**Análisis de Adquisición de Dispositivo IoT (Refrigerador)**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Autopsy**](#_lhc72lpw3wb5) **1**

[**2.1 Creación del caso:**](#_5d38uxjyswtl) **2**

[**3. Cuestiones**](#_pfzar7yxliz3) **3**

[**3.1 ¿Cuántos volúmenes componen esta imagen?**](#_2njr7nu7of5t) **3**

[**3.2 ¿Cuáles son los volúmenes que a priori tienen información analizable y que función tienen?**](#_4psfidb908zy) **4**

[**3.3 ¿Qué tipo de Sistema Operativo parece tener este dispositivo? ¿De qué distribución en concreto se trata?**](#_5dponinaqo15) **5**

[**3.4 ¿El sistema tiene varios usuarios? En caso afirmativo indica cuáles son.**](#_o9rn0oiopx9b) **5**

[**3.5 ¿El refrigerador tiene servicio bluethoot? Justifica tu respuesta.**](#_xwml3rh9usnw) **6**

[**3.6 El dispositivo que estamos analizando permite la navegación en la web. ¿sabrías decir si tenía alguna pestaña abierta en el momento de realizar la adquisición? En caso afirmativo indica que estaba visualizando el usuario en dicha pestaña.**](#_b8qqucpl02m0) **7**

[**3.7 Si nos fijamos en el historial de búsqueda del navegador del refrigerador, veremos cuales son los intereses del usuario dueño de este dispositivo. ¿Cuáles eran estos intereses?**](#_yeqrxpk100e4) **8**

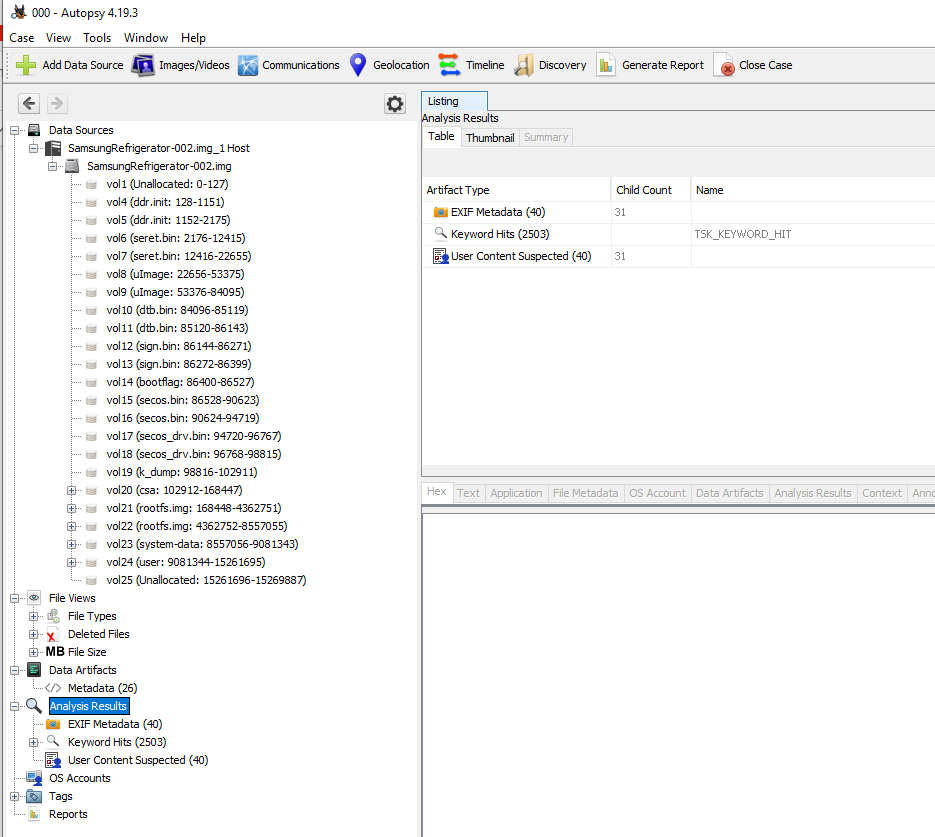
[**3.8 Lista alguna de las aplicaciones a las que tiene acceso el usuario propietario. Al menos una de ellas ha de ser una aplicación de terceros bastante conocida.**](#_89wcpiny5kpv) **8**

