

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL

**TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO
REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR
EN REDES Y TELECOMUNICACIONES**

ANTHONY ALEXANDER GUZMÁN MOLINA

anthony.guzman@epn.edu.ec

DIRECTOR: GABRIELA KATHERINE CEVALLOS SALAZAR

gabriela.cevalloss@epn.edu.ec

DMQ, febrero 2023

CERTIFICACIONES

Yo, Anthony Alexander Guzmán Molina declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.



ANTHONY ALEXANDER GUZMAN MOLINA

anthony.guzman@epn.edu.ec

anthoguz_219@outlook.es

Certifico que el presente trabajo de integración curricular fue desarrollado por Anthony Alexander Guzmán Molina, bajo mi supervisión.



GABRIELA KATHERINE CEVALLOS SALAZAR

DIRECTOR

gabriela.cevalloss@epn.edu.ec

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

Anthony Alexander Guzmán Molina

DEDICATORIA

Dedico este trabajo a todas esas personas que estuvieron acompañándome durante mi formación académica contribuyendo a mi crecimiento tanto personal como profesional.

Anthony Alexander Guzmán Molina

AGRADECIMIENTO

Primero agradezco a Dios por haber guiado mis pasos en todo momento.

A mis hermanos Gabriel, Johana, Daniel y Kelli por todo el apoyo que me han brindado a lo largo de mi preparación profesional.

A mi madre Susana, que de una u otra manera siempre estuvo ahí para mí.

A mi abuelito Manuel, por siempre formar parte de mi vida y enseñarme tanto.

A todos los amigos que estuvieron ahí para animarme cuando fue necesario, en especial a Joan y Henry.

A C.S por ser haber sido mi motivo para ser mejor.

A mí mismo por nunca haberme rendido.

A la Universidad por otorgarme los medios y las vivencias para conseguir mis metas.

Anthony Alexander Guzmán Molina

ÍNDICE DE CONTENIDOS

CERTIFICACIONES	I
DECLARACIÓN DE AUTORÍA.....	II
DEDICATORIA	III
AGRADECIMIENTO	IV
ÍNDICE DE CONTENIDOS.....	V
RESUMEN	VII
<i>ABSTRACT</i>	VIII
1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO	9
1.1 Objetivo general.....	9
1.2 Objetivos específicos.....	9
1.3 Alcance	9
1.4 Marco Teórico	9
Delitos informáticos en el Ecuador	9
Procedimiento para resolver o denunciar delitos informáticos	11
Validez legal de las evidencias	12
2 METODOLOGÍA.....	14
3 RESULTADOS	14
3.1 Investigación de normativas para la recopilación de evidencia digital	15
ISO/IEC 27037:2012	15
RFC 3227	16
UNE 71505.....	16
UNE 71506:2013.....	17
ISO/IEC 30121	18
Normativa local para la extracción de evidencia digital	18
3.2 Análisis de las metodologías de extracción de evidencia digital	18
Argentina (ISO 27037)	18
ISO/IEC 27037:2012	21

UNE 71506:2013.....	22
Cadena de custodia establecida por la Fiscalía General del Estado	26
Metodologías a nivel local.....	27
3.3 Herramientas de <i>software</i> para la extracción de evidencia digital	30
<i>FTK Imager</i>	30
<i>AUTOPSY</i>	31
Recuva	32
<i>DiskDigger</i>	33
<i>Oxygen Forensic</i>	34
<i>Magnet RAM Capture</i>	35
Andriller	35
3.4 Implementación de herramientas para la extracción de evidencias digitales	36
<i>Magnet RAM Capture</i>	39
<i>FTK Imager</i>	41
<i>AUTOPSY</i>	44
<i>DiskDigger</i>	46
Andriller	49
4 CONCLUSIONES.....	50
5 RECOMENDACIONES	52
6 REFERENCIAS BIBLIOGRÁFICAS	53
7 ANEXOS.....	i
ANEXO I: Certificado de Originalidad	i
ANEXO II: Enlaces	ii

RESUMEN

Los avances tecnológicos han traído consigo una adopción acelerada de las Tecnologías de la información, y esto a su vez ha desatado el aumento de los delitos informáticos, entre los cuales se encuentran el fraude, el lavado de dinero, el robo de información entre otros. En este panorama se hace necesaria la existencia de guías metodológicas, que proporcionen a los agentes policiales la capacidad de enfrentar esta problemática utilizando evidencias contundentes con base legal.

El Ecuador no se ha visto exento de esta realidad, por lo cual en el presente trabajo de integración curricular se investiga acerca de normativa internacional para el manejo de evidencia digital: ISO 27037, RFC 3227, UNE 71505. Además, se investiga a nivel local la existencia de normativa.

A partir de esto se analizan metodologías empleadas por otros países y a nivel local, para la extracción de evidencia digital, presentando aquellas que han logrado ser adoptadas por diferentes países o también las que se plantean con ese objetivo.

Un aspecto importante para considerar son las herramientas que permiten obtener dichas evidencias, para ello se ha realizado el análisis de estas considerando su costo, ventajas y desventajas. Para observar su funcionamiento se han implementado dentro de un escenario apegado a la realidad.

PALABRAS CLAVE: Evidencia Digital, Normativa Digital, Guía Metodológica, Análisis forense, Herramientas de extracción forense.

ABSTRACT

Technological advances have brought with them an accelerated adoption of Information Technologies, and this in turn has unleashed the increase in computer crimes, among which are fraud, money laundering, information theft, among others. In this scenario, it is necessary to have methodological guides that provide police officers with the ability to deal with this problem using compelling evidence with a legal basis.

Ecuador has not been exempt from this reality, which is why in the present work on curricular integration, international regulations for the management of digital evidence are being investigated: ISO 27037, RFC 3227, UNE 71505. In addition, the existence of regulations is being investigated at the local level.

Based on this, methodologies used by other countries and at the local level are analyzed for the extraction of digital evidence, presenting those that have been adopted by different countries or also those that are proposed with that objective.

An important aspect to consider are the tools that allow obtaining such evidence, for which the analysis of various tools has been carried out considering their cost, advantages and disadvantages. To observe its operation, they have been implemented within a scenario attached to reality.

KEYWORDS: *Digital Evidence, Digital Regulations, Methodological Guide, Forensic Analysis, Forensic Extraction Tools.*

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

El presente proyecto realiza un análisis de normativas que tienen por objetivo el manejo adecuado de la evidencia digital, siendo este procedimiento muy importante para recopilar evidencias que tengan una validez legal y técnica para investigaciones de delitos informáticos. Se pretende investigar acerca de herramientas de extracción de evidencia digital, sus ventajas y desventajas, su funcionamiento y la forma de emplearlas.

1.1 Objetivo general

Implementar herramientas para la extracción de evidencia digital.

1.2 Objetivos específicos

- Investigar normativas para la recopilación de evidencia digital.
- Analizar metodologías de extracción de evidencia digital.
- Analizar *software* para la extracción de evidencia digital.
- Implementar las herramientas.

1.3 Alcance

El presente proyecto conlleva el análisis de normativa nacional e internacional que aborde el manejo de evidencia digital, además de metodologías para el adecuado tratamiento y extracción de esta. Se analizarán herramientas que permitan extraer las evidencias, destacando sus características, costo, ventajas y desventajas; para proceder a implementar, al menos cuatro herramientas, observando su funcionamiento y resultados.

1.4 Marco Teórico

Delitos informáticos en el Ecuador

Los delitos informáticos o cibernéticos en el país han aumentado de manera progresiva gracias a la inmensa acogida tecnológica que se ha producido en los últimos años, se estima que al menos un 79.21% de la ciudadanía ecuatoriana cuenta con acceso al Internet. Debido a esto el informe estadístico publicado por la Unidad de Ciberdelitos de la Policía muestra que a partir del año 2020 hasta 2022 se han registrado 3183 delitos cibernéticos; tan solo en los primeros seis meses de 2022 se estiman alrededor de 650

delitos correspondientes al ámbito informático, siendo las principales provincias afectadas Guayas, Manabí, Pichincha, Imbabura, Azuay y Carchi [1].

Los delitos informáticos más frecuentes en el país registrados desde 2017 a 2021 son [2]:

- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones con un total de 1.265 casos.
- Estafa con un total de 79.784 casos.
- Apropiación fraudulenta por medios electrónicos con un total de 10.393 casos.
- Violación de la intimidad con un total de 9.091 casos.

A continuación, se presentan incidentes informáticos que afectaron a diferentes instituciones en el país, en cada suceso fue relevante el trabajo de un peritaje informático, estableciendo metodologías de extracción de evidencias que garanticen la integridad de la misma ante un tribunal.

Ataque informático en la Asamblea Nacional

El ataque tuvo suceso el 28 de junio de 2022 durante la noche y se produjo en la votación por parte de la Asamblea Nacional para decidir la destitución del Presidente de la República. En dicho ataque los delincuentes accedieron de manera remota a los equipos informáticos de al menos cuatro asambleístas con el objetivo de manipular la votación en curso, haciendo que los votos sean afirmativos. A pesar de las múltiples afirmaciones referentes a la calidad del sistema de seguridad, el presidente de la Asamblea Nacional presentó el caso en la Fiscalía; en la pericia se plantea realizar el análisis de vulneración informático, virus, puertos, entre otros [3].

Una vez realizado el peritaje en los computadores o curules de cuatro asambleístas, específicamente en el registro de conexiones remotas del *software Anydesk*, el informe técnico determinó la intromisión externa de una única IP que conocía los datos de acceso de los asambleístas para acceder al sistema, por lo cual se asume que las credenciales de los legisladores fueron obtenidas mediante el uso de ingeniería social u otros medios [3].

Banco del Austro contra Wells Fargo Bank

En enero de 2015 atacantes lograron robar alrededor 12 millones de dólares del Banco del Austro, esto gracias a que lograron obtener las credenciales de la Sociedad para las Comunicaciones Financieras Interbancarias Internacionales (SWIFT) de uno de los

empleados de la institución bancaria ecuatoriana. La demanda presentada por el Banco del Austro alega que la institución Wells Fargo no pudo detectar las transferencias no autorizadas antes de ser enviadas al resto de bancos, afirmando que utilizando *malware* los atacantes lograron ingresar de manera remota a sus equipos para realizar las transacciones fraudulentas. La institución bancaria logró recuperar alrededor de 2.8 millones mientras inicia procesos legales en Hong Kong con el objetivo de recuperar el dinero restante [4].

Ataque interno al sistema informático del Consejo de la Judicatura

Se estima que desde el año 2020 a 2021 una red interna se encargaba de acceder, de manera no autorizada, al sistema informático de la Judicatura para elegir a los jueces seleccionados durante los sorteos de la institución; en esta red delictiva se encontraban tanto jueces, funcionarios y abogados. Durante el peritaje informático a la evidencia encontrada en la residencia y despacho del juez del Tribunal Contencioso Tributario de Guayaquil se confirmó la implicación de este en el delito. Por otra parte, un análisis realizado a los sistemas informáticos de la institución confirmó que el sistema no ha vuelto a ser vulnerado desde el año 2021, año donde también se realizaron denuncias a causa de manipulación en los sorteos [5].

Procedimiento para resolver o denunciar delitos informáticos

Los delitos informáticos se encuentran establecidos en el Ecuador dentro de la normativa vigente en la Ley de mensajes de datos y firmas electrónicas del año 2002, en donde se regula por primera vez en Ecuador los delitos informáticos. Posteriormente se regula la Ley de Comercio Electrónico y el Código Orgánico Integral Penal (COIP), tipificando los delitos informáticos como tal, la Corte Nacional de Justicia no define un procedimiento específico para el tratamiento de los delitos informáticos en el Ecuador [6].

Denuncia de los delitos informáticos

Las denuncias de delitos informáticos se realizan en los Servicios de Atención Ciudadana de la Fiscalía, los cuales se encuentran repartidos por todo el país, tan solo en Pichincha existen alrededor de 21 establecimientos. La Fiscalía del Estado también proporciona el servicio denominado Atención integral de recepción de denuncias de presuntos hechos delictivos también conocido como SAI, actualmente existen ocho puntos de atención Integral en Quito. Por otra parte, las denuncias también pueden ser receptadas en las oficinas de las Unidades de Policía Comunitaria, así como en la Policía Judicial [7].

Se debe considerar que desde el año 2011 existe en el Ecuador departamentos especializados en ciberdelitos, uno de ellos es la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador la cual entro en funcionamiento en el año 2012, con su sede en Pichincha, se encarga de delitos en los cuales se presente el uso de las tecnologías de la información. Esta unidad fue creada bajo el nombre de Unidad de Investigación de Delitos Tecnológicos en el año 2011 para de manera posterior cambiar su nombre y trabajar en conjunto con el resto de los departamentos de la Policía Nacional del Ecuador [8].

Consideraciones para poder realizar una denuncia por delitos informáticos:

- El denunciante requiere portar la cédula de identidad para poder presentar la denuncia.
- No se requiere contar con un representante legal como por ejemplo un abogado.
- El trámite se realiza de manera gratuita.

También existe el servicio online proporcionado por la Fiscalía de Pichincha para la recepción de denuncias de robo y hurto en línea, aun así, es necesario recalcar que no contienen un apartado específico para los ciberdelitos.

Validez legal de las evidencias

Las evidencias digitales son aquellos datos o información que se han almacenado en formato digital y que pueden ser utilizados como prueba en un procedimiento legal. Las evidencias digitales pueden incluir correos electrónicos, mensajes de texto, imágenes, videos, documentos de texto, registros de transacciones en línea y otros tipos de datos que se han almacenado en formatos digitales [9].

La evidencia digital debe cumplir con ciertos criterios para mantener una validez legal. En general, estos criterios incluyen [10]:

- Autenticidad: La evidencia digital debe ser auténtica, es decir, debe ser posible determinar de manera confiable que la evidencia proviene de la fuente que se afirma que proviene.
- Integridad: La evidencia digital debe mantenerse en su forma original y no debe haber sido alterada de ninguna manera, para lo cual debe mantenerse una cadena de custodia.
- Confiabilidad: La evidencia digital debe ser confiable y debe poder ser verificada de manera confiable.
- Relevancia: La evidencia digital debe ser relevante para el asunto en cuestión.

