**Análisis de Adquisición de dispositivo Android**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

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

[**2. Autopsy**](#_6cjeyhiwgeys) **2**

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

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

[**3.1 ¿Cuál es el código de verificación de la app de mensajería Wickr Me que se recibió por sms? ¿Cuándo fue recibido este mensaje? Indica la fecha completa (día, mes, año y hora) en formato estándar GMT.**](#_th4wgnhox33t) **3**

[**3.2 El 15 de marzo de 2019, a las 19:16, el usuario del teléfono realizó una llamada. ¿Con qué estado/región se contactó en esa ocasión? ¿Cuánto duró esa llamada?**](#_sxx6r130kmyi) **3**

[**3.3 Se ha localizado una cookie, de nombre “cid”, relacionada con una empresa que gestiona pagos en internet llamada stripe.com. Indica claramente el valor de esta cookie y cuándo fue accedida por última vez, usando un formato de dd/mm/yyyy, hh/mm/ss, en GMT**](#_twuiszy17vvv) **4**

[**3.4 ¿Cuál es el sitio web que ha sido visitado durante más tiempo en el navegador Chrome?**](#_cxj7w3py88ij) **5**

[**3.5 Investiga en qué formato se muestra el tiempo de visita de cada página e indica durante cuántos minutos se estuvo visitando esta página**](#_tfk8t96rp3jk) **6**

[**3.6 ¿Cuál fue la última página en la que el usuario hizo login en chrome?**](#_jp8a8am9nmbq) **7**

[**3.7 ¿A qué hora fue tomada la foto de Darth Vader?**](#_b532klpvhaf3) **7**

[**3.8 ¿Qué mensaje de estado tiene Josh Hickman en Whatsapp?**](#_bqjtfrisf880) **8**

[**3.9 ¿El usuario ha conectado a whatsapp en su versión web alguna vez?**](#_k61bgtfdr0ag) **8**

[**3.10 ¿Se ha enviado alguna imagen desde el whatsapp? Si es así, indica dónde has obtenido este dato y pon una captura de la imagen.**](#_qoe753juh1f) **8**

[**3.11 Parece que hay una conversación registrada en la app de Facebook. Indica los siguientes aspectos:**](#_zfqgkxisctg4) **9**

[**3.12 En caso de que el usuario tuviera instalada la app de Telegram, ¿Cuántas cuentas tendría configuradas en el dispositivo?**](#_4gyjfj6lnbv) **11**

[**3.13 Un colaborador ha informado de que se ha usado Telegram para intercambiar una imagen con una ubicación que podría ser relevante para el caso. ¿Cuál es esa imagen?**](#_sn03hez9c8dj) **11**

[**3.14 Se ha observado que el usuario utilizaba la app de Instagram en el dispositivo. Indica la fecha y hora exactas (GMT) a la que se inició por última vez una videollamada en esta plataforma.**](#_dsihn7lgirln) **12**

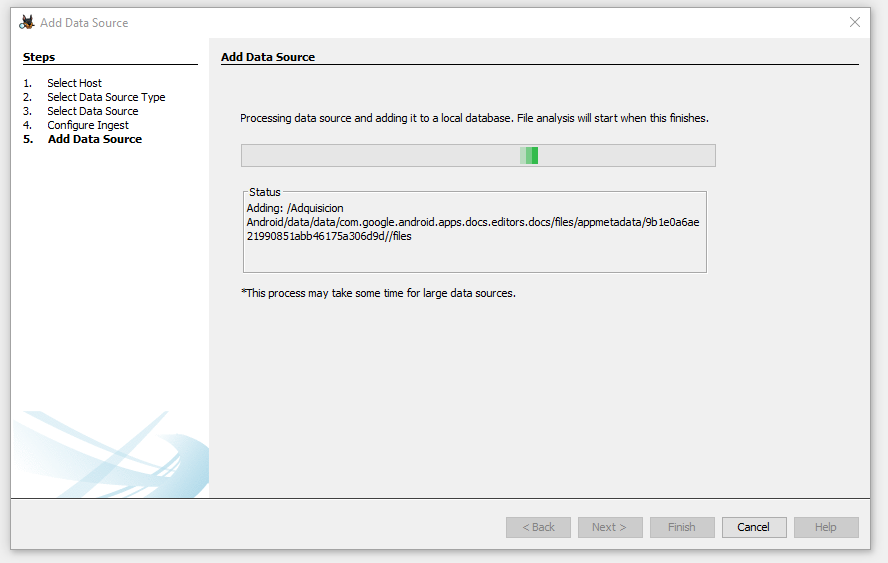
[**3.15 ¿Ha subido el usuario alguna foto a Instagram? Si es así, pon una captura de la foto.**](#_ninrsqlq45x5) **12**

[**3.16 Se ha detectado que el usuario del dispositivo ha estado usando una app llamada TextNow**](#_h3hv5exce961) **13**

[**3.17 Uno de los contactos de Twitter que tenía el usuario en su dispositivo tiene un “user\_id” con el valor “1077826757519073281”.**](#_igpl3vfhajjr) **14**

# **2. Autopsy**

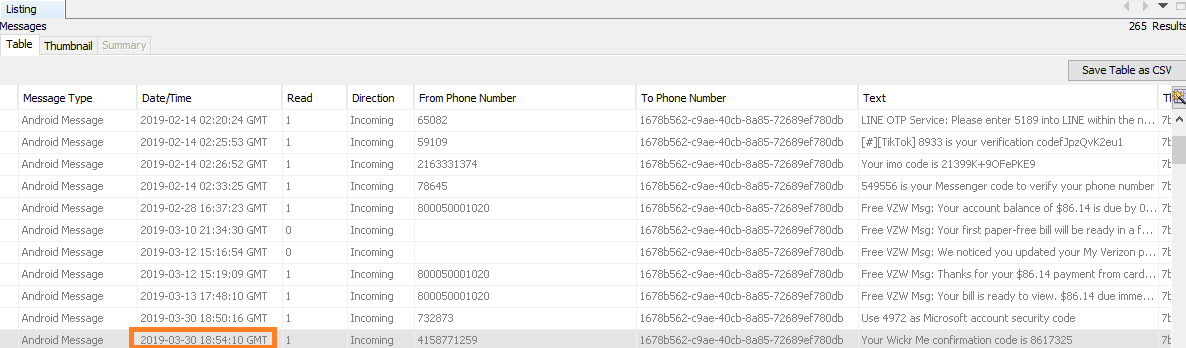
### **2.1 Creación del caso:**



Añadimos la fuente de evidencia proporcionada.

