ANTONIO BANDERAS
CARLOS MATEOS
DANIEL SÁNCHEZ
DIANA CADENA
LEONARDO LAURELES

# ANÁLISIS FORENSE Y ENDPOINT SECURITY CLOUD

**"EL ANÁLISIS FORENSE DIGITAL ES UN ÁREA DE LA CIBERSEGURIDAD QUE SE ENCARGA EN LA DETECCIÓN, ADQUISICIÓN, TRATAMIENTO, ANÁLISIS Y COMUNICACIÓN DE DATOS."**

**Costo asociado**

Cuestan alrededor de **24 millones de dólares** al año.

# EN MÉXICO...

**Víctimas**

**2/3** empresas fueron víctimas de ciberataques en **2018**

# RECUPERACIÓN DE DATOS

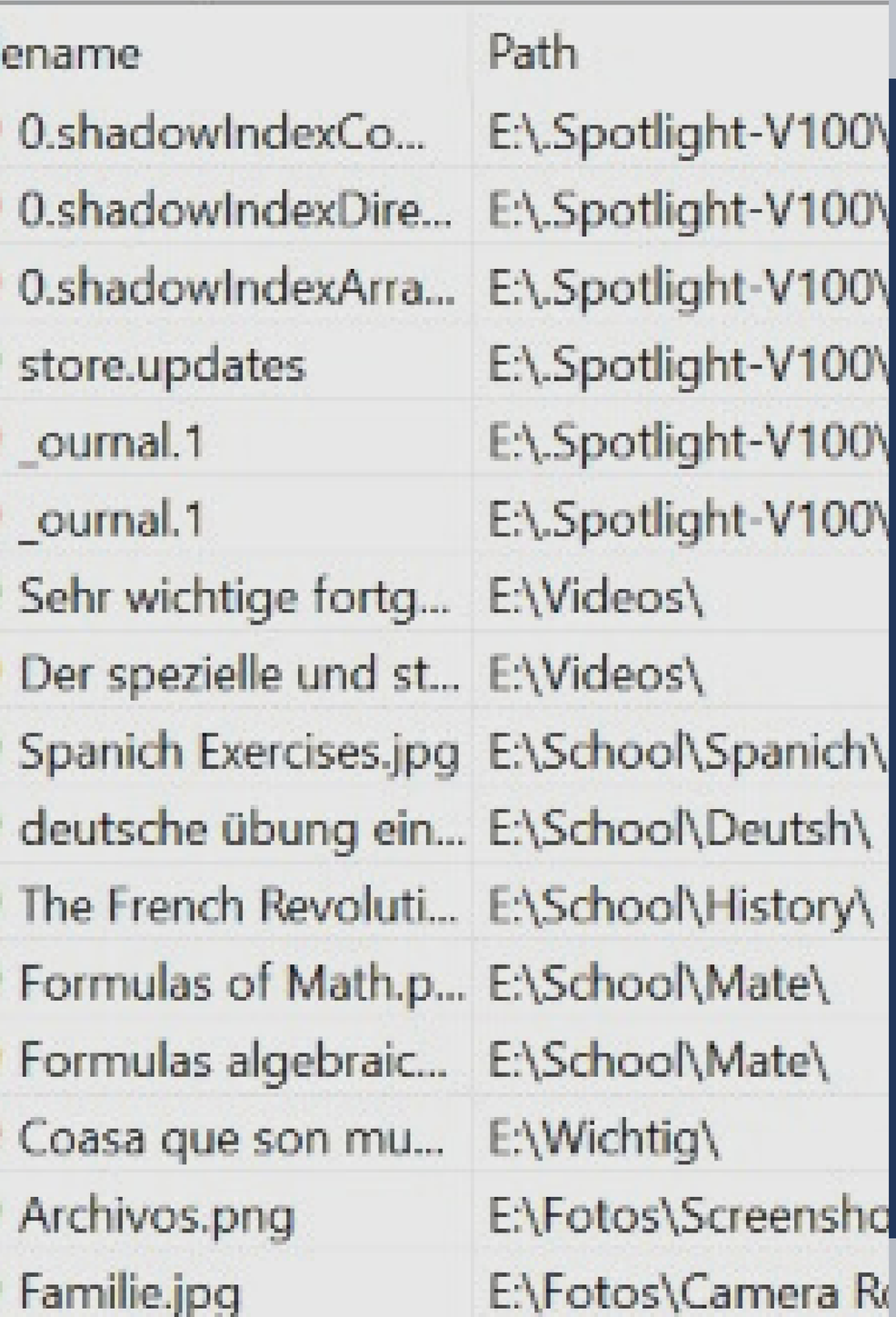
*Al borrar un archivo, se borra el acceso directo al archivo pero el disco duro sigue guardando la información hasta que se sobrescriba.*

**Recuva**

# DETECCIÓN DE VIRUS

*Los virus pueden representar distintos peligros para las empresas, por lo que su detección y tratado en etapas tempranas es de suma importancia. Estos pueden entrar por medio de páginas web, correos electrónicos (spam) y descargas sospechosas.*