- Documentación: Las evidencias deben mantener una documentación escrita de todos los procedimientos a los cuales han sido sometidas.

La cadena de custodia se refiere al registro de todos los movimientos de una evidencia desde que se recolecta hasta que se presenta en un juicio, garantizando que se ha llevado un procedimiento adecuado. Esto incluye quién la recolectó, en qué momento y lugar, cómo se transportó y almacenó, así como de quién llevó a cabo el análisis de las evidencias, y cualquier otra información relevante [9]. En el caso de las evidencias digitales, la cadena de custodia es aún más importante debido a la facilidad con la que se pueden alterar o eliminar estos tipos de evidencias, manteniendo de esta manera la menor contaminación posible de la evidencia.

Es importante tener en cuenta que los criterios de validez legal para la evidencia digital pueden variar según el sistema jurídico en el que se utilice. Actualmente en el Ecuador no existe una normativa o metodología vigente para garantizar la validez de este tipo de evidencias.

A nivel internacional, Reino Unido cuenta con normativas establecidas en el Código sobre la Policía y la Prueba Penal que regulan en cierta medida el manejo de las evidencias digitales dentro de las cuales se describe las etapas de recolección, examinación y análisis, por otra parte, países como Dinamarca, Suecia, Austria o Finlandia se considera el criterio del juez a cargo para mantener o no la admisibilidad de las evidencias digitales [11]. El Comité Europeo de Normalización (CEN) con miembros como Alemania, Bélgica, España o Francia aprobó en el año 2016 la ISO / IEC 27037 por lo cual esta norma es de aplicación obligatoria para los países miembros [12].

En Norteamérica, Estados Unidos mediante el Manual del Departamento de Justicia, especifica que el proceso para la obtención de evidencias digitales debe regirse a los mismos criterios de las evidencias tradicionales para ser admitida, por lo cual se siguen estándares y normativas que aseguren la integridad o autenticidad de las evidencias haciendo que estas sean admitidas dentro de los procesos penales [11].

Con respecto a Sudamérica, Argentina mantiene como base sobre el tratamiento de las evidencias digitales la "Guía de obtención, preservación y tratamiento de evidencia digital" la cual define directrices generales que deben llevarse a cabo durante un proceso penal considerando estándares internacionales [13]. Por otra parte, países como Colombia o Chile mantienen dentro de sus respectivas legislaciones la admisibilidad de las evidencias digitales, mas no definen procedimientos específicos, aun así, cabe

destacar que Colombia ha implementado ciertas disposiciones con el fin de que los documentos electrónicos y el peritaje informático sea admisible dentro de un proceso judicial [11].

2 METODOLOGÍA

El presente trabajo, acerca de las metodologías para la extracción de evidencia digital, muestra un análisis del tratamiento de esta, desde el momento de la obtención, hasta su utilización. El tipo de investigación que fue empleada es documental y aplicada; en primera instancia se realizó un análisis de la información obtenida de diferentes fuentes. Con el uso de este material documental se procedió con la aplicación práctica.

En primera instancia se investigó normativas clave en cuanto al manejo de evidencia digital, entre ellas la norma Internacional ISO 27037, RFC 3227, UNE 71505, UNE 71506:2013 y la ISO/IEC 30121. Se investigó además la existencia de normativas para la extracción de evidencia digital que sean aplicadas bajo la legislación del Estado ecuatoriano.

Se analizaron las metodologías empleadas por otros países para la extracción de evidencia digital basadas en las diferentes normas estudiadas. Además, se investigó a nivel local la existencia de una metodología reconocida bajo la legislación para ser aplicada en el ámbito de la extracción de evidencia digital, la cual mantenga la validez legal de esta ante la justicia ecuatoriana.

Se analizó siete herramientas de *software* empleadas para extraer la evidencia digital, detallando sus características técnicas y costos, así como una comparación de las ventajas y desventajas que presentan.

Finalmente se implementaron cinco herramientas que permiten extraer evidencia digital de una microSD, una memoria USB, una laptop y un teléfono *Android*. Se analizó su funcionamiento y los resultados obtenidos.

3 RESULTADOS

En los siguientes puntos se presenta un análisis de las diferentes normativas y metodologías aplicadas en el ámbito de las evidencias digitales, tanto en un contexto local como internacional. Posteriormente se analizan las metodologías de manera detallada con el objetivo de que estas puedan ser empleadas de manera práctica. En el último punto se realiza una aplicación de las metodologías para extraer datos de

diversos dispositivos finales, respetando cada uno de los parámetros que serán descritos tanto en el manejo como en la extracción de las evidencias digitales con el objetivo de que mantengan su validez legal.

3.1 Investigación de normativas para la recopilación de evidencia digital

A continuación, se realiza un análisis de las normativas más relevantes para el tratamiento y análisis de evidencias digitales a nivel mundial, considerando que cada país cuenta con la libertad de establecer el uso de estas o de sus propios estándares. Se debe tener en cuenta que el Ecuador no ha definido de manera explícita el uso de ninguna metodología específica dentro de su legislación.

ISO/IEC 27037:2012

La norma ISO 27037 es un conjunto de directrices para gestionar y evaluar las pruebas digitales. Fue creada por la Organización Internacional de Normalización (ISO). Esta organización desarrolla normas internacionales desde la tecnología de la comunicación hasta los equipos de seguridad. El objetivo de la creación de la ISO 27037 es crear un conjunto de normas que las organizaciones pudieran utilizar para gestionar sus pruebas digitales dándoles un valor probatorio [14].

ISO 27037 proporciona pautas para el tratamiento de evidencia digital, es un conjunto de principios que se utilizan para garantizar que todas las pruebas digitales se conserven, manejen y presenten de una manera que asegure su integridad. También explica cómo gestionar las pruebas digitales a lo largo de su ciclo de vida, incluyendo su recogida, almacenamiento, recuperación y eliminación. La guía también incluye información sobre las mejores prácticas para cada una de estas fases [15].

La norma es utilizada para garantizar que las pruebas se manejen adecuadamente, por otra parte, garantiza que los métodos utilizados para proteger los datos sean coherentes en todas las organizaciones, ayudando a las mismas a formar a sus empleados sobre cómo mantener la integridad de las pruebas digitales [14].

Las directrices de la norma ISO 27037 se pueden utilizar en los siguientes escenarios:

- Identificar la potencial evidencia digital.
- Preservar la evidencia digital durante el proceso de investigación.
- Brindar orientación sobre cómo presentar y manejar la evidencia digital.

Es importante tener en cuenta que la norma ISO 27037 presenta orientación en el manejo de las evidencias digitales de acuerdo con el tipo de dispositivo, encontrándose entre ellos equipos de almacenamiento digital, teléfonos móviles, ordenadores, entre otros [14].

RFC 3227

El RFC 3227 o "Guía Para Recolectar y Archivar Evidencia", es un estándar para la gestión y preservación de pruebas digitales. El objetivo del RFC 3227 es proporcionar un marco para la gestión y preservación de las pruebas digitales que pueda ser utilizado por los organismos encargados de la aplicación de la ley, las instituciones de justicia penal, los tribunales, los abogados y otras partes interesadas. Esta norma ayuda a garantizar la preservación de las pruebas críticas de manera que puedan ser vistas por los investigadores de una manera eficaz [16].

La guía contiene requisitos y directrices específicos para la recolección y almacenamiento de pruebas digitales diseñadas para mantener la integridad de los datos, así como su autenticación. Es necesario considerar que el RFC 3227 no aborda las cuestiones relativas a la recogida o conservación de pruebas procedentes de fuentes no digitales, como los documentos en papel.

Los principales objetivos del RFC 3227 son:

- Crear un enfoque uniforme para la gestión de las pruebas digitales en los tribunales federales.
- Fomentar el uso de las pruebas digitales en los procedimientos judiciales.
- Promover la investigación sobre la aplicación de las pruebas digitales.
- Fomentar el desarrollo de normas para la gestión, la conservación, el análisis y la presentación de las pruebas digitales.

UNE 71505

La norma UNE 71505 o "Sistema de Gestión de Evidencias Electrónicas" es una norma internacional para el tratamiento de las pruebas digitales fue creada por la Organización Internacional para la Normalización (ISO). Se publicó por primera vez en el año 2013 constando de tres partes: la primera abarca los principios y terminología en general, la segunda sobre la gestión de evidencias, y la tercera acerca de los diferentes formatos y mecanismo de manejar la información recabada. Su objetivo es garantizar que las pruebas se manejen de manera correcta, desde el momento en que se recogen hasta que se necesitan en los tribunales [17].

UNE 71505/2013-1, define el lenguaje, términos y conceptos básicos con el fin de que exista una mayor comprensión por parte de los participantes. UNE 71505/2013-2, asegura que durante el manejo de la información se garanticen los siguientes tres apartados:

- Autenticación e Integridad: busca mantener una cadena de custodia que garantice que la información no sea alterada.
- Disponibilidad y Totalidad: consiste en asegurar que las evidencias puedan ser accesibles y utilizadas en el momento que se lo requiera.
- Cumplimiento y Gestión: busca avalar que se han seguido los procedimientos establecidos y que se ha conseguido el resultado esperado luego de las gestiones realizadas.

Para garantizar que los apartados descritos anteriormente se cumplan, la UNE 71505/2013-2 establece que una organización debe mantener políticas y procedimientos para la gestión de evidencias electrónicas, definiendo responsabilidades y competencias con claridad, entre otros parámetros.

UNE 71505/2013-3 establece parámetros de formato para que las diferentes partes involucradas puedan compartir de manera segura las evidencias digitales, el formato incluye cabecera, contenido y credenciales de seguridad.

UNE 71506:2013

La UNE 71506 es la norma de gestión de la seguridad. La UNE 71506 ha sido desarrollada específicamente por el comité técnico AEN/CTN 71 Tecnología de la información de la Asociación Española de Normalización y Certificación (AENOR). El objetivo de esta metodología es proporcionar un procedimiento de análisis forense el cual complementa los procedimientos descritos dentro de la UNE 71505 en el sistema de gestión de las evidencias electrónicas [18].

Esta metodología está compuesta por diferentes fases las cuales son: preservación, adquisición, documentación, análisis y presentación, donde se describen parámetros tanto para la obtención como para el manejo de la evidencia digital. Por otra parte, también considera factores como el escenario en el cual la evidencia es hallada o el tipo de información que se desea obtener. La UNE 71506 garantiza mediante el uso de documentación, que se ha realizado un manejo adecuado de las evidencias, demostrando la integridad y confiabilidad de estas durante su presentación en un proceso judicial [19].

ISO/IEC 30121

La ISO/IEC 30121 es la norma internacional para el análisis forense digital. Define los requisitos mínimos que todas las organizaciones deben cumplir para estar preparados ante un análisis forense digital. La primera edición de la norma se publicó en 2015. Desde entonces, se han realizado varias actualizaciones importantes para reflejar las nuevas tecnologías y la evolución de los procedimientos de investigación criminal. Ha sido adoptada por muchas organizaciones de todo el mundo como base de las mejores prácticas para el manejo de las pruebas digitales, maximizando la disponibilidad y acceso a esta [20].

La ISO/IEC 30121 se creó para garantizar que las pruebas digitales se traten de forma coherente en las distintas organizaciones y para ayudar a garantizar que las pruebas digitales puedan utilizarse como prueba en los procedimientos judiciales.

Normativa local para la extracción de evidencia digital

Una vez realizada la investigación y descripción de las diferentes normativas enfocadas a la extracción de evidencia digital a nivel internacional, se procede a analizar la existencia de estas a nivel local. En el Ecuador no se encuentra adoptada ninguna clase de normativa dentro del Código Orgánico Integral Penal “COIP” que regule los procedimientos a los cuales los peritos informáticos deban someterse; cabe aclarar que el “COIP” si reconoce la cadena de custodia dentro del Art. 456 [21].

De la misma manera el Servicio Ecuatoriano de Normalización (INEN) no establece ningún reglamento centrado en la extracción de las evidencias digitales, por lo cual el uso de las normativas internacionales, como la ISO 27037 o el RFC 3227 y demás leyes aplicadas del país, proporcionan una base sobre la cual los peritos informáticos puedan garantizar la validez de las evidencias digitales [22].

3.2 Análisis de las metodologías de extracción de evidencia digital

Argentina (ISO 27037)

En el caso de Argentina, el país mantiene aprobada desde el año 2016 la aplicación de la “Guía de obtención, preservación y tratamiento de evidencia digital” dentro de su territorio. A continuación, se presenta un análisis del contenido expuesto dentro de esta documentación [23].

Recolección y preservación de la evidencia digital:

1. Asegurar la integridad del lugar y documentar cualquier procedimiento llevado a cabo, que pueda llegar a afectar de manera directa o indirecta a los equipos informáticos.
2. Identificar el estado en el que se encuentran los equipos: encendidos, apagados o suspendidos, para poder realizar las acciones correspondientes. De encontrarse suspendido el equipo y requerirse para el procedimiento su activación, se recomienda utilizar el movimiento del ratón para activar el sistema, evitando los clics u otro tipo de interacción que provoque el lanzamiento de algún tipo de *software* de protección.
3. Realizar un registro fotográfico o ilustrativo de los equipos en la escena del crimen antes de cualquier contacto con los mismos, donde se muestre tanto el monitor como la parte frontal y trasera de los equipos, permitiendo que se puedan observar las conexiones.
4. De acuerdo con el estado del equipo.
 - Apagado
 - No encender el equipo.
 - Retirar el cable de alimentación conectado al equipo y cualquier tipo de batería.
 - Retirar el resto de los cables y dispositivos externos.
 - Verificar que las unidades lectoras se encuentren cerradas y en caso de estar abiertas, registrar el contenido encontrado.
 - Encintar todos los puertos para asegurar que estos no puedan ser utilizados para alterar la información contenida.
 - Registrar la información de identificación del equipo y sus periféricos.
 - Encendido
 - La recomendación general es desconectar la alimentación del equipo encendido para preservar los datos.
 - En el caso de que se pueda observar a simple vista que los datos están siendo borrados o se tenga sospecha, se procede a desconectar la alimentación del equipo de manera inmediata, para de manera posterior seguir el procedimiento descrito para los equipos apagados.
 - Si a simple vista se observa evidencia de carácter probatorio o se puede demostrar que se encuentran programas activos con información

fundamental, estos deben ser respaldados en una unidad de almacenamiento que permita bloquear la escritura.

