**Análisis de Adquisición de dispositivo iOS**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

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

[**2. Autopsy**](#_v6ng9pitg6de) **2**

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

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

[**3.1 Indica la versión de iOS que tenía instalado el dispositivo en el momento de la adquisición.**](#_th4wgnhox33t) **3**

[**3.2 Es fundamental saber cuándo fue la última vez que el dispositivo fue encendido. Encuentra este dato, documenta el proceso y muestra la fecha y hora en formato GMT.**](#_ixbbo99nuems) **3**

[**3.3 ¿Con cuántos tipos de dispositivos BlueTooth se ha establecido conexión y cuándo fue la última fecha de conexión con cada uno de ellos?**](#_o382tqzaray) **4**

[**3.4 ¿De qué país y estados eran las personas con las que el usuario del teléfono estableció comunicación mediante llamadas?**](#_bxjv6pkp4jed) **5**

[**3.5 ¿Cuál es la dirección del usuario con el que estableció una llamada de FaceTime**](#_78sc7hy4p1iu) **6**

[**3.6 ¿Cuál es el número de teléfono de la persona de la ciudad Goldsboro**](#_45qf75dxqdq8) **7**

[**3.7 ¿Qué mensaje se envió y que se quería compartir con ello? ¿Qué actividad podemos deducir que hacía el usuario en base a este mensaje? Pon capturas de lo que encuentres.**](#_7ksmhtmq6hcl) **7**

[**3.8 ¿En qué fecha y hora (en formato GMT) fue enviado un mensaje que tenía como archivo adjunto un documento pdf con el título “How was an iPhone set up?.pdf” ? Pon una captura del contenido del documento.**](#_o16uy2pclvuw) **8**

[**3.9 Se sospecha que el dueño del dispositivo recibió un código de verificación el 24 de marzo de 2020, a las 01:28:49. ¿Cuál era ese código y a que plataforma pertenecía?**](#_h56hq7is6x58) **9**

[**3.10 ¿Cuál es la dirección de correo del propietario del dispositivo al que le llegan los correos?**](#_e5clcx58nwvc) **9**

[**3.11 En la galería de fotos del dispositivo se encuentra una foto tomada el 12 de abril de 2020 a las 11:25.**](#_1j43gcydu3ro) **10**

[**3.12 Según una captura de pantalla que hay en la galería, ¿Cómo se llama el nombre del álbum que estuvo escuchando el dueño del dispositivo en algún momento?**](#_a544w2embs5b) **11**

[**3.13 ¿Cuál es el nombre del SSID de la red local a la que se conectó el dispositivo?**](#_ozp2wjgml7rb) **12**

[**3.14 Averigua la última localización buscada por el usuario, indica la fecha en que se realizó la búsqueda, así como la latitud y la longitud, e incluye dos capturas de pantalla de google maps sobre la ubicación encontrada, una vista desde arriba y otra en modo street view. ¿Qué pretendía hacer posiblemente el usuario?**](#_a331k7f0v4ym) **13**

[**3.15 ¿Cuándo fue la última vez que el usuario puso el dispositivo en modo “no molestar”?**](#_4uzszp3m7ea2) **14**

[**3.16 Indica el modelo del único USB conectado al dispositivo.**](#_2n3ur1khk4ww) **14**

[**3.17 Escribe el listado de marcadores que tiene el usuario en el navegador predeterminado:**](#_9z7wkf8ba6nl) **14**

[**3.18 Fijándonos en el historial de navegación del usuario y en las páginas más visitadas, ¿cuál es la principal afición del usuario y su principal preocupación?**](#_o5xj4f92c3on) **15**

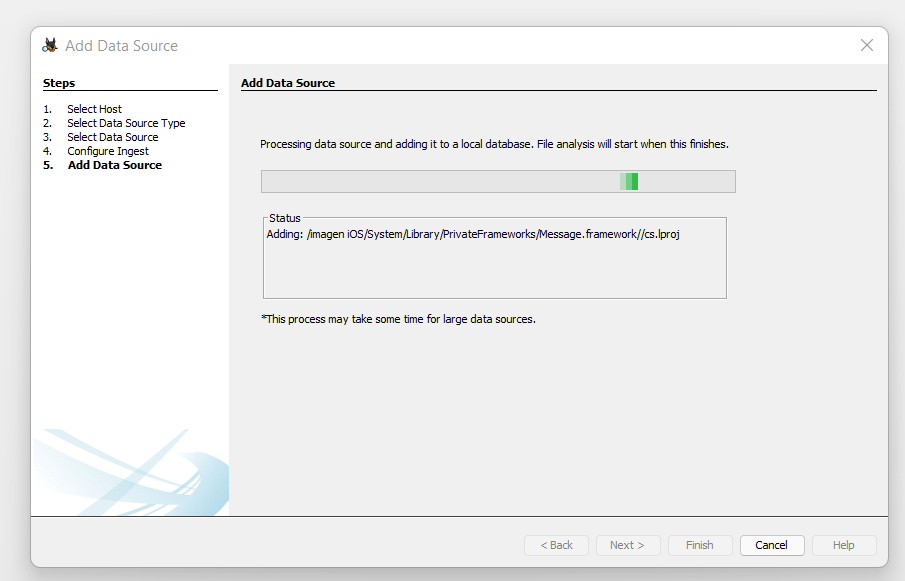
[**3.19 ¿Cuándo fueron accedidas por última vez las páginas más visitadas por parte del usuario?**](#_c37gfium7dfb) **15**

[**3.20 Indica cuál es la web que el usuario mantenía en una pestaña inactiva del navegador y que visitó por última vez el 28 de Marzo de 2020 a las 1:45:11**](#_q3b3p1x5kccq) **16**

