SOFTWARE PARA RECOLECCIÓN DE EVIDENCIAS DIGITALES RÁPIDAS EN SISTEMAS WINDOWS

Autores: Lic. Marcos Adrián Monti, Dr. David Luis La Red Martínez / Facultad de Ciencias Exactas y Naturales y Agrimensura / Universidad Nacional del Nordeste

RESUMEN

La necesidad de análisis de evidencia digital forense comprende ciertos desafíos en cuanto a escasez de herramientas de software disponibles, los altos costos y sobre todo los tiempos requeridos para llevar a cabo estos análisis, los cuales dependen en gran manera de la capacidad de los equipos involucrados. Resulta conveniente disponer de la capacidad de capturar información en el lugar del hecho utilizando las herramientas de software disponibles de manera inteligente de modo que sea posible discernir, cuando exista un gran volumen de equipos, cuáles podrían ser de interés a la causa judicial y cuáles no. En el presente trabajo se lleva a cabo el estudio de necesidad y factibilidad que fundamentan el proceso de desarrollo de un software de aplicación de campo para obtención de evidencia digital forense durante procedimientos de allanamiento; de acuerdo al protocolo de actuación vigente, este software será utilizado, además, como un "indicador" del contenido de los equipos bajo análisis, a fin de permitir al perito actuante tomar decisiones (como proceder al secuestro o no de un determinado equipo) en el lugar donde se está llevando a cabo dicho procedimiento.

Palabras clave:

Actividad de Usuario. Sistema Operativo. Navegador Web. Evidencia Digital. Informática Forense. Virtualización. Imagen Forense.

CONTEXTO

La Problemática se desarrolla en el contexto del análisis forense de evidencias digitales en el Poder Judicial, uno de los organismos públicos de la Provincia de Formosa.

La informática forense o el cómputo forense es el uso de métodos y técnicas científicas probadas, con el fin de identificar, preservar, validar, analizar, interpretar, documentar y presentar evidencia digital obtenida a partir de fuentes de información digital, con el propósito de facilitar la reconstrucción de hechos en una investigación legal, o ayudar a anticipar o prevenir acciones en contra de la ley [1][2]. De esta manera la Informática Forense actúa como una rama de la Informática que provee un complementario a la Criminalística clásica, enfocándose en el análisis de las evidencias digitales, que pudiesen existir, en cualquier escena del hecho [3][4].

En el campo de la criminalística, la tecnología y los sistemas de información resultan fundamentales para las ciencias forenses en el desarrollo de su objetivo que es descubrir y aportar pruebas físicas de los crímenes, a fin de esclarecer los hechos, la identidad de los sujetos que participaron en él, y la forma en que éstos llevaron a cabo la concreción de los mismos.

1. INTRODUCCIÓN

La evolución constante de las tecnologías ha venido de la mano o acompañado el desarrollo en todas las áreas de conocimiento a través de los años; el campo de los sistemas de información, específicamente, ha sido fundamental a la hora de asistir y acompañar a todas las ciencias, en el desarrollo de sus correspondientes actividades.

En la actualidad, los discos de equipos tipo PC que ejecutan alguna versión de Microsoft Windows tienen capacidad de 1 TeraByte o más, por lo cual la envergadura de información que albergan los mismos puede resultar muy significativa, resultando una tarea muy ardua y demandante la recopilación y análisis de datos.

En el laboratorio forense, es común realizar varias imágenes o copias forenses de los discos de los equipos aportados, con su correspondiente cálculo de valor hash, a fin de proceder a analizar los mismos [5], utilizando virtualización del sistema operativo [2] o algún software específico que permita "montar" los discos y sus particiones, conjuntamente con su sistema de archivos, sin tener que utilizar ni modificar el disco físico original [4][6].

Esta práctica, sin embargo, suele demandar cantidades enormes de espacio de almacenamiento en cualquier Laboratorio Forense, del orden de los cientos de Terabytes de datos; proporcional a la cantidad de equipos involucrados que han sido aportados en la causa en particular.

Asimismo los equipos necesarios para llevar a cabo la virtualización de los sistemas operativos y el análisis de datos, normalmente requieren tener la mayor cantidad posible de recursos disponibles en cuanto a procesador, memoria RAM y capacidad de almacenamiento en disco, siendo necesario en muchas ocasiones contar además con un servidor de almacenamiento en red o unidad NAS, instalado preferiblemente con redes cableadas y conexión de alta velocidad para cada uno de los equipos de trabajo.

