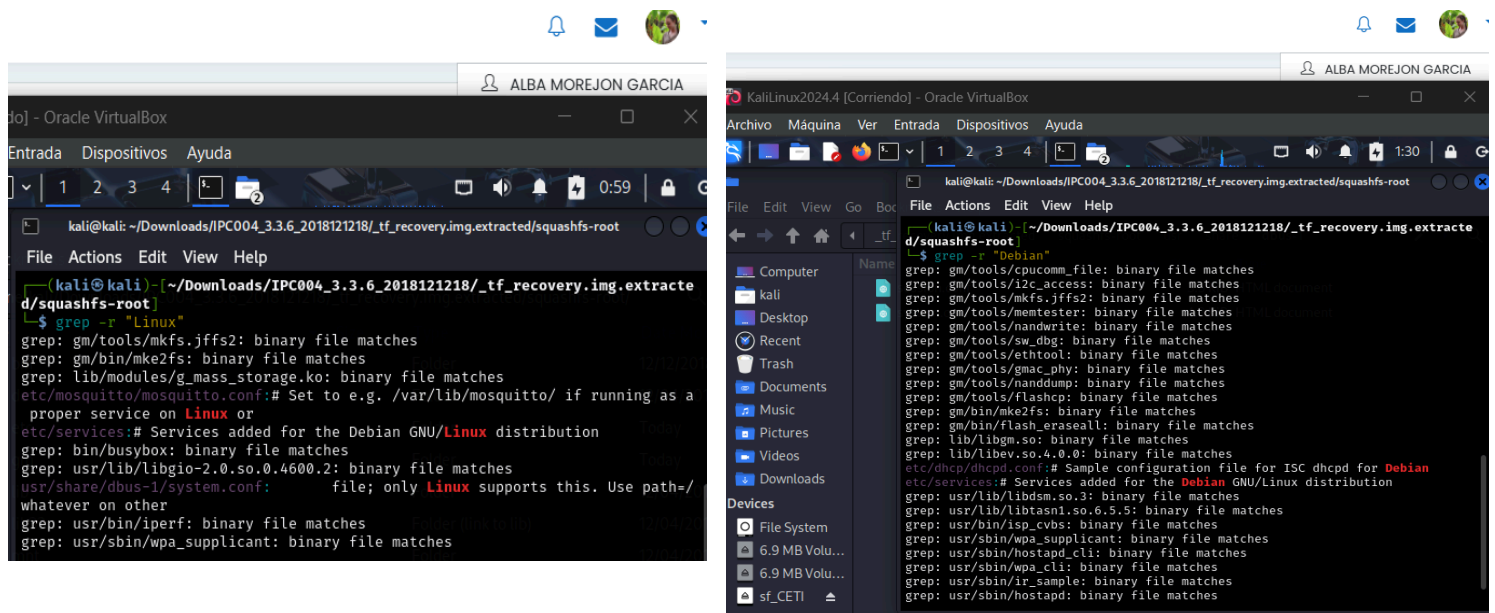
En el archivo `dhpd.conf` encontramos la configuración para el servidor DHCP, específicamente para sistemas basados en Debian.



Utilizamos también herramientas como `string` y `file` para analizar.

En concreto analizando los resultado de este archivo, el comando `strings` nos da información mayoritariamente sobre las bibliotecas que se están usando y el comando `file` nos da información acerca del archivo, es un ejecutable ELF de 32 bits, arquitectura ARM, vinculado con el interprete `/lib/ld-uClibc.so.0` que confirma que el entorno de ejecución es un sistema embebido basado en Linux.

Además si buscamos directamente las palabras clave en la ruta, encontramos archivos que coinciden o contienen las palabras “Linux” y “Debian”, que con otras palabras no obtenemos resultado.



¿Qué información podemos obtener del firmware de la cámara XIAOMI IMI Home Security Camera 1080P?

Configuración del sistema, archivos de configuración como dhcpd.conf, openssl.conf y wpa_supplicant.conf proporcionan detalles sobre la configuración de red, seguridad y autenticación. Los scripts de arranque (boot.sh, rcS) muestran cómo se inicializa el sistema y se configura el dispositivo durante el arranque.

