APLICACIÓN DE LAS FASES DEL ANÁLISIS FORENSE DIGITAL SIMULANDO UNA ESCENA DEL CRIMEN DENOMINADA “EL HACKER ASESINO”.

APPLICATION OF THE PHASES OF DIGITAL FORENSIC ANALYSIS SIMULATING A CRIME SCENE CALLED "THE HACKER KILLER”.

Jhon Fredy Pardo Salazar
jfpardos01@libertadores.edu.co

Jorge Luis Vitola
jlvitola01@libertadores.edu.co

Héctor Manuel Herrera Herrera
hmherrerah@libertadores.edu.co

Luis Alexis Plazas
laplazag@libertadores.edu.co

RESUMEN

En este artículo se hará una descripción de un caso hipotético, donde se aplican las fases del análisis forense digital, mostrando al lector, el uso y aplicación de técnicas en informática forense y criminalística, con el fin de hallar el que, quien, cómo, cuándo y dónde sucedieron los hechos del caso.

Esto permite tener un contexto amplio y claro en el tratamiento de la evidencia digital, logrando su identificación, adquisición y aseguramiento para presentación de resultados idóneos, en una investigación de tipo penal.

Finalmente se describirá a través del caso simulado, las fases de procesamiento de las evidencias, teniendo como principio garantizar la mismidad, autenticidad y seguridad de la información contenida en los dispositivos electrónicos encontrados en la escena del crimen, propiciando un análisis forense exhaustivo para generar hipótesis y relacionar la conducta con el autor del delito.

Palabras claves: cibercrimen, penal, evidencia digital, informática forense, criminalística.

ABSTRACT

This article will describe a hypothetical case, where the phases of digital forensic analysis are applied, showing the use and application to the reader and the application of techniques in computer forensics and criminalistics, in order to find what, who, how, when and where the facts of the case happened.
This allows to have a broad and clear context in the treatment of digital evidence, achieving its identification, acquisition and securing for presentation of suitable results, in a criminal investigation.
Finally, the phases of digital evidence processing will be described through the simulated case, having as a principle to guarantee the sameness, authenticity and security of the information contained in the electronic devices found at the crime scene, promoting a thorough forensic analysis to generate hypotheses and relate the behavior with the perpetrator of the crime.

Keywords: cybercrime, criminal, digital evidence, computer forensics, criminalistics.

1. INTRODUCCIÓN

El aumento exponencial de las actividades delictivas en Colombia derivas del inminente avance tecnológico permiten visualizar un alto grado de hallar evidencia digital en los lugares donde ocurren actividades delictivas y se utilizan medios tecnológicos para almacenar digitalmente la información, estos datos con un debido y apropiado manejo de técnicas y procedimientos de informática forense, pueden aportar a la función probatoria u orientativa para la individualización y juzgamiento del autor del delito.

Todos estos avances tecnológicos producidos año tras año, ponen a prueba la limitación y escasez de recursos tanto físicos como técnicos para hacer frente y socavar el aumento de delitos en Colombia, en especial atención, a la hora de enfrentar la posibilidad de encontrar, analizar y entregar una evidencia digital valedera dentro de un contexto penal, disciplinario y/o administrativo, en esta situación la informática forense es péndulo de gran importancia, nombrada como la ciencia adecuada para la obtención, preservación y análisis de evidencia en escenarios donde se encuentren dispositivos electrónicos.

No obstante, el desafío de la investigación digital parece quedar atrás ante al aumento de las nuevas tecnologías, entiéndase este en ejemplo con la aparición de toda clase de dispositivos, el aumento de capacidad de almacenamiento de los mismos, las nuevas formas de generar cibercrimen y la falta de legislación en Colombia son obstáculos para el informático forense en su labor diaria.

En este escrito se realiza la simulación de un caso (hipotético) que permitirá hacer uso de las fases del análisis forense digital, permitiendo llevar de la ficción al mundo real, las técnicas utilizadas para el esclarecimiento de un hecho delictivo.

Pregunta de Investigación

¿Son suficientes las fases del análisis forense digital para el esclarecimiento de una actividad delictiva en Colombia?

Objetivo General

Aplicar las fases del análisis forense digital de acuerdo con el proceso metodológico de identificar, recolectar, analizar y presentar evidencia digital con el fin de aportar un informe que apoye al esclarecimiento de una conducta de tipo penal.

Objetivos Específicos

● Identificar el caso mediante la metodología de la informática forense utilizada para la recolección de evidencia digital.

● Analizar a través de técnicas en informática forense y criminalística, las evidencias encontradas y responder las siguientes preguntas investigativas: ¿Qué?, ¿Quién?, ¿cómo?, ¿cuándo? y ¿Dónde?

● Proponer una metodología de buenas prácticas y acciones ante la actuación del primer responsable en casos relacionados con evidencia digital en Colombia.

ALCANCE

A partir del presente artículo se busca aplicar las fases del análisis forense digital en un caso hipotético, utilizando metodologías de buenas prácticas para llevar a cabo la investigación, con técnicas criminalísticas e informática forense; permitiendo generar resultados de valor probatorio en un estrado judicial en Colombia.

