Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencia de Datos y Matemáticas

Análisis Forense, Versión Técnica

MA2005B.201 Aplicación de criptografía y seguridad

Óscar Antonio Banderas Álvarez A01568492

Leonardo Laureles Olmedo A01659241

Carlos Mateos Perez A01654085

Diana Paola Cadena Nito A01197399

Daniel Sánchez Villarreal A01197699

En conjunto con: IPC Services

Supervisado por

Dr. Óscar Eduardo Labrada Gómez

Dr. Alberto Francisco Martínez Herrera

Monterrey, Nuevo León. Fecha: 22 de octubre de 2022

Índice

Resumen

El análisis forense digital se encarga de estudiar y analizar equipos y dispositivos tecnológicos, con el objetivo de obtener información que pueda ser útil como evidencia que pudiera ayudar a identificar, comprobar y solucionar delitos. En este caso, se trabaja con dos escenarios: el borrado de archivos y la introducción de virus a las computadoras. Para realizar esto, se utilizaron las herramientas de Recuva y Kaspersky Endpoint Security Cloud en el sistema operativo Windows. Con Recuva, se llevaron a cabo dos análisis y se recuperó el archivo que se había eliminado, entre otros. En cuanto a Kaspersky, se trató de infectar un dispositivo con malware pero estos fueron detectados por la herramienta. Contar con polítcas de ciberseguridad en una empresa es de suma importancia ya que las pérdidas o consecuencias de un ciberataque puede conllevar a pérdidas económicas de estas.

Palabras clave. *Análisis forense, Recuva, recuperación de datos, malware, Kaspersky.*

1. Introducción

En un mundo globalizado, el uso de los dispositivos electrónicos está al alcance de cualquier persona. Al hacer uso de estos dispositivos, las personas van dejando una huella digital; son datos que dan información acerca del comportamiento humano. (Gutiérrez Puebla, 2018). Esta huella digital luego puede ser utilizada por distintas organizaciones o empresas para identificar su población objetivo. El desarrollo digital se ha considerado como un gran avance para la humanidad pero también se debe tomar en consideración sus vulnerabilidades. Las personas están cada vez más expuestas a estos medios y no todas conocen las medidas de seguridad que se deben tomar, poniendo tanto a su información como a sí mismos en riesgo.

El concepto de la ciberseguridad ha sido cada vez más relevante por estos mismos desarrollos tecnológicos. Los datos que se generan en estos espacios se les puede dar un uso con fines buenos o malos. Cuando se habla de seguridad en medios digitales, deben de incluirse los peligros asociados, como lo son los ataques cibernéticos. Estos han ido aumentando y algunos ejemplos de ciberataques son: amenazas persistentes avanzadas, ataques contra infraestructuras críticas, ataques contra redes y sistemas, espionaje, infección con malware, robo y publicación de información clasificada o sensible. (Olmedo & Gavilánez, 2018).

En México, se estima que los ciberataques cuestan aproximadamente 24 millones de dólares anualmente. Los medios más comunes por los cuales se realizan estos ciberataques en el país son sitios web maliciosos, correos electrónicos, memorias USB y dispositivos externos. Además, en 2018, dos de tres empresas fueron víctimas de un ciberataque y México se posicionó en el segundo lugar de América Latina en cuanto a esto mismo. (RAMOS-TOXTLE, 2020). Existen distintas medidas que cualquier gobierno puede emplear y distintos procesos que son llevados a cabo cuando suceden incidentes de este tipo.

El análisis forense digital es un campo de investigación que impacta en diversos ámbitos: corporativo, investigaciones internas, criminales y de inteligencia, litigación civil y asuntos de seguridad nacional. (Cabrera, 2011). De acuerdo a la INTERPOL, este campo puede ser definido de la siguiente manera.

> "El análisis forense digital es un área de la ciberseguridad que se encarga en la detección,

adquisición, tratamiento, análisis y comunicación de datos."(Interpol, 2018).

Un análisis forense puede definirse como una metodología de tres pasos: extracción y preparación de datos, identificación de datos y análisis de los datos obtenidos así como un reporte asociado. (Díaz Muñoz, 2015). Como se ha mencionado anteriormente, la tecnología está cada vez más presente en actividades tanto personales como empresariales; esto hace casi necesario el análisis forense ya que toma en consideración la seguridad de los datos, la privacidad y la recuperación de la información ante desastres. (Cabrera, 2011). Cabe mencionar que este último es del interés del reporte.

Al realizar un análisis forense digital, es sumamente importante no alterar los dispositivos que se estén analizando y se debe llevar un extenso reporte sobre las actividades realizadas. En este reporte, deben incluirse fechas, personas encargadas, procedimientos realizados y su justificación, entre otras cosas. Dependiendo del dispositivo a analizar es que se emplean distintas técnicas y procedimientos; por ejemplo, cuando se trabaja con un disco duro cifrado, se debe obtener una imagen del dispositivo mientras el disco está encendido. (Cabrera, 2011).

En cuanto a los ámbitos que impacta este campo, el análisis forense puede ser utilizada en tribunales civiles o penales. Es en estas situaciones donde se debe tomar en consideración las cadenas de custodia, reportes detallados, validación de resultados e informes finales. El análisis forense también es realizado como parte de investigaciones internas en una empresa, las cuales pueden terminar en tribunal. No obstante, suelen utilizarse para determinar la causa de un problema tanto en sistemas como en ataques internos y externos. (Cabrera, 2011).

De igual manera, el análisis forense puede ser aplicado en cuestiones de seguridad y funcionamiento gubernamental. En general, un país es un blanco potencial para ataques y recopilación de datos por parte de gobiernos extranjeros. Por último, este análisis puede ser utilizado en cuestiones familiares como divorcios y custodia de menores. (Cabrera, 2011). Cabe mencionar que, sin importar el área donde se esté aplicando un análisis forense digital, la evidencia e información que sea recopilada debe de encontrarse en su estado más puro. Es decir, la información no puede ni debe de estar alterada; el apoyo que proporciona el análisis forense digital en las investigaciones es fundamental. Las pruebas pueden ir desde una computadora, teléfonos, hasta el historial de búsqueda en internet o el envío de mensajes, ya sea desde el teléfono hasta incluso por correo electrónico. El análisis forense digital busca extraer información contenida en pruebas electrónicas, y transformarla en información útil para la divulgación en otras áreas.

Una de las debilidades principales de la era digital es el borrado accidental, o intencional, de los datos; en el caso particular de este reporte, se está trabajando con una memoria USB a la que le fueron eliminados distintos archivos. En particular, uno de ellos es de suma importancia para la empresa en cuestión y es lo que se busca recuperar por medio de una herramienta que se explicará más adelante. Para saber cómo recuperar archivos, y cómo es esto posible, se deben establecer algunas bases en el tema.

Los archivos, datos, digitales se pueden comprender a través de los metadatos, los cuales se definen como

datos sobre los datos. Estos son elementos de organización de la información, la clasifican, categorizan o describen. (Méndez Rodríguez, 2001). Se puede decir que estos tienen tres elementos fundamentales, los cuales son su contenido, contexto y estructura. El contenido de los metadatos hace referencia al tema del documento, de qué trata. El contexto da información acerca de la creación del documento; quién lo creó, cuándo y dónde fue creado, entre otras. En cuanto a la estructura, esta da información sobre cómo se relacionan con otros objetos de información. (Díaz Muñoz, 2015).

Los documentos digitales pasan por cinco etapas, donde se le van sumando metadatos en cada una. Estas etapas son de creación, organización, búsqueda, uso y conservación y disposición. En la etapa de creación, se incorporan metadatos que facilitan su descripción, gestión y administración. En la etapa de organización, los metadatos son referentes a su registro. (Méndez Rodríguez, 2001). En la tercera etapa, de búsqueda, se crean metadatos que producen algoritmos que ayudan a mejorar los procesos de almacenamiento y recuperación. En la etapa de uso, se incorporan metadatos en cuanto a la versión del archivo o notas de uso. Por último, en la etapa de conservación, los metadatos guardan información ya sea sobre la disposición o conservación del archivo. (Méndez Rodríguez, 2001).

Dependiendo del equipo tecnológico sobre el cual se esté trabajando es que se pueden emplear distintas metodologías para recuperar la información faltante. En relación a los metadatos, se pueden utilizar técnicas de *File and Data Carving*; estas se basan en la estructura de los formatos reconocidos. (Garcés Pérez, 2021). Para el *Data Carving*, basta con reconocer la estructura para poder recuperar el archivo aún y cuando no se tengan metadatos disponibles; esto las hace muy efectivas y útiles sobre cualquier tipo de almacenamiento. En cuanto al *File Carving*, este se encarga de recuperar archivos sin daño alguno almacenados por medio del análisis del contenido. (Garcés Pérez, 2021).

Por ejemplo, al borrar un archivo de una computadora, realmente lo que se borra es el acceso directo al archivo; es decir, el sistema operativo borra la entrada del sistema de archivos. No obstante, el disco duro sigue guardando esa información hasta que se sobrescriba. Existen herramientas que facilitan este proceso pero de igual manera puede realizarse por medio de la terminal; en este caso, se trabajó con la herramienta Recuva. Este es un software que recupera archivos eliminados y trabaja con el sistema operativo Windows.

Una de las ventajas de este software es que, además de que existe una versión gratuita sin límite de cantidad de archivos a recuperar, también permite recuperarlos sin importar de qué manera fueron eliminados. Entre los tipos de archivos a recuperar se encuentran las imágenes, videos, música, archivos comprimidos e incluso e-mails de Outlook. Asimismo, es muy sencillo de usar pues únicamente debe seleccionarse la fuente que se busca inspeccionar y se recupera la información. Cabe destacar que la recuperación exitosa de la información dependerá de su estatus; Recuva lo codifica por colores: verde, naranja y rojo. Un archivo marcado como verde puede ser recuperado fácil y rápidamente; los archivos naranja de igual pueden ser recuperados pero el tiempo es más extenso. En cuanto a los archivos rojos, estos son más difíciles de recuperar y no todos los archivos son recuperados.

Retomando un poco la realización de reportes de análisis forense, la persona investigadora puede apoyarse

en diversas herramientas, una de estas siendo Kaspersky Endopoint Security Cloud. Esta herramienta protege servidores de archivos y computadoras Windows, dispositivos macOS, móviles iOS y Android e incluso Microsoft Office 365. Todo esto puede realizarse desde cualquier lugar por medio de una consola basada en la nube, además de que es muy sencillo para las personas conectarse a dicha consola ya que se puede realizar de manera remota. Kaspersky Endopoint Security Cloud es fácil de usar, los administradores pueden encontrarse en cualquier lugar y como quiera monitorear a los empleados. Por ejemplo, pueden ver qué usuarios pierden el tiempo en redes sociales o aplicaciones de mensajería. Sin embargo, el área fuerte de esta herramienta es que puede escanear todos los dispositivos con la finalidad de encontrar amenazas. En dado caso de que se encuentre una amenaza, la herramienta es capaz de eliminarla y generar un reporte donde se incluya una visualización de los ataques para ver la causa y la ruta de estos. Esto último es de gran utilidad puesto que muchas herramientas simplemente detectan y eliminan las amenazas, pero si se requiere hacer un reporte de análisis forense, es de suma importancia contar con toda la información del ataque. (Kaspersky, S/A)

Para una empresa, es de suma importancia contar con las medidas de seguridad necesarias para evitar tanto ciberataques como pérdidas de información; estos pueden representar grandes costos para las empresas por lo que deben ser mitigadas en la medida de lo posible. A continuación, se plantearán y desarrollaran estos dos escenarios: pérdida de información importante de una memoria USB y la infección de equipos con malware. Esto con la finalidad de recrear estos escenarios delicados para las empresas y poder ofrecer cierto marco para su prevención y tratamiento.

2. Desarrollo

2.1. Recuperación de datos con Recuva

El primer paso que se realizó fue abrir la memoria USB en el ordenador, para verificar si sí contaba con alguna información y de qué tipo era; se encontraron 4 carpetas con 8 imágenes y 2 videos. Previo a la recuperación de la información con el software, se creó una copia de los contenidos de la memoria USB como medida preventiva. Es importante crear una nueva carpeta en la computadora para que el programa Recuva, deposite los archivos recuperados; en este caso se decidió nombrar dicha carpeta con el nombre de "Archivos Recuperados". Posterior a esto, se procedió a recuperar la información; para esto, se requiere abrir el software en la computadora y dar click en el botón *Next*. Esto se muestra en la figura 1.

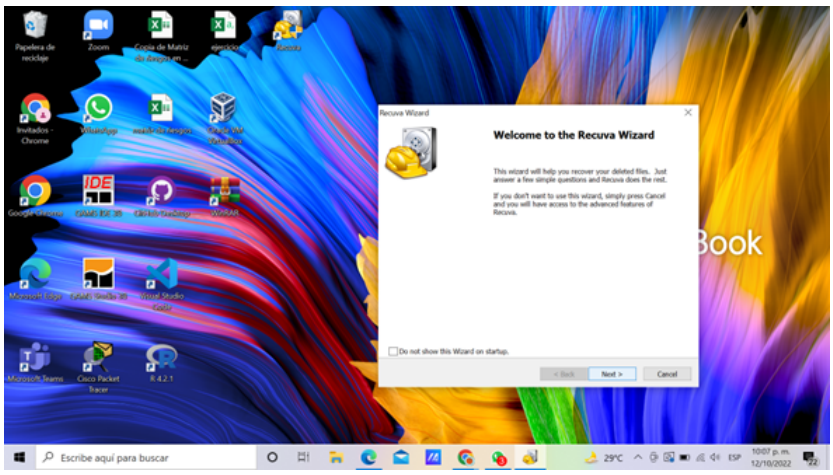

Figura 1: Inicio del software Recuva

Luego, se selecciona la opción de *All files* seguido de la selección de ubicación; para esto se escoge la opción *Select files* y luego *Kingston*, el cual es el nombre de la memoria USB a analizar. Esto se visualiza en las figuras 2 y 3.

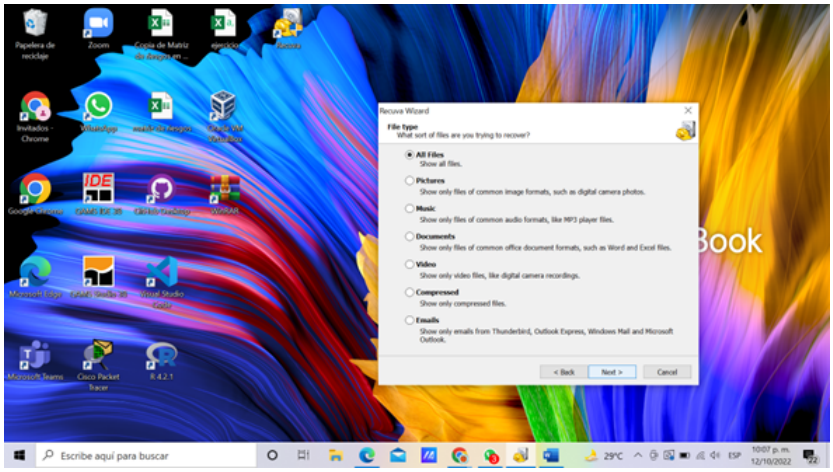

Figura 2: Seleccionar la opción de buscar cualquier tipo de archivo

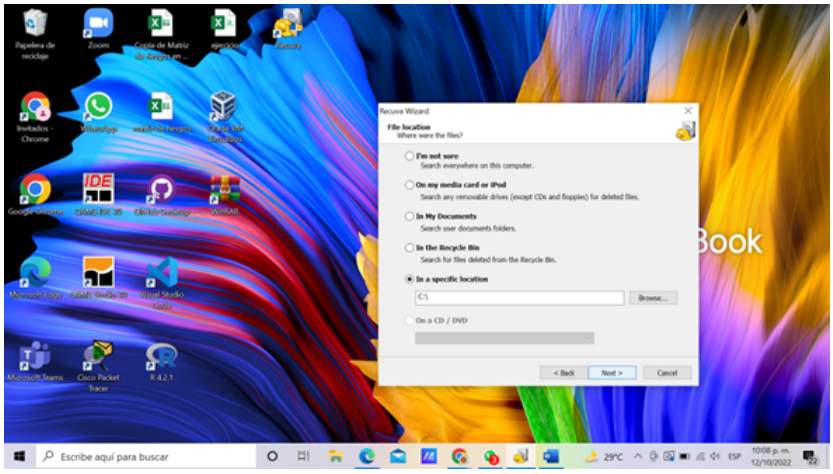

Figura 3: Seleccionar la opción de buscar en un lugar específico, el USB

Por último, se deja el espacio en blanco y se da click en *Start* para comenzar a utilizar el programa.

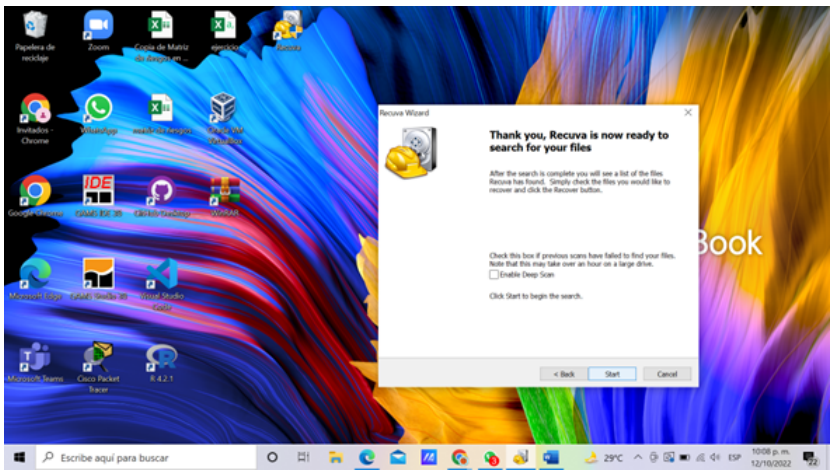

Figura 4: Iniciar el software

Una vez iniciado Recuva, se despliega la siguiente pantalla donde se pueden visualizar los estados de los archivos previamente mencionados (verde, naranja y rojo).

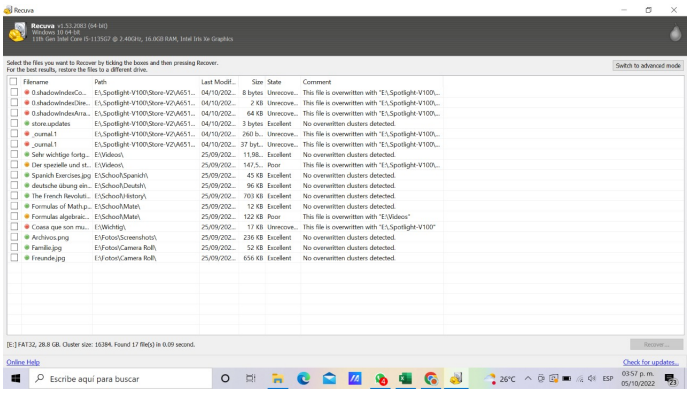

Figura 5: Interfaz de Recuva al realizar los pasos anteriores

Una vez realizado el análisis, se observaron los siguientes archivos.

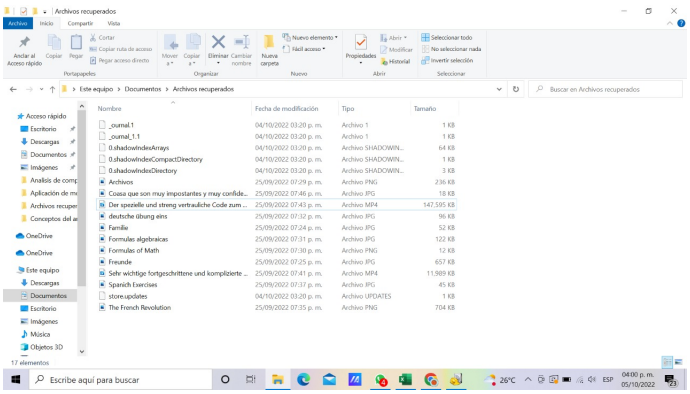

Figura 6: Archivos recuperados mostrados en la carpeta

Además de este análisis sencillo, se optó por realizar un escaneo profundo para poder encontrar una mayor cantidad de archivos. Para realizar este escaneo, se repiten los pasos del escaneo normal y en la parte superior derecha, en la figura 5, se encuentra el botón *Switch to advanced mode*. Se da click en él y, posteriormente, en el botón *Options*; se abre una ventana y se selecciona la pestaña *Actions* y la opción

Deep Scan. Finalmente, se da click en *OK* y *Scan*; este escaneo podrá ser más tardado pero ayudará a que se pueda encontrar una mayor cantidad de archivos. Los archivos que se encontraron se muestran de las figuras 7 a 9.

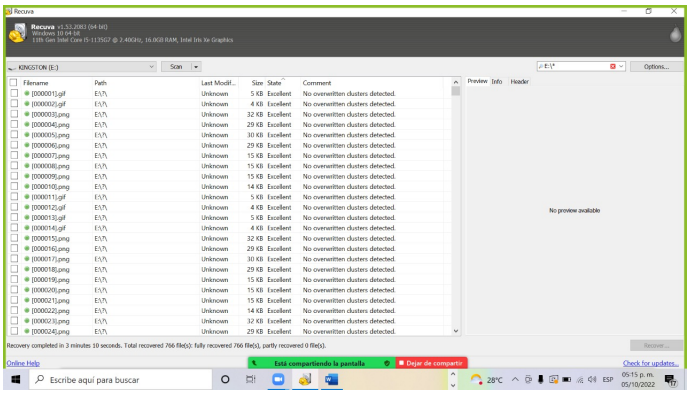

Figura 7: Interfaz de Recuva al aplicar el escaneo profundo

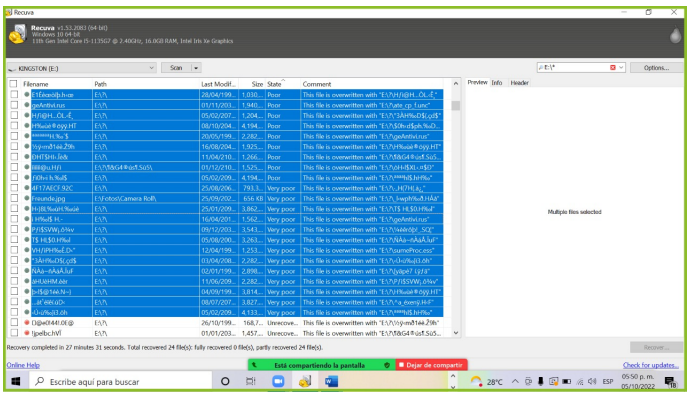

Figura 8: Interfaz de Recuva al aplicar el escaneo profundo

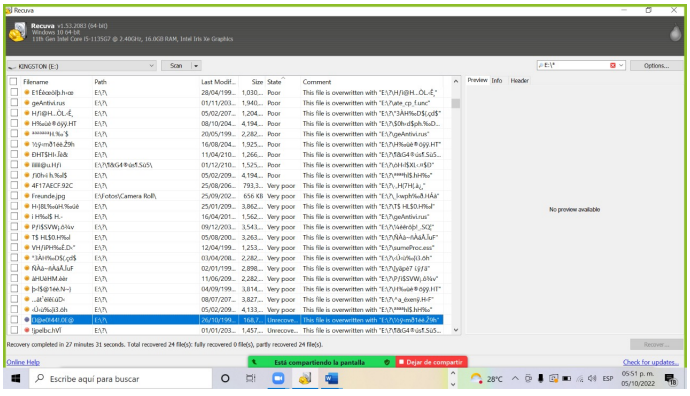

Figura 9: Interfaz de Recuva al aplicar el escaneo profundo

2.2. Kaspersky Endpoint Security Cloud Reporte Forense

Para realizar esta parte del reporte, primero se tuvo que instalar el software VirtualBox para trabajar dentro de una máquina virtual. Esto se debe realizar como medida preventiva puesto que, al trabajar con malware, existía un riesgo potencial de infectar y vulnerar los equipos propios. Dentro de una máquina virtual con el sistema operativo Windows10, se comenzó ingresando al sitio *Kaspersky Cloud* con las credenciales proporcionadas por la Organización SocioFormadora (OSF). Posteriormente, se ingresó a la pestaña *Paquete de Distribución* para descargar el paquete de instalación desde la consola de Kaspersky.

Una vez finalizada la instalación del paquete, se compartió con el equipo para que se pudiera ejecutar el instalador desde distintas máquinas virtuales. Posteriormente, se realizó la asignación de dispositivo al perfil de seguridad y usuarios. Para esto, se requiere ingresar a la sección de *Dispositivos*, donde se seleccionó el dispositivo a asignar y se dio clic en *Aceptar*. Al asignar el usuario, se asignó en automático el perfil de seguridad asignado inicialmente.

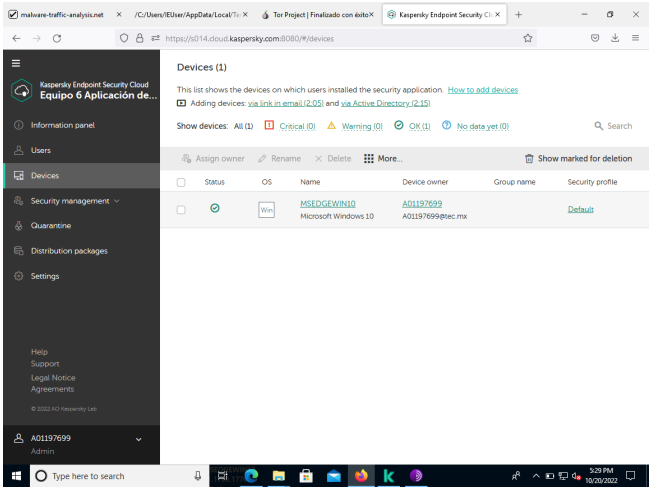

Figura 10: Sección de dispositivos en Kaspersky

El siguiente paso fue descargar los malwares desde la página proporcionada por la OSF; se descargaron algunos virus y se procedió a analizar y verificar las amenazas detectadas en los dispositivos administrados. Para poder visualizar esta información, se debe ingresar a la sección *Alertas de Endpoint Detection and Response*, la cual muestra información de las amenazas detectadas y el origen de la detección. Dentro de dicha sección, se encontraron las alertas de los malwares que se habían detectado. Luego, se prosiguió a examinar la alerta con la finalidad de observar la gráfica de la cadena de desarrollo, el cuál brinda información acerca de la detección. Entre esta información, se pueden encontrar actividades que se llevaron a cabo en el dispositivo durante la detección, la categoría de la amenaza detectada y el origen del archivo. Además, la gráfica de cadena muestra si se han creado archivos adicionales en el dispositivo y cuáles son, así como el establecimiento de nuevas conexiones de red y cambios en claves de registro. En el caso de los virus descargados, se observó que las gráficas de cadena únicamente mostraban la palabra *detected* debido a que los virus ya habían sido analizados previamente. Por esto mismo, se tomó la decisión de descargar distintos malwares de la misma página para verificar si esto ocurría solamente con ese virus en particular o si era algo recurrente con los virus de esa página. Al finalizar estos procedimientos,

se observó que el patrón se repetía por lo que se optó por descargar malware proveniente de otras páginas.

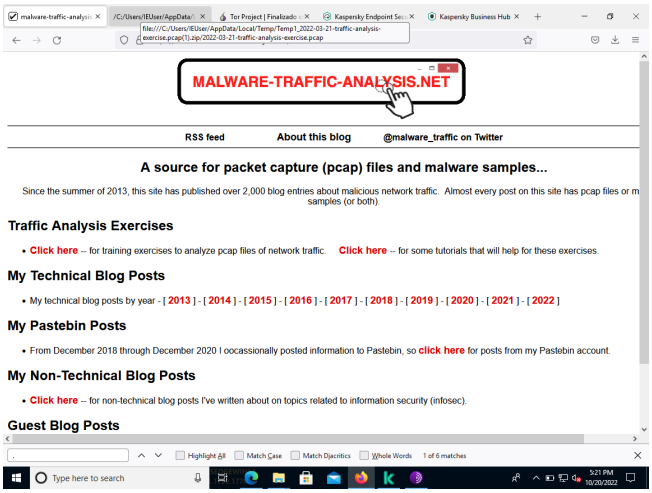

Figura 11: Página de malware proporcionada por el socio formador

Para esto, se descargó primero el buscador *Tor* para proceder al buscador especializado *Torch*. Este último es un buscador de *dark web*, de donde se descargaron otros malwares; para esto, primero se buscó *exe virus Windows* para encontrar un malware que pudiera ser descargado y ejecutado en la máquina virtual. Al navegar por el buscador, se ingresó a un foro llamado *BestCarding World* y descargó un archivo llamado *PlasmaHTTP.exe*.

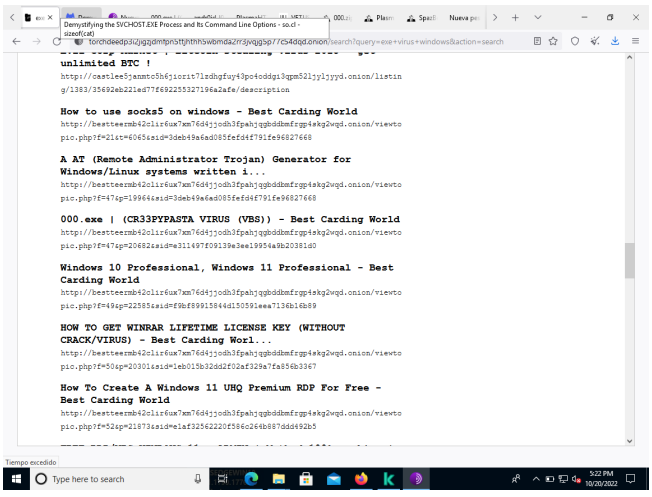

Figura 12: Resultado de búsqueda en Torch

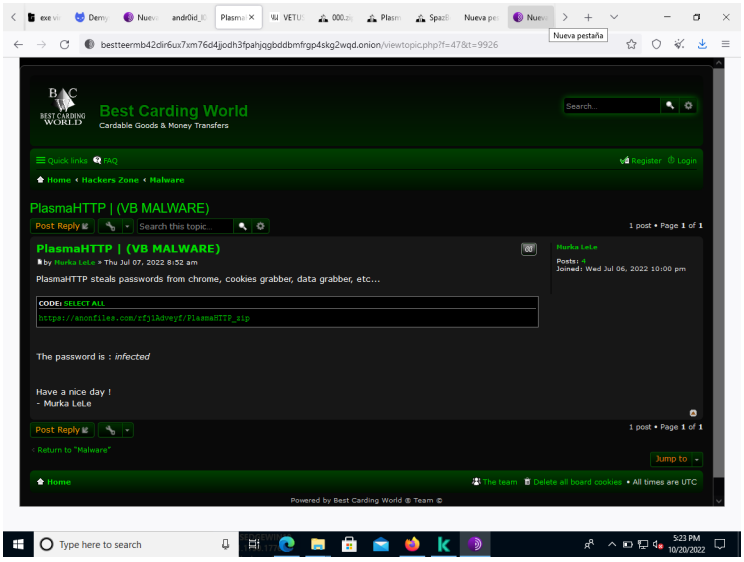

Figura 13: Foro BestCarding World en el que se encuentra el malware

Al hacer clic en este, se descarga un archivo *.zip*, donde se encuentra una carpeta para ejecutar dentro de la máquina virtual. Antes de poder descargar el virus, la carpeta pide una contraseña; la cuál es *infected*. Una vez ejecutado el archivo, se elimina inmediatamente de la máquina virtual al ser identificado por Kaspersky.

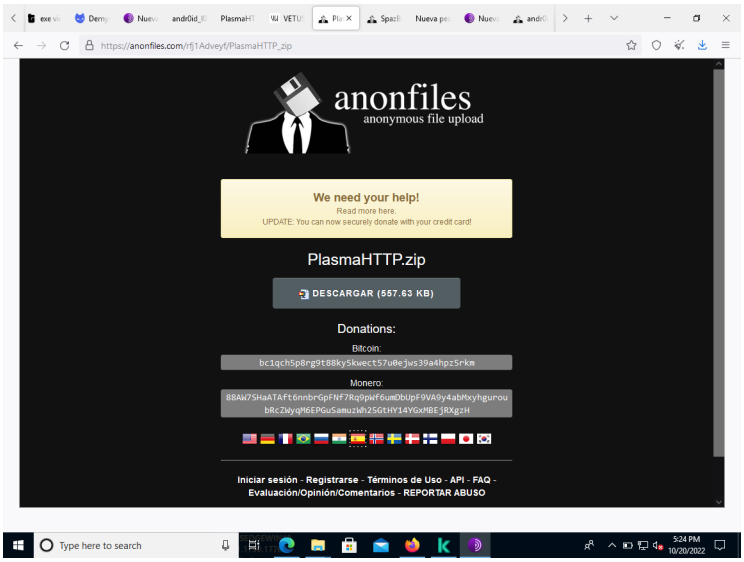

Figura 14: Sitio externo en el cuál se descarga el archivo .zip

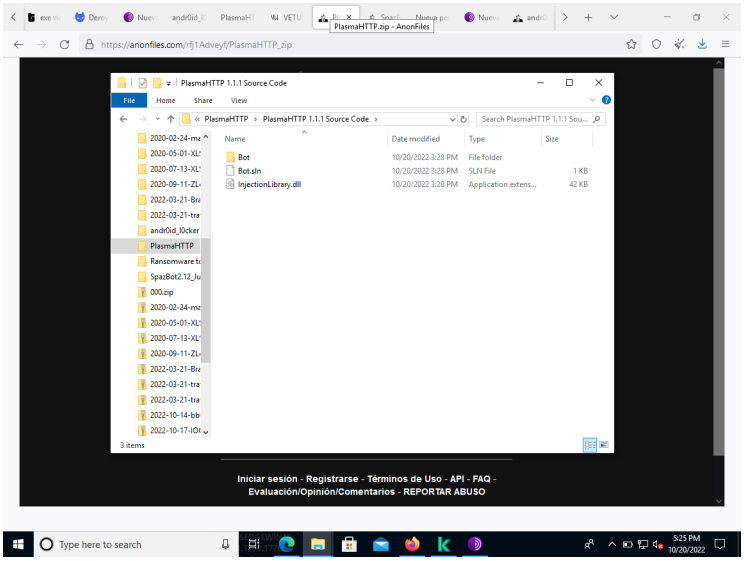

Figura 15: Carpeta con el archivo borrado PlasmaHTTP.exe

3. Resultados

3.1. Recuva

Al terminar con el primer análisis, se obtuvieron 17 documentos en total; es decir, se encontraron 7 nuevos documentos nuevos lo que significa que se encontró información previamente borrada. Se observaron los estados de cada archivo (verde, naranja y rojo) así como otras columnas que dan información acerca de estos; metadatos como la dirección en donde se encuentra el archivo, fecha de la última modificación, tamaño y el estado del archivo. De estos 17 archivos, únicamente 11 se podían abrir; 6 estaban dañados y no se pudo identificar la información que contenían.

En el segundo análisis, se recuperaron un total de 12,944 archivos de los cuales 766 estaban en un estado "verde" y se pudieron rescatar todos. Del estado "amarillo", se recuperaron 26 archivos y existían dos clasificaciones para estos: *poor* y *very poor*. Los archivos en *poor* suelen ser más recuperables ya que una minoría de sus clusters han sido sobrescritos mientras que en los archivos *very poor*, la mayoría de sus clusters han sido sobrescritos (Forums, 2016). En cuanto a los archivos en un estado de "rojo", se encontraron aproximadamente 11,000 de estos.

En los archivos marcados como verdes, se encontraron únicamente imágenes como el logo de Google, el instructivo de Windows en diferentes idiomas en formato Word, algunas de las imágenes que aparecieron en el primer análisis, diversos símbolos, entre otros. En esta sección se encontraba el archivo de interés principal. La finalidad de recuperar la información de la memoria USB era recuperar un archivo con información confidencial; un archivo que fue borrado por un empleado en Alemania. Se recuperó una carpeta con el nombre *Wichtig*, lo cuál significa *Importante*, dónde se encontró el archivo *Cosas que son muy importantes y muy confidenciales que deben de ser muy secretas.jpg*. Al recuperar la imagen y abrirla, se muestra un folder con la leyenda *Confidential*, por lo que se concluye que esa es la imagen que se

estaba buscando. La recuperación de dicha información tardó 3 minutos con 10 segundos. Los archivos en estado amarillo fueron referentes a imágenes y links relacionados con Kaspersky. La recuperación de dicha información tardó 27 minutos con 31 segundos.

Figura 16: Imagen Recuperada

3.2. Kaspersky

El proceso de revisión del equipo afectado consta de identificar el origen y desarrollo de la amenaza e indicadores de compromiso; a continuación se desglosan los descubrimientos de estos pasos.

1. **Origen de la amenaza.** En la siguiente tabla, se especifican los detalles del origen de la amenaza detectada con Kaspersky Endpoint Security. Se encuentra en dónde empezó la amenaza, así como el paso en el que se encuentra el malware. Además el PID (Process ID) del sistema que es un indicador del proceso de forma unícova.

Parámetro de Inicio	Tipo	PID del Sistema	Crítico	Nivel de Integridad
C:\\Windows\explorer.exe	Proceso	4712	No	Media

Cuadro 1: Origen de la amenaza

La siguiente tabla indica el usuario que ejecutó la amenaza así como la hora en la que se realizó.

Usuario	Hora
MSEDGEWIN10\EUser	19/10/2022 17:34

En la siguiente imagen, se puede apreciar un resumen de las tablas anteriores.

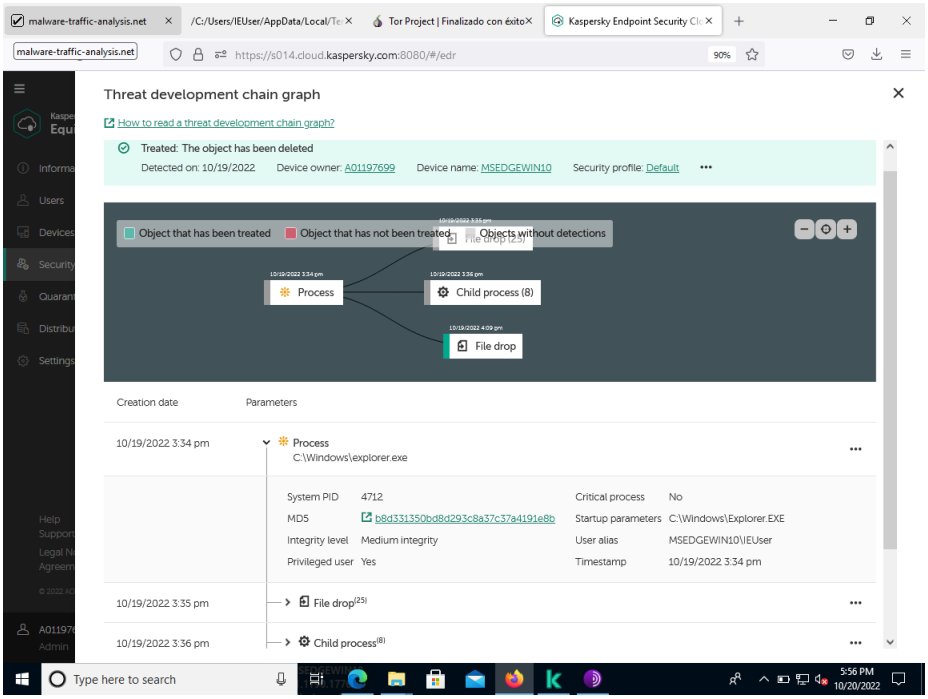

Figura 17: Gráfica de cadena y análisis de proceso

Además de la gráfica de cadena, se puede encontrar un link con información más detallada del archivo. Este tiene como dirección a *Kaspersky Threat Intelligence Portal*, donde se observa si el archivo es una amenaza o un archivo conocido.

2. **Desarrollo de la amenaza.** En esta etapa, se observan los datos relacionados a *Child Process*, como se muestran en las siguientes imágenes.

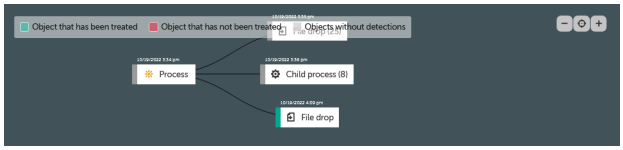

Figura 18: Elementos de gráfica de cadena

En la figura 18, se puede observar que se cuenta con un total de 8 procesos, además de indicar si estos son críticos o no así como el nivel de seguridad que tiene. Finalmente, se muestran los parámetros de inicio y el Process ID.

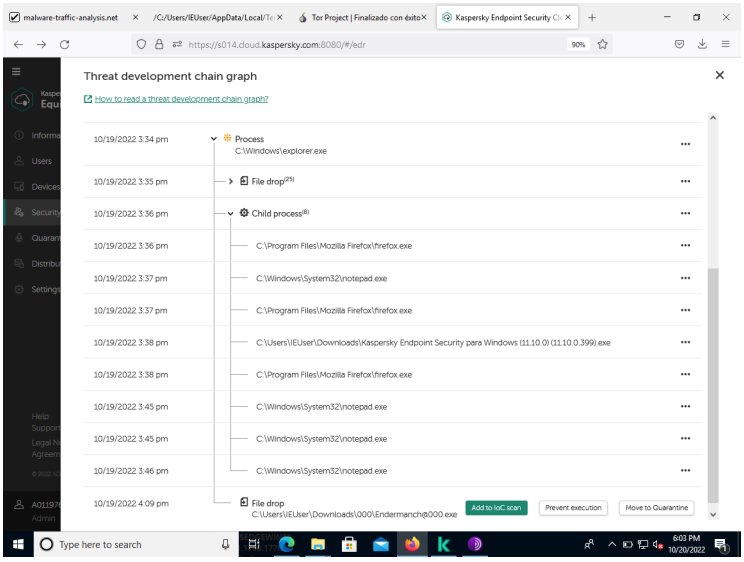

Figura 19: Child Process

En cuanto a la figura 19, se pueden observar todos los *Child Process*, que son los procesos secundarios que surgen después de que algún archivo, aplicación o programa es ejecutado. Esto es algo común ya que usualmente en los malwares se ejecutan en los *Parent Processes* y los *Child Processes* quedan en un área gris. En la siguiente imagen, se puede apreciar el *File Drop* junto con los distintos detalles sobre los primeros elementos y rutas y su hora de detección.

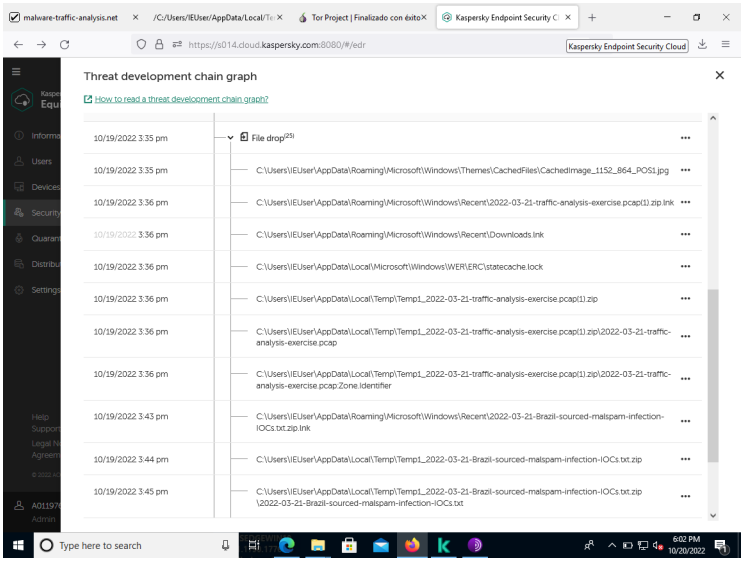

Figura 20: File drop

3. **Indicadores de compromiso.** De acuerdo con Kaspersky Endpoint Security Cloud-EDR, se detecta un archivo malicioso bloqueado, con los siguientes indicadores de compromiso mostrados en la tabla siguiente.

Ruta	Amenaza	Tipo	Acción	Hora de detección
https://anonfiles.com/rfj1Adveyf/PlasmaHTTP_zip	UDS:Dangerous ObjectMultiGeneric	Archivo	Eliminado	20/10/2022 17:29
Indicadores				
Sha-256			**MD5**	
4ea1f2ecf7eb12896f2cbf8683dae8546d2b8dc43cf7710d68ce99e127c0a966			f2b7074e1543720a9a98fda660e02688	

Cuadro 2: Indicadores

De igual manera, se puede observar el último proceso de *Filedrop* donde termina el análisis.

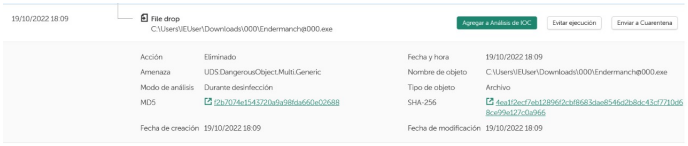

Figura 21: Resumen de Filedrp

Además, se muestran los hashes MD5 y SHA-256 junto con los links del análisis de lo que se obtiene. En ambos casos, el análisis nos arroja que es un malware, por lo que es necesario que Kaspersky elimine el archivo.

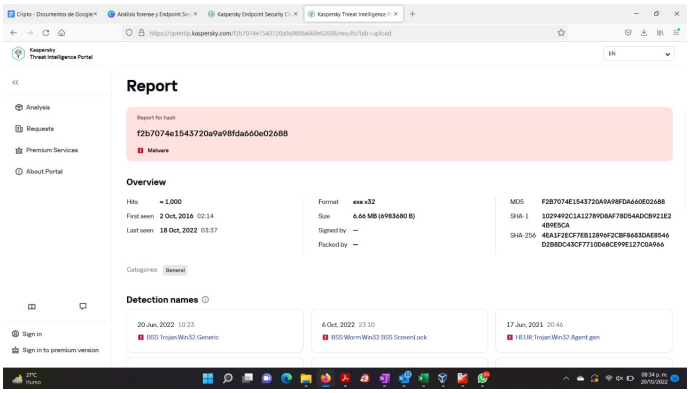

Figura 22: MD5

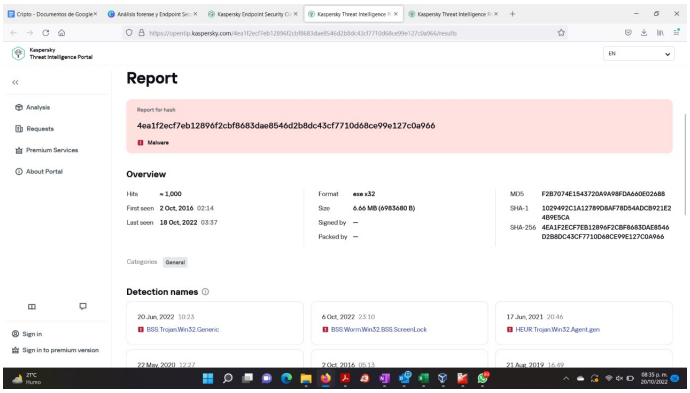

Figura 23: SHA-256

Esta herramienta nos brinda un veredicto conciso sobre el carácter peligroso/seguro del objeto ya que ofrecen información detallada sobre qué tan sospechoso es un archivo y en qué aspectos. Por ejemplo, nos

muestra que el archivo detectado es una amenaza, qué tienen de malo, qué tan frecuente es la infección, a qué amenazas se asemejan y qué herramientas se usaron para crearlo. Además, brinda información sobre la fecha que fue visto por primera vez así como la última, el formato y el tamaño.

Es importante mencionar como los hashes SHA-256 y MD5 contienen listas de hashes de malware, muchas de ellas son de acceso público. Estas listas están conformadas por valores hash de las piezas de malware o de algunas partes pequeñas y reconocibles de estas piezas. Por esto mismo, si un usuario detecta un archivo sospechoso, puede consultarlo en la bases de datos públicas; de esta forma sabrá si se trata de un malware. Por otra parte, los antivirus detectan y bloquean los malwares comparando los hashes con sus propias bases de datos.

4. Conclusiones

Existen distintas medidas que pueden ser llevadas a cabo por las empresas y organizaciones para mitigar o evitar la pérdida de información. A pesar de que existan medidas para recuperar sus archivos y demás, como se describió con anterioridad, esta recuperación puede tener un costo asociado. Minimizar costos es de gran relevancia para las empresas, por lo que tener las medidas necesarias para esto es de interés. Entre estas medidas de mitigación se encuentran el crear copias en la nube y tener cuidado en cuanto a dónde se conectan los dispositivos (USB).

El respaldo de la información por medio de las copias en la nube se asegura de que, en caso de algún siniestro, no se sufran pérdidas de información. Es importante que, como propietario de la información, no se confíe en su totalidad en el entorno. Una buena medida sería mantener respaldos tanto físicos como digitales; ambas tienen sus beneficios y áreas de oportunidad. Si se respalda la información únicamente por medios físicos, se corre el riesgo de que estos medios sean destruidos, haciendo imposible su recuperación. En cuanto a los respaldos digitales, se puede acceder a la información desde cualquier dispositivo electrónico con las credenciales correspondientes. Además, al estar almacenada en servidores remotos, el riesgo de que se pueda dañar, corromper o perder el disco duro físico y cualquier dato valioso es prácticamente nulo.

Otra medida de seguridad importante a tomar en consideración es el tener cuidado sobre dónde se conectan los dispositivos; en este caso, la USB. Conectarla a cualquier computadora o puerto, sin conocer el estado de estos mismos, es sumamente peligroso. Existe la posibilidad de que se coloque un malware en el dispositivo que sea capaz de robar la información en cuestión de segundos. Se deben de tener las precauciones necesarias para evitar esto; no introducir la memoria USB a dispositivos que no hayan sido autorizados.

Es importante tener protegido cualquier dispositivo electrónico ya que no solamente se protege la vida útil del producto, sino que también se está protegiendo la información personal, como se observa en el reporte. Por lo general, el uso de malwares se da con la finalidad de robar y obtener cualquier tipo de datos; estos suelen instalarse fácil y rápidamente en el dispositivo. Por esto mismo, es de suma importancia contar con un antivirus y medidas preventivas en general. Esto protege la información así como

da seguridad al usuario para navegar por el Internet. De igual manera, es importante resaltar que, aún contando con herramientas de protección, se debe hacer un uso responsable de la tecnología. Una de las herramientas recomendadas es Kaspersky ya que además de detectar y eliminar amenazas, es capaz de realizar el análisis forense que a su vez permite la interpretación de gráficas de desarrollo del ataque. Es decir, se identifica el tipo de ataque, su origen y las acciones realizadas.

Por último, es importante que al realizar un análisis forense digital, se tenga en mente qué es lo que se está buscando con dicho análisis. En este caso, se obtuvo una recuperación del archivo exitosa y se tomaron las medidas preventivas necesarias. Al realizar un escaneo profundo, la cantidad de archivos encontrados aumentó considerablemente por lo que es requerido poder discernir entre los archivos que son de interés y aquellos que sólo generan ruido. Además, se debe de realizar de la manera más controlada y limpia posible para evitar cualquier situación que desacredite el procedimiento realizado y la evidencia recuperada.

Referencias

Cabrera, G. J. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. *Apuntes de Ciencia & Sociedad*, *1*(2), 6.

Díaz Muñoz, D. S. (2015). *Análisis forense desde una perspectiva práctica* (B.S. thesis). Universidad Piloto de Colombia.

Forums, C. C. (2016). How is "unrecoverable" better than "poor"? https://community.ccleaner.com/topic/45573-how-is-unrecoverable-better-than-poor/

Garcés Pérez, O. L. (2021). Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática.

Gutiérrez Puebla, J. (2018). Big Data y nuevas geografías: la huella digital de las actividades humanas. *Documents d'análisi geográfica*, *64*(2), 0195-217.

Interpol. (2018). Análisis forense digital. https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

Kaspersky. (S/A). Ciberseguridad para empresas en crecimiento con recursos limitados. https://latam.kaspersky.com/small-to-medium-business-security/cloud

Méndez Rodríguez, E. M. (2001). Metadatos y recuperación de información: estándares, problemas y aplicabilidad en bibliotecas digitales.

Olmedo, J. I., & Gavilánez, F. L. (2018). Análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal*, *3*(9), 172-181.

RAMOS-TOXTLE, A. (2020). GESTIÓN ESTRATÉGICA DE LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS NACIONALES. *Revista Internacional de Ciencias Sociales y Humanidades SOCIOTAM*, *30*(2), 107-127.