HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL ORIENTADAS A INFRAESTRUCTURAS TI COMO MEDIO DE INVESTIGACIÓN EN DELITOS INFORMÁTICOS

KELLY KATHERINE RADA JIMENEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANCABERMEJA
2022

HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL ORIENTADAS A INFRAESTRUCTURAS TI COMO MEDIO DE INVESTIGACIÓN EN DELITOS INFORMÁTICOS

KELLY KATHERINE RADA JIMENEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. John Freddy Quintero
Director.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANCABERMEJA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Barrancabermeja, 21 de mayo de 2022

DEDICATORIA

Dedicado a mi hijo Daniel Felipe Cruz, quien fue el motivo a seguir creciendo profesionalmente, a mi esposo Luis Fernando, a mi mamá Agneris y a mis hermanas Wendy Paola y Nectalina Sofia por su amor, entusiasmo, comprensión, paciencia y apoyo incondicional en cada etapa vivida para la realización satisfactoria de este trabajo.

A Dios, a la Virgen María y al Espíritu Santo por la salud, protección y resiliencia en tiempos de pandemia para realizar mi entrega a tiempo.

AGRADECIMIENTOS

Agradezco a Dios por esta oportunidad, a mi familia, compañeros y tutores que me ayudaron durante todo el proceso.

Agradezco a la ingeniera Yenny Estella Núñez y el ingeniero John Freddy Quintero de la Universidad Nacional Abierta y a Distancia UNAD por su disposición y colaboración en el acompañamiento en el proceso para que fuera posible.

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

RESUMEN

Para las organizaciones es de suma importancia que todas las actividades que se realicen en su interior sean confidenciales, no por el hecho de querer ocultar o desviar información sino para prevenir posibles alteraciones, robos, copias u otros tipos de acciones que perjudiquen el buen funcionamiento de una empresa. Principalmente si se encuentran guardados en equipos tecnológicos siendo este el recurso más utilizado en la actualidad el cual ha permitido optimizar el manejo de sus operaciones.

Entre las herramientas más populares para un análisis forense digital aplicables en investigaciones de delitos informáticos están las herramientas de análisis de red como el Snort, Nmap, Wireshark, Xplico. También están las herramientas para tratamiento de discos: el Dcdd3, Mount Manager, Guymager. Herramientas para tratamiento de memoria como el Volatility, Memoryze, RedLine. Así mismo las herramientas para el análisis de aplicaciones OllyDbg, OfficeMalScanner, Radare, Process explorer, PDFStreamDumper. Y las Suites de aplicaciones como DEFT, EnCase, ForLEx, CAINE (Computer Aided Investígate Environment), Autopsy.

Estos instrumentos muestran los efectos de las situaciones generadas por las violaciones a los sistemas, proporcionan el conocimiento a las personas encargadas para que sepan cómo actuar ante un delito informático, las herramientas a utilizar para mejorar la seguridad de la información, logrando reducir el riesgo de los delitos informáticos.

Palabras Clave: Análisis Forense Digital, Delitos informáticos, Herramientas Forenses, Informática Forense, Información, Investigación, Seguridad Informática, Tecnología.

ABSTRACT

For organizations it is of the utmost importance that all activities carried out within them are confidential, not because they want to hide or divert information but to prevent possible alterations, theft, copies or other types of actions that may impair the proper functioning of a company. Mainly if they are stored in technological equipment, this being the most used resource today which has allowed to optimize the management of its operations.

Among the most popular tools for a digital forensic analysis applicable in computer crime investigations are network analysis tools such as Snort, Nmap, Wireshark, Xplico.

There are also the tools for disk handling: the Dcdd3, Mount Manager, Guymager.
Tools for memory treatment such as Volatility, Memoryze, RedLine.
Also, the tools for the analysis of OllyDbg, OfficeMalScanner, Radare, Process explorer, PDFStreamDumper applications.
And the Suites of applications like DEFT, ForLEx, CAINE (Computer Aided Investigate Environment), Autopsy.

These instruments show the effects of the situations generated by the violations of the systems, provide the knowledge to the people in charge so that they know how to act before a computer crime, the tools to be used to improve the security of the information, managing to reduce the risk of computer crimes.

KEYWORDS: Cybercrime, Computer Forensic Tools, Digital Forensic Analysis, Computer Crimes, Investigation, Computer Security, IT Security, Technology,

INTRODUCCIÓN

A medida que se tiene acceso a los datos corporativos fuera de las instalaciones y redes tradicionales de las organizaciones, la protección de los datos se ha convertido en una preocupación primordial para contrarrestar los incidentes informáticos debido a que las estrategias tradicionales de seguridad informática ya no son suficientes. La existencia de debilidades y/o vulnerabilidades en todas las organizaciones pueden ser explotadas de forma intencional o de manera no intencionada causando muchas veces daños y pérdidas significativas en la información por lo que se hace necesario la implementación de herramientas para la detección de posibles incidentes de seguridad y hallazgos de patrones anómalos que afectan a las infraestructuras TI.

En esta monografía se ha de tratar la importancia que hay en la utilización de las herramientas tecnológicas de análisis forense digital en las investigaciones de delitos informáticos, mostrando un apoyo relevante a la seguridad informática en las organizaciones públicas y privadas.

También se tendrá en cuenta las etapas o pasos para la ejecución de las investigaciones a las tecnologías de la información, éstas siendo componentes fundamentales en las operaciones o actividades de las compañías en la actualidad.

Considerando además la parte legal con respecto a la seguridad y a los colaboradores internos de las áreas en general que respalden y contribuyan con las investigaciones que puedan realizarse en los casos que se presenten violaciones a los dispositivos y equipos con conexiones directas e indirectas dentro y fuera en las instalaciones de las empresas.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La seguridad de la información se ha convertido en un tema de importancia tanto para las personas como para las empresas, ya que interactúan en todo tipo de ámbitos como lo social, comercial, financiera, política, etc.
Anteriormente cualquier información se encontraba plasmada sobre papel, es decir, documentos que contenían un sin número de actividades registradas de gran valor personal o corporativo; a pesar de encontrarse archivados en gavetas bien custodiados bajo llave, contaban con un riesgo que para algunos era muy alto y para otros no lo suficiente como para ser expuestos por terceros a la luz pública.
Con el paso del tiempo la situación cambió, con el incremento de la población aumentaron las necesidades de las personas, permitiendo el nacimiento y expansión de muchas empresas que enfrentarían los retos y desafíos posteriores, por lo tanto, se verían obligados a utilizar mejores herramientas como lo son las computadoras y maquinarías modernas más especializadas.

Debido a la expansión de las computadoras para el uso profesional y personal[1], crecimiento de la informática, omnipresencia y uso de las redes[2] de comunicaciones y el aumento de sistematización de la gestión de los procesos en las empresas en Colombia a partir del año 1980[3] hasta el día de hoy, las organizaciones colombianas no han estado exentas de incidentes de seguridad sino que, además tendrían que resistir otros factores como la supervivencia en el mercado nacional e internacional, mantenerse a la vanguardia, superar obstáculos como la competencia desleal y la felonía de los empleados, siendo este último un aspecto que provocaría incertidumbre a las empresas por el temor a que sus “secretos” sean revelados, es decir, la participación directa e indirecta de estos agentes conocedores de la información divulguen las estrategias, técnicas, fórmulas y demás intimidades de las empresas; pero no solo se debe tener en cuenta al personal interno sino también a los externos aún más si poseen altos conocimientos en el manejo de las tecnologías de la información.

“Es prácticamente imposible para una organización no estar sistematizada y por ende dejar de preocuparse por la seguridad de sus activos de información, los cuales se ven enfrentados a unas amenazas latentes generadas principalmente por la interconexión de su red interna con redes externas gracias al enlace

[1] KENT Karen, et al. SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 2006. [En línea]. Disponible en : https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875
[2] Ibíd., p.17.
[3] Publicaciones SEMANA S.A. Marzo 3 de 1957. La máquina que cambió al país. 2022. [En línea]. Disponible en : https://www.semana.com/especiales/articulo/marzo-1957-brla-maquina-cambio-pais/65917-3/

proporcionado por el proveedor que le da salida a internet (ARNEDO BLANCO, 2014) **.** He aquí uno de los principales indicios que suscitan la incertidumbre en la seguridad informática, situación aprovechada por los delincuentes cibernéticos para obtener la información deseada, en muchas ocasiones sin ser detectados violan los sistemas, dañándolos con algún virus causando detrimento organizacional puesto que lo robado suele ser analizado y aprovechado por la competencia.

1.2 FORMULACIÓN DEL PROBLEMA

A causa de la necesidad de las organizaciones de resolver efectivamente las investigaciones ante incidentes de seguridad y cómo actuar ante los ataques cibernéticos para evitar pérdidas económicas surge la necesidad de responder el siguiente interrogante: ¿Cómo las Herramientas de Análisis Forense Digital pueden contribuir al aseguramiento de las infraestructuras TI en relación con la identificación de incidentes, búsqueda y recopilación de evidencias?

2 JUSTIFICACIÓN

En el siguiente trabajo se ha de resaltar la importancia que tiene la utilización de herramientas de análisis forense digital como mecanismos de identificación de incidentes, búsqueda y recopilación de evidencias que ayudan a las organizaciones a las investigaciones de delitos informáticos e instrumentos de aseguramiento de las infraestructuras TI para implementar barreras de acceso a la información a personal externo y criminales cibernéticos, quienes al utilizar sus capacidades y habilidades sistémicas al manipular códigos y equipos a su voluntad para extraer, dañar y atentar contra la privacidad de la información en los diferentes dispositivos de almacenamiento de datos informáticos de los que disponen las organizaciones cuando estas no han ejecutado acciones necesarias de seguridad a tiempo.

Desde la aceleración del número de personas que trabajan desde casa que acceden los recursos de la organización desde cualquier dispositivo y en cualquier lugar, la colaboración digital y la seguridad empresarial ha cambiado. Las organizaciones han tenido que adaptarse a esta nueva realidad para no afectar la productividad, extendiendo el perímetro de seguridad no solo a la red local sino también a las aplicaciones utilizadas para el trabajo crítico del negocio alojadas fuera de la red corporativa, a los dispositivos de la red corporativa que trabajan en la ubicación física de los teletrabajadores y a los dispositivos personales de los teletrabajadores que acceden a los recursos del negocio, de esta manera con el propósito de proteger los activos .

A través de las herramientas de análisis forense digital se logra realizar investigaciones con profundidad, en la mayoría de los casos detectando la ubicación del cibercriminal, porque en la actualidad para toda persona u organización es recomendable estar alerta a cualquier movimiento o señal sospechosa relacionada a la información, en especial si se encuentra almacenada en algún dispositivo tecnológico siendo la actividad más común en esta época.

Este escrito se elabora para crear conciencia y persistencia en la seguridad informática que deben establecer la comunidad en general y en especial las empresas, quienes en algún momento pueden padecer del robo de información a través de equipos tecnológicos y puedan verse afectados drásticamente. Toda compañía debe contar con personal capacitado en sistemas, facultados para prevenir, analizar, controlar situaciones de riesgo cibernéticos, contando además con los programas necesarios al momento de realizar investigaciones por delitos informáticos.

Los daños y pérdidas económicas a la sociedad por la vulneración de la seguridad, delitos informáticos, terrorismo informático y otras ciberamenazas ha generado la necesidad a los gobiernos de crear y actualizar la legislación en

temas de seguridad de la información y ciberseguridad para los ciudadanos y las organizaciones.
En la región de América Latina y el Caribe, el avance normativo en la penalización del uso de las TIC y la creación de grupos especializados para la lucha contra los delitos informáticos tales como departamentos o secciones dedicados a delitos informáticos en entidades policiales, los equipos de respuesta ante emergencias informáticas CERT/CSIRT ha proporcionado una visión global de la ciberseguridad y aspectos importantes que facilitan la labor del analista forense informático en las investigaciones para la recolección de información, evidencia, identificación de activos, anomalías, técnicas de ataques, tipos de incidentes y tácticas empleadas por los delincuentes informáticos.

En Colombia existen leyes o normativas que prohíben la delincuencia informática y protegen la seguridad de la información estableciendo como delitos acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño Informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, circunstancias de agravación punitiva, hurto por medios informáticos y semejantes, transferencia no consentida de activos[4]. Todos estos atentados afectan la estabilidad organizacional.

La efectividad en las investigaciones realizadas por los analistas forenses de la informática depende principalmente de una serie de técnicas, procesos y conocimientos de aplicabilidad que permiten encontrar la causa del problema y sus atacantes; es por eso, que las compañías evitan las denuncias públicas sobre el quebrantamiento de su seguridad informática para no fomentar la desconfianza de los clientes y/o usuarios.

Por consiguiente, vale la pena destacar la importancia e implementación de estas herramientas de seguridad como soluciones para el rendimiento de la infraestructura de seguridad organizacional, disminución de costos ante incidentes de seguridad por toma de acciones necesarias en seguridad y fortalecimiento en las investigaciones de delitos informáticos para que no se presente impunidad desde ámbito legal.

[4]COLOMBIA. CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273. (5,enero,2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”. [En línea]. En: Diario Oficial. Enero, 2009. Nro.47.223. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Categorizar ocho herramientas de Análisis Forense Digital como mecanismo de identificación de incidentes.

3.2 OBJETIVOS ESPECÍFICOS

- Definir el Estado del arte de los delitos informáticos en la infraestructura TI y el papel de la informática forense como mecanismo de prevención y defensa.

- Establecer las fases de Análisis Forense Digital manejadas en las investigaciones de delitos informáticos en infraestructuras TI en Colombia.

- Identificar ocho tipos de herramientas de software teniendo en cuenta su función, características y finalidad dentro del análisis forense para tratar los incidentes de seguridad y/o delitos informáticos en las organizaciones.

- Realizar una prueba de concepto a las ocho herramientas de software forense consultadas para la elaboración de documento tipo manual.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Informática Forense. Ante la presencia de un incidente informático, la informática forense tiene como propósito explicar la forma cómo sucedió el incidente, recolectar información y elementos responsables del incidente. Para realizar el trabajo de análisis forense digital, los investigadores forenses informáticos deberán contar con conocimientos y habilidades necesarios para cada una de las fases de los análisis forenses en diversas fuentes de datos. Asimismo, los analistas forenses deben disponer de medios, herramientas de software y hardware y la de definición de los procedimientos, metodologías, mejores prácticas para la recolección de evidencias digitales.

Los autores Brian Carrier y Eugene Spafford define la informática forense como el proceso que utiliza la ciencia y la tecnología con el propósito de desarrollar y probar hipótesis que permitan responder preguntas sobre lo ocurrido en un incidente de seguridad o delito informático a través de la evidencia digital[5]. Asimismo, la Guía para la Integración de técnicas forenses en la respuesta a incidentes NIST SP 800-86 considera apropiada la definición del análisis forense digital como la aplicación de la ciencia a la identificación, recolección examen y análisis de datos mientras se preservan la integridad de la información que requiere mantener una estricta cadena de custodia de los datos[6]. De la misma manera, la Organización Internacional de Policía Criminal INTERPOL reconoce que el análisis forense digital es fundamental para las investigaciones de incidentes, ataques y delitos informáticos en las organizaciones de los países que implementan esta disciplina, ya que el análisis forense digital se encarga de la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados en medios electrónicos[7], que debe cumplir unas fases dentro del proceso de investigación, utilizar directrices técnicas, métodos, técnicas avanzadas forenses y herramientas especializadas para garantizar la integridad de los datos en la recolección de pruebas electrónicas o evidencia digital que apoyen las conclusiones de la investigación realizada siendo estas admisibles ante un tribunal.

Con el aumento del almacenamiento, uso y transferencia de la información digital y la variedad de las fuentes de datos de las que puede disponer las organizaciones, se hace necesario establecer y fortalecer la capacidad de realizar

---

[5] CARRIER B, SPAFFORD E. An Event-Based Digital Forensic Investigation Framework. 2004. [En línea]. Disponible en: https://digital-evidence.org/papers/dfrws_event.pdf

[6] KENT, K. Op. cit, p. 17.

[7] INTERPOL. Análisis Forense Digital. s.f. [En línea]. Disponible en: https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

análisis forense digital dentro de las organizaciones[8], de tal forma que los profesionales relacionados con la seguridad TI en las organizaciones puedan encontrar y utilizar herramientas y técnicas del análisis forense digital para satisfacer necesidades técnicas específicas[9] y cumplir propósitos como la detección de brechas de seguridad, servir de respuesta a incidentes de seguridad informática, reconstrucción de incidentes, investigación de delitos cibernéticos, recuperación de daños en los sistemas de información y redes, investigación de violaciones a políticas internas, solución y esclarecimiento de problemas operativos en los sistemas informáticos.

Muchas de las investigaciones de incidentes de seguridad y delitos informáticos son realizadas en las organizaciones cuando se sospecha que el empleado ha realizado acciones no autorizadas en los sistemas informáticos. La autora Ester Chicano Tejada señala en su obra llamada Gestión de incidentes de seguridad informática que el análisis forense informático es una parte fundamental dentro del procedimiento de gestión de incidentes de seguridad[10] porque tiene como finalidad averiguar cómo, quién y qué daños ha causado cualquier tipo de intrusión o ataque[11]. Para garantizar que las investigaciones de delitos e incidentes informáticos se realicen adecuadamente se deben emplear una variedad de equipos y herramientas forenses especializadas en la recopilación y tratamiento de evidencia digital[12] , de esta manera, se espera proteger la evidencia digital, disminuir la pérdida de información y minimizar los errores en la recolección de evidencias.

Para ayudar a mejorar las actividades de la seguridad informática en las infraestructuras críticas de las empresas tales como las de tecnología de la Información (TI), implica que las organizaciones comprendan la probabilidad de ocurrencia de un evento o incidente y los posibles impactos resultantes[13] y se reconozca que la aplicación de las buenas prácticas en el análisis forense digital e implementar técnicas, procedimientos y herramientas de software y hardware forenses válidas son apropiadas para resolver los incidentes de la seguridad informática dentro de la organización.

---

[8] KENT, K. Op. cit, p. 22.

[9] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST. Computer Forensic Tools & Techniques Catalog. 2022. [En línea]. Disponible en: https://toolcatalog.nist.gov/

[10] CHICANO TEJADA, Esther. Gestión de incidentes de seguridad informática (MF0488_3). Antequera, Málaga. IC Editorial. 2015. 270 p. Disponible en : https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44101?page=276. ISBN: 978-84-16207-15-2

[11] Ibíd., p.23

[12] UYANA Mónica, Escobar Milton. Propuesta de Diseño de un Área Informática Forense para un Equipo de Respuestas ante Incidentes de Seguridad Informáticos (CSIRT). s.f. [En línea]. Disponible en: http://repositorio.espe.edu.ec:8080/bitstream/21000/8123/1/AC-GSR-ESPE-047639.pdf

[13] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST. Framework for Improving Critical Infrastructure Cybersecurity. V1.1. 2018. [En línea]. Disponible en : https://www.nist.gov/system/files/documents/2018/12/10/framework esmellrev_20181102mn_clean.pdf

Las amenazas cibernéticas y las formas de ataques por la explotación de vulnerabilidades a los sistemas informáticos de las organizaciones en tiempo de la pandemia mundial de la covid-19 afectó considerablemente a sectores como el financiero, manufactura, energía, atención médica, fabricación de insumos y farmacéuticos[14] de todas las regiones del mundo. Debido a esto, las estrategias de seguridad han tenido que cambiar para proteger la información, detectar y tratar las vulnerabilidades que coloquen en riesgo a los sistemas de información organizacionales para mitigar los impactos y afectaciones a nivel empresarial.

4.1.2 Guías y mejores prácticas del Análisis Forense Digital. En cuanto a las recomendaciones, guías y mejores prácticas relacionados con el análisis forense digital se encuentran:

NIST SP 800-86[15]: Guía para la integración de técnicas forenses en la respuesta a incidentes (2006). Esta guía tiene como propósito presentar el análisis forense desde una perspectiva de TI[16]. Describe los procesos para realizar actividades forenses efectivas a sistemas informáticos y redes, informa sobre las tecnologías y forma de uso para actividades de respuesta de incidente.

NIST SP 800-44 versión 2[17]: Directrices sobre la protección de servidores web públicos (2007). Describe las prácticas para la elección de plataformas y software del servidor web, instalación configuración y mantenimiento de servidores web públicos seguros. Configuraciones de parches y actualizaciones, pruebas de seguridad entre otros.

RFC 3227 Guidelines for Evidence Collection and Archiving[18]: Directrices para la recolección de evidencias y su almacenamiento. Sirve como estándar para la recolección de información en los incidentes de seguridad debido a que la guía RFC 3227 incluye los principios a seguir durante la recopilación y archivos de pruebas, las consideraciones de factores como la volatilidad de la evidencia, privacidad de la información recopilada, aspectos legales de la evidencia, transparencia en el proceso de recolección de la evidencia y métodos utilizados, aspectos que se ha de tener cuenta al realizar documentación en el procedimiento de almacenamiento que permita garantizar la cadena de custodia

[14]PORTAFOLIO. Se duplicaron los ciberataques en 2020. 2021. [En línea]. [Fecha de consulta: marzo, 2022]. Disponible en: https://www.portafolio.co/economia/se-duplicaron-los-ciberataques-en-2020-549548

[15] NIST. SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.2006. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-86/final

[16] Ibíd., p.24.

[17] NIST. SP 800-44 versión 2, Guideline on Securing Public Web Servers. 2007. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en : https://csrc.nist.gov/publications/detail/sp/800-44/version-2/final

[18] BREZINKI, D. y KILLALEA T. Guideline for Evidence Collection and Archiving. RFC3227. 2002. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en: https://www.ietf.org/rfc/rfc3227.txt

de la evidencia y herramientas necesarias para llevar a cabo la recolección de evidencias.

ENFSI-BPM-FIT-01 Best Practice Manual for the Forensic Examination of Digital Technology[19] (2015): El manual de las mejores prácticas para el examen Forense de la tecnología digital tiene como objetivo definir las mejores prácticas europeas en el campo de la informática forense, destaca la importancia de la utilización de una metodología coherente para el análisis forense de equipos informáticos y teléfonos. Este documento incluye la recomendación formal al grupo de trabajo de informática forense para solo considerar la validación de procesos más que las herramientas de validación.

Good Practice Guide for Computer- Based Electronic Evidence ACPO 2012[20]: Guía para las buenas prácticas de manipulación adecuada de medios digitales[21] que puede ser aplicada a todo tipo de fuentes de datos informáticos y dispositivos móviles. Desarrollo por la Asociación de Comisarios de Policía del Reino Unido.

4.1.3 Modelos de procesos para la investigación forense digital. Diversos autores han desarrollado y propuesto a través de los años, diferentes modelos de procesos y Frameworks para realizar investigaciones forenses digitales con el propósito de formalizar los procedimientos forenses informáticos y análisis de evidencias digitales. A continuación, se mencionan algunos modelos de procesos para realizar el análisis forense digital son: NIJ del instituto nacional de justica de Estados Unidos (2001), el modelo DFRWS (2001), Modelo Gunsh, Carr y Reith (2002), el modelo Casey (2004), el modelo Cohen (2009), el modelo SRDIFM (2011) para describir el tratamiento de la evidencia digital.

En el año 2001, el Departamento de Justicia de los Estados Unidos publicó la propuesta de un modelo de proceso de análisis forense en la escena del delito. Esta guía es utilizada por entidades judiciales para la protección y reconocimiento de las evidencias digitales[22]. Este modelo de procesos se basa en cuatro fases:

- Recolección.
- Examinación.

[19]EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTE. Best Practice Manual for the Forensic Examination of Digital Technology. ENFSI-BPM-FIT-01. 2015. [En línea]. [Fecha de Consulta: marzo 2022] Disponible en : https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

[20] ACPO. Good Practice Guide for Computer-based Electronic Evidence. Official release version 4.0. [En línea]. Disponible en: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf

[21]LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. Paracuellos de Jarama, Madrid, RA-MA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=246

[22] SHIRVASTA Gulshan; SHARMA Kavita y DWIVEDI Akansha. Forensic Computing Models: Techical Overview. 2012. [En línea]. Disponible en: https://www.researchgate.net/publication/242524844_FORENSIC_COMPUTING_MODELS_TECHNICAL_OVERVIEW

- Análisis.
- Reporte.

El modelo DFRWS fue desarrollado durante el primer Digital Forensic Research Workshop (Taller de Investigación Forense Digital[23]) por G. Palmer en el año 2001 quien propuso un nuevo modelo de investigación forense digital que definió las clases de acción en la investigación digital. Este modelo incluye las fases[24] de:

- Identificación.
- Preservación.
- Colección.
- Examen.
- Análisis.
- Presentación.
- Decisión.

El modelo de proceso Forense Digital Abstracto (ADFM) por sus siglas en ingles de Abstract Digital Forensic Model, fue presentado en el año 2002 por los autores Gregg Gunsh, Mark Reith y Clint Carr como una propuesta mejorada del modelo DFRWS[25], agregando 3 etapas más al modelo proceso existente: preparación, estrategia de enfoque y devolución de Evidencia. Este modelo se fundamenta en nueves fases:

- Identificación.
- Preparación.
- Estrategia de enfoque.
- Preservación.
- Colección.
- Examen.
- Análisis.
- Presentación.
- Devolución de evidencia.

El modelo Casey es un modelo para el procesamiento y examen de la evidencia digital que puede aplicarse con éxito a sistemas informáticos autónomos y a entornos de Red[26], este modelo establece cuatro pasos:

---

[23] LAZARO DOMINGUEZ, Op. cit, p. 25

[24]LOPEZ JAVIER et al. Securing Information and Communications Systems: Principies, Technologies and Applications. 2008. [En línea]. ISBN 9781596932289. Disponible en: https://search-ebscohostcom.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=284257&lang=es&site=eds-live&scope=site.

[25]Ibíd., p. 26.

[26] LOPEZ JAVIER, Op cit, p. 26

- Reconocimiento.
- Preservación, colección y documentación.
- Clasificación, comparación e individualización.
- Reconstrucción.

El modelo cohen (2009) fue propuesto por Fred Cohen para describir las fases a seguir en el proceso de tratamiento para la evidencia digital en un contexto legal[27]. El modelo sistémico de investigación forense digital SRDIFM 2011 (System Digital Forensic Investigation) contiene once fases : Preparación, Aseguramiento de la escena, examen y reconocimiento, documentación de la escena, blindaje y recopilación de pruebas volátiles y no volátiles, preservación, examen, análisis, presentación, resultado y revisión[28].

Aunque no exista un modelo único para realizar una investigación forense digital, cada modelo forense ofrece sus ventajas para garantizar un procedimiento de análisis forense digital adecuado y sus limitaciones durante la investigación. Algunos modelos de procesos forenses están diseñados con más números de fases que otros por lo que el investigador debe de asegurarse que la metodología seleccionada cubra todas las condiciones de la investigación, el uso de herramientas de informática forense garantice la autenticidad de los datos que se obtienen y el tratamiento de evidencia digital hasta la disposición final con validez legal.

4.2 MARCO CONCEPTUAL

ANÁLISIS FORENSE DIGITAL: Disciplina que permite la detección de patrones anómalos y el rastreo de acciones ilícitas cometidos en sistemas digitales, dispositivos electrónicos y equipos de cómputo a través del uso de técnicas científicas, herramientas especializadas de software y hardware, conocimientos avanzados en informática, tecnologías de información y las comunicaciones, ataques e implicaciones y el empleo de una metodología estructurada para desarrollar el proceso de la identificación, adquisición, conservación, análisis y presentación de evidencias válidas, pertinentes e integras en las investigaciones informáticas.

[27] COHEN Fred. Digital Forensic Evidence Examination. Fifth Edition. 2009. [En línea].Disponible en: http://all.net/books/2013-DFE-Examination.pdf

[28] TAHIRI Soufiane. Mastering Mobile Forensics. [En línea]. 2016. Disponible en: https://www.packtpub.com/product/mastering-mobile-forensics/9781785287817

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Suceso o eventos no autorizados en sistemas, servicios o en una red que indica una situación de violación a las políticas, controles y seguridad de la información que compromete las operaciones de los recursos informáticos.

DELITOS INFORMÁTICOS: Carlos Sarzana, tratadista penal italiano menciona que los delitos informáticos son "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo"[29] .
Nidia Callegari define el concepto de delitos informáticos como "aquel que se da con la ayuda de la informática o de técnicas anexas"[30]
Romeo Casabona señala que los delitos informáticos corresponden a una multiplicidad de conductas ilícitas y no a una sola de carácter general[31]. De forma general, el término de delitos informáticos abarca a la gran diversidad de delitos que se cometen mediante el uso de nuevas tecnologías.

EVIDENCIA DIGITAL: Parte importante en una investigación forense que debe cumplir el principio de admisibilidad y reconocimiento. Es la Información que se recupera en formato electrónico por la realización de un análisis forense sin alteración de los datos de origen para determinar la relación entre un incidente de seguridad o delito informático y el autor y servir de apoyo probatorio en las investigaciones corporativas, judiciales y de seguridad nacional para sancionar conductas ilícitas informáticas. En las categorías que se dividen la evidencia digital se encuentra: los registros almacenados en un equipo informático, los registros generados por el equipo informático y los registros parciales de generación y almacenamiento en el equipo informático.

FUENTES DE DATOS PARA LA EVIDENCIA DIGITAL: Equipos informáticos que contienen datos o información de origen de un ataque informático o incidente de seguridad a un sistema informático que un analista forense digital utiliza para realizar el análisis, la búsqueda y extracción de la evidencia digital.

HERRAMIENTAS DE SOFTWARE FORENSE: Software de uso específico o conjunto integrado de software que se emplea en la realización de las actividades de análisis forense digital que incluye las categorías de licencias de software de código abierto y comercial.

SOFTWARE FORENSE: Software informático diseñado para garantizar las investigaciones forenses y análisis de delitos informáticos e incidentes de

[29] TREJO Carlos; DOMENECH, Gustavo y ORTIZ Karla. Revista pensamiento penal, La seguridad jurídica frente a los delitos informáticos. 2016. [En línea]. [Fecha de Consulta: septiembre 2021] Disponible en: http://www.pensamientopenal.com.ar/doctrina/44051-seguridad-juridica-frente-delitos-informaticos p.42
[30] ACURIO DEL PINO, Santiago. Delitos informáticos: Generalidades. 2016. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf p.10-14
[31] TREJO Carlos; DOMENECH, Gustavo y ORTIZ Karla. Op. cit, p.26

seguridad que permite la reconstrucción elementos probatorios digitales válidos, descubrimiento de riesgos, análisis de datos, extracción de información y procesamiento de evidencia digital relacionados con los datos que contienen las redes y dispositivos electrónicos.

TRATAMIENTO DE LA EVIDENCIA DIGITAL: Principios, prácticas, procesos y procedimientos que se ejecutan por parte de los investigadores forenses informáticos para el acceso, manejo, recolección y preservación de las evidencias digitales.

GESTIÓN DE INCIDENCIAS DE SEGURIDAD INFORMÁTICA: Proceso de implementación de herramientas y controles pertinentes en la detección, respuesta, reporte y tratamiento de incidentes y vulnerabilidades en las organizaciones.

ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES: Proceso de extracción y análisis de datos, archivos de sistemas y almacenamiento de dispositivos IOS y Android, datos de respaldo, datos WiFi, historial de navegación, emails, datos de GPS, historial de chats, datos eliminados en el dispositivo móvil, contactos, registros de llamadas entre otros, que permite obtener evidencia digital de los dispositivos móviles ante un incidente de seguridad.

VULNERABILIDAD: Parte del software que presenta brechas de seguridad que puede ser aprovechada por un atacante para crear una condición no deseada y causar problemas.

CADENA DE CUSTODIA : Conjunto de procedimientos que garantizan la autenticidad e integridad de las evidencias digitales encontradas[32] ante las autoridades competentes para probar el delito, grado de culpabilidad, la imputación o reparación de la víctima[33].

PRESERVACIÓN DIGITAL: Aplicación de técnicas activas de conservación informática[34] a documentos digitales de creación presentes o en el pasado para asegurar el mantenimiento y el uso a largo plazo.

PRUEBA DE CONCEPTO (PoC): Consideraciones y validaciones que se realiza a herramientas de software forense seleccionadas para comprobar la funcionalidad,

---

[32] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Evidencia Digital, Guía 13. 2016. [En línea]. [Fecha de Consulta: octubre 2021]. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

[33] FISCALÍA GENERAL DE LA NACIÓN. Manual del sistema de Cadena de Custodia. 2018. [En línea]. [Fecha de Consulta: octubre 2021]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

[34] TÉRMENS, Miquel. Preservación digital. 2014. Editorial UOC. [En línea]. [Fecha de Consulta: octubre 2021].Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/57604?page=20

el potencial, la viabilidad técnica, describir los beneficios de la implementación, las características y capacidades del software teniendo en cuenta factores como la usabilidad, efectividad, rendimiento, manejo en la integridad de los datos y aplicabilidad en procesos de análisis, diagnósticos, respuestas e investigación de incidentes de seguridad y mejoras en la seguridad de la información para las organizaciones.

4.3 MARCO HISTÓRICO

En la década de 1980 a medida que los computadores se volvieron de fácil uso, se conectaron a redes locales y área más amplias, junto con las maravillas del ciberespacio también aparecieron los delitos informáticos y la leyes y estándares legales quedaron obsoletas para abarcar estos nuevos delitos. En esta década, surgió la disciplina del análisis forense digital[35] como respuesta al incremento de delitos cometidos por el uso de sistemas informáticos como objeto de delito, instrumento para cometer el delito o utilizado para el almacenamiento de pruebas de un delito. Los investigadores pioneros en esta disciplina que en su mayoría hacia parte de la policía y de agencias federales se dieron cuenta que la evidencia no se encontraba en papel y nuevas fuentes de evidencia eran necesarias.

El desarrollo de programas y herramientas de informáticas forense a principios de los años 80 como ocurrió con Copy II PC en el año 1981 para realizar copias exactas de disquetes protegidas ante copias ilegales y la utilidad UnErase versión 1.0 para la recuperación de archivos, representó avances para el análisis forense digital. Solo hasta 1984 aparecieron las primeras herramientas forenses digitales, como Desktop Mountie diseñada por Andrew Rosen para la policía canadiense y el programa “Magnetic Media Program” lanzado por el FBI como herramienta oficial de análisis forense digital. Sin embargo, en esta época no existían suficientes herramientas forenses específicas para desempeñar el análisis forense digital lo que llevó a los desarrolladores a diseñar suites propias de utilidades forenses basadas en MS-DOS y a finales de los años ochenta se establecieron algunos procesos forenses.

En 1987 aparece la empresa Access Data con productos de software para la recuperación de contraseñas y análisis forense llamada Forensic Toolkit(FTK).

En 1995 se estableció la Organización Internacional de Pruebas informáticas (IOCE) para el intercambio de información sobre la investigación de delitos

[35] BODDINGTON, Richard. Practical Digital Forensics. Packt Publishing. 2016. [En línea]. [Fecha de consulta: octubre de 2021]. ISBN. 978-1-78588-710-9

informáticos, cuestiones forenses que se relacione con la informática[36], desarrollar recomendaciones y formular estándares de pruebas electrónicas.

En 1998 se estableció el grupo de trabajo sobre la evidencia digital(SWGDE) que se encargó del desarrollo de pautas y estándares. En este mismo año, se realiza el primer simposio de la INTERPOL sobre las ciencias forenses.

En octubre de 1999 fueron aprobados los principios internacionales para la recuperación estandarizada de la evidencia propuestos por la SWGDE.

En el año 2000, el FBI estableció el primer RCFL Laboratorio regional forense informático en San Diego California.

En el año 2001 se organizó el primer taller abierto dedicado a la ciencia forense digital, Digital Forensic Research Work (DFRWS) que dio la primera definición formal del análisis forense digital.

En el año 2001, se firmó el Convenio de Budapest como el primer tratado internacional para combatir Crímenes informáticos.[37]

En el año 2002 los investigadores Gunsch, Reith y Carr propusieron un modelo de análisis forense siguiendo los pasos de identificación, preparación, enfoque, preservación, recolección, examinación, análisis, presentación y devolución de pruebas.

En 2005 el análisis digital forense carecía aun de proceso de estandarización y se orientaba a Windows y en menor proporción a sistemas Linux.

En el año 2008 el comité técnico conjunto JTC de la organización internacional de normalización (ISO/IEC JTC 1)[38] exploró la viabilidad de normas para la gobernanza forense digital, pero hasta la fecha no existen estándares JTC1 que lo aborden de forma específica.

En el 2009 Sudresan Perumal presentó un modelo de investigación forense digital basado en la ley cibernética de Malasia. Este modelo se centra en el proceso de la adquisición de datos que incluye la adquisición de datos en vivo y datos estáticos en la investigación forense digital.

---

[36]FBI. Forensic Science Communications. 2000. [En línea]. [Fecha de consulta: 28 de septiembre 2021] Disponible en: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

[37] CANO MARTÍNEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Bogotá, Colombia: Universidad de los Andes. 2012. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/69374?page=281

[38] Ibíd., p.30.

En el año 2011 Ankit Agarwal et al. Propone un modelo sistemático de procedimiento forense digital (SRDFIM), ofreciendo un marco estandarizado y sistemático de 11 fases de acuerdo con la evidencia capturada en el equipo. El principal interés de este modelo es limitar los delitos cibernéticos y el fraude informático.

4.4 MARCO LEGAL

Un profesional que se dedique a la investigación forense digital debe conocer y entender todo aquello relacionado a la legislación vigente que regula todas las actividades y actuaciones durante el proceso de investigación del hecho delictivo asignado, las repercusiones legales, establecer evidencias pertinentes si la investigación corresponde a un delito penal, una falta administrativa o delito informático.

Convenio Sobre la Ciberdelincuencia Budapest 2001.

Firmado el 23 de noviembre de 2001 en Budapest, el Convenio sobre Ciberdelincuencia del consejo de Europa[39] se considera como la guía internacional jurídica en la lucha de la ciberdelincuencia, organizado en un preámbulo y cuatro capítulos distribuidos en 48 artículos. Actualmente, el convenio de Budapest tiene adherido a 65 países, que incluye a países de Latinoamérica como Panamá en el año 2014, Chile en el año 2017, Argentina, Costa Rica y Paraguay en el año 2018, Perú en el 2019 y Colombia en el año 2020[40].

El Convenio de Budapest pretende establecer un acuerdo penal común internacional frente a la ciberdelincuencia, estandarizar definiciones de los términos como sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico (Capítulo I, artículo 1), abordar medidas que deberán adoptarse a nivel nacional(Capitulo II, artículos 2 a 22) relacionado a la clasificación de delitos informáticos propuesta, las infracciones de derecho de autor, el fraude informático, la violación de seguridad, la pornografía infantil entre otros, establecer principios que permita la cooperación internacional contra el cibercrimen (Capítulo III, artículos 23 a 35) y finalmente las disposiciones finales del convenio (Capítulo IV, artículos 36 a 48).

[39] CONSEJO DE EUROPA. Convenio Sobre la Ciberdelincuencia Budapest, 23.XI.2001. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

[40] COLOMBIA. MINISTERIO DE RELACIONES EXTERIORES DE COLOMBIA. 2020. Colombia se adhiere al Convenio de Budapest contra ciberdelincuencia. [En línea]. Disponible en: https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Los delitos contemplados en el ámbito del cibercrimen se encuentran clasificados por el Convenio de Budapest en 4 grandes categorías así:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos: incluye los delitos que vulneran las propiedades de la seguridad de la información (confidencialidad, integridad y disponibilidad) tales como el acceso ilícito, la interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema y abuso de los dispositivos

- Delitos informáticos: abarca la falsificación informática y el fraude informático.

- Delitos relacionados con el contenido: incluye los delitos que se relacionan con la pornografía infantil en aspectos como la producción, oferta, difusión, adquisición y posesión de material pornográfico infantil en un sistema informático para la difusión.

- Delitos relacionados con infracciones de la propiedad intelectual y de derechos afines.

Adicionalmente, el Convenio sobre Ciberdelincuencia del consejo de Europa expone la necesidad de adoptar medidas legislativas para sancionar la tentativa y la complicidad en delitos tipificados en los artículos 2 a 10 y la responsabilidad jurídica con sanciones que sean efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad[41]

En el año 2003 se estableció el "Protocolo adicional al Convenio sobre ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos" con el propósito de ampliar la categoría de los delitos de contenido que se comenten mediante sistemas informáticos y mejorar los mecanismos de cooperación internacional establecidos en el Convenio de Budapest sobre la ciberdelincuencia.

Ley 527 de 1999

Reglamentó y definió el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones[42]. La ley 527 de 1999 establece el mismo valor

[41] CONSEJO DE EUROPA. Convenio Sobre la Ciberdelincuencia del Consejo de Europa. Artículo 13. [En línea]. [Fecha de consulta: octubre 2021] Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

[42] COLOMBIA. CONGRESO DE COLOMBIA. Ley 527 de 1999 (21,agosto,1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales. 2021. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

probatorio a las operaciones realizadas en medios digitales que en los medios físicos[43] reconociendo la importancia de la evidencia digital.

Respecto al Análisis Forense Digital en Colombia esta ley expone algunos criterios relacionados como por ejemplo en el Capítulo II: Aplicación de los requisitos jurídicos de los mensajes de datos específicamente en el artículo diez (10) ya que se refiere a la admisibilidad y fuerza probatoria de los mensajes de datos resaltando que " los mensajes de datos tienen total validez probatoria" otorgada en la disposiciones del Capítulo VIII del título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil[44].

De forma similar, en el artículo once (11) señala que en la apreciación de las pruebas se tendrá en cuenta la confiabilidad en la generación, archivo o comunicado del mensaje, la conservación de la integridad de la información, la forma en la que se identifique a su iniciador[45] y factores pertinentes.

Ley 1273 de 2009

Es la normatividad que se utiliza para penalizar los delitos cibernéticos en Colombia, se caracteriza por representar grandes avances en la regulación del Derecho informático. Con la ley 1273 se creó un nuevo bien jurídico tutelado llamado " De la protección de la información y de los datos" que pretende la preservación de la confidencialidad, integridad, seguridad y disponibilidad de los datos y los sistemas informáticos, incluyendo además los datos personales.

La ley 1273 de 2009 establece dos capítulos dedicados a las disposiciones relacionada a las sanciones por los actos de:

"Atentados contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos"[46] en la que tipifica los delitos de:

- Acceso abusivo a un sistema informático.
- Obstaculación ilegítima de un sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.

[43] BECERRA, Jairo, et al. El derecho y las tecnologías de la información y la comunicación TIC. [En línea]. [Fecha de consulta: octubre de 2021]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/16511/1/El-derecho-y-las-tecnolog%c3%adas-de-la-informaci%c3%b3n-y-la-comunicaci%c3%b3n-TIC.pdf

[44] COLOMBIA. Op. cit, p.33.

[45] COLOMBIA, Op. cit, p.33.

[46] COLOMBIA, Op. cit, p.20.

- Daño informático.
- Uso de software malicioso.
- Violación de datos personales suplantación de sitios web para capturar datos personales.

Y "atentados informáticos y otras infracciones"[47], que tipifica los delitos de:

- Hurto por medio informáticos y semejantes.
- Transferencia no consentida de activos.

De igual forma, la ley 1273 de 2009 indica los castigos de acuerdo con el delito con penas de prisión de duración entre cuarenta y ocho (48) meses hasta ciento veinte (120) meses, sanciones económicas de 100 a 1500 salarios mínimos legal vigente e incluye ocho (8) circunstancias de agravación punitiva[48] para las conductas descritas en el artículo 269H. Con esta ley también se logra judicializar a los individuos dedicados a las actividades de hackers, estafadores y saboteadores.

Ley 1453 de 2011

El artículo 53 de esta ley[49] aborda la disposición para la recuperación de producto de la transmisión de datos a través de las redes de las comunicaciones que modifica el artículo 236 de la ley 906 así:

Artículo 236: Recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones.

"Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado"[50]

[47] Ibíd., p.20.

[48] COLOMBIA, Op. cit, p.20.

[49]COLOMBIA. CONGRESO DE COLOMBIA. Ley 1453 (24,junio,2011). Por medio de la cual se reforma el Código de Procedimiento Penal, el código de Infancia y Adolescencia. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43202

[50] Ibíd., p.35.

De forma similar, por el artículo 14 de la ley 1908 de 2018 en el artículo 236 se adicionó el parágrafo:

"Cuando se trate de investigaciones contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados, la Policía Judicial dispondrá de un término de seis (6) meses en etapa de indagación y tres (3) meses en etapa de investigación, para que expertos en informática forense identifiquen, sustraigan, recojan, analicen y custodien la información que recuperen".

Resolución Reglamentaria 202 de 2012

Establece la creación del Grupo de Laboratorio de Informática Forense (LIF) para la Contraloría General de la república de Colombia, define como objetivo del grupo LIF servir de apoyo a los procesos de indagación preliminar, responsabilidad fiscal, procesos disciplinarios y control interno a través de la identificación, preservación, análisis y presentación de la evidencia digital[51] para que el elemento probatorio sea aceptado legalmente en los procesos mencionados y permitan el logro de resultados esperados por la Contraloría en el ejercicio de control fiscal y vigilancia.

Ley 1564 de 2012

Esta ley concierne al Código General del Proceso y otras disposiciones en Colombia. Se destacan tres artículos que se relacionan con proceso del análisis forense digital: el primero es el artículo 165 que define los medios de pruebas para el convencimiento del juez donde se incluye el dictamen pericial, la inspección judicial, documentos, indicios, informes y otros medios útiles[52], el segundo artículo es el 226 que menciona todo lo relacionado a la procedencia de la prueba pericial, quien hace el dictamen pericial, las competencias del perito para realizar un dictamen, presentación del dictamen entre otros. Y finalmente el articulo 243 expone las distintas clases de documentos como los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas etiquetas, sellos y todo objeto mueble que tenga características representativas o declaratorias.

