

0000

ANÁLISIS FORENSE Y ENDPOINT SECURITY CLOUD

ANTONIO BANDERAS
CARLOS MATEOS
DANIEL SÁNCHEZ
DIANA CADENA
LEONARDO LAURELES

0000

**"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

ename	Path	
0.shadowIndexCo...	E:\Spotlight-V100\	oooo
0.shadowIndexDire...	E:\Spotlight-V100\	
0.shadowIndexArra...	E:\Spotlight-V100\	
store.updates	E:\Spotlight-V100\	
_ournal.1	E:\Spotlight-V100\	
_ournal.1	E:\Spotlight-V100\	
Sehr wichtige fortg...	E:\Videos\	
Der spezielle und st...	E:\Videos\	
Spanich Exercises.jpg	E:\School\Spanich\	
deutsche Übung ein...	E:\School\Deutsh\	
The French Revoluti...	E:\School\History\	
Formulas of Math.p...	E:\School\Mate\	
Formulas algebraic...	E:\School\Mate\	
Coasa que son mu...	E:\Wichtig\	
Archivos.png	E:\Fotos\Screensho	
Familie.jpg	E:\Fotos\Camera R	

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*

g the boxes and then pressing Recover.
erent drive.

	Last Modif...	Size	Sta
Spotlight-V100\Store-V2\A651...	04/10/202...	8 bytes	Un
otlight-V100\Store-V2\A651...	04/10/202...	2 KB	Un
otlight-V100\Store-V2\A651...	04/10/202...	64 KB	Un
potlight-V100\Store-V2\A651...	04/10/202...	3 bytes	Exe
Spotlight-V100\Store-V2\A651...	04/10/202...	260 b...	Un
.Spotlight-V100\Store-V2\A651...	04/10/202...	37 byt...	Un
\Videos\	25/09/202...	11,98...	Exe
\Videos\	25/09/202...	147,5...	Po
E\School\Spanisch\	25/09/202...	45 KB	Exe
E\School\Deutsch\	25/09/202...	96 KB	Exe
E\School\History\	25/09/202...	703 KB	Exe
E\School\Mate\	25/09/202...	12 KB	Exe
E\School\Mate\	25/09/202...	122 KB	Po
E\Wichtig\	25/09/202...	17 KB	Un
E\Fotos\Screenshots\	25/09/202...	236 KB	Exe
E\Fotos\Camera Roll\	25/09/202...	52 KB	Exe
E\Fotos\Camera Roll\	25/09/202...	656 KB	Exe