[**4. Bibliografía**](#_fem0qc2tzi9b) **17**

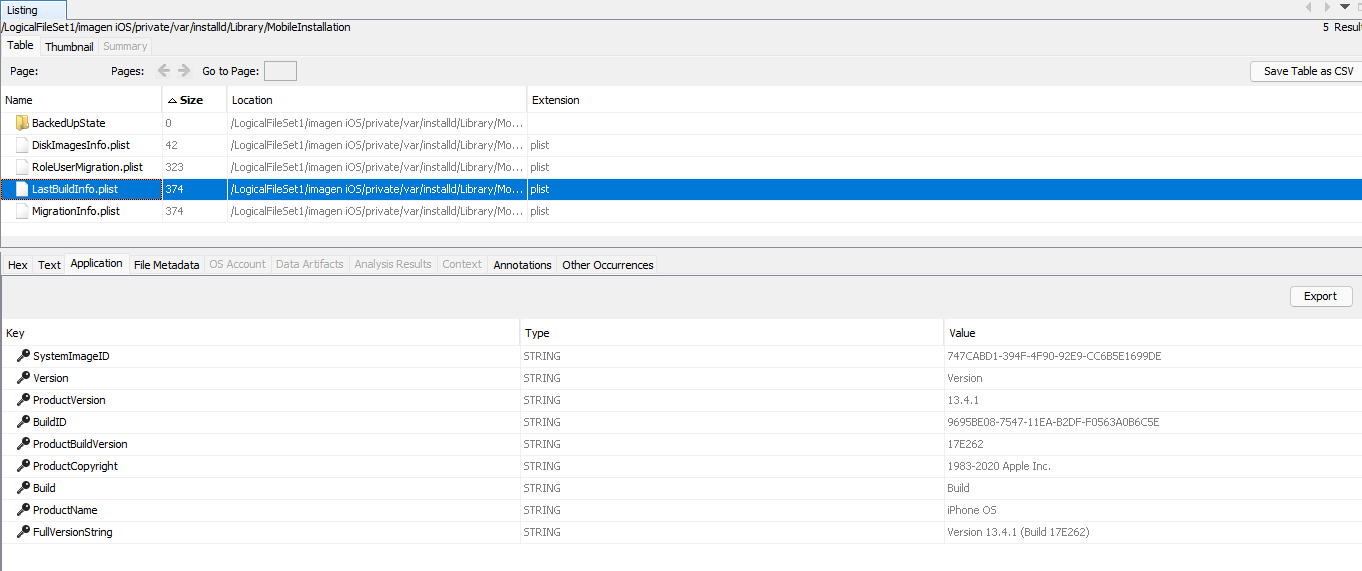
# **2. Autopsy**

### **2.1 Creación del caso:**



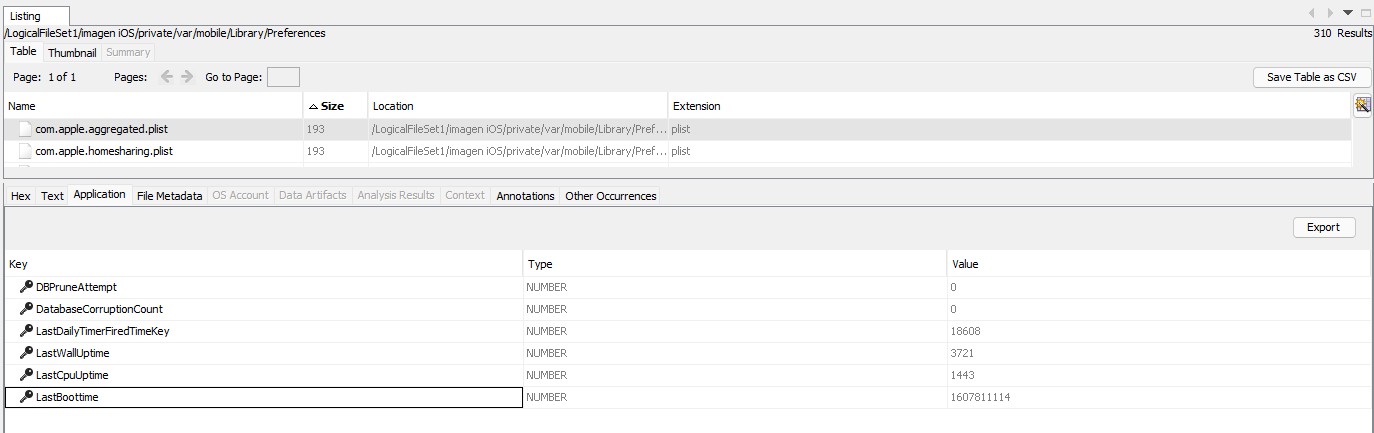
# **3. Cuestiones**

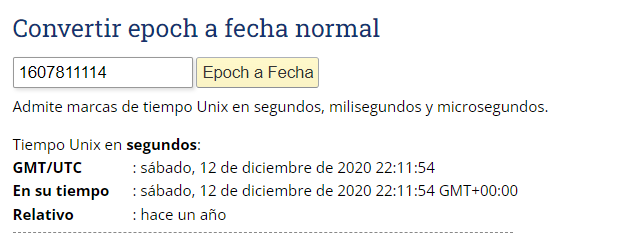
### **3.1 Indica la versión de iOS que tenía instalado el dispositivo en el momento de la adquisición.**



### **3.2 Es fundamental saber cuándo fue la última vez que el dispositivo fue encendido. Encuentra este dato, documenta el proceso y muestra la fecha y hora en formato GMT.**