[51] COLOMBIA. CONTRALORÍA GENERAL DE COLOMBIA. Resolución Reglamentaria 202 (7,diciembre,2012). Por la cual se deroga la Resolución Reglamentaria 126 de 2011 y se crea el grupo de Laboratorio de Informática Forense (LIF). 2012. [En línea]. Disponible en: https://normativa.colpensiones.gov.co/colpens/docs/resolucion_contraloria_0202_2012.htm

[52] COLOMBIA. CONGRESO DE COLOMBIA. Ley 1564. (12,julio,2012).Por medio de la cual se expide el Código General del proceso y se dictan otras disposiciones. 2012. [En línea]. En: diario Oficial. Julio,2012. Nro. 48.489. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012_pr004.html

Ley estatutaria 1581 de 2012

Establece las disposiciones generales para el tratamiento y protección de datos personales que se registren en cualquier base de datos en organizaciones de naturaleza pública o privada[53] . Tiene como objeto garantizar el cumplimiento de los artículos 15 y 20 de la constitución política de Colombia relacionados con el derecho a la intimidad, la consulta, actualización y rectificación de datos. Esta ley define en el artículo 4 los principios que se deben aplicar para el tratamiento de datos personales, dando importancia especialmente al principio de confidencialidad en el literal h . Por otra parte, la ley 1581 considera como categorías especiales de datos a los datos sensibles que pueden afectar la intimidad del titular o generar discriminación y el tratamiento de datos personales de niños, niñas y adolescente para asegurar el respeto a sus derechos.

Decreto 1377 de 2013

Creado para reglamentar parcialmente la ley 1581 de 2012, en aspectos relacionados con el tratamiento de datos en el ámbito personal o doméstico, establece las definiciones para los términos de aviso de privacidad, dato público, datos sensibles, proceso de transferencia y transmisión de datos personales. Asimismo, señala las disposiciones para la recolección de datos personales, autorización del tratamiento de los datos personales sensibles, revocatoria de la autorización del titular para el tratamiento de datos, limitaciones al tratamiento de datos de datos personales, parámetros para el tratamiento de datos personales de niños, niños y adolescentes, políticas para el tratamiento de datos personales, derechos de los titulares de la información, reglas para aplicar a la transmisión y transferencias internacionales de datos personales, señala la responsabilidad frente al tratamiento de datos personales, entre otras medidas. (Decreto 1377 de 2012. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Presidencia de la República de Colombia, Junio 27 de 2013)

[53]COLOMBIA. CONGRESO DE COLOMBIA. Ley estatutaria 1581 (18,octubre,2012). Por la cual se dictan disposiciones generales para la protección de datos personales. 2012. [En línea]. En: diario Oficial. Octubre,2012. Nro. 48.587. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

5 RESULTADOS DE LOS OBJETIVOS

5.1 ESTADO DEL ARTE DE LOS DELITOS INFORMÁTICOS EN LA INFRAESTRUCTURA TI

La capacidad de contrarrestar los delitos informáticos por parte de las organizaciones nacionales e internacionales, gobiernos y los usuarios de internet depende de gran medida del nivel de progreso e implementación de factores como normas legales, normas regulatorias, políticas y estrategias de seguridad informática, estándares para las tecnologías, educación y concientización de la existencia de delitos informáticos, habilidades y capacidad de respuesta ante incidentes de informáticos.

El reporte de ciberseguridad 2020 “Ciberseguridad: Riesgos, Avances y el camino a seguir en América Latina y el Caribe”[54] del Observatorio de la ciberseguridad en América Latina y el Caribe del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), menciona que los países de la región de América Latina y el Caribe han registrado avances significativos en temas de sensibilización de ciberseguridad, construcción de políticas, medidas y estrategias de ciberseguridad, implementación de equipos de respuesta CSIRT o CERT para el año 2020, sin embargo, todavía resulta un desafío para la gestión del riesgo cibernético en los sectores públicos y privados y la ciberresiliencia regional y nacional de los países Latinoamericanos y del Caribe.

La aparición de la pandemia mundial de la COVID 19 en el año 2020 llevó a las naciones a una situación de incertidumbre, a los gobiernos a establecer medidas de confinamiento y políticas públicas para manejar la crisis global y a las organizaciones a cambios disruptivos por la aceleración de la transformación digital en las operaciones, procesos y soluciones digitales para cubrir las necesidades de la empresa, permitir la continuidad del negocio, implementar el teletrabajo y resiliencia en los colaboradores; a su vez, esta condición de pandemia hizo visible el aumento de la generación de riesgos informáticos, problemas con la ciberseguridad y el incremento exponencial de los delitos informáticos a las organizaciones gubernamentales y privadas debido al evidente mejoramiento de las técnicas de ataques informáticos de los cibercriminales a nivel global en tiempos de pandemia

En Colombia, el crecimiento de delitos informáticos en el año 2020 se debió al desconocimiento de riesgos digitales, las buenas prácticas para el uso y protección de las tecnologías de información, propagación de publicidad y páginas web maliciosas, estafas en redes sociales, estafas románticas, ofertas laborales

[54] OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE. Reportes finales. 2020. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://observatoriociberseguridad.org/#/final-report

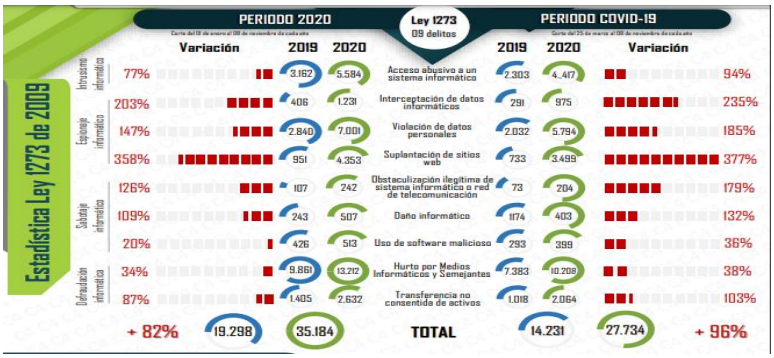
falsas y explotación de vulnerabilidades de seguridad cuando las personas fueron sometidas a medidas de aislamiento obligatorio (ver figura 1).

Figura 1. Comportamiento de los delitos informáticos en Colombia año 2020

Fuente: Asuntos legales. [En línea]. [Fecha de consulta: 27 de septiembre de 2021]. Disponible en : https://www.asuntoslegales.com.co/consumidor/los-delitos cometidos-por-medios-informaticos-crecieron-83-por-cuenta-de-lapandemia-3099 101

El centro cibernético Policial de Colombia identificó como principales modalidades de incidentes informáticos[55] ocurridos en el año 2020 a las estafas de compra y venta de producto, phishing, suplantación de identidad, vishing, malware y, por último, amenazas, injurias y calumnias en redes sociales. (ver figura 2).

Figura 2. Balance Cibercrimen en Colombia 2020



Fuente: Centro cibernético Policía Nacional de Colombia. Balance Cibercrimen 2020 – semana 45. [En línea]. [Fecha de consulta 27 de septiembre 2021]. Disponible en : https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrime n_2020_-_semana_45.pdf

[55] CENTRO CIBERNÉTICO POLICÍA NACIONAL DE COLOMBIA. Balance Cibercrimen 2020 – semana 45. [En línea]. [Fecha de consulta: 27 de septiembre 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_ cibercrimen_2020_-_semana_45.pdf

Algunos ejemplos de ciberataques que marcaron el año 2020 que se registraron por el impacto ocasionado en las operaciones de las organizaciones se encuentran:

- Una mayor actividad de grupos de ransomware como Ryuk, Maze, Egregor, REvil, Netwalker bajo la modalidad de ataques de Ransomware as a Service (RaaS) durante el 2020 en Estados Unidos, Reino Unido Europa y Latinoamérica para realizar ataques dirigidos a entidades gubernamentales y financieras, como por ejemplo, ataques de Maze en mayo del 2020 en Costa Rica y Brazil, el ataque de REvil(Sodinokibi) en julio del 2020 a la empresa Telecom en Argentina, el ataque de ransomware Ryuk a la empresa Finantra en Reino unido y Sopra Steria en Francia

- Ataques DDoS, estafas de Bitcoins, suplantación de sitios web, envío de correos masivos con enlaces maliciosos para difusión de malware.

- Hackeo masivo a sistemas y herramientas internas con ingeniería social utilizando señuelos como el tema del coronavirus, emergencia sanitaria del Covid-19, suplantación de identidad para robo de información confidencial tal como pasó con Twitter en julio del 2020 y el robo de credenciales de cuentas de usuarios de la plataforma Zoom.

- Acceso abusivo y violación de datos a Telegram en agosto del 2020.

- El Ataque a la empresa SolarWinds[56] en diciembre del año 2020 que afecto a millares de redes informáticas del gobierno de los Estados Unidos.

- El ciberataque al Oleoducto Colonial Pipeline con el ransomware DarkSide a los sistemas de la infraestructura energética de Estados Unidos a principios del mes de mayo del año 2021 que ocasionó la suspensión de las actividades en uno de los mayores oleoductos en Estados Unidos.

- El ataque informático a la plataforma digital del Ejercito Nacional de Colombia en mayo del año 2021.

La experta en ciberseguridad Nayia Barmpaliou señala que el resultado de la transición a la “era digital de todo”[57] por la pandemia del Covid-19 se traduce a un aumento extraordinario de ataques cibernéticos a infraestructura crítica, vulnerabilidades amplificadas, mayor probabilidad de ocurrencia de fraudes o

[56] BBC. SolarWinds: 5 ataques informáticos de Rusia que transformaron a la ciberseguridad en Estados Unidos. 2020.[En línea]. [Fecha de consulta: 24 de octubre de 2021]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-55381892

[57] OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, Op. cit, p.38.

robos de datos y la estimación de costos por daños de delitos informáticos para el año 2021 en el mundo alcanzará más $6 billones de dólares por lo que la necesidad de intensificar los esfuerzos por mejorar seguridad informática sobre todo en la región de América latina y el Caribe (ALC) requiere de la cooperación global en temas de ciberseguridad, inversión en la ciberseguridad, tecnologías y procesos digitales en las organizaciones para mantener las ventajas competitivas y mitigar los riesgos forma más efectiva ya que las organizaciones cada vez más acentúa la dependencia a la infraestructura digital.

Con el auge de la modalidad del teletrabajo implementada por las organizaciones ante la situación sanitaria por Covid-19 que aún en el año 2021 se sigue padeciendo, los trabajadores siguen desempeñando las actividades corporativas, reduciendo así los costos de operación a las empresas. Sin embargo, es la puerta de entrada peligrosa a los atacantes informáticos cuando las medidas de seguridad de la información son insuficientes en la conexión a la red corporativa desde la red de Internet del hogar del trabajador, la cual es la misma red donde se encuentra conectado con otros dispositivos inteligentes como Smart TV, computadoras, móviles y Tablet que los cibercriminales han aprovechado para explotar las vulnerabilidades de las tecnologías para realizar ataques a las empresas.

Debido a las condiciones actuales generadas por la pandemia, los entornos del teletrabajo han estado más expuesto a los incidentes de seguridad por lo que llevó a los investigadores informáticos, los procesos y procedimientos de análisis forense digital a la adaptación del teletrabajo forense para la adquisición de evidencias digitales, transferencia de documentación por sistemas telemáticos seguros, considerar tecnologías de accesos, videoconferencias y soluciones ante fallos en la plataforma de comunicación.

5.2 PAPEL DE LA INFORMÁTICA FORENSE COMO MECANISMO DE PREVENCIÓN Y DEFENSA.

Actualmente, muchas organizaciones y personas en general se enfrentan con diferentes clases de delitos informáticos que impiden el buen funcionamiento de sus actividades o de su diario vivir, provocando inseguridad e inestabilidad personal y corporativa con afectación a gran escala en su imagen frente al personal externo de las empresas, es decir, clientes o usuarios y en el caso de los individuos la afectación se dirige a familiares y amigos. Es por esto que para la obtención de pruebas o evidencias de un delito informático, los analistas informáticos forenses deben contar con elementos, técnicas y herramientas especializadas que les permita realizar las investigaciones más apropiadas de acuerdo con los delitos informáticos identificados y la ubicación de la información comprometida en las organizaciones y así presentar evidencias más acertadas

para la defensa o acusación de una persona o entidad involucrada en un incidente de seguridad.

De acuerdo con el tipo de incidente de seguridad informática presentado en las organizaciones, el análisis forense digital se realiza para cumplir 2 objetivos:

- Establecer lo sucedido en el sistema informático afectado y sujeto de investigación para presentar pruebas ante un tribunal sobre el procedimiento realizado para acceder al sistema y daños que ha producido cuando el incidente se trata de un hecho delictivo, intrusión informática y delitos que involucran al personal propietario del equipo informático y existe intervención de entidades policiales y judiciales.

- Servir de respuesta eficiente para identificar la responsabilidad sobre el incidente en la ejecución de acciones y eventos descubiertos durante el proceso de análisis de un incidente de seguridad. Este objetivo hace que la implementación de los servicios del análisis forense digital en las organizaciones sea considerada como solución avanzada para responder a los incidentes, detección y seguimiento de intrusos informáticos; de forma similar, los procedimientos forenses informáticos tales como la búsqueda de patrones de información, clasificación y recuperación de información cumplen el propósito de servicio complementario a la seguridad informática y la auditoria informática respecto a la gestión de incidentes de seguridad, confirmación de la existencia de la inseguridad informática en las organizaciones y revisión de las políticas de seguridad implementadas a los procesos corporativos ya que ofrece información relevante para: identificar los datos de la empresa que se pueden ver afectados, evaluar la efectividad de medidas que se requiere tomar ante la existencia de un incidente de seguridad para apoyar a la toma de decisiones, registrar y documentar los incidentes y/o eventos, emprender acciones legales, esclarecer los hechos y atribuciones a personal involucrado en incidentes de seguridad y presentar los resultados de forma adecuada que evite la impunidad del incidente.

Los investigadores forenses informáticos deben tener claro los tipos de conductas irregulares informáticas y delitos informáticos que pueden presentarse en diferentes ámbitos, así como también deberá tener en cuenta cual es la localización de la información y de los datos en el sistema informático o actividad del usuario que requiere la investigación forense para utilizar herramientas de software adecuadas para análisis forenses que permita preservar la escena del delito y las evidencias con integridad y confiabilidad.

Algunos autores, exponen características concretas relacionadas a los delitos informáticos, tal como menciona el investigador Miguel Ángel Davara Rodríguez en su obra “Derecho informático” de 1993, “El delito informático se define como la

realización de una acción que reuniendo las características que delimitan el concepto de delito, llevada a cabo por el uso de un elemento informático ya sea de hardware o de software[58].
En el libro "Temas de derecho informático: Delitos informáticos. Contratación electrónica. Protección jurídica de programas informáticos" del año 2002, Víctor Arbulú Martínez[59] señala que "el delito informático es todo comportamiento típico, antijuridico, culpable realizado mediante sistemas de procesamientos de datos, contra la información automatizada en perjuicio de una persona natural o jurídica. El delito informático es pluriofensivo ya que puede ir en contra del patrimonio, la intimidad, la seguridad pública y la seguridad informática".

Hugo Vizcardo en el año 2010 señaló que el delito informático representa un comportamiento ilícito, concreto en una acción antiética y sin autorización para procesar datos o transmitirlos. [60]

Pedro Arnedo(2014) referencia algunas conductas antijurídicas que atentan frecuentemente a las organizaciones y a las personas tales como el fraude informático, el contenido obsceno u ofensivo, el hostigamiento y/o acoso, el terrorismo virtual, la pornografía infantil, y delitos que atentan contra la propiedad intelectual[61].

A continuación, se describe de las formas que puede presentarse un delito informático:

- Fraude Informático: Es inducir a otro a hacer o restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio, casi siempre económico, casi siempre económico, utilizando medios informáticos[62] como correos electrónicos, mensajes a dispositivos móviles o páginas web fantasmas para ocasionar una pérdida. En esta modalidad de delito se evidencia el ofrecimiento de recompensas falsas por el intercambio de los datos personales o consignaciones de dinero. Aunque el fraude informático pueda relacionarse con los términos phishing y pharming, en la práctica corresponde a formas diferentes de llevarse a cabo.

[58]SERRANO LEYVA, Carmen. Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. 2021. [En línea]. [Fecha de consulta: octubre 2021] Disponible en: https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373/16528
[59] ARBULÚ MARTÍNEZ, Víctor "Temas De Derecho Informático. Delitos Informáticos. Contratación Electrónica. Protección Jurídica De Programas Informáticos". 2002, Citado por SERRANO LEYVA, Carmen. Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. 2021. p.35.
[60] SERRANO LEYVA, Op. cit, p.39.
[61] ARNEDO, Pedro. Herramientas de Análisis Forense y su Aplicabilidad en la Investigación de Delitos Informáticos. 2014. [En línea] [Fecha de consulta: 25 de enero de 2020]. Universidad Internacional de La Rioja. Valledupar, Colombia. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y
[62]Ibíd., p. 43

- Contenido obsceno u ofensivo: Hace referencia al envío de mensajes a través de internet con contenido que atenta contra la integridad de una o más personas u organizaciones (por medio de redes sociales, emails, etc.).[63]

- Hostigamiento / acoso: Delito que se concreta cuando se contacta a una persona para que realice o entregue algo bajo una situación de amenaza.[64] Hace parte del ciberacoso, el envío mensajes insultantes y ofensivos a persona o personas de manera privada o en un grupo en línea de cualquier red social, envío o divulgación de rumores, amenazas, material confidencial no autorizado, incitación de envío de información, datos, fotos y videos confidenciales que posteriormente puedan reenviarse a otros y exclusión a propósito de personas de algún grupo en línea.

- Terrorismo virtual: Se presenta cuando se ataca a una organización o estado para hacer daño a su sistema de información[65]. Ataques como ataque 0-days o día cero, denegación de servicio, acceso no autorizado, ataques masivos a bancos de un país, ataques a sistemas de aviones en un aeropuerto, difundir noticias falsas de atentados en internet, modificación de resultados electorales de un país, ataques a entidades gubernamentales son considerados como delitos de terrorismo virtual con origen en el mismo país del daño o generado desde el extranjero.

- Pornografía Infantil: Delito que se comete cuando se envían archivos de imágenes o video por la web con contenido sexual explícito con menores de edad[66] en donde se ve comprometida la integridad del menor de edad. La creación, distribución, posesión, almacenamiento, adquisición y exhibición de pornografía infantil con o sin fines de lucros son considerados como delitos relacionados con la pornografía infantil por el convenio del consejo de Europa para la protección de los niños contra la explotación y abuso sexual.

- Propiedad Intelectual: Delito que se comete en el momento que se accede a información privada o confidencial sin la autorización expresa de su autor, ya sea para su distribución gratuita o comercialización. [67]

- Ransomware: Modalidad de delito que se caracteriza por el secuestro de datos de personas u organizaciones utilizando códigos maliciosos en el que se infectan equipos informáticos y se cifran sus datos para inutilizar un sistema o impedir a un usuario el acceso a sus ficheros para luego así pedir una

[63] ARNEDO, Op. cit, p.43
[64] Ibíd., p.44
[65] Ibíd., p.44
[66] Ibíd., p.44
[67] Ibíd., p.44

recompensa por su liberación. El programa ransomware secuestra los datos y muestra un mensaje que exige un pago para restaurar la funcionalidad o la compra de algún programa para restablecer el sistema.

- Ingeniería social: Tipo de fraude informático basado en la manipulación del comportamiento de usuarios a través de engaños y mentiras con argumentos convincentes utilizando gran variedad de herramientas y técnicas[68].

- Phishing: Delito basado en la utilización de técnicas de ingeniería social y códigos maliciosos para la suplantación de identidad de empresas u organizaciones bancarias a través de correos electrónicos que se hacen pasar como confiables para solicitarle al destinatario la comprobación de los datos personales y cuentas bancarias haciendo clic a un link o hipervínculo enviado en el correo que los conduce a sitios web falsos y no a la organización real.

- Pharming: Ataque informático que es una variante del phishing, en el cual se explota una vulnerabilidad en el software de los servidores o de los usuarios que permite que el atacante redirija un nombre de dominio a otra máquina diferente[69] utilizando un código malicioso en el equipo del usuario víctima para que siempre acceda a la misma página web falsa.

- Smishing: Engaño que emplea el envío de mensaje de textos fraudulentos o SMS fraudulentos a usuarios de teléfonos móviles para capturar datos del destinatario y beneficios económicos[70].

- Spyware y Keylogger: La instalación y uso de spyware y Keylogger para la recolección de información no autorizada tales como datos personales, contraseñas, número de tarjeta de créditos, hábitos de navegación del usuario con fines fraudulentos en los equipos informáticos se considera como delito de estafa informática.

- Cryptojacking: Delito basado en el ingreso y uso no autorizado ni detectado de un dispositivo para la minería de criptomonedas sin el consentimiento del propietario del dispositivo mediante engaños para la descarga e instalación de software malicioso de minería en el sistema o el empleo de script en

[68] ESCRIVÁ GASCÓ, Gema. Seguridad informática. 2013. [En línea]. [Fecha de consulta: enero 2020]. Madrid, España: Macmillan Iberia, S.A. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=122.

[69] COLOBRAN, HUGUET, Miquel, et al. Administración de sistemas operativos en red, Editorial UOC, 2008. [En línea] [Fecha de consulta: 25 de enero de 2020]. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3206493

[70] ESCRIVÁ GASCÓ, Gema. Seguridad informática. 2013. [En línea]. [Fecha de consulta: enero 2020]. Madrid, España: Macmillan Iberia, S.A. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=124.

navegadores web para la extracción de criptomonedas sin aviso en segundo plano.

- Ciberespionaje: Delito de robo de información clasificada que puede ser de tipo militar, político, económico o personal mediante el uso de las tecnologías de la información y la comunicación (TIC) por parte de personas, grupos o empresas para obtener algún beneficio económico o personal[71]

- Carta Nigeriana: Modalidad de estafa a través de correo electrónico donde se ilusiona a la víctima con una fortuna inexistente para persuadirla a pagar sumas de dineros por adelantado para acceder a la supuesta herencia.[72]

- Apps estafa: Forma de fraude informático por medio de aplicaciones que contienen códigos maliciosos o "malware", funciones ocultas, imitaciones fraudulentas de la versión legítima de la app, descripción engañosa de uso y difíciles de cancelar que se encargan de realizar cobros excesivos al usuario, robo de datos y suplantación de identidad. En esta modalidad de delito informático, el atacante se aprovecha del usuario víctima utilizando técnicas de ingeniería social para motivarlo a descargar e instalar la aplicación fraudulenta en el dispositivo móvil desde una página web fraudulenta o en la tienda de aplicaciones.

Como puede notarse son diferentes formas de ataque por parte de delincuentes informáticos manipuladas a su antojo sin el más mínimo respeto a la integridad personal. Desafortunadamente, los atacantes cibernéticos emplean cada vez más técnicas sofisticadas e innovadoras para realizar ataques de gran impacto en los sistemas TI de las organizaciones.

A causa de estos actos que atentan contra la seguridad de las organizaciones, se han creado herramientas muy útiles, sofisticadas, con gran efectividad y técnicas que contribuyen en el desarrollo de las investigaciones de delitos informáticos, a la evaluación de las amenazas informáticas de la organización y la detección de forma oportuna de incidentes informáticos para contrarrestar los efectos y fortalecer la capacidad de respuesta ante incidentes por parte de la organización.

[71] UNOD. s.f. Ciberespionaje. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: : https://www.unodc.org/e4j/es/cybercrime/module-14/key-issues/Cyberespionage.html

[72] CENTRO CIBERNÉTICO POLICIAL DE COLOMBIA. Carta Nigeriana. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://caivirtual.policia.gov.co/contenido/carta-nigeriana-herencia

5.3 FASES DE ANÁLISIS FORENSE MANEJADAS EN LAS INVESTIGACIONES DE DELITOS INFORMÁTICOS EN INFRAESTRUCTURAS TI EN COLOMBIA

El Análisis Forense Digital hace referencia al conjunto de principios y técnicas[73] que se utilizan para adquirir, conservar, documentar, analizar y presentar las evidencias digitales válidas y necesarias en investigaciones internas corporativas, procesos judiciales, investigaciones de seguridad nacional e inteligencia. La práctica de las investigaciones forenses realizada por los profesionales informáticos forenses incluye muchos retos como un minucioso entendimiento de la legislación informática y total precaución de lo se requiere analizar e investigar en la fuente de los datos, dispositivos a examinar o elementos significativos de la evidencia digital, por lo que los analistas forenses deben realizar una serie de procedimientos que ayudan a que las investigaciones realizadas en la escena del crimen y las pruebas que de esta se obtengan, tengan el valor necesario ante un tribunal.

En el ámbito internacional, la norma ISO/IEC 27037:2012 se considera como el estándar forense que describe los procedimientos y las mejores prácticas que los analistas informáticos forenses deben aplicar para el tratamiento y manejo adecuado de la evidencia digital. La ISO/IEC 27037:2012[74] define como fases del proceso del manejo de evidencia digital para los investigadores forenses a las actividades de identificación, recopilación, adquisición y preservación de evidencia digital orientando de esta manera a las organizaciones en la formalidad de procesos para el aseguramiento de evidencia digital basada en los principios de relevancia, confiabilidad y suficiencia que impliquen dispositivos de almacenamiento digital, componentes informáticos, discos duros, discos ópticos, disquetes, CD, DVD, teléfonos móviles, tarjetas de memorias, computadores, cámaras digitales, redes que se basen en protocolos TCP/IP y demás, sistemas de navegación móvil para fines probatorios.

Identificación: reconocimiento inicial para hallar la evidencia digital física o lógica.

Recolección: recolección de la evidencia y traslado al laboratorio, para lo cual debe tener en cuenta los recursos informáticos y el tiempo disponibles en el lugar de los hechos. El proceso se debe documentar.

Adquisición: incluye realizar la copia exacta del contenido físico o lógico de los objetos involucrados en la investigación.

---

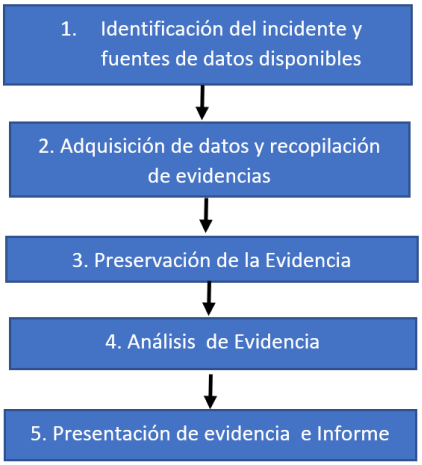
[73]LÓPEZ DELGADO, Miguel. Análisis Forense Digital. 2007. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[74]ISO. ISO/IEC 27037:2012. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.iso.org/standard/44381.html

Preservación: Se refiere a que la evidencia digital debe conservar su integridad durante todo el proceso.

López Delgado (2007)[75] destaca cinco fases necesarias para realizar el Análisis Forense Digital: Identificación de incidente, Recopilación de evidencias, Preservación de la evidencia, Análisis de la evidencia y Documentación y Presentación de los resultados. La mayoría de los modelos de procesos para realizar el análisis forense digital siguen cuatros fases básicas en las investigaciones: adquisición, examen, análisis e informe.

Figura 3. Fases del Análisis Forense Digital de un incidente informático.



Fuente. Elaboración Propia.

En Colombia, los profesionales que realizan las investigaciones forenses digitales, apoyan los procesos de la cadena de custodia de información digital, documentan los reportes basándose en la información recopilada y preparan la evidencia para ser utilizada por terceros, deben tener en cuenta los lineamentos penales que rigen el análisis de la evidencia digital para los delitos informáticos que se encuentran establecidos en: la Ley 527 de 1999 o Ley del Comercio Electrónico que define los procedimientos a seguir para mantener archivos digitales y se puedan usar como evidencia; el Código de Procedimiento Penal – ley 906 de 2004 Título I Capítulo V correspondiente a todo el proceso de la cadena de Custodia. De igual forma, en esta ley, el artículo 270 define la actuación del perito, el Título II en el Capítulo único señala los elementos materiales probatorios; la Ley 1273 de 2009 o Ley de la protección de la información y los datos, Ley 1581 de 2012 o ley de Tratamiento de datos personales, Documento CONPES 3701 de 2011 lineamientos de políticas para ciberseguridad y ciberdefensa, Documento

[75]LÓPEZ DELGADO. Op. cit, p. 47

CONPES 3854 de 2016 Política Nacional de seguridad Digital, Guía No13 Evidencia Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de 2016, Manual del Sistema de Cadena de Custodia de la fiscalía General de la Nación de 2018.

Asimismo, los profesionales o expertos en seguridad informática deben contar con certificaciones reconocidas que acrediten las habilidades en seguridad informática avanzada, análisis forenses, técnicas antiforenses que utilizan los atacantes informáticos, hacking ético, amenazas persistentes avanzadas, respuestas de incidentes, uso de herramientas de hardware y software forenses, pentesting, destrezas en la detección de ataques informáticos, ISO 27001, entre otras; A continuación, se menciona algunas certificaciones importantes como: GIAC (certificación Global de Aseguramiento de la Información), CHFI (Computer Hacking Forensic Investigation) de EC-Council, CEH(Hacker Ético Certificado o profesional en pruebas de penetración) de EC-Council, ESCA (Analista de Seguridad certificado), CISSP (Certified Information Systems Security Professional), CISM (Certificación para gerenciar la seguridad de información) de ISACA, Q/SSE (Qualified Software Security Expert), ACE (AccesData Certified Examiner), GCFA (Analista forense certificado GIAC), certificación OSCP, Certificación EnCE (Certificación en conocimientos de Encase avanzados Forensic II), CCNA (Cisco Certified Network Associate) y CCNP de Cisco, entre otros.

Debido a la fragilidad y volatibilidad de la evidencia digital en los procesos judiciales relacionados a los delitos informáticos, los investigadores forenses deben procurar que la evidencia digital presentada sea reconocida como evidencia válida y formal. Por esta razón, la evidencia digital requiere de un tratamiento especial para cumplir las características legales definidas en la legislación Colombiana tales como la autenticidad, suficiencia, confiabilidad, relevancia, presentación correcta de la cadena de custodia y conformidad legislativa.

5.3.1 Procedimientos para la recolección y manejo de la Evidencia Digital

En relación con el análisis forense digital en Colombia, los profesionales forenses informáticos deben tener claro los procedimientos establecidos en la Guía número 13 de Seguridad y Privacidad de la Información: Evidencia Digital del Ministerio de Tecnologías de Información y Comunicaciones y el Manual de Procedimientos del Sistema de cadena de Custodia. Asimismo, los analistas informáticos forenses en Colombia tienen en cuenta las buenas prácticas de la norma ISO/IEC 27042:2015 para el análisis e interpretación de evidencia digital y estándar ISO/IEC 27037:2016 para los procesos de identificación, recopilación, adquisición y preservación de evidencias digitales. Entidades como la Policía Nacional de Colombia toma como referente adicional de lineamientos para el tratamiento y obtención de la evidencia digital a las “Directrices globales para laboratorios

forenses digitales" de 2019 de la INTERPOL[76] para fortalecer las metodologías anteriormente mencionadas ante la necesidad de resolver situaciones delictivas informáticas en procesos legales utilizando la evidencia digital.

5.3.1.1 Procedimiento de Evidencia Digital de MinTIC Colombia.

La Guía número 13 de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de Información y Comunicaciones de Colombia[77] se refiere a las medidas que se deben tener en cuenta respecto con la Evidencia Digital, por ejemplo, verificar si se requiere la realización del procedimiento de evidencia digital cuando se reporta un incidente, reducir la alteración y pérdidas de datos, crear y llevar bitácoras de las actividades con las respectivas hora y fechas específicas de realización, analizar todos los datos recolectados en la investigación, elaborar y presentar un reporte de los hallazgos con toda la información relevante y necesaria de la investigación.

A continuación, la figura 4 expone los procesos recomendados**.**

Figura 4. Diagrama de proceso de Evidencia Digital, MinTIC.

Fuente: Ministerio de Tecnologías de Información y Comunicaciones de Colombia, Disponible en: https://mintic.gov.co/gestionti/615/articles5482_G13_Evidencia_Digital.pdf

[76]INTERPOL. Global Guidelines for Digital Forensics Laboratories. 2019. [En línea]. [Consulta: octubre 2021]. Disponible en: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

[77]MINTIC. Evidencia Digital, Guía No 13. 2016. [En línea]. [Consulta: octubre 2021] Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

La guía número 13 de Evidencia Digital de MinTIC, recomienda realizar verificación previa del evento reportado como incidente para evaluar y decidir si existe algún atentado contra la disponibilidad, la integridad o confidencialidad de la información que requiera de un análisis forense basado en metodología general del procedimiento de evidencia digital. Una vez realizada la labor de verificación y confirmación de incidente, el analista forense debe proceder con la primera fase de la metodología. Así mismo, la guía advierte a las organizaciones la importancia de contactarse con el Grupo de Respuesta a Emergencia Cibernéticas COLCERT o CCP para el acompañamiento de todos los procesos de recolección y/o análisis de la evidencia cuando el caso del incidente lo requiera.

Fase 1. Aislamiento de la Escena.

Esta fase define los procedimientos para realizar el aislamiento de la escena del incidente con el propósito de evitar la corrupción de la zona donde se produjo el incidente y la contaminación o alteración de la evidencia. Los procedimientos que se deben ejecutar en esta fase son:

- Fotografiar el equipo o lugar del incidente antes de realizar alguna operación o tocarlo.

- Establecer un perímetro de seguridad, para que nadie puede acercarse.

- Verificar el estado del equipo. Cuando el equipo se encuentre encendido, no debe apagarse y realizar las siguientes operaciones:

    - Sellar todos los puertos USB, puerto firewire, Unidades CD/DVD etc.. que imposibilite alteraciones posteriores al registro de la escena del incidente.

    - Tomar fotografías que registre la pantalla del equipo del incidente (software corriendo, documentos abiertos, notificaciones, hora y fecha entre otros..).

    - Asegurar el equipo (Si se trata de un portátil, encargarse del encendido con el cargador hasta hacer entrega o iniciar el análisis respectivo.

    - Capturar la información volátil del equipo cuando sea posible antes que se apague empleando las herramientas forenses necesarias.

- En el caso que el equipo se encuentre apagado, evitar encender el equipo ya que podría alterar la escena o borrar información que se podría obtener posteriormente.

- Recolectar la información con elementos necesarios tales como las estaciones forenses, dispositivos de backups, medios formateados y/o estériles, cámaras

digitales, cintas y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rotulo o etiquetas etc..

- Garantizar la cadena de custodia de la información con el almacenamiento de la información original en un sitio de acceso restringido.

- Obtener información de dispositivos que tuvieron contacto o interacción con el equipo en cuestión (firewalls, switches, Access points etc..).

Fase 2. Identificación de Fuentes de Información y Adquisición de datos.

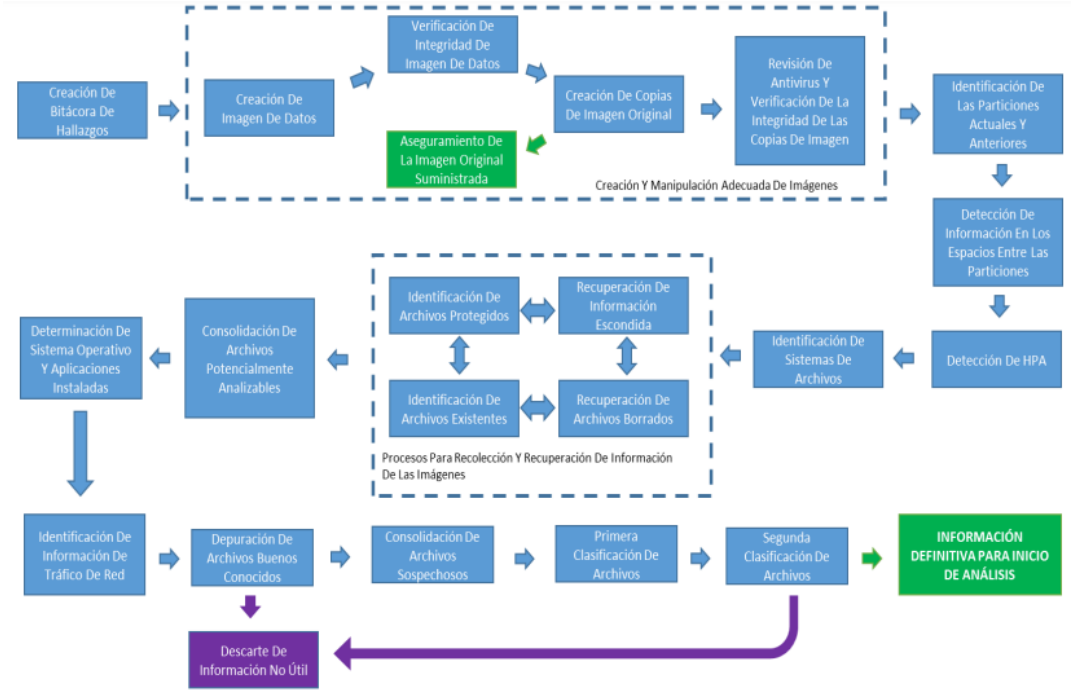
Esta fase tiene como propósito definir las fuentes de datos más comunes para extraer la información requerida para el proceso de evidencia digital, tales como: los computadores de escritorios y portátiles, servidores, almacenamiento en red, dispositivos USB, Discos duros extraíbles, CD/DVD, Discos Ópticos y Magnéticos, Firewire, Celulares, cámaras digitales, grabadoras de video y audio, registros o log del sistema entre otros.

De igual manera, la guía número 13 establece tres pasos fundamentales que se deben realizar para la adquisición de los datos tras la identificación de las fuentes de información. Los tres pasos principales para la adquisición de datos comprenden: primero, la planificación de la adquisición de los datos; segundo, la adquisición de los datos y tercero, la verificación de la integridad de los datos recolectados. El primer paso considera solo las fuentes específicas de información y el orden a realizar la extracción de la información de acuerdo con la volatilidad de la información, complejidad de extracción o según la experiencia del analista. El segundo paso, se refiere al proceso de recolección de información con el uso de las herramientas forenses para copiar datos volátiles y no volátiles, ya sea por acceso local al sistema o a través de la red. Por último, el paso de la verificación de la integridad de los datos recolectados requiere emplear herramientas de cálculos de resumen de mensajes que generan un valor determinado con fines legales para certificar la autenticidad de la información de fuente original y la copia. La realización de la cadena de custodia debe realizarse con total cuidado desde el momento que se establezca que la información va a utilizarse con fines legales especialmente en el registro de cada acción, desde el inicio de la recolección, el almacenamiento, la forma como se guarda, la persona quien lo realiza y la hora exacta, las herramientas utilizadas para el proceso de recolección etc..

Fase 3. Examinación y recolección de información

Esta fase se realiza después de la identificación de las fuentes de información, llevando a cabo una secuencia de procesos (figura 5) para la recolección y examinación de medios/ información así:

Figura 5. Diagrama de Examinación y Recolección de Información.



Fuente: Ministerio de Tecnologías de Información y Comunicaciones de Colombia, Disponible en: https://mintic.gov.co/gestionti/615/articles5482_G13_Evidencia_Digital.pdf

- Creación del archivo/bitácora de hallazgo (Cadena de custodia): Este proceso garantiza la creación y aseguramiento de un documento que puede ser físico o electrónico para llevar el historial de las actividades realizadas y hallazgos encontrados que facilite la reconstrucción del caso posteriormente.

- Imagen de Datos: Proceso para generar las imágenes de datos pertinentes al caso que se investiga. Las herramientas recomendadas para la extracción de imagen en este proceso son Linux dd o Encase Forensic Software.

- Verificación de Integridad de la imagen : Proceso que se realizar para calcular el compendio criptográfico (SHA1/MD5) a cada imagen suministrada para la comparación con el de la fuente original. Teniendo en cuenta el resultado de la comparación, el analista rechaza o aprueba la imagen de datos. Por lo que, si la comparación arroja un resultado negativo, la imagen suministrada se debe rechazar.

- Creación de una copia de la imagen suministrada: Como se ha dicho que análisis de datos nunca se debe trabajar sobre la imagen original suministrada, este proceso permite realizar una copia master y a partir de esta, se debe producir las imágenes que se requieran.

- Aseguramiento de la imagen original suministrada: Este proceso debe garantizar la conservación de la cadena de custodia de la imagen suministrada sin alteraciones y el mantenimiento de la validez jurídica de la evidencia.

- Revisión Antivirus y verificación de la integridad de la Copia de la Imagen: Se refiere al aseguramiento y verificación en la copia de la imagen que no tenga algún tipo de virus. Así mismo, se debe verificar la integridad de la copia periódicamente en todo el proceso del análisis de datos siguiendo el procedimiento del Manual Único de Cadena de Custodia de la Fiscalía[78].

- Identificación de la particiones actuales y anteriores: Permite reconocer las particiones del dispositivo, las características especiales de la información y plantear las estrategias adecuadas para recuperar la información.

- Detección de Información en los espacios entre las particiones: Al detectarse datos en estas zonas de la imagen, se debe realizar un análisis para establecer si existe algún tipo de información relevante que contribuya a la investigación. Si estos archivos están protegidos deben ser tenidos en cuenta en la fase de la identificación de archivos protegidos o incluirlos en los archivos definidos como potencialmente analizables.

- Detección de un HPA (Host Protected Area): Este proceso se realiza únicamente cuando los Metadatos indican la existencia del HPA. Si esto sucede, se debe realizar el proceso de detección de información en los espacios entre las particiones.

- Identificación del Sistema de Archivos: Luego de precisar las particiones en el dispositivo, se hace necesaria la identificación del sistema de archivos con la finalidad de realizar las actividades posteriores del análisis de datos.

- Recuperación de archivos borrados: En este paso, el analista debe tratar de recuperar la mayor cantidad de archivos borrados del sistema de archivos con el propósito de preservar evidencias. Los archivos potencialmente analizables están formados por los archivos que se han recuperado exitosamente, exceptuando los archivos protegidos que son tenidos en cuenta en la fase de identificación de archivos protegidos.

[78] FISCALÍA GENERAL DE LA NACIÓN, Colombia. Manual del sistema de cadena de custodia. 2018. [En línea]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

- Recuperación de Información escondida: Se refiere al proceso de examinar de manera exhaustiva el slack space, campos reservados y espacios etiquetados en el sistema de archivos. Los archivos protegidos también serán tenidos en cuenta en el análisis de archivos protegidos.

- Identificación de archivos existentes: Luego de la recuperación de los datos, se realiza la clasificación de los archivos como protegidos y no protegidos. Los archivos no protegidos son aquellos archivos potencialmente analizables mientras que los archivos protegidos hacen parte de la fase de análisis de archivos protegidos.

- Consolidación de archivos potencialmente analizables: En este paso se fijan los archivos encontrados en los procesos anteriores.

- La determinación del Sistema Operativo y las aplicaciones instaladas, la identificación de la información de tráfico de Red, la depuración de archivos, la consolidación de archivos sospechosos y la clasificación de archivos en primera y segunda clasificación hacen parte del procedimiento de examinación y recolección de información.

Esta fase también indica a los analistas forenses el uso de estampas de tiempos precisas con sincronización de hora o servicio NTP para garantizar la precisión e integridad de la información recolectada.

Fase 4. Análisis de Datos.

Esta fase tiene como propósito identificar la información valiosa y relevante que se extrajo de las diferentes fuentes de información (logs, archivos, eventos, fotos, videos, entre otros). Dicha fase involucra cuatro etapas: El análisis de la información prioritaria basado en la exclusión de archivos prioritarios de acuerdo con la relevancia y criterios del investigador, siendo esta etapa iterativa hasta la resolución del caso o falta de datos para analizar; la generación de listado de archivos comprometidos con el caso requiere del criterio del investigador para conformar el grupo de archivos pertinentes a la evidencia del caso; la obtención de la línea de tiempo de la evidencia permite la reconstrucción de los hechos utilizando los atributos de tiempo de los archivos. El analista debe considerar las estampas de tiempo más comunes como la fecha de modificación, la fecha de acceso y la fecha de creación para la sincronización de los sistemas de información con NTP que le permita realizar el adecuado proceso de análisis del incidente; la elaboración del informe de hallazgos permite al analista describir elementos relevantes al caso y la forma de descubrimiento.

Fase 5. Reporte.

Esta fase permite conocer el resultado de la información y evidencia que se obtuvo en la fase de análisis de datos. El reporte debe incluir aspectos como el resultado de los análisis efectuados por el analista forense, herramientas y procedimientos utilizados en la recolección y análisis de la información, definición de la presentación del informe y audiencia a la que se dirige, definición de actuaciones pertinentes para corregir el incidente, justificar las conclusiones, hipótesis o explicaciones alternativas presentadas en el documento y presentar recomendaciones respecto a las políticas, procedimientos, herramientas y demás observaciones del proceso forense.

5.3.1.2 Manual Cadena de Custodia de la Fiscalía General de la Nación

En Colombia, el Manual para el manejo de la Custodia de evidencias e información recolectada que indica el procedimiento para la Evidencia Digital de la guía 13 de MinTIC fue actualizado por la Fiscalía General de la Nación en el mes de abril de 2018. Este manual define las pautas que se deben llevar a cabo para el tratamiento de los elementos de prueba y evidencia física para garantizar la fiabilidad de la prueba durante todo el proceso de análisis forense. Aunque el manual está dirigido al manejo de la evidencia Física contempla algunas acciones que pueden ser aplicadas para el tratamiento de la evidencia Digital.

En el caso de la evidencia digital, el manual de cadena de custodia indica en el esquema de formas de recolección, embalaje y recomendaciones para realizar el tratamiento de dispositivos de almacenamiento digital (computadores, USB, discos duros entre otros) y celulares, como parámetros: el estudio que se requiere, el área de destino, acciones para la recolección y embalaje y las precauciones (tabla 1) que se requieren como medidas para prevenir la posible pérdida, deterioro o borrado de cualquier tipo de información que se encuentre contenida en este tipo de elemento material probatorio EMP y evidencia física EF de tipo digital.

Como procedimientos que se puede distinguir en este manual para el manejo de la evidencia digital se encuentran: la forma de aislamiento de la evidencia digital en el lugar de los hechos a través de la desconexión total de la red, el control de energía estática con bolsas antiestáticas o con otros materiales que eviten la exposición de la evidencia digital a condiciones ambientales de altas temperaturas, humedad, caídas, golpes, daños por ralladuras, evitar rótulos sobre la superficie de los dispositivos de contenido de información digital y recomendaciones para la recolección de datos en los dispositivos cuando se encuentren en estado apagado o encendido, llevar registros de las actividades realizadas para la Cadena de custodia y formatos diligenciados pertinentes al procedimiento, entre otros. De igual manera, el analista forense digital debe

registrar los aspectos relacionado a los dispositivos de almacenamiento digital y celulares tales como, la marca, el modelo, capacidad de memoria, almacenamiento, características del dispositivo, tipo de puertos posibles, accesorios del dispositivo en el lugar de los hechos, etc.. para realizar de forma adecuada la recolección e identificación de la evidencia digital en el formato llamado "Registro Cadena de Custodia"[79].

Tabla 1. Esquema para el manejo la de la Evidencia Digital en la Cadena de Custodia

	Tipo de EMP Y EF	
Aspectos	**Computadores (De Escritorio, Portátiles, Servidores) y Dispositivos de Almacenamiento digital**	**Celulares**
Estudio Solicitado	Recuperación y extracción de Información. Análisis de Código malicioso Estudio técnico o evidencia digital. Cálculo de función HASH para las imágenes	Recuperación y extracción de Información. Identificación de software malicioso Identificación de cuentas de usuarios, aplicaciones y sistema operativo instalado. Relación de la información entre dispositivos. Análisis link de comunicación
Área de Destino	Informática forense o el Área que establezca la entidad	Informática forense o el Área que establezca la entidad.
Recolección y Embalaje	Obtener datos volátiles, si el dispositivo se encuentra encendido con herramientas de software especializadas; tomar fotografías del contenido de la pantalla. Desconectar el equipo directamente de la fuente de alimentación. Sí el dispositivo se trata de un portátil, se debe retirar la batería y embalar todos los elementos: el adaptador de corriente, batería y cables. Extraer el disco duro y especificar las características del equipo de cómputo de donde se extrae. Utilizar para el embalaje bolsas antiestáticas o materiales que disminuyan las condiciones de calor, humedad electromagnetismo, tales como las bolsas tipo burbuja, plástico, cajas de cartón o plásticas. Solicitar cuando sea posible, las contraseñas de descifrado, desbloqueo y acceso a dispositivos.	No encender el dispositivo si se encuentra apagado. No retire la batería, tarjeta SIM o la tarjeta de almacenamiento del equipo. Aislar al equipo de señales cuando se encuentre encendido (colocarlo en modo avión, bolsa Faraday, entre otros). Apagar el teléfono para evaluar si el encendido del equipo presenta algún bloqueo por patrón, contraseña o huella. Solicitar cuando sea posible, las contraseñas de descifrado, desbloqueo y acceso a dispositivos. El embalaje del equipo debe ser individual.

[79]FISCALÍA GENERAL DE LA NACIÓN. Manual del sistema de cadena de custodia. 2018. [En línea]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

Tabla 1 . Esquema para el manejo la de la Evidencia Digital en la Cadena de Custodia. (Continuación)

Precauciones	Evitar la exposición de la evidencia digital a golpes, caídas, altas temperaturas, vibraciones, ondas electromagnéticas, ralladuras etc..; manipular el equipo únicamente cuando sea necesario; evitar el uso de rótulos, marcadores o adhesivos sobre la superficie del dispositivo que contiene la evidencia digital, llevar el equipo pronto al laboratorio.	Evitar la exposición de la evidencia digital a golpes, caídas, altas temperaturas, vibraciones, ondas electromagnéticas, ralladuras etc..; manipular el equipo únicamente cuando sea necesario; evitar el uso de rótulos, marcadores o adhesivos sobre la superficie del dispositivo que contiene la evidencia digital, llevar el equipo pronto al laboratorio.

Fuente: Elaboración propia, basado en el Manual del Sistema de Cadena de Custodia de la Fiscalía General de la Nación, disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

5.3.1.3 Manual Único de Policía Judicial

El Manual destaca aspectos importantes y criterios unificados para el desarrollo de las actividades de la Policía Judicial en los procesos de apoyo a las investigaciones penales, obtención legal de información, recolección de evidencias y elementos materiales probatorios de acuerdo con la normatividad legal, constitucional y de jurisprudencia para el territorio Colombiano.

Con respecto a la realización del Análisis forense Digital para los delitos informáticos, el manual Único de la Policía Judicial[80] señala los aspectos básicos y relevantes para la búsqueda de información en bases de datos, el procedimiento de los analistas para la interceptación de comunicaciones, la recuperación de información en dispositivos o servidores con almacenamiento físico o virtual, el proceso de cadena de custodia; También, establece que un equipo encargado de la Policía Nacional de Colombia y el CTI (Cuerpo Técnico de investigación de la Fiscalía General de la Nación) son los que se ocupan de los procesos de búsqueda, recolección y aseguramiento de la evidencia mediante el servicio de criminalística de campo, la prestación del servicio pericial, servicios de laboratorios forenses que se requiera en las entidades públicas, entidades privadas o a particulares. En el Manual Único de Policía Judicial se puede distinguir que las actividades que desarrolla el servidor experto de la policía

[80]COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Consejo Nacional De Policía Judicial. Manual Único de Policía Judicial. Versión N.2. [En línea]. [Consulta: octubre 2021]. Disponible en : https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

judicial en informática forense incluyen las fases de inspección de lugar de los hechos, identificación de la información, extracción y recolección de la evidencia de tipo digital, embalaje de medios de almacenamiento electrónico con evidencia digital bajo protocolos para la cadena de custodia, análisis e Informe de resultados y hallazgos obtenidos.

Dentro de las directrices establecidas para el manejo y tratamiento de la evidencia de tipo digital en el Manual Único de Policía Judicial, se encuentran las siguientes:

- Se requiere de una orden judicial para realizar la recopilación de evidencias de tipo digital en equipos terminales, dispositivos o servidores con almacenamiento físico o virtual.

- Se debe garantizar la reserva de la información obtenida.

- La recopilación de la información que se realice debe estar dirigida a fines probatorios.

- Documentar el lugar de los hechos, relacionar las claves de acceso a los equipos, aplicaciones y archivos.

- Documentar el formato de policía judicial con la información relacionada a la escena del hecho del incidente, ubicación del incidente, conexiones, estado de los elementos encontrados, hallazgos pertinentes, anexar fotografías.

- El descubrimiento, recolección, recuperación, análisis y custodia de la evidencia de tipo digital estará a cargo de los expertos en informática forense.

- Se debe embalar los medios de almacenamiento electrónico en bolsas antiestáticas, plásticas, de papel o cajas de cartón sin rótulos o adhesivos en la superficie.

- Registrar la marca, el modelo y serie del equipo de cómputo portátil o de escritorio para realizar el embalaje y sellar los puertos y conexiones del dispositivo.

En la siguiente gráfica se observa los procesos relacionados con el análisis forense digital que realiza la policía judicial en investigaciones de delitos informáticos.

Figura 6. Servicios de Informática Forense para la Policía Judicial de Colombia.

Estudio o análisis	CTI	INML y CF	DIJÍN - PONAL	¿Puede ser requerido dentro de acto urgente?
Extracción de información a equipos terminales móviles	✓		✓	SI
Tratamiento y análisis de la evidencia digital.	✓		✓	NO
Realizar imágenes forenses			✓	NO
Recolectar datos volátiles			✓	SI
Identificación y recolección de evidencia digital Logs, bases de datos, sistemas de información, servidores, máquinas virtuales y datos volátiles	✓			SI
Examen en laboratorio de dispositivos de almacenamiento digital y dispositivos móviles	✓			NO
Adquisición de imagen forense de medios de almacenamiento digital	✓			NO
Recuperación de información eliminada u oculta	✓			
Búsqueda de información específica	✓			
Desciframiento de archivos	✓			
Extracción de información	✓			
Obtención de información dejada al navegar	✓			
Identificación de software empleado en la comisión de hechos delictivos	✓			
Verificación de software en casos de usurpación de código fuente	✓			
Análisis de malware	✓			
Duplicado de medios de almacenamiento digital con fines de traslado de evidencia a otros procesos judiciales.	✓			

Fuente: Consejo Nacional de Policía Judicial, Fiscalía general de la Nación. Disponible en : https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

5.3.1.4 Global Guidelines for Digital Forensics Laboratories de INTERPOL

Es un documento modelo que brinda las directrices para el aseguramiento de la evidencia digital como admisible en los tribunales de justicia nacionales e internacionales, dirigidos a los países miembros de la INTERPOL.

En las directrices de la INTERPOL para los laboratorios forenses digitales[81] se explica los procedimientos necesarios para implementar y administrar un laboratorio forense digital (DFL) y las pautas técnicas para administrar y procesar la evidencia digital. Esta guía puede ser utilizada por los países para fortalecer los procesos de análisis forense digital en sus territorios. (INTERPOL, Global Guidelines for Digital Forensics Laboratories. 2019).

[81]INTERPOL. Global Guidelines Digital Forensics Laboratories. 2019. [En línea]. [Fecha de consulta: octubre, 2021]. Disponible en: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics Laboratory.pdf

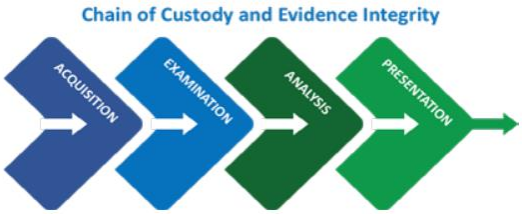
Para la gestión de un caso en laboratorio digital forense, las directrices de la INTERPOL recomiendan siete pasos (figura 7) : recibir una solicitud, registrar el caso, registrar la evidencia digital, tomar fotografías del estado de la evidencia, realizar el análisis, devolver la evidencia y cerrar el caso; para asegurar que el trabajo realizado por el forense digital con la evidencia de tipo digital sea admisible.

Figura 7. Pasos para la gestión de casos en el Laboratorio Digital Forense.

Fuente: INTERPOL. Disponible en :https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

Así mismo, las directrices de INTERPOL establecen que se requiere de cuatro fases para la realización del análisis de la evidencia digital en el laboratorio digital forense: Adquisición, examen, análisis y presentación. Además, el documento recomienda que la cadena de custodia debe estar actualizada durante todo el proceso de manipulación, se debe asegurar la integridad de la evidencia digital en todo momento y repetir las fases de examen y análisis hasta satisfacer la solicitud del caso asignado.

Figura 8. Modelo de procesos para el análisis de la evidencia digital.



Fuente: INTERPOL. Disponible en :https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

En enero del año 2018 en la ciudad de Bogotá, en Colombia se abrió el primer laboratorio forense de Cibercrimen infantil[82] de Suramérica, en alianza con Estados unidos a través de la oficina de Investigaciones de seguridad Nacional del

[82] U.S. Immigration and Customs Enforcerment. Policía Nacional de Colombia e ICE abren laboratorio forense dedicado a la explotación infantil. 2018. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.ice.gov/es/news/releases/policia-nacional-de-colombia-e-ice-abren-laboratorio-forense-dedicado-0

servicio de Inmigración (HSI) y control de aduanas de los Estados unidos (ICE) para realizar investigaciones de delitos de explotación infantil, analizar evidencias y material probatorio que afecten a la integridad infantil y adolescente. Debido a que Colombia no tenía un laboratorio forense de cibercrimen dedicado al análisis de medios electrónicos, las investigaciones se retrasaban considerablemente.

Para el año 2020, en Cartagena Colombia se instaló el Laboratorio de Investigación de Delitos cibernéticos transnacional (TC2IL) como apoyo en las investigaciones de la explotación sexual infantil y delitos cibernéticos transnacionales. Siendo el segundo laboratorio forense en Colombia para el fortalecimiento de las capacidades técnicas de la Policía Nacional de Colombia y los fiscales. El equipo forense informático del que dispone el laboratorio forense (TC2IL) permite los expertos utilizar técnicas avanzadas en investigación forense y realizar legalmente la extracción de datos borrados y cifrados de dispositivos como celulares, portátiles, computadores etc.. para la obtención de pruebas delictivas para combatir delitos cibernéticos, explotación sexual infantil, pornografía infantil, delitos relacionados con el narcotráfico, la falsificación de documentos, fraudes bancarios entre otros.

5.3.2 Modelo de procesos de Análisis Forense Digital Estándar

A continuación, se presenta un modelo de procesos de análisis forense digital estándar basado en 6 fases que protege del principio de la admisibilidad y validez en las evidencias digitales obtenidas:

- Esterilidad de los medios informáticos de trabajo: Se refiere al proceso inicial que debe realizar el investigador forense informático para verificar la validez de conservación de esterilidad de los medios informáticos requeridos para iniciar la investigación forense, hecho que implica que se garantice que las herramientas a utilizar en el proceso forense son confiables porque no han sufrido algún tipo de alteración, sustitución, contaminación ni han sido expuestas a variaciones magnéticas, laser, o similares[83] que puedan afectar la evidencia digital.

- Adquisición: Es la fase que tiene como finalidad obtener los elementos de la evidencia digital a partir de un soporte o fuente de datos y asegurar la prueba electrónica para desarrollar el proceso de investigación. Debido a que la escena original del incidente informático no debe ser jamás alterada para garantizar la comprobación de los resultados de la evidencia digital por

[83] CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Bogotá, Colombia: Universidad de los Andes. 2012. [En línea]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/69374?page=172. ISBN. 978-958-695-492-1

cualquiera de las partes implicadas durante proceso de investigación, es necesario que el investigador forense informático realice la copia exacta del contenido de la información digital que se identifica en los soportes de datos disponibles como objeto de análisis e investigación en el incidente. En la fase de adquisición se recomienda tener en cuenta la condición de volatilidad de la información para la recolección de la evidencia digital, por eso se debe recolectar primero los datos que se encuentren en el orden de mayor volatilidad al orden de menor volatilidad. Asimismo, se debe efectuar copias de las imágenes de discos de los dispositivos implicados, CD, USB,DVD, Memory Card y Disco Duro en los medios informáticos verificados con anterioridad como esterilizados.

- Validación y preservación de los datos adquiridos: Con el fin de garantizar la integridad de la información obtenida en los medios informáticos esterilizados previamente sea igual a los datos de la escena del incidente informático original, se establece la cadena de custodia para todas las fuentes de información relevantes en el proceso de investigación. En esta fase los analistas forenses digitales deben tener como mínimo 2 copias de respaldo de la información original, la copia original de los datos del incidente y realizar la práctica de cálculo y uso de hash en la información obtenida y archivos considerados como importantes para dejar constancia que la información no ha sufrido alguna alteración y la evidencia digital pueda cumplir los principios de confiabilidad, validez e integridad para la presentación ante un juez.

- Análisis y descubrimiento de evidencia: Una vez que se finalice la verificación de la correspondencia e igualdad del código hash de las copias de información con la copia de la información original, se procede a realizar un análisis exhaustivo que permita la reconstrucción de la línea de tiempo al incidente y el levantamiento de evidencia digital que pueda ser admitida ante un juez.

  La fase de análisis resulta de gran complejidad técnica para los investigadores forenses informáticos debido a que se hace necesario utilizar softwares y hardware especializados para realizar el estudio, la interpretación de los datos que se obtienen por la ejecución de procesos como la aplicación de filtros de ordenación y búsqueda de los datos disponibles, la correlación de actividad, búsqueda de patrones de comportamiento y actividad del usuario, búsquedas por tipo de archivos, búsqueda de formatos especial de archivo, análisis de logs de accesos, análisis de fotos, videos, imágenes, búsqueda de palabras claves, contactos frecuentes y mensajes de correo electrónico, análisis de historial de navegación en internet, redes sociales del usuario, aplicaciones instaladas, recuperación de archivos, entre otros; y la extracción de conclusiones de los datos obtenidos para que se puedan relacionar con los hechos que se investigan.

- Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizado: En esta fase el profesional encargado de la investigación con la evidencia digital debe documentar claramente los procesos realizados, los aspectos correspondientes de las herramientas utilizadas tales como versiones y licencias, los resultados obtenidos en los procesos de investigación, esto con el fin de garantizar la validez de la investigación y prevenir que la evidencia digital pueda ser desechada por el juez.

- Informe: Una vez finalizado el análisis de las evidencias y documentación de los procesos realizado en la investigación, el analista forense digital y/o perito informático debe presentar los resultados encontrados, describir los procesos y técnicas realizadas y conclusiones que determinen si se ha realizado un hecho delictivo con la evidencia analizada en un informe escrito claro, preciso, y ordenado. En esta fase, generalmente se entrega dos tipos de informes, el informe ejecutivo que se dirige a la gerencia y a los responsables de la seguridad informática en la organización y el segundo informe denominado informe técnico que utiliza un lenguaje técnico para detallar la investigación realizada.

De acuerdo con la información obtenida a través de diferentes fuentes se permite resaltar y afianzar aún más la gran importancia y beneficios al momento de utilizar técnicas y herramientas de análisis forense en las investigaciones de delitos informáticos, incidentes de seguridad informática y detección de fallos preventivos permitiendo así encontrar el o los culpables de las violaciones, fallas, amenazas, lesiones y demás atentados sufridos, los cuales ocasionan graves consecuencias para las organizaciones tanto privadas como públicas y/o persona particular.

5.4 TIPOS DE HERRAMIENTAS DE SOFTWARE MÁS UTILIZADOS EN EL ANÁLISIS FORENSE DIGITAL PARA TRATAR LOS INCIDENTES DE SEGURIDAD Y/O DELITOS INFORMÁTICOS EN LAS ORGANIZACIONES

5.4.1 Herramientas Forenses

La actividad de la ciencia forense en el área informática ha recibido diferentes denominaciones por parte de autores tales como: informática forense, análisis forense digital, análisis forense informático, digital forensics, cómputo forense y computer forensics. En el año 2001 en el taller de investigación de informática forense Digital Forensic Research Workshop (DFRWS) se definió el concepto de la informática forense como el empleo de métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales procedentes de fuentes digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos o ayudar a la prevención de actos no autorizados y capaces de provocar una alteración en operaciones planificadas de organismos y empresas[84].

La investigación de los delitos informáticos en las infraestructuras TI puede resultar una labor compleja para el analista forense cuando no aplica los métodos, las técnicas, procedimientos, ni las herramientas de software y hardware adecuadas para establecer los comportamientos ilegales en el tratamiento y/o transmisión de los datos y los abusos informáticos a los que se ve expuesto una organización y mucho menos si el profesional forense desconoce la legislación vigente penal del país donde ejerce su labor y que regula las investigaciones forenses, define los delitos informáticos a analizar e implicaciones legales.

Teniendo en cuenta la definición de informática forense establecida por el Digital Forensic Research Workshop (DFRWS), un analista forense informático debe considerar hacer uso de herramientas forenses y métodos que pueden estar homologadas o no por otros profesionales y que demuestran soluciones con un alto nivel de eficacia, credibilidad, integridad y validez jurídica de resultados ante la comprobación minuciosa de una comunidad de profesionales de investigadores, autoridades judiciales, tribunales y otras entidades de carácter decisorio.

Existen numerosas herramientas forenses comerciales y gratuitas que un analista forense informático puede utilizar en las investigaciones a los soportes o fuentes de datos y dispositivos de almacenamiento de archivos informáticos comprometidos en un incidente de seguridad que contribuyen a las buenas

[84] LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta 23 de Agosto de 2021]. Paracuellos de Jarama, Madrid, RA-MA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=19.

prácticas de preservación de elementos de la evidencia, aseguramiento de la información en una cadena de custodia, adquisición y duplicación exacta de la imagen de la evidencia original, identificación, búsqueda, inspección, análisis, comprensión e interpretación de toda la información que se encuentra en la evidencia en el tipo de almacenamiento de datos del caso del delito informático que se encuentre investigando.

En el año 2014, Francisco Lázaro propone un listado de herramienta de software gratuitos y comerciales [85] que permiten realizar análisis forense digital. De forma similar, Ester Chicano destaca que la elección de herramientas adecuadas por parte de los profesionales informáticos para realizar el análisis forense digital debe tener en cuenta el sistema operativo que utiliza el investigador para realizar los análisis de la información digital y las preferencias en el uso de software libre y software comercial[86]. De igual manera, en el año 2016 los autores argentinos Luis Enrique Arellano y María Elena Darahuge en su obra titulada "Manual de informática forense: Bases metodológicas: Científica, Sistémica, Criminalística, Tecnológica-Pericial y Marco Legal" clasifican las herramientas de software forense en: conjunto de herramientas integradas, herramientas individuales e integradas en paquetes de función específicas, herramientas de funciones específicas, herramientas para el borrado seguro, limpieza y desinfección, herramientas para la duplicación de discos, herramientas para la duplicación en forma remota, herramientas para el manejo de particiones, herramientas para el análisis de Red, herramientas para la recuperación de archivos eliminados, herramientas para la recuperación de archivos encriptados o con claves, herramientas para la recuperación de archivos de la papelera de reciclaje, herramienta de recuperación de datos de Telefonía, celulares, PDA y GPS, herramientas para la elaboración de informe pericial, herramientas de análisis de correo electrónico y herramientas de análisis de código malicioso o Malware.

Teniendo en cuenta estas consideraciones y criterios de clasificación de herramientas forenses, en la tabla 2 se pretende definir cuáles son las herramientas de software forense más utilizadas para los procesos de captura y análisis de información de las evidencias digitales por los investigadores y especialistas forenses según el tipo de medio informático o soporte de datos.

[85] LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=310.
[86] CHICANO TEJADA, E. Gestión de Incidentes de seguridad. IFTCT0109.2014. IC Editorial. ISBN:978-84-16351-70-1

Tabla 2. Herramientas Forenses

Herramientas de Software Forense	
Tipo de Herramienta	**Nombre de la Herramienta**
De Disco y Captura de Datos	EnCase Forensic Imager, FTK Imager, X-Ways Forense, OSFMount Live RAM Capture, Recuva, Disk2vhd, Disk Drill, Easy NTFS Data Recovery, EaseUS Data (Partition) Recovery 9.0, Nuix Investigator, Digital Forensics Framework, SIFT, Autopsy, Wise Data Recovery, Wondershare Recoverit Data Recovery.
De Análisis de Registro	MUI Cacheview, Regripper-registry decoder
De Análisis de correo electrónico	FTK (Forensic Toolkit), Autopsy, EDB, MBOX Viewer PRO, Email Tracker Pro.
Forense de Red	Wireshark, Xplico, Tcpdump, Network Miner, TCPFLOW.
De Dispositivos móviles	Santoku, Elcolmsoft iOS Forensic, Oxygen Forensic Suite, UFED Cellebrite, OSAF, MOBILedit.
De Adquisición y Análisis de Memoria	Responder CE, Volatility, Redline, Bulk Extractor
De Recuperación de Contraseñas	Ntpwedit, ntpasswp, MailPass View, Passware
De Análisis de Malware	Microsoft Process Monitor, PDF Stream Dumper, EsetSys Inspector, Firebug, VirusTotal.
Sistemas operativos orientados a informática forense	CAINE, KALI LINUX, DEFT Linux, DEFT Zero, Linux Matriux.
De Análisis a navegadores web	MyLastSearch, FBCacheView, BrowsingHistoryView, Browser History Viewer, ImageCacheViewer
De funciones específicas: hash y comprobación de integridad	HashMyFiles, QuickHash, Exiftool

Fuente. Elaboración Propia.

5.4.1.1 Herramientas de Disco y de Captura de Datos.

Este conjunto de herramientas de software forense son utilizadas por los analistas forenses para la extracción de imágenes de discos duros que se pretenden investigar, la protección, reparación y mejoramiento del rendimiento del disco duro investigado, optimizar espacio en el disco, recuperación y captura de información contenida en un disco duro que ha sido eliminada o se encuentra existente en el

sistema informático para cualquier tipo de formato de imágenes, videos, documentos, Pdf, textos, entre otros.
Se encuentra en esta categoría las siguientes herramientas:

ENCASE FORENSIC IMAGER: Herramienta comercial versátil, muy reconocida internacionalmente para las investigaciones forenses como realización de imágenes, de departamentos de seguridad en organizaciones, administradores de justicia, policía y empresas a nivel mundial.
Se distingue por ser una herramienta de investigación de entorno gráfico basada en Windows que facilita la labor del analista forense informático para la recolección de datos digital de datos, duplicación exacta del dispositivo bit a bit o fuente original, verificación de la evidencia con generación de valores hash MD5 automáticamente para preservar la integridad de la evidencia recolectada y sea válida para efectos legales en procedimientos judiciales y/o investigaciones corporativas.

Encase, también realiza las funciones de examinador de datos al acceder con vista previa a disco y volúmenes, unidades y otros medios para consultas rápidas y sencillas, compatibilidad de sistemas de archivos, compatibilidad de archivos de correos electrónicos, indexador de datos, análisis de historial web y correo electrónico, realización de búsquedas simultaneas con los archivos de la evidencia a partir de una imagen generada por la herramienta Encase, los dispositivos o discos relacionados de la misma investigación, permite resguardar el caso de análisis de la evidencia, automatizar las tareas de búsquedas y análisis que requieren mucho tiempo en la investigación, generar informes periciales adecuados con elementos, indicaciones y comentarios relevantes en la investigación que pueden ser presentados en los tribunales judiciales y la exportación del archivo con el análisis forense en formato RTF o HTML.

WONDERSHARE RECOVERIT DATA RECOVERY - RECUVA -DISK DRILL**:** Estas herramientas permiten la recuperación de archivos, fotos, documentos videos, música y audios que han sido eliminados o inaccesibles en un disco duro, en discos duros formateados, en discos extraíbles, particiones de discos pérdidas, en dispositivos electrónicos como tarjetas de memorias, memorias USB, cámaras digitales, grabadoras, papelera de reciclaje entre otros, por medio de un escaneo profundo al iniciar la ejecución de la herramienta por los parámetros seleccionados por el investigador forense para la búsqueda de archivos sin preocuparse por el tiempo requerido porque muestra a los usuarios el progreso del escaneo y el tiempo estimado para obtener el resultado del escaneo. Estas herramientas forenses cuentan versiones gratuitas y comerciales disponibles para Windows 10/8/7/Vista/XP y Mac.

VISORES DE ARCHIVOS – FILESEE- FREE FILE OPENER – FREE OPENER: Herramientas gratuitas o comerciales que permite al analista forense abrir, visualizar y editar diferentes formatos de archivos, tales como imágenes, texto, música, video audio.

X-WAYS FORENSE - IMDISK -OSFMOUNT - FTK IMAGER: Herramientas que permite la clonación y captura de una o varias imágenes de un disco duro, lectura de sistemas de archivos y particiones, archivos sin formatos, imágenes ISO,VHD,VMDK, VDI y VHDX, identificación de particiones pérdidas o eliminadas de los discos automáticamente, recuperación de datos de forma rápida y potente.

AUTOPSY: Considerada como una de las principales herramientas forenses de código abierto, rápida, de fácil uso para analizar cualquier clase de dispositivos móviles y medios digitales[87], sirve de apoyo a las actividades del analista forense para las investigaciones forense ante las autoridades judiciales e investigaciones corporativas. Autopsy permite el análisis de sistemas de archivos y volúmenes de evidencias digitales presentadas en imágenes de un disco o partición con sistemas operativos Windows, Linux, Unix y OS X. Así como también, la generación de informes de los análisis efectuados en la herramienta identificando detalles importantes en la investigación que puede ser exportado en diferentes formatos.

5.4.1.2 Herramientas de Análisis de Registro.

Permite obtener todos los datos relacionados a los registros generados en equipos informáticos que tienen el sistema operativo Windows instalado y cuando se produce la instalación de programas. Estos registros pueden ser: configuración de usuarios del sistema, ruta y permisos de acceso a ficheros, archivos o carpetas, ficheros ejecutados, configuración del sistema, dirección IP de la red, aplicaciones instaladas y en ejecución, entre otros.

Hace parte de la categoría de análisis de registro, las siguientes herramientas:

REGRIPPER – REGISTRY DECODER: Herramientas de código abierto para extraer analizar de la información de los registros, mostrando al final un listado detallado de dicha información.

MUI CACHEVIEW: Herramienta de software que permite al investigador visualizar, examinar y editar todos los elementos relacionados con el MUICache y las aplicaciones que se están ejecutando.

---

[87] Basis Technology. Autopsy Digital Forensic. Autopsy. 2021. [En línea]. [Fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.autopsy.com/about/

REGISTRY RECON: Permite la extracción, la recuperación y análisis de información de los registros del sistema Windows que se han eliminado.

5.4.1.3 Herramientas Análisis de Correo Electrónico.

Los ataques cibernéticos a las organizaciones, gobiernos e individuos como los engaños digitales, las estafas, el robo de datos, la suplantación de identidad, la propagación de códigos maliciosos, los insultos o amenazas generalmente se llevan a cabo a través del envío de correos electrónicos para llegar a las víctimas seleccionados. Es por esto que los analistas forenses deben contar con herramientas especializadas para la búsqueda de evidencias válidas relacionada con la información de correos electrónicos alterados y/o eliminados para obtener los datos originales como fecha de creación, fecha de envío, el remitente original, encabezados entre otros. Pertenece a esta categoría de herramientas:

FTK (FORENSIC TOOLKIT): Herramienta con interfaz de fácil uso para el análisis de correos electrónicos, imágenes forenses, visualización de datos en múltiples formatos, procesamiento de datos más rápido, desencriptado de archivos, recuperación de contraseñas entre otros.

EINDEUTIG**:** Herramienta para el reconocimiento de los formatos de los archivos de correos electrónicos, la extracción y exportación de contenido del correo electrónico investigado a una hoja de cálculo y visualización de archivos adjunto en caso de encontrarlos.

MBOX Viewer PRO: Herramienta para visualizar, buscar y exportar archivos MBOX, permite convertir archivos MBOX a PDF, puede exportar archivos MBOX a archivos PDF con archivos adjuntos, visualización previa de archivos MBOX de forma segura en cualquier plataforma y sin ninguna dependencia del cliente de correo electrónico.

5.4.1.4 Herramientas Forenses de Red**.**

Herramientas utilizadas para encontrar registros de eventos sospechosos en la red, malware, conexiones anómalas en la red e identificación de ataques. Se distingue en esta categoría de herramientas forense de Red:

WIRESHARK: Herramienta de software libre, multiplataforma, para la captura de paquetes de la red, analizador de protocolos utilizados para la conexión que permite la detección de posibles problemas en la transmisión de paquetes, permite

examinar el tráfico de una red viva o capturado en un archivo guardado en un disco mediante una interfaz gráfica[88].

XPLICO: Extrae captura de tráfico de una red, información contenida en aplicaciones, información de correo electrónico, información de llamadas VoIP, contenidos HTTP, entre otros.

TCPDUMP: Herramienta de análisis de tráfico de paquetes de red por línea de comando en Linux y Unix.

5.4.1.5 Herramientas de Análisis de Dispositivos Móviles:

Permite realizar la extracción y análisis detallados a los datos contenidos en un dispositivo móvil y protección de la integridad del dispositivo analizado. A esta categoría de herramienta forense se encuentra:

OXYGEN SUITE FORENSE: Herramienta que extrae, decodifica y analiza datos de dispositivos móviles tales como registro de llamadas mensajería de texto, emails, documentos, contactos entre otros, copias de seguridad, tarjetas de memorias y la nube, así como archivos de sistemas de Windows, linux y Mac Os.

XRY: Diseñada para la recuperación de todo tipo de información que se encuentre en el dispositivo móvil, así como las características de este, viene con un dispositivo para hardware y para software.

5.4.1.6 Herramientas de Adquisición y Análisis de Memoria.

Permite adquirir la información o instrucciones que almacenadas en la memoria RAM para realizar un análisis de ella en busca de evidencia.

RESPONDER CE: Esta herramienta permite capturar la memoria RAM, para su posterior análisis.

VOLATILITY: Herramienta que se encarga de realizar seguimiento a los procesos indicados por el analista forense digital, con el propósito de extraer información útil para realizar el análisis posterior.

[88]Wireshark. About Wireshark. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.wireshark.org/

5.4.1.7 Herramientas de Recuperación de Contraseñas.

Permite al analista forense descifrar las contraseñas para el ingreso correos electrónicos, equipos informáticos, aplicaciones, documentos, sitios web, entre otros, que solicitan contraseñas para su ingreso y de esta forma, extraer la información que sirva de evidencia digital para la investigación. Ejemplo de estas herramientas se encuentran:

NTPWEDIT – NTPASSWP: Editores de contraseña de administrador /usuarios, para los sistemas basados en Windows NT/ Windows 2000, XP, Vista, 7 y 8.

MAIL PASSVIEW: Herramienta de recuperación de contraseñas de cuentas de correos electrónicos.

5.4.1.8 Herramientas de Análisis de Malware.

Permite identificar cuál es el elemento del sistema o de la red que presenta la infección y verificar como se produjo el incidente de seguridad en el sistema.

MICROSOFT PROCESS MONITOR: Esta herramienta permite identificar si se han realizado acciones maliciosas en los registros, en el sistema de archivos o en las conexiones de red.

ESETSYS INSPECTOR: Permite guardar información del estado del sistema antes y después de la ejecución de un código malicioso, para identificar los cambios que se pudieron haber realizado en el sistema.

FIREBUG: Realiza análisis de aplicaciones web, mostrando el código que la compone, identificando de esta forma el código malicioso que haya sido ejecutado sobre ella.

En la siguiente lista se observarán más tipos de herramientas forense en diferentes categorías que pueden ser utilizadas en investigaciones de delitos informáticos:

- Adquisición y Análisis de la Memoria: Hace referencia al conjunto de utilidades que permite la adquisición de la memoria RAM para posteriormente hacer un análisis con ella. En esta categoría se encuentra:
  - FTK Imager: Permite hacer captura y análisis de la memoria RAM
  - Dumpit: Realiza volcados de la memoria RAM y lo convierte a un fichero.

- Pd Proccess Dumper: Disponible para Windows y Linux, permite la conversión de un proceso de la memoria a un fichero.

- Memorize: Realiza un análisis de la memoria RAM para sistemas operativos Windows y OSX ya sea sobre el sistema en vivo o de una imagen del sistema.

- Montaje De Discos: Herramientas de software forenses utilizadas para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla. A continuación, se relaciona las herramientas de este tipo; así :

  - ImDisk: Utilidad de código abierto y gratuito, controlador de disco virtual para montaje de discos duros virtuales, CD y DVD desde los archivos de imagen.

  - OSFMount: Permite el montaje de archivos de imágenes de discos local en Windows asignando una letra de unidad como si fuera un disco físico[89].

  - Raw2VMDK: Utilidad para crear archivos .VMDK desde una imagen de archivos con formato raw/dd

  - FTK Imager: Permite adquirir imágenes de dispositivos de almacenamiento, montaje de discos y conversión de las imágenes extraídas de un formato a otro.

  - Vhdtool: Herramienta de software que permite convertir el formato raw/dd a .vhd para realizar el montaje desde el administrador de discos en Windows.

  - LiveView: Herramienta gráfica forense en java que crea una máquina virtual VMware a partir de una imagen de disco o un disco físico[90] sin procesar para permitirle al investigador forense iniciar la imagen o el disco sin realizar modificaciones.

  - Mount Image Pro: Permite montar archivos de imágenes forenses de diferentes formatos en Windows asignando una letra de unidad[91]

[89] PassMark Software. OSFMount. 2021. [En línea]. [Fecha de consulta: septiembre 2021].Disponible en: https://www.osforensics.com/tools/mount-disk-images.html

[90] SourceForge. Live View. 2013. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: http://liveview.sourceforge.net/

[91] GetData Forensic. About Mount Image Pro.2021. [En línea]. [Fecha de consulta: octubre 2021] Disponible en: https://getdataforensics.com/product/mount-image-pro/

permitiendo todo el acceso del contenido de la imagen al usuario para explorar, abrir y ejecutar programas de Windows y aplicaciones en sistema de archivos montado y la exportación de archivos de forma segura sin cambiar el contenido del archivo de imagen.

- FileDisk: Puede realizar el montaje dinámico de sistemas de archivos en Windows[92] para acceder a los archivos de imágenes como si se trataran de unidades físicas permitiendo así el análisis del contenido en el montaje de solo lectura de la imagen obtenida con herramientas forenses Windows.

- Carving y Herramientas de Disco: En esta categoría se encuentra las herramientas forenses que se utilizan para recuperar información perdida, dañada, borrada o transformada, recuperar particiones y estructuras de discos, buscar patrones y ficheros que presenten un contenido específico tales como: imágenes, vídeos, audios etc..

  - PhotoRec: Software gratuito, multiplataforma para la recuperación de archivos perdidos y/o borrados como documentos imágenes, vídeo, archivos de discos duros, particiones perdidas, archivos en CD- ROM, discos ópticos, memorias de cámaras mediante la búsqueda profunda de datos sin tener en cuenta el sistema de archivos.

  - Scalpel: Software utilizado en la investigación forense para la recuperación de archivos, ficheros o directorios borrados de sistemas operativos Windows y Linux de forma rápida. Es Independiente del sistema de archivos.

  - Bulk_extractor: Permite la recuperación de cualquier tipo de datos desde una imagen, carpeta o ficheros, discos y volcado de memoria.

  - CNWrecovery: Software de investigación de datos que permite la recuperación de archivos, fotos, videos, datos perdidos en sectores corruptos de discos, formateados o discos particionados CD, DVD, cámaras, fotos eliminadas en la memoria y archivos de videos fragmentados creando una imagen de disco que pueda ser tratada como un disco normal para aplicar la recuperación de archivos e incorpora utilidades de Carving en disco duros, Memory Card, dispositivos almacenamiento, USB entre otros que trabajan con sistemas de archivos NTFS, FAT32, MAC, XFS y más.

[92] LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. Madrid, RA-MA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=116.

- Restoration: Herramienta de software utilizada para la recuperación de datos por su simplicidad, facilidad de uso al usuario, velocidad de ejecución y escaneo que incluye lo necesario para restaurar archivos de unidades internas, pendrives USB, Memory Card y demás dispositivos.

- Rstudio: Herramienta de software comercial y multiplataforma para la recuperación de datos de discos locales, discos extraíbles, de cualquier sistema de disco NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS+ (Macintosh), Little y Big Endian en sus distintas variaciones UFS1/UFS2 (FreeBSD/OpenBSD/NetBSD/Solaris) y particiones Ext2/Ext3/Ext4 FS, así como también de máquinas clientes con conexión a una LAN o a Internet.

- WinHEX: Orientado a la recuperación de datos forenses, permite la edición y clonación de discos como la recuperación de particiones.

- Email Forensic Software: Softwares gratuitos o pagos utilizados para el análisis forense de correos electrónicos como Outlook, Google Apps, Exchange Server, O365, IMAP, ICloud, permite la creación de un repositorio de casos y análisis de evidencia, Escaneo OCR, recuperación de datos de correos electrónicos eliminados, búsqueda en varios idiomas, genera vista de valores hash de correos electrónicos y generación de informes completos del análisis detallado en formatos como PDF, Html, CVS, MSG, EML, TIFF, PST. En este tipo de software encontramos a MailXaminer (gratuito) y a MailPro+(comercial) de la empresa SysTools[93], E3: Email (comercial) de paraben, FreeViewer OST Viewer, Free EDB Viewer(gratuito), SQL LDF Viewer, FreeViewer MBOX Viewer, DBX Viewer, Free CDR Viewer.

- Recycle Bin Data Carver: Tipo de herramientas forense para recuperar ficheros eliminados, tales como :

  - Foremost: Permite la recuperación de archivos eliminados en diferentes formatos para el sistema operativo Linux.

  - DMDE: Software para la búsqueda, edición y recuperación de datos en discos[94], compatible con FAT12/16, FAT32, NTFS, Ext2/3/, ReFS, HFS, creación de disco y clones, constructor de RAID, funciona en Windows, DOS, MacOS y Linux e incorpora utilidades de Carving.

[93]SysTools. Email Forensic Software. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.systoolsgroup.com/email-forensics.html

[94] DMDE Software. About DMDE.2020. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://dmde.com/

- Utilidades para el Sistema de Ficheros: Grupo de herramientas de software para realizar análisis de datos y búsqueda de ficheros esenciales en un incidente. Se distinguen las siguientes herramientas:

  - AnalyzeMFT: Herramienta de Python diseñada para el análisis completo de MTF de forma eficiente en un archivo de salida en formato CVS.

  - MFT Extractor: Herramienta utilizada para la extracción de la MFT.

  - INDXParse: Herramienta que analiza los atributos de los registros INDX, recupera información de los slack space de los atributos, extrae nombres y tamaños de archivos e indica la línea de tiempo para los índices y fichero del tipo $I30 que se examinan.

  - Mft2Csv: Colección de herramientas de software que permite el volcado de registros MTF y extracción de datos en la MTF a archivo CSV.

  - MFT_Parser: Herramienta de software que se utiliza para la extracción y análisis de la MFT.

  - Prefetch Parser y Winprefectchview : Herramientas utilizadas para extraer y analizar el directorio prefetch y generar reportes en formato simple como HTML para su verificación.

  - FileAssassin: Se utiliza para eliminar archivos y carpetas sospechosos de malware en los sistemas.

- Análisis de Malware: Software forense que se utiliza para analizar y detectar archivos de comportamiento sospechoso.

  - PDF Tools de Didier Stevens: Analiza y extrae código Javascript sospechoso introducido en un documento PDF.

  - PDFStreamDumper: Herramienta de Windows que se requiere para el análisis de documentos PDF maliciosos.

  - Malpdfobj : Herramienta que genera un JSON que contiene toda la información extraída y decodificada de un PDF malicioso para hacerlo más visible.

  - Proccess explorer: Permite acceso e información de los procesos.

- Capture BAT: Proporciona una visión significativa de operación e interacción de un ejecutable sospechoso o malware en un sistema host. Facilita el monitoreo de la actividad del sistema o de un ejecutable, archivo de sistema, registro y procesos de actividad[95].

- Regshot: Herramienta de código abierto para el análisis de Malware. Permite adquirir snapshot del registro y realiza la comparación de registros para establecer las diferencias[96].

- OllyDbg: Desensamblador y depurador para el análisis de malware en aplicaciones o procesos[97].

- OfficeMalScanner: Herramienta forense para encontrar código malicioso en documentos de Microsoft Office[98].

- Bintext: Permite la extracción de cadena en formato ASCII, UNICODE y string de un ejecutable o fichero sospechoso, revelando evidencia de ofuscación del archivo.[99]

- VirusTotal: Herramienta de servicio de escaneo en línea que realiza el análisis de archivos sospechosos para detectar tipos de malware[100].

- LordPE: Herramienta de software gratuita para realizar volcado de procesos de memoria y ejecutables[101]. Se utiliza para desempaquetar malware.

- IDA Pro: Herramienta para la depuración y manejo de aplicaciones[102]. Desensamblador para el análisis de malware.

- FileInsight: Herramienta que se utiliza para el análisis y detección de virus y malware en sitios web, archivos y descargas sospechosas[103].

---

[95] SIKORSKI Michael y Honing Andrew. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2012. [En línea]. ISBN 1-593272901.

[96] Ibíd. p. 77.

[97] Ibíd. p. 77.

[98] Ibíd. p. 77.

[99] AQUILINA James et al. Malware Forensics: Investigating and Analyzing Malicious Code. 2008. [En línea]. ISBN 978-1-59749-268-3

[100] MALIN Cameron et al. Malware Forensics Field Guide for Windows Systems. Digital Forensics Field Guides. 2012. [En línea]. ISBN 978-1-59749-472-4

[101] AQUILINA James et al. Op. cit, p. 77.

[102]HEX-RAYS. A powerful disassembler and a versatile debugger. 2022. [En línea]. Disponible en https://hex-rays.com/ida-pro/

[103]MCAFEE. FileInsight. 2022. [En línea]. Disponible en: https://www.mcafee.com/enterprise/es-es/downloads/free-tools/fileInsight.html

- Volatility: Framework de herramientas gratuitas multiplataforma para la extracción y análisis avanzado de evidencia digital desde la memoria volátil RAM[104].

- Radare: Framework de línea de comando e interfaz gráfica orientada al uso de ingeniería inversa, forense y hacking.

- Shellcode2exe: Utilidad de Python que puede convertir y compilar Shellcode en archivos ejecutables[105].

- Jsunpack-n: Emulador de la funcionalidad del navegador cuando se visita una URL con el propósito detectar de exploits que tenga como objetivo un navegador y vulnerabilidades en los complementos del navegador.

- Framework Forense: Entorno de trabajo que establece lineamientos estandarizados de conceptos, prácticas, tecnologías y criterios relacionados al análisis forense de evidencias digitales.

  - PTK: Optimiza la generación de hash de archivos, análisis de imagen de archivos. Tiene opciones para indexar duplicados forenses como parámetro de búsqueda para crear una línea de tiempo del sistema de archivos, calcula hashes de archivos, realiza análisis de firmas/encabezados, indexación de palabras claves y coincidencias de firmas[106].

  - SANS SIFT Workstation: Grupo de herramientas forenses y de respuestas a incidentes de código abierto y gratuitas diseñado para realizar análisis forenses digitales detallados en una variedad de entornos[107]. Está orientado a linux.

  - CAINE: Proporciona un entorno Forense completo organizado por módulos de herramientas de software para apoyar al analista forense digital en las fases de la investigación digital.

  - Log2timeline: Framework de código abierto para la creación automática de una línea de tiempo que abarca archivos de registro asociado a la actividad

[104] MALIN Cameron et al. Op. cit, p. 77.
[105] Ibíd. p. 78
[106] Ibíd. p. 78
[107] SANS. SIFT Workstation. 2022. [En línea]. Disponible en: https://sans.org/tools/sift-workstation/

del archivo en el sistema y extracción de marcas de tiempo de otras ubicaciones[108] como actividad del navegador, bases de datos, entre otras.

- OSForensics: Identificador de archivos cuyo contenido no coincide con la extensión del archivo, incorpora un visor de archivos para el análisis del contenido de los archivos, genera y verifica valores hash para archivos o volumen de disco. Asimismo, permite la creación y restauración de archivos de imágenes de unidades del sistema para realizar el análisis forense sin afectar la integridad de la información[109]. Permite la búsqueda, recuperación y restauración de archivos eliminados e imágenes de varios formatos de archivo de imagen. Crea firma forense de unidad de disco duro para preservar la información, estructura de archivos, directorios presentes, atributos del archivo, tamaño y ruta del archivo. Proporciona un visor de línea de tiempo para la identificación de la actividad del sistema tales como fecha de creación de archivos, historial de navegación web, registros y más. Ayuda a descubrir la actividad del navegador web de los usuarios, identifica tendencias y patrones del usuario para acceder a sitios web, uso de unidades USB, redes inalámbricas, inicio de sesión en páginas web, contraseñas, descargas recientes, entre otros[110].

- Plaso: Herramienta de software orientada a la creación automática de super líneas de tiempo para ayudar a los investigadores y analistas a correlacionar gran cantidad de información encontradas en registros y archivos de equipos informáticos[111] que se investigan.

- Digital Forensic Framework DFF: Framework de código abierto con entorno gráfico para el análisis e investigaciones judiciales.

- Análisis del Registro De Windows: Permite la recopilación de datos valiosos de los registros de Windows en una investigación forense tales como las características e información del sistema operativo instalado, cuentas de usuarios, permisos de usuarios, softwares y dispositivos instalados en el sistema operativo, ejecución de archivos, direcciones IP asignadas, atributos de la fecha de creación, modificación y acceso de archivos, documentos y carpetas, dispositivos de almacenamiento conectados, etc ..

[108] ANSON Steve. Applied Incident Response. 2020. [En línea]. Indianápolis. Wiley. ISBN. 978-1-119-56026-5

[109]PASSMARK Software. Drive Imaging. 2022 [En línea] .[Fecha de consulta: marzo, 2022] https://www.osforensics.com/drive-imaging.html

[110]PASSMARK Software. Verify and Match Files. 2022 [En línea] .[Fecha de consulta: marzo, 2022] Disponible en: https://www.osforensics.com/verify-and-match-files.html

[111]Plaso(log2timeline). Welcome to the Plaso Documentation. s.f. [En línea]. Disponible en: https://plaso.readthedocs.io/en/latest/

- RegRipper: Marco de trabajo que ejecuta varios complementos, individual o en grupo para la extracción de datos específicos del Registro del sistema, análisis y traducción de datos necesarios en una investigación forense. RegRipper no es una aplicación de visualización ni aplicación de navegación de la estructura de los registros, sino que analiza datos de valores binarios para mostrar contenidos que no serían visibles en una aplicación de visor[112]. Esta aplicación se puede descargar de forma independiente y además se encuentra disponible en distribuciones de aplicaciones forenses basadas en Linux.

- Windows Registry Recovery WRR: Aplicación de interfaz gráfica que permite al analista forense ver el contenido del archivo de un subárbol del registro del sistema, proporciona información disponible de los componentes de los archivos y búsqueda de indicadores específicos dentro de un archivo específico[113].

- Shellbag Forensics: Permite el análisis de los Shellbag que se han encontrados en los registros de Windows.

- Herramientas De Red: Todo lo relacionado con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, etc.

  - WireShark: Herramienta para realizar la captura de tráfico de red, permite el análisis de paquetes de datos proporcionando información detallada del protocolo que se utiliza para la captura del paquete de datos, realiza búsqueda y filtrado de paquetes de paquetes basado en criterios definidos y visualización de estadísticas. Este software tiene versiones disponibles para Windows, Linux, Mac Os y UNIX.

  - Network Miner: Herramienta de software forense de versión de código abierto y comercial que se utiliza para la extracción de información de paquetes de datos capturados en la red y sniffer pasivo para la red.

  - Netwitness Investigator: Herramienta de software que proporciona información sobre las amenazas a la que verse expuesta el entorno TI

[112] CARVEY Harlan. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. [En línea]. ISBN 978-0-12-803291-6.
[113] Ibíd., p. 80.

analizado para establecer la respuesta correcta de seguridad[114], limitar daño a los usuarios y proteger la información crítica de la organización

- Network Appliance Forensic Toolkit: Grupo de herramientas para realizar el análisis forense de red y seguridad de redes, búsqueda de tráfico anómalo, visualización del funcionamiento y rendimiento de la red, evaluación de riesgos, detención de intentos de explotación de vulnerabilidades de la red, y establecimiento del uso de protocolos y hardware en la red.

- Xplico: Extrae datos específicos de aplicaciones y protocolos contenido en una captura de datos de red (archivo pcap o captura de red en tiempo real). Esta herramienta de código abierto es capaz de extraer información contenida en protocolos como HTTP, POP, IMAP, SIP, TCP y SMTP. Proporciona información detallada de solicitudes de DNS capturadas al utilizar los paquetes de DNS capturados de la red como búsqueda inversa de DNS[115].

- Snort: Herramienta de código abierto para la seguridad de red. Sirve como rastreador de paquetes de datos recibidos y enviados en la red, realiza análisis de tráfico y registro de paquetes en tiempo real y funciona como un sistema completo de prevención de intrusiones en la red[116].

- Splunk: Solución avanzada de analisis de la seguridad y respuesta automatizada que se utiliza para el monitoreo de seguridad, seguridad en la nube, detección avanzada de amenazas, rastreador de vulnerabilidades, auditoria y cumplimiento de seguridad. Asimismo, Splunk establece alcances y causas de incidentes de seguridad, determina la correlación de incidentes y aborda necesidades de seguridad en la infraestructura y equipos de las organizaciones[117].

- AlientVault OSSIM: Sistema de gestión de la seguridad de la información y gestión de eventos (SIEM) de código abierto que proporciona una plataforma unificada para la evaluación de amenazas y vulnerabilidades, detección de intrusos, respuesta a ataques informáticos, descubrimiento e inventarios de activos, monitoreo de comportamiento a entornos físicos y virtuales locales y correlación de eventos en los sistemas informáticos,

---

[114] NETWITNESS. NETWITNESS. 2022. [En línea]. Disponible en: https://www.netwitness.com/en-us/tools/netwitness-platform-demo/

[115] JOHANSEN Gerald. Digital Forensic and Incident Response. 2017. [En línea]. Disponible en: https://search-ebscohostcom.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1562684&lang=es&site=eds-live&scope=site. ISBN. 978-1-78728-868-3

[116] CISCO. ¿Qué es Snort?. 2022. [En línea]. Disponible en: https://www.snort.org/.

[117] SPLUNK. Features. Dive into your security data. 2022. [En línea]. Disponible en : https://www.splunk.com/en_us/cyber-security/forensics-and-investigation.html

gestión de registro, supervisión de la nube de AWS Y AZURE y monitoreo de seguridad de aplicaciones en la nube[118]

- Recuperación De Contraseñas: Herramientas de software para la recuperación de contraseñas, por fuerza bruta, en formularios, en navegadores.

  - NT Password Edit: Editor de contraseña para sistema operativo Windows, Windows 2000, XP, Vista, 7 y 8. Permite cambiar o eliminar las contraseñas de cuentas de sistema local.

  - Ntpasswd: Editor de contraseña para usuarios avanzados que permite cambiar la contraseña en el sistema operativo Windows.

  - Chntpw: Herramienta de línea de comando que sirve para cambiar la configuración del usuario, cambiar contraseñas de usuarios en Windows NT/2000, XP, Vista, 7, 8, 10 y editar la configuración de registro Windows.

  - Pwdump7: Se utiliza para extraer el archivo SAM (Security Account Manager del sistema Windows) en un archivo de texto al que pueden acceder otras aplicaciones.

  - SAMInside / OphCrack / L0phtcrack: Hacen un volcado de los hashes. Herramientas para obtener el fichero SAM y extraer las contraseñas de usuarios del sistema Windows.

- Herramientas de análisis forenses para dispositivos móviles: A continuación, en esta sección se presenta las herramientas de análisis forenses para dispositivos móviles gratuitas y comerciales de gran utilidad y fiabilidad cuando se trata de la extracción de información y recuperación de datos:

  Para dispositivos móviles Android:

  - Android-locdump: Software que permite obtener la geolocalización del dispositivo.

  - Androguard: Herramienta de software para la ingeniera inversa a dispositivos Android. Se utiliza para el análisis de malware en dispositivos móviles Android.

[118] AT&T Business. AlienVault OSSIM. 2022. [En línea]. Disponible en: https://cybersecurity.att.com/products/ossim

- Osaf: Framework para Android para la investigación de malware en aplicaciones Android.

- Santoku: Distribución de Linux orientada al análisis forense de dispositivos móviles.

- XRY : Soluciones físicas y lógicas que proporciona a los investigadores métodos probables para la recuperación de información de dispositivos móviles.

- MOBILedit Forense Express: Software para la gestión del contenido de dispositivos telefónicos, extracción de datos del teléfono móvil, recuperación de datos eliminados y la investigación forense móvil.

Para dispositivos móviles iPhone:

- iPhone Analyzer: Herramienta de software forense para IPhone. Examina la estructura interna de archivos del dispositivo iPhone.

- Tenorshare UltData: Software para la recuperación de archivos de datos de dispositivos iPhone[119].

- iPhone Backup Browser: Extrae ficheros de una copia de seguridad realizada anteriormente.

- iPhone-Dataprotection: Herramienta forense para iOS de código abierto para extraer archivos backup.

- iPBA2: Permite la exploración de backups iOS desde un entorno gráfico.

- Oxygen Forensics Suite: Plataforma de software forense para la extracción, decodificación y análisis de datos avanzado de diversas fuentes digitales como dispositivos móviles, drones, seguridad de dispositivos y servicios en la nube[120]. Como herramienta de software forense para dispositivos móviles proporciona información de los atributos del dispositivo analizado como especificaciones, modelo, marca, datos de la tarjeta SIM, cuentas del usuario propietario del dispositivo, aplicaciones y servicios instalados, contraseñas mediante la extracción y recuperación de datos de tarjeta SIM y medios.

[119] TENORSHARE. Tenorshare UltData. 2022. [En línea]. [Fecha de consulta: marzo de 2022] Disponible en: https://www.tenorshare.net/ads/iphone-data-retrieve.html

[120] OXYGEN FORENSICS. Oxygen Forensic Detective. 2022.[En línea]. [Fecha de consulta: marzo de 2022].Disponible en: https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective

5.5 PRUEBA DE CONCEPTO DE HERRAMIENTAS DE SOFTWARES FORENSES.

Con el objetivo de demostrar la aplicabilidad, agilidad y eficacia de las herramientas forenses en un proceso de investigación de incidentes de seguridad, análisis de delitos informáticos, evaluación para el mejoramiento de la seguridad informática en los procesos de las organizaciones y la realización de tareas específicas, se realizó pruebas con una muestra de 8 herramientas de software forense de funciones específicas como: FTK Imager, Wondershare Recovery, QuickHash, FTK Forensic Tools, MOBILedit Forensic Express, Blade, Wireshark y Autopsy; haciendo uso de distintas con fuentes de datos para la búsqueda, recolección y análisis de evidencia digital para realizar la prueba de conceptos.

Cada vez más las herramientas disponibles para el proceso de análisis forense digital aplicadas en las investigaciones judiciales que implica evidencias informáticas las cuales pueden ser pagas o gratuitas resultan más accesibles para el uso e implementación de tareas específicas de las herramientas de software forense en las organizaciones. Ciertas características y capacidades de soluciones de software utilizadas en el proceso de análisis forense se pueden aplicar a los procesos de diagnósticos y respuestas a incidentes organizacionales como la adquisición de imágenes de disco, recuperación de archivos, visor de imágenes, visores de correos, documentos y archivos por categorías, recuperación de datos de dispositivos móviles, análisis de malware, análisis de red, escanear imágenes de discos y archivos, volcados de memorias, historial web, recuperación de archivos eliminados entre otros; proporcionando así la posibilidad de análisis variados y presentación de información relevante que puede ser exportada bajo algún tipo de extensión.

Pasos previos a la realización de pruebas de concepto:

Para comenzar, se tiene un escenario supuesto de una organización comercial que desea implementar alternativas de herramientas de software forenses gratuitas y pagas en el área TI para investigación y respuesta a incidentes, aplicación de mayor nivel de seguridad informática en la entidad, así como para la protección de datos comerciales y clientes.

El profesional TI de la empresa comercial tiene sospecha que un equipo de cómputo portátil de la organización asignado a un empleado que trabaja de forma remota ha sido atacado, debido a los reportes continuos de incidentes recibidos con el equipo por bajo rendimiento, borrado accidental de archivos, pérdida de información, robo de información en navegación web; por ello es necesario que el profesional TI considere soluciones de software válidas que cubran las situaciones de esta naturaleza, identifique las áreas de riesgos, permita obtener información útil para detectar el incidente, el tipo de ataque, como se produjo el incidente, responsable del incidente, mejor manera de resolver el incidente, recuperar la

operación regular del equipo comprometido en el incidente e informar el impacto del incidente con reportes que incluyan visualización de los procesos realizados.

5.5.1 PoC Adquisición de Imágenes de disco: FTK IMAGER v4.5.03

Para realizar el procedimiento de adquisición de información del disco duro del equipo de cómputo del escenario supuesto, se debe crear una imagen de disco duro, este proceso se realiza sin desconectar el disco duro del equipo. Asimismo, para el almacenamiento de la imagen de disco se requiere de un disco duro externo para transportar la información.

FTK Imager es una herramienta de software forense muy utilizada por los investigadores forenses informáticos expertos para la obtener imágenes de diversas fuentes de datos y visualización previa de datos para evaluar rápidamente la evidencia digital.

Tabla 3. Características de FTK Imager

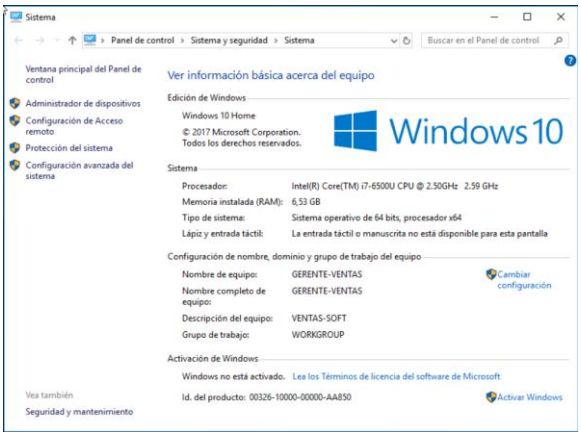
FTK Imager	
Aspectos	**Características**
Versión	4.5.03 Gratuita
Empresa	AccessData
Descargar en:	https://accessdata.com/product-download/ftk-imager-version-4-5
Instalación y ejecución de ftkimager.exe	Desde la computadora local a examinar. Ejecución desde memoria USB.
Funcionalidad	Crear copias de datos informáticos sin alterar la evidencia digital original de discos duros locales, CD/DVD, disquetes, carpetas completas, archivos individuales, discos zip entre otros. Montar una imagen de solo lectura y obtener vista previa del contenido de la imagen forense exactamente igual como lo ve el usuario en la unidad original donde está la información almacenada. Ver y recuperar archivos eliminados. Exportar archivos y carpetas de las imágenes forenses. Crear archivos hash MD5 y SHA-1 para verificar la integridad de la imagen creada. Generar informes hash para archivos e imágenes de disco.

Fuente. Elaboración Propia.

A continuación, se muestra como el profesional TI trabaja con la herramienta forense FTK Imager versión 4.5.03 para realizar la fase de adquisición de información en el proceso de análisis digital forense que le permita identificar el incidente y utiliza un disco duro externo Toshiba 500GB como dispositivo de almacenamiento de la evidencia digital para la cadena de custodia:

- En el escenario supuesto, la fuente de datos para adquirir la evidencia digital y gestionar el incidente se refiere al equipo de cómputo GERENTE-VENTAS que tiene instalado el sistema operativo Windows 10.

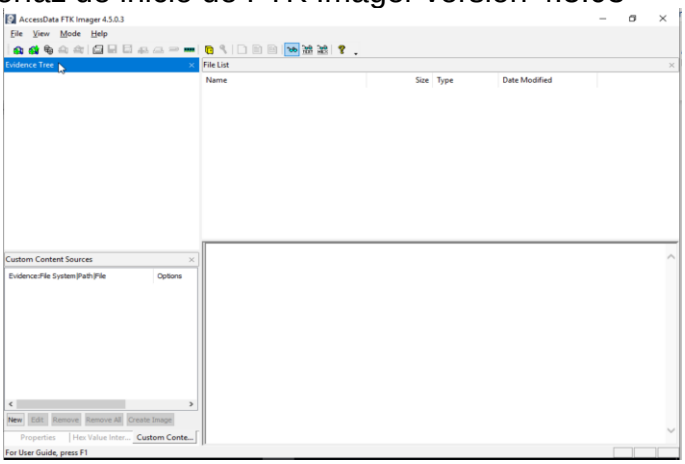
Figura 9. Características de Sistema Operativo Windows para realizar una imagen forense



Fuente. Elaboración Propia.

- Previamente, el archivo ejecutable FTK Imager.exe se instaló en la máquina a examinar y se realiza la ejecución de la herramienta de software forense como administrador.

Figura 10. Interfaz de inicio de FTK Imager versión 4.5.03

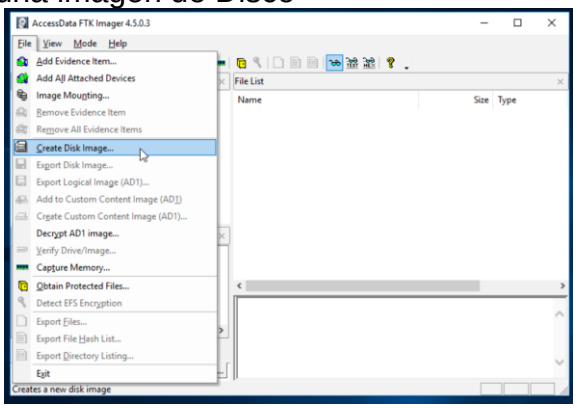


Fuente. Elaboración Propia.

- El profesional informático al iniciar la herramienta FTK Imager, debe seleccionar el menú archivo para encontrar las funciones disponibles relacionadas con el análisis forense como: adicionar evidencia, montaje de una imagen, crear una imagen de disco, capturar memoria, obtener archivos protegidos entre otros.

- Después de identificar la fuente de datos para la extracción de la información, el analista forense digital debe crear una copia de datos informáticos sin alterar la evidencia digital original del disco duros local sin desconectarlo del equipo. Para esto selecciona la opción “Crear Imagen de Disco” o “Create Disk Image”.

Figura 11. Crear una imagen de Disco

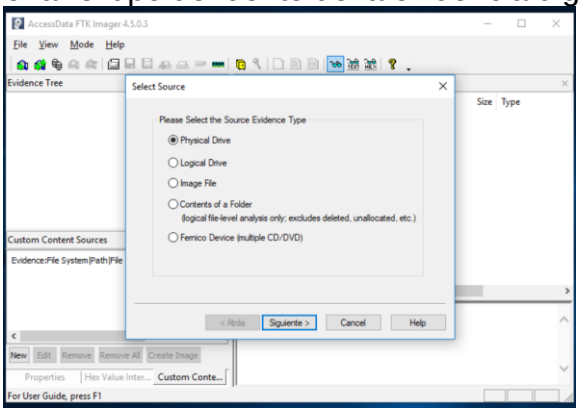


Fuente. Elaboración Propia.

Es importante que el profesional TI utilice un bloqueador de escritura para crear imágenes de disco o de particiones de disco con FTK Imager.

- Seleccionar el tipo de fuente de datos de la que se requiere crear la imagen.

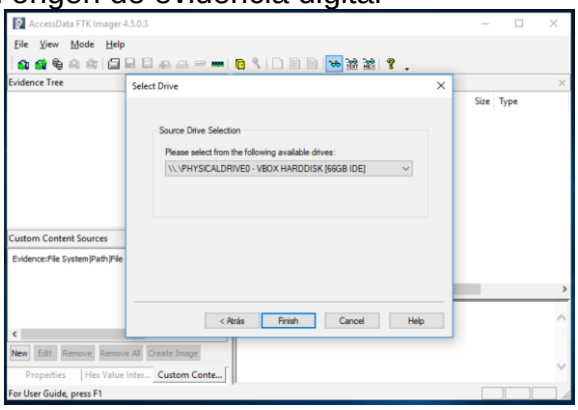
Figura 12. Seleccionar el tipo de fuente de la evidencia digital



Fuente. Elaboración Propia.

- Seleccionar la unidad origen del disco o particiones de disco del dispositivo a analizar para crear la imagen.

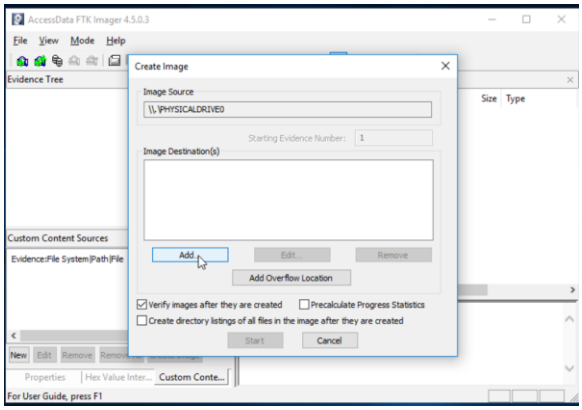
Figura 12. Unidad origen de evidencia digital



Fuente. Elaboración Propia.

- FTK Imager permite la escritura de un archivo de imagen a un solo destino o la escritura simultánea de varias imágenes de archivos a diferentes destinos utilizando la misma fuente de datos o unidad de origen de datos. Finalmente, crear la imagen al hacer clic en el botón Agregar.

Figura 12. Unidad origen de evidencia digital

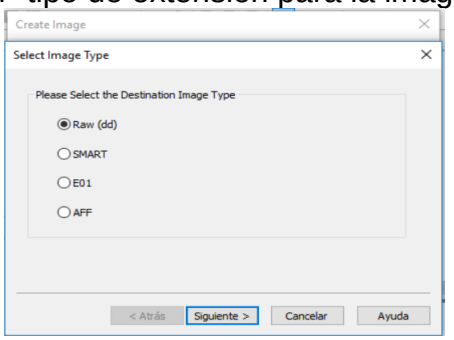


Fuente. Elaboración Propia.

- La herramienta forense FTK Imager permite crear imágenes de varios formatos de extensión tales como, la extensión de archivo Raw (dd) para crear imágenes sin comprimir o puras, la extensión de archivo E01 para crear imagen de disco en el formato de imagen del software EnCase, la extensión

de archivo AFF para una crear imagen de disco en formato forense avanzado requerido en procedimientos judiciales para la captura de evidencia digital y la extensión de archivo SMART para crear imagen en formato para otras herramientas de recuperación de archivos.

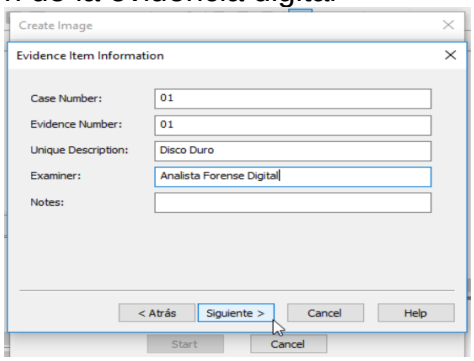
Figura 13. Seleccionar tipo de extensión para la imagen de disco a crear



Fuente. Elaboración Propia.

- En cada investigación, se recomienda al profesional informático diligenciar la información relacionada al caso como el número de caso, número de prueba, descripción del dispositivo, nombre del investigador y observaciones útiles para el tratamiento de la evidencia digital.

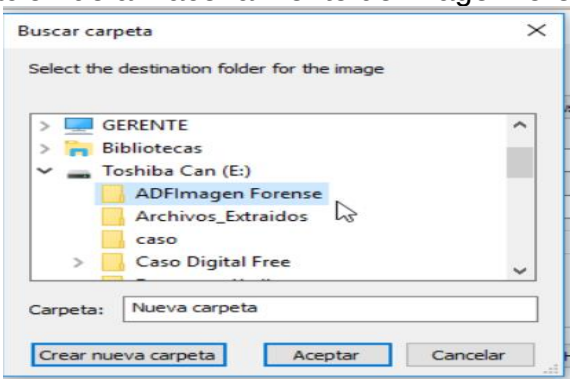
Figura 14. Información de la evidencia digital



Fuente. Elaboración Propia.

- Para almacenar la imagen forense, se debe especificar la ubicación de la carpeta destino de la imagen en una unidad externa con suficiente espacio de almacenamiento.

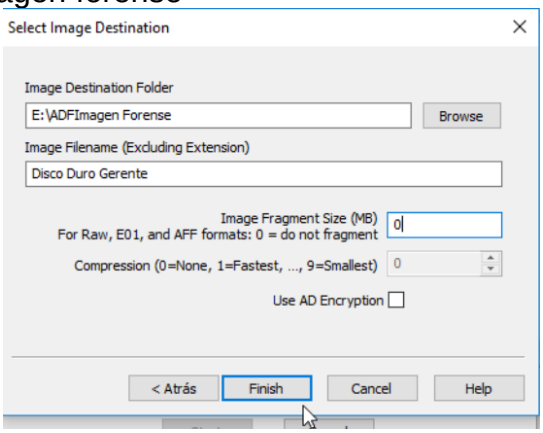
Figura 15. Ubicación de almacenamiento de imagen forense



Fuente. Elaboración Propia.

Así mismo, se debe especificar el tamaño del fragmento de la imagen agregando el tamaño 0 para el formato Raw, E01 y AFF. En el caso de realizar una encriptación de la imagen marcar la opción de encriptación AD para la nueva imagen y agregar una contraseña o certificado.

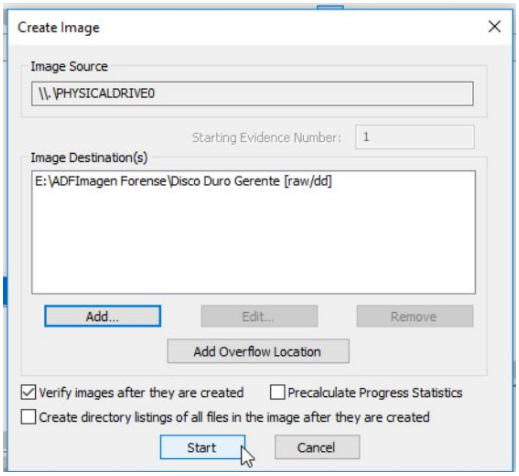
Figura 16. Guardar imagen forense



Fuente. Elaboración Propia.

- En este punto de creación de la imagen con FTK Imager, el analista puede agregar más ubicaciones de almacenamiento destino para realizar el proceso de forma simultánea. Para este caso, el profesional TI solo desea almacenar la imagen de disco con el nombre Disco Duro Gerente en formato raw/dd en la unidad externa E en la carpeta ADFImagenForense.

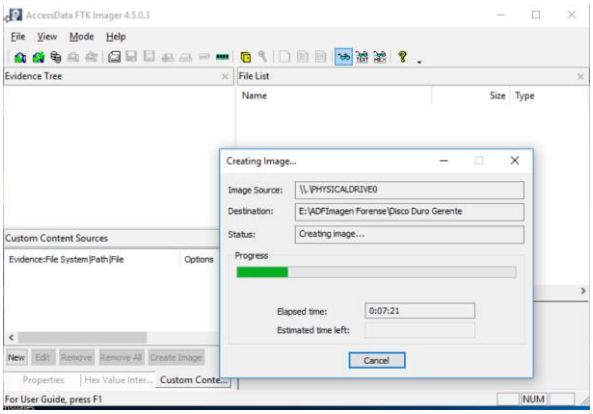
Figura 17. Verificar unidades para guardar la imagen forense



Fuente. Elaboración Propia.

- Al iniciar el proceso de creación de la imagen de disco con FTK Imager, la herramienta brinda al investigador el tiempo estimado de duración del proceso.

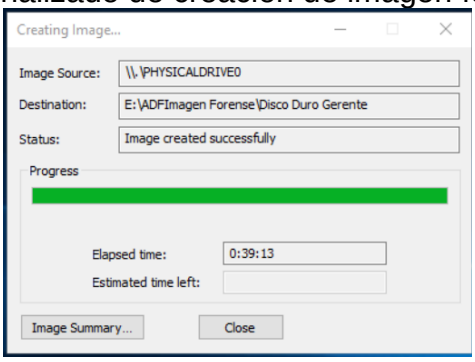
Figura 18. Iniciar proceso de creación de imagen forense



Fuente. Elaboración Propia.

- Una vez finalizado el proceso de crear la imagen, el investigador puede ver el resumen de la imagen.

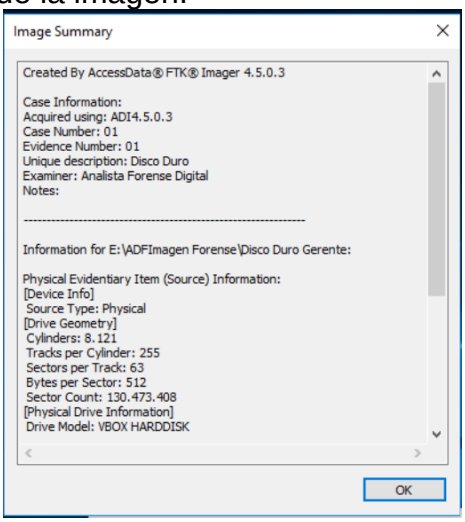
Figura 19. Proceso finalizado de creación de imagen forense .



Fuente: Elaboración Propia.

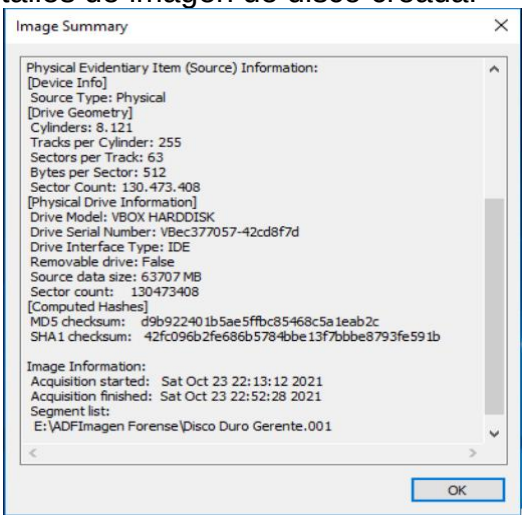
- FTK Imager presenta información detallada que incluye la verificación hash MD5 y SHA-1.

Figura 20. Resumen de la imagen.



Fuente. Elaboración Propia.

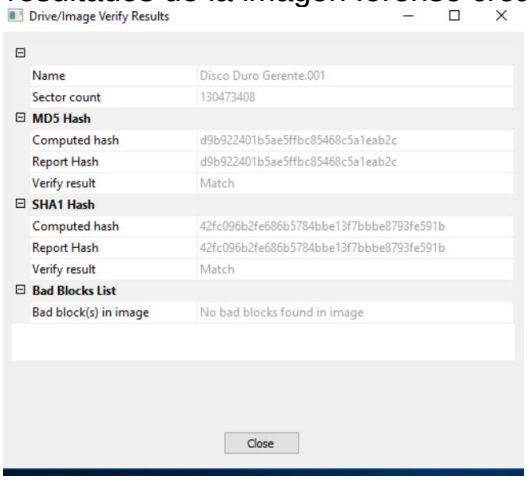
Figura 21. Ver detalles de imagen de disco creada.



Fuente. Elaboración Propia.

- Finalmente, se puede observar el valor hash MD5 Y SHA-1 de la imagen de disco obtenida con FTK Imager.

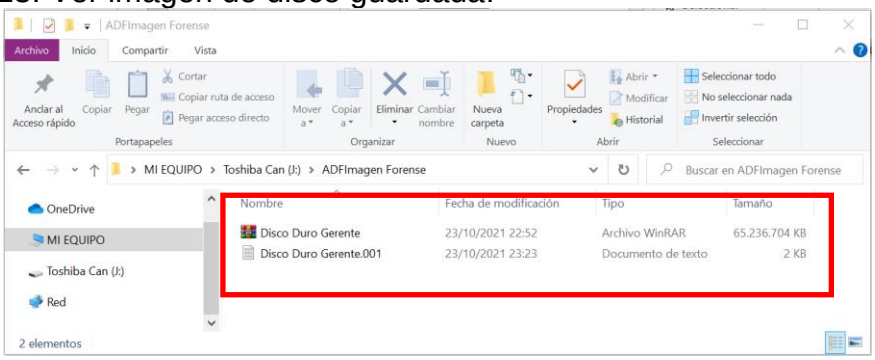
Figura 22. Verificar resultados de la imagen forense creada



Fuente. Elaboración Propia.

- Por último, se verifica la ubicación donde se exportó los archivos y carpetas de la imagen de disco forense que ha sido creada.

Figura 23. Ver imagen de disco guardada.



Fuente. Elaboración Propia.

5.5.2 PoC Análisis Forense Digital para Dispositivos móviles: MOBILedit Forensic Express PRO v7.1.0.16451

Para realizar el análisis forense digital a dispositivos móviles tales como el teléfono móvil, smartphone, Tablet, cámaras fotográficas, Smartwatch o relojes inteligentes, drones, entre otros; el investigador debe conocer las particularidades del dispositivo a examinar como fabricante, modelo, tipo de dispositivo, sistema operativo, versión de sistema operativo, tipo de conectores físicos y lógicos que contiene el dispositivo, mecanismo de seguridad del dispositivo como contraseñas, patrón de desbloqueo, código PIN, huella dactilar, reconocimiento facial, etc..; conocimiento en aplicaciones móviles, recuperación de datos en la nube, programación y procesos para la preservación de integridad de los datos en el dispositivo que permita realizar la extracción de la evidencia digital de forma eficaz.

Aunque existen herramientas de software forense especializadas en dispositivos móviles, muchas veces se presenta dificultad técnica para la recuperación de datos y preservación de la evidencia digital cuando el analista desconoce las funcionalidades adecuadas para gestionar la investigación o no tiene conocimiento especializado en el manejo de la configuración del dispositivo para acceder a la información que contiene.

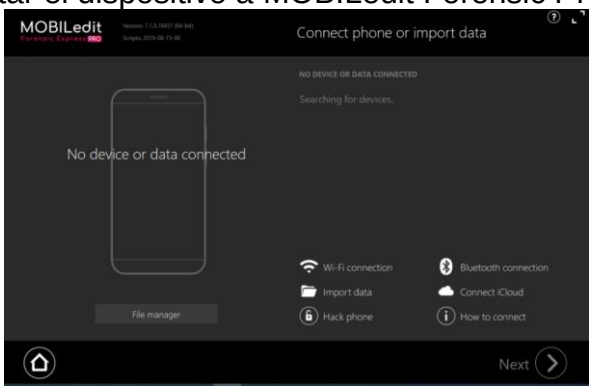
MOBILedit Forensic Express[121] es una herramienta de software forense comercial de la empresa Compelson para dispositivos móviles de función multipropósito para recopilación de evidencia como copias de seguridad, restauración, edición masiva de datos, recuperación de datos, extracción de datos del dispositivo, extracción de datos eliminados como el historial de llamadas, mensajes de texto,

[121] COMPELSON. MOBILedit Forensic Express. All-in-one tool used to gather evidence from phones. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.mobiledit.com/forensic-express

contactos, contraseñas y datos de aplicaciones de red social, fotos, videos, notas, grabaciones de voz , archivos de datos, recordatorios, etc.., analizador de aplicaciones avanzado y generador de informes en formato PDF, XLS o HTML compatibles con otras herramientas de análisis de datos para dispositivos móviles.

- La herramienta MOBILedit Forensic Express Pro en la versión 7.1.0.16451 es compatible con gran variedad de versiones de sistemas operativos Android, iOS y Windows. Para iniciar el uso de la herramienta se debe conectar el dispositivo móvil al equipo de cómputo para la detección automática.

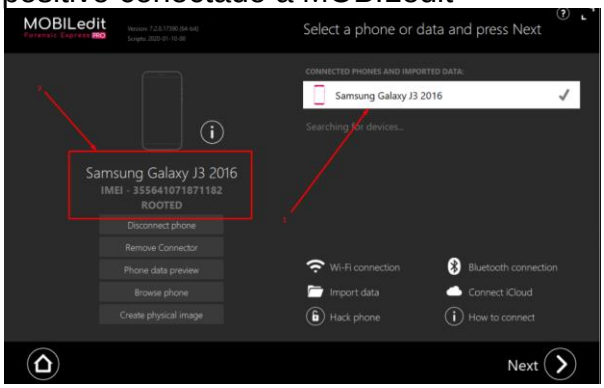
Figura 24. Conectar el dispositivo a MOBILedit Forensic PRO



Fuente. Compelson. Disponible en : https://forensic.manuals.mobiledit.com /MM/Connection-wizard.1806663935.html

- MOBILedit Forensic Express Pro en la versión 7.1.0.16451 ofrece la posibilidad de conectar el dispositivo móvil a través de WI-FI, Bluetooth y cable USB para extraer información. Para este caso, el dispositivo móvil se ha conectado a través de cable USB a la herramienta, detectando automáticamente el modelo del teléfono móvil como Samsung Galaxy J3 2016.

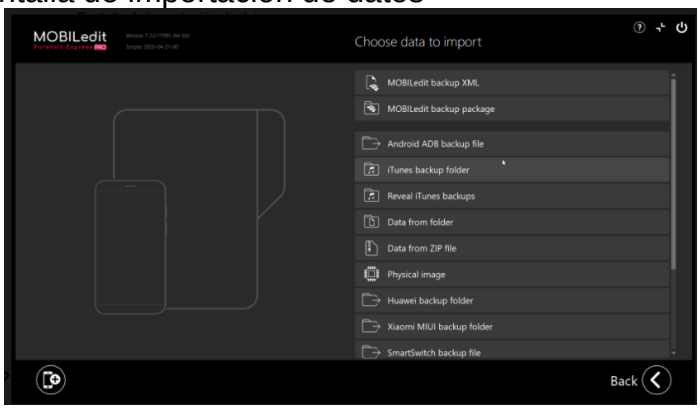
Figura 25. Ver dispositivo conectado a MOBILedit



Fuente. Compelson. Disponible en : https://forensic.manuals.mobiledit.com/MM/ 1821474845/qweqeq.png?inst-v=eb11f669-8c59-4e34-ad25-4caf68fef91e

- MOBILedit Forensic Express Pro permite varias posibilidades de importación de datos, no solo utiliza el teléfono propiamente en sí, sino que puede trabajar con otros archivos ya generados por otras herramientas o archivos extraído de otras maneras.

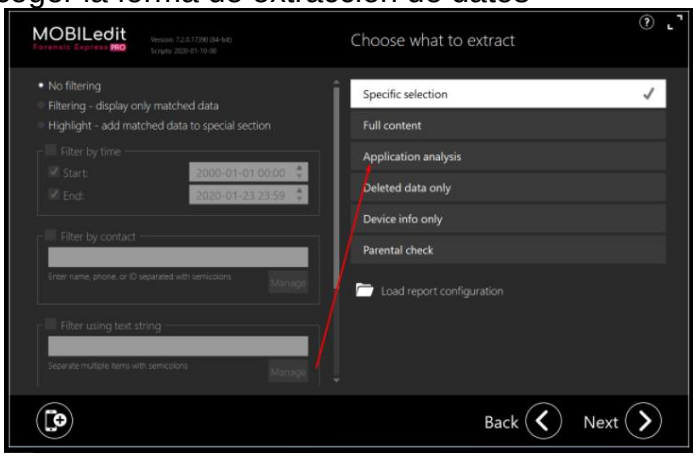
Figura 26. Pantalla de importación de datos



Fuente. Compelson. Disponible en : https://forensic.manuals.mobiledit.com/MM/Import-data.1806467272.html

- Para realizar la extracción de la información del dispositivo móvil, el investigador debe seleccionar la categoría de datos desea obtener a través de la herramienta MOBILedit, como contenido completo, análisis de aplicaciones, datos eliminados únicamente, información del dispositivo, control parental.

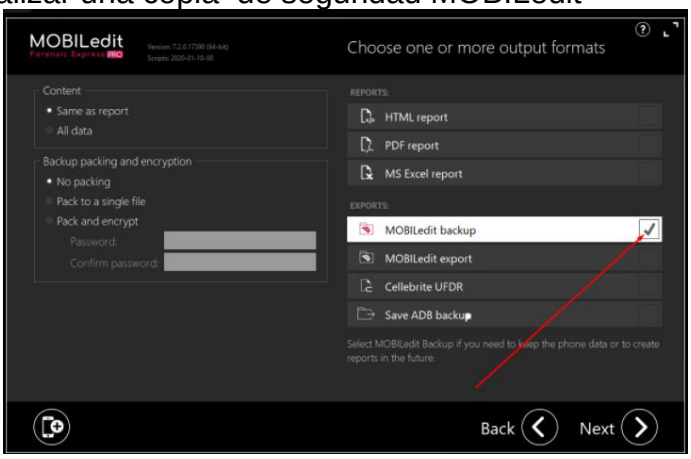
Figura 27. Escoger la forma de extracción de datos



Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/How-to-make-an-application-backup.1821474845.html

- Luego de seleccionar como la información a extraer la opción llamada análisis de aplicaciones, el profesional TI debe realizar una copia de seguridad MOBILedit.

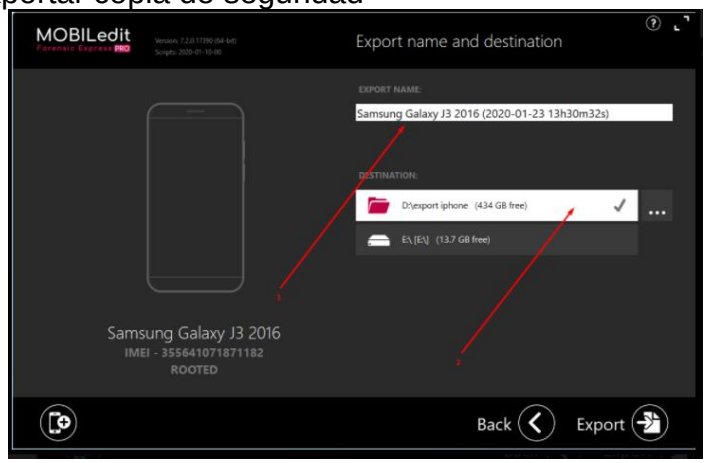
Figura 28. Realizar una copia de seguridad MOBILedit



Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/How-to-make-an-application-backup.1821474845.html

- Ahora, se verá el nombre de la exportación de la carpeta y la ubicación de destino de la carpeta a exportar.

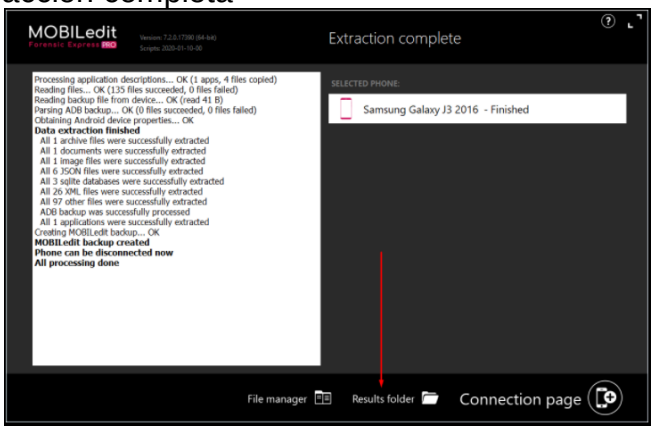
Figura 29. Exportar copia de seguridad



Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/How-to-make-an-application-backup.1821474845.html

- Luego, la herramienta MOBILedit realiza la copia de seguridad a la aplicación seleccionada y se puede ver los datos respaldados.

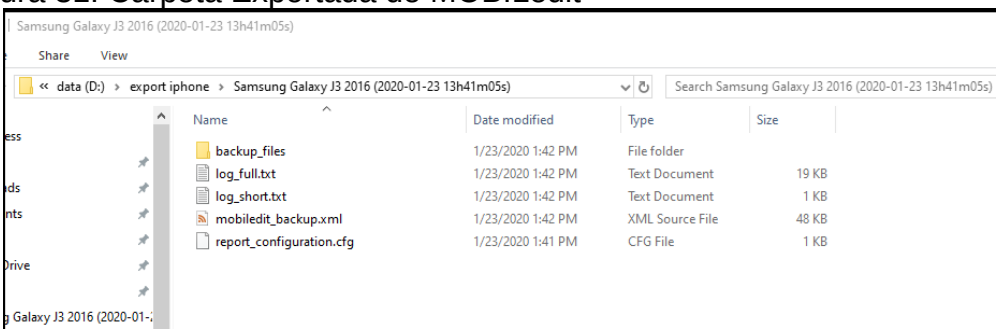
Figura 30. Extracción completa



Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/How-to-make-an-application-backup.1821474845.html

- Finalmente, se obtiene la carpeta de nombre " Samsung Galaxy J3 2016 (2020-01-23 13H41m05s)" en la ruta especificada que contiene las carpetas y archivos que contiene la aplicación analizada.

