“Universidad Internacional de La Rioja en México”

Informática Forense y Respuesta ante Incidentes

Proyecto:

Actividad 3: Obtención y análisis de un volcado de memoria de un equipo vivo

Profesor:

OSCAR MANUEL LIRA

Autor:

Juan Luis Cruz Aristeo.

Fecha de entrega:

12/08/2024

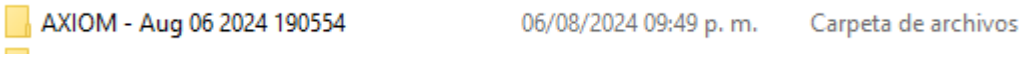
Objetivos

El objetivo principal de esta actividad es el análisis de la información contenida en un dispositivo móvil.

Para realizar la actividad, se puede analizar la copia de seguridad facilitada con cualquier herramienta de las que se han visto en clase u otra que se considere necesaria. Como recomendación sobre las posibles herramientas de análisis a utilizar, tenéis: iPhone Analyzer, dr.fone o iBackup Viewer.

En esta actividad se hizo de las herramientas AXIOM:

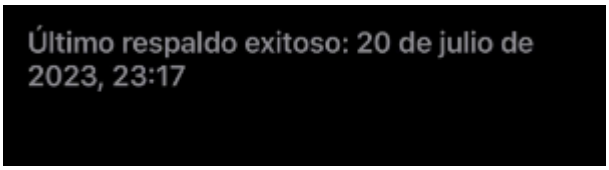
Se realizo la copia con AXIOUM process



Se examina con AXIOM Examine.

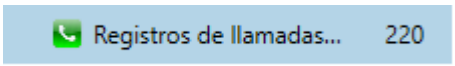
Ahora resolveremos las siguientes preguntas.

- 1. ¿Cuál es la fecha de creación del último *backup?*



- 2. ¿Cuál es el ICCID de la SIM utilizada en el terminal?

- 3. ¿Cuántas llamadas se han realizado con el dispositivo?

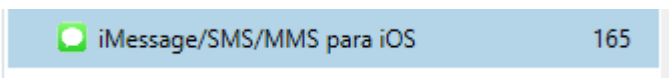


- 4. ¿A qué número se realizó la de mayor duración?

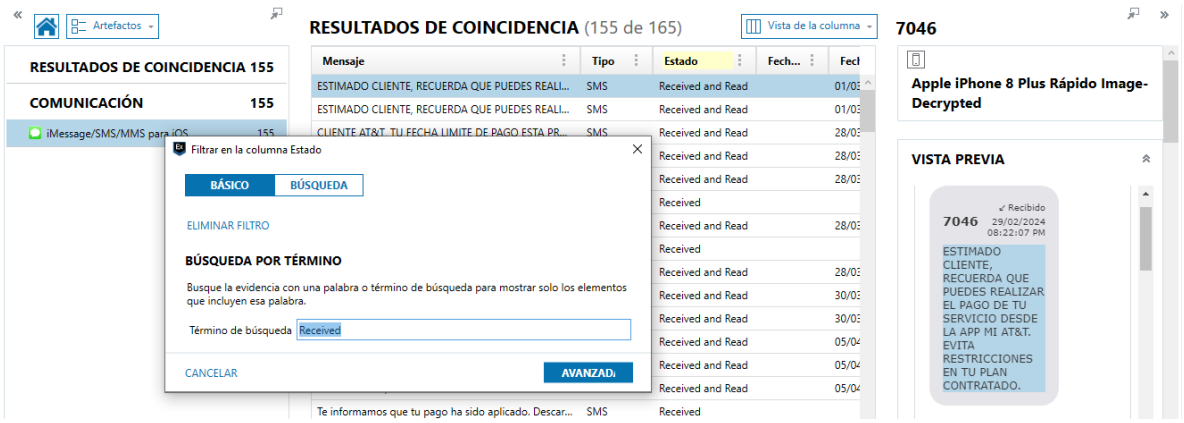
- INFORMACIÓN DE EVIDENCIA

- 5. ¿Cuántos SMS se han recibido?

