Marco metodológico para el análisis forense al navegador web Internet Explorer

Jose Manuel Cruz Cuellar
Universidad Piloto de Colombia
josemcruz17@hotmail.com

Resumen—En el presente artículo se busca plantear una propuesta metodológica para realizar análisis forense al navegador web Internet Explorer, con base en las mejores prácticas de análisis forenses en el mundo, entendiendo que no existe una única metodología estándar que permita recolectar y manejar evidencia digital dado un incidente de seguridad. Por tanto, se consolida en este documento el mejor procedimiento posible para analizar de manera forense los navegadores web, y así poder seguir un proceso coherente y ordenado de tal forma que se obtengan resultados confiables y similares cada vez que se aplique la metodología propuesta, pretendiendo que con las pruebas digitales analizadas se identifique a los responsables del incidente y ayuden a esclarecer lo sucedido y por supuesto puedan ser admitidas en un proceso judicial. Además se presenta un caso pequeño pero practico sobre un delito informático donde se pondrá a prueba el marco metodológico desarrollado en el presente artículo.

Palabras clave—Análisis forenses, evidencia digital, Internet Explorer, metodología, navegador web.

Abstract—In the present paper, seeks to present a methodological proposal to make forensic analysis to the web browser Internet Explorer, based on the best practices of forensic analysis in the world, understanding that there is no a only standard methodology that allows to collect and manage digital evidence given a security incident. Thus, consolidates in this document the best possible procedure for analyze forensically web browsers, and so to have a coherent and orderly process, such that is obtained reliable and similar results each time that is applied the proposed methodology, pretending than with digital evidence analyzed is identified to the responsible of the incident and help clarify what happened and of course they can be admitted in a prosecution. A small but practical case is presented on a cyber crime which will test the methodological framework developed in this article.

Keywords—Forensic analysis, digital evidence, Internet Explorer, methodology, web browser.

I. INTRODUCCIÓN

El uso y la evolución de las Tecnologías de Información y la Comunicación (TIC) han proporcionado nuevas y mejores oportunidades a las empresas para que estas estén innovando y puedan sostenerse frente a la competencia, transformando los procesos de intercambio y producción de información. Es importante mencionar, que el uso indebido de las mismas por personas o empresas inescrupulosas que ejecutan ataques en contra de la integridad de los sistemas informáticos, genera caos en los sectores tanto privados como públicos, en especial en el sector comercial y bancario, debido a que estas se debilitan institucionalmente y pierden credibilidad al momento de presentarse un incidente de seguridad, a tal punto que algunas de ellas deben ceder espacios a sus competidores o en el peor de los casos desaparecer, teniendo en cuenta que los medios de comunicación (cuarto poder) están pendientes de este tipo de sectores.

Por este motivo, se desarrollan nuevas herramientas y se abren nuevos campos con el fin de descubrir a los autores del delito y armar el rompecabezas de la escena del crimen digital, con base a las evidencias dejadas por el transgresor, las cuales muchas veces quedan almacenadas en forma digital en los equipos informáticos. Sin embargo, hay un problema, ya que los computadores guardan la información de manera tal que no puede ser recuperada como prueba utilizando medios comunes, sino por personal capacitado en lo forense los cuales están dotados de herramientas idóneas para combatir este tipo de infracciones.

El personal forense debe acudir a las mejores prácticas internacionales para adelantar un análisis forense digital, teniendo en cuenta de asegurar la evidencia digital encontrada en los diferentes sistemas informáticos y tecnológicos presentes en la escena del crimen, ya que la generación significativa de esta es lo más importante en una investigación forense, para esclarecer lo sucedido y tenga validez jurídica ante un juez o tribunal de justicia.

Para que la evidencia digital tenga la propiedad de admisibilidad debe cumplir con 4 criterios que le permitan a un juez validar o no las pruebas digitales, siendo estas [1]:

- Autenticidad: Es entendida como aquella característica legal, que muestra la no alterabilidad de los medios originales y que la evidencia ha sido generada y registrada en el lugar de los hechos.
- Confiabilidad: Se dice que los elementos probatorios son confiables cuando vienen de fuentes que son creíbles y verificables, es decir, una prueba digital seria confiable, si el sistema que la produjo no ha sido violado y estuviese en correcto funcionamiento al momento de recibir, almacenar o generar la prueba.
- Suficiencia: Una prueba es suficiente si ésta es completa.
- Conformidad por las leyes y reglas de la administración de justicia: Este último criterio hace alusión a que las evidencias digitales, deben acogerse a los requisitos enunciados en nuestros códigos de procedimiento y el resto de las disposiciones legales de nuestro ordenamiento. Tales leyes y reglas están contempladas en el artículo 178 del Código de

Procedimiento Civil y el artículo 235 del Código de Procedimiento Penal y concordantes.

La evidencia digital es la materia prima para los investigadores, por eso es indispensable contar con un procedimiento estándar bien definido que permita manejar la evidencia de forma adecuada, pero el problema está en que no se cuenta con un sola metodología de análisis forense, incluyendo para navegadores web.

Antes de elaborar una guía para el análisis forense al navegador web Internet Explorer, es importante tener en cuenta varios factores como lo son los estándares de investigación forense más importantes en la actualidad alrededor del mundo, las herramientas que servirán para analizar los rastros que deja un navegador en un computador, conceptos de informática forense y conocer los principios de admisibilidad de la evidencia. Además de lo anterior, es fundamental entender el funcionamiento del navegador web Internet Explorer, sus características y los archivos que genera y almacena, y que tienen valor en una investigación formal y adecuada.

Este artículo empieza con una pequeña introducción de lo que es la informática forense, para seguir luego con la recopilación de las mejores prácticas dentro de la disciplina de las directrices forenses, sentado de esta manera las bases para la metodología que se propone en este documento relacionado con el análisis forense en el navegador web Internet Explorer.

El objetivo de esta investigación es proponer y aplicar un marco metodológico para análisis forenses al navegador web, para tal objetivo haremos uso de procedimientos de la informática forense, entendimiento del navegador web y por supuesto de herramientas forenses destinadas para la adquisición y análisis de información presentes en el navegador. Además, es una propuesta que ayudara a complementar y profundizar en temas relacionados con el análisis forense en Internet Explorer.

II. GUÍAS PARA ANÁLISIS FORENSES

Es normal que en las empresas reporten vulnerabilidades en sistemas de información, dadas las fallas bien sea tecnológicas, humanas o procedimentales sobre las infraestructuras de computación, ofreciendo un escenario perfecto para que los intrusos informáticos se aprovechen de estas. Estos intrusos tienen diferentes estrategias, habilidades y motivaciones que desconsuelan al cuerpo de TI de las empresas, puesto que las modalidades de ataque cambian de un caso a otro. Hay que decir también, que los intrusos que provienen desde adentro de las empresas generan más peligro dado que tienen las credenciales para acceder a la información, pero el número de intrusiones que provienen de afuera son mayores debido a que los intrusos tienen todo el tiempo del caso para lanzar un ataque. [2]

En la actualidad las empresas están invirtiendo más recursos en seguridad informática que permitan mitigar los riesgos, desembolsando grandes sumas de dinero al área de TI para que gestionen estos recursos, implementando como controles antivirus, firewall, backup o antispam, siendo estos los más adoptados. Sin embargo, estas medidas no son suficientes, ya que las empresas siguen reportando incidentes, que para el caso de Colombia en los últimos 12 meses fueron infección por malware, falta de disponibilidad y phishing los que más se presentaron [3]. Además de los anteriores incidentes, las empresas de hoy en día presentan problemas de privacidad, robo de información confidencial o espionaje o fraude, a través del uso indebido de las tecnologías de información. De esta manera cuando la seguridad de la empresa ha sido vulnerada, la informática forense entra a jugar un papel importante.