**Valor LastBoot.**

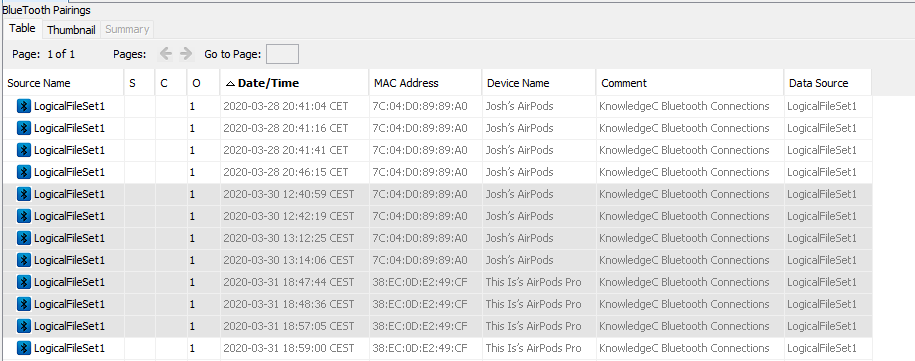




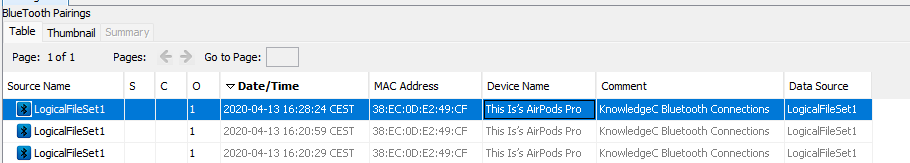
### **3.3 ¿Con cuántos tipos de dispositivos BlueTooth se ha establecido conexión y cuándo fue la última fecha de conexión con cada uno de ellos?**

En DataArtefacts -> Bluetooth Pairings.

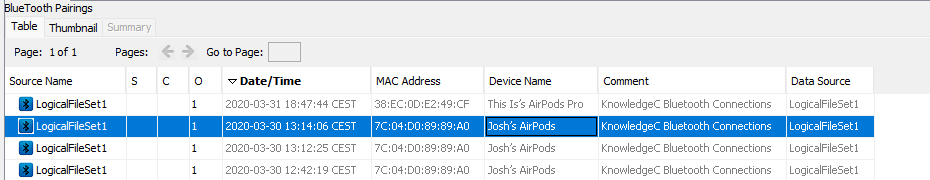
**2 Dispositivos.**



**Última conexión This is AirPods Pro:**



**Última conexión JohnAirPods:**

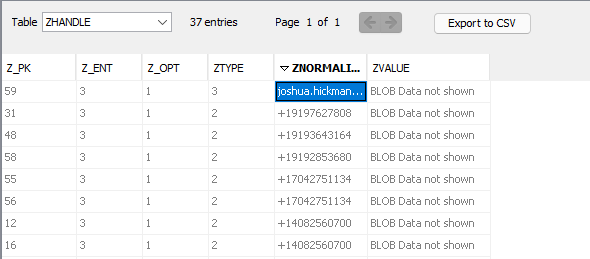


### **3.4 ¿De qué país y estados eran las personas con las que el usuario del teléfono estableció comunicación mediante llamadas?**

Lista de números:

### 

Haciendo uso de CallHistory.storedata db:



Haciendo uso de la base de datos podemos conseguir averiguar la ubicación:

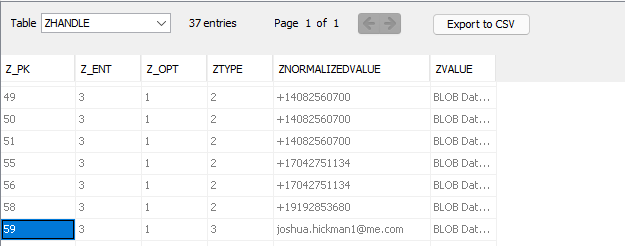


### **3.5 ¿Cuál es la dirección del usuario con el que estableció una llamada de FaceTime**

Haciendo uso de CallHistory.storedata db:

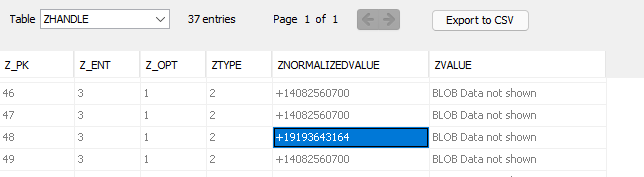
### 

Dirección del usuario asociado:



### **3.6 ¿Cuál es el número de teléfono de la persona de la ciudad Goldsboro**

Numero de telefono:



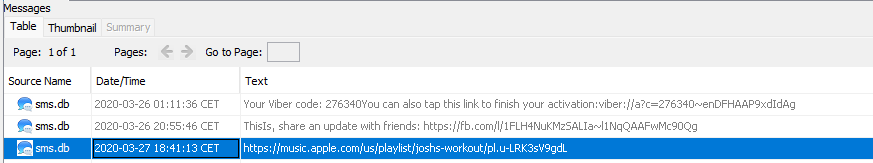
Ubicación e identificación:

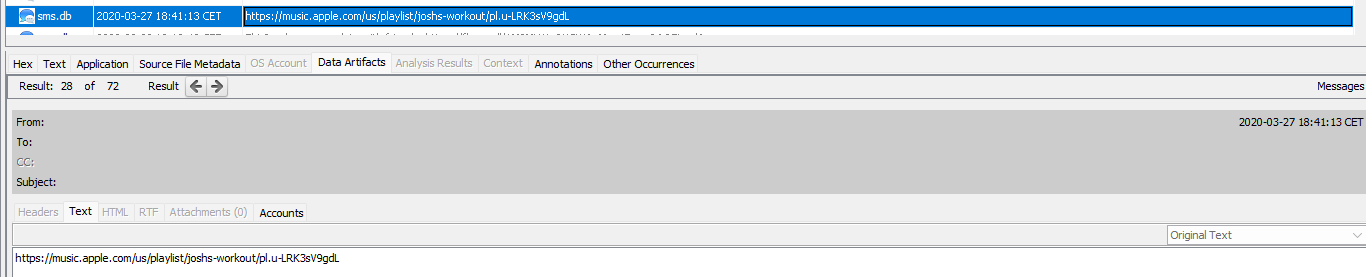


### 

### **3.7 ¿Qué mensaje se envió y que se quería compartir con ello? ¿Qué actividad podemos deducir que hacía el usuario en base a este mensaje? Pon capturas de lo que encuentres.**

El 27 de marzo de 2020 a las 18:41:13 se recibió un mensaje por la aplicación de Mensaje.