ANÁLISIS PROFUNDO

12,944 archivos encontrados

12,934 archivos nuevos

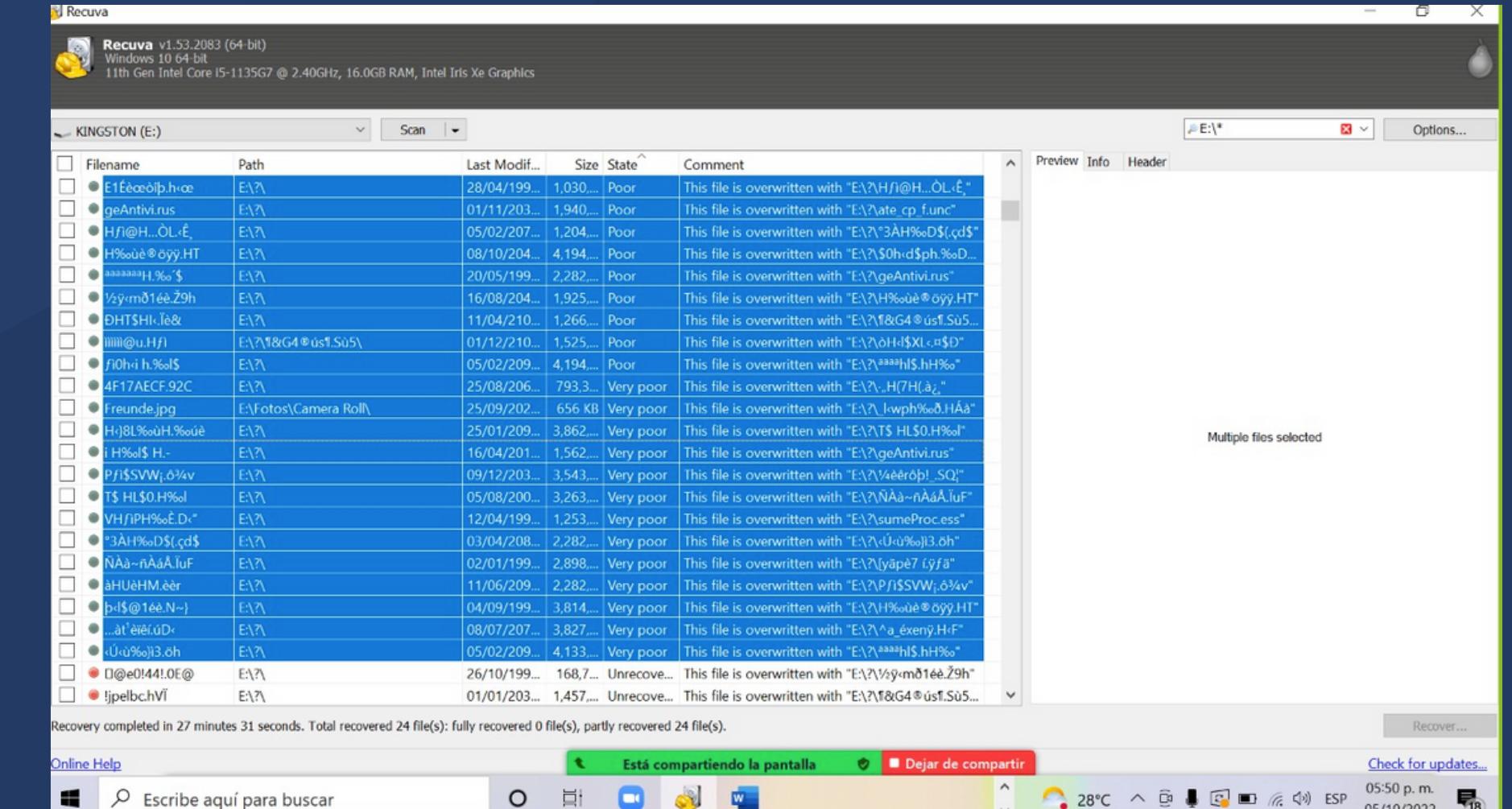
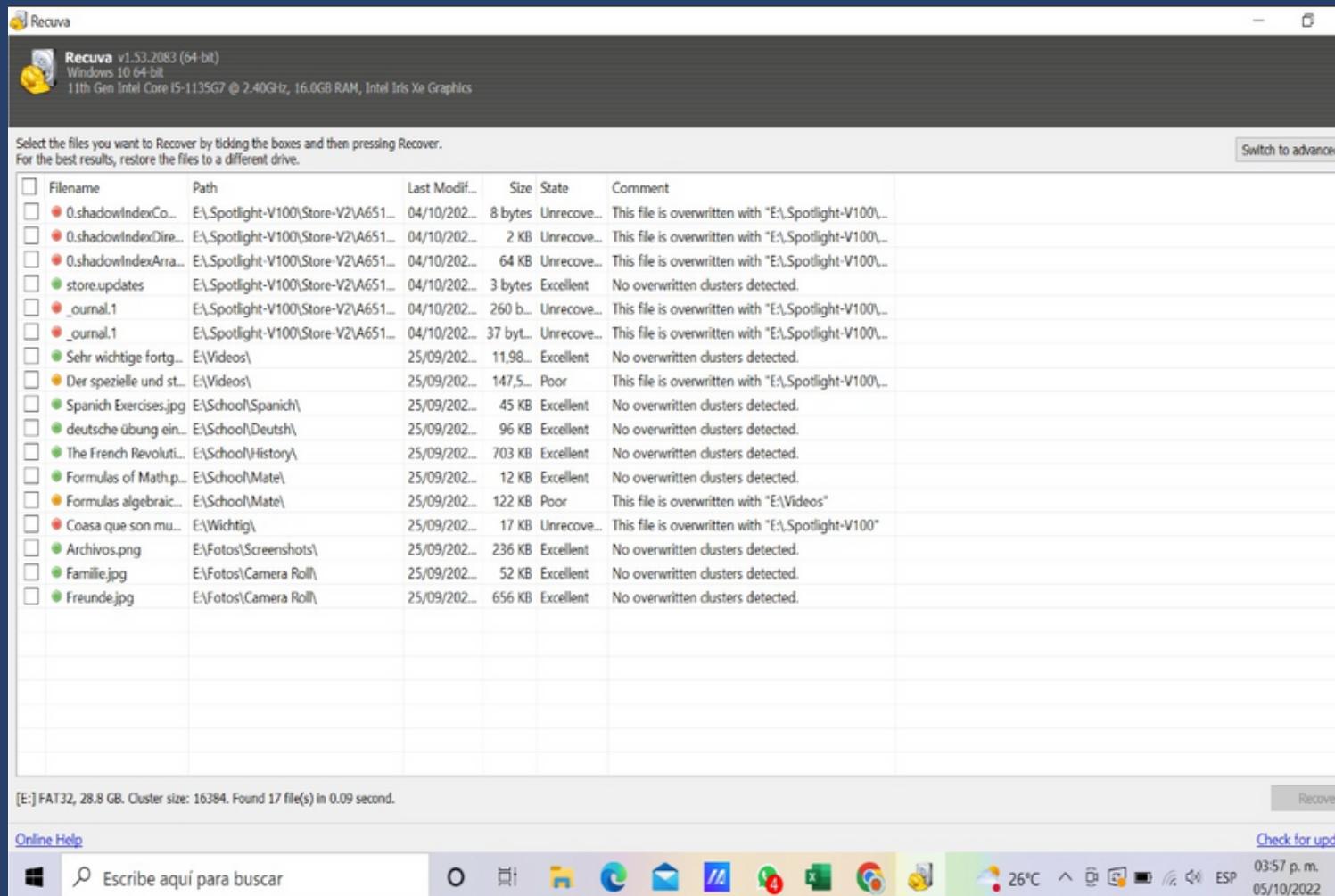
766 edo. verde

26 edo. amarillo

11,000 edo. rojo

.gif	E:\A\	Unknown
J.gif	E:\A\	Unknown
3].png	E:\A\	Unknown
4].png	E:\A\	Unknown
05].png	E:\A\	Unknown
06].png	E:\A\	Unknown
07].png	E:\A\	Unknown
0008].png	E:\A\	Unknown
00009].png	E:\A\	Unknown
00010].png	E:\A\	Unknown
000011].gif	E:\A\	Unknown
[000012].gif	E:\A\	Unknown
[000013].gif	E:\A\	Unknown
[000014].gif	E:\A\	Unknown
● [000015].png	E:\A\	Unknown
● [000016].png	E:\A\	Unknown
● [000017].png	E:\A\	Unknown
● [000018].png	E:\A\	Unknown
● [000019].png	E:\A\	Unknown
● [000020].png	E:\A\	Unknown
● [000021].png	E:\A\	Unknown
● [000022].png	E:\A\	Unknown
● [000023].png	E:\A\	Unknown
● [000024].png	E:\A\	Unknown

COMPARATIVA



oooo

**Tiempo de
recuperación:**

27 minutos con 31
segundos

**IMAGEN
ENCONTRADA**



oooo

Pasos a seguir:

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

Devices (1)

This list shows the devices on which users installed the security application. [How to add devices](#)

Adding devices: [via link in email \(2:05\)](#) and [via Active Directory \(2:15\)](#)

Show devices: All (1) ! Critical (0) ! Warning (0) ! OK (1) ? No data yet (0)

	Assign owner		Rename		Delete		More...
<input type="checkbox"/>	Status	OS	Name	Device owner		Group name	
<input type="checkbox"/>	✓	Win	MSEDGEWIN10 Microsoft Windows 10	A01197699 A01197699@tec.mx			

MALWARE-TRAFFIC-ANALYSIS.NET

RSS feed About this blog @malware_traffic on Twitter

A source for packet capture (pcap) files and malware samples...

In the summer of 2013, this site has published over 2,000 blog entries about malicious network traffic. Almost every post on this site has pcap files or malware samples (or both).

Analysis Exercises

-- for training exercises to analyze pcap files of network traffic. [Click here](#) -- for some tutorials that will help for these exercises.

Technical Blog Posts

blog posts by year - [\[2013 \]](#) - [\[2014 \]](#) - [\[2015 \]](#) - [\[2016 \]](#) - [\[2017 \]](#) - [\[2018 \]](#) - [\[2019 \]](#) - [\[2020 \]](#) - [\[2021 \]](#) - [\[2022 \]](#)

Non-Technical Blog Posts

In December 2018 through December 2020 I occasionally posted information to Pastebin, so [click here](#) for posts from my Pastebin account.

Technical Blog Posts

-- for non-technical blog posts I've written about on topics related to information security (infosec).

Posts

Search to search



BÚSQUEDA EN SITIOS EXTERNOS

The screenshot shows a web browser window with multiple tabs open. The active tab displays search results for "exe + virus + windows". The results include links to various malicious software and carding forums. Some of the visible titles and URLs are:

- unlimited BTC !
<http://castlee5janmtc5h6jiorit7lzdhgfuy43po4oddgij3qpm52ljyljyyd.onion/listin>
- How to use socks5 on windows - Best Carding World
<http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/viewtopic.php?f=21&t=6065&sid=3deb49a6ad085fefdf4f791fe96827668>
- A AT (Remote Administrator Trojan) Generator for Windows/Linux systems written i...
<http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/viewtopic.php?f=47&p=19964&sid=3deb49a6ad085fefdf4f791fe96827668>
- 000.exe | (CR33PY PASTA VIRUS (VBS)) - Best Carding World
<http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/viewtopic.php?f=47&p=20682&sid=e311497f09139e3ee19954a9b20381d0>
- Windows 10 Professional, Windows 11 Professional - Best Carding World
<http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/viewtopic.php?f=49&p=22585&sid=f9bf89915844d150591eea7136b16b89>
- HOW TO GET WINRAR LIFETIME LICENSE KEY (WITHOUT CRACK/VIRUS) - Best Carding Wor...
<http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/viewtopic.php?f=50&p=20301&sid=leb015b32dd2f02af329a7fa856b3367>
- How To Create A Windows 11 UHQ Premium RDP For Free - