UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Edison Condor

Angel García

Isaac Velasco

Daniel Velasco

TUTOR: Ing. Ronie Stalin Martínez Gordon, Mtr.

Análisis de evidencias electrónicas en la aplicación de mensajería Whatsapp en dispositivos Android

QUITO – ECUADOR | 2024

APROBACIÓN DEL TUTOR

Yo, **Ronie Stalin Martínez Gordon**, certifico que conozco los autores del presente trabajo siendo la persona responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

Ronie Martínez

DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

Nosotros, **Ángel Cristóbal García Adum, Edison Richard Cóndor Licero, Daniel Esteban Velasco Pilpe, Isaac Israel Velasco Pilpe**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada. Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

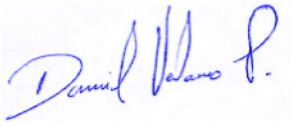
Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Ángel Cristóbal García Adum

C.I.: 1206098202

Edison Richard Cóndor Licero

C.I.: 1720138963



Daniel Esteban Velasco Pilpe

C.I.: 1723529259

Isaac Israel Velasco Pilpe

C.I.: 1723603278

DEDICATORIA

Dedicamos este logro a nuestros queridos padres, quienes han sido nuestra fuente inagotable de amor, apoyo y motivación. Su sacrificio, comprensión y constante aliento nos han guiado en cada paso de este camino. Agradecemos de corazón su fe inquebrantable en nosotros, su paciencia en los momentos difíciles y su alegría en cada uno de nuestros triunfos. Este éxito es tan suyo como nuestro, pues sin su incondicional respaldo, no habría sido posible. Les dedicamos con gratitud y amor esta tesis, reflejo del esfuerzo y dedicación compartidos.

AGRADECIMIENTO

Agradecemos a Dios por otorgarnos la sabiduría, la paciencia y la fortaleza necesarias para superar las adversidades y poder concluir exitosamente nuestra tesis. Valoramos profundamente la guía de los docentes de la Facultad de Cyberseguridades, quienes, además de transmitirnos sus valiosos conocimientos relacionados con nuestra carrera, comparten generosamente sus experiencias de vida. Su guía ha sido fundamental, no solo en nuestro desarrollo profesional, sino también en el personal, inspirándonos a ser mejores seres humanos y profesionales más empáticos y comprometidos. Su dedicación y enseñanza nos han preparado para enfrentar los desafíos futuros con integridad y humanidad.

RESUMEN

En los últimos años, las comunicaciones electrónicas, especialmente a través de aplicaciones de mensajería instantánea como WhatsApp, han pasado a ser una parte esencial de la vida cotidiana. Estas plataformas se han erigido como una fuente invaluable de evidencia para investigaciones en casos judiciales. Simultáneamente, se ha observado un notable incremento en la adopción de dispositivos móviles que utilizan el sistema operativo Android, posicionándose como el líder indiscutible del mercado a nivel global. Esta tendencia subraya la importancia de desarrollar sistemas forenses especializados en la extracción, análisis y preservación de pruebas digitales provenientes de aplicaciones como WhatsApp en dispositivos Android. Esto resulta crucial para asegurar la autenticidad y legitimidad de las pruebas digitales en investigaciones legales. La metodología propuesta se basa en el modelo armonizado de 8 pasos de la norma ISO/IEC 27037, lo cual permite realizar peritajes informáticos con un alto grado de rigor y confiabilidad. Asimismo, se considerarán las normas nacionales pertinentes al realizar dichos peritajes. Se llevarán a cabo procedimientos y escenarios controlados, utilizando tanto casos sintéticos como datos reales, con el fin de evaluar la efectividad y utilidad de las técnicas desarrolladas. Para ello, se medirán métricas clave, como la tasa de éxito en la extracción de evidencia y la relevancia de los datos recuperados, lo que permitirá obtener una evaluación integral del sistema forense propuesto.

Palabras clave: WhatsApp; Android; Forense; Análisis; Investigación

ABSTRACT

In recent years, electronic communications, especially through instant messaging applications like WhatsApp, have become an essential part of everyday life. These platforms have emerged as invaluable sources of evidence for investigations in legal cases. Simultaneously, there has been a significant increase in the adoption of mobile devices using the Android operating system, positioning it as the undisputed leader in the global market. This trend underscores the importance of developing specialized forensic systems for the extraction, analysis, and preservation of digital evidence from applications like WhatsApp on Android devices. This is crucial to ensure the authenticity and legitimacy of digital evidence in legal investigations. The proposed methodology is based on the harmonized 8-step model of the ISO/IEC 27037 standard, which allows for highly rigorous and reliable computer forensics. Additionally, relevant national standards will be considered when conducting these forensic examinations. Controlled procedures and scenarios will be carried out using both synthetic cases and real data to evaluate the effectiveness and usefulness of the developed techniques. Key metrics, such as the success rate in evidence extraction and the relevance of the recovered data, will be measured to provide a comprehensive assessment of the proposed forensic system.

Keywords: WhatsApp; Android; Forensic; Analysis; Investigation

ÍNDICE

Índice de tablas

Índice de figuras

Capítulo I

MARCO TEÓRICO

1.1. Introducción

Las aplicaciones de mensajería instantánea, como WhatsApp, han experimentado un crecimiento exponencial en popularidad en los últimos años. Esta plataforma es la más famosa en función del número de usuarios activos mensualmente, con cerca de 2 mil millones de usuarios (Dixon, 2024). Su adopción masiva se debe a una combinación de factores, como la accesibilidad, la gratuidad y la facilidad de uso. Estas herramientas digitales han transformado radicalmente nuestra manera de comunicarnos tanto en el ámbito personal como profesional.

En el ámbito personal, WhatsApp se ha vuelto esencial para mantenernos conectados con familiares y amigos, sin importar la distancia geográfica. La variedad de funciones que ofrece, como el envío de mensajes de texto, llamadas de voz y video, intercambio de fotos y vídeos, así como la capacidad de formar grupos de chat, nos permite estar al tanto de lo que sucede en nuestras vidas y compartir momentos importantes en tiempo real. Además, la opción de compartir ubicaciones en tiempo real ha sido útil para coordinar encuentros y garantizar la seguridad de las personas en situaciones de emergencia (Mohd Omar y Sani, 2020).

Pero la importancia de WhatsApp trasciende el ámbito personal. En el contexto de investigaciones judiciales y la lucha contra el crimen, estas aplicaciones de mensajería

instantánea juegan un papel crucial. La capacidad de enviar mensajes encriptados de extremo a extremo ha brindado a los usuarios una sensación de privacidad y seguridad en sus comunicaciones. Sin embargo, esta particularidad ha presentado dificultades para las autoridades encargadas de aplicar la ley, ya que frecuentemente necesitan acceder a las conversaciones de WhatsApp para investigar crímenes y llevar a los culpables ante la justicia (AlHidaifi, 2018).

En este sentido, las conversaciones y los datos generados en WhatsApp se han convertido en valiosas evidencias en casos judiciales. Los mensajes, los registros de llamadas, los archivos multimedia compartidos y los metadatos asociados pueden proporcionar información crucial para reconstruir eventos, establecer relaciones entre individuos, identificar conspiraciones y demostrar la culpabilidad o inocencia de los acusados. Estas evidencias digitales pueden complementar y respaldar otras pruebas recopiladas en una investigación criminal.

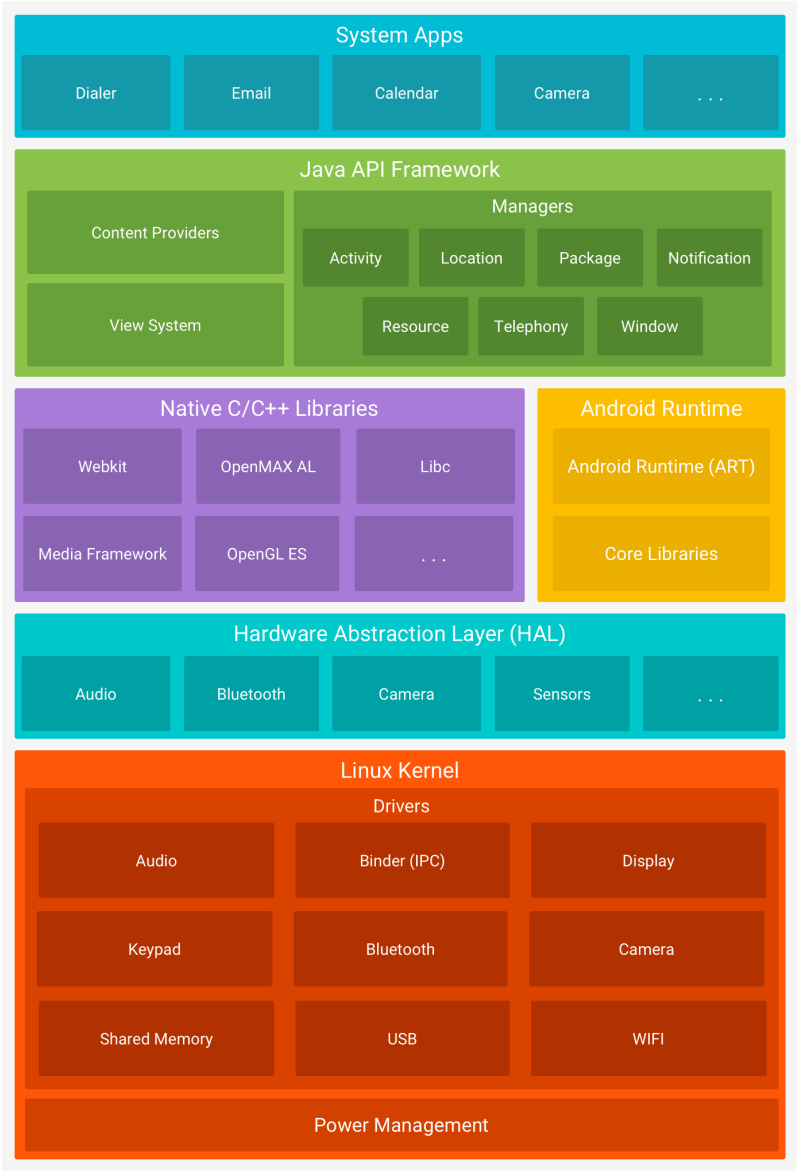
Además de su importancia en el ámbito judicial, es relevante destacar que el sistema operativo Android domina el mercado de dispositivos móviles con una cuota del 71 %, según un informe reciente de Statista (Roa, 2023). Esta abrumadora preponderancia convierte a los dispositivos Android en un objetivo primordial para el análisis forense y la recolección de evidencias electrónicas en diversos tipos de investigaciones legales y de seguridad digital.

Dado que WhatsApp es compatible con dispositivos Android, la información generada en la plataforma puede ser especialmente valiosa en investigaciones que involucren a usuarios de estos dispositivos. Los expertos en análisis forense digital han desarrollado técnicas y herramientas especializadas para extraer y examinar los datos almacenados en dispositivos Android, incluyendo conversaciones y archivos adjuntos de WhatsApp.

1.2. Arquitectura Android

El sistema operativo Android es una arquitectura de sistema abierto que emplea una estructura jerárquica. Como se ilustra en la siguiente figura, la estructura de Android se organiza en cinco capas (AlHidaifi, 2018):

Figura 1.1: Arquitectura de Android



(Developers, 2024)

1.1 Capa del kernel de Linux: El núcleo de Linux 2.6 constituye la capa fundamental del sistema operativo Android, siendo responsable de funciones esenciales del sistema como la gestión de memoria, procesos, dispositivos y energía. Este núcleo facilita una mejor interacción con los dispositivos periféricos del teléfono inteligente (Ekanayake, 2018).

1.2 Capa de abstracción de hardware (HAL): Esta capa se sitúa sobre el núcleo de Linux y ofrece una interfaz entre los servicios del sistema y los controladores de dispositivos correspondientes. Permite que Android sea independiente de los controladores de bajo (Khan y Shahzad, 2016).

1.3 Capa de Bibliotecas Nativas: El sistema Android incorpora un conjunto de bibliotecas principales que los desarrolladores pueden utilizar a través del marco de aplicaciones de Android. Entre estas bibliotecas se encuentran SQLite, FreeType, Webkit, OpenGL ES y Media Framework. Escritas en C++, estas bibliotecas permiten al dispositivo gestionar diversos tipos de datos (Khan y Shahzad, 2016).

1.4 Marco de aplicación: Las funciones básicas del dispositivo son gestionadas por la capa de aplicación, la cual ofrece interfaces de programación de aplicaciones (API) a las aplicaciones de usuario. Estas APIs se utilizan para diversas tareas, como recibir notificaciones, acceder al sistema de telefonía y compartir datos. El marco de la aplicación consta de un administrador de actividad que trabaja para administrar la actividad de la aplicación, proveedores de contenido responsables de administrar el intercambio de datos entre aplicaciones, un administrador de ubicación que trabaja para administrar ubicaciones a través de GPS, un administrador de telefonía responsable de administrar las llamadas de voz en las aplicaciones y administrar el diversos recursos utilizados en aplicaciones por el administrador de recursos (Ekanayake, 2018).

1.5 Capa de Aplicaciones: Esta capa es la capa superior en la arquitectura de Android; Incluye las aplicaciones básicas, como la aplicación de administrador de contactos, la aplicación de SMS, la aplicación de marcador y la aplicación de navegador web. Esta capa también incluye aplicaciones desarrolladas por terceros. Dado que los desarrolladores externos tienen acceso a esta capa, pueden volver a desarrollar algunas funciones y aplicaciones básicas, como la interfaz de usuario y otras aplicaciones, para reemplazar las aplicaciones básicas del sistema; Esta es una característica importante del sistema Android de código abierto. Las solicitudes son escritas por desarrolladores en java. Las aplicaciones desarrolladas son interpretadas por la máquina virtual Dalvik, la cual es reemplazada por Android Runtime (ART) (Ekanayake, 2018).

1.3. Sistemas de archivos de Android:

El sistema operativo Android emplea un sistema de archivos para organizar los datos en el almacenamiento, la eficiencia del sistema de archivos depende de la velocidad de almacenamiento, lectura y recuperación de datos. En la plataforma Android se utilizan el sistema de asignación de archivos 32 (FAT32), otro sistema de archivos flash 2 (YAFFS2) y el sistema de archivos extendido (EXT). Estos sistemas se utilizan para operar el dispositivo, arrancar, almacenar y recuperar datos. Además, estos sistemas se utilizan para organizar datos y archivos en la memoria SD. En la memoria flash, se utiliza el sistema de archivos YAFFS2 (Khan y Shahzad, 2016).

1.4. WhatsApp:

WhatsApp (WA) es una aplicación de mensajería instantánea muy popular para dispositivos móviles. Permite a los usuarios enviar mensajes de texto, imágenes, videos, audios y otros archivos, como documentos PDF. Además, ofrece la opción de crear grupos para enviar contenido a varios destinatarios a la vez. La mensajería en WA está protegida con cifrado de extremo a extremo, lo que garantiza que ningún intermediario pueda leer los mensajes intercambiados entre dos usuarios de WA (Shidek y Wardana, 2020).

WA almacena sus datos en la memoria interna del dispositivo y se conecta automáticamente a la libreta de contactos, detectando a los usuarios de la app. Incluye el proceso com.whatsapp que es un procedimiento para operar el servicio de gestión de medios externos y el servicio de mensajería que se ejecuta en segundo plano (Alhassan, 2017).

En sus inicios, WA usaba una base de datos no cifrada llamada "msgstore.db" para almacenar los mensajes. Posteriormente, se desarrolló un mecanismo de cifrado para la base de datos WA en la plataforma Android utilizando cifrado avanzado (AES) con una clave de cifrado de 192 bits de longitud, renombrando la base de datos a "msgstore.db.crypt". En versiones recientes se emplea AES-256 y la base de datos se denomina "msgstore.db.crypt12"(Alhassan, 2017).

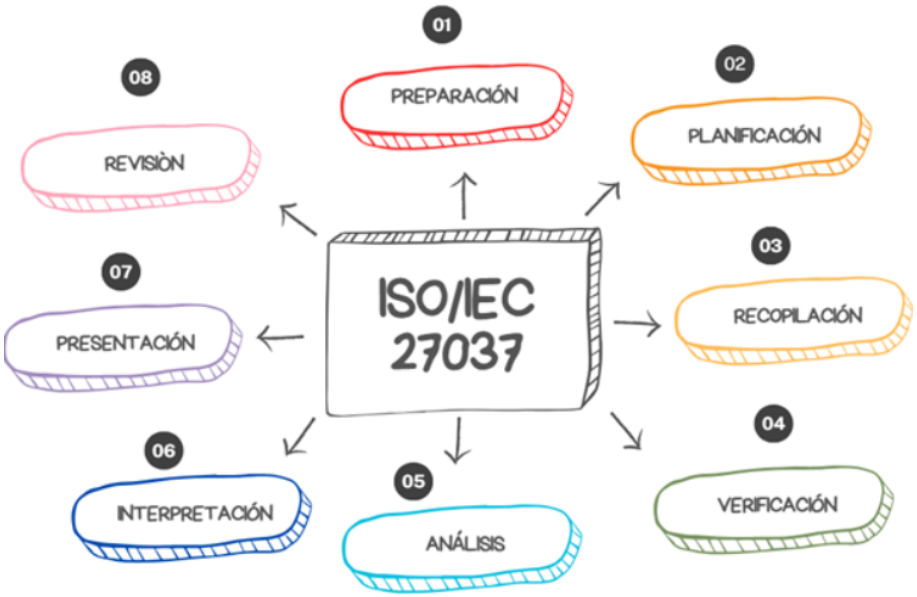
1.5. Norma ISO/ICE 27037:2012

La norma ISO/IEC 27037:2012 establece directrices detalladas para la identificación hasta la preservación de evidencia digital, sustituyendo guías anteriores como la RFC

3227 que se encontraban más desactualizadas. Esta norma ofrece un enfoque actualizado y adaptado a los dispositivos y tecnologías contemporáneas, proporcionando así a los peritos informáticos un marco estandarizado y completo para actuar con precisión y fiabilidad. En última instancia, garantiza la integridad y autenticidad de la evidencia en investigaciones legales. (Rafael_L_R, 2012).

1.6. Modelo Armonizado de 8 pasos: Investigación de Incidentes de Seguridad Informática

Figura 1.2: Modelo Armonizado



Fuente: Elaboración Propia

Preparación:

- Establecimiento de objetivos: Investigar posibles violaciones de seguridad en sis-

temas informáticos de una empresa.

- Identificación de recursos necesarios: Personal especializado en análisis forense digital, herramientas de adquisición de datos, registro de incidentes, etc.
- Definición de roles y responsabilidades: Nombramiento de líder de equipo, expertos en análisis forense digital, personal de apoyo, etc.

Planificación:

- Desarrollo de un plan detallado: Definición de pasos a seguir, incluyendo identificación de fuentes de evidencia, métodos de adquisición y plazos.
- Evaluación de riesgos: Identificación de posibles riesgos, como alteración accidental de datos o pérdida de evidencia.
- Selección de herramientas y métodos de adquisición: Determinación de herramientas forenses digitales adecuadas para el tipo de evidencia a adquirir.

Recopilación:

- Adquisición de evidencia digital: Utilización de herramientas forenses para recopilar datos de los sistemas informáticos involucrados en el incidente.
- Preservación de la evidencia: Implementación de acciones destinadas a asegurar la integridad y autenticidad de los datos recolectados, como la utilización de algoritmos criptográficos para generar hashes.

Verificación:

- Validación de la evidencia recopilada: Verificación de que los datos adquiridos son representativos y relevantes para la investigación.
- Autenticidad e integridad: Verificación de la autenticidad y la integridad de los datos mediante la comparación de hashes y otros procedimientos de validación.

Análisis:

- Examen de la evidencia digital: Análisis de los datos recopilados para identificar patrones, anomalías o cualquier otra información relevante.
- Aplicación de técnicas forenses digitales: Uso de herramientas y métodos para extraer y procesar datos de manera efectiva.

Interpretación:

- Evaluación de los resultados del análisis: Interpretación de los hallazgos para determinar su significancia en relación con los objetivos de la investigación.
- Identificación de posibles implicaciones y conclusiones: Determinación de las posibles causas y efectos del incidente de seguridad.

Presentación:

- Preparación de informes: Documentación detallada del proceso de adquisición y análisis de evidencia digital, incluyendo los hallazgos, conclusiones y recomendaciones.
- Comunicación de los resultados: Presentación clara y concisa de los hallazgos ante las partes interesadas, utilizando un lenguaje accesible y adecuado para el público objetivo.

Revisión:

- Evaluación post-implementación: Revisión del proceso de adquisición de evidencia digital para identificar áreas de mejora y ajustar el enfoque según sea necesario.
- Aprendizaje continuo: Incorporación de lecciones aprendidas en futuras investigaciones y mejoras en los procedimientos y protocolos de adquisición de evidencia digital.

1.7. Marco Legal en el Ecuador

La consideración de la normativa legal vigente en Ecuador es fundamental al abordar la extracción de información en dispositivos móviles y su aplicación en las diversas etapas del análisis forense. Este estudio de investigación se basa en varios artículos y reglamentos extraídos de cuerpos legislativos clave, como el Código Integral Penal, la Ley de Comercio Electrónico, el Reglamento del Sistema Pericial y el Código Orgánico General de Procesos. Cada uno de estos instrumentos legales ofrece directrices y regulaciones esenciales que garantizan la legalidad y legitimidad de las prácticas forenses en el contexto ecuatoriano.

El Código Integral Penal establece las disposiciones legales relativas a los delitos informáticos y las sanciones aplicables, proporcionando un marco legal claro para la extracción y análisis de datos digitales. Por su parte, la Ley de Comercio Electrónico aborda aspectos cruciales relacionados con la autenticidad y validez de la evidencia digital, asegurando que los datos obtenidos de dispositivos móviles sean admisibles en procesos judiciales. El Reglamento del Sistema Pericial define los procedimientos y

estándares que deben seguir los peritos al realizar análisis forenses, asegurando la integridad y confiabilidad de los resultados obtenidos. Finalmente, el Código Orgánico General de Procesos establece las normas para la presentación y evaluación de la evidencia digital en los procedimientos judiciales, estableciendo los criterios que deben cumplirse para que dicha evidencia sea considerada válida y efectiva en el ámbito legal.

Tabla 1.1: Leyes y artículos relacionados con la extracción de información en el Ecuador

Ley/Código	**Artículo**	**Detalle**
Código Orgánico Integral Penal (COIP)	Art. 69 (2a)	Establece el comiso de bienes, fondos, activos o instrumentos como dispositivos informáticos utilizados para cometer delitos.
	Art. 191	Sanciona la reprogramación o modificación de información de equipos terminales móviles.
	Art. 230	Sanciona la interceptación ilegal de datos, diseño de software malicioso y clonación de tarjetas de pago.
	Art. 232	Sanciona el ataque a la integridad de sistemas informáticos, como destrucción o alteración de datos.
	Art. 456	Establece la cadena de custodia para elementos físicos o contenido digital como prueba.
	Art. 477	Autoriza el reconocimiento de grabaciones, videos, datos informáticos como prueba.
	Art. 498	Establece los medios de prueba, incluyendo documentos, testimonios y pericias.
	Art. 500	Establece reglas para el contenido digital como prueba.
Ley de Comercio Electrónico	Art. 2	Reconoce el valor jurídico de los mensajes de datos.
	Art. 7	Establece requisitos para que la información se considere original.
	Art. 8	Establece requisitos para la conservación de mensajes de datos.
	Art. 10	Establece la procedencia e identidad de un mensaje de datos.
	Art. 54	Normas para la práctica de la prueba con mensajes de datos.
	Art. 55	Establece la valoración de la prueba con mensajes de datos.
Reglamento del Sistema Pericial	Art. 19	Establece las obligaciones de los peritos.
	Art. 20	Establece la forma de presentar informes periciales.
Código Orgánico General de Procesos	Art. 221	Define quién es considerado perito.
	Art. 222	Establece normas para la declaración de peritos en audiencia.
	Art. 223	Establece la imparcialidad del perito.
	Art. 226	normas para solicitar un informe pericial para mejor resolver.
	Art. 227	Establece la finalidad y contenido de la prueba pericial.