2. REFERENTES TEÓRICOS

Antecedentes

La investigación criminalística es una función de la policía, que cada día cobra mayor vigencia en el ámbito mundial para ocupar el verdadero sitial que le corresponde como ciencia, en la determinación de la existencia del delito y la averiguación del delincuente. (lopez calvo, 2003)

Por ejemplo, en investigaciones que día a día se dificultan, por el crecimiento de toda clase de dispositivos electrónicos, el aumento en los volúmenes de información que deben recopilarse, almacenarse y analizarse, el surgimiento de nuevos paradigmas de crímenes (cibercrimen), la falta de legislación que cobije todo tipo de investigación cuando sobrepasa los límites de las jurisdicciones legales, la débil capacidad del poder judicial para entender, interpretar y valorar la evidencia digital. (Jose, 2021)

De ahí que los medios electrónicos como las memorias flash USB y otros dispositivos de almacenamiento, son fuentes donde se archiva todo contenido compartido y creado en los medios tecnológicos (celular, computador, tablets, entre otros), en las que se recogen y se registran las actividades, gustos, tendencias, imágenes y escritos de las personas, quedando al descubierto la sensibilidad y fragilidad de la información que pueden llegar a contener los medios digitales, puesto que en el almacenamiento se conserva el registro de archivos personales y públicos. (Enríquez, 2020)

Hoy, muchas de las huellas y evidencias, cuya recolección es necesaria para demostrar la comisión de un determinado delito, están en soporte digital, por lo que la informática ha permeado casi todos los entornos: la mayoría de los documentos, fotos, videos y controles de recursos de todo tipo se han adaptado al ámbito tecnológico contemporáneo. (Otros, 2020)

De igual manera, la evolución tecnológica propició que la informática forense avanzara a gran escala, a causa de la mutación del accionar delincuencial y criminal, por lo cual el investigador y perito, debe estar en capacidad de afrontar cualquier escenario criminal y una de las maneras en que pueda lograrlo es mediante buenas prácticas en los procedimientos que realice, más en el tema de preservación y recolección de evidencia, por tal razón y en conclusión es necesario aprender a utilizar los recursos necesarios con los que se cuenten y que estos sean de fácil acceso utilizando buenas prácticas para no incurrir en errores y sean válidos en cualquier estrado judicial. (Calderon, 2021)

Por esta razón, todas las técnicas utilizadas para la recogida y análisis de evidencias digitales deben estar respaldadas por una buena metodología científica y documentadas en un protocolo de actuación, que recoja tanto los aspectos técnicos de la informática como los aspectos legales que se derivan de su peculiaridad forense. (Francisca Rodríguez, 2011)

Sin dejar atrás la importancia de la identificación de datos volátiles y no volátiles que son un aspecto vital de la informática forense. La validación y examen de la evidencia de volatilidad ayuda a “contar la historia” soportada en el estado de la evidencia en el momento de la recopilación. En los casos donde el código malicioso reside en la memoria, se puede contar una historia completa; de lo contrario, la volatilidad hace que se pierda parte de dicha historia por falta de datos o pruebas. (Bidgoli, 2006)

En este sentido para una correcta investigación, es necesario comprender e interpretar el análisis forense digital, por lo cual Miguel López indica que es “un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial” (p.10), dentro de los cuales se pueden encontrar delitos como: (homicidios, fraude financiero, terrorismo, pornografía infantil (grooming), piratería de software, hacking, spam, entre otros). (Delgado, 2007)

Términos y Definiciones

Axiom: Es una herramienta forense digital confiable y probada en el campo que le permite recuperar datos eliminados e investigar evidencia digital desde cualquier tipo de dispositivo digital. y analizar evidencia de fuentes informáticas, en la nube y móviles. (magnetforensics, s.f.)

Autopsy: Es una herramienta de código abierto que, permite identificar y analizar sobre imágenes forense de pruebas que se hallan recolectado en una escena del crimen. (Autopsy)Criminología: Es una ciencia que se centra en el cómo y por qué de los fenómenos delictivos y la reacción social frente a estos. (Santiago Redondo, 2014)

Datos Volátiles: Datos de un determinado sistema que se pierden una vez dicho sistema es reiniciado o apagado. (esgeeks, s.f.)

Elementos Materiales Probatorios: Huellas, rastros, manchas, residuos, vestigios, dinero, Armas, instrumentos, el mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax y similares, dejados por la ejecución de la actividad delictiva. (Republica C. d., Función Pública, 2004)

Evidencia Digital: La evidencia digital es el conjunto de datos en formato digital (código binario), como archivos con contenido, metadatos, conexiones de tráfico en la red, discos duros, tarjetas o memorias USB que puedan ser utilizados por los tribunales para esclarecer unos hechos. (Lemontech, 2021)

Forensic USB 3.0 Bridge: Bloqueador de escritura portátil que permite la adquisición forense de dispositivos USB 3.0. (Opentext, s.f.)

FTK Forensic Toolkit de AccessData: Es una herramienta para la recolección de imagen forense de los equipos de cómputo. (Exterro, s.f.)

MOBILedit Forensic Express: Es el extractor de evidencia de teléfonos móviles del celular y cloud para procedimientos investigativos. (mobiledit, s.f.)