[**3.9 ¿Cuál es el correo utilizado por el usuario para crear la cuenta Samsung del dispositivo?**](#_8jddr5wa8k3e) **9**

[**3.10 En el listado de aplicaciones del usuario propietario, hay una que se encarga de realizar fotografías al contenido del frigorífico. Indica la ruta donde se encuentran estas imágenes y pon capturas de algunas de ellas.**](#_o5n7j9doigtd) **10**

# **2. Autopsy**

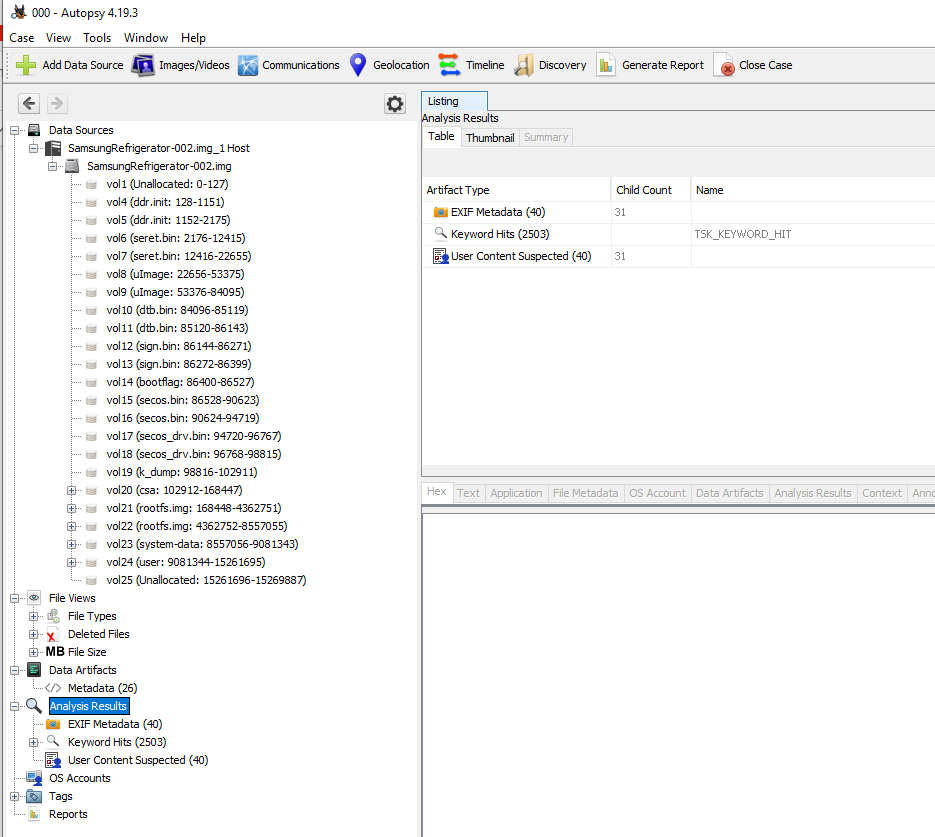
### **2.1 Creación del caso:**



Añadimos la fuente de evidencia proporcionada.

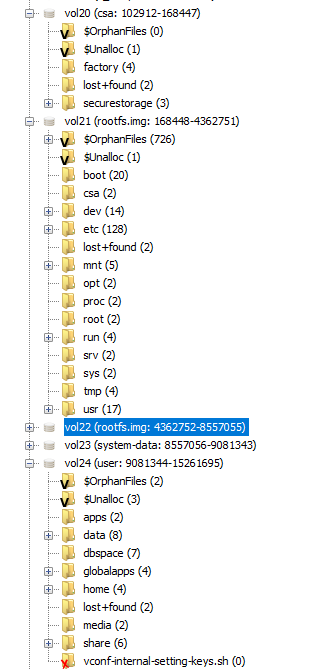
# **3. Cuestiones**

### **3.1 ¿Cuántos volúmenes componen esta imagen?**



Se compone de un total de 25 volúmenes.

### **3.2 ¿Cuáles son los volúmenes que a priori tienen información analizable y que función tienen?**



Los volúmenes analizables y sus funciones son los siguientes: 20, 21, 22, 23 y 24.