Actualmente, existen numerosas herramientas de software capaces de realizar la imagen forense de los discos rígidos [8], para luego proceder al análisis de los mismos, según los criterios establecidos por el perito a cargo; sin embargo las mismas en su mayoría son muy exigentes en cuanto a costo, tiempo demandado y hardware requerido.

Por todos estos motivos, cualquier investigación que estuviera en curso puede prolongarse en el tiempo mucho más de lo deseado; es oportuno entonces contar con alternativas viables que sean de bajo costo, con pocas exigencias de hardware y demanden el menor tiempo posible.

LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Para llevar a cabo un proceso de investigación y desarrollo primeramente se definieron cuáles serían los **objetivos Generales abordados**:

Los objetivos del trabajo consistieron en el estudio, recopilación y análisis de datos que son factibles de recuperar en sistemas que ejecutan el sistema operativo Microsoft Windows sobre la actividad de el/los usuario/s del mismo, con el objetivo de desarrollar herramientas de software que permitan automatizar las tareas de captura de información.

Los temas que se abordaron han sido todos aquellos concernientes a los detalles específicos de los sistemas Windows, su funcionamiento general, el almacenamiento de datos de usuario y cómo los mismos podrían aportar soluciones en la búsqueda de información útil para investigaciones forenses y el desarrollo de herramientas que puedan servir para tal fin. La investigación resultó en la concepción y desarrollo de un sistema automatizado para recolección de datos forenses en sistemas Windows, de acuerdo a los principios fundamentales de dicha ciencia [7][8].

Datos y aplicaciones comúnmente disponibles en Windows

De acuerdo a lo que se visualiza en la mayoría de sistemas Windows así como en lo sugerido desde sitios web comunes como "www.makeuseof.com" [9], "es.digitaltrends.com" [10], "www.microsoft.com" [11] y "www.computerworld.com" [12], es posible constatar la presencia de cierto software de base en todas las instalaciones de Windows.

Estos poseen, por ejemplo, Microsoft Internet Explorer o Microsoft Edge, por lo general, el cual ya está incluido desde Windows 10, asimismo existen navegadores alternativos que son de uso popular como ser Google Chrome, Opera o Firefox.

Este conjunto de navegadores, por lo general, constituyen las vías principales por las cuales el usuario realiza su interacción con redes

sociales además de permitir la visualización de imágenes, videos, noticias, etc.
Asimismo a través del análisis de datos resguardados en caché y sus correspondientes archivos de historial, es posible recuperar el registro de búsquedas o consultas realizadas en los mismos, a los diferentes motores de búsqueda online, obteniendo datos extra como el tipo de búsqueda realizada (texto, imágenes, videos), y la fecha y hora en que se realizaron.
En cuanto a otros programas incluidos en instalaciones Windows podemos encontrar el editor de texto y explorador de archivos, reproductor de audio y videos a través de Windows Media Player y archivos de imágenes a través de Visualizador de Fotos o simplemente Fotos de Microsoft, los cuales se incluyen por defecto en cualquier instalación de este Sistema Operativo.
Es necesario destacar que, si bien existen aplicaciones instalables a través de la Microsoft store, en las versiones más modernas de Windows, como ser Instagram, Tik Tok, Telegram y WhatsApp Desktop, etc; el análisis de las mismas excede los alcances de los objetivos que fueran planteados durante el desarrollo del presente trabajo, por lo cual en mayor medida, se ha priorizado capturar la actividad del usuario a través de los navegadores de Internet.
Las herramientas mencionadas anteriormente poseen, adicionalmente, información privada sobre el/los perfiles de usuario guardados por cada red social, sitio, cuenta bancaria, etc., a la que el mismo ha accedido. Debido a lo mencionado, además de datos de navegación y marcadores, tendríamos datos sobre las cuentas resguardadas en dicho navegador, siempre y cuando el usuario haya decidido recordar las mismas en dicho navegador y dispositivo.

Software y aplicaciones para extracción de datos en Windows

De acuerdo a lo planteado anteriormente, es posible concluir que, en forma general, es posible obtener bastante información sobre el uso del sistema, a partir de los registros que guarda el propio Sistema Operativo.
Asimismo, la información básica sobre cuentas de usuario, Interacción en redes sociales y otros sitios de internet, se obtendrá únicamente a través de los mismos Navegadores Web, por lo tanto es conveniente centrar el estudio en la obtención de dichos datos; existen numerosos recursos y métodos para obtener estos datos, sin embargo uno de los recursos más mencionado por los sitios web especializados [13] el de las numerosas herramientas gratuitas disponibles en el sitio de herramientas de Nirsoft [14].
Es posible observar la gran colección de software especializado en herramientas para Windows.
Entre ellas se cuentan con herramientas tanto para Obtención de datos en Navegadores Web como para obtención de Información del sistema.

Diseño de la aplicación "Forensic Portable"

De acuerdo a lo mencionado oportunamente, se procedió al diseño y desarrollo de una aplicación de tipo portable, capaz de ejecutarse sin requerir ningún tipo de instalación; liviana, tanto en términos de requerimientos de hardware como en performance y tamaño en disco y con una interfaz simple, buscando un uso intuitivo y entendible, incluso para personal no técnico.
De acuerdo al uso para el cual fue concebida, esta aplicación no incluye un módulo para realizar análisis de superficie y búsqueda de archivos borrados, al ser una operación que, por lo general, demora mucho tiempo y para lo cual se requerirá el secuestro de la unidad a fin de realizar un análisis más extenso, en el Laboratorio Forense.
Se utilizó para esto el entorno de programación de Visual Studio 2019 y el leguaje C# conjuntamente con las herramientas mencionadas de Nirsoft y la herramienta de Copia incorporada Robocopy.

RESULTADOS OBTENIDOS

Se ha obtenido como resultado una aplicación de tipo portable capaz de ejecutarse en

sistemas Windows desde cualquier dispositivo o unidad de disco portátil.
La aplicación muestra dos secciones donde podemos elegir el destino (carpeta o directorio) donde van a resguardarse todos los datos, y por otro la opción de copia forense de archivos o recuperación de datos del sistema (ver Fig. 1).

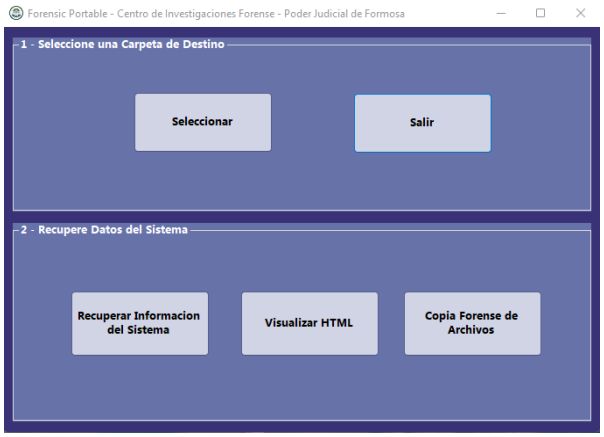

FIG. 1: Ventana Principal de la aplicación "Forensic Portable" [fuente propia].

El primer formulario que se visualiza en "1- Seleccione Carpeta de Destino" se encarga de establecer las configuraciones básicas para iniciar la recuperación de datos, este paso resulta necesario para establecer el destino de los datos, para lo cual se requiere un directorio válido.
A fin de mantener lo más inalterado posible el sistema huésped, es altamente recomendable elegir un dispositivo de almacenamiento externo como destino, en lugar de carpetas ubicadas dentro del sistema de archivos del equipo host.

Módulo de Recuperación de datos del Sistema

A la derecha es posible visualizar información básica del sistema y a la izquierda seleccionar el tipo de información que se busca recuperar.
Desde aquí es posible obtener información de uso del sistema mediante los datos proporcionados tanto por los navegadores Web como de los registros del sistema operativo (Fig. 2).

Dicha información es obtenida a través del lanzamiento o ejecución de las aplicaciones mencionadas en capítulos anteriores en "modo silencioso", es decir, a través de la ventana de comandos, sin utilizar ningún tipo de interfaz de usuario; esto permite recabar los datos de forma eficiente y rápida, al no requerir ningún otro tipo de interacción adicional, además es posible seleccionar, en el mismo módulo, qué procesos específicos lanzar, de acuerdo a la información que se quiere obtener.

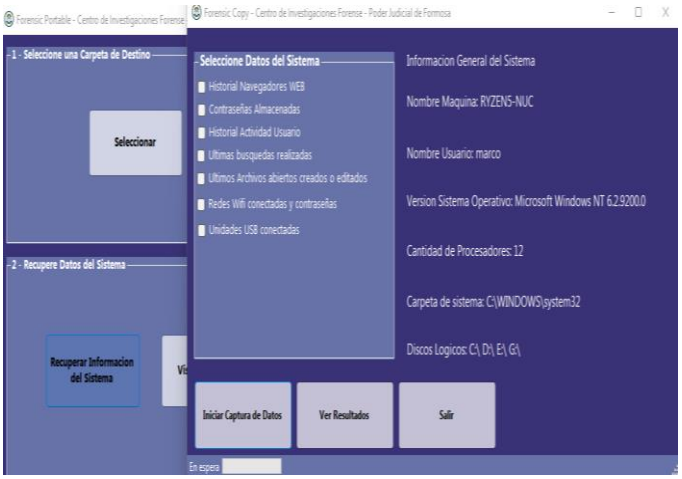

FIG. 2: Ventana módulo de recuperación de datos del sistema [fuente propia].