Fuente: Elaboración Propia

Capítulo II

MARCO METODOLÓGICO

2.1. Herramientas

Autopsy: es una plataforma de código abierto para el análisis forense digital, reconocida por su facilidad de uso, rapidez de resolución y una amplia variedad de plugins para realizar tareas específicas. Permite examinar teléfonos móviles, discos, tarjetas de memoria y otros dispositivos de almacenamiento de datos. Se utiliza en una amplia gama de casos que requieren análisis forense digital, como fraudes, robos de datos empresariales o suplantación de identidad. No obstante, su uso principal destaca en casos relacionados con la pornografía infantil, donde ha sido crucial para detectar evidencia y contribuir a enjuiciar a los responsables. Autopsy puede recuperar una amplia cantidad de archivos incluidos mensajes de WhatsApp, videos, fotos, correos electrónicos, y más, incluso si han sido eliminados por el investigado en un intento de evadir a las autoridades y la justicia (*Autopsy, una herramienta de análisis digital forense*, 2020).

Avilla Forensics: es una herramienta forense digital que permite a los profesionales en Informática Forense obtener evidencias digitales completas. Entre sus características más destacadas se encuentran la capacidad de realizar copias de seguridad, analizar dispositivos y descifrar datos de WhatsApp. Además, Avilla Forensics ofrece la posibilidad de montar imágenes forenses en una máquina virtual directamente desde la herramienta, conectar y analizar múltiples dispositivos Android e iPhone de forma simultánea, y

procesar y analizar la evidencia digital de manera eficiente. La herramienta se destaca por su simplicidad y su interfaz amigable, permitiendo a los usuarios navegar fácilmente por sus funciones y acceder rápidamente a las herramientas (Avilla, s.f.).

Tras comparar ambas herramientas, se optó por utilizar Avilla Forensics debido a su enfoque exclusivo en WhatsApp. Esta herramienta permite visualizar conversaciones, mensajes eliminados, archivos multimedia enviados y recibidos, así como las llamadas realizadas en la aplicación. En contraste, Autopsy se especializa en la recuperación de archivos y requiere trabajar con la base de datos de WhatsApp, lo que no asegura un manejo adecuado de la información. Esto se debe a que la base de datos podría haber sido alterada y no reflejaría si un mensaje fue eliminado, ya que, si no está presente en la base de datos, no sería posible detectarlo.

Tabla 2.1: Comparativa Herramientas

Característica	Autopsy	Avilla Forensics
Código Abierto	Sí (Licencia GPLv2)	Si (Licencia GPLv3)
Complejidad	Alta	Baja
Rapidez de Resolución	Alta (Procesamiento rápido)	Alta (Optimizada para eficiencia)
Gama de Plugins	Amplia (Más de 400 plugins)	Limitada (Plugins específicos)
Dispositivos Soportados	Amplia (Discos, tarjetas de memoria, teléfonos celulares, otros)	Android e iPhone
Casos de Uso	Ideal para análisis forense completo que abarca imágenes de disco, archivos, registros, memoria y datos de red	Adecuado para tareas básicas de análisis de imágenes de disco, extracción de archivos y análisis de metadatos
Ejemplos de uso	Examinar imágenes de disco de computadoras comprometidas en busca de malware, analizar archivos y registros para identificar actividades sospechosas, responder a incidentes de ciberseguridad	Extraer archivos de imágenes de disco para recuperar datos, analizar metadatos para obtener información sobre archivos, calcular hashes de archivos para verificar la integridad
Copias de Seguridad	No	Sí (Creación y restauración)
Análisis de Dispositivos	Sí (Análisis en profundidad)	Sí (Análisis forense completo)
Descifrado de Datos de WhatsApp	Sí (Incluye mensajes eliminados)	Sí (Funcionalidad específica)
Montaje de Imágenes Forenses	Sí (Soporte para diferentes formatos)	Sí (Montaje directo en herramienta)
Conexión y Análisis Múltiples Dispositivos	Limitada (Un dispositivo a la vez)	Sí (Análisis simultáneo)
Procesamiento y Análisis de Evidencia Digital	Eficiente (Algoritmos optimizados)	Eficiente (Herramientas integradas)
Interfaz	Amigable (Navegación sencilla)	Amigable (Diseño intuitivo)
Comunidad	Gran comunidad de usuarios y desarrolladores con soporte activo	Comunidad más pequeña, pero en crecimiento
Soporte	Comunidad activa (Foros, documentación)	Soporte técnico comercial
Capacitación	Tutoriales disponibles (En línea y presenciales)	Capacitación ofrecida por desarrolladores

Fuente: Elaboración Propia

2.2. Metodología

Esta investigación emplea una metodología mixta, combinando elementos tanto cualitativos como cuantitativos. El enfoque cualitativo se utiliza para analizar el contenido textual de los chats de WhatsApp, mientras que el enfoque cuantitativo se utiliza para procesar y analizar los metadatos asociados a los chats. La combinación de estos dos enfoques permite obtener una comprensión completa de los datos y extraer información relevante para la investigación.

Participantes

Los participantes de esta investigación son los usuarios de WhatsApp cuyos chats están siendo analizados. El análisis se realiza con el consentimiento de los usuarios o con una orden judicial, según corresponda.

Evidencia

La evidencia analizada en esta investigación son los chats de WhatsApp, que incluyen mensajes de texto, archivos multimedia y metadatos. Los chats se extraen de los dispositivos móviles de los usuarios utilizando Avilla Forensics.

Procedimiento de Análisis

El análisis forense de los chats de WhatsApp se realiza siguiendo el modelo armonizado que se lo resumió en las siguientes cinco etapas:

1. **Preparación y Planificación:**

    - Definir el alcance del análisis.
    - Obtener las autorizaciones necesarias.
    - Preservar la evidencia.

- Preparar la herramienta Avilla Forensics.

2. **Recopilación y Verificación de la Evidencia:**

   - Conectar el dispositivo móvil a la computadora forense.
   - Extraer los chats de WhatsApp con Avilla Forensics.
   - Verificar la integridad de la evidencia.

3. **Análisis e Interpretación de la Evidencia:**

   - Cargar la evidencia en Avilla Forensics.
   - Realizar un análisis exhaustivo de los chats de WhatsApp.
   - Identificar la evidencia potencialmente relevante.
   - Exportar la evidencia en un formato adecuado.

4. **Presentación de la Evidencia:**

   - Elaborar un informe forense detallado.
   - Presentar la evidencia en un tribunal u otro entorno legal relevante.

5. **Revisión:**

   - Identificar cuellos de botella, limitaciones o desafíos
   - Desarrollar nuevas guías y mejores prácticas para la adquisición de evidencia digital.

Consideraciones Éticas

Se han implementado las siguientes acciones para asegurar la ética de la investigación:

- Obtener el consentimiento informado de los participantes o una orden judicial.
- Mantener la privacidad de la información de los usuarios.
- Manejar la evidencia de manera segura y responsable.
- Cumplir con todas las leyes y regulaciones aplicables.

Capítulo III

ANÁLISIS Y RESULTADOS

Los resultados del estudio demostraron que es posible obtener una amplia gama de pruebas forenses a partir de un dispositivo móvil Android, incluyendo registros de llamadas, mensajes de texto, fotos y videos. Para realizar este estudio, se emplearon los dispositivos y programas mencionados en la Tabla 3.1.

Tabla 3.1: Dispositivos, herramientas y especificaciones

No.	Nombre	Especificación
1	Laptop	Toshiba Satellite, Intel Core i5, RAM: 16 GB, Windows 10
2	Cable USB	Cable USB Tipo C
3	Herramienta forense	Avilla Forensics
4	Dispositivo móvil	Huawei

Fuente: Elaboración Propia

El dispositivo móvil especificado en la Tabla 3.1 se empleó como dispositivo de prueba en el estudio. Además, se utilizó la herramienta forense "Avilla Forensics" para adquirir datos forenses de la evidencia y generar un valor MD5 para verificar su integridad antes del análisis

1. **Preparación y Planificación**

   En esta fase se identifican, autorizan y documentan las pruebas y los datos. La prueba utilizada en este estudio es un dispositivo móvil Huawei, cuyos datos se

han documentado como se muestra en la Tabla 3.2.

Tabla 3.2: Especificaciones del dispositivo móvil de prueba

Nombre	Huawei Y6P
Número de modelo	MED-LX9
IMEI	862229045141324
Versión Sistema Operativo	Android 10 EMUI 10.1

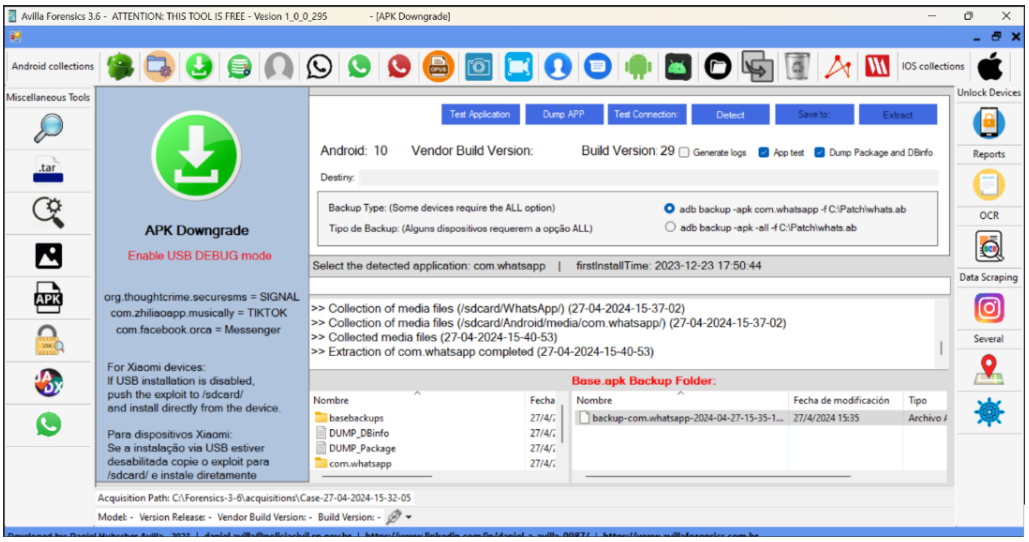
Fuente: Elaboración Propia

También en esta etapa, las pruebas y los datos se aseguran para preservar su integridad y protegerlos de cualquier cambio o destrucción, así como para garantizar que estas pruebas o los datos que contienen no se utilicen indebidamente.

2. **Recopilación y Verificación de la Evidencia**

Durante esta etapa, se procede a recopilar evidencia digital del dispositivo móvil Android sin necesidad de realizar el proceso de root. La recopilación de evidencia digital se efectúa mediante el uso de la herramienta forense Avilla Forensics. El método utilizado es la copia de seguridad lógica ADB, tal como se ilustra en la figura adjunta.

Figura 3.1: Copia de Seguridad de WA

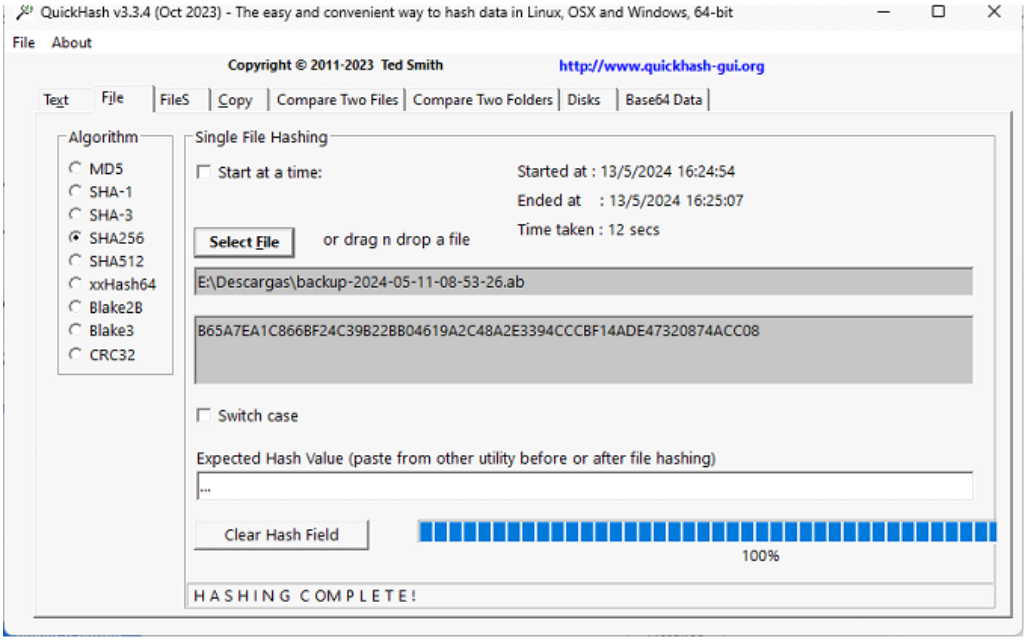


Fuente: Elaboración Propia

Este método permite obtener una copia completa de los datos del dispositivo, incluyendo aplicaciones, mensajes, registros del sistema y archivos multimedia, sin necesidad de rootear el teléfono. La copia de seguridad se genera en un formato estándar que puede ser analizado posteriormente con herramientas forenses especializadas.

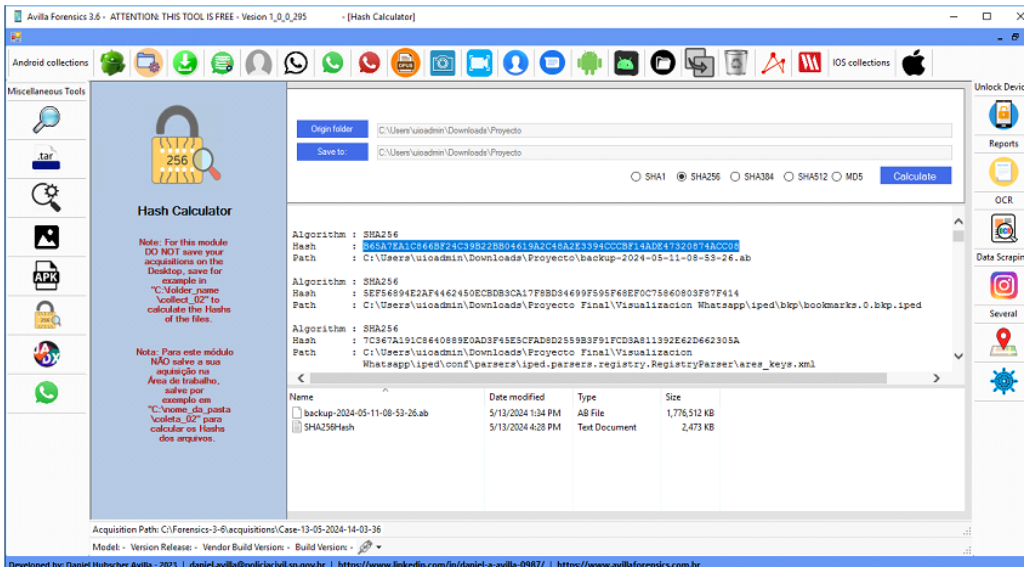
Para verificar que los resultados de la adquisición son idénticos al archivo original que se encuentra en el dispositivo móvil Android, se calculó el valor SHA256 generado por la herramienta Avilla Forensics y se comparó con el valor SHA256 generado por la herramienta Quick HASH, lo cual nos dio el mismo resultado como se puede ver en las siguientes figuras.

Figura 3.2: Generación de Hash con Quick Hash



Fuente: Elaboración Propia

Figura 3.3: Generación de Hash con Avilla



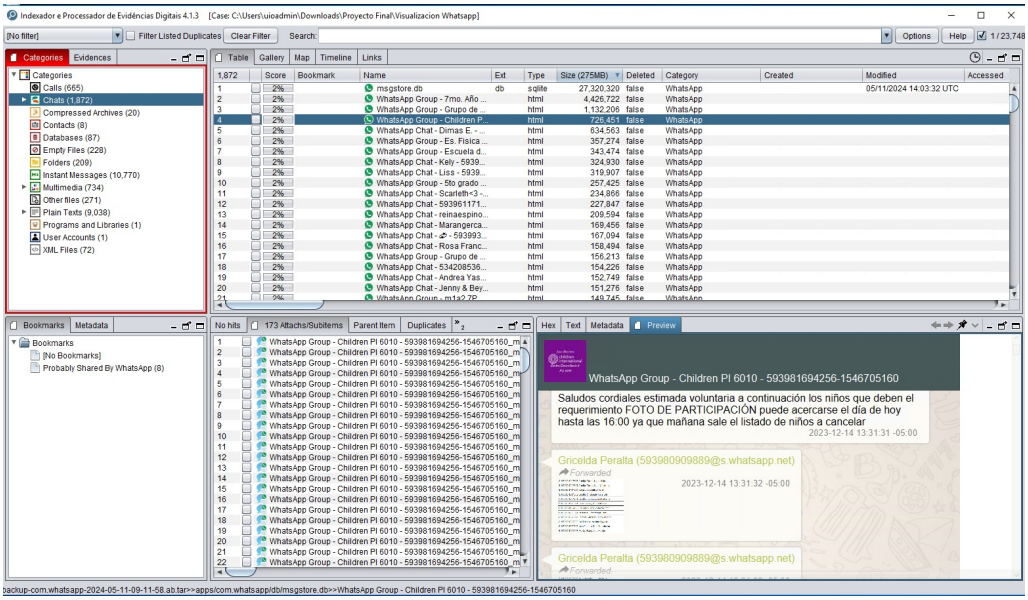
Fuente: Elaboración Propia

3. **Análisis e Interpretación de la Evidencia**

   En esta fase se procedió a encontrar pruebas relevantes en los chats y llamadas de WhatsApp, así como en los archivos de audio, vídeo y fotos compartidos a través de la aplicación.

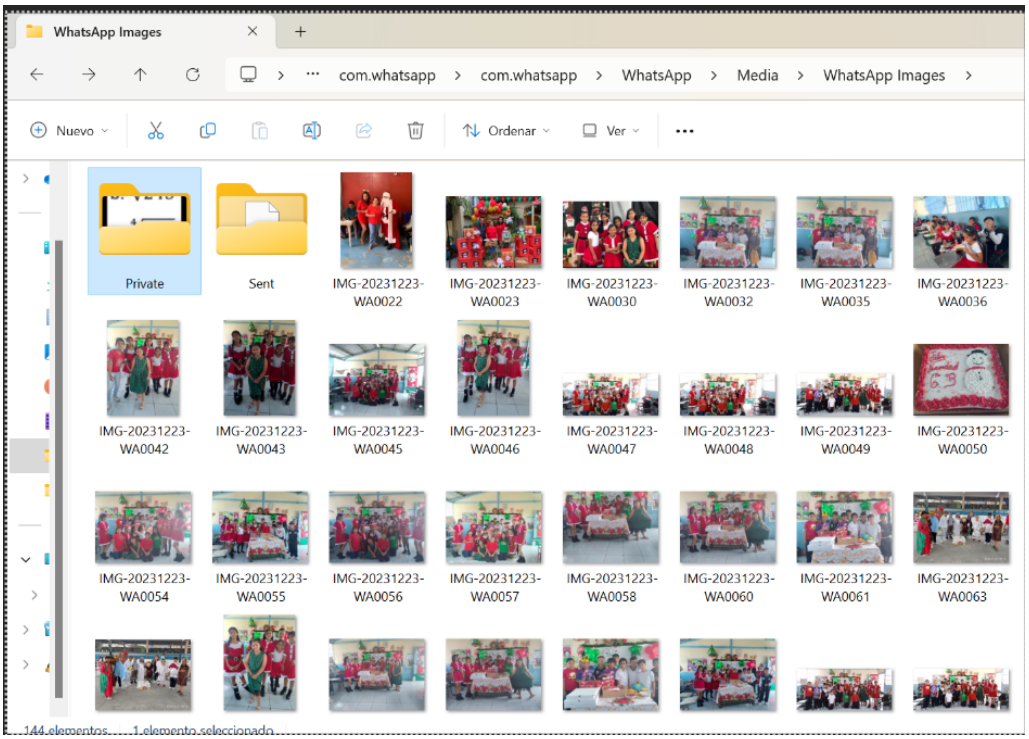
   Para ello, se utilizó la herramienta IPEDTools que viene integrada en Avilla Forensics para así poder procesar y analizar las evidencias digitales. Esta herramienta permitió revisar las listas de mensajes de WhatsApp y leer los detalles de los mensajes existentes, también se pudo visualizar los archivos multimedia intercambiados y los archivos compartidos, como se ve en las siguientes figuras.

