



**INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS
(ITLA)
Tecnólogo en Informática Forense**

INFORME DE LEVANTAMIENTO:

DIRECCIÓN DEL LEVANTAMIENTO

NUMERO DE CASO

Autopista Las Américas, km. 27, PCSD, La Caleta, Boca Chica, República Dominicana.	ITLA-1319
---------------------------------------------------------------------------------------	-----------

NOMBRE DEL AGRAVIADO

TIPO DE HECHO

Desconocido por el momento	Narcotráfico
------------------------------	--------------

DETALLE DEL CASO

**FECHA DE
LLEGADA**

TIEMPO DE LLEGADA

Posible vinculación de Narcotráfico	04-05-2024	12:15 P:M horas / formato 24 horas
-------------------------------------	------------	---------------------------------------

**ENC. DEL LEVANTAMIENTO EN EL TIEMPO
DE LLEGADA**

CONDICIÓN DE LA ESCENA

Alan José Martínez Muñoz	Buena iluminación, lugar bien organizado.
--------------------------	-------------------------------------------

PERSONAL QUE PARTICIPO EN EL PROCESAMIENTO DE LA ESCENA

NOMBRE COMPLETO

FUNCIÓN

Alan José Martínez Muñoz	Técnico de levantamiento
Pedro Navaja	Chofer
Julio José	Fotografo

INFORME DE LEVANTAMIENTO

“LabsForensicX

ANTECEDENTES

El día 15 de noviembre de 2024, a las 9:15 AM, Se desplazó la unidad de levantamiento de evidencias electrónicas del Departamento de Informática Forense de LabsForensicX en respuesta a una solicitud de Juan Martínez, Rector del Instituto Tecnológico de las Américas (ITLA), ubicado en La Caleta, Boca Chica, República Dominicana. La unidad de recolección estuvo conformada por Alan José Martínez Muñoz (Técnico de levantamiento), Pedro Navaja (Chofer) y Julio José (Fotógrafo).

La intervención fue requerida debido a una sospecha de actividad relacionada con Narcotráfico, en la cual, presuntamente, se estaban utilizando dispositivos móviles para coordinar operaciones ilícitas. La institución afectada el Instituto tecnológico de las Américas, informó que en el dispositivo existía una posible conversación de WhatsApp vinculada a la operación ilegal y que se podrían localizar imágenes comprometedoras en el almacenamiento de la aplicación.

El equipo fue recibido por Juan Martínez Rector de la institución quien facilitó el acceso al dispositivo móvil sospechoso. Inmediatamente, el equipo procedió a identificar y extraer manualmente el chat de WhatsApp relevante y localizar una imagen específica en la carpeta de medios de la aplicación.



Edificio 2

Administración



Oficina Administrativa



Mesa de

PROCEDIMIENTO TECNICO UTILIZADO

Fase de Identificación:

Se fotografió la siguiente información dentro del dispositivo:

- Marca y modelo
- Número de serie (IMEI)
- Versión del sistema operativo
- Capacidad de almacenamiento (total y disponible)
- Estado de la batería
- version de Ws instalado, usuario asigando a ese WS

Fase de Recolección:

Se exportó un chat mediante el medio de transferencia de datos (Bluetooth) hacia una computadora segura para su preservación y se documentó donde se alojó dicho archivo.

Se realizó un ADB Backup al dispositivo, para realizar la búsqueda de las imágenes alojadas de WhatsApp en el dispositivo.


Fase de Preservación:

Uso de Bluetooth para exportar chat e imagen a una computadora segura y se procedió a calcular el valor hash de dichos archivos con una herramienta para esos fines, para verificar su integridad.

Documentación:

Se redactó todo el proceso durante su identificación, recolección y preservación, se plasmaron imágenes que apoyen cada proceso y cada información del dispositivo.

Herramientas o técnicas utilizadas

	Avilla Forensics es una herramienta forense móvil gratuita, lanzada en febrero de 2021, diseñada para ayudar a los investigadores a obtener información y evidencia de dispositivos móviles.
	Microsoft Word es un procesador de textos ampliamente utilizado que permite crear, editar y dar formato a documentos. Con Word, se pueden redactar desde cartas y ensayos hasta informes complejos con gráficos, tablas, y diseños personalizados.
	MD5 Calculator es una herramienta que genera el <i>hash</i> MD5 de un archivo o texto específico. MD5 es un algoritmo que produce un valor hexadecimal único, conocido como "huella digital" del archivo
	Bluetooth es un estándar de tecnología inalámbrica de corto alcance que se utiliza para intercambiar datos entre dispositivos fijos y móviles en distancias cortas y construir redes de área personal.