OSForensics: herramienta que permite usar Hash Sets para identificar rápidamente archivos seguros conocidos. (PassMark, s.f.)

Marco Legal

1. Ley 1581 de 2012 - Tratamiento de datos personales (Republica S. d.)
2. Ley 1273 de 2009 - Delitos Informáticos. (Republica C. d., 2009)
3. ISO/IEC 27037 DE 2012 - Tecnología de la información. Técnicas de seguridad Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales. (ISO/IEC, ISO/IEC)
4. ISO/IEC 27042 DE 2015 - Tecnología de la información – técnicas de seguridad – lineamientos para el análisis e interpretación de evidencia digital. (ISO/IEC, ISO/IEC)
5. NIST SP800-86 - Instituto nacional de estándares y tecnología – (guía para la integración de técnicas forenses a la respuesta a incidentes. (NIST)
6. Guía seguridad y privacidad de la información (Mintic, 2016)
7. Manual de Cadena de Custodia. (Nación, 2018)
8. Investigación forense digital en entidades del Estado colombiano: Acercamiento a la Ley
9. 1952 de 2019 – Delitos Informáticos. (Darling Stella Solano, 2019)

3. METODOLOGÍA

Para el desarrollo de este proyecto se tiene en cuenta la creación de un caso (hipotético) que llevado de la ficción a la realidad, dará un contexto claro y entendible de la manera cómo actuar a la hora de una investigación criminal que sea conexa a la evidencia digital, se asume una perspectiva interpretativa partiendo del hecho para planificar el comportamiento más adecuado desde una parte metódica y práctica, según la experiencia adquirida en las áreas de investigación criminal, criminalística e informática forense, Se inscribe en el enfoque cualitativo porque pretende profundizar en el análisis, más que generalizar. (Gómez, 2018)

Se estructura mediante un proceso de cuatro fases ilustradas en el siguiente esquema

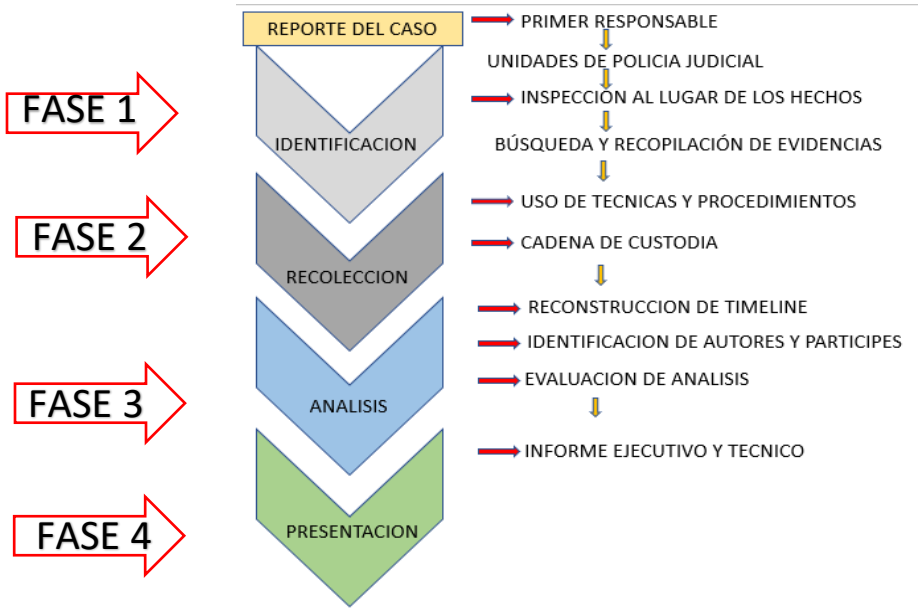

Figura 1 *Metodología del análisis forense digital Fuente: Autor*

Nota. Las fases permiten un adecuado y metódico proceso con el tratamiento de la evidencia digital.

4. ANALISIS Y RESULTADOS

Simulación del caso: El hacker asesino
Información preliminar:

Reporte del caso

Información preliminar:

El día 15 de diciembre del año 2022, se recibe información vía telefónica por parte de una ciudadanía, indicando un fuerte ruido al parecer un disparo de arma, en el apartamento 401, edificio santo VIC, localidad de chapinero en Bogotá, de igual manera observo salir del lugar a una persona de género masculino, que huyo en un vehículo particular color gris.

Unidades designadas para la verificación del lugar:

Primer responsable: Patrulla de vigilancia (cuadrante): acuden de manera inmediata, llegan al lugar y observan una persona de género femenino, arrojada en el suelo sin signos vitales con una herida de arma de fuego en la cabeza y observan unos dispositivos electrónicos alrededor.

Figura 2 Escena del crimen *Fuente: Autor*

Buenas prácticas y acciones

1. Aislar y proteger la escena, utilizar cinta de acordonamiento, vehículos, motocicletas institucionales o personal uniformado.
2. Verificar la seguridad del lugar, realizar observancia sobre objetos extraños, transeúntes u otro aspecto de importancia que genere sospechas.
3. Solicitar apoyo de otras unidades si es necesario
4. No alterar los elementos materiales probatorios y evidencia física

Al observar dispositivos electrónicos aplicar la siguiente metodología

1. Cuando se trate de equipos de cómputo se debe seguir la regla de oro, si está encendido se deja encendido y procurar que no se bloquee, si esta apagado dejarlo en ese estado.
2. Cuando se trate de equipos de telefonía celular, se debe colocar el dispositivo en modo avión, de igual manera evitar el bloqueo de solicitud de patrón o pin de seguridad.

Nota: es posible que se pueda hacer uso de las exploraciones dactiloscópicas con el fin de hallar huellas latentes que pueden ser del posible autor del delito.

Fase 1: Identificación

Es el proceso mediante el cual se analiza la posibilidad de hallar, buscar o dar el reconocimiento de una prueba digital, mediante unos procedimientos establecidos; ligando esta etapa a la ciencia de la criminalística sería el espacio propicio para proceder a inspeccionar un lugar de los hechos, este se define como una acción táctica que se realiza

siempre que sea posible a los efectos de obtener huellas o evidencias por las cuales se explique qué aconteció, así como identificar tanto a las víctimas como a los victimarios, con el fin de desplegar un proceso investigativo, se logra observar que es una fase de gran relevancia siendo el inicio a una investigación positiva.

"El principio de intercambio de Locard, referente a cualquier escena del crimen indica que, en cualquier contacto en esta, supone un intercambio de evidencias ya que el criminal deja rastros o huellas del ilícito o se las lleva consigo, este principio permite a los criminalísticos o investigadores establecer un cierto porcentaje de éxito en el inicio de la investigación".

Unidades de Policía Judicial:

La central de radio reporta el caso y son designadas las patrullas (Pluton 1) del grupo de investigación de homicidios y (Coral 2) del grupo de investigación criminalística.

Pluton 1: funcionarios de policía judicial encargados de liderar la investigación
Coral 2: funcionarios expertos en estudios o áreas de la criminalística, encargados de identificar, proteger y procesar una escena del crimen, aplicando técnicas y procedimientos con el fin de hallar, recolectar y custodiar los elementos materiales probatorios que sirven para el esclarecimiento de los hechos.

Inspección al lugar de los hechos:

Las unidades de Criminalística reciben el lugar por parte de las unidades de Policía (cuadrante), mediante el informe de actuación del primer responsable, que indica lo referente con la protección, observación e información obtenida de los hechos.

Ingresan al lugar, definiendo que en todo el procesamiento se hace uso de las técnicas de la fotografía forense, documentando el paso a paso de lo actuado y se sigue la siguiente metodología.

1. Identificar un punto focal inicial para efectuar una correcta observación y análisis el lugar de los hechos.
2. Establecer las medidas de protección del personal, verificando zonas de evacuación.
3. Se establece el método de búsqueda (espiral).

Búsqueda y recopilación de evidencias

1. Identificar elementos materiales probatorios: pelos, fibras, cabellos, uñas, saliva, semen, sangre, medios de almacenamiento digital y los dispositivos de procesamiento con datos o información potenciales para la investigación.

2. Iniciar el proceso de numeración consecutiva de cada hallazgo

Fase 2: Recolección

Después de haber identificado las evidencias, el personal inicia el aseguramiento físico de los elementos materiales probatorios, se deben seguir los protocolos y estándares internacionales.

Uso de técnicas y procedimientos: Se hallan los siguientes elementos materiales probatorios.

Figura 3 *E.M.P 1: (01) Cuerpo sin vida, género femenino Fuente: Autor*

El equipo de criminalística realiza el procedimiento de inspección técnica a cadáver, aplicando las técnicas y procedimientos establecidos en la guía inspección al lugar de los hechos y/o al cadáver de la fiscalía general de la nación.

Figura 4 *E.M.P 2: (01) computador portátil marca HP modelo HP 15-da1073, serial CND918D Fuente: Autor*

Se trata de un equipo de cómputo que se encuentra encendido, por esta razón aplica el siguiente procedimiento:

Inserta una memoria USB al computador previamente bloqueada contra escritura por hardware utilizando el dispositivo Tableau Forensic USB 3.0, se ejecuta el programa FTK Imager versión 4.7.1.2 y aplica obtención de datos volátiles, mediante la opción capture memory, esta evidencia será enmarcada para el caso como el EMP 4.

Figura 5 *E.M.P 3: (01) Equipo terminal móvil, marca Iphone, modelo AJXR9, color gris. Fuente: Autor*

Se trata de un teléfono celular, marca Samsung Galaxy modelo A04, color gris, sin número de IMEI no visible, el personal de criminalística realiza una observación externa al dispositivo, observa un patrón de huella latente y deciden realizar una exploración dactiloscópica sobre el mismo, se obtiene un fragmento de huella, que para el caso será denominada como el E.M.P 5, para finalizar el procedimiento se realiza embalaje de los elementos materiales probatorios de acuerdo a los parámetros del manual cadena de custodia.

Cadena de custodia

Es el procedimiento que permite el aseguramiento y confidencialidad de los elementos materiales probatorios (E.M.P), mediante el control de la cronología de movimiento de los mismos.