Figura 3.4: Mensajes WA



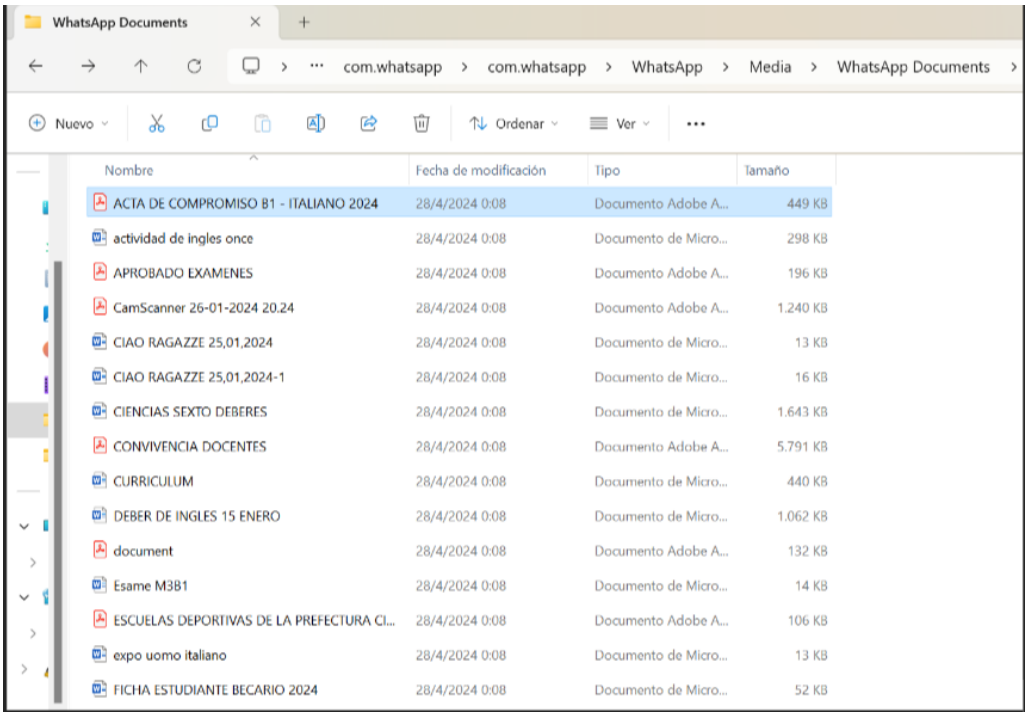
Fuente: Elaboración Propia

Figura 3.5: Imágenes WA



Fuente: Elaboración Propia

Figura 3.6: Archivos WA



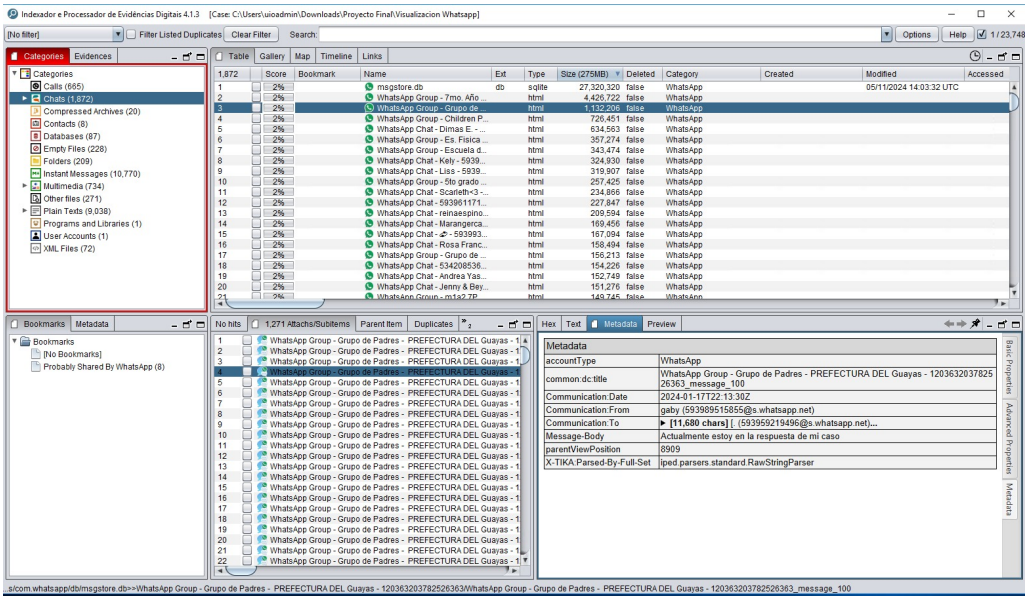
Fuente: Elaboración Propia

También se pudo obtener la siguiente información con la ayuda de la herramienta Avilla Fonrensics:

- **Metadata de chats de WA**

  Podemos ver la metadata de cada uno de los mensajes que se han realizado. También se puede observar cuándo se envió el mensaje, el texto y el contacto que lo envió.

Figura 3.7: Metadata WA

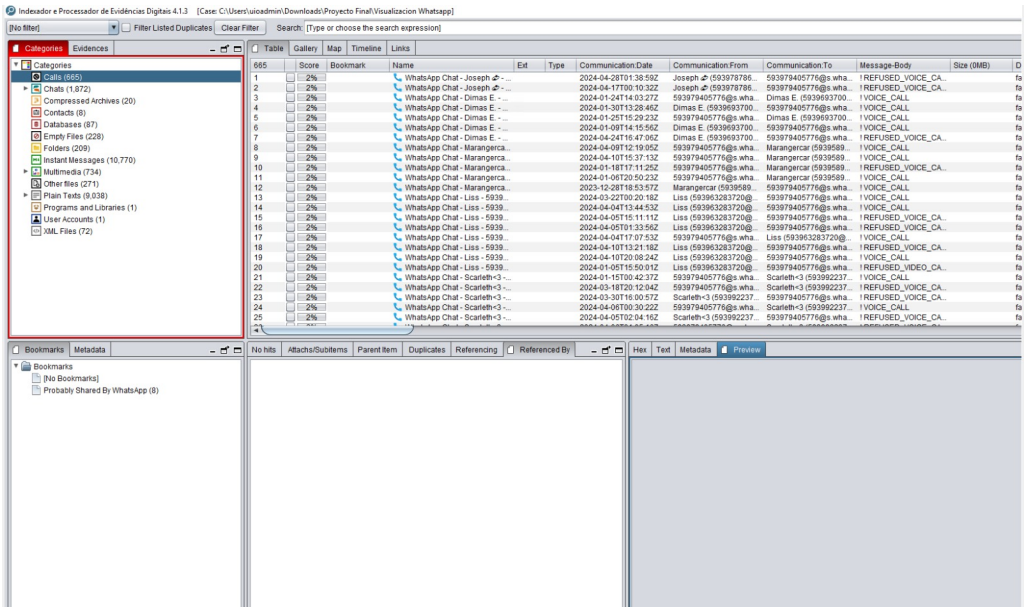


Fuente: Elaboración Propia

- **Análisis de llamadas mediante WA**

  Se puede observar el origen y el destino de las llamadas, así como si las llamadas fueron rechazadas o si se estableció comunicación.

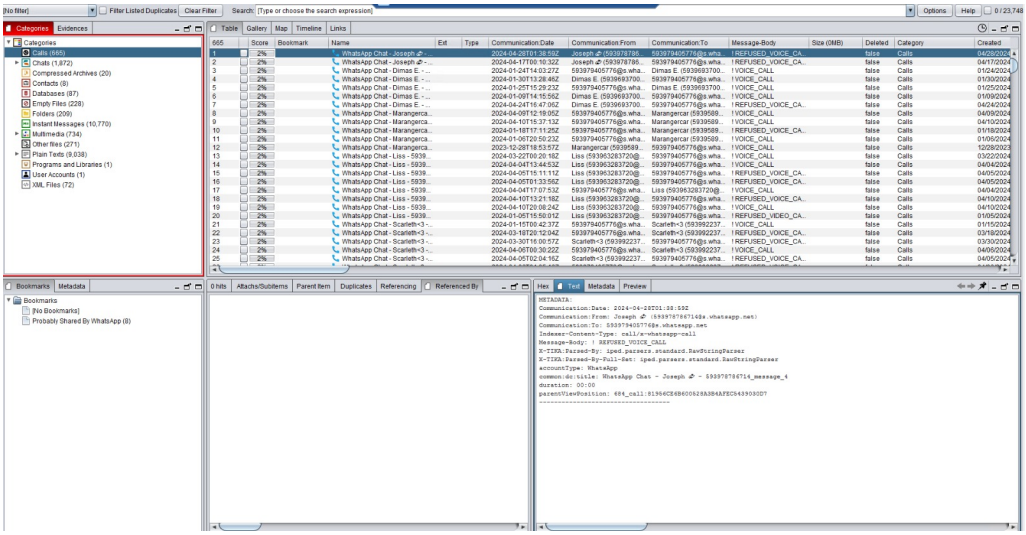
Figura 3.8: Llamadas de WA



Fuente: Elaboración Propia

Se hizo un análisis de una muestra de llamadas realizadas en el dispositivo. La llamada que se muestra en la figura 3.9, realizada entre 5939787867xx y 5939794057xx, es rechazada y no tiene un tiempo de duración de la llamada.

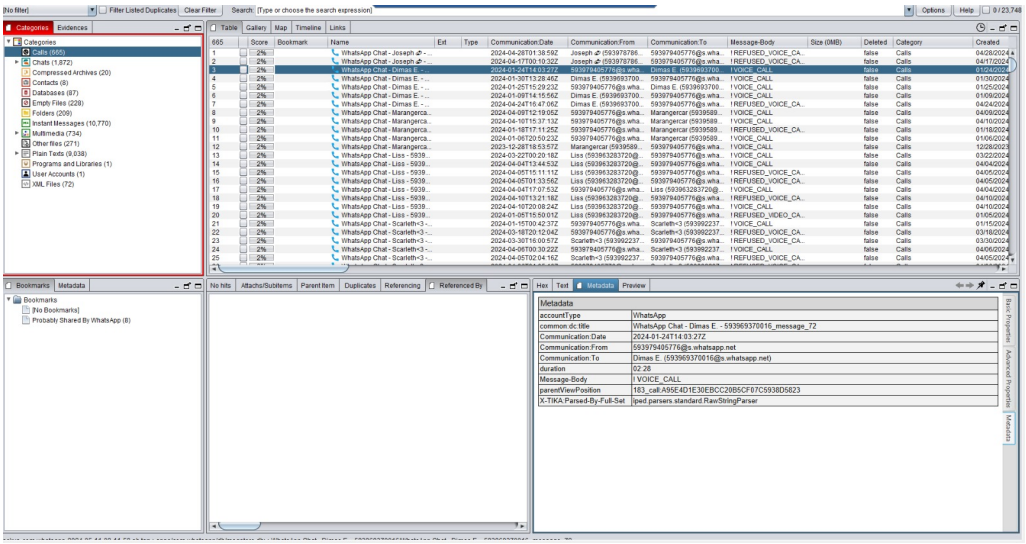
Figura 3.9: Llamada rechazada en WA



Fuente: Elaboración Propia

En la llamada que se muestra en la figura 3.10 podemos observar que existió una comunicación entre 5939794057xx y 5939693700xx y la llamada tuvo una duración de 2 minutos 28 segundos.

Figura 3.10: Llamada conectada en WA

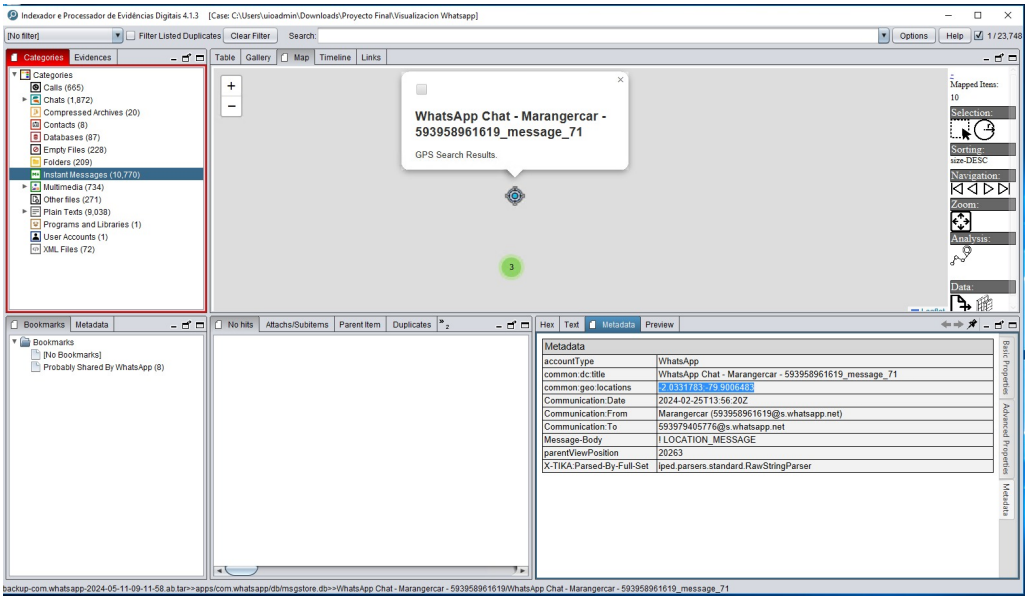


Fuente: Elaboración Propia

- **Análisis de geolocalización de mensajes de WA**

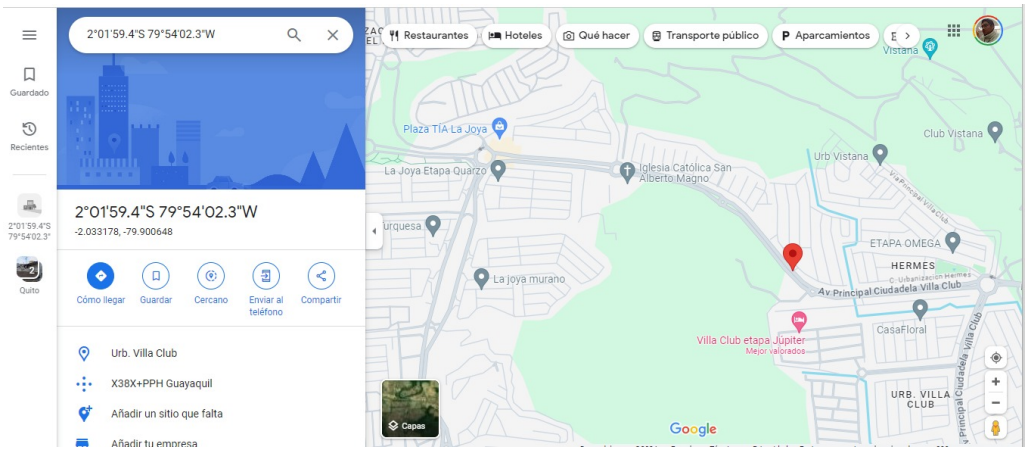
  La herramienta también permite realizar un análisis de Geolocalización de los mensajes, pero cabe recalcar que para esto es necesario que el dispositivo que envió el mensaje haya tenido activo el GPS.

Figura 3.11: Geolocalización de un mensaje en WA



Fuente: Elaboración Propia

Figura 3.12: Mapa con las coordenadas del mensaje



Fuente: Elaboración Propia

4. **Presentación de la Evidencia**

   Esta fase implica la sistematización de los hallazgos, la organización de la evidencia y la redacción de un informe comprensible para las partes involucradas en la investigación.

   En la tabla 3.3 se muestran los resultados del análisis forense realizado con la herramienta Avilla Forensics. Los detalles de esta tabla representan los datos encontrados que coinciden con los datos del dispositivo móvil Android que se utilizó como prueba. Para obtener detalles sobre los datos encontrados, consulte el apéndice A.

Tabla 3.3: Resultados de las pruebas

Información	**Hallazgos**
Número de teléfono	0984943056
Nombre de usuario	593984943056
Llamadas	665
Chats	1.872
Archivos comprimidos	20
Contactos	8
Mensajes instantáneos	10.770
Archivos multimedia	734

Fuente: Elaboración Propia

5. **Revisión**

   - **Identificar cuellos de botella, limitaciones o desafíos**

     Si bien el estudio se realizó con un dispositivo móvil Android en funcionamiento y desbloqueado, es importante considerar los escenarios en que el dispositivo sospechoso se encuentre bloqueado, con la pantalla no funcional o sin batería. En estos casos, se hace necesario implementar herramientas y mecanismos alternativos para la extracción de evidencia digital.

   - **Desarrollar nuevas guías y mejores prácticas para la adquisición de evidencia digital**

     Se ha desarrollado una guía detallada para el adecuado uso de la herramienta Avilla Forensics, y también un modelo de informe pericial, los cuales se pueden visualizar en los anexos.

Capítulo IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

El objetivo primordial de este estudio fue evaluar técnicas forenses avanzadas para la extracción y análisis de evidencias electrónicas de la aplicación de mensajería WhatsApp en dispositivos Android. Mediante un enfoque metodológico riguroso que integró análisis cualitativos y cuantitativos, se abordaron los desafíos específicos presentados por la encriptación de extremo a extremo de WhatsApp.

En la fase inicial del estudio, se llevó a cabo un análisis exhaustivo de la arquitectura y los mecanismos de seguridad de WhatsApp, identificando puntos clave para la aplicación confiable de técnicas forenses. Este análisis cualitativo resultó fundamental para comprender los desafíos técnicos y legales del proceso forense.

Luego, se adquirió y configuró un dispositivo Android para simular escenarios realistas de uso de WhatsApp y evaluar la efectividad de las técnicas forenses.

A través de un proceso iterativo de desarrollo y evaluación, se exploraron diversos enfoques para la extracción y análisis de datos de WhatsApp, tanto a nivel de software como de hardware. Estas técnicas se evaluaron rigurosamente en términos de su capacidad para extraer diferentes tipos de datos, preservar la integridad de las pruebas y

cumplir con los requisitos legales y éticos.

Los resultados de esta investigación contribuyen significativamente al avance del conocimiento y las capacidades forenses en el análisis de evidencias electrónicas de WhatsApp en dispositivos Android. Las técnicas desarrolladas ofrecen a los profesionales forenses e investigadores legales herramientas confiables y efectivas para recopilar y analizar pruebas cruciales en casos relacionados con WhatsApp, lo que resulta vital en la lucha contra el cibercrimen y la resolución de disputas legales.

Además de su aporte práctico, este estudio también proporciona valiosos conocimientos teóricos sobre los desafíos y técnicas involucradas en el análisis forense de aplicaciones de mensajería encriptadas en dispositivos móviles. Los hallazgos y métodos presentados pueden servir como base para futuras investigaciones y desarrollos en este campo en constante evolución.

4.2. Recomendaciones

Recomendamos continuar con la investigación y desarrollo de técnicas forenses adaptativas que puedan mantenerse al día con los cambios tecnológicos, especialmente enfocándose en automatizar y simplificar los procesos forenses relacionados con el aná-

lisis de WhatsApp en dispositivos Android. Además, se sugiere explorar métodos para la extracción de datos de otras aplicaciones de mensajería encriptadas. Por último, se insta a desarrollar herramientas y flujos de trabajo más intuitivos y fáciles de usar para el análisis forense de dispositivos móviles en general, lo que mejorará la eficiencia y la precisión de las investigaciones.

BIBLIOGRAFÍA

Alhassan, J. K. e. a. (2017, October). Forensic acquisition of data from a crypt 12 encrypted database of whatsapp. En *2nd international engineering conference.*

AlHidaifi, S. (2018). Mobile forensics: Android platforms and whatsapp extraction tools. *International Journal of Computer Applications*, *179*(47), 25–29. doi: 10.5120/ijca2018917264

Autopsy, una herramienta de análisis digital forense. (2020). Descargado de https://www.tusclases.com.ar/blog/autopsy-herramienta-analisis-digital-forenseÂă

Avilla, D. (s.f.). *Avillaforensics: Avilla forensics 3.0.* Descargado de https://www.avillaforensics.com/ (https://www.avillaforensics.com/)

Bommisetty, S., Tamma, R., y Mahalik, H. (2014). *Practical mobile forensics* (1st ed.). Packt Publishing. Descargado de https://www.packtpub.com/product/practical-mobile-forensics/9781783288311

Clement, J. (s.f.). *most popular global mobile messaging apps 2020.* Descargado de https://www.statista.com/statistics/307143/growth-of-whatsapp-usage-worldwide/

Consejo de la Judicatura de Ecuador. (2015). *Reglamento del sistema permicial integral de la función judicial.* Registro Oficial. Descargado de https://www.funcionjudicial.gob.ec/index.php/es/normativa/reglamentos/5173-reglamento-del-sistema-permicial-integral-de-la-funcion-judicial.html (Registro

Oficial Suplemento No. 573)

Developers, A. (2024). *Arquitectura de la plataforma.* Descargado de https://developer.android.com/guide/platform?hl=es-419

Dixon, S. J. (2024). Most popular messaging apps 2024. *Statista*. Descargado de https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Ekanayake, N. (2018, July). Android operating system. En (pp. 1–11). doi: 10.13140/RG.2.2.20829.72169

et al., U. (2019). Analysis whatsapp forensic and visualization in android smartphone with support vector machine (svm) method. En *Journal of physics: Conference series* (Vol. 1196). doi: 10.1088/1742-6596/1196/1/012064

Forensics, A. (s.f.). *Avilla forensics.* Descargado de https://www.ucapem.group/site/repositorio/avilla-f/Âă

Han, E. S., y Goleman, R. M. A., Daniel; Boyatzis. (2019). Is whatsapp the future of workplace communication?: Investigating the use of whatsapp in decision-making episodes. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Jhala, K., y Ghote, L. L. (2015). Whatsapp forensics: Decryption of encrypted whatsapp databases on non rooted android devices. *Journal of Information Technology Software Engineering*, *05*(02), 2–5. doi: 10.4172/2165-7866.1000147

Johansen, G. (2018). *Digital forensics and incident response: Incident response techniques and procedures*. Apress. Descargado de https://www.apress.com/gp/book/9781484238379

Khan, J., y Shahzad, S. (2016). Android architecture and related security risks. *Asian Journal of Technology Management Research*, *05*(December 2015), 2249–892.

Mohd Omar, N. A. A., y Sani, N. A. (2020). Is whatsapp the future of workplace communication?: Investigating the use of whatsapp in decision-making episodes. *Journal of Nusantara Studies*, *5*(1), 414–442. doi: 10.24200/jonus.vol5iss1pp414-442

Rafael_L_R. (2012, 23 de oct). Iso/iec 27037:2012 nueva norma para la recopilación de evidencias. *Perito Informático y Tecnológico - PeritoIT*. Descargado de https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/

Reiber, L. (2018). *Mobile forensic investigations: A guide to evidence collection, analysis, and presentation*. McGraw-Hill Education. Descargado de https://www.mheducation.com/highered/product/mobile-forensic-investigations-guide-evidence-collection-analysis-presentation-reiber/M9781260117192.html

República del Ecuador. (2002). *Ley de comercio electrónico, firmas y mensajes de datos*. Registro Oficial. Descargado de https://www.contraloria.gob.ec/Ley_de_Comercio_Electronico_Firmas_y_Mensajes_de_Datos.pdf (Registro Oficial Suplemento No. 557)

República del Ecuador. (2015). *Código orgánico general de procesos (cogep)*. Registro Oficial. Descargado de https://www.funcionjudicial.gob.ec/www/pdf/cogep.pdf (Registro Oficial Suplemento No. 506)

República del Ecuador. (2021). *Código orgánico integral penal (coip)*. Registro Oficial. Descargado de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf (Registro Oficial Suplemento No. 180)

Roa, M. M. (s.f.). *El mapa mundial de android e ios.* Descargado de https://es.statista.com/grafico/29620/sistema-operativo-movil-con-la-mayor-cuota-de-mercado-por-pais/

Shidek, C. N., H., y Wardana, A. A. (2020). Whatsapp chat visualizer: A visualization of whatsapp messenger's artifact using the timeline method. *International Journal on Information and Communication Technology (IJoICT)*, *6*(1). doi: 10.21108/ijoict.2020.61.489

Studytonight. (2020). *Android architecture - software stack of android*. Study tonight Technologies Pvt. Ltd. Descargado de https://www.studytonight.com/android/android_architecture#

Udenze, S., y Oshionebo, B. (2020). Investigating "whatsapp" for collaborative learning among undergraduates. *Etkileşim*, *3*(5), 24–50. doi: 10.32739/etkilesim.2020.5.92

Umar, R. I., R., y Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(3), 949–955. doi: 10.18517/ijaseit.8.3.3591

Informe Forense

Link: Descargar Informe Forense

UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

AUTORES: Edison Condor

Angel García

Isaac Velasco

Daniel Velasco

Informe Forense

QUITO – ECUADOR | 2024

Antecedentes.

El presente informe de análisis forense se lleva a cabo como parte del requisito de graduación del máster y tiene como objetivo aplicar los conocimientos y habilidades adquiridos durante el programa en un escenario práctico de análisis forense digital.

La investigación se centra en la recuperación de conversaciones de WhatsApp en un dispositivo móvil Huawei MED-LX9 con sistema operativo Android 10. Esta tarea desempeña un papel crucial en el proyecto final, ya que proporciona una oportunidad para aplicar técnicas y metodologías de análisis forense digital en un entorno real.

El análisis forense se llevará a cabo utilizando la herramienta Avilla Forensics, la cual se especializa en realizar análisis sobre el aplicativo WhatsApp proporcionando una visión integral de las conversaciones de WhatsApp almacenadas en el dispositivo, así como cualquier otra información relevante para la investigación.

Análisis.

El desarrollo del análisis se realizará en base al modelo armonizado, siguiendo cada una de las etapas las cuales se describen a continuación.

Fase de Preparación.

Objetivos:

- Recuperar las conversaciones de WhatsApp almacenadas en el dispositivo para su posterior análisis.
- Garantizar la preservación adecuada de la integridad y autenticidad de la evidencia digital para su posterior presentación.
- Realizar un análisis detallado de la evidencia digital recuperada para identificar posibles conversaciones borradas.

Identificación de recursos:

Para el desarrollo de la investigación se utilizaran las siguientes herramientas.

HERRAMIENTAS	
HERRAMIENTAS FORENSES	Avilla Forensics IPEDTools
RESPALDO DE DATOS	Avilla Forensics

Información del dispositivo a analizar.

ESTADO Y CARACTERISTICAS DEL DISPOSITIVO			
Estado del dispositivo	**Encendido**	**X**	**Apagado**
Protegido por algún tipo de clave	**SI**	**X**	**NO**
EN CASO DE TENER PROTECCIÓN (TIPO)			
Patrón		X	
PIN			
Contraseña			

Huella digital	
Reconocimiento Facial	
CARACTERÍSTICAS DEL DISPOSITIVO	
Marca del teléfono	HUAWEI
Modelo del teléfono	MED-LX9
Numero serial IMEI	862229045141324

Definición de roles:

El análisis lo realizaron los cuatro estudiantes de la carrera Máster en Ciberseguridad, con los siguientes roles.

Nombres	Rol
García Adum Ángel Cristóbal	**Líder del equipo**
Cóndor Licero Edison Richard	**Analista forense**
Velasco Pilpe Daniel Esteban	**Analista forense**
Velasco Pilpe Isaac Israel	**Analista forense**

Fase de Preparación.

Desarrollo del plan:

Se describe el desarrollo del plan a seguir.

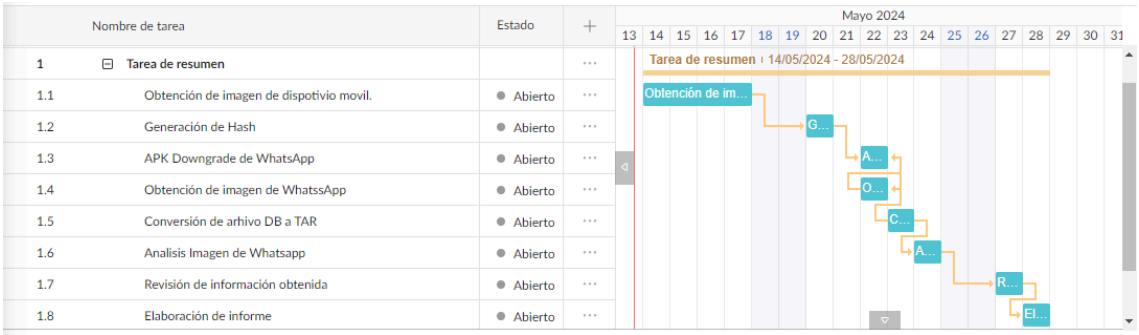


Ilustración 1 Diagrama de GANT

- Obtención de imagen del dispositivo. – en esta etapa se generará la imagen del dispositivo para poder realizar la manipulación sobre esta y no directamente sobre el dispositivo.
- Generación de HASH. – la generación del HASH permitirá garantizar que se está trabajando sobre la imagen obtenida sin una manipulación de la información.
- APK Downgrade de WhatsApp. – este procedimiento se realiza para poder obtener un respaldo de la aplicación, evitando las seguridades de las nuevas versiones.
- Obtención de imagen de Whatsapp. – esta imagen nos permitirá realizar un análisis de los chats, llamadas, archivos que contenga la aplicación.
- Conversión de archivo DB a TAR. – la imagen se genera en extensión .db, sin embargo es necesario realizar una conversión a .tar para poder realizar el análisis.
- Revisión de información. – este proceso mostrará la información de la aplicación.
- Elaboración de informe. – es necesario realizar un informe donde se detalla las evidencias encontradas.

Fase de Recopilación.

En esta fase se procede a realizar una imagen del dispositivo, la cual será parte del análisis con el fin de precautelar los datos.

Se requiere:

- El dispositivo desbloqueado
- El dispositivo en modo avión
- El dispositivo en modo desarrollador
- Activar depuración por USB
- Activar que no se bloqueé el dispositivo durante el proceso de respaldo

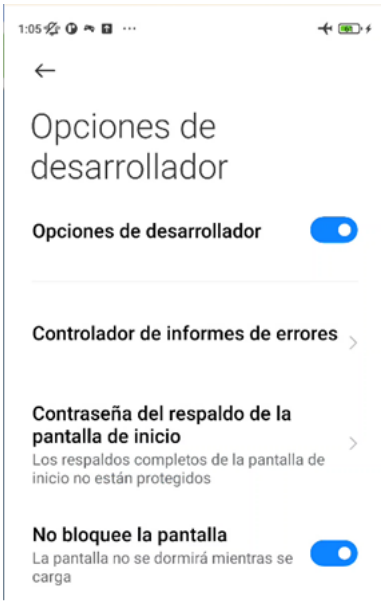


Ilustración 2 Activar opciones de desarrollador.

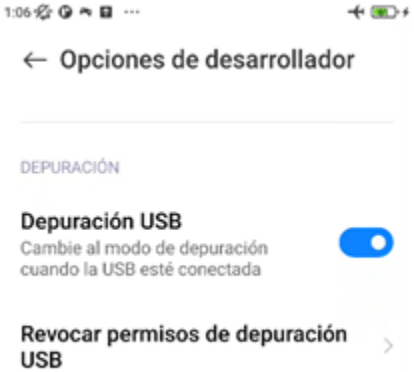


Ilustración 3 Activar depuracion USB.

Una vez que cumplimos con los pasos detallados, procedemos a obtener la imagen a través de la herramienta Avilla Forensics, para lo cual conectamos el dispositivo al computador.

Ilustración 4 Avilla Forensics

Realizamos clic en Test de conexión, esto nos permitirá validar que la herramienta vea al dispositivo, si el test es correcto, observamos el dispositivo Android que tenemos conectado, así como el modelo.

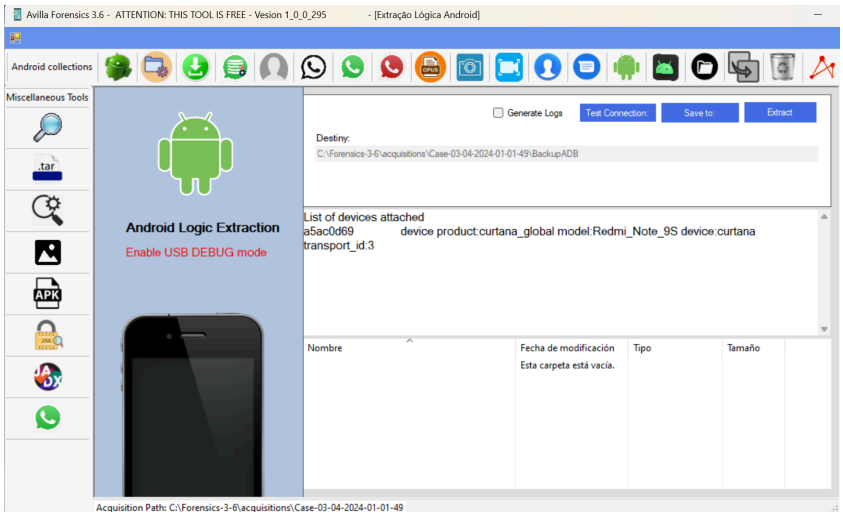


Ilustración 5 Test de Conexión

Una vez que el test es correcto, procedemos a generar la imagen del dispositivo, para lo cual damos clic en  , este proceso puede tardar, todo dependerá de la cantidad de información del dispositivo.

Ilustración 6 Obtensión de imagen.

Una vez que el respaldo se generó, procedemos a clic en detect  , para ver qué aplicaciones pueden ser realizadas un análisis forense, en este caso observamos que nos indica que se puede analizar WhatssApp.

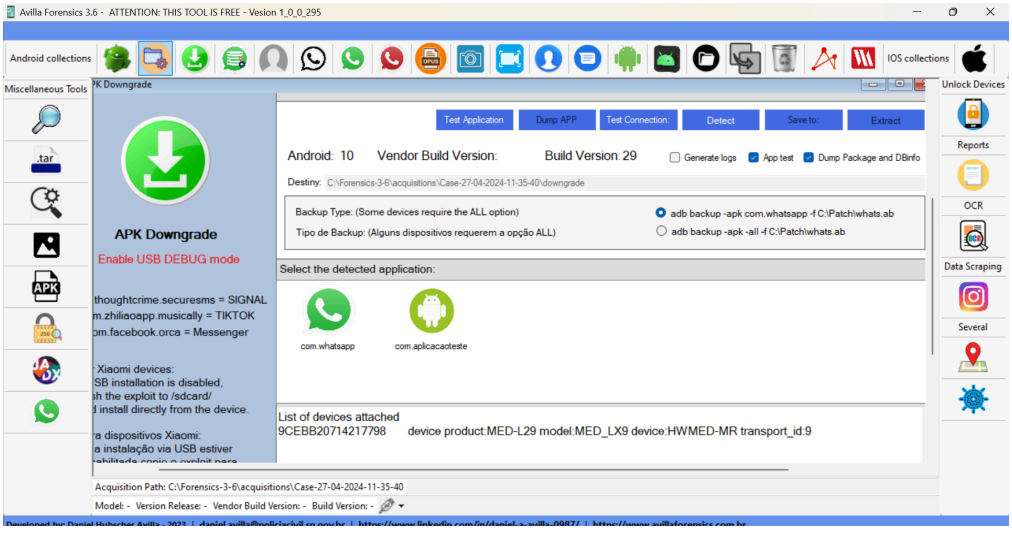


Ilustración 7 Verificación de Apps.

Procedemos a realizar el downgrade de la aplicación whatsapp para evitar que los filtros de seguridad o encriptación nos impidan realizar el análisis, para lo cual damos clic en  y guardamos el contenido de la aplicación en un repositorio.

El aplicativo solicita realizar un reinicio para realizar el proceso de downgrade.

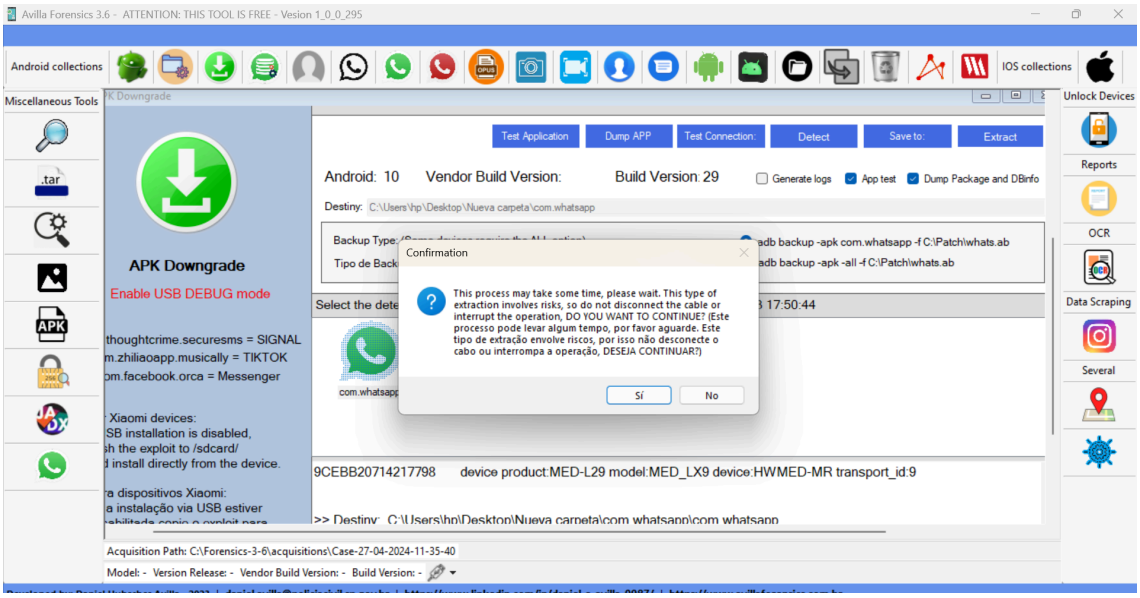


Ilustración 8 Downgrade de app.

Una vez que el proceso culmine se generará un archivo .db.

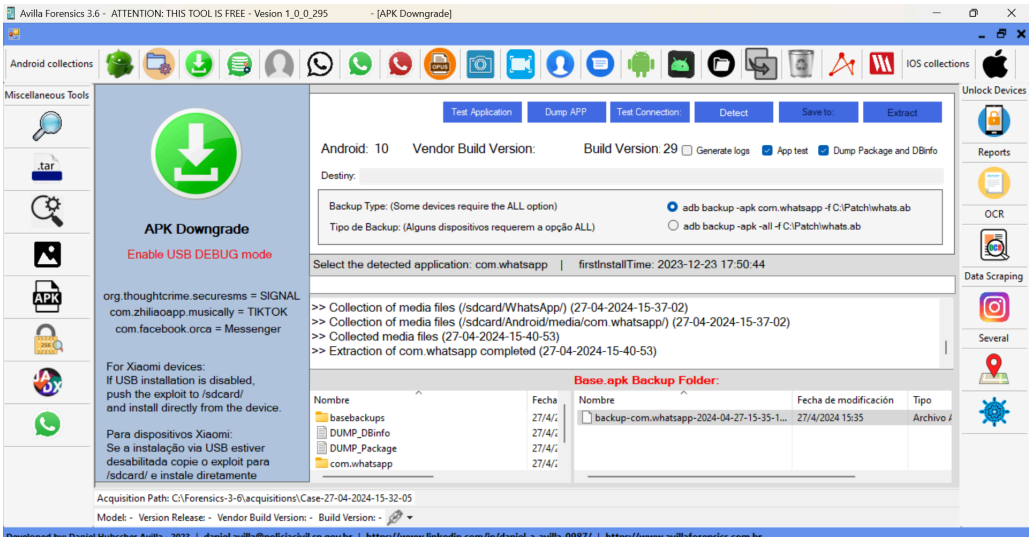


Ilustración 9 Downgrade exitoso.

Nombre	Fecha de modificación	Tipo	Tamaño
backup-com.whatsapp-2024-04-27-15-35-15.ab	27/4/2024 15:35	Archivo AB	46.001 KB

Ilustración 10 Archivo DB.

Una vez que obtenemos el archivo .db, procedemos a realizar una conversión a .tar, esto permitirá que la información sea legible y analizable.

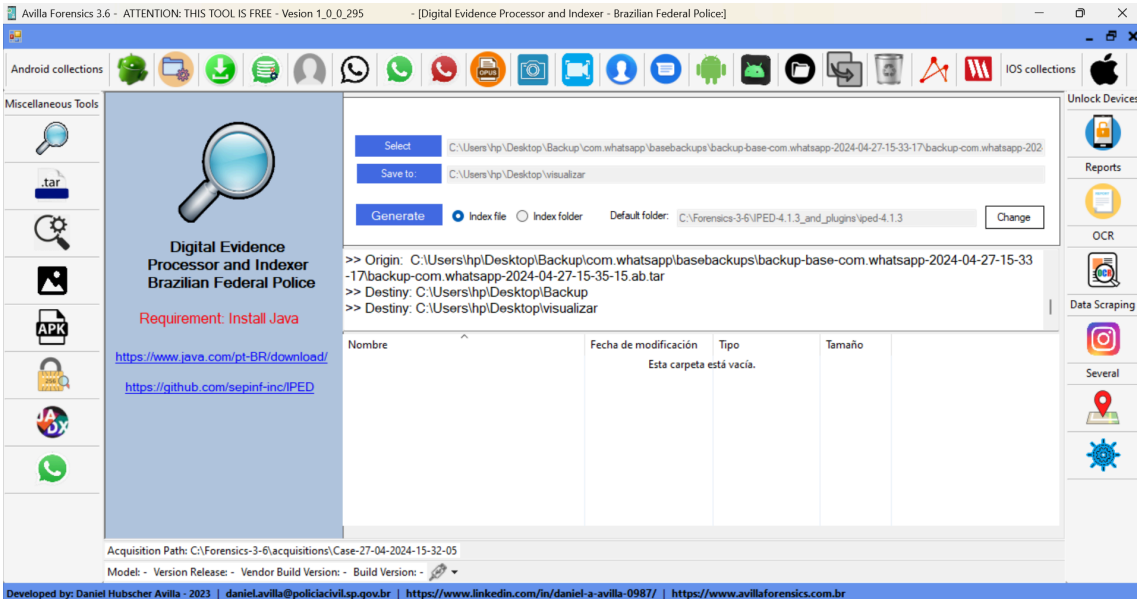


Ilustración 11 Conversión .TAR.

Una vez realizada la conversión, procedemos a realizar el análisis de la información del respaldo de WhatsApp.

Ilustración 12 Analisis de la informacion.

Fase de Verificación.

En esta fase, se procede a generar el hash de verificación, en este caso usaremos el algoritmo SHA256, para la generación de este, lo realizamos con la herramienta Quick HASH.

El hash SHA256 es:

B65A7EA1C866BF24C39B22BB04619A2C48A2E3394CCCBF14ADE47320874ACC08

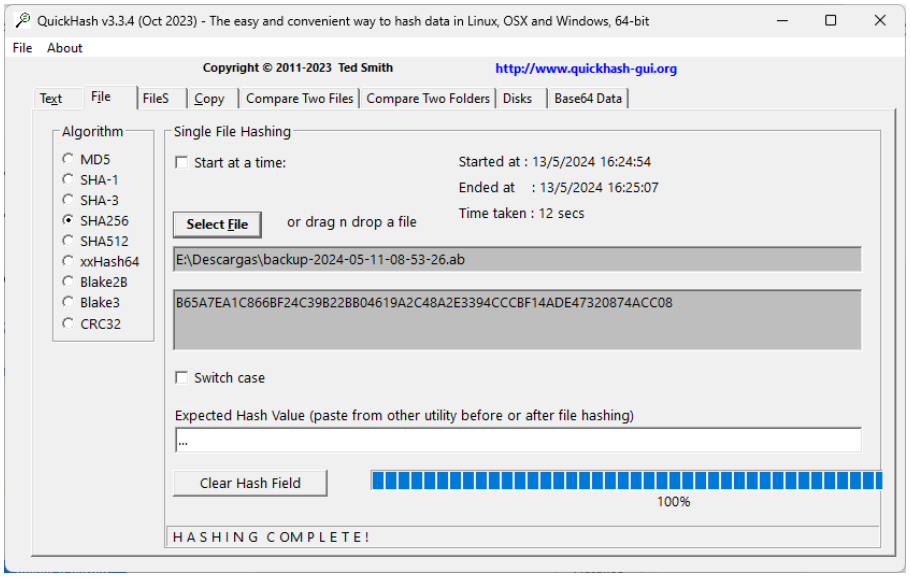


Ilustración 13 Generación Hash.

Este procedimiento también se puede realizar a través de Avilla Forensics, el cual genera el mismo hash que se obtuvo.

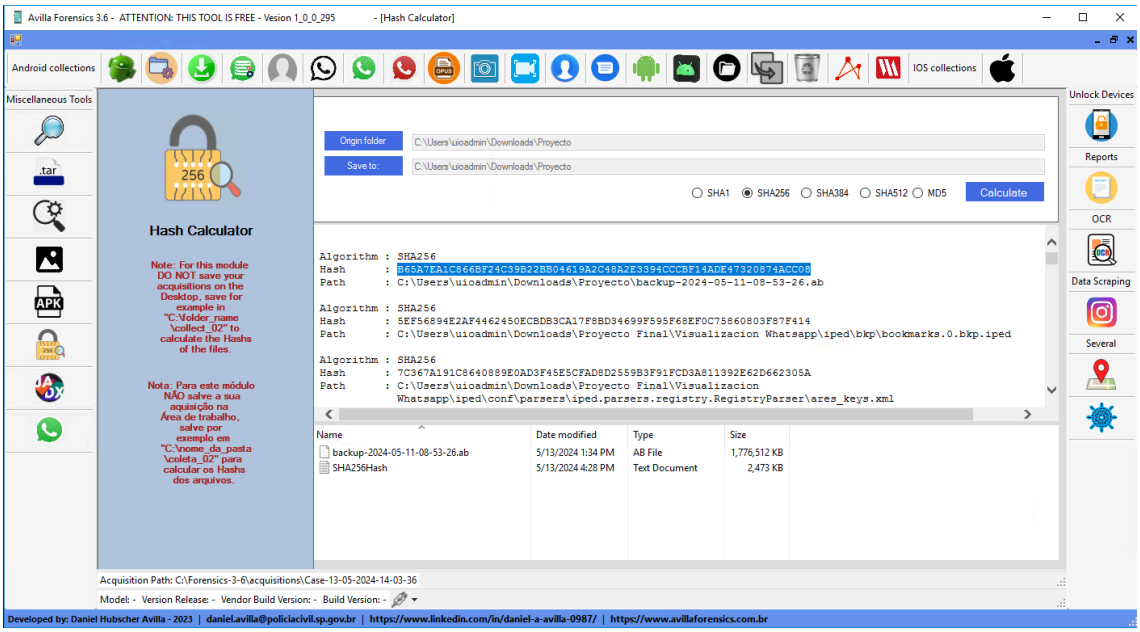


Ilustración 14 HASH

Fase de interpretación.

Evaluación de los resultados del análisis. – una vez ejecutado el análisis de la herramienta Avilla Forensics, podemos observar la información que obtuvo la herramienta.

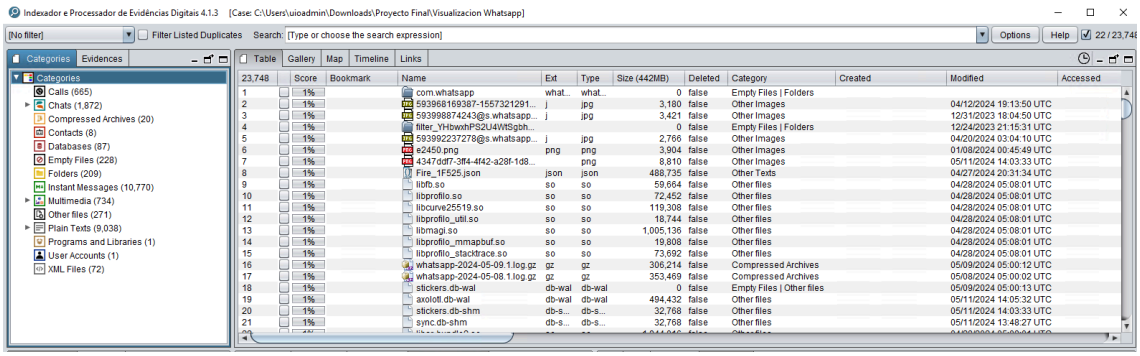


Ilustración 15 Evidencia Obtenida.

Tipo de evidencia	Cantidad
Llamadas	665
Chats	1.872
Archivos comprimidos	20
Contactos	8
Bases de datos	87
Archivos Vacíos	228
Carpetas	209
Mensajes instantáneos	10.770
Archivos multimedia	734
Otros Archivivos	271
Cuentas	1

Análisis de llamadas.

Se evidencia que existe un registro de 665 llamadas, en la pantalla principal nos permite el origen y el destino de las llamadas, así como si las llamadas fueron rechazadas o si hubo comunicación, se realiza un análisis de una muestra de llamadas realizadas en el dispositivo.

