APUNTES 04

REALIZACIÓN DE ANÁLISIS FORENSES EN IOT

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

1. Realización de análisis forenses en internet of things (iot).
    1.1. Identificar los dispositivos a analizar.
    1.2. Adquirir, analizar y extraer las evidencias.
    1.3. Línea temporal y cadena de custodia.
    1.4. Elaborar, presentar y exponer las conclusiones.

1.- REALIZACIÓN DE ANÁLISIS FORENSES EN INTERNET OF THINGS (IOT).

Caso práctico

María recibe una nueva llamada para trabajar en un caso dónde se investiga la actividad de un usuario.
Al llegar a la escena encuentra el portátil y teléfono móvil del sospechoso y sabe que durante el proceso de identificación encuentre nuevas evidencias que podrían no ser evidentes a simple vista pero que podrían aportar información al caso (piensa en el reloj inteligente del sospechoso, el sistema del coche eléctrico que hay en el garaje, o incluso pequeños electrodomésticos)
Sabe que estos dispositivos forman parte del Internet de las Cosas o IoT y que podrían aportar visibilidad sobre la localización del usuario, su actividad, relaciones con terceros, etc...
A nivel forense sabe que el escenario se complica desde la primera fase del análisis forense ya que la identificación ya no es tan sencilla y luego viene la adquisición de sistemas que ni siquiera conoce los detalles de cómo funcionan por dentro.. será un auténtico reto…

IoT trae muchas oportunidades y problemas para el análisis forense. La recopilación de datos forenses de dispositivos con interfaces y capacidades muy limitadas para el almacenamiento y procesamiento de datos es un desafío.
Por otro lado, la agregación de pequeñas piezas de datos de estos dispositivos puede proporcionar una visibilidad sin precedentes desde varias perspectivas. Eso abre un nuevo capítulo en el análisis forense digital.
El predominio futuro de dispositivos IoT proporcionará una gran cantidad de datos relevantes desde el punto de vista forense.

1.1.- IDENTIFICAR LOS DISPOSITIVOS A ANALIZAR.

A día de hoy no hay definida una metodología y un marco para el análisis forense de IoT. El análisis forense de IoT aún está en un estado muy inicial y se basa en metodologías y marcos de análisis forense digital estándar que pueden no ser completamente adecuados viendo la gran diversidad de dispositivos IoT existentes.
La primera fase de la metodología forense es la identificación y es aquí donde encontramos más cambios. Saber si ese reloj inteligente, nevera, televisión ha recogido datos que puedan aportar a la investigación es importante.
Con el análisis forense de IoT, lo primero que debe hacer un analista es identificar las fuentes de evidencia disponibles en la escena del delito. El investigador debe establecer qué dispositivos registraron datos relevantes para la investigación. La pregunta que debe responderse es:

- ¿Cómo interactúa este IoT con su entorno?
- ¿Qué tipo de datos recoge?
- ¿Esos datos aportan algún tipo de información relevante para la investigación?

Una vez que el investigador ha podido plantearse o contestar a estas preguntas entonces puede saber si es una evidencia válida. Además, se considera una buena práctica anotar todas las posibles evidencias aunque luego se descarten. Nunca se sabe si podrían ser relevantes.
De todas maneras el gran reto no es este sino ser capaces de reconocer la presentación de todos sistemas IoT y la identificación de los mismos. Finalmente una amplia gama de dispositivos diferentes dificulta tener un enfoque estandarizado para la recopilación de evidencias.

1.2.- ADQUIRIR, ANALIZAR Y EXTRAER LAS EVIDENCIAS.

Después de la identificación viene la adquisición y el escenario del forense de IoT vuelve a cambiar, en este caso una vez que tenemos la evidencia identificada el analista deberá plantearse las siguientes cuestiones:

- ¿Tengo alguna limitación para la recolección?
- ¿Qué tipo de sistema operativo y sistema de ficheros usa?
- ¿Qué formatos y dónde usa para almacenar los registros?
- ¿Tengo algún reto legal? (físicas, estándares de propiedad, legales).

Por ejemplo el dispositivo puede tener un sistema operativo cerrado, un sistema de ficheros no estandarizado o incluso el dispositivo puede contener datos sobre diferentes usuarios, no solo sobre los que son relevantes para la investigación. La identificación de los datos de un determinado usuario en un sistema cerrado no es una tarea sencilla. Si a esto añadimos que a nivel legal puede que accedamos sin quererlo a datos personales de usuarios no relacionados con la investigación hace que todo se complique.

De manera resumida tenemos los siguientes riesgos:

Técnicos

- Sistemas operativos cerrados o no documentados
- Sistemas de ficheros cerrado o no documentados
- Dificultad para acceder a los datos relevantes específicos
- Conectores o interfaces no estándar.
- Falta de mecanismos de seguridad que no permitan el borrado de eventos o evidencias

Organizativos

- Poca capacidad de estandarización del proceso
- Dificultad de formación nuevos miembros del equipo

Legales

- Acceso a información sensible (datos médicos, biométricos, personales) de usuarios no relacionados con la investigación
- Falta aún de base legal para admitir según que evidencias en proceso judicial

1.3.- LÍNEA TEMPORAL Y CADENA DE CUSTODIA.

Una cadena de custodia fiable -de dónde proceden los datos, quién los ha manejado, quién los ha modificado (y qué ha cambiado), y cuándo ha ocurrido todo esto exactamente- es fundamental para garantizar la validez de la evidencia en un proceso judicial.

Pero en un entorno de IoT conseguir esto no es nada sencillo. A veces el origen de los datos es un concentrador o bridge que puede provocar eventos que no son confiables ya sea por un error en la fuente o por una línea de tiempo errónea.

Por tanto tenemos dos puntos claros de fallo en la cadena de custodia:

- El seguimiento fiable de la fuente: Quién envió, recibió y alteró los datos (y si estaba autorizado a hacerlo),
- Línea temporal: Cuándo sucedieron estos hechos mediante un sellado de tiempo o timestamp coherente

Los dispositivos de IoT que por diseño suelen tener más fallos que sistemas IT tradicionales y que sufren mayores pérdidas de datos (porque no están configurados para ser robustos) generan múltiples eventos de los cuales muchos no son confiables. Al final el analista acaba trabajando con una mezcla de eventos considerados fiables con otros muchos corruptos o con información no confiable, produciéndose una mezcla que no deja discernir lo válido de lo descartable impactando en la línea temporal, en la validez de la fuente y por tanto condiciona la cadena de custodia y a la propia evidencia en si.

