Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Análisis Forense Informático

UD04. Análisis de IoT.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

Pixabay (Dominio público)

María se enfrente 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 qué tipo de servicios o conexiones realizar por lo que analiza su firmware para tener más detalles de dónde, qué y cómo buscar.

¿Qué te pedimos que hagas?

✓ **Apartado 1: Análisis de IoT**

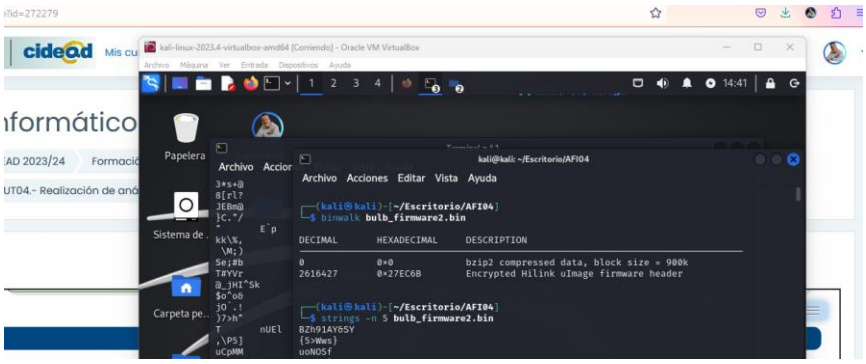
Esta tarea nos enfrentaremos a uno de los principales retos que tenemos cuando tenemos que analizar un dispositivo de IoT que desconocemos su funcionamiento.

➢ 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 https://drive.google.com/drive/folders/1U7vZameivlfhaOiSLYfbujV1ZOOMhrIb

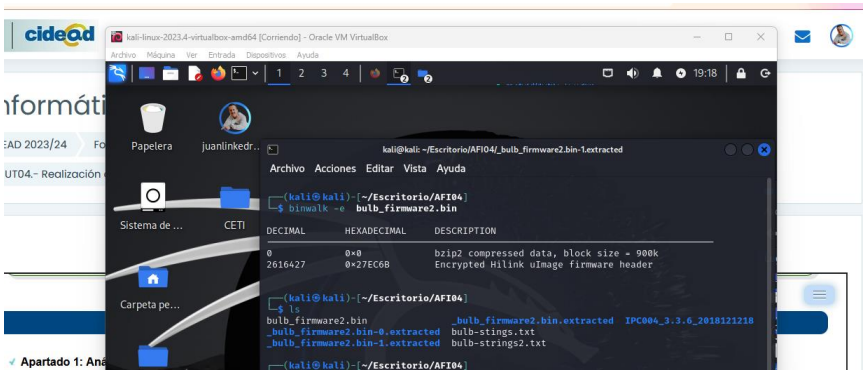
Vamos a revisar el archivo con **`binwalk`**:

`binwalk bulk_firmware2.bin`

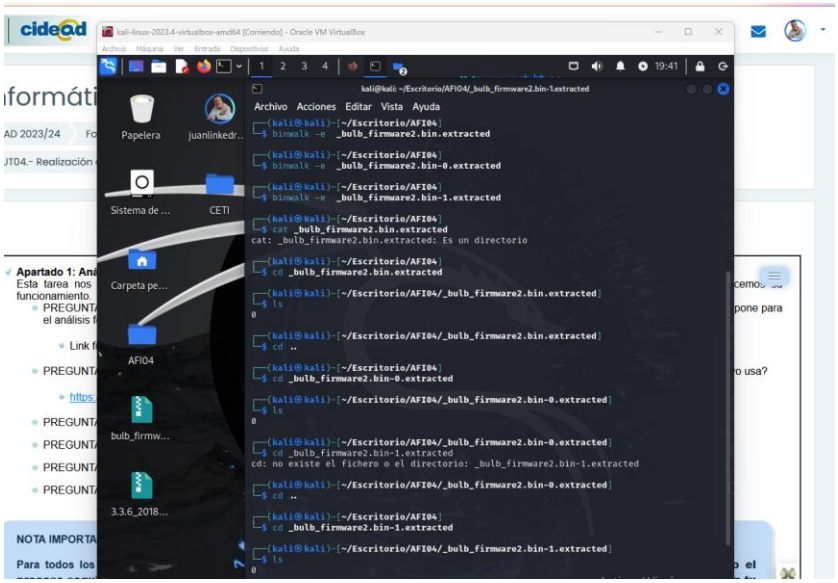


Vemos que es un archivo comprimido, y del que, aunque intentemos sacar datos mediante **`strings`**, no nos aporta mayor información.