# **3. Cuestiones**

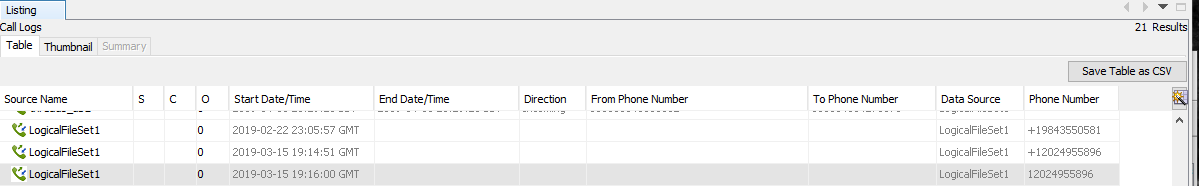
### **3.1 ¿Cuál es el código de verificación de la app de mensajería Wickr Me que se recibió por sms? ¿Cuándo fue recibido este mensaje? Indica la fecha completa (día, mes, año y hora) en formato estándar GMT.**

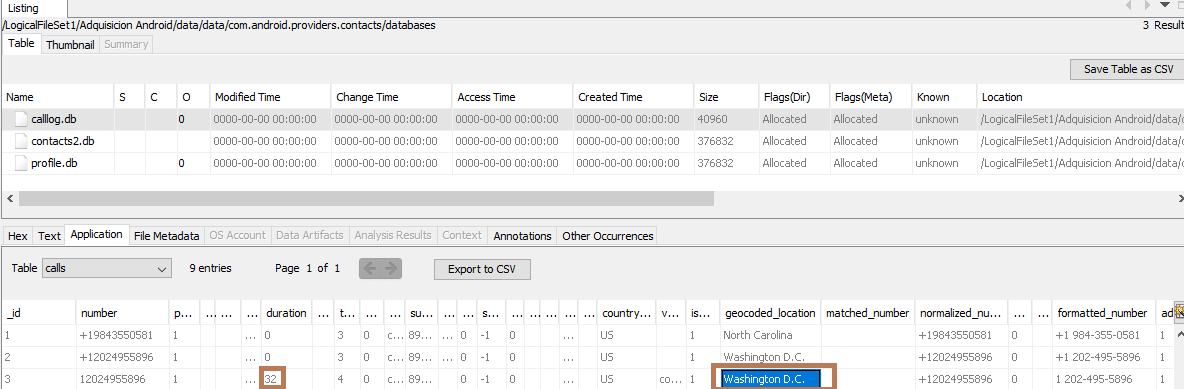


El codigo es: 8617325

2019-03-30 18:54:10 GMT

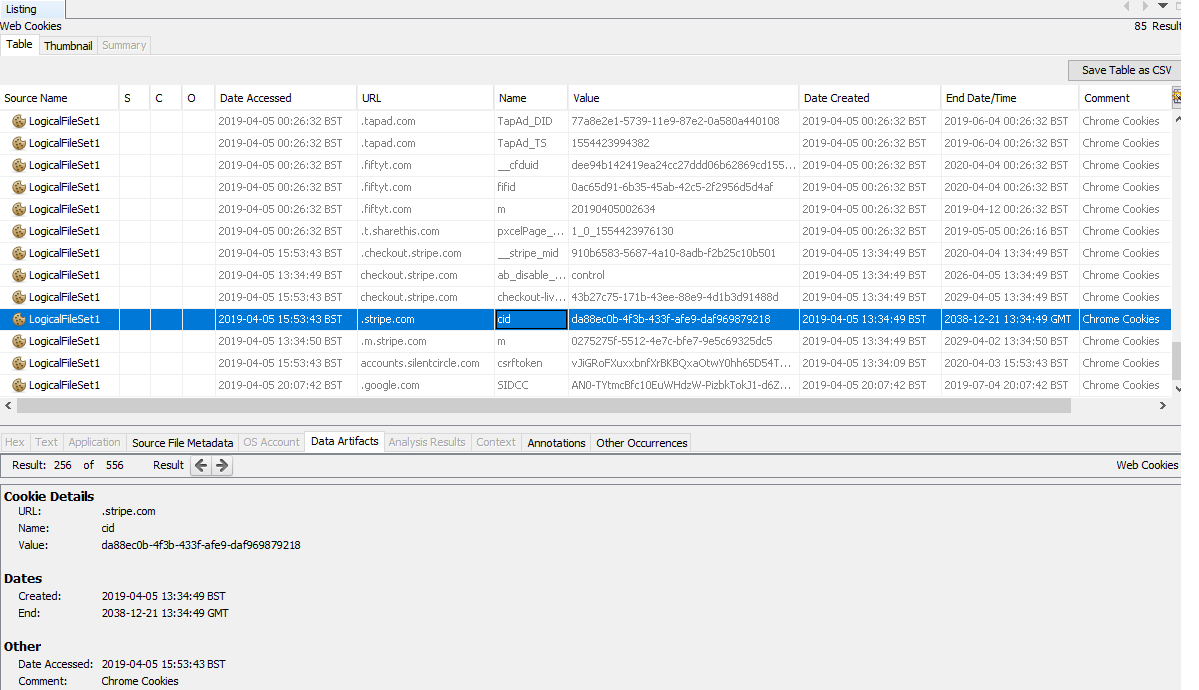
### **3.2 El 15 de marzo de 2019, a las 19:16, el usuario del teléfono realizó una llamada. ¿Con qué estado/región se contactó en esa ocasión? ¿Cuánto duró esa llamada?**