**Kaspersky Endpoint Security**




# RECUPERACIÓN DE DATOS ELIMINADOS

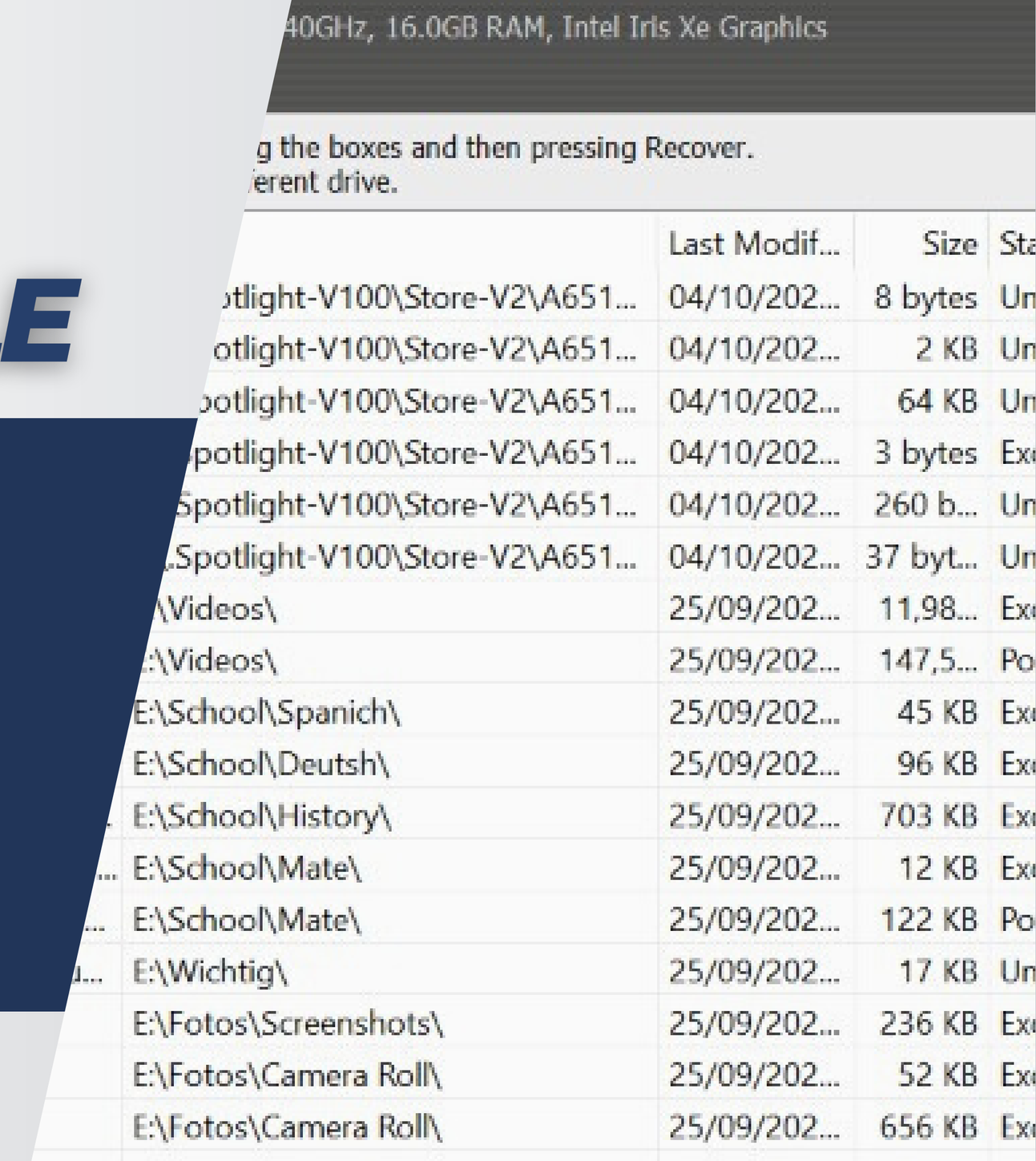
**Pasos a seguir:**

- Acceder a la USB para conocer su contenido.
- Realizar un respaldo de los datos.
- Escaneo simple y profundo para ver todos los archivos eliminados.
- Obtener archivos en sus estados verdes, amarillo y rojo.
- Identificar el archivo borrado importante para la empresa.

# ANÁLISIS SIMPLE

17 archivos encontrados
7 archivos nuevos

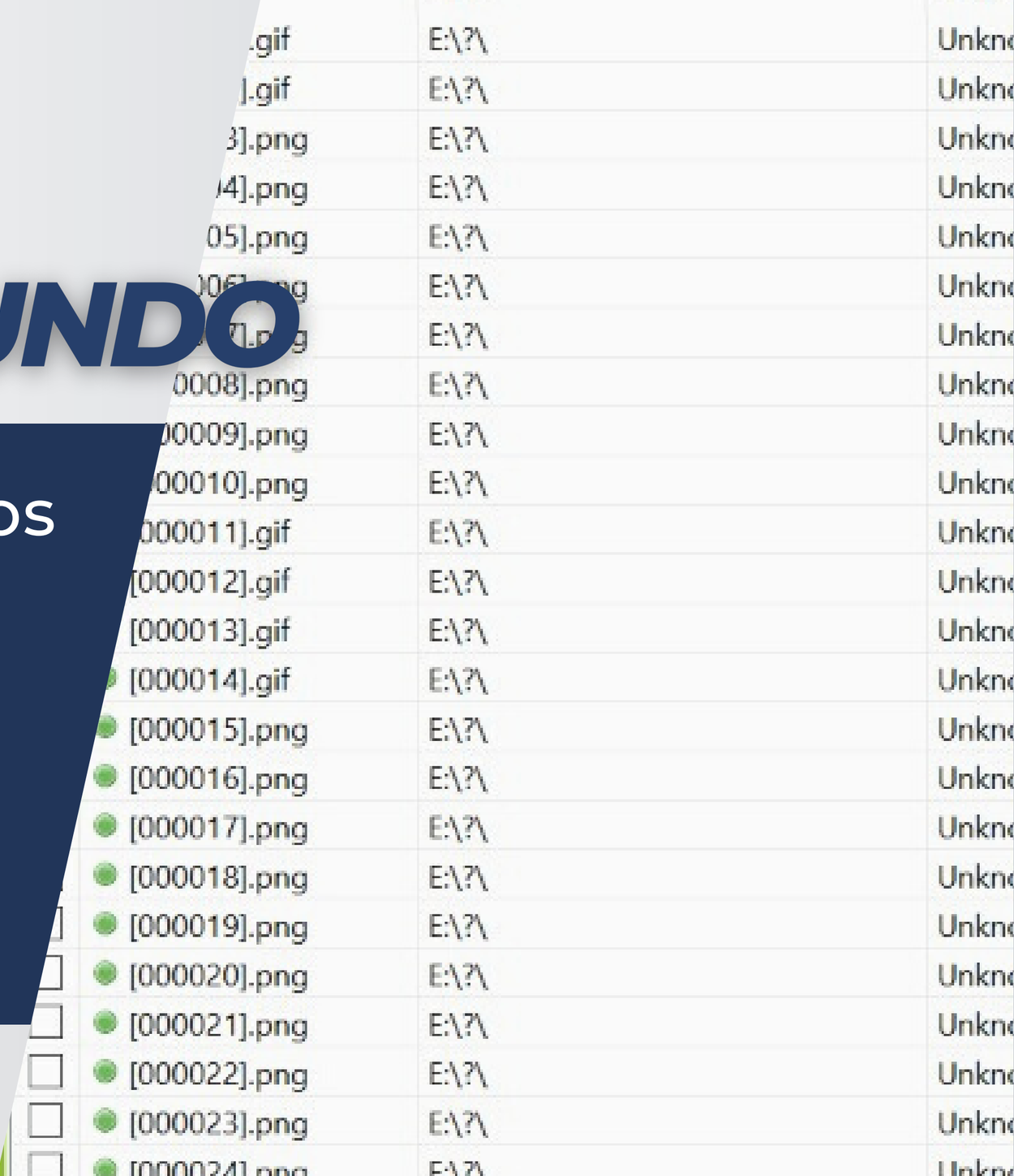
*ubicación, última modificación, tamaño y estado de cada archivo*