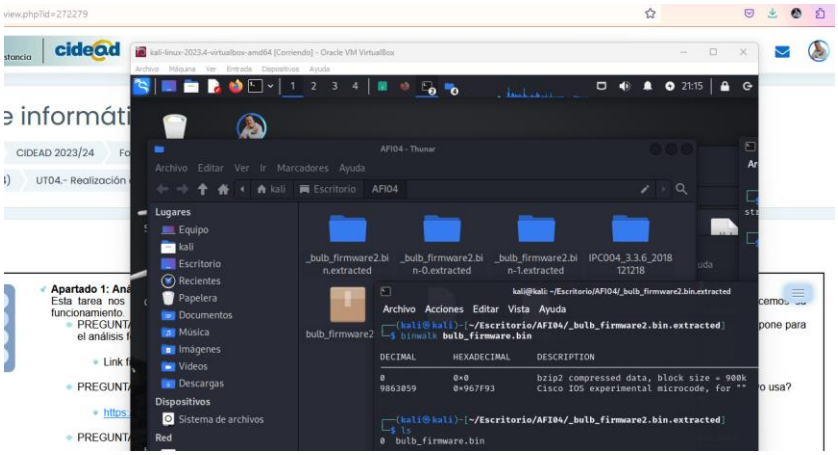
Vamos a ver su contenido para intentar conseguir algo más:



No parecen aportar nada más.

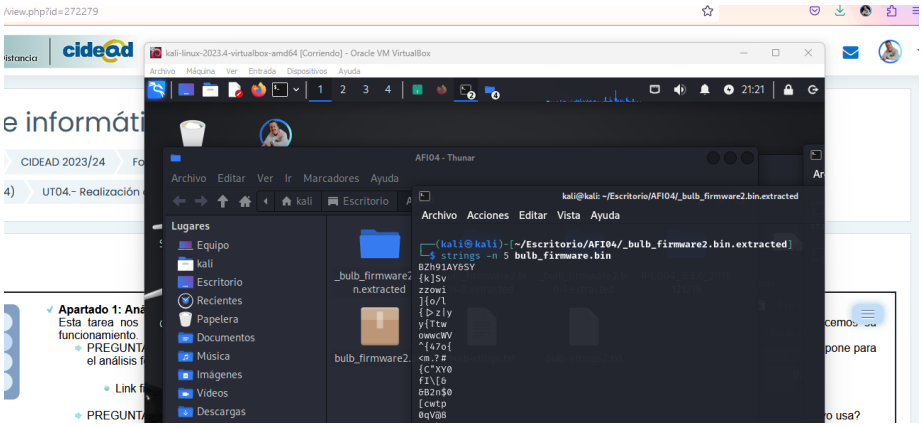


Intentaré probar con la extracción de datos desde **`_bulb_firmware2.bin.extracted`**



Probamos a ver si hay algo reseñable.

Intentamos encontrar mediante **`strings`** información que resaltar, pero no lo es posible hasta donde he podido:



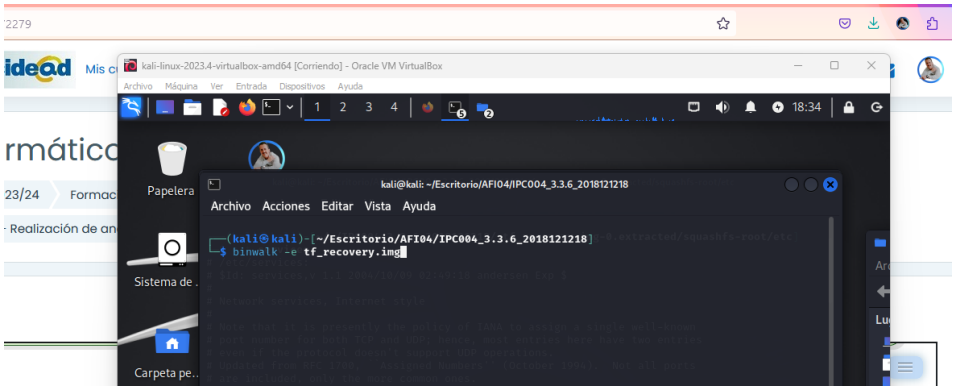
Queda clara la dificultad de encontrar resultados y realizar un correcto análisis cuando nos llegan elementos cifrados.

