UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIEROS EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

EVALUACIÓN DE HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES BAJO ANDROID, AÑO 2022

AUTOR(A)(ES):

ALEXIS RONALDO CUEVA CANDO
JUAN FERNANDO FLORES CULQUI

DIRECTOR(A):

ING. DANILO BARRENO

GUARANDA – ECUADOR

2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

EVALUACIÓN DE HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES BAJO ANDROID, AÑO 2022

AGRADECIMIENTO

Agradecer en primer lugar a nuestro director, Ing. Danilo Barreno por la entrega y apoyo que nos ha brindado para la realización de este trabajo, también agradecer a nuestros pares académicos Dra. Edelmira Guevara y Dr. Carlos Taco; extender nuestro agradecimiento a la Universidad Estatal de Bolívar que nos brindó la formación académica, ética y moral a lo largo de estos años de estudio para poder obtener nuestro título profesional y ser profesionales competentes y útiles en nuestra sociedad, agradecer a nuestros docentes por compartir sus valiosos conocimientos con gran profesionalismo los cuales utilizaremos para el bien de nuestra sociedad.

Juan F. Flores y Alexis R. Cueva

DEDICATORIA

El presente trabajo de titulación está dedicado a mi familia que siempre me han apoyado en mis estudios, principalmente a mi madre María Teresa C. que, con amor, paciencia y esfuerzo, ha sido el pilar fundamental para poder alcanzar hoy un sueño más, gracias por inculcarme un ejemplo de superación y esfuerzo para nunca darme por vencido en medio de la adversidad. Dedicar también a mis tíos Remigio F. y Fabián F. por el apoyo que han brindado durante mi formación académica.

Finalmente, quisiera dedicar este logro a mis amigos y personas que siempre confiaron en mí y apoyarme cuando más lo necesitaba, gracias por estar a mi lado a lo largo de esta gran travesía.

Juan F. Flores

El presente trabajo investigativo lo dedico principalmente a Dios, por ser la fuerza y motivación para completar con este arduo proceso que me permite alcanzar uno de los sueños más esperados. A mis padres, por su gran labor, trabajo, apoyo e impulso a lo largo de todos estos años, de no ser por ustedes no sería posible mi lugar hasta aquí, ni mucho menos llegar a ser lo que deseo. Desde el fondo de mi corazón todo el orgullo y privilegio ha sido y será ser su hijo, por confiar en mí y por la sabiduría al momento de guiar mi vida gracias eternas papás.

A mi hermana por acompañarme lo largo de todos mis años de estudio, por el apoyo moral y por siempre encontrar puntos en común que nos unen, a ti gracias por ser muchas veces el aliento que necesitaba.

Alexis R. Cueva

UEB
UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Danilo Barreno, Dra. Edelmira Guevara y Dr. Carlos Taco, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "EVALUACIÓN DE HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES BAJO ANDROID, AÑO 2022" desarrollado por los señores Flores Culqui Juan Fernando y Cueva Cando Alexis Ronaldo.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 17 de noviembre del 2022

Ing. Danilo Barreno
Director

Dra. Edelmira Guevara
Par Académico

Dr. Carlos Taco
Par Académico

DERECHOS DE AUTOR

Yo/Nosotros, **JUAN FERNANDO FLORES CULQUI y ALEXIS RONALDO CUEVA CANDO** portadores de las cédulas de identidad **N° 0250051471** y **2200204168** respectivamente**,** en calidad de autor/res y titular/es de los derechos morales y patrimoniales del Trabajo de Titulación: **EVALUACIÓN DE HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES BAJO ANDROID, AÑO 2022,** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por: JUAN FERNANDO FLORES CULQUI

Juan Fernando Flores
CI. 0250051471

Firmado electrónicamente por: ALEXIS RONALDO CUEVA CANDO

Alexis Cueva
CI. 2200204168

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

El análisis forense está comprometido con los procesos investigativos sobre certezas de carácter tecnológico además de mantener, reunir, analizar y mostrar las derivaciones del análisis de este tipo de evidencia (digital). Este proceso implica el uso de metodologías adecuadamente estructuradas para su tratamiento.

Los dispositivos móviles han marcado un hito en cuanto a la masificación de la comunicación en tiempo real y asíncrono. En mayor porcentaje las personas son usuarios de estos dispositivos con sistema operativo Android en sus diferentes versiones, las cuales han evolucionado en cuanto a rendimiento y seguridad, pero esta última sigue siendo una debilidad, debido a que cada cierto periodo de tiempo se continúa descubriendo vulnerabilidades que están ahí pero que no han sido detectadas.

Las nuevas versiones del sistema operativo vienen cargadas con parches que mitigan algunas de las vulnerabilidades más comunes en este tipo de arquitectura que son fácilmente accesibles por métodos informáticos, por mencionar algunos tenemos; ataques de fuerza bruta, denegación de servicios, ataques de control de flujo, ataques basados en SMS, entre otros, pero aún no es suficiente para controlar que un ataque se complete por lo que al término de estos se debe proceder a la aplicación de técnicas y metodologías con alcance para recopilar, almacenar, extraer, documentar y mostrar evidencias informáticas que de forma convincente sean de apoyo en los debidos procesos judiciales que el país y sus leyes así lo reconozcan.

Como base fundamental para la ejecución de estas técnicas se debe contar con el equipo y el software informático que permitirá adentrarse en el dispositivo móvil.

Contando con un alto porcentaje de uso de estos dispositivos se propone en este proyecto un estudio comparativo de las diferentes herramientas de software para el análisis forense a dispositivos móviles, así como sus funcionalidades y características de las cuales se irá midiendo el alcance con parámetros que se ajusten en lo posible a la obtención de datos, su costo, generación de informes y compatibilidad con las distintas plataformas. A continuación, con los resultados se procederá a seleccionar la herramienta que cumpla con la mayor cantidad de opciones a estimar y proceder a evaluar la funcionalidad que ha presentado la herramienta y la variedad de servicios

que brinda para el análisis forense, de forma tal que se pueda identificar la herramienta mejor calificada para este tipo de procesos informáticos.

RESUMEN

En base al creciente apogeo de los dispositivos móviles a nivel mundial, sobre todo los usuarios de Android, se ha generado un incremento en los actos ilícitos hacia estos equipos, razón por la cual la ciencia forense requiere del uso de herramientas (software) para el análisis de estos, de tal manera que se pueda recopilar información relevante que aporte a los procesos judiciales del país. En este trabajo se plantea exhibir las herramientas disponibles para la ejecución de un análisis forense en equipos con sistema operativo Android en sus diferentes versiones, además de efectuar un estudio comparativo de las características y funcionalidades que presentan las herramientas seleccionadas. Se expondrá las múltiples vulnerabilidades de seguridad del S.O Android hasta la reciente publicación. El trabajo propone una revisión esquematizada de las características que cada herramienta presenta, considerando como criterio para su estimación la operatividad multiplataforma, costes y versiones soportadas, asimismo de las funciones que disponen. Se elegirá y evaluará una herramienta en base al cumplimiento mayoritario de los parámetros establecidos para su comparación y se detallará los resultados del proceso evaluativo de la herramienta. Con el estudio finalizado se podrá inferir el cumplimiento a los criterios evaluativos y si las herramientas atienden en su mayoría las necesidades esenciales del proceso, pero se indicará que se pueden ajustar a diferentes situaciones a la que un profesional forense se pueda enfrentar, aunque están presentes puntos a considerar como el coste de licencia, los requerimientos esenciales para el funcionamiento y la funcionalidad en diferentes plataformas.

Palabras clave: Android, Dispositivos móviles, Análisis Forense

ABSTRACT

Based on the growing popularity of mobile devices worldwide, especially Android users, there has been an increase in illegal acts against these devices, which is why forensic science requires the use of tools (software) for the analysis of these devices, so that relevant information can be collected to contribute to the country's judicial processes. In this work we propose to exhibit the tools available for the execution of a forensic analysis in equipment with Android operating system in its different versions, in addition to a comparative study of the characteristics and functionalities of the selected tools. The multiple security vulnerabilities of the Android OS up to the recent publication will be exposed. The work proposes a schematic review of the characteristics that each tool presents, considering as criteria for its estimation the multiplatform operability, costs and supported versions, as well as the functions they have. A tool will be chosen and evaluated based on the majority compliance with the parameters established for comparison and the results of the tool evaluation process will be detailed.

With the finalized study it will be possible to infer the compliance with the evaluation criteria and if the tools meet the essential needs of the process, but it will be indicated that they can be adjusted to different situations that a forensic professional may face, although there are points to consider such as the license cost, the essential requirements for the operation and the functionality in different platforms.

Keywords: Android, Mobile Devices Forensics, Forensic Analysis

CAPÍTULO I.

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

La velocidad con la que ha evolucionado la tecnología, hace que los ciberdelincuentes encuentren en ella una poderosa arma para cometer una amplia gama de actividades ilícitas. Cada vez son más grandes los tipos de delitos que se apoyan en las Tecnologías de la Información y Comunicación.

Según Denise Giusto (2019), los dispositivos móviles de Android presentaron hasta junio del 2019 vulnerabilidades con un total de 86 fallos de seguridad, cantidad que representa el 14% de vulnerabilidades de esta plataforma hasta 2018, año en que la cantidad que la Common Vulnerabilities and Exposures (CVE) ascendió a los 611 fallos divulgados. Sin embargo, para el año 2019 el 68% de fallos publicados tuvieron un nivel alto de criticidad y sumado a ello un 29% permitía la ejecución de código malintencionado, representando así una desmejora en tema de seguridad lo que ha obligado a los usuarios, a la instalación de parches de seguridad, y es que el promedio de malware ronda las 240 nuevas variantes resultando ser Android la cuarta arquitectura con mayor cantidad de variantes de malware. Entre los tipos de ataques que podemos encontrar son: Ataques de Fuerza Bruta, Denegación de servicios (DOS), Cross-site scripting (XSS), Ataques USSD (Datos Suplementarios del Servicio No Estructurados), Ataques de conexión USB, Vulnerabilidades y ataques basados en la cámara, Ataques de Control de Flujo y Ataques basados SMS.

Con base en lo anterior, podemos decir que, es evidente que las vulnerabilidades del sistema operativo Android permiten que los ciberataques ocurran, una vez que estos

ocurren se debe detallar lo sucedido, es decir, aplicar procedimientos y técnicas metodológicas que identifiquen, recopilen, almacenen, extraigan, interpreten, documenten y presenten evidencia de dispositivos informáticos de una manera que sea aceptable durante procedimientos judiciales o administrativos.

1.2. Formulación del Problema

¿Qué características son relevantes para la evaluación de herramientas de análisis forense en dispositivos móviles bajo Android?

1.3. Preguntas de Investigación

¿Qué vulnerabilidades tiene el sistema operativo Android en sus diferentes versiones a partir del año 2020 en adelante?

¿Cuál es el costo, funcionalidades y que tan accesibles son las herramientas para análisis forense existentes?

¿Cuál es el procedimiento a seguir para realizar un análisis forense con una herramienta específica?

1.4. Justificación

Según González (2021), la seguridad es fundamental a todos los niveles. No solo se monitorean en las computadoras sino también en los dispositivos móviles, las vulnerabilidades no son malas, lo realmente peligroso es que las vulnerabilidades existen y no se detectan y siempre es así, es uno de los objetivos del código abierto. La capacidad de descubrir vulnerabilidades a través de la comunidad de desarrolladores.

Este trabajo de investigación se centra en los dispositivos móviles que se ejecutan bajo el sistema operativo Android, esto debido a que es el de mayor popularidad; Shum (2020), nos menciona que en el año 2020 había 5.190 millones de usuarios únicos haciendo

uso de esta tecnología, de los cuáles el 74% utilizan esta plataforma para el funcionamiento de los dispositivos. En el 2019, la plataforma tuvo un dominio del 83%, que para ese momento tenía una presencia de dispositivos móviles de 1.372 mil millones de dispositivos.

Conocer las herramientas forenses móviles es de gran importancia ya que nos permite garantizar que la identificación, obtención y análisis forense no sea alterada para ser presentada como evidencia durante un proceso judicial. El uso de estas herramientas trae grandes beneficios ya que identificar el crimen informático ayudará a ubicar a los responsables, permitiendo comenzar la formalización legal de los hechos. Además, que la evidencia presentada será inalterable gracias al apoyo de un informe forense técnico que será el aval en una exposición y análisis técnico de los dichos legales conforme a derecho.

Este proyecto está enmarcado en la línea de investigación de la Ingeniería de Software, Redes y Telecomunicaciones, en la sub-línea Seguridades de las aplicaciones.

1.5. Objetivos:

General:

- Evaluar las diferentes herramientas que existen para el análisis forense en dispositivos móviles bajo Android.

Específicos:

- Analizar las vulnerabilidades del Sistema Operativo (SO) Android en sus diferentes versiones a partir del año 2020.
- Identificar herramientas para análisis forense con base a un estudio comparativo.
- Aplicar la herramienta seleccionada para el análisis forense.

- Evaluar los resultados de la aplicación seleccionada para el análisis forense en un periodo de tiempo.

1.6. Idea a Defender

Este método de estudio de los dispositivos móviles está enfocado a la indagación de los datos almacenados del usuario y la extrapolación de las actividades desarrolladas en los teléfonos celulares (smartphone), mismas que son el motivo principal para la vulneración de los servicios por agentes externos, la realización de este trabajo investigativo permitirá evidenciar las vulnerabilidades en materia de seguridad más comunes por donde un (atacante) puede acceder a un dispositivo móvil, recogiendo evidencia digital en forma de registros almacenados, generados y parcialmente generados de modo que se facilité la identificación de intrusos. Entonces el estudio y uso de herramientas de análisis forense para dispositivos móviles Android nos permitirá identificar, recopilar, almacenar, extraer, interpretar, documentar y presentar evidencia digital de una manera sustancial y que sea aceptable durante un proceso judicial.

CAPÍTULO II.

MARCO TEÓRICO

2.1. Antecedentes

En primer lugar, se tiene que, en noviembre de 2019, fue presentado en el Departamento de Informática de la Escuela Politécnica Superior Jaén el trabajo de fin de máster ***Herramientas de Análisis Forense para Android*** por Costa Silva, Luiza A., como requisito para optar al título de Máster en Seguridad Informática.

En este trabajo, se encuentran disponibles una serie de herramientas para realizar análisis forenses en dispositivos móviles y métodos recomendados para ayudar a los profesionales forenses a realizar su trabajo. El estudio propone cuatro etapas: Recolección, Validación, Análisis y Reporte, prestando especial atención a las dos primeras etapas por ser las más técnicas. También se proporcionan plantillas como base para el registro de datos y el análisis forense. La investigación nos brinda funciones de acceso a datos, tutoriales con instrucciones para completar la documentación requerida para un proyecto forense y brinda pasos para extraer datos de un dispositivo usando algunas de las herramientas expuestas.

Esta investigación ayudó a comprender que ninguna herramienta por sí sola cubre todas las necesidades posibles, pero, sobre todo, los analistas pueden elegir tantas herramientas como sea posible para ayudarlos a elegir la que mejor se adapte a sus necesidades.

Este trabajo es muy relevante para la investigación actual, ya que nos proporciona una gran cantidad de material sobre el uso de herramientas forenses, a través de datos claros y precisos, así como descripciones detalladas.

Un segundo trabajo de Medina y Hernández (2020), se denomina: ***Análisis forense para Móviles*** nos da a conocer el análisis y metodología que se requiere al momento de realizar la inspección forense de los dispositivos móviles que sirven como evidencia en un caso. También describe varios tipos de software forense que pueden ayudarlo a obtener información para usarla como evidencia.

Este artículo describe algunos protocolos y métodos a considerar al momento de llevar a cabo un análisis forense. Dándonos ciertos procedimientos que se deben efectuar en el manejo de la evidencia digital, como son la identificación, recolección, adquisición y preservación de la evidencia que puede ser probatorio.

Este trabajo se relaciona con la investigación planteada, ya que nos muestra varios softwares que se encuentran vigentes y actualizados para poder obtener toda la información necesaria de forma segura y documentada. También explica de manera eficaz cómo se debe hacer el análisis forense en un dispositivo móvil, explicando y mostrando las diferencias entre el SIM y el ME.

2.2. Científico

Sistema Operativo.

Este sirve como intermediario entre el usuario y el hardware. Es decir, cada ocasión que se ejecuta un programa en el ordenador, el sistema es el que le permite abrir el programa, accediendo a los recursos hardware y periféricos que se necesite para funcionar correctamente y especificar la cantidad de memoria a usar en función de ello. Además, es responsable de brindar servicios que faciliten la ejecución eficiente y la administración de recursos de las aplicaciones que se ejecutan en el sistema (Adeva, 2022).

Vulnerabilidades.

Las vulnerabilidades son debilidades del sistema operativo, software o sistema que permiten a un atacante comprometer la confidencialidad, integridad, disponibilidad, control de acceso y consistencia de un sistema o sus datos y aplicaciones (Marker, s.f.).

Ciencias Forenses.

Las ciencias forenses son un conjunto de áreas en las que los especialistas trabajan juntos para investigar una actividad delictiva. Esto significa ayudar a los jueces a tratar de encontrar respuestas a las preguntas que surgen en el caso de inspecciones de la escena del crimen y otros actos de causa sospechosa (Ezequiel, 2019).

Este conjunto de áreas permite buscar y comprender esencialmente qué pasó, como sucedió, cuándo aconteció, dónde ocurrió, por qué se hizo, entre otras preguntas que se hacen los especialistas.

Informática Forense.

Para UNIR (2021) la tecnología de la información es una parte importante de la investigación forense en el ámbito digital, ya que se enfoca específicamente en los delitos cometidos a través de dispositivos informáticos como redes, computadoras y medios de almacenamiento digital. Esto es especialmente cierto si la tecnología está involucrada como fuente o víctima del delito.

La informática forense es esencial cuando se quiere: detectar adecuadamente y obtener evidencia de delitos cibernéticos, apoyar los litigios para llevar a los delincuentes a juicio, ayudar a proteger contra los delitos en línea, como la violencia y el acoso.

2.3. Conceptual

Vulnerabilidades.

Según AMBIT TEAM (2020) las vulnerabilidades son fallas o debilidades que comprometen la seguridad de un sistema de información. Este es un "agujero" que puede ser causado por errores de configuración, pasos faltantes o fallas de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (como los sistemas operativos) para infiltrarse en ellos, realizar actividades ilegales, robar información confidencial o interferir en las operaciones.

Las vulnerabilidades son una de las principales razones por las que las empresas pueden sufrir ataques informáticos en sus sistemas. Por ello, siempre es recomendable actualizar las aplicaciones de tu dispositivo celular, el sistema de protección y el sistema operativo a la última versión. Esto se debe a que estas actualizaciones incluyen muchas correcciones para las vulnerabilidades encontradas.

Los sistemas y aplicaciones informáticas son constantemente vulnerables a algunas fallas en su diseño, estructura o código. No importa cuán pequeño sea este error, puede amenazar los sistemas y la información y puede ser una puerta de entrada para ataques externos o internos. Las principales vulnerabilidades suelen aparecer en las siguientes ubicaciones:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos.

Vulnerabilidades producidas por contraseñas

Con el teletrabajo y la computación en la nube, la gestión de contraseñas se ha convertido en una de las principales prioridades de la ciberseguridad. Debe utilizar su usuario y contraseña para acceder a la plataforma de trabajo de su empresa. El uso de una contraseña débil hace que su sistema sea vulnerable. La intrusión de terceros no autorizados que podrían robar, cambiar o eliminar información si la contraseña es fácil de descifrar, cambiar la configuración si tiene los permisos adecuados o apagar su computadora porque puede causarlo.

Vulnerabilidades producidas por usuarios

Una de las principales causas de los ataques informáticos está relacionada con el mal uso o uso descuidado por parte de los usuarios. Otorgar permisos o autorizaciones incorrectamente puede llevar a los usuarios a acceder a opciones de administración o configuración no preparadas, cometiendo errores y poniendo en peligro su organización.

Las malas prácticas a nivel de ciberseguridad y la falta de capacitación también crean vulnerabilidades, como la apertura de archivos de fuentes sospechosas, el fraude publicitario fraudulento y la apertura de correos electrónicos fraudulentos. Estas acciones son amenazas de ataques como el phishing (robo de información personal).

Vulnerabilidades de Ejecución Remota de Código (RCE)

Como menciona el sitio web LIMPIATUWEB (s.f.) la ejecución remota de código (RCE) es un tipo de vulnerabilidad que permite a un atacante acceder a un servidor o base de datos y cambiar de propietario. Durante un ataque RCE, el atacante utiliza malware (software malicioso) para secuestrar el servidor que aloja un sitio web.

Los ataques RCE son extremadamente peligrosos porque los ciber atacantes ejecutan cualquier tipo de código malicioso en un servidor vulnerable sin restricciones.

Dentro de los tipos de RCE tenemos:

- **Inyecciones SQL:** Estos ocurren cuando un atacante accede a la base de datos del sitio web para insertar nuevos datos la base de datos.
- **Secuencias de Comandos entre Sitios:** Esta afecta directamente a los visitantes de su sitio web y no al servidor. Un atacante podría robar fácilmente una contraseña de un usuario legítimo o robar detalles de la tarjeta de crédito o débito.

Vulnerabilidades de Elevación de Privilegios (EoP)

Aumento De Privilegios (s.f.) Los atacantes inician encontrando debilidades en las defensas de una organización y accediendo al sistema. En muchos casos, este primer punto de entrada no proporciona al atacante el nivel requerido de acceso o datos. Luego intentan elevar los privilegios para obtener más privilegios o acceder a sistemas adicionales más sensibles.

En ciertos casos, un atacante que intente elevar un privilegio puede encontrar que la puerta está "abierta". Es decir, tienen controles de seguridad insuficientes o no se adhieren al principio de privilegio mínimo, y los usuarios tienen más privilegios de los que realmente necesitan.

Existen dos tipos de elevación de privilegios:

- **Elevación de privilegios horizontales:** Un atacante eleva los privilegios secuestrando otra cuenta y explotando los privilegios legítimos otorgados a otros usuarios.
- **Elevación vertical de privilegios:** Un atacante está tratando de obtener más privilegios o acceso utilizando una cuenta comprometida existente.

Vulnerabilidades de Divulgación de Información (IDENTIFICACIÓN, ID)

Como menciona Microsoft (2022) La divulgación información proporciona al atacante información valiosa sobre el sistema. Por lo tanto, considere siempre la información que divulga y si puede ser utilizada por usuarios malintencionados. A continuación, se lista los posibles ataques de divulgación de información que se pueden dar:

- **Seguridad de mensajes y HTTP:** Si está utilizando seguridad a nivel de mensajes además de la capa de transporte HTTP, tenga en cuenta que la seguridad a nivel de mensajes no protege los encabezados HTTP.
- **Volcados de Memoria:** se origina por medio de un error en una aplicación y los archivos de registro.
- **Certificados transferidos sin cifrar:** Para autenticar un cliente con un certificado X.509, el certificado se pasa abierto en el encabezado SOAP.

Vulnerabilidades de denegación de servicio (DoS)

El sitio web AMBIT TEAM (2020) menciona que un ataque de denegación de servicio (DoS) ocurre cuando el servidor recibe una gran cantidad de solicitudes de acceso, lo que sobrecarga el sistema y hace que el servidor se bloquee o funcione mal (acceso retrasado o mensajes de error de rebote). Para realizar este tipo de ataques se utilizan muchos ordenadores (bots) que automáticamente hacen peticiones a este servidor.

Informática forense

La informática forense se define como una disciplina que se compone de dos elementos fundamentales, el derecho y la informática, las cuales buscan reunir y examinar datos de sistemas computacionales tales como: redes de datos, comunicaciones y unidades de almacenamiento masivo. En referencia a brechas de seguridad informática, lo redactado se concede como prueba ante un juez, para ello es vital la etapa de recolección de pruebas

significativas. Un investigador forense indaga en específico evidencia singular que toma por nombre “dato latente”. En el área de la seguridad informática, la naturaleza de estos datos los hace poco accesibles, razón por la que es requerido un nivel más complejo de indagación de los expertos en informática forense (González, 2021).

Análisis forense digital

El análisis forense digital se conforma de un conjunto de diversas técnicas que tienen como finalidad encontrar datos de gran significancia que no hayan sido alterados. Derivado de un equipo o dispositivo tecnológico, dando la preferencia de localizar información secreta o que ha sido descartada. Al ejecutarse un análisis forense digital, es fundamental sostener en el marco de lo técnico la integridad de los dispositivos de almacenamiento masivo, esto debe su importancia a la utilidad que se le dé en procesos judiciales (Sanchis, 2018).

Objetivos del análisis forense

Según Elaine (2018), la informática forense busca la prevención, aspecto que hace que empresas y profesionales sean auditados basándose en varias pruebas de carácter técnico ante mecanismos de seguridad configurados en dispositivos computacionales e incluso sobre los términos y políticas de seguridad adoptadas en una institución.