Figura 31. Carpeta Exportada de MOBILedit



Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/How-to-make-an-application-backup.1821474845.html

- Los reportes forenses generados por MOBILedit Express depende del criterio de selección de los datos analizados, extraídos y filtrados por la herramienta. En la categoría de datos para la presentación de informes se encuentran: capturas de pantalla de configuración del informe, resumen de los datos recopilados, cuentas vinculadas al dispositivo móvil, contactos encontrados, recopilación de mensajes telefónicos, mensajes de aplicaciones, mensajes eliminados, detalles del mensaje, mensajes de correo electrónico, registro de llamadas, audios, datos de aplicaciones, listado de aplicaciones, archivos de imagen, fotos videos, documentos, notificaciones, datos de redes WiFi,

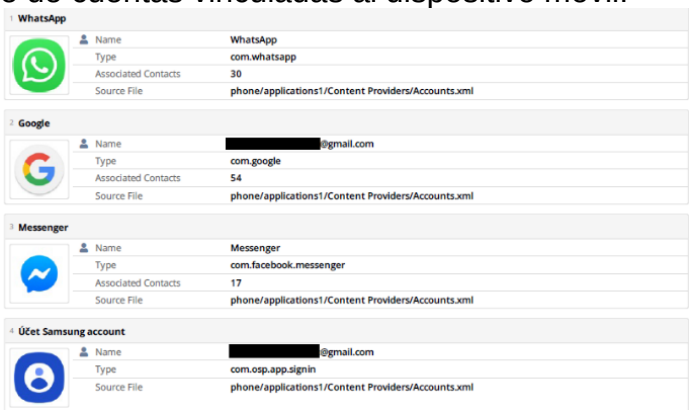
navegación web, contraseñas, ubicación GPS, emparejamiento Bluetooth y más .

Figura 32. Configurar Informe de hallazgos.

Fuente. Compelson. Disponible en : https://forensic.manuals.mobiledit.com/MM/Full-content-vs.-Specific-selection.1809809489.html

En la siguiente figura se observa que las cuentas vinculadas en el dispositivo móvil se encuentra Facebook, Google, Messenger y una cuenta para usuario Samsung.

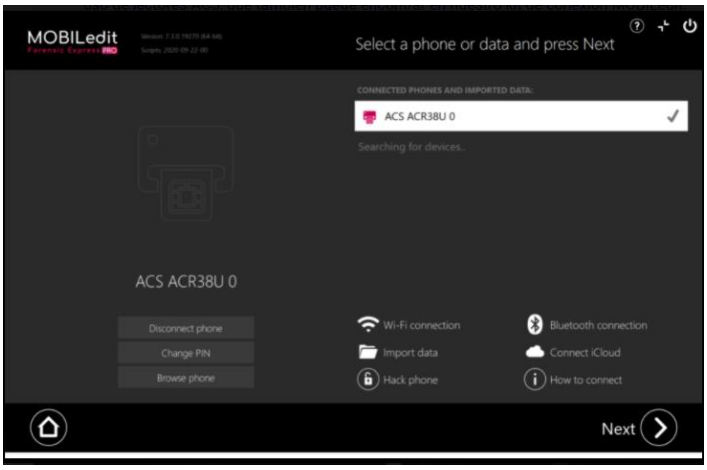
Figura 33. Informe de cuentas vinculadas al dispositivo móvil.



Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/Data---Accounts.1809383545.html

- MOBILedit Forensic Express Pro puede hacer la recuperación de datos con la funcionalidad clonación de tarjetas SIM y crear una tarjeta SIM personalizada a partir de la importación de datos de la SIM Card del teléfono móvil conectado.

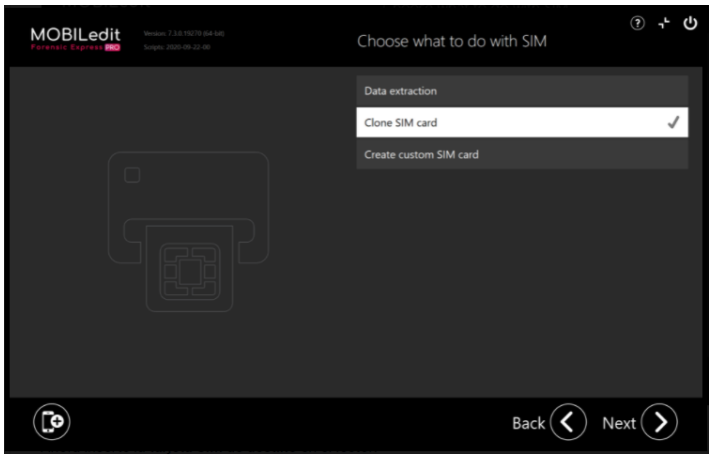
Figura 34. SIM Card Detectada en el dispositivo móvil con MOBILedit.



Fuente. Compelson. Disponible en : https://forensic.manuals.mobiledit.com/MM/Built-in-SIM-Cloning.2176712742.html

- En la herramienta MOBILedit Forensic Express Pro se debe seleccionar la opción Clonación de SIM Card para recuperación de datos desde la SIM Card del dispositivo móvil analizado y esperar que el proceso de clonación termine.

Figura 35. Clonación de SIM Card con MOBILedit.

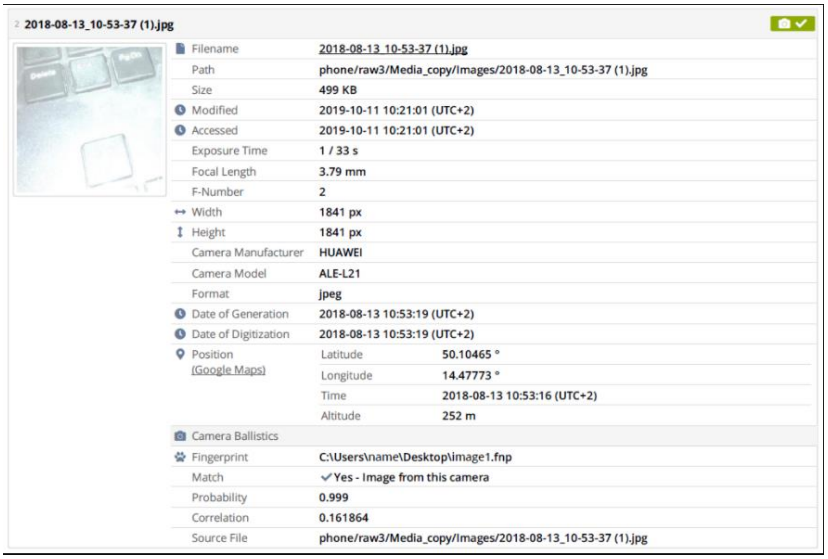


Fuente. Compelson. Disponible en :https://forensic.manuals.mobiledit.com/MM/Built-in-SIM-Cloning.2176712742.html

- MOBILedit Forensic Express posee un complemento de software forense llamado Camera Ballistics que utiliza métodos algorítmicos avanzados como analizador de fotos de cámara para determinar si las fotos extraídas del teléfono móvil fueron tomadas por el dispositivo analizado o no. Con esta herramienta, el investigador obtiene información relevante de las fotos

descargadas, compartidas, recibidas o eliminadas como vista de imágenes, marca, modelo, coordenadas GPS, configuración de la cámara, probabilidad y correlación con de cámara del dispositivo; que puede presentar como evidencia digital mediante un informe PDF generado por la herramienta Camera Ballistics.

Figura 36. Resultado análisis Camera Ballistics de MOBILedit Forense Express.



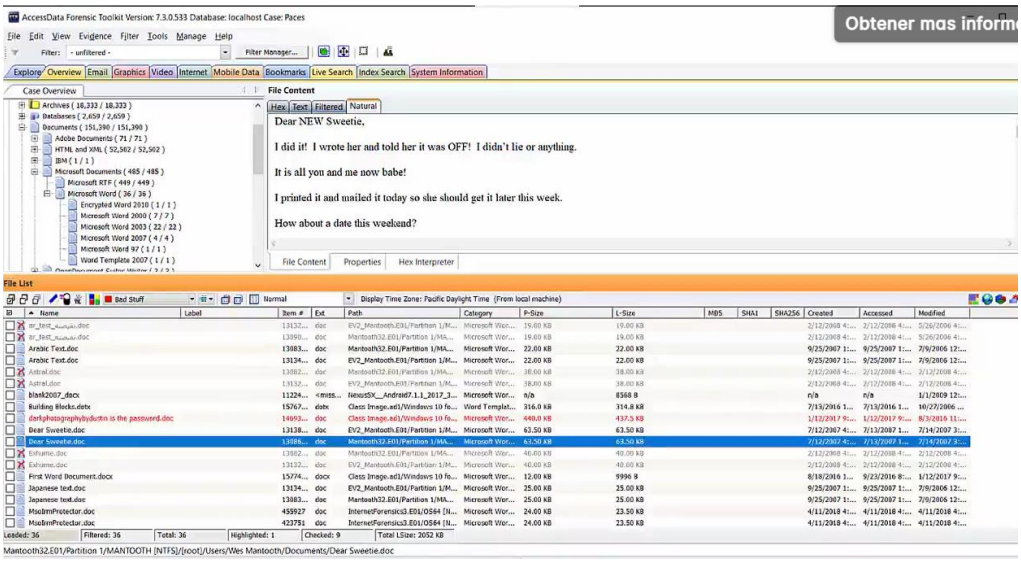
Fuente. Compelson. Disponible en: https://forensic.manuals.mobiledit.com/MM/Camera-Ballistics.1809743974.html

5.5.3 PoC Suite Forense: Forensic ToolKit (FTK)

Herramienta de software comercial de análisis forense digital de la empresa AccessData diseñada para crear imágenes de disco duros, análisis de registro, escanear slack space de fragmentos de archivos, examinar correos electrónicos, reconocimiento de esteganografía, descifrar contraseñas y archivos. La solución de investigación digital FTK tiene gran reconocimiento por la comunidad científica internacional, por las empresas privadas dedicadas a prestar servicios de informática forense, profesionales expertos corporativos y de gran utilidad en los laboratorios forenses digitales de entidades públicas, esto se debe por la facilidad de uso, interfaz intuitiva, velocidad y estabilidad en el procesamiento de la evidencia digital, la visualización de archivos, correos electrónicos, redes sociales en múltiples formatos, con gráficos de clúster, gráficos circulares, geolocalización, cronogramas que ayudan a establecer de relaciones y elementos claves en las investigaciones forenses.

En la siguiente imagen se observa el análisis realizado con Forensics TooolKit FTK versión 7.3.0533. a un archivo de extensión .doc que se encuentra en una imagen forense.

Figura 37. Ver contenido de archivo .doc con FTK Forensic Toolkit.



Fuente. AccessData. Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

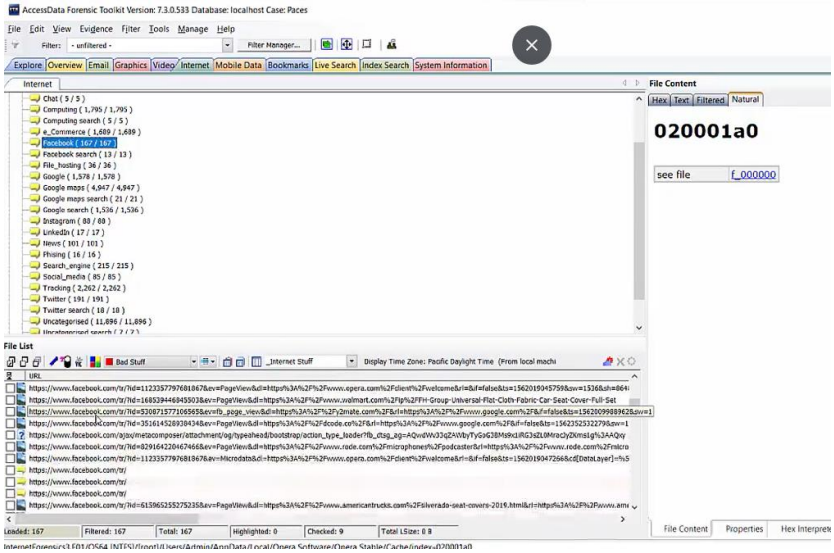
FTK incluye una sección para el análisis de datos forense de dispositivos móviles.

Figura 38. Elementos de análisis de datos móviles.

Fuente. AccessData. Disponible en : https://ad-pdf.s3.amazonaws.com/ftk/7.x/7.3.x/Lab_7_3_RN.pdf

La herramienta FTK examinó y recuperó los archivos que estaban en un disco duro como se muestra en la siguiente figura.

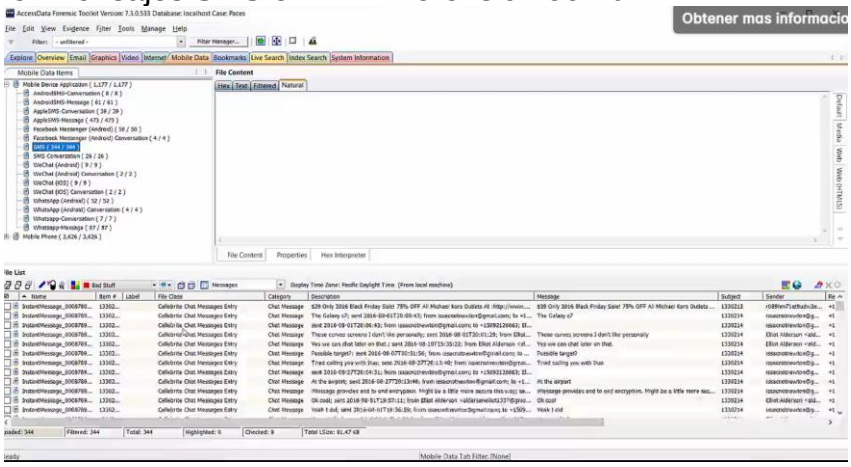
Figura 39. Ver contendido de Facebook con FTK Forensic Toolkit.



Fuente. AccessData. Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

FTK Forensics Toolkit permite localizar, administrar y filtrar datos de mensajes de aplicaciones de dispositivos móviles como SMS, Facebook Messenger, WhatsApp entre otros.

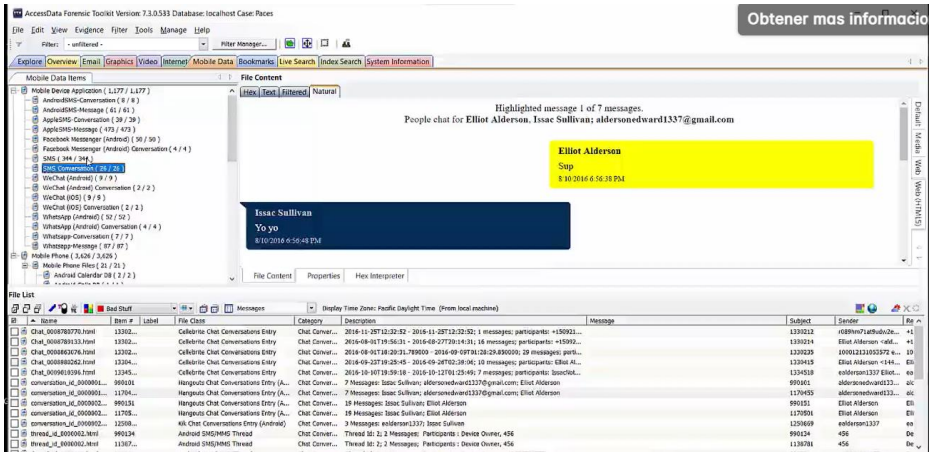
Figura 40. Ver mensajes SMS en FTK Forensic Toolkit.



Fuente. AccessData. Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

Desde el árbol de categorías de datos para dispositivos móviles, FTK permite procesar el contenido de todas de las conversaciones de chat y SMS, así de esta forma, el investigador forense obtiene una fácil lectura de las conversaciones.

Figura 41. Ver contenido de mensajes SMS en FTK Forensic Toolkit



Fuente. AccessData. Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

5.5.4 PoC Recuperación de Datos: Wondershare Recoverit v9.0.2

Toda organización está expuesta a los incidentes de seguridad de la información por la eliminación accidental de archivos importantes, pérdidas de archivos, daños en unidades de almacenamiento de datos, daños en los equipos de cómputos, datos perdidos por particiones eliminados entre otros, por lo que se hace necesario que las empresas puedan contar con una herramienta de software de recuperación de datos potente con funciones forenses. Wondershare Recoverit es una herramienta de software para la recuperación de datos rápida y avanzada que se adapta a todo tipo de organizaciones que cuentan con sistemas operativos Windows y Mac.

Tabla 4. Características Wondershare Recoverit

WONDERSHARE RECOVERIT	
Aspectos	**Características**
Versión	v9.0.2 para Windows. Comercial.
Empresa	Wondershare Technology
Descargar en:	https://recoverit.wondershare.es/buy/business.html
Funciones	Recuperación de datos de disco duro, de unidades USB Externas, de particiones formateadas, de archivos eliminados. Recuperación de fotos, recuperación de audio, recuperación de correo electrónico y otros formatos. Recuperación de la tarjeta SD. Recuperación avanzada de videos, reparación de videos corruptos, truncados o rotos, Acceso a datos de equipos de cómputos averiados desde una unidad USB de arranque.

Fuente. Elaboración Propia.

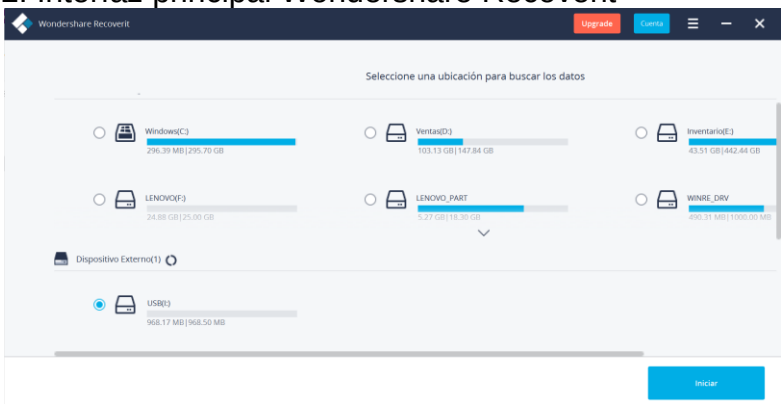
A continuación, se describe los pasos relacionados a la recuperación de datos que debe realizarse a una memoria USB y la recuperación de archivos de una partición de Disco Duro (unidad D) llamado Ventas utilizando la herramienta de

software Wondershare Recoverit versión 9.0.2 en un equipo de cómputo con sistema operativo Windows.

Pasos para la recuperación de datos del escenario propuesto:

- Primero, al iniciar la herramienta Wondershare Recoverit versión 9.0.2 verificar que el tipo de fuentes de datos de la información a recuperar sea detectado por la herramienta.

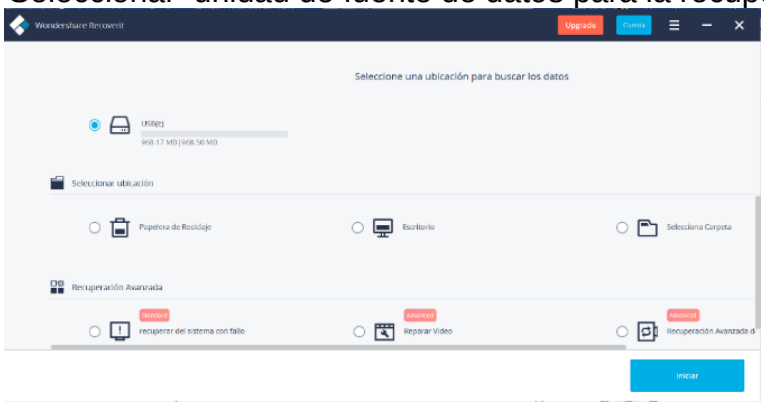
Figura 42. Interfaz principal Wondershare Recoverit



Fuente. Fuente. Elaboración Propia.

- Luego, se selecciona como fuente de datos el dispositivo externo unidad (I) detectado con el nombre USB que se relaciona con la memoria USB para recuperar la información eliminada y dar clic en el botón Iniciar para comenzar el escaneo.

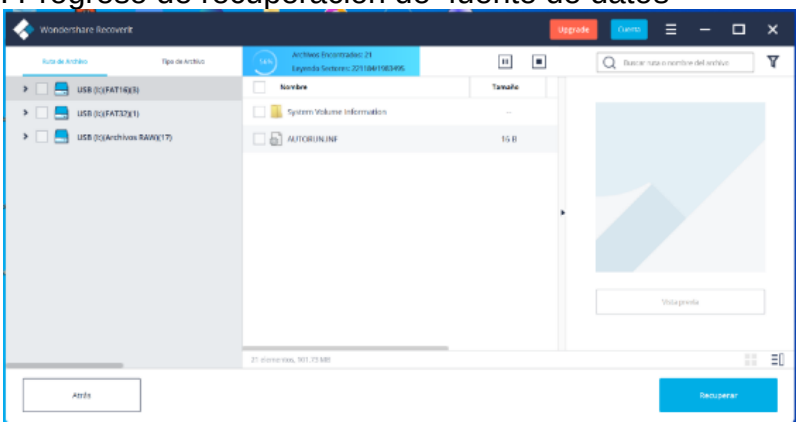
Figura 43. Seleccionar unidad de fuente de datos para la recuperación



Fuente. Fuente. Elaboración Propia.

- En la interfaz se puede observar los resultados del escaneo en tiempo real y se espera que termine el proceso de escaneo automático y vista previa de los archivos en la herramienta Wondershare Recoverit.

Figura 44. Progreso de recuperación de fuente de datos



Fuente. Fuente. Elaboración Propia.

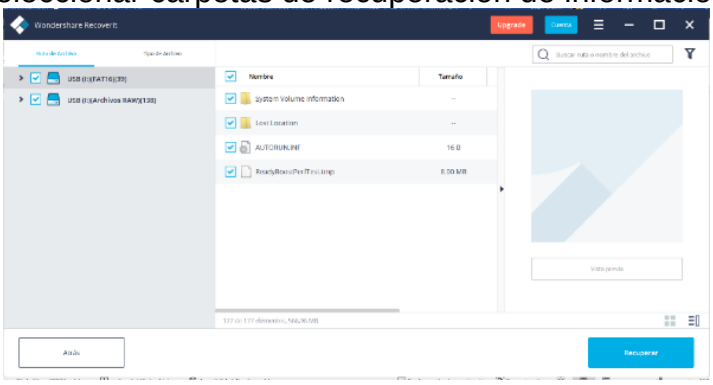
- Cuando el proceso de escaneo termina, Wondershare indica el número de archivos que ha recuperado.

Figura 45. Escaneo finalizado de Wondershare Recoverit

Fuente. Elaboración Propia.

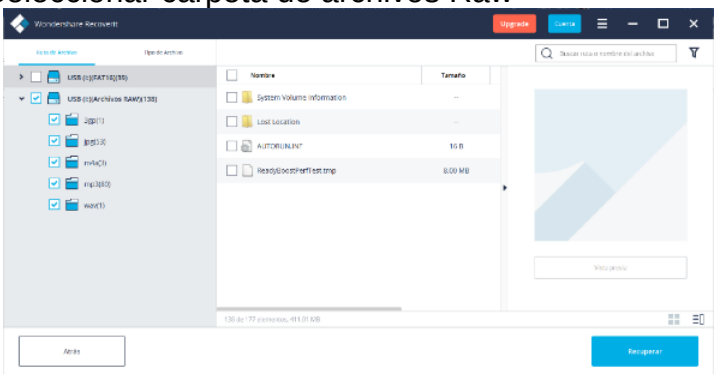
- En este punto, el profesional de seguridad TI puede observar el tipo de información recuperado. Para esto, el investigador debe hacer clic en el archivo que desea visualizar.

Figura 46. Seleccionar carpetas de recuperación de información.



Fuente. Elaboración Propia.

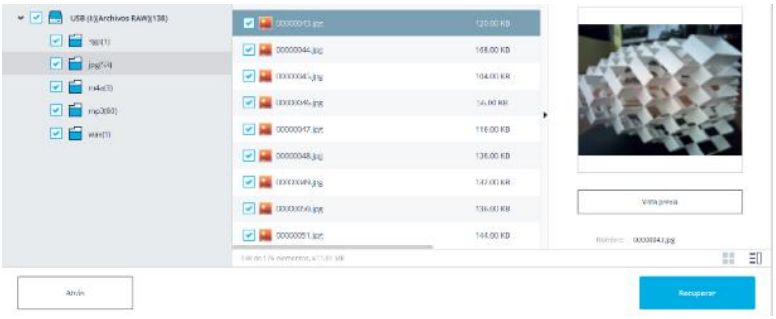
Figura 47. Seleccionar carpeta de archivos Raw



Fuente. Elaboración Propia.

- Wondershare Recoverit muestra en la ventana de previsualización de las fotos información sobre el archivo seleccionado: nombre, tamaño, ruta de ubicación y fecha de modificación.

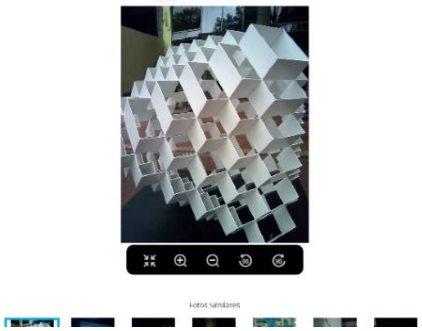
Figura 48. Seleccionar archivo



Fuente. Elaboración Propia.

- Así mismo, Wondershare permite mostrar la foto en pantalla completa, ampliar, alejar o rotar la foto seleccionada. Además, la interfaz muestra al investigador otras fotos similares a la referencia.

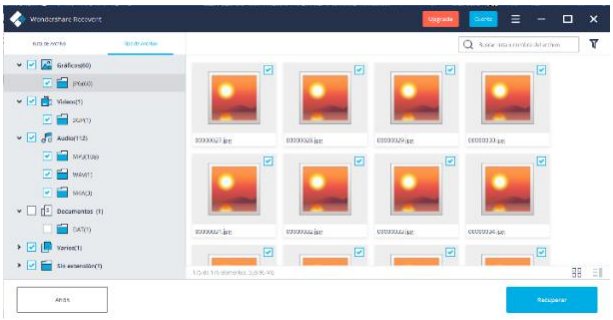
Figura 49. Ver imagen recuperada



Fuente. Elaboración Propia.

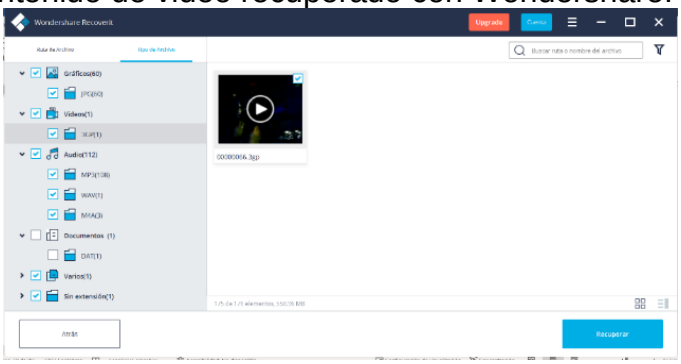
De forma similar, se puede previsualizar otro tipo de archivos como audios, videos, documentos, Pdf, correos electrónicos, archivos sin extensión, archivos comprimidos etc..

Figura 50. Seleccionar archivos para previsualizar.



Fuente. Elaboración Propia.

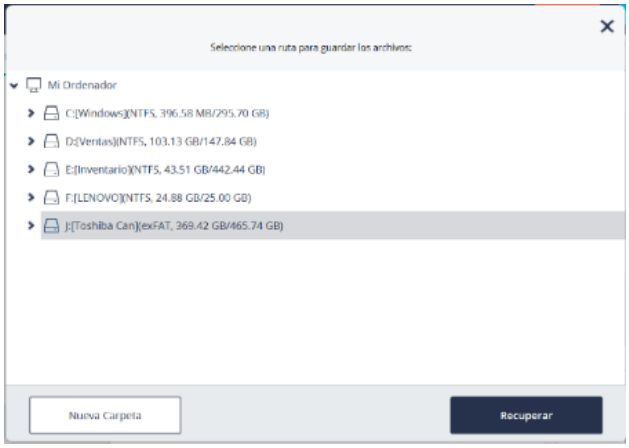
Figura 51. Ver contenido de video recuperado con Wondershare.



Fuente. Elaboración Propia.

- Finalmente, luego de revisar los archivos que se desean recuperar, seleccionar una ubicación de almacenamiento para enviar los archivos recuperados diferente a la unidad donde se ha borrado los datos.

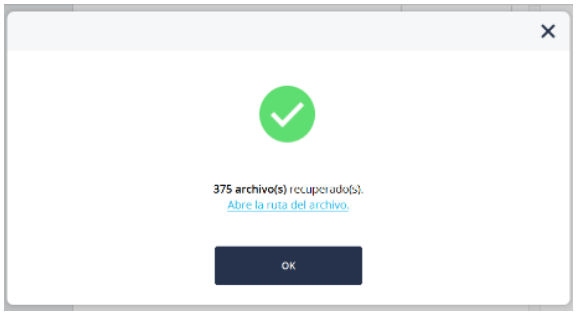
Figura 52. Seleccionar unidad para guardar información recuperada



Fuente. Elaboración Propia.

- Dar clic en el botón Recuperar para finalizar el proceso de recuperación de datos.

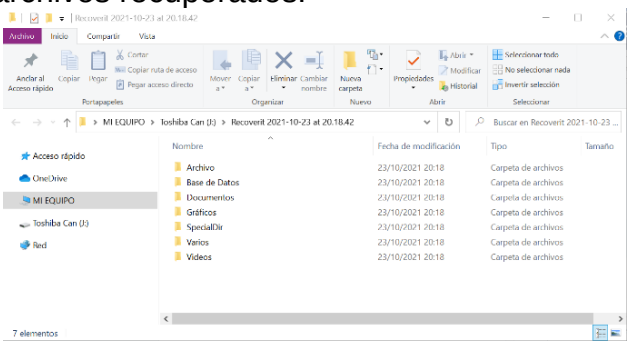
Figura 53. Proceso Finalizado



Fuente. Elaboración Propia.

- Por último, se verifica que los archivos recuperados se encuentren disponibles en la ruta establecida previamente.

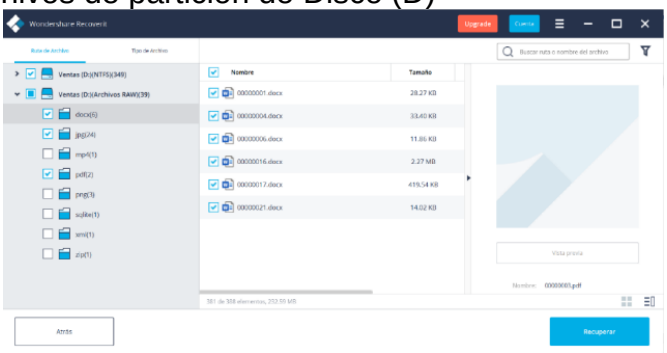
Figura 54. Ver archivos recuperados.



Fuente. Elaboración Propia.

Asimismo, se realizó la recuperación de datos de la partición (D) de un equipo de cómputo del escenario supuesto. A continuación, en las siguientes figuras se muestran los tipos de datos encontrados.

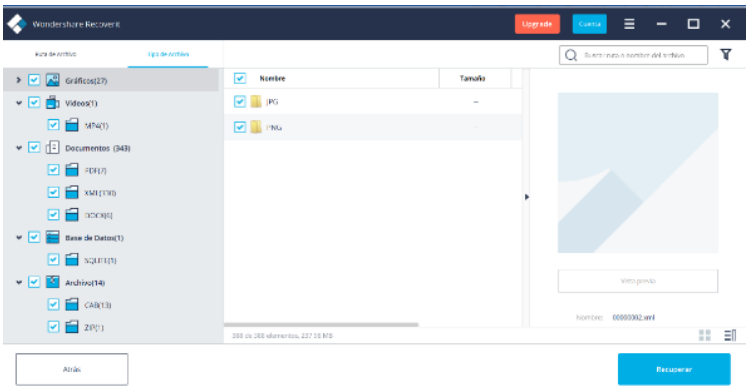
Figura 55. Ver archivos de partición de Disco (D)



Fuente. Elaboración Propia.

En esta imagen se observa los tipos de gráficos JPG e IMA que contiene la partición (D)

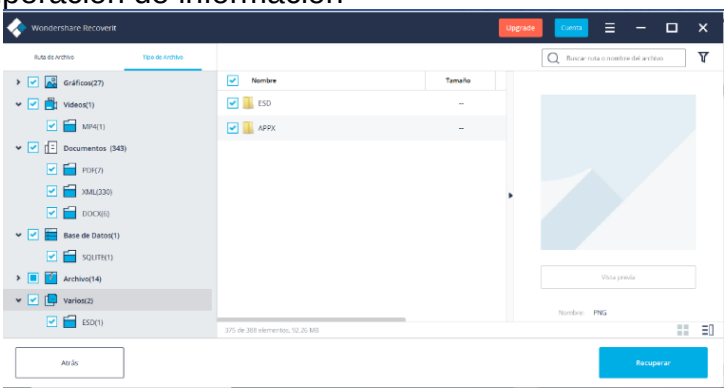
Figura 56. Ver tipo de gráficos recuperados.



Fuente. Elaboración Propia.

De forma similar, se puede observar los tipos de videos, tipos de documentos, tipo de base de datos y otros archivos que contiene la recuperación de datos de la partición (D) VENTAS.

Figura 57. Recuperación de información

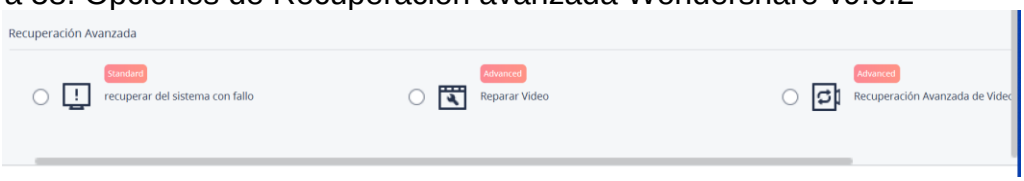


Fuente. Elaboración Propia.

5.5.4.1 Recuperación avanzada con Wondershare Recoverit

La herramienta Wondershare Recoverit ofrece soluciones que permite la recuperación de datos avanzada en un equipo que presenta avería, reparación de un video y la recuperación avanzada de video.

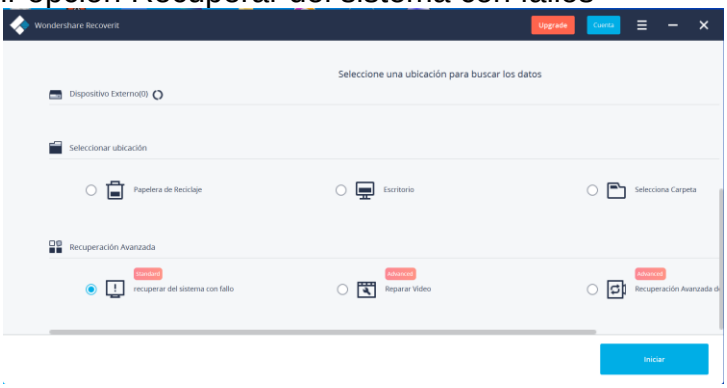
Figura 58. Opciones de Recuperación avanzada Wondershare v9.0.2



Fuente. Elaboración Propia.

Para iniciar la recuperación de datos en un sistema que presenta una falla, en la herramienta Wondershare Recoverit v9.0.2 se debe seleccionar la opción: Recuperar del sistema con fallos y luego dar clic en el botón iniciar.

Figura 59. Elegir opción Recuperar del sistema con fallos



Fuente. Elaboración Propia.

- Después, se debe crear una unidad USB de arranque y hacer clic en el botón Iniciar.

Figura 60. Iniciar creación de USB de arranque.

Fuente. Elaboración Propia.

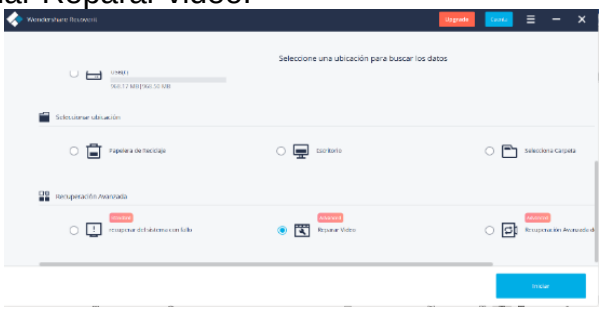
- Luego, se conecta un dispositivo USB al equipo de cómputo que presenta la falla y se inicia la recuperación de datos.

Figura 61. Seleccionar unidad USB de arranque

Fuente. Elaboración Propia.

- La funcionalidad de la recuperación avanzada de video que proporciona la herramienta de software Wondershare Recoverit v9.0.2 resulta una excelente solución cuando en la organización se presenta algún tipo de incidente informático relacionado a la pérdida de archivos de video. Para ejecutar esta función, en la interfaz principal de Wondershare Recoverit, se debe seleccionar la función de recuperación avanzada: Reparar video.

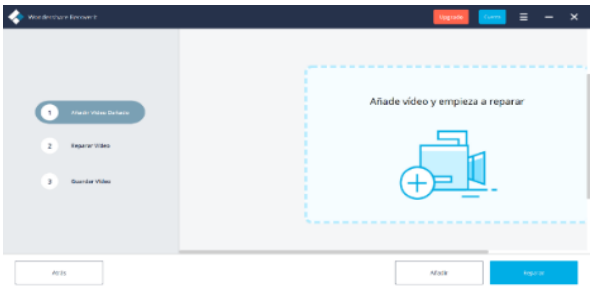
Figura 62. Seleccionar Reparar video.



Fuente. Elaboración Propia.

Cuando se inicie la función, se debe cargar el video o fragmento de video que se desea recuperar.

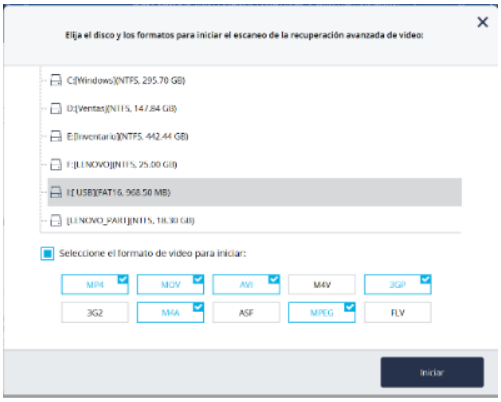
Figura 63. Ver opción Añadir video



Fuente. Elaboración Propia.

Después, el software Wondershare Recoverit indica que se debe elegir una ruta para guardar el video recuperado.

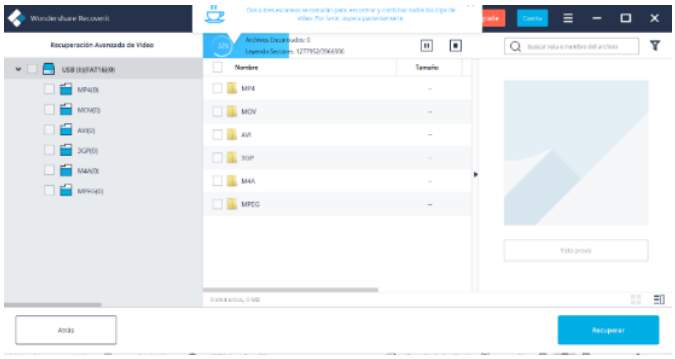
Figura 64. Seleccionar disco y formato de video para iniciar escaneo.



Fuente. Elaboración Propia.

Esperar la recuperación de video avanzada sin interrumpir el escaneo.

Figura 65. Esperar progreso



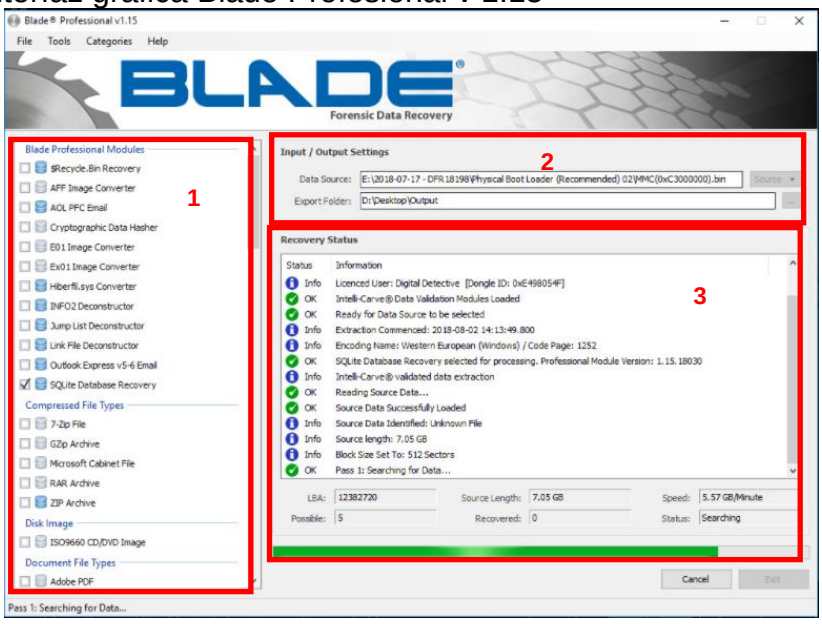
Fuente. Elaboración Propia.

5.5.5 PoC Data Carving: BLADE Profesional v1.15

Blade es una herramienta de software forense digital de tipo comercial que basa en Windows para realizar data carving avanzado en imágenes forenses, discos físicos/lógicos, teléfonos móviles, volcado binario por sectores y la recuperación de datos a la medida, de forma rápida y precisa. Blade utiliza el motor de tecnología Intelli-Carve® en el proceso de recuperación de datos avanzados para garantizar la precisión, estructura e integridad en los datos que recupera.

La solución de software forense Blade Professional v1.15 requiere de la inserción de una licencia de llave USB válida para la instalación en el equipo de cómputo del analista forense. Cuando se ejecuta la herramienta Blade se puede observar que la interfaz gráfica se divide en 3 secciones : la primera sección contiene el módulo de perfiles de recuperación de datos que emplea la tecnología Intelli-Carve®, tipo de archivo para comprimir los datos recuperados, imagen de disco, tipo de archivos de documentos, datos almacenados de correo electrónicos, entre otros; En la segunda sección se indica la ubicación de la fuente de datos origen y la ruta de ubicación de la carpeta para exportar los datos recuperados por la herramienta Blade; la tercera sección muestra al analista forense información sobre el estado del proceso de recuperación y talla de archivos.

Figura 66. Interfaz gráfica Blade Profesional v 1.15



Fuente. Digital Detective Group. Disponible en: https://www.digital-detective.net/product/blade-professional-v1/

La siguiente tabla muestra las características de la versión Blade Profesional v.1.15.

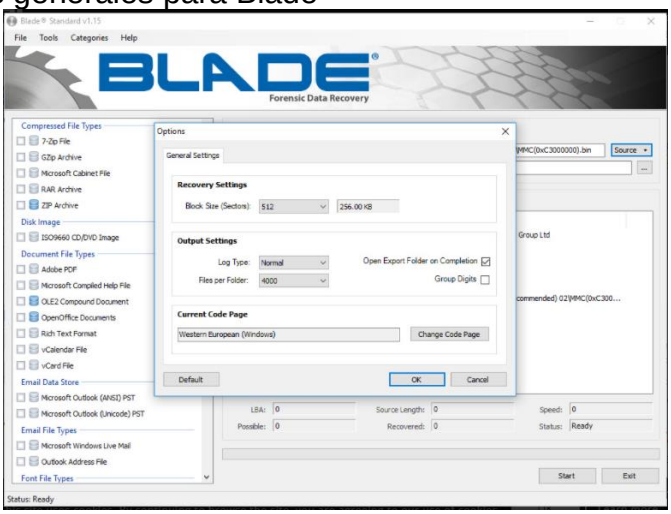
Tabla 5. Características de Blade Profesional

BLADE PROFESIONAL	
Aspectos	**Características**
Versión	Para Windows v1.15 de 64 bits. Comercial.
Empresa	Digital Detective Group
Descargar en:	https://www.digital-detective.net/product/blade-professional-v1/
Instalación y ejecución	Desde una computadora con llave de licencia USB
Funcionalidad	- Admite gran variedad de formatos de imágenes forenses: *.e01, *.ex01, *.001, *.s01, *.aff, *.afd, *.afm, *.vmdk, *.vhd, *.000, *.001, *.dd. *.img,*.ima, *.raw, *.dmp, *.dump, *.crash, *.vmen, *.mdmp, *.bin, *.dat, *.unallocated, *.rec, *.data, *.binary y *.xry. - Recupera registros y archivos eliminados. - Permite la configuración de parámetros de perfiles para la recuperación de datos. - Convertidor de imágenes tipo AFF, E01 y más. - Recupera correos electrónicos de AOL y Outlook Express. - Hash de datos criptográficos. - Recuperación de bases de datos SQLite. - Perfil de recuperación de datos de tecnología Intelli-Carve® como INFO2 Deconstructor, Link File Deconstructor, Convertidor Hiberfil.sys. - Potente búsqueda de expresiones regulares. - Soporte nativo para el procesamiento de dispositivos físicos (discos duros) y dispositivos lógicos. - Volcados de memoria. - Tallar volcado de memoria. - Volcado de datos de teléfono móvil. - Data carving Avanzado con motor de tecnología Intelli-Carve® - Soporte AFF. - Uso de Nuevos perfiles de recuperación de datos para la extracción de tipos de datos como archivos de marcadores HTML, archivos Registry Hive, archivos de texto (UTF-16), archivos vCalender, archivos vCard, archivos de Windows Cabinet y archivos de ayuda compilado Microsoft.

Fuente. Elaboración Propia, basado en documentación de Blade profesional v1.15

Con la herramienta Blade profesional v1.15 los profesionales TI podrán extraer datos que no han sido posible recuperar con otras herramientas forenses tradicionales. Para esto, el analista forense debe seleccionar los ajustes necesarios para la recuperación de los datos, tamaño de sector de recuperación y parámetros de salida.