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

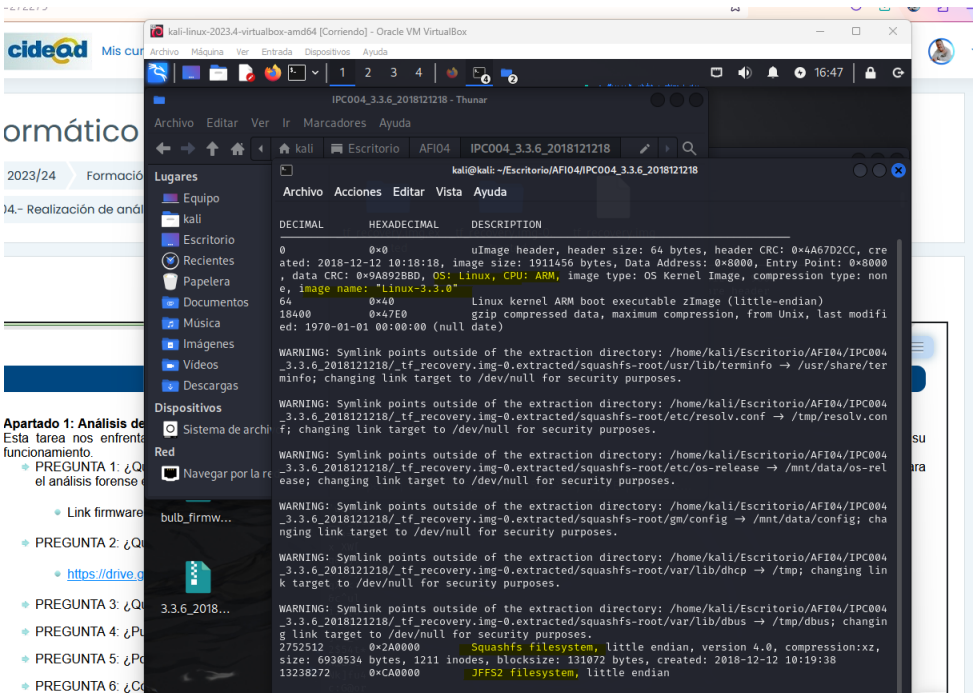
  - https://drive.google.com/file/d/1pB_XqoHGLN9yA51HgD9QHoxpx588Kn1v/view?usp=sharing

    Realizamos la extracción de archivos con **`binwalk`**:

    `binwalk -e tf_recovery.img`



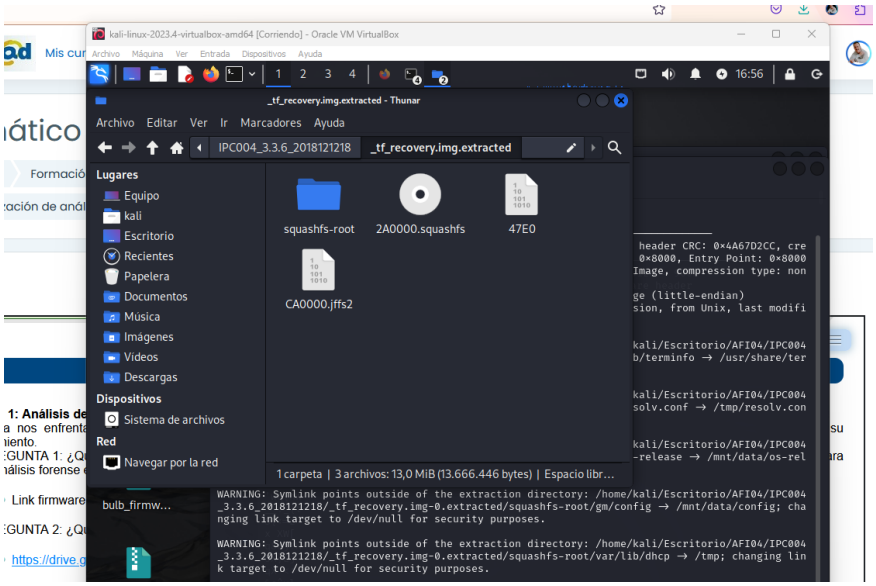
    Ejecutamos para comprobar los datos de la extracción.

