UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACUTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

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

AUTOR

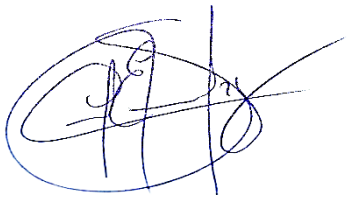
FREDDY JOSÉ MIRABÁ QUIMÍ

LA LIBERTAD – ECUADOR
2021

APROBACIÒN DEL TUTOR

En mi calidad de tutor del trabajo de componente práctico del examen de carácter complexivo: “DISEÑO DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL TOMANDO COMO BASE EQUIPOS CON EL SISTEMA OPERATIVO WINDOWS 8.1”, elaborado por el sr. Mirabá Quimí Freddy José, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

La Libertad**,** 18 de agosto del 2021

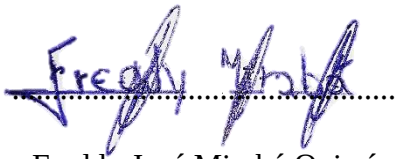


……..

Ing. Carlos Sánchez León, Mgt

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Freddy José Mirabá Quimí

AGRADECIMIENTO

Primero agradecer a Dios, por ser el ser supremo que guía cada uno de mis pasos y darme las fuerzas suficientes para seguir en la lucha de alcanzar mi meta de ser un profesional.

A mis docentes, por tener la pasión de impartir cada una de sus cátedras y ser esas personas que nos preparan no solo profesional, sino también personalmente, en especial aquellos tutores del presente trabajo realizado, gracias por la paciencia y guía.

A mis compañeros de clases, que dentro de las aulas siempre hubo el respeto y las palabras de aliento necesarias para juntos cumplir con esta meta, especialmente a aquellos con los que se ha logrado formar una linda amistad, dándonos la motivación necesaria para no rendirnos en el camino.

A la Universidad Estatal Península de Santa Elena, por permitir abrir sus puertas y lograr formarme profesionalmente.

Freddy José Mirabá Quimí

DEDICATORIA

A Dios por bendecirme y darme la oportunidad de seguir viviendo cada día y llegar a cumplir esta meta.

A mi Señora madre, Geoconda Quimí Parra, por haberme guiado por el camino del bien, por ser el pilar fundamental en mi formación como profesional, y ser la persona que me ha dado las fuerzas necesarias para seguir adelante, brindándome siempre su amor y apoyo incondicional en cada momento.

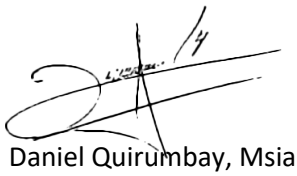
A mi padre, que se que desde el cielo bendice, cuida y guía cada uno de mis pasos.

A mis familiares que de alguna forma han aportado con su granito de arena y me han dado las fuerzas y la confianza necesaria que se necesita para lograr esta importante meta.

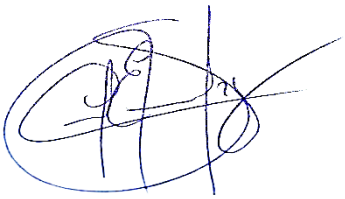
Freddy José Mirabá Quimí

TRIBUNAL DE GRADO

Ing. Washington Torres Guin, Mgt
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN



Ing. Daniel Quirumbay, Msia
DOCENTE ESPECIALISTA



Ing. Carlos Sánchez León, Mgt
DOCENTE TUTOR

Ing. Alicia Andrade Vera, Mgt
DOCENTE GUÍA UIC

RESUMEN

Dentro de la presente propuesta tecnológica se apreciará el diseño de una guía metodológica para el análisis forense digital, en base a un sistema operativo, para su elaboración se ha establecido el uso de las cinco fases principales de la metodología UNE 71506:2013, la cual es considerada para el uso de extracción de evidencias digitales, mediante la designación e implementación de software de código abierto y mostrando las diferentes herramientas que se puedan usar y el cómo hacerlo, teniendo así el paso a paso del proceso de creación de una copia de un disco duro, que recibe el nombre de imagen forense, posterior análisis y extracción de evidencia digital.

La guía estará elaborada para personas que tengan el conocimiento básico de informática forense que se deseen preparar en este ámbito, así mismo en la fase de documentación, se tendrá un ejemplo de informe pericial, el cual va a contener la información y los datos obtenidos en la recolección de la información basado en un caso de estudio, mostrando los diferentes tipos de evidencias que se puedan encontrar con el uso del software establecido.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

LISTA DE ANEXOS

INTRODUCCIÓN

La presente guía de análisis forense digital será elaborada en base a un sistema operativo Windows 8.1 por esta razón se puede usar de manera general al Sistema Operativo Windows, no es una guía de sistemas embebidos, memorias volátiles o de red, se ha tomado como referencia principal la metodología UNE 71506:2013 con sus cinco fases principales que son reservadas para realizar un correcto proceso de extracción de evidencias.

Se ha establecido el uso de software de código abierto, y el paso a paso de usarlos, tomando en cuenta las diferentes fases de la metodología establecida, dichos pasos serán plasmados dentro del capítulo tres que es donde estará el proceso de su elaboración, posteriormente, se encontrará un ejemplo de informe pericial, donde se plasmará los diferentes datos obtenidos, así mismo se hallará los puntos más esenciales para elaborarlo.

Dicha guía permitirá a los peritos informáticos que se están preparando en este ámbito a obtener un conocimiento del proceso de extracción de evidencias digitales, el uso de las diferentes herramientas será funcionales hacia el sistema operativo Windows, el correcto o mal uso y actualización de las herramientas dependerán del equipo y de la persona que haga el uso de ellas.

CAPÍTULO 1

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

En la actualidad existe poco acceso a guías de análisis forense en base a equipos con un Sistema Operativo, por ende, hay una falta de conocimientos técnicos para la respectiva extracción de diferentes tipos de evidencias que podrían ser usadas para un caso en donde se vería involucrada la extracción de evidencia digital, todo se está digitalizando y por ende la evidencia en papel o en este caso escrito está siendo cada vez más escasa [1].

La delincuencia informática mundial causa un perjuicio de 114 mil millones de dólares anuales, según estudios se determinó que más de dos tercios de adultos en línea (69%) han sido víctimas de ciberdelincuencia alguna vez en la vida [2].

La falta de una guía metodología para el análisis forense digital en base a equipos con S.O Windows 8.1 tiene la desventaja de que al momento de existir un caso, no se tenga un cierto grado de conocimiento en cuanto a un análisis, sea este realizado por el perito informático a cargo, o en su caso a la interpretación de un fiscal o la persona que esté llevando este proceso de manera judicial, puesto que existirían diferentes tipos de datos por analizar, si se trata de alguna situación en particular. El escenario de existir un vacío de conocimiento en el ámbito forense digital tendría la desventaja de que los datos encontrados hayan sido en vano, existiendo la posibilidad de no saber qué hacer con ellos.

Mediante una entrevista realizada hacia un profesional del peritaje informático, teniendo un intercambio de ideas, se ha llegado a la conclusión que, para hacer este tipo de manual de análisis digital forense, se debe hacer una gran recolección de información, puesto que este tipo de procesos tiene un nivel de complejidad alto, por el motivo de que no existe mucho material para la elaboración de una guía, esto se debe a que se han hecho de manera muy general al Sistema Operativo Windows. Definir el tipo de metodología por aplicar, los posibles incidentes que se llegaran a encontrar y la elaboración de la guía misma, serían los pilares fundamentales para su correcta realización [3].

En la Universidad Autónoma de Barcelona en España, uno de los trabajos de titulación de masterado fue: Análisis forense en entornos Windows, que uno de sus objetivos fue extraer evidencias posibles tras un incidente de seguridad y para la realización de este fue

de suma importancia seguir diferentes tipos de métodos de recolección de datos, condicionados mayormente en las evidencias propuestas para la extracción de las mismas siguiendo estándares relacionados a la seguridad digital [4].

En Argentina en la Universidad de Morón, se desarrolló una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto, que comprende en la utilización de herramientas informáticas para la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para dañar individuos, organizaciones, empresas o a la sociedad en general [5].

En nuestro país en la Universidad Internacional SEK, uno de los temas para la maestría en tecnologías de la información fue: Desarrollo de una guía metodológica para el análisis forense en equipos de cómputo con Sistema Operativo Mac OS X en el Ecuador, llevando a cabo un análisis a equipos de cómputo con un sistema operativo no tan visto comercialmente en el país, puesto que hay muy pocas personas u organizaciones que deciden trabajan en un ambiente de Mac [1].

A partir de la recolección de información, metodología, herramientas, artículos y demás datos se procederá a realizar una guía metodológica para el análisis forense en base a equipos con S.O Windows 8.1 que facilitará tanto a un analista de peritaje informático, como a un fiscal o en su caso a la sociedad en general que deseen tener el conocimiento del proceso que ocurre al momento de extraer información digital.

1.2 DESCRIPCIÓN DEL PROYECTO.

Se propone realizar una guía metodológica para el análisis forense digital tomando como base equipos con Sistema Operativo Windows 8.1 para personas que tengan un conocimiento básico en el peritaje informático, o en su caso a la sociedad que desee obtener el conocimiento necesario y se sienta atraída en saber el proceso de la recolección de información digital.

Para la elaboración de esta guía metodológica se tomará en cuenta unos factores muy importantes que son establecer la metodología a usar para su elaboración, definir las diferentes herramientas (hardware y software) a utilizar para la recolección de la información, tomando en cuenta la lectura de los artículos que estén relacionados a la informática forense.

El presente documento tendrá las siguientes fases a realizar basado en la metodología UNE 71506:2013.

Fase de Preservación.

- Garantizar la no perdida de las evidencias.
- Verificar el equipo o elementos a analizar.
- Mantener una validez jurídica de las evidencias recopiladas, solo si es necesario.
- Evitar que la información sea alterada, dañada o manipulada ya sea por causas humanas o naturales.

Fase de Adquisición.

- Recopilación de las evidencias físicas o digitales.
- Verificar la autenticidad del equipo a analizar.
- Obtener las diferentes herramientas (hardware y software) para la recopilación de la información.
- Realización de una copia de la evidencia encontrada.

Fase de Análisis.

- Hacer el uso de las herramientas para el análisis forense.
- Escoger el método de investigación a ser aplicado.

- ❖ Evitar comprometer la integridad de la información extraída de las evidencias.

Fase de Documentación.

- ❖ Documentar en un informe pericial los datos obtenidos durante el proceso de extracción de las evidencias.
- ❖ Evidenciar el proceso realizado mediante fotografías o capturas de pantalla.
- ❖ En el informe pericial, plasmar las conclusiones del proceso realizado.

Fase de Presentación.

- ❖ Presentar los resultados obtenidos del análisis forense.
- ❖ Realizar una presentación convincente y entendible, detallando las diferentes herramientas y metodologías usadas durante el proceso.
- ❖ Detallar las conclusiones expuestas en la fase de documentación.

Para la elaboración de la guía es necesario reconocer las herramientas que se puedan usar para la recopilación de la información; entre ellas estarían las siguientes.

Autopsy: Es la principal plataforma forense digital de código abierto de extremo a extremo. Construido por la tecnología Basis con las características principales que se espera en las herramientas forenses comerciales. Autopsy es una solución de investigación de disco duro-rápida, exhaustiva y eficiente que evoluciona según sus necesidades [6].

Caine: Un Sistema Operativo de una distribución de GNU/Linux, que ofrece un entorno forense completo que se organiza para integrar las herramientas de software existentes como módulos de software y para proporcionar una interfaz gráfica amigable [7].

Forensic Toolkit (FTK): Es una herramienta de imágenes y vista previa de datos que permite evaluar rápidamente la evidencia electrónica para determinar si se justifica un análisis adicional con una herramienta forense. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos informáticos sin realizar cambios en la evidencia original [8].

Kali Linux: Está basada en Debian, y fue diseñada principalmente para la auditoria y seguridad informática en general, sin embargo, cuenta con una serie de herramientas preinstaladas para análisis forense [9].

Hélix live CD: Es una solución de seguridad cibernética que proporciona respuestas a incidentes, análisis forenses informáticos y e-discovery en una interfaz fácil de usar [10].

VMware Workstation 15.5 Pro: Es un hipervisor de escritorio estándar del sector para ejecutar máquinas virtuales en PC con Linux o Windows [11].

DiskDigger: Esta herramienta recupera archivos perdidos de un disco duro, tarjetas de memoria, unidades flash USB, también tiene la facilidad de hacer este mismo proceso hacia una imagen forense [12].

El proyecto contribuirá a la línea de investigación de seguridad de la información, puesto a que ayuda a la toma de decisiones mediante una recopilación de información exhaustiva, garantizando un soporte de decisiones en tiempo real hacia las diferentes personas que puedan hacer uso de este.

1.3 OBJETIVOS DEL PROYECTO.

1.3.1 OBJETIVO GENERAL.

Elaborar una guía para el análisis forense tomando como base equipos de SO Windows 8.1, mediante el uso de la metodología UNE 71506:2013 y herramientas de análisis forense digital, para demostrar el proceso de extracción de evidencia digital.

1.3.2 OBJETIVOS ESPECÍFICOS.

- Aplicar la información de las fases de la metodología UNE 71506:2013 para tener un buen manejo de la evidencia digital durante el análisis.

- Seleccionar las diferentes herramientas de código abierto (open source) que sirvan de ayuda al momento de realizar el proceso de búsqueda del análisis forense digital.

- Desarrollar una guía metodológica para análisis forense digital, siguiendo el proceso de cada una de las fases de la metodología establecida UNE 71506:2013.

- Mostrar un ejemplo de informe pericial en el que se evidencia los resultados obtenidos, en base a la fase de documentación.

1.4 JUSTIFICACIÓN DEL PROYECTO.

Actualmente existen diferentes escenarios en donde la información de una persona ha sido comprometida, un equipo de cómputo o una herramienta informática se llega a convertir en una gran ayuda para los Peritos Informáticos que buscan información de un caso en especial [1]. Esta guía servirá de gran ayuda al momento de querer saber cómo obtener información necesaria de un equipo con S.O Windows.

El Código Orgánico Integral Penal (COIP) actualmente vigente presenta una sección de artículos donde se identifican diferentes delitos más comunes que suceden en el país, sin embargo, muchos de estos delitos no son cubiertos en dicho escrito [13]. Partiendo de esta idea se realizará un manual con diferentes puntos a tomar en cuenta para el respectivo análisis digital forense a equipos de cómputo considerando los diferentes puntos tratados en el COIP en cuanto a equipos informáticos.

Se proporcionará información relacionada al análisis forense digital, tomando como base al sistema operativo Windows 8.1, anteriormente se han realizado pruebas sobre el Sistema Operativo Windows XP, tomando una cantidad de evidencias que en su caso pueden ser utilizadas al SO Windows en general, puesto que su estructura es bastante similar.

La realización de la presente guía metodológica de análisis forense a equipos de cómputo tiene como beneficiarios directos a las personas que se desean preparar al peritaje informático, puesto que sería de una gran ayuda contar con los diferentes conocimientos que vaya a obtener al momento de analizar el trabajo a realizarse.

Los jueces o fiscales serian beneficiaros indirectos, porque de esta manera tendrían una base de conocimiento de cómo fue el proceso de la extracción de evidencia de los peritos informáticos de algún caso en especial que se esté tratando, puesto que ellos no tienen tanto conocimiento en la extracción de información, y de esta manera puedan dar una sentencia en base a su conocimiento de los diferentes artículos de las leyes y especialmente del peritaje informático.

La sociedad en general también serían los beneficiarios indirectos, teniendo en sus manos a una guía de cómo es el proceso de análisis digital forense, de cierta manera tendrían el

conocimiento básico de cómo es o fue el proceso, y de esta forma se pueda defender delante de un tribunal si este fuera el caso.

Cabe recalcar que la presente investigación a desarrollar es de tipo experimental y documental, mediante la recolección de información de diferentes fuentes bibliográficas y aprendizaje durante la realización de esta, serán necesarias para poder sustentar la información sustraída mediante el análisis digital.

El análisis forense digital de equipos informáticos permite de cierta manera buscar y encontrar una solución de diferentes tipos de conflictos o casos relacionados a la seguridad informática y en su caso a la protección de los datos de una persona o entidad. Gracias a este tipo de análisis las personas o entidades obtienen una respuesta en cuanto a la privacidad de sus datos, el robo de información, espionaje, fraude entre otros tipos de ataques informáticos, pueden ser resueltos mediante este tipo de análisis forense digital [14].

Se pretende mediante esta guía garantizar la integridad y confidencialidad, estas serán las bases primordiales para la correcta realización del escrito, aplicando de manera correcta las diferentes herramientas de análisis forense.

El tema propuesto está alineado a los objetivos del Plan Nacional de Desarrollo, específicamente al eje:

Eje 2.- Economía al servicio de la sociedad

Objetivo 5.- Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [15].

Política 5.6.- Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades [15].

1.5 ALCANCE.

La elaboración de esta guía metodológica de análisis forense tomando como base equipos con Sistema Operativo Windows 8.1, permitirá obtener un nivel de conocimiento del análisis digital forense, hacia las personas que estén dispuestas a indagar el proceso de recopilación de evidencias, mejorando y guiando un análisis exhaustivo.

Este presente proyecto garantizará la recopilación de información del mayor porcentaje del contenido de un disco duro de un equipo por analizar, los datos más importantes que podrían servir como evidencia de un caso en específico, estos serían; imágenes, documentos o cuadros de texto, videos, etc. Las personas que vayan a hacer uso de ella deberían tener un pequeño margen de conocimiento del análisis forense digital, esta guía mostrará las cinco fases de la metodología UNE 71506:2013 donde las personas que sientan la curiosidad de saber el proceso de recolección de información vean los pasos a realizar.

También sirve de base para la recopilación de información de un equipo, aunque el uso de este sería responsabilidad de las personas que estarían tomando los conocimientos del presente documento, esta guía estará hecha solo para el análisis forense hacia equipos con sistema operativo Windows, no es una guía de análisis forense de redes, de sistemas embebidos o análisis forense de memoria volátil.

La recolección de la información estaría basada en el uso de las herramientas mencionadas a lo largo de la elaboración del proyecto, la funcionabilidad de las herramientas establecidas es netamente para trabajar con el sistema operativo Windows, la falta de actualización de las herramientas o el mal uso de estas no son responsabilidad del autor del presente proyecto.

CAPÍTULO 2

2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO.

2.1 MARCO TEÓRICO

2.1.1Análisis forense digital

El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean validos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos [16].

2.1.2 Guía metodológica.

Una guía metodológica es la sistematización y documentación de un proceso, actividad, práctica, metodología o proceso de negocio. La guía describe las distintas operaciones o pasos en su secuencia lógica, señalando generalmente quién, cómo, dónde, cuándo y para qué han de realizarse. Una guía metodológica debe necesariamente basarse en una experiencia probada (incorporando información de soporte) y debe incorporar las claves del éxito para su implementación [17].

2.1.3 Tipos de análisis forense.

Existe el llamado análisis forense de sistemas, a partir del cual se tratarán los diferentes incidentes de seguridad producidos en servidores y estaciones de trabajo como son los sistemas operativos MAC OS, los correspondientes a Microsoft como Windows 10, 8, 7, así como los sistemas GNU/Linux. Otro tipo de análisis forense sería el correspondiente a redes, que englobaría el estudio de todos aquellos incidentes que atenten contra la seguridad de redes cableadas, Wireless o bluetooth. Finalmente, se destacaría otro tipo de análisis forense como el correspondiente a los sistemas embebidos, donde se estudiarán incidentes producidos en móviles o PDA. Esta clase de sistemas poseen una estructura muy similar a la de un ordenador personal [18].

2.1.4 Software de código abierto vs. Comercial.

Hay veces que, si un examinador forense ve algo que no parece correcto o que no tiene ningún sentido, se puede usar software de código abierto para validar el software comercial mediante la comparación de resultados. Si los resultados de diferentes softwares varían en formas que no se esperaban, entonces es hora de realizar una investigación y / o soporte técnico de software. Una cosa sobre el software de código abierto es que no hay soporte técnico [19].

El presupuesto también importa. El software líder en la industria y la capacitación forense no son baratos. Una gran cantidad de software de código abierto es gratuito y muchos de los principales proveedores ofrecen herramientas gratuitas, especialmente para las fuerzas del orden. Todo buen laboratorio forense debe tener un equilibrio saludable de software forense de calidad por parte de proveedores líderes y de código abierto, y el conocimiento para respaldarlos [19].

2.1.5 Perito.

Un Perito es una persona con formación, capacitación, conocimientos y experiencia en un ámbito técnico, cuyo testimonio puede ayudar en la resolución de conflictos en la vía prejudicial o judicial. El juez puede considerar el testimonio del Perito sobre los hechos a la hora de dictar sentencia, pero éste puede ser preguntado por cualquier aspecto técnico del caso, por los letrados o el propio juez [20].

2.1.6 Perito informático.

La mayoría de los jueces no tienen formación especializada en tecnología. Entonces, ¿cómo pueden saber si una prueba tecnológica es válida en un procedimiento judicial? ¿Cómo consiguen los abogados esas pruebas a la hora de presentarlas en un juicio? A través de un perito informático judicial. Los peritos informáticos son los profesionales que se encargan de dar soporte a particulares, empresas u organizaciones a la hora de presentar pruebas tecnológicas ante un tribunal. Ellos son quien se encargan de analizar la veracidad de dichas pruebas y de exponerlas de forma clara y sencilla para que puedan ser comprendidas por un juez [21].

2.1.7 Delitos Cibernéticos más comunes en el Ecuador asociados a los artículos del COIP [22].

TIPO DE DELITO	ARTÍCULO DEL COIP APLICABLE
Accesos no autorizados. **Fallos y vulnerabilidades.**	Art. 178. Violación de la intimidad. Art. 190. Apropiación fraudulenta de Medios Electrónicos. Art. 211. Supresión, alteración o suposición de la identidad y estado civil. Art. 212. Suplantación de identidad. Art. 213. Transferencia electrónica de activo patrimonial. Art. 234. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
Pornografía. **Pornografía Infantil.**	Art. 103. Pornografía con utilización de niños, niñas o adolescentes.
Estafas. **Correos Nigerianos, Loterías, Actualización de Información Bancaria (Phishing).**	Art. 190. Apropiación fraudulenta por medios electrónicos. Art. 211. Supresión, alteración o suposición de la identidad y estado civil.
Secuestro, Extorsión. **Rasomware.**	Art. 212. Suplantación de identidad.
Robo de Identidad. **Escucha de redes, Phishing**	Art. 178. Violación de la intimidad. Art. 211. Supresión, alteración o suposición de la identidad y estado civil.
Robo de Información.	Art. 190. Apropiación fraudulenta por medios electrónicos. Art. 229. Revelación ilegal de base de datos. Art. 230. Intercepción ilegal de datos.
Código malicioso. **Virus, Malware, Vulneraciones**	Art. 231. Transferencia electrónica de activo patrimonial. Art. 232. Ataque a la integridad de sistemas informáticos.

Interrupción del servicio, Denegación de servicio distribuido. **DDO, DDoS.**	Art. 232. Ataque a la integridad de sistemas informáticos. Art. 233. Delitos contra la información pública reservada.
Utilización no autorizada de servicios. Actividades propias, hacktivismo, botnets.	Art. 233. Delitos contra la información pública reservada.

Tabla 1: Delitos cibernéticos asociados al COIP: Paula Romina Jaramillo.

2.2 METODOLOGÍA DEL PROYECTO

2.2.1 METODOLOGÍA DE LA INVESTIGACIÓN

Un estudio exploratorio se efectúa cuando no se han realizado investigaciones previas o existe poca información acerca del objeto de estudio [23]. En la presente guía metodológica para el análisis forense digital se ha tomado como base al Sistema Operativo Windows 8.1, pese a que lo hacen de manera general a Windows, se aplicará este tipo de estudio de investigación, para hacer la respectiva recolección de información indagando en diferentes fuentes bibliográficas y a la observación de los procesos ya realizados de manera similar.

La investigación diagnostica del presente proyecto se la realizará mediante un proceso de recopilación documental y bibliográfica, indagando y recolectando información de diferentes fuentes de acuerdo con el proyecto planteado, y de entrevistas realizadas a una profesional en la materia de análisis forense, por su experiencia en recuperación y recolección datos informáticos digitales.

2.2.2 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Para la recolección de información se han usado dos tipos de técnicas que son de entrevista y recopilación documental y bibliográfica.

En **entrevista** se obtiene una opinión profesional, por parte de una persona experimentada en el ámbito de peritaje informático por medio de un cuestionario, estableciendo preguntas referentes a la elaboración de una guía de análisis forense. (**Ver Anexo 1**).

En **recopilación documental y bibliográfica**, se busca información de diferentes fuentes bibliográficas de acuerdo con el tema establecido, para poder tener una mejor idea con respecto a la elaboración de la guía, y de proyectos similares.

2.2.3 METODOLOGÍA DE DESARROLLO

La metodología UNE 71506:2013 servirá como base para la realización de la guía de análisis forense digital, dicha metodología está hecha para el uso de un análisis forense de las evidencias electrónicas [24].

Esta metodología se la estableció por medio de un estudio del Ing. Byron Loarte, el cual hizo la evaluación de diferentes tipos de metodologías para análisis forense digitales, entre las cuales estaban: CASEY, NIST, Francisco Lázaro, Forensic Control y DFRWS, donde los aspectos más importantes a considerar fueron: adaptabilidad, implementación, práctica, documentación y fases claramente detalladas, siendo esta una de las mejores evaluadas [1].

Esta metodología de análisis forense digital consta de 5 fases que son las siguientes:

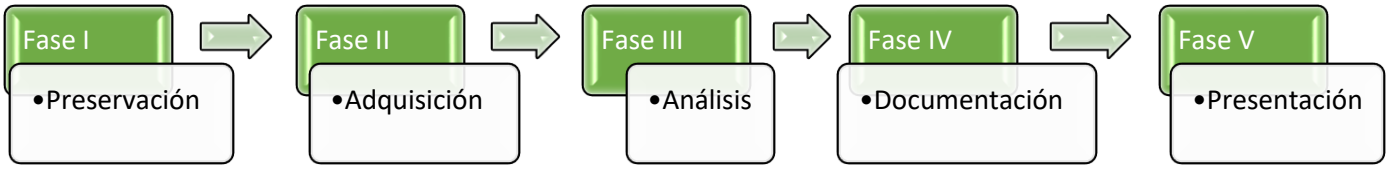


Figura 1:Fases de la metodología UNE 71506:2013

Fase I. Preservación: Dentro de esta fase se lleva a cabo que no exista la pérdida de las evidencias, sean estas digitales o físicas, verificar el equipo o elementos a analizar, mantener una validez jurídica de las evidencias recopiladas, solo en el caso de ser necesario, evitar que la información sea alterada, dañada o manipulada ya sea por causas humanas o naturales.

Fase II. Adquisición: En esta fase se procederá a recopilar las evidencias físicas o digitales, verificar la autenticidad del equipo a analizar, obtener las diferentes herramientas de hardware y software para la recopilación de la información, realizar una copia de la evidencia encontrada para no dañar la evidencia original.

Fase III Análisis: Se procede a hacer el uso de las herramientas para el análisis forense, escoger el método de investigación a ser aplicado, evitar comprometer la integridad de la información extraída de las evidencias.

Fase IV. Documentación: Dentro de esta fase se procede a documentar por medio de un informe pericial la extracción de las evidencias, evidenciar los datos extraídos mediante fotografías o capturas de pantalla, elaborar un informe técnico de conclusiones del proceso realizado.

Fase V. Presentación: En esta fase se presentan los diferentes resultados obtenidos del análisis forense, realizar una presentación convincente y entendible, detallando las diferentes herramientas y metodologías usadas durante el proceso, detallar las conclusiones expuestas en la fase de documentación.

CAPÍTULO 3

3. PROPUESTA

Luego de obtener la suficiente información dentro de la investigación, en este punto se procederá a la elaboración de la guía metodológica planteada.

3.1 IDENTIFICACIÓN DE LA ESCENA DEL DELITO. (Caso de estudio) Interceptación Policial a una vivienda.

La policía nacional logra interceptar una casa donde la ciudadanía ha dado alerta de que dentro del inmueble habitan personas sospechosas de actos ilícitos, y dan información de movimientos inseguros, esto se debe a que ingresan personas con distinta personalidad cada día.

Los moradores del sector aseguran que las personas que habitan en ella ocultan algo, y es por lo que han hecho un llamado a las autoridades, puesto que en los últimos días han escuchado ruidos de peleas dentro de la vivienda, la policía nacional prepara una intercepción y una orden judicial para poder acceder a la vivienda.

Una vez dentro encuentran a tres personas en ella, revisan la casa y hallan distintos dispositivos electrónicos, entre los más encontrados hay teléfonos celulares, también en un cuarto de la vivienda se logra hallar un computador de escritorio, el cual está apagado que se presume el dueño de este sería una de las personas que habitan en la casa.

Hacen la detención de las tres personas y que posteriormente serán investigadas por las autoridades, pero para asegurar las cosas se selecciona a una persona para que haga el proceso de peritaje informático o extracción de evidencias hacia el computador encontrado, esta persona llega al lugar y hace el proceso respectivo para preparar el equipo y llevarlo a su laboratorio, y de esta forma hacer el respectivo análisis.

Se tratará de encontrar datos, entre estas fotos de los celulares, documentos de texto, entre otros, que sirvan de ayuda para que el fiscal compruebe si las sospechas de la ciudadanía hacia estas personas son ciertas, pues se presume que estarían involucradas en el robo de celulares en el sector, puesto que desde que han llegado a habitar la vivienda, se ha incrementado el robo.

3.2 DESARROLLO DE LA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL.

3.2.1 Introducción

La siguiente guía está basada en las cinco fases de la metodología UNE 71506:2013, puesto está hecha para la correcta extracción de evidencias digitales, también se tomará en cuenta los reglamentos del Código Orgánico de Integración Penal (COIP), que es una de las normativas legales vigentes dentro del país.

Para la correcta elaboración de la guía es de suma importancia que se cumplan cada una de las fases de la metodología establecida y de esta manera considerar los procesos que se lleven a cabo en cada una de estas, dentro del análisis de evidencia digital. Se garantiza la integridad de la evidencia digital en todo momento.

3.2.2 Objetivos.

- Englobar los aspectos importantes a considerar en un análisis forense mediante las cinco fases de la metodología UNE 71506:2013.
- Proporcionar información relacionada con el análisis forense digital, en especial en entornos Windows.
- Centrar el proceso de toma de evidencias, realizando las pruebas sobre Windows 8.1

3.2.3 Requerimientos.

- Identificar al investigador forense que se hará cargo de la recolección de información digital.
- Evidencia con su respectiva cadena de custodia certificada y garantizada.
- Formulario con los datos personales del perito o investigador.
- Formulario de los datos personales de los involucrados dentro de la escena y sus declaraciones.
- Formulario con las especificaciones técnicas del equipo por analizar.

3.2.3.1 Puntos importantes a considerar

- Se debe identificar las herramientas de hardware y software que posteriormente serán usadas para la recopilación y extracción de información digital, es de suma importancia tenerlas listas para hacer el respectivo análisis.
- Proceder con la extracción del disco duro del equipo e identificar las diferentes unidades extraíbles conectadas y mantenerlas etiquetadas para su posterior análisis.
- Crear una imagen forense del disco duro usando el software AccessData FTK, pero antes de ello se debe bloquear la escritura de los puertos USB, puesto que no se debe trabajar con la evidencia original.
- Se hace el uso de las herramientas establecidas para el análisis forense y extracción de evidencias de la imagen forense del disco duro generado.
- Documentar mediante un informe pericial las evidencias encontradas dentro el proceso de extracción.
- Dentro del informe pericial, mencionar las observaciones encontradas en el proceso de análisis de la imagen forense del disco duro original.
- En el informe redactado no usar palabras técnicas, las estrictamente necesarias, considerando al lector que no es técnico informático.
- Presentar el informe a la autoridad que corresponda.
- Tener los respaldos técnicos informáticos de la secuencia lógica de la extracción de datos encontrados en la imagen forense.
- Se puede presentar el informe mediante ilustraciones gráficas, esto lo indica el Articulo 511, inciso seis y siete del COIP.
- En la presentación solo se debe dar información del trabajo realizado.

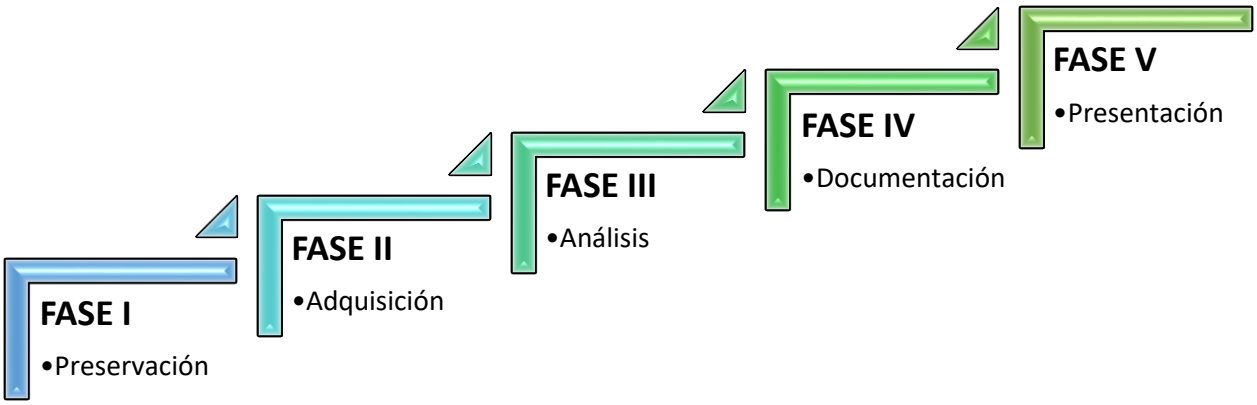


Tabla 2: Fases de la metodología UNE 71506:2013

3.2.4 FASE I. Preservación

Dentro de esta fase se lleva a cabo la verificación del equipo por analizar, es decir, que esté tal y como lo dejaron sus dueños, que estén siendo procesados o analizados, también en esta fase uno de los propósitos es determinar quién sería la persona encargada de llevar a cabo el proceso de extracción de las evidencias. Según el Artículo 12 de la Resolución 040-2014 el cual establece que la elección de Peritos sea este de tipo civil o penal, será realizado respectivamente por un juez [25]. Respetando los principios de profesionalidad, especialidad, transparencia, alternabilidad e igualdad, cabe recalcar que esta persona debe estar calificada y tomar en cuenta que sea capaz de cumplir con la responsabilidad que se le está asignando.

Equipo informático por analizar dentro de esta fase:

Figura 2: Estado del equipo por analizar

Especificaciones técnicas:

Procesador	Intel Atom CPU D425 de 1.8 GHz
Disco Duro	Tipo Serial ATA Device particionado. 176 GB sistema y 290 GB libres
Memoria	4 GB DDR3 de 800 MHz
Motherboard	Placa de escritotio Intel D425KT mini ITX DDR3 con microporcesador incorporado.

Tabla 3: Especificaciones Técnicas del Equipo

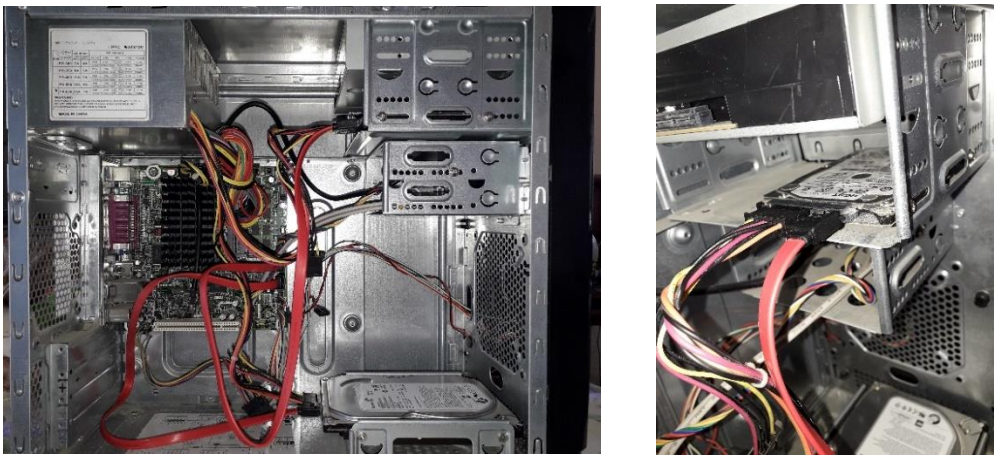


Figura 3: Componentes internos del equipo

Antes de iniciar el proceso de recoleccion de informacion, existen formularios que serán llenados con toda la informacion necesaria del caso.

Formulario N° 1: En este ejemplo se llenará de informacion personal del perito a cargo del proceso de investigacion. (**Ver Anexo 2**)

3.2.5 FASE II. Adquisición

En esta fase se procederá seleccionar los diferentes tipos de herramientas a usar dentro del proceso de extraccion de evidencia digital, es de suma importancia identificar cual es el propósito de cada hardware y software, dicho proceso sera mencionado a lo largo de esta fase, estos serán usados una vez que el equipo haya sido identificado, siguiendo el proceso de la fase anterior.

Es necesario saber el estado del equipo por analizar, esto quiere decir, verificar los dos principales estados de como se encontró el equipo informático y seguir correctamente pasos para su posterior indagacion, estos estados a considerar son:

1. Equipo apagado.

Si equipo se encuentra apagado al momento de llegar a una escena, tomar en cuenta lo siguiente:

- No encender el equipo: El equipo encontrado debe permanecer tal y como está, si se llega a encender es posible que la evidencia almacenada pueda ser alterada.

- Es importanque que existan dentro de la escena testigos que corrovoren el estado del equipo, y que esta sea la forma de que el perito o la persona a analizarlo tenga entre sus manos una evidencia sin alteración alguna.

- Hacer una copia de la evidencia original y no trabajar directamente en ella, esta copia tiene un nombre de imagen forense o copia de bit a bit, y para hacer esto existen herramientas que seran usadas para este proceso, se recomienda hacer dos copias del disco original.

- El equipo a ser analizado debe ser transportado con el mayor cuidado posible hacia el laboratorio o el lugar donde se vaya hacer el respectivo analisis, el equipo y los diferentes componentes encontrados deben ser etiquetados y embalados, esto incluye dispositivos extraíbles como, tarjetas de memoria, usb, cableado,etc. A este proceso se lo conoce como Cadena de Custodia.

2. Equipo encendido.

En el caso de encontrar el equipo encendido, tomar en cuenta lo siguiente:

- No se debe apagar, esto se debe a que la información dentro del mismo puede perderse, puede darse el caso que el dueño original este conectado remotamente en el.

- Anotar la información del equipo encendido, entre estas; hora y fecha actual, programas ejecutandose, directorios abiertos, nombre de la red en caso de estar conectado a internet y el nombre del usuario.

La escena del delito se refiere a identificar como ha sido encontrado el equipo en el lugar donde se hace el hallazgo, intervienen las personas que se encuentren en el lugar, incluido el perito informático.

Los agentes de policia, abogados, familiares, o personas que de una u otra forma se encuentren en el sitio, seran testigos del reconocimiento y posterior traslado del equipo informático a analizar. Esto excluye al perito informático, puesto que seria la persona que va hacer el proceso de la extraccion de la evidencia.

Para esto se realiza otros tipos de formularios que el perito procederá a llenar identificando el entrono de la escena.

Formulario N° 2: Dentro de este ejemplo se hallará informacion referente a la escena o entorno y el estado del equipo a analizar. (**Ver Anexo 3**)

Formulario N° 3: En este ejemplo de formulario se llenará información del equipo y los medios de almacenamiento encontrados, los cuales serán transportados hacia el laboratorio o el lugar donde se hará el respectivo proceso de análisis. (**Ver Anexo 4**)

Para llevar a cabo todo esto es importante conocer e identificar los diferentes tipos de herramientas a usar durante este proceso, entre estas tenemos:

Hardware.

El hardware por usar dentro del proceso es el adaptador Sata a USB, este va a permitir leer las unidades de almacenamiento hacia el entorno que se desea trabajar, también una unidad de almacenamiento en este caso un disco duro que sirva para almacenar la imagen forense por generar, también un computador para poder hacer el proceso de creación de copia y posteriormente el análisis de esta, estos son unos ejemplos.

Figura 4: Herramientas de hardware.

También dentro de estas herramientas podemos encontrar destornilladores, tijeras, guantes, pulsera antiestática, cableado etc. las antes mencionadas servirán para el proceso de desmontaje y montaje del equipo.

Software.

Las herramientas instaladas para hacer el proceso de copia bit a bit o imagen forense y posterior análisis son:

AccessData FTK Imager versión 4.2.1. Este software nos ayudará hacer el proceso de la creación de la imagen forense del disco duro, dándole una identificación al caso, una descripción y a la persona encargada de hacer la copia.