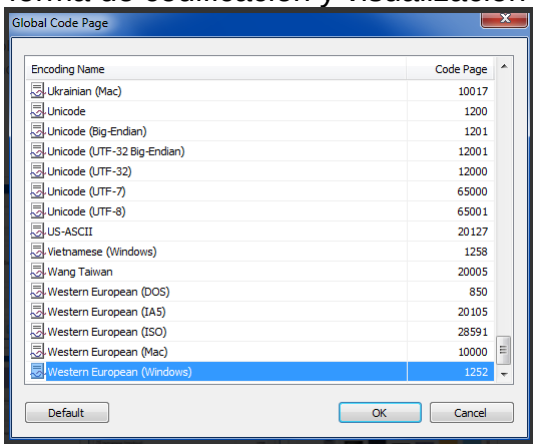
Figura 67. Ajustes generales para Blade



Fuente. Digital Detective Group. Disponible en: https://www.digital-detective.net/product/blade-professional-v1/

En los ajustes generales se incluye como parámetro de salida la selección del nombre de codificación del archivo.

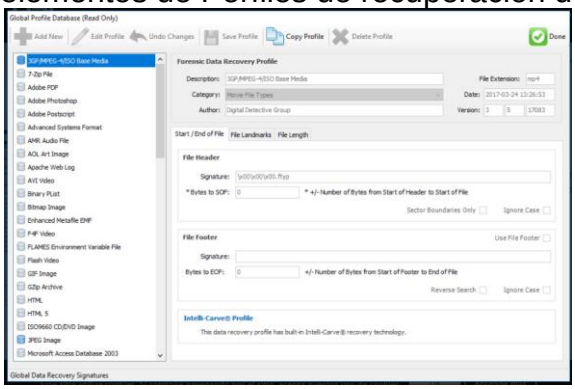
Figura 68. Seleccionar forma de codificación y visualización



Fuente: Digital Detective Group. Disponible en: https://www.digital-detective.net/digital-forensic-software/blade-forensic-data-recovery/

El analista forense puede recuperar los datos con la herramienta Blade a través de perfiles de recuperación globales que se encuentran almacenados en una base de datos que no puede modificar o crear un perfil de recuperación personalizado.

Figura 69. Visualizar elementos de Perfiles de recuperación de datos globales

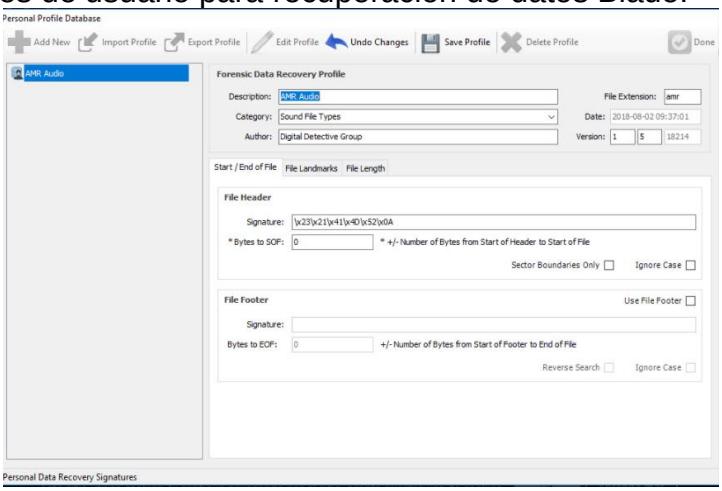


Fuente. Digital Detective Group. Disponible en: https://www.digital-detective.net/product/blade-professional-v1/

En la siguiente figura se observa los elementos para crear un nuevo perfil de recuperación. En el ejemplo se crea un perfil para recuperar archivos de sonido. En el panel de perfil de recuperación de datos forense se ingresa el nombre del perfil, la categoría del archivo para agrupar tipos similares de perfiles de recuperación, el autor, en la figura se utiliza la extensión AMR como el identificador de audio que utilizará Blade para la recuperación de datos. En el campo firma de la sección de encabezado del archivo, se observa la expresión regular de cadena que identifica a ese patrón de bytes al comienzo de un archivo[122] .

[122]Digital Detective Group. Creating Blade Data Recovery profiles. 2014. Disponible en: https://kb.digital-detective.net/display/Blade/Creating+Blade+Data+Recovery+Profiles

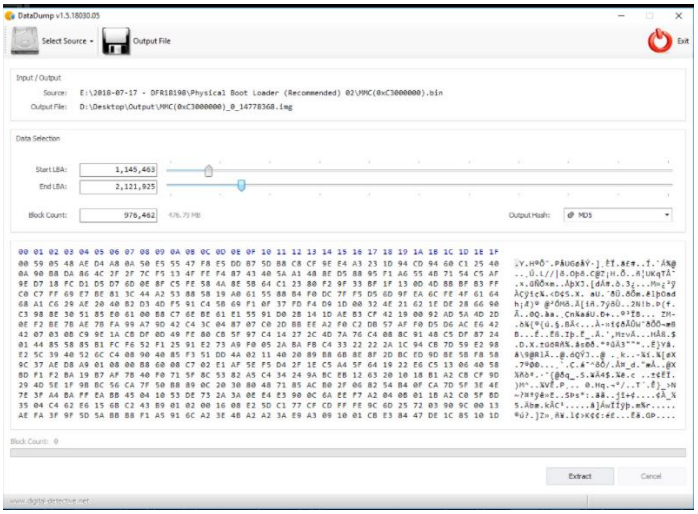
Figura 70. Perfiles de usuario para recuperación de datos Blade.



Fuente. Digital Detective Group. Disponible en: https://www.digital-detective.net/product/blade-professional-v1/

Así mismo, la herramienta forense Blade Professional v1.15 permite realizar el volcado de datos.

Figura 71. Volcado de datos con Blade



Fuente. Digital Detective Group. Disponible en: https://www.digital-detective.net/product/blade-professional-v1/

Blade Professional v1.15 ofrece una gama amplia de funcionalidades para la recuperación avanzada de datos que ayuda a los investigadores forenses a la extracción precisa de evidencia digital.

5.5.6 PoC Función Hash: QuickHash GUI v3.3.0

QuickHash GUI es una herramienta de software open source de función Hash de datos que proporciona una interfaz gráfica de fácil uso que se puede emplear en la investigación forense informática para establecer la integridad de los archivos que se han extraído de un software forense como evidencia digital mediante la realización de hash, permite la comprobación de integridad de archivos al utilizar algoritmos de hash: MD5, SHA1, SHA-3, SHA512, xxHash64, Blake2B y Blake3 y CRC32 y así de esta manera ayuda a mantener la cadena de custodia durante el todo el proceso del tratamiento de la información. Se encuentra disponible para los sistemas operativos Linux, Windows y Mac OSX.

Tabla 6. Características QuickHash GUI

QuickHash GUI	
Aspectos	**Características**
Versión	Para Windows v3.3.0 64 bits. Gratuito. Con licencia GPL2.
Desarrollado por	Ted Smith
Descargar en:	https://www.quickhash-gui.org/downloads/
Instalación y ejecución	- No requiere instalación. - Se puede ejecutar desde unidad USB, disco extraíble o desde una computadora.
Funcionalidad	- Generación de hash para archivos, carpetas, textos. - Comprobación de hash de uno o varios ficheros con varios algoritmos hash. - Verificador de coincidencias de hash. - Comparador de archivos, carpetas, documentos y textos. - Comparación de hash de dos o más carpetas. - Calcular hash a Disco Duro con privilegios de administrador y con el algoritmo SHA-1. - Rapidez para calcular valores hash. - Algoritmo de hash como MD5, SHA-1, SHA256, SHA512, xxHash64, Blake2B, Blake3 y CRC32. - Permite exportar registros en formato CVS, HTML o copiar los resultados en el portapapeles de Windows - Código Abierto - Admite imágenes forenses con extensión E01 (archivo de imagen Encase) - Hash recursivo. - Multiplataforma(Windows, Linux y Apple Mac OSX) - Interfaz de fácil uso, muy intuitiva.

Fuente. Elaboración Propia, basado en manual de usuario QuickHash GUI v3.3.0.

La interfaz inicial de QuickHash GUI v3.3.0 proporciona al profesional informático pestañas para realizar el cálculo de un hash y la comprobación de valores de hash a través de la selección de algoritmos de hash criptográficos que se requiere para mantener la integridad de la información analizada. La pestaña TEXT permite calcular el valor hash a fragmentos de textos, párrafos, cadenas de caracteres, lista de valores, datos de clave pública que se pueden copiar en el cuadro de texto disponible. De igual manera, el analista informático dispone en esta pestaña de opciones como:

- El campo llamado VALOR DE HASH ESPERADO, que le permite comparar el hash del segmento de texto que ingresa contra un valor hash existente.

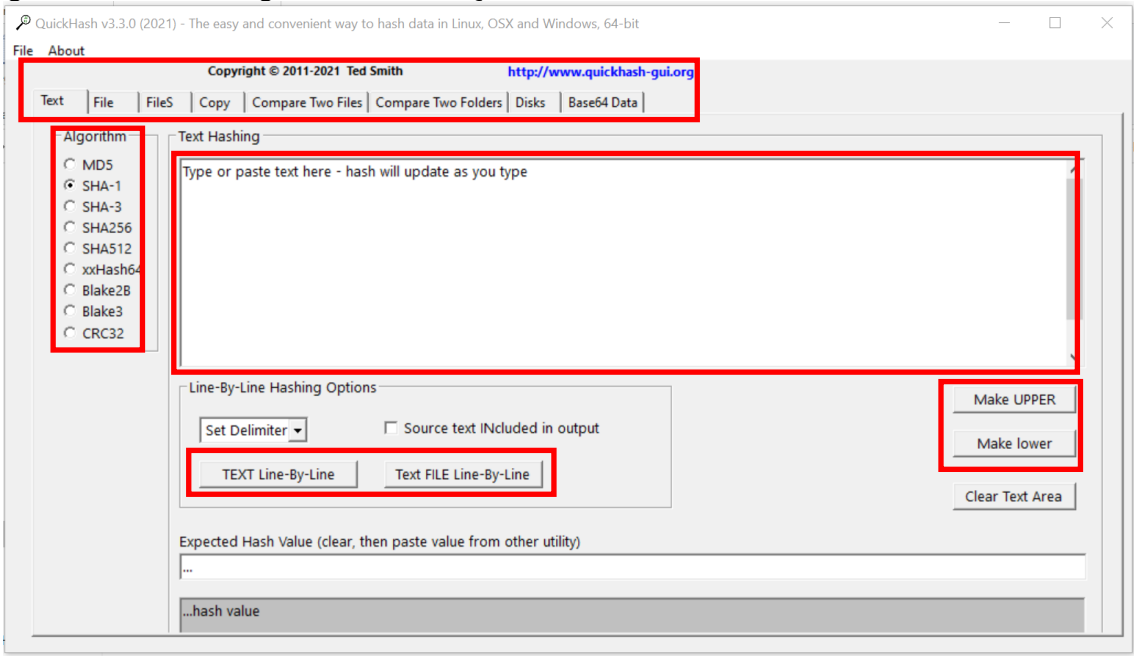
- El botón Hash línea por línea cuando se requiere calcular valores hash a un listado de direcciones de correo electrónicos.

- El botón Archivo de Texto línea por línea para abrir un archivo de texto grande y calcular el valor hash línea por línea del archivo.

- La casilla verificación para incluir o excluir datos del texto origen para calcular el archivo hash de salida.

- Botones de conversión del texto que se ingresa a mayúsculas y minúsculas.

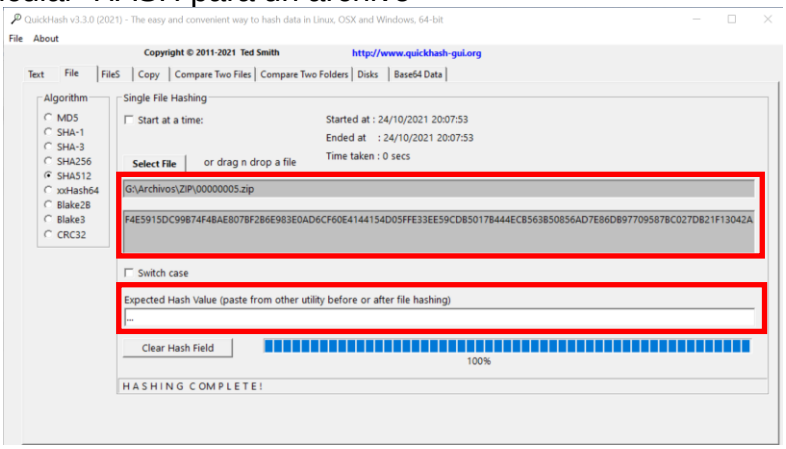
Figura 72. Interfaz gráfica Inicial Quick Hash



Fuente. Elaboración Propia.

La pestaña FILE se utiliza cuando se requiere aplicar un hash a un archivo individual o a imágenes forenses. También incluye un indicador de progreso de cálculo de hash y el campo VALOR ESPERADO para realizar la comparación del hash generado por QuickHash y el hash ingresado archivo proporcionado por el usuario. Esta opción es útil para el especialista forense digital cuando tiene que calcular el hash de fragmentos individuales de una imagen forense o requiere la comprobación de un fragmento en particular de la imagen que no se ha copiado o movido desde una copia maestra.

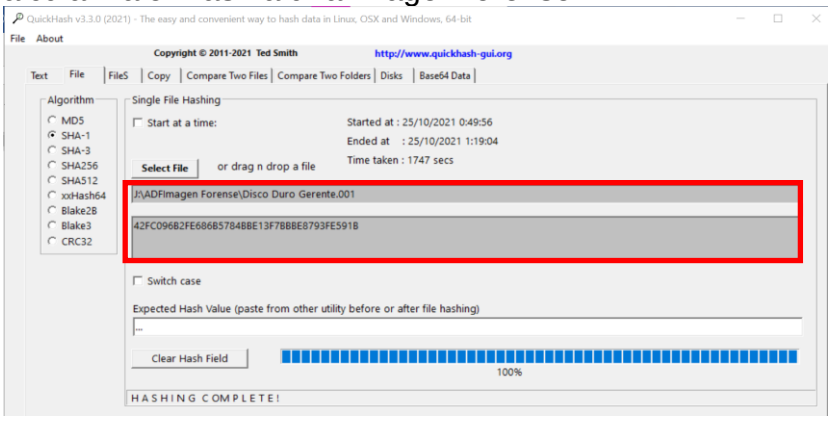
Figura 73. Calcular HASH para un archivo



Fuente. Elaboración Propia.

Desde la pestaña FILE se puede calcular el valor hash de una imagen forense de cualquier extensión. La siguiente imagen muestra cómo se genera un hash SHA-1 a la imagen forense que se extrajo del disco duro de un equipo de cómputo del escenario supuesto de una organización comercial.

Figura 74. Calcular valor hash a una imagen forense.

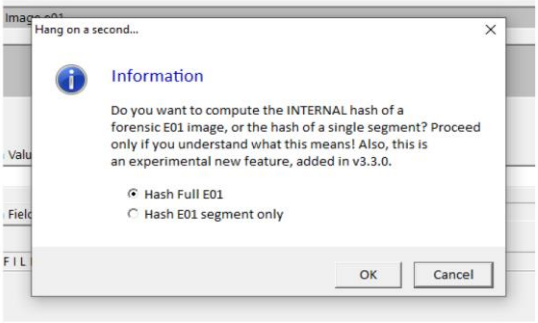


Fuente. Elaboración Propia.

Cuando un especialista forense digital necesita calcular el hash de un archivo de imagen forense de extensión E01(extensión utilizada por el software encase para

archivos de imagen), utiliza la pestaña “FILE”, selecciona el tipo de hash a realizar: completo o por segmento y aceptar.

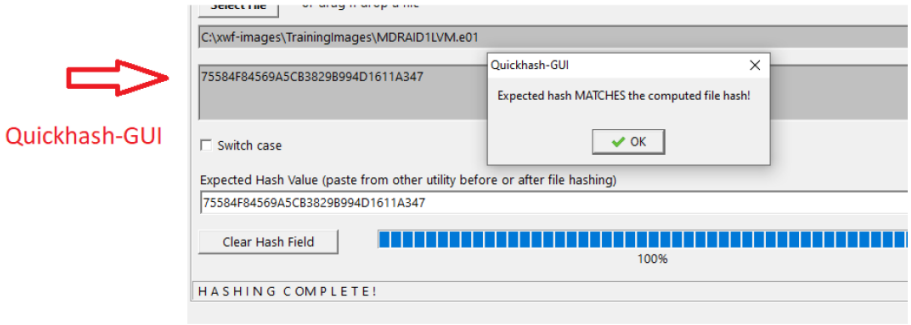
Figura 75. Ventana que se muestra al seleccionar archivo de imagen .E01



Fuente. QuickHash. User Manual. 2020. Disponible en : https://www.quickhash-gui.org/download/user-manual/

La versión QuickHash v3.3.0 permite seleccionar un archivo dentro de una imagen forense de extensión .E01 y aplicar un hash a los datos internos o segmentos de imagen que se seleccionaron.

Figura 76. Aplicar hash a datos internos de imagen .E01

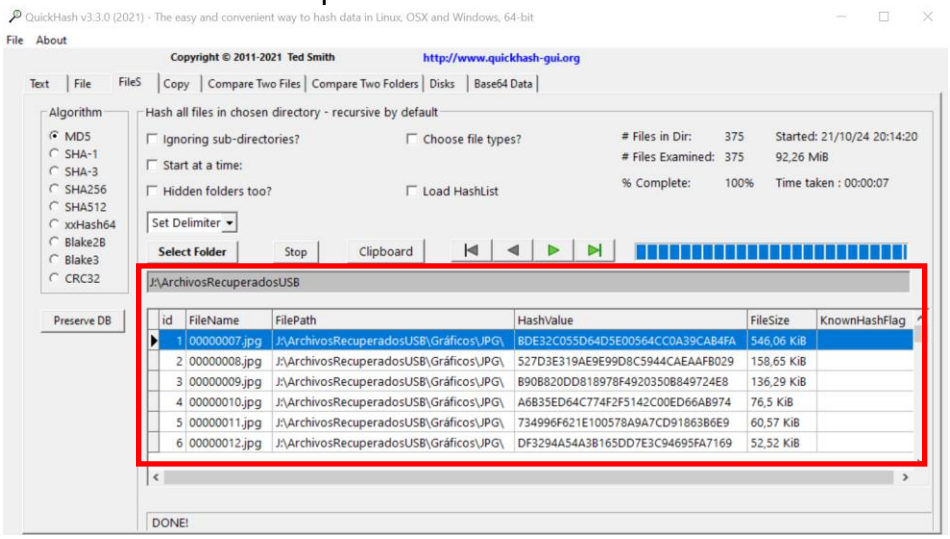


Fuente. QuickHash. User Manual. 2020. Disponible en : https://www.quickhash-gui.org/download/user-manual/

En la pestaña de navegación FILES se puede calcular los valores hash de todos archivos que se encuentran en una carpeta o directorio con opciones recursivas descritas en las casillas: ¿Ignorar subdirectorios?, para calcular hash de archivos en la raíz del directorio que se elige; ¿Las carpetas ocultas también?, para aplicar hash a los archivos que encuentre en carpetas ocultas; ¿Seleccionar tipos de archivos? ; la casilla Cargar un listado Hash permite importar una lista de valores hash existente en la última columna de la visualización de cuadrícula para realizar la comparación entre el listado hash ingresado por el usuario y los hashes generados por QuickHash v3.3.0. Cuando esta casilla no se encuentra habilitada

para calcular hash a los archivos seleccionados, la última columna de la cuadrícula de visualización se presentará vacía, tal como sucede en la siguiente figura.

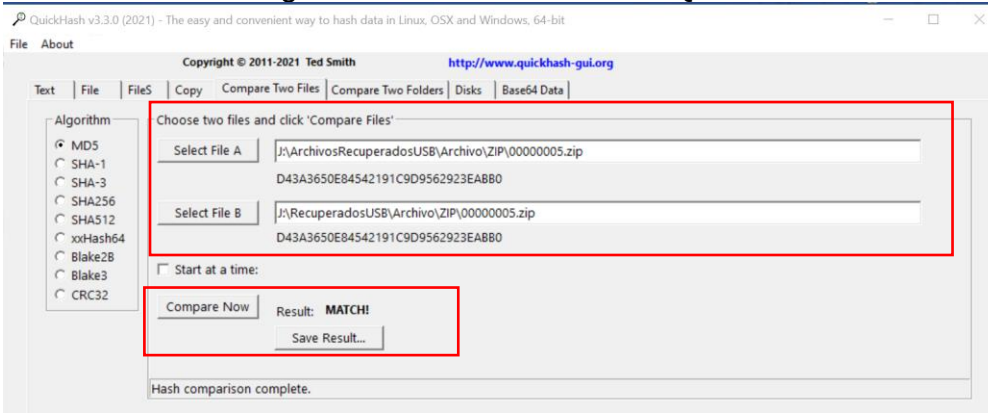
Figura 77. Calcular Hash a carpeta de archivos



Fuente. Elaboración Propia.

QuickHash GUI V3.3.0 en la pestaña COMPARE TWO FILES, permite al profesional informático comprobar la integridad de dos archivos de forma automática. Los resultados de comparación de los archivos se pueden guardar en un archivo de texto.

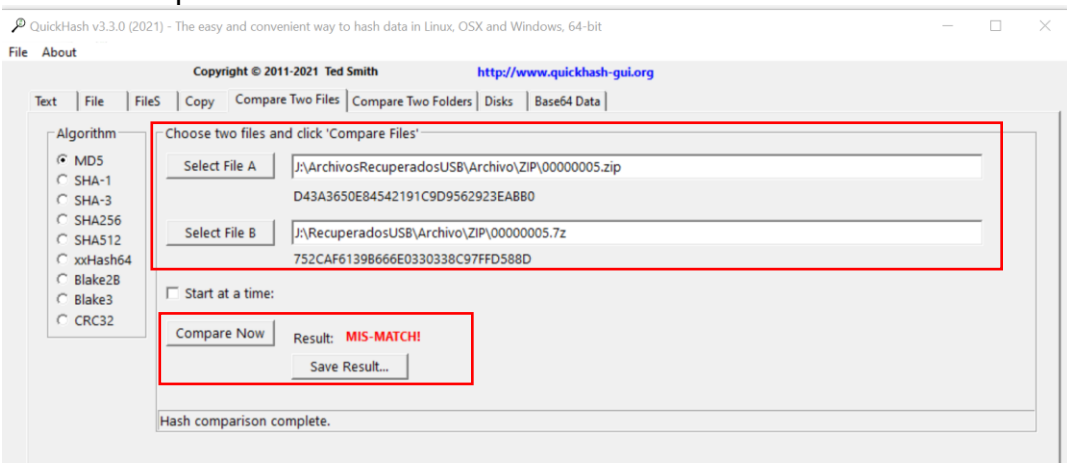
Figura 78. Verificar la integridad de dos archivos con QuickHash



Fuente. Elaboración Propia.

Esta opción es ideal cuando se trata de comparar archivos de tamaño grande y se dispone de poco tiempo en la aplicación de hash a cada uno de los archivos que contienen los directorios seleccionados para la comprobación de integridad.

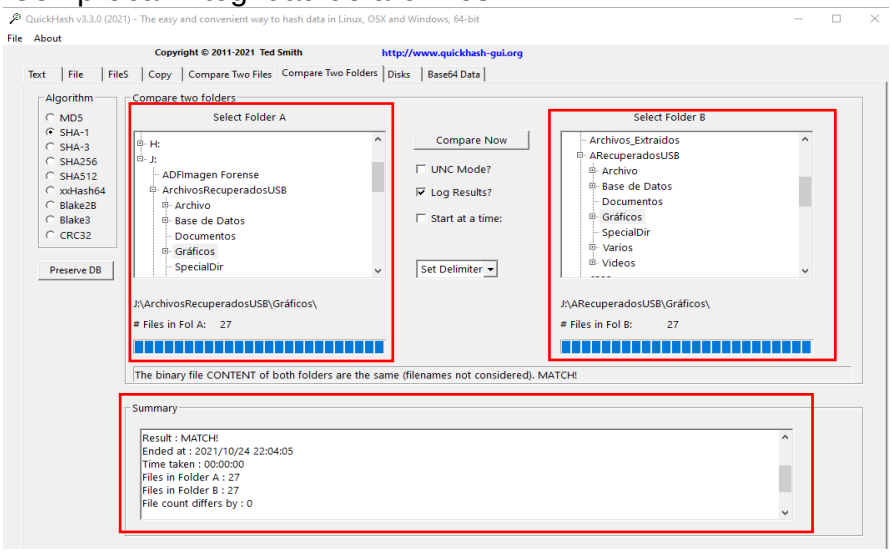
Figura 79. Comparar hash de archivos



Fuente. Elaboración Propia.

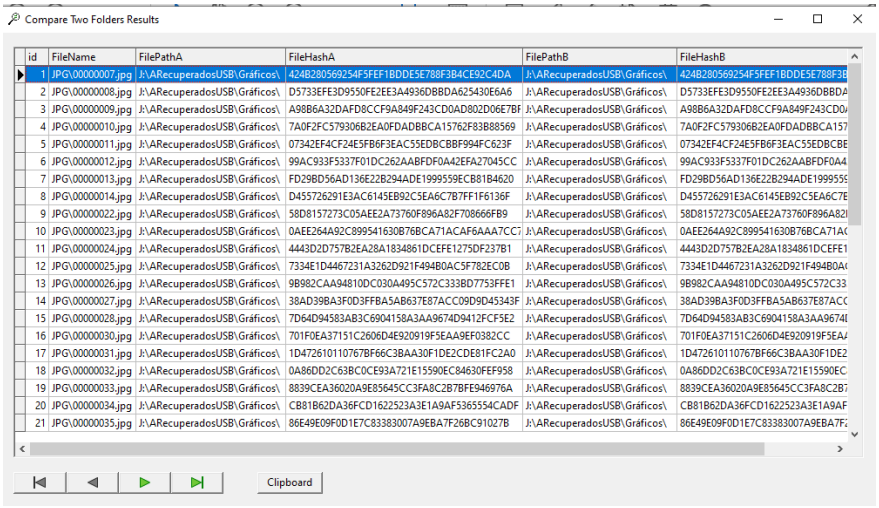
La pestaña COMPARE TWO FOLDERS, permite la comparación del contenido de archivos de dos carpetas. Esta funcionalidad permite comprobar la integridad de las carpetas que se utilizan para mantener la cadena de custodia en el tratamiento de la información y verificar el contenido de los archivos cuando existe diferencia de datos al realizar la comparación de dos carpetas de archivos fuentes.

Figura 80. Comprobar integridad de archivos



Fuente. Elaboración Propia.

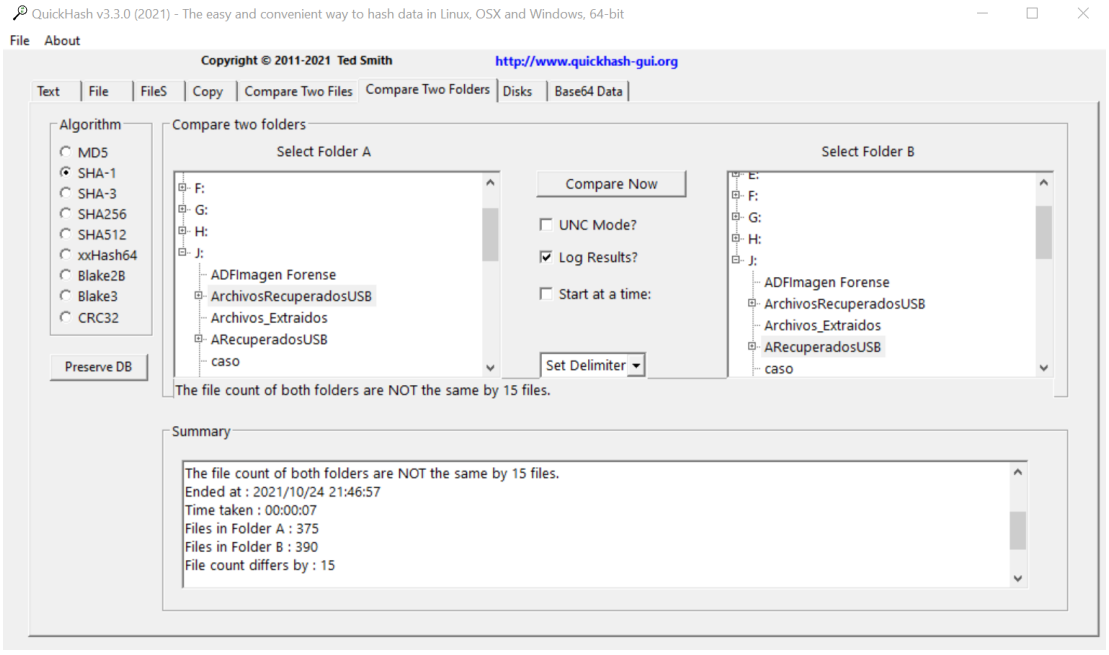
Figura 81. Resultados de coincidencia de valores de HASH



Fuente. Elaboración Propia.

En la siguiente figura se observa una diferencia de 15 archivos de datos al realizar la comparación de recuento de archivos y el contenido de la carpeta ArchivosRecuperadosUSB frente al contenido de la carpeta ARecuperadosUSB.

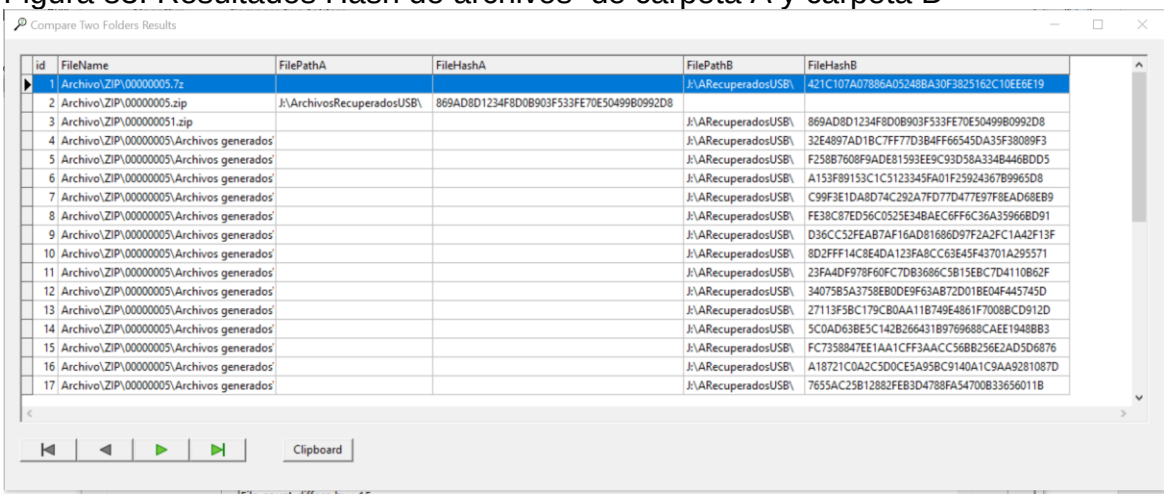
Figura 82. Ver comparación de archivos



Fuente. Elaboración Propia.

Para verificar las coincidencias, las diferencias en el contenido de cada archivo que se analiza, la duplicación de hash, hash faltantes y nombre de archivos faltantes, el profesional informático se dirige a la cuadrícula de visualización. Esta funcionalidad resalta los valores hash para cada archivo cuando se presenta disparidad en el recuento de archivos.

Figura 83. Resultados Hash de archivos de carpeta A y carpeta B

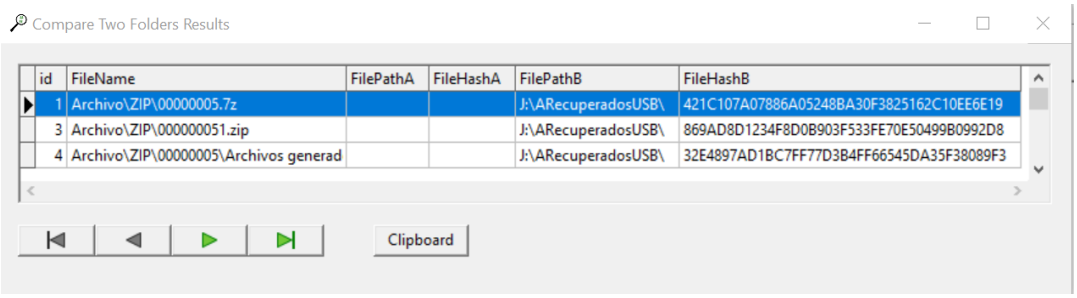


id	FileName	FilePathA	FileHashA	FilePathB	FileHashB
1	Archivo\ZIP\00000005.7z			J:\ARecuperadosUSB\	421C107A07886A05248BA30F3825162C10EE6E19
2	Archivo\ZIP\00000005.zip	J:\ArchivosRecuperadosUSB\	869AD8D1234F8D0B903F533FE70E50499B0992D8		
3	Archivo\ZIP\000000051.zip			J:\ARecuperadosUSB\	869AD8D1234F8D0B903F533FE70E50499B0992D8
4	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	32E4897AD1BC7FF77D3B4FF66545DA35F38089F3
5	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	F258B7608F9ADE81593EE9C93D58A334B446BDD5
6	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	A153F89153C1C5123345FA01F25924367B9965D8
7	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	C99F3E1DA8D74C292A7FD77D477E97F8EAD68EB9
8	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	FE38C87ED56C0525E34BAEC6FF6C36A35966BD91
9	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	D36CC52FEAB7AF16AD81686D97F2A2FC1A42F13F
10	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	8D2FFF14C8E4DA123FA8CC63E45F43701A295571
11	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	23FA4DF978F60FC7DB3686C5B15EBC7D4110B62F
12	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	34075B5A3758EB0DE9F63AB72D01BE04F445745D
13	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	27113F5BC179CB0AA11B749E4861F7008BCD912D
14	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	5C0AD63BE5C142B266431B9769688CAEE1948BB3
15	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	FC7358847EE1AA1CFF3AACC56BB256E2AD5D6876
16	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	A18721C0A2C5D0CE5A95BC9140A1C9AA9281087D
17	Archivo\ZIP\00000005\Archivos generados			J:\ARecuperadosUSB\	7655AC25B12882FEB3D4788FA54700B33656011B

Fuente. Elaboración Propia.

La siguiente figura muestra un valor de hash del contenido de un archivo de extensión .7z con nombre de archivo 00000005.7z que se encuentra solo en la carpeta B y no aparece coincidencia de contenido hash en la carpeta A.

Figura 84. Archivo No encontrado de la fuente A

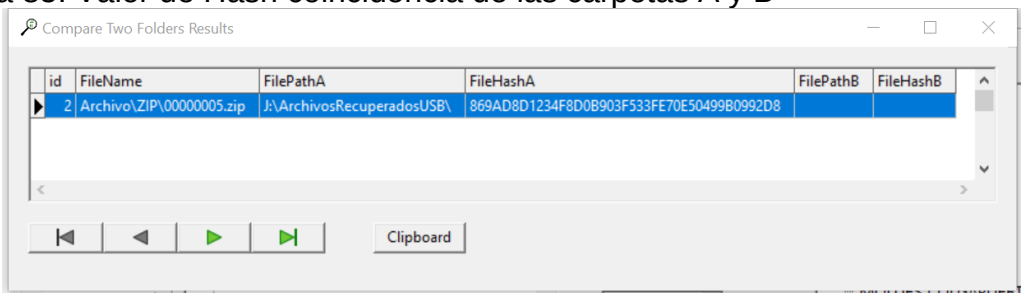


id	FileName	FilePathA	FileHashA	FilePathB	FileHashB
1	Archivo\ZIP\00000005.7z			J:\ARecuperadosUSB\	421C107A07886A05248BA30F3825162C10EE6E19
3	Archivo\ZIP\000000051.zip			J:\ARecuperadosUSB\	869AD8D1234F8D0B903F533FE70E50499B0992D8
4	Archivo\ZIP\00000005\Archivos generad			J:\ARecuperadosUSB\	32E4897AD1BC7FF77D3B4FF66545DA35F38089F3

Fuente. Elaboración Propia.

De igual manera, la cuadrícula de visualización presenta un valor de hash del contenido de un archivo de extensión .zip con nombre 00000005.zip que se encuentra en la carpeta A que no aparece en la carpeta B, pero si existe un archivo en la carpeta B llamado 000000051.zip que tiene coincidencia del valor hash del archivo 00000005.zip que pertenece a la carpeta A.

Figura 85. Valor de Hash coincidencia de las carpetas A y B

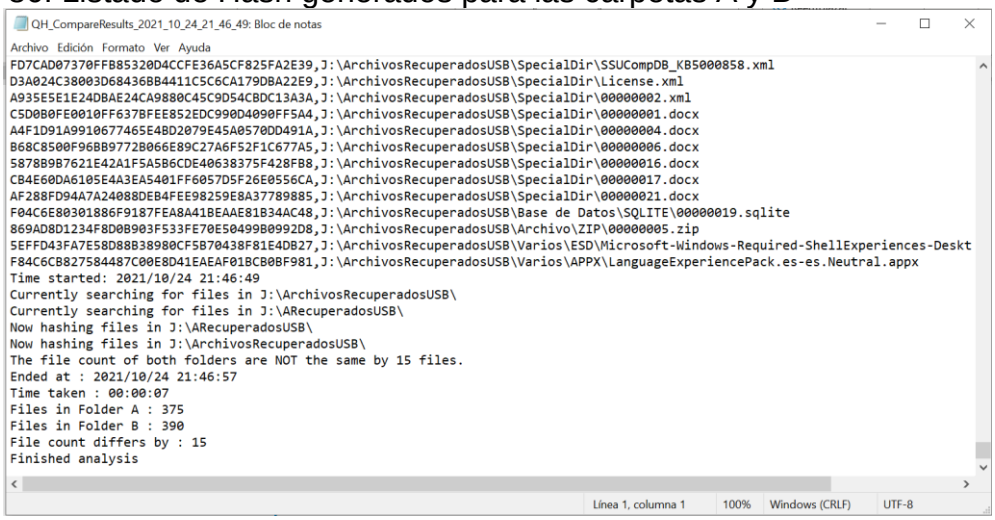


Fuente. Elaboración Propia.

QuickHash GUI v3.3.0 permite el guardar los resultados de los valores de hash generados en la comprobación de integridad de las carpetas seleccionadas en un archivo de texto organizado línea por línea para cada archivo que contienen las carpetas fuentes de análisis de datos.

La siguiente figura muestra los resultados de comparación de valores hash para la carpeta A de ubicación J:\ArchivosRecuperadosUSB\ y la carpeta B en la ubicación J:\ARecuperadosUSB\.

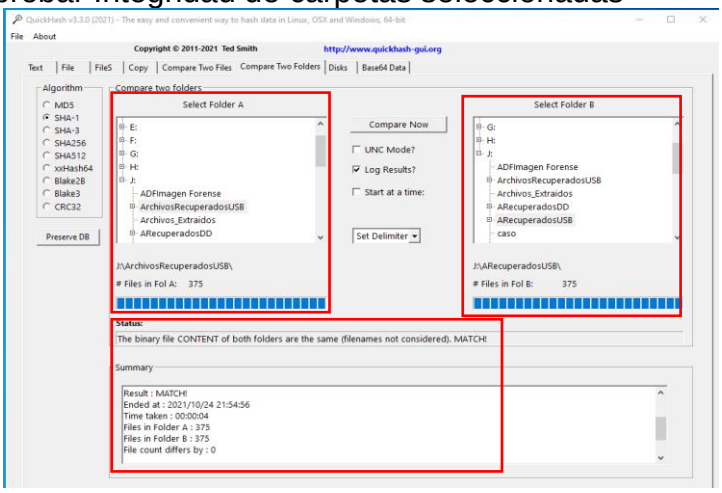
Figura 86. Listado de Hash generados para las carpetas A y B



Fuente. Elaboración Propia.

La siguiente figura muestra cómo es el proceso de cálculo de valor hash cuando las dos carpetas seleccionadas coinciden. De esta manera, QuickHash ayuda a los profesionales informáticos a garantizar la integridad de los datos analizados en un proceso de tratamiento de la información.

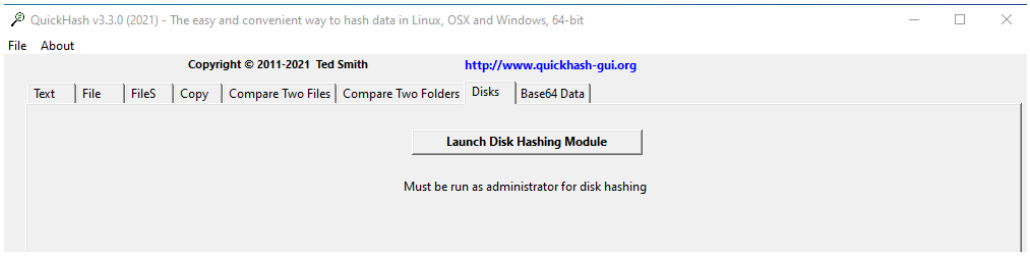
Figura 87. Comprobar Integridad de carpetas seleccionadas



Fuente. Elaboración Propia.

Desde la pestaña DISK se puede calcular un hash para un disco físico completo y volúmenes lógicos. Para ejecutar esta funcionalidad, el profesional informático debe contar con permisos de administrador del sistema.

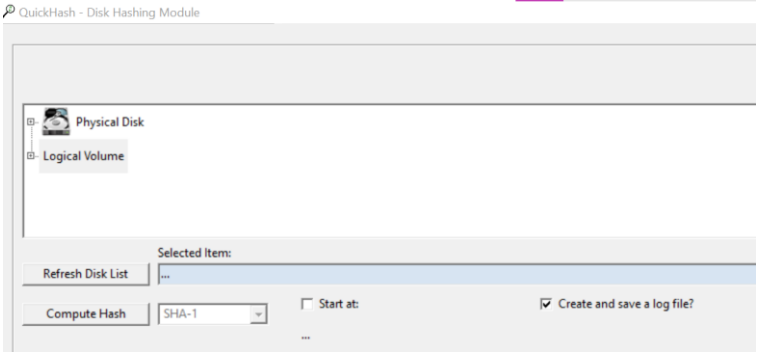
Figura 88. Crear hash a un Disco.



Fuente. Elaboración Propia.

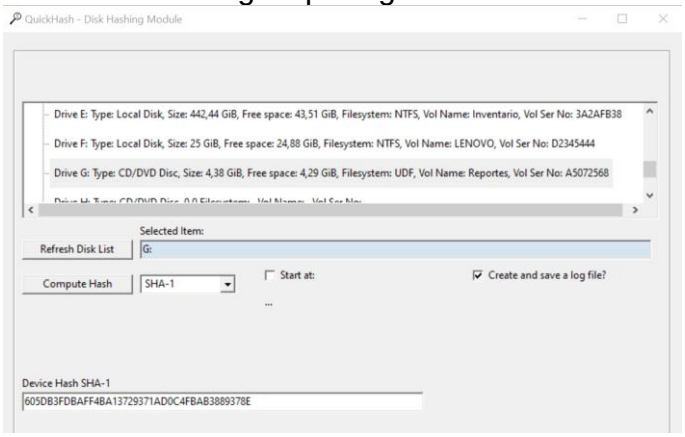
La siguiente figura muestra el proceso para generar un valor hash a un volumen lógico, al hacer clic al botón INICIAR MÓDULO DE HASH DE DISCO.

Figura 89. Módulo de QuickHash para crear Hash de volumen lógico



Fuente. Elaboración Propia.

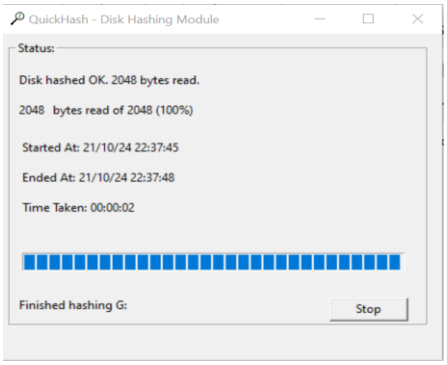
Figura 90. Seleccionar volumen lógico para generar el valor Hash



Fuente. Elaboración Propia.

QuickHash proporciona una barra de proceso para visualizar el estado de generación de un valor hash a un volumen lógico, la fecha, la hora de inicio y finalización del cálculo de hash al volumen lógico analizado y el tiempo requerido

Figura 91. Creando hash



Fuente. Elaboración Propia.

Finalmente, se selecciona la ubicación de la carpeta para guardar el resultado que contiene el valor de hash generado para el volumen lógico analizado disponible en un archivo de texto.

Figura 92. Ver hash creado para la unidad (G)

Fuente. Elaboración Propia.

5.5.7 PoC Análisis de Imagen Forense : AUTOPSY v4.19.1

Figura 93 . Características de Autopsy

Fuente. Elaboración propia.

Pasos previos :

- Se obtiene una imagen forense del equipo de cómputo del escenario propuesto con herramienta FTK Imager.

- Para preservar la evidencia original en la cadena de custodia, se realiza una copia de la imagen forense original.

- Se comprueba la integridad de la imagen forense copia con la imagen forense original con la herramienta forense QuickHash.

Para comprobar las funcionalidades de la herramienta forense AUTOPSY en el análisis del escenario propuesto, se realiza los siguientes pasos :

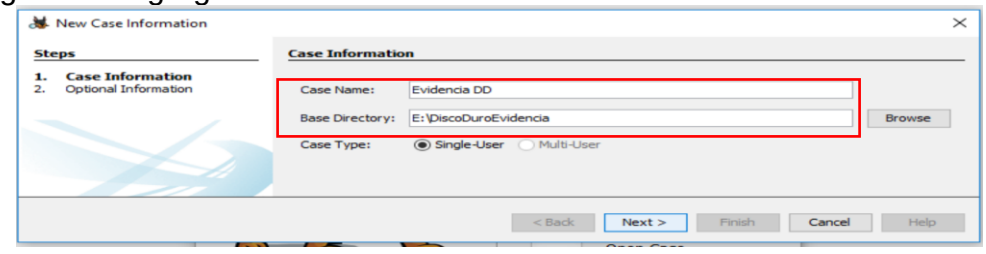
- Se realiza la creación de un nuevo caso en la herramienta Autopsy al hacer clic en el botón Nuevo Caso.