- El análisis forense facilita la detección de posibles fallos de seguridad que puede contar un dispositivo, con el fin de enmendar en situaciones que lo amerite.
- Los profesionales de este campo son capaces de componer ciertas guías sobre el manejo de sistemas computacionales, con el afán de sostener un nivel óptimo de seguridad para cada dispositivo, de modo que en lo posible se prevenga cualquier responsabilidad que deje vulnerable la información de valor de una institución.

- En situaciones donde una institución tenga brechas de seguridad, el analista forense tiene la tarea de reunir datos y pruebas significativas para indagar sobre el inicio y punto de donde se generó un ataque o en su defecto, dar con las condiciones que han dado espacio a que ocurra esta actividad.

Precedentes del análisis forense

De acuerdo con Rodríguez Muñoz (2015) en el ámbito de una investigación forense, el empleo y manejo de métodos, las herramientas no ocupan gran relevancia si los datos reunidos no pueden ser acreditados, siempre que se acate con la ejecución de los requerimientos, así como las instituciones judiciales contemplen que el trabajo de investigación es fiable.

Para que esto sea así, toda investigación forense debe dar cumplimiento a lo siguiente:

- Aceptabilidad: en el mundo de la seguridad informática están presentes muchos aplicativos con la capacidad de ejecutar un correcto proceso de indagación, por otro lado, están presentes aplicaciones que cuentan con respaldo de especialistas, que están en capacidad de generar un análisis más confiable, por tal razón se debe hacer uso de las mismas, ya que al hacer uso de nuevas tecnologías, muchas de estas, no han sido evaluadas por expertos dando lugar a que estás arrojen resultados poco confiables que favorezcan a que la investigación sea descartada (Rodríguez, 2015).
- Integridad: la información reunida durante el proceso de análisis, debe mantenerse sin modificaciones ni alteraciones de ninguna naturaleza, como verificación de ello, los recursos de almacenamiento que están siendo analizados tienen la obligatoriedad de mantenerse sellados y a la vez se debe contar con varios respaldos

del mismo y sus hashes deben ser similares. Esto se debe a que uno de los respaldos será sometido al análisis de datos, uno será netamente respaldo y la última se emplea para la defensa del caso para que la parte investigada exponga su contra informe.

- Credibilidad: esta característica hace referencia a que todo lo efectuado debe ser comprobable, la recolección de información y la ejecución de las herramientas serán notables, además el indagador debe tener entendimiento suficiente que le permita garantizar que está preparado para terminar un proceso investigativo.
- Relación causa efecto: esta característica que no responde a las responsabilidades del indagador sobre el desarrollo de la resolución en lo que concierne a culpabilidad o responsabilidad de los actores en un hecho particular, el procedimiento usado por el mencionado debe permitir generar una justificación de los sucesos a modo de causa y efecto.
- Carácter repetible: esta característica indica que independientemente del procedimiento de trabajo a usarse o del encargado de ejecutar el proceso de indagación, el resultado de la información obtenida de entrada deberá generar los mismos efectos en su salida.
- Documentación: todo el proceso realizado por el indagador estará estrictamente documentado, debido a que la documentación reunida se intercambiará y emplea una estructura previamente diseñada, esto hace que el investigador cuente con un esquema que llegue hacer demostrado si se da una situación de impugnación por ambigüedades o por cualquier otra causa. La documentación debe contar con ciertos campos estrictamente necesarios debido a la naturaleza del proceso.

Evidencia digital

En palabras de Sanchis (2018) la evidencia digital se considera a todo aquello que puede considerarse pruebas, evidencias y actividades reunidas, generados o que se albergan mediante dispositivos electrónicos y tecnologías de última generación. Para poder hacer uso de este recurso en una investigación se requiere de expertos, ya que estos son los encargados de reunir estos datos que ganan valor y significancia para estos procesos.

Se debe tener en cuenta que no solo los dispositivos electrónicos y equipos de última tecnología e internet, son medios de donde se puede rescatar datos en formato digital. Pero eso no deja de lado el hecho de que toda tecnología puede emplearse para el cometimiento de actos delictivos.

Manejo de Indicios y/o evidencia digital

Como indica la fiscalía general del estado (2014) para el manejo de la evidencia digital se presenta un instructivo de una serie de actividades normadas y que deben respetarse con los siguientes apartados:

1. ***Propósito***

   Establecer los procedimientos técnicos-científicos de cadena de custodia en el levantamiento de indicios y/o evidencia digital, para las intervenciones de los servidores policiales o civiles del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses y alcanzar niveles óptimos de eficiencia en la investigación de un hecho punible.

2. ***Responsabilidad***

   Es responsabilidad de todo servidor policial o civil del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, el aplicar el proceso

o procedimiento correcto, para la conservación y tratamiento adecuado de los indicios y/o evidencia digital e iniciar la cadena de custodia.

3. Actividades

En el análisis informático de campo, en los casos de dispositivos y equipos informáticos, considerando los siguientes escenarios:

3.1. Fijación Digital de los dispositivos y equipos informáticos en funcionamiento:

La fijación digital se fundamenta en tres tomas fotográficas:

a) Estado inicial del equipo, componentes y conexiones (accesorios externos del equipo)
b) Plaquetas de identificaciones técnicas (número de serie y modelo)
c) Fijación del escritorio (ubicación de los iconos instalados por programas)

i. **Captura de la Memoria RAM.**

a) Acoplamiento físico por un interfaz nuevo (USB, disco externo, cd, DVD, etc) proporcionado por el Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses.
b) Volcado (adquisición) de la información capturada al medio externo para su conservación y preservación.
c) Apagar el dispositivo y/o equipo informático
d) Entrega del medio de almacenamiento, al Centro de Acopio e inicio de cadena de custodia.

j. Fijación Digital de los dispositivos y equipos informáticos que se encuentran apagados:

a) Identificación del dispositivo y/o equipo informático, componentes y conexiones (accesorios externos del equipo)
b) Plaquetas de identificaciones técnicas (número de serie y modelo)
c) Fijación del indicio en el lugar de los hechos e inicio de cadena de custodia

Análisis forense en el entorno móvil

Como indica Coscollano (2019) las computadoras siguen siendo los dispositivos electrónicos más utilizados en la empresa, pero los teléfonos inteligentes y las tabletas son las herramientas favoritas de los usuarios para la comunicación diaria, tanto personal como comercial. Igual o mejor que la comunicación por correo electrónico es la comunicación que se produce mediante el uso de aplicaciones móviles como la mensajería instantánea (WhatsApp, Telegram, etc.) o las redes sociales (Twitter, Instagram, Facebook). En ellos, la información corre y se almacena únicamente en el dispositivo móvil utilizado.

Sin embargo, al explorar el mundo empresarial, pocas veces te encuentras con la posibilidad de acceder a dispositivos móviles. Estos pueden ser propiedad del empleado, pero, aunque pertenezcan a una empresa, suele ser más violento preguntar al empleado por el móvil que por el ordenador. Por el contrario, sucede en las investigaciones de las fuerzas de seguridad nacional, ya que los teléfonos móviles suelen ser una parte importante de una investigación.

En cuanto a las computadoras, existen muchas herramientas dedicadas al análisis forense de dispositivos móviles que facilitan el acceso y la copia de contenido, mantienen la unicidad y se adaptan a cada modelo de sistema operativo.

Este tipo de dispositivo tiene muchas características que hacen de la investigación forense una tarea compleja y difícil, desafiando a los expertos en este campo por las siguientes razones:

- Gestión del caso: La información contenida en los dispositivos móviles es mucho más volátil debido a que es un elemento que puede perderse u olvidarse fácilmente debido a la naturaleza de la movilidad del dispositivo, así como al espacio de almacenamiento. Así como las herramientas de análisis forense implican identificar y recuperar datos borrados, lo cierto es que la probabilidad de éxito es inversamente proporcional al tiempo que se ha utilizado el dispositivo.
- Dificultad técnica y conocimiento especializado: El análisis forense de teléfonos móviles no es un proceso fácil, incluso con la experiencia y las herramientas. Los factores específicos del dispositivo, como el estado y la configuración, pueden hacer que el contenido sea inaccesible. Por ejemplo, el teléfono está apagado en el momento del análisis y está protegido por un PIN o contraseña desconocidos.
- Plataformas: Tradicionalmente, cuando hablamos de dispositivos móviles, hablamos de teléfonos, pero hay una variedad de dispositivos, desde teléfonos inteligentes hasta tabletas, reproductores de MP3, cámaras, relojes inteligentes, drones y Sistemas de Posicionamiento Global (GPS).
- Fabricantes: Para los smartphones, conocer el tipo y modelo del dispositivo no es sencillo. Actualmente, hay cientos de fabricantes que lanzan un promedio de 15 modelos al año. Incluso los analistas experimentados pueden tener dificultades para identificar un modelo mediante una inspección visual. En muchos modelos, la única forma de acceder a los datos impresos en el dispositivo es quitar primero la batería.

Existe el riesgo de que el terminal se bloquee y se pierdan los datos en la memoria. Para evitar esto, se pueden utilizar herramientas forenses para facilitar la identificación después de conectar el dispositivo.

Android

Como afirma Adeva (2022) cuando hablamos de Google, estamos hablando de gigantes de Internet no solo por su popular motor de búsqueda, sino por todos sus servicios y lo que representa en el mundo actual de Internet y tecnología. Es que, además de contar con multitud de servicios y herramientas, es el propietario del sistema operativo para dispositivos móviles que encontramos en la mayoría de smartphones y tablets actualmente.

Android es un sistema operativo móvil diseñado para dispositivos móviles con pantalla táctil, como teléfonos inteligentes y tabletas, también lo encontrarás en otros dispositivos, como relojes inteligentes, televisores o sistemas multimedia en algunos modelos de automóviles. Android es un sistema operativo desarrollado por Google, basado en el kernel de Linux y otros softwares de código abierto, es fácil de usar en muchas aplicaciones y ha contribuido significativamente al uso generalizado de muchos dispositivos inteligentes.

Originalmente desarrollado por Android Inc. y posteriormente adquirido por Google en 2005, se lanzó en 2007, dos años después, para seguir desarrollando los estándares abiertos para dispositivos móviles. El principal código fuente de Android, comúnmente conocido como Android Open Source Project (AOSP), está atrayendo la atención como el sistema operativo móvil más utilizado del mundo, con una participación de mercado de más del 90 % en 2018. Antes de iOS, siendo su competencia directa.

Principales componentes del sistema operativo Android. Dentro de la arquitectura del sistema en sí, podemos resaltar los siguientes componentes claves de Android:

- Núcleo Linux: El núcleo del sistema es Linux, que actúa como una capa de abstracción entre el hardware del dispositivo y las aplicaciones instaladas. Además, el sistema operativo de Google se basa en Linux para otros servicios básicos, como seguridad, administración de memoria, administración de procesos, pilas de red y controladores.
- Runtime: El sistema operativo móvil de Google incluye un conjunto de bibliotecas que brindan la mayor parte de la funcionalidad disponible en la biblioteca base del lenguaje de programación Java. Cada aplicación de Android ejecuta su propio proceso utilizando una instancia de la máquina virtual Dalvik. Hasta la versión 5.0, esta máquina ejecutaba archivos en formato. dex, pero a partir de esta versión emplea el ART completamente compilado cuando se instala una aplicación.
- Bibliotecas: El sistema operativo Android contiene una serie de bibliotecas C o C ++ utilizadas por varios componentes del sistema. Estas funciones se proporcionan a los desarrolladores a través del marco de aplicación de Android. Entre estas bibliotecas destacan las bibliotecas System C, Media, Graphics, 3D o SQLite.
- Marco del trabajo de aplicaciones: En el entorno de Google, los desarrolladores pueden acceder a las mismas API de Workbench utilizadas en la aplicación base. Y la arquitectura de Android está diseñada para facilitar la reutilización de componentes. Es decir, cualquier aplicación puede exponer su funcionalidad y otras aplicaciones pueden utilizarlas dentro de las reglas de seguridad.

- Aplicaciones: Android tiene ciertas aplicaciones básicas que le permiten usar las funciones básicas de su dispositivo, como correo electrónico, mensajes de texto, SMS, calendarios, mapas, navegadores, contactos y más. Estas aplicaciones están desarrolladas en el lenguaje Java.

Vulnerabilidades en Android

Android, al ser el SO más utilizado en el mundo, presenta vulnerabilidades en algunos de sus componentes como cualquier SO existente que pueden llegar a verse afectados, tales como el framework, kernel, entre otros. A continuación, revisaremos las vulnerabilidades encontradas en Android desde el año 2020 en adelante.

Framework. Las vulnerabilidades en el framework permiten que una aplicación maliciosa local evite los requisitos de interacción del usuario para así tener acceso a permisos adicionales.

Tabla 1

Vulnerabilidades en el Framework de Android, año 2020

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0001	EoP	Moderada	10
CVE-2020-0003	EoP	Alta	8.0
CVE-2020-0004	DoS	Alta	8.0, 8.1, 9, 10
CVE-2020-0014	EoP	Alta	8.0, 8.1, 9, 10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0015	EoP	Alta	8.0, 8.1, 9, 10
CVE-2019-2200	EoP	Alta	10
CVE-2020-0017	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0018	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0020	ID	Alta	10
CVE-2020-0021	DoS	Alta	10
CVE-2020-0031	ID	Alta	10
CVE-2020-0080	EoP	Alta	10
CVE-2020-0081	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0082	EoP	Alta	10
CVE-2019-5018	EoP	Alta	8.0, 8.1, 9, 10
CVE-2019-8457	ID	Alta	8.0, 8.1, 9, 10
CVE-2019-9936	ID	Moderada	8.0, 8.1, 9, 10
CVE-2020-0096	EoP	Crítico	8.0, 8.1, 9

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0098	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0114	EoP	Alta	10
CVE-2020-0115	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0121	ID	Alta	10
CVE-2020-0122	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0227	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0240	RCE	Alta	10
CVE-2020-0238	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0257	EoP	Alta	10
CVE-2020-0239	IDENTIFICACIÓN	Alta	9, 10
CVE-2020-0249	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10
CVE-2020-0258	IDENTIFICACIÓN	Alta	10
CVE-2020-0247	DoS	Alta	8.0, 8.1, 10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0074	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0388	EoP	Alta	10
CVE-2020-0391	EoP	Alta	9, 10
CVE-2020-0401	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0382	ID	Alta	10
CVE-2020-0389	ID	Alta	10
CVE-2020-0390	ID	Alta	10
CVE-2020-0395	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0397	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0399	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0420	EoP	Alta	11
CVE-2020-0421	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0246	IDENTIFICACIÓN	Alta	10, 11
CVE-2020-0412	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0419	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2020-0074	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0388	EoP	Alta	10
CVE-2020-0391	EoP	Alta	9, 10
CVE-2020-0401	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0382	ID	Alta	10
CVE-2020-0389	ID	Alta	10
CVE-2020-0390	ID	Alta	10
CVE-2020-0395	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0397	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0399	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0420	EoP	Alta	11
CVE-2020-0421	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0246	IDENTIFICACIÓN	Alta	10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0412	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0419	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2020-0441	DoS	Crítica	8.0, 8.1, 9, 10, 11
CVE-2020-0442	DoS	Crítica	8.0, 8.1, 9, 10, 11
CVE-2020-0418	EoP	Alta	10
CVE-2020-0439	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0454	IDENTIFICACIÓN	Alta	9
CVE-2020-0443	DoS	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0099	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0294	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0440	EoP	Alta	11
CVE-2020-0459	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10
CVE-2020-0464	IDENTIFICACIÓN	Alta	10
CVE-2020-0467	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0468	IDENTIFICACIÓN	Alta	10, 11
CVE-2020-0469	DoS	Alta	11

Tabla 2

Vulnerabilidades en el Framework de Android, año 2021

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0313	DoS	Crítica	8.0, 8.1, 9, 10, 11
CVE-2021-0303	EoP	Alta	11
CVE-2021-0306	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0307	EoP	Alta	10, 11
CVE-2021-0310	EoP	Alta	11
CVE-2021-0315	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0317	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0318	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0319	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0304	ID	Alta	8.0, 8.1, 9, 10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0309	ID	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0321	ID	Alta	11
CVE-2021-0322	ID	Alta	9, 10, 11
CVE-2019-9376	DoS	Alta	8.0, 8.1, 9
CVE-2020-15999	RCE	Moderada	8.0, 8.1, 9, 10, 11
CVE-2021-0302	EoP	Alta	8.1, 9, 10
CVE-2021-0305	EoP	Alta	8.1, 9, 10
CVE-2021-0314	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0327	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0330	EoP	Alta	9, 10, 11
CVE-2021-0334	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0337	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0339	EoP	Alta	8.1, 9, 10
CVE-2021-0340	EoP	Alta	10
CVE-2021-0338	DoS	Alta	10, 11
CVE-2021-0391	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0398	EoP	Alta	11
CVE-2021-0400	EoP	Alta	9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0426	EoP	Alta	11
CVE-2021-0427	EoP	Alta	11
CVE-2021-0432	EoP	Alta	11
CVE-2021-0438	EoP	Alta	8.1, 9, 10
CVE-2021-0439	EoP	Alta	11
CVE-2021-0442	EoP	Alta	11
CVE-2021-0443	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0444	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0472	EoP	Alta	9, 10, 11
CVE-2021-0485	EoP	Alta	11
CVE-2021-0487	EoP	Alta	11
CVE-2021-0521	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0441	EoP	Alta	10
CVE-2021-0486	EoP	Alta	10, 11
CVE-2021-0640	EoP	Alta	9, 10, 11
CVE-2021-0645	EoP	Alta	11
CVE-2021-0646	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0687	Dos	Crítica	8.1, 9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0595	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0683	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0684	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0685	EoP	Alta	11
CVE-2021-0688	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0686	IDENTIFICACIÓN	Alta	10, 11
CVE-2021-0652	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0705	EoP	Alta	10, 11
CVE-2021-0708	EoP	Alta	8.1, 9, 10, 11
CVE-2020-15358	IDENTIFICACIÓN	Alta	11
CVE-2021-0702	IDENTIFICACIÓN	Alta	11
CVE-2021-0651	DoS	Alta	9, 10, 11
CVE-2021-0799	EoP	Alta	12
CVE-2021-0921	EoP	Alta	11
CVE-2021-0923	EoP	Alta	12
CVE-2021-0926	EoP	Alta	9, 10, 11, 12
CVE-2021-0933	EoP	Alta	9, 10, 11, 12
CVE-2020-13871	IDENTIFICACIÓN	Alta	11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0653	IDENTIFICACIÓN	Alta	9, 10, 11
CVE-2021-0922	EoP	Moderada	11

Tabla 3

Vulnerabilidades en el Framework de Android, año 2022

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-39630	EoP	Alta	12
CVE-2021-39632	EoP	Alta	11, 12
CVE-2020-0338	IDENTIFICACIÓN	Alta	9, 10
CVE-2021-0694	EoP	Alta	11
CVE-2021-39794	EoP	Alta	11, 12, 12L
CVE-2021-39796	EoP	Alta	10, 11, 12, 12L
CVE-2021-39797	EoP	Alta	12, 12L
CVE-2021-39798	EoP	Alta	12, 12L
CVE-2021-39799	EoP	Alta	12, 12L
CVE-2021-39662	EoP	Alta	11, 12

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2022-20004	EoP	Alta	10, 11, 12, 12L
CVE-2022-20005	EoP	Alta	10, 11, 12, 12L
CVE-2022-20007	EoP	Alta	10, 11, 12, 12L
CVE-2021-39700	IDENTIFICACIÓN	Moderada	10, 11, 12
CVE-2021-39691	EoP	Alta	10, 11, 12
CVE-2022-20006	EoP	Alta	10, 11, 12, 12L
CVE-2022-20125	EoP	Alta	10, 11, 12, 12L
CVE-2022-20138	EoP	Alta	10, 11, 12, 12L

Sistema. Las vulnerabilidades en el sistema permiten que un ataque remoto use una transmisión específicamente diseñada con el fin de obtener acceso a permisos adicionales.

Tabla 4

Vulnerabilidades en el Sistema de Android, año 2020

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0006	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0007	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0008	ID	Alta	8.0, 8.1, 9, 10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0022	DoS	Moderada	10
CVE-2020-0022	RCE	Crítica	8.0, 8.1, 9
CVE-2020-0023	ID	Crítica	10
CVE-2020-0005	EOP	Alta	8.0, 8.1, 9, 10
CVE-2020-0026	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0027	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0028	ID	Alta	9
CVE-2020-0036	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0035	ID	Alta	8.0, 8.1, 9
CVE-2020-0029	ID	Alta	10
CVE-2020-0037	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0038	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0039	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0070	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0071	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0072	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0073	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0103	RCE	Crítica	9, 10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0102	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0109	EoP	Alta	9, 10
CVE-2020-0105	EoP	Alta	9, 10
CVE-2020-0024	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0092	IDENTIFICACIÓN	Alta	10
CVE-2020-0106	IDENTIFICACIÓN	Alta	10
CVE-2020-0104	IDENTIFICACIÓN	Moderada	9, 10
CVE-2020-0117	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-8597	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0116	ID	Alta	10
CVE-2020-0119	ID	Alta	10
CVE-2020-0224	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0225	RCE	Crítica	10
CVE-2020-0107	IDENTIFICACIÓN	Alta	10
CVE-2020-0108	EoP	Alta	8.1, 9, 10
CVE-2020-0256	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0248	IDENTIFICACIÓN	Alta	10
CVE-2020-0250	IDENTIFICACIÓN	Alta	10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0380	RCE	Crítica	8.0, 8.1, 9, 10
CVE-2020-0396	ID	Crítica	8.0, 8.1, 9, 10
CVE-2020-0386	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0394	EoP	Alta	8.0, 8.1, 9, 10
CVE-2020-0379	ID	Alta	8.0, 8.1, 9, 10
CVE-2020-0215	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0416	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0377	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0378	IDENTIFICACIÓN	Alta	9, 10, 11
CVE-2020-0398	IDENTIFICACIÓN	Alta	10, 11
CVE-2020-0400	IDENTIFICACIÓN	Alta	10, 11
CVE-2020-0410	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0413	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0415	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0422	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0449	RCE	Crítica	8.0, 8.1, 9, 10, 11
CVE-2020-12856	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0424	IDENTIFICACIÓN	Alta	9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2020-0448	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0450	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0453	IDENTIFICACIÓN	Alta	8.0, 8.1, 9
CVE-2020-0437	DoS	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-0460	IDENTIFICACIÓN	Alta	11
CVE-2020-0463	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11
CVE-2020-15802	IDENTIFICACIÓN	Alta	8.0, 8.1, 9, 10, 11

Tabla 5

Vulnerabilidades en el Sistema de Android, año 2021

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0316	RCE	Crítica	8.0, 8.1, 9, 10, 11
CVE-2020-0471	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0308	EoP	Alta	8.0, 8.1, 9, 10, 11
CVE-2021-0320	ID	Alta	10, 11
CVE-2021-0326	RCE	Crítica	8.1, 9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0328	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0329	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0331	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0333	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0336	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0397	RCE	Crítica	8.1, 9, 10, 11
CVE-2017-14491	RCE	Alta	8.1, 9, 10, 11
CVE-2021-0393	RCE	Alta	8.1, 9, 10, 11
CVE-2021-0396	RCE	Alta	8.1, 9, 10, 11
CVE-2021-0390	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0392	EoP	Alta	9, 10, 11
CVE-2021-0394	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0430	RCE	Crítica	10, 11
CVE-2021-0429	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0433	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0446	EoP	Alta	11
CVE-2021-0431	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0435	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0473	RCE	Crítica	8.1, 9, 10, 11
CVE-2021-0474	RCE	Crítica	8.1, 9, 10, 11
CVE-2021-0475	RCE	Crítica	10, 11
CVE-2021-0476	EoP	Alta	9, 10, 11
CVE-2021-0477	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0481	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0466	IDENTIFICACIÓN	Alta	10
CVE-2021-0480	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0507	RCE	Crítica	8.1, 9, 10, 11
CVE-2021-0516	EoP	Crítica	8.1, 9, 10, 11
CVE-2021-0505	EoP	Alta	11
CVE-2021-0506	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0523	EoP	Alta	10, 11
CVE-2021-0504	IDENTIFICACIÓN	Alta	11
CVE-2021-0517	IDENTIFICACIÓN	Alta	11
CVE-2021-0522	IDENTIFICACIÓN	Alta	9, 10, 11
CVE-2020-0417	EoP	Alta	8.1, 9, 10

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0585	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0586	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0589	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0594	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0600	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0602	EoP	Alta	10, 11
CVE-2021-0588	IDENTIFICACIÓN	Alta	8.1, 9
CVE-2021-0590	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0596	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0597	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0599	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0604	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0591	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0593	EoP	Alta	8.1, 9, 10, 11
CVE-2021-0584	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0641	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0642	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0598	EoP	Alta	8.1, 9, 10, 11

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0692	EoP	Alta	9, 10, 11
CVE-2021-0428	IDENTIFICACIÓN	Alta	10
CVE-2021-0644	IDENTIFICACIÓN	Alta	10, 11
CVE-2021-0682	IDENTIFICACIÓN	Alta	8.1, 9, 10, 11
CVE-2021-0693	IDENTIFICACIÓN	Alta	11
CVE-2021-0691	EoP	Moderado	11
CVE-2021-0870	RCE	Crítica	8.1, 9, 10, 11
CVE-2021-0918	RCE	Crítica	12
CVE-2021-0930	RCE	Crítica	9, 10, 11, 12
CVE-2021-0434	EoP	Alta	9, 10, 11
CVE-2021-0649	EoP	Alta	11
CVE-2021-0932	EoP	Alta	10
CVE-2021-0925	IDENTIFICACIÓN	Alta	12
CVE-2021-0931	IDENTIFICACIÓN	Alta	9, 10, 11, 12
CVE-2021-0919	DoS	Alta	9, 10, 11
CVE-2021-0968	RCE	Crítica	9, 10, 11, 12
CVE-2021-0956	EoP	Crítica	11, 12
CVE-2021-0953	EoP	Alta	9, 10, 11, 12

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-0954	EoP	Alta	10, 11
CVE-2021-0963	EoP	Alta	9, 10, 11, 12
CVE-2021-0965	EoP	Alta	9, 10, 11, 12
CVE-2021-0952	IDENTIFICACIÓN	Alta	9, 10, 11, 12
CVE-2021-0966	IDENTIFICACIÓN	Alta	11, 12
CVE-2021-0958	DoS	Moderado	11, 12
CVE-2021-0969	DoS	Moderado	10, 11

Tabla 6

Vulnerabilidades en el Sistema de Android, año 2022

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-39618	EoP	Alta	9, 10, 11, 12
CVE-2021-39620	EoP	Alta	11, 12
CVE-2021-39621	EoP	Alta	9, 10, 11, 12
CVE-2021-39622	EoP	Alta	9, 10, 11
CVE-2021-39625	EoP	Alta	9, 10, 11, 12
CVE-2021-39626	EoP	Alta	9, 10, 11, 12

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-39627	EoP	Alta	9, 10, 11, 12
CVE-2021-39629	EoP	Alta	9, 10, 11, 12
CVE-2021-0643	IDENTIFICACIÓN	Alta	10, 11, 12
CVE-2021-39628	IDENTIFICACIÓN	Alta	10, 11
CVE-2021-39659	DoS	Alta	10, 11, 12
CVE-2021-39675	EoP	Crítica	12
CVE-2021-39668	EoP	Alta	11, 12
CVE-2021-39669	EoP	Alta	11, 12
CVE-2021-39671	EoP	Alta	12
CVE-2021-39674	EoP	Alta	10, 11, 12
CVE-2021-0706	DoS	Alta	10, 11
CVE-2021-39708	EoP	Crítica	12
CVE-2021-0957	EoP	Alta	10, 11, 12
CVE-2021-39701	EoP	Alta	11, 12
CVE-2021-39702	EoP	Alta	12
CVE-2021-39703	EoP	Alta	12
CVE-2021-39704	EoP	Alta	10, 11, 12
CVE-2021-39706	EoP	Alta	10, 11, 12

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2021-39707	EoP	Alta	10, 11, 12
CVE-2021-39709	EoP	Alta	12
CVE-2021-39808	EoP	Alta	10, 11, 12
CVE-2021-39805	IDENTIFICACIÓN	Alta	12, 12L
CVE-2021-39809	IDENTIFICACIÓN	Alta	10, 11, 12, 12L
CVE-2022-20113	EoP	Alta	12, 12L
CVE-2022-20114	EoP	Alta	10, 11, 12, 12L
CVE-2022-20116	EoP	Alta	12, 12L
CVE-2022-20010	IDENTIFICACIÓN	Alta	12, 12L
CVE-2022-20011	IDENTIFICACIÓN	Alta	10, 11, 12, 12L
CVE-2022-20115	IDENTIFICACIÓN	Alta	12, 12L
CVE-2021-39670	DoS	Alta	12, 12L
CVE-2022-20112	DoS	Alta	10, 11, 12, 12L
CVE-2022-20127	RCE	Crítica	10, 11, 12, 12L
CVE-2022-20140	EoP	Crítica	12, 12L
CVE-2022-20145	EoP	Crítica	11
CVE-2022-20124	EoP	Alta	10, 11, 12, 12L
CVE-2022-20126	EoP	Alta	10, 11, 12, 12L

CVE	Tipo	Gravedad	Versión de Android Parcheada
CVE-2022-20133	EoP	Alta	10, 11, 12, 12L
CVE-2022-20134	EoP	Alta	10, 11, 12, 12L
CVE-2022-20135	EoP	Alta	10, 11, 12, 12L
CVE-2022-20137	EoP	Alta	12, 12L
CVE-2022-20142	EoP	Alta	10, 11, 12, 12L
CVE-2022-20144	EoP	Alta	10, 11, 12, 12L
CVE-2022-20147	EoP	Alta	10, 11, 12, 12L
CVE-2022-20123	IDENTIFICACIÓN	Alta	10, 11, 12, 12L
CVE-2022-20131	IDENTIFICACIÓN	Alta	10, 11, 12, 12L
CVE-2022-20129	DoS	Alta	10, 11, 12, 12L
CVE-2022-20143	DoS	Alta	10, 11, 12, 12L

Kernel. Las vulnerabilidades en el kernel permiten que una aplicación local maliciosa ejecute código arbitrario en un contexto de proceso privilegiado.

Tabla 7

Vulnerabilidades en el Kernel de Android año 2020

CVE	Tipo	Gravedad	Componente
CVE-2019-17666	RCE	Crítica	Realtek rtlwifi driver

CVE	Tipo	Gravedad	Componente
CVE-2018-20856	EoP	Alta	Kernel
CVE-2019-15214	EoP	Alta	Sound subsystem
CVE-2020-0009	EoP	Alta	ashmem
CVE-2020-0030	EoP	Alta	Binder driver
CVE-2019-11599	EoP	Alta	Memory Map Subsystem
CVE-2019-19527	EoP	Alta	USB
CVE-2019-19537	EoP	Alta	USB
CVE-2019-15239	EoP	Alta	Networking
CVE-2020-0041	EoP	Alta	Binder
CVE-2019-19524	EoP	Alta	USB input driver
CVE-2019-19532	EoP	Alta	USB HID drivers
CVE-2019-19807	EoP	Alta	Audio Subsystem
CVE-2020-0110	EoP	Alta	Programador del núcleo
CVE-2019-19536	IDENTIFICACIÓN	Alta	Controlador PCAN-USB
CVE-2020-8647	EoP	Alta	Kernel TTY support
CVE-2020-8648	EoP	Alta	Kernel TTY support

CVE	Tipo	Gravedad	Componente
CVE-2020-8428	ID	Alta	Kernel
CVE-2018-20669	EoP	Alta	controlador i915
CVE-2019-18282	EoP	Alta	Pila de red de Linux
CVE-2019-20636	EoP	Alta	controlador de entrada
CVE-2020-10751	EoP	Alta	SELinux
CVE-2020-12464	EoP	Alta	Subsistema USB de Linux
CVE-2019-16746	IDENTIFICACIÓN	Alta	Subsistema inalámbrico de Linux
CVE-2019-19769	EoP	Alta	Storage subsystem
CVE-2020-0404	EoP	Alta	USB driver
CVE-2020-0407	ID	Alta	F2FS
CVE-2020-0423	EoP	Alta	Aglutinante
CVE-2020-0444	EoP	Alta	Sistema de auditoría del núcleo
CVE-2020-0465	EoP	Alta	Kernel
CVE-2020-0466	EoP	Alta	Subsistema de

			E/S

Tabla 8

Vulnerabilidades en el Kernel de Android año 2021

CVE	Tipo	Gravedad	Componente
CVE-2020-10732	ID	Alta	ELF core dumps
CVE-2020-10766	ID	Alta	Speculative execution
CVE-2020-10767	ID	Alta	Linux kernel
CVE-2017-18509	EoP	Alta	multidifusión IPv6
CVE-2021-0399	EoP	Alta	xt_qtaguid
CVE-2020-15436	EoP	Alta	Subsistema de dispositivo de bloque de kernel
CVE-2020-25705	IDENTIFICACIÓN	Alta	ICMP
CVE-2020-29661	EoP	Alta	TTY
CVE-2020-14305	EoP	Alta	Voz sobre IP H.323
CVE-2021-0512	EoP	Alta	ESCONDIDO
CVE-2020-14381	EoP	Alta	Futex
CVE-2021-3347	EoP	Alta	Futex
CVE-2021-28375	EoP	Alta	RPC rápido

CVE	Tipo	Gravedad	Componente
CVE-2021-0695	IDENTIFICACIÓN	Alta	Kernel
CVE-2020-29660	EoP	Alta	TTY
CVE-2020-10768	IDENTIFICACIÓN	Alta	Protecciones i86 Spectre v2
CVE-2020-10768	IDENTIFICACIÓN	Alta	Compatibilidad con enrutadores Qualcomm IPC
CVE-2021-0920	EoP	Alta	Kernel
CVE-2021-0924	EoP	Alta	USB
CVE-2021-0929	EoP	Alta	ION
CVE-2021-33909	EoP	Alta	sistema de archivos
CVE-2021-38204	EoP	Alta	USB
CVE-2021-0961	IDENTIFICACIÓN	Moderado	Filtro de red

Tabla 9

Vulnerabilidades en el Kernel de Android año 2022

CVE	Tipo	Gravedad	Componente
CVE-2021-39634	EoP	Alta	Kernel
CVE-2021-39633	IDENTIFICACIÓN	Alta	Kernel
CVE-2020-29368	EoP	Alta	Gestión de la memoria del núcleo

CVE	Tipo	Gravedad	Componente
CVE-2021-39685	EoP	Alta	Linux
CVE-2021-39686	EoP	Alta	Aglutinante
CVE-2021-39698	EoP	Alta	Kernel
CVE-2021-3655	IDENTIFICACIÓN	Alta	SCTP
CVE-2021-0707	EoP	Alta	dma-buf
CVE-2021-39801	EoP	Alta	ION
CVE-2021-39802	EoP	Alta	Gestión de la memoria
CVE-2021-39800	IDENTIFICACIÓN	Alta	ION
CVE-2022-0847	EoP	Alta	tubería
CVE-2022-20009	EoP	Alta	linux
CVE-2022-20008	IDENTIFICACIÓN	Alta	SD MMC
CVE-2021-22600	EoP	Moderado	Kernel

Como podemos observar, Android tiene una gran cantidad de vulnerabilidades de diferentes tipos que se ha ido recopilando desde del año 2020 en adelante, donde la vulnerabilidad que más destaca es la de tipo EoP que está clasificada en un rango de gravedad de alto y crítico. A continuación, detallaremos las vulnerabilidades de gravedad crítica y que por ende han sido las más explotadas:

- **CVE-2020-0096:** Localizada en la función startActivities del archivo ActivityStartController.java, existe una posible escalada de privilegios debido a un

adjunto confuso. Esto podría llevar a una escalada local de privilegios sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

- **CVE-2020-0441:** Localizadas en las funciones Message y toBundle del archivo Notification.java, existe un posible agotamiento de recursos debido a una validación de entrada inadecuada. Esto podría llevar a una denegación de servicio remota que requiera un reinicio del dispositivo para solucionarlo sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0442:** Localizadas en las funciones Message y toBundle del archivo Notification.java, existe una posible ralentización de la interfaz de usuario o un bloqueo debido a una validación de entrada inadecuada. Esto podría conducir a una denegación de servicio remota si se recibe un archivo de contacto malicioso, sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0313:** Localizada en la función isWordBreakAfter del archivo LayoutUtils.cpp, existe una posible forma de ralentizar o bloquear un TextView debido a una validación de entrada inadecuada. Esto podría llevar a una denegación de servicio remota sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0687:** Localizada en la función ellipsize del archivo Layout.java, existe un posible ANR debido a una validación de entrada inadecuada. Esto podría llevar

a una denegación de servicio local sin necesidad de privilegios de ejecución adicionales. Se necesita la interacción del usuario para su explotación.

- **CVE-2020-0022:** Localizada en la función reassemble_and_dispatch del archivo packet_fragmenter.cc, existe una posible escritura fuera de límites debido a un cálculo de límites incorrecto. Esto podría conducir a la ejecución remota de código a través de Bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0023:** Localizada en la función setPhonebookAccessPermission del archivo AdapterService.java, existe una posible divulgación de los contactos del usuario a través de bluetooth debido a la falta de comprobación de permisos. Esto podría conducir a la divulgación de información local si una aplicación maliciosa habilita los contactos a través de una conexión bluetooth, con privilegios de ejecución de usuario necesarios.
- **CVE-2020-0070:** Localizada en la función rw_t2t_update_lock_attributes del archivo rw_t2t_ndef.cc, existe una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría llevar a la ejecución remota de código sobre NFC sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0071:** Localizada en la función rw_t2t_extract_default_locks_info del archivo rw_t2t_ndef.cc, existe una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría llevar a la ejecución remota de código sobre NFC sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

- **CVE-2020-0072:** Localizada en la función rw_t2t_handle_tlv_detect_rsp del archivo rw_t2t_ndef.cc, existe una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría llevar a la ejecución remota de código sobre NFC sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0073:** Localizada en la función rw_t2t_handle_tlv_detect_rsp del archivo rw_t2t_ndef.cc, existe una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría llevar a la ejecución remota de código sobre NFC sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0103:** Localizada en la función a2dp_aac_decoder_cleanup del archivo a2dp_aac_decoder.cc, existe un posible free inválido debido a la corrupción de memoria. Esto podría conducir a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0117:** Localizada en la función aes_cmac del archivo aes_cmac.cc, existe una posible escritura fuera de límites debido a un desbordamiento de enteros. Esto podría llevar a la ejecución remota de código en el servidor bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-8597:** Localizada en la función eap.c en pppd en ppp 2.4.2 hasta 2.4.8 tiene un desbordamiento de buffer rhostname en las funciones eap_request y eap_response.

- **CVE-2020-0224:** Localizada en la función FastKeyAccumulator::GetKeysSlow del archivo keys.cc, existe una posible escritura fuera de límites debido a una confusión de tipos. Esto podría llevar a la ejecución remota de código al procesar una configuración de proxy sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0225:** Localizada en la función a2dp_vendor_ldac_decoder_decode_packet del archivo a2dp_vendor_ldac_decoder.cc, existe una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría conducir a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0380:** Localizada en la función allocExcessBits del archivo bitalloc.c, existe una posible escritura fuera de límites debido a una comprobación de límites incorrecta. Esto podría conducir a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0396:** Localizada en varios lugares de la Telefonía, hay una posible derivación de permisos debido a un PendingIntent inseguro. Esto podría conducir a la divulgación de información local con privilegios de ejecución de usuario necesarios. La interacción del usuario no es necesaria para la explotación.
- **CVE-2020-0449:** Localizada en la función btm_sec_disconnected del archivo btm_sec.cc, existe una posible corrupción de memoria debido a un uso después de free. Esto podría llevar a la ejecución remota de código en el servidor Bluetooth sin

necesidad de privilegios de ejecución adicionales. Se necesita la interacción del usuario para la explotación.

- **CVE-2021-0316:** Localizada en la función avrc_pars_vendor_cmd del archivo avrc_pars_tg.cc, hay una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría conducir a la ejecución remota de código a través de Bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0326:** Localizada en la función p2p_copy_client_info del archivo p2p.c, hay una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría conducir a la ejecución remota de código si el dispositivo de destino está realizando una búsqueda de Wi-Fi Direct, sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0397:** Localizada en la función sdp_copy_raw_data del archivo sdp_discovery.cc, existe un posible compromiso del sistema debido a un doble free. Esto podría llevar a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0430:** Localizada en la función rw_mfc_handle_read_op del archivo rw_mfc.cc, hay una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría conducir a la ejecución remota de código a través de un paquete NFC malicioso sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

- **CVE-2021-0473:** Localizada en la función rw_t3t_process_error del archivo rw_t3t.cc, existe un posible doble free debido a datos no inicializados. Esto podría llevar a la ejecución remota de código sobre NFC sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0474:** Localizada en la función avrc_msg_cback del archivo avrc_api.cc, existe una posible escritura fuera de límites debido a un desbordamiento de búfer de la pila. Esto podría conducir a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0475:** Localizada en la función on_l2cap_data_ind del archivo btif_sock_l2cap.cc, existe una posible corrupción de memoria debido a un uso después de free. Esto podría conducir a la ejecución remota de código a través de Bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0507:** Localizada en la función handle_rc_metamsg_cmd de btif_rc.cc, hay una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría conducir a la ejecución remota de código a través de Bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0516:** Localizada en la función p2p_process_prov_disc_req del archivo p2p_pd.c, existe una posible lectura y escritura fuera de límites debido a un uso después de free. Esto podría conducir a una escalada remota de privilegios sin

necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

- **CVE-2021-0870:** Localizada en la función RW_SetActivatedTagType del archivo rw_main.cc, existe una posible corrupción de memoria debido a una condición de carrera. Esto podría llevar a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0918:** Localizada en la función gatt_process_notification del archivo gatt_cl.cc, hay una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría conducir a la ejecución remota de código a través de Bluetooth sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0930:** Localizada en la función phNxpNciHal_process_ext_rsp del archivo phNxpNciHal_ext.cc, hay una posible escritura fuera de límites debido a una comprobación de límites que falta. Esto podría llevar a la ejecución remota de código sobre NFC sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-0968:** Localizada en las funciones osi_malloc y osi_calloc del archivo allocator.cc, existe una posible escritura fuera de límites debido a un desbordamiento de enteros. Esto podría conducir a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

- **CVE-2021-0956:** Localizada en la función NfcTag::discoverTechnologies (activación) del archivo NfcTag.cpp, existe una posible escritura fuera de límites debido a una comprobación de límites incorrecta. Esto podría conducir a una escalada remota de privilegios sin necesidad de privilegios adicionales de ejecución del sistema. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-39675:** Localizada en la función GKI_getbuf del archivo gki_buffer.cc, existe una posible escritura fuera de límites debido a un desbordamiento de búfer de la pila. Esto podría conducir a una escalada remota de privilegios sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2021-39708:** Localizada en la función gatt_process_notification del archivo gatt_cl.cc, existe una posible escritura fuera de límites debido a una comprobación de límites incorrecta. Esto podría conducir a una escalada remota de privilegios sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2022-20127:** Localizada en la función ce_t4t_data_cback del archivo ce_t4t.cc, existe una posible escritura fuera de límites debido a un doble free. Esto podría conducir a la ejecución remota de código sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2022-20140:** Localizada en la función read_multi_rsp del archivo gatt_sr.cc, existe una posible escritura fuera de límites debido a una comprobación de límites incorrecta. Esto podría conducir a una escalada remota de privilegios sin necesidad

de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

- **CVE-2022-20145:** Localizada en la función startLegacyVpnPrivileged del archivo Vpn.java, existe una posible forma de recuperar las credenciales de la VPN debido a un ataque de bajada de protocolo. Esto podría conducir a una escalada remota de privilegios si se utiliza un AP Wi-Fi malicioso, sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.
- **CVE-2019-17666:** Localizada en rtl_p2p_noa_ie de drivers/net/wireless/realtek/rtlwifi/ps.c en el kernel de Linux hasta la versión 5.3.6 carece de cierta comprobación de límite superior, lo que conduce a un desbordamiento de búfer.

Categorías de Herramientas de Análisis Forense.

Están disponibles hoy una vasta cantidad de herramientas de análisis forense para varios dispositivos móviles, incluyendo Android. De esa manera, para una adquisición y análisis bien sucedida, es muy importante que el examinador conozca los recursos y tipos de herramientas disponibles. De otra manera, se podría poner en riesgo la integridad de los datos recuperados durante el proceso de análisis forense.

Comprender los diversos tipos de herramientas de adquisición móvil y los datos que son capaces de recuperar es importante para un examinador forense móvil. Las herramientas y metodologías son categorizadas de forma piramidal que van del Nivel 1 al Nivel 5.

Figura 1

Sistema de categorización de herramientas para dispositivos móviles.

Nota. Ilustración en modo pirámide que describe la categorización de los diversos tipos de herramientas para la adquisición de datos móviles. Adaptado de (Ayers et al., 2014).

Nivel 1 (Extracción Manual). Los métodos de extracción manual involucran el registro de información que aparece en la pantalla de un dispositivo móvil cuando se emplea la interfaz de usuario. El contenido que se muestra en la pantalla LCD debe editarse manualmente por medio de botones, teclados o pantallas táctiles para la visualización de contenidos en dispositivos móviles. Los datos descubiertos se pueden grabar con una cámara digital externa. Es imposible recuperar la información eliminada a este nivel.

Nivel 2 (Extracción Lógica). Los métodos de extracción lógica se usan con más frecuencia en este momento y son levemente técnicos, lo que requiere un entrenamiento de nivel principiante. Aquí, el analista accede a los datos a través de una conexión USB, WLAN, Bluetooth, etc. Las herramientas de extracción lógica comienzan enviando una

serie de comandos a través de la interfaz establecida desde la computadora al dispositivo móvil.

Nivel 3 (Hex Dumping/JTAG): Esta técnica es el método más utilizado por las herramientas en este nivel. Esto implica cargar un cargador de arranque modificado (u otro software) en un área protegida de la memoria (por ejemplo, RAM) en el dispositivo. Este proceso de carga se logra conectando el puerto de datos del dispositivo móvil a una caja intermitente y la caja intermitente se conecta a su vez a la estación de trabajo forense.

Nivel 4 (Chip-Off): Los métodos Chip-Off se refieren a la adquisición de datos directamente desde la memoria flash de un dispositivo móvil. Esta extracción requiere la eliminación física de la memoria flash. Chip-Off brinda a los examinadores la capacidad de crear una imagen binaria del chip extraído. Para proporcionar al examinador datos en un archivo de formato binario contiguo, el algoritmo de nivelación de desgaste debe ser de ingeniería inversa.

Nivel 5 (Micro Read). Consiste en registrar la observación física de las puertas en un chip NAND o NOR con el uso de un microscopio electrónico. Debido a los tecnicismos extremos involucrados al realizar una lectura micro, este nivel de adquisición sólo se intentará para casos de alto perfil equivalentes a una crisis de seguridad nacional después de que se hayan agotado todas las demás técnicas de adquisición. La adquisición exitosa a este nivel requeriría un equipo de expertos, equipo adecuado, tiempo y un conocimiento profundo de la información propietaria (Ayers et al., 2014).

Herramientas Disponibles

Debido a la gran cantidad de herramientas disponibles, el tipo de dispositivo y los datos extraídos juegan un papel importante en la elección de la herramienta a utilizar.

Ahora es bien sabido que las herramientas no tienen que ser costosas para ser efectivas. Además, a medida que aumenta la tendencia del desarrollo de aplicaciones móviles, existen algunas herramientas gratuitas para ayudarlo a analizar su dispositivo Android. Sin embargo, en el campo del análisis forense, las herramientas pagas aún dominan y tienden a ofrecer servicios y opciones más completas que las herramientas gratuitas.

Es interesante probar diferentes herramientas en un dispositivo de prueba para ver qué herramienta funciona mejor para cada situación y dispositivo. Además, la familiaridad con la funcionalidad de la herramienta es una gran ventaja a la hora de realizar extracciones.

Es importante recordar que todas las herramientas pueden manejar errores. Puede ser un error de implementación o desarrollo en la propia herramienta, o puede que la estructura de datos generada por otro programa sea incorrecta. De esta manera, tiene un alto nivel de confianza y comprensión. Las habilidades con las herramientas son esenciales para una operación adecuada.

Aquí se enumeran tanto las herramientas diseñadas específicamente para el análisis de Android como las herramientas con características más generales, pero, no obstante, es muy útil para el análisis forense y se puede utilizar en dispositivos Android (Costa Silva, 2019, 17).

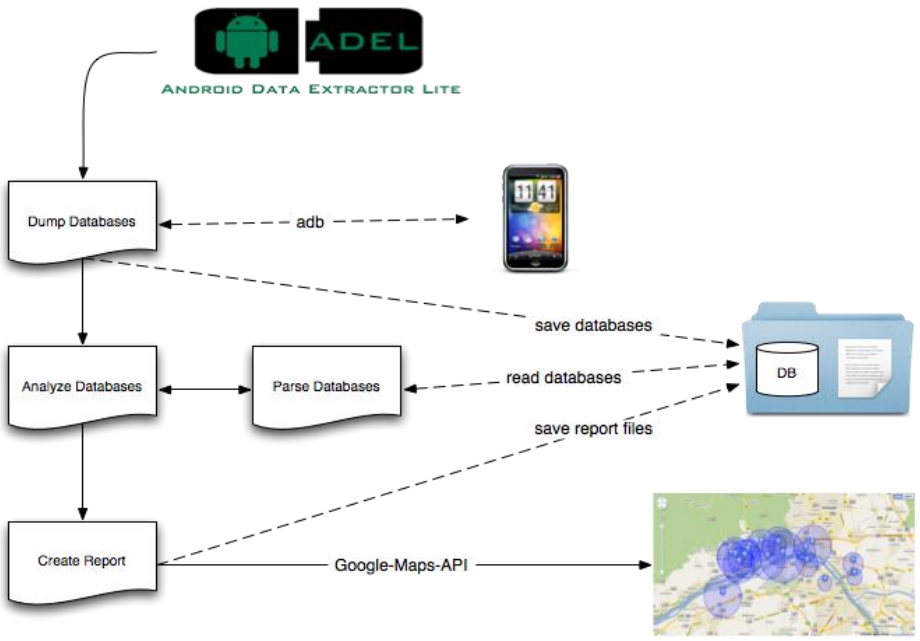
ADEL – Android Data Extractor Lite.

Como describe Forensic Blog (s.f.) ADEL, significa "Android Data Extractor Lite". ADEL se desarrolló para las versiones 2.x de Android y puede volcar automáticamente archivos de base de datos SQLite seleccionados de dispositivos Android y extraer el contenido almacenado en los archivos volcados. En esta sección describimos las principales tareas de

ADEL y qué pasos realiza realmente la herramienta. Sin embargo, hay condiciones que deben darse para que ADEL funcione correctamente. Utiliza el kit de desarrollo de software de Android (Android SDK) y especialmente el deamon adb para volcar los archivos de la base de datos en la máquina del investigador. Estas condiciones se recogen en los siguientes apartados, correspondientes a las tareas correspondientes. Un diagrama de flujo que muestra la estructura de ADEL se muestra en la siguiente figura:

Figura 2

Flujo de procesos de ADEL



Nota. Ilustración que define los procesos de la aplicación ADEL y su funcionalidad. Adaptado de (Costa Silva, 2019).

ADEL está destinado a tratar los datos de forma correcta. Este objetivo se alcanza por el hecho de que las actividades no se realizan directamente en el teléfono, sino en una copia de las bases de datos. Este procedimiento asegura que los datos no se modifiquen, ni por

los usuarios de ADEL ni por un sistema operativo no comprometido. Para probar la corrección forense de ADEL, los valores hash se calculan antes y después de cada análisis, para garantizar que los datos descargados no hayan cambiado durante el análisis.

Contiene dos módulos separados: el módulo de análisis y el de informe. Existen interfaces predefinidas entre estos módulos y ambos se pueden modificar fácilmente con funciones adicionales. La estructura modular permite volcar y analizar más bases de datos de teléfonos inteligentes sin gran esfuerzo y facilita las actualizaciones del sistema en el futuro.

El uso de ADEL pretende ser lo más simple posible para permitir su uso tanto por personas cualificadas como por no expertos. En el mejor de los casos, el análisis del teléfono móvil se realiza de forma autónoma para que el usuario no reciba ningún aviso de procesos internos. Además, el módulo de informe crea un informe detallado en un formato legible, que incluye todos los datos decodificados. Durante la ejecución, ADEL opcionalmente escribe un extenso archivo de registro donde se rastrean todos los pasos importantes que se ejecutaron.

La versión actual de ADEL está disponible en el repositorio de GitHub, y la base de datos analizada y procesada contiene la siguiente información:

- Información del teléfono y de la tarjeta SIM (por ejemplo, IMSI y número de serie)
- Directorio telefónico y listas de llamadas,
- Entradas de calendario,
- Mensajes SMS,
- Ubicaciones GPS de diferentes fuentes en el teléfono inteligente

Androl4b.

Según Velasco, (2017) Androl4b es una herramienta de emulación que está desarrollada en base al sistema operativo libre Ubuntu Mate, y permite el desarrollo de procesos de indagación forense con gran nivel de detalle en específico para aplicaciones de Android. El emulador trae consigo un abanico de apps, herramientas y guías a modo de tutoriales específicamente diseñados para probar sus funcionalidades, efectuar tests de seguridad y estudios de análisis sobre las aplicaciones

Herramientas que tiene Androl4b

- Radare2: este es una plantilla de Unix para ingeniería inversa que permite emplear diferentes tools en la consola.
- Frida: esté tool permite la inyección de combinaciones de código en JavaScript, con el fin de favorecer la indagación de apps de sistemas operativos como Windows, macOS, Linux y Android.
- ByteCodeViewer: esta herramienta permite editar, depurar y descompilar apps de Android (APK), para así poder realizar el proceso de ingeniería inversa.
- Mobile Security Framework (Mobsf); la función principal de este tool está diseñada para efectuar tareas de pentesting sobre apps de Android.
- Dozer: ofrece gran variedad de tools y recursos en materia de seguridad para Android.
- APKtool: la herramienta permite directamente efectuar acciones de ingeniería inversa sobre apps de Android.
- BurpSuite: cuenta con una agrupación de apps de seguridad.
- Wireshark: esta herramienta permite la revisión de package y protocolos que emplea una red.

- Qark: este tool es empleado en la indagación y la búsqueda de defectos en materia de seguridad sobre apps de Android.

Cabe mencionar que esta herramienta es Open Source, de modo que está disponible para su descarga en forma libre desde su repositorio oficial en la plataforma GitHub. Actualmente se halla en la tercera versión, la cual trae consigo nuevas versiones de apps y laboratorios que permiten conocer su funcionalidad y alcance, y sobre todo está al día para ejecutarse sobre versiones de Ubuntu Mate 17.04 en adelante.

Dr. Fone Toolkit.

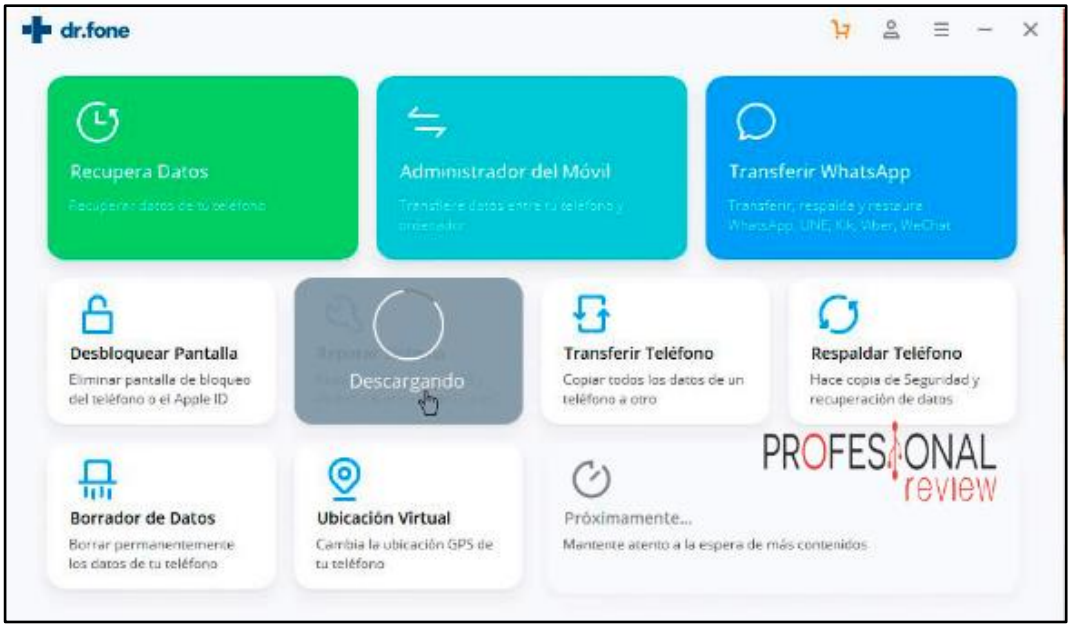
Este software permite la administración de un dispositivo móvil inteligente que brinda opciones de recuperación de datos eliminados del dispositivo, gestión del smartphone, transferencia en aplicaciones como: WhatsApp, Viber entre otras, mover los datos en su totalidad, tener conocimiento del sitio donde está el dispositivo o restaurar un S.O.

Presenta distintas funciones ahora bien para poder sacarle el máximo provecho, deberemos contar con la app para el dispositivo móvil y la app de escritorio para Windows o Mac. Se destaca que esta app forma parte de la familia de Wondershare.

Programa Windows dr. fone. Como menciona Aller (2019) esta app para escritorio en Windows, se ejecuta en base a módulos, esto se refiere a que luego del proceso mismo de instalación, se deberá descargar el módulo que necesitemos, esto hace que el usuario tenga el control de lo que va a instalar, aunque Wondershare presenta un kit de tools que se venden por separado.

Figura 3

Vista inicial del sistema Windows Dr. fone



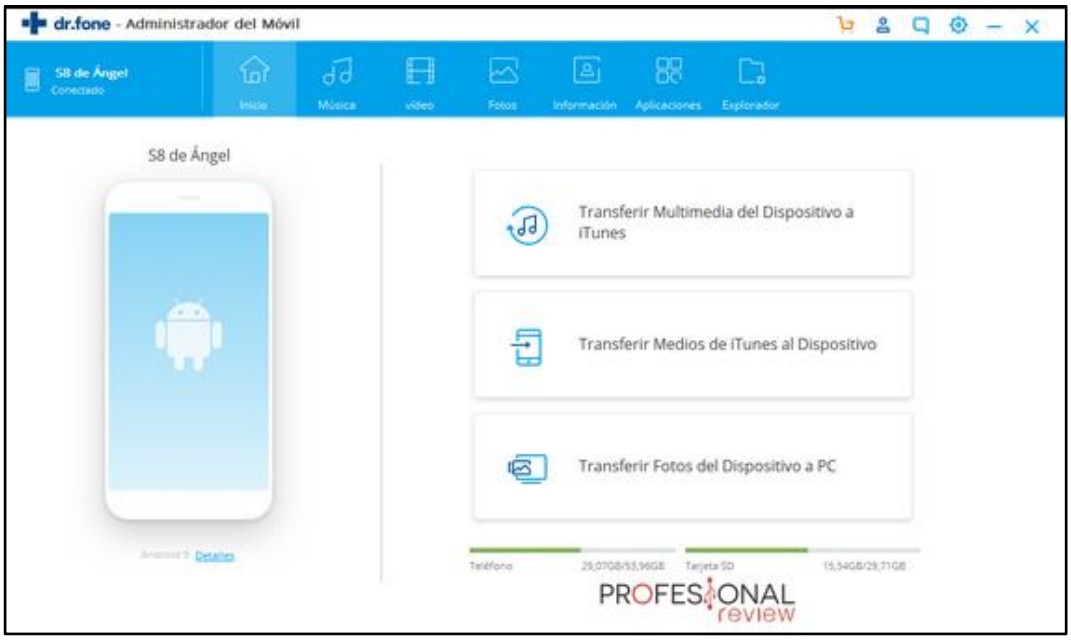
Nota. Ilustración que representa una captura de pantalla de la ventana principal de la aplicación Dr. Fone. Adaptado de (Aller, 2019).

Esta herramienta tiene su objetivo específico para la administración de servicios de mensajería, así presenta cuatro funciones cómo: Transferir mensajes de WhatsApp, otra de ellas es el Respaldo de mensajes de WhatsApp convirtiéndose esta en la transferencia de mensaje a un computador de escritorio, por último, presenta la Restauración de mensaje de WhatsApp tanto para smartphones iOS y Android. Si se da el caso de contener algún respaldo en una PC, esta se podrá recuperar directamente al smartphone.

La interfaz de administración facilita la navegación entre carpetas como es hacia diferentes medios de almacenamiento como SD o Almacenamiento interno. Se destaca que, si un dispositivo no ha entrado en estado de root, el acceso a ciertas secciones estará restringido.

Figura 4

Interfaz de administración del smartphone



Nota. Captura de pantalla que presenta la ventana principal al iniciar la aplicación Dr. Fone. Adaptado de (Aller, 2019).

Otra función destacable es la recuperación de datos, está a su vez se da la tarea de archivar los datos recuperado por tipo pudiendo ser estas fotos, videos, sms, llamadas entre otros.

La función de transferencia de información de un smartphone a otro, se permite siempre y cuando se conecten ambos dispositivos al PC, la función del computador es la de puente y de este modo se puede transferir.

Entre otras funciones que brinda el sistema está el respaldo de seguridad, formatear todo el dispositivo y/o reparar el S.O, respecto a la localización por GPS se acciona al conectar el smartphone.

Es vital mencionar que, al conectar el smartphone al PC, sucede una operación que descarga la app MobileGo, la cual permite aumentar el rendimiento del smartphone. Una

vez se ejecuta se visualiza una interfaz simple y agradable con un menú poco cargado el cual conjuga las funciones de los primeros módulos elementales.

Blacklight.

Como indica Costa Silva (2019) este software es desarrollado por la empresa americana BlackBag Technologies, en un principio fue ideado exclusivamente para Mac. En la actualidad el sistema puede ejecutarse en Mac y Windows, la herramienta permite la obtención en sentido lógico de los sistemas Android e iOS, y sumado a ello la obtención para los ordenadores.

El software mantiene su compatibilidad desde versiones 4.0.4 de Android hasta la 8.1, en específico para dispositivos de marca Samsung, HTC, LG y Nexus. Presenta ciertos costos para la obtención de la licencia para funcionar. Acciones que el software posibilita al usuario:

- Información del dispositivo, cuentas actuales y borradas
- Logs de registro por concepto de comunicaciones entrantes, salientes y canceladas
- Información de agenda, de notas en texto plano y de contactos registrados
- SMS y MMS
- Ficheros de multimedia y texto plano
- Información de enlace de medios enlazados con antelación al sistema, en el cual se hallan historial con datos de fecha y hora para dispositivos de almacenamiento USB y el acceso de usuario agregado.

Este software permite una indagación más ágil empleando filtros, que permiten separar y mostrar información relevante en un mar de información recolectada. Los filtros permiten evidenciar una clasificación por atributos como: nombre, peso, tipo de archivo y

fecha de creación, tipo de acceso o si ha sido editado. Además, permite el empleo de códigos hash para separar los datos requeridos.

La función de revisión de multimedia y aquellos ficheros que mantengan información relacionada a GPS, el software facilita la visualización sobre el mapa de Google (Maps), otra ventaja que presenta es la organización para archivos con formato de jpg o mp4, en base al tono de color que se almacena en el fichero y triar de los cuadros que conforman un video.

En todo lo que a revisión compete su alcance es tal que revisa logs de llamadas, correo en diferentes formatos, SMS e incluso historial de los sistemas de los sistemas como Social Networks.

La herramienta tiene en su haber un módulo para la generación de informes muy concreto y adaptable, facilitando a los usuarios migrar vastas cantidades de información.

FonePaw

Según Ben (2022) describe esta herramienta es distinguida por su gran labor al momento de realizar un proceso de restauración de información que ha sido extraviada, en dispositivos inteligentes tanto móviles y tabletas con S.O Android.

Se ejecuta en equipos como: Sony, Lenovo, Samsung, Xiaomi, HTC, ZTE, Motorola etc. FonePaw tiene la capacidad de reparar archivos eliminados, seas estos de media, números de teléfono, mensajes, WhatsApp, archivos de audio, historial de llamadas. Para ejecutarse y empezar a realizar su trabajo requiere:

- En primer lugar, conectar el smartphone Android a un pc mediante un cable USB. A continuación, realiza la instalación y ejecución del programa para que halle el dispositivo conectado.

- Seguidamente deberá autorizar, es decir la habilitación en modo depuración USB que viene en el smartphone, acción que no provoca daños en el celular.
- Ahora bien, el programa detectará el smartphone o tableta
- Para finalizar se da inicio a la exploración, del smartphone para en el proceso hallar aquellos archivos que han sido extraviados o eliminados.

Se debe tomar en cuenta, que el software, aunque presenta grandes ventajas a su vez cuenta con grandes limitantes como:

- Límite de tipos de archivos compatibles para el proceso de exploración
- El proceso de escaneo resulta ser demoroso
- No es gratuito

Mobilyze

Como menciona Costa Silva (2019) el software Mobilyze es una herramienta creada por la empresa BlackBag tecnologies, es considerada como una elección más simple que BlackLight, entre sus principales capacidades estás están dirigidas a la importación lógica de los smartphones, sean Android o iOS.

Para hacer uso de la herramienta se debe adquirir su licencia que se estima en una cantidad de 1000 dólares, este precio a pagar permite que se brinde soporte a la herramienta SMS.

La afinidad de esta herramienta va desde versiones de Android 4.0.4 hasta la versión 8.0, están disponibles para dispositivos de marcas como, Samsung, Motorola, HTC, LG y Google Nexus.

Este software presenta una interfaz muy sencilla que facilita su operación, en el proceso de importar datos, es decir que solo hace falta conectar el smartphone a un puerto

USB, del computador donde este instalado Mobilyze esto hace que de forma inmediata se inicie la copia y se provea la adquisición de datos significativa del smartphone.

Mobilyze ejecuta la importación lógica de los datos, favoreciendo al acceso total o parcial de la información al instante. Permite respaldar la información original además si sucede alguna interrupción durante el proceso, la información que ya se ha respaldado será protegida. A continuación, se presentan algunos de los tipos de información que el software puede importar:

- Información del dispositivo y el usuario actual y de los eliminados
- Historial de llamadas
- Información de contactos y notas
- SMS y MMS
- Ficheros multimedia y de doc.

El software cuenta con la opción de uso de filtros sea por fecha y tiempo, búsqueda por palabras llave, clases y generar una marca de tiempo que agilice el proceso de análisis de los datos recolectados, sumado a esto provee support para SMS grupal en dispositivos Samsung. Por otro lado, hace que el historial de llamadas sea analizado, correos de voz, texto e inclusive las acciones efectuadas en social networks como Facebook, Twitter y Linkedln.

El software Mobilyze cuenta con la funcionalidad de informes, en la cual permite añadir todos los datos a los usuarios y también la opción de migrar a formatos como .pdf y .html

Andriller

Según Sacco (2021) es un software práctico que se conforma de un grupo de herramientas forenses exclusivas para teléfonos inteligentes. Este software puede realizar tareas de importación forenses en forma de solo lectura que no son perjudiciales, desde smartphones Android. En su reciente versión 3.6.1 de octubre del año pasado, es posible su obtención desde su repositorio en el sitio github.

La utilidad de este software, es esencial al operar sobre los S.O de Android y en específico es muy utilizado en los casos de peritajes sobre la red social Whatsapp. Entre sus cualidades más representativas está el descifrado del patrón de lock screen, el código PIN, decodificadores modificables para información de apps en bases de datos Android, para descodificar comunicaciones. Además, los procesos de absorción y los decodificadores se encargan de brindar informes sobre lo recolectado en formatos de tipo HTML y XLSX.

Principales Funcionalidades:

- Sustracción de información automática y parsing de datos
- Sustracción de información en dispositivos no-rooteados mediante copia de seguridad
- Sustracción de información con permisos de ráiz: root ADB Daemon, CWM recovery mode, o SU binary
- Analizado de la organización de folders, archivos Tarball y Respaldos Android
- Elección del descifrado de la base de datos de WhatsApp tanto para (msgstore.db.crypt, msgstore.db.crypst5, msgstore.db.crypt7 y msgstore.db.crypt8).
- Agrietamiento de PIN y contraseña del smartphone

- Extrae archivos de respaldo Android.

Oxygen Forensic Detective

El sitio web OXYGEN FORENSICS (s.f.) Oxygen Forensic® Detective es una plataforma de software forense todo en uno creada para extraer, decodificar y analizar datos de múltiples fuentes digitales: dispositivos móviles e IoT, copias de seguridad de dispositivos, UICC y tarjetas de medios, drones y servicios en la nube. Oxygen Forensic® Detective también puede encontrar y extraer una amplia gama de artefactos, archivos del sistema y credenciales de máquinas con Windows, macOS y Linux.

Las tecnologías innovadoras y de vanguardia implementadas en Oxygen Forensic® Detective incluyen, entre otras, eludir bloqueos de pantalla, localizar contraseñas para copias de seguridad cifradas, extraer y analizar datos de aplicaciones seguras y descubrir datos eliminados.

Además, se pueden investigar múltiples extracciones en una sola interfaz para obtener una imagen completa de los datos. Mediante el uso de herramientas analíticas integradas líderes en la industria para encontrar conexiones sociales, crear líneas de tiempo y categorizar imágenes, las fuerzas del orden, los investigadores corporativos y otro personal autorizado pueden ayudar a hacer de este mundo un lugar más seguro.

Funcionalidades soportadas:

- Descifra contraseñas y tokens de cualquier red social además de mostrar contraseñas utilizadas para conectarse a internet a través de WiFi.
- Importa varias copias de seguridad de iOS, Android, Windows Phone
- Permite recuperar todo el registro de llamadas del dispositivo

- Permite acceder a los servicios en la nube de: WhatsApp, Telegram, iCloud, Facebook, Instagram, entre otras.
- Permite generar y personalizar informes de los datos obtenidos en los siguientes formatos: PDF, XLS, RFT Y XML.
- Ver información detallada sobre el dispositivo y su dueño
- Accede a la galería de fotos de los dispositivos, así como también los archivos de audio y vídeo
- Extrae y visualiza la geolocalización del dispositivo de varias fuentes: aplicaciones, cabeceras EXIF de fotos y vídeo, historial de conexiones WiFi.
- Acceder a los SMS, MMS, E-mail, etc.
- Recupera los calendarios, notas y tareas del usuario.

2.4. Legal

El auge de la tecnología en los últimos años ha generado en el mundo un impacto a nivel global, que ha traído una gran ventaja para el acceso a datos que a la postre ha motivado al desarrollo de nuevas formas de generar recursos económicos, las cuales han transformado la forma en que el mundo se desarrolla.

Con la facilidad de acceso a conectividad inalámbrica y el uso de dispositivos tecnológicos, hoy por hoy se generan grandes utilidades para la población mundial que ha dado lugar a nuevas formas de cometer actos ilícitos de naturaleza tecnológica. Siendo así surge la innegable necesidad de poder controlar estos actos que perjudican y violan la privacidad del usuario común.

Estos actos han impulsado a que las organizaciones encargadas de la regulación nacional e internacional se están viendo obligados a generar reglamentos, manuales y leyes

que viabilicen la intervención de la justicia en este tipo de actos que afectan a los sistemas tecnológicos tanto de dispositivos como PC o smartphones.

Las actividades de análisis forense informático se basan en regulaciones impuestas por un gobierno para su territorio. La significancia de que un proceso de análisis forense tenga validez en cada gobierno dentro de su ámbito legal y a pesar de que el experto informático no sea como tal un conocedor del ámbito legal, por lo menos debe tener presente artículos de la legislación que rige en cada territorio.

En la siguiente sección, se citan los artículos más relevantes que se encuentran en vigencia en el territorio nacional de la república del Ecuador en aspectos se seguridad de la información:

Como se menciona, en el Título 1 respecto al art 18 y su definición de infracción penal expresa que:

"Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código" (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 17).

"Los tipos penales describen los elementos de las conductas penalmente relevantes" (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 18).

El COIP, se conforma de principios de los cuales se amplía su instauración en su Art. 454 en el cual afirma que:

El anuncio y práctica de la prueba se regirá por los siguientes principios:

1. Oportunidad. - Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio.

   Los elementos de convicción deben ser presentados en la etapa de evaluación y preparatoria de juicio. Las investigaciones y pericias practicadas durante la

investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia oral de juicio.

Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido de forma anticipada.

2. Inmediación. - Las o los juzgadores y las partes procesales deberán estar presentes en la práctica de la prueba.
3. Contradicción. - Las partes tienen derecho a conocer oportunamente y controvertir las pruebas, tanto las que son producidas en la audiencia de juicio como las testimoniales que se practiquen en forma anticipada.
4. Libertad probatoria. - Todos los hechos y circunstancias pertinentes al caso, se podrán probar por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas.
5. Pertinencia. - Las pruebas deberán referirse, directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción y sus consecuencias, así como a la responsabilidad penal de la persona procesada.
6. Exclusión. - Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal.

Se admitirán aquellos medios de prueba que se refieran a las conversaciones que haya tenido la o el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones preacordadas (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 148-149).

El COIP, describe los procesos preparatorios necesarios para efectuar un juicio este se plasma en su Art. 604 sobre Audiencia preparatoria de juicio donde asienta que:

Para la sustanciación de la audiencia preparatoria del juicio, se seguirán además de las reglas comunes a las audiencias establecidas en este Código, las siguientes:

1. Instalada la audiencia, la o el juzgador solicitará a los sujetos procesales se pronuncien sobre los vicios formales respecto de lo actuado hasta ese momento procesal; de ser pertinente, serán subsanados en la misma audiencia.
2. La o el juzgador resolverá sobre cuestiones referentes a la existencia de requisitos de procedibilidad, cuestiones prejudiciales, competencia y cuestiones de procedimiento que puedan afectar la validez del proceso. La nulidad se declarará siempre que pueda influir en la decisión del proceso o provoque indefensión. Toda omisión hace responsable a las o los juzgadores que en ella han incurrido, quienes serán condenados en las costas respectivas.
3. La o el juzgador ofrecerá la palabra a la o al fiscal que expondrá los fundamentos de su acusación. Luego intervendrá la o el acusador particular, si lo hay y la o el defensor público o privado de la persona procesada.
4. Concluida la intervención de los sujetos procesales, si no hay vicios de procedimiento que afecten la validez procesal, continuará la audiencia, para lo cual las partes deberán:
    a) Anunciar la totalidad de las pruebas, que serán presentadas en la audiencia de juicio, incluyendo las destinadas a fijar la reparación integral para lo cual se podrá escuchar a la víctima, formular solicitudes, objeciones y

planteamientos que estimen relevantes referidos a la oferta de prueba realizada por los demás intervinientes.

b) En ningún caso la o el juzgador podrá decretar la práctica de pruebas de oficio.

c) Solicitar la exclusión, rechazo o inadmisibilidad de los medios de prueba, que estén encaminadas a probar hechos notorios o que por otro motivo no requieran prueba.

La o el juzgador rechazará o aceptará la objeción y en este último caso declarará qué evidencias son ineficaces hasta ese momento procesal; excluirá la práctica de medios de prueba ilegales, incluyendo los que se han obtenido o practicado con violación de los requisitos formales, las normas y garantías previstas en los instrumentos internacionales de protección de derechos humanos, la Constitución y este Código.

d) Los acuerdos probatorios podrán realizarse por mutuo acuerdo entre las partes o a petición de una de ellas cuando sea innecesario probar el hecho, inclusive sobre la comparecencia de los peritos para que rindan testimonio sobre los informes presentados.

5. Concluidas las intervenciones de los sujetos procesales la o el juzgador comunicará motivadamente de manera verbal a los presentes su resolución que se considerará notificada en el mismo acto. Se conservará la grabación de las actuaciones y exposiciones realizadas en la audiencia.

El secretario elaborará, bajo su responsabilidad y su firma, el extracto de la audiencia, que recogerá la identidad de los comparecientes, los procedimientos especiales alternativos del

proceso ordinario que se ha aplicado, las alegaciones, los incidentes y la resolución de la o el juzgador (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 196-197).

El COIP describe los delitos en contra de los sistemas de información y comunicación en su Art. 229 mencionando que:

La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 79).

Continuando con los delitos se presenta otro tipo de acto mencionado en su Art. 230 donde explica que:

Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o

modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 80).

En el territorio nacional los ataques dirigidos contra sistemas informáticos están respaldados por la ley, en su Art. 232 el cual denota que:

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruye o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

   Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 80-81).

El COIP indica que los actos en los cuales una persona no tenga acceso respaldado para acceder a un sistema tendrán consecuencias, aclara de forma explícita en su Art. 234 reflejando que:

La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (CÓDIGO INTEGRAL PENAL, COIP, 2018, pág. 81).

CAPITULO III.

METODOLOGÍA

En este capítulo se explicarán los diferentes procesos para la aplicación de los métodos de investigación que se realizarán.

3.1. Tipo de Investigación

Los tipos de investigación que son utilizados para el desarrollo del proyecto son:

Investigación Documental - Bibliográfica.

Se trabajará en el uso de la modalidad de investigación bibliográfica buscando apalancar el conocimiento de los investigadores para el desarrollo del proyecto a través de: tesis, artículos, libros y documentación en línea que brinden información relevante.

Investigación explicativa.

Nuestra investigación va enfocando en la obtención de información de las diferentes herramientas que se utilizan para realizar análisis forenses, donde nos va a permitir aumentar la comprensión del funcionamiento de estas herramientas.

Investigación cualitativa.

Mediante la investigación cualitativa se van a estudiar e investigar las características y funciones soportadas de las herramientas forenses existentes para Android.

3.2. Enfoque de la investigación

Cualitativa.

El enfoque de la investigación será cualitativo porque se estudiarán e investigarán las características especiales y funciones soportadas de las herramientas forenses existentes para Android.

3.3. Métodos de Investigación

Los métodos de investigación a utilizar para esta investigación son:

Método Bibliográfico.

El método biográfico nos permitirá utilizar técnicas y estrategias de investigación con el fin de localizar, identificar y acceder a los documentos necesarios que contengan la información pertinente para la realización de esta investigación.

Método Inductivo

"El método inductivo es aquel procedimiento de investigación que pone en práctica el pensamiento o razonamiento inductivo. Este último se caracteriza por ser ampliativo, o sea, generalizador, ya que parte de premisas cuya verdad apoya la conclusión, pero no la garantiza" (Editorial Etecé, 2020).

Este método nos permite seguir una serie de pasos, iniciando con la observación de determinados hechos, de los cuales, registramos, analizaremos y contrastaremos la información obtenida para poder dar una explicación o teoría.

3.4. Técnicas e Instrumentos de Recopilación de Datos

Fichas de observación.

Las fichas de observación nos permitirán recolectar y registrar los datos obtenidos para analizar de forma ordenada y minuciosa las herramientas forenses.

3.5. Universo, Población y Muestra

Universo

Actualmente existen alrededor de 63 herramientas para análisis forense entre gratuitas y de pago.

Población

De las 63 herramientas antes mencionadas, 8 son de uso exclusivo para los dispositivos móviles Android que siguen en funcionamiento actualmente.

Muestra

La muestra seleccionada será igual a la población, es decir, nuestra muestra será de 8 herramientas.

3.6. Procesamiento de la Información

Para el procesamiento de la información se hará uso de la herramienta informática Excel en su versión 2016, perteneciente al paquete de herramientas ofimáticas de Office. Mediante el empleo de esta herramienta se procesan los datos obtenidos en las fichas de observación.

CAPITULO IV.

RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y Discusión de Resultados

Para obtener información de las características y funcionalidades de estas herramientas, se probó cada una de estas herramientas para posteriormente proceder a llenar las fichas de observación con la información obtenida. Se realizó ocho fichas de observación, una por cada herramienta.

De la información obtenida y al finalizar la evaluación de las herramientas para el análisis forense la información generada por las fichas de observación, se encuentran detalladas en la siguiente tabla comparativa.

Tabla 10

Tabla comparativa de las características de las herramientas descritas.

REQUISITOS DEL	HERRAMIENTA	ADEL	Androl4b	Dr. Fone	FonePaw	BlackLight	Mobilyze	Andriller	Oxygen Forensic Detective

	Sistema Operacional	Script para Python	Máquina virtual, basada en Ubuntu Mate	Windows versión: 10, 8, 7 Vista, XP Mac OS X 10.8 o superior	Windows versión: 10, 8, 7 Vista, XP Mac OS X 10.8 o superior	Windows versión: 7 o Superior Mac OS X El Capitan (10.11.4) o superior	Windows versión: 7 o Superior Mac OS X Yosemite (10.10) o superior	Windows versión: Xp, Vista 7, 8 o Linux	Windows versión: 7, 8 y 10
	Requerimientos mínimos para ejecución	(ND)	(ND)	CPU: 1GHz Intel Memoria de: 512mb	CPU: Intel/AMD Memoria de: 1GB	CPU: 2.7 GHz Intel Core i7 Memoria de: 16GB DDR3	CPU: 2.6 GHz Intel Dual Core i5 Memoria de: 8GB 1067 MHz DDR3	(ND)	(ND)
CARACTERISTICAS ESPECIALES	Coste	Gratuito	Gratuito	Disponible en US $39,95 Cuenta con versión de prueba	Desde US $76,90 Cuenta con versión de prueba	Valor de US$ 3,400	Valor US$ 1.000	Gratuita	Privativa
	Versión de Android	Android 2.0 y Posterior	Cambiante referente a la funcionalidad	Android 2.1 y superior	Android 2.1 hasta 8.0	Android 4.0.4 hasta 8.1	Android 4.0.4 hasta 8.0	Android 4.o y superior	Android 4.o y superior
FUNCIONALIDADES SOPORTAD	Recuperación de informaciones del dispositivo	✓	✓	✓	✓	✓	✓	✓	**(X)**
	Recuperación de llamadas	✓	✓	✓	✓	✓	✓	✓	**(X)**

	Recuperación de contactos	✓	✓	✓	✓	✓	✓	✓	**(X)**
	Recuperación de entradas de calendario	✓	✓	✓	✓	✓	✓	✓	✓
	Recuperación de mensajes (SMS y MMS)	✓	✓	✓	✓	✓	✓	✓	✓
	Recuperación de correo electrónico	✓	✓	✓	✓	✓	✓	✓	✓
	Recuperación de archivos multimedia	✓	✓	✓	✓	✓	✓	✓	✓
	Recuperación de ubicación GPS	✓	**(X)**	**(X)**	**(X)**	✓	✓	✓	✓
	Recuperación de datos borrados	✓	**(X)**	✓	✓	✓	✓	✓	✓
	Recuperación de datos de conexión	**(X)**	**(X)**	**(X)**	**(X)**	✓	✓	✓	**(X)**
	Preservación de datos	✓	**(X)**	**(X)**	**(X)**	✓	✓	✓	✓
	Informes de datos recuperados	✓	Cambiante referente a la funcionalidad	✓	✓	✓	✓	✓	✓

	Personalización de informes	**(X)**	Cambiante referente a la funcionalidad	**(X)**	**(X)**	✓	✓	✓	**(X)**

Nota. Tabla resumen que presenta características y funcionalidades de las herramientas descritas para este trabajo.

Como podemos observar, estas herramientas cumplen parcialmente con las funcionalidades que una herramienta de análisis forense debe tener. Sin embargo, hay tres herramientas que destacan, BlackLight, Mobilyze, y Andriller. Estas tres herramientas cumplen su totalidad con las funciones necesarias para poder realizar un análisis forense.

Un factor a tomar en cuenta es el coste que tienen estas herramientas, por ello, hemos seleccionado como la mejor herramienta a Andriller, ya que, esta herramienta es gratuita y cuenta con otra funcionalidad que la complementa.

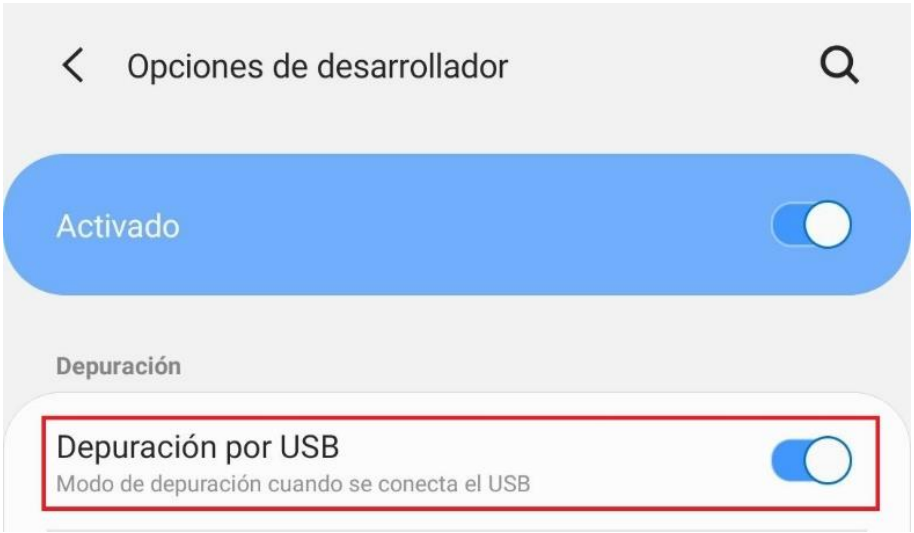
Una de estas funcionalidades es WhatsApp Crypt, que nos permite desencriptar los chats de esta aplicación de mensajería.

Para proceder a extraer la información de un dispositivo móvil Android, haremos uso del dispositivo móvil de uno de los investigadores, para ello seguiremos los siguientes pasos:

Activar la depuración USB del móvil, para poder activar esta opción tenemos que acceder a la información del dispositivo y presionar 8 veces el número de compilación del dispositivo para poder acceder a las opciones de desarrollador donde se encuentra esta opción.

Figura 5

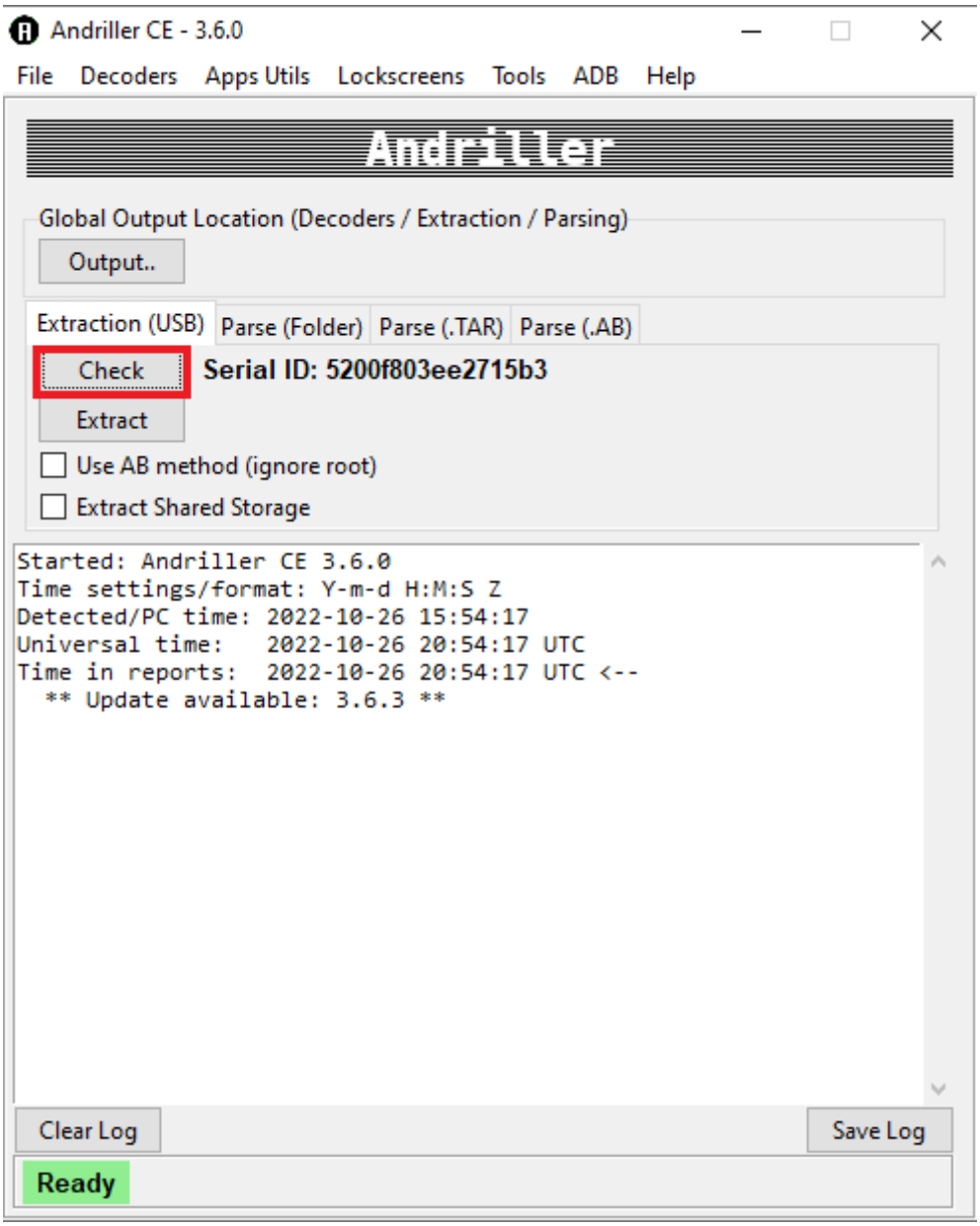
Activación de la depuración USB del dispositivo móvil



Una vez tengamos activada la depuración USB, conectamos el dispositivo móvil al computador para que la herramienta reconozca el móvil. Hacemos click en Check para verificar que el dispositivo esté conectado al computador.

Figura 6

Verificación del dispositivo conectado al computador

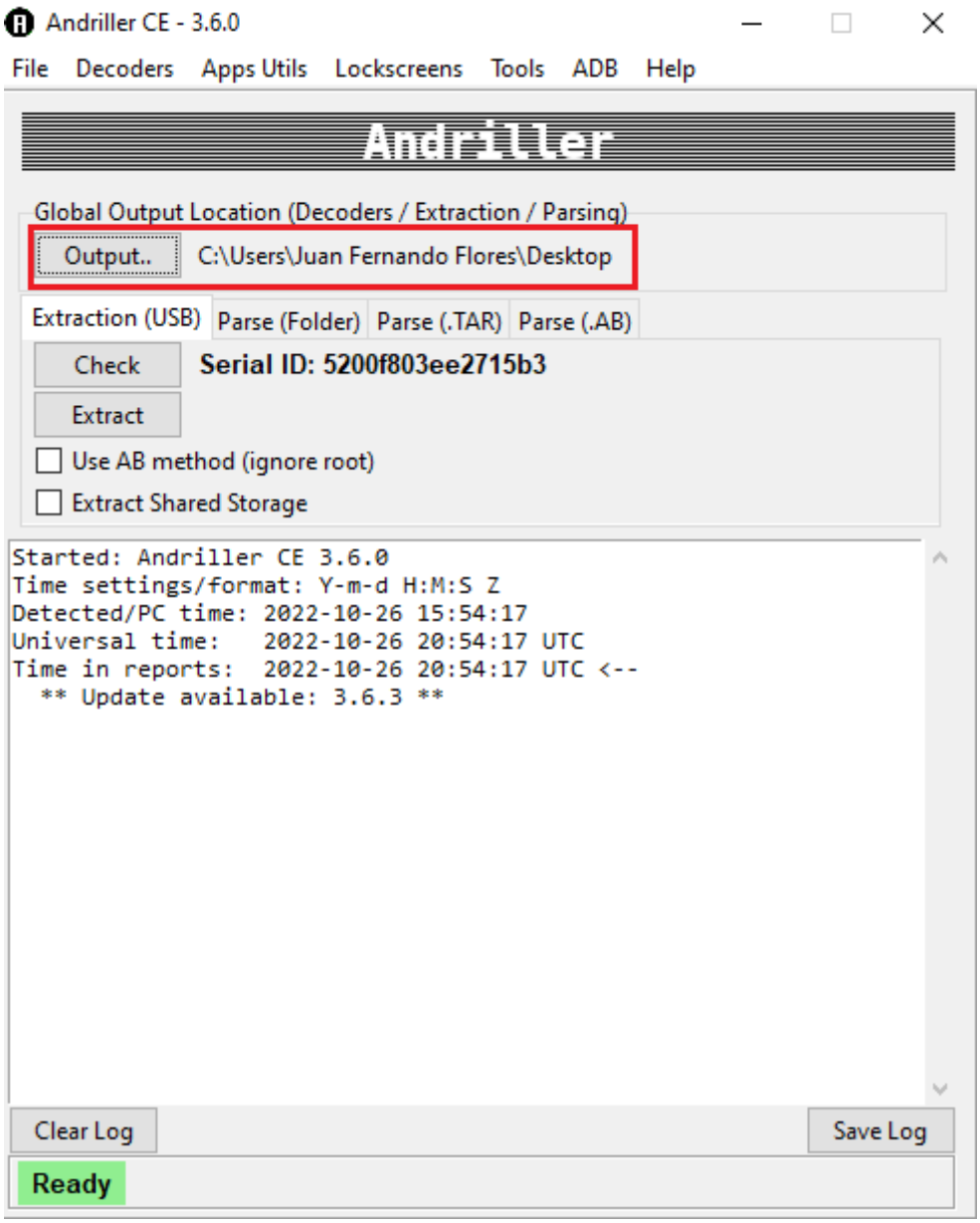


Nota. Cuando la herramienta reconoce al dispositivo, se puede observar un Serial ID, este corresponde al número de serie del dispositivo conectado.

Luego de esto, seleccionaremos el lugar donde se guardará la información extraída, para ello, haremos click en la opción Output y seleccionamos la ubicación, en este caso lo guardaremos en el Escritorio.

Figura 7

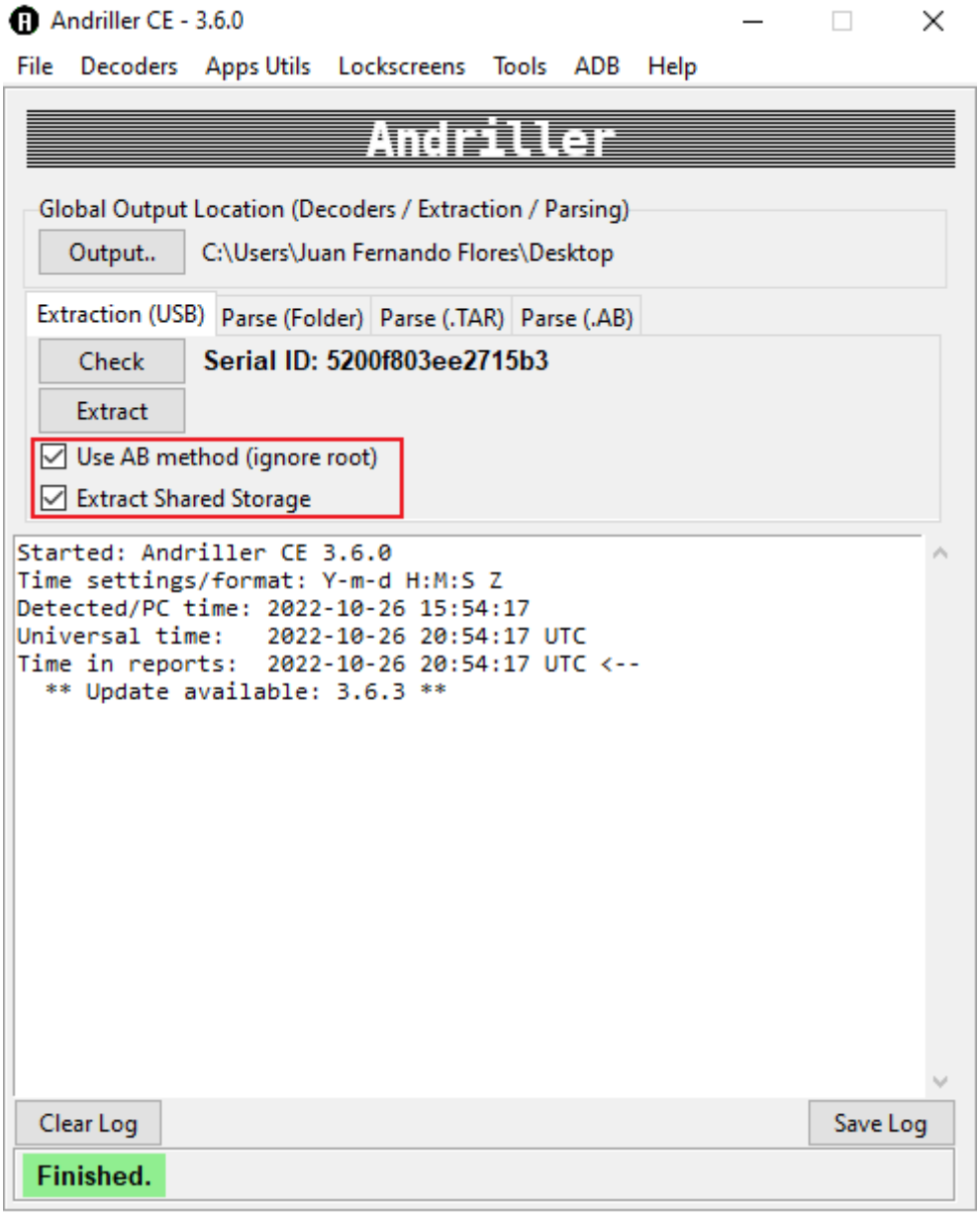
Selección de la ubicación donde se guardará la información extraída



Ahora seleccionamos las opciones Use AB method (ignore) y Extract Shared Storage para poder extraer la información del dispositivo móvil, una vez hecho esto, le damos click en la opción Extract.

Figura 8

Selección de las opciones Use AB method (ignore) y Extract Shared Storage

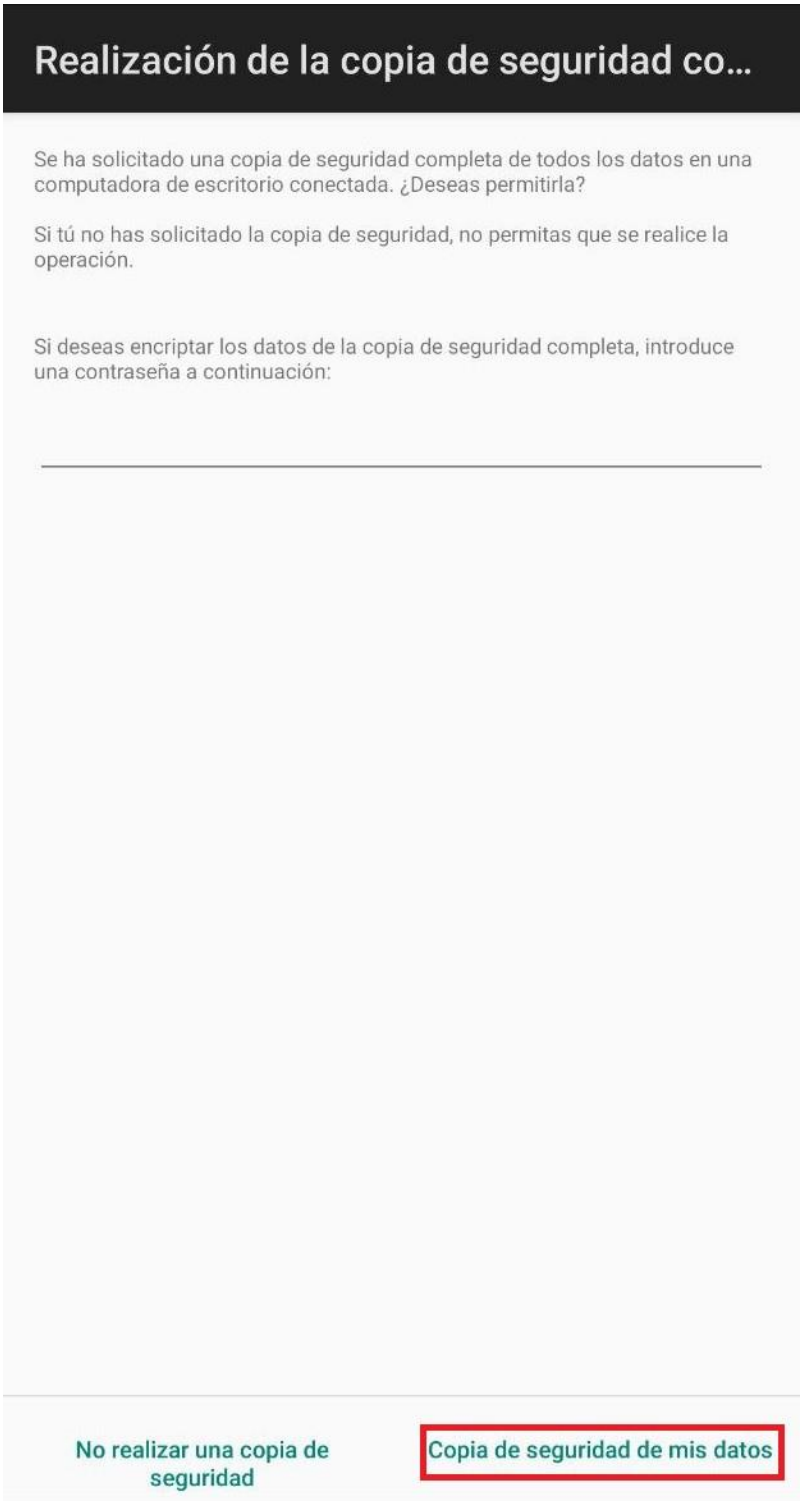


Nota. Es importante seleccionar estas opciones, ya que sin esto la herramienta no puede realizar la extracción de información del dispositivo.

En el dispositivo móvil, daremos autorización para poder realizar una copia de seguridad del dispositivo. Para ello, presionamos en la opción Copia de seguridad de mis datos.

Figura 9

Autorización para realizar la copia de seguridad del dispositivo



Una vez finalice en proceso de extracción, la herramienta nos mostrará un informe general con toda la información que se ha extraído del dispositivo móvil.

Figura 10

Informe general de la información extraída

This report was generated using Andriller CE # (This field is editable in Preferences)

[Andriller Report]

Type	Data
Serial	5200f803ee2715b3
Status	device
Permisson	shell
Wifi Mac	
Local_Time	2022-10-18 10:08:20 Hora de verano central (M&#65533;xico)
Device_Time	2022-10-18 10:08:17 -05
Accounts	• com.google: • com.google: • com.osp.app.signin: j • com.samsung.android.exchange: • com.samsung.android.email: j • com.samsung.android.email • com.whatsapp: \ • org.telegram.messenger • com.truecaller.account: T • com.facebook.messenger: M • com.twitter.android.auth.login: • com.twitter.android.auth.login: • com.microsoft.office: • com.microsoft.skydrive: • com.facebook.auth.login: • com.facebook.auth.login: • com.osp.app.signin:
Application	Shared Storage (2980)
Application	Android Calendar (47)

 # andriller.com # (This field is editable in Preferences)

Nota. El informe muestra información del dispositivo como el serial, la Wifi MAC, las cuentas que están asociadas a ese dispositivo, etc. Por cuestiones de seguridad se ha pixelado las cuentas y el wifi MAC que se encuentran asociadas al dispositivo del investigador.

En el apartado Shared Storage del informe, nos muestra todos los archivos multimedia que se pudo extraer del dispositivo.

Figura 11

Archivos multimedia extraídos del dispositivo

Shared Storage

Total: 2980

Index	Directory	Filename	Size	Modified
1	shared/0/Movies/Instagram	VID_112680123_163918_220.mp4	125.8KB	2022-08-21 23:46:38 UTC
2	shared/0/snaptube/db	app_database.db-shm	32.0KB	2022-10-17 17:59:15 UTC
3	shared/0/snaptube/db	app_database.db	64.0KB	2022-10-06 00:24:18 UTC
4	shared/0/snaptube/db	app_database.db-wal	382.3KB	2022-10-15 22:49:20 UTC
5	shared/0/snaptube/.config	.udid_time	10	2022-08-18 13:55:21 UTC
6	shared/0/DCIM/Facebook	FB_IMG_1662427285285.jpg	81.2KB	2022-09-06 01:21:25 UTC
7	shared/0/DCIM/Facebook	FB_IMG_1666060639871.jpg	30.9KB	2022-10-18 02:37:19 UTC
8	shared/0/DCIM/Facebook	FB_IMG_1664467417975.jpg	49.0KB	2022-09-29 16:03:37 UTC
9	shared/0/DCIM/Facebook	FB_IMG_1661917013482.jpg	64.1KB	2022-08-31 03:36:53 UTC
10	shared/0/DCIM/Facebook	FB_IMG_1665373894225.jpg	32.1KB	2022-10-10 03:51:34 UTC
11	shared/0/DCIM/Facebook	FB_IMG_1662815237993.jpg	57.3KB	2022-09-10 13:07:18 UTC
12	shared/0/DCIM/Facebook	FB_IMG_1662495419609.jpg	131.1KB	2022-09-06 20:16:59 UTC
13	shared/0/DCIM/Facebook	FB_IMG_1665794385155.jpg	89.4KB	2022-10-15 00:39:45 UTC
14	shared/0/DCIM/Facebook	FB_IMG_1665549573903.jpg	11.1KB	2022-10-12 04:39:33 UTC
15	shared/0/DCIM/Facebook	FB_IMG_1666069367629.jpg	17.1KB	2022-10-18 05:02:47 UTC
16	shared/0/DCIM/Facebook	FB_IMG_1665499032977.jpg	34.4KB	2022-10-11 14:37:12 UTC
17	shared/0/DCIM/Facebook	FB_IMG_1662821577990.jpg	25.6KB	2022-09-10 14:52:57 UTC
18	shared/0/DCIM/Facebook	FB_IMG_1661479306730.jpg	15.3KB	2022-08-26 02:01:46 UTC
19	shared/0/DCIM/Facebook	FB_IMG_1664988577752.jpg	74.6KB	2022-10-05 16:49:37 UTC
20	shared/0/DCIM/Facebook	FB_IMG_1663999799959.jpg	90.4KB	2022-09-24 06:09:59 UTC
21	shared/0/DCIM/Facebook	FB_IMG_1666069325956.jpg	62.5KB	2022-10-18 05:02:05 UTC
22	shared/0/DCIM/Facebook	FB_IMG_1663163670343.jpg	70.4KB	2022-09-14 13:54:30 UTC
23	shared/0/DCIM/Facebook	FB_IMG_1665505029131.jpg	33.1KB	2022-10-11 16:17:09 UTC
24	shared/0/DCIM/Facebook	FB_IMG_1661654788490.jpg	39.6KB	2022-08-28 02:46:28 UTC

Por otro lado, en el aparado Android Calendar, encontramos toda la información del calendario del dispositivo.

Figura 12

Información del calendario del dispositivo

Android Calendar

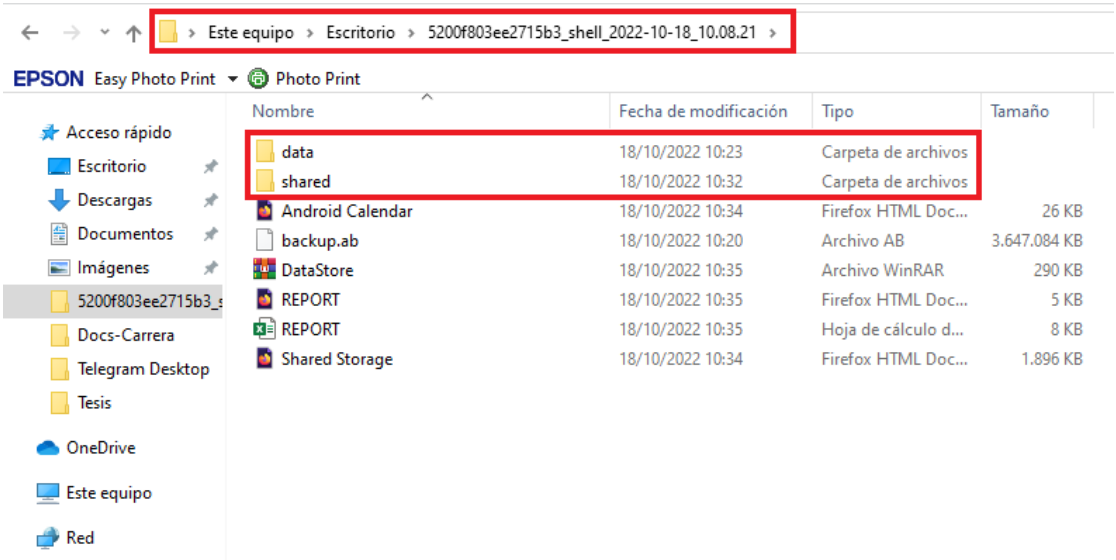
Total: 47

Index	Title	Location	Description	Time	Start	End
42	descanso laboral correspondiente a Día de la Independencia		Día festivo	2023-08-12 00:00:00 UTC	2023-08-11 00:00:00 UTC	2023-08-12 00:00:00 UTC
14	Día de la Independencia		Día festivo	2023-08-11 00:00:00 UTC	2023-08-10 00:00:00 UTC	2023-08-11 00:00:00 UTC
21	Natalicio de Simón Bolivar		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2023-07-25 00:00:00 UTC	2023-07-24 00:00:00 UTC	2023-07-25 00:00:00 UTC
20	descanso laboral correspondiente a Batalla de Pichincha		Día festivo	2023-05-27 00:00:00 UTC	2023-05-26 00:00:00 UTC	2023-05-27 00:00:00 UTC
40	Batalla de Pichincha		Día festivo	2023-05-25 00:00:00 UTC	2023-05-24 00:00:00 UTC	2023-05-25 00:00:00 UTC
2	¡Feliz cumpleaños!		¡Feliz cumpleaños!	2023-05-22 00:00:00 UTC	2023-05-21 00:00:00 UTC	2023-05-22 00:00:00 UTC
13	Día del Trabajo		Día festivo	2023-05-02 00:00:00 UTC	2023-05-01 00:00:00 UTC	2023-05-02 00:00:00 UTC
30	Pascua		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2023-04-10 00:00:00 UTC	2023-04-09 00:00:00 UTC	2023-04-10 00:00:00 UTC
19	Sábado de Gloria		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2023-04-09 00:00:00 UTC	2023-04-08 00:00:00 UTC	2023-04-09 00:00:00 UTC
18	Viernes Santo		Día festivo	2023-04-08 00:00:00 UTC	2023-04-07 00:00:00 UTC	2023-04-08 00:00:00 UTC
39	Jueves Santo		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2023-04-07 00:00:00 UTC	2023-04-06 00:00:00 UTC	2023-04-07 00:00:00 UTC
38	Martes de Carnaval		Día festivo	2023-02-22 00:00:00 UTC	2023-02-21 00:00:00 UTC	2023-02-22 00:00:00 UTC
37	Lunes de Carnaval		Día festivo	2023-02-21 00:00:00 UTC	2023-02-20 00:00:00 UTC	2023-02-21 00:00:00 UTC
29	descanso laboral correspondiente a Día de Año Nuevo		Día festivo	2023-01-03 00:00:00 UTC	2023-01-02 00:00:00 UTC	2023-01-03 00:00:00 UTC
12	Día de Año Nuevo		Día festivo	2023-01-02 00:00:00 UTC	2023-01-01 00:00:00 UTC	2023-01-02 00:00:00 UTC
11	Noche Vieja		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2023-01-01 00:00:00 UTC	2022-12-31 00:00:00 UTC	2023-01-01 00:00:00 UTC
28	Navidad		Día festivo	2022-12-26 00:00:00 UTC	2022-12-25 00:00:00 UTC	2022-12-26 00:00:00 UTC
47	Fundación de Quito		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2022-12-07 00:00:00 UTC	2022-12-06 00:00:00 UTC	2022-12-07 00:00:00 UTC
36	Día de los Muertos		Día festivo	2022-11-05 00:00:00 UTC	2022-11-04 00:00:00 UTC	2022-11-05 00:00:00 UTC
10	Independencia de Cuenca		Día festivo	2022-11-04 00:00:00 UTC	2022-11-03 00:00:00 UTC	2022-11-04 00:00:00 UTC
27	Día de los Muertos		Celebración Para ocultar las celebraciones, ve a Configuración en Google Calendar > Festivos en Ecuador	2022-11-03 00:00:00 UTC	2022-11-02 00:00:00 UTC	2022-11-03 00:00:00 UTC
9	descanso laboral correspondiente a Independencia de Guayaquil		Día festivo	2022-10-11 00:00:00 UTC	2022-10-10 00:00:00 UTC	2022-10-11 00:00:00 UTC
35	Independencia de Guayaquil		Día festivo	2022-10-10 00:00:00 UTC	2022-10-09 00:00:00 UTC	2022-10-10 00:00:00 UTC
46	Feriado del Día de la Independencia		Día festivo	2022-08-13 00:00:00 UTC	2022-08-12 00:00:00 UTC	2022-08-13 00:00:00 UTC

En el Escritorio del ordenador (donde anteriormente habíamos seleccionado que se guarde la información) encontramos la carpeta llamada 5200f803ee2715b3_shell_2022-10-18_10.08.21, si entramos en esta carpeta, encontraremos más información del dispositivo como el informe generado por la herramienta en formatos PDF y Excel. Además, encontramos dos carpetas de interés llamadas data y shared.

Figura 13

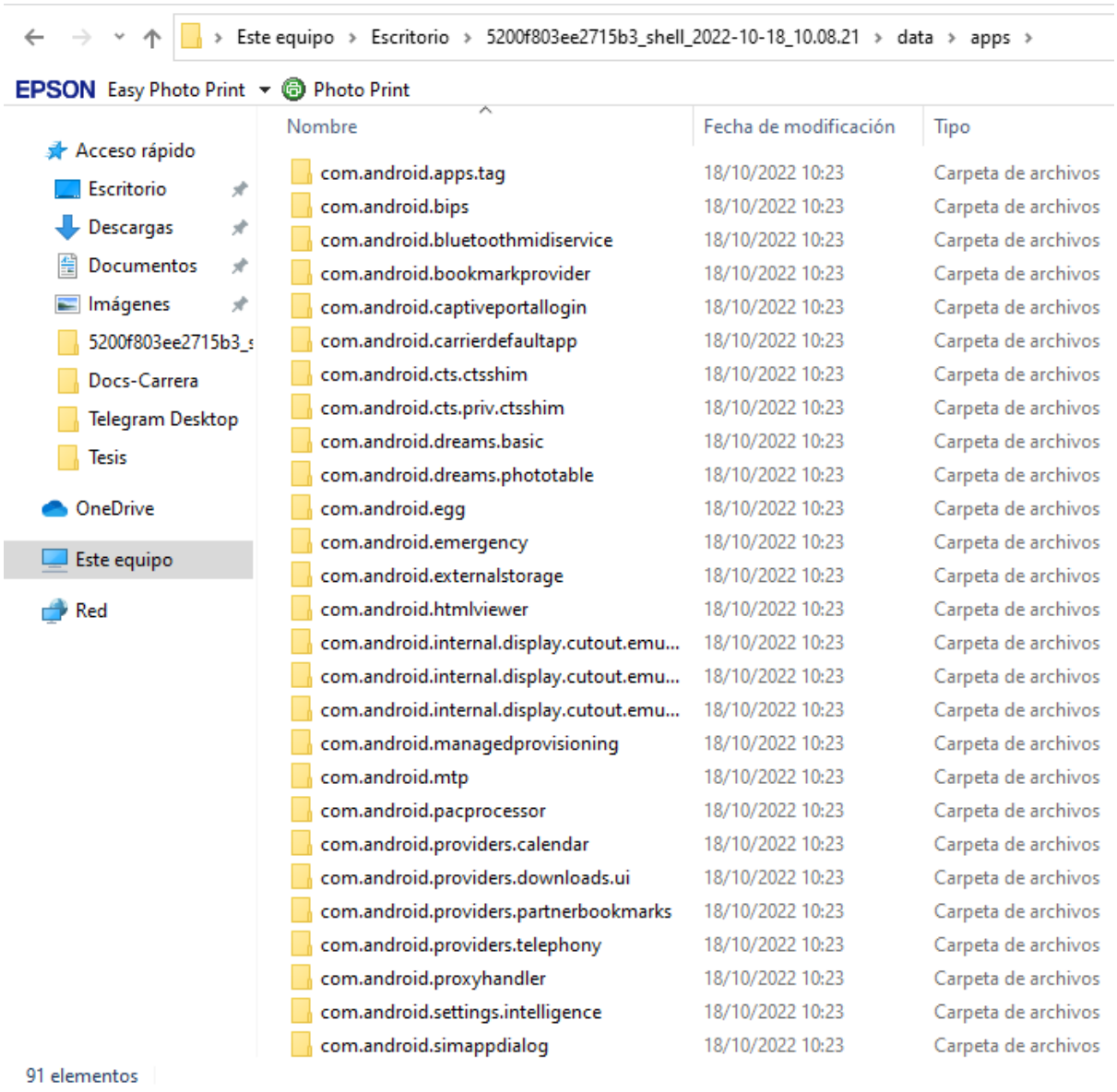
Contenido de carpeta 5200f803ee2715b3_shell_2022-10-18_10.08.21



Si ingresamos a la carpeta data, encontramos información relacionada a las aplicaciones instaladas en el dispositivo.

Figura 14

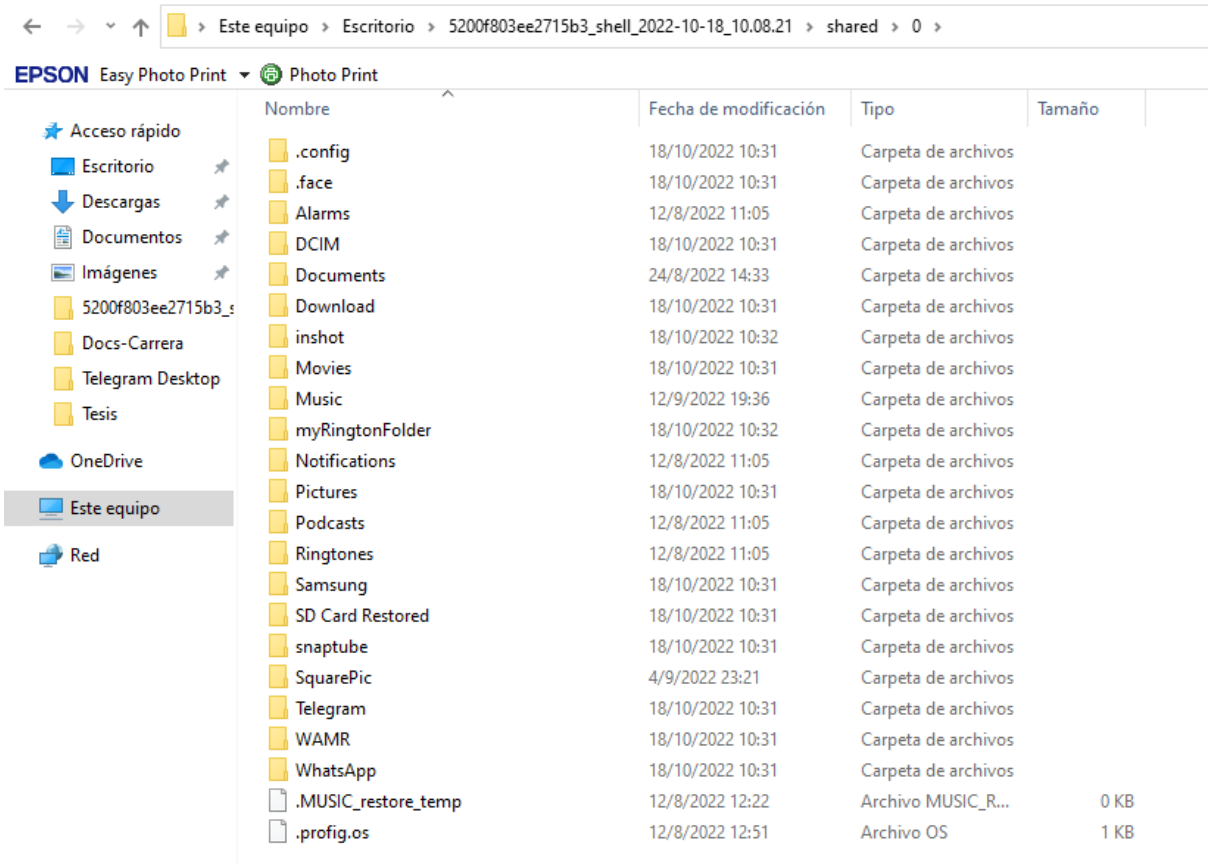
Listado de aplicaciones instaladas en el dispositivo



Por otro lado, en la carpeta shared, podemos observar dos carpetas llamadas 0 y 1, en la carpeta 0 encontraremos todas las carpetas donde se encuentran los archivos que están alojados en la memoria interna del dispositivo.

Figura 15

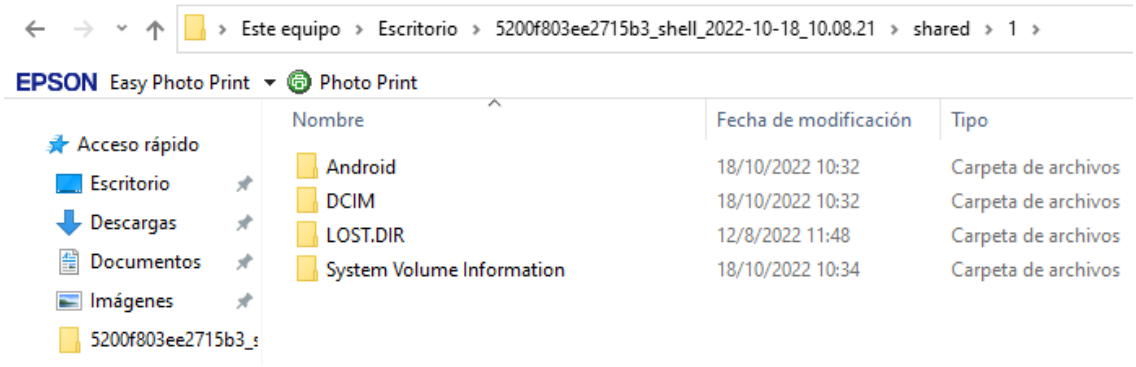
Listado de carpetas donde se encuentran todos los archivos existentes en el dispositivo



En la carpeta 1 se encuentran los archivos pertenecientes a la tarjeta de memoria extraíble (Tarjeta SD) conectada del dispositivo.

Figura 16

Listado de carpetas donde se encuentran todos los archivos pertenecientes a la Tarjeta SD



Nota. Estos archivos serán extraídos por la herramienta siempre y cuando haya una Tarjeta SD conectada al dispositivo.

Andriller es capaz de extraer una gran cantidad de información de un dispositivo móvil, esta herramienta es de gran ayuda al momento de realizar un análisis forense en dispositivo móvil con Android. Los archivos extraídos tales como: fotos, videos, PDF, Word, Excel, chats de WhatsApp, notas de voz, llamadas y mensajes de texto son de vital importancia ya que estos archivos nos servirán de evidencia para poder vincular al criminal con el caso que se esté investigando.

Figura 17

Lista de archivos multimedia del dispositivo

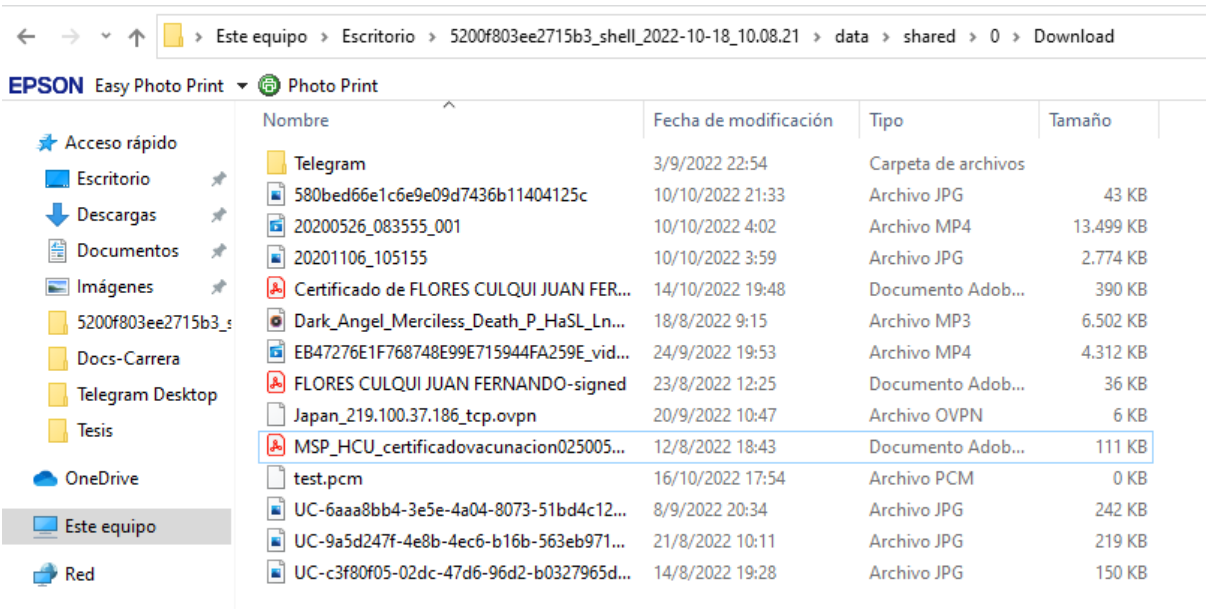
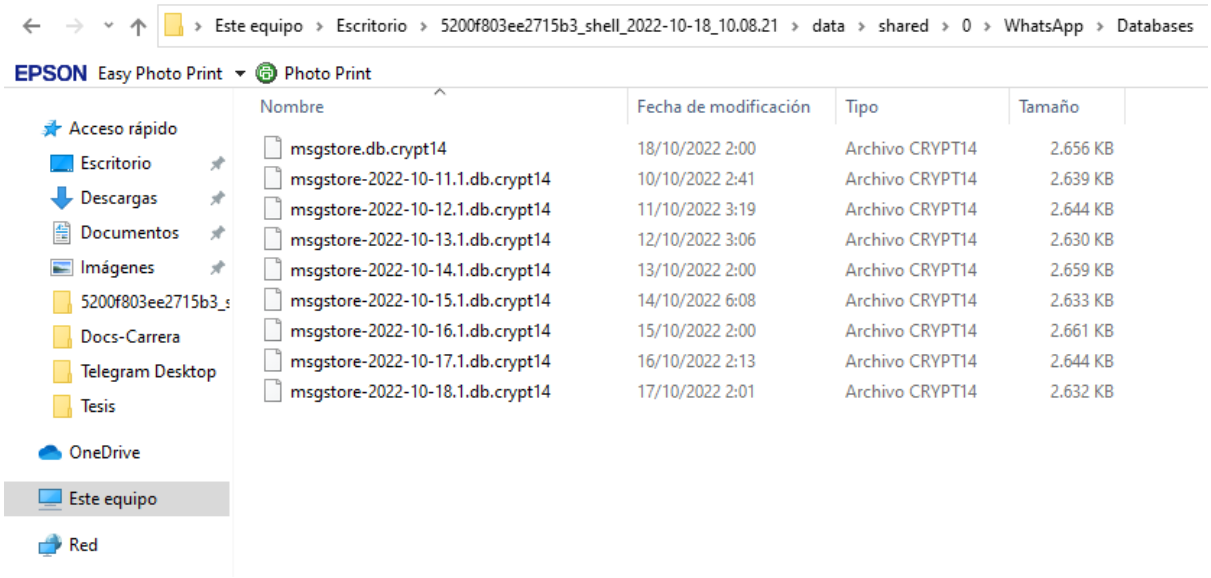


Figura 18

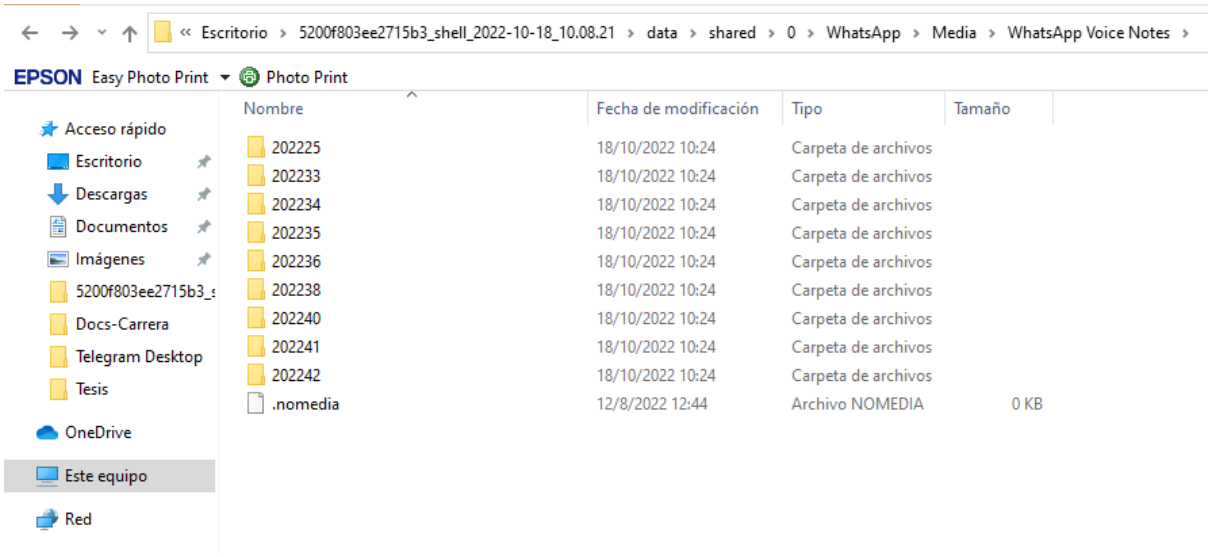
Chats de WhatsApp



Nota. Los chats deben ser desencriptados para poder ver su contenido.

Figura 19

Notas de voz de WhatsApp



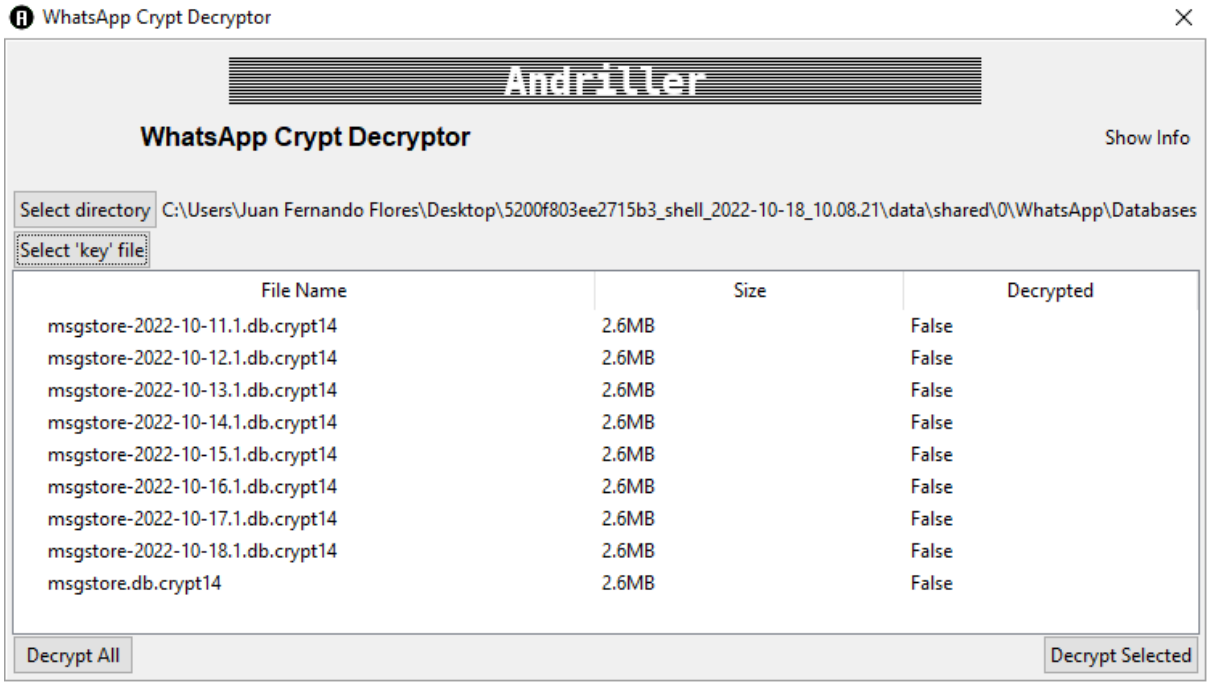
Nota. Las notas de voz de WhatsApp se encuentran organizadas por fechas en sus respectivas carpetas.

Como se mencionaba anteriormente, Andriller cuenta con otra opción de extracción de información, la funcionalidad WhatsApp Crypt nos permitirá desencriptar todos los chats de

esta aplicación de mensajería. Esta opción hace uso de una “Key” que solo podrá ser leía si el dispositivo se encuentre rooteado. Si el dispositivo no está rooteado no se podrá ver esta “Key”.

Figura 20

Interfaz gráfica de WhatsApp Crypt



Cabe señalar que la información extraída de este dispositivo se hizo sin rootearlo para salvaguardar la integridad y seguridad del dispositivo del investigador, ya que el rooteo es procedimiento que compromete mucho al dispositivo teniendo acceso total al SO Android, además de perder la garantía del dispositivo por parte del fabricante y perder actualizaciones de seguridad.

CONCLUSIONES

- Android, como cualquier sistema operativo o cualquier software presenta vulnerabilidades de cualquier tipo, estas se producen por el incremento de usuarios que usan Android, lo que hace que el código abierto del sistema operativo se vea más accesible a los ciberdelincuentes, los cuales mejoran sus estrategias para poder robar información. Además, dichas vulnerabilidades también se producen por culpa del usuario ya que, por la falta de conocimiento que tienen en seguridad, instalan aplicaciones no oficiales o modificadas de fuentes desconocidas, aumentado las vulnerabilidades en el sistema operativo.
- Como resultado del análisis efectuado a las diferentes herramientas y en base a los parámetros establecidos se ha determinado que la herramienta Andriller es la mejor candidata para efectuar los procesos de análisis, debido a que presenta mejores características como; un mínimo requerimientos para su ejecución, es multiplataforma, soporta las diferentes versiones de Android, tiene licencia de uso gratuita y además cuenta con una mayor cantidad de funcionalidades requeridas para el proceso de análisis forense en dispositivos móviles con S.O Android.
- Respecto a la identificación de herramientas se investigó las más empleadas en la actualidad y las que se acoplan a los parámetros establecidos para la realización del estudio comparativo, tomando como característica esencial para su selección su operatividad en dispositivos Android, en consecuencia, se acogieron un total de ocho herramientas para el desarrollo de este trabajo.
- Con la selección de la herramienta se procedió a evaluar la funcionalidad de Andriller, en la cual se ha desarrollado el procedimiento de acceso al dispositivo y a sus datos, la herramienta facilitó la extracción y respaldo para poder

gestionar así su información, al culminar el proceso se genera un archivo en donde se ha almacenado toda la información del dispositivo; contando con archivos de formato multimedia, información y base de datos de las aplicaciones, acceso a información de calendario, entre otros. Estos resultados se muestran almacenados en carpetas con identificación especifica, así como el reporte de extracción que se visualiza en el navegador. Cabe mencionar que el proceso de evaluación se realizó sobre un dispositivo sin rooteo ya que este proceso compromete la integridad, seguridad y garantía del mismo. Por lo tanto, se ha comprobado que las funcionalidades del software cumplen de forma efectiva con su función.

RECOMENDACIONES

- El estudio refleja que Android presente una gran cantidad de vulnerabilidades de todo tipo en los diferentes componentes de sistema operativo desde el año 2020 en adelante. Para poder evitar que estas vulnerabilidades pongan en riesgo nuestra información, se recomienda actualizar siempre el dispositivo, ya que estas actualizaciones vienen con parches de seguridad que corrigen estos errores de seguridad. Además, evitar instalar aplicaciones modificadas o no oficiales, por el hecho de que estas aplicaciones normalmente tienen malware, lo que pone en riesgo nuestra información en Android.
- El estudio ha demostrado que la herramienta seleccionada presenta un alto grado de cumplimiento en referencia a las funcionalidades que presta, destacando la gratuidad de su licencia por lo tanto, se sugiere que la universidad fomente el desarrollo de programas (software) para el análisis forense en dispositivos móviles con la finalidad de poder dotar al país de software gratuito que permita realizar el análisis de dispositivos, permitiendo abaratar los costes en materia de licencias para las instituciones legales de estado apoyando de esta forma al desarrollo de los procesos judiciales del país.
- El estudio reveló que las funciones elementales de la herramienta trabajan de forma eficiente, ante esto señalamos que cuenta con acciones avanzadas que requieren de ciertos procesos informáticos para acceder a los privilegios del dispositivo para su acción. Por lo tanto, se aconseja que, en futuros trabajos enmarcados en el análisis forense a dispositivos móviles, investigar a fondo procesos como el rooteo de celulares y el respaldo de información del mismo, de esta forma se podrá hacer uso de estas funciones como también para las escogidas en este trabajo.

- Si la información extraída por medio de estas herramientas es escasa para poder presentarlo como evidencia durante un proceso judicial, se recomienda utilizar otros métodos de extracción de información para así poder presentar una evidencia digital sólida que permita a las autoridades pertinentes juzgar y dictaminar un veredicto acorde a los delitos informáticos por los cuales se lo acusa.

REFERENCIAS

ADEL – Android Data Extractor Lite – forensic blog. (s.f.). forensic blog. https://forensics.spreitzenbarth.de/adel/

Adeva, R. (11 de marzo de 2022). *Android: qué es, versiones, aplicaciones y cómo saber la versión instalada.* ADSLZone https://www.adslzone.net/reportajes/software/que-es-android/

Adeva, R. (27 de mayo de 2022). *Sistema operativo: qué es, cómo funciona, partes y tipos de SO.* ADSLZone https://www.adslzone.net/reportajes/software/que-es-sistema-operativo/

Aller, Á. (24 de diciembre de 2019). *Dr.fone: conecta tu móvil y gestiónalo en sencillos pasos.* Profesional Review. https://www.profesionalreview.com/2019/12/24/dr-fone/

AMBIT TEAM. (10 de noviembre de 2020). *Tipos de Vulnerabilidades y Amenazas informáticas.* AMBIT - BST. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Android Security. (s.f.). *Android Open Source Project*. https://source.android.com/security

Aumento de privilegios. (s.f.). Ciberseguridad. https://ciberseguridad.com/amenzas/aumento-privilegios/

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics.* NIST Technical Series Publications. http://dx.doi.org/10.6028/NIST.SP.800-101r1

Ben, J. (2022, 01 11*). La mejor alternativa a la recuperación de datos de FonePaw para Android en 2022.* iOS Data https://es.ios-data-recovery.com/fonepaw-android-recovery-alternative/

CÓDIGO INTEGRAL PENAL [COIP]. Ley 0 de 2014. 10 de febrero de 2014 (Ecuador)

Coscollano, C. (13 de marzo de 2019). *El análisis forense en dispositivos móviles - Redseguridad.* Red Seguridad. https://www.redseguridad.com/especialidades-tic/auditoria-e-investigacion/analisis-forense-en-dispositivos-moviles_20190313.html

Costa Silva, L. A. (2019). *HERRAMIENTAS DE ANÁLISIS FORENSE PARA ANDROID.* [TRABAJO DE FIN DE MÁSTER, UNIVERSIDAD DE JAÉN] https://tauja.ujaen.es/bitstream/10953.1/11909/1/TFM_LuizaAraujoCostaSilva_vf.pdf

Editorial Etecé. (29 de septiembre de 2020). *Método Inductivo.* Concepto. https://concepto.de/metodo-inductivo/

Elaine. (16 de mayo de 2018). *Objetivos de la informática forense.* OnRetrieval. https://onretrieval.com/objetivos-de-la-informatica-forense/

Ezequiel. (23 de junio de 2019). *Qué son las Ciencias Forenses y cuáles son las principales ramas.* Indubitado. https://indubitado.catedrauno.com/2019/que-son-las-ciencias-forenses-y-cuales-son-las-principales-ramas/

Fiscalía General del Estado. (2014, 09 9). *Area de Cadena de Custodia.* Fiscalía General del Estado. https://www.fiscalia.gob.ec/area-de-cadena-de-custodia/

González, D. (20 de septiembre de 2021). *¿Qué es la informática forense?* Imagar. https://www.imagar.com/blog-desarrollo-web/que-es-la-informatica-forense/

LIMPIATUWEB. (s.f.). *Ejecución de código remoto: Guía completa sobre este tipo de infección* | LimpiatuWeb.com. Desinfectamos tu página web de virus y malware. https://limpiatuweb.com/blog/ejecucion-codigo-remoto/

Marker, G. (s.f.). *Todo sobre Vulnerabilidades informáticas: Cómo protegerse*. Tecnología + Informática. Retrieved Junio 12, 2022, from https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

Medina Gómez, D. A., & Hernández Bejarano, M. (31 de diciembre de 2020). *Análisis forense para Móviles.* https://www.fundacionavenir.net/revista/index.php/avenir/article/view/105/57

Microsoft. (2022, 06 23*). Divulgación de información* - WCF. Microsoft Docs. https://docs.microsoft.com/es-es/dotnet/framework/wcf/feature-details/information-disclosure

OXYGEN FORENSICS. (s.f.*). Mobile forensic solutions: software and hardware.* Oxygen Forensics - Mobile forensic solutions: software and hardware. https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective

Rodríguez, O. H. (2015). ESTUDIO DE METODOLOGÍAS DE ANÁLISIS FORENSE ANTE INCIDENTES DE CIBERSEGURIDAD [TRABAJO DE FIN MÁSTER, UNIVERSIDAD POLITÉCNICA DE MADRID]. https://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Oscar_Rodriguez_Munoz_2015.pdf

Sacco, L. (24 de marzo de 2021). *▷ Mi Arsenal De Software: Andriller V3.5.3* | PERITOS INFORMATICOS | 2022. Perito Informático. https://peritosinformaticos.ar/andriller-2022/

Sanchis, E. (1 de octubre de 2018*). ¿Qué es el análisis forense digital? | Informático Forense.* Peritos Informaticos. https://peritos-informaticos.com/que-es-analisis-forense-digital

Sanchis, E. (1 de octubre de 2018). *Qué son las evidencias digitales y cómo se obtienen.* Peritos Informaticos. https://peritos-informaticos.com/que-son-las-evidencias-digitales

Shum, Y. M. (4 de marzo de 2020). *Situación Global Mobile 2020 - 5.190 millones de usuarios únicos.* Yi Min Shum Xie. https://yiminshum.com/mobile-movil-app-2020/

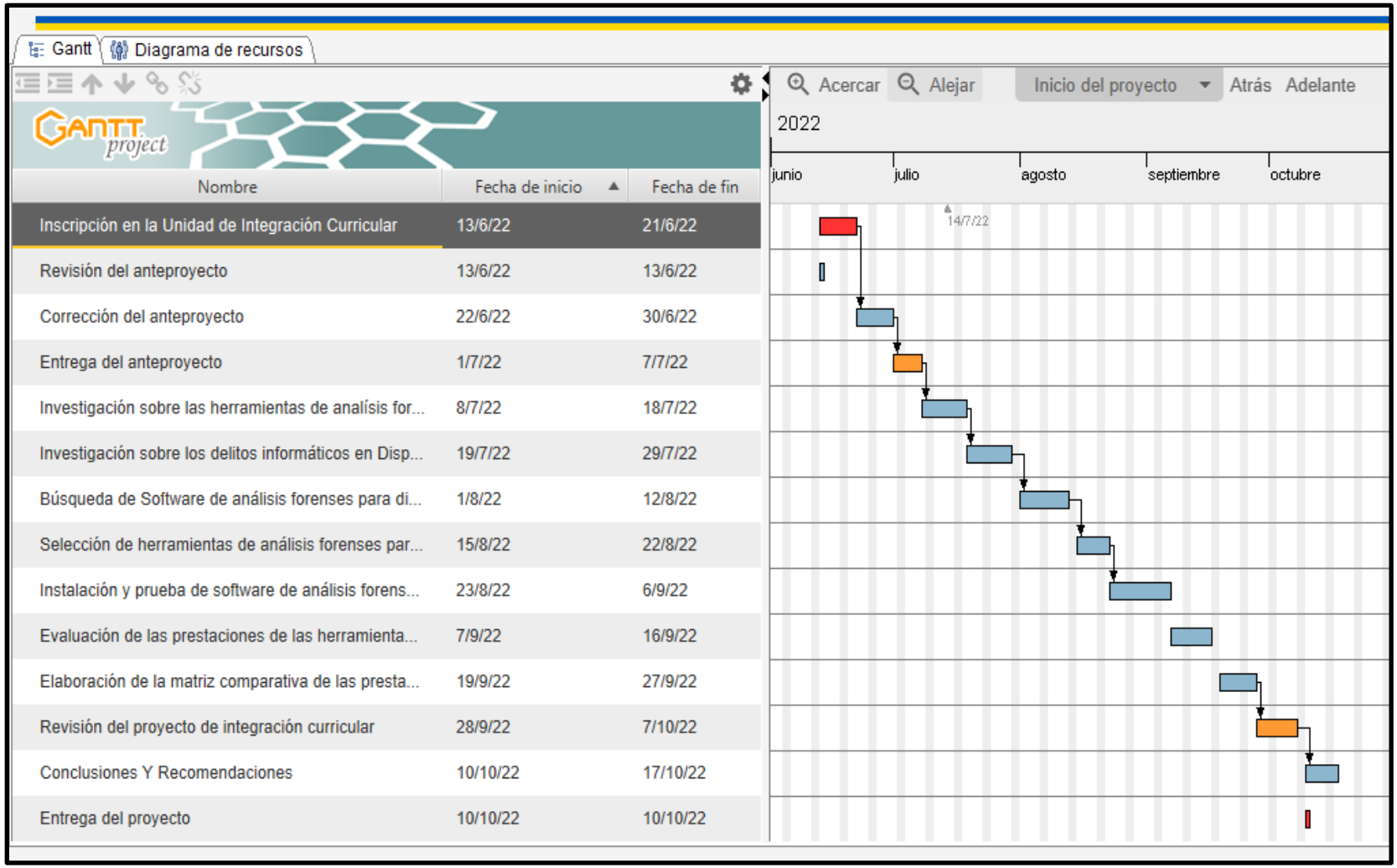
UNIR. (24 de junio de 2021). *Informática Forense: en qué consiste y ejemplos de aplicación.* UNIR. https://www.unir.net/ingenieria/revista/informatica-forense/

Universidad Latina. (14 de diciembre de 2021). *¡Descubre qué son las Ciencias Forenses! UNILA.* Unila. https://www.unila.edu.mx/que-son-ciencias-forenses/

Velasco, R. (15 de octubre de 2017). *Androl4b, una máquina virtual para análisis forense de apps de Android.* Redes Zone. https://www.redeszone.net/2017/10/15/androl4b-analisis-forense-android/

ANEXOS

Cronograma (Gantt)



Nombre	Fecha de inicio	Fecha de fin
Inscripción en la Unidad de Integración Curricular	13/6/22	21/6/22
Revisión del anteproyecto	13/6/22	13/6/22
Corrección del anteproyecto	22/6/22	30/6/22
Entrega del anteproyecto	1/7/22	7/7/22
Investigación sobre las herramientas de analísis for...	8/7/22	18/7/22
Investigación sobre los delitos informáticos en Disp...	19/7/22	29/7/22
Búsqueda de Software de análisis forenses para di...	1/8/22	12/8/22
Selección de herramientas de análisis forenses par...	15/8/22	22/8/22
Instalación y prueba de software de análisis forens...	23/8/22	6/9/22
Evaluación de las prestaciones de las herramienta...	7/9/22	16/9/22
Elaboración de la matriz comparativa de las presta...	19/9/22	27/9/22
Revisión del proyecto de integración curricular	28/9/22	7/10/22
Conclusiones Y Recomendaciones	10/10/22	17/10/22
Entrega del proyecto	10/10/22	10/10/22

Untitled Gantt Project

1 jul. 2022

2

Tarea

Nombre	Fecha de inicio	Fecha de fin
Inscripción en la Unidad de Integración Curricular	13/6/22	21/6/22
Revisión del anteproyecto	13/6/22	13/6/22
Corrección del anteproyecto	22/6/22	30/6/22
Entrega del anteproyecto	1/7/22	7/7/22
Investigación sobre las herramientas de analísis forenses	8/7/22	18/7/22
Investigación sobre los delitos informáticos en Dispositivos Móviles	19/7/22	29/7/22
Búsqueda de Software de análisis forenses para dispositivos móviles (libres y privativos)	1/8/22	12/8/22
Selección de herramientas de análisis forenses para dispositivos móviles (libres y privativos)	15/8/22	22/8/22
Instalación y prueba de software de análisis forenses (herramientas seleccionadas)	23/8/22	6/9/22
Evaluación de las prestaciones de las herramientas (libres y privativas)	7/9/22	16/9/22
Elaboración de la matriz comparativa de las prestaciones y utilidades de las herramientas seleccionadas	19/9/22	27/9/22
Conclusiones Y Recomendaciones	10/10/22	17/10/22
Revisión del proyecto de integración curricular	28/9/22	7/10/22
Entrega del proyecto	10/10/22	10/10/22

Presupuesto Ejecutado

RECURSO	CANTIDAD	COSTO	TOTAL
RERSONAL (HUMANO)	2	$0.00	$0.00
PC PORTATIL	2	$0.00	$0.00
SMARTPHONE	1	$0.00	$0.00
PAQUETE OFFICE	2	$69.00	$138.00
IMPRESORA	1	$350.00	$350.00
RESMA DE PAPEL	2	$4.00	$8.00
INTERNET	MENSUAL (POR 6 MESES)	$20.00	$120.00
ELECTRICIDAD	MENSUAL (POR 6 MESES)	$30.00	$180.00
PRESUPUESTO TOTAL			$796.00

ING. DANILO GEOVANNY BARRRENO NARANJO, EN CALIDAD DE DIRECTOR(A) DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**Evaluación de herramientas para el Análisis Forense en Dispositivos Móviles bajo Android, año 2022**", presentado por Alexis Ronaldo Cueva Cando y Juan Fernando Flores Culqui estudiantes de la **carrea de Software** pasó el análisis de coincidencia no accidental en la herramienta URKUND, reflejando un **porcentaje de similitud del 7%**, como se puede evidenciar en el documento adjunto.