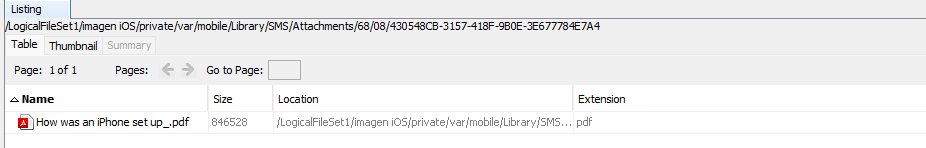
Podemos ver que el contenido del mensaje: se trata de un enlace.

### 

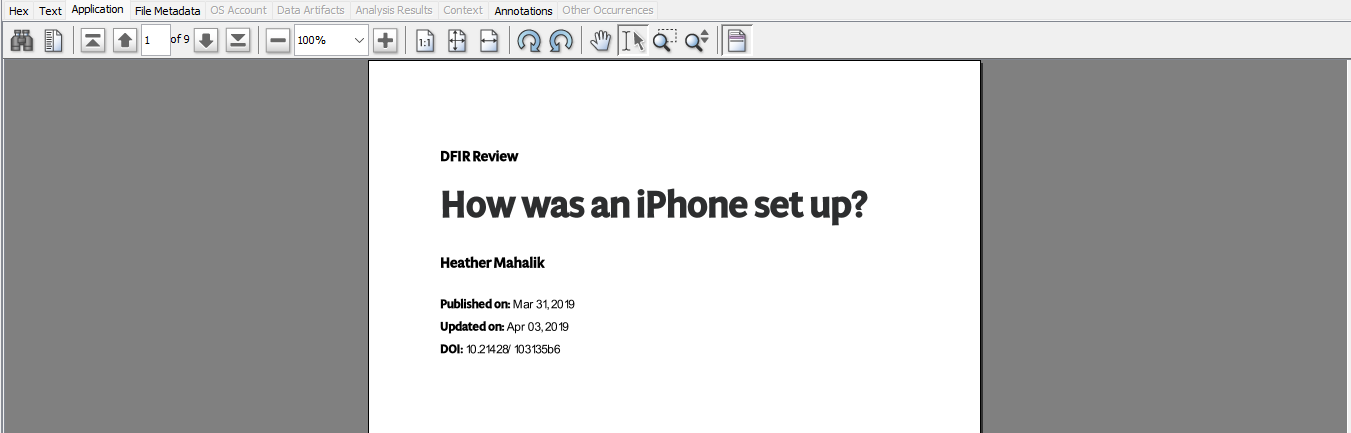
### **3.8 ¿En qué fecha y hora (en formato GMT) fue enviado un mensaje que tenía como archivo adjunto un documento pdf con el título “How was an iPhone set up?.pdf” ? Pon una captura del contenido del documento.**

Revisando la base de datos obtenemos el mensaje donde se adjunta dicho archivo:

### 



Lo visualizamos:

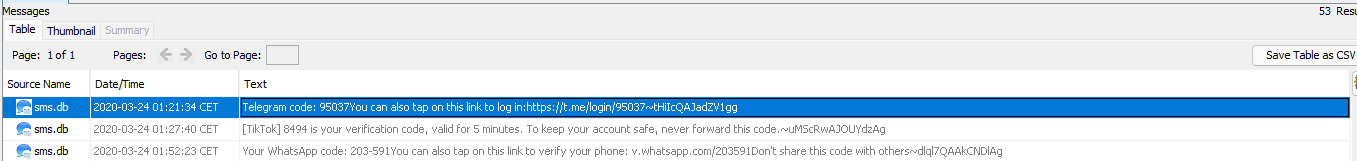


### **3.9 Se sospecha que el dueño del dispositivo recibió un código de verificación el 24 de marzo de 2020, a las 01:28:49. ¿Cuál era ese código y a que plataforma pertenecía?**

Accediendo a través de Data Artifacts -> Messages

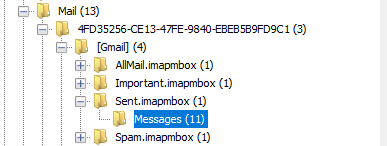
Observamos los diferentes mensajes recibidos.

Se trata de la plataforma Tiktok.

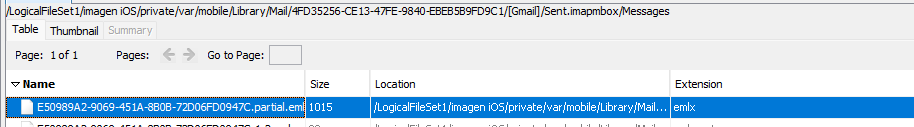
****

### **3.10 ¿Cuál es la dirección de correo del propietario del dispositivo al que le llegan los correos?**

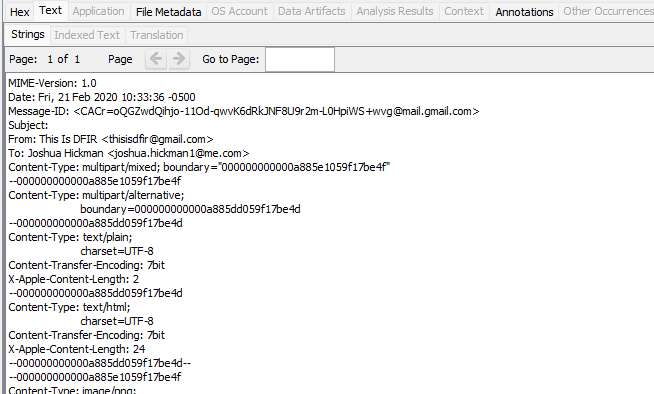
Navegamos hasta donde se guardan los correos enviados desde Gmail.