Volumen 20: Archivos del sistema

Volumen 21: Archivos del sistema

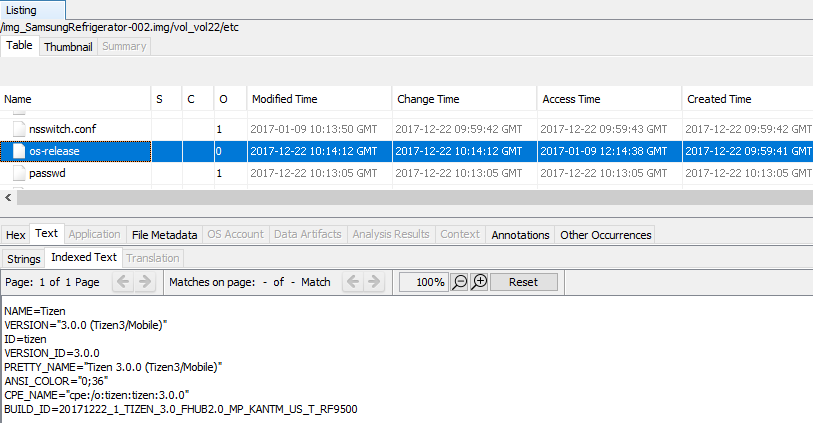
Volumen 22: Archivos del sistema

Volumen 23: Datos del sistema

Volumen 24: Datos de los usuarios

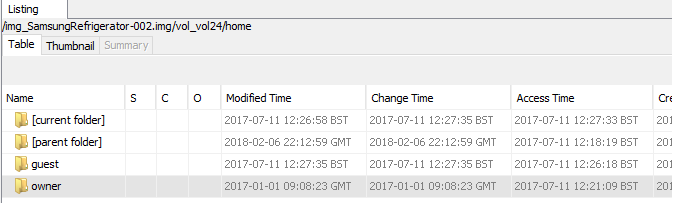
### **3.3 ¿Qué tipo de Sistema Operativo parece tener este dispositivo? ¿De qué distribución en concreto se trata?**

Fijándonos en los volúmenes 21, 22 y 23, conseguimos ver similitudes con un sistema operativo linux o android.



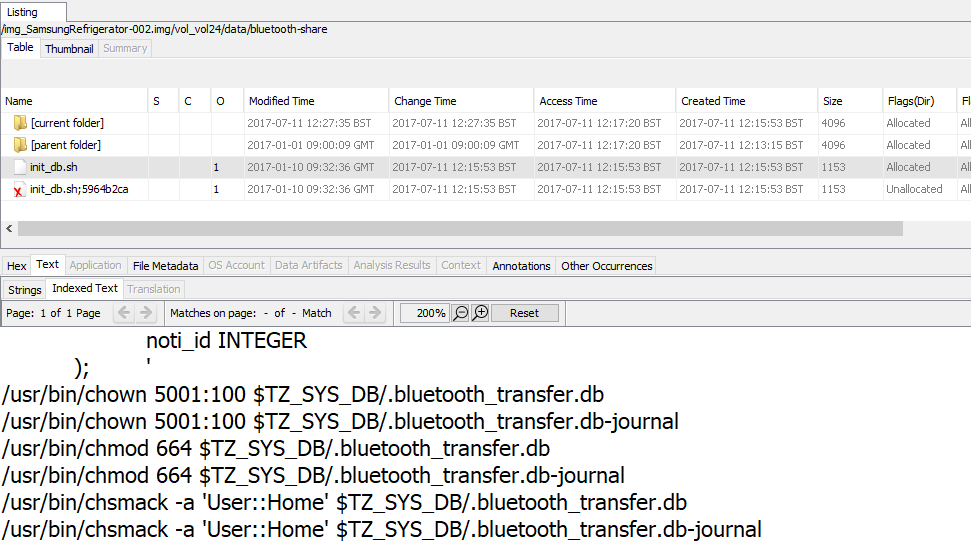
En esta ruta podemos ver detalles del sistema operativo, el nombre de la distribución es Tizen y la versión es Mobile 3.0.