Guaranda, 27 de Febrero 2023

Atentamente,

Ing. Danilo Geovanny Barreno Naranjo
Director

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

Ouriginal by Turnitin

Document Information

Analyzed document	Tesis-final.pdf (D159371048)
Submitted	2/24/2023 2:22:00 AM
Submitted by	
Submitter email	juaflores@mailes.ueb.edu.ec
Similarity	7%
Analysis address	dbarreno.ueb@analysis.urkund.com

Sources included in the report

Entire Document

Hit and source - focused comparison, Side by Side

Submitted text	As student entered the text in the submitted document.
Matching text	As the text appears in the source.

Ficha de observación

Facultad de Ciencias Administrativas, Gestión Empresarial e Informática.

Carrera de Software.

Ficha de Observación	
Nombre de la Herramienta:	
Objetivo de la Ficha: Determinar cuáles son los requerimientos del sistema, características y funciones soportadas de la herramienta forense.	
Requisitos del Sistema	
Sistema Operacional	
Requerimientos mínimos	

Características Especiales	
Coste	
Versión de Android	

Funcionalidades Soportadas	
Recuperación de informaciones del dispositivo	
Recuperación de llamadas	
Recuperación de contactos	
Recuperación de entradas de calendario	
Recuperación de mensajes (SMS y MMS)	

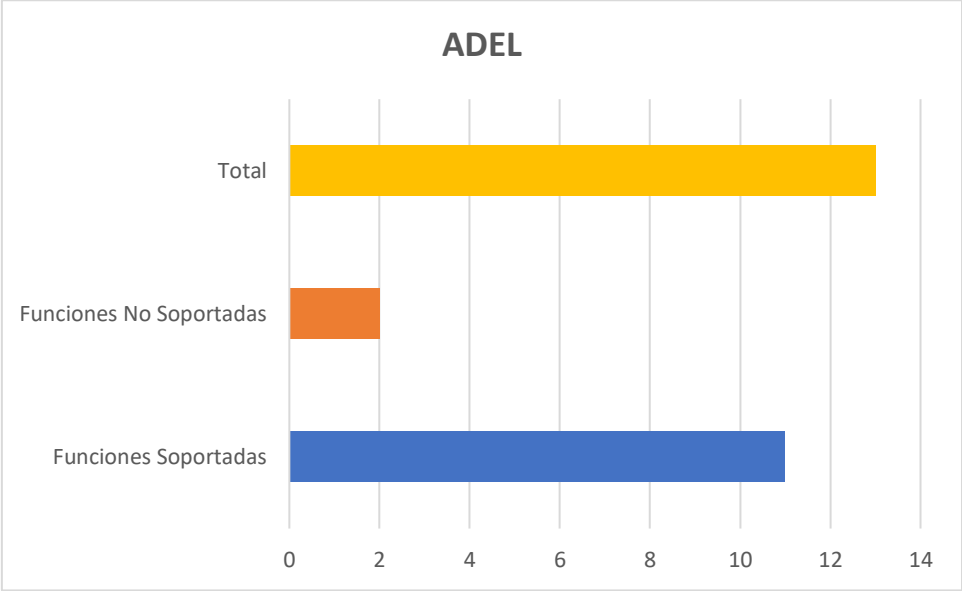
Recuperación de correo	
Recuperación de archivos multimedia	
Recuperación de ubicación GPS	
Recuperación de datos borrados	
Recuperación de datos de conexión	
Preservación de datos	
Informe de datos recuperados	
Personalización de informes	

Procesamiento y análisis de la información

En el siguiente apartado se presentan los resultados obtenidos de la aplicación de la ficha de observación a cada herramienta de análisis forense para el Sistema Operativo Android. Para lo siguiente se ha hecho uso del paquete de software de Office Excel, de tal manera que se representan los resultados de mediate tablas y gráficos de tipo (barra) respectivamente.

1. **ADEL**

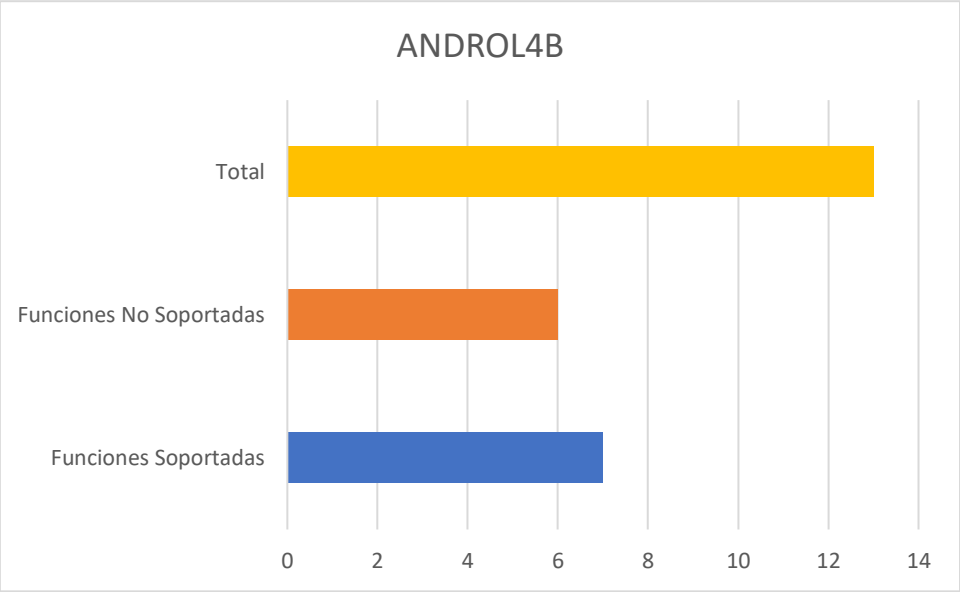
OPCIONES	FRECUENCIA
Funciones Soportadas	11
Funciones No Soportadas	2
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 11 funcionalidades soportadas, así mismo las 2 restantes que representan: función de recuperación de datos de conexión y personalización de informes no están soportadas por la herramienta.

2. ANDROL4B

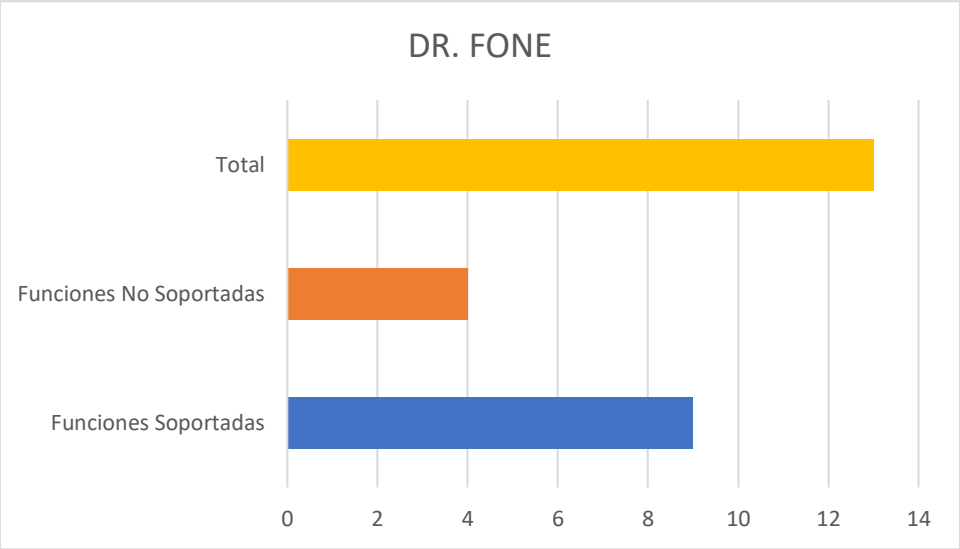
OPCIONES	FRECUENCIA
Funciones Soportadas	7
Funciones No Soportadas	6
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 7 funcionalidades soportadas, así mismo los 6 restantes que representan: recuperación de ubicación GPS, recuperación de datos borrados, recuperación de datos de conexión, preservación de datos, informe de datos recuperados y personalización de informes no están soportadas por la herramienta.

3. DR. FONE

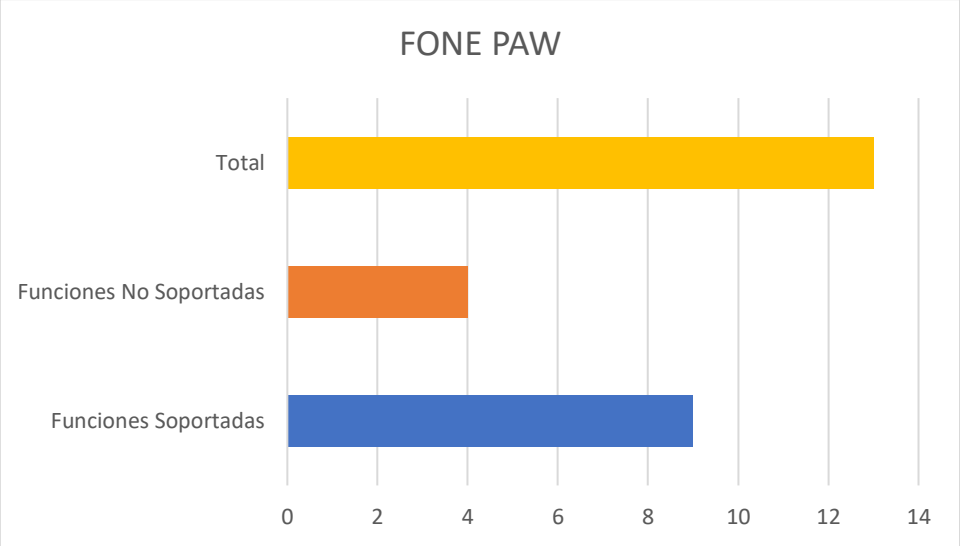
OPCIONES	FRECUENCIA
Funciones Soportadas	9
Funciones No Soportadas	4
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 9 funcionalidades soportadas, así mismo los 4 restantes que representan: recuperación de ubicación GPS, recuperación de datos de conexión, preservación de datos y personalización de informes no son soportadas por la herramienta.

4. FONE PAW

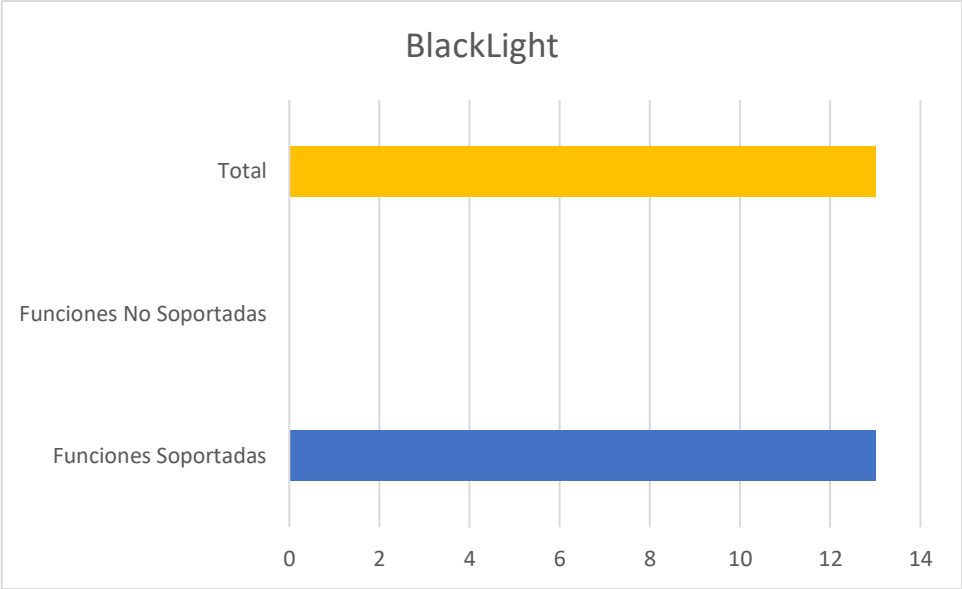
OPCIONES	FRECUENCIA
Funciones Soportadas	9
Funciones No Soportadas	4
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 9 funcionalidades soportadas, así mismo los 4 restantes que representan: recuperación de ubicación GPS, recuperación de datos de conexión, preservación de datos y personalización de informes no son soportadas por la herramienta.

5. BLACKLIGHT

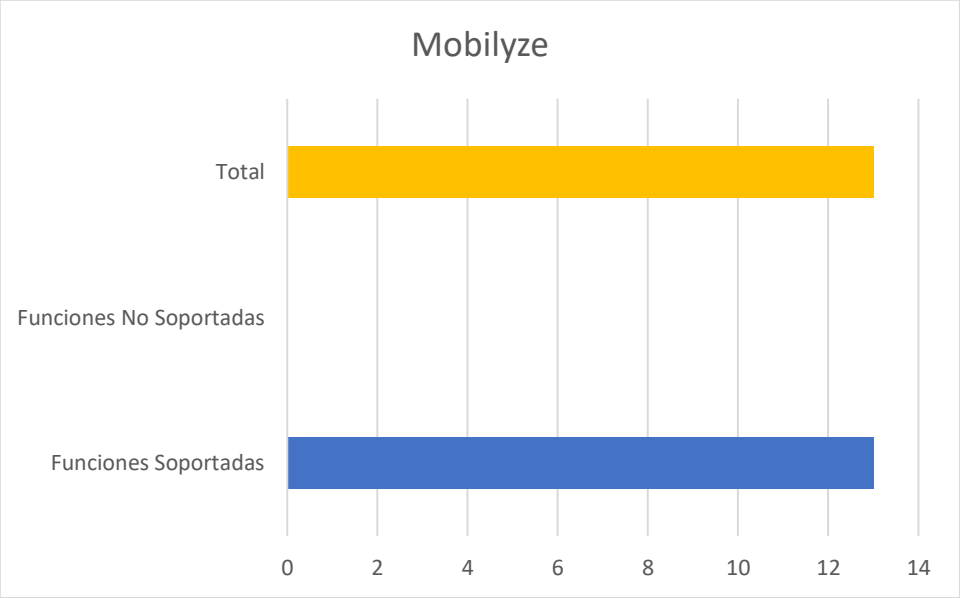
OPCIONES	FRECUENCIA
Funciones Soportadas	13
Funciones No Soportadas	0
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 13 funcionalidades soportadas.

6. MOBILYZE

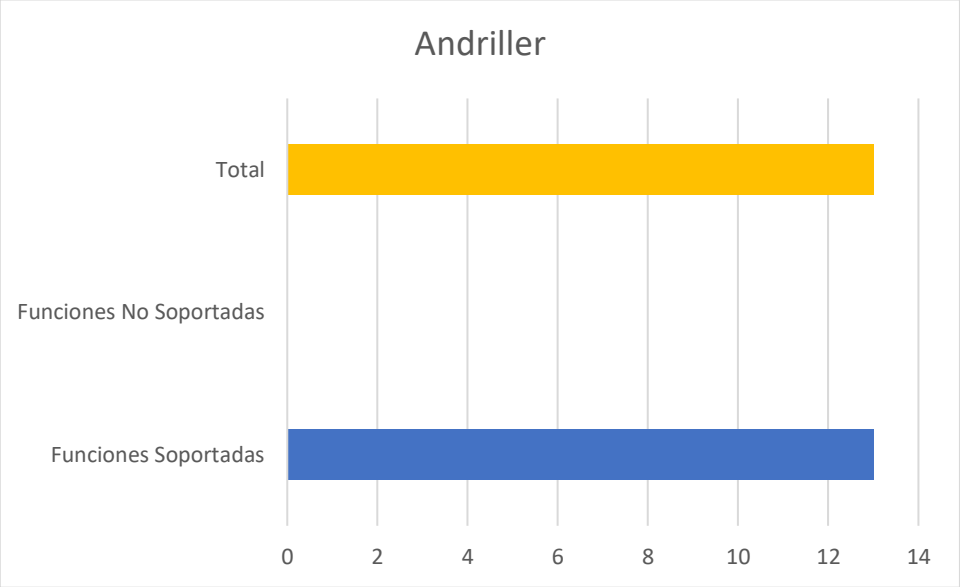
OPCIONES	FRECUENCIA
Funciones Soportadas	13
Funciones No Soportadas	0
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 13 funcionalidades soportadas.

7. ANDRILLER

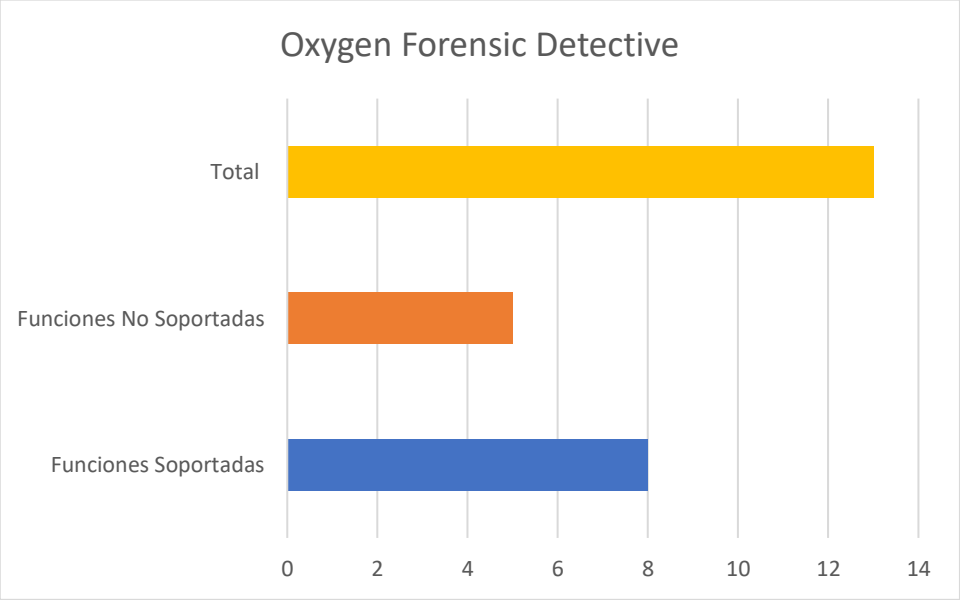
OPCIONES	FRECUENCIA
Funciones Soportadas	13
Funciones No Soportadas	0
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 13 funcionalidades soportadas.

8. OXYGEN FORENSIC DETECTIVE

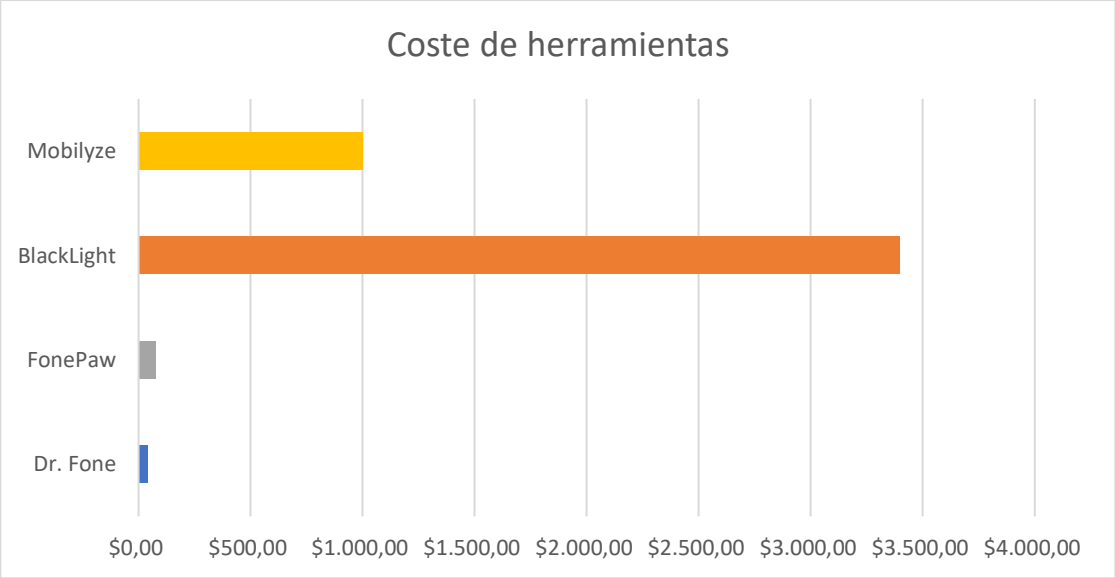
OPCIONES	FRECUENCIA
Funciones Soportadas	8
Funciones No Soportadas	5
Total	13



Interpretación: Respecto a la representación del gráfico se puede apreciar que la herramienta cuenta con un total de 8 funcionalidades soportadas, así mismo los 5 restantes que representan: recuperación de informaciones del dispositivo, recuperación de llamadas, recuperación de contactos, recuperación de datos de conexión y personalización de informes no son soportadas por la herramienta.

9. SECCIÓN DE COSTES

OPCIONES	COSTE
Dr. Fone	$39,95
FonePaw	$76,90
BlackLight	$3.400,00
Mobilyze	$1.000,00



Interpretación: Respecto a la representación del gráfico se puede apreciar que 4 de las ocho herramientas tienen un costo total por concepto de uso de licencias así tenemos: Dr. Fone con un valor de $39, 95 dólares, Fone Paw con un valor de $76,90 dólares, BlackLight con un valor de $3.400,00 dólares y Mobilyze con un valor de $1.000,00 dólares.