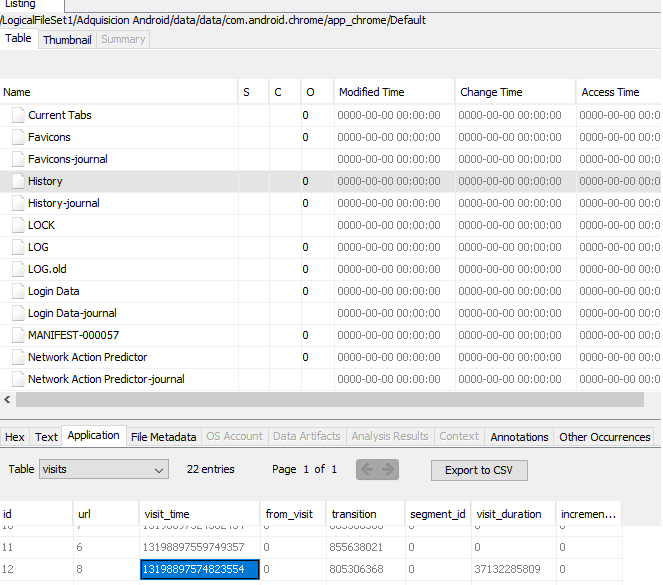


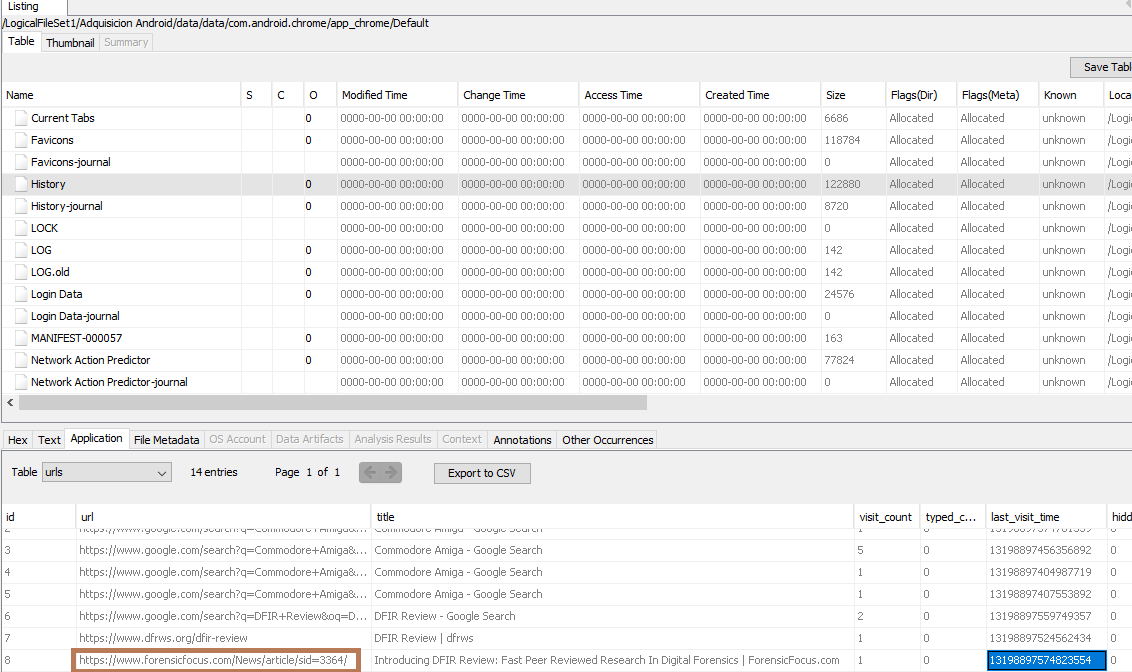
Contacto con Washington D.C y la duración fue de 32 minutos.

### **3.3 Se ha localizado una cookie, de nombre “cid”, relacionada con una empresa que gestiona pagos en internet llamada stripe.com. Indica claramente el valor de esta cookie y cuándo fue accedida por última vez, usando un formato de dd/mm/yyyy, hh/mm/ss, en GMT**



### **3.4 ¿Cuál es el sitio web que ha sido visitado durante más tiempo en el navegador Chrome?**

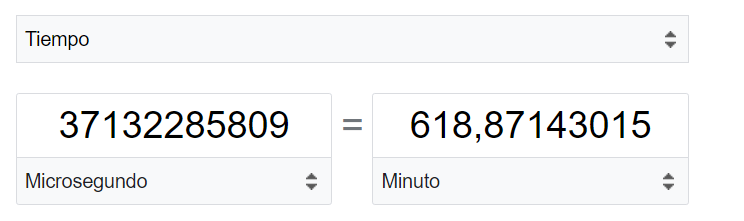




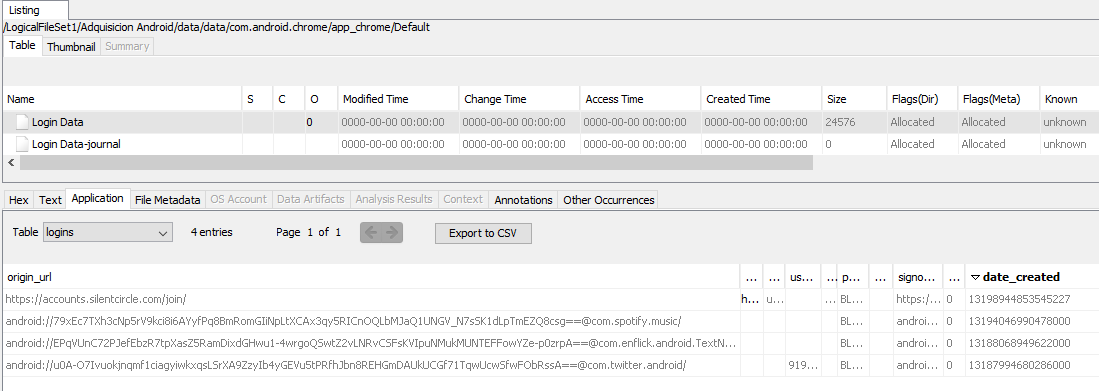
Se trata de: https://www.forensicfocus.com/News/article/sid=3364/

### **3.5 Investiga en qué formato se muestra el tiempo de visita de cada página e indica durante cuántos minutos se estuvo visitando esta página**

Chrome lo muestra en microsegundos, realizamos la conversión..