### **3.4 ¿El sistema tiene varios usuarios? En caso afirmativo indica cuáles son.**



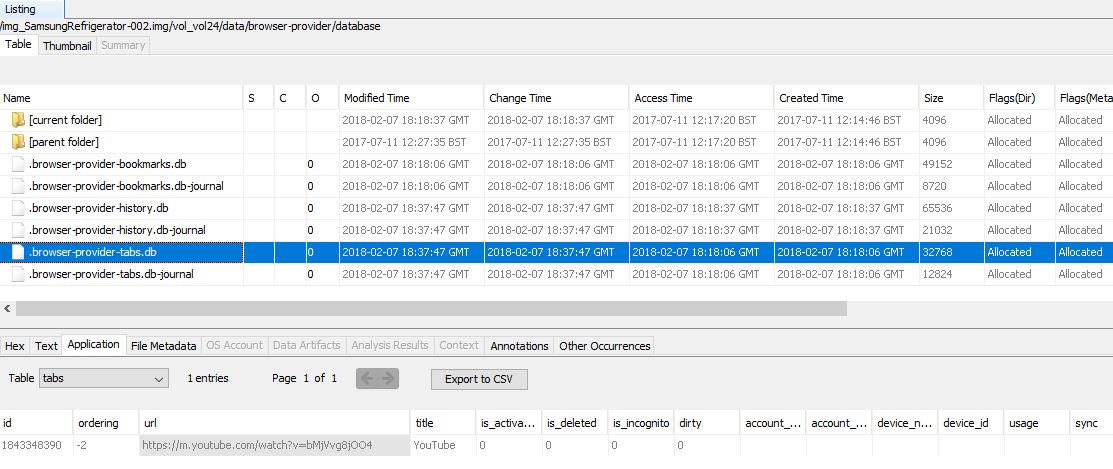
El sistema tiene dos cuentas de usuarios las cuales son: Owner y Guest.

### **3.5 ¿El refrigerador tiene servicio bluethoot? Justifica tu respuesta.**



Podemos observar como el sistema cuenta con directorios, archivos y bases de datos para el servicio bluetooth.

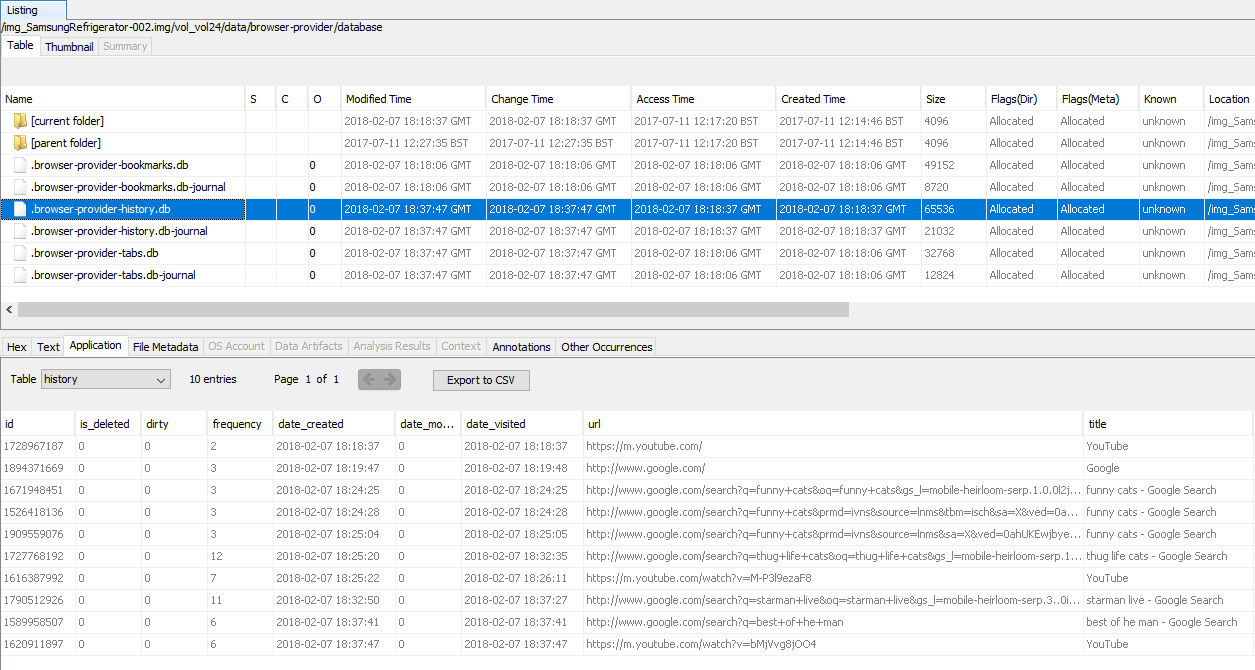
### **3.6 El dispositivo que estamos analizando permite la navegación en la web. ¿sabrías decir si tenía alguna pestaña abierta en el momento de realizar la adquisición? En caso afirmativo indica que estaba visualizando el usuario en dicha pestaña.**