El FBI ha definido la informática forense como la ciencia de adquirir, preservar, recuperar y presentar datos que han sido procesados electrónicamente y almacenados en soportes informáticos [4]. Esta hace su aparición en 1984 cuando la organización antes nombrada y otras agencias policiales comenzaron a desarrollar programas para examinar las evidencias de los computadores, luego a finales de los años 90, el FBI observó que las pruebas digitales tenían el mismo potencial para combatir a los delincuentes que un examen de ADN. Por eso se creó la IOCE (Internacional Organization of Computer Evidence), la cual desarrolló una serie de principios aplicados a los procedimientos en el uso de las pruebas digitales para que pudieran ser utilizadas en juzgados de otros países [5]:

- En la manipulación de la evidencia digital, las acciones tomadas no deben alterar dicha prueba.
- Cuando sea necesario que una persona acceda a la evidencia digital original, debe estar capacitada idóneamente en el área.
- Toda actividad relacionada con la incautación, acceso, almacenamiento o la transferencia de la evidencia debe estar documentada, preservada y disponible para su estudio.
- Cada persona es responsable de todas las acciones tomadas frente a la evidencia mientras esta se encuentra en su poder.
- Cualquier agencia encargada de la recogida, acceso, almacenamiento o trasferencia de la evidencia digital debe regirse por estos principios.

La finalidad de la informática forense, consiste en realizar un proceso de búsqueda minuciosa a través de todos los medios informáticos implicados, para reconstruir los acontecimientos que tuvieron lugar desde el momento cuando el sistema estuvo en su estado integro hasta el momento cuando se vio comprometido el mismo, identificando autores del delito, posibles alteraciones, manipulaciones, fugas o destrucciones de datos. Pero también se habla de la utilización de la informática forense como medida preventiva, mediante la práctica de diversas pruebas técnicas, auditando los mecanismos de protección instalados como seguridad a los sistemas de información.

A pesar que no existe un solo procedimiento genérico para análisis forense todos buscan la misma finalidad, que es la de identificar evidencia digital para ser utilizada dentro de una investigación. Todas las guías presentan una serie de etapas para recuperar la mayor de cantidad de información con el propósito de asistir en la reconstrucción de eventos. Hay

diferentes tipos de planteamientos, que varían según el criterio de la institución y/o persona que definen la guía. Para la elaboración de la guía propuesta para el presente artículo se tuvieron en cuenta dos guías existentes a nivel mundial de mejores prácticas en análisis forense.

A. Examen forense de la evidencia digital: Una guía para el cumplimiento de la ley.

Esta guía ofrece cinco pasos básicos para llevar a cabo un análisis forense a un computador, los cuales se detallan a continuación [6]:

1. Desarrollo de políticas y procedimientos: Los departamentos deben crear políticas y procedimientos para el funcionamiento o establecimiento de una unidad de análisis forense computacional. Dentro de este primer paso se debe establecer la misión, el personal que laborará en la unidad, se deben tener en cuenta consideraciones administrativas como por ejemplo, la concesión de las licencias de software y los recursos económicos para la adquisición del software y hardware a utilizar. Además debe diligenciar la solicitud de los servicios forenses y tener un procedimiento técnico para examinar evidencia digital, este procedimiento debe ser documentado y debe estar probado para que los resultados obtenidos sean confiables.

2. Evaluación de la evidencia: Se debe hacer una valoración del caso para determinar el curso de acción. Tal valoración consiste en identificar la naturaleza del hardware y software, detallar las circunstancias que rodean el caso, revisar la autorización legal para acceder a realizar el análisis forense y establecer las posibles pruebas solicitadas.

2.1. Evaluación del caso: El equipo de análisis forense antes de proceder con la adquisición de la evidencia digital, tiene que considerar lo siguiente:

- Discutir si otros procesos forenses necesitan realizarse en la escena (por ejemplo, análisis de ADN, huellas dactilares, etc.).
- Determinar el equipo necesario.
- Priorizar el orden en que la evidencia debe ser adquirida.
- Determinar el potencial de evidencia que se podría encontrar (por ejemplo, fotografías, documentos, registros financieros, etc.).
- Tener en cuenta la relevancia de los componentes periféricos, ya que componentes como impresoras o escáneres, no son de competencia del personal de análisis forense.
- Evaluar los niveles de habilidad de los usuarios de los equipos comprometidos (por ejemplo, esteganografia, cifrado, etc.).

2.2. Consideraciones del lugar: En algunas ocasiones, el examinador solo podrá tener la oportunidad de hacer lo siguiente en el lugar de los hechos:

- Entrevista con el administrador y los usuarios del sistema.
- Determinar las redes presentes.
- Evaluar las condiciones generales del caso.
- Identificar el tipo de computadores.

2.3. Evaluación del sitio para el procesamiento de la evidencia: Es preferible realizar un examen en un entorno controlado, como un área de trabajo o laboratorio dedicado al análisis forense. Para evaluar el sitio se podría considerar lo siguiente:

- El tiempo necesario en el lugar para llevar a cabo la recuperación de la evidencia.
- La logística y preocupaciones del personal forense asociado con el despliegue a largo plazo.
- La idoneidad de los equipos y los recursos del sitio de examen.

2.4. Consideraciones legales: Tener en cuenta las leyes relacionadas con una investigación forense para no infringir ninguna de ella y que las pruebas examinadas pueda ser validas en un proceso legal. También considerar el alcance de búsqueda por parte del cuerpo forense.

2.5. Valoración de la evidencia: Se debe considerar otros aspectos antes de recolectar la evidencia como:

- Determinar la condición de la evidencia para así mismo embalarla, transportarla o almacenarla.
- Determinar cómo documentar las pruebas (por ejemplo, con fotografías, notas, etc.).
- Evaluar las ubicaciones de almacenamiento para tener en cuenta las interferencias electromagnéticas que pueden llegar a afectar los datos que sirven como evidencia.

3. Adquisición de la evidencia: La evidencia digital es frágil y puede ser dañada, destruida o alterada por la manipulación o examen inadecuado. Es por eso que para protegerla y preservarla se deben tener ciertas precauciones, tomando en cuenta los siguientes pasos:

- Documentar el hardware y software utilizado por el equipo forense para atender el caso.
- Verificar el funcionamiento correcto de las herramientas forenses (hardware y software) antes de emplearlas en la escena o en el laboratorio.
- Desmontar el computador a ser examinado para permitir el acceso físico a los dispositivos de almacenamientos.
- Identificar, documentar y desconectar los dispositivos de almacenamientos que necesitan ser adquiridos para recuperar sus datos, estos pueden ser internos y/o externos.
- Asegurar que los dispositivos de almacenamientos del examinador se encuentran esterilizados para no contaminar la evidencia.
- Verificar la adquisición exitosa de los datos mediante una huella digital que permita establecer que la copia y los datos originales son idénticos.

4. Examen de la evidencia: Las personas que realizan el examen de la evidencia digital deben estar capacitadas y la adquisición de esta debió hacerse mediante procedimientos forenses

aceptados. El examen no debe realizarse sobre la evidencia original sino sobre copias realizadas en el paso anterior. Al llevar a cabo el examen se deben considerar lo siguiente:

4.1. Preparación: Se debe planificar cual va a ser el directorio de trabajo donde se almacenarían los datos recogidos.

4.2. Extracción: Existe 2 tipos de extracción: la física y la lógica.

- Extracción física: En este paso se identifica y recupera los datos de toda la unidad física sin tener en cuenta el sistema de archivos.
- Extracción lógica: La extracción de los datos de la unidad de forma lógica se basa en el sistema de archivos. Este tipo de extracción permite revelar la estructura de directorios, nombres y atributos de los archivos.

4.3. Análisis de los datos extraídos: El análisis es el proceso de interpretar los datos extraídos para determinar su significado.

4.4. Conclusión: Los resultados obtenidos con los diversos tipos de análisis deben verse en conjunto para poder sacar una conclusión completa.

5. Documentación y presentación del informe: El examinador es el responsable de informar sus hallazgos y conclusiones luego del análisis a la evidencia digital. La documentación es un proceso continuo que se realiza en cada una de las fases de la metodología. Esta debe ser completa, comprensible y exacta.

B. Guía para las mejores prácticas en el examen forense de tecnología digital.

La IOCE publicó esta guía que contiene un procedimiento de computación forense. También los principios generales, personal, herramientas, entre otros temas relacionados con el proceso forense de evidencia digital. A continuación se explicara el manejo de la evidencia digital según la IOCE [7]:

1. Localización y recuperación de la evidencia digital en la escena: El personal forense puede acudir a la escena o puede dar consejos a los demás asistentes para que recuperen los datos. Teniendo en cuenta lo siguiente:

1.1 Precauciones contra la contaminación:

- Precauciones de no contaminar objetos que pueden ser útiles para otros exámenes (por ejemplo, huellas dactilares y ADN).
- Todos los equipos de almacenamiento y los contenedores de transporte deben ser nuevos o limpiados a fondo antes de su uso.
- Se debe tener cuidado cuando se esté manipulando la evidencia de que no hayan sustancias potencialmente peligrosas, pues de ser así se debe documentar.
- Tener precaución con las emisiones electromagnéticas que generan algunos dispositivos como los teléfonos celulares y PDA, pues una mala manipulación de estos podría alterar la evidencia. Se recomienda utilizar bolsas faraday o un recipiente vacío de pintura con su respectiva tapa para aislar las emisiones.

1.2. Buscando en la escena:

- Todos los dispositivos que sean objeto de estudio, deben ser protegidos para reducir el riesgo de pérdida, daño o alteración considerando que esta es frágil.
- En los procedimientos de búsqueda y obtención de la evidencia es pertinente que los sospechosos y los testigos se mantengan lejos del material electrónico.
- En la escena se debe buscar de forma exhaustiva y sistemática, orientado a aquellas áreas donde sería más probable encontrar objetos con carácter probatorio.

1.3. Recolección de la evidencia:

- En lo posible, los elementos recuperados en la escena deben ser examinados en un espacio de trabajo forense como un laboratorio y no el lugar de los hechos.
- Es importante que los objetos incautados para el examen forense se conserven de forma segura luego de las prácticas realizadas en la escena.

1.4. Embalaje, etiquetado y documentación:

- Todos los objetos que puedan aportar pruebas deben ser embalados y sellados tan pronto se toman. Además no se deben volver abrir hasta llegar al laboratorio.
- Es indispensable documentar el momento de la incautación de los objetos de la escena ya sea del sospechoso o de la víctima, describiendo la ubicación exacta de los objetos recuperados. También es útil elaborar un croquis de la ubicación y fotografiar la escena como un recordatorio de los hechos.
- La evidencia digital debe transportarse con mucho cuidado para evitar daños físicos, vibraciones, campos magnéticos, temperaturas extremas o humedad.

2. Examen de la evidencia digital: Todos los objetos que son sometidos a examen deben ser revisados, a fin de que su integridad no se haya afectado durante el embalaje o transporte. En esta fase los analistas o examinadores deben utilizar una serie de herramientas y técnicas que ofrezcan el mayor potencial para la localización e identificación de información relevante.

Aparte de los hallazgos generados en el transcurso del examen, existen otros registros tales como: fotografías, notas de observaciones, documentación de herramientas utilizadas (hardware y software), entrevistas, registros sobre el movimiento de la evidencia, detalles de los elementos que se presentan al laboratorio, etc., dando de esta manera soporte a los hallazgos encontrados durante el examen en el laboratorio.

3. Evaluación e interpretación: Existen varias maneras de informar los resultados de un examen digital según la IOCE: el informe técnico, la opinión del investigador y la opinión valorativa.

4. Presentación de la prueba escrita: El objetivo del informe es suministrar al lector toda la información relevante de la investigación de una forma clara, sin ambigüedades,

concisa y estructurada, para que el lector asimile la información lo más fácil posible.

III. MARCO METODOLÓGICO PARA EL ANÁLISIS FORENSE AL NAVEGADOR WEB INTERNET EXPLORER.

Lo más importante en una investigación forense es proteger la evidencia digital, considerando que esta es volátil y se le debe garantizar su integridad para llegar a conclusiones asertivas y exactas y pueda ser determinante en un caso judicial. Teniendo en cuenta lo anterior, es importante seguir un procedimiento estándar como los nombrados en el capítulo anterior que asegure la adquisición y análisis de la evidencia digital con el fin de reconstruir la secuencia temporal del ataque, determinar cómo se realizó el ataque, evaluar el impacto causado al sistema, identificar el autor del incidente, etc. Además de las dos guías expuestas como mejores prácticas en análisis forense, se tuvieron en cuenta otros estándares, generando con base en estos y otros elementos, un marco metodológico para la investigación forense al navegador web Internet Explorer.

En este capítulo del artículo, se presenta la propuesta del marco metodológico encaminado a realizar investigaciones forenses al navegador web Internet Explorer. El marco metodológico consta de cuatro fases: preparación, adquisición de datos, análisis de datos y presentación de resultados. Luego de la realización de la metodología forense, esta será aplicada a un escenario simulando un incidente con el propósito de validarla.

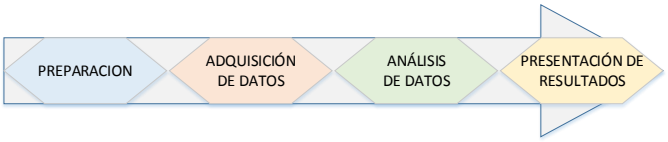

Fig. 1 Metodología propuesta por El autor.

A. Fase de preparación

La fase de preparación es la primera fase que se debe realizar en una investigación forense al navegador web Internet Explorer. Este proceso incluye asegurar y evaluar la escena, documentar la escena, una investigación preliminar, las herramientas a utilizar, definir el equipo forense y la autorización para proceder con la investigación.

1. Asegurar y evaluar la escena: El primero en responder ante un incidente es el oficial de seguridad de la organización, este debe identificar visualmente todas las posibles pruebas y asegurar la integridad tanto de las pruebas digitales como las físicas. Dentro de las acciones que debe realizar el primer nivel de respuesta para asegurar y evaluar la escena son [8]:

- Asegurar que personas no autorizadas tengan acceso a los dispositivos electrónicos de la escena.
- Rechazar ofertas de ayuda o asistencia técnica de personas no autorizadas.
- Retirar todas las personas de la escena del crimen o del área de la cual las pruebas se deben recoger.
- Asegurar todos los dispositivos electrónicos, incluyendo dispositivos personales.
- Seguir las políticas de la organización para asegurar la escena del crimen electrónico.
- Fotografiar y documentar las evidencias.
- Asegurar que ningún dispositivo electrónico vaya ser alterado.

Componentes electrónicos que no son de almacenamiento como el ratón, el teclado, etc., pueden tener evidencia como huellas dactilares, ADN u otra evidencia física que deben ser conservados.

2. Documentación de la escena: Es importante documentar o crear un registro no solamente de las evidencias digitales sino también de la escena del crimen electrónico en general.

2.1. Identificación y documentación de posibles fuentes de datos: Las fuentes más comunes de datos son los desktop, laptops, servidores y dispositivos de almacenamiento en red, pero hay que tener en cuenta que estos sistemas tienen unidades internas de lecturas de CD y DVD, así como varios tipos de puertos para que otros dispositivos de almacenamiento puedan ser conectados como las memorias USB, teléfonos celulares, reproductores de audio, cámaras digitales, entre otros.