Analizamos los distintos correos electrónicos



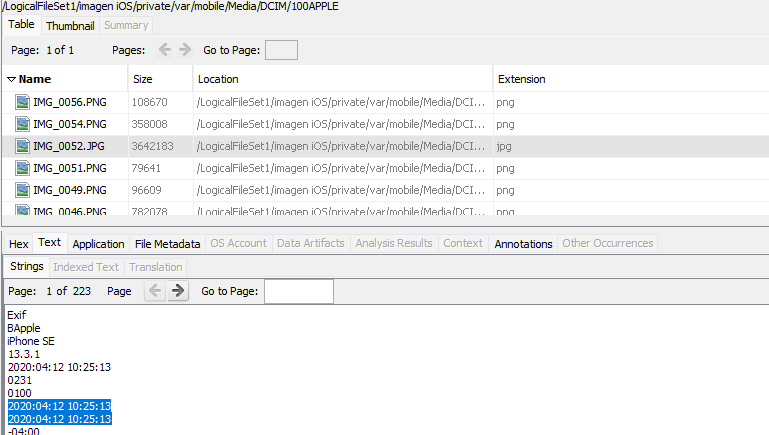
Podemos observar tanto el emisor como el receptor de dicho correo



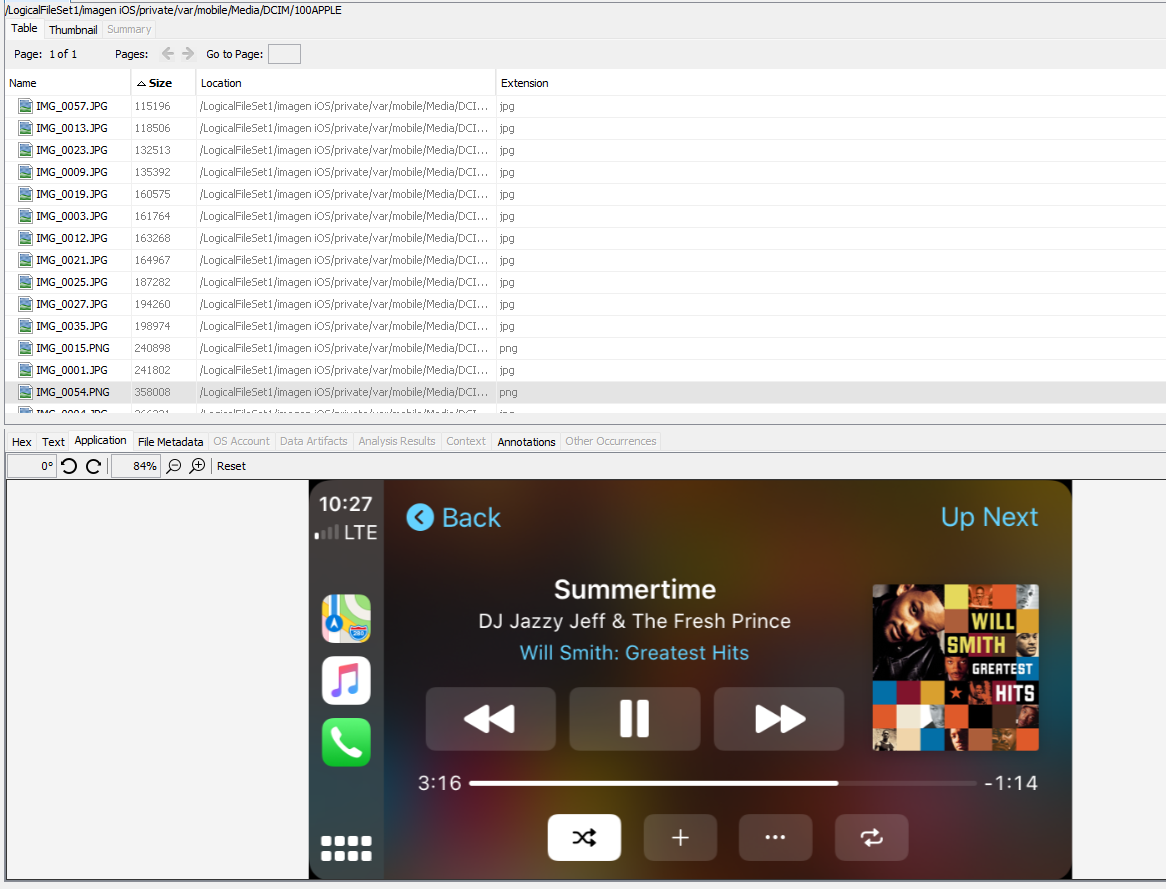
### 

### 

### **3.11 En la galería de fotos del dispositivo se encuentra una foto tomada el 12 de abril de 2020 a las 11:25.**



### **3.12 Según una captura de pantalla que hay en la galería, ¿Cómo se llama el nombre del álbum que estuvo escuchando el dueño del dispositivo en algún momento?**



