# Software para recolección de evidencias digitales rápidas en sistemas Windows

# Software for rapid digital evidence collection on Windows systems

**Marcos Adrián Monti**
Universidad Nacional del Nordeste, Corrientes, Argentina
marcosadrian65@gmail.com

**David Luis la Red Martínez**
Universidad Nacional del Nordeste, Corrientes, Argentina
lrmdavid@exa.unne.edu.ar
ORCID: 0000-0003-2038-6468

doi: https://doi.org/10.36825/RITI.11.24.009

Recibido: Septiembre 09, 2023
Aceptado: Diciembre 01, 2023

**Resumen:** En el campo de la Informática Forense, existen numerosos criterios a tener en cuenta a la hora de determinar qué elementos resultan pertinentes para obtener información útil que sirva para esclarecer una causa. En un procedimiento de allanamiento, cuando existen numerosos elementos tecnológicos que podrían ser candidatos al secuestro para realizar análisis exhaustivos en el laboratorio, se hace necesario discernir qué elementos serían de interés y cuáles no aportarían información útil, debido a que los tiempos de análisis crecen exponencialmente, a medida que se añaden más equipos y dispositivos de almacenamiento masivo a la lista de equipos a secuestrar. En el presente trabajo se presenta un software de aplicación para obtención de evidencia digital forense durante procedimientos de allanamiento, de acuerdo con el 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, Evidencia Digital, Informática Forense, Virtualización, Imagen Forense.*

**Abstract:** In the field of Digital Forensics, there are numerous criteria to consider when determining which elements are relevant for obtaining useful information to clarify a case. During a search and seizure procedure, when there are numerous technological items that could be candidates for confiscation for in-depth analysis in the laboratory, it becomes necessary to discern which elements would be of interest, and which would not provide useful information. This is because the analysis times grow exponentially as more equipment and mass storage devices are added to the list of items to be seized. In this paper, we present an "on-site" application software for obtaining digital forensic evidence during search and seizure procedures, following the current protocol of action. This software will also be used as an "indicator" of the content of the equipment under analysis, allowing the acting expert to make decisions (such as whether to confiscate a specific piece of equipment or not) at the location where the procedure is being carried out.

***Keywords:*** *User Activity, Operating System, Digital Evidence, Computer Forensics, Virtualization, Forensic Image.*

## 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; en el ámbito 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. Asimismo, 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 ellos, y la forma en que éstos llevaron a cabo la concreción de aquellos.

En general, la criminalística se puede definir como la reconstrucción de una historia a partir de las huellas que esta ha dejado; es la acción de observar a detalle los acontecimientos y enfocarse en el esclarecimiento de crímenes o delitos, a través del uso de la ciencia [1], [2]. En otras palabras, la criminalística se encarga del análisis científico de un sitio donde se ha cometido posiblemente un delito, y de la validación pericial de las evidencias que genera.

La Informática o 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 [3]. De esta manera, la Informática Forense actúa como una rama de la Informática que provee un complemento a la Criminalística clásica, enfocándose en el análisis de las evidencias digitales, que pudiesen existir, en cualquier escena del hecho.

Resulta necesario destacar que, aun cuando un delito no sea informático, es altamente probable que existan pruebas digitales que pudieran resultar de interés o aportar datos que sirvan para esclarecer la causa que se investiga, y, en general, es posible afirmar que casi todas las actividades que se realizan con un dispositivo (de forma manual o automática) dejan una evidencia en forma de archivos de logs, mensajes, registros en una base de datos, registro de ubicaciones, datos de *login*, etc., la cual puede analizarse junto con el resto de pruebas de un caso, a fin de aportar información útil para la resolución del mismo.

En el presente trabajo se plantea la realización de un software que sea capaz de obtener dicha información, específicamente en sistemas Windows, a fin de posibilitar la captura de datos relevantes de forma rápida en cualquier dispositivo compatible; esta información podrá servir tanto como para tener una vista previa del contenido de dicho equipo o en su defecto, utilizar el resguardo de estos datos como información útil a la causa, sin necesidad de proceder a realizar mayores operaciones sobre el equipo original, evitando de esa manera el secuestro del mismo.

## 2. Estado del arte

En la actualidad, los discos duros de equipos tipo PC (computadoras personales) que ejecutan alguna versión de *Microsoft Windows*, pueden llegar a tener capacidades de entre 128 Gigabytes a 1 Terabyte o más, por lo cual la cantidad 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 virtuales o copias forenses de los discos duros de los equipos aportados, con su correspondiente cálculo de valor hash, a fin de proceder a analizar los mismos, utilizando virtualización del sistema operativo [4] o algún software específico que permita montar dichas imágenes y sus particiones, conjuntamente con su sistema de archivos, sin tener que utilizar ni modificar el disco físico original [4], [5].

Esta práctica, sin embargo, suele demandar cantidades enormes de espacio de almacenamiento en el 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 judicial 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 de acceso aleatorio (RAM por sus siglas en inglés) y capacidad de almacenamiento en disco, siendo necesario en muchas ocasiones contar además con un

servidor de almacenamiento en red o unidad de almacenamiento en red (NAS por sus siglas en inglés), instalado preferentemente 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 [6], para luego proceder al análisis de estos según los criterios establecidos por el perito a cargo; sin embargo, esas herramientas 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.

Esto resulta especialmente útil en aquellos casos en los cuales no se requiere un análisis de gran profundidad (principalmente escaneo de superficie para imágenes, videos, audio o documentos borrados), sino obtener datos generales del/los usuario/s del sistema y la actividad reciente del/los mismo/s (archivos recientemente abiertos, historial de navegación web, cuentas de usuario registradas, hora de encendido y apagado del equipo, etc.). Dicho software resulta también de utilidad fundamental en aquellos casos donde el equipo de informática forense está procediendo, de manera independiente o conjuntamente con otras fuerzas de seguridad, a cumplir con una orden de allanamiento [7], la cual requiere obtener datos rápidamente de los equipos tipo PC, Notebook o Netbook ejecutando sistemas Windows que, potencialmente, podrían aportar datos de interés a la causa investigada, pero, no es posible o no resulta conveniente, por razones prácticas, secuestrar dichos equipos, de acuerdo a los protocolos correspondientes [7], para realizar el análisis propiamente dicho en el laboratorio de Informática Forense.

Las órdenes de allanamiento, por lo general, se conciben teniendo en cuenta un objetivo específico, el cual siempre consiste en recopilar algún tipo de información sobre los usuarios de los sistemas, de acuerdo con el tipo de investigación que se está llevando a cabo y que involucra un delito cometido a través de medios informáticos (ciberdelitos). Existen por lo tanto instrucciones o pautas específicas a seguir sobre los equipos o dispositivos de los cuales se quiere extraer información. En los casos en que se requieren datos en general, como se mencionó anteriormente, es posible resguardar la información solicitada en un medio extraíble (disco portátil o pendrive), que esté totalmente en blanco, de manera que se proceda a resguardar dicho medio (conteniendo la copia de datos del/los equipo/s) y no el equipo original. Todo ello posterior a la elaboración del formulario de cadena de custodia correspondiente, además del sellado, precintado (con número único) y firma de testigos, del paquete que contendrá el medio extraíble con la información solicitada.

## 3. Materiales y métodos

Siguiendo la pauta de recolectar información disponible en los sistemas *Windows*, se realizará un análisis de lo que se tiene a disposición en este aspecto. De acuerdo con lo que se visualiza en la mayoría de las versiones del mismo, así como en lo sugerido desde sitios web como el sitio *www.makeuseof.com* [8], *es.digitaltrends.com* [9], *www.microsoft.com* [10] y *www.computerworld.com* [11], 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, constituye 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 consultas realizadas en los mismos, obteniendo datos extra como el tipo de búsqueda realizada (texto, imágenes, videos), y la fecha y hora en que se realizaron.

### *3.1. Datos de Aplicaciones Comunes en Windows*

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*, como por ejemplo *Instagram*, *Tik Tok*, *Telegram* y *WhatsApp Desktop*, etc., y otras fuentes como ser redes sociales (RRSS

por su acrónimo), se ha priorizado capturar la actividad del usuario a través de los navegadores de Internet, sin embargo, se abordará este aspecto en futuras actualizaciones del software.

Los navegadores de Internet poseen, adicionalmente, información privada sobre los perfiles de usuario guardados por cada red social, sitio, cuenta bancaria, etc., a la que los mismos han accedido; por lo cual, además de datos de navegación y marcadores, tendríamos datos sobre las cuentas resguardadas en dicho navegador, siempre y cuando los usuarios hayan decidido recordar las mismas en dicho navegador.

### 3.1.1. Navegador Google Chrome

En cuanto a navegación en la red se refiere, es en la actualidad, por margen amplio, el navegador más utilizado [12], tanto en el mercado de PC's de escritorio o *laptops* como en equipos móviles, por lo cual resulta indispensable conocer los datos que contiene, así como las distintas opciones para obtenerlos. El navegador incluye una sección desde la cual es posible acceder a la sesión de usuario activa además de información adicional como los datos de pago y contraseñas almacenadas en el navegador como puede visualizarse en la Figura 1.

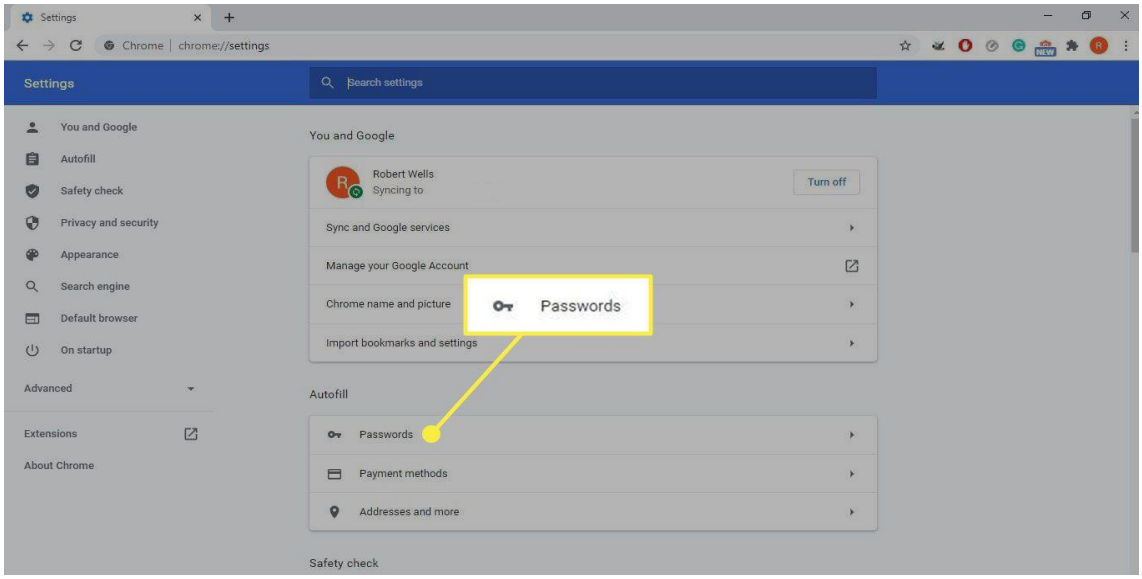



**Figura 1**. Datos de usuario en el Navegador Google Chrome [13].

La figura anterior, muestra la ruta de acceso típica ("Chrome://settings") que debe escribirse en la barra de navegación para visualizar la configuración en el navegador *Chrome* de la empresa *Google*. Es posible encontrar en la misma las secciones *passwords* o contraseñas, que permite configurar las distintas claves almacenadas en el mismo, organizadas por cada sitio web o red social a la cual el usuario tiene acceso.

Esta información resulta fundamental para un sinnúmero de casos donde ocurren delitos informáticos, ya que, permiten asociar al usuario físico o real de la PC o equipo portátil que se está analizando con los distintos *avatar's* o usuarios virtuales que el mismo utiliza en las redes sociales o sitios web a los que accede.

Por otra parte, resulta factible realizar un análisis de la actividad del usuario utilizando información que guarda el mismo sistema operativo en el Visor de eventos [14], [15].

### 3.1.2. Visor de eventos de Windows

En los sistemas operativos Windows, existe un servicio que se encarga de registrar en segundo plano todos los eventos que ocurren en el uso diario de un equipo, estos sucesos se registran para poder realizar un "historial", en caso de que se registren fallas, a fin de localizar su origen y de esta manera poder plantear una posible solución a la misma.

Estas fallas o eventos inesperados pueden ocurrir por diversas cuestiones, por ejemplo, un error en la ejecución de código de algún programa, una excepción, un problema con un dispositivo físico o virtual, etc., los

cuales pueden terminar desencadenando una serie de sucesos que conllevan a la inestabilidad e incluso el colapso total del sistema operativo huésped.

De esta forma, podemos separar los eventos que recoge el sistema operativo en cinco apartados diferentes:

- *Aplicación*: todos los eventos que están relacionados con las aplicaciones del sistema operativo. Desde lanzamientos con éxito y sin problemas hasta actualizaciones, cambios internos y, por supuesto, errores.
- *Seguridad*: los eventos de seguridad que tienen lugar dentro del sistema operativo. La mayoría de ellos son simplemente auditorías que no aportan gran cosa, pero si ocurre una quiebra de seguridad, o simplemente un inicio de sesión no autorizado, esta aparecerá reflejada aquí.
- *Instalación*: registros de las instalaciones del sistema. Podemos encontrar información sobre los programas que se han instalado, así como de las actualizaciones del sistema.
- *Sistema*: este es el apartado más completo y que más información interesante ofrecerá. En él se puede encontrar todo lo que ocurre en el sistema, desde eventos que se han completado con éxito hasta los errores más críticos causados por el Kernel o por algún controlador.
- *Eventos reenviados*: como su nombre indica, aquí se registran los eventos que han sido reenviados a otras categorías internas del sistema, o a un servidor central.

De esta formal, gracias a estos registros de Windows se podrá saber al detalle todo lo que está pasando bajo el escritorio. Seguramente se podrá encontrar información de lo más interesante que, de otras formas, hubiera pasado totalmente desapercibida (Figura 2).

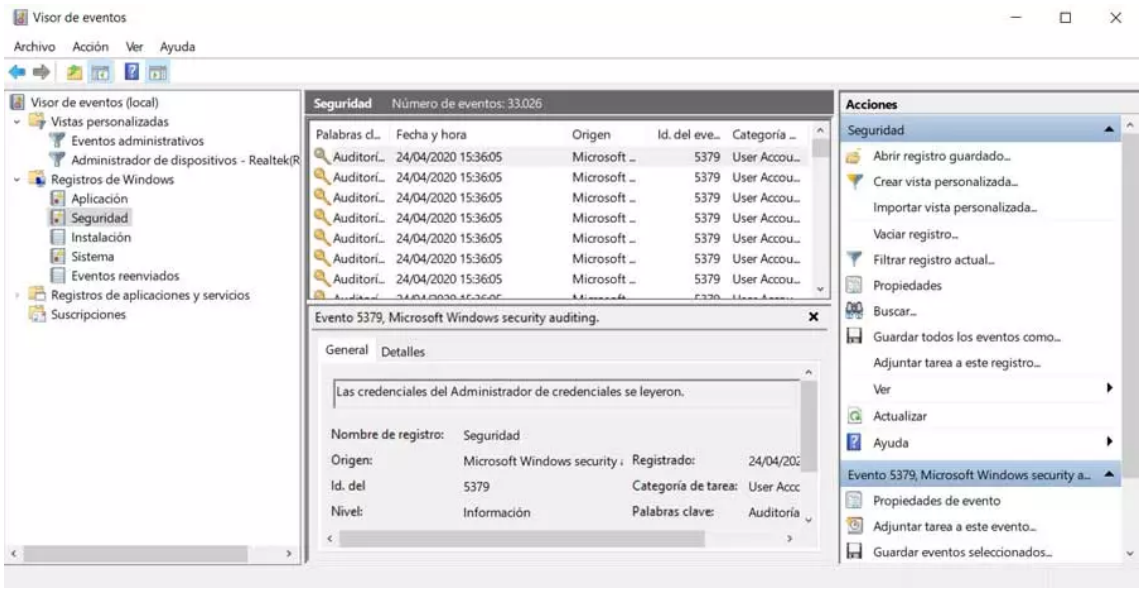



**Figura 2.** Aplicación Visor de Eventos de Windows [Fuente: propia]. Desde aquí es posible inspeccionar todos sucesos y eventos, agrupados por categoría, que están almacenados en los registros del Sistema.

### 3.1.3. Explorador de Windows

Es el gestor de archivos instalado por defecto en *Windows*, y que utilizan todas las versiones de dicho sistema operativo a partir de *Windows 95*, tiene la capacidad de administrar ficheros, carpetas y conexiones de red, así como buscar archivos y componentes relacionados [16]. En sus versiones sucesivas, ha ido incorporando nuevas funciones no relacionadas con la administración de archivos, como la reproducción de audio y videos, el inicio de programas, entre otros, de la misma forma, el escritorio y la barra de tareas también han pasado a formar parte de este explorador [16].

Es útil destacar que la expansión de funcionalidades de esta herramienta desde su origen y la integración cada vez más profunda con otros elementos del sistema operativo, hacen posible sacar provecho de esta, a fin de obtener cierta información de uso, por ejemplo, es factible obtener la lista de archivos recientemente usados, con lo cual se podría saber qué elementos fueron recientemente abiertos, creados y editados. Además de la información que se pudiera recabar en el sistema operativo y sus aplicaciones, también sería de interés poder realizar una

visualización y copia forense de algunos o todos los archivos de interés presentes en la PC, por lo general del tipo imágenes, video, documentos y audio.

### *3.2. Software y aplicaciones para extracción de datos en Windows*

De acuerdo con 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. De igual manera, 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 obtenerlos, sin embargo, uno de los más mencionados por los sitios online especializados [17] consiste en el uso de las numerosas herramientas gratuitas disponibles en el sitio de herramientas de *Nirsoft* [18] (Figura 3).

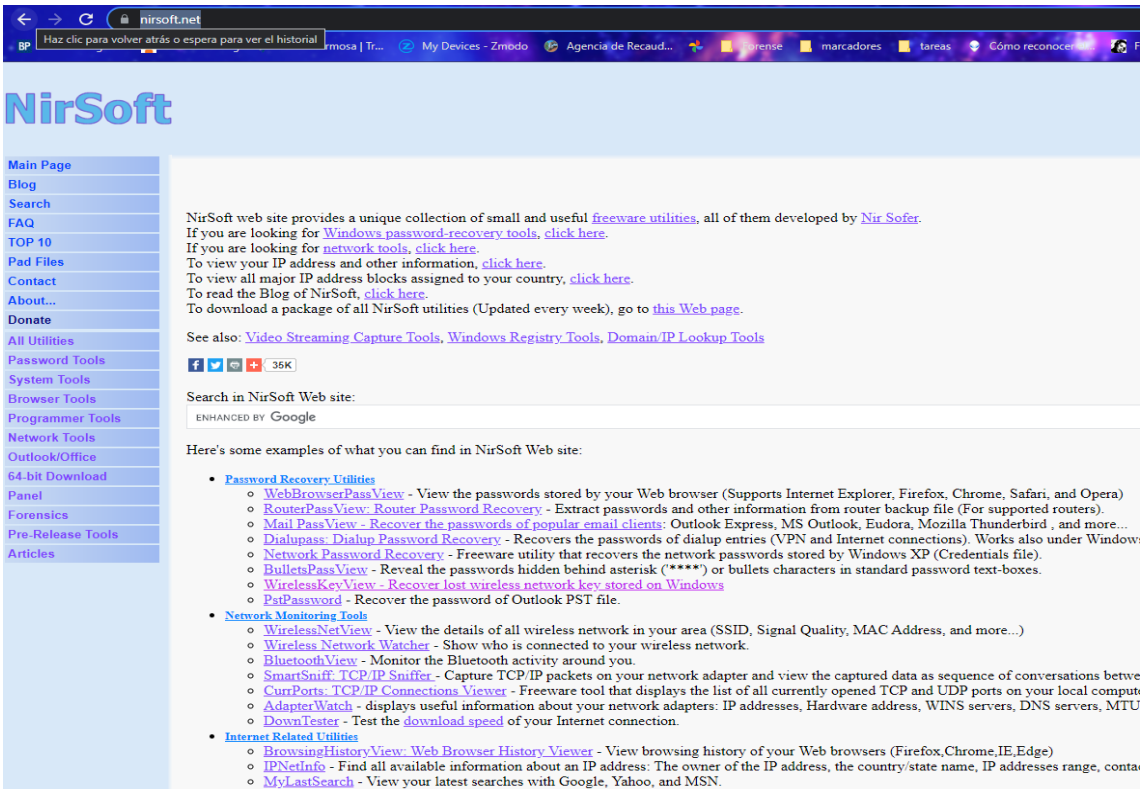



**Figura 3.** Sitio Web de herramientas de *Nirsoft* [18].

#### 3.2.1. Historial de navegación del usuario

La aplicación *BrowsingHistoryView* es una utilidad para sistemas *Windows* que lee los datos del historial de diferentes navegadores web (*Mozilla Firefox*, *Google Chrome*, *Internet Explorer*, *Microsoft Edge*, *Opera*) y muestra el historial de navegación de todos estos navegadores web en una tabla [19]. La tabla del historial de navegación contiene la siguiente información:

- Dirección URL visitada.
- Título.
- Hora de la visita.
- Recuento de visitas (cantidad de veces que se accedió al mismo sitio).
- Navegador web.
- Perfil de usuario.

Asimismo, la herramienta permite ver el historial de navegación de todos los perfiles de usuario en un sistema en ejecución, así como obtener el historial de navegación desde un disco duro externo. También es posible exportar

el historial de navegación a un archivo CSV (valores separados por coma), a un archivo HTML o incluso XML, desde la línea de comandos, sin utilizar ningún tipo de interfaz de usuario (Figura 4).

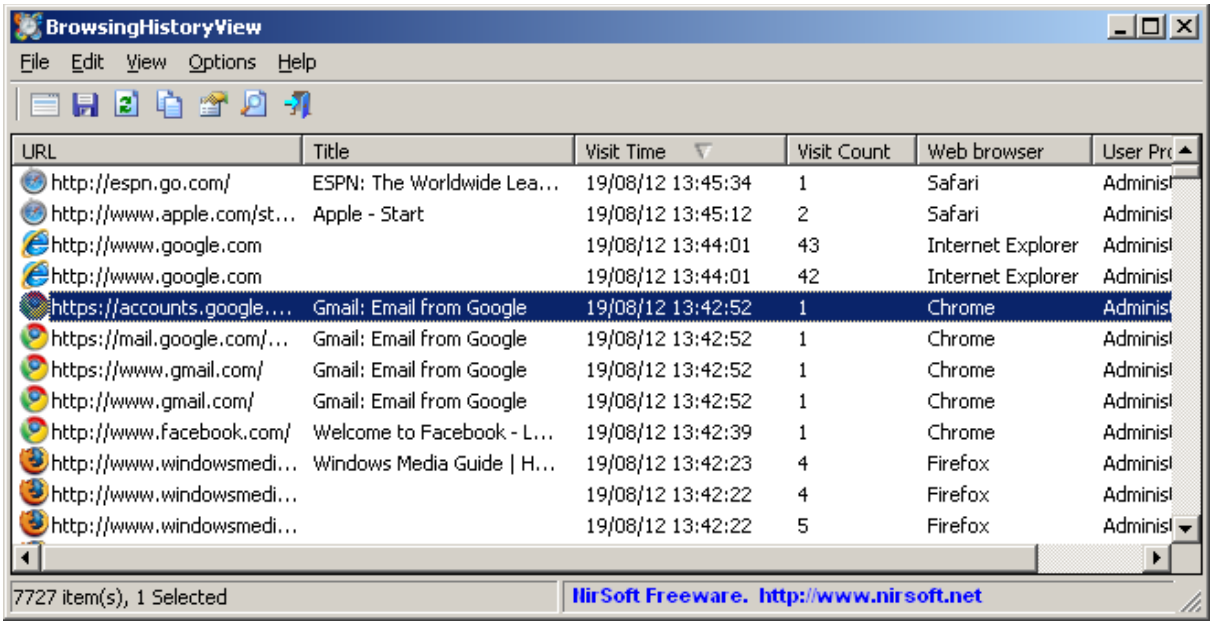



**Figura 4.** Ventana principal de la Aplicación *BrowsingHistoryView* [19].

3.2.2. Datos de cuentas almacenadas

Continuando con el análisis de navegadores la herramienta *WebBrowserPassView* o visor de contraseñas en navegadores web, resulta de gran utilidad, al posibilitar la extracción de datos de Internet *Explorer*, *Microsoft Edge*, *Mozilla Firefox*, *Google Chrome*, *Safari*, y *Opera*. Es capaz de recuperar usuario y contraseña de cualquier sitio web, incluyendo *Facebook*, *Yahoo!*, *Google* y *Gmail*, con la única restricción de que dichas credenciales hayan sido almacenadas previamente por dicho navegador [20].

3.2.3. Últimas búsquedas realizadas

Aprovechando también datos almacenados en navegadores web, se utiliza la herramienta *MyLastSeach* o mis últimas búsquedas, a fin de obtener información relacionada con los términos de consultas realizadas en los motores de búsqueda online más populares como ser *Google*, *Yahoo!* o *MSN*; es posible conocer también datos de búsquedas realizadas en sitios de redes sociales como ser *Twitter*, *Facebook* o *MySpace*.

3.2.4 Historial de actividad de usuario

Con el software *LastActivityView* o visor de últimas actividades se tiene una herramienta que recopila información de varias fuentes dentro de un sistema Windows en ejecución y presenta un registro de las acciones realizadas por el usuario y los eventos ocurridos en esa computadora (Figura 5).

3.2.5. Historial de archivos abiertos

A fin de obtener más información sobre documentos que hubiesen sido visualizados o editados en el sistema, resulta útil contar con la información de la herramienta *OpenedFilesView* o vista de archivos abiertos, la cual proporciona información detallada sobre el historial de archivos abiertos en el sistema.

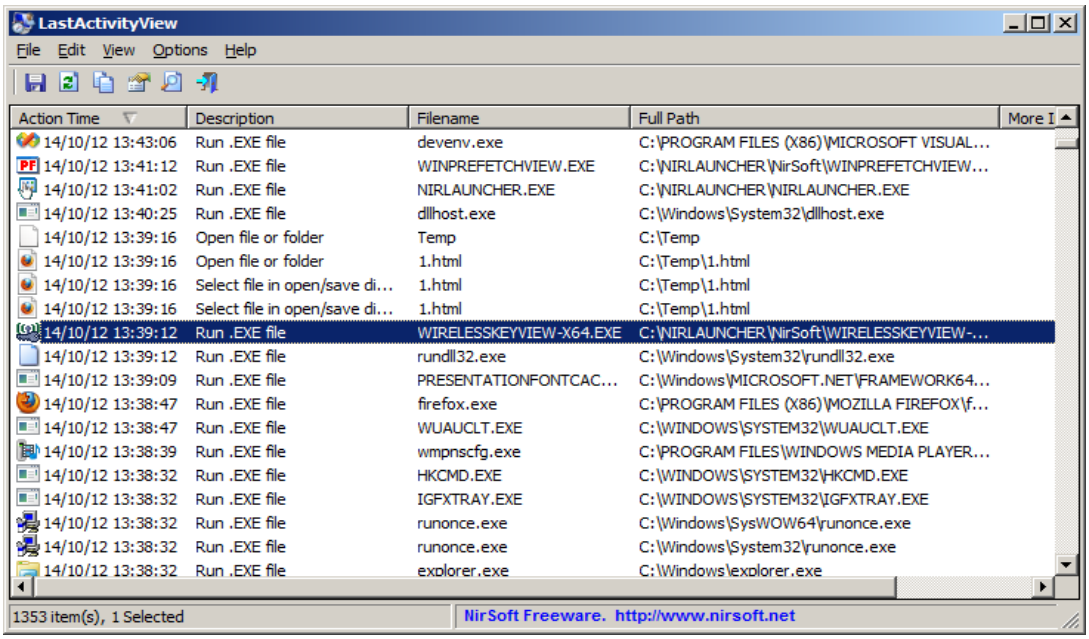



**Figura 5.** Ventana principal de la Aplicación *LastActivityView* [21].

3.2.6. Dispositivos conectados por USB

Cuando se realizan búsquedas en un allanamiento en proceso, resulta útil poder identificar, de alguna manera, si existen unidades extraíbles o dispositivos externos de almacenamiento masivo, los cuales podrían ser unidades simples tipo pendrive o discos rígidos portátiles. La razón de esto es que, muchas veces, la información más sensible y que, podría ser de interés a la investigación en curso, se resguarda en dispositivos externos a la/s computadora/s, generalmente, a fin de contar con un *backup* o respaldo de dicha información, en caso de fallo de los equipos tipo PC utilizados normalmente o simplemente como un almacén externo de archivos privados que no se desea almacenar o mantener en los dispositivos tipo PC o Laptop del domicilio.

La herramienta *USBDeview* o vista de dispositivos USB, es otra herramienta que permite conocer la lista de dispositivos que están conectados actualmente a la computadora anfitrión, así como todos los dispositivos USB que se utilizaron en la misma.

3.2.7 Redes inalámbricas almacenadas

La aplicación *WirelessKeyView* o vista de claves inalámbricas, permite conocer el detalle de las redes inalámbricas a las cuales se conecta el equipo, esta información resulta útil especialmente en dispositivos como notebooks o laptops, debido a su característica portátil que permite que se utilicen fácilmente en cualquier lugar lejano a la red física. Esto permite conocer los puntos de acceso a través de los cuales podría haberse cometido un potencial delito que involucre acceso ilegal a redes privadas, obtención de información protegida, vulnerar sitios web de acceso público a través de Internet, etc.

3.2.8. Copia forense de archivos

De acuerdo con lo visto en apartados anteriores, sería posible concluir que la información básica del sistema anfitrión podría ser cubierta, utilizando individualmente estas herramientas, sin embargo, es necesario destacar la necesidad de contar con la posibilidad de realizar copia de determinados archivos, que podrían ser de tipo audio, imágenes, documentos o videos, que podrían ser de interés, para la causa judicial que se investiga.

Se utiliza para ello la herramienta *Robocopy* o copia robusta de archivos, una herramienta incorporada en todas las versiones de Windows y que proporciona una forma eficiente y rápida de obtener copias de archivo de cualquier disco de origen.

Con esta utilidad es posible efectuar búsquedas y visualizaciones 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 (Figura 6).

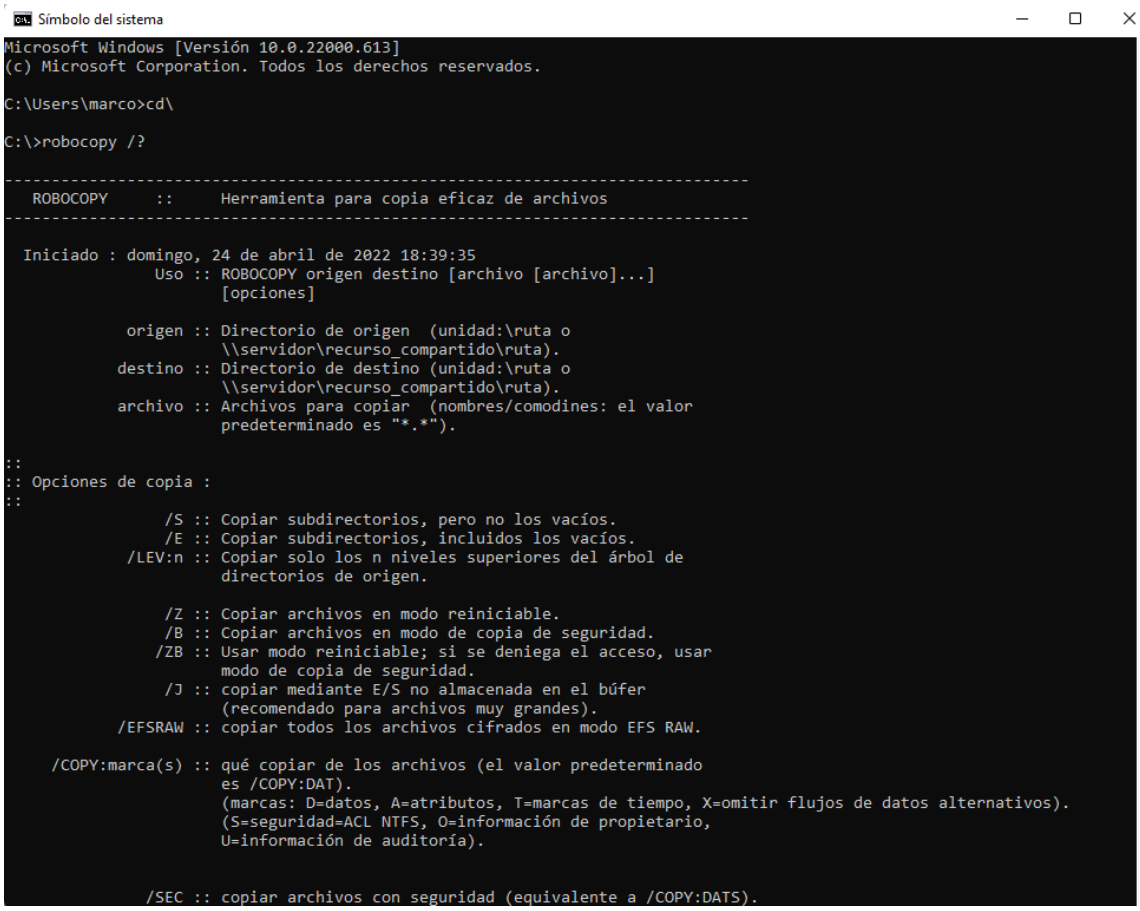



**Figura 6.** Ventana de comandos de la aplicación *Robocopy* [Fuente: Propia].

Finalmente, en cuanto a la actualización de componentes, cabe mencionar que, de momento, es posible actualizar cada aplicación de *Nirsoft* de forma manual, reemplazando las incluidas por nuevas versiones, esto nos permitiría mantener compatibilidad con las actualizaciones de Windows y el software de terceros como ser los navegadores Web.

## 4. Resultados

De acuerdo con 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, con una interfaz simple, buscando un uso intuitivo y entendible, incluso para personal no técnico.

Conforme 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. Para el desarrollo de la aplicación se utilizó el entorno de programación de *Visual Studio 2019* y el leguaje *C#* junto con las herramientas mencionadas de *Nirsoft* y la de copia incorporada *Robocopy*.

La aplicación muestra dos secciones donde se puede elegir el destino (carpeta o directorio) donde van a resguardarse todos los datos, y la opción de copia forense de archivos o recuperación de datos del sistema. El primer formulario que se visualiza en “1-Seleccione Carpeta de Destino”, permite 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.

Una vez seleccionada la unidad o carpeta destino, se crea una nueva carpeta con el nombre correspondiente al equipo en el cual se está ejecutando la aplicación. La clase *System* que incorpora *C#* posee a su vez la clase *Environment*, desde la cual es posible conocer datos básicos del sistema huésped [22] como por ejemplo la versión del sistema operativo, obtener el directorio del sistema, el nombre del usuario actual, la lista de discos lógicos disponibles, etc. (Figura 7).

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 (Figura 8). Dicha información es obtenida a través del lanzamiento o ejecución de las aplicaciones mencionadas previamente 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 con la información que se quiere obtener.

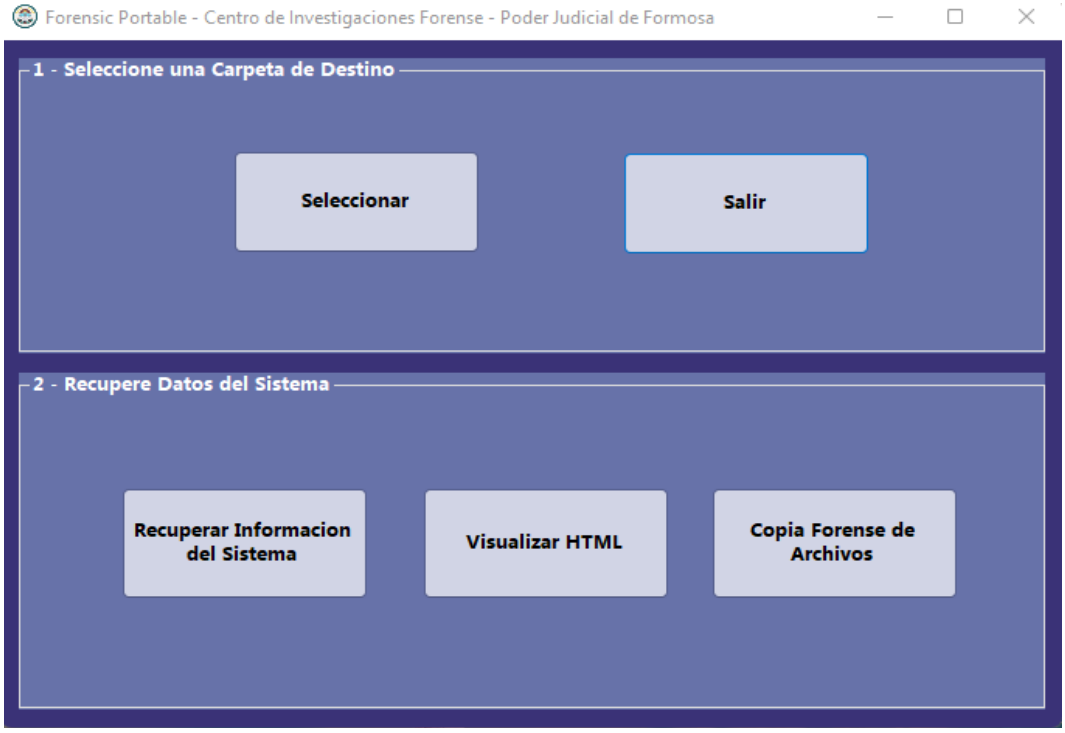



**Figura 7.** Ventana Principal de la aplicación *Forensic Portable* [Fuente: Propia].

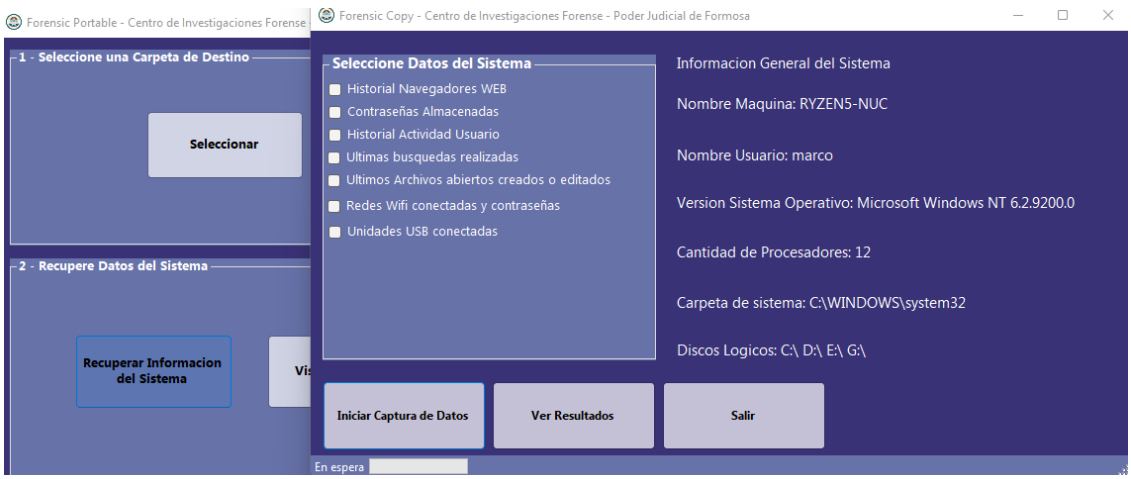
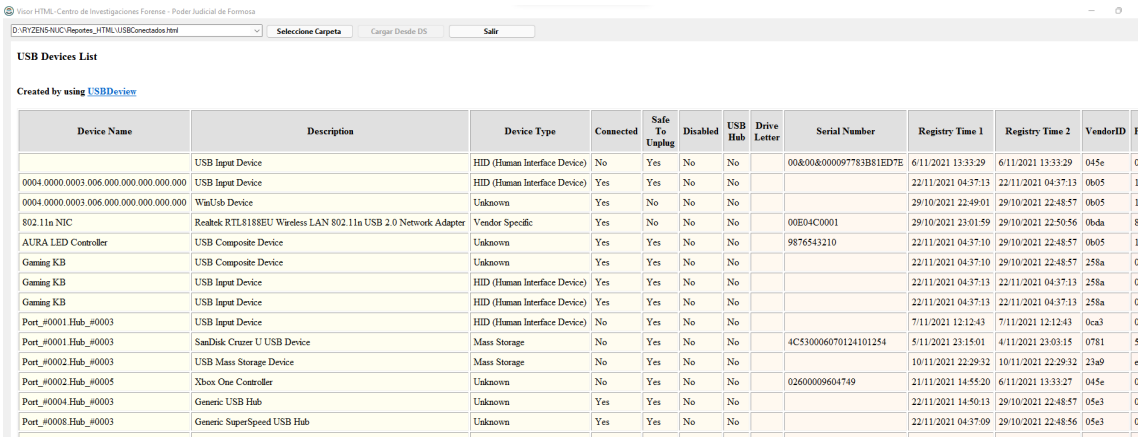



**Figura 8.** Ventana módulo de recuperación de datos del sistema [Fuente: Propia].

A fin de posibilitar la visualización inmediata de los resultados, se provee un módulo para visualizar archivos de tipo *HTML* en el botón *Ver Resultados*, el cual provee un vínculo hacia el formulario llamado *Visualizador HTML*. El mismo cuenta con un control de tipo *ComboBox* [23], que funciona como lista desplegable y un botón desde el cual se puede indicar una unidad o carpeta desde donde se realizará una búsqueda automática de todos los archivos HTML encontrados a fin de cargarlos en la lista desplegable y, posteriormente, proceder a visualizarlo en la parte central del formulario (Figura 9).

Finalmente, en el último botón del menú principal se tiene el acceso al módulo de resguardo de archivos, con el que se podrá realizar un respaldo [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 previsualización de estos, utilizando controles especiales incorporados al formulario (Figura 10).




| Device Name | Description | Device Type | Connected | Safe To Unplug | Disabled | USB Hub | Drive Letter | Serial Number | Registry Time 1 | Registry Time 2 | VendorID |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | 00&00&000097783B81EDTE | 6/11/2021 13:33:29 | 6/11/2021 13:33:29 | 045e |
| 0004.0000.0003.006.000.000.000.000.000 | USB Input Device | HID (Human Interface Device) | Yes | Yes | No | No | | | 22/11/2021 04:37:13 | 22/11/2021 04:37:13 | 0b05 |
| 0004.0000.0003.006.000.000.000.000.000 | WinUsb Device | Unknown | Yes | No | No | No | | | 29/10/2021 22:49:01 | 29/10/2021 22:48:57 | 0b05 |
| 802.11n NIC | Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter | Vendor Specific | Yes | No | No | No | | 00E04C0001 | 29/10/2021 23:01:59 | 29/10/2021 22:50:56 | 0bda |
| AURA LED Controller | USB Composite Device | Unknown | Yes | Yes | No | No | | 9876543210 | 22/11/2021 04:37:10 | 29/10/2021 22:48:57 | 0b05 |
| Gaming KB | USB Composite Device | Unknown | Yes | Yes | No | No | | | 22/11/2021 04:37:10 | 29/10/2021 22:48:57 | 258a |
| Gaming KB | USB Input Device | HID (Human Interface Device) | Yes | Yes | No | No | | | 22/11/2021 04:37:13 | 22/11/2021 04:37:13 | 258a |
| Gaming KB | USB Input Device | HID (Human Interface Device) | Yes | Yes | No | No | | | 22/11/2021 04:37:13 | 22/11/2021 04:37:13 | 258a |
| Port_#0001.Hub_#0003 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | | 7/11/2021 12:12:43 | 7/11/2021 12:12:43 | 0ca3 |
| Port_#0001.Hub_#0003 | SanDisk Cruzer U USB Device | Mass Storage | No | Yes | No | No | | 4C530006070124101254 | 5/11/2021 23:15:01 | 4/11/2021 23:03:15 | 0781 |
| Port_#0002.Hub_#0003 | USB Mass Storage Device | Mass Storage | No | Yes | No | No | | | 10/11/2021 22:29:32 | 10/11/2021 22:29:32 | 23a9 |
| Port_#0002.Hub_#0005 | Xbox One Controller | Unknown | No | Yes | No | No | | 02600009604749 | 21/11/2021 14:55:20 | 6/11/2021 13:33:27 | 045e |
| Port_#0004.Hub_#0003 | Generic USB Hub | Unknown | Yes | Yes | No | No | | | 22/11/2021 14:50:13 | 29/10/2021 22:48:57 | 05e3 |
| Port_#0008.Hub_#0003 | Generic SuperSpeed USB Hub | Unknown | Yes | Yes | No | No | | | 22/11/2021 04:37:09 | 29/10/2021 22:48:56 | 05e3 |

**Figura 9.** Módulo visor HTML [Fuente: Propia].

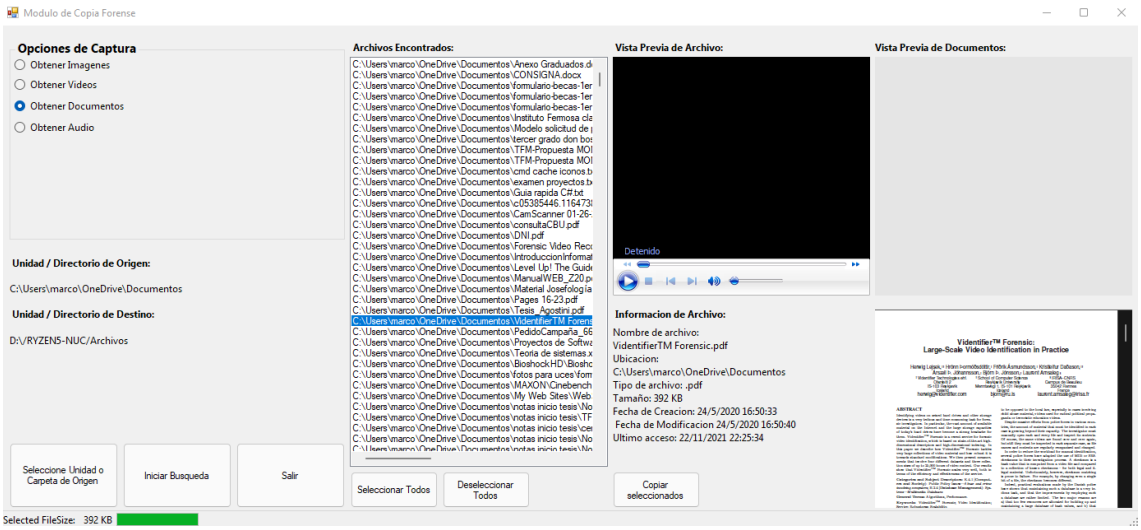



**Figura 10.** Módulo de copia forense [Fuente: Propia].

Es necesario mencionar que el presente desarrollo se enmarca en la normativa descripta en el Protocolo de Actuación para Pericias Informáticas [24], vigente actualmente en el Centro de Investigaciones Forense del Poder Judicial de la Provincia de Formosa, Argentina.

A fin de ilustrar el procedimiento de copia, utilizando la herramienta, se muestra un ejemplo (Figura 11) donde se realiza una búsqueda muy simple de archivos de tipo imágenes, inicialmente, el proceso realizara una búsqueda en la carpeta inicial detectando y listando las coincidencias para los tipos de archivos soportados, seguidamente, realizara el mismo proceso de forma recursiva para todas las subcarpetas encontradas, mostrando el resultado como una lista de archivos seleccionable.

Es posible previsualizar los archivos a fin de facilitar el proceso de selección, ya que utilizando la tecla Ctrl y pulsando sobre cada elemento el mismo queda seleccionado, seguidamente, se puede iniciar el proceso de copia

forense pulsando en *Copiar seleccionados*; es importante destacar que la herramienta proporciona también el detalle de los metadatos correspondientes a cada archivo seleccionado.

Este módulo incluye soporte para la Selección múltiple de archivos en la lista de resultados de búsqueda, se mostrara además, en tiempo real, el tamaño que ocupa en el disco duro dicha selección (Figura 12).

Por cada archivo, es posible previsualizar el contenido (en el caso de documentos), o reproducirlo (para archivos multimedia), además, es posible conocer información básica sobre el mismo (ubicación, tamaño, etc.). El proceso de copia puede iniciarse una vez seleccionados los archivos de interés, mediante código, se procede a lanzar la aplicación *Robocopy* con parámetros especiales para poder mantener los datos originales de cada archivo en el proceso, se creará un nuevo sub-proceso dedicado para cada uno de los archivos a copiar, actualizando la barra de progreso incorporada en la barra de estado, a medida que dicha operación vaya finalizando.

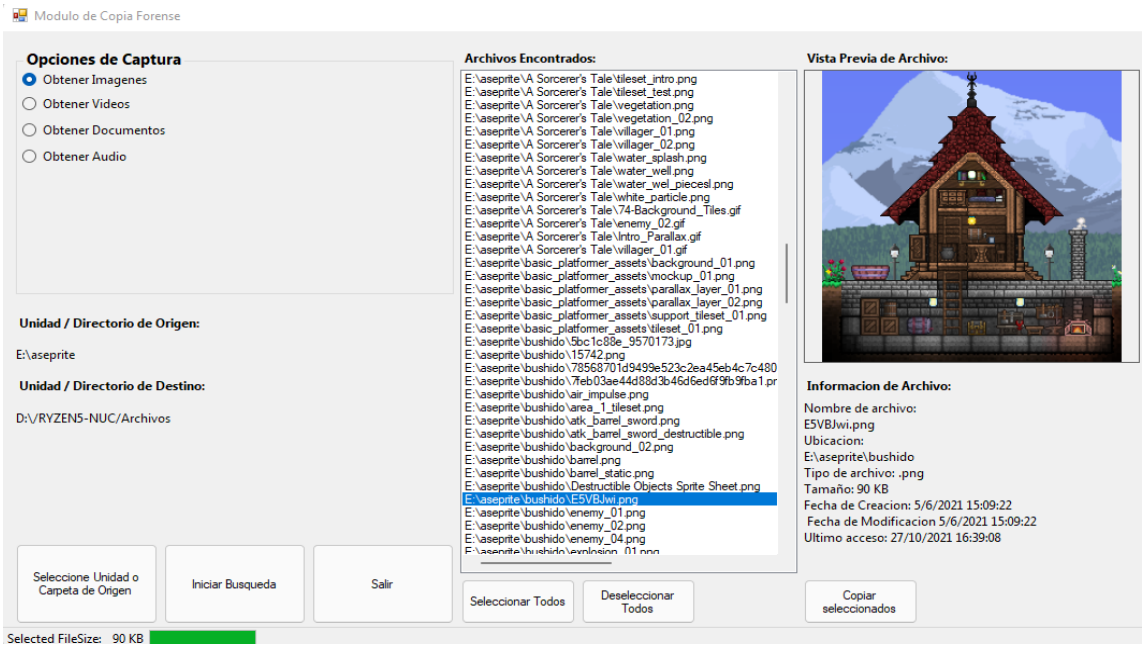



**Figura 11.** Módulo de copia forense, búsqueda de imágenes [Fuente: Propia].

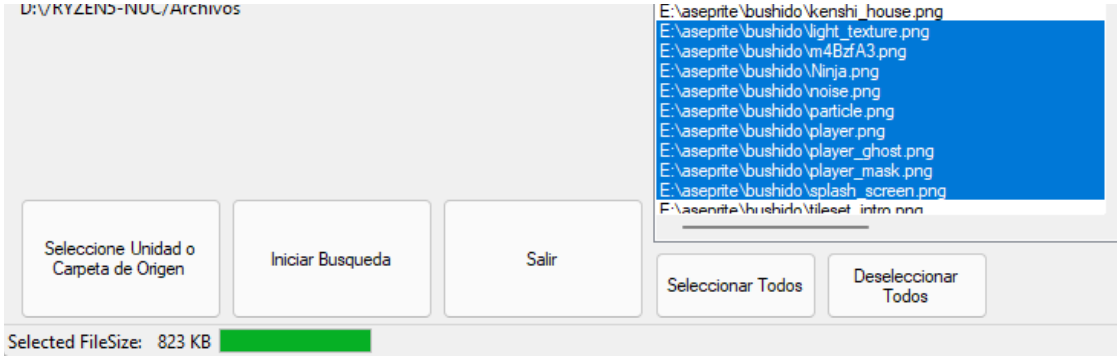



**Figura 12**. Módulo de copia forense, selección de archivos [Fuente: Propia].

## 5. Conclusiones

De acuerdo con lo mostrado precedentemente, ha sido factible aplicar las herramientas y métodos de extracción de datos estudiados para diseñar y codificar una aplicación capaz de satisfacer los requerimientos buscados. Con la combinación del uso de la tecnología .NET, comandos simples incluidos en sistemas Windows y aplicaciones de uso libre como las de *Nirsoft* [18], es posible obtener una gran cantidad de información sobre el uso del sistema.

Es necesario destacar que la posibilidad de realizar la copia forense de aquellos archivos que pudieran resultar de interés resulta fundamental a la hora de realizar un análisis más detallado de la información recabada (mediante sus metadatos correspondientes) [25], y poder proveer un informe más preciso y detallado, en la realización del informe pericial.

Debe mencionarse el hecho innegable de que la información provista por la posibilidad de realizar un estudio *in situ* de los equipos que se encuentran en el lugar, permite a los peritos actuantes centrar su investigación en aquellos dispositivos que arrojan un resultado positivo, de acuerdo siempre al tipo de información que se está buscando.

La posibilidad de obtener una copia forense de archivos individuales, de acuerdo a los criterios establecidos, además de registros en formato HTML de la información recabada, permite en muchos casos obtener información suficiente para ser útil por sí misma en una causa y evitar de esta manera el secuestro innecesario del equipo en cuestión, lo cual conlleva a un ahorro significativo de costos en cuanto a tiempo, debido a la necesidad de procesamiento masivo de información, y de almacenamiento, al no requerirse imágenes forenses de cada equipo que deban ser luego montadas para su respectivo análisis.

Como línea futura del trabajo está contemplado el estudio y desarrollo de un sistema de actualizaciones automáticas, para las aplicaciones relacionadas con este producto. Además, está previsto el soporte para aplicaciones instaladas a través de la *Microsoft Store*. Asimismo, se tiene proyectado evaluar la posibilidad de generar una versión de este sistema para el sistema operativo Linux, tomando como plataforma básica el GobLin, GNU/Linux para Gobiernos [26].

## 6. Referencias


[1] Bosquet Pastor, S. (2015). *Criminalística Forense*. Editorial Tirant Lo Blanch.

[2] Blanco, H. (2020). *Tecnología Informática e Investigación Criminal*. Editorial La Ley.

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

[4] Piccirilli, D. A. (2013). La forensia como herramienta en la pericia informática. *Revista Latinoamericana de Ingeniería de Software*, 1 (6), 237-240. https://doi.org/10.18294/relais.2013.237-240

[5] Acurio del Pino, S. M. (2010). Manual de manejo de evidencias digitales y entornos informáticos, versión 2.0. *AR: Revista de derecho informático*, (140). https://dialnet.unirioja.es/servlet/articulo?codigo=3259955

[6] Rivas López, J. L., Rifà Pous, H., Serra i Ruiz, J. (2009). *Análisis forense de sistemas informáticos*. UOC Universitat Oberta de Catalunya.

[7] Salas Ordinola, E., Ramírez García, A., Núñez Mori, O. (2011*).* Propuesta de Protocolo para la Recolección de Evidencias Digitales Relacionado con la Legislación Peruana. *AR: Revista de derecho informático*, 1-8. https://www.alfa-redi.org/sites/default/files/articles/files/salas.pdf

[8] Stegner, B. (2022). *15 Must-Have Windows Apps and Software for Any New PC*. https://www.makeuseof.com/new-windows-pc-must-have-applications-to-install-first/

[9] Lopes, M., López, J. (2021). *Las mejores apps para Windows que debes tener*. https://es.digitaltrends.com/computadoras/mejores-apps-para-windows/

[10] Muchmore, M. (2023). *The Best Apps in the Windows 11 Store for 2023.* https://www.pcmag.com/picks/best-apps-in-the-windows-11-store

[11] Bradley, S. (2021). *30+ free and cheap apps for Windows 10*. https://www.computerworld.com/article/3602030/top-30-free-cheap-apps-for-windows-10.html

[12] Martin, J. (2021). *Best web browsers. https://www.techadvisor.com/article/728377/best-web-browsers-2021.html*

[13] Orgera, S. (2023). *How to See Passwords in Chrome*. https://www.lifewire.com/show-passwords-in-chrome-4580283

[14] Microsoft. (2023). *Revisar eventos y errores mediante visor de eventos*. https://docs.microsoft.com/es-es/microsoft-365/security/defender-endpoint/event-error-codes?view=o365-worldwide

[15] Onieva, D. (2022). *Visualiza y gestiona de un modo más efectivo los eventos de Windows.* https://www.softzone.es/windows/como-se-hace/ver-eventos-fulleventlogview/

[16] Rouse, M. (2017). *Windows Explorer*. https://www.techopedia.com/definition/13522/windows-explorer

[17] Haider, K. (2022). *25 utilidades de NirSoft para aprovechar al máximo Windows.* https://geekflare.com/es/nirsoft-utilities/

[18] NirSoft. (2023). *Freeware utilities: password recovery, system utilities, desktop utilities - for Windows*. https://www.nirsoft.net/

[19]NirSoft. (2023). *BrowsingHistoryView - View the browsing history of your web browser*. https://www.nirsoft.net/utils/browsing_history_view.html
[20]NirSoft. (2023). *WebBrowserPassView - Recover lost passwords stored in your web browser*. https://www.nirsoft.net/utils/web_browser_password.html
[21]NirSoft. (2023). *LastActivityView - View the latest computer activity in Windows operating system*. https://www.nirsoft.net/utils/computer_activity_view.html
[22]Microsoft Learn. (2023). *Environment Class (System)*. https://docs.microsoft.com/en-us/dotnet/api/system.environment?view=net-6.0
[23]Microsoft Learn. (2023). *ComboBox Clase (System.Windows.Forms)*. https://learn.microsoft.com/es-es/dotnet/api/system.windows.forms.combobox?view=windowsdesktop-7.0
[24]Figueredo, R. (2021). *Protocolo de Actuación para Pericias Informáticas*. Poder Judicial de Formosa.
[25]Boixo, I. (2003). *Guía de buenas prácticas para el peritaje informático en recuperación de imágenes y documentos*. https://peritoit.files.wordpress.com/2012/03/guia-buenas-practicas-para-la-recuperacion-de-ficheros-e-imagenes.pdf
[26]Brys, C., La Red Martínez, D. L. (2022). GobLin: El Sistema Operativo GNU/Linux para Gobiernos. *Revista de Investigación en Tecnologías de la Información*, *10* (22), 1–14. https://doi.org/10.36825/RITI.10.22.001