Luego de identificar los dispositivos electrónicos con posible evidencia, estos se documentan para conocer sus características y el estado en el que se encontraba luego de reportarse el incidente:

- Marca del equipo.
- Modelo.
- Características del equipo.
- Dirección MAC.
- Dirección IP
- Número de serie.
- Sistema operativo.
- Encendido o apagado.
- Protegido por contraseña.
- Dispositivos conectados.

2.2. Entrevista con el administrador y usuarios del sistema: Se debe obtener información de estas personas quienes son los que conocen e interactúan con el sistema, dicha información corresponde a nombres de usuarios, contraseñas, ISP usado, cuentas de correo electrónico, documentación del software instalado, puertos abiertos, procesos lentos, entre otros.

2.3. Documentación inicial de la escena: La escena del crimen debe ser lo más detallada posible mediante fotos, videos, notas y bocetos para ayudar a recrear los detalles de la escena más tarde.

También incluye documentar toda la locación: el tipo, la ubicación, ubicación de los computadores, conexiones físicas y conexiones WIFI, pues este último podría indicar que existe evidencia más allá de la escena inicial.

3. Investigación preliminar: Consiste en descubrir posibles sospechosos, las partes afectadas, criticidad de la situación y analizar el impacto de los negocios, es decir, perdida en ingresos, perdida de información confidencial, costos de recuperación, tiempos de inactividad, pérdida de credibilidad e imagen, entre otros. Lo anterior servirá en un juicio para imputarle los cargos correspondientes al autor intelectual y material de los hechos, teniendo en cuenta las leyes de cada país.

4. Herramientas forenses a utilizar: Existen un sin número herramientas forenses tanto de software como de hardware que se utilizan para la extracción y análisis de la evidencia. A nivel de software hay herramientas para adquisición y análisis de la memoria, montaje de discos, análisis de malware, análisis de registros de Windows, recuperación de contraseñas, dispositivos móviles, entre otros.

Es importante que estas estén revisadas, actualizadas, en buen estado y no contaminadas. También hay que identificar si la herramienta es soportada por el sistema operativo. Tener en cuenta si tienen algún costo o son gratuitas e igualmente hay que documentarlas.

Para seleccionar las herramientas que se utilizaran en la extracción y análisis de la evidencia los investigadores deben basarse sobre ciertos atributos que están poseen, de acuerdo con Brian Carrier, estos son algunos de ellos [9]:

- Usabilidad: La herramienta debe presentar los datos de forma clara y precisa para que el investigador no interprete los datos de forma errónea.
- Integral: Las pruebas permitirán tanto acusar como defender a las personas involucradas en el caso.
- Precisión: Asegurar de que los datos de salida son exactos, teniendo en cuenta un posible margen de error.
- Determinista: Es la característica de la herramienta de producir los mismos valores de salida ante los mismos valores de entrada y de configuración.
- Verificable: Verificar los resultados, ya sea manualmente o con una segunda herramienta.

5. Identificación de los miembros del equipo de investigación: Se deben definir claramente las funciones y responsabilidades de todas las personas que realizan o ayudan con las actividades forenses. Esto incluye las acciones llevadas a cabo durante el manejo de incidentes y las actividades de trabajo de rutina (por ejemplo, la administración del sistema, solucionadores de problemas de red, etc.), es decir, que todos los equipos internos y externos de la organización que puedan participar en los esfuerzos forenses deben hacerlo teniendo cada persona roles bien definidos que puedan aportar a la investigación [10]. Dentro de los roles genéricos en una investigación forense están: el equipo de respuesta inmediata, los investigadores, los técnicos, los custodios de la evidencia, los examinadores forenses y los analistas forenses.

6. Autorización para iniciar la investigación forense: Los investigadores forenses deben estar autorizados para proceder a realizar la investigación forense firmando un acuerdo de confidencialidad o privacidad de que la información adquirida y analizada no será divulgada a terceros que puedan aprovecharse de la situación. Además los investigadores no deben inmiscuirse en la privacidad de las personas, es decir, no deben recoger información de áreas que no tienen motivos para acceder (por ejemplo, archivos personales) a menos de que tengan una justificación fuerte para hacerlo.

El producto final de esta primera fase, es un documento detallado con información que permita un punto de partida para la adquisición de los datos y para la producción del documento final. Se inicia el trámite de la cadena de custodia.

B. Fase de adquisición de datos

Luego de documentar la escena, seleccionar las herramientas que se van a utilizar, tener definido el equipo y la autorización para proceder con la investigación forense, los analistas necesitan adquirir los datos de las fuentes, entre ellos los diversos archivos que el navegador web genera y almacena como lo son el historial, las cookies y la cache. Para dicha extracción debe utilizarse el siguiente proceso [10]:

1. Desarrollar un plan para la adquisición de los datos: El analista cuenta con muchas fuentes de datos posibles y de todas ellas debe extraer su contenido, por tanto, es fundamental crear un plan para priorizar las fuentes, es decir, establecer un orden en que los datos deben ser adquiridos, teniendo en cuenta los siguientes factores:

1.1. Valor probable: El analista con base a la comprensión de la situación y a su experiencia debe calcular el valor que tiene cada fuente de datos.

1.2. Volatilidad: Son los datos en un sistema vivo que una vez se apague se pierden, así que los datos volátiles tienen prioridad sobre los no volátiles. Para la recolección de las pruebas se debe proceder de mayor a menor volatilidad de la siguiente manera [11]:

- Registros de la cache.
- Tabla de enrutamiento, tabla de procesos, estadísticas del kernel y memoria RAM.
- Sistemas de archivos temporales.
- Registros remotos y datos de monitoreo relevantes del sistema de estudio.
- Configuración física y topología de la red.
- Dispositivos de almacenamiento.

1.3. Cantidad de esfuerzo requerido: El esfuerzo no solamente hace referencia al tiempo dedicado por los analistas

para obtener los datos de las fuentes, sino también el costo de los equipos y servicios extras.

2. Adquirir los datos: Si los datos no han sido adquiridos aun por herramientas de seguridad, herramientas de análisis u otros medios, el proceso general para la adquisición de datos supone el uso de herramientas forenses para recoger los datos volátiles y duplicar los datos de las fuentes no volátiles.

Antes de empezar con la adquisición de los datos, es importante documentar cualquier actividad en el equipo, componentes o dispositivos, además de confirmar el estado de energía del computador. En la figura 2, se observa que el estado del computador juega un papel determinante para proceder con la recolección, pues dependiendo si el equipo esta encendido se debe actuar de tal forma que los datos volátiles no se pierdan y se documente y fotografíe toda información de valor probatorio que se observe en la pantalla, como un programa, una imagen, correo electrónico, un sitio web, etc., pero si el computador se encuentra apagado, no habrían datos para recoger de inmediato sino únicamente los datos no volátiles.