Para poder solucionar este problema deberemos de revisar de forma manual y mediante herramientas la validez de las fuentes de información, descartando las que generen eventos no confiables y tratando de tener una línea temporal coherente.

1.4.- ELABORAR, PRESENTAR Y EXPONER LAS CONCLUSIONES.

Uno de los puntos mas importantes dentro del análisis forense es poder exponer los resultados de las investigaciones. Si tenemos un escenario donde:

- La evidencia no es confiable, produciendo información no veraz
- Puede ser alterada o borrada sin mecanismos de seguridad
- Cadena de custodia poco solida derivada de todo lo anterior

Hace que a nivel de reporting tengamos que tener hacer hincapié en muchos aspectos clave para que nuestro informe sea veraz y pueda aportar en un proceso judicial.

Las principales recomendaciones: deben describir la naturaleza de la fuente de información

- Los tipos de eventos
- Su línea de tiempo
- La naturaleza de sus errores si hubiera
- La confiabilidad
- Describir la cadena de custodia y su proceso de elaboración

Autoevaluación I

Identifica si las siguientes frases son verdaderas o falsas

1- Los entornos de IoT son todo ventajas.
   a) Verdadero
   b) Falso

2- Los entornos de IoT suponen un gran avance a nivel forense pero implica muchos retos.
   a) Verdadero
   b) Falso

3- Los dispositivos IoT no están del todo documentados.
   a) Verdadero
   b) Falso

4- Un forense en IoT implica un trabajo adicional de conocer el sistema operativo, ficheros...
   a) Verdadero
   b) Falso

TEST I

1. En entornos de IoT una amplia gama de dispositivos diferentes provoca:
   a. Incremento del entorno cloud y local.
   b. Tener un enfoque estandarizado para la recopilación de evidencias.
   c. Muchas comunicaciones unificadas.
   d. Modelos de servicio diferente.
2. ¿Qué reto legal puede suponer la evidencia de un dispositivo IoT?:
   a. Qué el fabricante sea estándard.
   b. Contrato del proveedor del dispositivo.
   c. Qué la prueba no sea admisible.
   d. Fabricantes fuera de la Unión Europea.
3. La nube pública no implica la figura del proveedor. ¿Verdadero o falso?
   a. Verdadero
   b. Falso
4. ¿Qué problema nos encontramos en IoT?:
   a. Entornos de nube de terceros.
   b. Sistemas operativos cerrados o no documentados.
   c. Ninguna.
   d. Nuevos usuarios maliciosos.
5. Los dispositivos de IoT tienen estandarizado donde y como almacenan la información. ¿Verdadero o falso?
   a. Verdadero
   b. Falso
6. Una nube híbrida no supone un término intermedio entre nube dedicada pública o privada. ¿Verdadero o falso?
   a. Verdadero
   b. Falso
7. La metodología y procesos forenses en entornos de IoT sufre de dificultades para estandarizarse. ¿Verdadero o Falso?
   a. Verdadero
   b. Falso
8. ¿Qué provocará el forense en IoT?:
   a. Se abre una nueva era dorada del forense.
   b. Sistema de procesado de información basado en nube.
   c. Modelo de propiedad del dato distinto.
   d. Conjunto de herramientas forenses nuevas.
9. Los forenses en IoT rara vez llegan a juicio. ¿Verdadero o falso?
   a. Verdadero
   b. Falso
10. No hay una estandarización del tipo de eventos de IoT. ¿Verdadero o falso?
   a. Verdadero
   b. Falso

TEST II

1.La propiedad del dato en entornos de IoT depende del estado. ¿Verdadero o falso?
   a. Verdadero
   b. Falso

2.¿A qué retos se enfrenta un analista cuando llega a un escenario de posible presencia de IoT?:

   a. Procesar evidencias.
   b. Detectar comunicaciones no tradicionales.
   c. Normativas específicas.
   d. Ser capaces de reconocer la presencia de todos sistemas IoT.

3. ¿Qué necesitamos saber para elegir modelo de nube?:
   a. Datos sobre los que necesitamos mayor control.
   b. Disponibilidad de los datos necesaria para los servicios.
   c. Presupuesto con el que contamos.
   d. Todas las anteriores.

4.La principal fase impactada en un forense en IoT es la del Informe o Exposición de los hechos. ¿Verdadero o falso?
   a. Verdadero
   b. Falso

5. En modelos de IoT no existen herramientas forenses específicas. ¿Verdadero o falso?
Seleccione una:
   a. Verdadero
   b. Falso

6. ¿Qué fase o fases se ven seriamente impactadas en un forense en IoT?:
   a. Procesamiento e informe final.
   b. Procesamiento.
   c. Identificación y Adquisición.
   d. Informe final

7. A día de hoy hay definida una metodología y un marco para el análisis forense de IoT desarrollada por la Unión Europea. ¿Verdadero o falso?
   a. Verdadero
   b. Falso

8. ¿Qué situación nos encontramos en los dispositivos IoT?:
   a. Más capacidad computacional.
   b. Falta de mecanismos de seguridad que no permitan el borrado de eventos o evidencias.
   c. Mejora en la disponibilidad del dato.
   d. Mejores tiempos de respuesta.

9. Los analistas forenses prefieren evitar las complicaciones técnicas de un forense en IoT. ¿Verdadero o falso?
   a. Verdadero
   b. Falso

10.Las herramientas forenses específicas de IoT aún están en un estado muy inicial. ¿Verdadero o Falso?
   a. Verdadero
   b. Falso

Respuestas:
Autoevaluación I: 1 b), 2 a), 3 a), 4 a)
TEST I: 1 b), 2c), 3b), 4b) 5b), 6b). 7a), 8a), 9b), 10a)
TEST II: 1 b), 2d), 3d), 4b) 5b), 6c). 7b), 8b), 9b), 10a)

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.