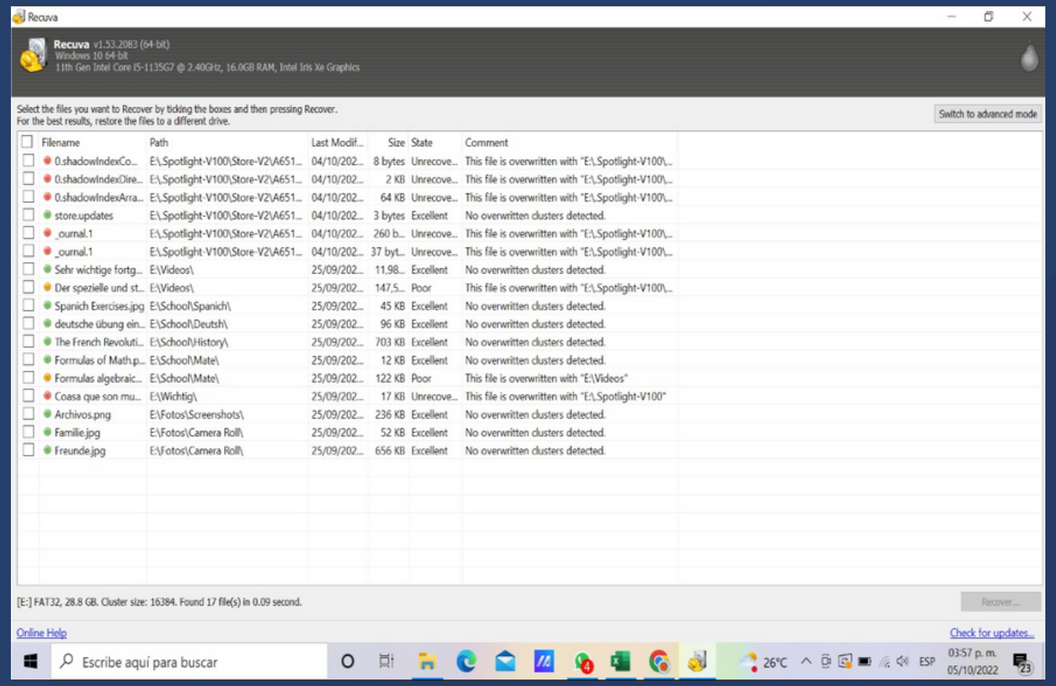
# ANÁLISIS PROFUNDO

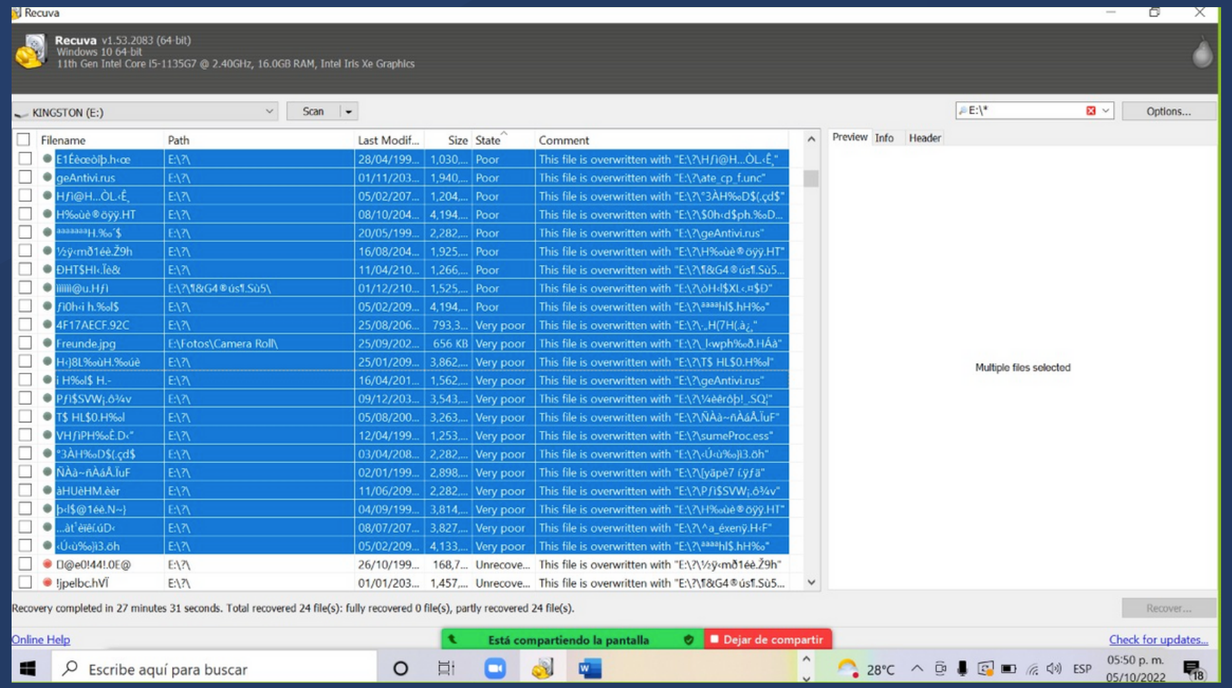
12,944 archivos encontrados
12,934 archivos nuevos