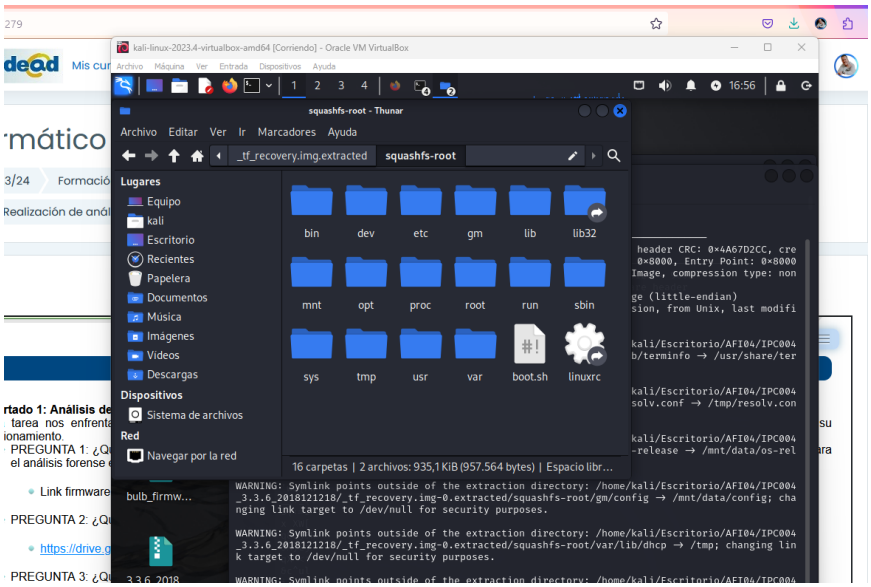


    Podemos observar tras esto, que utiliza un sistema operativo **`Linux 3.3.0`** basado en **`ARM`**, con dos sistemas de ficheros, **`Squashfs`** y **`JFFS2`**.

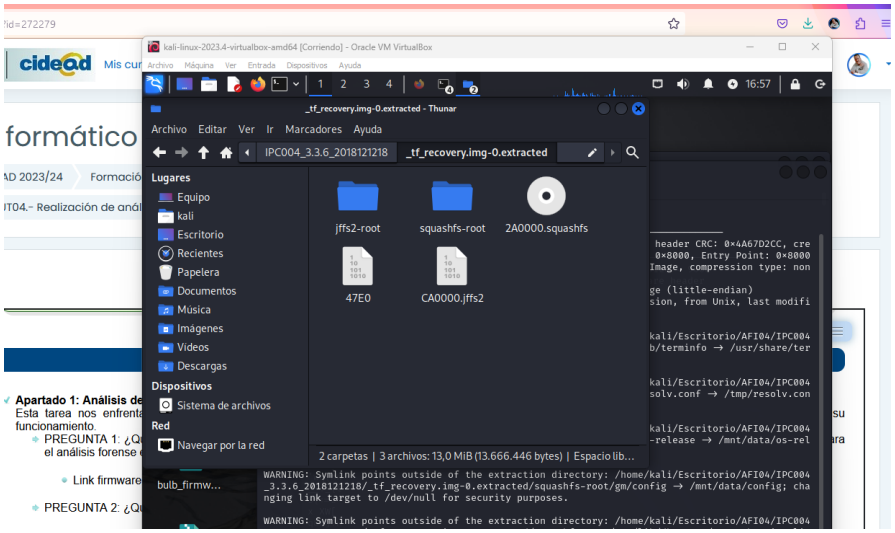
    Ha extraído en el proceso dos carpetas: **`_tf_recovery.img.extracted`** y **`_tf_recovery.img-0.extracted`**.