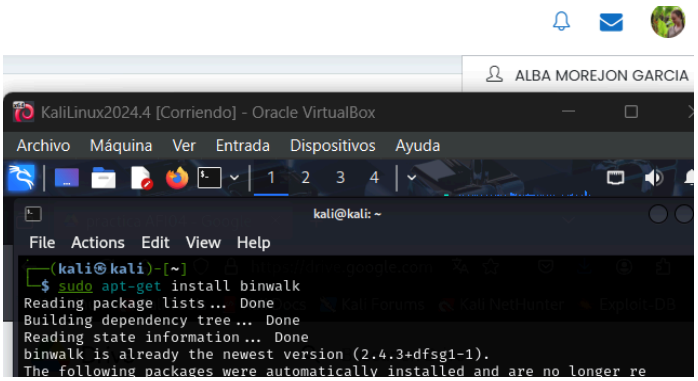
Apartado 1: Análisis de IoT

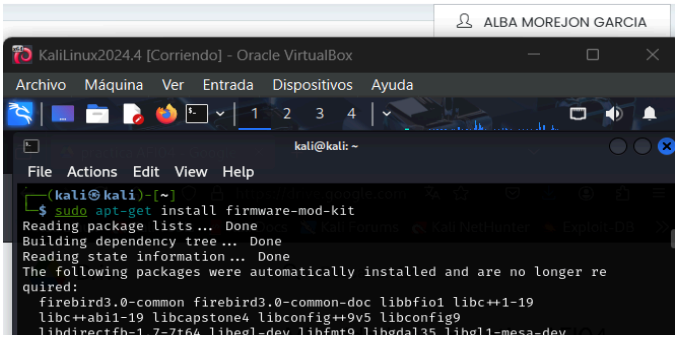
En esta tarea nos enfrentaremos a uno de los principales retos que tenemos cuando tenemos que analizar un dispositivo de IoT que desconocemos su funcionamiento.

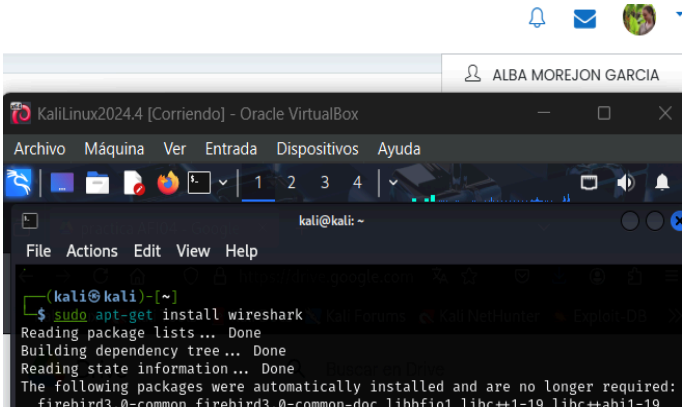
PREGUNTA 1: ¿Qué información podemos obtener del firmware de la siguiente de la bombilla (dispositivo IoT)? ¿Por qué sucede esto? ¿Qué supone para el análisis forense esta situación?