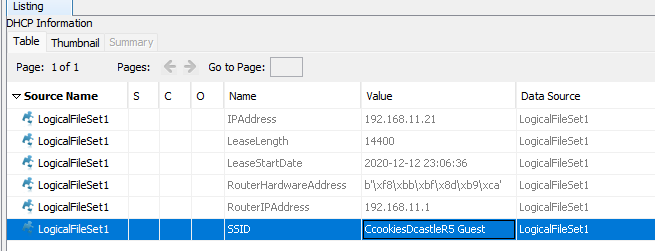
Will Smith: Greatest Hits

### **3.13 ¿Cuál es el nombre del SSID de la red local a la que se conectó el dispositivo?**

Accediendo a Data Artifacts -> DHCP Information

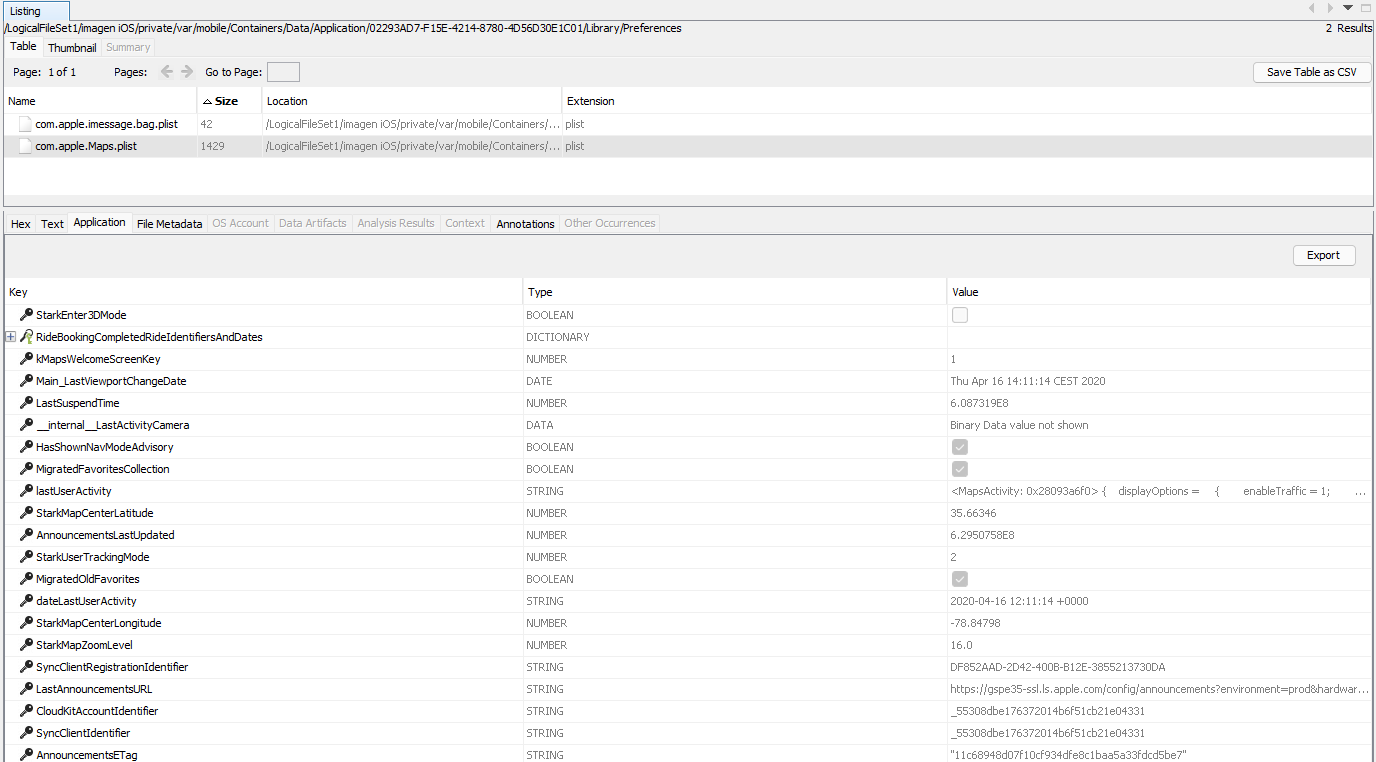
Observamos el SSID de la red.