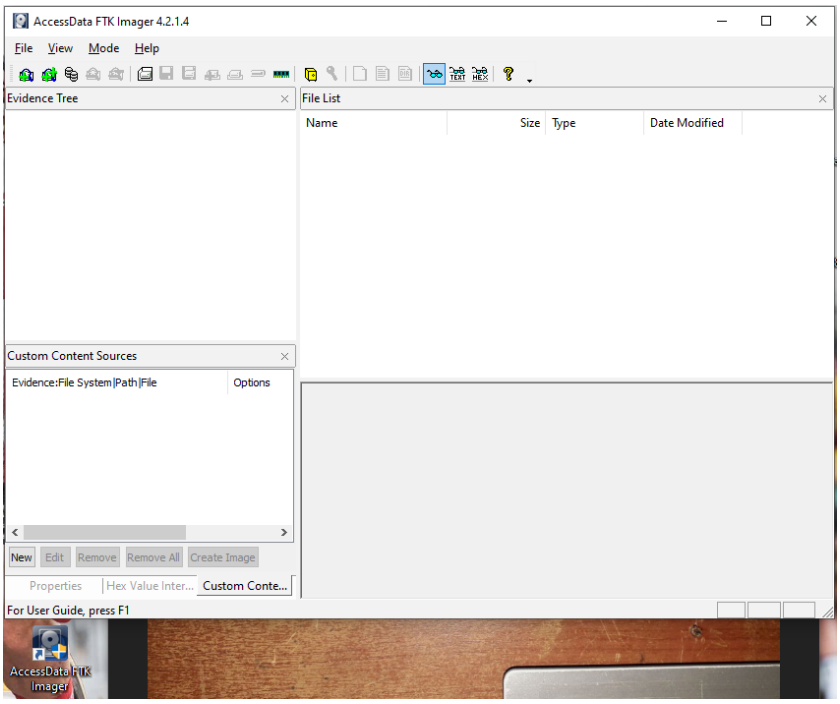


Figura 5: Pantalla principal de AccessData

También encontramos **Autopsy**, que es un software especializado para la extracción de la información dentro de una imagen forense generada por la copia de un disco duro.

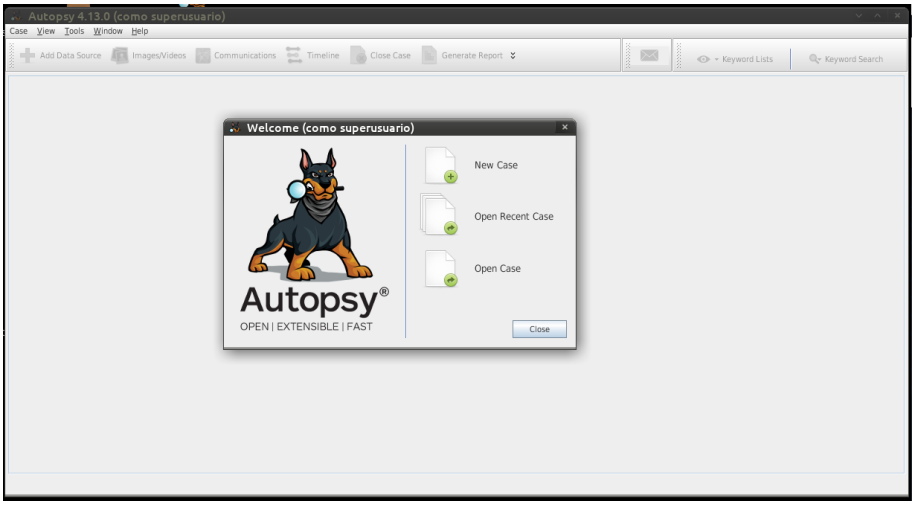


Figura 6: Pantalla principal de Autopsy

.

DiskDigger versión 1.43.67. Es un software que ayuda a la recuperación de diferentes tipos de archivos de un Disco Duro, Memorias USB, tarjetas de memoria y de imágenes forenses generadas.

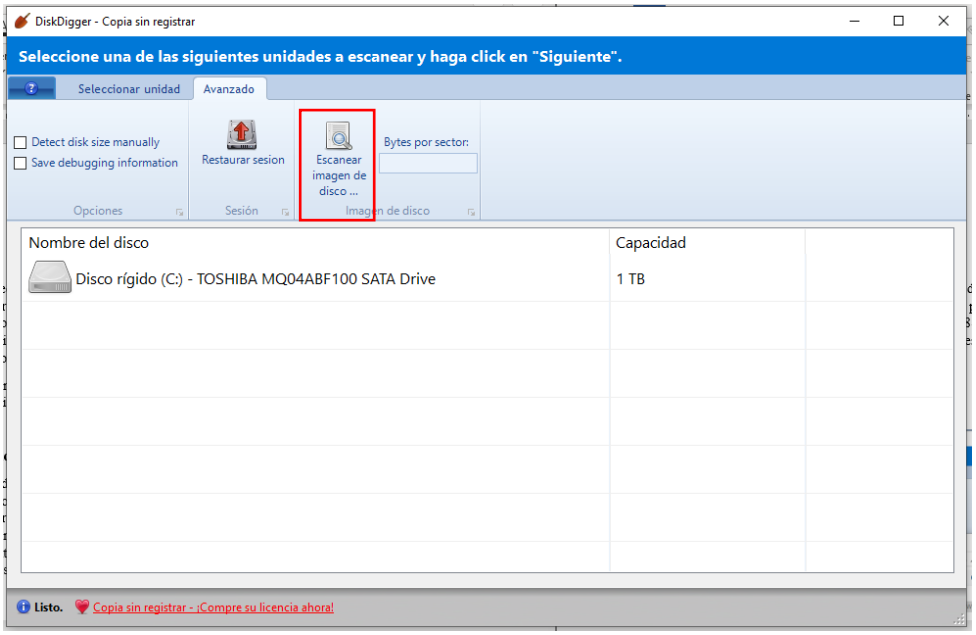


Figura 7: Pantalla principal de DiskDigger

Una vez identificado el equipo se procede con el respectivo embalaje y etiquetado.

Figura 8: Proceso de embalaje y etiquetado del case por analizar

Cuando el equipo se encuentre en el sitio donde se hará el respectivo análisis, el perito a cargo tomará todas las medidas necesarias para realizar el proceso de extraccion del disco duro, esto lo debe hacer con el mayor cuidado posible garantizando la integridad durante el proceso.

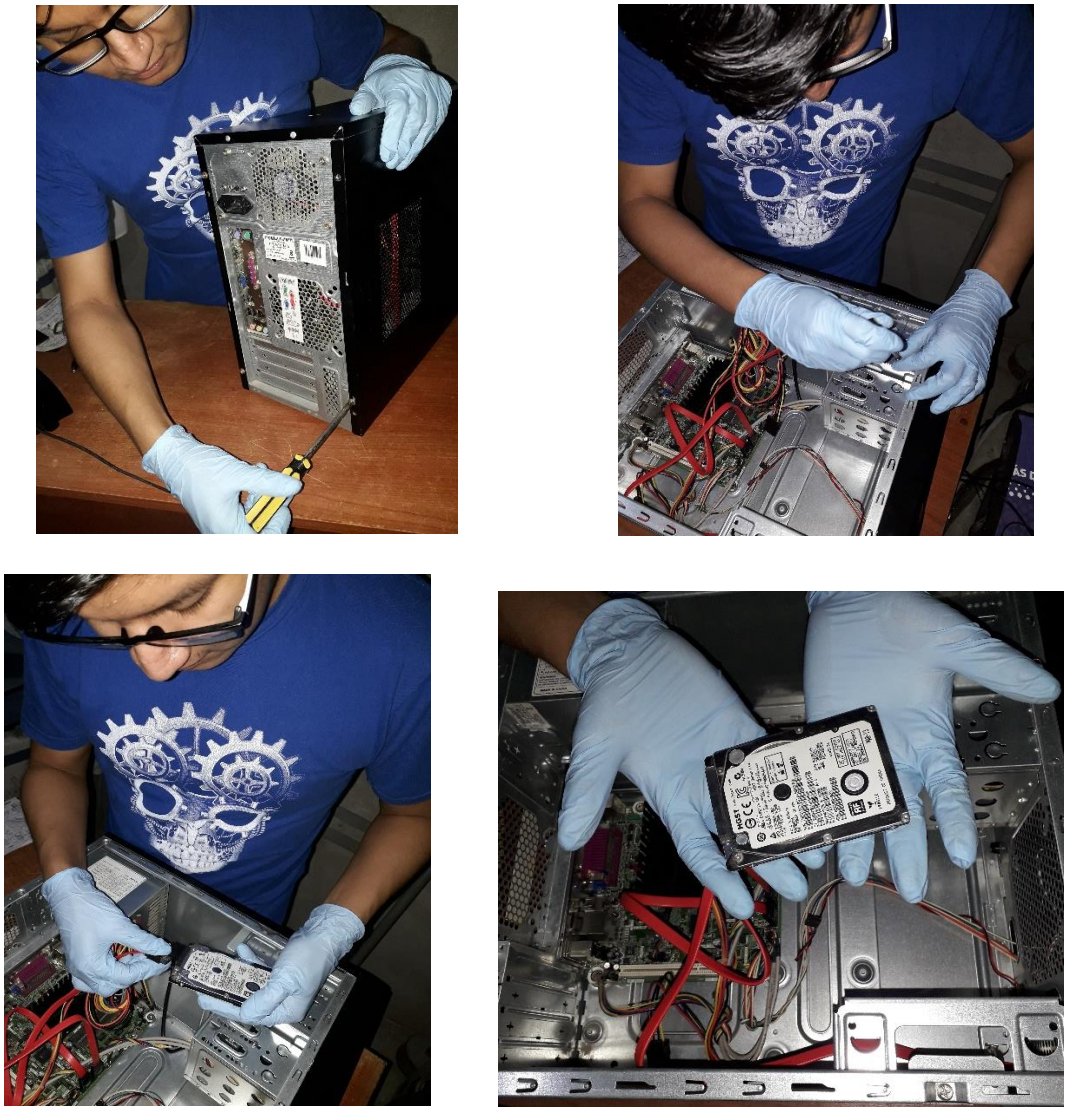


Figura 9: Proceso de extracción del Disco Duro

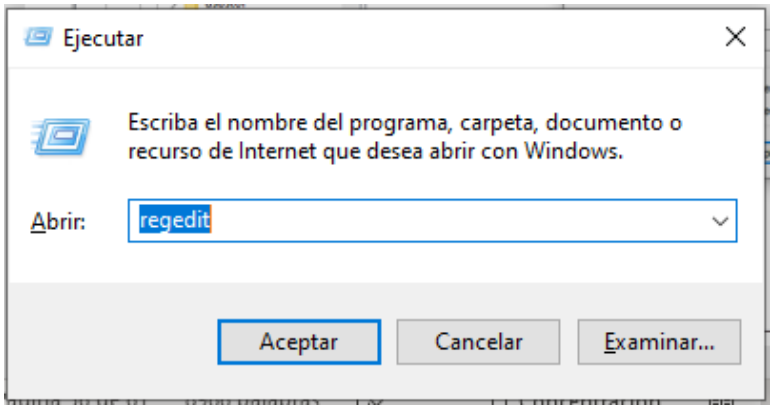
Posteriormente luego de extraer el disco duro procederá a conectarlo hacia el equipo que utilizará para hacer el proceso del análisis y relizar la copia del disco la cual es llamada imagen forense.

Figura 10: Preparar y conectar Disco Duro para creación de Imagen Forense

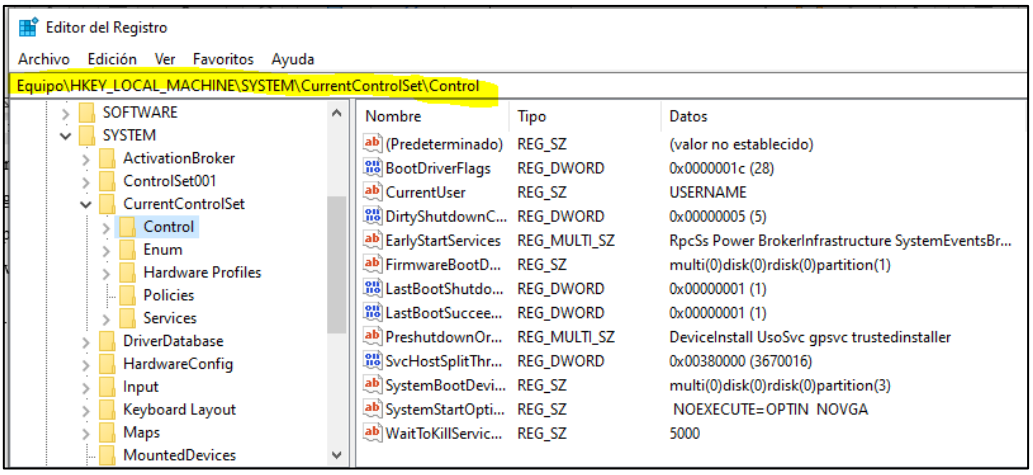
Inico del proceso de creación de la Imagen Forense.

Una vez adquirido y preparado el disco duro del equipo es de suma importancia preparar el software para la creación de la imagen forense, uno de los primeros pasos y mas importantes es activar la proteccion de escritura de USB, esto se puede hacer con el editor de registro.

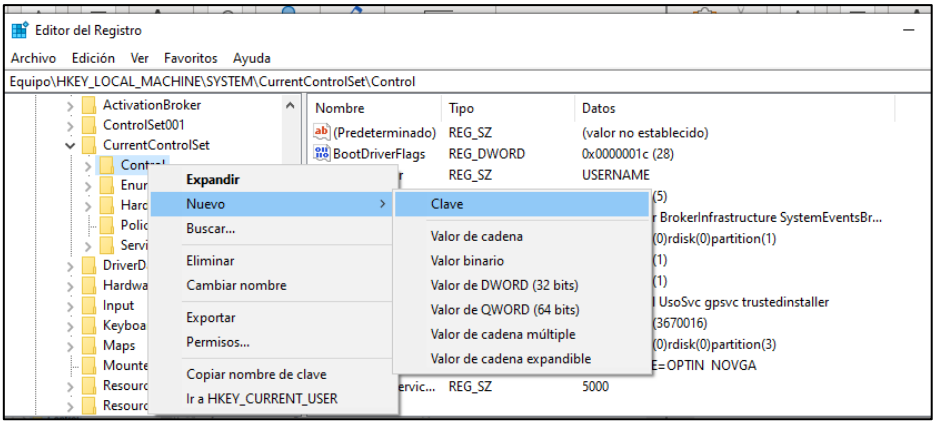
1. Ejecutar el editor de registro (regedit)



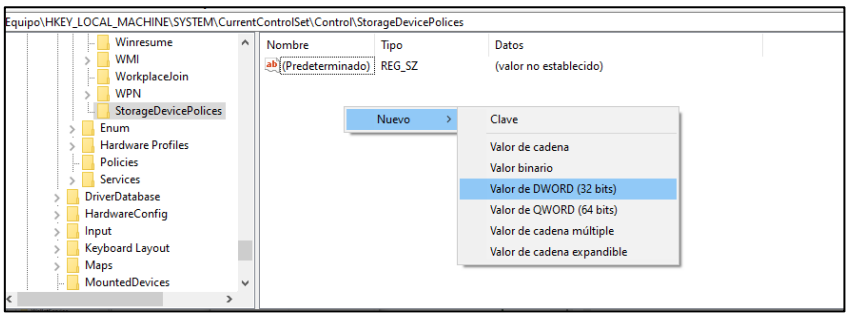
2. Nos dirigimos a la sigueinte ruta:
   Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control



3. Clic derecho sobre la carpeta Control y se crea una nueva clave con el nombre de StorageDevicePolices.



4. Una vez creada la clave se procede a crear el control de proteccion de escritura con el nombre de WriteProject



5. Luego se modifica con clic derecho, automaticamente aparecerá el valor de 0, para activar la proteccion de escritura se cambia el 0 por el 1 y al aceptar se guarda los cambios.

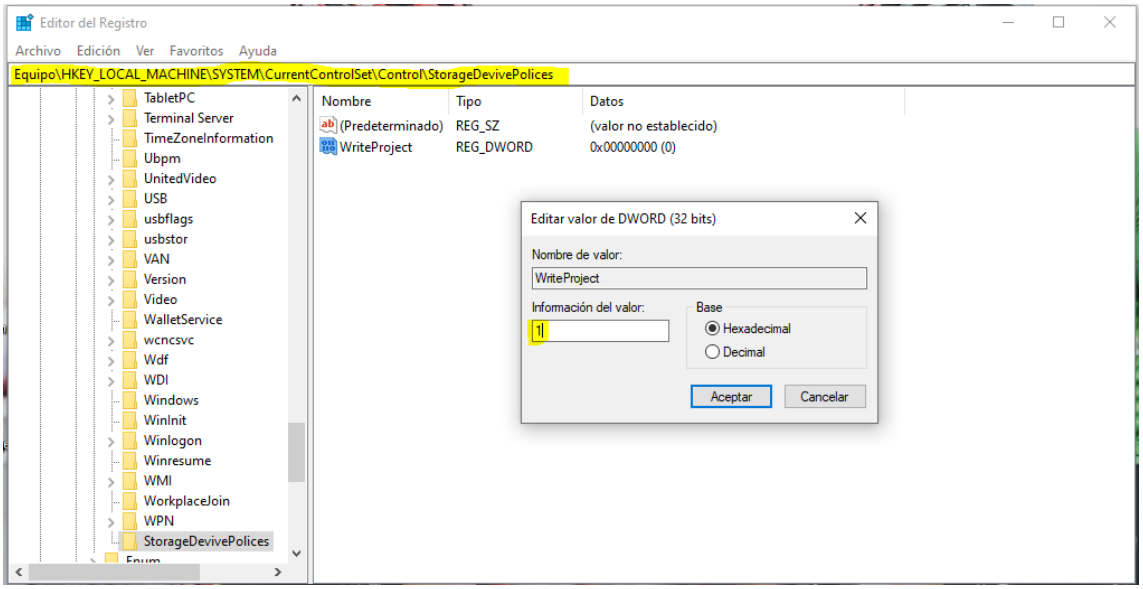


Figura 11: Activación de la protección de escritura por medio del Editor de Registro

Activar la proteccion de escritura ayuda a que la imagen por crear sea integra y se pueda evitar que se copien archivos hacia el disco y así asegurar que la copia y sus archivos permanezcan intactos.

Luego se procede a conectar el disco al equipo que será usado para la respectiva creación de la imagen, para ello se usará AccessData FTK Imager versión 4.2.1.4

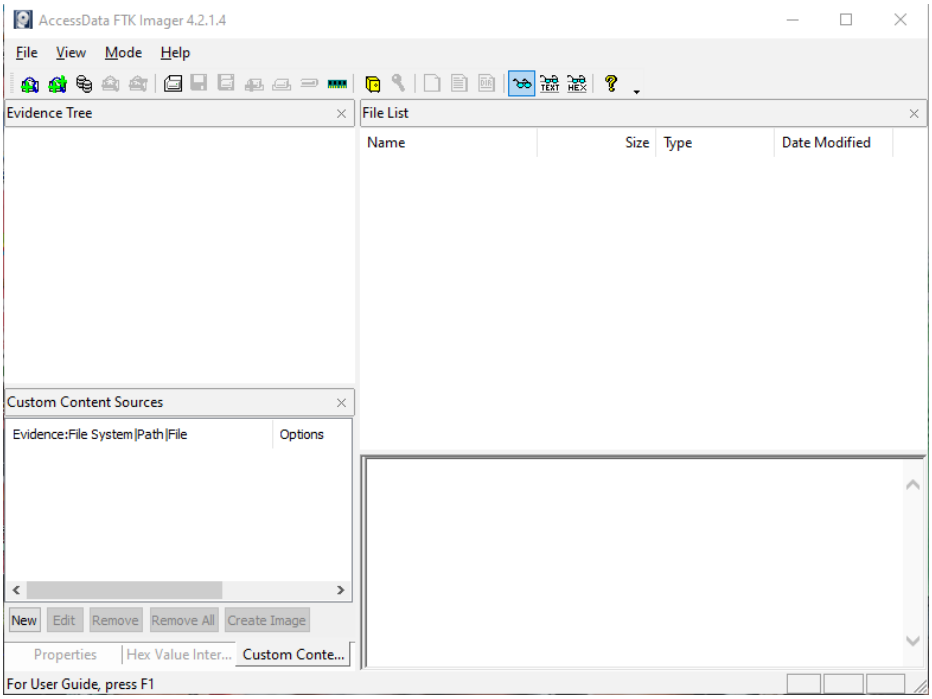
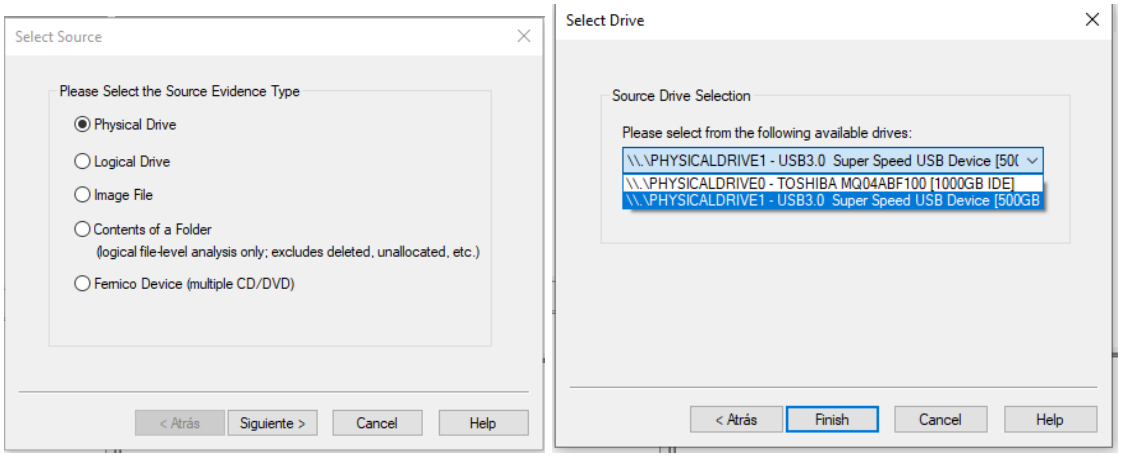


Figura 12: Pantalla principal de AccessData

6. Se ejecuta AccessData FTK Imager y se selecciona la unidad de disco conectada, se escoge el disco con 500GB de capacidad.



7. A continuación, se elige el tipo de imagen, información de la evidencia y la ruta donde será almacenada.

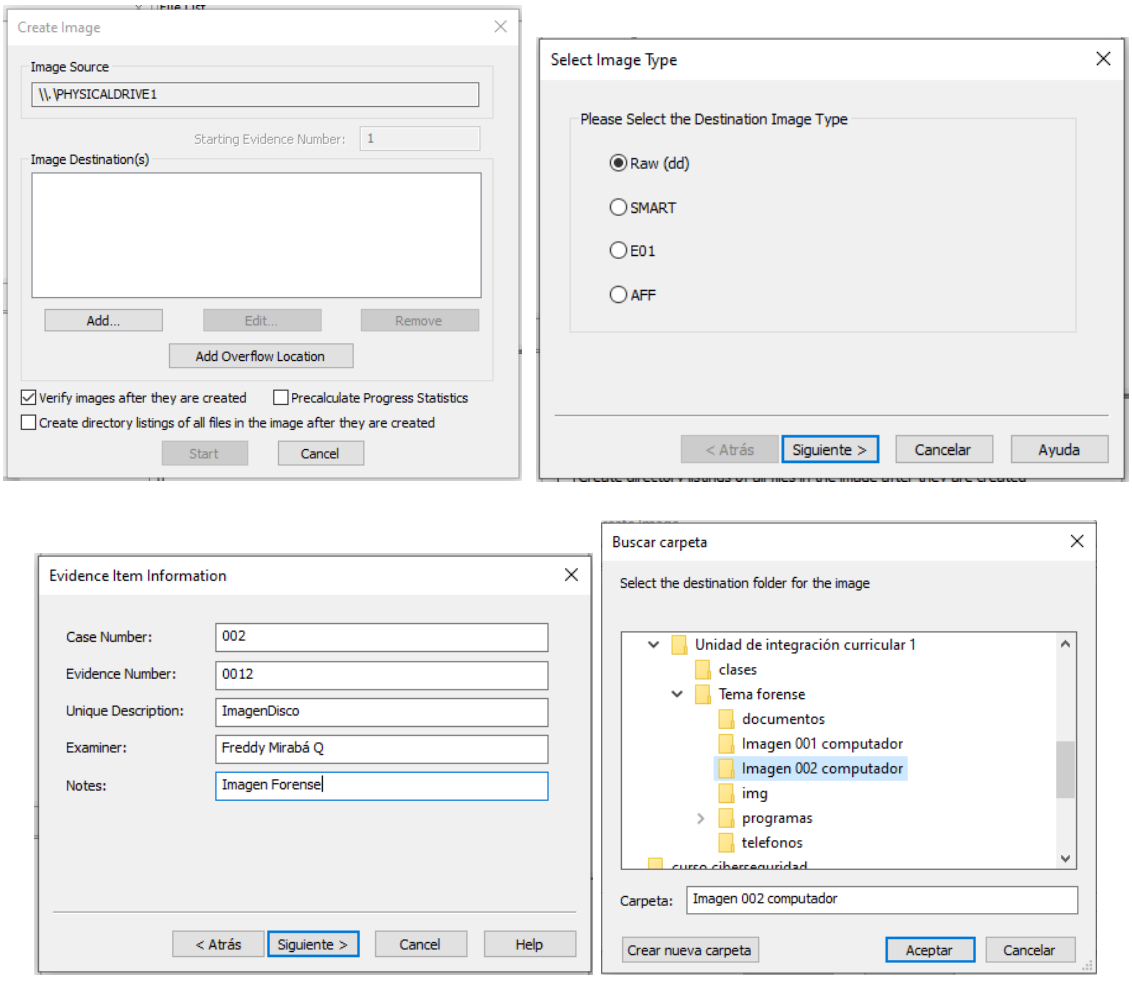
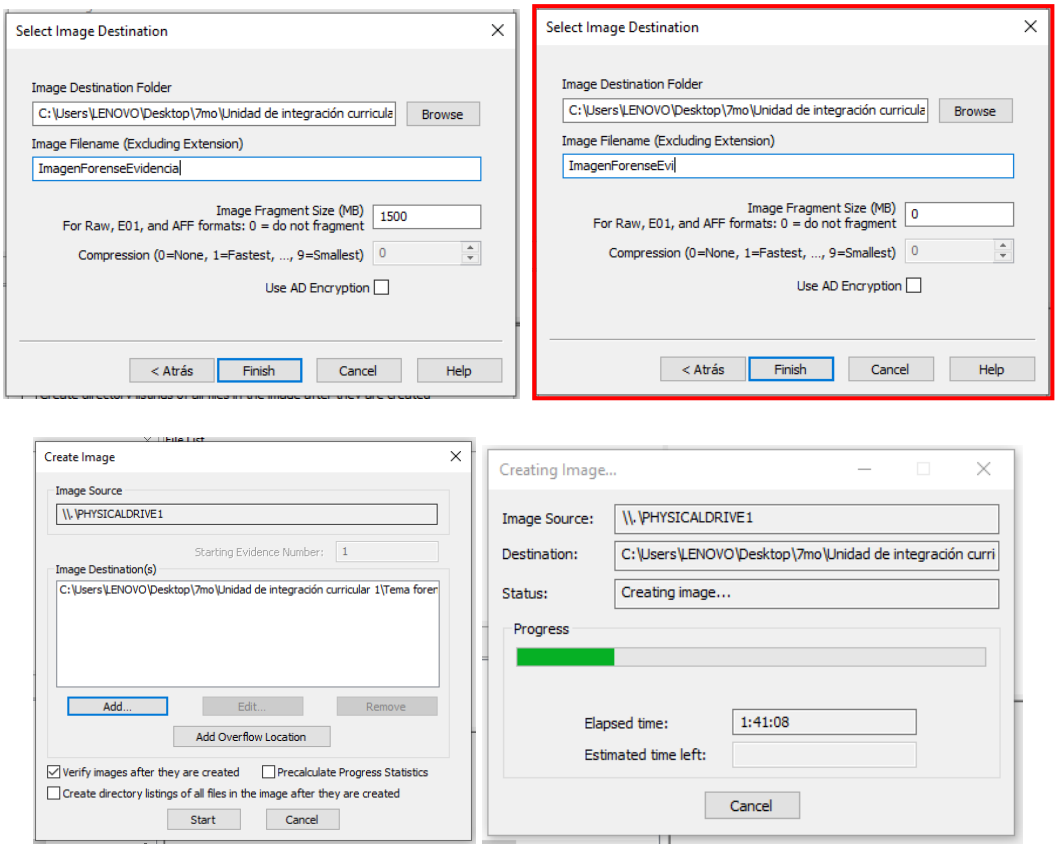


Figura 13: Proceso de creación de la imagen forense

8. Se le asigna un nombre a la imagen por generar y en Image Fragment Size le asignamos el valor de 0, esto se hace para generar la imagen con la misma capacidad que el disco fisico luego clic en finish, y comenzará su creación.



9. Una vez creada la Imagen del disco, aparecerá el proceso de verificación del código HASH, este proceso tambien tomará un tiempo, este código Hash es una serie de caracteres que representan a un codigo único de la imagen del disco creada. Esto garantiza la integridad de la respectiva creación, si el codigo Hash no coincide con el reporte, la imagen del disco ha sido modificada y por lo tanto no se considera una imagen exacta del Disco Duro original.

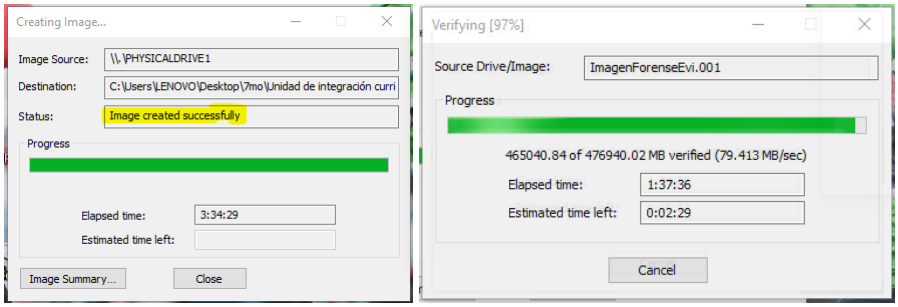


Figura 14: Imagen forense y verificación

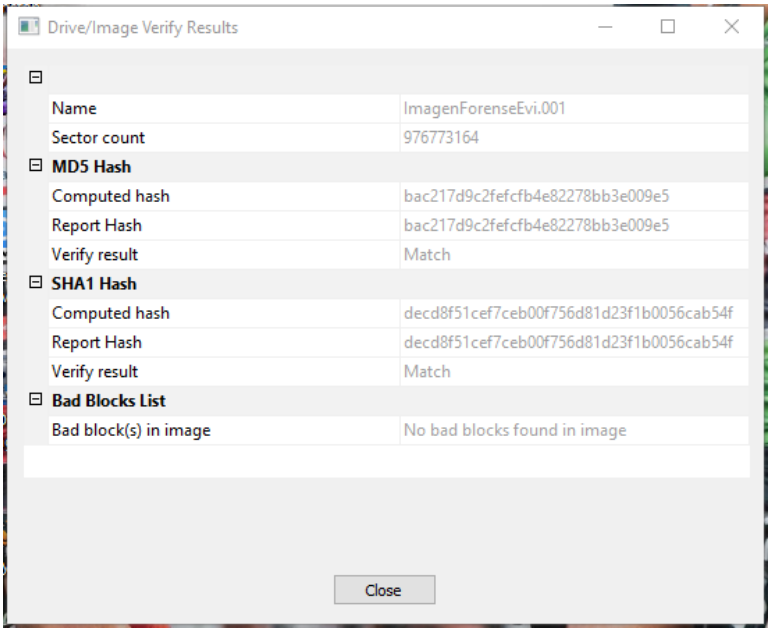


Figura 15: Verificación del código Hash de la Imagen Forense generada

Cuando se hayan cumplido todos estos pasos se puede decir que la Imagen forense ha sido creada con éxito, y la se podrá encontrar en la ruta elegida para ser almacenada.

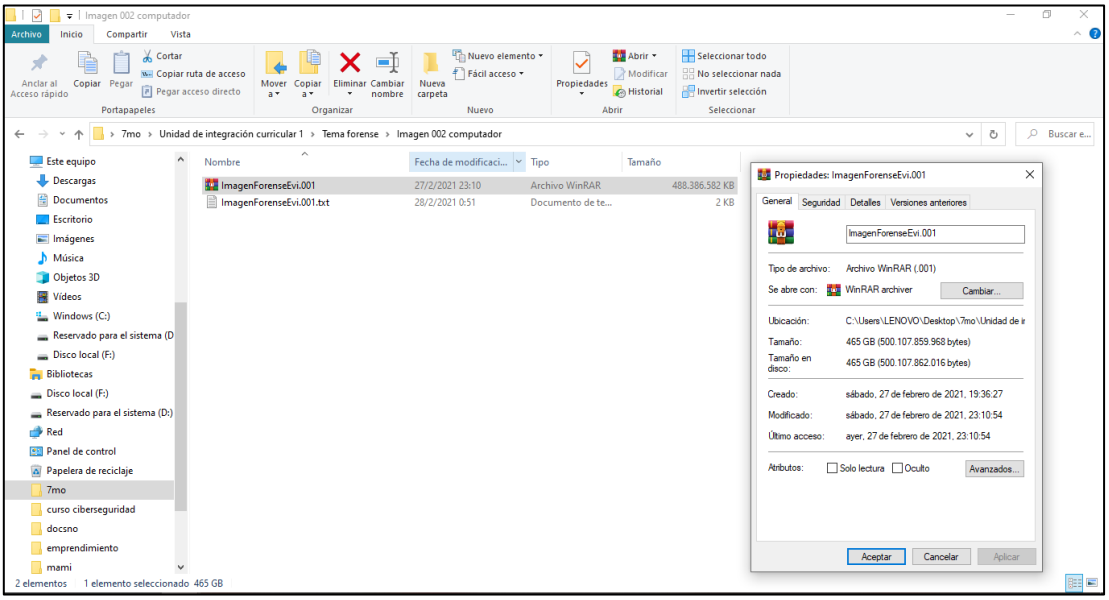


Figura 16: Imagen forense almacenada en la ruta indicada

3.2.6 Fase III. Análisis

Proceso de análisis de Imagen Forense generada.

Cuando se genera la imagen forense del disco duro el siguiente paso es hacer el proceso de análisis, se usará el software forense Autopsy, tiene las características necesarias para poder hacer este tipo de investigaciones forenses digitales.

1. Al ejecutar Autopsy se elige nuevo caso, luego de esto se le asigna un nombre al caso y la ruta donde se desea almacenar.

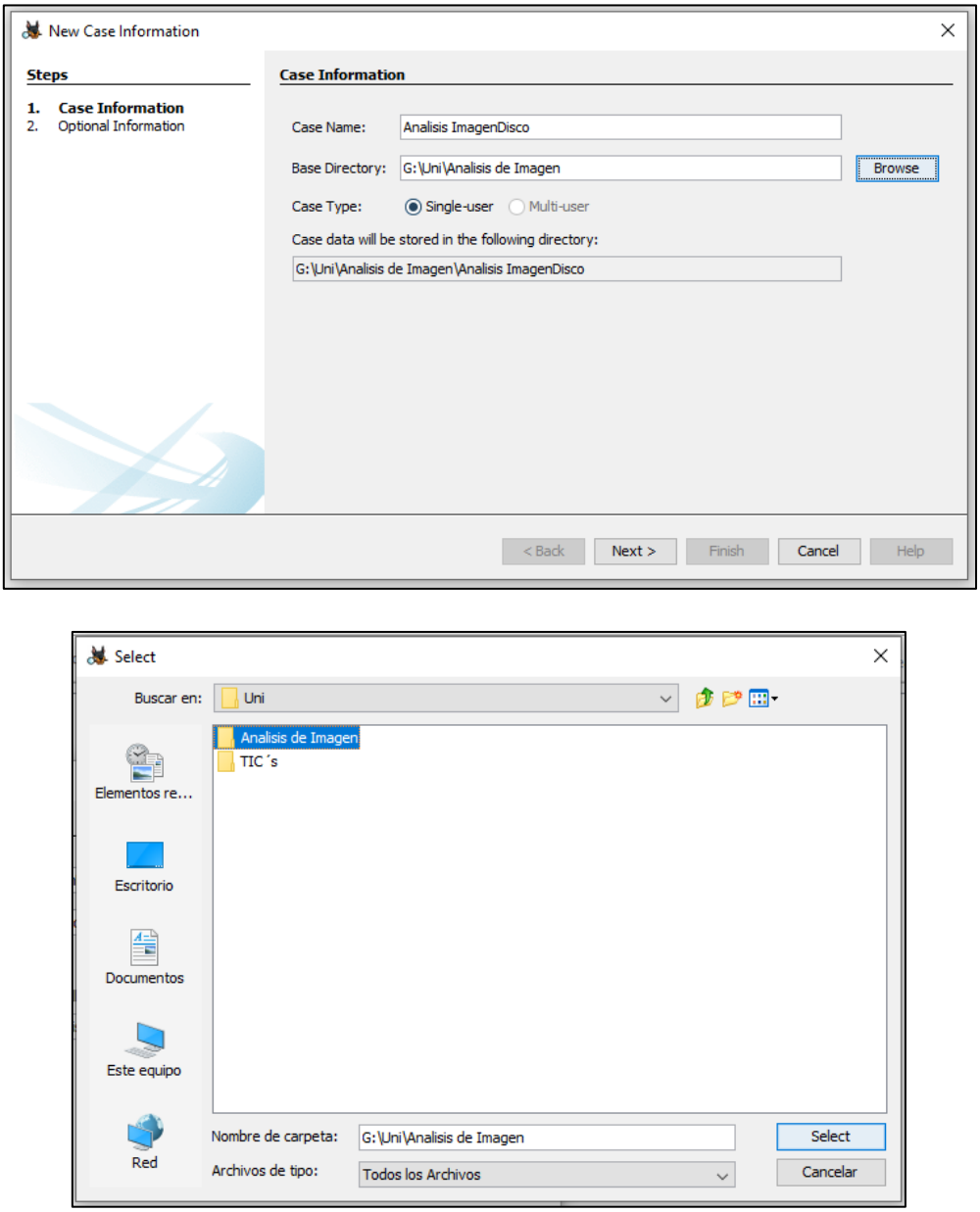
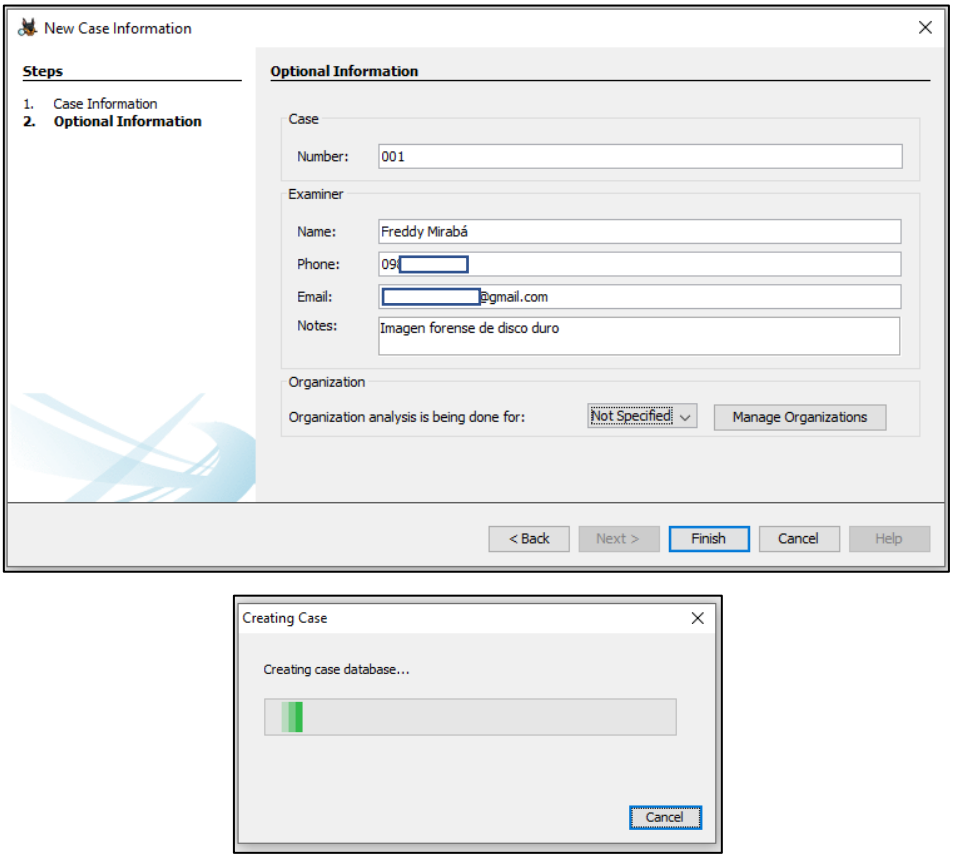


Figura 17: Creación de la información del caso

2. El siguiente punto es agregar la información de los datos del perito informático o persona encargada de hacer el proceso del análisis. Posteriormente al dar clic en finalizar comenzará el proceso de creación de la base de datos del caso.



3. Luego se procede a seleccionar la opción de imagen de disco que es lo que se analizará, luego siguiente.

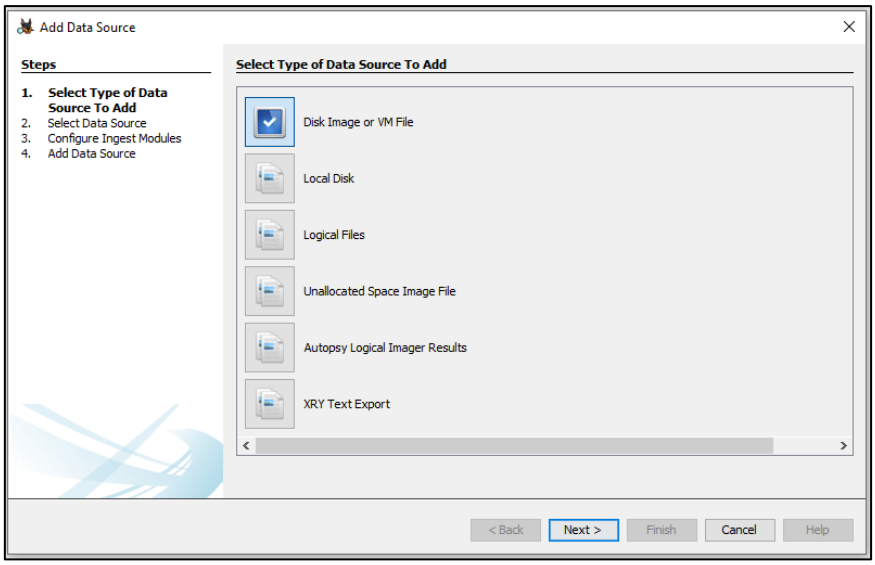
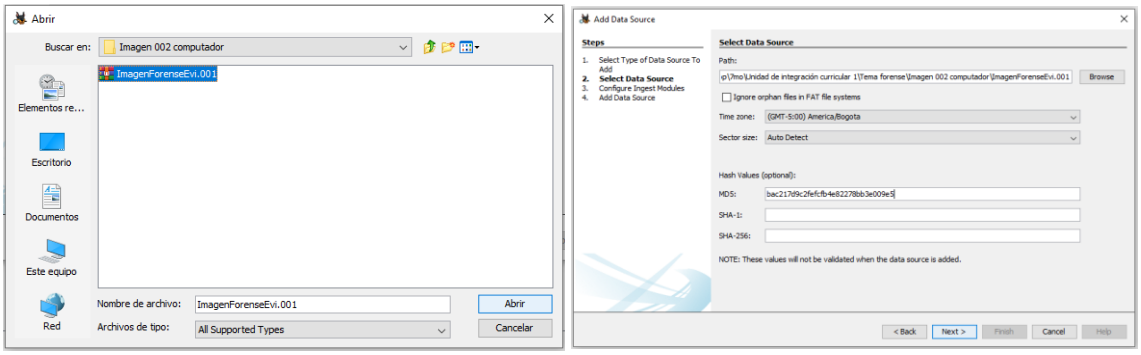
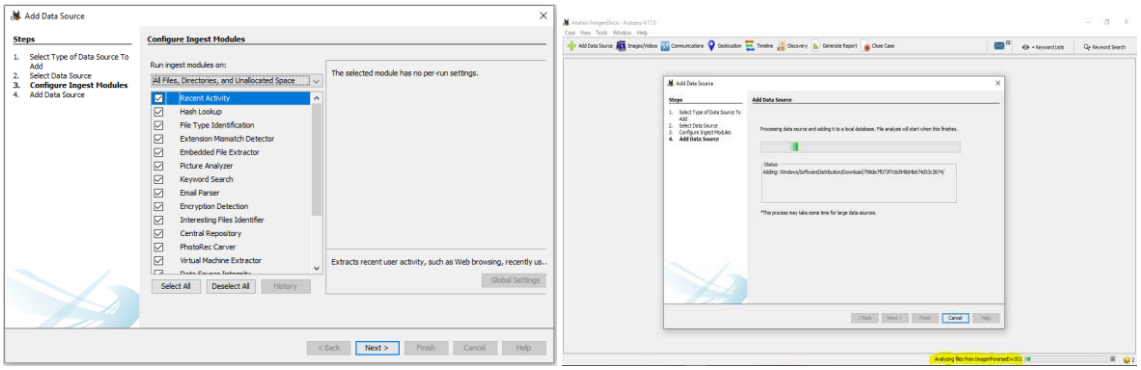


Figura 18: Datos y selección de la Imagen Forense

4. En este punto se selecciona la Imagen Forense Creada con AccessData, se elige la zona horaria y de ser posible agregar el código Hash generado (opcional).



5. Se seleccionan los módulos que se desean analizar y comenzará el proceso del análisis, este proceso tomará un tiempo, puesto que la imagen que se está analizando posee tamaño alrededor de 500GB.



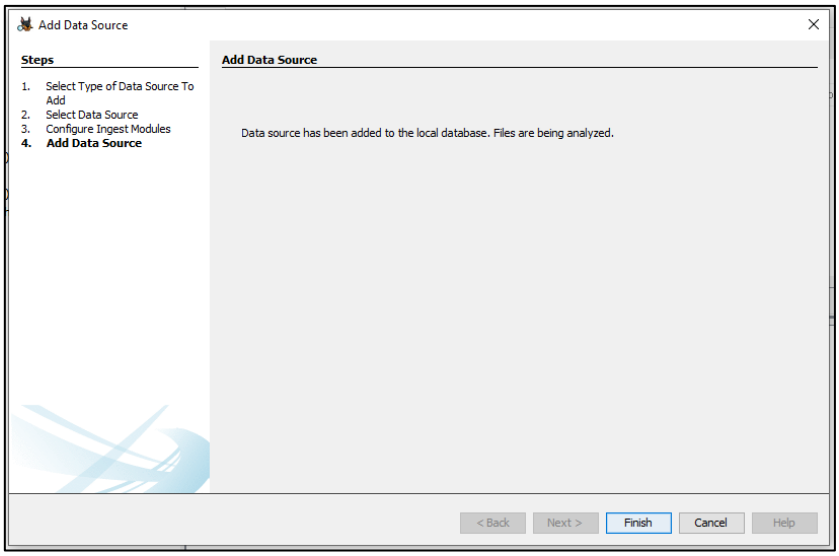


Figura 19: Inicio del proceso de análisis de la imagen forense

6. En la parte izquierda de la pantalla se visualizarán los diferentes módulos que se estén analizando, junto con el nombre del archivo escogido, y en la parte inferior el porcentaje de la ejecución del proceso de análisis también tomará el tiempo que sea necesario.

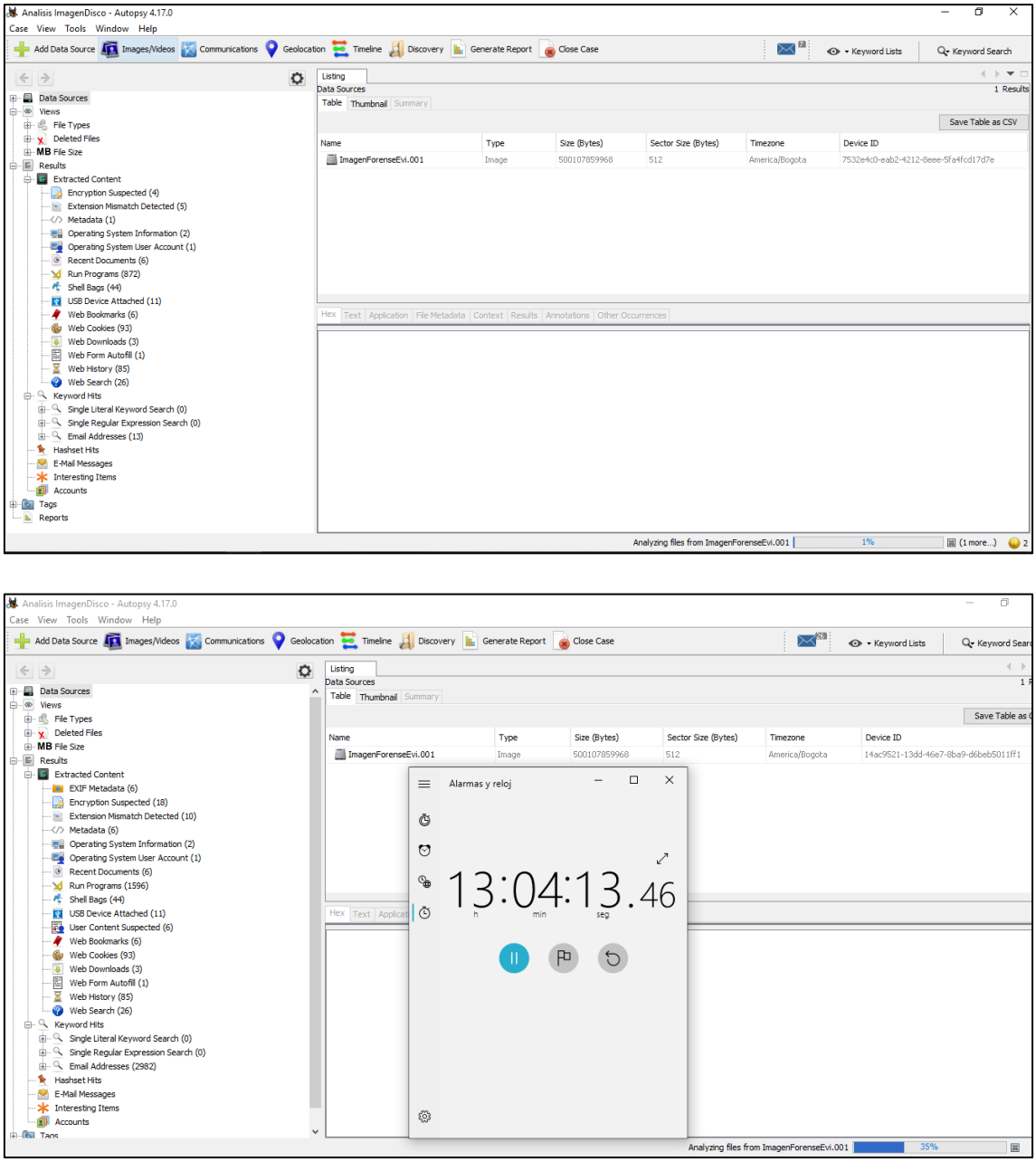


Figura 20: Proceso y espera del análisis

7. Finalizado el proceso de análisis se procede a indagar los tipos de archivos que se han encontrado y extraer la información que se considere útil para el caso que se esté gestionando. Este proceso tardó alrededor de 30 horas, aunque este tiempo dependerá del tipo de disco que se esté analizando y de las capacidades del computador, si es un disco de menor capacidad el tiempo durará mucho menos.

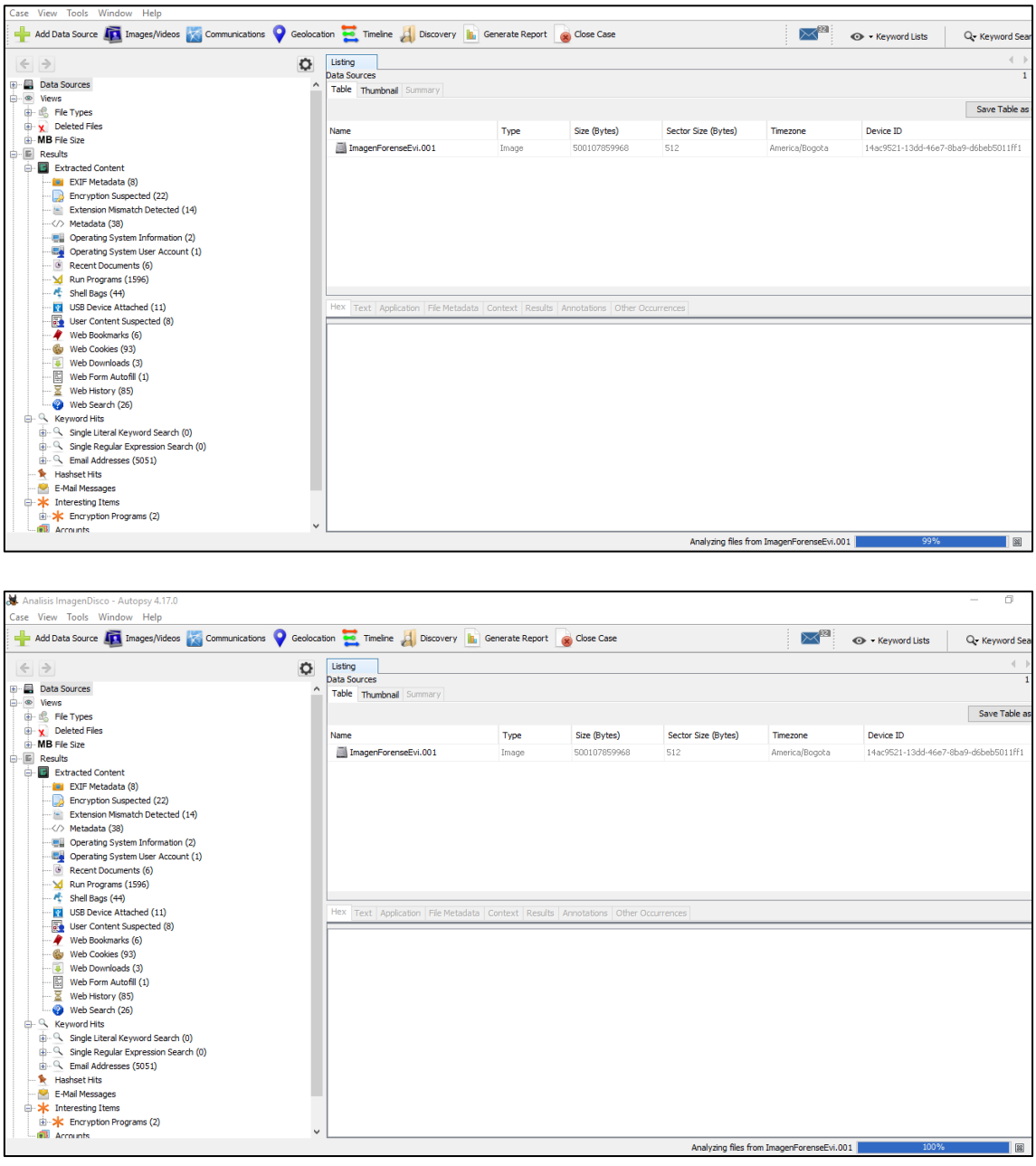


Figura 21: Duración y finalización del proceso de extracción de información

Una vez finalizada la extracción de información, se puede notar el tamaño de la información encontrada del caso, esta capacidad se la puede identificar en la carpeta creada para este proceso. Posteriormente se indaga los tipos de archivos obtenidos y sus respectivas extensiones.

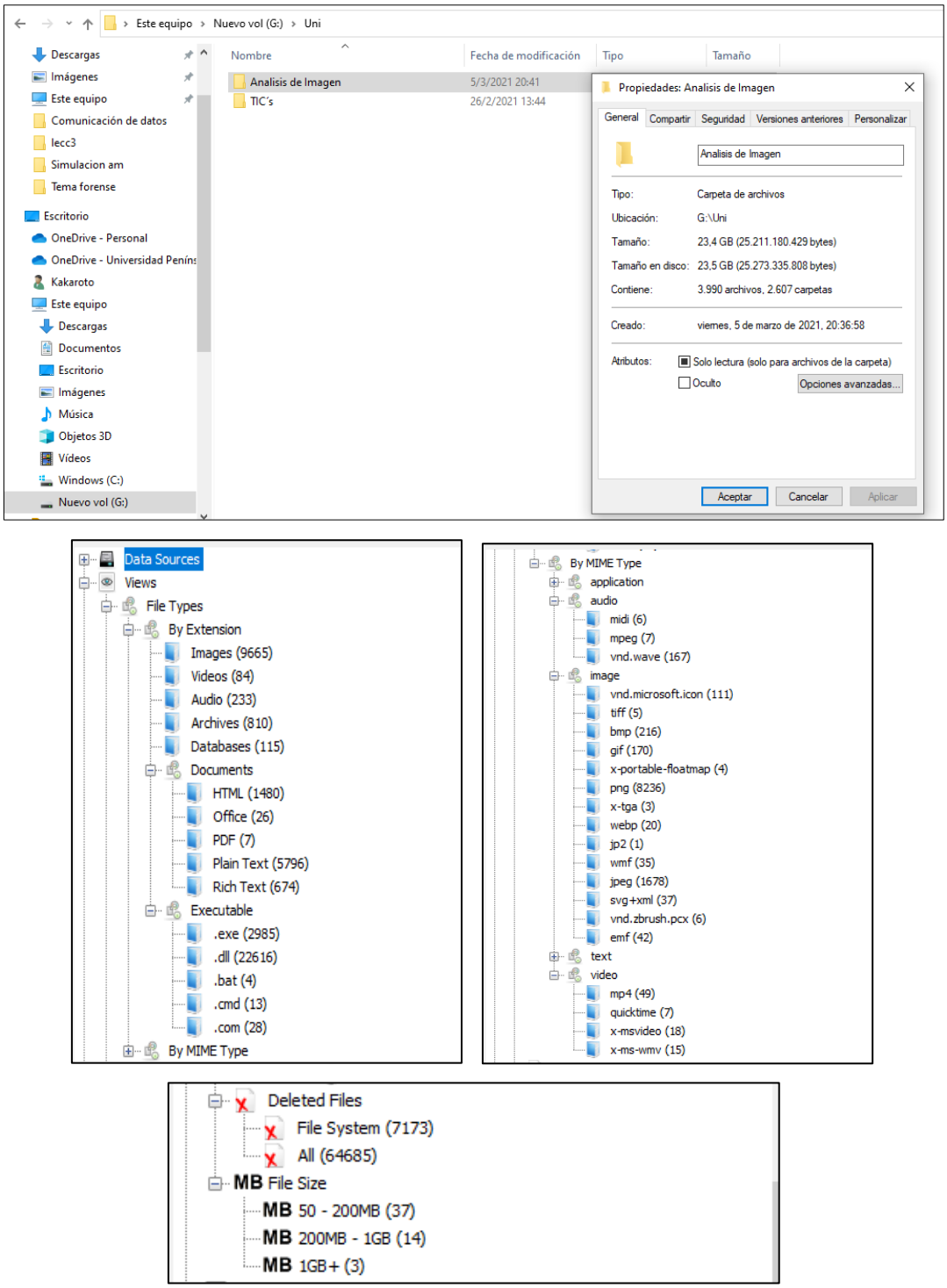


Figura 22: Verificación de los tipos de archivos e información por indagar

Se procede a indagar la información extraída, se ha llegado a obtener información valiosa entre ellas el nombre del dueño del computador, sistema operativo, imágenes y archivos que tienen relación con el caso que se está gestionando.

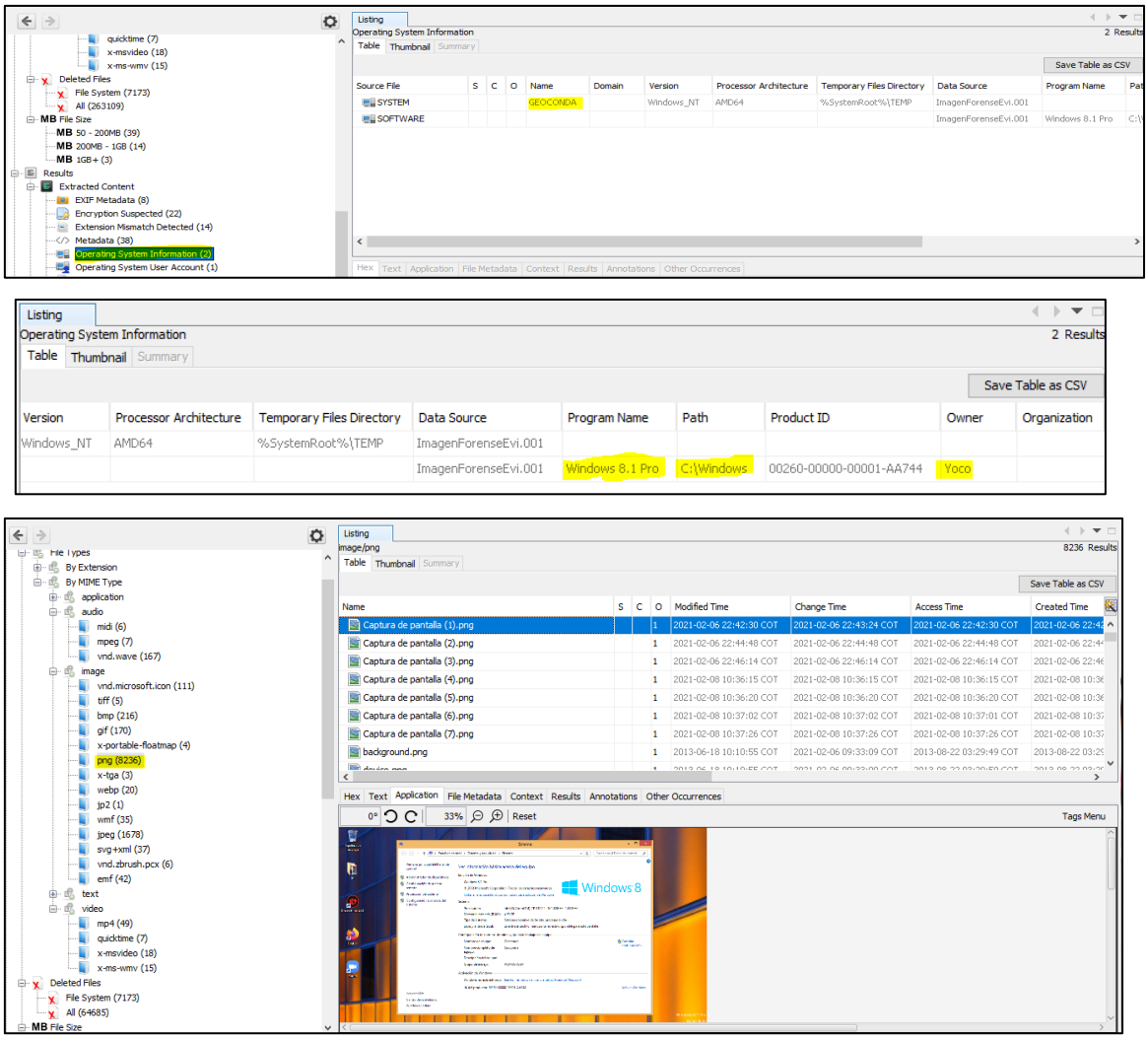


Figura 23: Captura de pantalla y datos del dueño del computador analizado

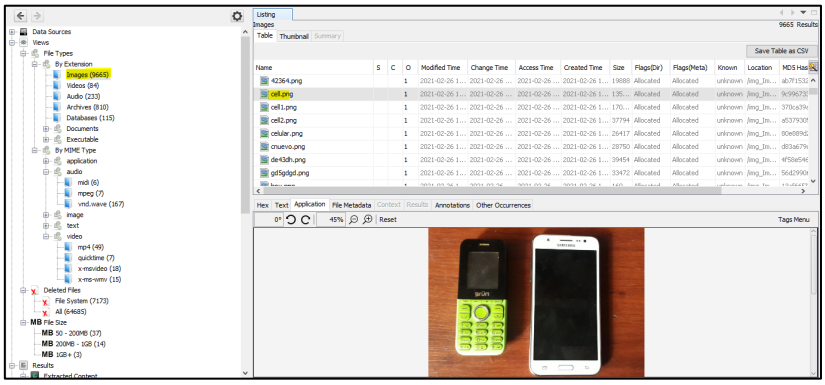


Figura 24: Imágenes obtenidas

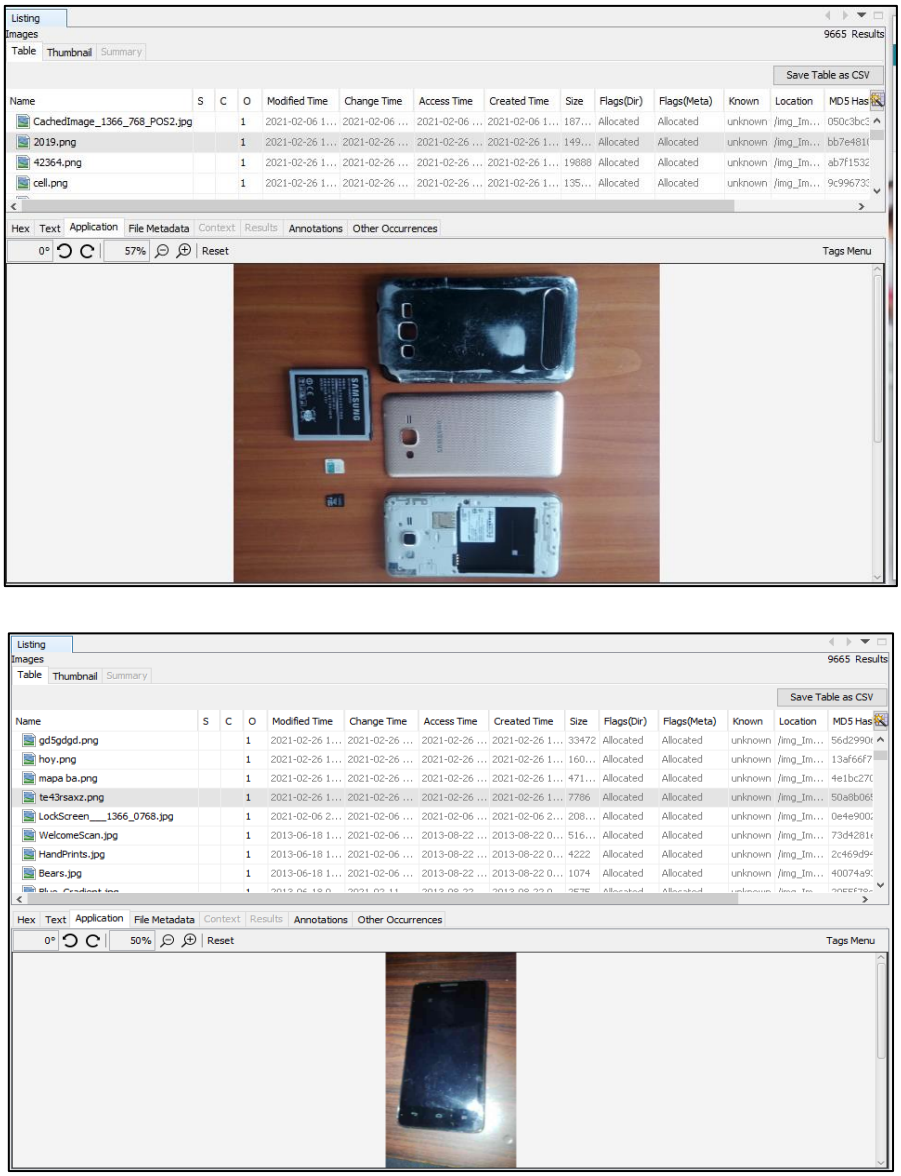


Figura 25: Imagen obtenida2

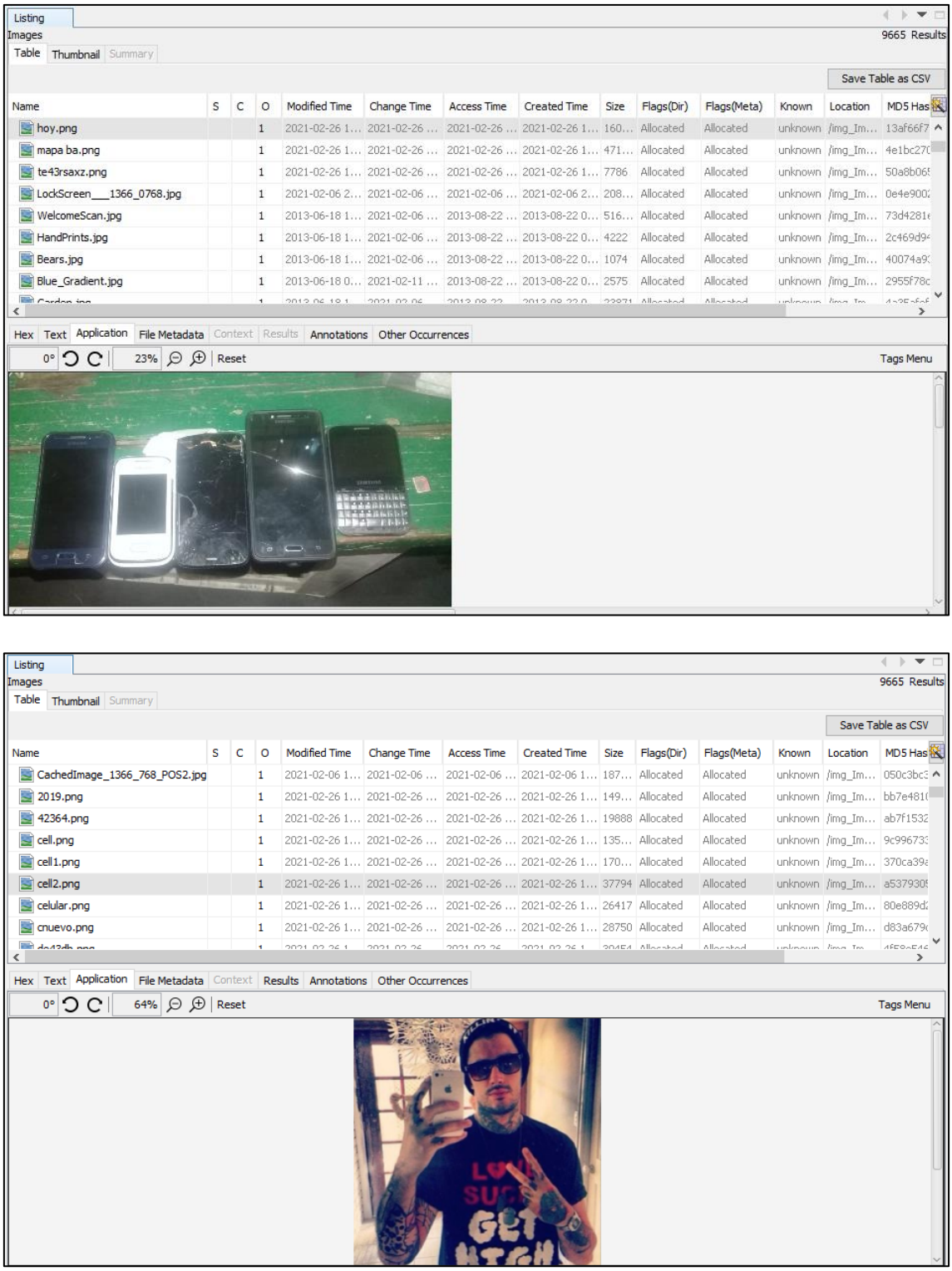


Figura 26: Fotos obtenidas

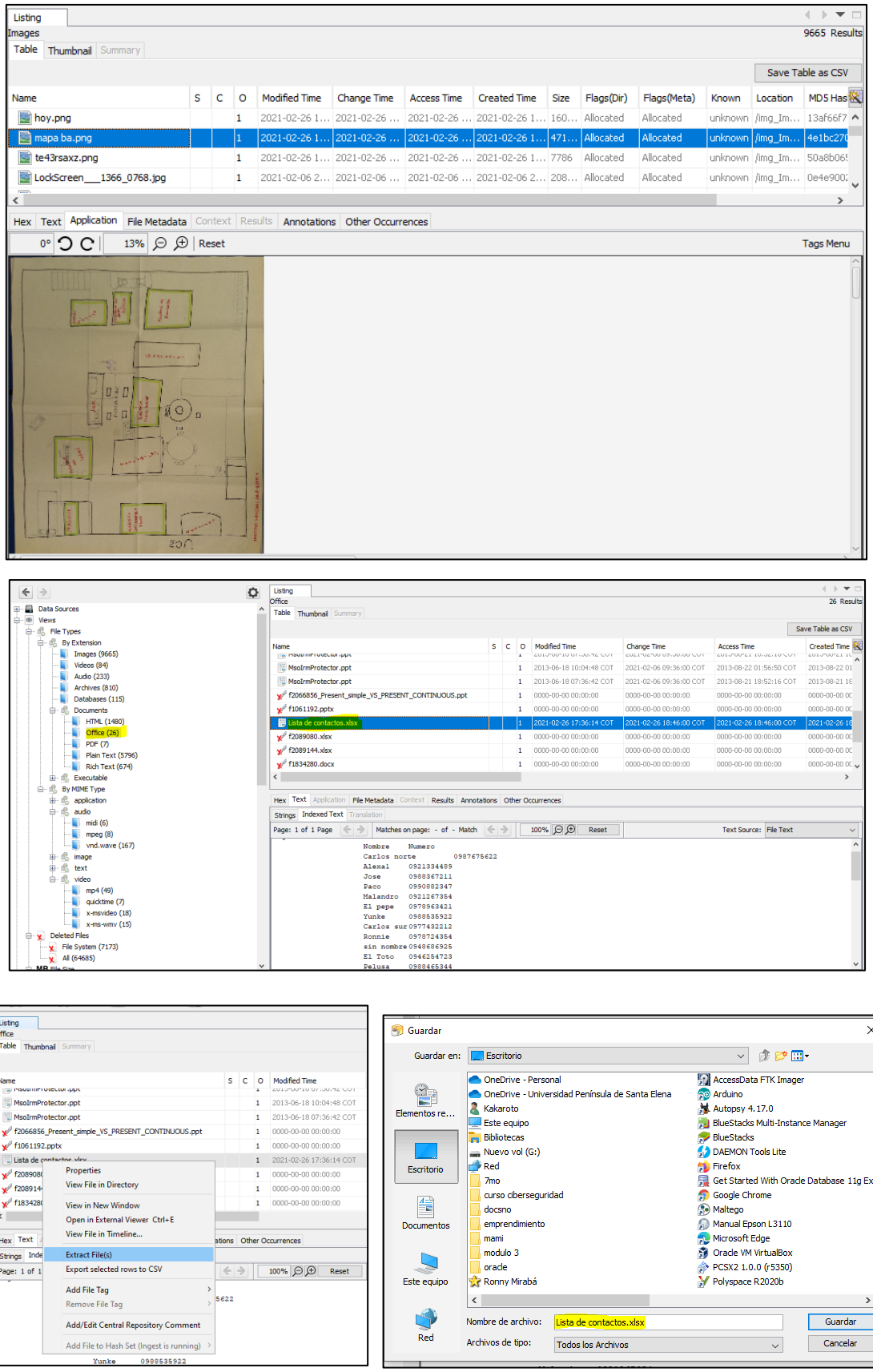
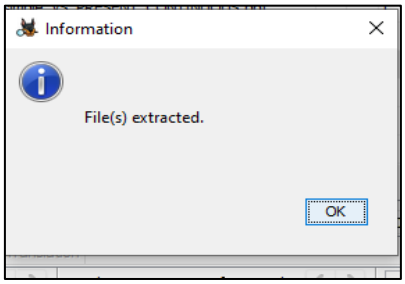


Figura 27: Datos de fotos y archivo encontrado

Se procede hacer la extracción del archivo .xlsx para su posterior verificación de datos almacenados.



Autoguardado Lista de contactos.xlsx

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revis

Pegar Calibri 11 Texto

Portapapeles Fuente Alineación

C13 0946254723

	A	B	C	D	E
1					
2		**Nombre**	**Numero**		
3		Carlos norte	0987675622		
4		Alexa1	0921334489		
5		Jose	0988367211		
6		Paco	0990882347		
7		Malandro	0921267354		
8		El pepe	0978963421		
9		Yunke	0988535922		
10		Carlos sur	0977432212		
11		Ronnie	0978724354		
12		sin nombre	0948686925		
13		El Toto	0946254723		
14		Pelusa	0988465344		
15		Guille	0987675634		

Figura 28: Extracción del archivo y verificación de datos

3.2.7 Fase IV. Documentación

Dentro de esta fase se procede a realizar un informe pericial (**Ver Anexo 5**) que será realizado por el perito informático, o en su caso por la persona que estuvo a cargo de hacer todo el proceso de la extracción de la evidencia digital, una vez elaborado se considera que sea presentado de manera física o en un formato de PDF a quien corresponda.

El formato base puede ser descargado desde la página oficial del Consejo de la Judicatura, en el apartado de peritos, es importante que el perito informático considere toda la información necesaria y sea redactada.

El objetivo final de un informe de peritaje es proporcionar la información que permite al tribunal, al juez o al abogado realizar correctamente su trabajo [26].

Para la elaboración del informe se surgiere, que se tomen en consideración los siguientes puntos:

- Identificación del perito
- Identificación de la escena del delito
- Objetivo del informe
- Descripción del dispositivo analizado
- Método y herramientas usadas
- Análisis y resultados
- Conclusiones
- Firma del responsable

Identificación del perito: Debe contener una breve descripción de la persona a cargo del caso, entre los puntos a redactar serian: Nombres, Identificación, Cargo, Caso asignado y Fecha de elaboración.

Identificación de la escena del delito: Un párrafo donde se identifique el caso que está investigando, tomando en consideración a las personas que le otorgaron dicha responsabilidad.

Objetivos del informe: Se incluye los objetivos del informe redactado, los objetivos dependerán del tipo de evidencia que se extrajo durante el proceso.

Descripción del dispositivo analizado: Se describe el tipo de dispositivo analizado, esto incluye las especificaciones técnicas de hardware y software.

Método y herramientas usadas: Hay que mencionar la metodología que se usó durante el proceso y las herramientas de hardware y software.

Análisis y resultados: Se redacta como se hizo el proceso de extracción de la evidencia y cuáles fueron los resultados obtenidos durante el mismo.

Conclusiones: en este punto se redacta los puntos más importantes de la pericia y los que se consideren claves al momento de realizar la extracción de la información.

Firma del responsable: Al final del informe se plasma la firma de la persona responsable de la elaboración del informe.

3.2.8 Fase V. Presentación

Esta fase final trata de prácticamente presentar el informe pericial elaborado en la fase anterior de Documentación, esta presentación se la hace con una única observación, esto quiere decir que se la hace de forma presencial. Este informe se lo presenta delante de un juez o tribunal si fuera el caso.

La persona encargada del proceso o el perito designado debe prepararse para contestar acertadamente todo tipo de preguntas que se hagan con respecto a su trabajo realizado. Teniendo la capacidad profesional para defender su trabajo, dentro de esta presentación se resalta un punto muy importante, este es no usar palabras netamente técnicas en cuanto al área de la informática se refiere, esto se debe porque las personas que estarán presentes no son expertas en el tema. Por lo tanto, debe hacerse entender.

Sin embargo, los peritos volverán a declarar cuantas veces lo ordene el juzgador en la audiencia del juicio, como lo establece el Artículo 503, inciso tres del COIP. Existen algunas habilidades y destrezas que debe tener en cuenta al momento de presentar su trabajo, las cuales son:

- Tener una vestimenta que este adecuada al contexto.
- Mantener una actitud respetuosa hacia los demás profesionales que podrían discrepar su informe.
- Responder a las diferentes preguntas de una manera clara y comprensible.
- Deberá acreditar su experiencia y exponer los fundamentos de los resultados de su pericia.
- Puede ayudarse con ilustraciones gráficas, estas ilustraciones también las puede usar para responder una pregunta si es necesario.
- Debe estar preparado cuando el juez ordene un debate entre peritos de ambos lados, manteniendo siempre el respeto y profesionalidad del caso.
- No debe aclarar si existe un culpable del caso en cuestión, esto no sería nada ético y profesional de su parte.

CONCLUSIONES

- El desarrollo de esta guía de análisis forense digital permitirá saber y fortalecer el proceso de extracción de evidencias.
- La fase de análisis, una de las importantes dentro del presente trabajo, nos permite trabajar con las herramientas que fueron establecidas para realizar el proceso de extracción de información que sea considerada útil.
- Los pasos que se siguieron fueron establecidos por las cinco fases de la metodología UNE 71506:2013 gracias a ello se estableció un orden dentro del proceso.
- Los datos que se han encontrado una vez hecho el análisis de la imagen forense, se los podrá plasmar dentro del informe pericial.

RECOMENDACIONES

- Tener en claro que metodología usar al momento de querer realizar una guía, esta buena elección ayuda tener una base de como comenzar el proceso.
- No se debe trabajar directamente con el disco, se recomienda realizar más de una copia, tener un respaldo adicional ayuda un correcto análisis en el caso de daño o pérdida.
- Al momento de querer hacer el proceso de extracción de evidencias es recomendable cumplir con los pasos de la metodología que se establezca, esto ayuda a tener un orden al momento de realizar un análisis.
- Es importante contar con las herramientas necesarias al momento de realizar un análisis, con ellas se agiliza el proceso para la creación de la imagen forense y su posterior análisis.
- Esta guía esta hecha para tener el conocimiento del proceso de creación de una imagen forense y posterior extracción de evidencias, no es un sustento para ser usado legalmente.
- Las herramientas usadas son de software libre, por lo tanto, dentro de un ambiente real no podrían ser validas.

BIBLIOGRAFÍA

[1] L. C. Byron, «UISEK,» 2018. [En línea]. Available: https://repositorio.uisek.edu.ec/bitstream/123456789/2758/1/LOARTE-BYRON.pdf.

[2] E. Flores, M. Asanza y M. Berrones, «EconPapers,» Septiembre 2014. [En línea]. Available: https://www.eumed.net/rev/cccss/29/ciberdelincuencia.html.

[3] L. Haz López, Interviewee, *Ing. En Sistemas Computacionales. Msi.*. [Entrevista]. Noviembre 2020.

[4] J. León Marcos y M. Lozano Merino, «Incibe,» [En línea]. Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72987/6/jjlmarcosTFM1217Memoria.pdf.

[5] D. Pereira y J. Eterovic, «core.ac,» [En línea]. Available: https://core.ac.uk/download/pdf/296377028.pdf.

[6] Basis, «Autopsy Digital Forensics,» [En línea]. Available: https://www.autopsy.com/.

[7] N. Bassetti, «https://www.caine-live.net/,» GNU/Linux. [En línea].

[8] AccessData, «AccesData. An exterro company,» ACCES DATA, [En línea]. Available: https://accessdata.com/products-services/forensic-toolkit-ftk.

[9] D. GNU/Linux, «KALI by offensive Security,» GNU/Linux, 13 Marzo 2013. [En línea]. Available: https://www.kali.org/.

[10] e-fense, «e-fense Carpe Datum,» Carpe Datum, [En línea]. Available: http://www.e-fense.com/.

[11] VMware, «wmwareLatam,» VMware, Inc, [En línea]. Available: https://www.vmware.com/latam/products/workstation-pro/workstation-pro-evaluation.html. [Último acceso: 14 Febrero 2021].

[12] D. Brant, «DiskDigger,» Enero 2021. [En línea]. Available: https://diskdigger.org/.

[13] G. T. Gabriela, «UPS,» 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/8943/1/UPS-CT005203.pdf.

[14] M. López, «OAS.org,» Junio 2007. [En línea]. Available: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf. [Último acceso: 2021].

[15] G. N. d. Ecuador, «planificacion.gob.ec,» 2017. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/downloads/2017/10/PNBV-26-OCT-FINAL_0K.compressed1.pdf.

[16] R. Creutzburg, M. Sánchez, J. Flores, C. Chapela y C. Ricalde, Seguridad Informática y Análisis Forense Digital, Brandenburg: Wikipedians, 2016.

[17] M. T. Robles Belmonte, «DOCPLAYER,» 2017. [En línea]. Available: https://docplayer.es/38155519-Guia-metodologica-que-es-como-se-realiza-1-definicion-de-objetivo-alcance-y-audiencia-aprobacion-difusion-edicion-y-diseno.html. [Último acceso: Junio 2021].

[18] PRAKMATIC, «Prakmatic.com,» 2021. [En línea]. Available: https://www.prakmatic.com/tipos-de-analisis-forense-para-tratar-incidentes-de-seguridad/. [Último acceso: Junio 2021].

[19] «CIBERSEGURIDAD,» wordpress, 2021. [En línea]. Available: https://ciberseguridad.com/servicios/analisis-forense/. [Último acceso: Junio 2021].

[20] PERITO JUDICIAL GROUP, «peritojudicial,» PJGROUP, [En línea]. Available: https://peritojudicial.com/que-es-un-perito-como-ser-perito/. [Último acceso: Junio 2021].

[21] F. Tablado, «GRUPO ATICO34,» 26 Mayo 2020. [En línea]. Available: https://protecciondatos-lopd.com/empresas/perito-informatico-peritaje/. [Último acceso: Junio 2021].

[22] P. R. Jaramillo Montoya, «puce.edu.ec,» Junio 2019. [En línea]. Available: http://repositorio.puce.edu.ec/bitstream/handle/22000/17774/Romina_Jaramillo_Tabajo_de_Titulacion.pdf?sequence=1&isAllowed=y. [Último acceso: Julio 2021].

[23] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, METODOLOGÍA DE LA INVESTIGACIÓN, México: Mc Graw Hill Education, 1998.

[24] UNE, «Audea,» 13 Septiembre 2013. [En línea]. Available: https://www.audea.com/aenor-publica-nueva-norma-une-715062013/.

[25] «CONSEJO DE LA JUDICATURA,» 2014. [En línea]. Available: https://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2014cj/040-2014.pdf. [Último acceso: 5 Febrero 2021].

[26] C. Aldama, «ALDAMA. Informática Legal,» [En línea]. Available: https://informatica-legal.es/informes-periciales-perito-contratar/. [Último acceso: 12 Marzo 2021].

[27] R. 3227, «CiberForensic,» 16 Junio 2020. [En línea]. Available: https://www.ciberforensic.com/directrices-rfc-3227. [Último acceso: 12 Febrero 2021].

[28] SOURCE FORGE, «guymager,» 3 Mayo 2020. [En línea]. Available: https://guymager.sourceforge.io/. [Último acceso: 14 Febrero 2021].

ANEXOS

Anexo 1: Formato de entrevista

Universidad Estatal Península de Santa Elena
Santa Elena – La Libertad
Entrevista de Tema de Proyecto de Titulación

DISEÑO DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL EN EQUIPOS CON SISTEMA OPERATIVO WINDOWS 8.1

Nombre: _____

Profesión: _____

Cargo laboral: _____

Preguntas:

¿Qué opina acerca de la elaboración de una guía metodológica para un análisis forense digital?

¿Qué se debe hacer antes de realizar una guía para análisis forense digital?

¿Qué elementos o herramientas hay que considera que son útiles para realizar un análisis forense?

¿Qué tan importante considera la evidencia digital dentro de un proceso judicial?

¿Cuál metodología cree usted que sería la más factible de usar para la elaboración de este trabajo de titulación?

¿Qué recomendaciones daría al momento de hacer la documentación una vez finalizado el proceso de extracción de la información?

Anexo 2: Formulario de información personal del perito a cargo del proceso de investigación

FORMULARIO N° 1	
Lugar y Fecha	
Nombres y Apellidos	
Numero de cédula	
e-mail	
Especializacion	
Codigo de Perito	
Institucion	
Firma del Perito a cargo del caso **----------**	

Anexo 3: Formulario de información referente a la escena o entorno y el estado del equipo a analizar

FORMULARIO N° 2		
Lugar		
Id del caso		
Fecha y Hora		
Número de personas en la escena		
Declaraciones de las personas		
Nombres de las personas en la escena		
Nombres de personas que tendrán acceso al equipo por analizar.		
Descripción del Equipo por Analizar		
Id de equipo (etiqueta)		
Tipo de dispositivo		
Descripción del dispositivo (fisica)		
Estado encendido	Si	No
Estado apagado	Si	No

Ubicación		
Dispositivos conectados		
Conexión a Internet	Si	No
Foto del Dispositivo		
Observaciones		
Firma del Perito Informático ----------	Firma del Notario o Fiscal ----------	

Anexo 4: Formulario de información del equipo y los medios de almacenamiento encontrados

FORMULARIO N° 3 Recopilacion y transporte de la evidencia					
Id del caso					
Nombre del Perito					
Numero de Etiqueta					
Fecha y hora					
Lugar					
Equipo encontrado					
Estado			Encendido	Apagado	
Observación					
Descripción del Equipo					
Marca del Equipo	Serie	Memoria RAM	Procesador	Sistema Operativo	Disco Duro
Descripción de medios de almacenamiento					
Tipo de dispositivo		Marca		Capacidad	
Firmas					
Firma del Perito Informático ----------		Firma del Notario o Fiscal ----------			

Anexo 5: Informe Pericial

La Libertad, 15 de noviembre del 2020

“INFORME PERICIAL”

Yo, Freddy José Mirabá Quimí con cedula de ciudadanía N° 2450000000 siendo considerado como perito informático calificado por la republica del Ecuador, pongo en contexto que se me ha sido asignado el caso N° 9999999-9 por sospechas de hurto de dispositivos móviles. Informo que a los 9 días del mes de noviembre del año 2020 alrededor de las 9 Am se me ha asignado el cargo de perito informático.

Y es por lo que redacto los puntos más relevantes del proceso de extracción de evidencia en el siguiente escrito.

Identificación de la escena del delito.

Dentro del caso N° 9999999-9 se informa que la policía nacional intercepta una vivienda donde los moradores han dado información de supuesto robo de dispositivos móviles y consideran que los sospechosos habitan en ella. Se ha encontrado un computador para proceder hacer el respectivo análisis forense digital, el cual se ha entregado al perito informático designado para que proceda hacer su trabajo. Dicho caso ha sido asignado por el fiscal de turno.

Objetivos del informe.

- Trasladar el equipo informático al lugar donde se hará el proceso de análisis.
- Usar las herramientas adecuadas que cumplan con el análisis.
- Extraer evidencia que se considere importante del caso en cuestión, fotos, documentos, etc.
- Identificar los datos encontrados y presentarlos en el presente informe.

Método y herramientas usadas.

Para el proceso de extracción de la evidencia se usó la norma: UNE 71506:2013, que es una de las normas más adecuadas para el caso de análisis forense, por lo que sus fases están bien definidas y se sigue un orden para este tipo de análisis.

Las herramientas de hardware y software usadas para este proceso han sido definidas por el perito, puesto que es el mismo que hará el uso de estas, y es favorable que se sienta con toda la comodidad necesaria durante el proceso que se le ha asignado.

Tabla de herramientas de hardware y software usadas.

HARDWARE	SOFTWARE
Laptop Lenovo Ideapad Core i5	Windows
Lector de Disco Duro 3.5 Sata a Usb	Regedit
Lector de Disco Duro 2.5 Sata a Usb	AccessData FTK
Herramientas: • Destornilladores • Cuchillo • Guantes • Pulsera antiestática • Tijeras	Autopsy

Descripción del dispositivo analizado

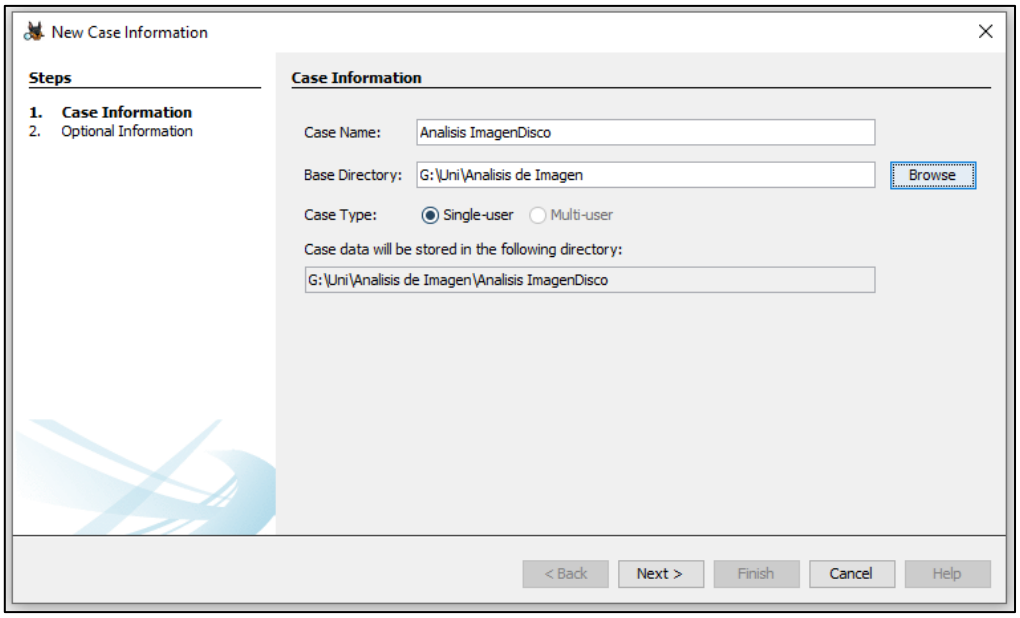
Especificaciones técnicas:

Procesador	**Intel Atom CPU D425 de 1.8 GHz**
Disco Duro	Tipo Serial ATA Device particionado. 176 GB sistema y 290 GB libres
Memoria	4 GB DDR3 de 800 MHz
Motherboard	Placa de escritotio Intel D425KT mini ITX DDR3 con microporcesador incorporado.

Análisis y Resultados.

Proceso de análisis de Imagen Forense generada.

Una vez se haya generado la imagen forense del disco duro el siguiente paso es hacer el proceso de análisis, para este proceso se usará el software forense Autopsy, tiene las cualidades necesarias para poder hacer este tipo de investigaciones forenses digitales.



Finalizada la extracción de información, se puede notar el tamaño de información encontrada, esta capacidad se la puede identificar en la carpeta creada para este proceso. Posteriormente se indaga los tipos de archivos obtenidos y sus respectivas extensiones.

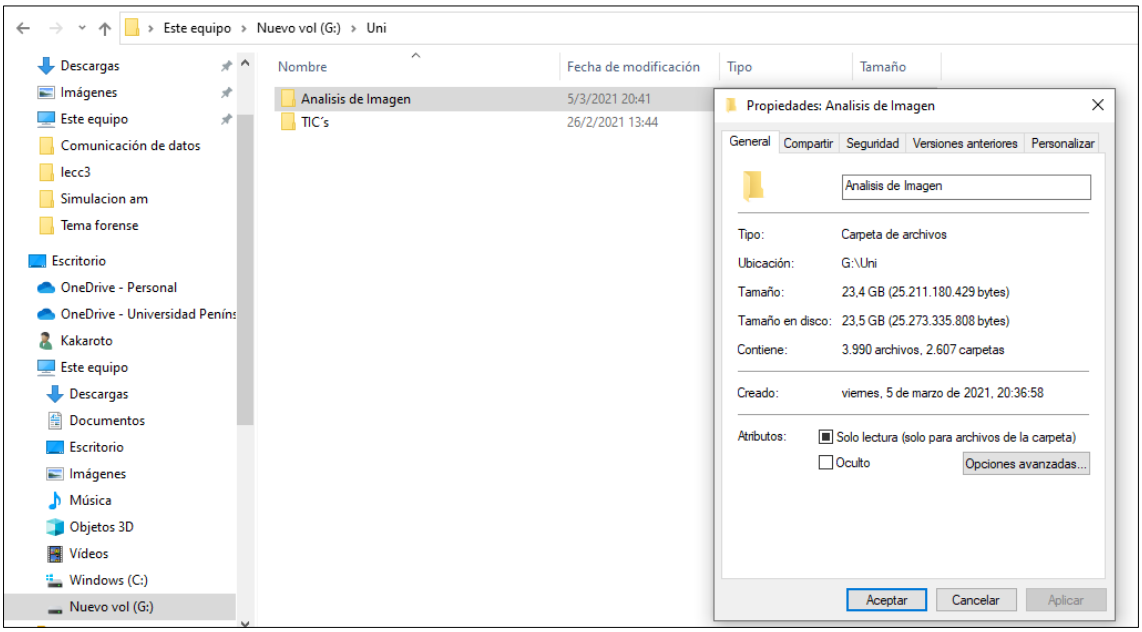


Figura Capacidad de la carpeta del caso generado.

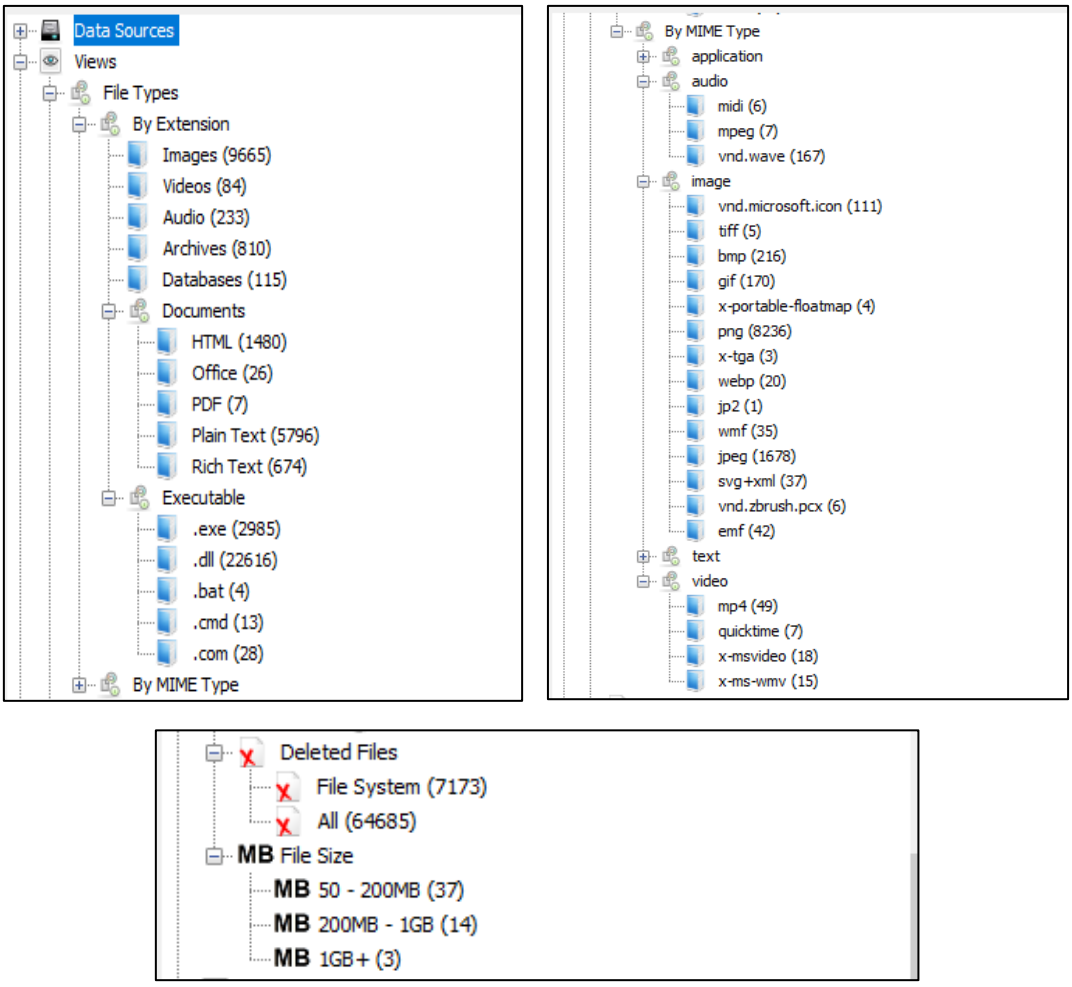
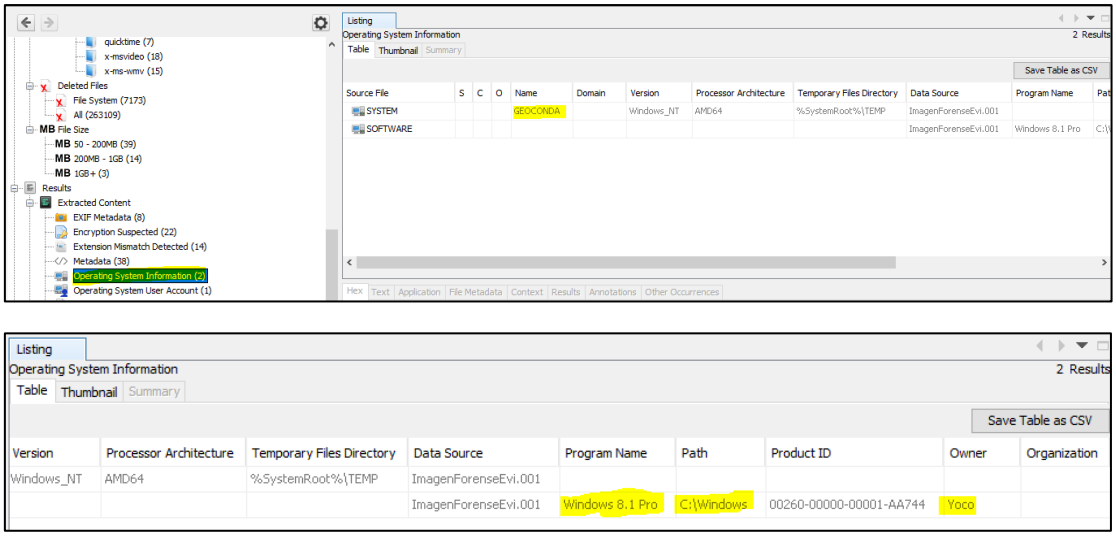


Figura Verificación de los tipos de archivos e información por indagar

Indagando se ha llegado a obtener información, entre ellas el nombre del dueño del computador e imágenes y archivos que tienen relación con el caso que se está gestionando.