Para este caso las unidades de criminalísticas custodian los E.M.P y realizan los siguientes pasos:

- El E.M.P 1 - (Cuerpo sin vida): es entregado a Medicina Legal (Colombia), con el fin de que se determine las causas y manera de la muerte.
- Los E.M.P 2 - (computador), EMP 3 - (celular) y EMP 4 - (datos volátiles) son entregados al investigador líder para que haga las solicitudes ante el laboratorio de Informática forense para aplicación de procedimientos y análisis de la Información.
- El E.M.P 5 - (fragmento dactilar), es remitido ante el laboratorio de dactiloscopia con el fin de realizar técnicas de revelado y trasplante de fragmentos de origen lofoscopico.

Fase 3: Análisis

Es un proceso metodológico que permite la reconstrucción de los hechos, verificando cada dato disponible, incluye la creación de una línea de tiempo, que enlaza una cadena de eventos o acontecimientos relevantes en un hecho determinado.
Nos permite visualizar las circunstancias de tiempo, modo y lugar producto del ilícito, respondiendo las preguntas más importantes en una investigación (quien, como, cuando, donde Y ¿Por qué?).

Para este caso, los lideres de la investigación presentan los elementos materiales probatorios ante el laboratorio de informática forense con su debida cadena de custodia, solicitando lo siguiente:

E.M.P 2: Realizar imagen forense, análisis de evidencia digital, presentación de reporte detallado con reconstrucción de línea de tiempo.

E.M.P 3: Extracción de información del dispositivo móvil, obtener registro de contactos, mensajes, imágenes, videos, conversaciones, historial de chat, redes sociales, en especial realizar una línea de tiempo en relación con los hechos ocurridos el día 15 de diciembre del año 2022.

EMP 4: Realizar análisis de memoria volátil, entregar informe ejecutivo y técnico.

Entorno de trabajo:

Laboratorio de informática forense dotado con dispositivos y herramientas apropiadas para la generación de imágenes forenses, verificación de memoria volátil y extracción de información de dispositivos celulares que permiten un análisis forense detallado y eficaz.

Equipos e instrumentos empleados

- Equipo forense, marca Sony Vaio
- Una cámara fotográfica marca Canon, referencia ELPH 180, 20 mega pixeles
- Software FTK Imager, versión 4.7.1.2

- Software Mobiledit, versión 10.1.0.25985
- Software axiom versión 61
- Software autopsy, versión 4.20.0
- Software Fred, versión 9.1
- Software thumderbird, versión 102.11.2
- Software Volatility versión 2.6

Principios técnicos utilizados.

1. Principio de Disponibilidad: Cuando la información es accesible a los usuarios autorizados en el momento de requerirla.
2. Principio de no Repudiación: Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en dicho evento.
3. Principio de Integridad: Cuando se garantiza que la información es exacta y completa, no se modifica desde el momento de su creación y se almacena en un formato que asegura la exactitud de la información original.
4. Observancia: Cuando se lleva el registro de los eventos importantes

Actividades realizadas en el laboratorio de informática forense:

Para la evidencia número 2, (01) computador portátil marca HP modelo HP 15-da1073, serial CND918D, el perito procede a realizar lo siguiente:

1. Realiza la fijación fotográfica del elemento material de prueba
2. Retira el disco duro del equipo, obteniendo un disco de estado solido SSD, marca KingStone, serial SDFGWR4A, capacidad de almacenamiento 500 GB. Procede a la creación de la imagen forense
3. Conecta el disco de estado sólido al adaptador Hard Disk Box y al bloqueador contra escritura marca Tableau Forensic.
4. Conecta el bloqueador forense al equipo de cómputo, el sistema operativo reconoce el dispositivo conectado en la unidad D: Ejecuta el software FTK Imager, utiliza las opciones Create Disk Image y physical drive, posteriormente escoge la unidad D:, estableciendo el formato E01 y la información de la evidencia (Imagen 2), se establece el destino final de la imagen forense con el nombre Imagen_Forense_Evidencia, es fragmentada para 1 archivo y tipo de comprensión 6, clic en start e inicia el procedimiento.

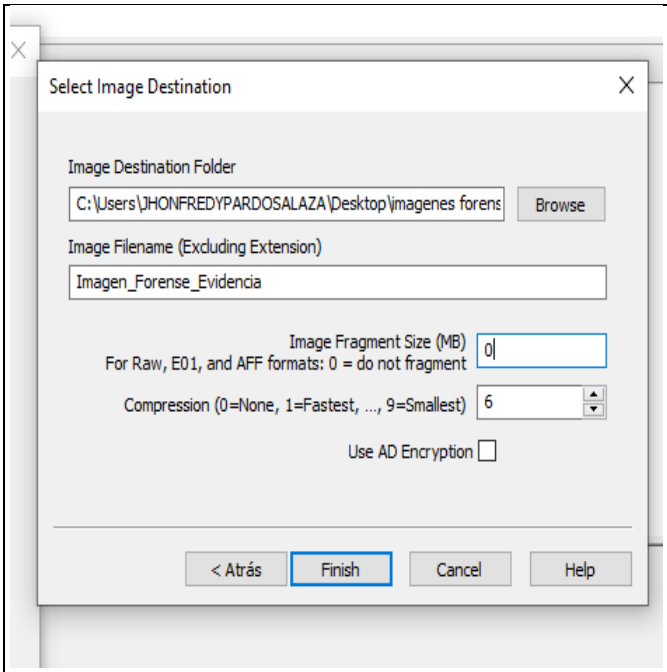

Figura 6 *Fragmentación imagen forense Fuente: Autor*

Como resultado del procedimiento, se puede verificar la creación de la imagen forense física en la unidad de destino seleccionada junto con el archivo de verificación hash e información del caso (imagen 5), posteriormente se procede a agregar la imagen forense en el programa FTK Imager verificando el contenido (figura 8).