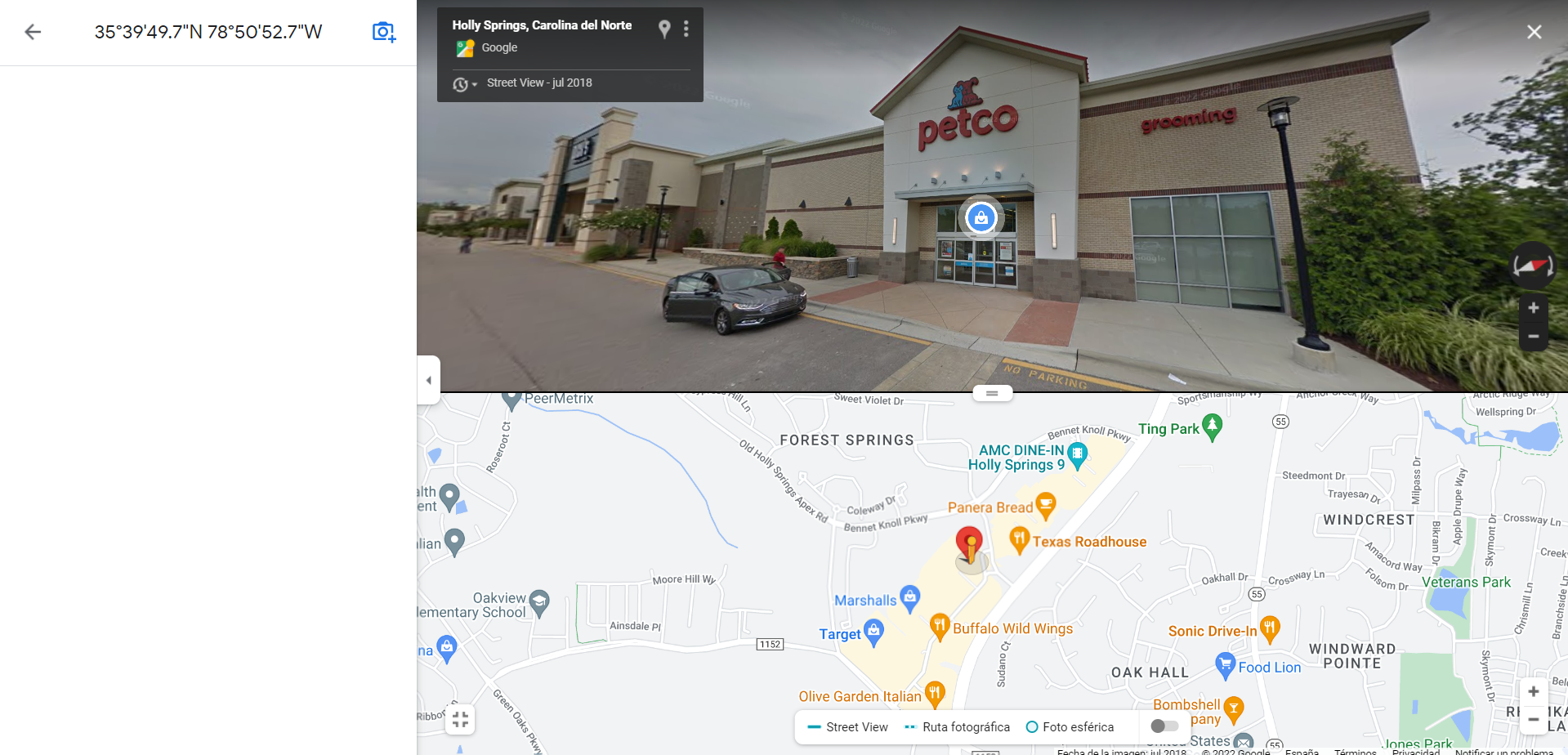
### 



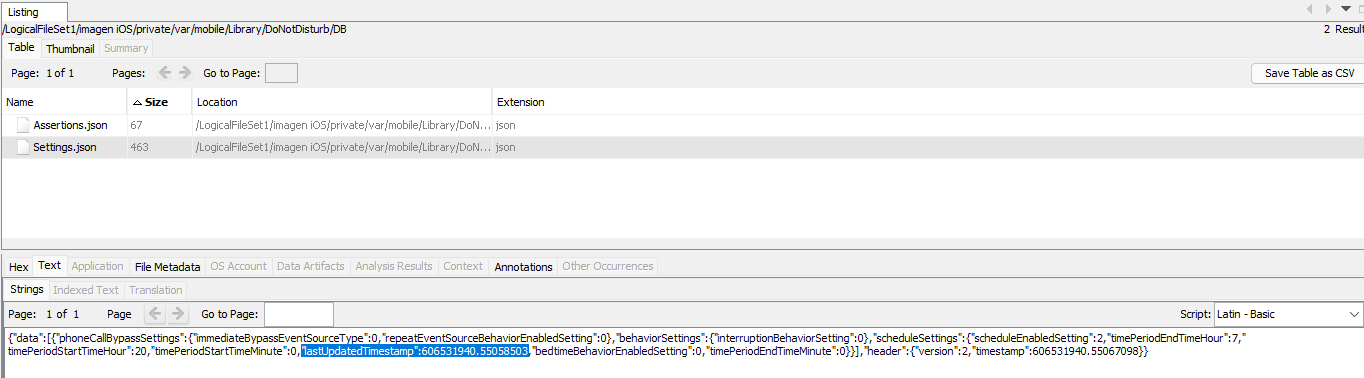
### **3.14 Averigua la última localización buscada por el usuario, indica la fecha en que se realizó la búsqueda, así como la latitud y la longitud, e incluye dos capturas de pantalla de google maps sobre la ubicación encontrada, una vista desde arriba y otra en modo *street view*. ¿Qué pretendía hacer posiblemente el usuario?**

Saber cuál fue la última ubicación que buscó el usuario nos puede resultar de gran interés para sacar conclusiones sobre las últimas acciones que realizó el usuario.