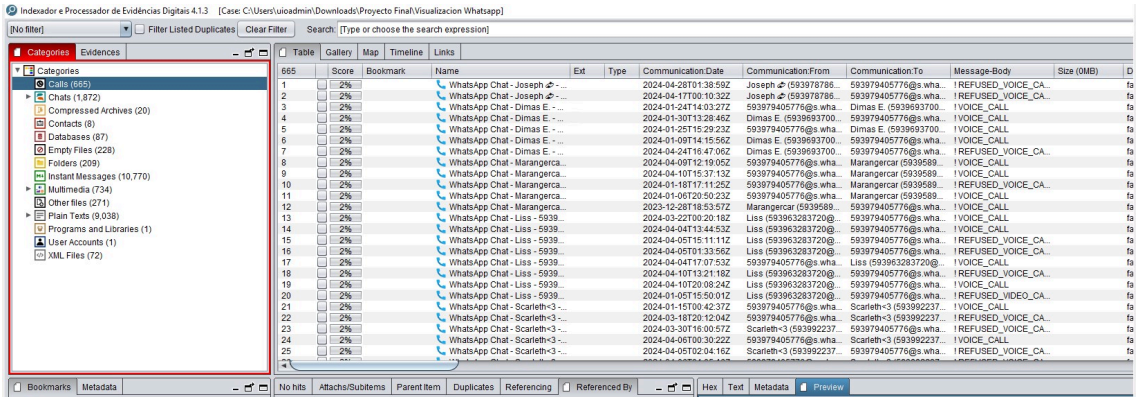


Ilustración 16 Llamadas.

La llamada 1, realizada entre Joseph (593978786714@s.whatsapp.net) y 593979405776@s.whatsapp.net, es rechazada y no tiene un tiempo de duración de la llamada.

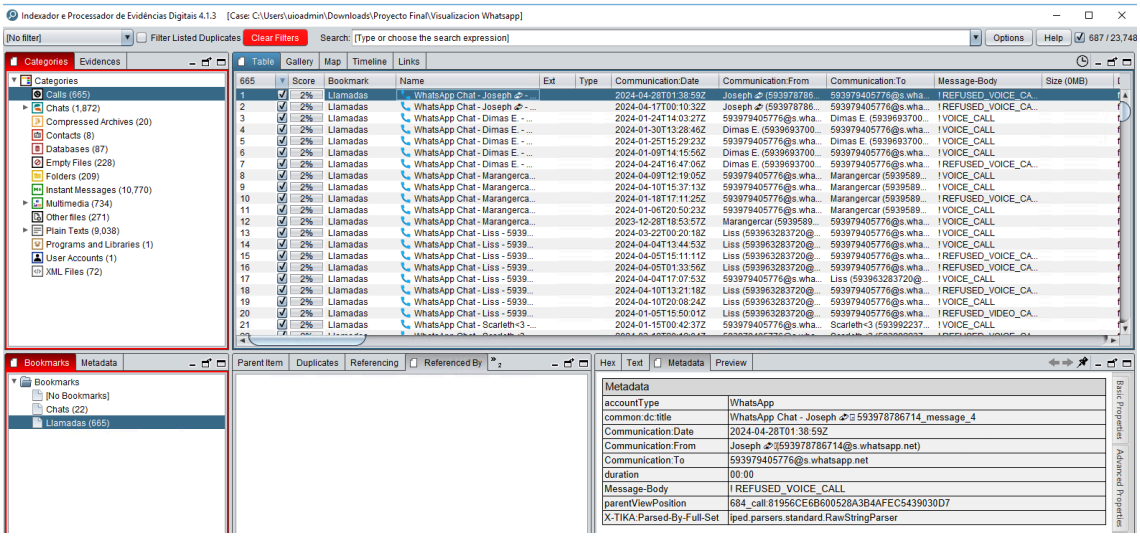


Ilustración 17 Llamada 1

En esta llamada podemos observar que existió una comunicación entre 593979405776@s.whatsapp.net y Dimas E. (593969370016@s.whatsapp.net) y la llamada tuvo una duración de 2 minutos 28 segundos.

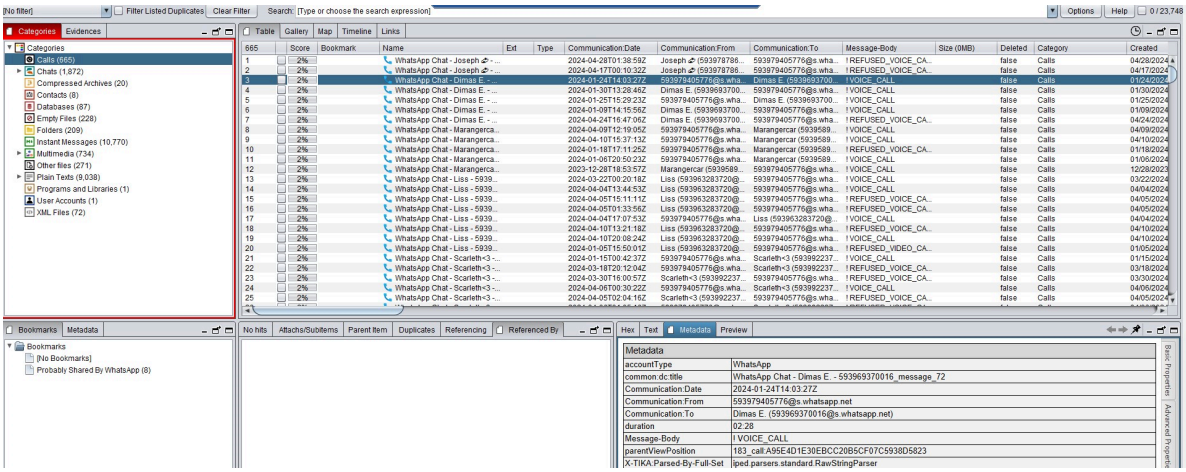


Ilustración 18 Llamada 2

En esta llamada podemos observar que existió una comunicación entre Dimas E. (593969370016@s.whatsapp.net) y 593979405776@s.whatsapp.net y la llamada tuvo una duración de 1 minuto 02 segundos.

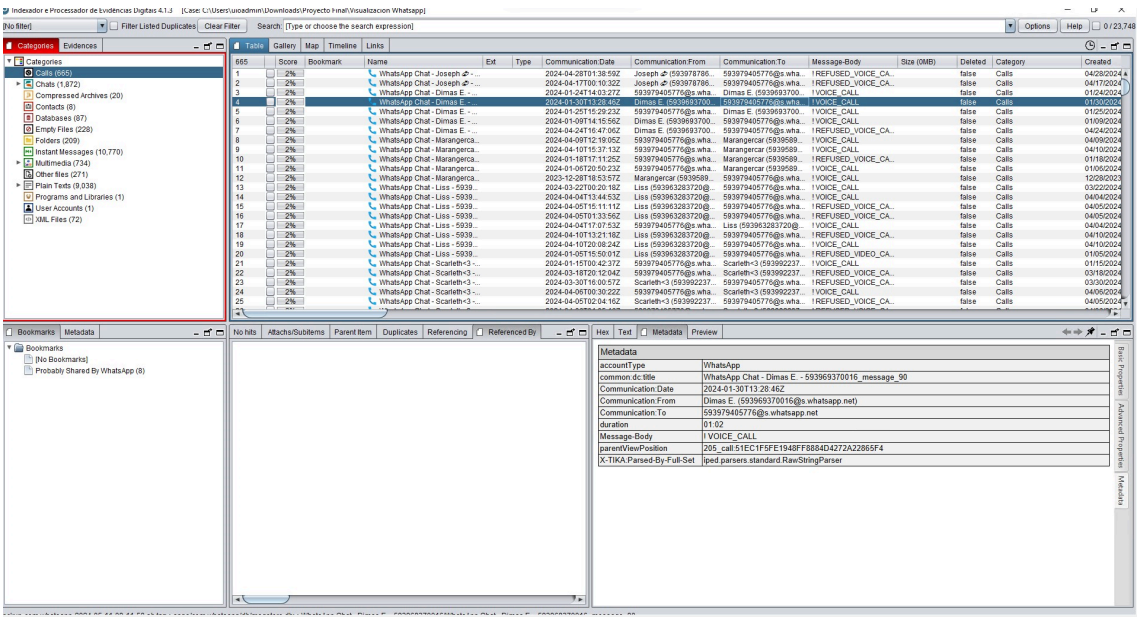


Ilustración 19 Llamada 3.

Por medio de la aplicación podemos ver si las llamadas fueron borradas o modificada la información, en este caso las llamadas no han sido borradas y tampoco existe una alteración en la información.

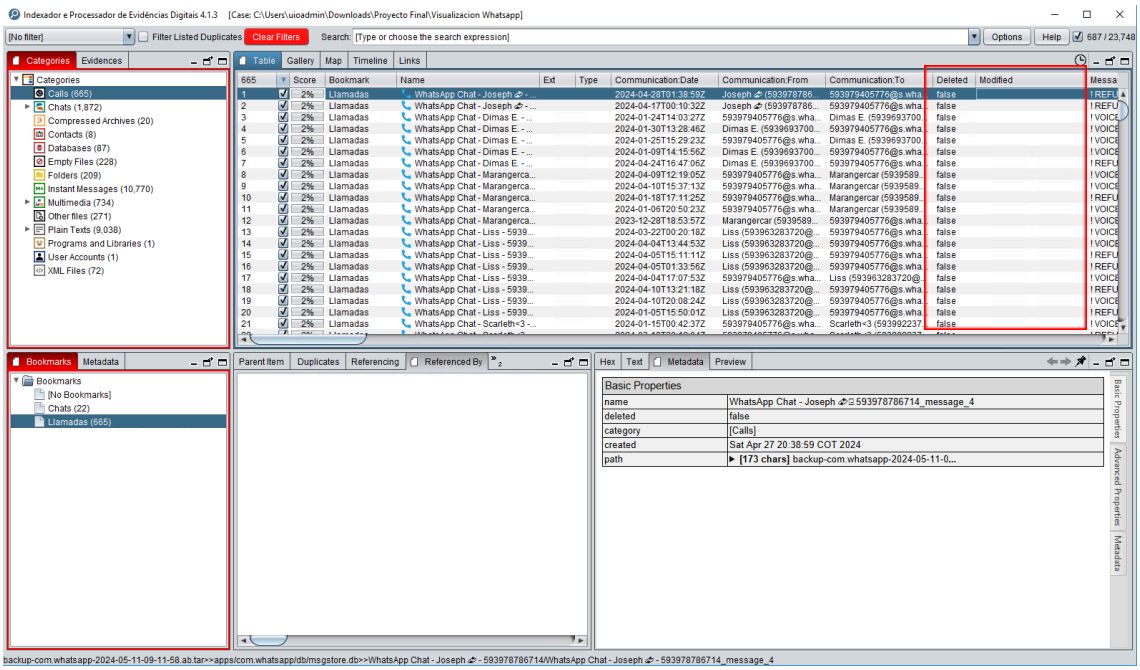


Ilustración 20 Alteración de llamadas.

La aplicación permite ver la línea de tiempo de las llamadas, esto nos permite observar cuando se realizaron de forma visual, con otro podemos determinar los días que más llamadas se tuvo.

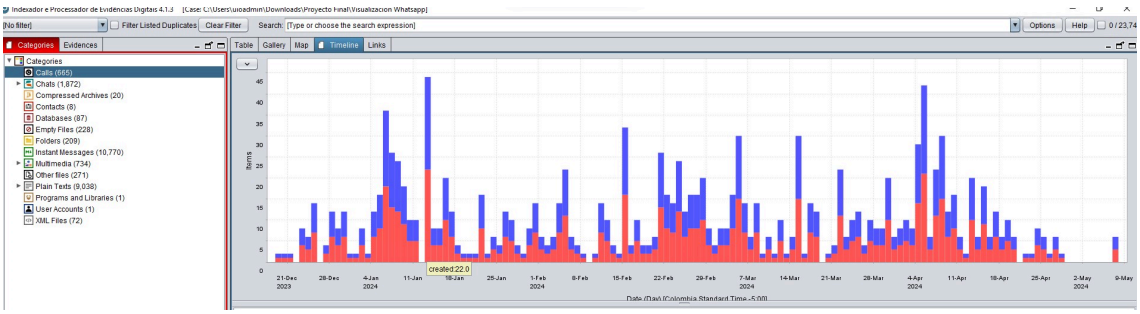


Ilustración 21 Linea de tiempo.

Podemos analizar también la forma en la que se interconectan las llamadas, esta herramienta nos permite ver un mapa de conexiones que realiza WhatsApp entre los dispositivos, tanto para llamadas punto a punto como grupales.

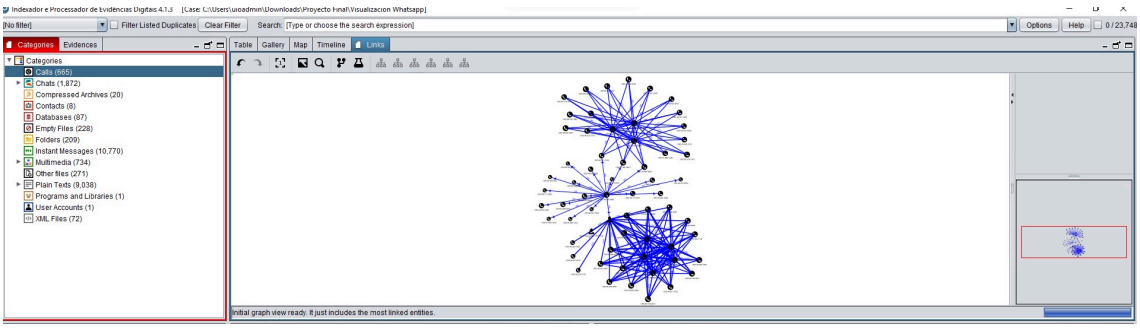


Ilustración 22 Mapa de conexiones.

Análisis de Chats.

Se evidencia que existe un registro de 1.872 chats, en la pantalla principal nos las conversaciones que se mantuvo a través de la app WhatsApp, así también como si fueron eliminados o modificados, así como el hash de cada uno de los mensajes, esta información es vital para evitar alteración en las evidencias.

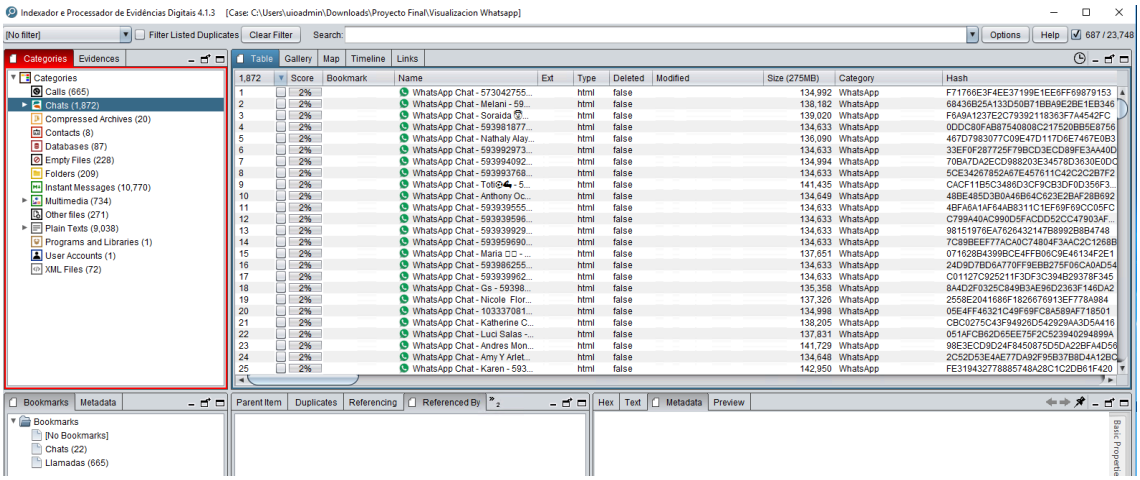


Ilustración 23 Chats

Aquí podemos observar una conversación de un grupo de WhatsApp.

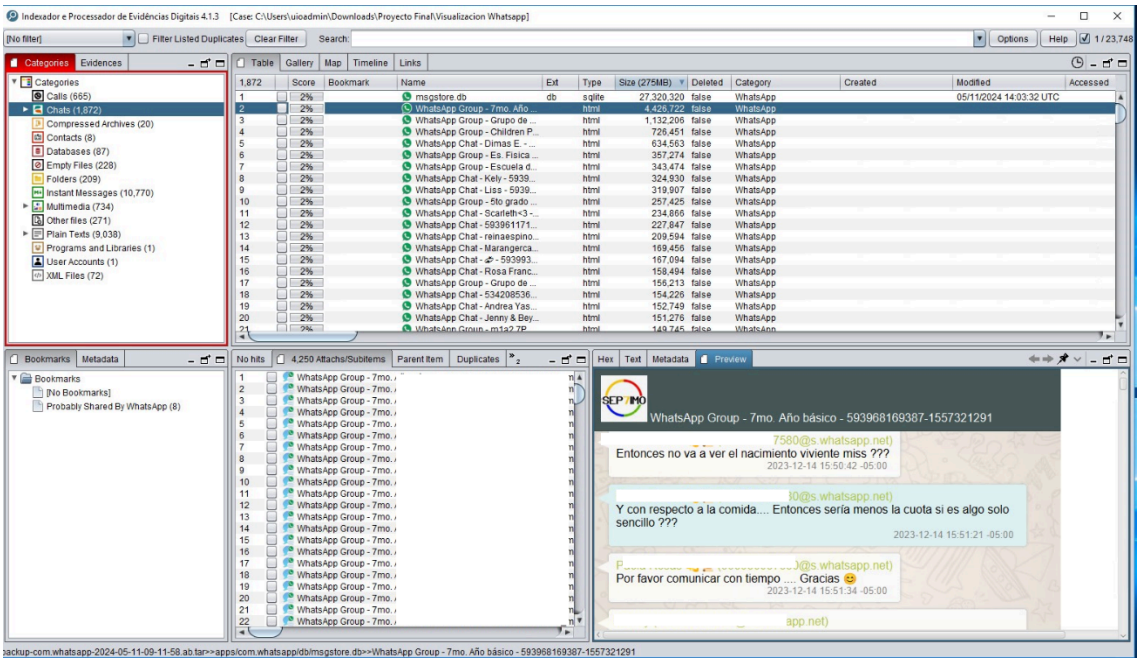


Ilustración 24 Conversación 1.

Así también podríamos ver la metadata de cada uno de los mensajes que se han realizado, aquí podemos observar cuando se envió el mensaje, el texto, el contacto que lo envió.

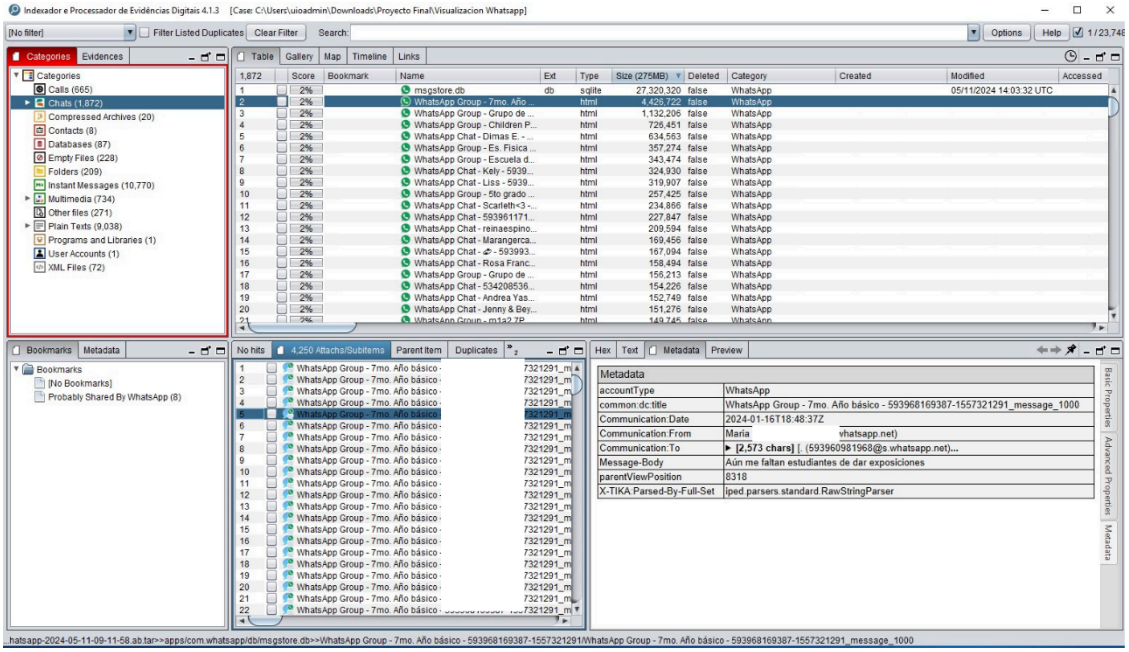


Ilustración 25 Analisis de Metadata.

Conversación de grupo de Whatsapp.

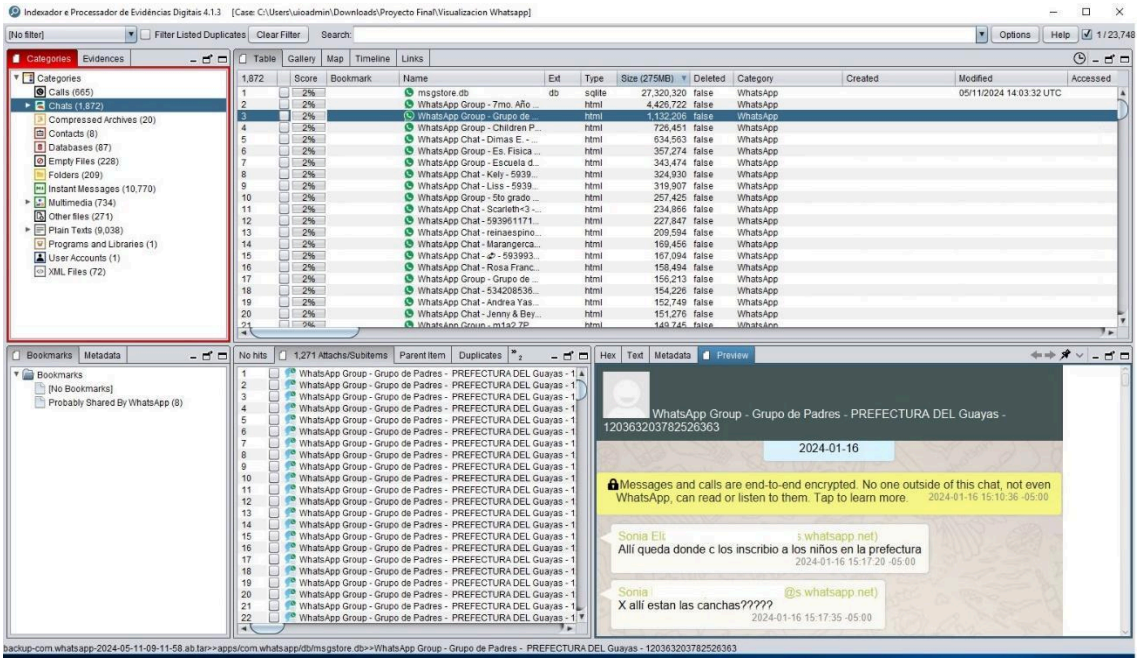


Ilustración 26 Conversación 2

Conversación mantenida con un contacto, aquí podemos observar el registro de las llamadas que se ha mantenido con este contacto.