Si permite la navegación web y contaba con una pestaña abierta en YouTube, con la siguiente url:

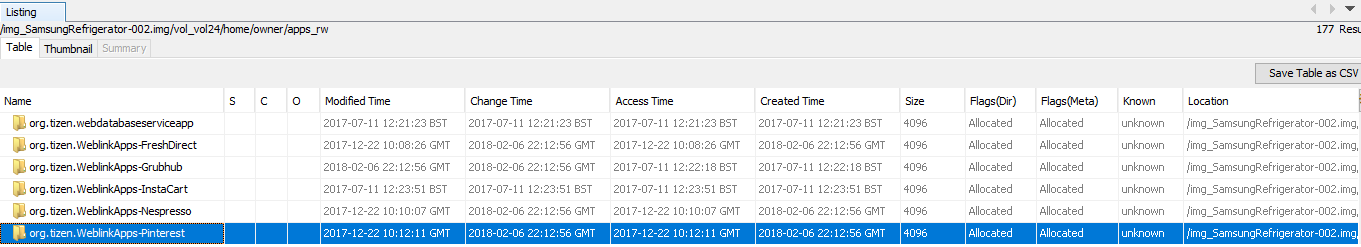
* https://m.youtube.com/watch?v=bMjVvg8jOO4

### **3.7 Si nos fijamos en el historial de búsqueda del navegador del refrigerador, veremos cuales son los intereses del usuario dueño de este dispositivo. ¿Cuáles eran estos intereses?**



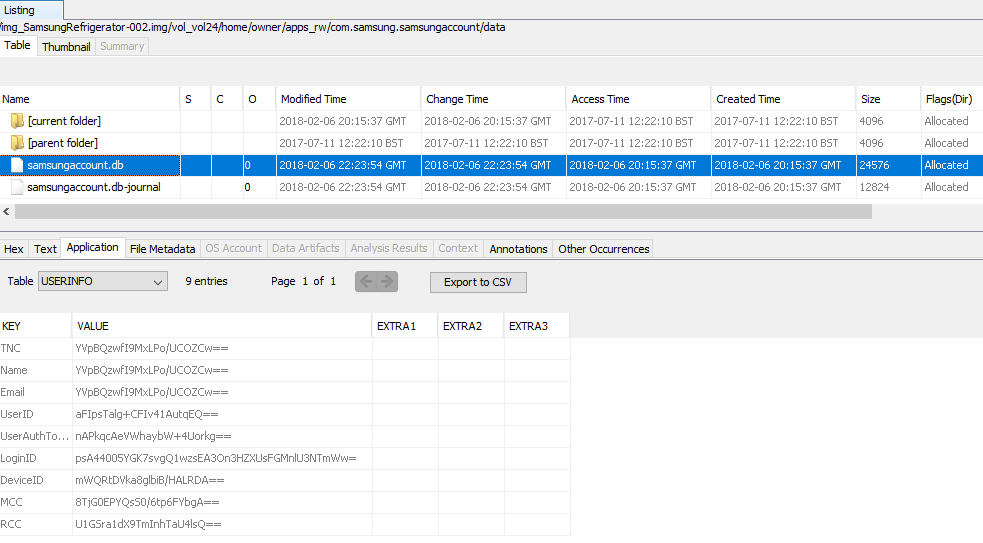
Podemos decir que sus intereses son: los gatos, he-man y starman.

### **3.8 Lista alguna de las aplicaciones a las que tiene acceso el usuario propietario. Al menos una de ellas ha de ser una aplicación de terceros bastante conocida.**



Podemos ver aplicaciones como: FreshDirect, Grubhub, InstaCart, Nespresso, Pinterest, etc…

### **3.9 ¿Cuál es el correo utilizado por el usuario para crear la cuenta Samsung del dispositivo?**



Esta es la información que nos encontramos en el directorio donde se almacenan los datos de la cuenta Samsung.

### **3.10 En el listado de aplicaciones del usuario propietario, hay una que se encarga de realizar fotografías al contenido del frigorífico. Indica la ruta donde se encuentran estas imágenes y pon capturas de algunas de ellas.**