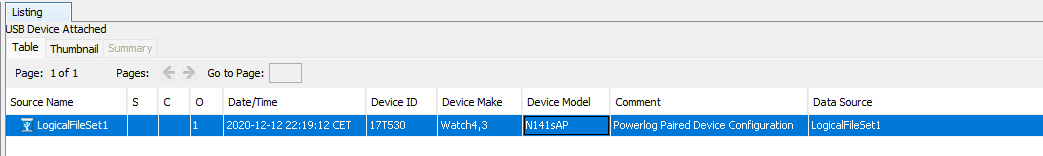


### **3.15 ¿Cuándo fue la última vez que el usuario puso el dispositivo en modo “no molestar”?**



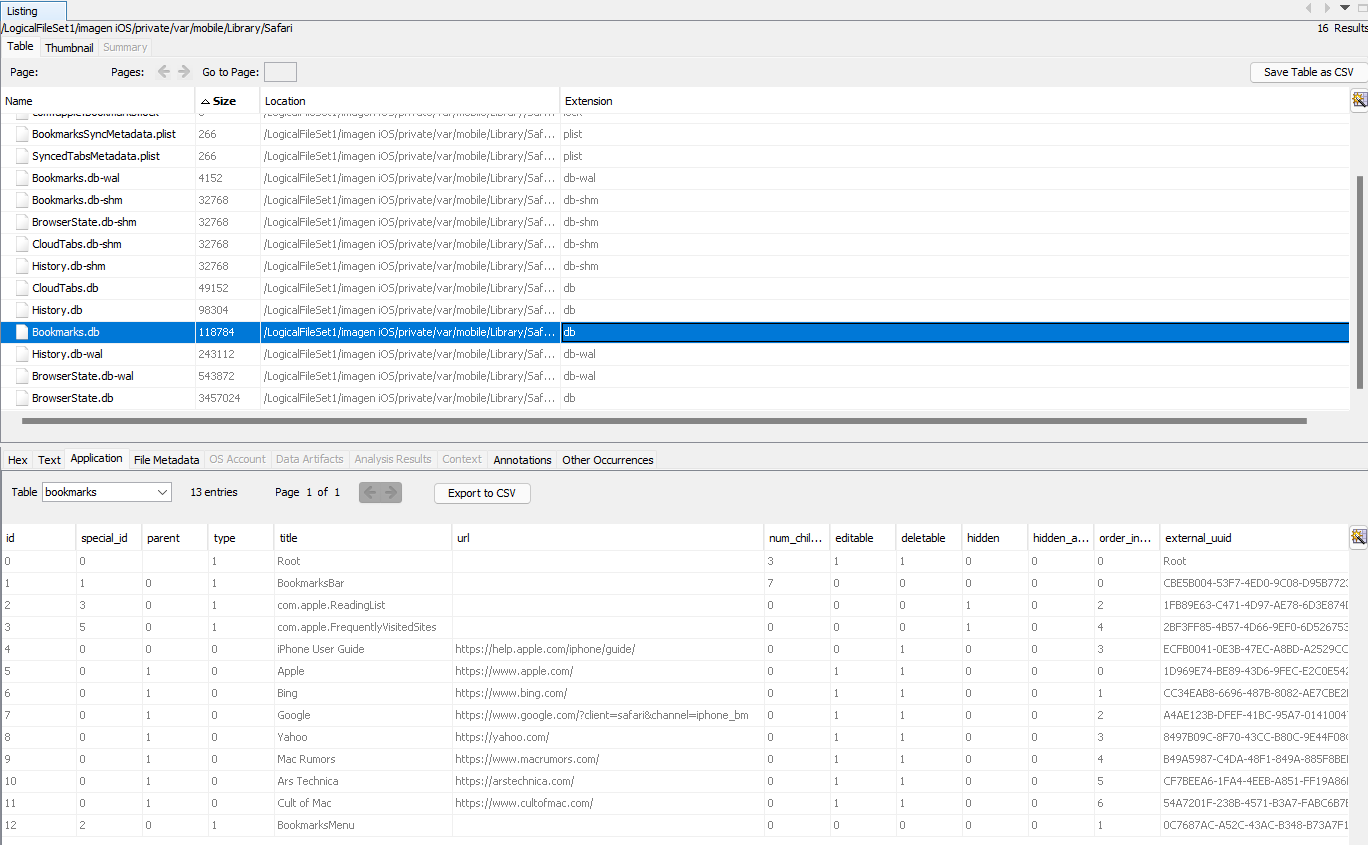
### **3.16 Indica el modelo del único USB conectado al dispositivo.**

Dentro de Data Artifacts -> USB Device Attached



### **3.17 Escribe el listado de marcadores que tiene el usuario en el navegador predeterminado:**

Utilizando la base de datos bookmarks.db



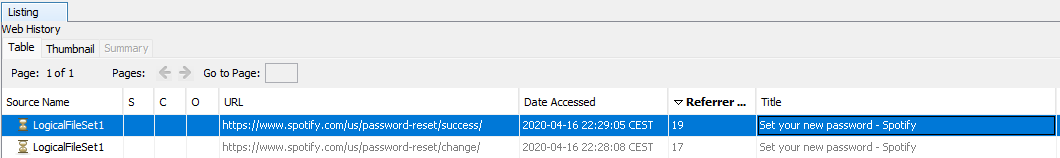
### **3.18 Fijándonos en el historial de navegación del usuario y en las páginas más visitadas, ¿cuál es la principal afición del usuario y su principal preocupación?**

### 

La afición se trata del béisbol y su preocupación cuando se reanudará la MLB.

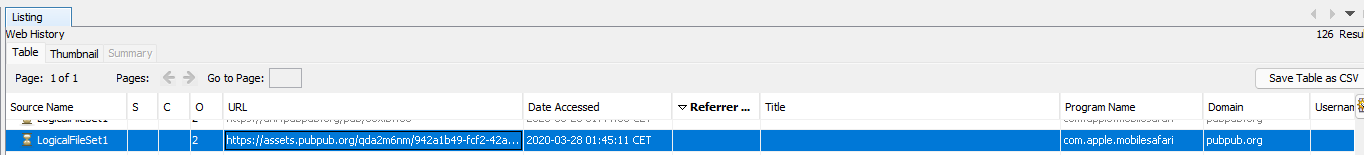
### **3.19 ¿Cuándo fueron accedidas por última vez las páginas más visitadas por parte del usuario?**

Desde Data Artifacts -> Web History



### **3.20 Indica cuál es la web que el usuario mantenía en una pestaña inactiva del navegador y que visitó por última vez el 28 de Marzo de 2020 a las 1:45:11**

Por regla general, cuando una página que visitamos nos interesa no la cerramos, sino que realizamos dos tipos de acciones. Una sería agregar a marcadores del navegador, y otra es mantenerla abierta en una pestaña del navegador por si la queremos visitar más adelante.



# **4. Bibliografía**

<https://www3.gobiernodecanarias.org/medusa/evagd/stacruztf/pluginfile.php/700250/mod_resource/content/1/Poster%20AnA%CC%83%C2%A1lisis%20Forense%20en%20Smartphones.pdf>

<https://docs.google.com/presentation/d/1hhd99NgWRTL9wmZkRqDxtVPSnQBAzeOYMZigP0JLqro/edit#slide=id.p>

<https://www.google.es/maps/place/35%C2%B039'49.7%22N+78%C2%B050'52.7%22W/@35.6638099,-78.8501609,17z/data=!3m1!4b1!4m5!3m4!1s0x0:0xcd3f153bb051aeff!8m2!3d35.6638056!4d-78.8479722?hl=es>