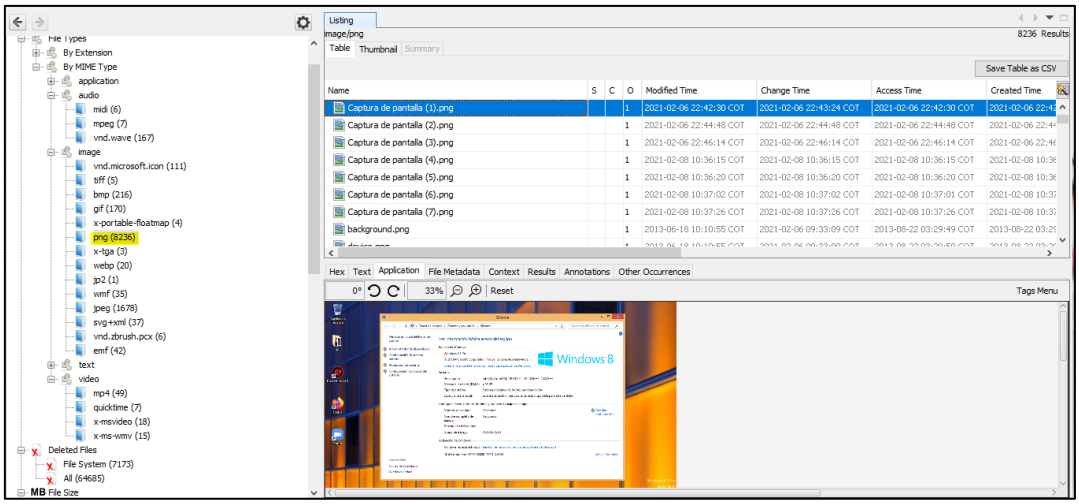


Figura Captura de pantalla y datos del computador analizado y el Sistema Operativo.

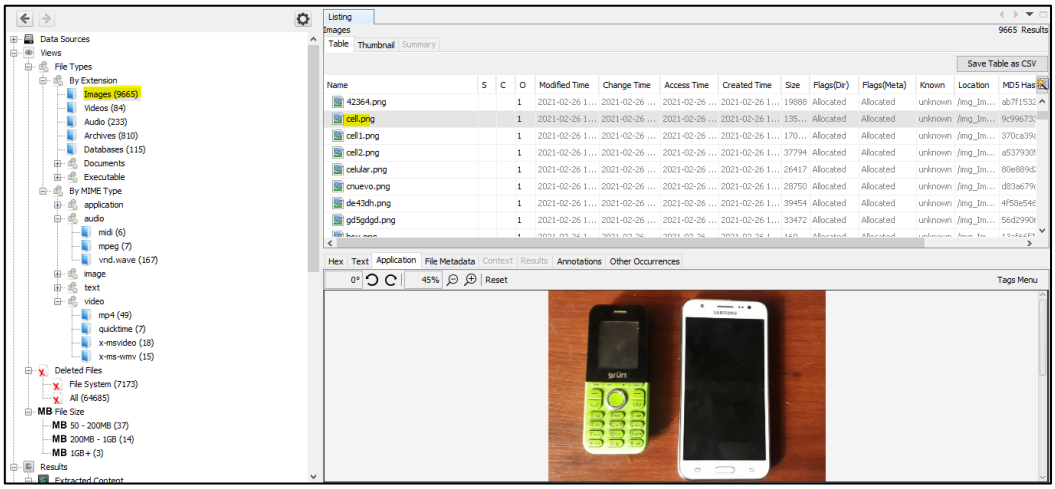
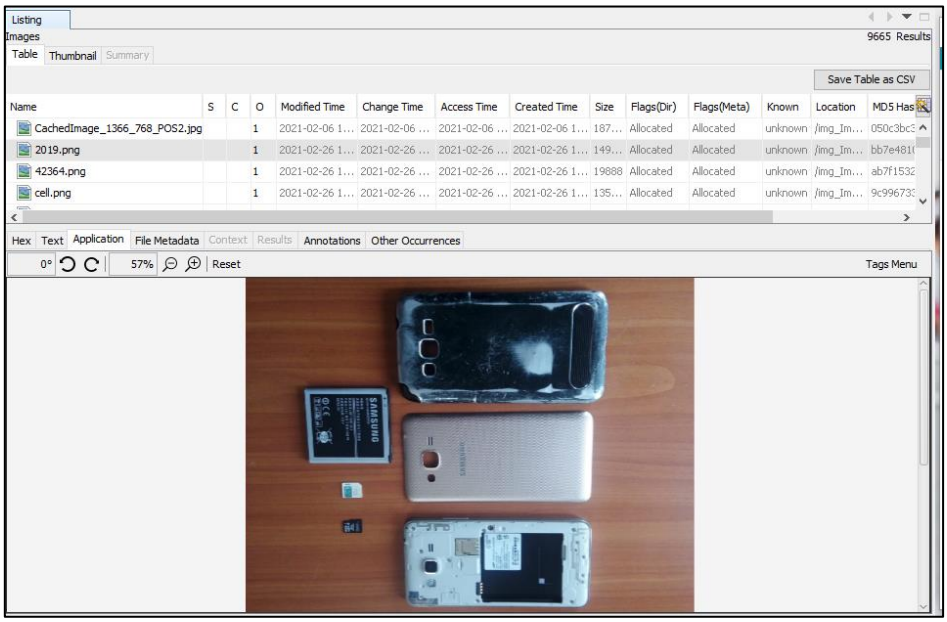


Figura Foto obtenida



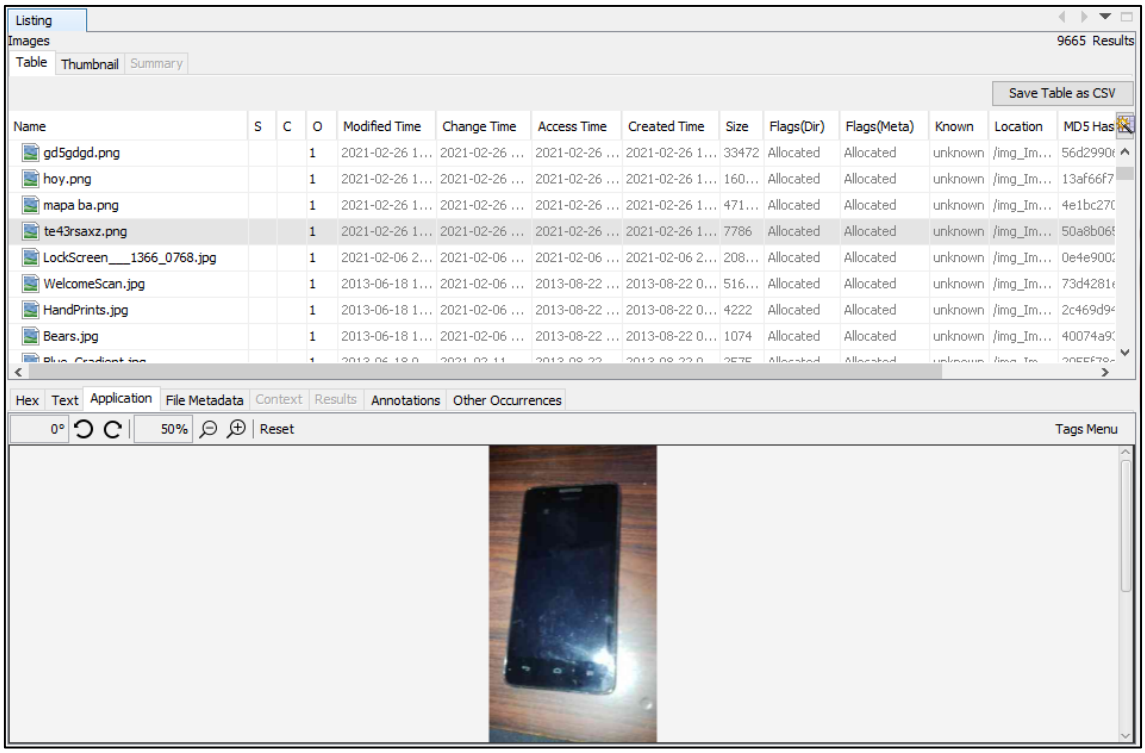
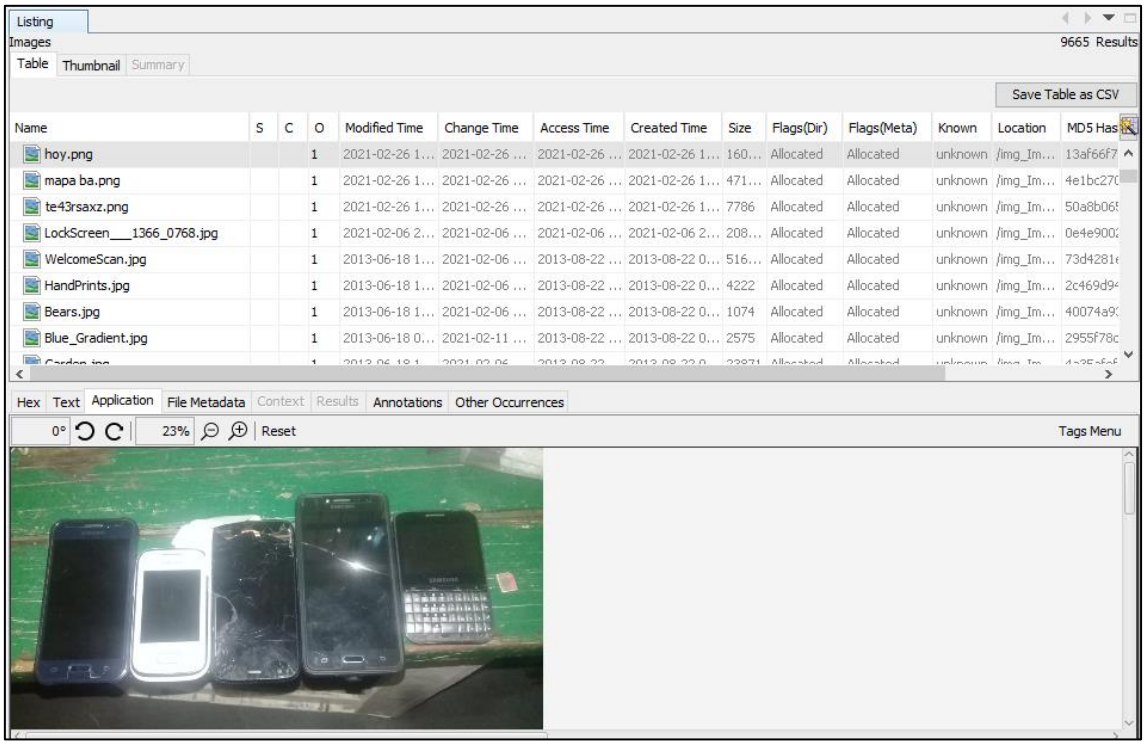


Figura Foto obtenida



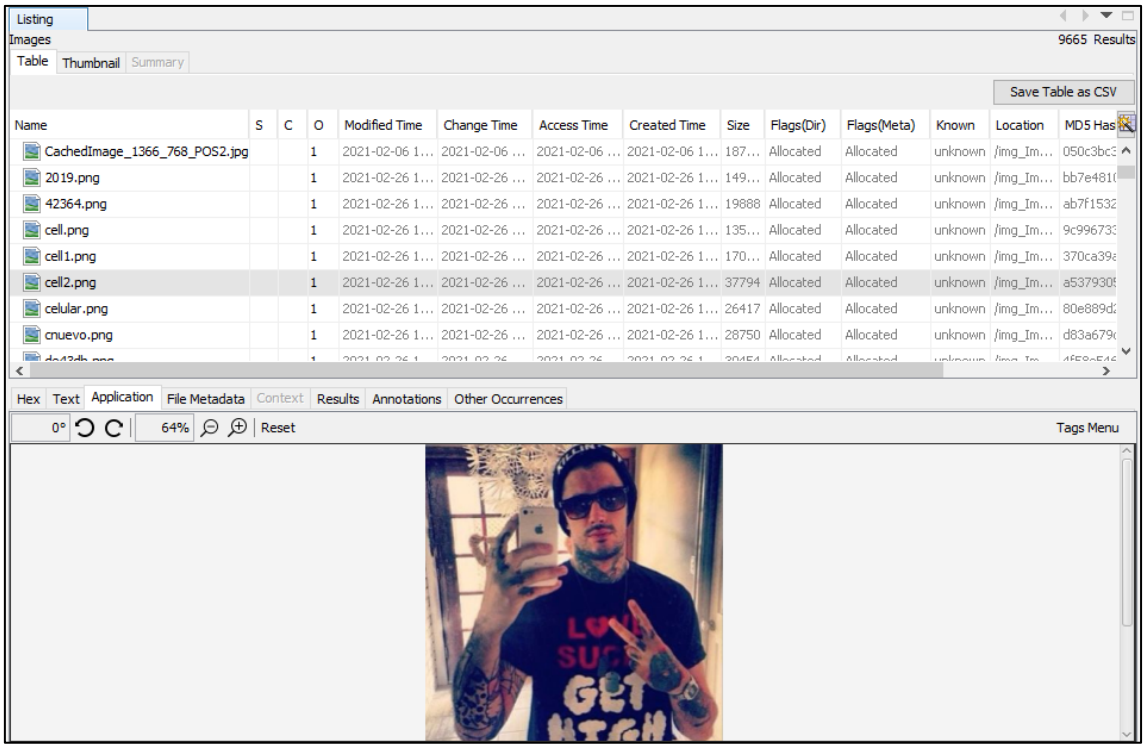


Figura Foto Obtenida

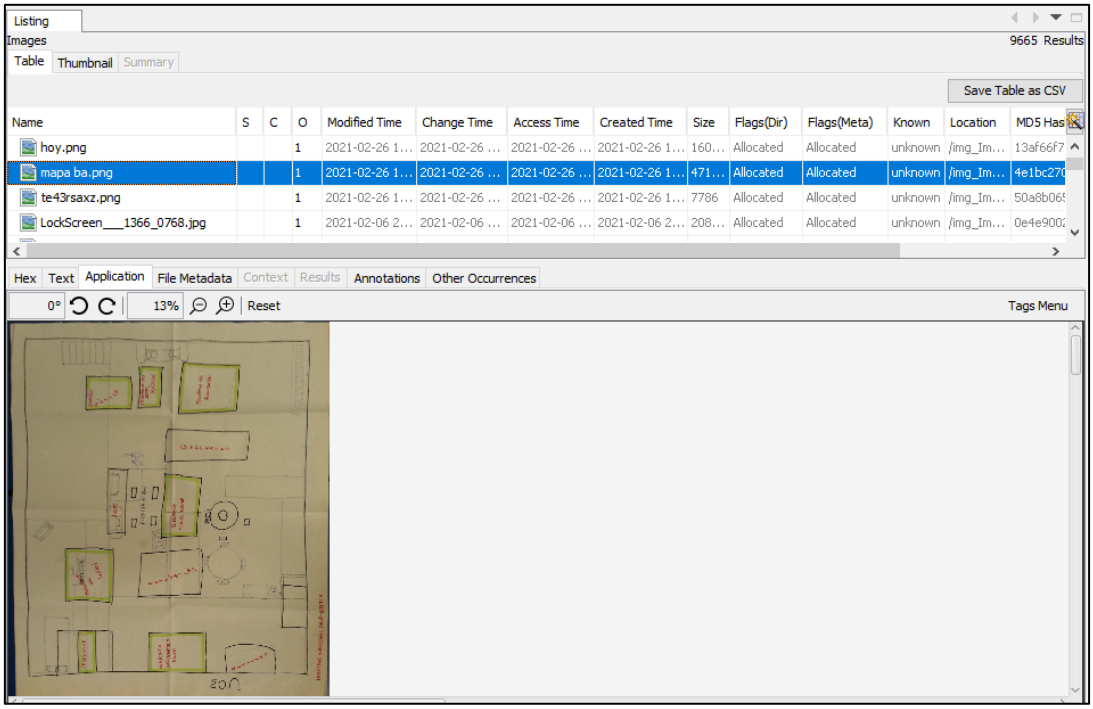
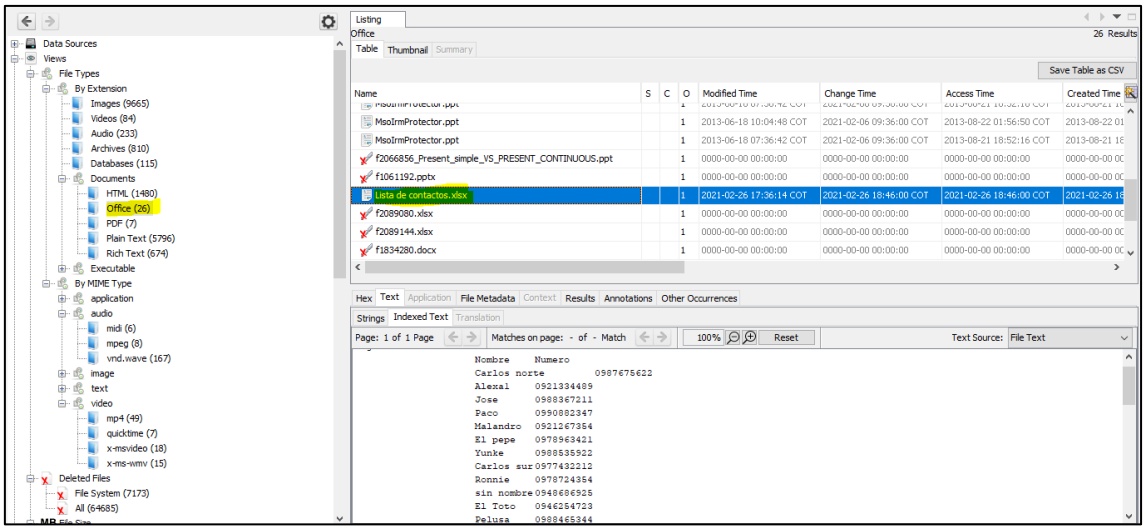


Figura Foto de un croquis obtenido



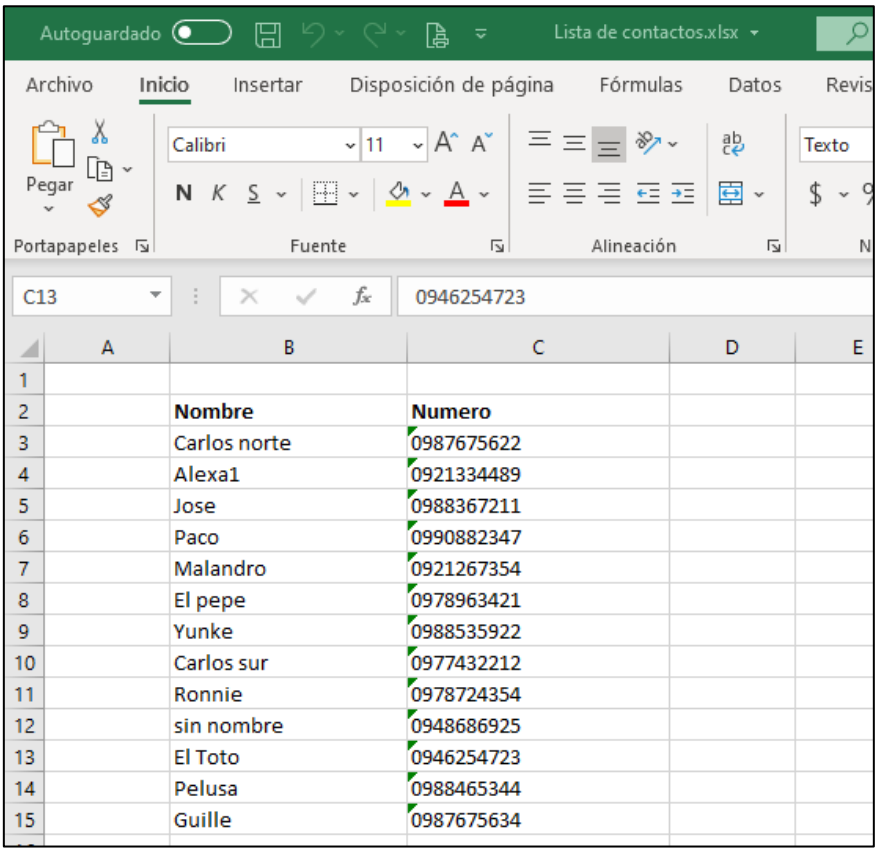


Figura Extracción del archivo y análisis de datos

Conclusiones.

A partir del respectivo análisis de la imagen forense generada, se puede mencionar los siguientes puntos:

- Se hizo un doble análisis en la imagen forense, es necesario saber el tamaño de la información que se esté analizando para poder almacenarla.

- Las fotos y los diferentes datos se los pudo extraer de las carpetas generadas con el software Autopsy, mostrando sus respectivas extensiones.

- El sistema operativo del equipo analizado es un Windows 8.1, así mismo se muestra el nombre del usuario.

_____

Freddy Mirabá Quimí

Perito Informático

CI: 2400000000