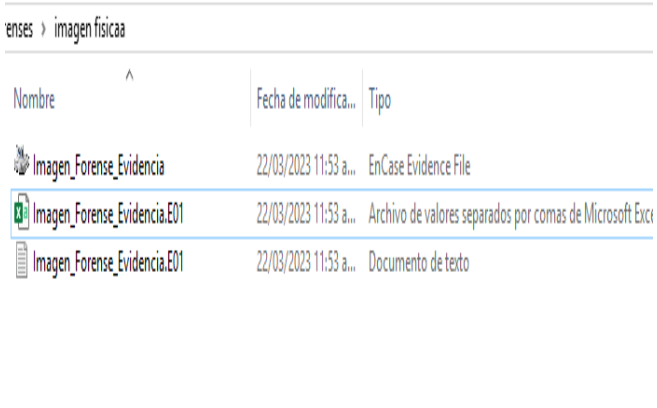

Figura 7 *Verificación imagen forense Fuente: Autor*

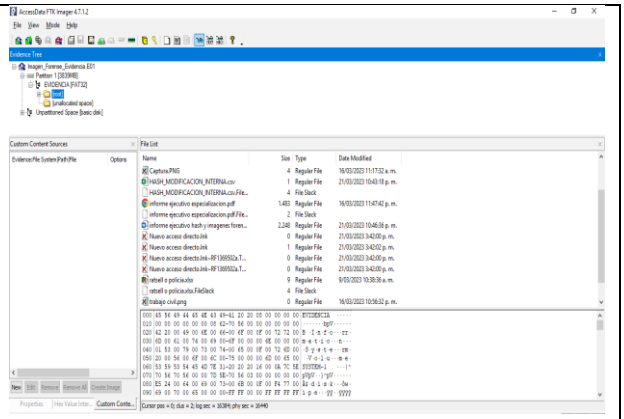

Figura 8 *Imagen forense Fuente: Autor*

Para la evidencia número 3, (01) Equipo terminal móvil, marca Iphone, modelo AJXR9, color gris, el perito procede a realizar la fijación fotográfica del elemento material de prueba

y sigue los siguientes pasos para realizar la extracción de la información del dispositivo.

1. El celular es puesto en modo avión
2. Se realiza verificación del dispositivo, se habilita la opción de modo desarrollador, depuración por USB y permanecer activo.
3. Se ejecuta el programa mobiledit y se conecta el dispositivo a la estación forense, se procede a realizar una extracción lógica de la información, la cual es almacenada en un disco duro externo, previamente esterilizado.
4. Se utiliza un duplicador forense con el fin de realizar una copia exacta bit a bit de la información, copia que será destinada para el análisis de la información, permitiendo conservar la integridad de la información principal.
5. Se realiza verificación y creación de valores de identificación única HASH.
6. El disco duro original es marcado, embalado técnicamente, rotulado y sometido a cadena de custodia.

Fase 4: Informe

Se utilizan las herramientas de software (Axiom Process y Autopsy), para la indexación de los datos o información contenidos en la imagen forense del equipo de cómputo y el dispositivo celular.

Como resultado de la indexación de la información en el Software Axiom process, se obtiene un archivo con extensión (.axn), que posteriormente es ejecutado con el Software Axiom Examiner.

Se incorporan las siguientes búsquedas de palabras claves en las dos herramientas, con el fin de minimizar la búsqueda y encontrar pistas que permitan el esclarecimiento de los hechos.

Malware	Virus	Matar
hacker	Dinero	troyano
Ojo con la policía	Dirección IP	policía