Servicios y funcionalidades, identificamos servicios como mdev para la gestión del dispositivo y cpucomm_file para la comunicación entre CPUs. Existen archivos de comunicación de módulos del kernel (frammap.ko, cpu_com_fa726.ko, mod_probe).

Seguridad y criptografía, se utiliza OpenSSL para generar y manejar certificados, lo que indica la implementación de medidas de seguridad y cifrado.

Hardware, encontramos información sobre el dispositivo y el hardware en específico, así como la comunicación (i2c) y la gestión de memoria en archivos como i2c_access y fremap.

¿Qué sistema operativo usa?

Tras analizar el firmware facilitado, podemos decir que la cámara XIAOMI IMI Home Security Camera 1080P utiliza una variante de Linux basada en Debian. Esto se confirma por:

Encontramos archivos y configuraciones típicas de sistemas Linux: archivos como dhcpd.conf, openssl.conf y wpa_supplicant.conf proporcionan detalles sobre la configuración de red, seguridad y autenticación.

Había referencias específicas a Debian en archivos de configuración: archivos como dhcpd.conf y services mencionan específicamente Debian.

La utilización de herramientas y bibliotecas comunes en sistemas embebidos Linux: herramientas como uClibc, mdev y el uso de modprobe para cargar los módulos del kernel, son típicos de sistemas Linux embebidos.

En resumen el análisis del firmware revela que la cámara utiliza un sistema operativo Linux basado en Debian, optimizado para un entorno embebido destinado a tareas particulares con configuraciones específicas para la gestión de red, seguridad y hardware.

PREGUNTA 3: ¿Qué sistema de ficheros usa?

El sistema de ficheros utilizados por la XIAOMI IMI Home Security Camera 1080P es SquashFS. Esto se deduce porque al descomprimir el archivo facilitado que contiene el firmware, obtenemos la carpeta llamada “IPC004_3.3.6_2018121218/_tf_recovery.img.extracted/squashfs-root”, que indica que el contenido del firmware fue extraído de una imagen SquashFS (Squashfs es un sistema de archivos comprimidos de solo lectura para Linux).

PREGUNTA 4: ¿Puedes decir algunos servicios que use?

Algunos servicios que hemos encontrado en el firmware de la cámara son:

- mdev, utilizado para la gestión de dispositivos.
- cpucomm_file, para la comunicación entre CPUs.
- wpa_supplicant, para la autenticación en redes inalámbricas.
- openssl: para generar certificados de seguridad.
- fremap, para gestionar la memoria
- modprobe, para cargar módulos kernel

PREGUNTA 5: ¿Podrías decirnos qué usuarios tiene?

Los usuarios definidos en el archivo /etc/passwd, incluye usuarios con privilegios administrativos, para ejecución de procesos del sistema, la sincronización, servicios de correo...:

```
root::0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/false
bin:x:2:2:bin:/bin:/bin/false
sys:x:3:3:sys:/dev:/bin/false
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/false
www-data:x:33:33:www-data:/var/www:/bin/false
operator:x:37:37:Operator:/var:/bin/false
nobody:x:99:99:nobody:/home:/bin/false
dbus:x:1000:1000:DBus messagebus user:/var/run/dbus:/bin/false
mosquitto:x:1001:99:Mosquitto user:/:/bin/false
```

PREGUNTA 6: ¿Cómo se llama este tipo de análisis?

En este caso decir que estamos llevando a cabo un análisis forense no sería cierto, porque es una disciplina que se centra en la recopilación y análisis de evidencias para investigar delitos cibernéticos o abordar cuestiones legales.

Para un análisis simple cuyo objetivo es obtener información sobre el sistema, el tipo de análisis descriptivo sería el más adecuado. Este tipo de análisis se centra en resumir y presentar datos sobre lo analizado, para proporcionar una visión general del sistema. En el contexto de este ejercicio implicaría:

- Revisar archivos de configuración, para entender cómo está configurado el sistema (dhcpd.conf, openssl.conf, wpa_supplicant)
- Examinar scripts de arranque para ver cómo se inicia el sistema (boot.sh y rcS).
- Identificar usuarios y servicios (/etc/passwd).

El análisis descriptivo permite obtener una versión clara y concisa de la configuración y el funcionamiento del sistema.