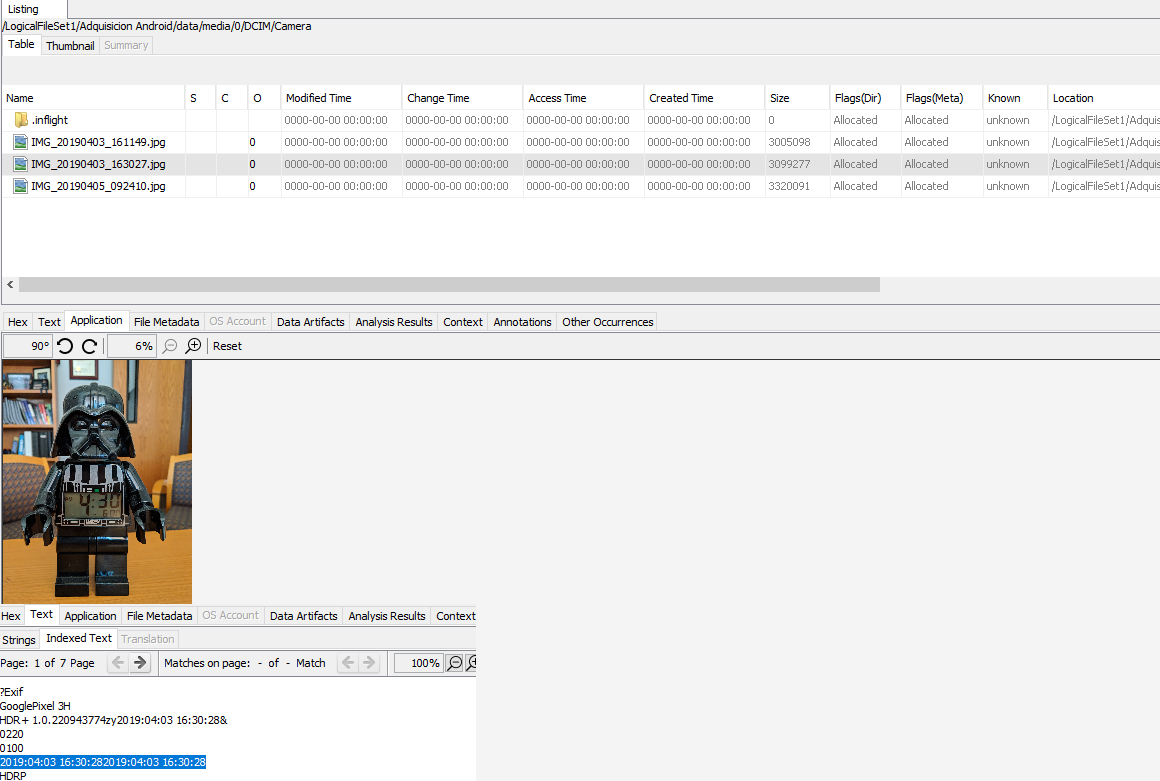


### **3.6 ¿Cuál fue la última página en la que el usuario hizo login en chrome?**

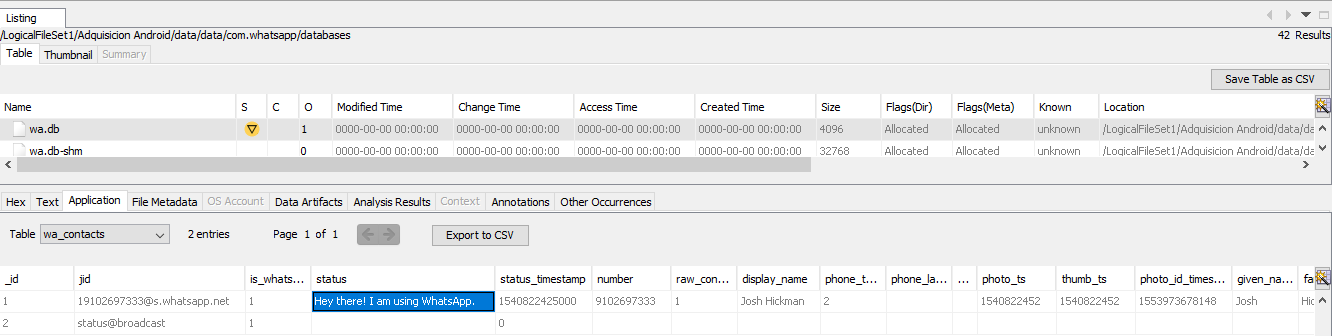


La última pagina es: https://accounts.silentcircle.com/join/

### **3.7 ¿A qué hora fue tomada la foto de Darth Vader?**

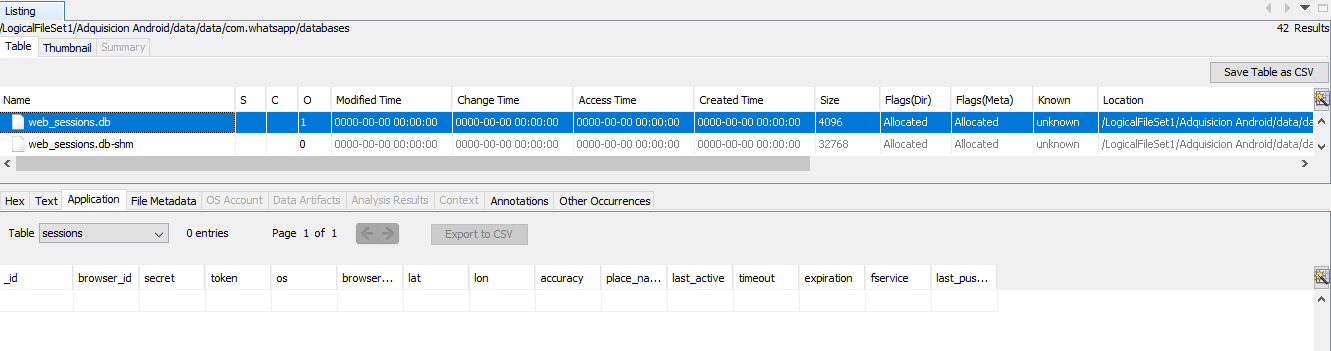


### **3.8 ¿Qué mensaje de estado tiene Josh Hickman en Whatsapp?**



Posee el mensaje de estado: “Hey there! I am using WhatsApp.”

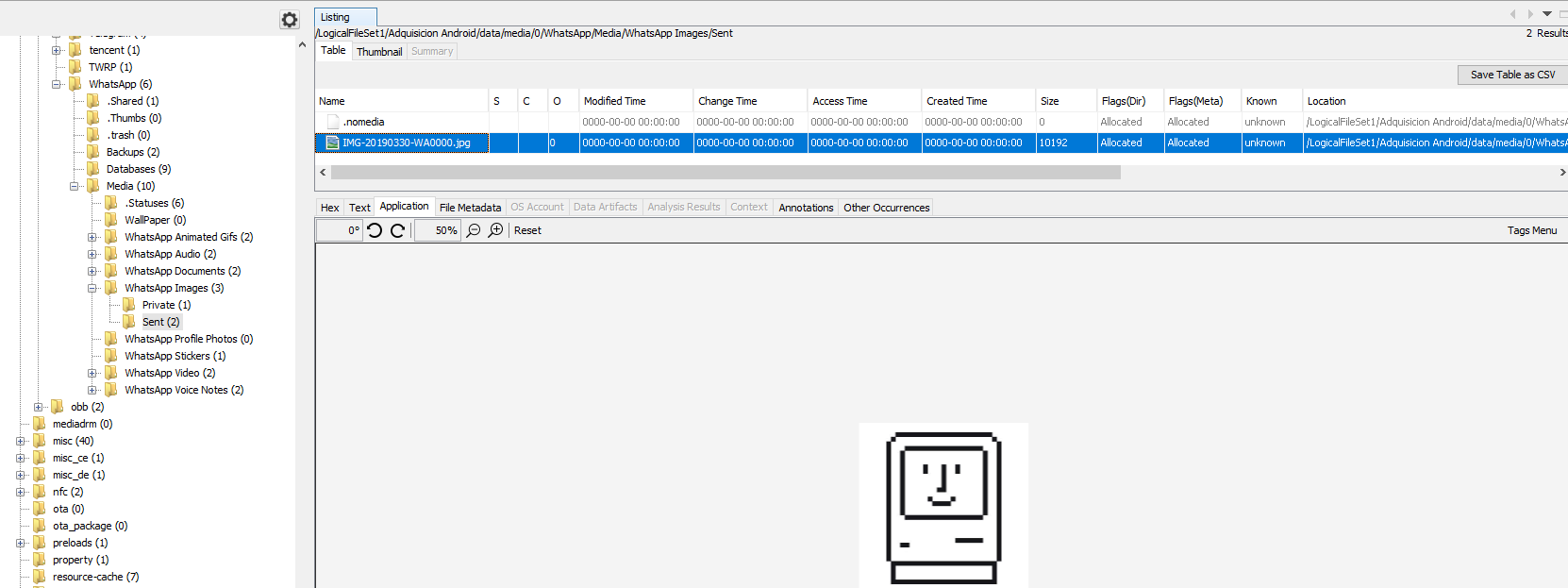
### **3.9 ¿El usuario ha conectado a whatsapp en su versión web alguna vez?**



No se encuentran registros de ninguna sesión.

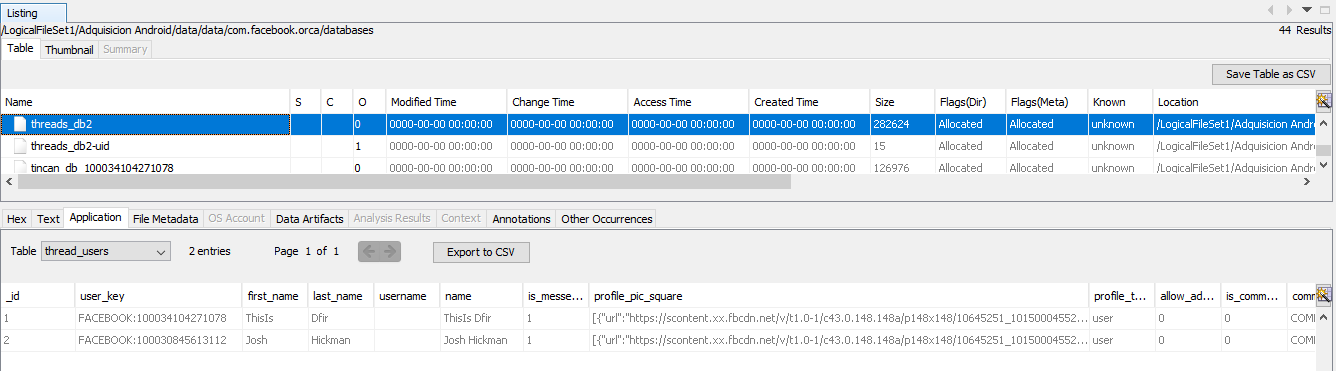
### **3.10 ¿Se ha enviado alguna imagen desde el whatsapp? Si es así, indica dónde has obtenido este dato y pon una captura de la imagen.**

Comprobando la ruta donde se almacenan las imágenes enviadas por la aplicación.

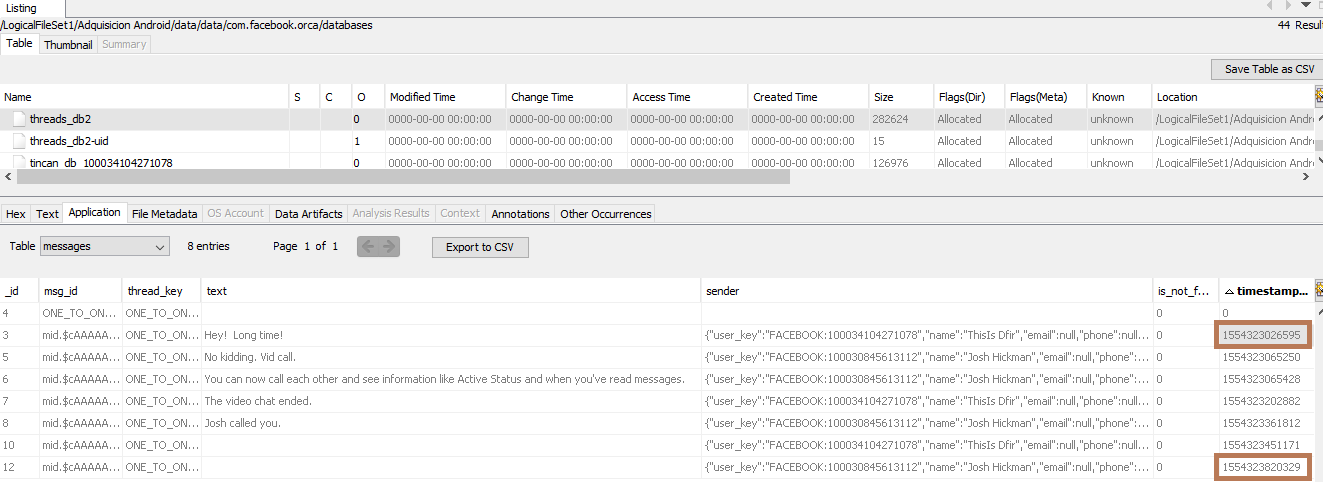


### **3.11 Parece que hay una conversación registrada en la app de Facebook. Indica los siguientes aspectos:**

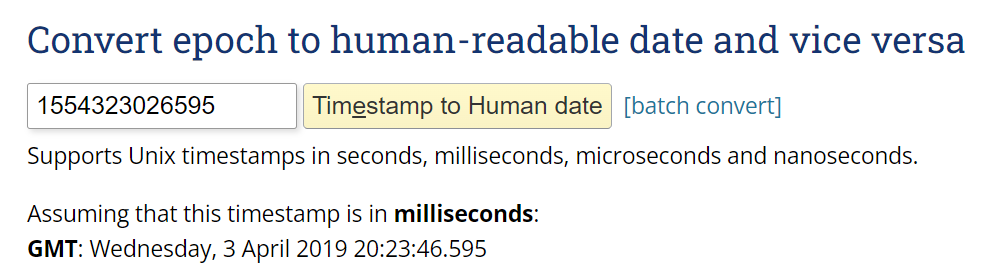
* Usuarios implicados en esta conversación.



* Hora de inicio y fin de esta conversación.



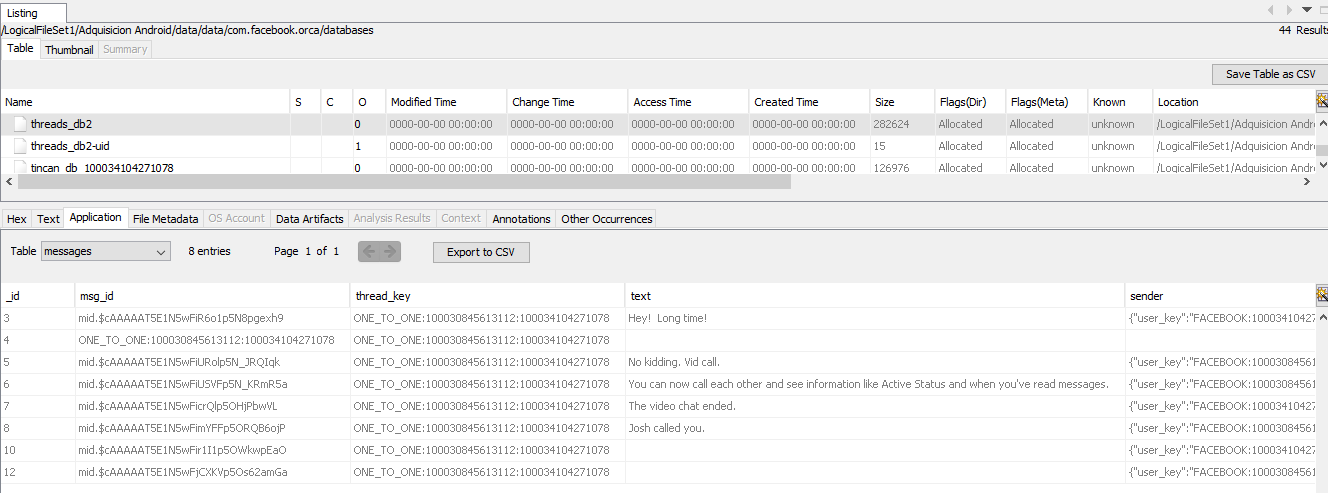
Inicio:



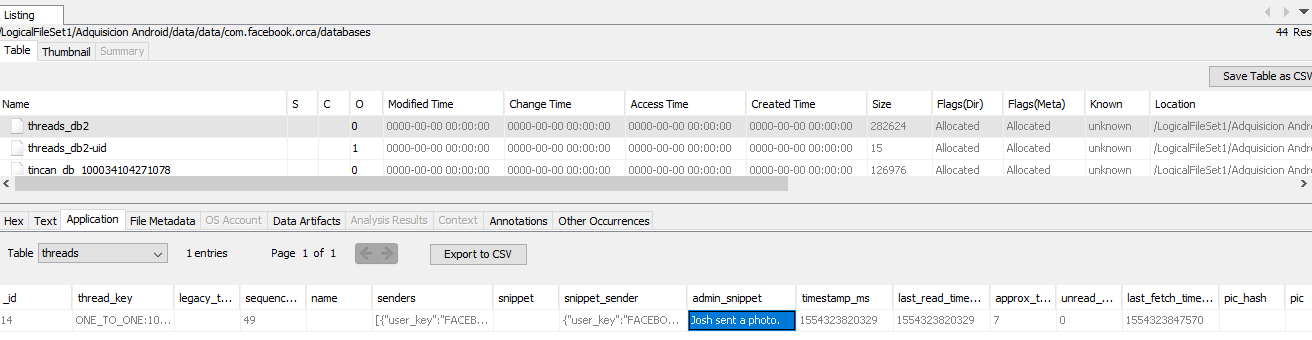
Final:



* Contenido de la conversación.

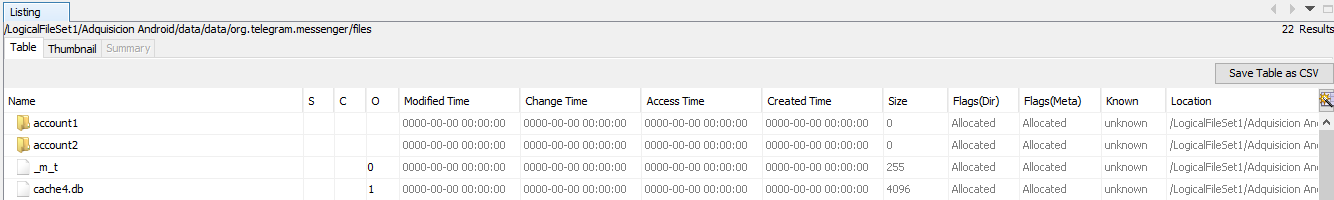


* Parece que se envió una foto en esa conversación. Basándonos en las evidencias que tenemos, ¿crees que la foto enviada se tomó en el momento de la conversación o ya estaba en la galería del usuario?



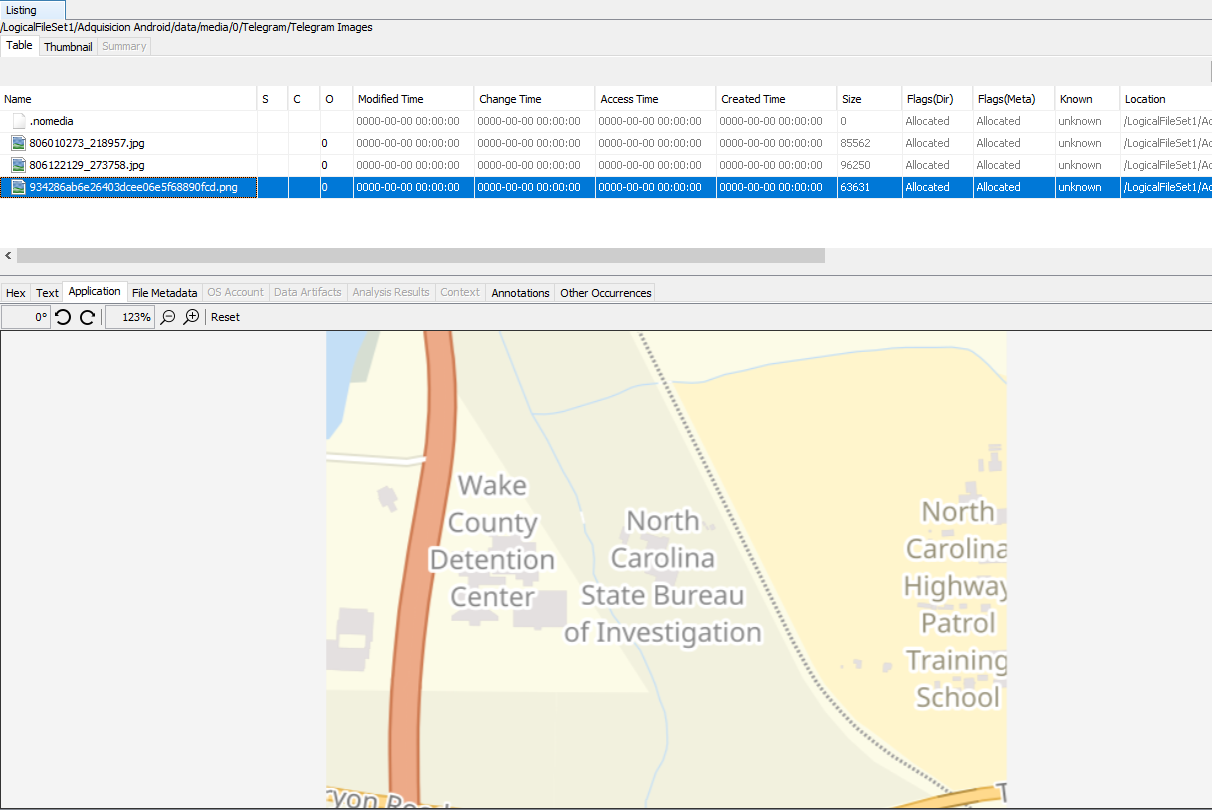
La foto se encontraba en la galería del usuario.

### **3.12 En caso de que el usuario tuviera instalada la app de Telegram, ¿Cuántas cuentas tendría configuradas en el dispositivo?**

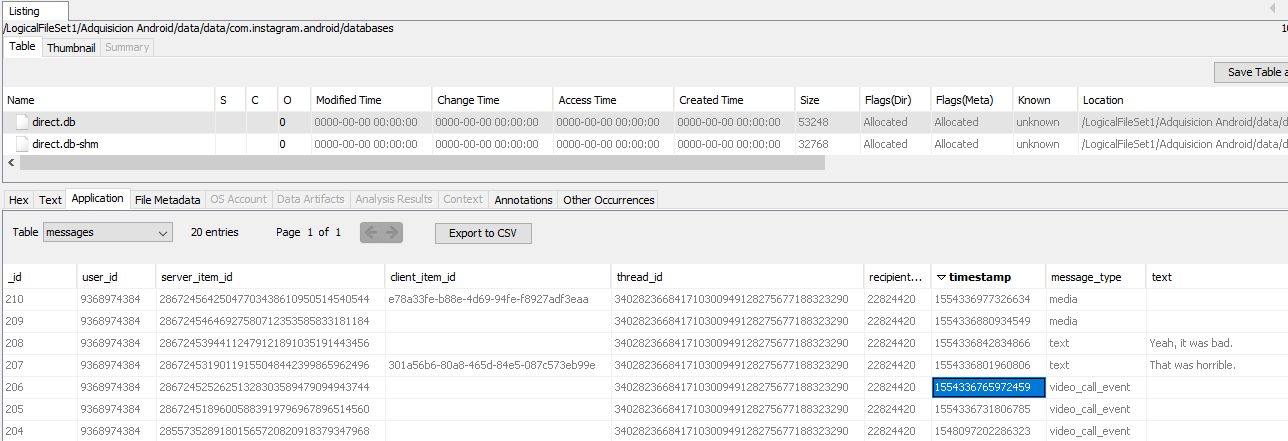


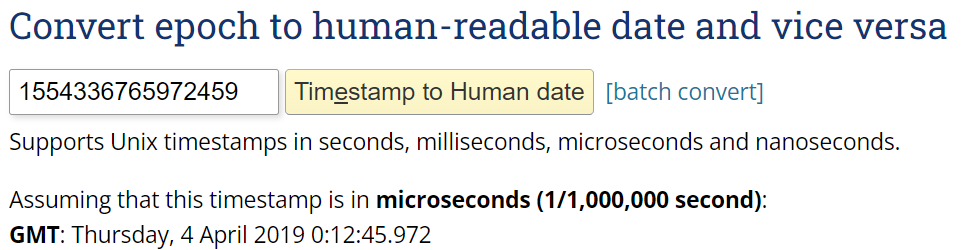
Son 2 en este dispositivo.

### **3.13 Un colaborador ha informado de que se ha usado Telegram para intercambiar una imagen con una ubicación que podría ser relevante para el caso. ¿Cuál es esa imagen?**

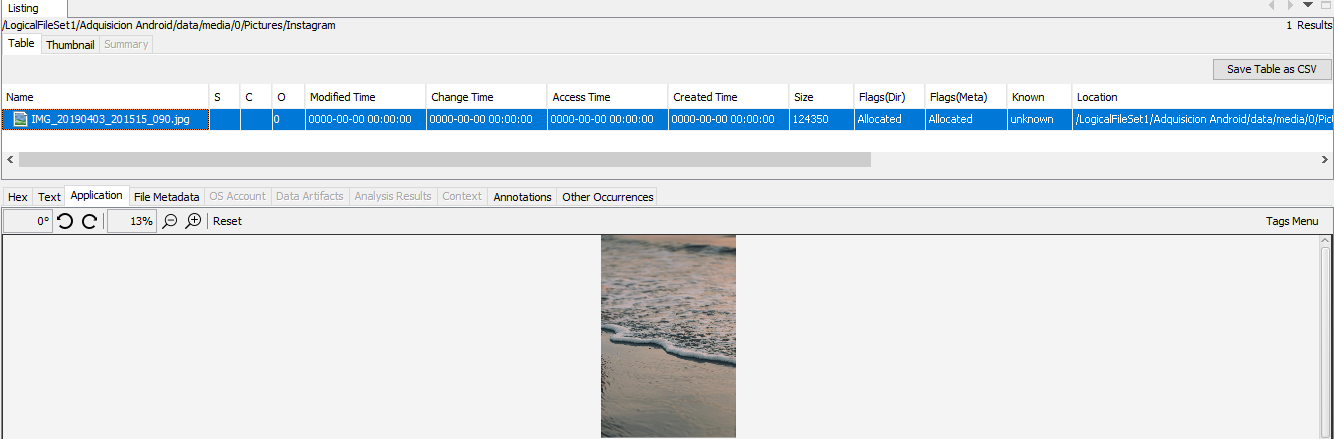


### **3.14 Se ha observado que el usuario utilizaba la app de Instagram en el dispositivo. Indica la fecha y hora exactas (GMT) a la que se inició por última vez una videollamada en esta plataforma.**



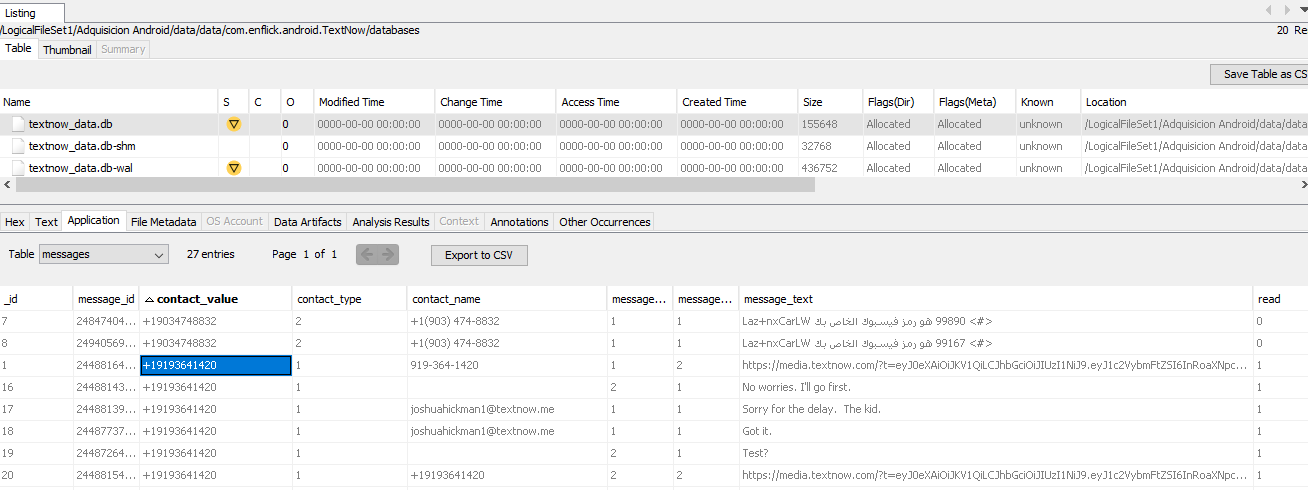
.

### **3.15 ¿Ha subido el usuario alguna foto a Instagram? Si es así, pon una captura de la foto.**



### **3.16 Se ha detectado que el usuario del dispositivo ha estado usando una app llamada TextNow**

En ella ha mantenido contacto con un usuario cuyo número de teléfono es 919-364-1420. Necesitamos saber qué tipo de equipo informático usaba este contacto, ¿sabrías decir cuál es? Justifica la respuesta.

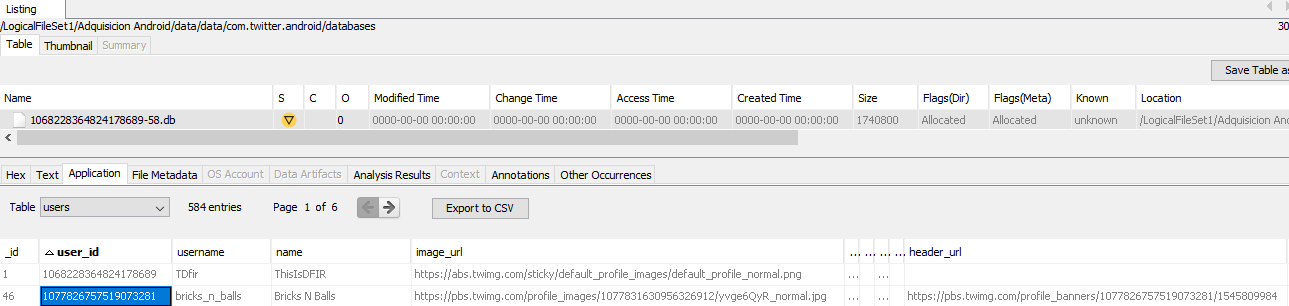


Visitamos el enlace y tenemos esta imagen que nos indica el tipo de dispositivo:



### **3.17 Uno de los contactos de Twitter que tenía el usuario en su dispositivo tiene un “user\_id” con el valor “1077826757519073281”.**

Muestra el nombre de este usuario:

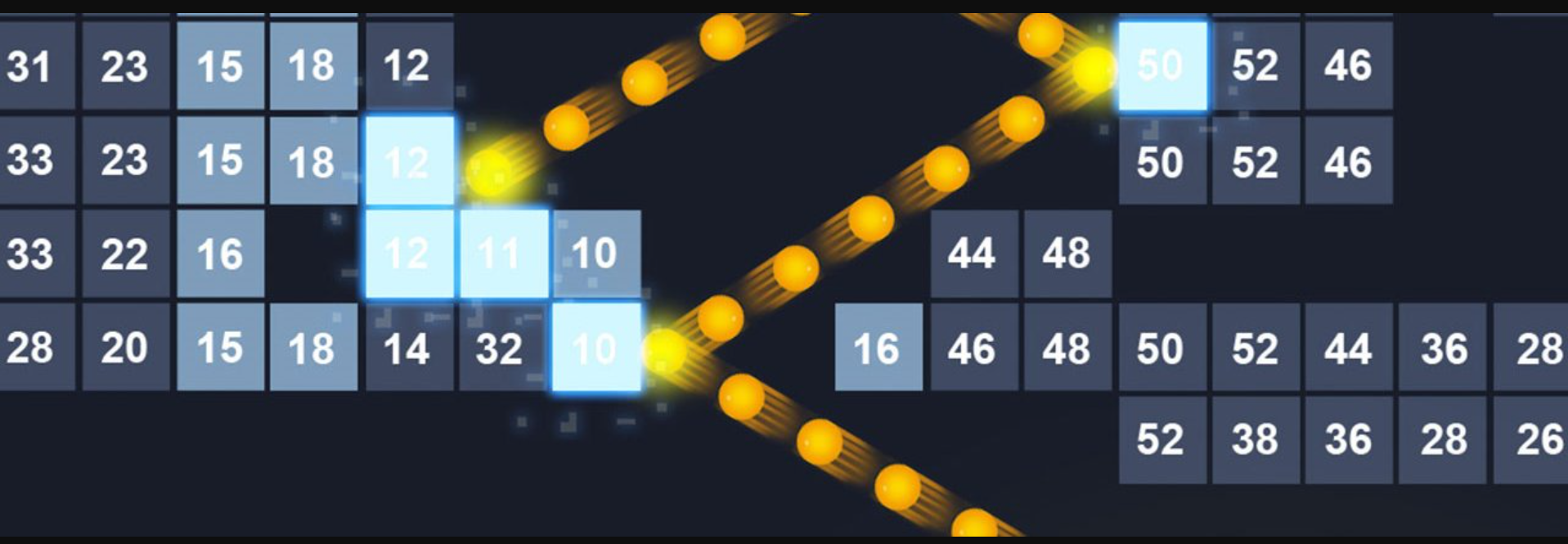


* Bricks N Balls

Su foto de perfil:



Su imagen de cabecera de perfil:



### 