*766 edo. verde*
*26 edo. amarillo*
*11,000 edo. rojo*



# COMPARATIVA



**Tiempo de recuperación:**

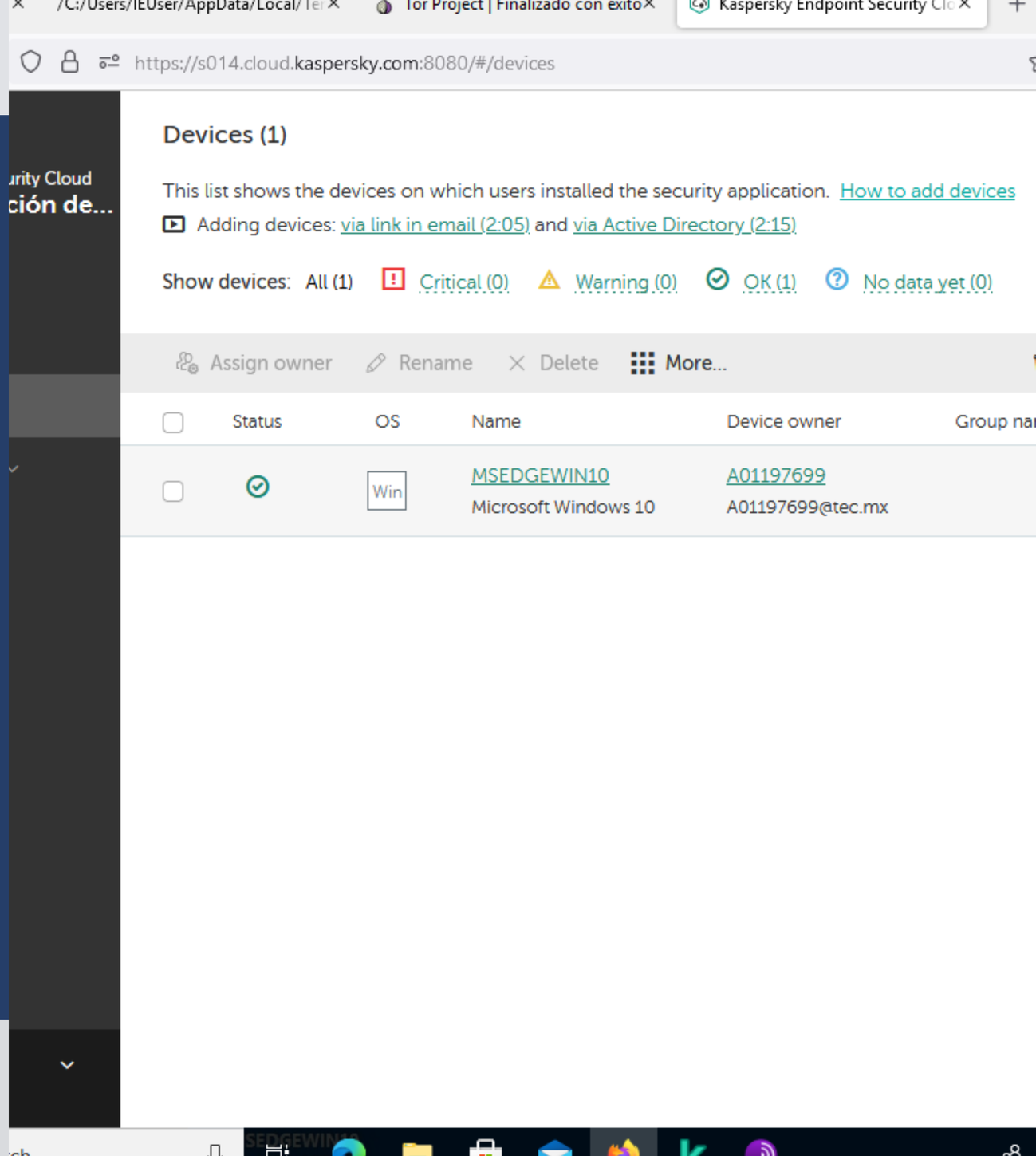
27 minutos con 31 segundos

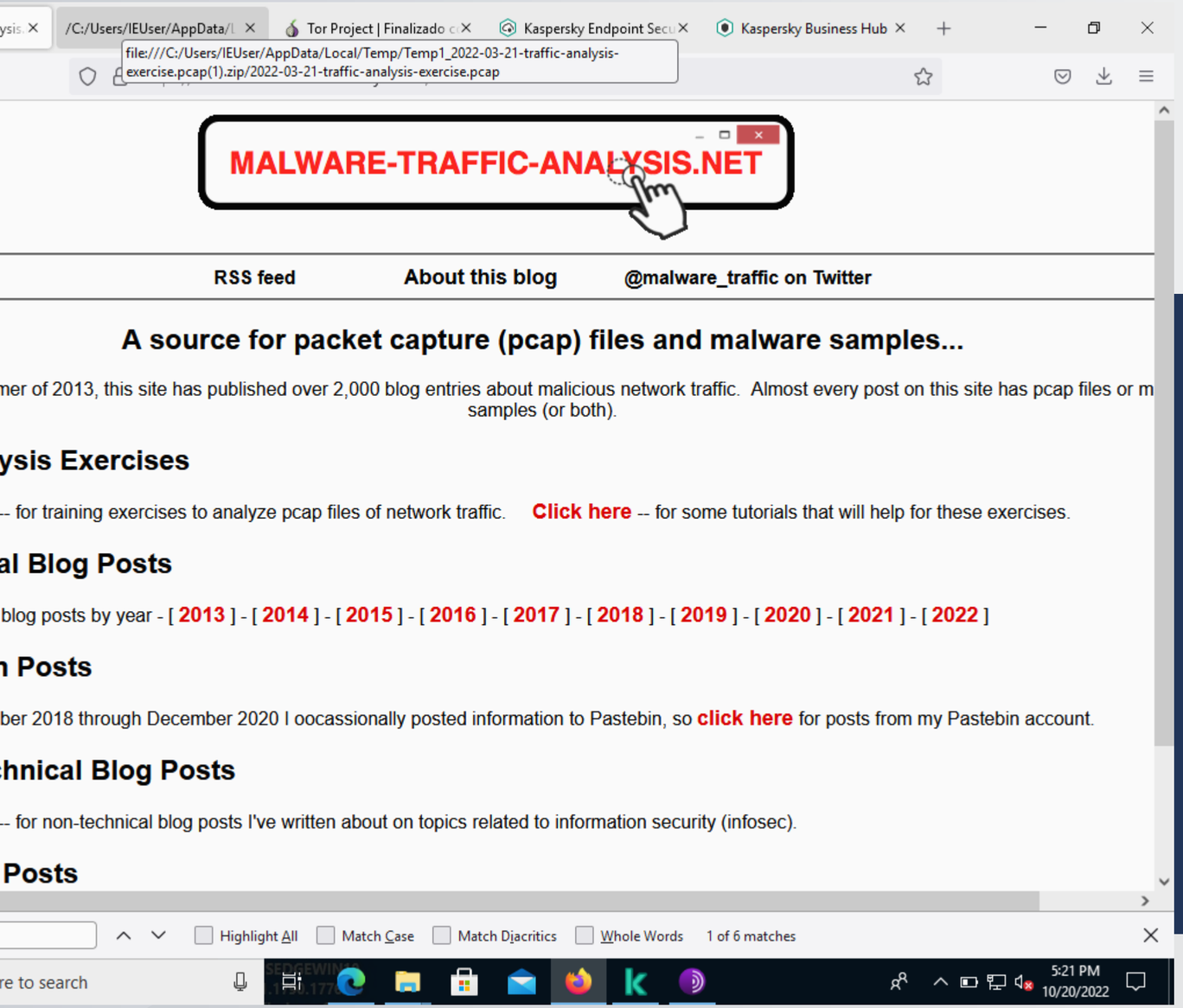

# IMAGEN ENCONTRADA

# KASPERSKY

**Pasos a seguir:**

- Instalación de Kaspersky
- Asignación de Dispositivos a Perfil de Seguridad y Usuarios



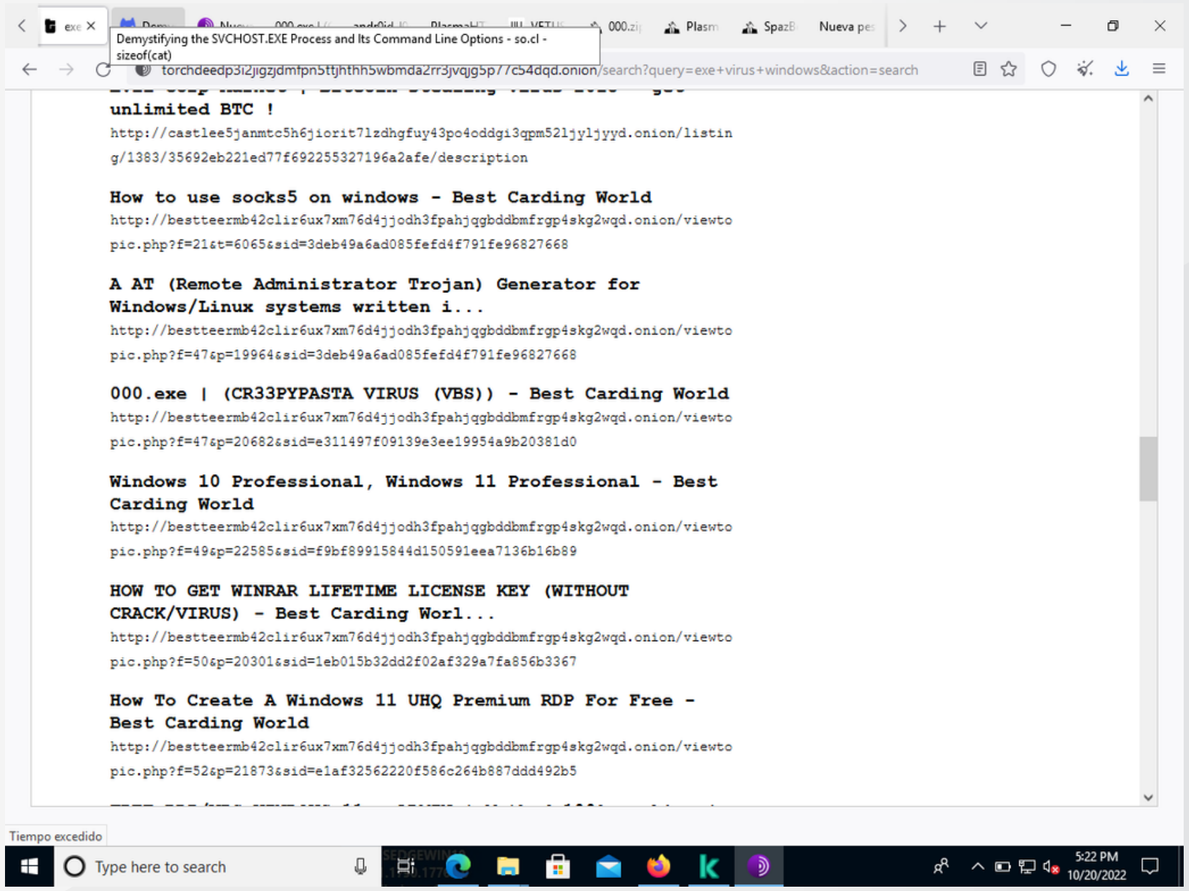


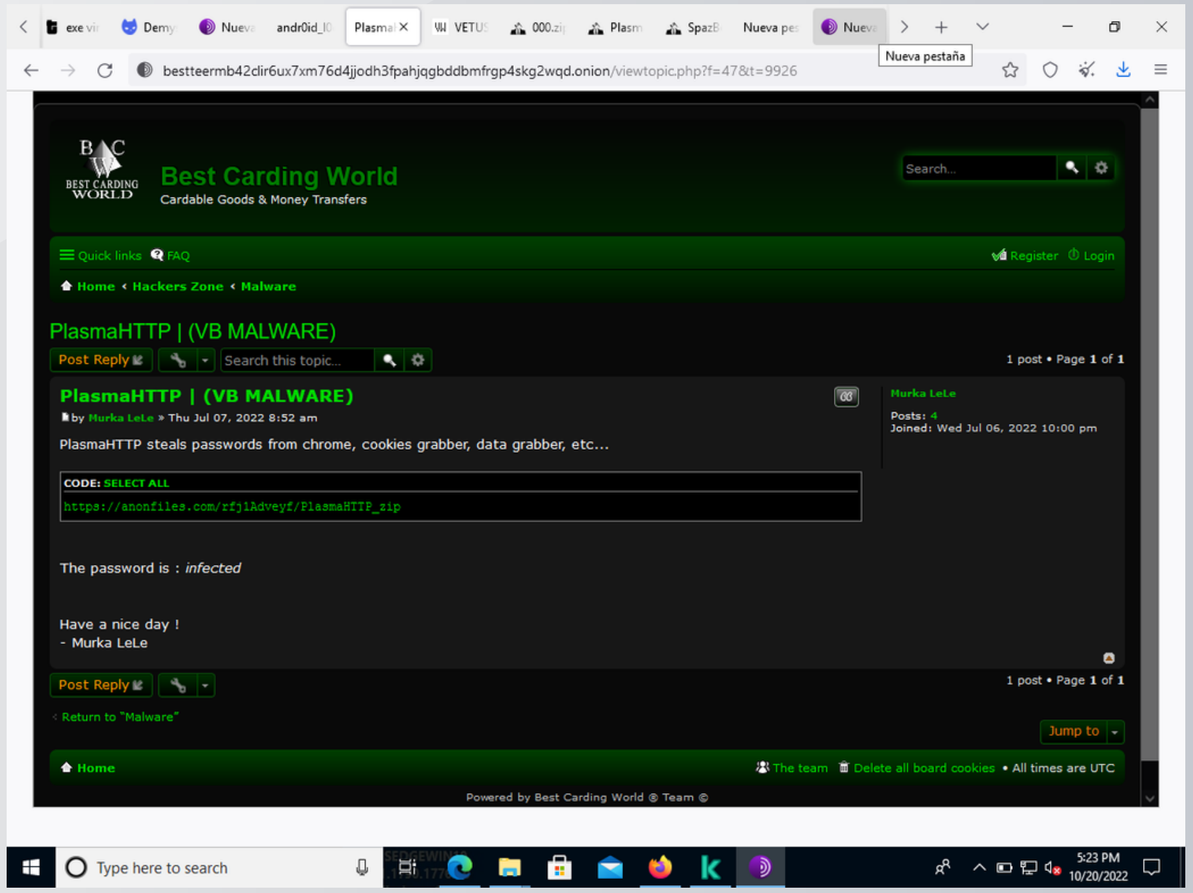

# ANÁLISIS DE MALWARE

Página proporcionada por la OSF

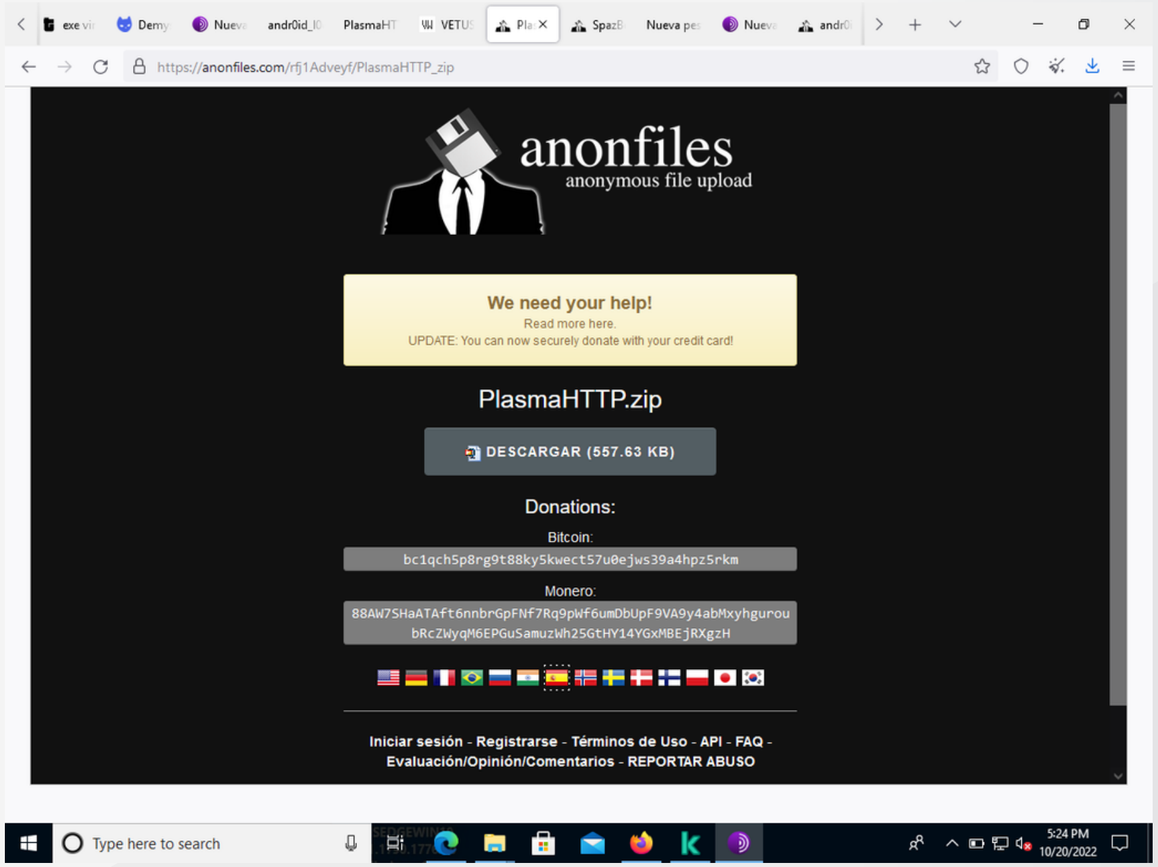
Análisis y verificación de amenazas detectadas

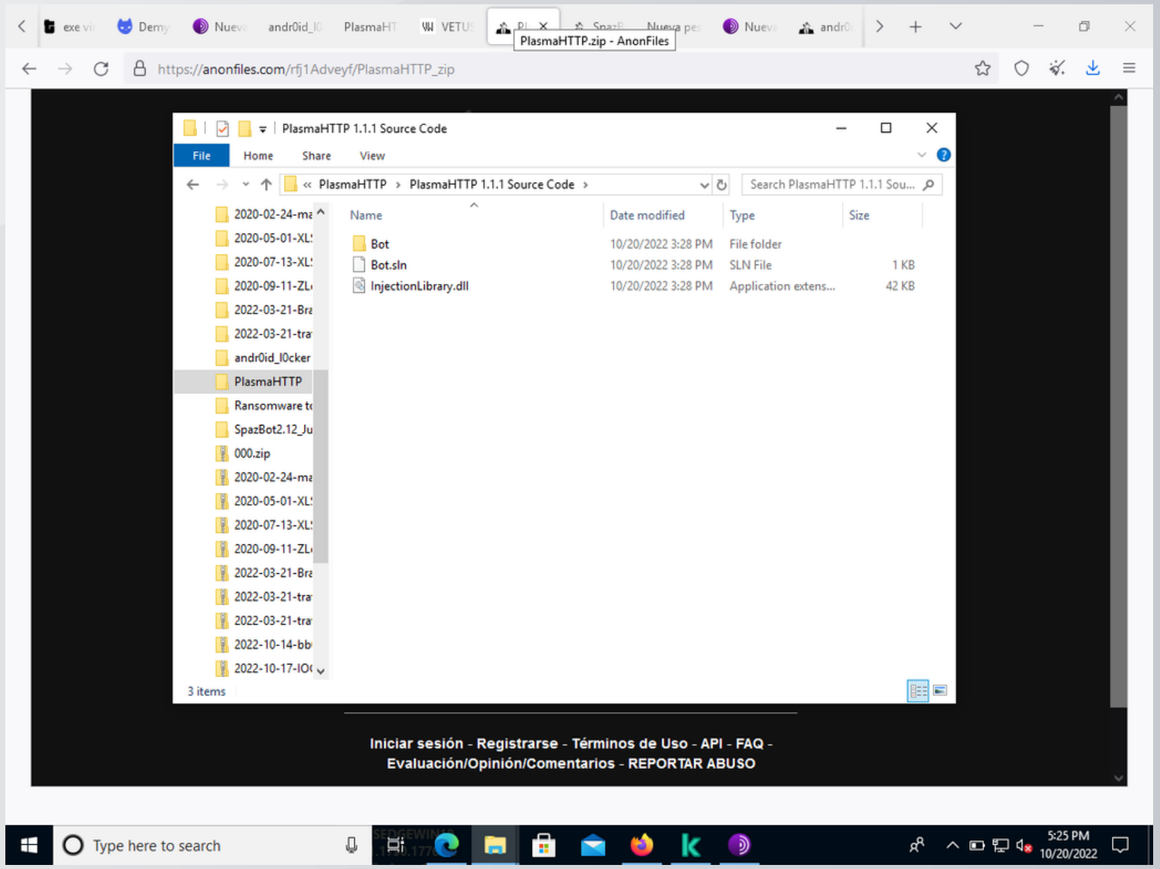
# BÚSQUEDA EN SITIOS EXTERNOS



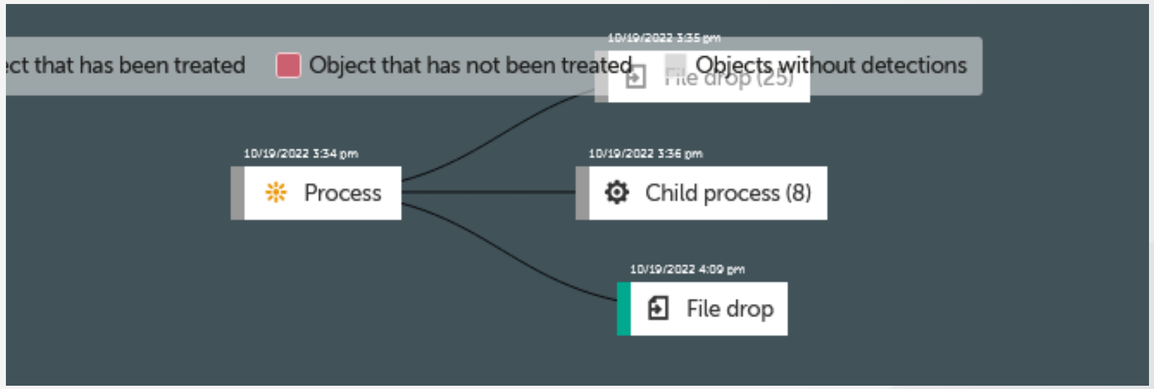



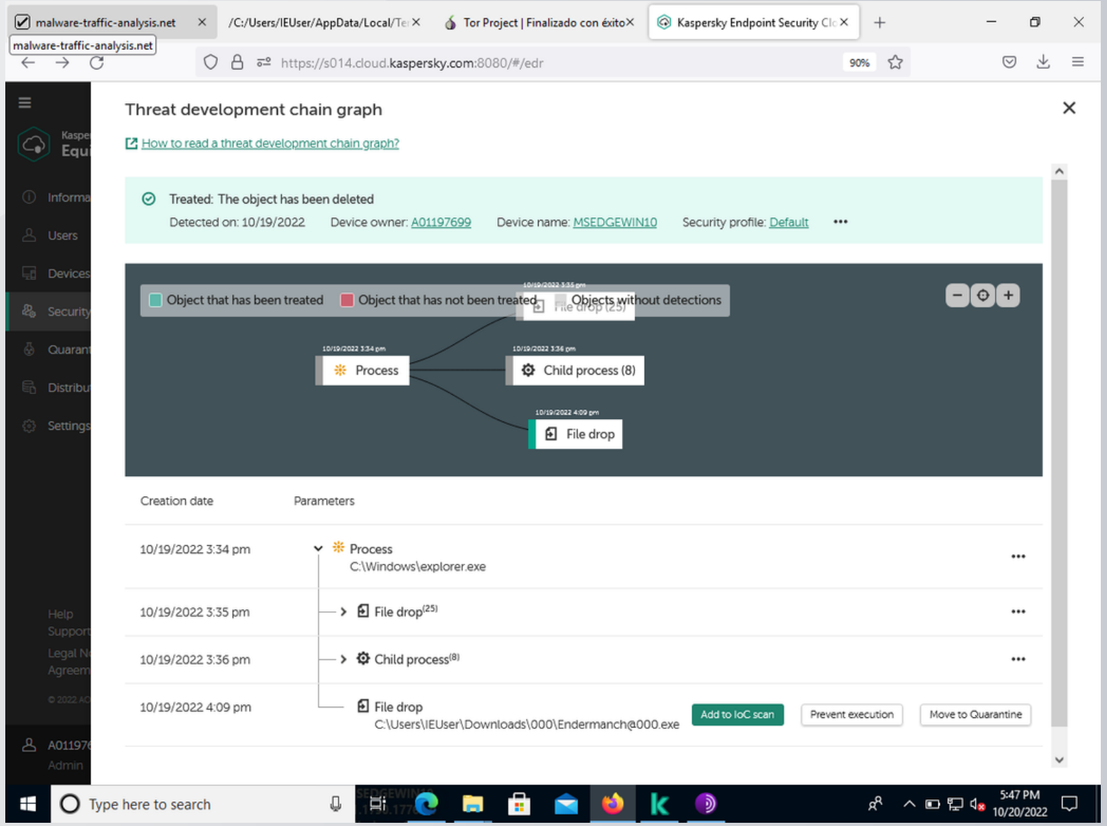
# ARCHIVO UTILIZADO



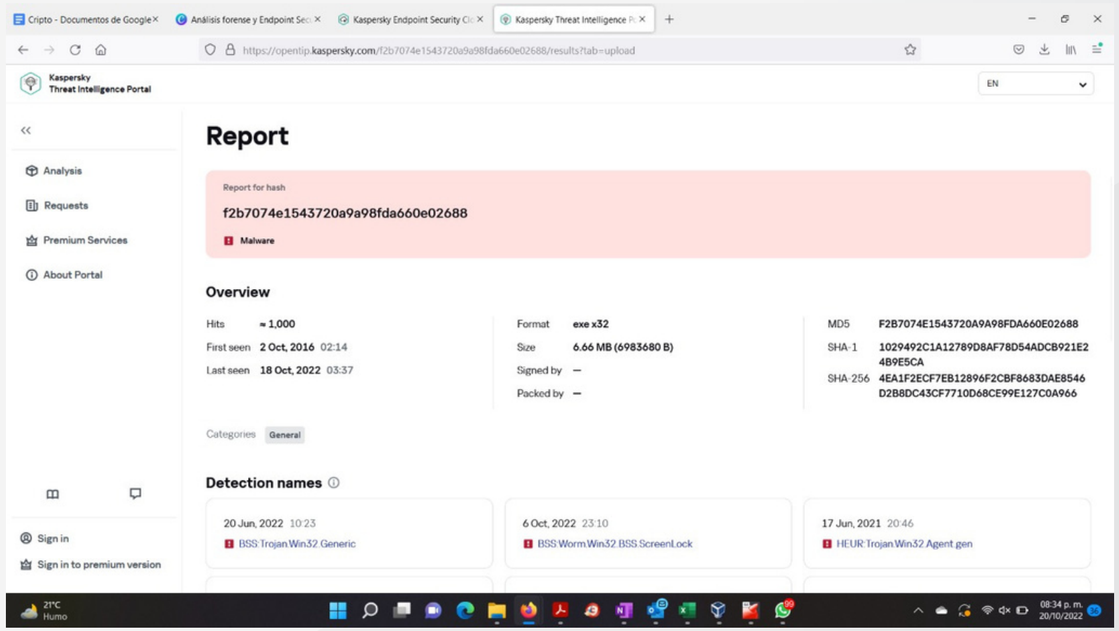



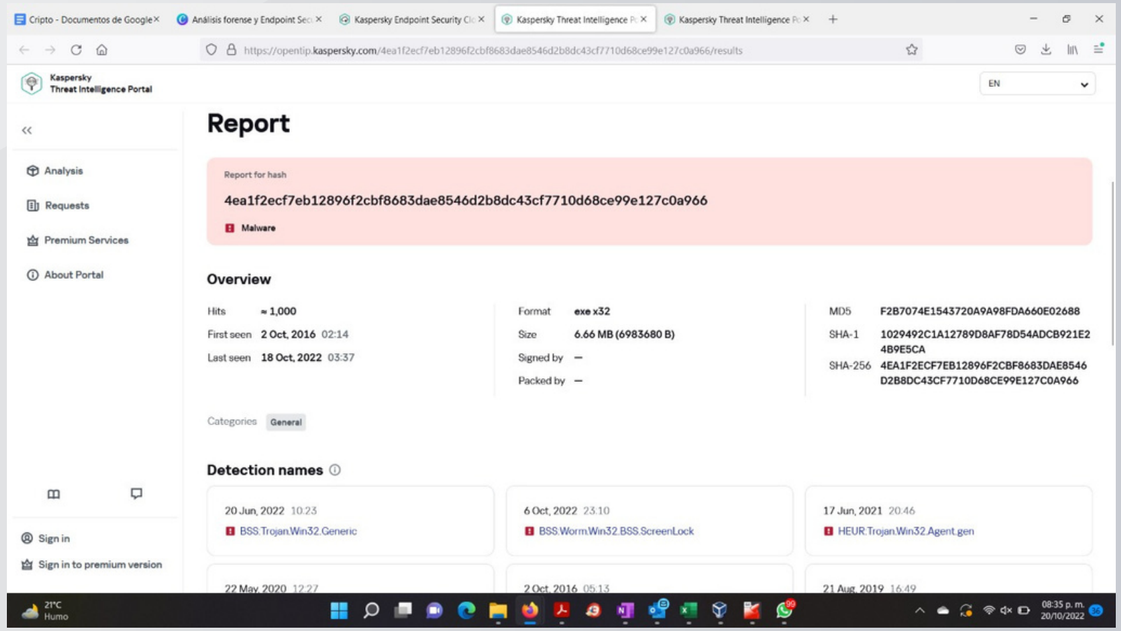
# *KASPERSKY* GRÁFICO DE CADENA



# KASPERSKY THREAT INTELLIGENCE PORTAL



# CONCLUSIONES

Tener cuidado sobre dónde se conectan los dispositivos

Mantener claros los objetivos del análisis forense, no desviarse

Mantener respaldos tanto físicos como digitales

Tomar medidas necesarias de protección ante amenazas y ataques