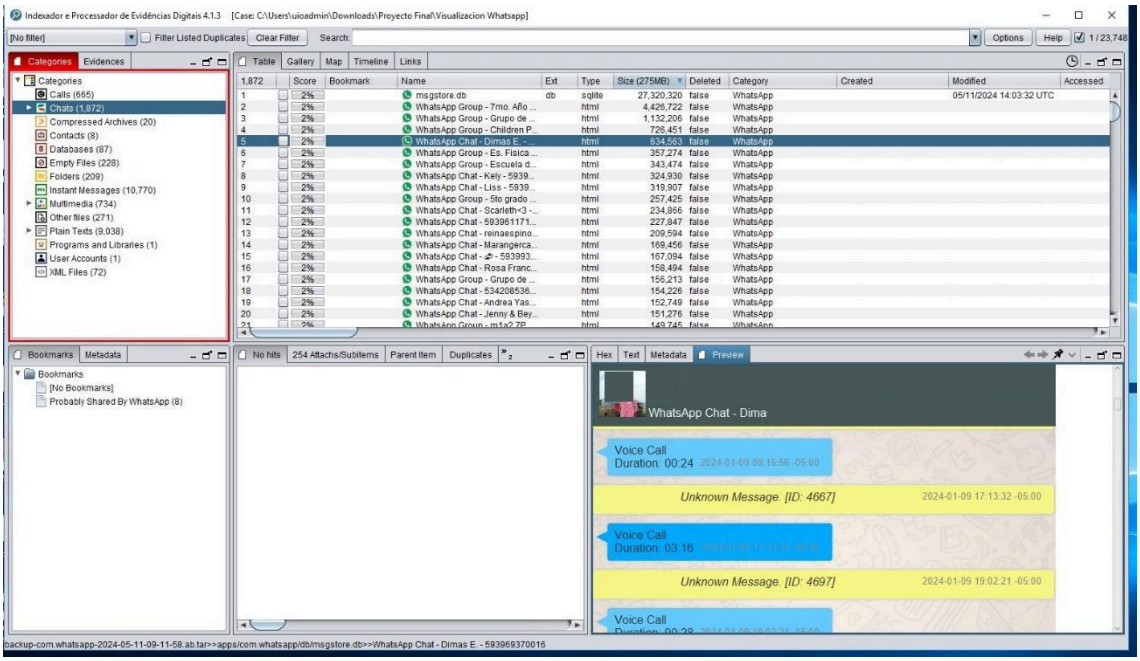


Ilustración 27 Conversación 3

Conversación de un grupo de WhatsApp.

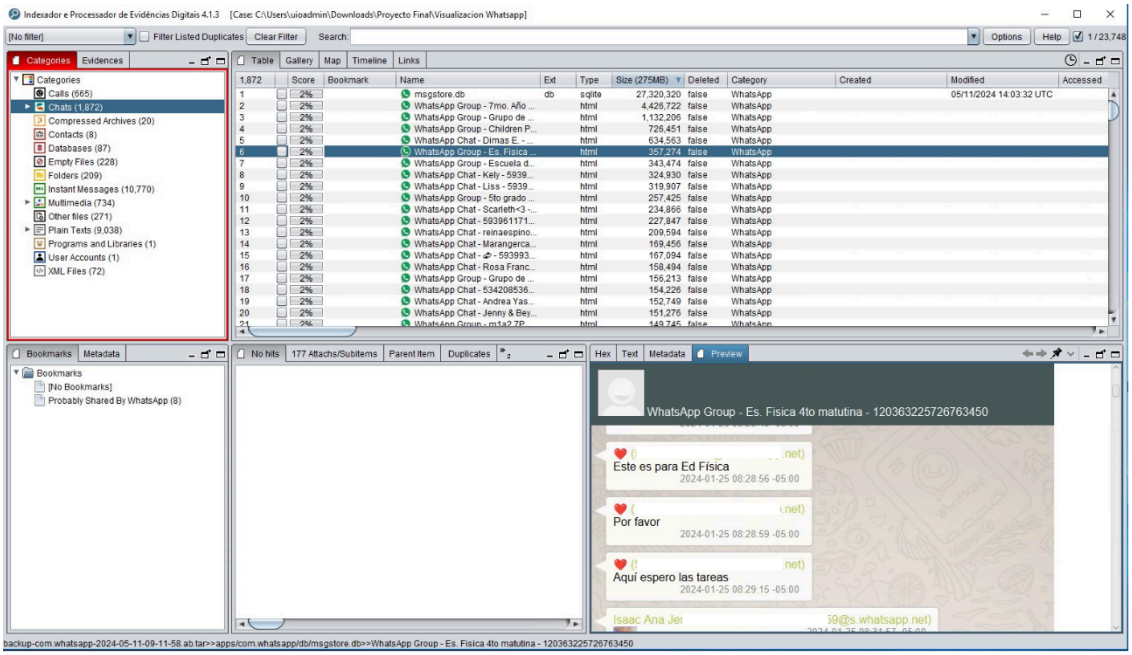


Ilustración 28 Conversación 4

Análisis de compartición de contactos.

Se evidencia que existe un registro de 8 contactos compartidos entre los chats.

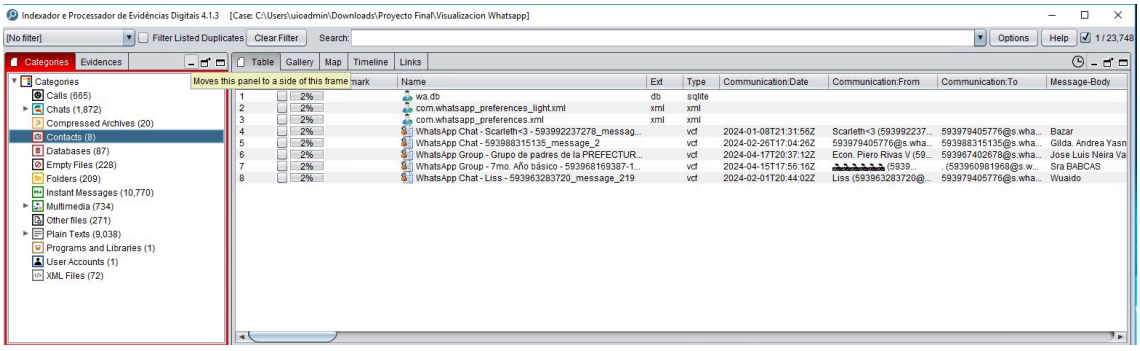


Ilustración 29 Compartición de contactos.

En las siguientes imágenes se puede evidenciar que se comparten los contactos y su respectiva información.

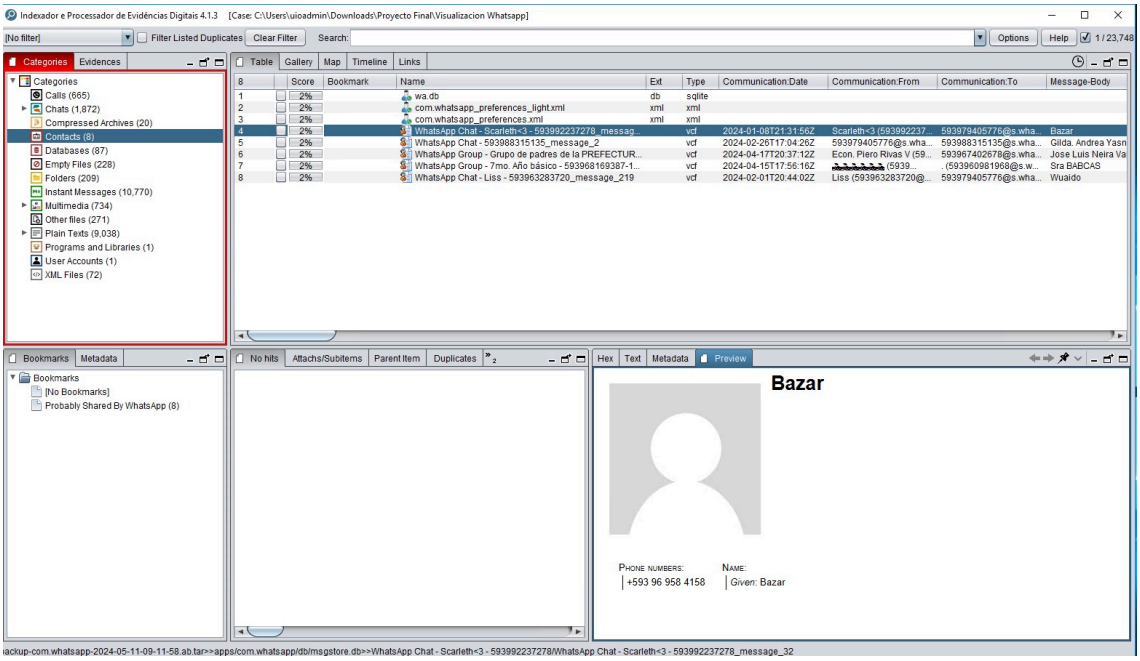


Ilustración 30 Contacto 1.

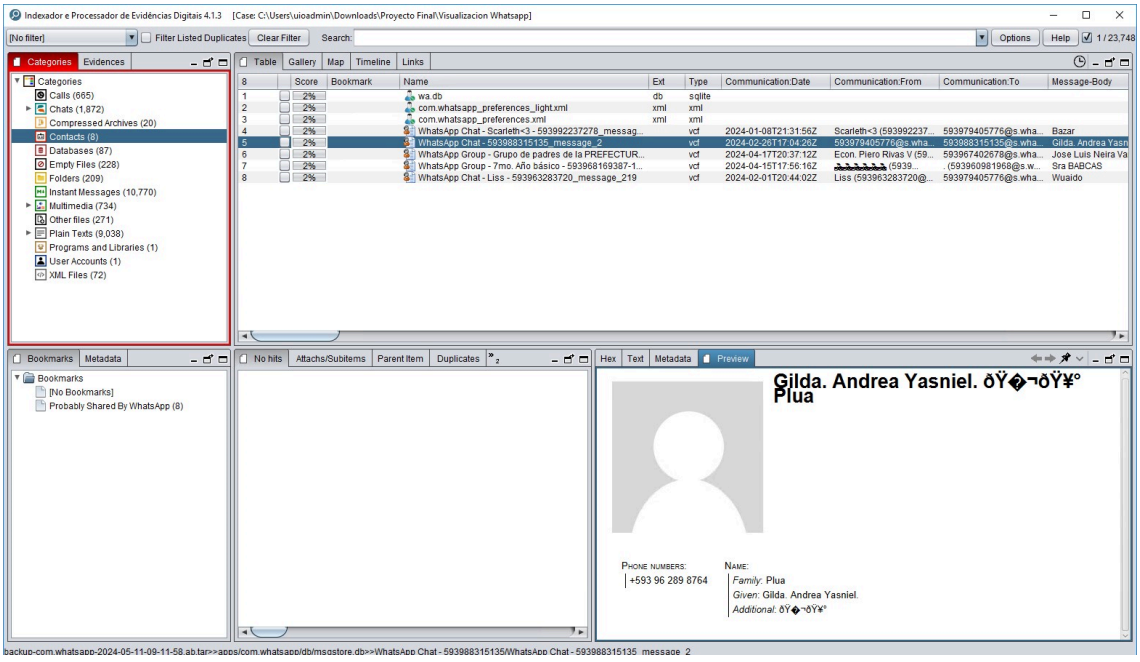


Ilustración 31 Contacto 2.

Análisis de mensajes.

Se evidencia que existe un registro de 10.770 mensajes en la aplicación, aquí podemos ver el origen y el destino de los mensajes, así como el contenido.

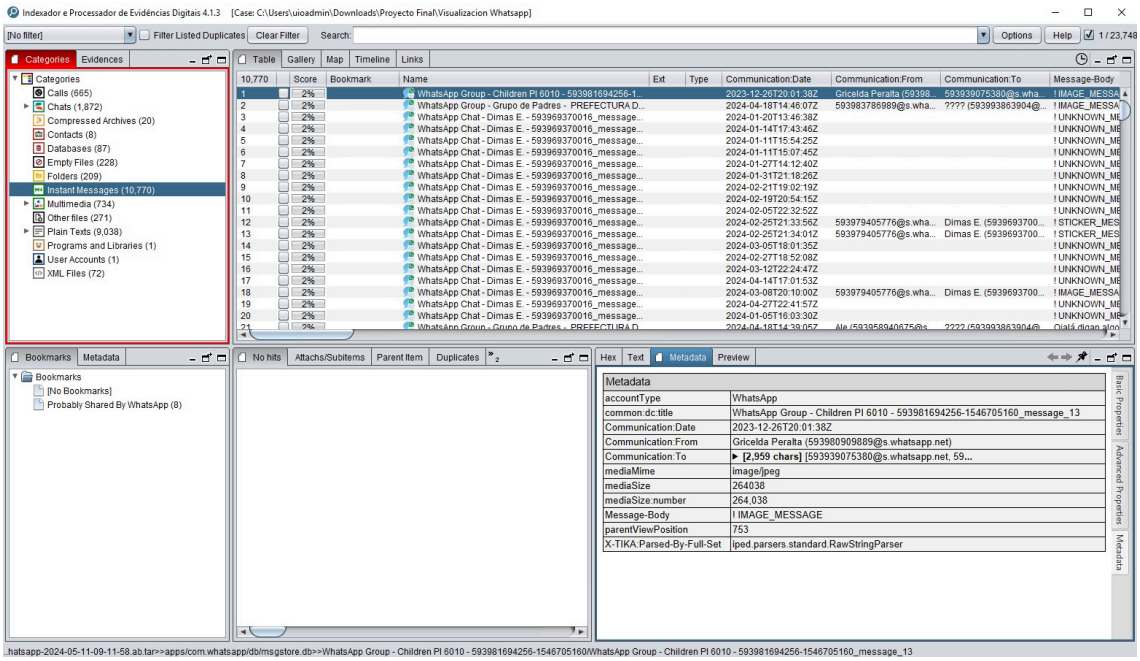


Ilustración 32 Mensajes

La herramienta permite realizar un análisis de Geolocalización de los mensajes, para esto es necesario que el dispositivo que envió el mensaje tenga activo el GPS.

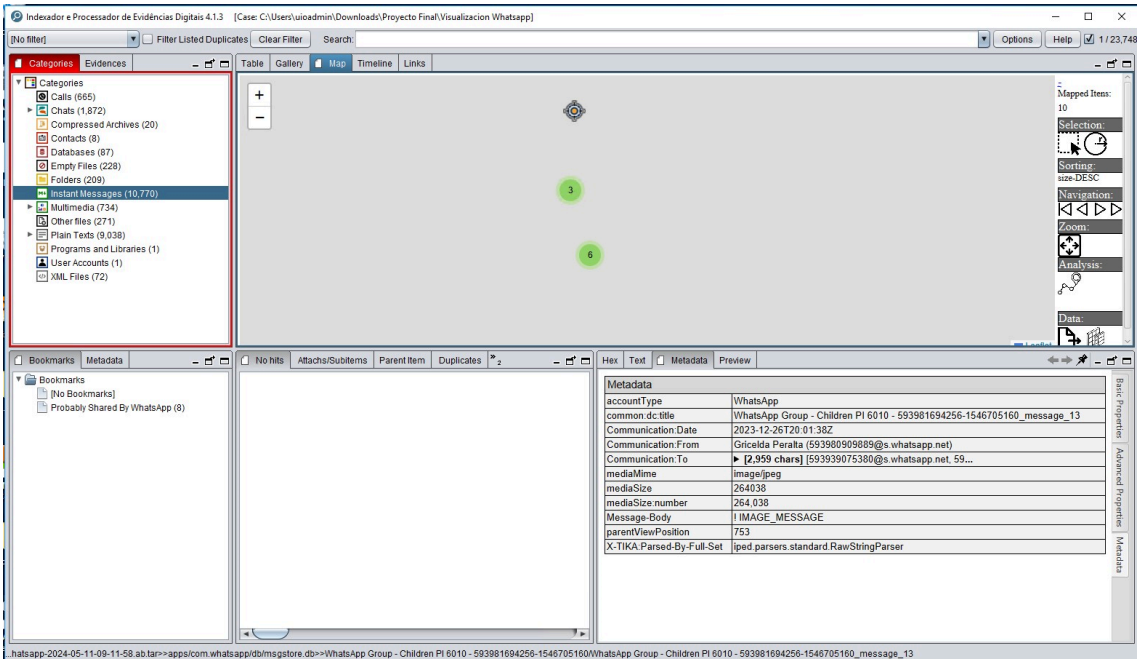


Ilustración 33 Mapa.

Aquí podemos ver las coordenadas de donde se envió el mensaje.

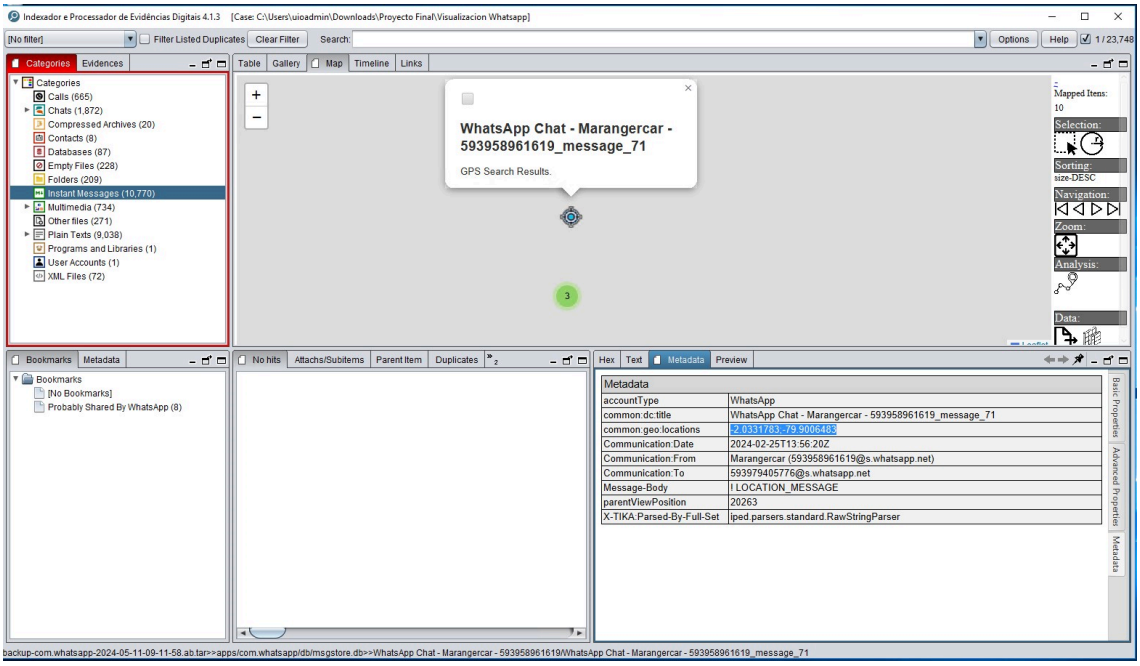
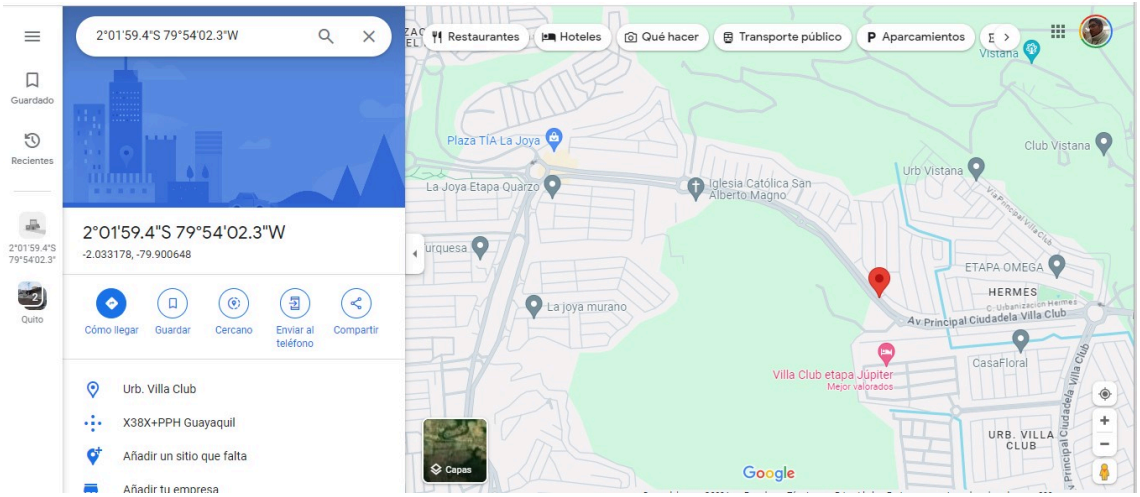


Ilustración 34 Coordenadas 1.

Analizamos las coordenadas y obtenemos la ubicación.



Se realiza el análisis de los mensajes con geolocalización y su ubicación en el mapa.

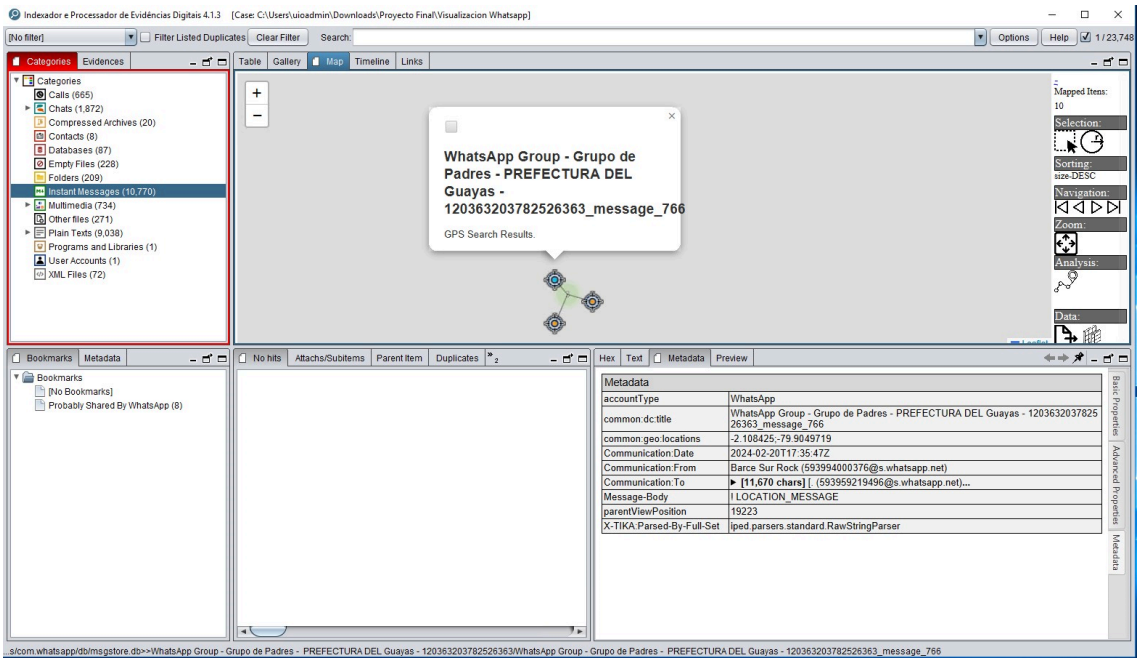


Ilustración 35 Geolocalización 2.