Observamos su contenido:

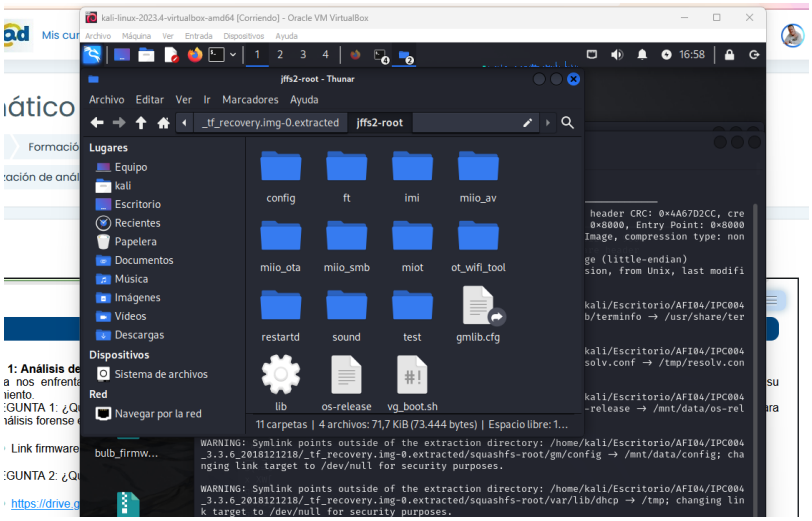




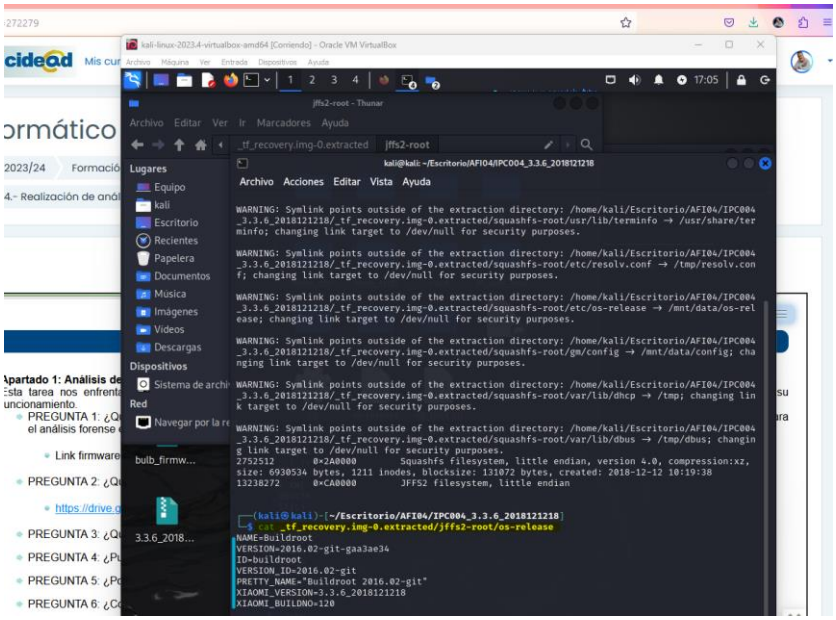
Vamos con la siguiente. Encontramos los nombres de los dos sistemas…



Abrimos el primero y algo llama la atención: parece ser un sistema propietario.

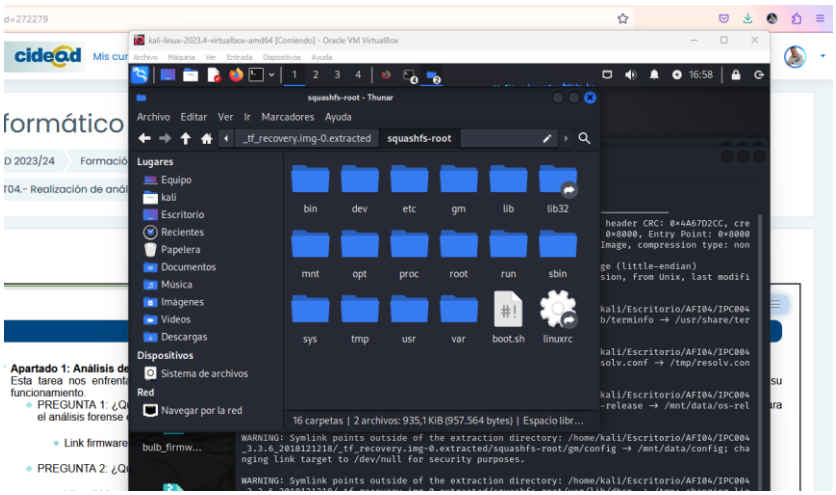


Vamos a observar el archivo **`os-release`** para confirmar esta sospecha:



Efectivamente, es un sistema **`XIAOMI`** en su versión **`3.3.6_2018121218`**.

`Squashshfs`, por su parte, mantiene los directorios típicos de un sistema **`Linux`**.



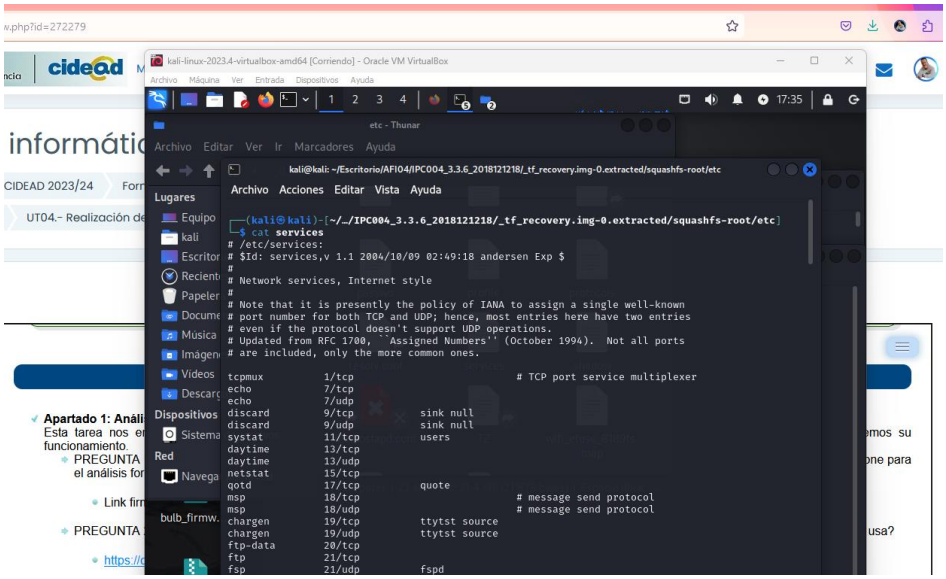
➢ PREGUNTA 3: ¿Qué sistema de ficheros usa?

Como se apuntaba en la pregunta anterior, usa **Squasfs** y **JFFS2** como sistemas de ficheros.

➢ PREGUNTA 4: ¿Puedes decir algunos servicios que use?

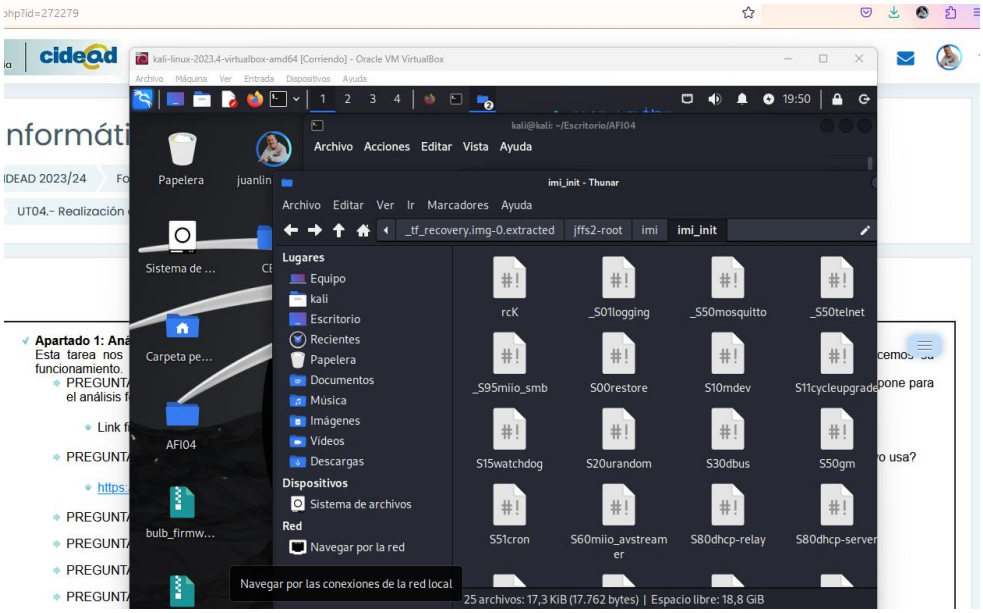
Vamos a encontrarnos dos localizaciones:

Como suele ser en estas distribuciones, podemos encontrar este tipo de dato del directorio **/etc/services**. Accedemos y vemos **ssh**, **ftp**, **telnet**, **smtp**,**nextstep**, **saft**… Son servicios disponibles, pero que no tienen por qué utilizarse.



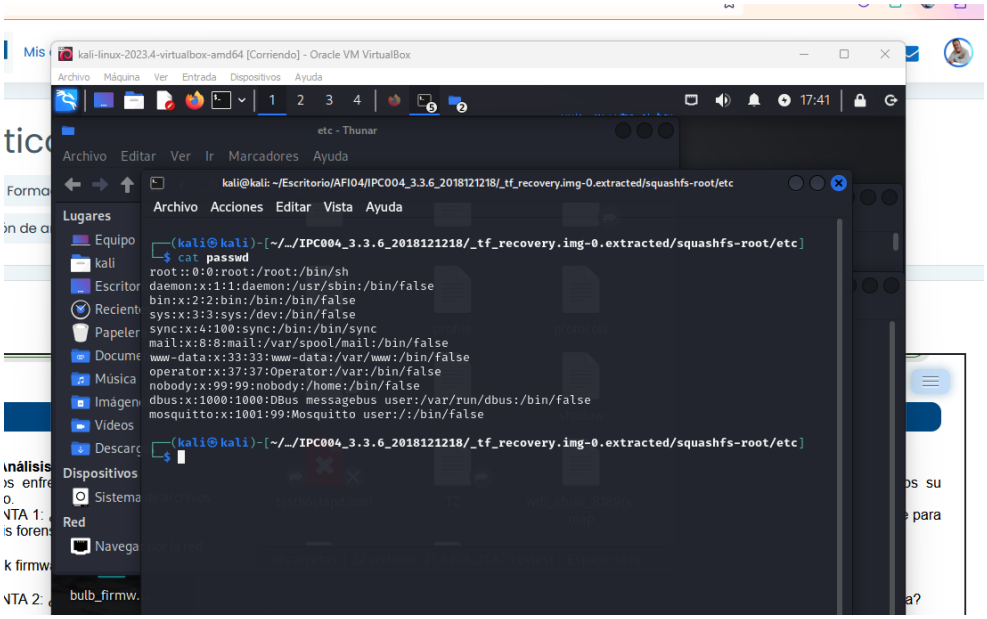
Por otro lado, tenemos los servicios configurados para utilizarse al arrancar el sistema creado.

Estos están en el directorio **jffs2-root/imi/imi_init**, donde están servicios como **rcK**, **mosquitto**, **telnet**, **restore**…



➢ PREGUNTA 5: ¿Podrías decirnos que usuarios tiene?

Como en el caso anterior, vamos al directorio **`/etc/password`** para poder visualizarlos.



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

Es un análisis de ingeniería inversa del firmware, donde hemos intentado examinar el código de los archivos volcados, en este caso, más que para encontrar o identificar vulnerabilidades, conocer un poco su compleja estructura, sus datos y funcionamiento.

Webgrafía.

https://www.mecd.es/cidead/aulavirtual/course/view.php?id=2367#section-4