5. En el caso de que existan redes inalámbricas, estas deben ser registradas detallando las conexiones existentes entre los dispositivos por medio de otro equipo, detallando la información de estos como puertos abiertos y cerrados, los servicios o aplicaciones utilizadas, etc. Además, se debe considerar la posible intrusión a la red de manera externa por lo cual el personal encargado debe registrar el suceso y bloquear el acceso a la misma. Una vez ejecutado el registro se deben realizar los procedimientos de manejo de equipos descritos con anterioridad.
6. Cualquier otro equipo electrónico que puede considerarse como potencial evidencia debe ser resguardado como se detalla en el punto de Embalaje, traslado y resguardo de la evidencia digital, salvo en casos excepcionales que requieran que se interactúe con los mismos.

Embalaje, traslado y resguardo de la evidencia digital

1. Documentar la evidencia digital debidamente.
2. Embalar toda la evidencia en paquetes con envoltorios antiestáticos o de papel madera o cartón.
3. Evitar que los métodos de recolección de evidencias provoquen daños o deformación en los equipos.
4. En caso de requerirse que dispositivos celulares se mantengan encendidos, estos deben ser cubiertos de manera que se garantice el bloqueo de la señal de estos.
5. Recolectar todas las fuentes de energía vinculadas a los equipos.
6. Mantener la evidencia fuera del alcance de factores externos que puedan provocar la pérdida o el daño de esta.

Manipulación idónea del *hardware*

1. Debe llevarse a cabo en instalaciones acondicionadas para el tratamiento de estos, manteniendo además protecciones adecuadas que eviten el daño de los componentes sensibles.

Imagen o copia forense y uso de hash

1. Realizar la copia de respaldo del disco de manera directa extrayendo el disco físico, o de manera indirecta mediante un dispositivo externo. Considerando los siguientes aspectos:
 - Utilizar un bloqueador de escritura asegurando que los datos no sean modificados.
 - Realizar el cálculo hash de dicha copia forense con el objetivo de mantener la integridad de esta.

Además de lo antes expuesto en la guía, se consideran los siguientes principios básicos durante todo el proceso:

1. Evitar la contaminación de la escena o la evidencia, alejando del lugar a todo el personal que no sea requerido.
2. Asegurar que las acciones llevadas a cabo por los agentes de seguridad no alteren de ninguna manera los datos digitales contenidos dentro de los equipos.
3. Garantizar que, en caso de requerir acceder a la información, el personal a cargo de realizar el contacto con la evidencia cuente con el conocimiento suficiente, justificando los motivos por los cuales fue necesario el acceso a la información y los procedimientos llevados a cabo.
4. Registrar todo el proceso de manipulación de la evidencia de manera detallada, preservando la cadena de custodia de esta.

ISO/IEC 27037:2012

La normativa ISO/IEC 27037:2012 presenta cuatro directrices generales sobre las cuales se fundamenta [12].

1. Justiciable: Argumenta los motivos por los cuales se consideró a un procedimiento o decisión como la mejor opción sobre otras alternativas.
2. Auditable: Proporciona respaldos mediante documentación y registros que permitan validar que se han llevado a cabo procedimientos que cumplen con las leyes o reglamentos establecidos.
3. Replicable y Reproducible: Garantiza que los procedimientos llevados a cabo puedan ser replicados bajo las mismas condiciones e instrumentos obteniendo los mismos resultados o variando estos últimos para conseguir resultados similares.
4. Defendible: Asegura que las herramientas utilizadas dentro de cada procedimiento han sido validadas y comparadas con otras.

Las etapas que deben seguir los procedimientos para que se conserve la integridad y valides de las evidencias según la norma son [24]:

1. Identificación: Determinar la localización de la potencial evidencia tanto física como lógica.
2. Adquisición: Recolección de los dispositivos que puedan contener la posible evidencia o una copia de esta, así como la documentación correspondiente a cada una de estas.
3. Preservación: Mantener la evidencia fuera de posibles modificaciones, mientras se conserva la cadena de custodia que garantice la integridad de los datos.

UNE 71506:2013

El objeto de esta norma es definir y complementar el proceso de análisis forense en la gestión del ciclo de pruebas informáticas. Establece un método para preservar, recolectar, documentar, analizar y presentar evidencia informática. El presente análisis se ha llevado se ha realizado en base a la documentación provista por la UNE [25], así como de análisis complementarios de sitios web especializados [26] [18].

Fase de preservación

La fase de preservación de la metodología se refiere a la conservación adecuada de las evidencias digitales para garantizar su integridad y confiabilidad durante el proceso judicial. Se deben utilizar medidas de seguridad y procedimientos especializados desde su recolección para proteger las evidencias de posibles alteraciones o cambios, hasta su presentación en el proceso judicial.

El personal calificado deberá mantener dicha evidencia en un lugar seguro hasta que se hayan completado los procedimientos profesionales.

Fase de adquisición

En la fase de Adquisición de la metodología describe el procedimiento a llevarse a cabo para la obtención de las evidencias digitales. Dado que los procesos pueden variar de acuerdo con el estado de los equipos, la metodología considera los escenarios en que han sido hallados los equipos electrónicos buscando mantener en todo momento la integridad de la información. Posteriormente se realiza una clonación de bajo nivel de los datos originales utilizando procedimientos documentados para garantizar que el proceso de adquisición sea reproducible y repetible, además se calcula un código hash para cada prueba.

Si la ubicación del incidente está físicamente aislada, se deben seguir algunas de las precauciones que se enumeran a continuación:

1. Se deben retirar todas las personas no autorizadas de la escena del crimen.
2. Identifique el administrador del sistema en caso de necesitar soporte técnico.
3. Mantenga el estado del dispositivo, si está encendido, no lo apague y viceversa.
4. Busque notas sobre la contraseña o el PIN utilizado para acceder al dispositivo.
5. Fotografíe el estado inicial de la escena para que se pueda restaurar más tarde.
6. Etiquete el cableado y los dispositivos.
7. Ubique dispositivos inalámbricos instalados e identifique su modo de conexión.
8. No desconecte la alimentación si la evidencia está almacenada en medios volátiles.
9. Compruebe si hay dispositivos de almacenamiento adicionales insertados en los dispositivos digitales.

Dado que el estado del sistema es fundamental y puede comprometer la integridad de las pruebas potenciales con relativa facilidad, el proceso de recopilación no es el mismo para los sistemas encendidos y apagados.

Si el sistema está apagado, la recomendación básica es realizar un borrado seguro del soporte que será clonado y utilizar un dispositivo de bloqueo de escritura (*hardware o software*). Para dispositivos móviles, si lleva una tarjeta SIM, se debe extraer la información contenida en la tarjeta SIM. Si no conoce su número PIN o PUK, debe ser solicitado al proveedor de telefonía por orden judicial. Se debe calcular el hash para toda la información extraída.

Si el sistema este encendido, se procederá a su comprobación desde su grado de volatilidad. Se diferencian dos niveles de volatilidad:

- La información sobre memoria *RAM*, particiones y archivos de paginación, procesos de red y sistemas operativos en ejecución.
- La información sobre el sistema de archivos y los datos contenidos en los sectores del dispositivo de bloque.

En un entorno virtualizado, cada máquina virtual consta de varios archivos. La configuración del *hardware* del dispositivo utilizado para el almacenamiento y uno o más discos físicos o virtuales. La información que se obtiene aquí es un disco virtual y un volcado de parte de la *RAM* utilizada en este entorno. De esta forma, una vez que tenga todos los archivos de configuración de la máquina virtual y del disco virtual, debería poder recrear el entorno original para su análisis.

Fase de documentación

Esta fase describe por completo el procedimiento aplicado, esto quiere decir que se detallan las acciones llevadas a cabo durante el análisis, así como las herramientas utilizadas siguiendo en todo momento una cadena de custodia que puede evidenciar el correcto manejo de la información hasta el momento en el que se envía el informe pericial.

La gestión documental incluye, en particular, los siguientes documentos:

- Un documento informático de recepción de evidencia capaz de auto seguir la solicitud de análisis y evidencia.
- Registro de documentos recibidos, la documentación que acompaña a la evidencia incluye una descripción para que esta llegue al ambiente analítico, así como los estudios y aprobaciones requeridas para estos análisis.
- Registro de evidencia detallando cada prueba y su estado al momento de su recepción.
- Un registro inicial que describe el proceso de clonación.
- Un registro de evidencia que refleja qué acción se realizó, dónde se realizó y cuándo se realizó.
- Registro de tareas de análisis inicial.
- Registro de la tarea final de análisis de datos y la posición temporal de las pruebas en el caso de que se paralice temporalmente la investigación.

Fase de análisis

En la fase de análisis se busca llevar a cabo procesos capaces de satisfacer las necesidades del peritaje sean estos la recuperación de ficheros, análisis del sistemas operativos o particiones, entre otros; estos procesos deben mantener los principios: auditables, repetibles y defendibles. El procedimiento que debe seguirse en la fase de análisis se detalla a continuación:

- Verificar que el laboratorio se encuentra capacitado para realizar el estudio propuesto.
- Desarrollar una representación ilustrativa que muestre la relación entre las evidencias entre sí y los implicados, de acuerdo a la documentación del caso.
- Asegurar que se ha mantenido la cadena de custodia de la evidencia antes de su llegada para el análisis.
- Obtener las autorizaciones legales correspondientes para realizar el análisis y manejo de las evidencias.

- Verificar el estado de deterioro en el que se encuentran las evidencias, comprobando si es posible la realización de este.
- En el caso de que nuevas evidencias sean detectadas se debe realizar todo el procedimiento correspondiente a la gestión, preservación, custodia, etc. Además, se debe notificar al solicitante del análisis de estos hechos.
- Documentar la hora de la BIOS del equipo, para posteriores comparaciones dentro del análisis forense.
- Mantener un orden de prioridad en el análisis.

El análisis que se debe llevar a cabo para el estudio de particiones y sistemas de archivos debe llevarse a cabo considerando los siguientes puntos:

- Identificar y numerar las particiones existentes, así como las que hubieran existido.
- Reconocer las zonas del disco que se encuentren ocultas para el sistema operativo.
- Definir el tipo de sistema de archivos de las particiones o contenedores e identificar entre ellos al que almacena el sistema operativo del equipo y su tipo de arranque.
- Reconocer los archivos protegidos por cifrado o contraseña dentro del almacenamiento.

El análisis para sistemas operativos se centra en reconocer el sistema, los usuarios y las políticas de seguridad aplicada, respetando los siguientes criterios descritos a continuación:

- Reconocer el Sistema Operativo del equipo, así como su versión y actualizaciones.
- Identificar los usuarios dentro del Sistema Operativo, así como sus permisos y políticas de seguridad.
- Identificar el *software* y *hardware* que haya sido instalado en el equipo.

En el caso de ficheros borrados, se tratará de conseguir una recuperación parcial o total de los datos. Los métodos aplicados, así como la información obtenida debe ser documentada en un informe pericial.

Si se presentan memorias volátiles como la memoria *RAM*, se realizará el estudio de los procesos activos, los archivos abiertos, así como también los puertos abiertos o

dispositivo de almacenamiento conectados entre otros, considerando que estos parámetros se presentan únicamente en el momento concreto del estudio.

Considerando los aspectos descritos anteriormente, el análisis detallado de las evidencias contendrá la siguiente información:

- Información esencial como es: el *hardware*, datos de fecha y hora, entre otros.
- Dispositivos reconocidos por el equipo.
- Descripción de la pantalla principal y elementos de la papelera.
- Información de las tarjetas de red como dirección *MAC* y dirección *IP*.
- Historial de las comunicaciones salientes y entrantes.
- Revisión de *logs*.
- Identificación de la información contenida en espacios no visibles de las particiones, así como de los espacios vacíos.
- Información de los documentos impresos.
- Identificación de archivos recientes.
- Identificación de las aplicaciones en el equipo.
- Análisis de los metadatos relevantes.
- Análisis de las carpetas de usuario.
- Identificación de aplicaciones de virtualización.
- Análisis de bases de datos encontradas.
- Información acerca de archivos cifrados.
- Información acerca de la navegación web.
- Información obtenida mediante el análisis de correo y mensajería, adjuntando la lista de contactos.

Fase de presentación

En esta fase se presenta el informe pericial donde se describen los resultados obtenidos mediante la fase de análisis, esta información podría llegar a ser utilizada dentro del proceso judicial; es necesario considerar que debe ser escrito en un lenguaje no técnico. La fase de presentación finaliza el proceso de la cadena de custodia.

Cadena de custodia establecida por la Fiscalía General del Estado

Se señala que es responsabilidad del perito, sea este civil o policial, el aplicar el procedimiento adecuado para la conservación y tratamiento de las evidencias, así como iniciar la cadena de custodia. En el documento provisto por la Fiscalía General del Estado se detalla los siguientes procedimientos [27].

Fijación digital de los equipos que se encuentren encendidos o en funcionamiento

- Requiere de tres diferentes registros fotográficos:
 - El estado original en el cual es hallado el equipo, así como los componentes y accesorios externos de este.
 - Las placas de identificación donde deben constar los números de serie y los modelos de los equipos encontrados.
 - La pantalla principal del equipo.

- Captura de memorias volátiles o *RAM*:
 - Realizar el acoplamiento físico utilizando una interfaz nueva sea esta USB, DVD u otra, provista por el Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses.
 - Empezar la adquisición de la información para su posterior conservación y protección.
 - Realizar el apagado de los equipos.
 - Entregar la información obtenida al centro de almacenamiento e iniciar con la cadena de custodia de la evidencia.