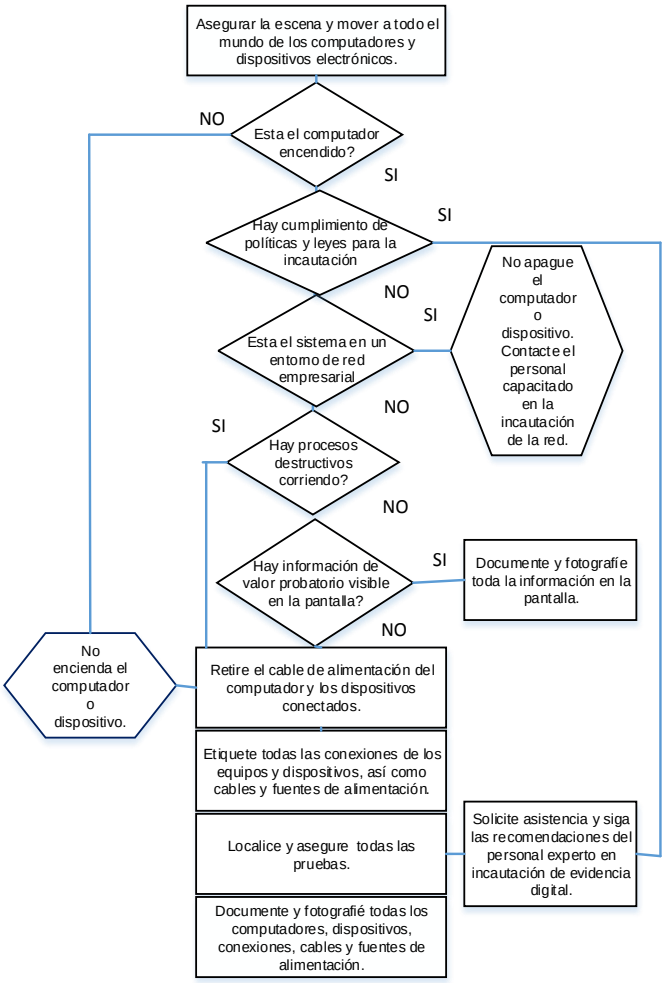

Fig. 2 Recolección de evidencia digital [8]

En una investigación forense se puede recoger una gran cantidad de datos producto de las evidencias volátiles y no volátiles, por tanto, el uso de discos externos USB, son una opción interesante, ya que permiten flexibilidad en el manejo y transporte de grandes cantidades de información.

Lo primero que se debe obtener es toda la información volátil del sistema, luego la contenida en los discos o soportes en general, de este último, es importante decir que se debe realizar no una copia de seguridad sino una copia bit a bit de la unidad de almacenamiento para preservar toda la información que contenga, incluyendo ficheros eliminados, metadatos, etc. Además los analistas pueden utilizar un bloqueador de escritura, con el objetivo de asegurar que durante el proceso de copiado no se altere los datos en el soporte original, manteniendo así, la integridad de los datos originales y de las copias.

De otro lado, los navegadores web son una de las aplicaciones que más utilizan los usuarios y pueden aportar elementos importantes en algunas investigaciones, como son los sitios web favoritos, el historial de los sitios web visitados, la cache y las cookies (incluyendo su creación y fecha de caducidad).
Los analistas deben recoger datos de interés que ayuden a esclarecer la situación, pero muchas veces no es tan fácil, dado que en el caso de los navegadores web es común tener varios instalados en un equipo y las herramientas a utilizar difieren de un navegador a otro.

Las herramientas forenses más importantes para la adquisición de datos del navegador web Internet Explorer son: BrowsingHistoryView, ImageCacheViewer, IEcookiesView, MyLastSearch y FavoritesView.

3. Preservar la evidencia: Luego de que los datos han sido adquiridos, se debe realizar por lo menos una copia más de las evidencias obtenidas, luego se verifica la integridad de cada copia por medio de funciones hash como MD5 o SHA1 y se comparan para asegurar que sean idénticas.

Otro aspecto a tener cuenta, es la cadena de custodia, en donde se recolecta la información referente a cada uno de los eventos que se han realizado con las evidencias, tales como:

- Cuándo, dónde y por quién fue la evidencia descubierta y recogida.
- Quien, cuándo y en qué se embalo y transportó la evidencia.
- En qué estado se recibió.
- Quienes y porque razón tuvieron contacto con la evidencia.
- Durante cuánto tiempo tuvieron la custodia.

Toda esta información es útil para poder llevar una administración adecuada de las evidencias, con el propósito de que esta sea admisible en un proceso legal.
La ley 527 de 1999, define unos requisitos legales para que las evidencias digitales en Colombia tengan validez jurídica.

4. Procedimientos de embalaje, transporte y almacenamiento de la evidencia digital: Los computadores y los dispositivos electrónicos donde se almacena la evidencia son frágiles y sensibles a temperaturas extremas, humedad, golpes,

electricidad estática y campos magnéticos, por lo tanto debe tener precauciones cuando se documente, fotografíe, embale, transporte y almacene para evitar alterar, dañar o destruir los datos [8].

4.1. Procedimiento de embalaje:
- Toda la evidencia digital recolectada debe estar documentada, etiquetada, fotografiada, grabada o esbozada, e inventariada antes de ser empacada. Todas las conexiones y dispositivos conectados debe estar etiquetados.
- Solo bolsas de papel, cajas de cartón y envases antiestáticos deben ser utilizados para embalar la evidencia digital.
- Asegurarse que la evidencia mientras se transporta no se doble, raye o se deforme.
- Etiquetar todos los recipientes utilizados para embalar.

4.2. Procedimiento de transporte:
- Proteger la evidencia de campos magnéticos producidos por transmisores de radio e imanes de los altavoces.
- Evitar mantener la evidencia prologados periodos de tiempo en un vehículo, ya que el frio, calor y la humedad pueden destruirla.
- Asegurar las pruebas digitales mientras se transporta para evitar daños de golpes y vibraciones.
- Documentar el transporte de la evidencia digital.

4.3. Procedimiento de almacenamiento:
- Las pruebas deben estar inventariadas de acuerdo con las políticas de la agencia forense.
- Almacenar la evidencia en un ambiente de clima controlado para que no esté sujeta a temperaturas extremas.
- Asegurar la evidencia a fin que no esté expuesta a campos magnéticos, humedad, polvo, vibración o cualquier otro elemento que pueda dañarla o destruirla.

C. Fase de análisis de datos

Una vez se tienen las evidencias digitales recopiladas y almacenadas de forma adecuada, la siguiente tarea es la de analizar dichas evidencias con los datos disponibles para reconstruir la línea temporal del ataque, estableciendo la serie de acontecimientos que ocurrieron momentos antes del ataque, hasta su descubrimiento. Esta es la fase más larga y laboriosa de todo el proceso forense, por tanto, las personas que analizan las evidencias deben estar capacitadas para este fin.

Al finalizar esta fase de análisis de datos se debe conocer cómo se realizó el ataque, quienes fueron los autores del incidente, cuál era el objetivo del ataque, cual fue el impacto causado al sistema, etc.

Para analizar la evidencia se recomienda seguir los siguientes pasos [12]:

1. Preparación del entorno de trabajo: Se debe acondicionar un lugar de trabajo adecuado para realizar el análisis a las evidencias. Esto incluye recursos tales como herramientas forenses (hardware y software), estaciones de trabajo, discos duros, software de virtualización, diferentes sistemas operativos, entre otros.

En lo posible desistir de utilizar los dispositivos de almacenamiento originales, y más bien trabajar con las imágenes de las copias, las cuales se montarán tal cual como se encontraron en el sistema comprometido, es decir, manteniendo la misma estructura de particiones y el sistema de archivos.

2. Secuencia temporal del ataque: Una vez se tengan las imágenes montadas en la estación de trabajo, la siguiente labor es reconstruir la línea temporal del ataque y para eso se necesita recopilar la siguiente información de los ficheros:

- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tipo de fichero y tamaño.
- Permisos de acceso.
- Usuarios y grupo a quien pertenece.
- Si estaba oculto o no y si fue borrado o no.

Un punto de partida para el análisis es ordenar las marcas de tiempo MACD, para buscar ficheros que han sido modificados, accedidos, creados o borrados recientemente, y que además se encuentren en rutas poco comunes.

Luego centrarse en averiguar la ubicación de los archivos ocultos, sus rutas y el tipo de fichero, buscar también los archivos borrados o fragmentos de estos, ya que pudieron ser borrados por los atacantes.