Figura 94. Crear Caso en Autopsy

Fuente. Elaboración Propia.

- Se ingresa la información que se requiere para iniciar el análisis forense digital en la herramienta AUTOPSY relacionado al nuevo caso tales como el nombre del caso y la ubicación para guardar el caso.

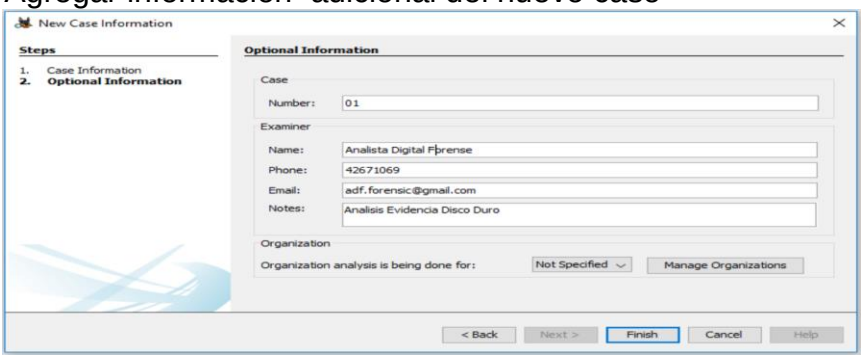
Figura 95. Agregar información del nuevo caso



Fuente. Elaboración Propia.

- A continuación, se debe agregar el número del caso y datos del investigador o analista encargado.

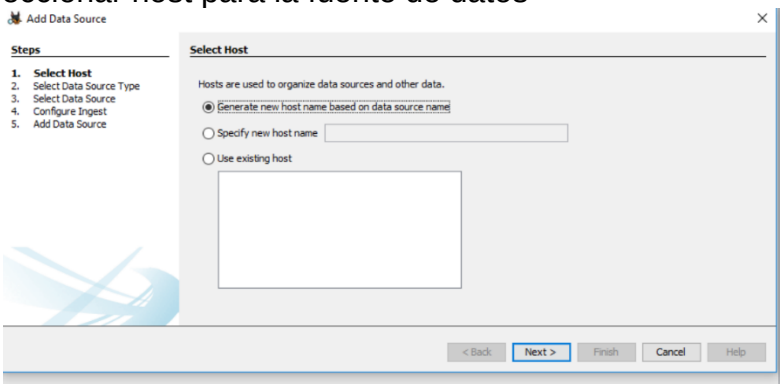
Figura 96. Agregar información adicional del nuevo caso



Fuente. Elaboración Propia.

En el proceso de creación de un nuevo caso con la herramienta Autopsy v4.19.1 se debe asociar un host para la fuente de datos que se va a agregar al nuevo caso. Existe tres opciones para elegir el host de la fuente de datos: generar un nuevo host que se base en el nombre de la fuente de datos, especificar un nombre de host y utilizar un host existente. Este proceso se realiza porque no es posible utilizar la copia de la fuente de datos en la carpeta del caso nuevo para realizar un análisis con la herramienta Autopsy.

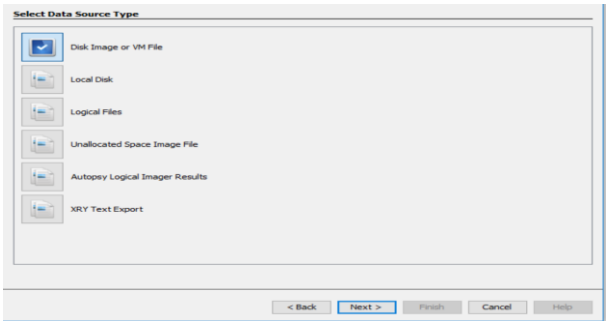
Figura 97. Seleccionar host para la fuente de datos



Fuente. Elaboración Propia.

- Luego, se selecciona el tipo de fuente de datos (un archivo de imagen del Disco, un Disco duro, pendrives, tarjetas de memorias, Archivos lógicos, exportación de archivos desde XRY, archivos de imágenes de espacio no asignados y más) que se desea agregar con la imagen o archivo a examinar en la herramienta Autopsy.

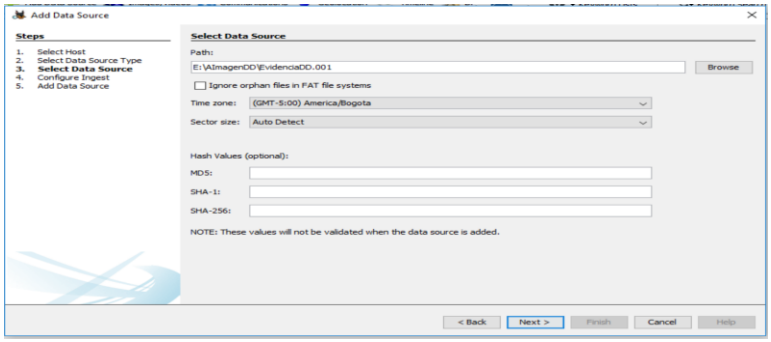
Figura 98. Seleccionar fuente de datos de la Evidencia



Fuente. Elaboración Propia.

En esta imagen, el analista informático selecciona la ruta de la fuente de datos para que la herramienta Autopsy examine los archivos correspondientes a la fuente de datos.

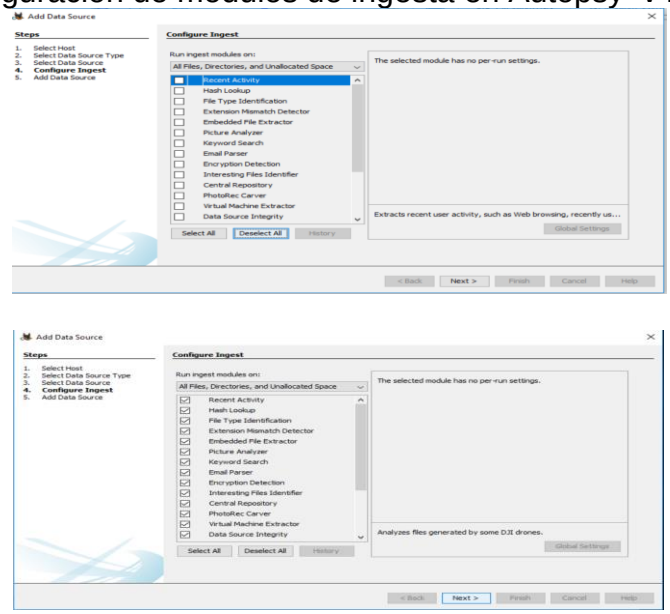
Figura 99. Seleccionar ruta de localización de la Evidencia



Fuente. Elaboración Propia.

- Una vez que se finalice el proceso anterior, se configura el módulo de Ingesta. Para esto, el analista informático debe marcar o desmarcar las opciones que considere necesarias para realizar las operaciones de análisis, recuperación, identificación, extracción y cálculo de hash pertinentes al contenido de los archivos que hacen parte de la evidencia digital.

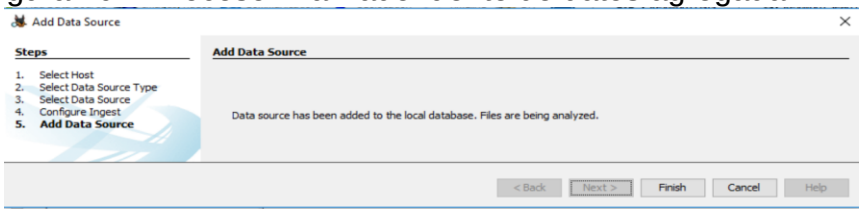
Figura 100. Configuración de módulos de ingesta en Autopsy v4.19.1



Fuente. Elaboración Propia.

- Después de cargar la fuente de datos de la evidencia digital, se debe esperar la finalización del proceso de análisis de herramienta forense AUTOPSY para visualizar el contenido de la evidencia digital.

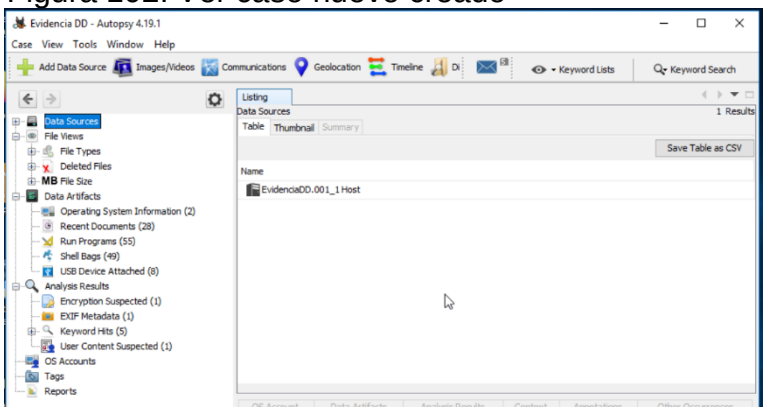
Figura 101. Proceso finalizado fuente de datos agregada



Fuente. Elaboración Propia.

- Finalmente, el investigador informático puede visualizar el contenido del análisis de la fuente de datos desde el caso nuevo que ha creado desde la interfaz de usuario de Autopsy v4.19.1.

Figura 102. Ver caso nuevo creado

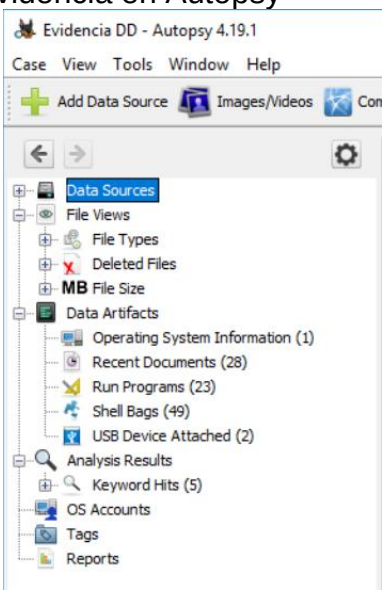


Fuente. Elaboración Propia.

La interfaz de usuario de la herramienta de software forense AUTOPSY v4.19.1 se divide en seis áreas principales: el visor de árbol de evidencia, el visor de resultados, el visor de contenido, búsqueda por palabras claves y un área de estado.

Desde el visor de árbol de evidencia, el analista informático puede realizar la navegación en los distintos archivos que ha encontrado Autopsy en el análisis de la fuente de datos para consolidar la evidencia digital.

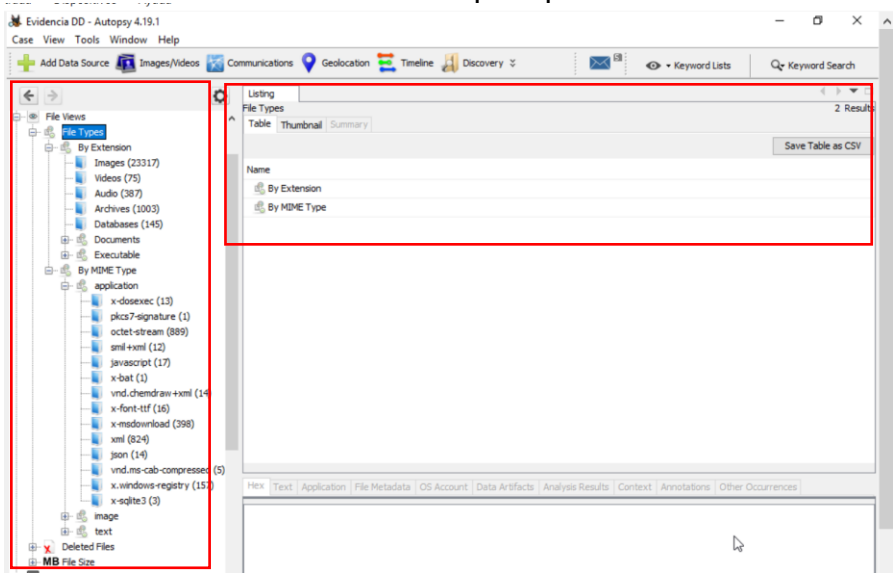
Figura 103. Visor de árbol de evidencia en Autopsy



Fuente. Elaboración Propia.

De esta manera, el analista informático selecciona elementos con el propósito de examinar y visualizar los resultados de los archivos de acuerdo con la extensión, por la naturaleza del formato del archivo, archivos borrados y más.

Figura 104. Visor de árbol de evidencia por tipos de archivos

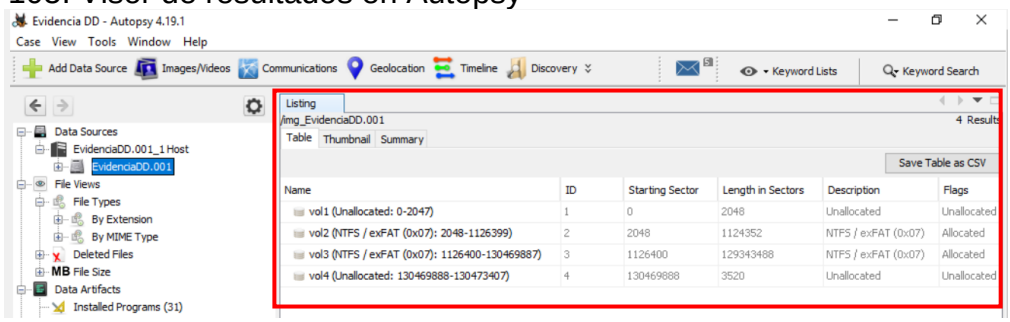


Fuente. Elaboración Propia.

Autopsy v4.19.1 permite analizar todo el contenido de las unidades lógicas encontradas en la fuente de datos agregadas al caso. En el área del visor de resultados, la herramienta Autopsy permite listar las características relevantes de los datos que encuentra como el nombre, fecha de acceso, titulo, localización, modificación del archivo, resultados del archivo, metadata del archivo, vista previa del archivo.

En la siguiente figura se observa en el visor de resultados las particiones encontradas en la imagen forense agregada al seleccionar la fuente de datos EvidenciaDD.001 en el visor de árbol de evidencia.

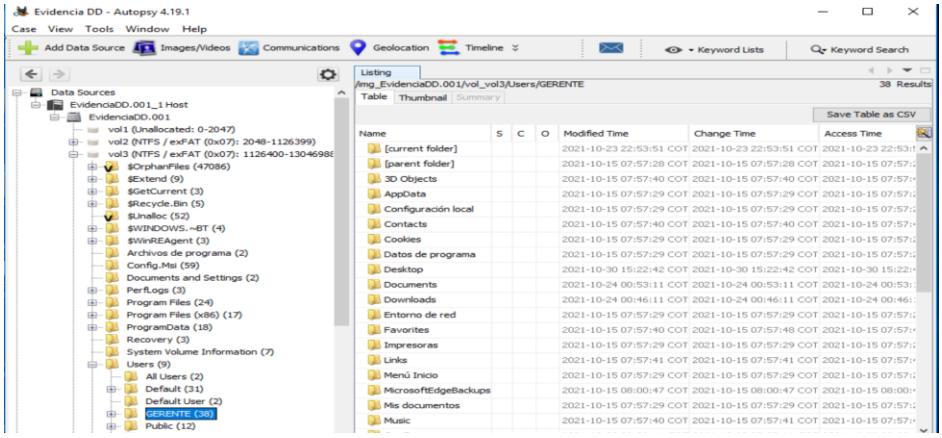
Figura 105. Visor de resultados en Autopsy



Fuente. Elaboración Propia.

En esta figura se muestra elementos de los archivos encontrados en el Usuario Gerente de la imagen EvidenciaDD.001 como el nombre de los archivos, la ruta para acceder a los archivos encontrados, la fecha de creación y modificación de archivos, el acceso a los archivos y tamaño del archivo.

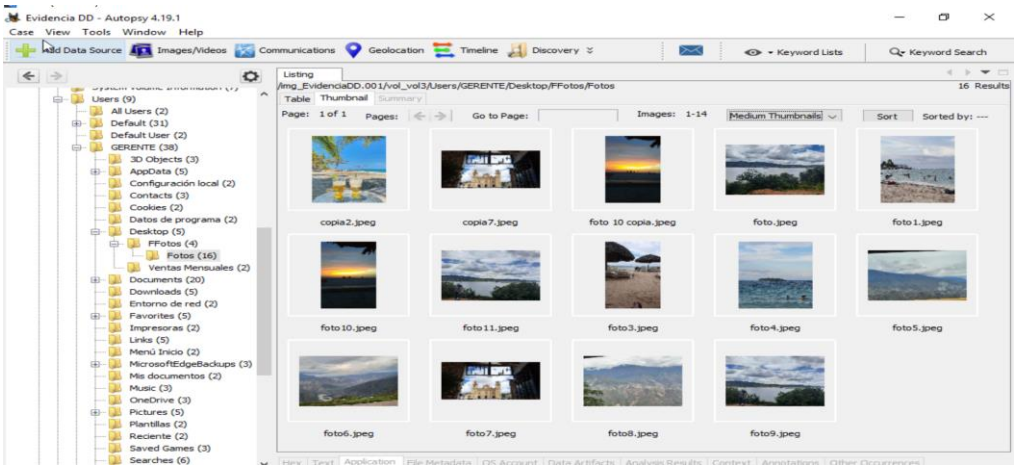
Figura 106. Análisis de archivos usuario GERENTE



Fuente. Elaboración Propia.

El visor de contenido de Autopsy v4.19.1 se utiliza en la investigación forense digital para la visualización de un archivo específico al seleccionar un archivo en el área del visor de resultados. En esta figura se observa que en el caso creado por Autopsy llamado EvidenciaDD, el analista informático examina el contenido de la carpeta FFotos que se encuentra ubicada en el escritorio del usuario Gerente.

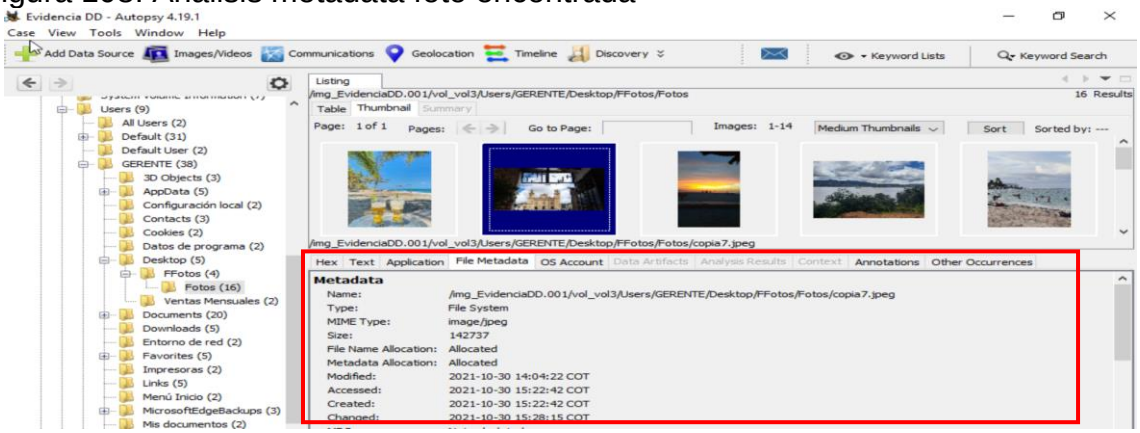
Figura 107. Contenido de carpeta “FFotos” del Usuario Gerente



Fuente. Elaboración Propia.

El área del visor de contenido de Autopsy v4.19.1 permite mostrar los datos del contenido de un archivo específico seleccionado en diferentes formatos como hexadecimal, texto, aplicación, metadatos del archivo, cadenas, marcadores de datos asociados, cuenta de sistema operativo asociada al resultado, resultados de análisis, contexto del archivo, anotaciones y otras instancias para el archivo seleccionado.

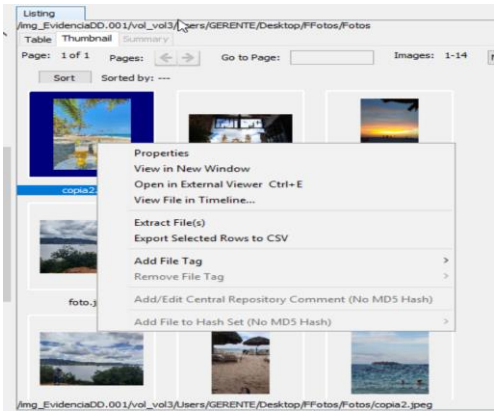
Figura 108. Análisis metadata foto encontrada



Fuente. Elaboración Propia.

La extracción y visualización de los archivos de interés para el analista forense digital es muy fácil con la herramienta Autopsy v4.19.1 tan solo se requiere hacer un clic derecho en archivo y aparecerán las opciones de: propiedades del archivo, ver en una nueva ventana, ver archivo en la línea de tiempo, extraer el archivo, exportar líneas seleccionadas a un CVS, agregar etiquetas al archivo, adicionar un hash, remover etiquetas entre otras opciones.

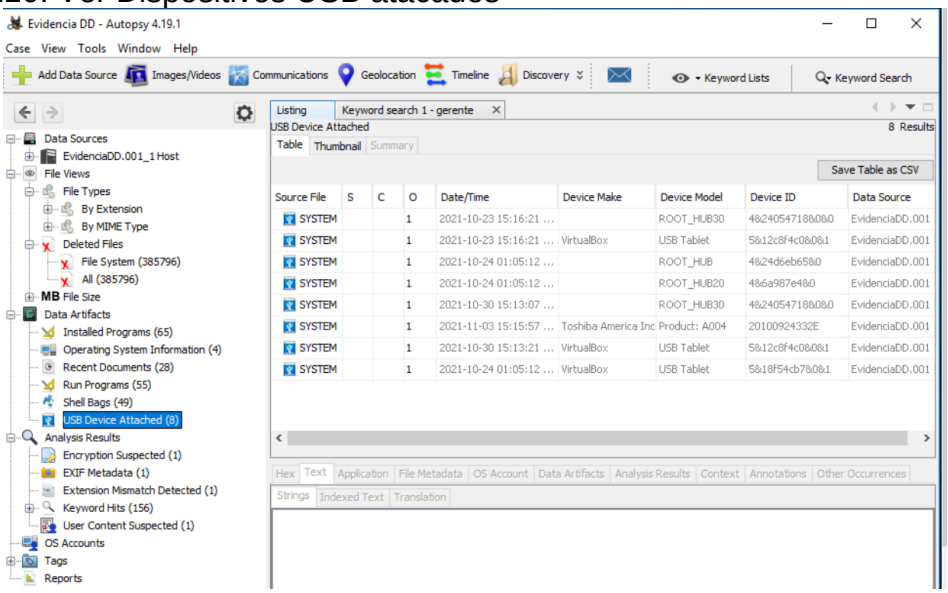
Figura 109. Ver propiedades de archivo



Fuente. Elaboración Propia.

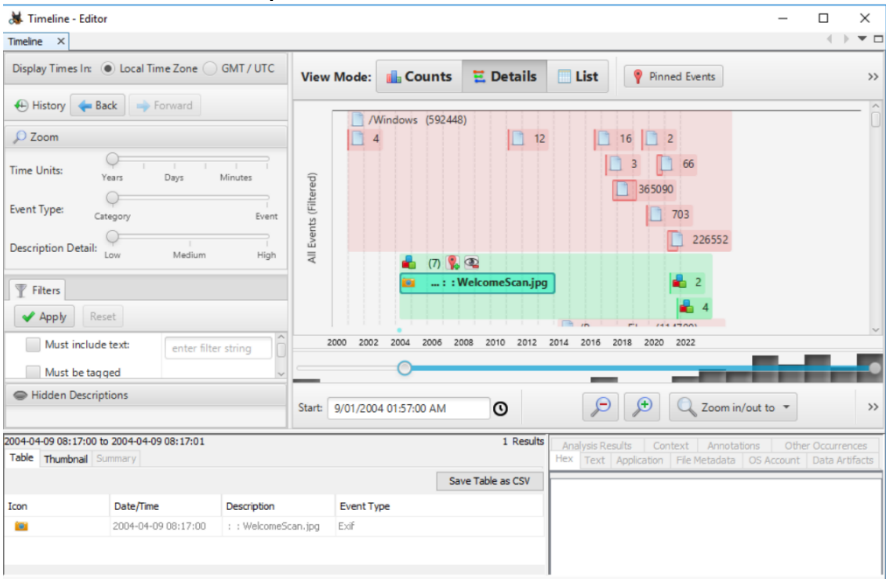
Autopsy v4.19.1 tiene una sección en el visor de árbol de visualización de la evidencia llamada Artefacto de datos que proporciona al analista informático detalles de la actividad del usuario que ayuda al establecimiento de hipótesis para la investigación que se lleva a cabo.

Figura 110. Ver Dispositivos USB atacados



Fuente. Elaboración Propia.

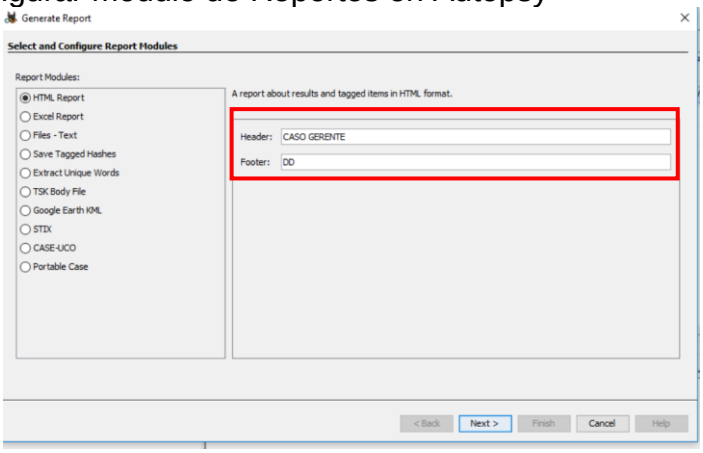
Figura 111. Ver línea de tiempo



Fuente. Elaboración Propia.

Autopsy v4.19.1 dispone de un módulo de informe que permite la extracción de información importante en la investigación de un caso. Para crear un informe forense informático en Autopsy de tipo HTML, el analista informático se dirige a interfaz gráfica inicial en la barra de menú opción TOOLS o Herramientas, luego hacer clic en la opción Generar Reportes. De esta manera, el investigador puede seleccionar la presentación del reporte e incluir la cabecera y pie de página que aparecerán en el informe, las fuentes de datos y los datos del reporte, para terminar, se debe hacer clic en el botón finalizar.

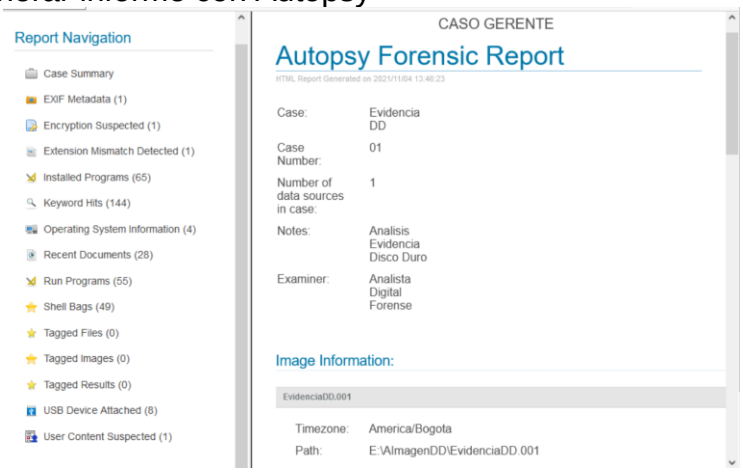
Figura 112. Configurar módulo de Reportes en Autopsy



Fuente. Elaboración Propia.

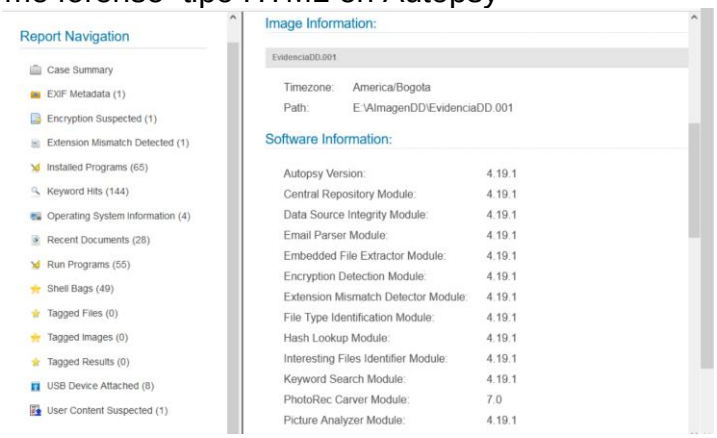
El informe tipo HTML generado con la herramienta de software forense Autopsy se verá de forma similar a las siguientes figuras:

Figura 113. Generar informe con Autopsy



Fuente. Elaboración Propia.

Figura 114. Informe forense tipo HTML en Autopsy



Fuente. Elaboración Propia.

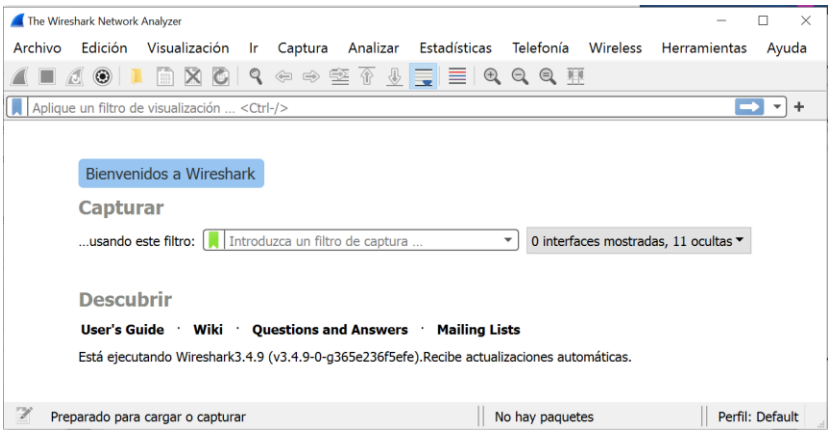
5.5.8 PoC Análisis Forense de Redes: WIRESHARK v3.4.9

Wireshark es una herramienta de software muy poderosa utilizado por los profesionales TI expertos para realizar el análisis forense de red. Wireshark es un analizador de protocolo de red, multiplataforma, disponible de forma gratuita, es de código abierto y con licencia GPLv2. Este analizador de paquetes de red presenta los datos de los paquetes capturados con el mayor detalle posible. Por las características y funcionalidades que presenta Wireshark les permite a los analistas, investigadores y profesionales informáticos examinar los problemas de seguridad de la red, solucionar problemas de red, verificar las aplicaciones de red, depurar las implementaciones de los protocolos y conocer los aspectos internos del protocolo de red.

A continuación, se muestra algunos ajustes de configuración general para el uso de la herramienta Wireshark en la versión 3.4.9 que permite detectar, capturar y analizar el tráfico de red para la identificación de las amenazas de la red que se examina.

Wireshark v3.4.9 permite la visualización de registro de eventos en la red que analiza mediante la captura del tráfico de red que genera los dispositivos cuando realizan algún tipo de conexión por el uso de protocolos, indicando qué dispositivo hizo la petición, la dirección IP del dispositivo que hace la petición, IP destino de la petición de conexión, Información de la petición, respuesta de la petición, puertos de conexión de origen y destino utilizados por los dispositivos, protocolo utilizado para la conexión, dirección MAC de dispositivos conectados, bytes capturados entre otros.

Figura 115. Interfaz de Inicio Wireshark v3.4.9



Fuente. Elaboración Propia.

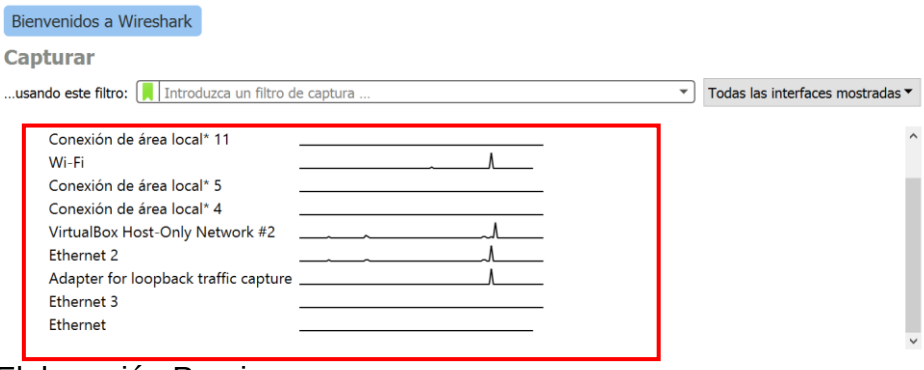
Desde la interface principal de Wireshark se puede realizar la captura de paquetes de una red, utilizando el filtro de captura de las interfaces de red detectadas.

Figura 116. Filtro de captura en Wireshark

Fuente. Elaboración Propia.

De acuerdo con el criterio seleccionado en el filtro de captura de interfaz de red, en la pantalla de inicio de Wireshark se mostrará las interfaces detectadas para obtener una captura del tráfico de red. Luego, se elige la interfaz de red sobre la cual se desea realizar la captura de paquetes de red.

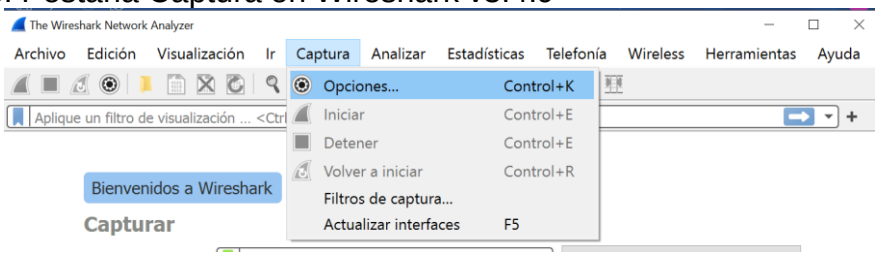
Figura 117. Interfaz Tráfico de Red detectado Wireshark



Fuente. Elaboración Propia.

Un investigador informático puede capturar el tráfico de red desde la interfaz gráfica de inicio de Wireshark con solo hacer clic en la pestaña CAPTURA o en el icono Opciones de Captura en el menú de herramientas.

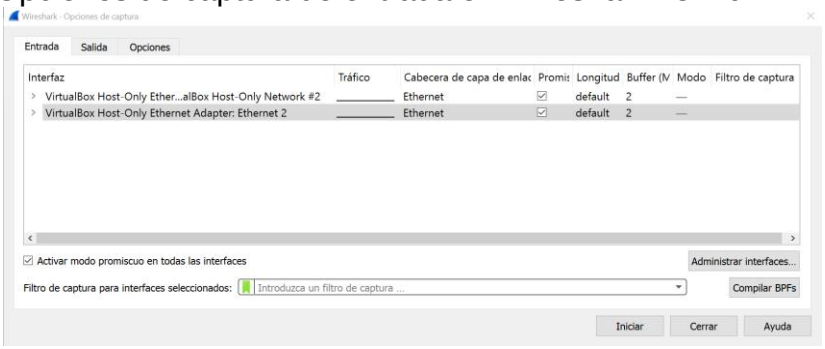
Figura 118. Pestaña Captura en Wireshark v3.4.9



Fuente. Elaboración Propia.

Al ejecutar Opciones de Captura, Wireshark presenta las opciones de entradas, las opciones de salida y las opciones de visualización de la captura de paquetes de red. En la pestaña opciones de entrada se muestra las interfaces de red habilitadas por defecto en Wireshark. En este caso, en la siguiente la figura se muestra que Wireshark tiene solo dos interfaces de red habilitadas en modo promiscuo para capturar de paquetes .

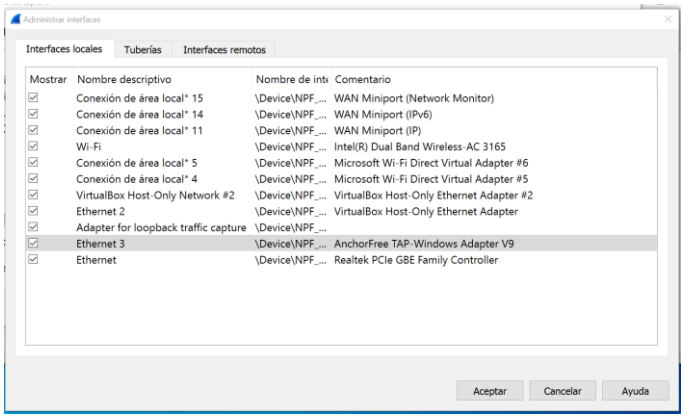
Figura 119. Opciones de captura de entrada en Wireshark v3.4.9



Fuente. Elaboración Propia.

Si el analista informático requiere analizar un tipo de interfaz de red diferente al predeterminado en la configuración de opciones de entrada en wireshark, este debe hacer clic en el botón Administrar Interfaces, pestaña Interfaces locales y seleccionar las interfaces de red que necesita para realizar el análisis de tráfico de red

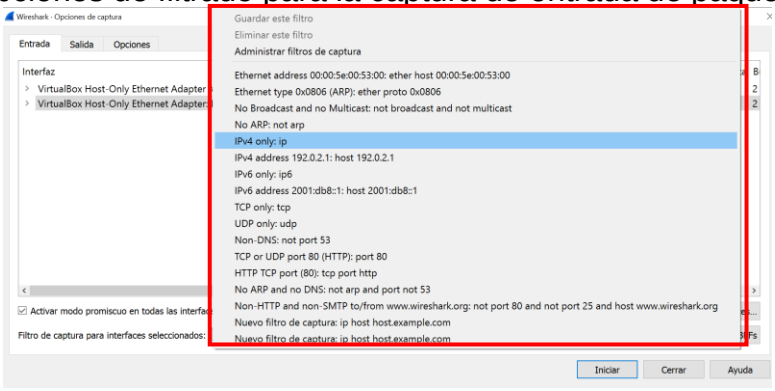
Figura 120. Administrar Interfaces a examinar con Wireshark v3.4.9



Fuente. Elaboración Propia.

La interfaz de captura de entrada proporciona las opciones de filtros de protocolos predefinidos para ejecutar el filtro de captura de paquetes de acuerdo con la interfaz de red seleccionada.

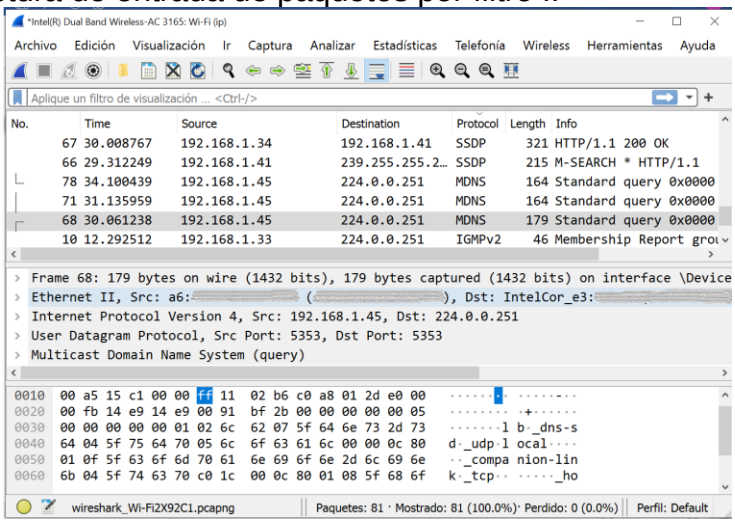
Figura 121. Opciones de filtrado para la captura de entrada de paquetes



Fuente. Elaboración Propia.

En esta figura se observa que la interfaz de red seleccionada para llevar a cabo la captura de tráfico de red es una Red Wi-Fi aplicando el filtro de captura de entrada IPv4 only: ip.

Figura 122. Captura de entrada de paquetes por filtro IP

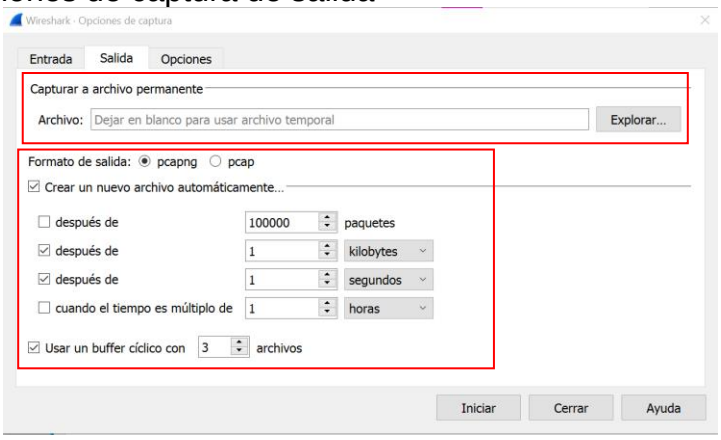


Fuente. Elaboración Propia.

En la opción de salida de la captura de paquetes indica el formato de salida del archivo de captura, la ubicación del directorio y crear nuevos ficheros a partir de la activación de unos filtros de tamaño y tiempo para detener la captura de paquetes. También, se puede habilitar la opción de número de buffer cíclico para indicar el

número de los últimos ficheros que van llegando en la captura de paquetes. De esta manera, se libera los ficheros antiguos para evitar la saturación de almacenamiento de información en el equipo que ejecuta la herramienta de software Wireshark.

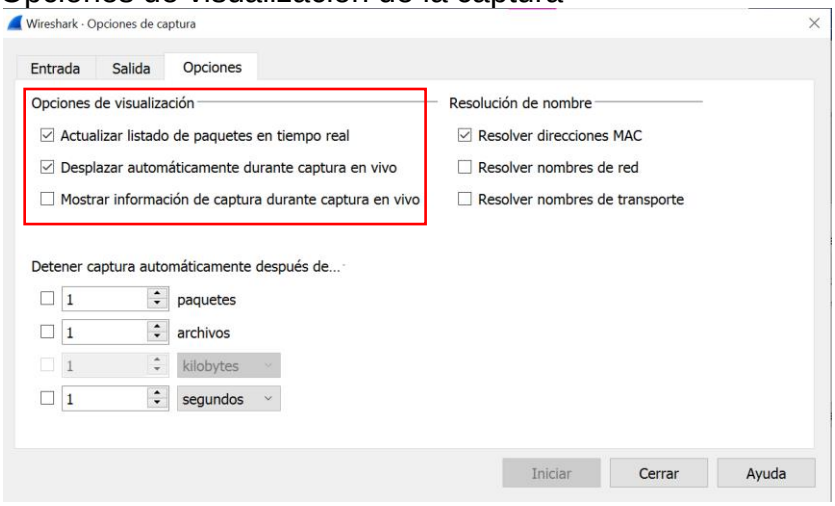
Figura 123. Opciones de captura de salida



Fuente. Elaboración Propia

La pestaña Opciones, sección Opciones de visualización permite habilitar la actualización del listado de paquete en tiempo real, desplazamiento de paquetes de forma automática, así como mostrar información extra de la captura. En la misma pestaña se encuentra la sección Resolución de nombres para habilitar por direcciones MAC, resolución por nombre de red y resolución de nombre de transporte o puertos. Además, se puede habilitar las opciones para detener la captura por número de paquetes, por número de archivos o por cantidad de tiempo en segundos.

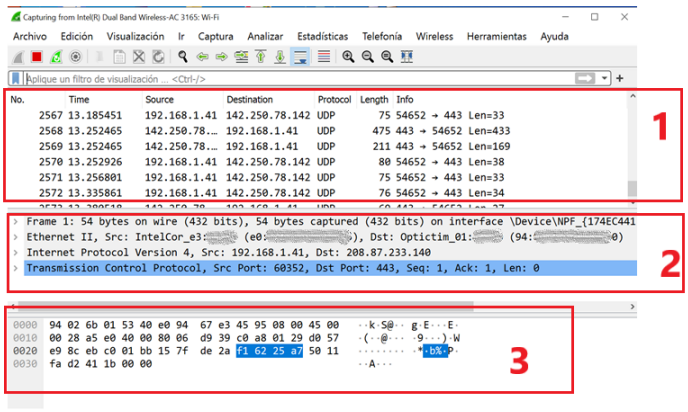
Figura 124. Opciones de visualización de la captura



Fuente. Elaboración Propia.

Una vez que se ha capturado el tráfico de paquetes de la interfaz de red seleccionada se puede ver el funcionamiento de Wireshark. La interfaz gráfica de funcionamiento de la herramienta de software Wireshark se distribuye en tres paneles de visualización de los hallazgos del tráfico de red seleccionado. El primer panel es el panel superior llamado listado de paquetes, el segundo es el panel central llamado panel de Detalles de información del paquete y el tercer panel es el panel inferior llamado panel de Bytes de paquetes. En la siguiente figura se observa la configuración predeterminada de visualización de paquetes en Wireshark versión 3.4.9.

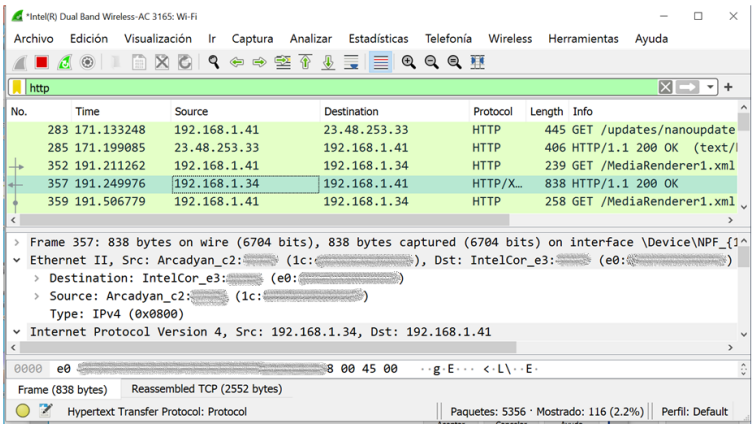
Figura 125. Captura de tráfico Red WI-FI con Wireshark v3.4.9



Fuente. Elaboración Propia.

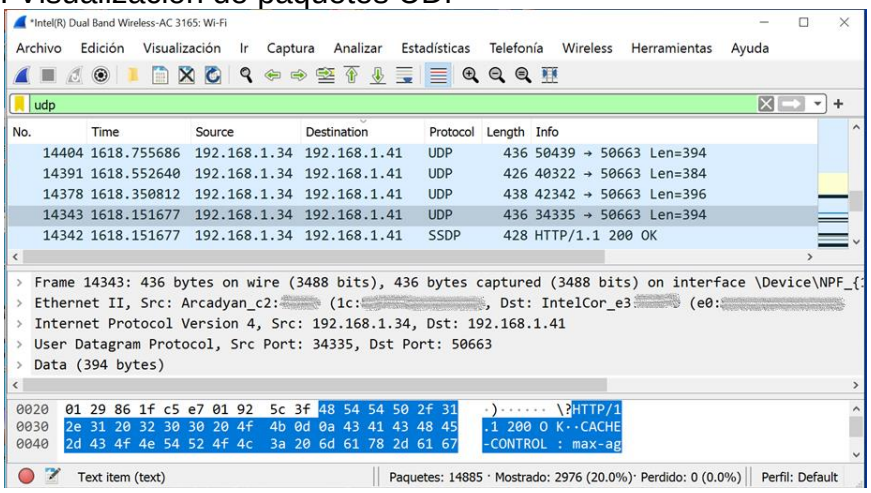
En Wireshark versión 3.4.9 se puede aplicar los filtros de visualización por protocolos TCP/IP,UDP, ARP, DHCP, QUIC, ICMP, DNS y más protocolos para la recolección de información relevante en el análisis de una red.

Figura 126. Filtrado de visualización de tráfico de red por protocolo HTTP



Fuente. Fuente. Elaboración Propia.

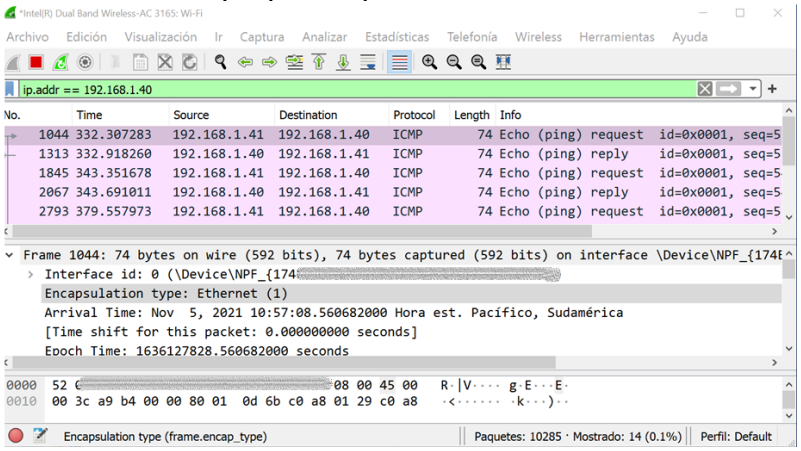
Figura 127. Visualización de paquetes UDP



Fuente. Elaboración Propia.

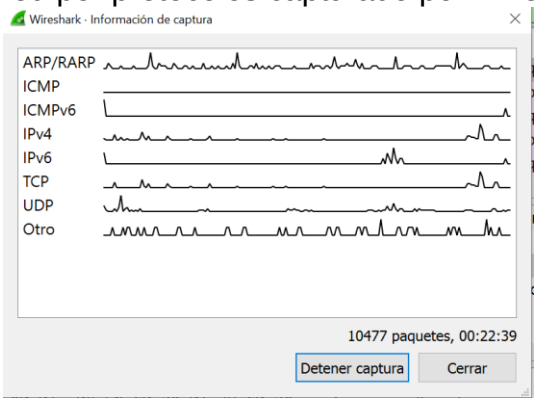
Wireshark permite la creación de filtros de visualización mediante el uso de operadores de comparación. Tal como se muestra en la siguiente figura, en donde Wireshark muestra solo los paquetes desde o hacia la dirección IP 192.168.1.40 al comprobar que existe esta dirección IP en la subred que examina.

Figura 128. Visualización de paquetes por dirección IP



Fuente. Elaboración Propia.

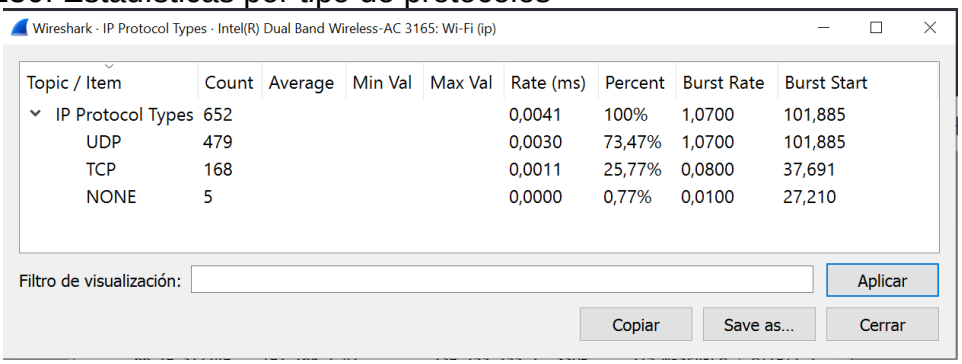
Figura 129. Tráfico de red por protocolos capturado por Wireshark v3.4.9



Fuente. Elaboración Propia.

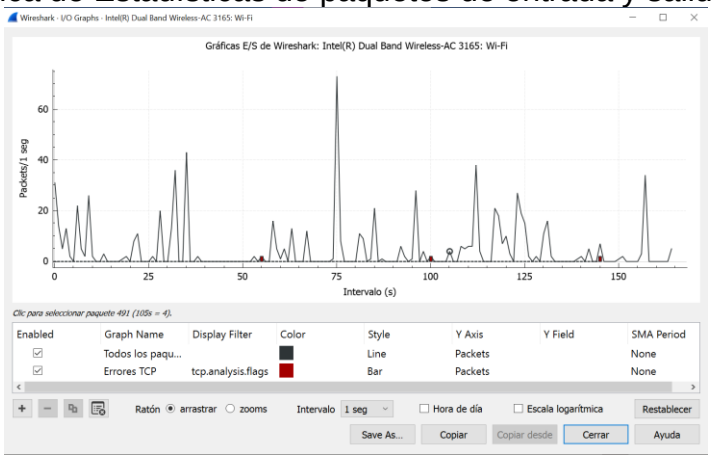
Con Wireshark versión 3.4.9 se puede obtener datos estadísticos relevantes para el análisis de las capturas de trafico de red en el modo en vivo de captura de paquetes de red y capturas de paquetes de red guardados. Para visualizar las estadísticas en Wireshark, el analista informático se dirige a la pestaña ESTADISTICA y selecciona las opciones estadísticas de preferencia para el análisis de paquetes de red.

Figura 130. Estadísticas por tipo de protocolos



Fuente. Elaboración Propia.

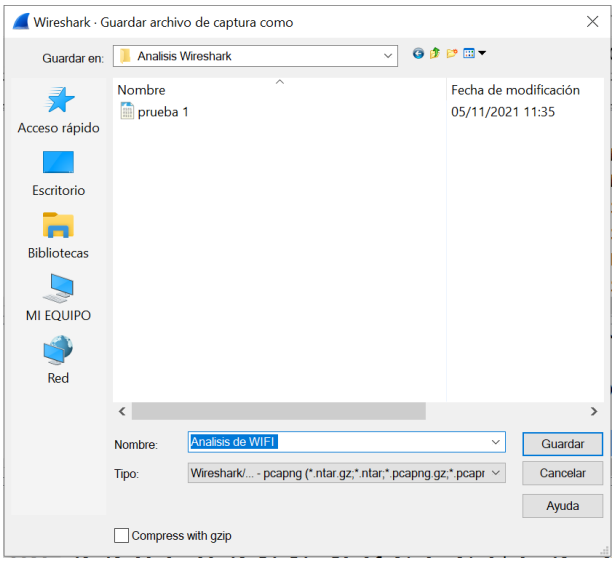
Figura 131. Gráfica de Estadísticas de paquetes de entrada y salida



Fuente. Elaboración Propia.

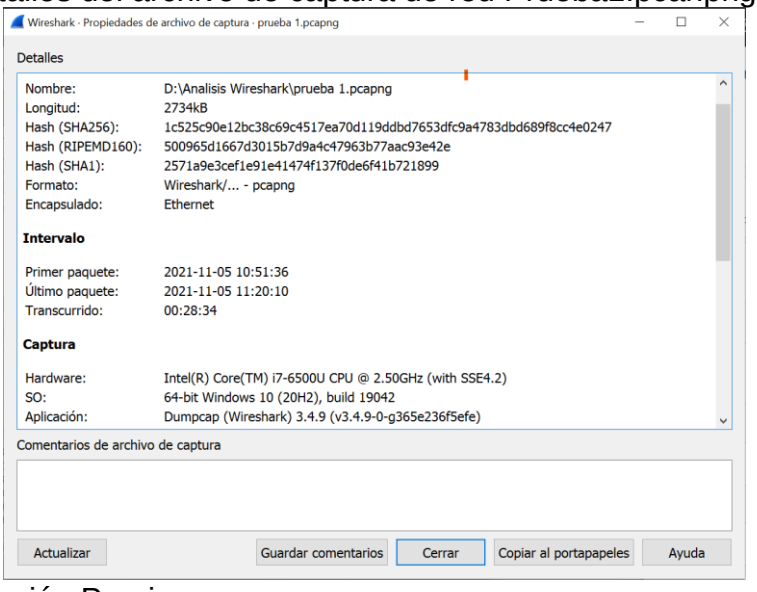
Finalmente, el analista informático guarda la captura de paquetes de red realizado con Wireshark versión 3.4.9 en un directorio de preferencia para el posterior análisis de red y verificación de las propiedades del archivo de captura guardado.

Figura 132. Guardar archivo de captura de red con extensión .pcanpng



Fuente. Elaboración Propia.

Figura 133. Detalles del archivo de captura de red Prueba1.pcanpng



Fuente. Elaboración Propia.

6 CONCLUSIONES

En este documento, se planteó la importancia de implementar el análisis forense digital en las infraestructuras TI organizacionales para verificar el impacto del incidente informático, realizar la interpretación de incidentes informáticos, ejecutar una metodología apropiada de acuerdo con las características del incidente informático y el uso de herramientas de software forense adecuadas para cada procedimiento realizado en una investigación forense.

Se evidencia que la utilización de las herramientas de análisis forense en las investigaciones de delitos informáticos pueden servir para las organizaciones colombianas como instrumentos que permiten mostrar los efectos de las situaciones generadas por las violaciones a los sistemas, proporcionan el conocimiento a las personas encargadas del área TI para que sepan cómo actuar ante un delito informático e implementar nuevas herramientas para mejorar la seguridad de la información, logrando reducir el riesgo de los delitos informáticos.

Se concluye que existe gran variedad de herramientas de software forenses de tipo comercial y gratuito que permiten a los profesionales que se dedican al análisis forense digital, elegir las soluciones de software más adecuadas según el criterio de factores como la utilidad, velocidad y eficacia en el procesamiento de datos en las fuentes de datos disponibles para realizar las investigaciones digitales de forma completa y exhaustiva, en búsqueda de información relevante en donde los hallazgos sea evidencia digital válida ante tribunales y autoridades competentes.

Se especificó que todo proceso llevado a cabo por un profesional TI para la realización del análisis forense digital en las organizaciones actualmente, requiere que el profesional investigador informático debe contar con conocimientos especializados en temas jurídicos relacionados con la regulación de la labor que realiza, certificaciones relacionadas a la investigación forense digital, experiencia en los procedimientos técnicos para el manejo y tratamiento de la evidencia digital, habilidades en el manejo y comprensión de las capacidades de las soluciones de software forenses para el uso adecuado y pertinente en las investigaciones forense.

Se presentaron los procedimientos técnicos para el tratamiento de la evidencia digital y las características de las fases establecidas para llevar a cabo el análisis forense digital en Colombia, con la finalidad de presentar como se lleva a cabo actualmente los procesos de recolección y tratamiento para obtener de evidencia digital válida e integra en las investigaciones forenses informáticas.

Con el avance de la tecnología en los procesos de negocio de las organizaciones, la implementación del trabajo remoto por la situación actual de pandemia por

Covid-19 y la tendencia creciente de delitos informáticos e incidentes de seguridad se presentó la necesidad en las organizaciones de tomar medidas que refuercen las investigaciones corporativas internas y estrategias de seguridad que requieren del proceso de análisis forense digital como solución de gestión.

Se evaluó ocho herramientas de software forense seleccionadas demostrando el funcionamiento, las características y el alcance en la recuperación de información en escenarios propuestos en los sistemas TI y así proponer el uso e implementación de cada una de ellas para realizar investigaciones forenses digitales y respuestas a incidentes en las organizaciones

7 RECOMENDACIONES

Se recomienda a las organizaciones establecer los procesos de análisis forense informáticos como complemento a las acciones definidas en la gestión de la seguridad informática para las operaciones del negocio no solo para las investigaciones de incidentes de seguridad o ciberdelitos sino también como solución para la detección de fallos y diagnósticos de seguridad en la infraestructura TI para reducir una posible ocurrencia de incidente, en el que los procedimientos a realizar se deberán basar en las mejores prácticas, estándares TI y legislación vigente para el tratamiento de la evidencia digital.

Para las organizaciones se recomienda en caso de presentar alguna situación sospechosa que atenta la privacidad e intimidad o le genera inseguridad en las actividades diarias del negocio contar con un personal idóneo en sistemas temas de seguridad informática, realizar diagnósticos de los sistemas TI en la organización con procesos de análisis forense digital, capacitar al personal sobre estrategias para evitar ser víctimas de modalidades de delitos informáticos e importancia de la seguridad informática en la entidad.

Un proceso de investigación forense digital en las organizaciones puede verse comprometido ante la ausencia de evidencia digital, por esta razón se recomienda a las organizaciones solicitar ayuda a las autoridades judiciales competentes cuando esta no dispone de la experiencia en la recolección y tratamiento de evidencia digital, ni personal capacitado para la labor de recolección de información de incidentes presentado o se trata de un delito cibernético y/o incidente de gran afectación para la organización.

Debido al creciente aumento de las modalidades de delitos informáticos que atentan considerablemente la integridad, la confidencialidad y la disponibilidad de los datos en los sistemas TI de las empresas y la aparición de nuevas vulnerabilidades y amenazas, se recomienda a los profesionales informáticos en seguridad conocer las categorías de funcionalidades de software forense, descargar y probar nuevas soluciones de software forense comerciales y gratuitas de funciones específicas para realizar investigaciones de incidentes con mayor rapidez y confiabilidad según el necesidad del caso.

Se recomienda a los profesionales informáticos TI capacitarse en la normatividad específica de Colombia relacionada con la extracción y tratamiento de la evidencia digital, procedimientos para asegurar la cadena de custodia judicial, protección de datos, tipificación de los delitos informáticos, comercio electrónico, fases para realizar el análisis forense digital, derecho a la intimidad y privacidad de información, gestión de laboratorios forenses digitales y manejo de incidentes informáticos.

BIBLIOGRAFÍA

ACCESSDATA. AD Lab 7.3 Release Notes. 2020. [En línea]. [Consulta: octubre 2021]. Disponible en: https://ad-pdf.s3.amazonaws.com/ftk/7.x/7.3.x/Lab_7_3_RN.pdf

ACCESSDATA. [En línea]. 2021. Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

ACURIO DEL PINO, Santiago. 2016. Delitos informáticos: Generalidades. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf p.10-14

ACPO. Good Practice Guide for Computer-based Electronic Evidence. Official release version 4.0. [En línea]. Disponible en: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf

ANSON Steve. Applied Incident Response. 2020. [En línea]. Indianápolis. Wiley. ISBN. 978-1-119-56026-5

AQUILINA James et al. Malware Forensics: Investigating and Analyzing Malicious Code. 2008. [En línea]. ISBN 978-1-59749-268-3.

ARNEDO, Pedro. Herramientas de Análisis Forense y su Aplicabilidad en la Investigación de Delitos Informáticos. 2014. [En línea] [Fecha de consulta: 25 de enero de 2020]. Universidad Internacional de La Rioja. Valledupar, Colombia. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

ARSENAL RECON. Registry Recon. [En línea]. [Fecha de consulta: 20 de octubre de 2021]. Disponible en : http://www.arsenalrecon.com/ apps/recon/

AT&T Business. AlienVault OSSIM. 2022. [En línea]. Disponible en: https://cybersecurity.att.com/products/ossim

BASIS TECHNOLOGY Corp. Autopsy. 2021. [En línea]. [Fecha de consulta: 23 de octubre de 2021]. Disponible en : https://www.autopsy.com/about/

BASIS TECHNOLOGY Corp. Autopsy User Documentation 4.19.1, Graphical digital forensics platform for The Sleuth Kit and other tools. 2021. [En línea] [Fecha de consulta: 10 de noviembre de 2021]. Disponible en: http://sleuthkit.org/autopsy/docs/user-docs/4.19.1//index.html

BBC. SolarWinds: 5 ataques informáticos de Rusia que transformaron a la ciberseguridad en Estados Unidos. 2020. [En línea]. [Fecha de consulta: 24 de octubre de 2021]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-55381892

BECERRA, Jairo, et al. El derecho y las tecnologías de la información y la comunicación TIC. [En línea]. [Fecha de consulta: octubre de 2021]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/16511/1/El-derecho-y-las-tecnolog%c3%adas-de-la-informaci%c3%b3n-y-la-comunicaci%c3%b3n-TIC.pdf

BODDINGTON, Richard. Practical Digital Forensics. Packt Publishing. 2016 [En línea]. [Fecha de consulta: octubre de 2021]. ISB 978-1-78588-710-9

BREZINKI, D. y KILLALEA T. Guideline for Evidence Collection and Archiving. RFC3227. 2002. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en: https://www.ietf.org/rfc/rfc3227.txt

CANO MARTÍNEZ, Jeimy José. 2012. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Bogotá, Colombia: Universidad de los Andes. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/69374?page=281. ISBN. 978-958-695-492-1

CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Bogotá, Colombia: Universidad de los Andes. 2012. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/69374?page=172. ISBN. 978-958-695-492-1

CARRIER B, SPAFFORD E. An Event-Based Digital Forensic Investigation Framework. 2004. [En línea]. Disponible en: https://digital-evidence.org/papers/ dfrws_event.pdf

CARVEY Harlan. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. [En línea]. ISBN 978-0-12-803291-6.

CASTILLO, Luisa & BOHADA, John. Informática Forense en Colombia. Grupo de Investigación MUISCA. Revista Ciencia, Innovación y Tecnología p.86/Voll.II/2015. Fundación Universitaria Juan de Castellanos, Tunja, Colombia. Disponible en : https://www.jdc.edu.co/revistas/index.php/rciyt/article /view/113/102

CASTRO ROMERO, Martha Irene, et al. La informática Forense desde un enfoque práctico. 2020. [En línea]. [Fecha de consulta: octubre de 2021]. Disponible en : https://www.3ciencias.com/wpcontent/uploads/2020/09/LAINFORM%C3%81TICA-FORENSE-DESDE-UN-ENFOQUE-PR%C3%81CTICO.pdf

CCLEANER. Recuva: Recupera tus archivos borrados rápida y fácilmente. 2021. [En línea]. [Fecha de consulta: septiembre 2021] Disponible en : https://www.ccleaner.com/recuva

CENTRO CIBERNÉTICO POLICÍA NACIONAL DE COLOMBIA. Balance Cibercrimen 2020 – semana 45. [En línea]. [Fecha de consulta: 27 de septiembre 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_ cibercrimen_2020_-_semana_45.pdf

CHICANO TEJADA, Esther. Gestión de Incidentes de seguridad. IFTCT0109. 2014. IC Editorial. ISBN:978-84-16351-70-1

CHICANO TEJADA, Esther. Gestión de incidentes de seguridad informática (MF0488_3). Antequera, Málaga. IC Editorial. 2015. [En línea]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44101?page=276. ISBN: 978-84-16207-15-2

CISCO. ¿Qué es Snort?. 2022. [En línea]. Disponible en: https://www.snort.org/.

CENTRO CIBERNÉTICO POLICIAL DE COLOMBIA. Carta Nigeriana. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://caivirtual.policia.gov.co/ contenido/carta-nigeriana-herencia

CLEVERFILES. Disk Drill para MacOS. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://www.cleverfiles.com/es/

CNW Recovery Developments Ltd. CnW Recovey, Data recovery software. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.cnwrecovery.com/

COHEN FRED. Digital Forensic Evidence Examination. Fifth Edition. 2009. [En línea]. Disponible en: http://all.net/books/2013-DFE-Examination.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273. (5,enero,2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”. [En línea]. En: Diario Oficial. Enero,2009. Nro.47.223. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1453. (24,junio,2011). Por medio de la cual se reforma el Código de Procedimiento Penal, el código de Infancia y Adolescencia. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/ gestornormativo/norma.php?i=43202

COLOMBIA. CONGRESO DE COLOMBIA. Ley 527. (21,agosto,1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales. 2021. [En línea]. En: Diario Oficial. Enero,2009. Nro. 47.223. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1564. (12,julio,2012).Por medio de la cual se expide el Código General del proceso y se dictan otras disposiciones. 2012. [En línea]. En: diario Oficial. Julio,2012. Nro. 48.489. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012_pr004.html

COLOMBIA. CONGRESO DE COLOMBIA. Ley estatutaria 1581 (18,octubre,2012). Por la cual se dictan disposiciones generales para la protección de datos personales. 2012. [En línea]. En: diario Oficial. Octubre,2012. Nro. 48.587. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

COLOMBIA. CONTRALORÍA GENERAL DE COLOMBIA. Resolución Reglamentaria 202 (7,diciembre,2012). Por la cual se deroga la Resolución Reglamentaria 126 de 2011 y se crea el grupo de Laboratorio de Informática Forense (LIF). 2012. [En línea]. Disponible en: https://normativa.colpensiones.gov.co/colpens/docs/resolucion_contraloria_0202_2012.htm

COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Consejo Nacional De Policía Judicial. Manual Único de Policía Judicial. Versión N.2. [En línea]. [Consulta: octubre, 2021]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

COLOMBIA. MINISTERIO DE RELACIONES EXTERIORES DE COLOMBIA. 2020. Colombia se adhiere al Convenio de Budapest contra ciberdelincuencia. [En línea]. Disponible en: https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Evidencia Digital, Guía 13. 2016. [En línea]. [Fecha de Consulta: octubre 2021]. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

COLOBRAN HUGUET, Miquel, et al. Administración de sistemas operativos en red, Editorial UOC, 2008. [En línea] [Fecha de consulta: 25 de enero de 2020]. Disponible en:http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3206493

COMPELSON. [En línea]. 2021. Disponible en: https://forensic.manuals.mobiledit.com/MM/Camera-Ballistics.1809743974.html

COMPELSON. MOBILedit Forensic Express. All-in-one tool used to gather evidence from phones. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.mobiledit.com/forensic-express

COMPELSON. User Guide-MOBILedit Forensic Express. 2021. [En línea]. Disponible en : https://forensic.manuals.mobiledit.com /MM/Connection-wizard.1806663935.html

COMPELSON. [En línea]. 2021. Disponible en : https://forensic.manuals.mobiledit.com/MM/1821474845/qweqeq.png?inst-v=eb11f669-8c59-4e34-ad25-4caf68fef91e

COMPELSON. [En línea]. 2021. Disponible en : https://forensic.manuals.mobiledit.com/MM/Built-in-SIM-Cloning.2176712742.html

COMPELSON. [En línea]. 2021. Disponible en : https://forensic.manuals.mobiledit.com/MM/Data---Accounts.1809383545.html

COMPELSON. [En línea]. 2021. Disponible en : https://forensic.manuals.mobiledit.com/MM/Full-content-vs.-Specific-selection.1809809489.html

COMPELSON. [En línea]. 2021. Disponible en : https://forensic.manuals.mobiledit.com/MM/How-to-make-an-application-backup.1821474845.html

COMPELSON. [En línea]. 2021. Disponible en : https://forensic.manuals.mobiledit.com/MM/Import-data.1806467272.html

CONEXIÓN INVERSA. Forensics Power Tools (Listado de herramientas forenses). 2013. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html.

CONEXIÓN INVERSA. Forense en correos electrónicos. 2008. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: http://conexioninversa.blogspot.com/2008/11/forense-en-correo-electrnicos-outlook.html

CONEXIÓN INVERSA. Forensics con Volatility. 2009. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : http://conexioninversa.blogspot.com/2009/02/forensics-con-volatility.html

CONPILAR News. Las 10 herramientas forenses más conocidas que funcionan en linux. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://conpilar.es/las-10-herramientas-forenses-mas-conocidas-que-funcionan-en-linux/

CONSEJO DE EUROPA. Convenio Sobre la Ciberdelincuencia Budapest, 23.XI.2001. [En línea]. [Consultado: octubre 2021]. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

CONSEJO DE EUROPA. Convenio Sobre la Ciberdelincuencia del Consejo de Europa. Artículo 13. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

DMDE Software. About DMDE. 2020. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://dmde.com/

DIGITAL DETECTIVE GROUP Ltda. BLADE. 2021. [En línea]. [Fecha de consulta: 15 de octubre de 2021]. Disponible en: https://www.digital-detective.net/product/blade-professional-v1/

DIGITAL DETECTIVE GROUP Ltda. Creating Blade Data Recovery profiles. 2014. [En línea]. [Fecha de consulta: 25 de octubre de 2021]. Disponible en: https://kb.digitaldetective.net/display/Blade/Creating+Blade+Data+Recovery+Profiles

DIGITAL DETECTIVE GROUP. [En línea]. 2021. Disponible en: https://www.digital-detective.net/digital-forensic-software/blade-forensic-data-recovery/

DIGITOFORENSE, Investigación digital. Encase Forensic. 2021. [En línea]. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.digitoforense.cl/productos/encase-forensic/

ESCRIVÁ GASCÓ, Gema. Seguridad informática. 2013. [En línea]. [Fecha de consulta: febrero 2020]. Madrid, España: Macmillan Iberia, S.A. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=122.

ESCRIVÁ GASCÓ, Gema. Seguridad informática. 2013. [En línea]. [Fecha de consulta: febrero 2020]. Madrid, España: Macmillan Iberia, S.A. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=124.

ESET. Incidente de Twitter: empleados fueron engañados mediante phishing telefónico. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/08/03/incidente-seguridad-twitter-empleados-enganados-phishing-telefonico/

ESET. ESET SysInspector: Herramienta gratuita de diagnóstico de la PC. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.eset.com/co/soporte/diagnostico-de-pc-gratuito/

ESET. Xplico, Framework forense para el análisis de trafico de red. 2013. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.welivesecurity.com/la-es/2013/08/20/xplico-framework-forense-analisis-trafico-red/

ESET Welivesecurity. Uso de filtros en WireShark para detectar actividad maliciosa. 2013. [En línea] [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: http://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/

ESET Welivesecurity. Herramientas para el análisis dinámico de malware. 2011. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : http://www.welivesecurity.com/ la-es/2011/12/22/herramientas-analisis-dinamico-malware/

ESET. 5 grupos de ransomware con más impacto en América Latina en 2020. 2021. [En línea]. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.welivesecurity.com/la-es/infographics/grupos-ransomware-mas-impacto-america-latina-2020/

EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTE. Best Practice Manual for the Forensic Examination of Digital Technology. ENFSI-BPM-FIT-01. 2015. [En línea]. [Fecha de Consulta: marzo 2022]. Disponible en: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

FBI. Forensic Science Communications. 2000. [En línea]. [Fecha de consulta: 28 de septiembre 2021]. Disponible en: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

FILESEE. FileSee: A powerful All-In-One viewer. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : http://www.filesee.com/

FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Manual del sistema de Cadena de Custodia. 2018. [En línea]. [Fecha de Consulta: octubre 2021]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

FORENSIC Artifacts. Registry: MUICache. 2010. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : http://forensicartifacts.com/2010/08/registry-muicache

FREEVIEWER. Top Free Email Forensic Tools for Investigating Different Email Clients and Extensions. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://www.freeviewer.org/email-forensics/free-tools.html

GETDATA FORENSIC. About Mount Image Pro. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://getdataforensics.com/product/mount-image-pro/

GÓMEZ, Dany. Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. 2020. Revista Ratio Juris. 15(.30) 220-240. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://doi-org.bibliotecavirtual.unad.edu.co/10.24142/raju.v15n30a11

HARD2BIT. Análisis de malware: enfoque y caso práctico, Seguridad informática. 2013. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/

HERJAVEC GROUP. Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

HERNANDO Sergio. Xplico. Una herramienta de análisis forense de tráfico de red. 2009. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: http://www.sahw.com/wp/ archivos/2009/09/01/xplico-una-herramienta-de-analisis-forense-de-trafico-de-red/

HEX-RAYS. A powerful disassembler and a versatile debugger. 2022. [En línea]. Disponible en https://hex-rays.com/ida-pro/

INCOGNITO FORENSIC Foundation. List of 15 most Powerful Forensic Tools. 2019. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://ifflab.org/list-of-15-most-powerful-forensic-tools/

IFORENSEColombia. Teletrabajo y la seguridad de la información; cómo prepararse. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.informaticaforense.com.co/teletrabajo-y-seguridad-de-la-informacion-como-prepararse/

INOVTEC. Consultoría y Soluciones HI-TEC. Oxygen Forensic. s.f. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.inovtec.com.mx/ analisis-forense-en-telefonos-celulares/

INTERPOL. Global Guidelines for Digital Forensics Laboratories. 2019. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

INTERPOL. Análisis Forense Digital. s.f. [En línea]. Disponible en : https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

IT Master Mag. Los ciberataques que marcaron el 2020. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.itmastersmag.com/noticias-analisis/los-ciberataques-que-marcaron-el-2020/

ISO. ISO/IEC 27037:2012. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.iso.org/standard/44381.html

JOHANSEN Gerald. Digital Forensic and Incident Response. 2017. [En línea]. Disponible en: https://search-ebscohostcom.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1562684&lang=es&site=eds-live&scope=site. ISBN. 978-1-78728-868-3

KANELLIS, Panagiotis et al. Digital Crime and Forensic Science in Cyberspace. 2006. IG Global. [En línea]. ISBN 1-59140-874-1

KALITOOLS. RegRipper Package Description. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://tools.kali.org/forensics/regripper

KENT Karen, et al. SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 2006. [En línea]. Disponible en : https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875

LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta marzo de 2022]. Paracuellos de Jarama, Madrid, RA-MA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=246

LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. Paracuellos de Jarama, Madrid, RA-MA Editorial. 2014. [En línea]. [Fecha de consulta 23 de Agosto de 2021]. Disponible en: https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=19.

LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=310.

LÁZARO DOMÍNGUEZ, Francisco. Introducción a la informática forense. 2014. [En línea]. Madrid, RA-MA Editorial. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=116.

LORENZO, José. Mejores herramientas gratuitas de informática forenses. 2020. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

LÓPEZ DELGADO, Miguel. Análisis Forense Digital. 2007. [En Línea]. [Fecha de consulta: octubre, 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

LOPEZ JAVIER et al. Securing Information and Communications Systems: Principies, Technologies and Applications. 2008. [En línea]. ISBN 9781596932289. Disponible en : https://search-ebscohostcom.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=284257&lang=es&site=eds-live&scope=site.

MALIN Cameron et al. Malware Forensics Field Guide for Windows Systems. Digital Forensics Field Guides. 2012. [En línea]. ISBN 978-1-59749-472-4

MCAFEE. FileInsight. 2022. [En línea]. Disponible en: https://www.mcafee.com/enterprise/es-es/downloads/free-tools/fileInsight.html

MINTIC. Evidencia Digital, Guía No 13. 2016. [En línea]. [Consulta: octubre, 2021] Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

MSAB. Qué es XRY. Introducción a la tecnología forense móvil y extracciones de teléfonos móviles. [En línea]. [Fecha de consulta: octubre 2021] Disponible en: https://www.msab.com/download/product_sheets/spanish_product_sheets/XRY_What-isXRY_ES.pdf

MSAB. Diez razones para elegir XRY sobre otro software forense móvil. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.msab.com/product/xry-extract/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST. Computer Forensic Tools & Techniques Catalog. 2022. [En línea]. Disponible en: https://toolcatalog.nist.gov/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST. Framework for Improving Critical Infrastructure Cybersecurity. V1.1. 2018. [En línea]. Disponible en : https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

NETWITNESS. NETWITNESS. 2022. [En línea]. Disponible en: https://www.netwitness.com/en-us/tools/netwitness-platform-demo/

NIST. SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. 2006. [En línea]. [Fecha de Consulta: septiembre 2021] Disponible en: https://csrc.nist.gov/publications/detail/sp/800-86/final

NIST. SP 800-44 versión 2, Guideline on Securing Public Web Servers. 2007. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en : https://csrc.nist.gov/publications/detail/sp/800-44/version-2/final

OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE. Reportes finales. 2020. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://observatoriociberseguridad.org/#/final-report

OEA y BID. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe, 2020. [En línea]. [Fecha de consulta: 20 de octubre de 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

ONDATA Internacional. Encase Forensic Software: Características y funciones. 2021. [En línea]. [Fecha de consulta: octubre 2021] Disponible en : https://www.ondata.es/recuperar/encase_forensic.html.

OPENTEXT. OpenText Encase Forensic overview. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://security.opentext.com/encase-forensic

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Habilidades de Análisis Forense Informático. s.f. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : http://www.oas.org/juridico/english/cyb_mex_forense.pdf

OXYGEN FORENSIC. Oxygen Forensic, Detective Features. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective.

OXYGEN FORENSIC. Oxygen Forensic, Características Kit. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.oxygen-forensic.com/es/products/oxygen-forensic-kit

OXYGEN FORENSICS. Oxygen Forensic Detective. 2022. [En línea]. [Fecha de consulta: marzo de 2022]. Disponible en: https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective

Plaso(log2timeline). Welcome to the Plaso Documentation. s.f. [En línea]. Disponible en: https://plaso.readthedocs.io/en/latest/

PASSMARK SOFTWARE. OSFMount. 2021.[En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://www.osforensics.com/tools/mount-disk-images.html

PASSMARK Software. Verify and Match Files. 2022. [En línea]. Fecha de consulta: marzo 2022]. Disponible en: https://www.osforensics.com/verify-and-match-files.html

PASSMARK Software. Drive Imaging. 2022. [En línea]. [Fecha de consulta: marzo, 2022]. Disponible en: https://www.osforensics.com/drive-imaging.html

PORTAFOLIO. Informática forense: el reto es que llegue a las empresas. 2018. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://www.portafolio.co/negocios/empresas/informatica-forense-el-reto-es-que-llegue-a-las-empresas-513432

PORTAFOLIO. Se duplicaron los ciberataques en 2020. 2021 [En línea]. [Fecha de consulta: marzo, 2022]. Disponible en: https://www.portafolio.co/economia/se-duplicaron-los-ciberataques-en-2020-549548

Publicaciones SEMANA S.A. Marzo 3 de 1957. La máquina que cambió al país. 2022. [En línea]. Disponible en: https://www.semana.com/especiales/articulo/marzo-1957-brla-maquina-cambio-pais/65917-3/

QUICKHASH. User Manual. 2020. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.quickhash-gui.org/download/user-manual/

SAAVEDRA, R. informática forense y teletrabajo en tiempos de virus. 2020. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.redseguridad.com/especialidades-tic/informaticaforense-y-teletrabajo-en-tiempos-de-virus_20201103.html

SANS. SIFT Workstation. 2022. [En línea]. [Fecha de consulta: marzo 2022]. Disponible en: https://sans.org/tools/sift-workstation/

SEGURIDAD Y REDES. Análisis de Red con Wireshark – Interpretando los Datos. 2008. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/

SERRANO LEYVA, Carmen. Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373/16528

SHIRVASTA Gulshan; SHARMA Kavita y DWIVEDI Akansha. Forensic Computing Models: Techical Overview. 2012. [En línea]. Disponible en: https://www.researchgate.net/publication/242524844_FORENSIC_COMPUTING_MODELS_TECHNICAL_OVERVIEW

SIKORSKI Michael y Honing Andrew. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2012. [En línea]. ISBN 1-593272901.

SYSTOOLS. Email Forensic Software. 2021. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en: https://www.systoolsgroup.com/email-forensics.html

SYSTOOLS. SysTools MBOX Viewer Pro. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.systoolsgroup.com/mbox-viewer-pro.html

SOFTONIC. Microsoft Process Monitor. S.f. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : http://microsoft-process-monitor.softonic.com/

SOURCEFORGE. Quick Guide. 2013. [En línea]. [Fecha de consulta: septiembre 2021]. Disponible en : http://liveview.sourceforge.net/guide.html

SPLUNK. Features. Dive into your security data. 2022. [En línea]. Disponible en : https://www.splunk.com/en_us/cyber-security/forensics-and-investigation.html

TAHIRI SOUFIANE. Mastering Mobile Forensics. [En línea]. 2016. Disponible en: https://www.packtpub.com/product/mastering-mobile-forensics/9781785287817

TÉRMENS, Miquel. Preservación digital. 2014. Editorial UOC. [En línea] [Fecha de consulta: octubre 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/57604?page=20

TENORSHARE. Tenorshare UltData. 2022. [En línea]. [Fecha de consulta: marzo de 2022] Disponible en: https://www.tenorshare.net/ads/iphone-data-retrieve.html

TREJO, Carlos; DOMENECH, Gustavo y ORTIZ Karla. Revista pensamiento penal, La seguridad jurídica frente a los delitos informáticos. 2016. [En línea]. [Fecha de Consulta: septiembre 2021]. Disponible en: http://www.pensamientopenal.com.ar/doctrina/44051-seguridad-juridica-frente-delitos-informaticos

UNODC. s.f. Ciberespionaje. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.unodc.org/e4j/es/cybercrime/module-14/keyissues/cyberespionage.html

U.S. IMMIGRATION AND CUSTOMS ENFORCERMENT. Policía Nacional de Colombia e ICE abren laboratorio forense dedicado a la explotación infantil. 2018. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.ice.gov/es/news/releases/policia-nacional-de-colombia-e-ice-abren-laboratorio-forense-dedicado-0

UYANA Mónica, Escobar Milton. Propuesta de Diseño de un Área Informática Forense para un Equipo de Respuestas ante Incidentes de Seguridad Informáticos (CSIRT). s.f. [En línea]. Disponible en:http://repositorio.espe.edu.ec:8080/bitstream/21000/8123/1/AC-GSR-ESPE-047639.pdf

UYANA Mónica. Propuesta de Diseño de un Área Informática Forense para un Equipo de Respuestas ante Incidentes de Seguridad Informáticos (CSIRT). 2014. [En línea]. Disponible en : http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE -047639.pdf

WIRESHARK Team. About Wireshark. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en : https://www.wireshark.org/

WIRESHARK Team. Wireshark 3.4.9. Release Notes. 2021. [En línea]. [Fecha de consulta: octubre 2021]. Disponible en: https://www.wireshark.org/docs/relnotes/wireshark-3.4.9.html

WIRESHARK Team. Wireshark Training. s.f. [En línea]. Disponible en: https://www.wireshark.org/docs

WONDERSHARE. Recoverit Data Recovery.2021. [En línea]. Disponible en : https://recoverit.wondershare.es/data-recovery.html

WONDERSHARE. Recupera los datos perdidos en Mac como un profesional. 2021. [En línea]. Disponible en : https://recoverit.wondershare.es/data-recovery-mac.html

WONDERSHARE. Recoverit-Software de recuperación de datos Gratis V9.7. 2021. [En línea]. Disponible en : https://recoverit.wondershare.es/data-recovery-free.html

WONDERSHARE. Wondershare Recoverit 9.0. [En línea]. Disponible en : https://recoverit.wondershare.es/support/recoverit-9-updates.html

XPLICO. About Xplico. 2021. [En línea]. Disponible en : https://www.xplico.org/about.

XPLICO. Xplico System. 2021. [En línea]. Disponible en : https://www.xplico.org/about.

ANEXOS

Anexo A. Sustentación.
https://drive.google.com/file/d/1r8ELKxx6hUg9Qv95B2zl5DSm9xYoKhCh/view?usp=sharing

Anexo B. RAE.

RESUMEN ANALITICO RAE	
Fecha de Realización	26/10/2021
Programa	Especialización Seguridad Informática
Línea de Investigación	Gestión de Sistemas, administración de tecnologías, Informática forense digital.
Título	HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL ORIENTADAS A INFRAESTRUCTURAS TI COMO MEDIO DE INVESTIGACIÓN EN DELITOS INFORMÁTICOS
Autor	Rada Jiménez Kelly Katherine
Palabras Claves	Informática forense digital, análisis forense digital, herramientas forenses, software forense, evidencia digital.
Descripción	El tema de la monografía se relaciona con el análisis digital forense y la informática forense en relación con el uso de las herramientas de software forense en los procesos de aseguramiento y tratamiento de la evidencia digital, así como la funcionalidad de estas en las organizaciones para la investigación de incidentes informáticos y gestión en la seguridad informática.
Fuentes bibliográficas destacadas	A continuación, se relaciona las fuentes bibliográficas más importantes: ARNEDO, Pedro. 2014. Herramientas de Análisis Forense y su Aplicabilidad en la Investigación de Delitos Informáticos. Universidad Internacional de La Rioja. Valledupar. CASTILLO, L., Bohada, J. Informática Forense en Colombia. Grupo de Investigación MUISCA. Revista Ciencia, Innovación y Tecnología p.86/Voll.II/2015. Fundación Universitaria Juan de Castellanos, Tunja, Colombia. [En línea]Disponible en : https://www.jdc.edu.co/revistas/index.php/rciyt/article /view/113/102 CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. 2009. [En línea]Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

	FISCALÍA GENERAL DE LA NACIÓN DE COLOMBIA. Manual de procedimiento para la cadena de custodia. [En línea]. Disponible en:https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf GÓMEZ D. Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. 2020. Revista Ratio Juris. 15(.30) 220-240 Disponible en : https://doi-org.bibliotecavirtual.unad.edu.co/10.24142/raju.v15n30a11 ISO/IEC 27037:2012. [En línea]. 2012. Disponible en: https://www.iso.org/standard/44381.html LÁZARO DOMÍNGUEZ, F. Introducción a la informática forense.2014. Paracuellos de Jarama, Madrid, RA-MA Editorial. Disponible en : https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/106250?page=19. MINTIC. Guía No. 13, Seguridad y privacidad de la Información, Evidencia Digital. 2016. [En línea] Disponible en :https://mintic.gov.co/gestionti/615/articles5482_G13_Evidencia_Digital.pdf
Contenido del documento	La monografía que se presenta como trabajo de grado para obtener el título de Especialista en Seguridad informática de la Universidad Nacional Abierta y A Distancia UDR Barrancabermeja tiene como propósito definir la importancia del análisis forense digital en las infraestructuras tecnológicas en Colombia, describir las categorías de las herramientas de software forense y promover el uso de software forense para complementar la gestión de seguridad informática y respuesta a incidentes.
Conceptos adquiridos	Evidencia digital, análisis forense digital, cadena de custodia, software forense, delitos informáticos, protección de datos, validez jurídica, integridad de datos, funciones hash en investigaciones forense, privacidad de datos, fuente de datos.
Conclusiones:	
• Se planteó la importancia de implementar el análisis forense digital en las infraestructuras TI organizacionales para verificar el impacto del incidente informático, realizar la interpretación de incidentes informáticos, ejecutar una metodología apropiada de acuerdo con las características del incidente informático y el uso de herramientas de software forense adecuadas para cada procedimiento realizado en una investigación forense.	

- En este documento, se concluye que existe gran variedad de herramientas de software forenses de tipo comercial y gratuito que permiten a los profesionales que se dedican al análisis forense digital, elegir las soluciones de software más adecuadas según el criterio de factores como la utilidad, velocidad y eficacia en el procesamiento de datos en las fuentes de datos disponibles para realizar las investigaciones digitales de forma completa y exhaustiva, en búsqueda de información relevante en donde los hallazgos sea evidencia digital válida ante tribunales y autoridades competentes.

- Se especificó que todo proceso llevado a cabo por un profesional TI para la realización del análisis forense digital en las organizaciones actualmente, requiere que el profesional investigador informático debe contar con conocimientos especializados en temas jurídicos relacionados con la regulación de la labor que realiza, certificaciones relacionadas a la investigación forense digital, experiencia en los procedimientos técnicos para el manejo y tratamiento de la evidencia digital, habilidades en el manejo y comprensión de las capacidades de las soluciones de software forenses para el uso adecuado y pertinente en las investigaciones forense.

- Se presentaron los procedimientos técnicos para el tratamiento de la evidencia digital y las características de las fases establecidas para llevar a cabo el análisis forense digital en Colombia, con la finalidad de presentar como se lleva a cabo actualmente los procesos de recolección y tratamiento para obtener de evidencia digital válida e integra en las investigaciones forenses informáticas.

- Con el avance de la tecnología en los procesos de negocio de las organizaciones, la implementación del trabajo remoto por la situación actual de pandemia por Covid-19 y la tendencia creciente de delitos informáticos e incidentes de seguridad se presentó la necesidad en las organizaciones de tomar medidas que refuercen las investigaciones corporativas internas y estrategias de seguridad que requieren del proceso de análisis forense digital como solución de gestión.

- Se evaluó ocho herramientas de software forense seleccionadas demostrando el funcionamiento, las características y el alcance en la recuperación de información en escenarios propuestos en los sistemas TI y así proponer el uso e implementación de cada una de ellas para realizar investigaciones forenses digitales y respuestas a incidentes en las organizaciones

AUTOR: Kelly Katherine Rada Jimenez