Fijación digital de los equipos que se encuentren apagados

- Identificar el equipo, así como los componentes y accesorios externos de este.
- Realizar las placas de identificación donde debe constar los números de serie y los modelos de los equipos encontrados.
- Realizar la descripción ilustrativa de la escena de los hechos e inicio de la cadena de custodia.

Metodologías a nivel local

En el ámbito nacional como se ha descrito con anterioridad no se registra dentro de su legislación el uso de una metodología estándar, por lo cual, se han propuesto diferentes metodologías por parte de expertos en el área o mediante trabajos de fin carrera en instituciones educativas de tercer y cuarto nivel. Ambas basadas en estándares internacionales con el objetivo de garantizar su validez legal en el Ecuador.

Diseño de una Guía Metodológica para el Análisis Forense Digital tomando como base Equipos con el Sistema Operativo *Windows 8.1*

El diseño propuesto se basa en la metodología UNE 71506:2013, contemplando las cinco fases principales que se presentan en la misma, por otra parte se centra en el sistema operativo *Windows 8.1* por lo cual se encuentra desfasada con la llegada de nuevas versiones del sistema, además hace uso de herramientas de código abierto para la extracción de las evidencias enfocándose en discos duros, se hace énfasis en que el trabajo indica que ha sido elaborado para personas con un conocimiento básico de informática, ejemplificando ciertos procesos para mantener un mayor entendimiento de la metodología [19].

Desarrollo de una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo *Mac OS X* en el Ecuador

El trabajo presentado se basa en la metodología UNE 71506:2013 así como en la RFC 3727, de la misma manera contempla las cinco fases principales que se presentan en UNE 71506:2013, toma como enfoque el sistema *Mac OS X* por lo cual como se mencionó anteriormente puede quedar desactualizada frente a la presentación de nuevas versiones del sistema. La metodología contempla la normativa legal ecuatoriana vigente en el año de su publicación para garantizar su uso en tribunales; al estar dirigida para ser usada por peritos informáticos, cada fase de la metodología se encuentra sumamente detallada, ejemplificando al final de este documento los procesos de manera práctica [28].

Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012

Principalmente se basa en la norma ISO/IEC 27037:2012, toma aspectos presentes en las prácticas informáticas forenses implementadas en España, Argentina y Colombia; hace uso de seis fases desde la ubicación de la escena hasta el análisis de la evidencia, su aplicación no tiene un enfoque con ningún sistema operativo, pero se encuentra destinado a discos duros por lo cual se limita su campo de aplicación. La metodología se ha diseñado para ser empleada en el peritaje, ejemplificando su metodología en casos reales por personal profesional para garantizar la validez del mismo [28].

Marco de trabajo estandarizado para el análisis forense de la evidencia digital

Diseñada para proveer un marco de trabajo general a ser utilizado por los peritos en el ámbito del análisis forense, se sustenta bajo la metodología UNE 71506:2013, el RFC

3227, ISO/IEC 27037:2012; considerando además las recomendaciones y prácticas publicadas a nivel internacional, adecuándose a la normativa legal vigente en el Ecuador en el año de su publicación; para de esta manera asegurar su validez frente a un tribunal. Define cada uno de los aspectos a considerar en las diferentes fases de la metodología, haciendo énfasis en la obtención y el análisis de las evidencias digitales, dado que no se centra en un dispositivo específico, se presentan aspectos a considerar tanto de computadores como dispositivos móviles [29].

En Tabla 3.21 Resultados de las pruebas realizadas, se realiza una tabla comparativa de las características principales de las propuestas descritas con anterioridad.

Tabla 3.21 Resultados de las pruebas realizadas

Título	Año de publicación	Norma internacional en la que se basa	Dispositivos	Enfoque
Diseño de una Guía Metodológica para el Análisis Forense Digital tomando como base Equipos con el Sistema Operativo <i>Windows 8.1</i>	2021	- UNE 71506:2013	Computadoras	Sistema Operativo <i>Windows 8.1</i>
Desarrollo de una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo <i>Mac OS X</i> en el Ecuador	2018	- UNE 71506:2013 - RFC 3227	Computadoras	Mac OS X
Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037:2012	2019	- ISO/IEC 27037:2012	Computadoras	Discos Duros

Título	Año de publicación	Norma internacional en la que se basa	Dispositivos	Enfoque
Marco de trabajo estandarizado para el análisis forense de la evidencia digital	2017	- UNE 71506:2013 - RFC 3227	Equipos informáticos	General

Una vez realizado el análisis de las propuestas metodológicas a nivel local, se ha escogido la metodología “Desarrollo de una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo *Mac OS X*” como el modelo principal a ser aplicado dentro del presente trabajo para el tratamiento de la evidencia, dado el detalle con el cual se han descrito los procedimientos a llevarse a cabo en cada una de las fases. Además, considerara los aspectos recogidos por el “Marco de trabajo estandarizado para el análisis forense de la evidencia digital” dentro de la fase de análisis, ya que esta abarca una mayor cantidad de parámetros en comparación al resto de metodologías presentadas.

Por otra parte, considerando que los trabajos expuestos se basan en la misma metodología “UNE 71506:2013” estos podrían ser utilizados de manera complementaria dentro de las fases que así lo requieran.

3.3 Herramientas de *software* para la extracción de evidencia digital

***FTK Imager* [30] [31] [32]**

Es una herramienta destinada a la visualización y recopilación de posibles evidencias digitales contenidas en unidades de almacenamiento. Su interfaz es intuitiva, mostrando dos paneles de navegación, en la izquierda se muestran los datos presentes en forma de árbol, mientras que en el lado derecho se observa la información detallada de los archivos. A continuación, se realiza una descripción de la herramienta.

Características:

- Previsualización de los archivos contenidos dentro de la unidad de almacenamiento.
- Creación de imágenes forenses a partir de diferentes medios de almacenamiento.
- Creación de *hash* para verificar la identidad.

- Recuperación de archivos borrados que no han sido sobrescritos.
- Compatible con *Linux* y *Windows*.

Ventajas:

- Permite verificar con la vista previa si el contenido almacenado dentro de la unidad es relevante para la investigación.
- Las imágenes forenses se realizan bit a bit, por lo cual la copia mantiene el espacio no asignado o invisible de la unidad de almacenamiento original.
- Compatible con unidades de red.
- Recuperación del archivo de paginación.

Desventajas:

- No permite ningún otro tipo de análisis para los datos, además de la extracción de estos y la verificación del hash.
- Requiere de instalación, no cuenta con una versión portable.
- Tamaño mayor al de otras opciones similares.
- Requiere completar un formulario para su descarga.

Costo:

- Esta herramienta es de uso gratuito.

***AUTOPSY* [33]**

Es una herramienta destinada al análisis de datos en unidades de almacenamiento, *Autopsy* funciona como una interfaz gráfica para *The Sleuth Kit* (TSK) la cual es la librería que contiene las herramientas para llevar a cabo el proceso de análisis y recuperación de datos. A continuación, se realiza una descripción de la herramienta.

Características:

- Se basa en código libre por lo cual los usuarios pueden aportar a su desarrollo.
- Implementa la colaboración multiusuario permitiendo el análisis de los datos desde diferentes instancias al mismo tiempo, generando un informe unificado al finalizar.
- Mediante marcadores es posible identificar evidencia almacenada de casos anteriores que puedan llegar a ser relevantes o a relacionarse con el caso actual de trabajo.
- Compatible con unidades de almacenamiento y *smartphone*.
- Permite búsquedas por *hash* MD5.

Ventajas:

- Permite el uso de palabras clave para realizar una búsqueda más eficiente.
- Permite el trabajo simultáneo en un mismo caso.
- Recupera información o fracción de esta.
- Provee una interfaz gráfica.
- Permite agregar módulos para añadir o automatizar funcionalidades.
- Compatible con *Linux*, *Windows* y *Mac OS*.

Desventajas:

- No tiene una versión portable.
- Requiere la imagen forense previa.
- La interfaz puede llegar a ser compleja.
- Requiere un nivel de conocimiento sobre sectores de discos duros.

Costo:

- La herramienta es de código libre, por lo que su acceso es gratuito, aun así, ofrece suscripciones de pago para obtener asistencia, capacitación o módulos personalizados.

Recuva [34]

Es una herramienta de recuperación de datos desarrollada por *Piriform Software* la cual se ha popularizado por ser gratuita y presentar una interfaz intuitiva, es utilizada dentro de las herramientas para análisis forense de la metodología aplicada en España [30].

Características:

- Es capaz de recuperar archivos independientemente de su tipo.
- Compatibilidad con una gran cantidad de formatos de almacenamiento.
- Presenta el modo de escaneo profundo para encontrar un mayor número de archivos eliminados.
- Permite eliminar archivos de forma segura.

Ventajas:

- Capacidad para recuperar archivos en unidades de almacenamientos dañadas.
- Recupera archivos de unidades de almacenamiento formateadas.
- Presenta una interfaz gráfica amigable con el usuario.
- Presenta una vista previa de los archivos antes de su recuperación.
- Es multilinguaje.

Desventajas:

- Únicamente disponible en *Windows*.
- No cuenta con una versión portable oficial.
- No existe nuevas actualizaciones.
- Limita la cantidad de datos a recuperarse en su versión gratuita.
- Publicidad intrusiva al instalar.

Costo:

- La herramienta cuenta con una edición gratuita la cual permite la recuperación de los datos, mientras que la versión de pago añade soporte para discos virtuales actualizaciones automáticas y soporte especializado.

***DiskDigger* [35]**

La herramienta *DiskDigger* se centra en la recuperación de datos, tiene una amplia compatibilidad con todo tipo de dispositivos de almacenamiento y no requiere conocimientos especializados para su uso.

Características:

- Capacidad para recuperar archivos de distintas fuentes.
- Compatible con diferentes tipos de unidades de almacenamiento como tarjetas de memoria, discos duros, cámaras entre otros.
- Capacidad para recuperar archivos de diferentes tipos.

Ventajas:

- Es capaz de recuperar archivos tanto de particiones o unidades de almacenamiento formateadas.
- Capacidad para recuperar datos de unidades de almacenamiento dañadas.
- Permite la recuperación de archivos aun cuando la tabla de particiones ha sido borrada y es inaccesible para el usuario.
- Compatibilidad con *Windows* y *Mac OS*.
- Cuenta con versión para dispositivos móviles *Android*.

Desventajas:

- No presenta una versión portable.
- Su versión gratuita no permite le recuperación de archivos.

Costo:

- La herramienta cuenta con una versión gratuita que únicamente permite visualizar los archivos encontrados para su recuperación, pero no permite que estos sean recuperados, mientras que la versión de pago incluye soporte y permite la recuperación de los archivos.

Oxygen Forensic [35] [36]

Es un conjunto de herramienta enfocadas al análisis forense digital, cuenta con diferentes apartados permitiendo al usuario tanto extraer como analizar la información de una gran cantidad de dispositivos.

Características:

- Compatibilidad con una gran cantidad de sistemas móviles entre ellos *iOS* y *Android*.
- Capacidad para recuperar archivos eliminados.
- Capacidad para decodificar archivos con contraseña.
- Proporciona herramientas para simplificar el análisis de los datos.

Ventajas:

- Simpleza de uso, no requiere conocimientos avanzados.
- Interfaz intuitiva.
- Cuenta con una gran cantidad de funcionalidades.
- Permite crear informes en diferentes formatos.
- Provee soporte y actualizaciones.

Desventajas:

- Al ser un conjunto de herramientas su tamaño es significativo.
- No cuenta con una versión gratuita.
- Ciertas herramientas pueden requerir tanto de *software* como *hardware* adicional.

Costo:

- El paquete de herramientas es únicamente de pago, aun así, se puede hacer uso de una versión de prueba que ofrece acceso completo a las funcionalidades de la versión más básica por 20 días.

***Magnet RAM Capture* [38] [33]**

Es una herramienta destinada a realizar la adquisición de la información volátil contenida en la memoria *RAM* de una computadora, se ha diseñado para no provocar sobre escrituras en los datos del equipo durante la obtención de los datos.

Características:

- Permite volcar la información volátil del equipo a otra unidad de almacenamiento.
- Es una herramienta de código abierto.
- Permite fragmentar los archivos obtenidos para almacenarlos en varias unidades de almacenamiento.

Ventajas:

- Únicamente es compatible con *Windows*.
- No requiere de instalación.
- Puede obtener credenciales de cifrado almacenadas en la memoria *RAM*.
- Interfaz intuitiva.
- El tamaño de la herramienta es ligero.

Desventajas:

- Los datos obtenidos no se presentan de manera amigable con el usuario por lo que se requiere tener cierto nivel de conocimiento.
- Requiere una cantidad significativa de recursos por lo que puede provocar ralentizaciones en el sistema.
- Requiere de herramientas extra para analizar los datos obtenidos.
- No presenta una versión para sistemas operativos de 64 bits.

Costo:

- Al ser una herramienta de código abierto puede obtenerse manera gratuita, no cuenta con versiones de pago.

***Andriller* [39]**

Esta herramienta de análisis forense digital está destinada a ser utilizada con dispositivos *Android*, permite al usuario extraer y analizar la información en el equipo. A continuación, se detalla un análisis de la herramienta.

Características:

- Permite utilizar la extracción de los datos usando diferentes métodos como el modo *root*, *ADB*, entre otros.

- Presenta herramientas que permiten al usuario descifrar las claves de bloqueo para acceder al teléfono.
- Contiene funcionalidades para descomprimir bases de datos de programas como WhatsApp, Skype entre otros.

Ventajas:

- Compatible con *Windows* y *Linux*.
- Compatibilidad con la mayoría de los dispositivos *Android*.
- Tamaño ligero
- Presenta una interfaz sencilla.
- Es capaz de descifrar pantallas de bloqueo.

Desventajas:

- Requiere que los datos del dispositivo no se encuentren cifrados.
- Requiere que el dispositivo cuente con la depuración por USB activada.

Costo:

- Es una herramienta de código abierto por lo cual solo mantiene una versión la cual puede obtenerse de manera gratuita.

3.4 Implementación de herramientas para la extracción de evidencias digitales

Se ha planteado un escenario ficticio para la implementación de las herramientas de extracción de evidencias digitales, con el objetivo de aplicar las metodologías descritas en el punto 3.3 de una manera práctica.

Dentro del escenario propuesto de se han hallado cinco diferentes dispositivos electrónicos los cuales pueden considerarse como evidencia electrónica, estos se muestran en la Figura 3.1.

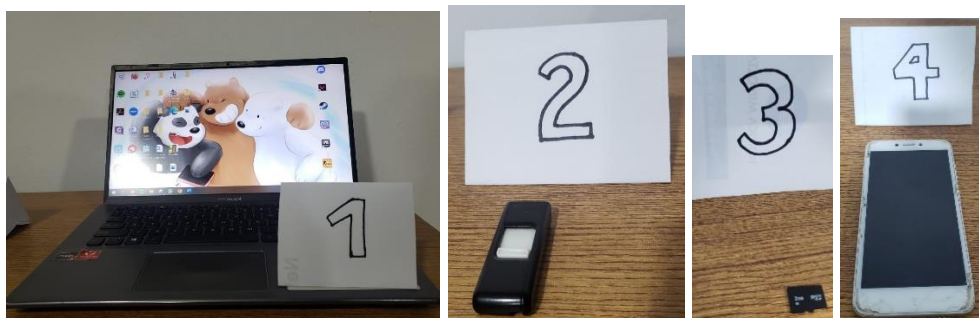


Figura 3.1 Evidencia electrónica hallada en la escena propuesta

Una vez determinada la evidencia electrónica presente en la escena, se procede con la identificación de esta, especificando la fecha de adquisición de los equipos, el número de evidencia correspondiente, y una breve descripción del dispositivo, este caso no se han añadido parámetros como el número de caso dado y la naturaleza ficticia del caso planteado. A continuación, se indican un listado de las evidencias, y tanto en la Figura 3.2 como en la Figura 3.3 se puede observar el etiquetado que se ha utilizado para la identificación de estas.

- Evidencia 01: Laptop Gris Asus.
- Evidencia 02: Memoria USB Sandisk Cruiser de 4GB.
- Evidencia 03: Memoria microSD de 2GB.
- Evidencia 04: Celular Xiaomi Blanco.



Figura 3.2 Evidencias 01 laptop y 02 memoria USB



Figura 3.3 Evidencias 03 memoria microSD y 04 celular Xiaomi

Es necesario recalcar que una vez que se ha almacenado y etiquetado a las evidencias, se inicia la cadena de custodia. Por lo cual, cualquier acción llevada a cabo sobre estas debe ser registrada con el objetivo de garantizar la integridad de estas, así como la validez de cualquier evidencia digital que pueda llegar a ser obtenida.

Para el análisis y manejo de la evidencia se ha utilizado el siguiente equipo:

- Guantes de látex para no dejar huellas o alterar la evidencia, ver Figura 3.4.
- Disco duro externo, observado en la Figura 3.5.
- Computadora de escritorio, observado en la Figura 3.6.
- Adaptadores de memoria microSD, ver Figura 3.7.



Figura 3.4 Guantes de látex



Figura 3.5 Disco Duro Externo



Figura 3.6 Computadora de escritorio



Figura 3.7 Adaptadores de memoria microSD

Magnet RAM Capture

En el caso de la Evidencia 01, laptop ASUS, al encontrarse encendida, se ha procedido de acuerdo con los parámetros descritos en la metodología donde se expone que el equipo debe mantenerse encendido para evitar la pérdida de la información potencial, para esto se ha mantenido un movimiento constante del *mouse* con el fin de prevenir que el equipo pueda llegar a apagarse. Dado a que en el escenario ficticio planteado no existen amenazas externas o intrusos, se puede proceder con la obtención de los datos almacenados en la memoria volátil.

En este caso se ha hecho uso de la herramienta *Magnet RAM Capture* la cual se puede obtener de manera gratuita dentro de la página oficial de *Magnet Forensic*, una vez obtenido el archivo ejecutable *Magnet RAM Capture*, es necesario preparar la unidad de almacenamiento donde será volcada la memoria volátil, en este caso se ha optado por usar un disco duro externo.

Una vez insertado el disco duro externo en la Evidencia 01, se debe correr *Magnet RAM Capture* dentro de la misma, es necesario definir una ruta y nombre para el archivo a obtenerse. En caso de que la unidad de almacenamiento no cuente con suficiente espacio para almacenar el volcado de la memoria, el programa permite al usuario dividir la información en partes, una vez el proceso se ha terminado se puede observar que el archivo ha sido creado de manera correcta, como se puede ver en la Figura 3.8.

Se debe recordar que es necesario crear el hash del mismo para garantizar la integridad de los datos en análisis posteriores. Utilizando el *software OSForensics* en la Figura 3.9 se observa la creación del hash y en la Figura 3.10 se muestra el contenido resultado del volcado de memoria, en este se puede observar información como el nombre del proceso, la hora, entre otros.

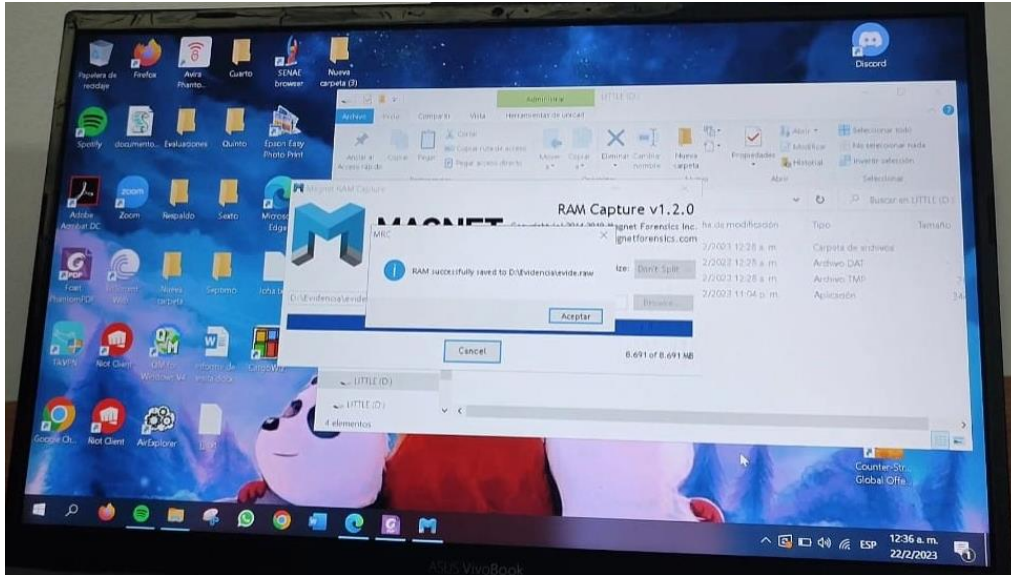


Figura 3.8 Volcado de memoria en la laptop Evidencia 01

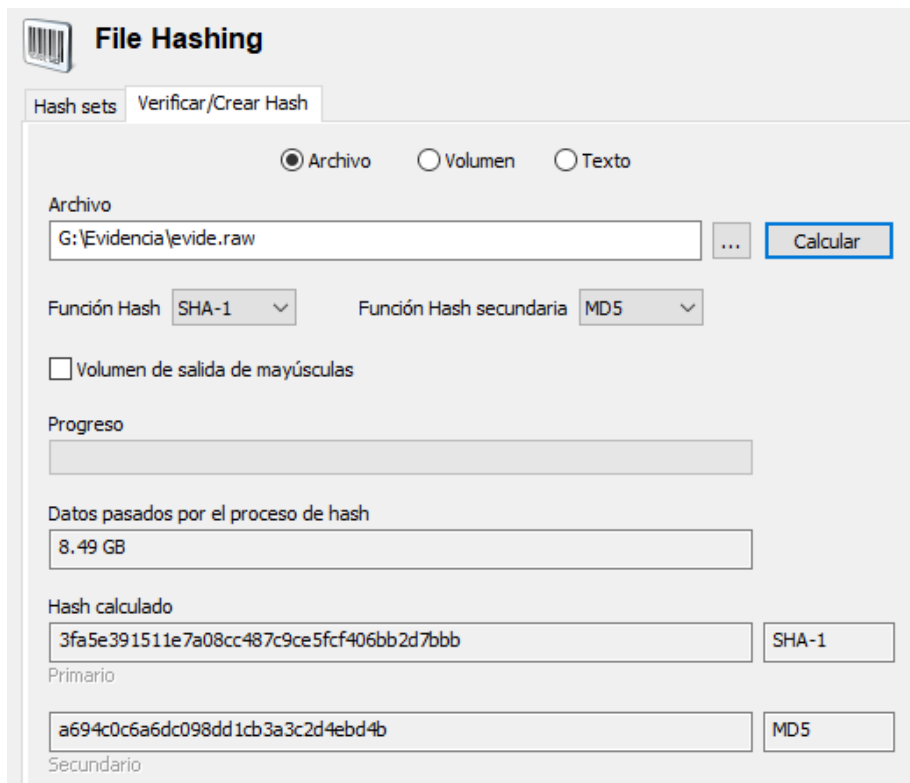


Figura 3.9 Creación del Hash para el archivo de volcado de la memoria RAM

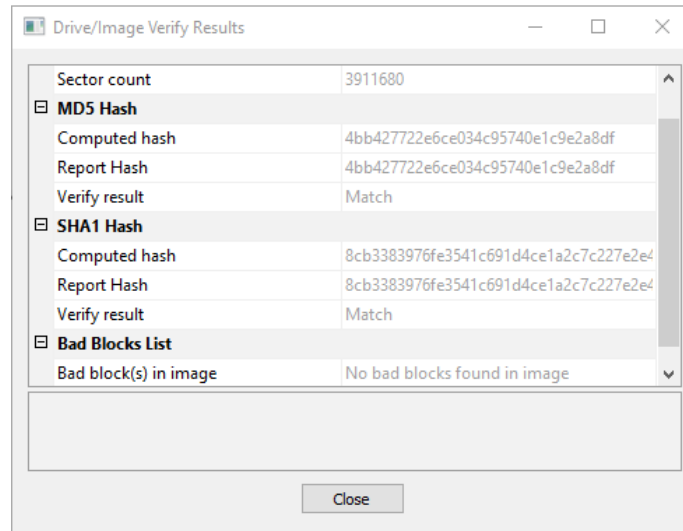


Figura 3.11 Hash obtenido de la imagen forense de microSD

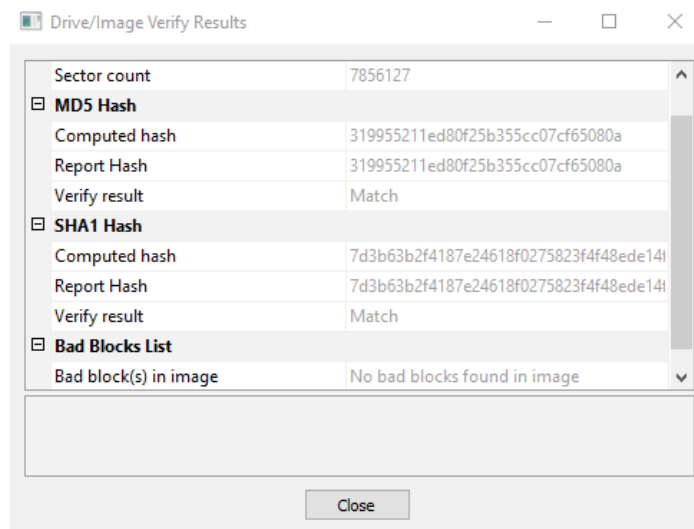


Figura 3.12 Hash obtenido de la imagen forense de memoria USB

Por otra parte, una vez se ha revisado el contenido de las imágenes, se pudo notar a simple vista que el contenido recuperado en la memoria microSD es nulo, siendo que todo el contenido que haya sido borrado se ha corrompido, mientras que en el caso de la memoria USB mucha de la información borrada podía ser recuperada de manera satisfactoria permitiendo visualizar el contenido de este, como se puede ver en la **¡Error! No se encuentra el origen de la referencia.** y Figura 3.14. Por otra parte, en el caso del disco duro la navegación se complicaba a causa de la cantidad de archivos, y las funcionalidades ofrecidas por la herramienta no eran capaces de permitir un análisis adecuado de los datos del disco, esto se puede observar en la Figura 3.15

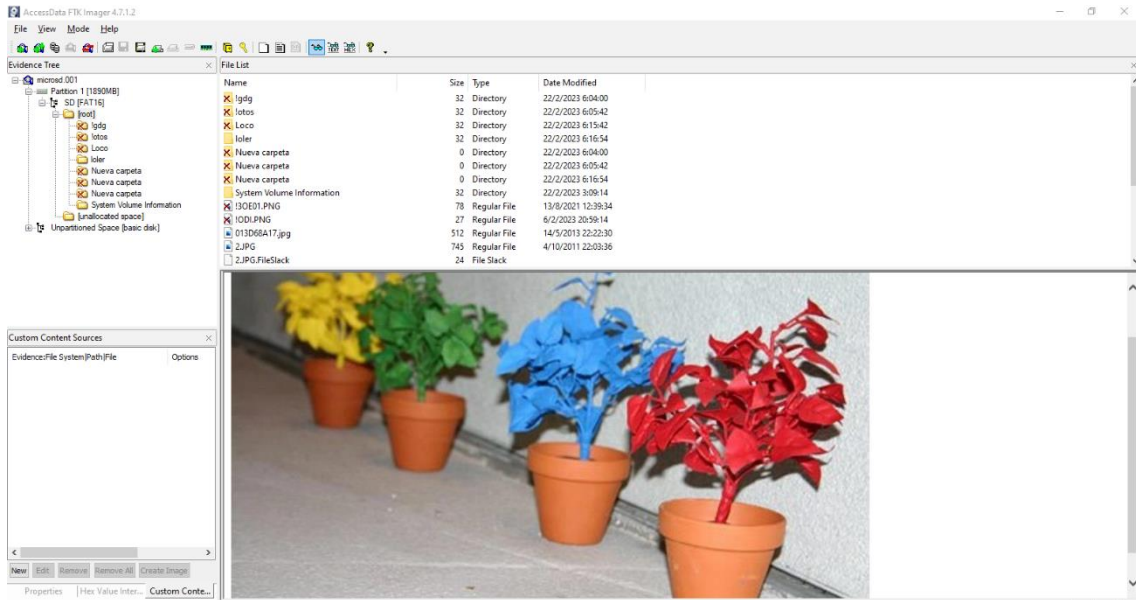


Figura 3.13 Información mostrada dentro de la imagen forense de la microSD

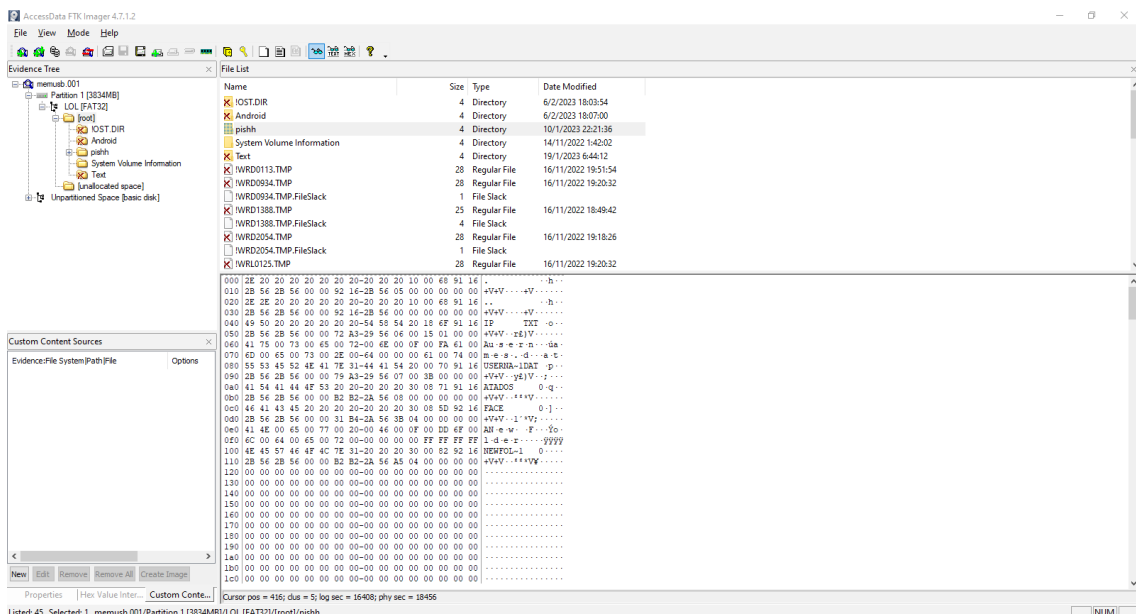


Figura 3.14 Información mostrada dentro de la imagen forense de la memoria USB

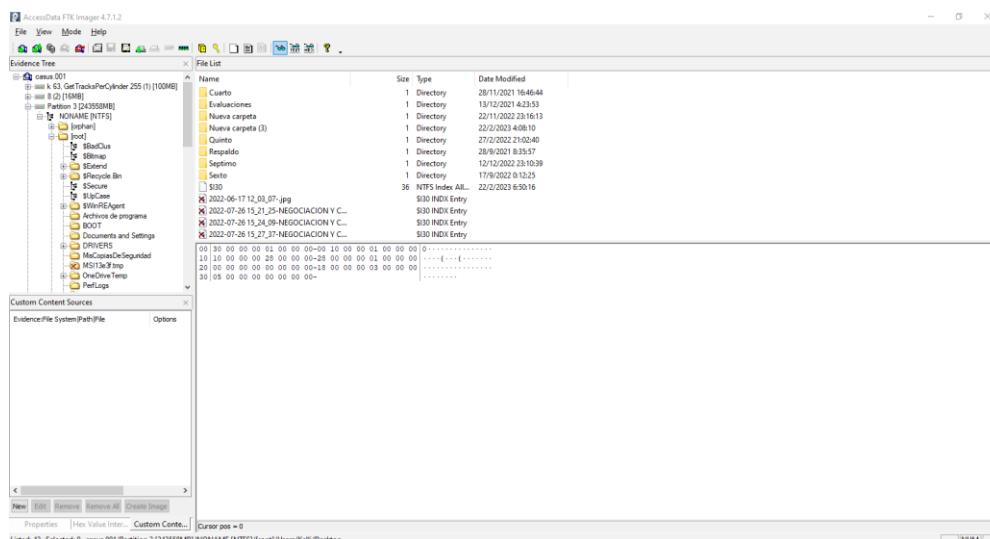


Figura 3.15 Información mostrada dentro de la imagen forense del disco duro

AUTOPSY

La herramienta *Autopsy* es una herramienta de análisis de imágenes forenses, así como de recuperación de datos, se han utilizado las imágenes forenses obtenidas con anterioridad ya que *Autopsy* no cuenta con herramientas para la creación de estas. Al añadir las imágenes al *software* este comenzó con el análisis de la información, a diferencia que otras herramientas *Autopsy* ofrece una interfaz intuitiva y varios apartados, entre ellos la búsqueda de palabras claves o la línea de tiempo que permite identificar los eventos de escritura que se han realizado en la unidad de almacenamiento como se muestra en la Figura 3.16.

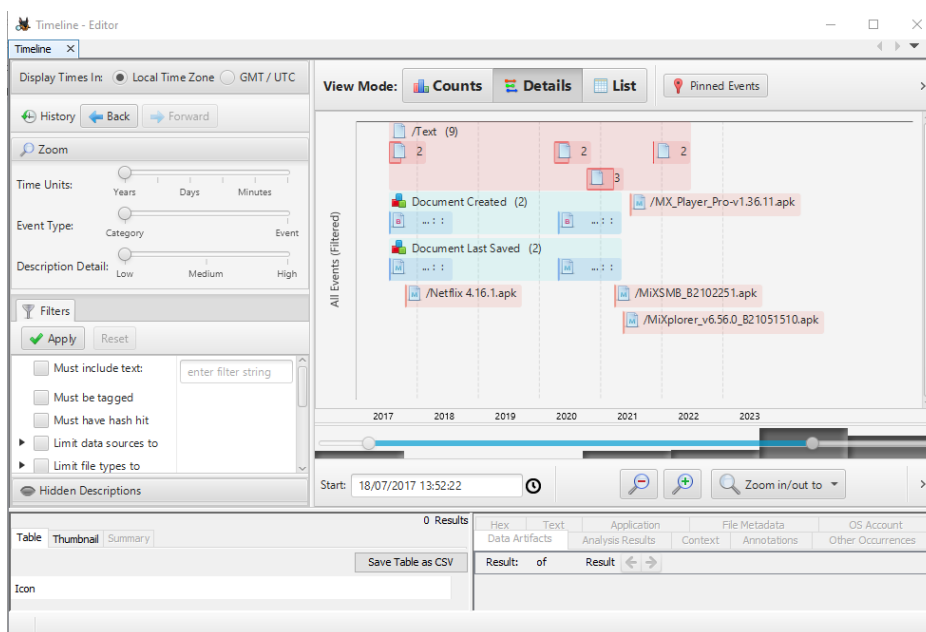


Figura 3.16 Línea de tiempo presentada por la herramienta *Autopsy*

Una vez se ha realizado el análisis de la imagen forense de la memoria microSD y de la memoria USB, se han obtenido los resultados que se pueden observar en la Figura 3.17 y Figura 3.18. El análisis de Autopsy ha arrojado una mayor cantidad de información significativa en comparación a otras opciones, su panel de navegación cuenta con diferentes apartados los cuales permiten al investigador ubicar información específica dentro del disco.

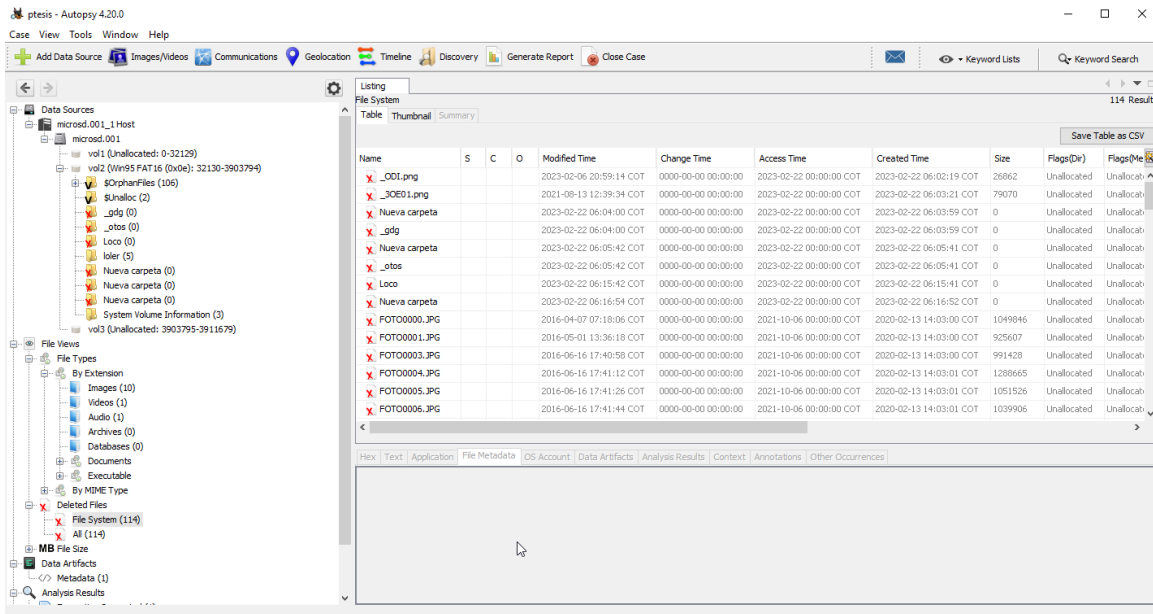


Figura 3.17 Análisis de la imagen forense de la microSD de Autopsy

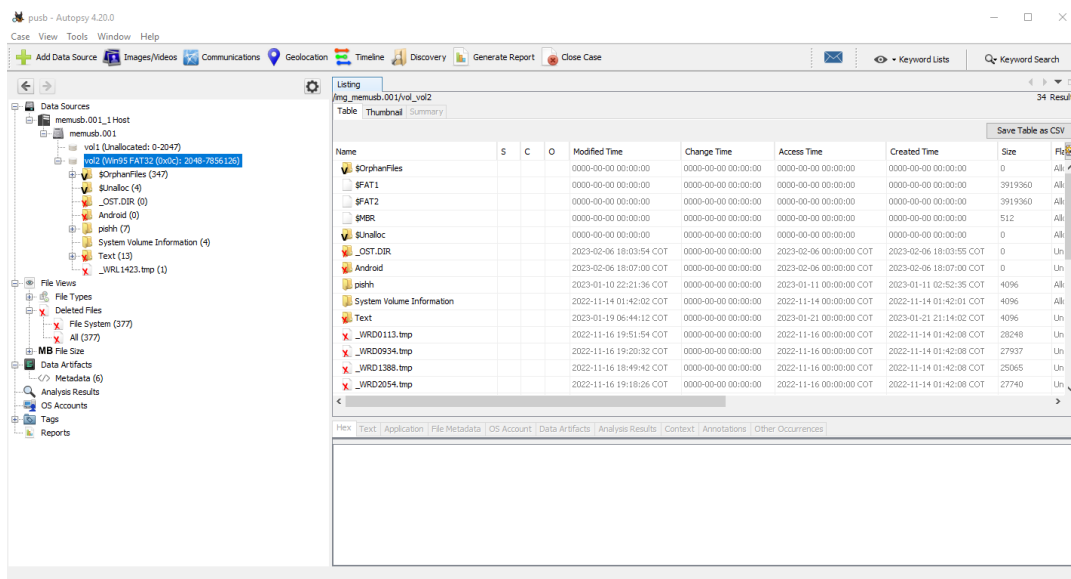
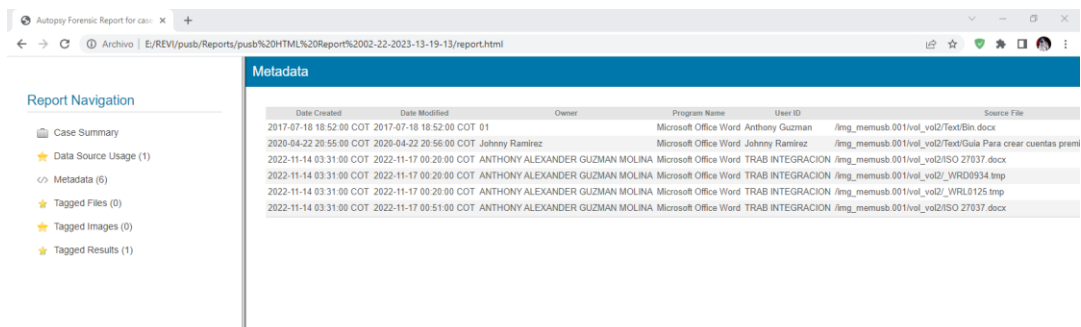


Figura 3.18 Análisis de la imagen forense de la memoria USB de Autopsy

Es importante recalcar que *Autopsy* ha hallado una mayor cantidad de datos borrados huérfanos, por lo cual dependerá además de la experticia del perito encontrar la evidencia digital más relevante para el caso. Por otra parte, haciendo uso de los marcadores se puede generar un informe con los datos más importantes, como se observa en la Figura 3.19.



The screenshot shows a web browser window displaying an Autopsy forensic report. The browser's address bar shows the URL: E:/REV/pusb/Reports/pub%20HTML%20Report%2002-22-2023-13-19-13/report.html. On the left, there is a 'Report Navigation' sidebar with options: Case Summary, Data Source Usage (1), Metadata (6), Tagged Files (0), Tagged Images (0), and Tagged Results (1). The main content area is titled 'Metadata' and contains a table with the following columns: Date Created, Date Modified, Owner, Program Name, User ID, and Source File.

Date Created	Date Modified	Owner	Program Name	User ID	Source File
2017-07-18 18:52:00 COT	2017-07-18 18:52:00 COT	01	Microsoft Office Word	Anthony Guzman	/img_memusb.001/vol2/Text/Bin.docx
2020-04-22 20:55:00 COT	2020-04-22 20:56:00 COT	Johny Ramirez	Microsoft Office Word	Johny Ramirez	/img_memusb.001/vol2/Text/Guia Para crear cuentas premi
2022-11-14 03:31:00 COT	2022-11-17 00:20:00 COT	ANTHONY ALEXANDER GUZMAN MOLINA	Microsoft Office Word	TRAB INTEGRACION	/img_memusb.001/vol2/ISO 27037.docx
2022-11-14 03:31:00 COT	2022-11-17 00:20:00 COT	ANTHONY ALEXANDER GUZMAN MOLINA	Microsoft Office Word	TRAB INTEGRACION	/img_memusb.001/vol2/_WRD0934.tmp
2022-11-14 03:31:00 COT	2022-11-17 00:20:00 COT	ANTHONY ALEXANDER GUZMAN MOLINA	Microsoft Office Word	TRAB INTEGRACION	/img_memusb.001/vol2/_WRL0125.tmp
2022-11-14 03:31:00 COT	2022-11-17 00:51:00 COT	ANTHONY ALEXANDER GUZMAN MOLINA	Microsoft Office Word	TRAB INTEGRACION	/img_memusb.001/vol2/ISO 27037.docx

Figura 3.19 Reporte generado por *Autopsy*

DiskDigger

La herramienta *DiskDigger* es un *software* especializado en la recuperación de datos, a diferencia de otras opciones como *Recuva*, esta herramienta es compatible con imágenes forenses, por lo cual es ampliamente utilizada dentro del campo del análisis forense. *DiskDigger* se utilizó sobre las imágenes generadas con anterioridad utilizando el modo “cavar más profundo” el cual es capaz de encontrar una mayor cantidad de archivos especialmente cuando estos son de un tamaño reducido, se ha optado por esta opción, ya que, en un escenario real evidencias como correos, fotografías o mensajes son las más comunes.

Una vez que se han añadido las imágenes y se ha terminado el proceso de escaneo el *software* ha devuelto una cantidad considerable de archivos recuperables como se muestra en la Figura 3.20 y Figura 3.21. La diferencia más notable, frente a las otras opciones que se han utilizado dentro de este trabajo, es la capacidad de recuperar de manera total una gran cantidad de archivos. Como se puede observar en la Figura 3.22 y Figura 3.23 fue la única herramienta capaz de detectar archivos borrados y recuperarlos.

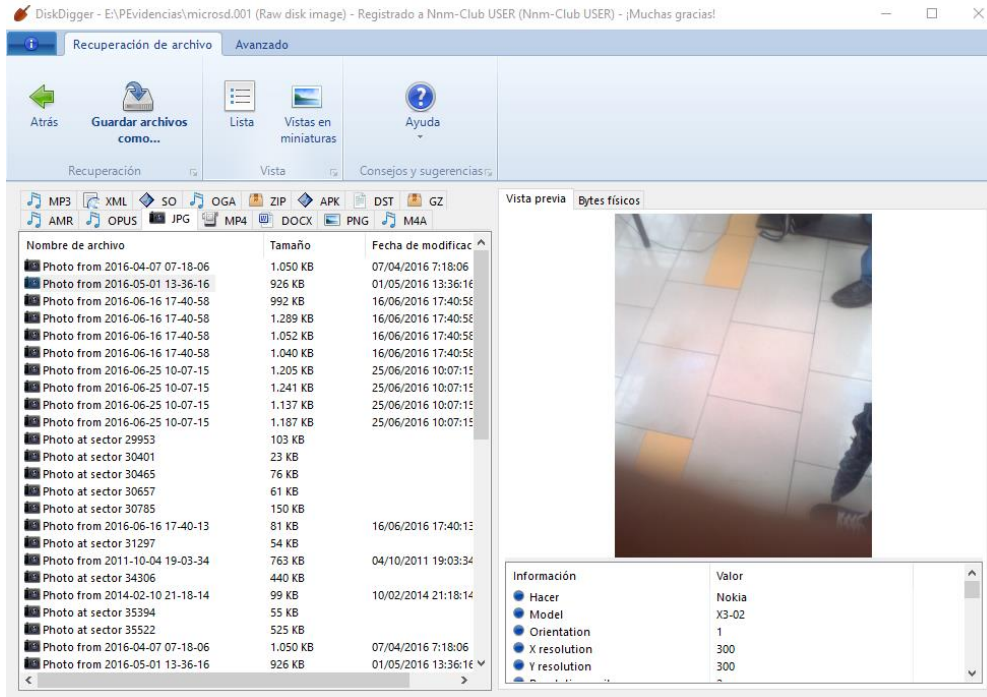


Figura 3.20 Archivos recuperables en la imagen forense de la microSD

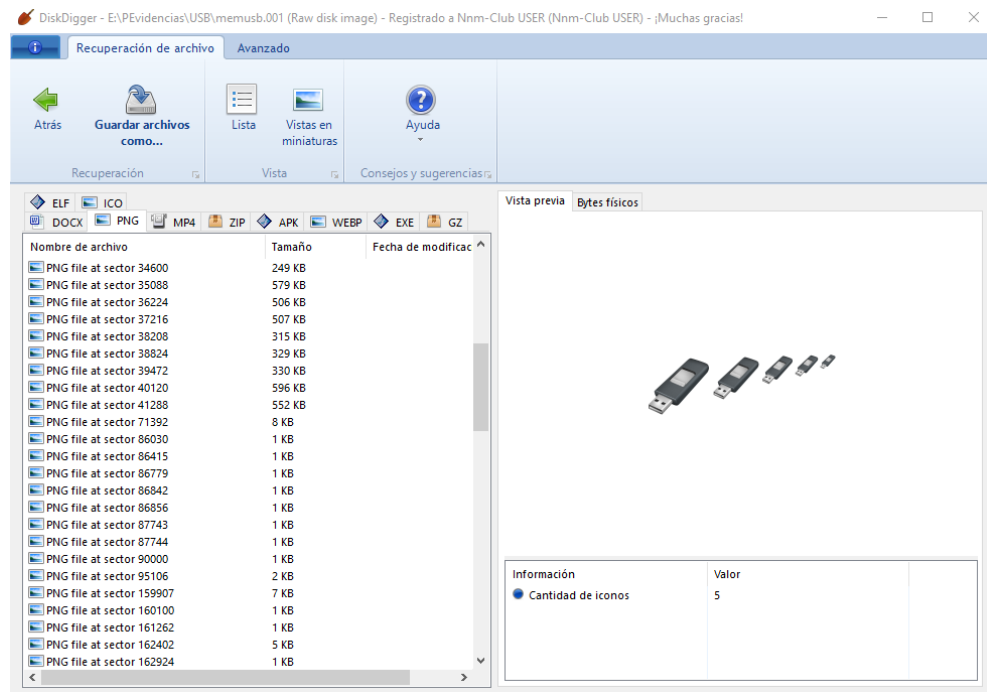


Figura 3.21 Archivos recuperables en la imagen forense de la memoria USB

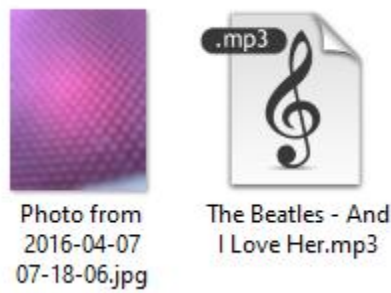


Figura 3.22 Archivos recuperados de la imagen forense de la microSD

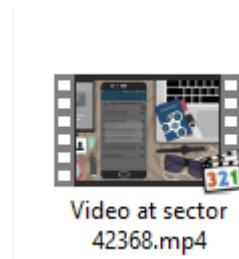


Figura 3.23 Archivos recuperados de la imagen forense de la memoria USB

Por otra parte, también permite al usuario crear un punto de restauración para poder recuperar los archivos sin la necesidad de realizar nuevamente el escaneo de las imágenes, así como de generar un reporte en Excel el cual contiene la información de los datos encontrados durante el análisis, como se observa en las Figura 3.24.

	A	B	C	D		A	B	C	D	
1	DiskDigger Deeper Mode report					1	DiskDigger Deeper Mode report			
2	Saved on 22/02/2023 13:40:42					2	Saved on 22/02/2023 13:47:29			
3	-----					3	-----			
4	Disk information:					4	Disk information:			
5	Model,Raw disk image					5	Model,Raw disk image			
6	Total bytes,2002780160					6	Total bytes,4022337024			
7	Total sectors,3911680					7	Total sectors,7856127			
8	-----					8	-----			
9	File type,Position on disk,Detected file size,Metadata					9	File type,Position on disk,Detected file size,Metadata			
10	JPG,4030976,1049846,Photo from 2016-04-07 07-18-06					10	PNG,9621504,482336,			
11	JPG,5112320,925607,Photo from 2016-05-01 13-36-16					11	PNG,10104832,689137,			
12	JPG,6062592,991428,Photo from 2016-06-16 17-40-58					12	PNG,10797056,705397,			
13	JPG,7078400,1288665,Photo from 2016-06-16 17-40-58					13	PNG,11505664,295980,			
14	JPG,8389120,1051526,Photo from 2016-06-16 17-40-58					14	PNG,11804672,298561,			
15	JPG,9470464,1039906,Photo from 2016-06-16 17-40-58					15	PNG,12103680,296504,			
16	JPG,10519040,1204602,Photo from 2016-06-25 10-07-15					16	PNG,12402688,628250,			
17	JPG,11731456,1240830,Photo from 2016-06-25 10-07-15					17	PNG,13033472,248452,			
18	JPG,12976640,1136509,Photo from 2016-06-25 10-07-15					18	PNG,13283328,578651,			
19	JPG,14123520,1186362,Photo from 2016-06-25 10-07-15					19	PNG,13869056,94176,			
20	JPG,15335936,102094,					20	PNG,13963264,83489,			
21	JPG,15565312,22622,					21	PNG,14049280,40584,			

Figura 3.24 Reportes de los archivos recuperables por *DiskDigger*

Andriller

La herramienta Andriller se especializa en la extracción de datos en equipos con sistema operativo *Android*, el *software* trabaja haciendo uso de las copias de seguridad por lo cual requiere que el equipo tenga activada la “depuración por USB” por lo que si el teléfono se encuentra bloqueado o mantiene esta opción desactivada no se podrá realizar la extracción de ningún tipo de dato.

Al iniciar Andriller se muestra la interfaz principal del programa donde se requiere una ubicación para guardar los datos extraídos, y se presentan tanto en botón de comprobación de conexión, así como el botón de extracción de datos. Entre las opciones presentes antes de realizar la extracción se encuentra la opción de usar el método “*Android Debug Bridge*” ignorando en los procesos el modo “*root*”, así como incluir o no información que se encuentre dentro de la memoria interna del dispositivo.

Al iniciar el proceso de extracción, la herramienta muestra un aviso en el cual se solicita al usuario aceptar la creación de la base de datos en el dispositivo para empezar con la captura de los datos como se puede observar en la Figura 3.25.

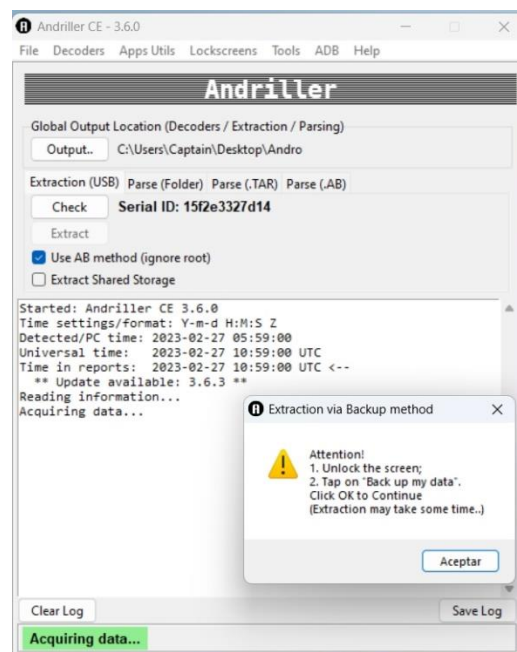


Figura 3.25 Extracción de datos con Andriller

Una vez se ha adquirido los datos en su totalidad Andriller genera un informe reporte en el cual se indican varios parámetros, entre los cuales se pueden encontrar el serial del equipo, el nivel de permiso utilizado, la hora, las cuentas halladas en el dispositivo y el número de archivos extraído de la memoria, en este caso en la Figura 3.26 se puede

ver la información que ha sido obtenida del dispositivo, esta dependerá en gran medida del modelo del equipo, el nivel de acceso y la seguridad del sistema.

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

[Andriller Report]

Type	Data
Serial	15f2e3327d14
Status	device
Permission	root-su
Ro.Product.Manufacturer	Xiaomi
Ro.Product.Model	Redmi 4X
Ro.Build.Version.Release	7.1.2
Ro.Build.Display.Id	N2G47H
Wifi Mac	18:f0:e4:39:64:7c
Local_Time	2023-02-27 05:48:38 Hora est. Pacífico, Sudamérica
Device_Time	2023-02-27 05:48:41 ECT
Accounts	<ul style="list-style-type: none"> • com.google: susimolina***gmail.com • com.whatsapp: Wha***pp • com.mgoogle: susimolina***gmail.com • com.zhilioapp.musically: Ti***k
Application	Shared Storage (0)
Application	Android Calendar (0)

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

Figura 3.26 Reporte generador por Andriller de los datos extraídos

Al finalizar con la fase de análisis forense se procede a realizar el respectivo informe pericial, en el caso del Ecuador el perito debe basarse en el formato de informe policial proporcionado por el Consejo de la Judicatura disponible en la página de la función judicial. Finalmente se deberá justificar de manera oral dentro del proceso legislativo las conclusiones a las cuales se ha llegado.

4 CONCLUSIONES

- Las normativas con mayor aceptación de manera parcial o total a nivel internacional son la ISO 27037 y la RFC 3227, la relevancia del contenido expuesto en estas permite que actualmente sigan vigentes complementándose a metodologías y adaptándose a las normativas legales de cada país para su uso.
- En el Ecuador no existe ningún tipo de normativa para la extracción de la evidencia digital implementada dentro de su legislación, debido al avance progresivo de las TICS esto viene a constituir una situación preocupante para el país, haciendo que Ecuador se mantenga relegado en términos de seguridad

informática con relación a otros países incluso de la región, lo cual será más evidente con el paso de los años.

- A nivel internacional la metodología con mayor adopción es la UNE 71506, la cual define las fases desde la adquisición hasta la presentación de la evidencia. A pesar de la acogida que tiene, esta metodología ha sido en su mayoría adoptada de manera parcial, ya que, países como España o Argentina la han combinado con otras normativas o recomendaciones haciendo que esta se adapte a la legislación de cada país. De la misma manera propuestas independientes para guías metodológicas la toman como referencia para su desarrollo.
- El Ecuador no cuenta con una metodología aceptada para el peritaje informático dentro de su legislación, contemplando únicamente parámetros básicos como la cadena de custodia o definiendo artículos concernientes a la protección de la información digital. Aun así, el país cuenta con una amplia propuesta de guías metodológicas basadas en las principales normativas y metodologías internacionales contando además con la reputación de expertos en la materia, los cuales han desarrollado guías apegadas a la legislación ecuatoriana enfocadas a todo tipo de dispositivos que pueden ser usadas como referencia en otros territorios.
- A pesar de que las normativas y metodologías exponen pautas y parámetros que deben considerarse durante todos los procesos llevados a cabo, ninguna guía presenta en su totalidad cada uno de los pasos que el perito informático debe llevar a cabo dado la inmensa variedad de situaciones que pueden presentarse. Por lo cual se debe considerar en gran medida la experticia del investigador encargado del caso.
- Se ha expuesto varias situaciones en las cuales puede ser extraída la evidencia digital y por esta misma razón se han analizado diferentes herramientas, algunas enfocadas a un solo tipo de dispositivo y otras que cuentan con paquetes completos para todo tipo de requerimientos. Escoger la herramienta adecuada de acuerdo a la situación, requiere de experiencia, ya que como se pudo evidenciar durante la aplicación de estas, a pesar de ser utilizadas para el mismo propósito pueden no responder de manera adecuada al cambiar de dispositivos.

Con esto se puede concluir que una única herramienta no puede ser capaz de garantizar la extracción de toda la información que el perito busque obtener, por lo que se requiere siempre mantener varias opciones incluso al realizar una misma tarea.

- Las herramientas para la extracción de evidencia digital cuentan con una inmensa variedad, incluso por el costo de estas. Por lo cual se debe tomar en cuenta que a pesar de que existen varias opciones gratuitas capaces de realizar procedimientos similares a una herramienta de pago, el soporte y sencillez obtenida de las opciones de pago es superior, haciendo que en muchos casos sea necesario optar por pagar, para poder obtener evidencias relevantes para el caso.

5 RECOMENDACIONES

- El uso de las herramientas disponibles para la extracción de evidencia digital en su mayoría requiere de una computadora con especificaciones técnicas altas, por lo cual se recomienda que entre mayores capacidades tenga la herramienta a ser utilizada la computadora deberá contar con las mejores características en lo que respecta a *hardware*.
- Al analizar dispositivos con tamaños de almacenamiento pequeños estos no presentan un mayor uso de recursos haciendo que el tiempo empleado no sea tan significativo incluso cuando se realiza una búsqueda general. Mientras que al analizar unidades de almacenamiento de mayor capacidad, dado que estos presentan una cantidad inmensa de archivos, es necesario que el perito conozca la información en la cual debe centrar la búsqueda incluso antes de empezar.
- En base a la investigación realizada, durante el peritaje informático se recomienda de manera indispensable tomar varias fuentes como referencia, dado que cada una de las guías metodologías toman diferentes perspectivas incluso en las mismas situaciones, por lo cual considerar todos estos aspectos durante el peritaje podría significar la obtención de mejores resultados.

- El conocer tanto acerca de la legislación ecuatoriana, así como de los casos relevantes sobre delitos informático antes de realizar un peritaje, puede marcar la diferencia entre garantizar la validez de las evidencias o que estas sean desechadas.

6 REFERENCIAS BIBLIOGRÁFICAS

- [1] C. Pazan, «3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020», *El Comercio*, 25 de julio de 2022. <https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html> (accedido 27 de febrero de 2023).
- [2] «Méndez - FISCALÍA GENERAL DEL ESTADO COMITÉ EDITORIAL.pdf». Accedido: 27 de febrero de 2023. [En línea]. Disponible en: <https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf>
- [3] «Crónica de un hackeo: ¿para qué y cómo se lo hizo? | Plan V». <https://www.planv.com.ec/historias/cronica/cronica-un-hackeo-que-y-como-se-lo-hizo> (accedido 27 de febrero de 2023).
- [4] «Ecuador bank's suit against Wells Fargo over cyber heist can go forward: ruling | Reuters». <https://www.reuters.com/article/us-wells-fargo-banco-del-austro-ruling-idUSKCN12J03J> (accedido 27 de febrero de 2023).
- [5] «Mafia interna vulneró sistema informático para escoger jueces a su gusto», *Primicias*. <https://www.primicias.ec/noticias/en-exclusiva/mafia-sorteos-judicatura-sistema-jueces/> (accedido 27 de febrero de 2023).
- [6] «Temas penales 3.pdf». Accedido: 27 de febrero de 2023. [En línea]. Disponible en: https://www.cortenacional.gob.ec/cnj/images/Produccion_CNJ/temas%20penales/Temas%20penales%203.pdf
- [7] D. D. S. Méndez, «FISCALÍA GENERAL DEL ESTADO COMITÉ EDITORIAL».
- [8] «La Unidad de Ciberdelito conmemora su 11vo aniversario de servicio a la ciudadanía – Policía Nacional del Ecuador». <https://www.policia.gob.ec/la-unidad-de-ciberdelito-conmemora-su-11vo-aniversario-de-servicio-a-la-ciudadania/> (accedido 27 de febrero de 2023).

- [9] «DSpace de Uniandes: Identificador inválido». <https://dspace.uniandes.edu.ec/bitstream/123456789/11653/1/TUBEXCOMAB023> (accedido 27 de febrero de 2023).
- [10] «Manual de Manejo de Evidencias Digitales y Entornos Informáticos».
- [11] V. L. Vivas, «ESTADO DEL PERITAJE INFORMÁTICO DE LA EVIDENCIA DIGITAL EN EL MARCO DE LA ADMINISTRACIÓN DE LA JUSTICIA EN COLOMBIA», 2017.
- [12] A. F. G. Molina, «GUÍA METODOLÓGICA PARA EL PERITAJE INFORMÁTICO APLICADO A LOS LABORATORIOS DE COMPUTACIÓN DE LA UNIVERSIDAD TECNOLÓGICA “INDOAMÉRICA”».
- [13] «Aprobaron la “Guía de obtención, preservación y tratamiento de evidencia digital” | Ministerio Público Fiscal». <https://www.mpf.gob.ar/blog/gils-carbo-aprobo-la-guia-de-obtencion-preservacion-y-tratamiento-de-evidencia-digital/> (accedido 27 de febrero de 2023).
- [14] «ISO 27037 Directrices de gestión de evidencias electrónicas – Evidencias electrónicas». <http://foro evidencias electronicas.org/iso-27037-directrices-de-gestion-de-evidencias-electronicas/> (accedido 27 de febrero de 2023).
- [15] «Norma para recopilación de evidencias – Servicio de Acreditación Ecuatoriano». <https://www.acreditacion.gob.ec/norma-para-recopilacion-de-evidencias/> (accedido 27 de febrero de 2023).
- [16] «Directrices RFC 3227 - Ciberforensic». <https://www.ciberforensic.com/directrices-rfc-3227> (accedido 27 de febrero de 2023).
- [17] P. Informático, «ISO 71505/2013 .Sistema de Gestión de Evidencias Electrónicas», *GlobátiKa Peritos Informáticos*, 23 de febrero de 2021. <https://peritosinformaticos.es/iso-71505-2013-perito-informatico/> (accedido 27 de febrero de 2023).
- [18] P. Informático, «ISO 71506/2013. Metodología para el análisis forense de las evidencias electrónicas.», *GlobátiKa Peritos Informáticos*, 23 de febrero de 2021. <https://peritosinformaticos.es/iso-71506-2013-perito-informatico/> (accedido 27 de febrero de 2023).
- [19] F. J. M. Quimí, «LA LIBERTAD – ECUADOR».
- [20] «ISO/IEC 30121:2015(en), Information technology — Governance of digital forensic risk framework». <https://www.iso.org/obp/ui/es/#iso:std:iso-iec:30121:ed-1:v1:en> (accedido 27 de febrero de 2023).

- [21] «COIP_act_feb-2021.pdf». Accedido: 27 de febrero de 2023. [En línea]. Disponible en: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- [22] R. A. Proaño-Escalante, A. F. Gavilanes-Molina, R. A. Proaño-Escalante, y A. F. Gavilanes-Molina, «Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana», *Enfoque UTE*, vol. 9, n.º 1, pp. 90-101, mar. 2018, doi: 10.29019/enfoqueute.v9n1.229.
- [23] «PGN-0756-2016-001.pdf». Accedido: 27 de febrero de 2023. [En línea]. Disponible en: <https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf>
- [24] «Repositorio de la Universidad Internacional SEK Ecuador: Identificador inválido». <https://repositorio.uisek.edu.ec/bitstream/123456789/4020/1/Valencia%20Sasil%2> (accedido 27 de febrero de 2023).
- [25] «UNE 71506:2013 Tecnologías de la Información (TI). Metodología...» <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051414> (accedido 27 de febrero de 2023).
- [26] «Estándares nacionales e internacionales que puede seguir un perito informático para realizar el análisis forense de una evidencia y para la elaboración de un peritaje informático». <https://peritoinformaticocolegiado.es/blog/estandares-nacionales-e-internacionales-que-puede-seguir-un-perito-informatico-para-realizar-el-analisis-forense-de-una-evidencia-y-para-la-elaboracion-de-un-peritaje-informatico/> (accedido 27 de febrero de 2023).
- [27] «Fiscalía General del Estado | Página no encontrada». https://www.fiscalia.gob.ec/wp-content/uploads/2014/08/files_archivos%20AC_COIP%20073%20FGE_Area (accedido 27 de febrero de 2023).
- [28] B. G. L. Cajamarca, «DECLARACION JURAMENTADA».
- [29] «71. 1390-9304 GRIJALVA JUAN 2017.pdf». Accedido: 27 de febrero de 2023. [En línea]. Disponible en: <https://repositorio.uisek.edu.ec/bitstream/123456789/2991/1/71.%201390-9304%20GRIJALVA%20JUAN%202017.pdf>
- [30] «FTK Imager», *Exterro*. <https://www.exterro.com/ftk-imager> (accedido 27 de febrero de 2023).
- [31] «TFM_Fernán dez_Maceira_2021.pdf». Accedido: 27 de febrero de 2023. [En línea]. Disponible en:

- https://ebuah.uah.es/dspace/bitstream/handle/10017/49565/TFM_Fern%C3%A1n%20dez_Maceira_2021.pdf?sequence=1&isAllowed=y.%20
- [32] E. Y. A. Meneses y E. F. Jaramillo, «Programa Académico Ingeniería de Sistemas».
- [33] «opsy | Digital Forensics», *Autopsy*. <https://www.autopsy.com/> (accedido 27 de febrero de 2023).
- [34] «Download Recuva | Recover deleted files, free!» <https://www.ccleaner.com/es-es/recuva> (accedido 27 de febrero de 2023).
- [35] «4DDiG-Windows/Mac Recuperación de Datos». https://www.4ddig.net/es/ads/4ddig-data-recovery.html?gclid=EAlaIqobChMI7YeU2NuT_QIVB9DtCh3UtgttEAAYASAAEgJSkvD_BwE%C3%A7 (accedido 27 de febrero de 2023).
- [36] «Análisis forense», *Ciberseguridad*. <https://ciberseguridad.com/servicios/analisis-forense/> (accedido 27 de febrero de 2023).
- [37] «Oxygen Forensics - Mobile forensic solutions: software and hardware». <https://www.oxygen-forensic.com/es/> (accedido 27 de febrero de 2023).
- [38] «Acquire Memory with MAGNET RAM Capture». <https://support.magnetforensics.com/s/article/Acquire-Memory-with-MAGNET-RAM-Capture> (accedido 27 de febrero de 2023).
- [39] D. Sazonov, «Andriller CE (Community Edition)». 26 de febrero de 2023. Accedido: 27 de febrero de 2023. [En línea]. Disponible en: <https://github.com/den4uk/andriller>

7 ANEXOS

ANEXO I: CERTIFICADO DE ORIGINALIDAD

CERTIFICADO DE ORIGINALIDAD

Quito, D.M. 28 de febrero de 2023

De mi consideración:

Yo, GABRIELA KATHERINE CEVALLOS SALAZAR, en calidad de Director del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL asociado al proyecto IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL elaborado por el estudiante ANTHONY ALEXANDER GUZMAN MOLINA de la carrera en TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES, certifico que he empleado la herramienta Turnitin para la revisión de originalidad del documento escrito completo producto del Trabajo de Integración Curricular indicado.

El documento escrito tiene un índice de similitud del 18%.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente documento para los trámites de titulación.

NOTA: Se adjunta el informe generado por la herramienta Turnitin.

LINK:

https://epnecuador-my.sharepoint.com/:b/g/personal/gabriela_cevalloss_epn_edu_ec/EedZbNnWNapMnTz-AZEBqMUBNVQL9NWHQbpkeoFk1LthzQ?e=gf9A1i

Atentamente,



GABRIELA KATHERINE CEVALLOS SALAZAR

Docente

ESFOT

ANEXO II: ENLACES

Anexo II.I Código QR de la implementación y pruebas de funcionamiento