Los archivos logs son generados de forma automática por el sistema operativo o por aplicaciones, conteniendo datos sobre errores de inicialización, accesos al equipo, creación de cuentas de usuario, estado del sistema, etc., así que estos deben ser examinados con detalle, intentando buscar una correlación temporal entre eventos.

3. Establecer cómo se realizó el ataque: Luego de tener una línea de tiempo acerca de los acontecimientos en el sistema, ahora hay que averiguar cómo se ingresó a este, investigando cuales pudieron ser las vulnerabilidades que causaron la brecha de seguridad y que herramientas se utilizaron para lanzar el ataque. Para lo anterior, se deben tener en cuenta los archivos sospechosos y/o recientes al descubrimiento del ataque, incluyendo los archivos de logs, claves, cuentas de usuarios, etc.

Para determinar cómo se realizó el ataque, se puede partir por revisar los servicios abiertos y procesos que se recolectaron como evidencia volátil. Examinar con detalles aquellos archivos que parecen sospechosos y en general las circunstancias que rodean la escena. También documentarse sobre las vulnerabilidades que se sospechan que pudieron ser aprovechadas por el atacante y como las pudo haber explotado, con el objetivo de reproducir sobre una máquina igual que la

comprometida, los mismos eventos encontrados entre las evidencias.

4. Identificación de los autores del ataque: Para lograr identificar quienes causaron el incidente, los analistas se deben valer de los datos volátiles recogidos en la anterior fase, intentando averiguar la dirección IP de donde se lanzó el ataque, los puertos utilizados, buscar además en los logs de conexiones de red, e igualmente buscar entre los archivos borrados por si el atacante quiso borrar las evidencias.

La dirección IP es uno de los factores más importantes para identificar a los sospechosos, pero se debe tener cuidado puesto existen técnicas para engañar la ubicación real del ataque, como por ejemplo, con técnicas de IP spoofing o con ordenadores zombis, por tal razón, se tendrá que verificar y validar la dirección IP sospechosa.

La identificación de los autores del ataque, se debe realizar si se quiere llevar a cabo investigaciones internas en la organización o se quiere emprender un proceso legal. En caso que no se desee hacer lo anterior, los esfuerzos pueden ir encaminados por ejemplo a mejorar la seguridad del sistema.

5. Evaluación del impacto causado al sistema: Por medio del análisis forense se puede determinar qué es lo que han hecho los atacantes al sistema afectado, permitiendo realizar una estimación del impacto causado, teniendo en cuenta incluso el impacto negativo a nivel técnico, además de lo crítico que eran los sistemas atacados, ya que el impacto difiere del tipo de servicio o negocio que presta la organización.

Se puede elaborar un BIA (Business Impact Analysis) para analizar los impactos financieros y operacionales que causó el atacante en la organización, sus áreas o procesos.

Para terminar esta fase, se deben relacionar todos los elementos nombrados anteriormente, para proporcionar una imagen más completa frente al caso de investigación.

D. Fase de presentación de resultados

Es esta última fase, se plasma por escrito de una forma clara, exacta y completa el procedimiento realizado en el análisis, los hallazgos, su interpretación y las conclusiones que de ellos se derivan. Hay que tener en cuenta en la redacción del informe a quien va dirigido, ya que en ocasiones el destinatario final no tiene los suficientes conocimientos técnicos sobre la materia, por tanto, la terminología usada en la presentación de resultados debe adecuarse a esta situación.

Generalmente se hacen dos tipos de informes, uno técnico y otro ejecutivo [12]:

1. Informe técnico: Los lectores de este tipo de informe son personas con un perfil técnico, como ingenieros de sistemas y sus afines. El objetivo del informe consiste en presentar con detalle el análisis realizado y debe contener al menos los siguientes puntos:

- Antecedentes del incidente.
- Adquisición de los datos
- Descripción de la evidencia.
- Análisis de la evidencia con la información del sistema analizado (aplicaciones, vulnerabilidades, servicios, etc.).
- Descripción de los hallazgos (herramientas usadas por el atacante, origen del ataque, huellas de la intrusión, etc.).
- Cronología de la intrusión.
- Conclusiones.
- Recomendaciones.

2. Informe ejecutivo: Los lectores de este informe son personas de la alta dirección de las empresas u organismos que no son especialistas en sistemas informáticos, así que el lenguaje utilizado debe ser común y si existe alguna jerga técnica, tiene que ser explicada de manera clara. La finalidad de este informe es plasmar un resumen del análisis realizado con lo más relevante de lo ocurrido en el sistema analizado y debe contener al menos los siguientes puntos:

- Desarrollo de la intrusión.
- Resultados del análisis.
- Recomendaciones.

IV. ESCENARIO DE VALIDACIÓN DEL MARCO METODOLÓGICO

El marco metodológico propuesto en el presente artículo fue validado con un sencillo escenario de prueba ficticia, el cual consiste en la acusación de un estudiante de la Universidad de los Andes por el delito de pornografía con menores, el cual se encuentra tipificado en el artículo 218 del Código Penal Colombiano (Ley 599 de 2000) que dice lo siguiente: "***El que fotografíe, filme, venda, compre, exhiba o de cualquier manera comercialice material pornográfico en el que participen menores de edad, incurrirá en prisión de seis (6) a ocho (8) años y multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes***".

En muchas investigaciones, la actividad de navegación web por lo regular proporciona pistas para la investigación, por eso una reconstrucción de la actividad de navegación web ayudaría a probar o refutar la acusación al estudiante de los Andes.

A continuación se validará cada una de las fases propuestas del marco metodológico, resumiendo los resultados obtenidos:

A. Fase de preparación

En la primera fase se aseguró y evalúo la escena, retirando las personas que estaban cerca de la evidencia para que no fueran a interferir con la investigación, así mismo se documentó por medio de fotos y notas lo hallado en la escena, se procedió luego con una entrevista al propietario para conocer con más detalles de su interacción con el dispositivo, siendo hasta el momento el único sospechoso del caso. Se identifica que en la escena hay un computador portátil marca Hewlett Packard, modelo HP Spectre XT Ultrabook PC, color gris, número de serie

CND3060HVC y el cual se encontraba apagado en el momento de la incautación. Igualmente, se creó el debido registro de la cadena de custodia.

Se determina que las herramientas a utilizar en este caso para adquirir y analizar la evidencia del navegador web Internet Explorer (único navegador instalado en el dispositivo) son BrowsingHistoryView, MyLastSearch, ImageCacheViewer y FBCacheView. Además de las herramientas nombradas se necesitaron otras como: FTK Imager, EnCase, HashMyFiles y UsbWriteProtect.

B. Fase de adquisición de los datos

La única fuente de datos con la que se cuenta es con el disco duro del computador portátil incautado, con base a esta fuente se investiga el caso, ya que no se encontraron más evidencias en la escena como por ejemplo memorias USB, discos duros extraíbles, celulares, etc.. Además el sistema estaba apagado en el momento de la incautación, por lo tanto, no había datos volátiles para recuperar.

Antes de adquirir los datos de la fuente, ésta se documentó, describiendo las características del dispositivo y luego se procedió a realizar una copia de la misma, de la siguiente manera:

Lo primero que se realizó para adquirir los datos de la fuente original fue utilizar el bloqueador de escritura a nivel de software llamado UsbWriteProtectect, de esta manera se tenía la garantía de que se preservarían los datos contenidos en el disco duro del portátil incautado luego de conectarse con el equipo donde se extraería y analizaría la evidencia.