Ingresamos al apartado

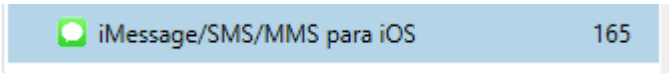


Y adentro vamos a filtrar la columna de estado a solo RECIBIDOS:

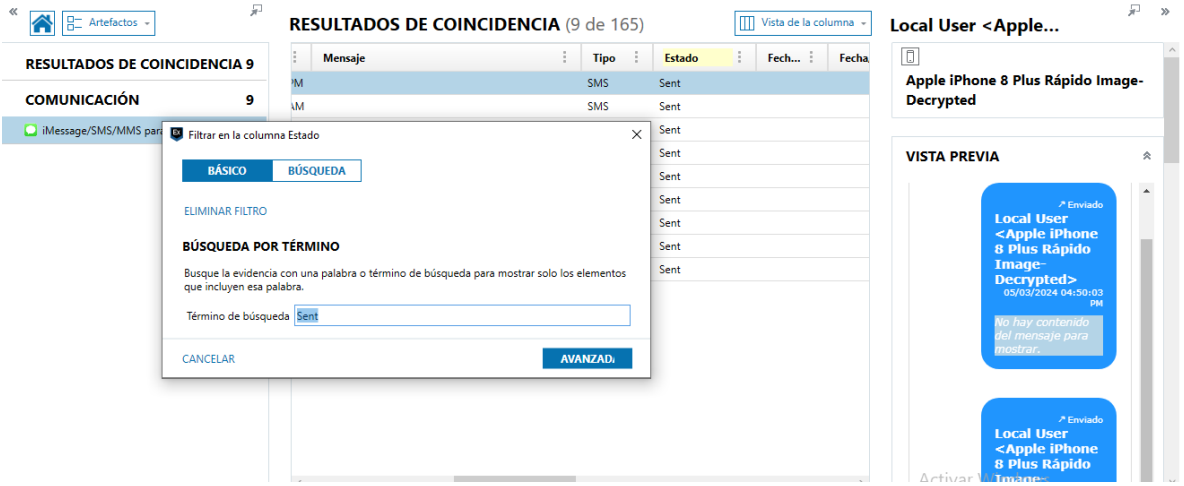


Nos arroja una coincidencia de 155 SMS recibidos.

- 6. ¿Cuántos SMS han sido enviados?
- Ingresamos al apartado

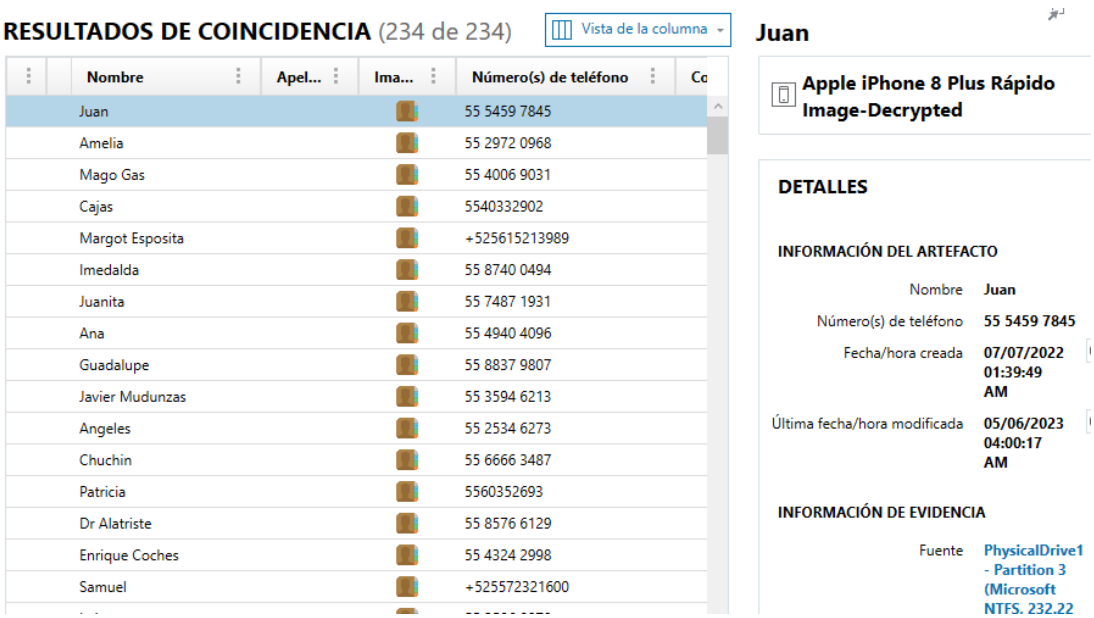


Y adentro vamos a filtrar la columna de estado a solo ENVIADOS:

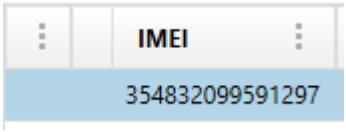


Nos arroja una coincidencia de 9 SMS enviados.

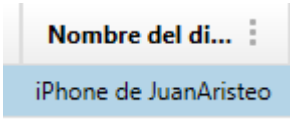
- 7. ¿Cuántos números de teléfono se han grabado en la agenda?



- 8. ¿Cuál es el IMEI del dispositivo?



- 9. ¿Cuál es el nombre del dispositivo?



DETALLES

INFORMACIÓN DEL ARTEFACTO

IMEI	**354832099591297**
Identificador de dispositivo único	**9EE5AF2B0633BF185B6429D2028C41E107F98100**
Número de serie	**FD3ZN148JCM4**
Nombre del dispositivo	**iPhone de JuanAristeo**

- 10. ¿El dispositivo tiene instalado WhatsApp? ¿Cómo ha llegado a la conclusión?

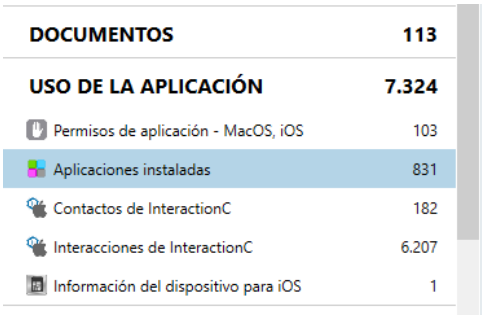
  R= Si cuenta con WhatsApp instalado, llegue a esa conclusión por que el último mensaje es de una fecha actualizada.

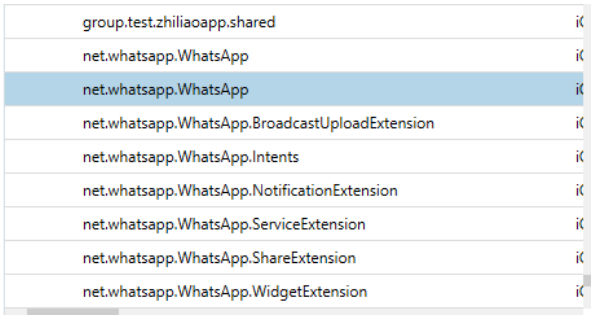
INFORMACIÓN DEL ARTEFACTO

Remitente	**Local User <Apple iPhone 8 Plus Rápido Image-Decrypted>**
Receptor	**5215610454460**
Apodo del receptor	**Juan Luis**
Fecha/hora del mensaje	**26/07/2024 10:54:32 PM**
Dirección del mensaje	**Outgoing**
ID. de conversación	**5215610454460@s.whatsapp.net**
Tipo de chat	**Individual**
Marcado	**No**
Reenviado	**No**

INFORMACIÓN DE EVIDENCIA

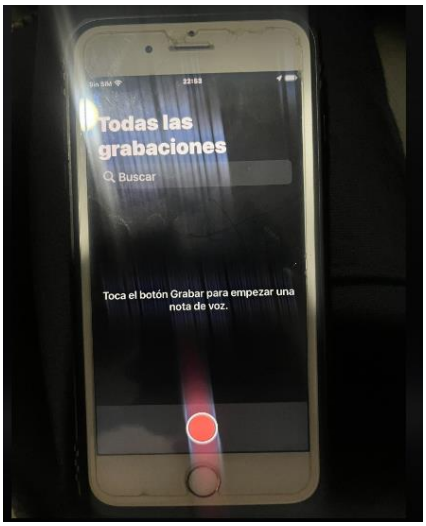
Además en aplicaciones instaladas encontramos los paquetes de WhatsApp





- 11. ¿Existe alguna grabación de voz? ¿Cuántas? ¿Dónde se ubican?

No el teléfono no contiene ninguna nota de voz. Ya que en la sección de medios debería haber un apartado con respecto a grabaciones de voz, por otro lado, también se verifica en el teléfono que no se encuentre ninguna grabación de voz.



- 12. ¿Hay alguna entrada en el bloc de notas? ¿Cuántas? ¿Dónde ha podido localizarla/s?

Si, 96 entradas, se localizan en la sección de documentos.