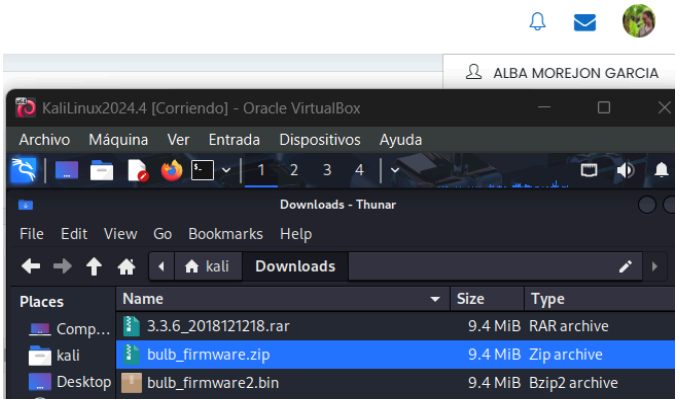
Link firmware

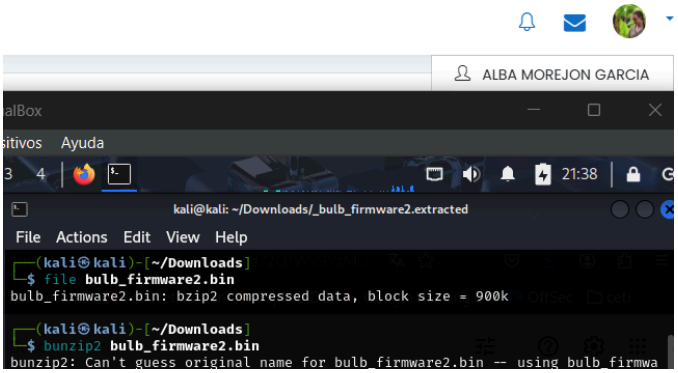
Instalación y descompresión del archivo

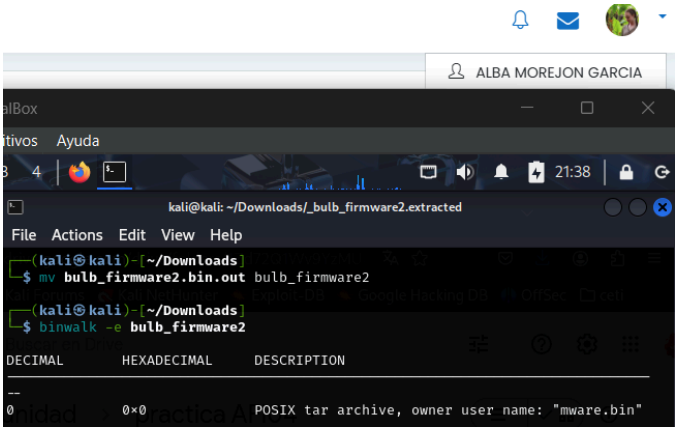


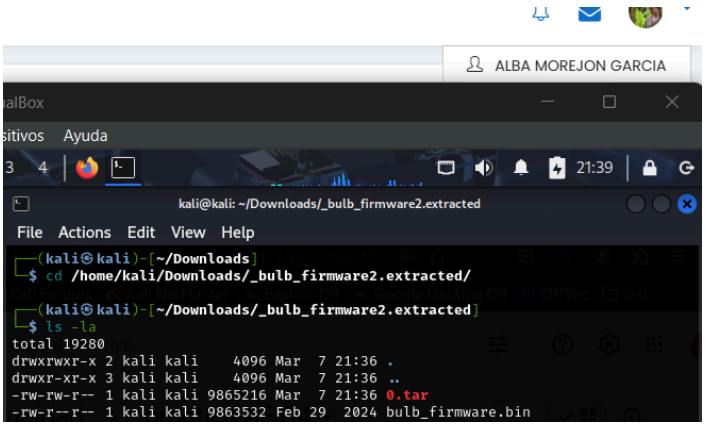


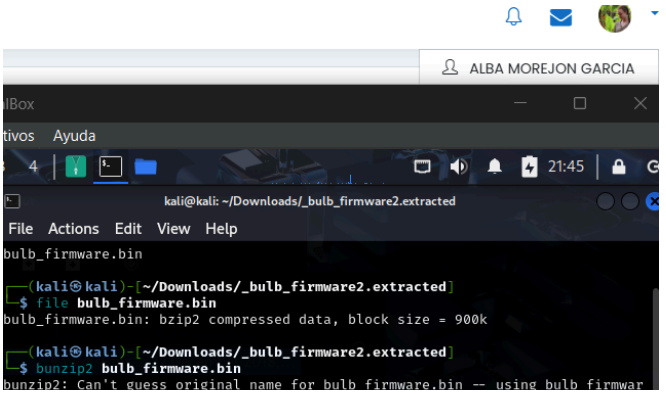


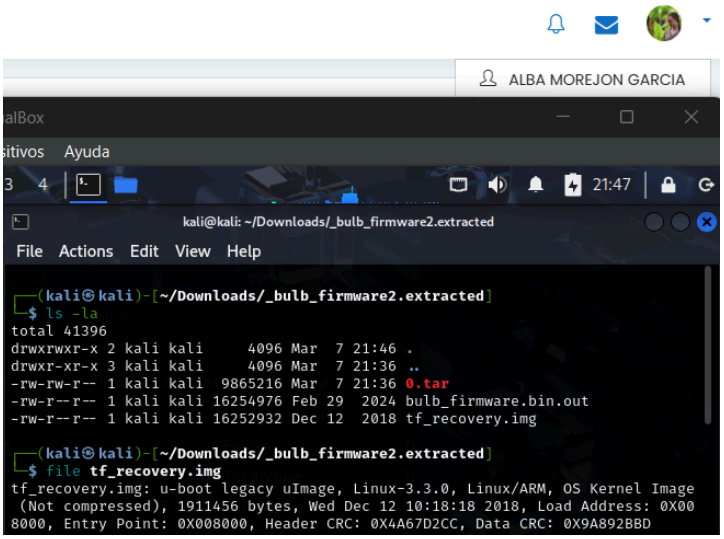


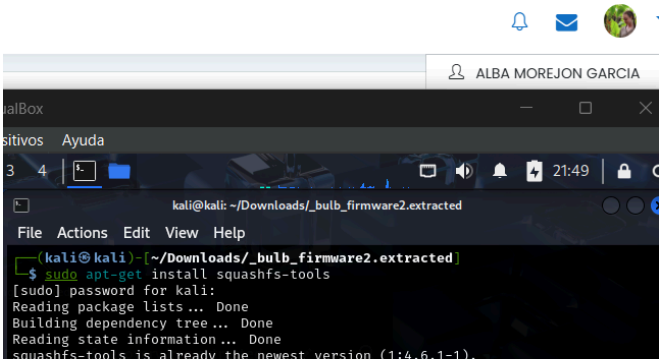




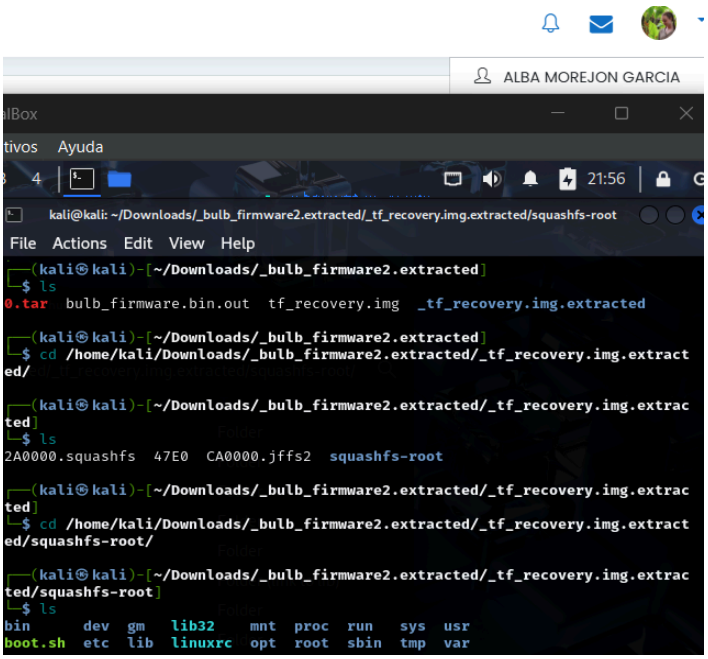






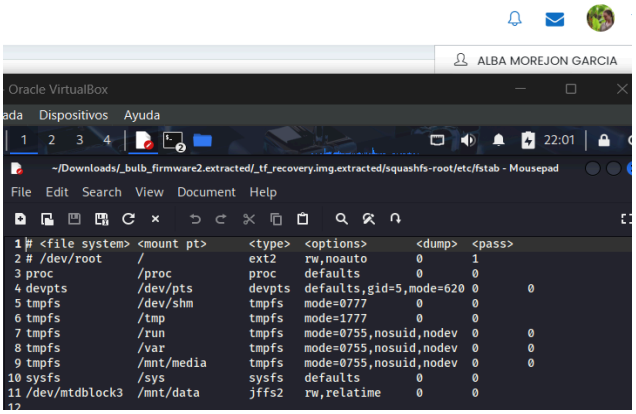


Archivos que tenemos actualmente

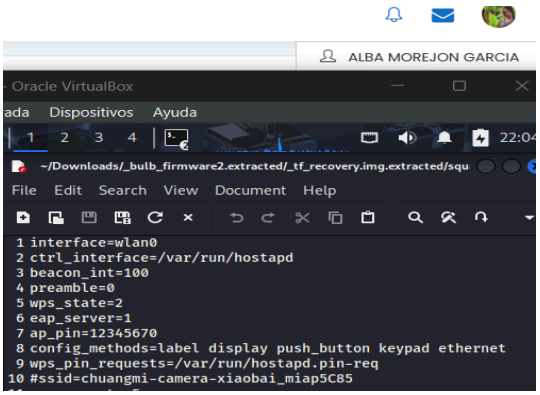


Vemos algunos archivos

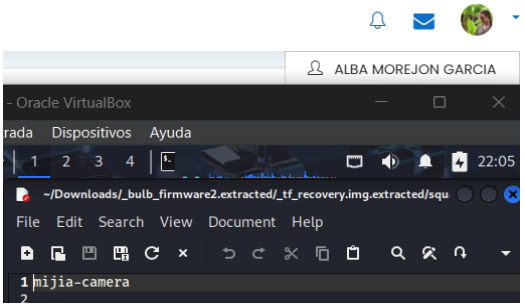
fstab:



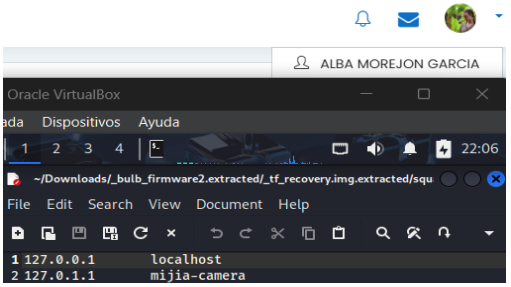
hostapd.conf:



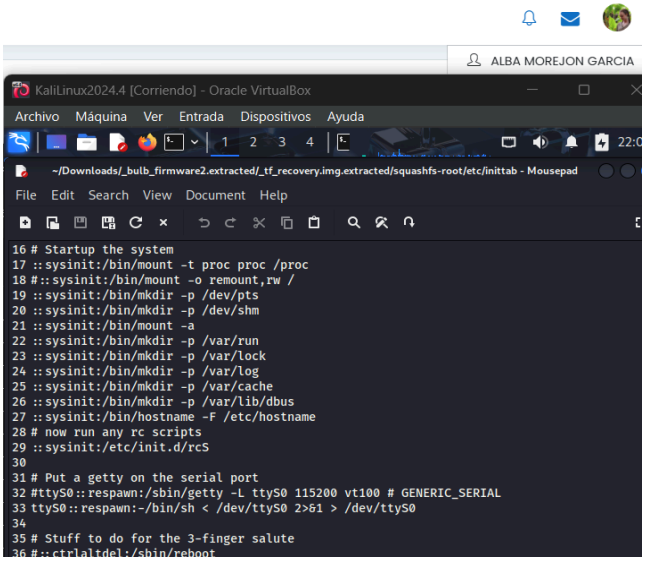
hostname:



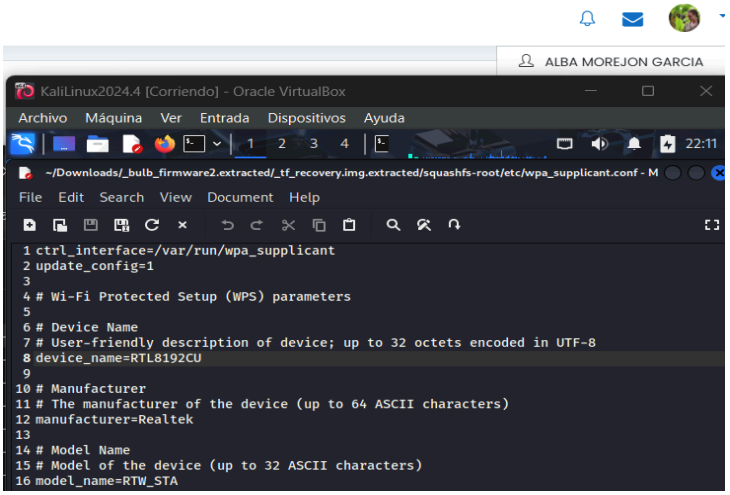
hosts:



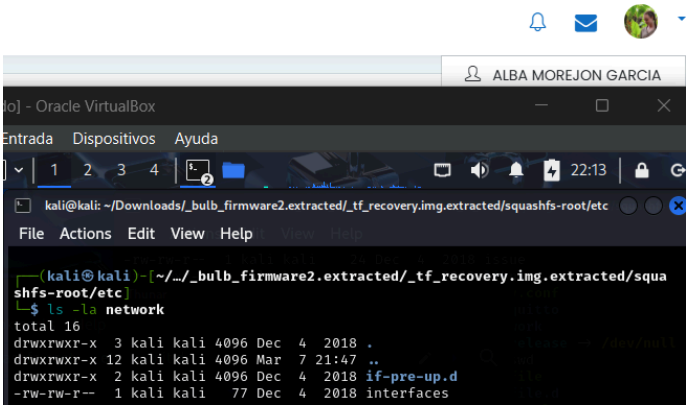
inittab:



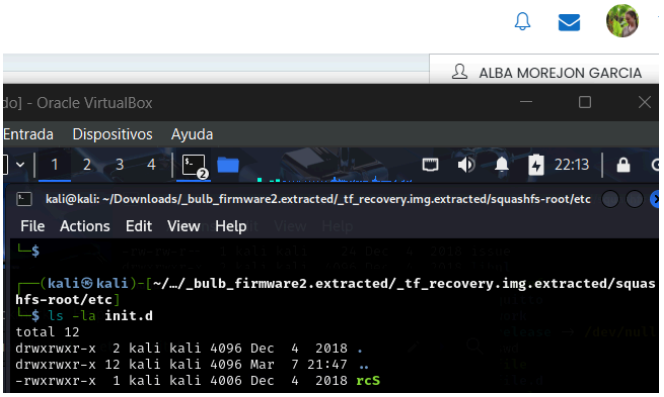
wpa_supplicant.conf:

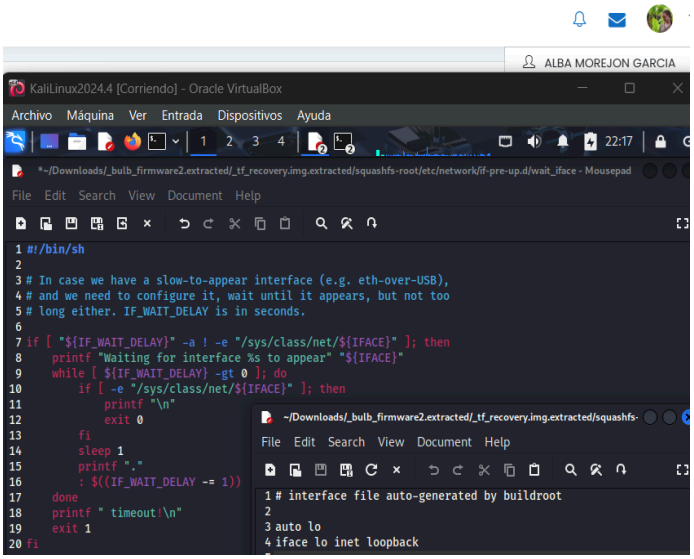


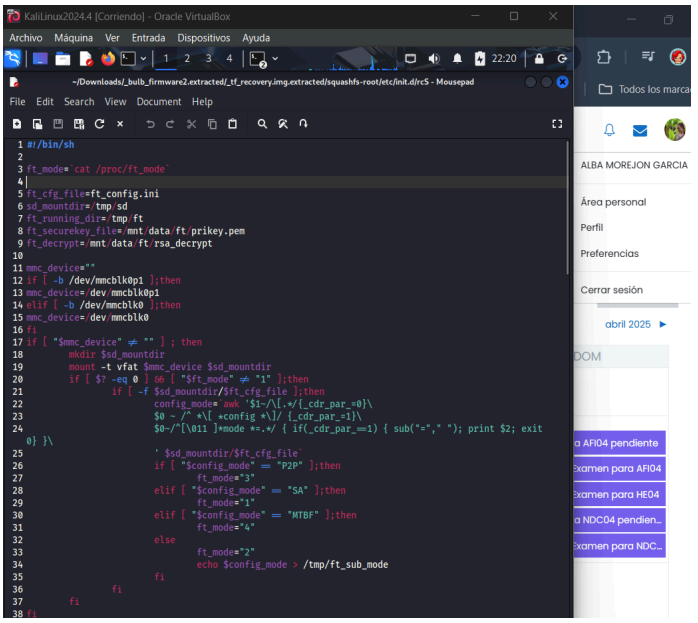
Carpeta network:



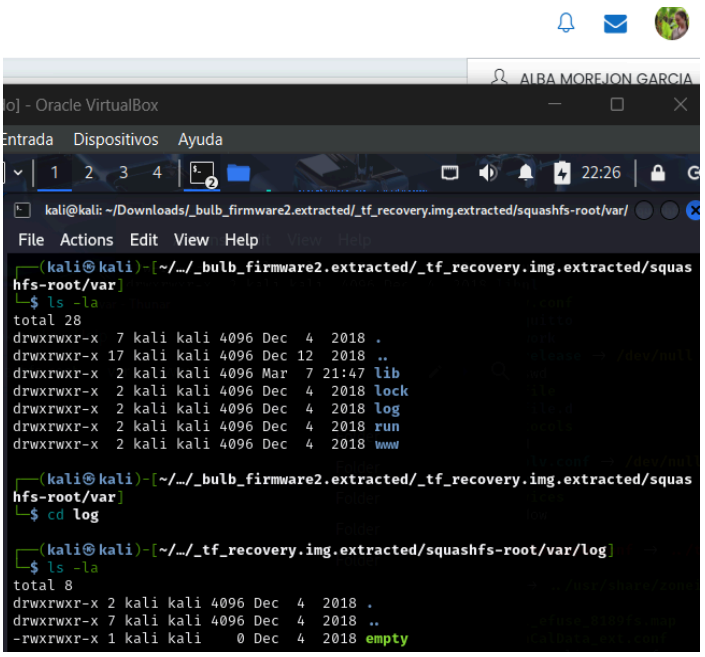
Carpeta inid.t:

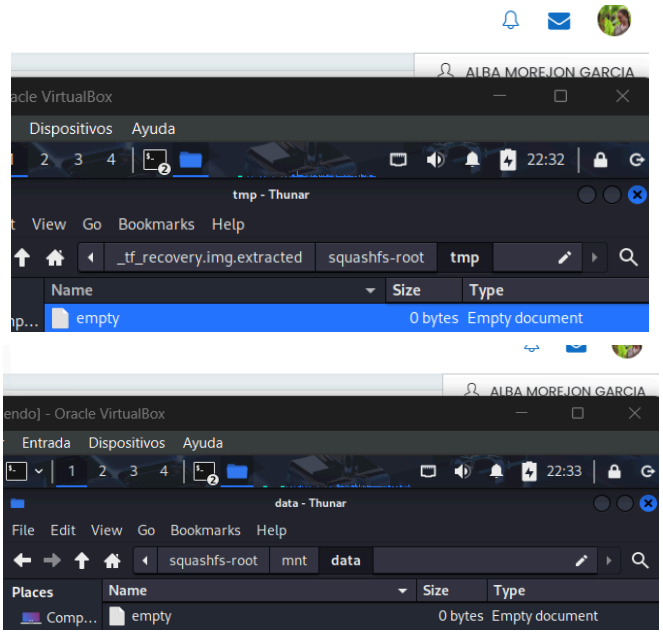






En otras carpetas como var, tmp o data, no encontramos archivos que se puedan analizar:





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.

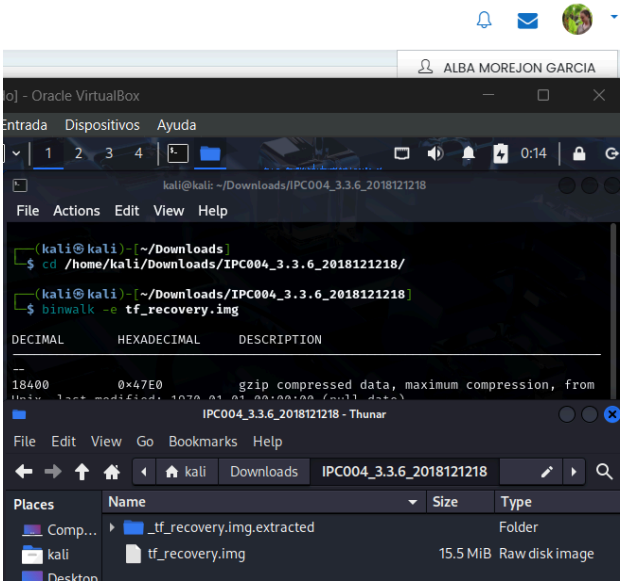
Recolección de evidencias, la información obtenida del firmware puede ser crucial para entender el comportamiento del dispositivo y recolectar evidencia en investigaciones forenses.

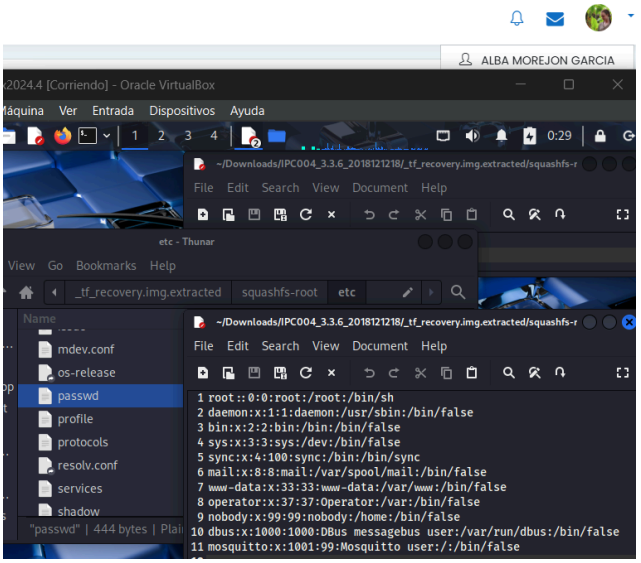
Compresión del funcionamiento del dispositivo, permite una comprensión detallada de cómo el dispositivo se comunica en la red, qué servicios se ejecutan y cómo se manejan las actualizaciones y configuraciones.

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

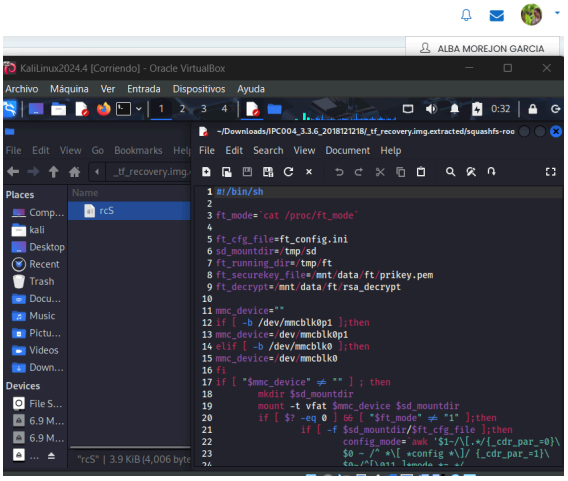
PREGUNTA 2: ¿Qué información podemos obtener del firmware de la cámara XIAOMI IMI Home Security Camera 1080P ? ¿Qué sistema operativo usa? Link al archivo

Descomprimimos 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/

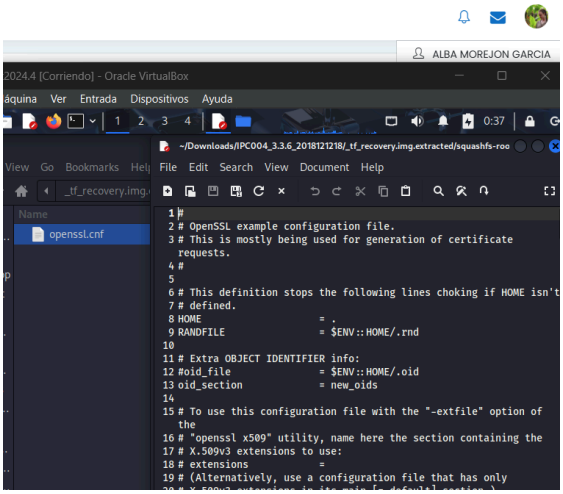




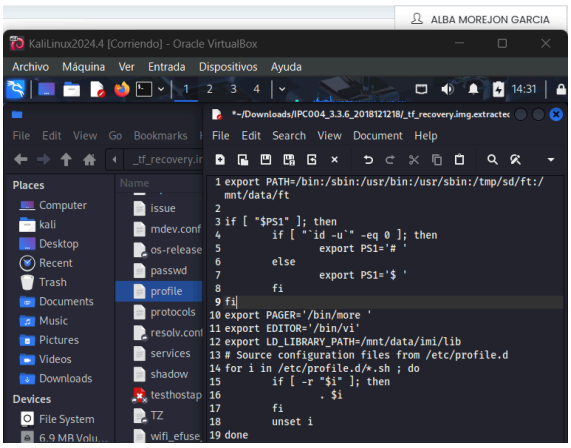
El archivo /etc/passwd, nos muestra los usuarios actuales del dispositivo y la presencia de usuarios como root, daemon, bin y sys, sugiere que el sistema operativo es una variante de Linux.



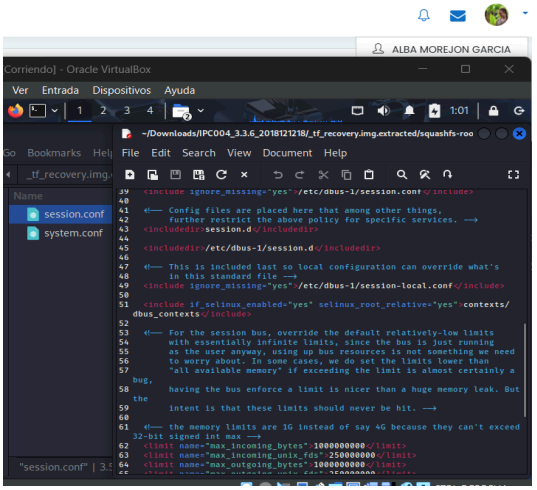
El archivo rcS es un script de inicialización que se ejecuta durante el arranque, destacamos la utilización de comandos como mount o la ejecución de scripts como ft_boot.sh.



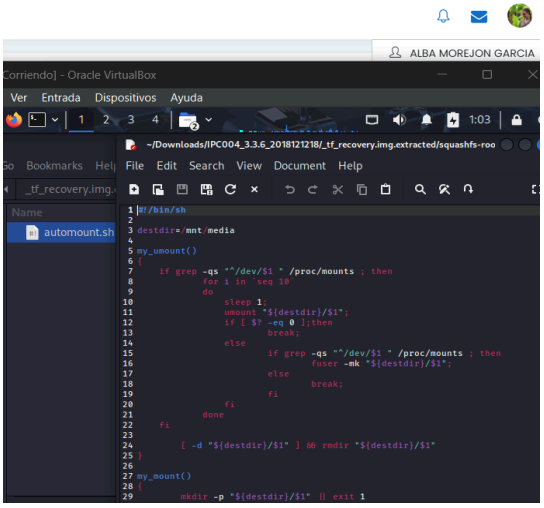
La configuración y el uso de Open SSL son comunes en sistemas Linux y la estructura del archivo es típica de estos archivos de configuración en estos sistemas.



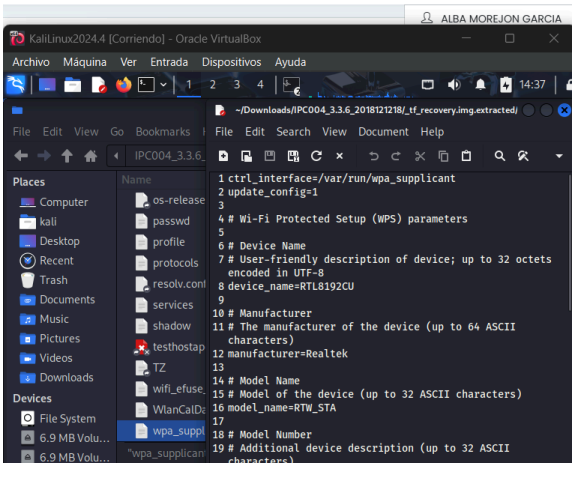
El archivo profile, es un archivo que establece variables de entorno y contiene rutas como /bin /sbin, /usr/bin… que son típicas de sistemas Linux (además, utiliza vi como editor).



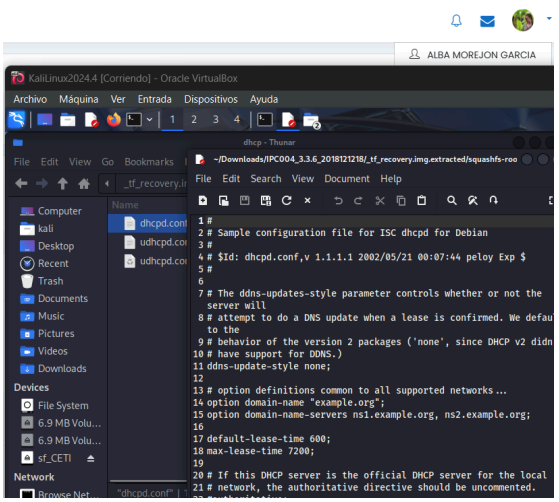
El archivo session.conf, configura D.Bus que es utilizado en sistemas Linux para la comunicación entre procesos.



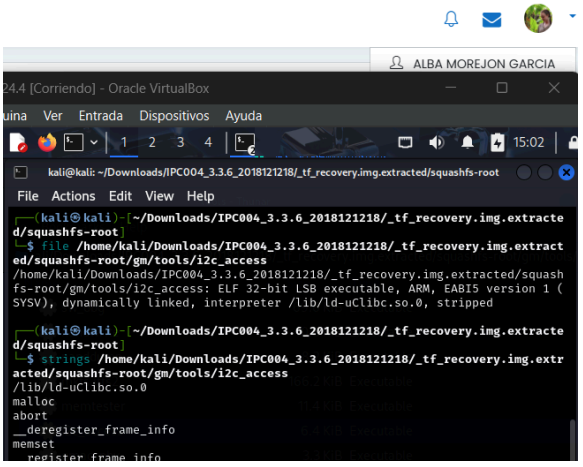
El script llamado automount.sh es un script de shell que comienza con #!/bin/sh, es común en sistemas Unix/Linux, maneja el montaje y desmontaje de dispositivos.



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



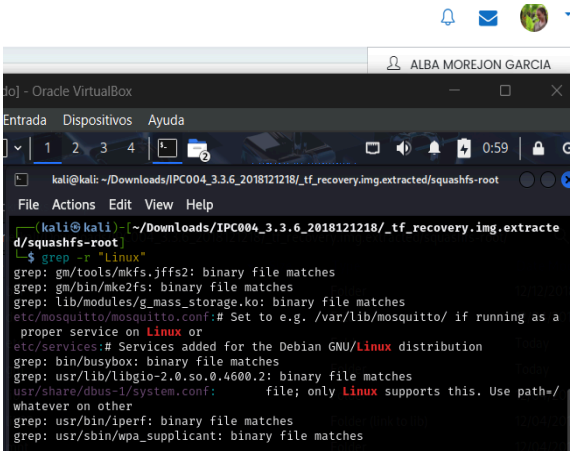
En el archivo dhpd.conf encontramos la configuración para el servidor DHCP, específicamente para sistemas basados en Debian.

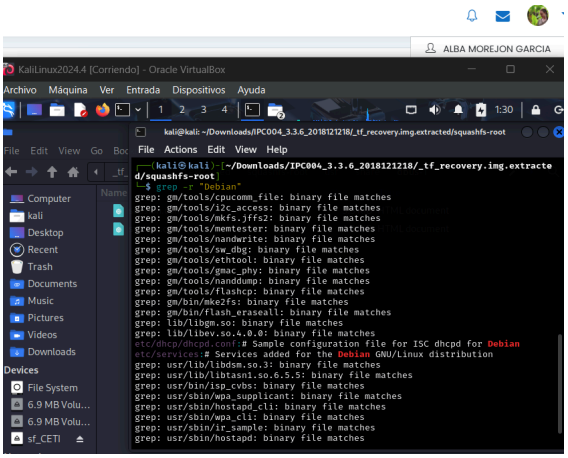


Utilizamos también herramientas como string y file para analizar.

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/psswd).

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