En seguida, con la herramienta HashMyFiles se le aplicó una función hash a la evidencia incautada, posterior a ello, en un disco duro previamente esterilizado con el software EnCase y conectado al cómputo forense, se realizó una copia bit a bit del medio original con FTK Imager. Por último, se volvió aplicar una función hash a la copia, garantizando que tanto la evidencia original como la copia sean idénticas.

El disco duro donde se almacenó la copia de la evidencia original también fue documentado y etiquetado, y la fuente original fue embalada en una bolsa antiestática y puesta en una caja fuerte.

Se realizó el procedimiento de la cadena de custodia, diligenciando el rotulo y su respectivo registro de continuidad muy detalladamente, conteniendo información como lugar del hallazgo, descripción del elemento probatorio, información de quien la recolectó, estado en que se encontró, entre otros.

C. Fase de análisis de datos

El análisis de datos sobre el navegador web Internet Explorer se realizó con cuatro herramientas: BrowsingHistoryView, MyLastSearch, ImageCacheViewer y FBCacheView, cada una de ellas aportó evidencias para esclarecer el caso investigado.

BrowsingHistoryView es una herramienta que permitió ver el historial de navegación de Internet Explorer, arrojando resultados en las pestañas URL visitadas, la fecha y hora de la visita, el contador de visitas, la versión del navegador y el perfil de usuario, mientras que en las pestañas título y el lugar de donde fue visitado, no muestra ningún contenido.

Se revisó cada URL visitada y se encontró que había 54 de ellas, en busca de contenido pornográfico infantil en forma de imágenes o videos como se observa en la figura 3. Las fechas que corresponde a este tipo de contenido oscilan entre el 22 de julio y el 26 de agosto. El contador de visitas fue una pestaña importante para este caso, ya que ayudo a identificar cuáles son los sitios web que más frecuentó el investigado, determinando que 8 URL asociadas a pornografía estaban dentro de los 10 sitios más visitados por el usuario.

URL	Visit Time	Visit Count
https://www.google.com.co/search?q=sexo+con+menores+de+edad&tbm...	26/08/2014 10:06:16 a. m.	24
https://www.google.com.co/search?q=sexo+con+menores+de+edad&tbm...	26/08/2014 10:06:16 a. m.	2
about:blank	26/08/2014 10:06:14 a. m.	363
https://www.google.com.co/search?q=sexo+infantil&source=lnms&sa=X&...	26/08/2014 10:05:24 a. m.	12
https://www.google.com.co/search?q=sexo+infantil&source=lnms&sa=X&...	26/08/2014 10:05:24 a. m.	2
https://www.google.com.co/search?q=sexo+infantil&source=lnms&tbm=i...	26/08/2014 10:04:41 a. m.	6
https://www.google.com.co/search?q=sexo+infantil&source=lnms&tbm=i...	26/08/2014 10:04:41 a. m.	2
https://www.google.com.co/search?q=sexo+infantil&source=lnms&sa=X&...	26/08/2014 10:04:36 a. m.	13
https://www.google.com.co/search?q=sexo+infantil&source=lnms&sa=X&...	26/08/2014 10:04:36 a. m.	3
http://www.antena3.com/videos-online/noticias/sociedad/video-pornograf...	26/08/2014 10:04:34 a. m.	6
http://secure-uk.imrworldwide.com/storageframe.html	26/08/2014 10:04:24 a. m.	1
https://www.google.com.co/search?tbm=isch&sa=1&q=sexo+infantil&oq...	26/08/2014 10:03:45 a. m.	1
https://www.google.com.co/search?q=porno+infantil&source=lnms&tbm...	26/08/2014 10:03:37 a. m.	18
https://www.google.com.co/search?q=porno+infantil&source=lnms&tbm...	26/08/2014 10:03:37 a. m.	3

Fig. 3 Captura de pantalla tomada en la ejecución de la aplicación BrowsingHistoryView por El autor.

A continuación se utilizó la herramienta MyLastSeach para identificar los últimos sitios web visitados por el acusado, mostrándonos los últimos 5 días de navegación web con Internet Explorer (22 de agosto de 2014 al 26 de agosto de 2014). Las últimas consultas de búsqueda que se han realizado se muestran en una tabla con las siguientes columnas: texto de búsqueda, motor de búsqueda, tipo de búsqueda (general, video o imágenes), navegador web y la URL de búsqueda.

Con base en la información obtenida por la herramienta, se identificó texto de búsqueda que tuviera relación con pornografía infantil, evidenciando que entre el 22 de agosto al 26 de agosto del presente año, se accedió a 18 búsquedas relacionadas con este tipo de contenido y dentro de las cuales 13 fueron realizadas el 26 de agosto como se aprecia en la figura 4. Además se determinó con esta herramienta que el implicado utilizó el motor de búsqueda Google, para ingresar a material obsceno que implicara menores de edad.

Search Text	Search Engine	Search Type	Search Time	Web Browser
porno	Google	General	26/08/2014 12:07:47 ...	Internet Explorer
porno infantil	Google	General	26/08/2014 12:07:57 ...	Internet Explorer
porno infantil colegios	Google	General	26/08/2014 12:09:53 ...	Internet Explorer
fotos con menores de edad	Google	General	26/08/2014 10:00:04 ...	Internet Explorer
niños porno	Google	General	26/08/2014 10:01:21 ...	Internet Explorer
porno infatil	Google	General	26/08/2014 10:01:46 ...	Internet Explorer
porno infatil	Google	General	26/08/2014 10:01:51 ...	Internet Explorer
porno+infantil	Google	General	26/08/2014 10:03:38 ...	Internet Explorer
porno infantil	Google	General	26/08/2014 10:03:38 ...	Internet Explorer
sexo infantil	Google	General	26/08/2014 10:05:23 ...	Internet Explorer
sexo con menores	Google	General	26/08/2014 10:05:29 ...	Internet Explorer
sexo+con+menores+de+ed...	Google	General	26/08/2014 10:06:18 ...	Internet Explorer
sexo con menores de edad	Google	General	26/08/2014 10:06:43 ...	Internet Explorer

Fig. 4 Captura de pantalla tomada en la ejecución de la aplicación MyLastSearch por El autor.

La tercera herramienta utilizada fue ImageCacheViewer, ésta permite escanear la memoria cache del navegador web Internet Explorer y ver las imágenes que aparecen en los sitios web que se ha visitado. Para cada archivo de imagen almacenado en cache se muestra la siguiente información: URL de la imagen, el navegador web que se utilizó para visitar la página, tipo de imagen, la fecha y hora de la imagen, fecha y hora de la navegación y el tamaño del archivo.

La herramienta encontró 1444 imágenes almacenadas en cache, las cuales todas fueron observadas rápidamente, pero solo las imágenes de interés para la investigación fueron tenidas en cuenta para un análisis más profundo.

De las 1444 imágenes en cache, 538 era evidencia electrónica para la investigación, ya que estaban asociadas a pornografía con menores. Además, como se observa en la figura 5, se determinó que el investigado estuvo buscando este tipo de contenido en la red social Facebook entre el 25 de julio y 20 de agosto de 2014 y almacenado en una carpeta de su perfil de usuario.

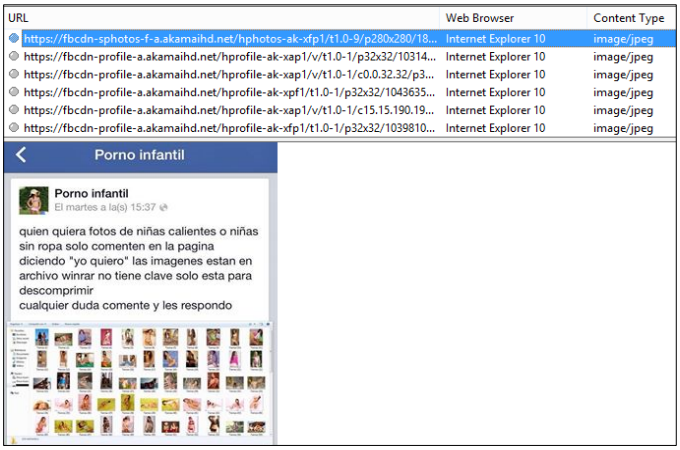

Fig. 5 Captura de pantalla tomada en la ejecución de la aplicación ImageCacheViewer por El autor.