Módulo de Copia Forense

Finalmente en el último botón del menú principal tendremos el módulo de copia forense; en el mismo tendremos la posibilidad de realizar una copia forense [9][10] de todos los archivos que resulten de interés, junto con su información básica correspondiente (tipo de archivo, tamaño, fecha de creación, etc.), además de permitir obtener una pre visualización de los mismos, utilizando controles especiales incorporados al formulario.
Es posible seleccionar el tipo de archivo que se buscará en la unidad o carpeta de origen indicada.
En este formulario es posible efectuar búsquedas y visualización de archivos de tipo imágenes soportando los formatos - jpg, jpeg, png, gif, raw, cr2, nef, tif, tiff, hdr-, videos de tipo - mp4, mov, wmv, avi, mkv, flv, f4v, swf

-, documentos de tipo – doc, txt, pdf, htm, ppt, xls - y de audio como ser - m4a, ogg, mp3, flac, wav, wma, acc, alac o aif -.

La pre visualización se realiza en el mismo módulo, mediante un control especial por cada tipo de archivo, estos se abren en modo de solo lectura con la sola finalidad de permitir examinar o reproducir el contenido del mismo a fin de poder discriminar si estos serán de interés o no para la investigación en curso, para posteriormente proceder a la selección y, seguidamente copia de los mismos.

La copia de archivos se realiza de modo "forense" bit a bit, conservando todos los atributos originales del mismo, de modo que los metadatos que fueran incluidos en cada archivo permanecerán sin alteración alguna en el dispositivo destino de los mismos.

FORMACION DE RECURSOS HUMANOS

El desarrollo se lleva a cabo en el Departamento de Informática del Laboratorio de Criminalística del Centro de Investigaciones Forense del Poder Judicial de Formosa.

En el marco de este proyecto se desarrolla la Tesis para la Maestría en Tecnologías de la Información de la Facultad de Ciencias Exactas y Naturales y Agrimensura de la Universidad Nacional del Nordeste contando como director de la misma al Dr. David Luis la Red Martínez.

BIBLIOGRAFÍA

[1] Da Rocha, J. - de Luca. J. A. (2014) Informática y Delito. Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP).

[2] Piccirilli, D. (2013). La forensia como herramienta en la pericia informática. Revista Latinoamericana de Ingeniería de Software, I(6):237-240.

[3] Presman, G. D. (2011) Investigación forense en redes sociales. Presentado en el XV Congreso Iberoamericano de Derecho e Informática, Buenos Aires.

[4] Presman, G. D. (2014) ISO/IEC 27037. Normalizando la práctica forense informática. Power point. Recuperado a partir de http://www.copitec.org.ar/comunicados/CAIF 2014/CAIF- Presman.pdf.

[5] Salas Ordinola, E., Ramírez García, A.; Núñez Mori, O. (2011) Propuesta de Protocolo para la Recolección de Evidencias Digitales Relacionado con la Legislación Peruana. Pontificia Universidad Católica del Perú. Publicado en alfa-redi, portal de Derecho y Nuevas Tecnologías.

[6] Acurio del Pino, S. (2010) Manual de manejo de evidencias digitales y entornos informáticos, versión 2.0. AR: Revista de derecho informático.

[7] Bonilla, J. E. (2009) Principios de computación forense. Power point.

[8] J. L. Rivas López, Análisis forense de sistemas informáticos, Cataluña: Eureca Media, SL, 2009.

[9] Ben Stegner, Digital Article (July 2021), MUO Online Technology Publications, https://www.makeuseof.com/new-windows-pc-must-have-applications-to-install-first/

[10] Revista online Digital Trends, https://es.digitaltrends.com/computadoras/mejores-apps-para-windows/

[11] Artículo online, sitio web oficial de Microsoft, https://www.microsoft.com/en-us/store/collections/essentialapps

[12] Revista Digital Computerworld, https://www.computerworld.com/article/3602030/top-30-free-cheap-apps-for-windows-10.html

[13] Articulo online, sitio Web de Geekflare, https://geekflare.com/es/nirsoft-utilities/

[14] Sitio Web de Nirsoft, https://www.nirsoft.net