Tabla 1 de palabras claves Fuente: Autor

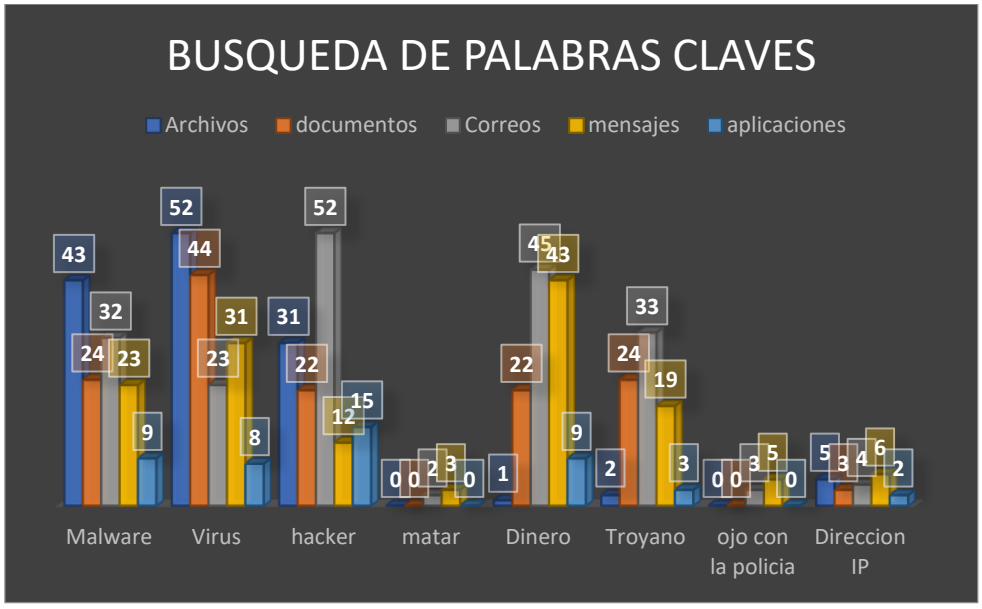

Figura 9 *Búsqueda palabras claves Fuente: Autor*

Para la evidencia número 4, (01) disco externo marca adata color negro serial 1m4321841339 de capacidad 1 TB, que contiene el volcado de memoria RAM del equipo de cómputo relacionado en la evidencia número 2, se procede a utilizar el software Volatility, cargando el archivo con extensión (.mem) y se utilizan los siguientes comandos.
Identificación de procesos en el sistema.

- volatility -f memory.img --profile=WinXPSP2x86
  pslist Svcscan: El resultado muestra el ID del proceso de cada servicio (si está activo y si pertenece a un proceso del usuario)
- volatility -f /root/test/win7_trial_64bit.raw --profile=Win7SP0x64 svcscan

Posteriormente se realiza un análisis forense, verificando la información de cada dato relacionado en las palabras claves y la memoria volátil; se pueden establecer varios parámetros importantes en la investigación.

Reconstrucción de línea de tiempo:

1. Se realizo el hallazgo del software malicioso denominado svchost.exe, usado para robar contraseñas en otros equipos; de igual forma se observó él envió por medio de correo electrónico a aproximadamente 32 personas.
2. Se encontraron documentos guías para la creación de software malicioso y phishing.
3. Se analizo la conversación con su pareja sentimental, visualizando una amenaza de muerte, toda vez que esta persona pretendía denunciarlo por las actividades ilícitas a las que se dedicaba.

4. Tenía procesos activos utilizando una máquina virtual, ejecutando la herramienta Zphisher; utilizada para capturar los datos de usuario y contraseña de redes sociales.
5. Tenía accesos remotos a otros dispositivos, utilizando la herramienta Droidjack; que es un troyano RAT (administración remota de herramientas), la cual había sido embebida en documentos con extensión (.pdf) y enviada por correos a aproximadamente a 134 personas.
6. Se logro identificar plenamente a la persona, mediante la búsqueda de la huella en la base de datos de la Registraduría Nacional del estado civil de Colombia.

Identificación de autores y participes:

Los anteriores hallazgos e hipótesis permitieron determinar que se trataba de una persona que cometía actividades delictivas usando sistemas informáticos, aprovechando conocimientos en el uso y manejo de diferentes sistemas operativos y software especializado.

Presentación de informe

La presentación se debe realizar mediante un informe técnico y ejecutivo, que debe seguir la siguiente estructura:

1. Línea de tiempo.
2. Evidencia digital.
3. Solicitudes específicas.
4. Objetivos.
5. Descripción y explicación de los principios y procedimientos técnicos utilizados.
6. Marco legal.
7. Instrumentos empleados y estado de mantenimiento.
8. Procedimientos empleados y resultados.
9. Interpretación de resultados / conclusiones.
10. Anexos.

Mediante la anterior estructura, permite al perito informática, presentar un resultado completo y de fácil entendimiento, para ser verificado por las partes actoras en estrados judiciales.

5. CONCLUSIONES

En este artículo, se aplicaron las fases del análisis forense digital, permitiendo correlacionar una escena del crimen (simulada), a cada una de estas etapas; se identificaron y recolectaron las evidencias mediante un proceso metodológico y practico que al ser analizadas permitió a los investigadores generar hipótesis y relacionar actividades del autor del delito.

Las metodologías utilizadas son entregadas de acuerdo con la experiencia adquirida en esta área, una propuesta de valor que al ser verificada puede ser aplicada por los funcionarios que investiguen este tipo de delitos o en su defecto encuentren algún tipo de evidencia en un lugar de los hechos.

Por estas razones en la recolección de evidencias no se pasó por alto ningún medio electrónico hallado en el sitio, para los investigadores forense los hallazgos permitieron el esclarecimiento del crimen, el acceso y los recursos utilizados fueron soportados dentro del marco legal colombiano. Por otra parte, los protocolos de ética y las recomendaciones de buenas prácticas en la recolección de datos y evidencias como elementos materiales probatorios fueron aceptadas en los estrados judiciales.

Como resultado de este ejercicio se tomaron las fases del análisis forense realizado en cada una de ellas, basados en los tres (3) principios de confidencialidad, integridad y disponibilidad de la información.

REFERENCIAS

Acosta, J. C. (2012). LIDERAZGO Y EMPRENDIMIENTO INNOVADOR EN NUEVAS EMPRESAS DE BASE TECNOLÓGICA.UN ESTUDIO DE CASOS BASADO EN UN ENFOQUE DE GESTIÓN DEL CONOCIMIENTO. *Real*, 5-13.

Ajzen, I., & Fishbein, M. (s.f.). The Influence of Attitudes on Behavior.

Autopsy. (s.f.). *Esgeeks.* Obtenido de https://esgeeks.com/autopsy-guia-analisis-forense-windows/

Bidgoli, H. (2006). *Handbook of information security: Key concepts, infrastructure, standards, and protocols.* John Wiley & Sons.

Calderon, C. A. (2021). *Buenas prácticas en informática forense, para el procesamiento de evidencia digital o información electrónicamente almacenada.* Hemeroteca Universidad Nacional.

Darling Stella Solano, M. a. (2019). *Policia Nacional.* Obtenido de https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/1698/2008

Delgado, M. L. (2007). *Análisis Forense Digital.*

Diez, S. (2014). La Actitud Conductual en las Intenciones Emprendedoras. 2.

Elizundia, M. E. (2015). Desempeño de nuevos negocios: perspectiva de género: Nueva performance empresarial: perspectiva de género. *ScienceDirect*.

Enríquez, L. C.-A.-M. (2020). *Nuevas Tecnologias En La Investigacion Criminal.* Cali.

esgeeks. (s.f.). *esgeeks.com*. Obtenido de https://esgeeks.com/forense-extraccion-datos-volatiles/
Exterro. (s.f.). *Exterro.com*. Obtenido de https://www.exterro.com/ftk-imager
Francisca Rodríguez, A. D. (2011). *La Informatica Forense: El Rstro Digital del Crimen.*
Gómez, L. S. (2018). Evidencia Digital en la Investigacion Penal.
ISO/IEC. (s.f.). *ISO/IEC.* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en
ISO/IEC. (s.f.). *ISO/IEC.* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en
Jose, H. O. (2021). *Crimen, Cibercrimen y Análisis Forense Informático.* Bogota - Colombia: Temis.
Lemontech. (11 de 08 de 2021). *Evidencias digitales: significado, objetivo y tratamiento*. Obtenido de https://blog.lemontech.com/evidencias-digitales/
lopez calvo, P. y. (2003). *Investigacion Criminal y Criminalística.* Bogota: Ed Temis,.
magnetforensics. (s.f.). *Magnetforensics.com*. Obtenido de https://support.magnetforensics.com/s/cyber-software-and-downloads?language=en_US
Mendes, L., & Santos, M. (2014). FACTORES QUE INFLUYEN EN EL USO DEL CONTENIDO GENERADO POR EL USUARIO EN ENINTERNET. *redalyc*, 607-625.
Mintic. (2016). *Mintic.gov.co.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-150505_G13_Evidencia_Digital.pdf
mobiledit. (s.f.). *www.mobiledit.com*. Obtenido de https://www.mobiledit.com/forensic-express/esp
Mora, R. (s.f.). ESTUDIO DE ACTITUDES EMPRENDEDORAS CON PROFESIONALES QUE CREARON EMPRESA: Study of Entrepreneurial Attitudes of Professionals who Create their own Companies. 70-83.
Moreno, J. (2013). ANALISIS DE LOS FACTORES QUE INFLUYEN EN LA INTENCIÓN EMPRENDEDORA DE LOS ESTUDIANTES UNIVERSITARIOS. *Reista digital de investigación en docencia*, 7.
Nación, F. G. (2018). *Fiscalía General de la Nación.* Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf
NIST. (s.f.). *NIST.* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
Opentext. (s.f.). *Security.Opentext.com*. Obtenido de https://security.opentext.com/tableau/hardware/details/t8u
Otros, V. N.-J.-E. (2020). *Informatíca Criminalistica; Una Especialidad en Desarrollo.* España: Dialnet - Articulo de Revista.
PassMark. (s.f.). *www.osforensics.com*. Obtenido de https://www.osforensics.com/products/index.php
Republica, C. d. (2009). *Función Pública.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492
Republica, S. d. (s.f.). *Senado de la Republica .* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
Rodríguez , A. (2009). Nuevas perspectivas para entender el emprendimiento empresarial.
Rueda, I., Sánchez, L., Herrero, Á., Blanco, B., & Fernández, A. (2013). ¿Existen niveles adecuados de formación y financiación que incentiven la intención emprendedora? Are the existing levels of training and access to finance enough to encourage entrepreneurial intention? *FIR, FAEDPYME International Review* .
Ruiz, M., Sanz, I., & Fuentes, M. (2015). Investigaciones Europeas de Dirección y Economía de la Empresa. *ScienceDirect*, 47-54.
Santiago Redondo, V. G. (2014). *Principios de Criminológía.* Revista Española de Investigacion Criminológia.

Valencia, A., Montoya, I., & Montoya, A. (2016). Intención emprendedora en estudiantes universitarios: Un estudio bibliométrico. *OmniaScience*, 883.