El último software utilizado para analizar la evidencia fue FBCacheView, el cual hace una lista de todas las imágenes de las páginas de Facebook que se ha visitado anteriormente, incluyendo fotos de perfil, imágenes subidas e imágenes de otros sitios web. Para cada imagen de Facebook se muestra la URL de la imagen, el navegador web utilizado, tipo de imagen, fecha y hora de la imagen, fecha y hora de la navegación, tamaño de la imagen y la URL externa (para las imágenes tomadas desde otro sitio web). Esta herramienta fue utilizada teniendo en cuenta que anteriormente se había demostrado la utilización de Facebook para buscar páginas pornográficas.

La herramienta FBCacheView arrojó 9211 imágenes, dentro de las cuales se encontraron alrededor de 3500 imágenes con asocio al delito atribuido al investigado. Muchas de las imágenes de los perfiles hacían alusión a menores de edad semidesnudas como se aduce en la figura 6, así mismo, se encontró que se habían subido varias imágenes impúdicas a Facebook en el mes de agosto de 2014, desde el computador portátil incautado.

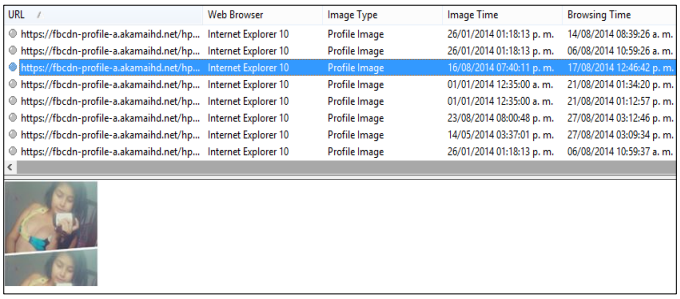

Fig. 6 Captura de pantalla tomada en la ejecución de la aplicación FBCacheView por El autor.

De acuerdo al análisis forense efectuado con 4 herramientas al navegador web Internet Explorer se determinó que el investigado está relacionado con material de pornografía infantil.

D. Fase de presentación de resultados

Con base a los resultados obtenidos con las herramientas forenses BrowsingHistoryView, MyLastSearch, ImageCacheViewer y FBCacheView se puede deducir que:

1. Se halló 54 URL asociadas a contenido sexual que involucraba menores de edad y 8 de esas URL estaban dentro de los 10 sitios más visitados por el usuario. La búsqueda de este tipo contenido se registró entre el 22 de julio y 26 de agosto de 2014.
2. El investigado no ingresaba directamente a los sitios web sino que utilizaba el motor de búsqueda Google para buscar pornografía con menores.
3. Se encontró 538 imágenes de lo que parecían ser niños en actos sexuales. Por lo general, en una investigación de pornografía se dejan rastros de imágenes y videos relacionados con este tipo de contenido.
4. Se revelo que el investigado ingresaba a Facebook para visitar perfiles de menores de edad semidesnudos e igualmente subía imágenes de estas características a la red social nombrada.

Lo anterior puede determinar la culpabilidad del estudiante de los Andes, no obstante, falto hacer verificaciones sobre las imágenes y videos que habían en el computador portátil del acusado, teniendo en cuenta que el investigado pudo haber eliminado u ocultado archivos, cambiado la extensión de los mismos, aplicado esteganografía, etc., por lo que la investigación forense requeriría de otras herramientas y por supuesto demanda de tiempo, aun así el análisis al navegador web Internet Explorer dio fuertes indicios para imputarle al estudiante implicado en el hecho, el delito atribuido como pornografía con menores.

V. CONCLUSIONES

En este trabajo se investigó a profundidad los mejores estándares de informática forense en general y los relacionados con los navegadores web. Lo anterior se realizó con el propósito de llevar a cabo un marco metodológico presentado en este trabajo, elaborado con base en diferentes procedimientos y conceptos investigados, y adaptándola para el manejo y

tratamiento forense del navegador web Internet Explorer. Luego de elaborado el marco metodológico, se comprobó la viabilidad de su aplicación, teniendo en cuenta las fases expuestas en dicho marco.

La realización de esta propuesta forense para investigar el navegador web Internet Explorer fue interesante, en la medida que existen pocas metodologías orientadas a este tema y dada la creciente demanda de computadores y usuarios de Internet, se hace indispensable tener presente el software que se instalan en los computadores que permite el acceso a Internet, llamado navegador, pues en este se almacena gran cantidad de información acerca del comportamiento del usuario cuando navega en los sitios web, por tanto el estudio forense a los navegadores web es pieza clave para la investigación, si se piensa que la gran mayoría de hogares y empresas, cuentan con computadores con acceso a Internet.

Por supuesto este marco metodológico desarrollado pretende obtener el mismo resultado, dado el mismo caso de investigación, pero es difícil contemplar la posibilidad que se presente un escenario igual en cada incidente, así que todos deben manejarse de formas distintas de acuerdo a su gravedad, preparación del equipo forense y las circunstancias. Cada investigación forense al navegador web Internet Explorer puede adaptar este marco metodológico de acuerdo al caso investigado.

REFERENCIAS

[1] J. Mosquera, A. Certain y J. Cano. (abril, 2005). Evidencia Digital: contexto, situación e implicaciones nacionales. [En línea]. Disponible en: http://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics90.pdf

[2] P. Díaz, G. Valle y D. Jones. (2011). Internal Vs. External Penetrations: A Computer Security Dilemma. Computing & Technology Department, Cameron University, Lawton, OK, USA. [En línea]. Disponible en: http://www.cameron.edu/~pdiaz-go/SAM3049.pdf.

[3] ESET. (2014). Eset Security Report Latinoamérica 2014. [En línea]. Disponible en: http://www.welivesecurity.com/wp-content/uploads/2014/06/informe_esr14.pdf

[4] M. Noblett, M. Pollitt y L. Presley. (2000). Recuperación y Examinar ordenador Evidencia Forense. FBI. [En línea]. Disponible en: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

[5] (2000). Evidencia digital: Normas y Principios: Grupo Científico de Trabajo sobre la Evidencia Digital (SWGDE) Organización Internacional de Evidencia Digital (IOCE). FBI. [En línea]. Disponible en: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/

[6] U.S. Department of Justicie. (abril, 2004). Forensic examination of digital evidence: A guide for law enforcement. [En línea]. Disponible en: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[7] IOCE. (abril, 2009). Guidelines for best practice in the forensic examination of digital technology. Versión 6. [En línea]. Disponible en: http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf

[8] U.S. Department of Justicie. (abril, 2008). Electronic crime scene investigation: A guide for first respoders. Second Edition. [En línea]. Disponible en: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

[9] B. Carrier. (2003). Defining digital forensic examination and analysis tools using abstraction layers. Volumen 1. [En línea]. Disponible en: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04C3F91-AFBB-FC13-4A2E0F13203BA980.pdf

[10] NIST. (2006). Guide to integrating forensic techniques into incident response. [En línea]. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

[11] D. Brzezinski y T. Killalea. (febrero, 2002). RFC 3227: Guidelines for evidence collection and archiving. [En línea]. Disponible en: https://www.ietf.org/rfc/rfc3227.txt.

[12] M. López. (junio, 2007). Análisis forense digital. 2da edición. [En línea]. Disponible en: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf