



INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE  
MONTERREY

Escuela de Ingeniería y Ciencias  
Ingeniería en Ciencia de Datos y Matemáticas

## **Análisis Forense - Versión técnica**

APLICACIÓN DE CRIPTOGRAFÍA Y SEGURIDAD

*Cantú Rodríguez Pamela* A01285128

*Ferreira Guadarrama Emiliano* A01654418

*Núñez López Daniel Isaac* A01654137

*Rincón Flores Mariana Ivette* A01654973

*Ugalde Jiménez Ana Sofía* A01702639

**en conjunto con IPC Services**

**Supervisado por**

Dr. Oscar Eduardo Labrada Gómez  
Dr. Alberto Francisco Martínez Herrera

Monterrey, Nuevo León, 5 de octubre de 2022

# Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Metodología</b>	<b>3</b>
2.1. Recuperación de Archivos . . . . .	3
2.1.1. Copia de Seguridad . . . . .	3
2.1.2. Recuperación de archivos . . . . .	4
2.1.3. Identificación de archivos . . . . .	7
2.2. Kaspersky Endpoint Security para Windows . . . . .	8
2.2.1. Máquinas Virtuales . . . . .	9
2.2.2. Instalación del antivirus . . . . .	9
2.2.3. Descarga de malware . . . . .	10
2.2.4. Monitoreo, detección y respuesta . . . . .	13
<b>3. Resultados</b>	<b>14</b>
3.1. Recuperación de Archivos . . . . .	14
3.2. Kaspersky Endpoint Security para Windows . . . . .	15
<b>4. Conclusiones</b>	<b>17</b>
4.1. Recuperación de Archivos . . . . .	17
4.2. Kaspersky Endpoint Security para Windows . . . . .	18

# 1. Introducción

La recuperación de datos e información se ha convertido en un pilar de la investigación forense, pues generalmente los datos son borrados o alterados con el fin de proteger información sensible (Prakash et al., 2022). Para este objetivo se utiliza el análisis forense digital, que es una rama de la policía científica centrada en la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados por medios electrónicos (Interpol, s.f.).

La recuperación de datos no solo es útil en el análisis forense digital, también es de gran beneficio para casos de pérdida de información causada por un borrado accidental, el formateo incorrecto del disco duro o del servidor, una reinstalación defectuosa de aplicaciones, fallas en el arranque del sistema, virus informáticos, apagado inesperado, entre otros (Pro, 2019). Dentro de la recuperación de datos existen diversas herramientas utilizadas en diferentes situaciones, así como para distintos objetivos y alcances.

En este reporte se presenta el proceso de recuperación de archivos borrados de una memoria USB mediante la versión doméstica de la herramienta Recuva, así como el procedimiento de identificación de archivos sospechosos. El caso presentado consiste en que una persona actúa maliciosamente, sobre-escribe la información y borra los archivos contenidos de una USB de una empresa Alemana; el objetivo es recuperar los archivos eliminados, incluyendo uno específico que contiene información confidencial y de relevancia para la empresa.

El uso predominante de Windows presenta una oportunidad para los cibercriminales. Por esta razón y por el crecimiento que han tenido los métodos y las herramientas para cometer ciberdelitos, ya no son suficientes las funciones de seguridad integradas y es necesario el uso de otras herramientas como Kaspersky. Kaspersky Endpoint Security para Windows combina sistemas de protección de varias capas con tecnologías como controles de aplicaciones, web y dispositivos, gestión de vulnerabilidades y parches, y cifrado de datos con el objetivo de proteger al cliente (Lab, 2022).

Además del contenido antes mencionado, en este reporte se expone la aplicación de la herramienta Kaspersky Endpoint Security para Windows en la detección de malware y amenazas utilizando

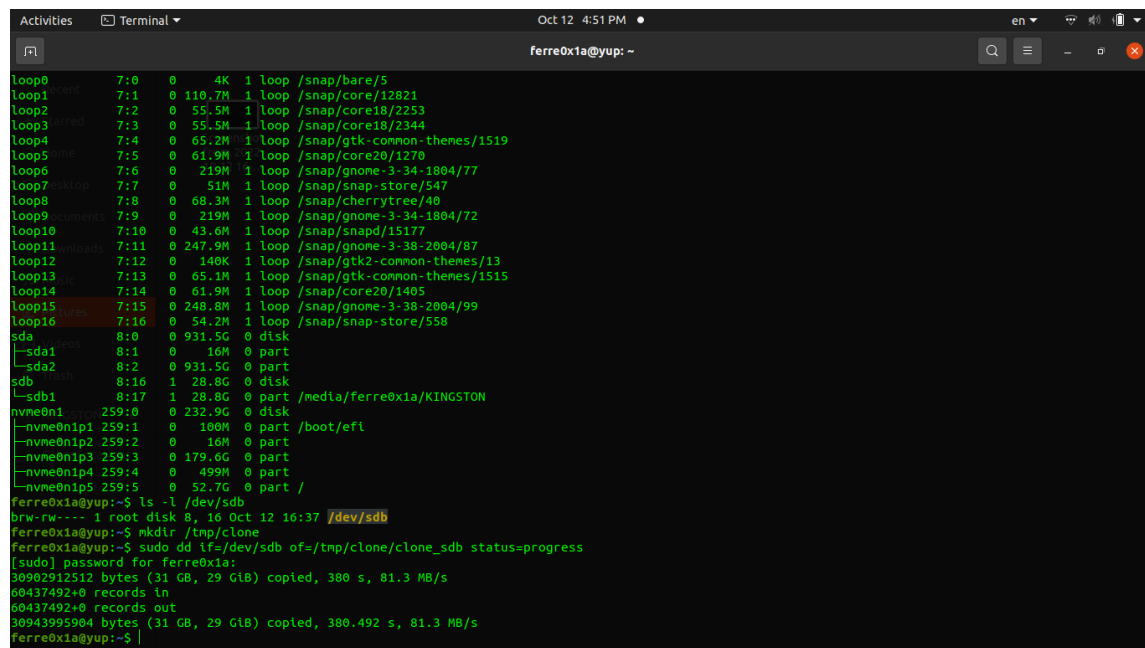
como equipo una máquina virtual con virus previamente cargados.

## 2. Metodología

### 2.1. Recuperación de Archivos

#### 2.1.1. Copia de Seguridad

Este no es un paso necesario, pero nos da mayor seguridad ya que en caso de que los archivos de la memoria fueran editados se podría regresar a esta copia. Para generar esta imagen se utilizó únicamente la terminal de Ubuntu:



```
Activities Terminal Oct 12 4:51 PM en
ferre0x1a@yup: ~
loop0 7:0 0 4K 1 loop /snap/bare/5
loop1 7:1 0 110.7M 1 loop /snap/core/12821
loop2 7:2 0 55.5M 1 loop /snap/core18/2253
loop3 7:3 0 55.5M 1 loop /snap/core18/2344
loop4 7:4 0 65.2M 1 loop /snap/gtk-common-themes/1519
loop5 7:5 0 61.9M 1 loop /snap/core20/1270
loop6 7:6 0 219M 1 loop /snap/gnome-3-34-1804/77
loop7 7:7 0 51M 1 loop /snap/snap-store/547
loop8 7:8 0 68.3M 1 loop /snap/cherrytree/40
loop9 7:9 0 219M 1 loop /snap/gnome-3-34-1804/72
loop10 7:10 0 43.6M 1 loop /snap/snapd/15177
loop11 7:11 0 247.9M 1 loop /snap/gnome-3-38-2004/87
loop12 7:12 0 140K 1 loop /snap/gtk2-common-themes/13
loop13 7:13 0 65.1M 1 loop /snap/gtk-common-themes/1515
loop14 7:14 0 61.9M 1 loop /snap/core20/1405
loop15 7:15 0 248.8M 1 loop /snap/gnome-3-38-2004/99
loop16 7:16 0 54.2M 1 loop /snap/snap-store/558
sda 8:0 0 931.5G 0 disk
|--sda1 8:1 0 16M 0 part
|--sda2 8:2 0 931.5G 0 part
sdb 8:16 1 28.8G 0 disk
|--sdb1 8:17 1 28.8G 0 part /media/ferre0x1a/KINGSTON
nvme0n1 259:0 0 232.9G 0 disk
|--nvme0n1p1 259:1 0 100M 0 part /boot/efl
|--nvme0n1p2 259:2 0 16M 0 part
|--nvme0n1p3 259:3 0 179.6G 0 part
|--nvme0n1p4 259:4 0 499M 0 part
|--nvme0n1p5 259:5 0 52.7G 0 part /
ferre0x1a@yup:~$ ls -l /dev/sdb
brw-rw---- 1 root disk 8, 16 Oct 12 16:37 /dev/sdb
ferre0x1a@yup:~$ mkdir /tmp/clone
ferre0x1a@yup:~$ sudo dd if=/dev/sdb of=/tmp/clone/clone_sdb status=progress
[sudo] password for ferre0x1a:
30902912512 bytes (31 GB, 29 GiB) copied, 380 s, 81.3 MB/s
60437492+0 records in
60437492+0 records out
30943995904 bytes (31 GB, 29 GiB) copied, 380.492 s, 81.3 MB/s
ferre0x1a@yup:~$
```

Figura 1: Terminal de Ubuntu para realizar la copia de seguridad.

Primero se utilizó el comando *lsblk* que muestra todos los discos conectados, las particiones y otra información. Aquí, gracias a la capacidad y el nombre del mount point, se puede observar

que la USB está montada como sdb. Después se creó un directorio en \tmp y empleó el comando *dd* para hacer una imagen del disco completo. Finalmente no fue necesario restaurar la USB pero siempre se tuvo la seguridad de que si se hacía algún cambio teníamos los archivos originales.

### **2.1.2. Recuperación de archivos**

Como se mencionó anteriormente, con el objetivo de recuperar la información perdida de la memoria USB se hizo uso de la herramienta Recuva de CCleaner.

Recuva es una aplicación que sirve para recuperar archivos de discos dañados o recientemente formateados, es capaz de restaurar cualquier tipo de archivo que se desee y de cualquier tipo de disco de almacenamiento.

Dentro del software, se pueden hacer escaneos simples, profundos y muy específicos si así se desea, con el fin de volver a ver el archivo deseado.

Igualmente, Recuva ofrece una función de borrado seguro, en la cual se emplean técnicas de sobre-escritura con estándares militares para asegurarse de que los archivos no se puedan restaurar. (CCleaner, s.f.)

A continuación se presentan los pasos seguidos para la recuperación de archivos.

PASO 1: Instalación de Recuva

Se accedió a la página: <https://www.ccleaner.com/recuva/download/standard>:

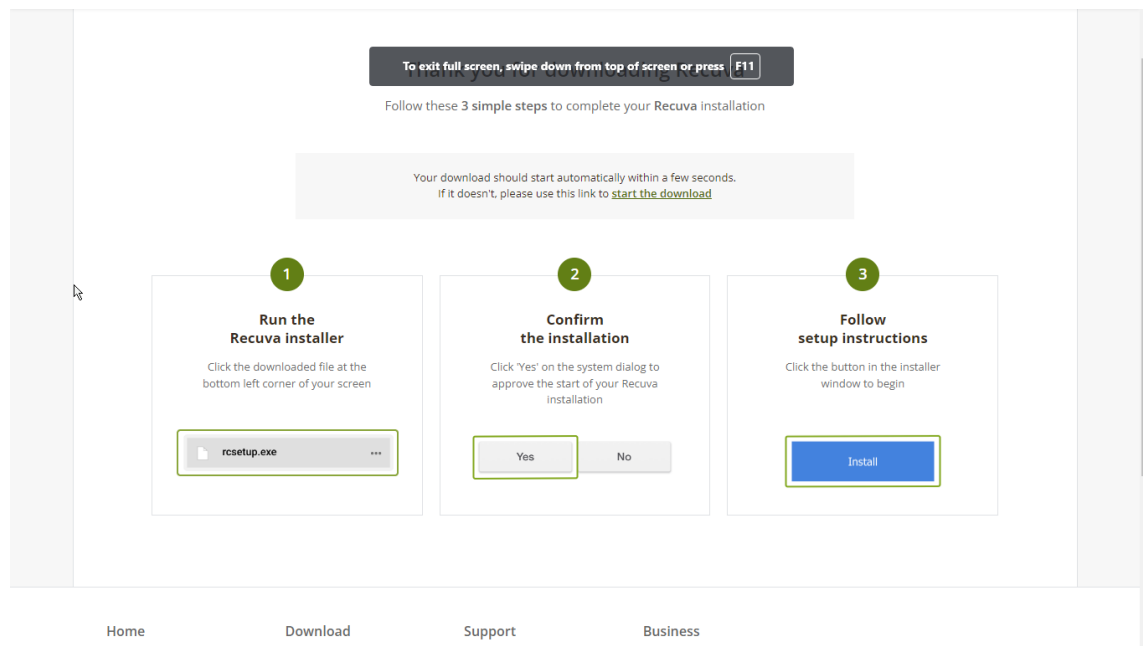


Figura 2: Página web de Recuva.

## PASO 2: Escaneo del disco

Después de descargar Recuva se muestra la siguiente ventana, y se da clic en **Run Recuva** como se muestra:

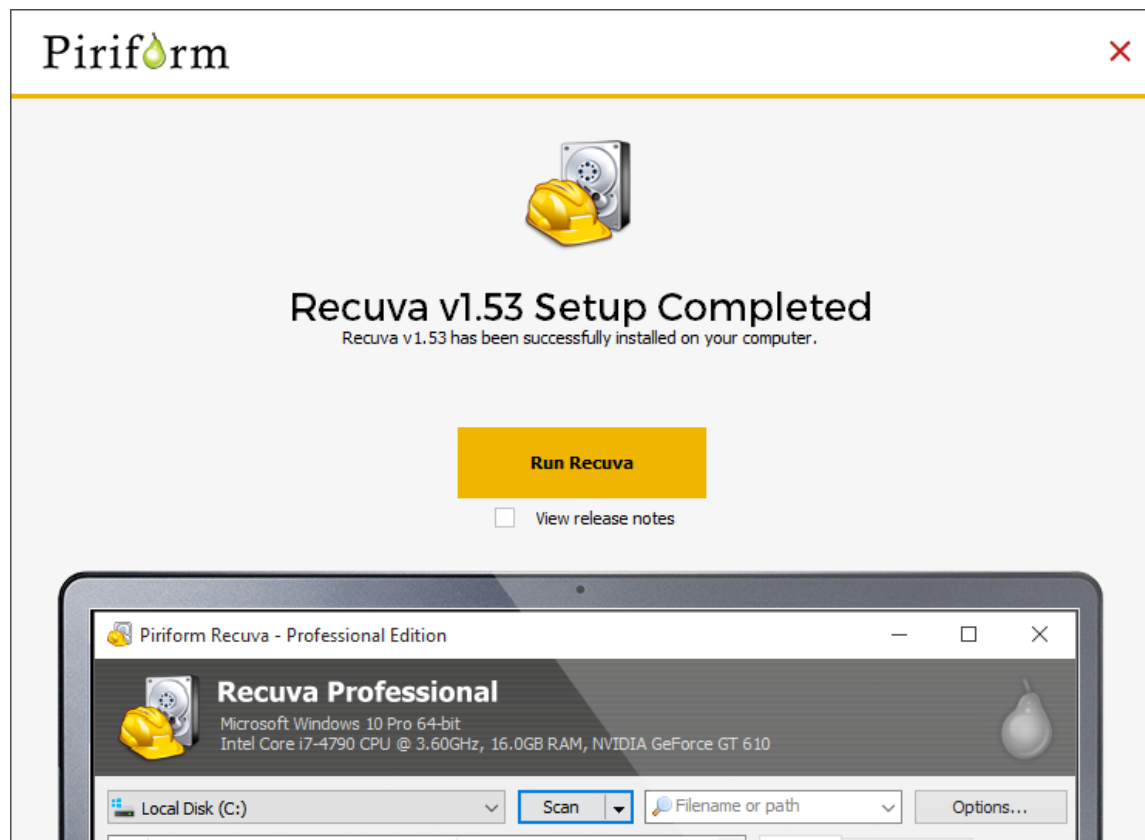


Figura 3: Instalación completa de Recuva.

Se sigue la guía del wizard y se elige la memoria USB como la ubicación de los archivos:

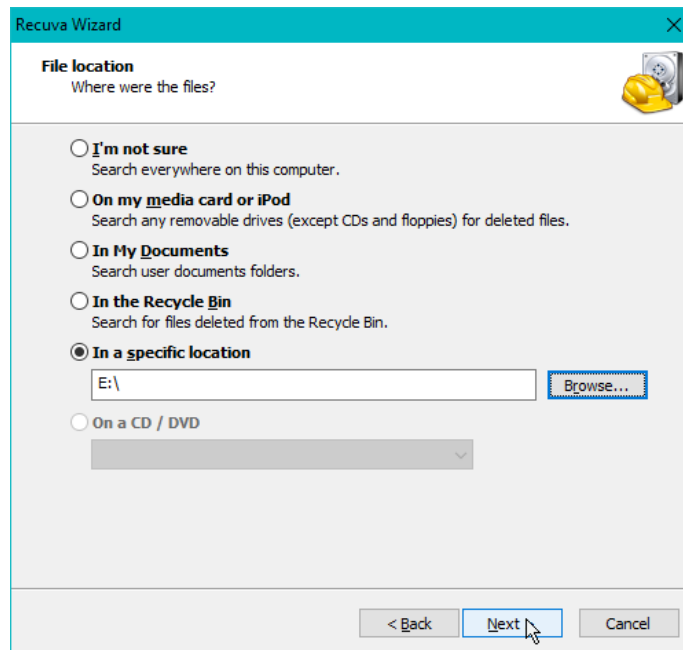


Figura 4: Instalador de Recuva.

### 2.1.3. Identificación de archivos

Para la identificación de archivos sospechosos se utilizaron diferentes estrategias, pero ya que se buscaba únicamente un archivo y el primer archivo mostrado parece ser el correcto nos enfocamos en las diferencias entre este y los demás archivos recuperados. Por ejemplo, la mayoría de los archivos se encuentran dentro de carpetas de aplicaciones como *Microsoft*, *Windows*, *Internet Explorer*, *Edge*, *Lenovo* y la mayoría parecen indicar que son archivos comunes de estas aplicaciones, como archivos PAK de diferentes idiomas para Edge, logos, archivos de configuración etc. Mientras que el archivo que se encontró es una imagen de 17 kb llamada *Çoasa que son muy importante y muy confidenciales que deben de ser muy secretas.jpg*". Las faltas de ortografía probablemente tienen que ver con que ya había sido borrada. Además no se encuentra dentro de ninguna de las carpetas mencionadas anteriormente y aunque no se encontraron meta-datos relevantes es muy claro que es el archivo confidencial que fue borrado. A continuación se muestran los archivos que serán recuperados:



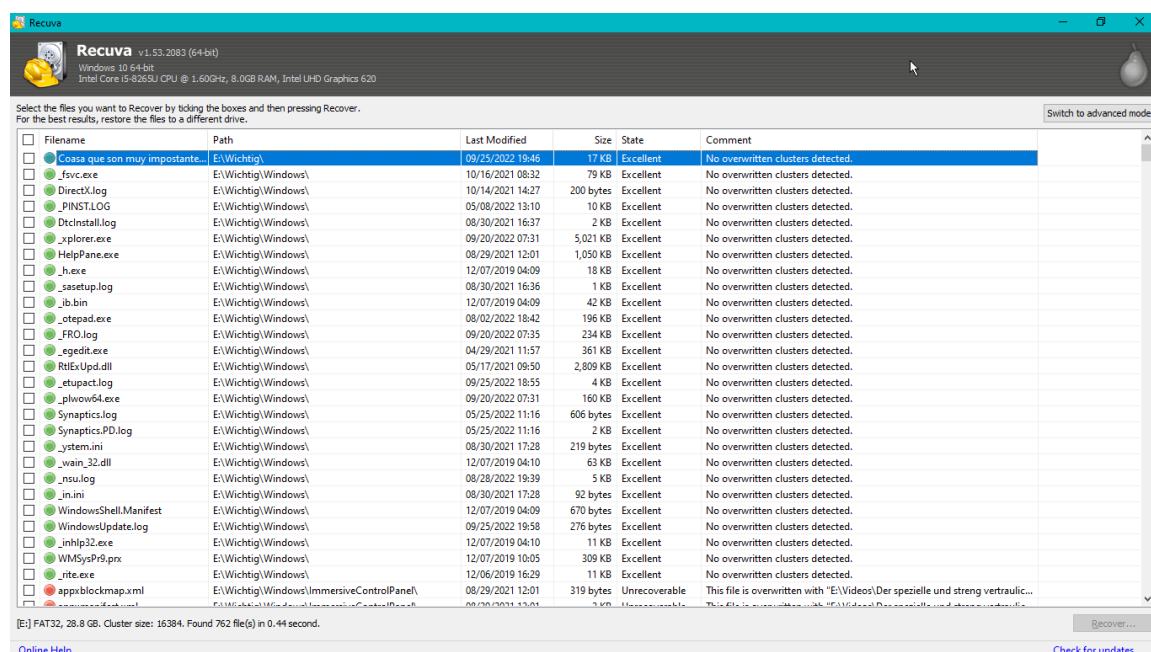


Figura 5: Posibles archivos a recuperar una vez ejecutado el software.

## 2.2. Kaspersky Endpoint Security para Windows

Como se mencionó anteriormente, *Kaspersky Endpoint Security for Windows* es la aplicación de seguridad más probada y premiada, con tecnologías de última generación creadas para proteger todos los endpoints de Windows y los datos que contienen (Lab, 2022). Los *endpoints* son dispositivos informáticos remotos que se comunican de un lado a otro con una red a la que están conectados; estos pueden ser desde servidores o computadoras de escritorio, hasta dispositivos móviles más pequeños como los celulares. Los endpoints representan los puntos de entrada vulnerables clave para los cibercriminales, en donde ejecutan código y explotan vulnerabilidades; así como donde hay activos para cifrar, filtrar o apalancar (Cyberpedia, 2022).

### 2.2.1. Máquinas Virtuales

De acuerdo con lo realizado en la actividad de la creación del laboratorio de pruebas, se utilizó la máquina virtual con Windows 10. Se preparó el ambiente desactivando Windows Defender desde el editor de registro, esto con el motivo de asegurarse de que no se active de forma autónoma ni al reiniciar la máquina virtual.

### 2.2.2. Instalación del antivirus

En línea con el manual proporcionado por IPC Services, una vez realizados los pasos pertinentes, se creó un enlace de descarga para así tener Kaspersky dentro de la máquina virtual que contendrá los distintos virus.

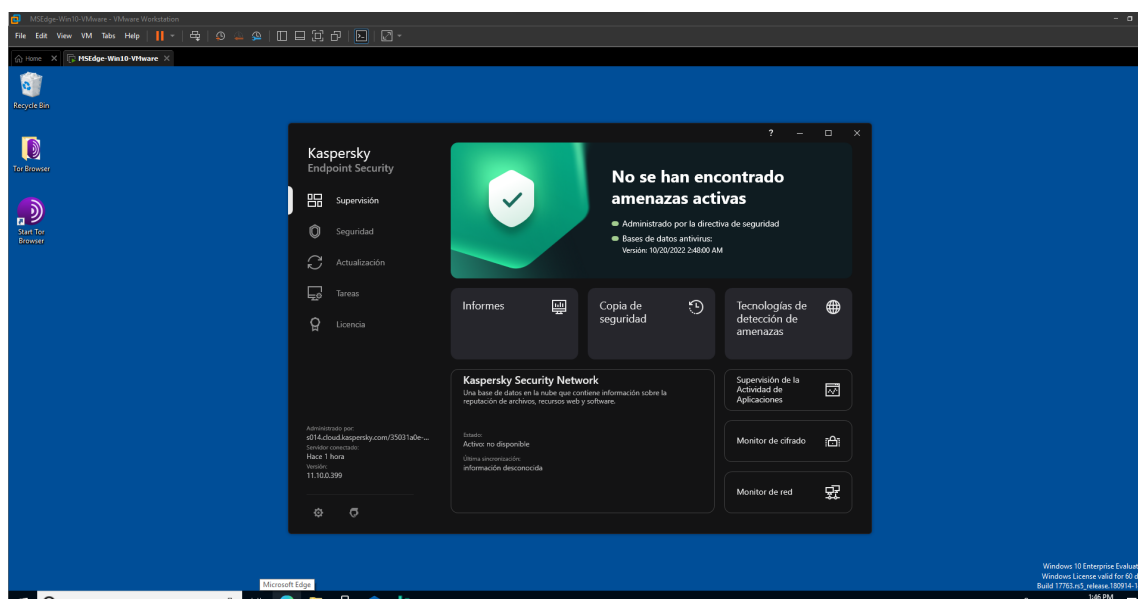


Figura 6: Kaspersky en Windows 10

### 2.2.3. Descarga de malware

Para descargar el malware que sería analizado con Kaspersky, se visitaron dos sitios, el primero, que fue proporcionado por IPC Services y el segundo, que fue encontrado utilizando Torch:

1. Malware Traffic Analysis (clearnet): En este sitio, se pueden encontrar diversos ataques y malware enfocados a las redes y su análisis, se descargó el malware llamado *ICEDID (BOK-BOT) INFECTION WITH COBALT STRIKE*". Al descargar el archivo, se encontró con un disco .ISO, se montó y se ejecutó el archivo que estaba adentro. Gráficamente no ocurrió nada, pero fue detectado por Kaspersky posteriormente.

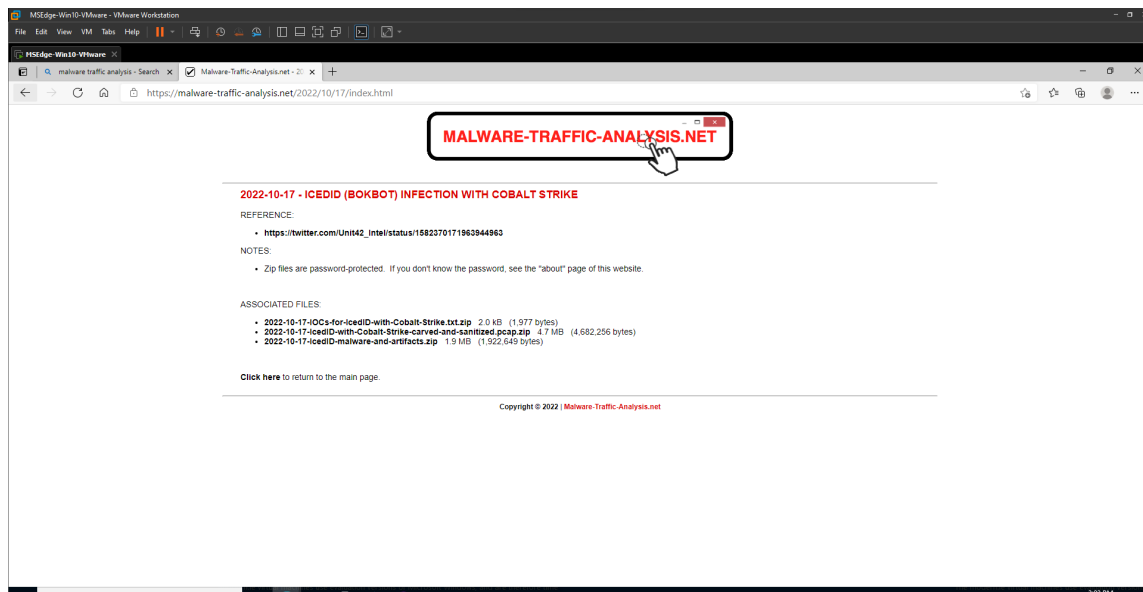


Figura 7: Malware Traffic Analysis

2. Best Carding World (darknet): Este sitio se encontró utilizando un motor de búsqueda llamado Torch, el cual, a diferencia de google, muestra resultados sin filtros. Se hizo la búsqueda *windows virus exe* y se llegó a dicho foro.

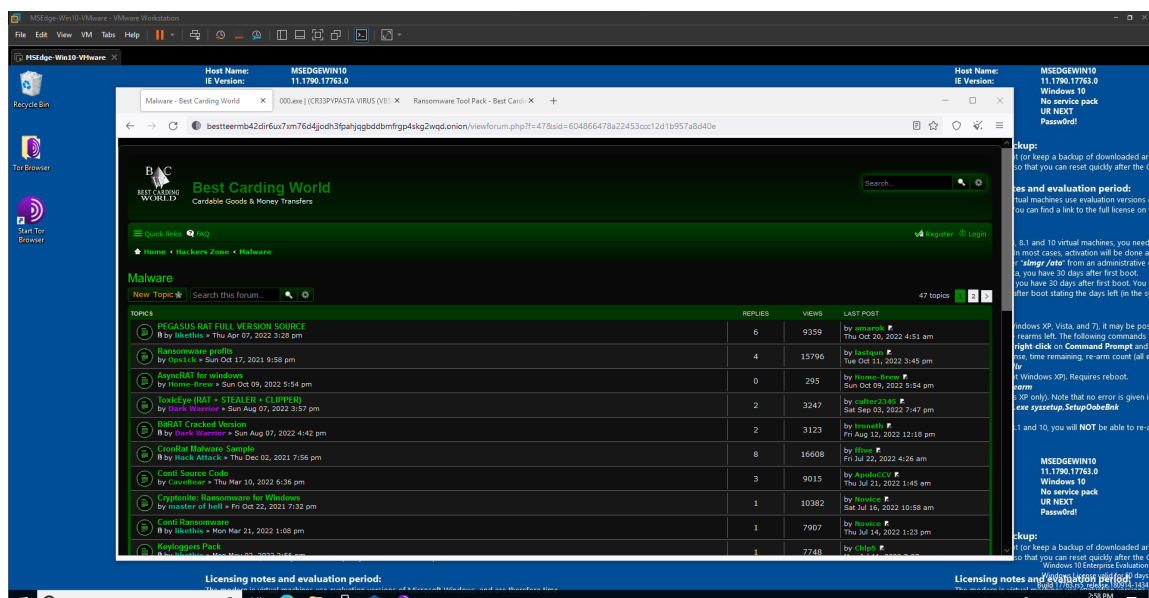


Figura 9: Best Carding World

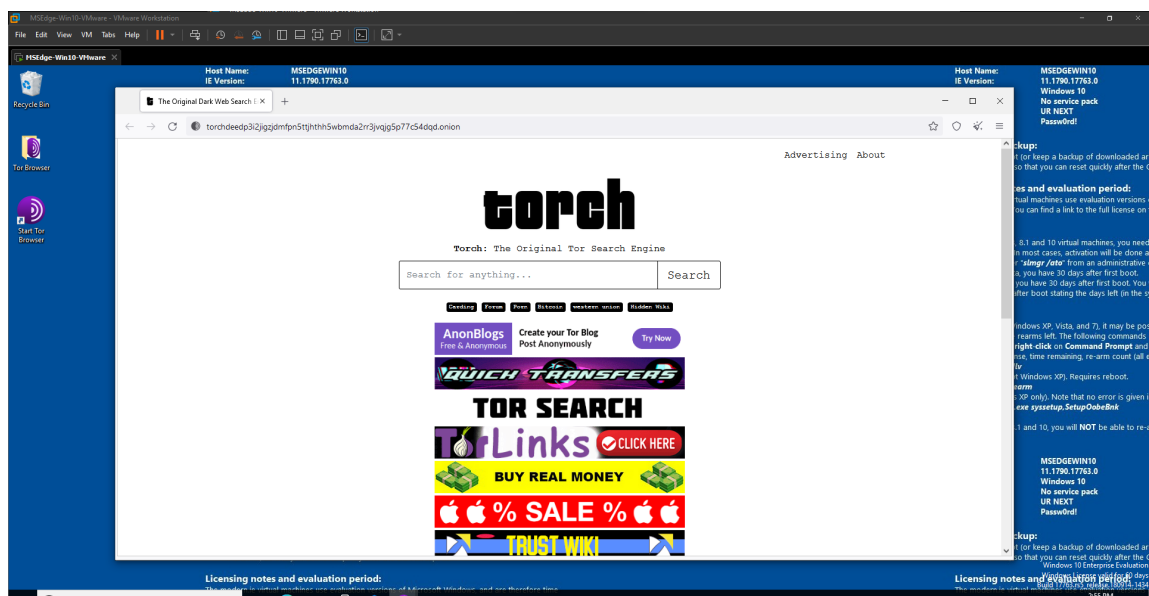


Figura 8: Torch

[H]

Una vez dentro del foro, se fue a la sección Malware y se descargaron 2 archivos, el primero llamado *000.exe* y el segundo fue un .zip que al analizarlo con Kaspersky se encontraron más de 50 archivos maliciosos. En este segundo .zip, se encontró el famoso ransomware *wannacry.exe*. Se supuso que ambos archivos ejecutables tenían efectos gráficos, por lo que se procedió a apagar Kaspersky y dejar la máquina completamente vulnerable. A continuación una breve descripción de lo que sucedió a nivel gráfico:

- a) *000.exe*: Se mostró una pantalla en blanco, una carretera y árboles, parpadeando y con distintos filtros. Se reinició la máquina virtual ya que no funcionaba ningún comando. Al encenderla, el nombre de usuario cambió a *UR NEXT*, el escritorio se llenó de imágenes con fondo rojo y texto con el mismo nombre de usuario, el administrador de tareas no se podía ejecutar y suponemos que algunos permisos se cambiaron automáticamente.

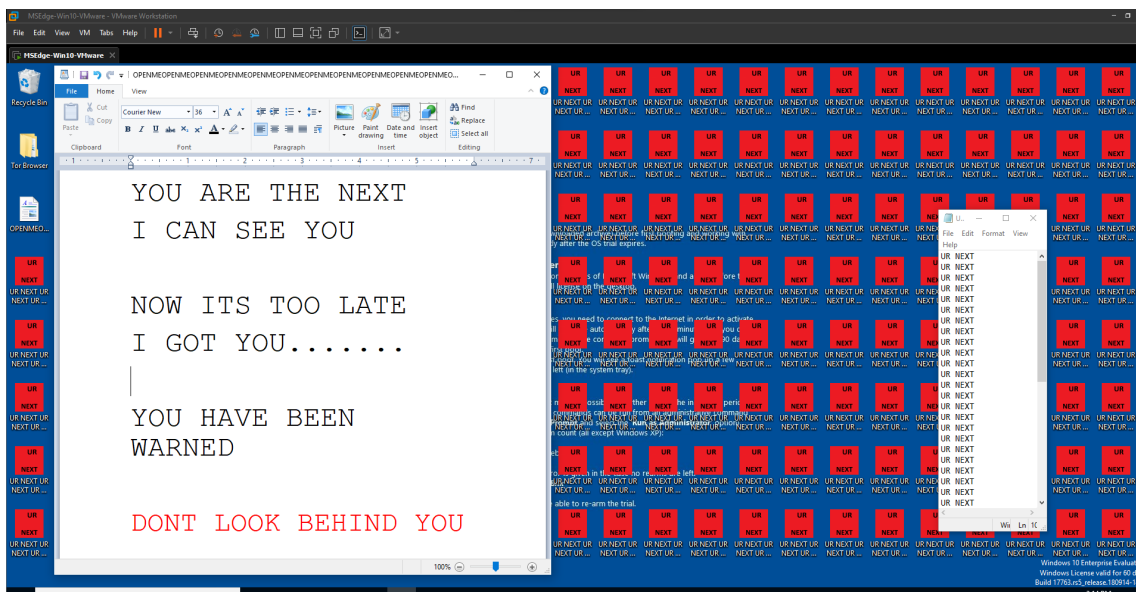


Figura 10: 000.exe

- b) *wannacry.exe*: Se refrescó la pantalla y en un instante se cifraron todos los archivos de la máquina virtual, se cambió el fondo de pantalla por las instrucciones para recuperar los archivos y el .exe con las instrucciones contenía una dirección de bitcoin pidiendo un depósito de \$600 USD para la recuperación de los archivos.

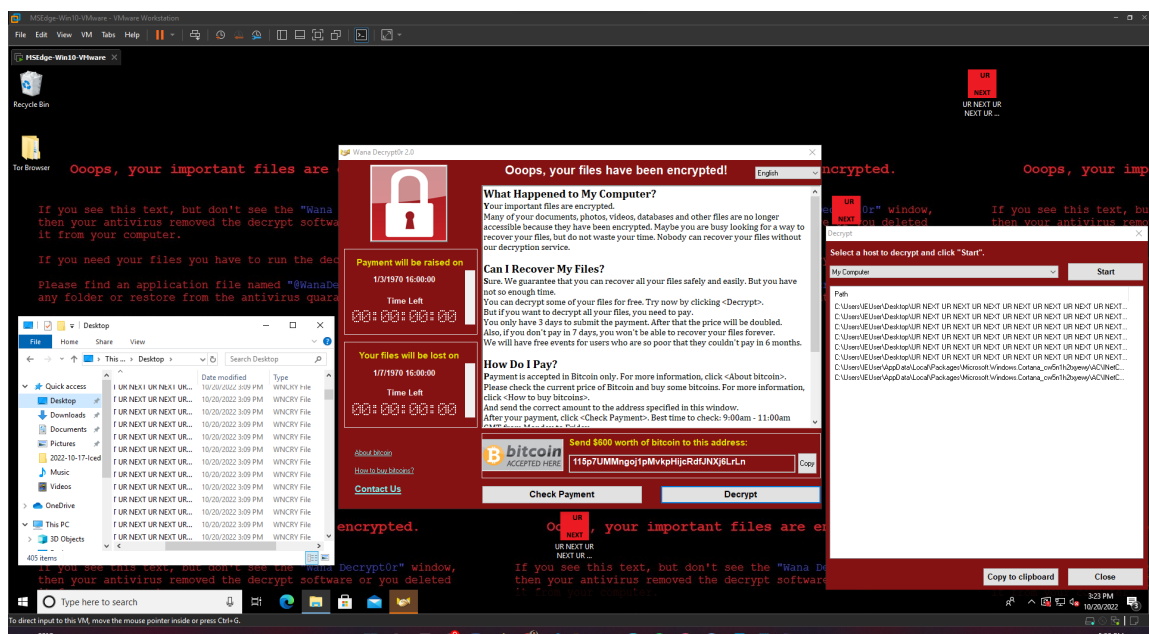


Figura 11: wannacry.exe

#### 2.2.4. Monitoreo, detección y respuesta

A través del portal de Kaspersky configuramos dos perfiles de protección, uno con todas las herramientas recomendadas activadas y otro con todas desactivadas. Esto dado que el antivirus con el perfil recomendado analizaba todas las descargas y en la mayoría de los casos borraba los archivos antes de que estos pudieran ser ejecutados.

### Threat development chain graph

[How to read a threat development chain graph?](#)

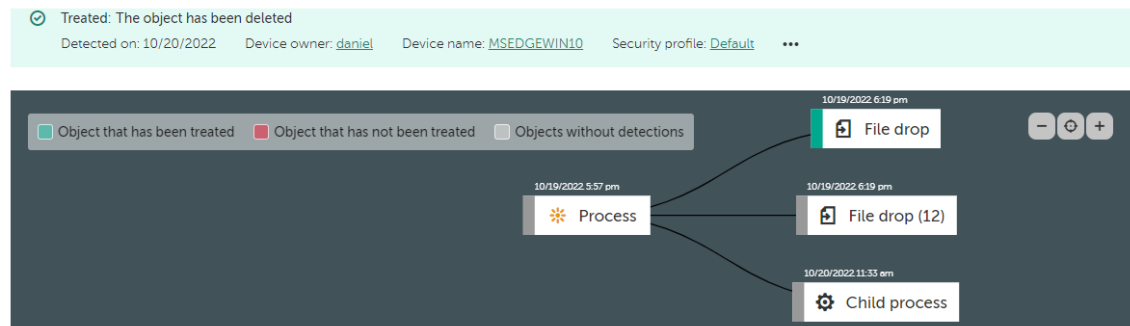


Figura 12: Gráfico de desarrollo de la amenaza

## 3. Resultados

### 3.1. Recuperación de Archivos

Se lograron identificar un total de 762 archivos borrados, algunos de ellos con círculos verdes, amarillos y rojos, los cuales representan el estado de los archivos. Entre estos archivos se logró encontrar el archivo objetivo con el mensaje oculto que es *Coasa que son muy importantes y muy confidenciales que deben de ser muy secretas.jpg* y se ve de la siguiente manera:



Figura 13: Imagen recuperada.

### 3.2. Kaspersky Endpoint Security para Windows

Utilizando el perfil inseguro fue posible descargar y correr un troyano que inició varios procesos antes de ser detectado y eliminado.



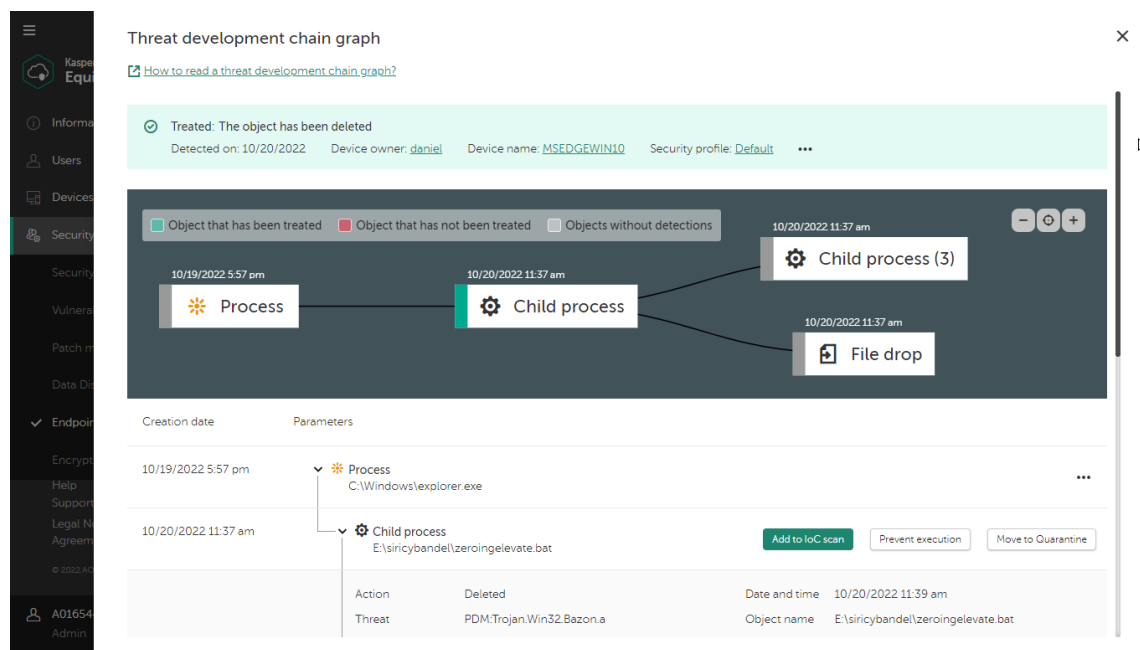


Figura 14: Gráfico de desarrollo del troyano

En los logs encontramos que este archivo fue detectado mediante análisis de comportamiento e instantáneamente se eliminó junto con los procesos que había iniciado

1. **xcopy** para copiar un archivo a una carpeta temporal
2. **rundll32** para ejecutar este archivo
3. **conhost** intentando abrir forzosamente una versión anterior de la aplicación, este comando en específico está relacionado con el ransomware Ryuk.

Otros procesos también pudieron crear procesos antes de ser detectados por el perfil inseguro de antivirus. Pero al cambiar al perfil recomendado y realizar un análisis se eliminaron 59 archivos maliciosos.

## Threats detected during last 7 days

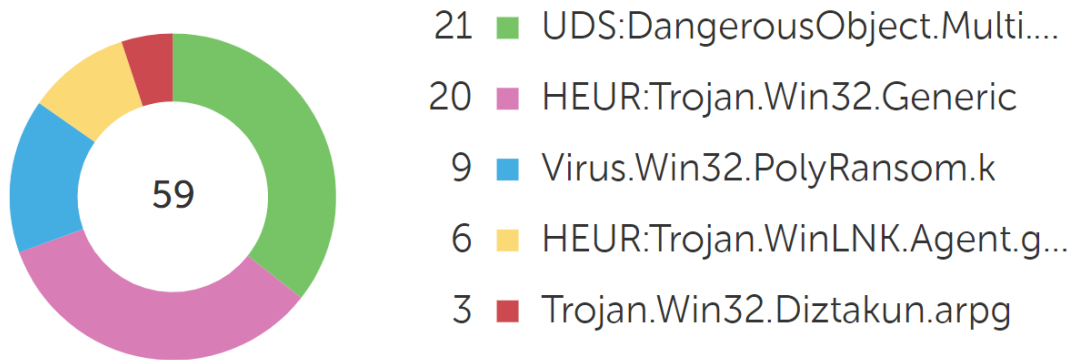


Figura 15: Amenazas detectadas por el antivirus

## 4. Conclusiones

### 4.1. Recuperación de Archivos

Después de haber finalizado con el análisis forense de la USB, se pudieron recuperar los archivos de color verde y algunos amarillos, sin embargo, los archivos que aparecían en rojo dentro del programa Recuva no pudieron recuperarse. A forma de resumen, se encontraron 762 archivos tras realizar un escaneo profundo, esto tomó un tiempo de aproximadamente 0.44 segundos. Algunos formatos de los archivos que se encontraron fueron ejecutables, imágenes, PAK, .dll, .xml, .log, .ini, .prx, etc. El objetivo se cumplió, habiendo encontrado una vasta cantidad de archivos en diversos idiomas, incluyendo el alemán, por lo que se asume que se logró la meta. Igualmente, como se mencionó en clase, se encontró un archivo que fungió como banderilla de haber realizado con éxito la actividad, este archivo tiene el nombre de *Čoasa que son muy impostantes y muy confidenciales que deben de ser muy secretas.jpg*, es una imagen y tiene la frase *CONFIDENTIAL*. Se decidió que este archivo era la banderilla ya que era el único que resaltaba de todos los demás.

## 4.2. Kaspersky Endpoint Security para Windows

Después de haber buscado malware para infectar la máquina virtual y haber analizado estos archivos con el antivirus de Kaspersky pudimos identificar distintos tipos de malware como troyanos y ransomware, además tuvimos la oportunidad de estudiar su comportamiento dentro de un ambiente seguro. Nos dimos cuenta de que el antivirus es muy eficiente porque identificó amenazas en base a diferentes parámetros como hashes, análisis de actividad, aprendizaje automático y control de accesos. Se cumplió el objetivo de identificar el tipo de ataques, sus orígenes y las acciones que realizaron a través del software de Kaspersky.

## Referencias

- CCleaner. (s.f.). Recuva: Recover your deleted files quickly and easily. <https://www.ccleaner.com/es-es/recuva>
- Cyberpedia. (2022). What is an Endpoint? <https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint>
- Interpol. (s.f.). Análisis forense digital. <https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital>
- Lab, A. K. (2022). Endpoint Security para Windows — Kaspersky. <https://latam.kaspersky.com/small-to-medium-business-security/endpoint-windows>
- Prakash, B., Rani, K., Prasad, S., & Sudha, T. (2022). Techniques in Computer Forensics: A Recovery perspective. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.4008&rep=rep1&type=pdf>
- Pro, I. (2019). Data recovery: Why is it so important? <https://www.itpro.co.uk/data-loss-prevention/28864/data-recovery-why-is-it-so-important#:~:text=In%5C%20technical%5C%20terms%5C%20data%5C%20recovery,applications%5C%20or%5C%20system%5C%20booting%5C%20failures>