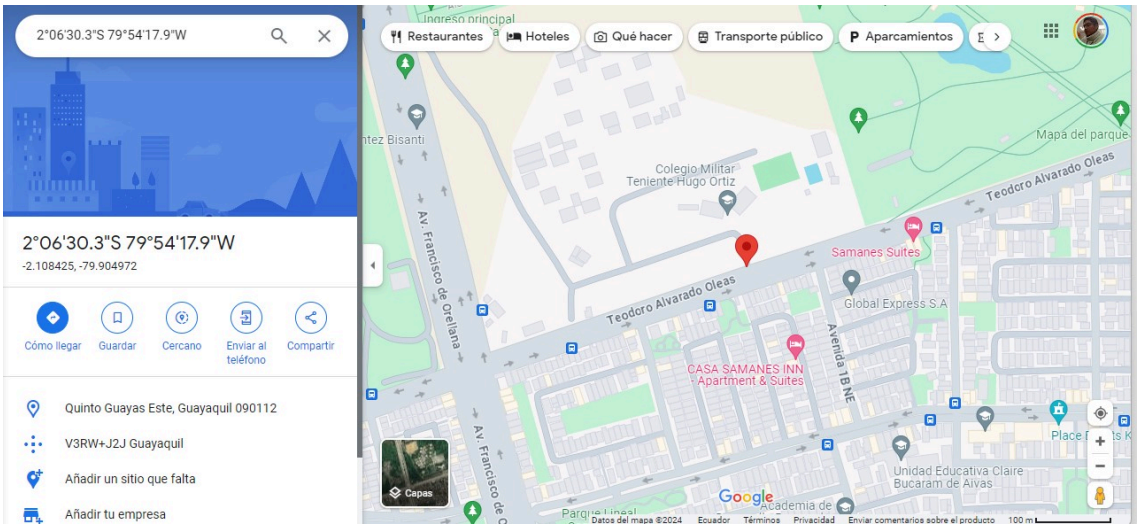


Ilustración 36 Ubicación 2

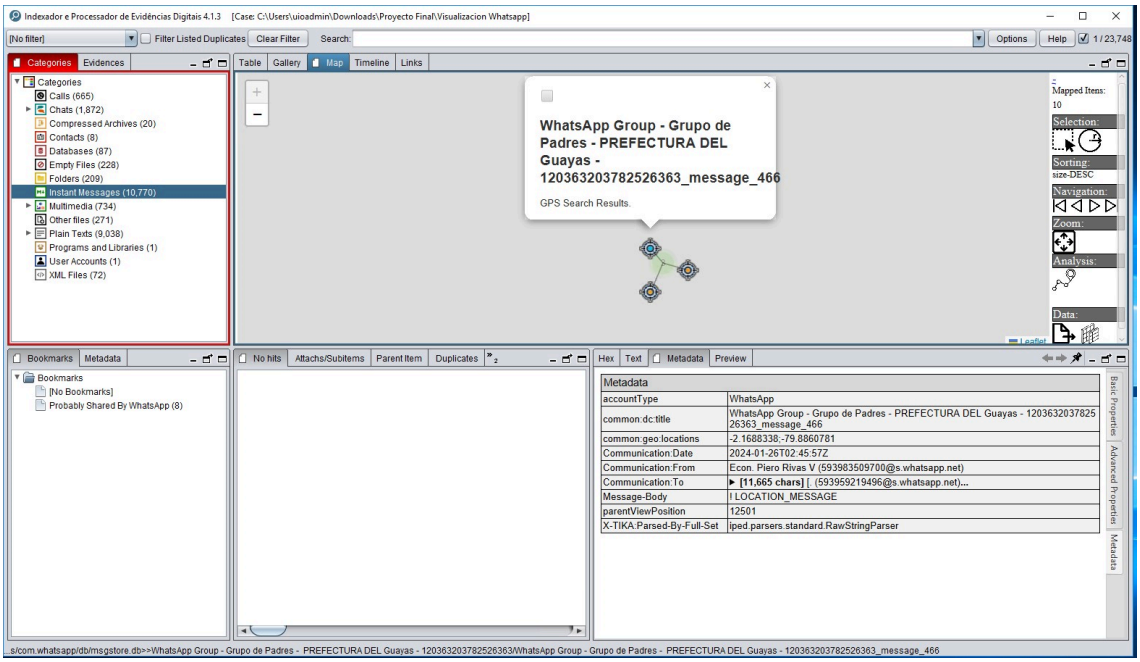


Ilustración 37 Geolocalización 3.

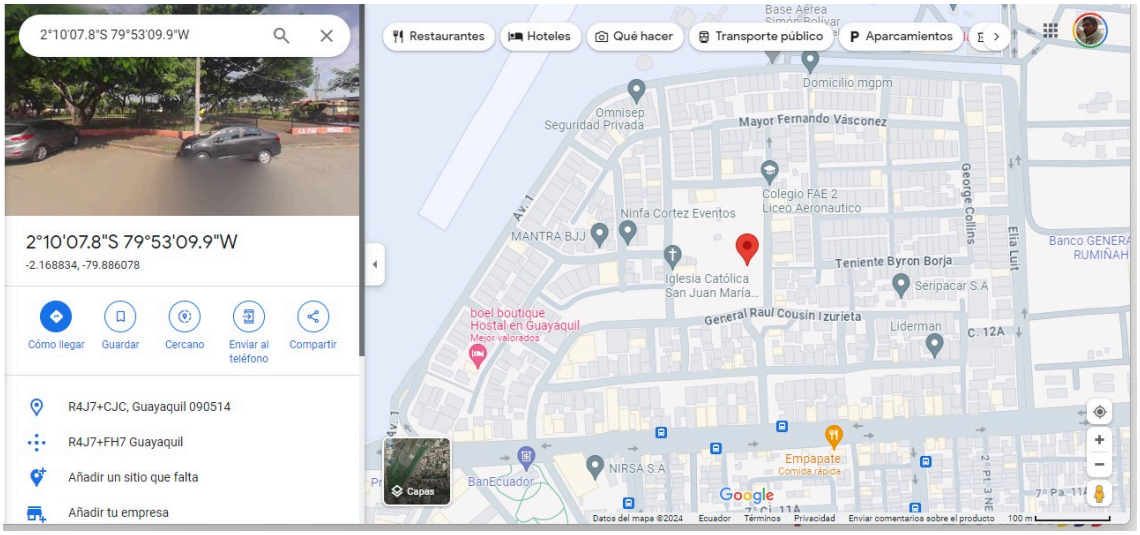


Ilustración 38 Ubicación 3.

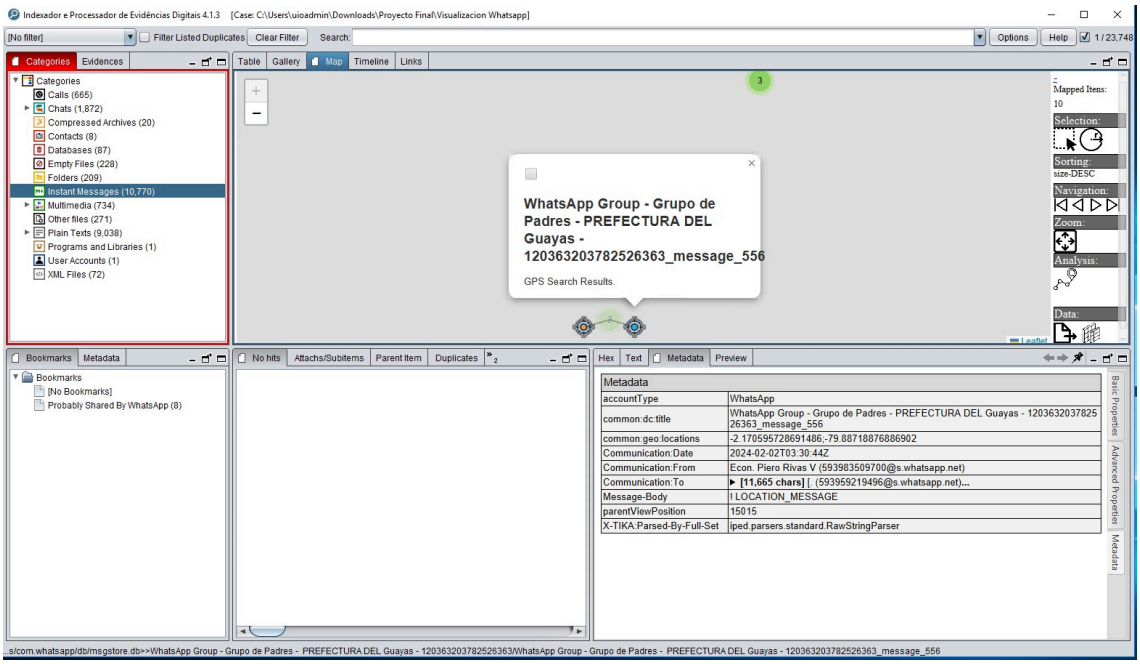


Ilustración 39 Geolocalización 4.

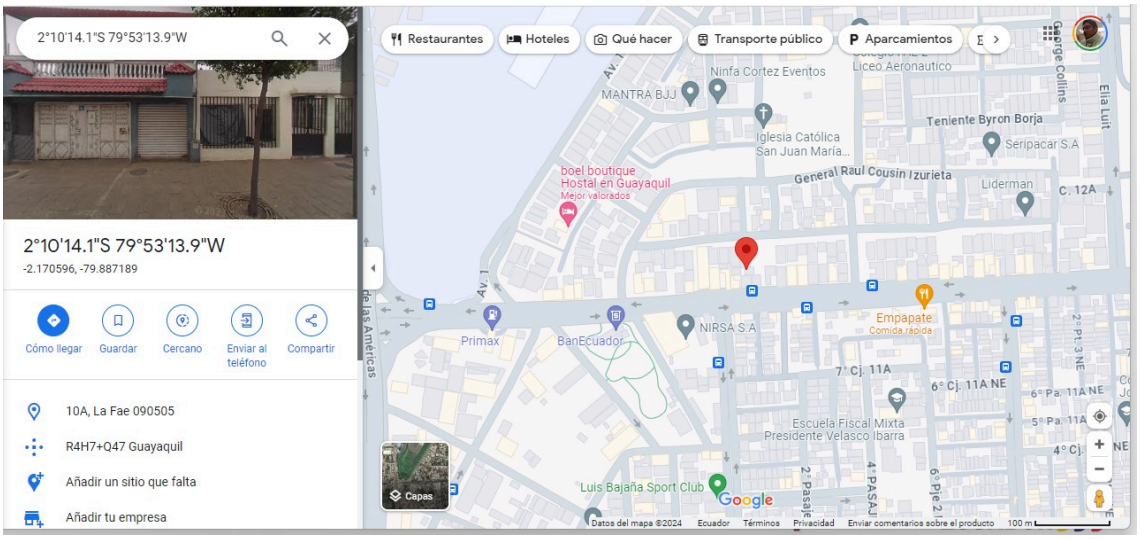


Ilustración 40 Ubicación 4.

Análisis de archivos multimedia.

Se evidencia que existe un registro de 734 archivos multimedia en la aplicación, aquí observamos que existen imágenes alojadas en la aplicación whatsapp, también podríamos saber si estas fueron borradas.

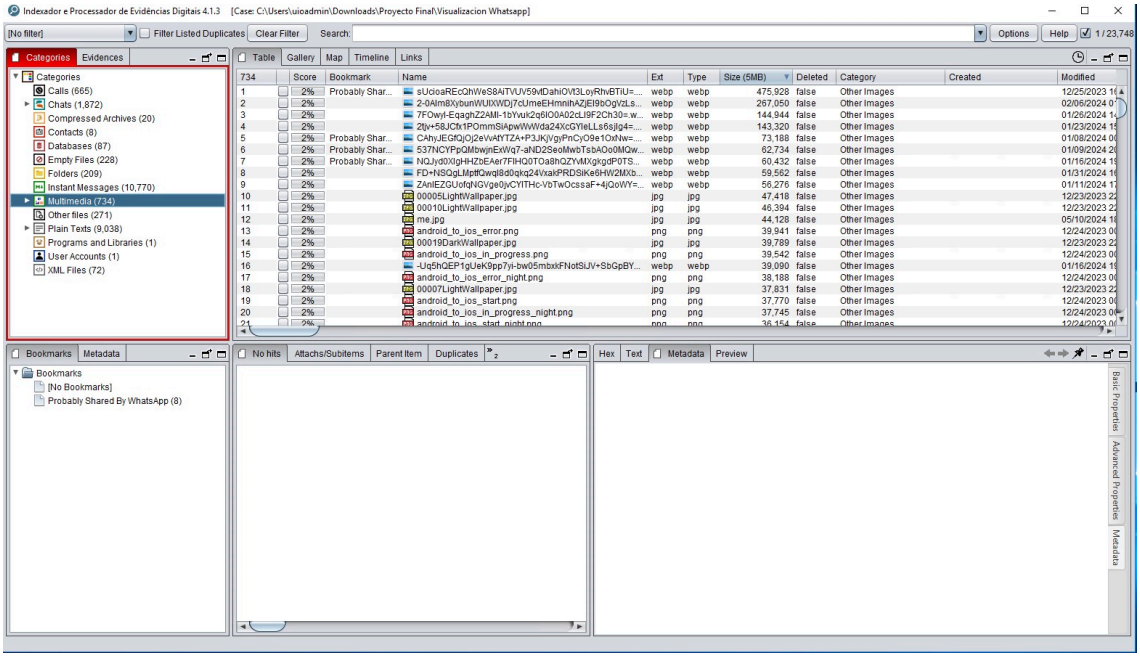


Ilustración 41 Archivos multimedia.

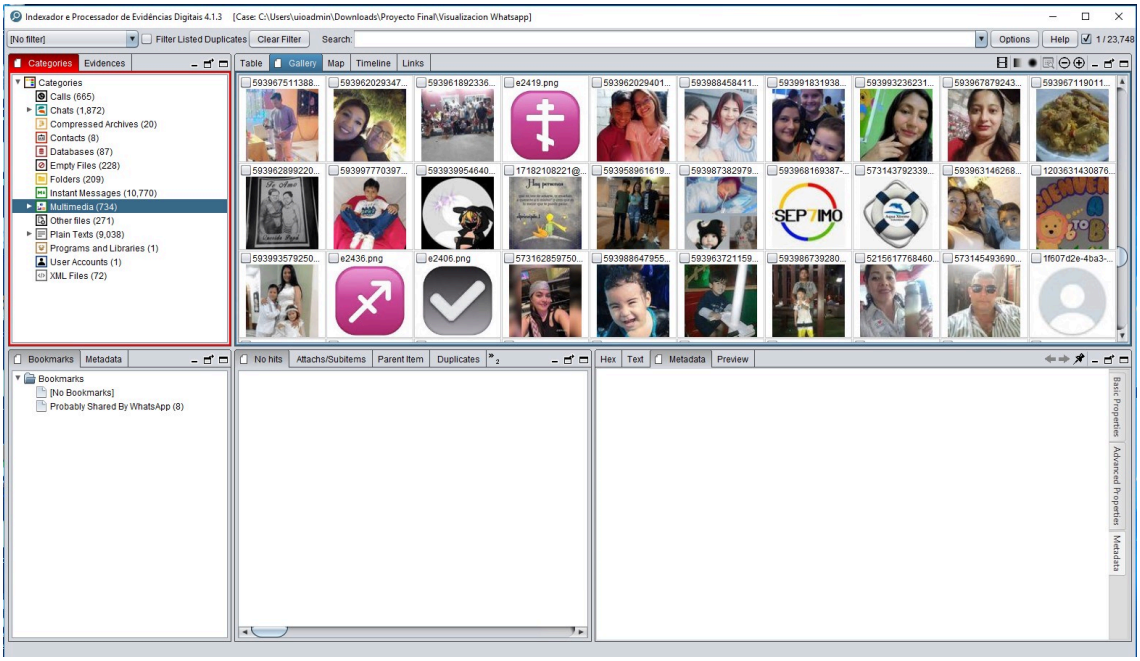


Ilustración 42 Archivos multimedia.

Se visualiza la línea de tiempo que fueron enviadas las imágenes.

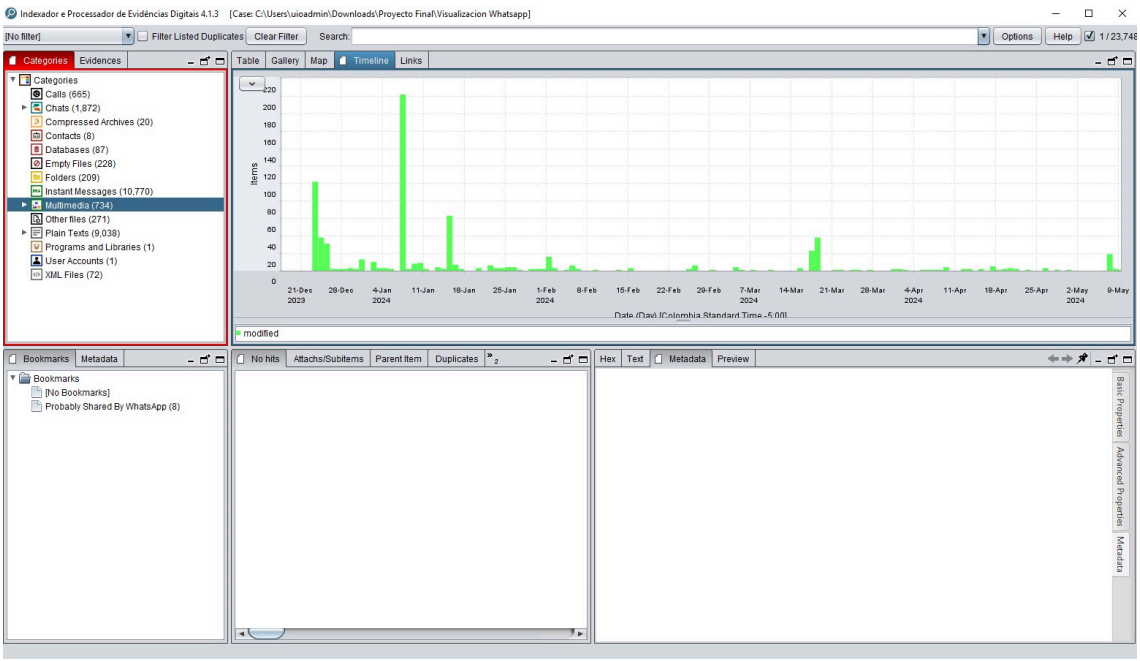


Ilustración 43 Archivos multimedia.

Análisis de cuenta de WhatsApp.

Aquí podemos obtener la información de la cuenta, así como el número de contacto al cual pertenece.

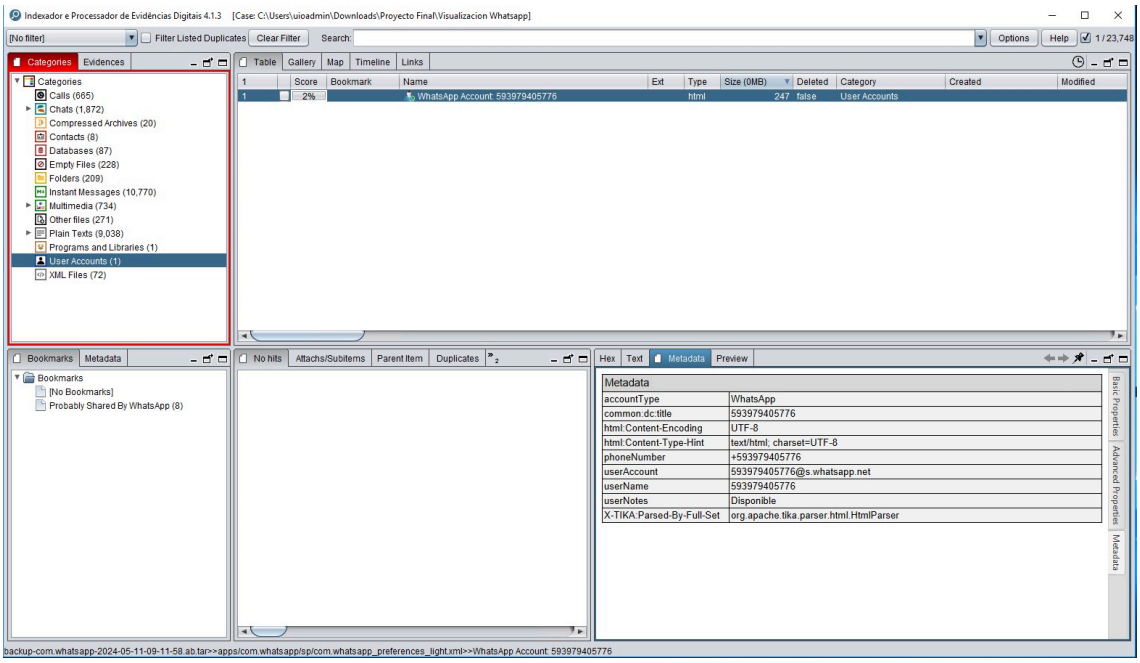


Ilustración 44 Cuenta WhatsApp.

Avilla Forensics además permite analizar la base de datos de WhatsApp a través de una herramienta que visualiza los chats que esta contiene, sin embargo, aquí no se muestra la información a detalle, simplemente muestra las conversaciones.

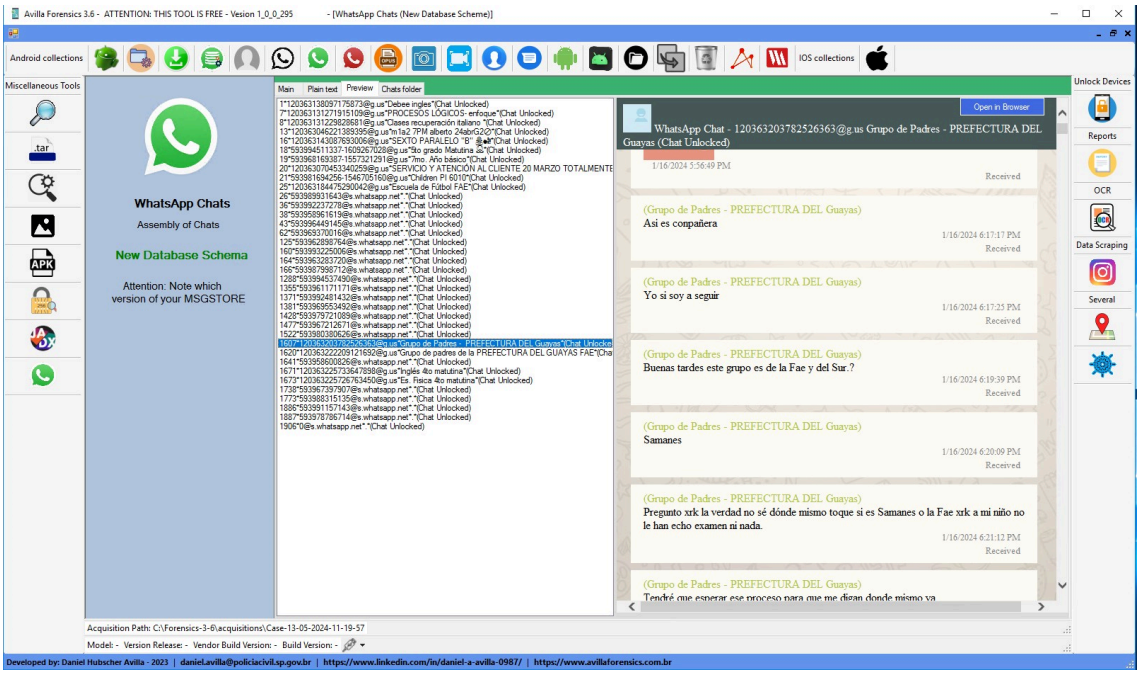


Ilustración 45 Vizualizador 1.

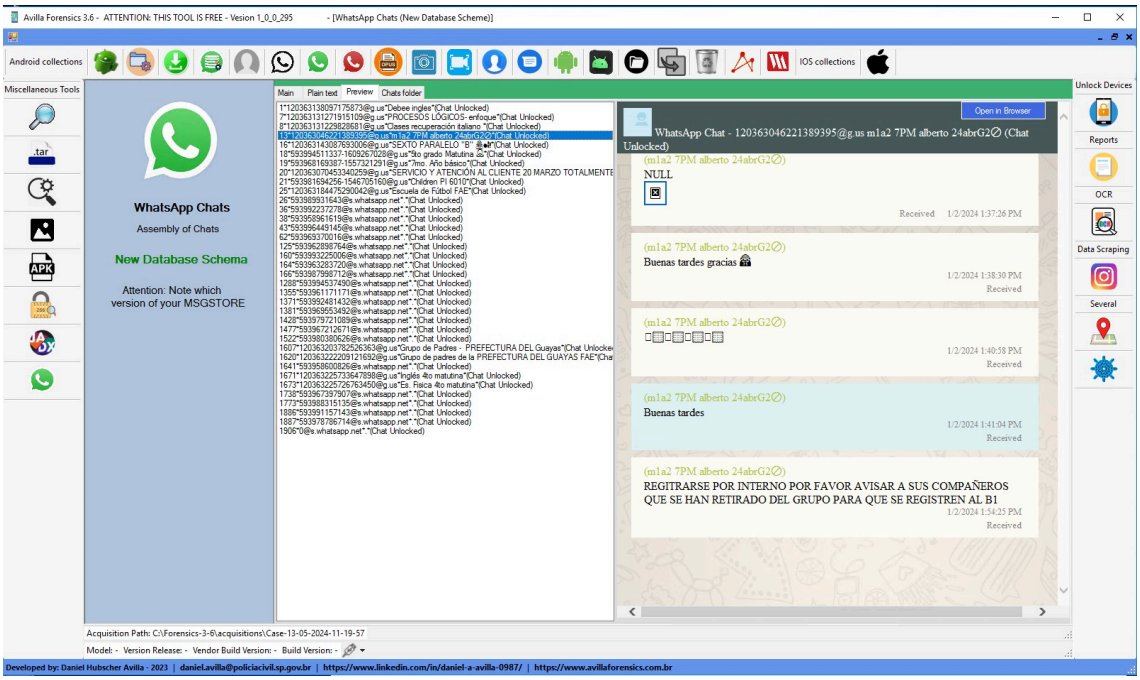


Ilustración 46 Vizualizador 2.

Manual Avilla Forensics

Link: Descargar Manual Técnico

UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

MANUAL TÉCNICO

AUTORES:

Condor Edison
García Ángel
Velasco Daniel
Velasco Isaac

TUTOR: Ronie Martinez

"Análisis de evidencias electrónicas en la aplicación de mensajería Whatsapp en dispositivos Android"

ÍNDICE GENERAL

CAPÍTULO I

GENERALIDADES

INTRODUCCIÓN

El presente manual técnico tiene como objetivo principal describir detalladamente los pasos seguidos para obtener las evidencias electrónicas en la aplicación de mensajería WhatsApp en dispositivos Android.

OBJETIVO DE ESTE MANUAL

El objetivo de este manual es que sirva como guía a los peritos infórmaticos el obtener evidencias electrónicas en la aplicación de mensajería WhatsApp en dispositivos Android.

A QUIEN VA DIRIGIO ESTE MANUAL

Este manual está orientado a los peritos informáticos.

ACERCA DE ESTE MANUAL

Este manual contiene ilustraciones e instrucciones que debe seguir un perito infórmatico para la obtención de evidencias electrónicas en la aplicación de mensajería WhatsApp en dispositivos Android.

CAPÍTULO II

APLICACIONES A UTILIZAR

AVILLA FORENSICS

Avilla Forensics es una que permite realizar copias de seguridad y analizar dispositivos o descifrar datos de WhatsApp y muchas funciones adicionales que ayudan a los profesionales en Informática Forense, a obtener evidencias digitales completas.

KINGROOT

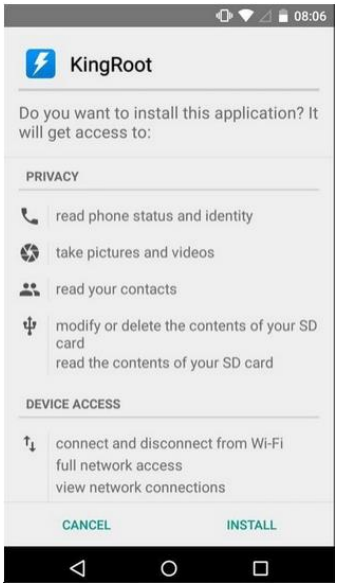
Kingroot es un software destinado a proporcionar accesos de usuario administrador con todos los permisos en teléfonos inteligentes, tabletas y dispositivos android que ejecutan versiones del sistema operativo Android.

CAPÍTULO III

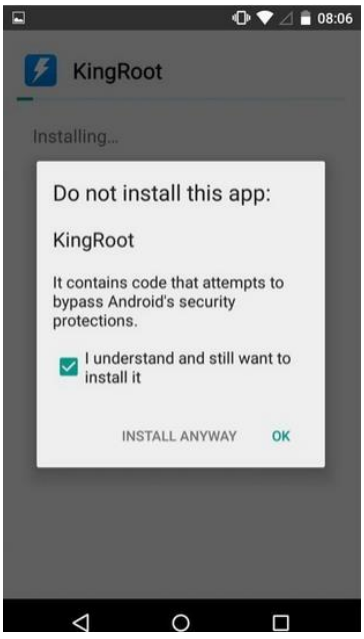
INSTALACIÓN de los programas a utilizar

INSTALACION DE KINGROOT

Descargamos Kingroot.apk desde la web, ejecutamos y damos clic en instalar

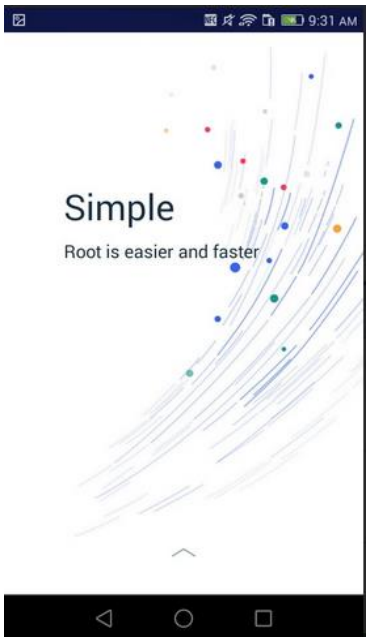


Nos aparecerá una alerta de seguridad y damos clic en installar de todas forma

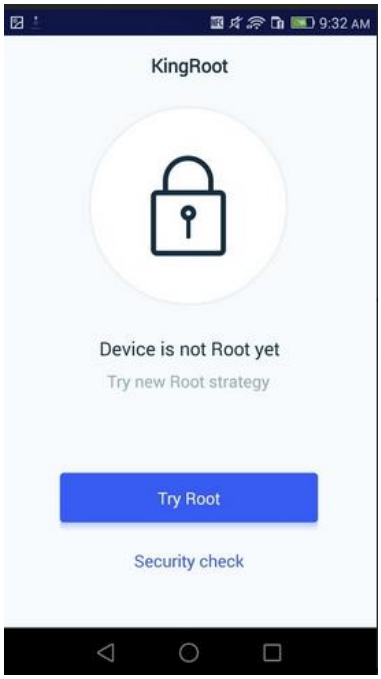


- **EJECUCIÓN Y OTORGACIÓN PERMISOS DE SUPERUSUARIO AL DISPOSITIVO ANDROID**

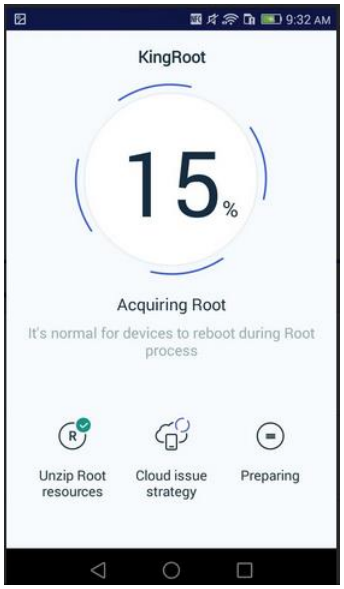
Después de haber instalado kingroot.apk ejecutamos el apk en nuestro dispositivo Android.



Aparecerá la siguiente pantalla y damos clic en probar root



Empezará a dar permisos de root al dispositivo android.



INSTALACIÓN DE AVILLA FORENSICS

Descargamos el programa Avilla Forensics desde el link https://github.com/AvillaDaniel/AvillaForensics?_ga=2.53585576.1841523922.1712120553-762174749.1712120552

La instalación del Programa es fácil, solo es ejecutar el AvillaSetup.exe y dar clic en instalar.

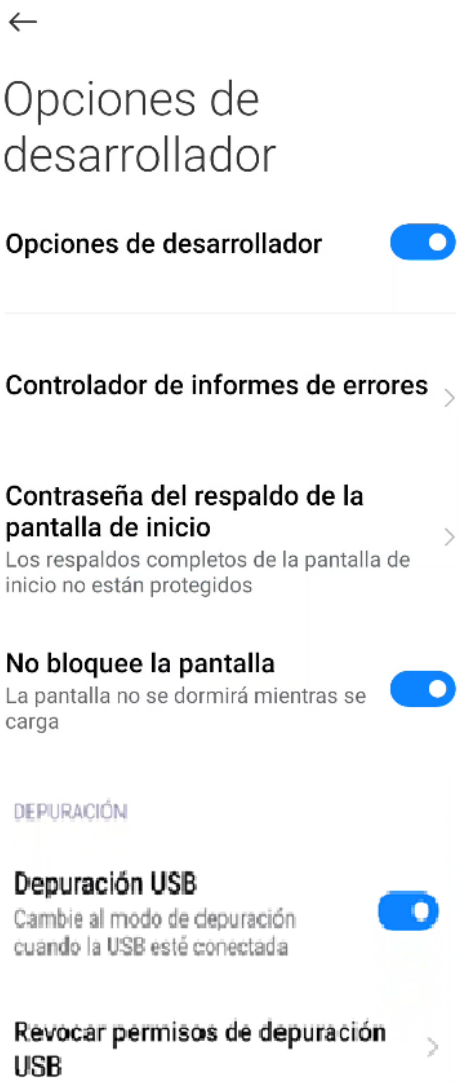
CAPÍTULO IV

CONFIGURACIÓN DEL DISPOSITIVO ANDROID A MODO DESARROLLADOR

Para activar el Modo Desarrollador nos vamos a Ajustes y pilsamos 7 veces sobre Número de compilación.

Después de haber activado el Modo Desarrollador nos vamos a Opcioens de Desarrolladot y activamos las siguientes opciones:

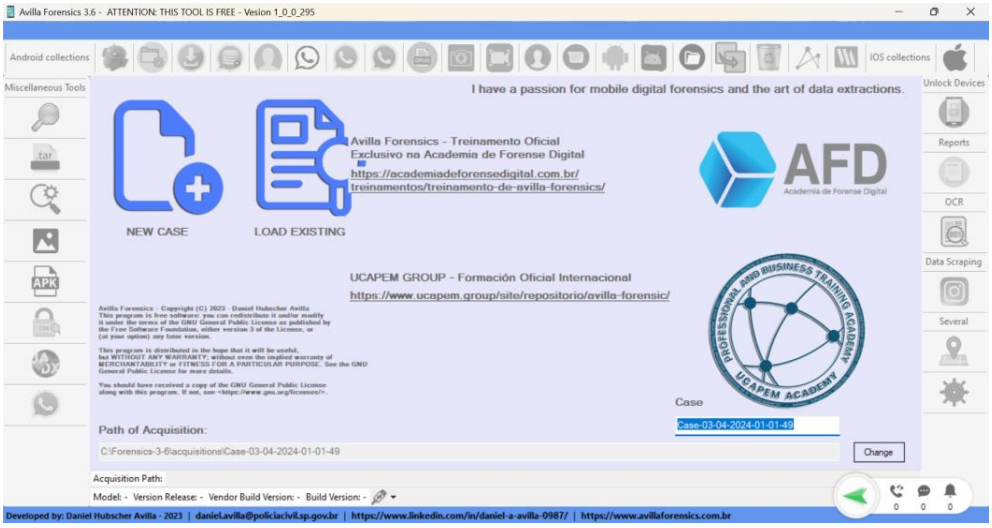
- No bloquear pantalla
- Depuración USB



CAPÍTULO V

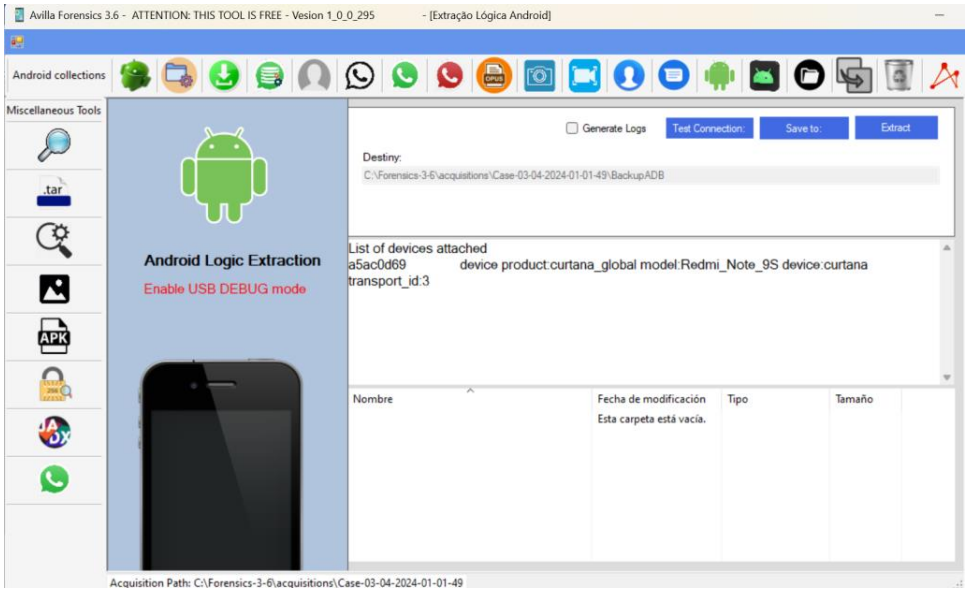
EJECUCIÓN DE BACKUP DE LAS BASE DE DATOS DE WHATSAPP CON AVILLAFORENSICS

- Ejecutamos el programa y procedemos a crear un nuevo caso

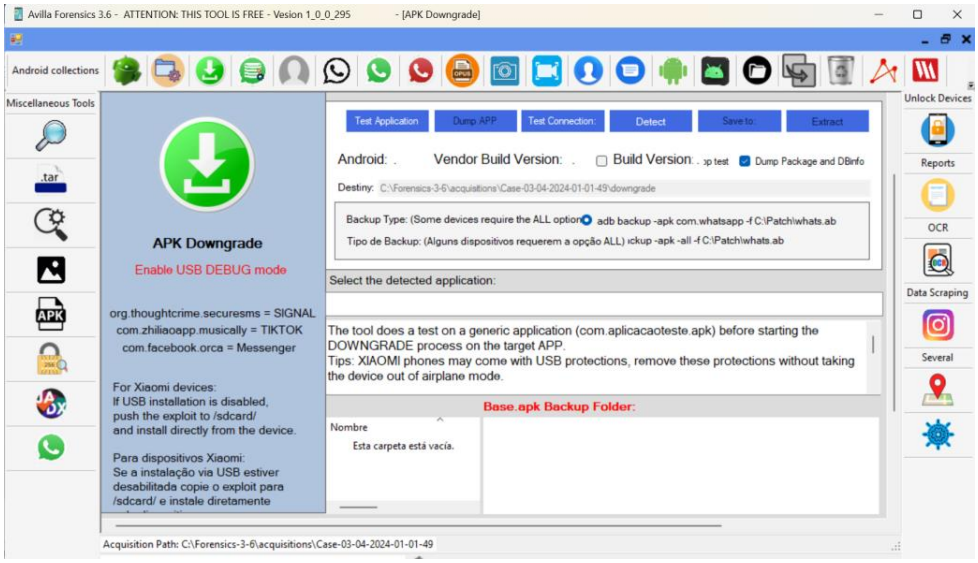


- Hacemos clic en Backup ADB y hacemos un test de conección con nuestro dispositivo.

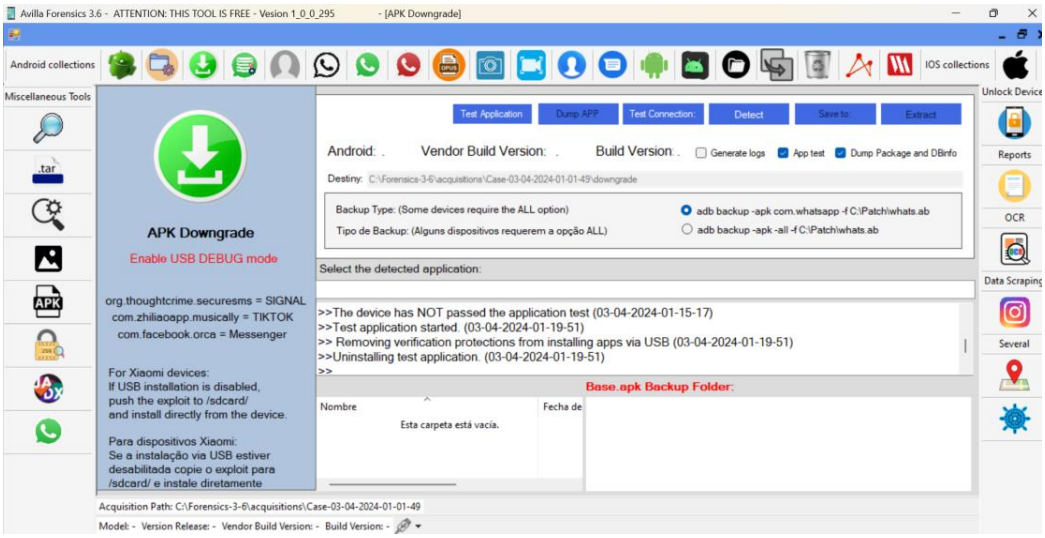
- Observamos los datos del dispositivo android que tenemos conectado.



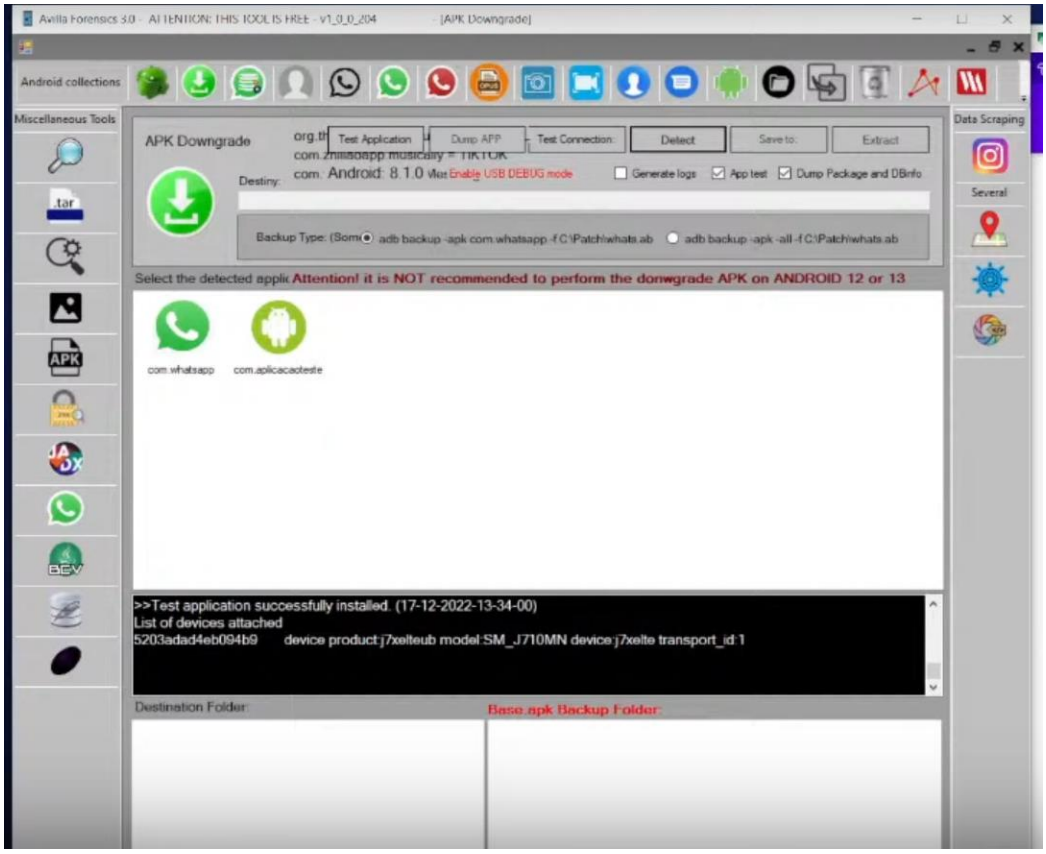
- Procedemos a realizar clic en APK DOwngrade



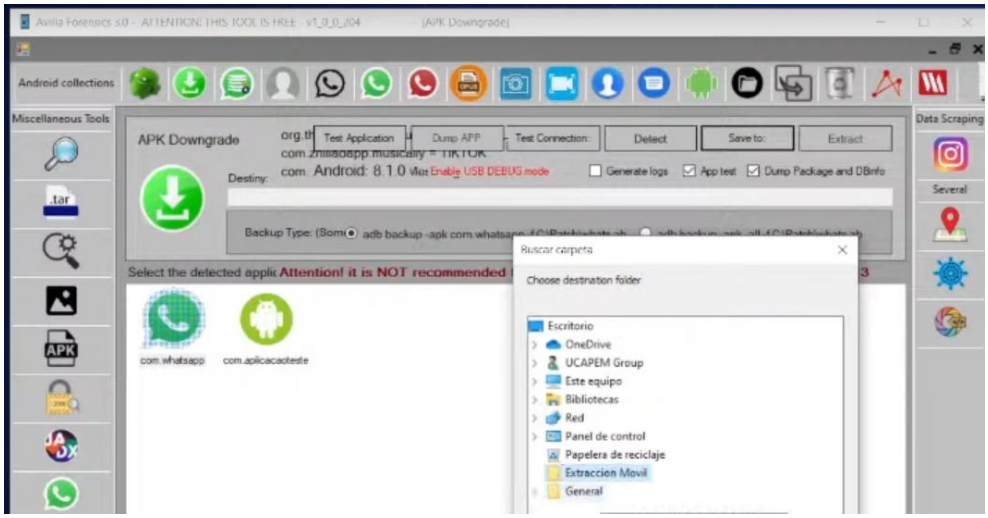
- Hacemos clic en Test de Aplicación.



Hacemos clic en Detect para ver que apk podemos hacer downgrade para poder trabajar en el, en este caso me salen dos apk, el cual es Whatsapp



- Seleccionar Whatsapp, escogemos la ruta en donde guardaremos los datos a extraer del aplicativo a analizar, en este caso sería WhatsApp y hacer clic en Guardar para extraer todos los datos de whatsapp



CAPÍTULO VI
RECOMENDACIONES

Se recomienda usar dispositivos Android con versiones 5 o superiores.