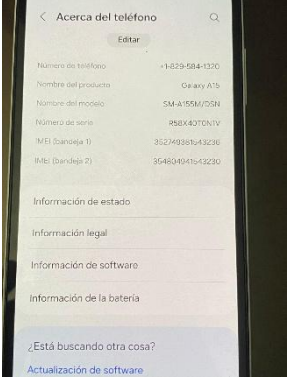
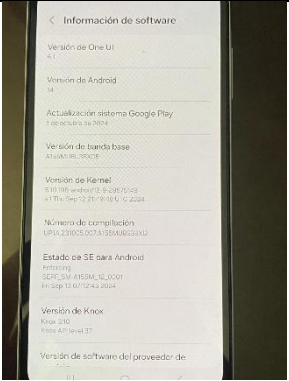
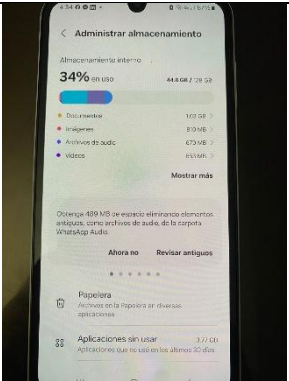
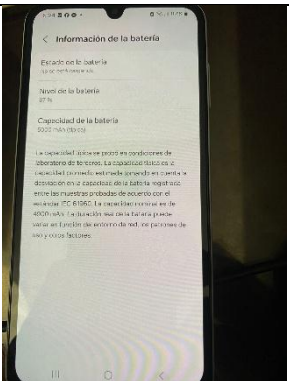
La metodología utilizada para realizar los procesos de adquisición, análisis y preservación de evidencias se basan en la norma ISO 27037:2012 (Tecnología de la información - Técnicas de seguridad - Guías para la identificación, recopilación, adquisición y preservación de evidencias digitales). Dicha norma tiene como principios, los siguientes:



- **Aplicación de métodos.** La evidencia digital debe ser adquirida del modo menos intrusivo posible, tratando de preservarla originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.
- **Proceso auditable.** Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se deben proporcionar trazas y evidencias de lo realizado y sus resultados.
- **Proceso reproducible.** Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.
- **Proceso defendible.** Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación. Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias.
- **Identificación.** Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales información eso elementos de prueba en sus dos posibles estados, el físico y el lógico, según sea el caso de cada evidencia.
- **Recolección y/o adquisición.** Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.
- **Conservación/preservación.** La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegro, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la prueba.

ACTA DE ADQUISICIÓN DE EVIDENCIAS

FECHA	NUMERO DE CASO	NOTAS DEL CASO
09/11/2024	ITLA-1319	Presunto Narcotrafico <hr/> <hr/> <hr/> <hr/>

Característica	Fotografia	Detalle
Marca y modelo		Samsung Galaxy A5

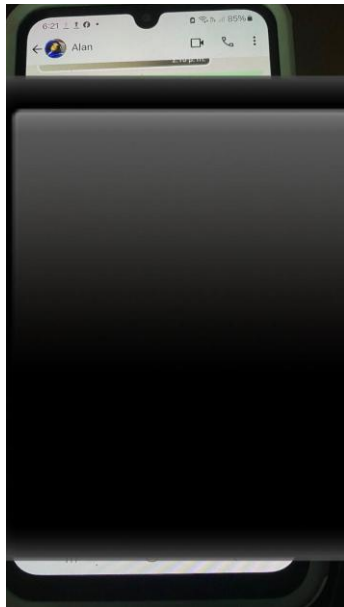
<p>Número de serie (IMEI)</p>		<p>Dual SIM</p> <p>1er IMEI: 352749381543236</p> <p>2do IMEI:</p> <p>354804941543230</p>
<p>Versión del sistema operativo</p>		<p>Android 14</p>
<p>Capacidad de almacenamiento (total y disponible)</p>		<p>El dispositivo cuenta con un almacenamiento de 128 GB, de los cuales 44.6 GB están en uso.</p>
<p>Estado de la batería</p>		<p>Estado de la batería: No se encuentra cargando, con su capacidad de 5000 mAh.</p>

Version de Ws instalado, usuario asigando a ese WS.	 	Se encuentra instalada la versión 2.24.22.78, Con el usuario Carmen Muñoz.
--------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------

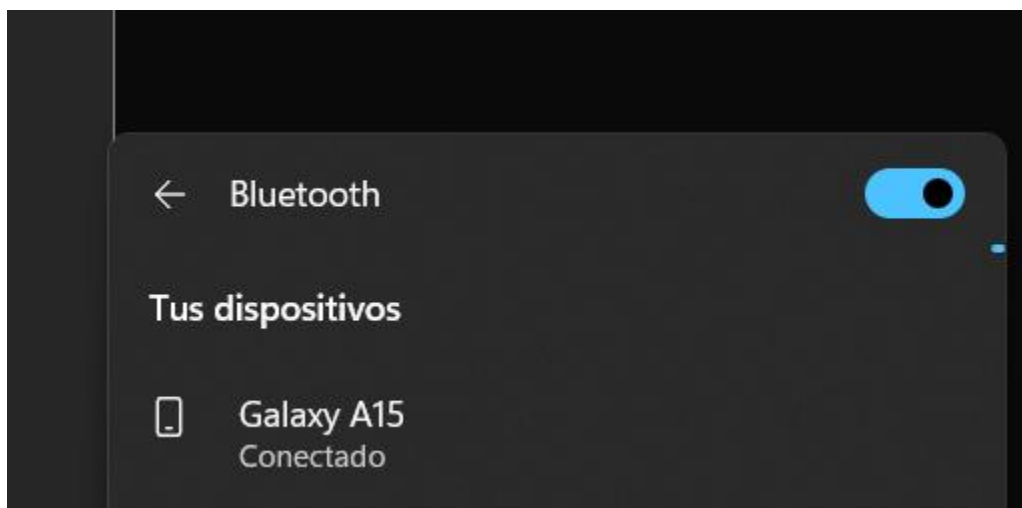
EVIDENCIA EVD-01X			
Tipo de Dispositivo:	<input type="checkbox"/> Ordenador de Sobremesa <input type="checkbox"/> Ordenador Portátil		
	<input checked="" type="checkbox"/> SmartPhone	<input type="checkbox"/> Tablet	
	<input type="checkbox"/> Pendrive	<input type="checkbox"/> Otros(Especificar):	
Tipo de Evidencia:	<input type="checkbox"/> Disco Duro (HDD) <input type="checkbox"/> Disco Sólido (SDD)	<input type="checkbox"/> RAID Nivel: <input type="checkbox"/> Correo electrónico <i>(Indicar cuenta en Buzón de Correo)</i>	<input type="checkbox"/> Memoria flash USB <input checked="" type="checkbox"/> Memoria Flash Smartphone/Tablet
Fabricante:	Vietnam		
Modelo:	SM-A155N/DSN		

Número de	R58X40T0N1V
Fabricante del Dispositivo:	Samsug
Modelo de Dispositivo:	Galaxy A15
IMEI de Dispositivo:	352749381543236
Número de Serie de Dispositivo:	

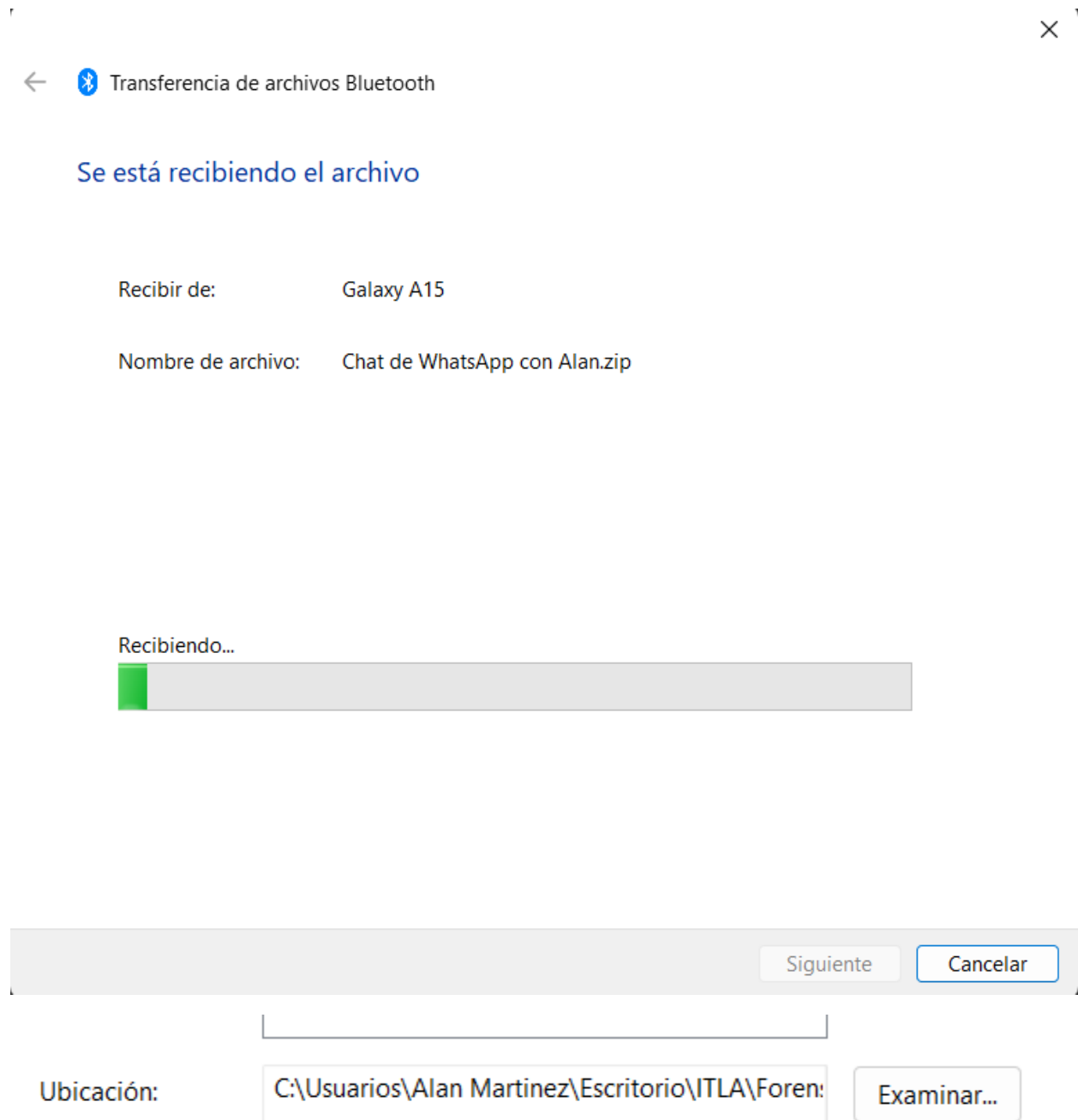
Se procedió a seleccionar el chat que vamos a extraer, en este caso el que tiene relación con el caso de narcotráfico, que sería el chat de Alan.



Vinculamos ambos dispositivos via bluetooth para poder realizar la transferencia de archivos.

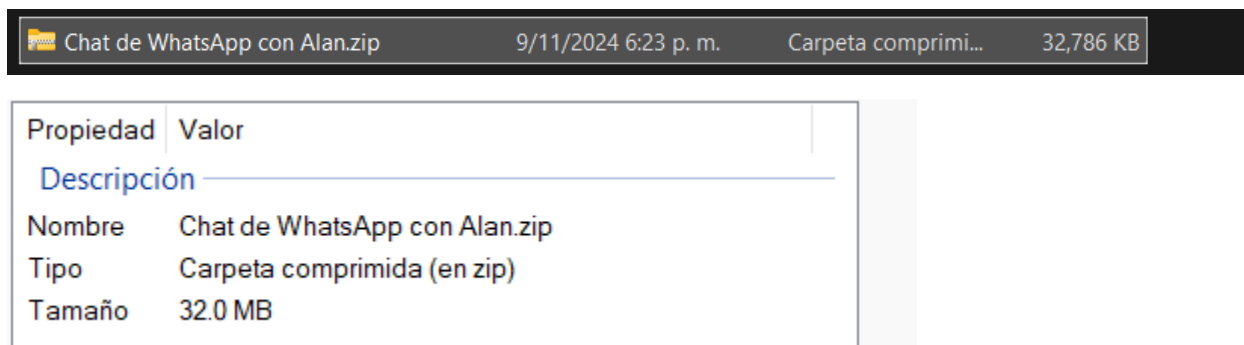


Se abrió el chat, pasamos a ajustes>mas>exportar chat. Seleccionamos la opción de Incluir archivos, donde va a extraer todo tipo de archivo multimedia

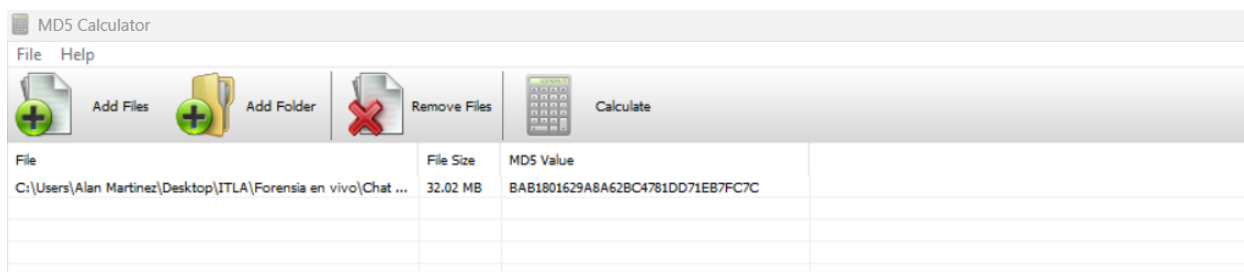


Establecemos la ruta donde queremos almacenar dicho archivo.

Se nos ha generado un archivo llamado Chat de WhatsApp de Alan.zip, con una capacidad de 32 MB. Almacenado en la siguiente ruta: C:\Users\Alan Martinez\Desktop\ITLA\Forensia en vivo.

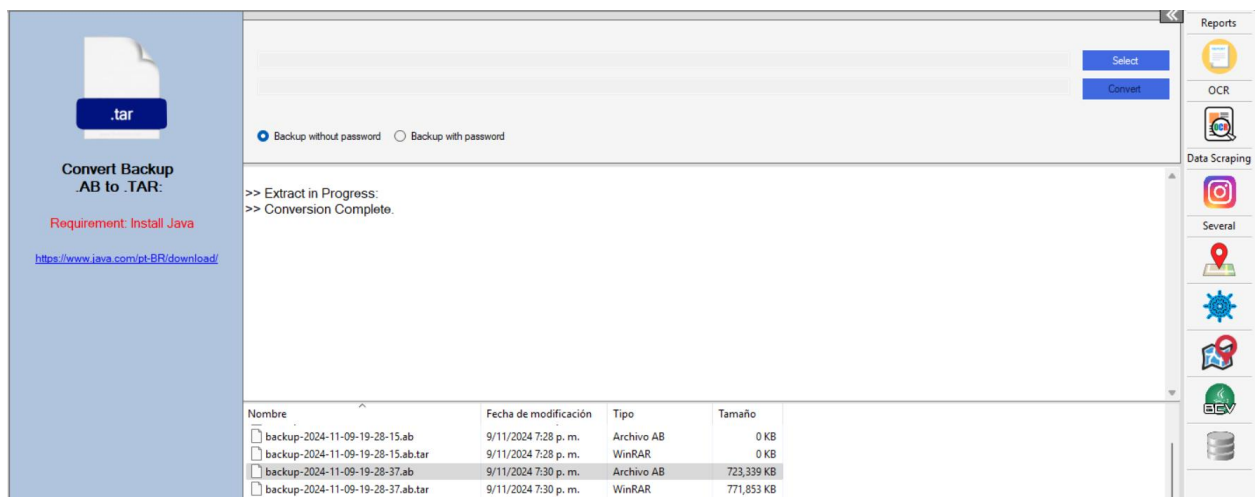
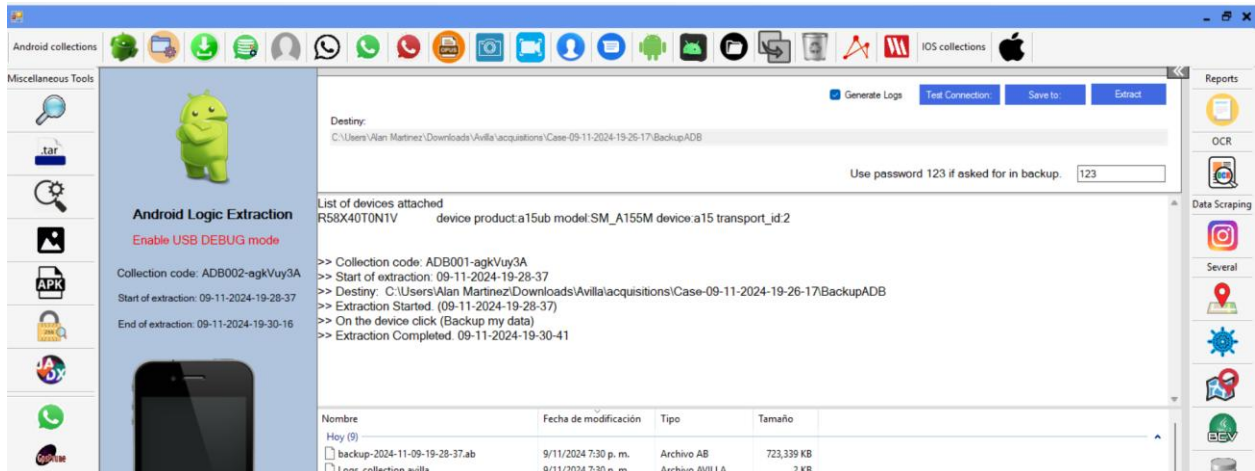


Con la herramienta MD5 calculator, procedimos a generar su valor hash.



Elegí Bluetooth como medio de transferencia de archivos porque es seguro, fácil de usar y no necesita cables ni internet. Al transferir los archivos directamente entre dispositivos, se corre con menos riesgo de que los datos sean interceptados.

Se procedió a realizar un ADB Backup utilizando la herramienta Avilla Forensics. El ADB Backup es una técnica que permite realizar una copia de seguridad completa del dispositivo Android, incluyendo aplicaciones, datos de usuario, configuraciones del sistema y otros archivos importantes.



Convertimos el archivo.db a un archivo ab.tar

Archivo generado por la herramienta.

backup-2024-11-09-19-28-37.ab.tar	9/11/2024 7:30 p. m.	WinRAR	771,853 KB
backup-2024-11-09-19-28-37.ab	9/11/2024 7:30 p. m.	Archivo AB	723,339 KB

Valores hash de ambos archivos.

File	File Size	MDS Value
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\backup-2024-11-09-19-28-37.ab.tar	753.76 MB	FF14A56C7831ADB8A1D84D9FB9218F8E
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\backup-2024-11-09-19-28-37.ab	706.39 MB	36A349D5D23F4333AA0D0F7BE8AAB027

Descomprimos el archivo.tar y lo almacenamos en una carpeta.

C:\Users\Alan Martinez\Downloads\Copia

Dentro de esta ruta vamos a buscar las imágenes de whatsapp, para eso vamos a navegar hasta C:\Users\Alan Martinez\Downloads\Copia\shared\0\Pictures\Whatsapp.

Hace mucho tiempo			
IMG-20231106-WA0011~2.jpg	6/11/2023 7:59 p. m.	Archivo JPG	238 KB
IMG-20231106-WA0011.jpg	6/11/2023 7:57 p. m.	Archivo JPG	162 KB
IMG-20231105-WA0025.jpg	6/11/2023 3:30 p. m.	Archivo JPG	184 KB
IMG-20231105-WA0005.jpg	6/11/2023 3:29 p. m.	Archivo JPG	200 KB
IMG-20231105-WA0006.jpg	6/11/2023 3:29 p. m.	Archivo JPG	198 KB
IMG-20231105-WA0012.jpg	6/11/2023 3:29 p. m.	Archivo JPG	305 KB
IMG-20231105-WA0013.jpg	6/11/2023 3:28 p. m.	Archivo JPG	309 KB
IMG-20231105-WA0014.jpg	6/11/2023 3:27 p. m.	Archivo JPG	146 KB
IMG-20231105-WA0015.jpg	6/11/2023 3:27 p. m.	Archivo JPG	175 KB

Donde podemos ver que se almacenan en el dispositivo 9 imágenes formato .jpg.

File	File Size	MD5 Value
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	199.47 KB	120ABC9D019A3B079F07AE2995A4A3CE
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	197.57 KB	C89C9FB411DD65E81214AF402B8100A1
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	304.07 KB	BEC416F5D2921B664D16789BA60FA348
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	308.37 KB	4CD091D6C8D85019E70F0F202446FEC0
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	145.41 KB	582338C1D3AE46539DDA57E78ED3B98F
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	174.54 KB	86717D5C76DC443B2AF08ED726BBA A05
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	183.1 KB	F98CAD98DD32AC03CC4449C67D49F356
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	161.65 KB	124D42A53601556AD8B627EBA6851EA6
C:\Users\Alan Martinez\Downloads\Avilla\acquisitions\Case-09-11-2024-19-26-17\BackupADB\Contenido\shared\0\Pictures\Whatsapp\IMG-2023...	237.55 KB	6748BC73598D068FD762A9A5BA1CE628

Valor hash de dichas imágenes.

FIRMA DE LOS TECNICOS DE LEVANTAMIENTO



Alan José Martínez Muñoz

Técnico de levantamiento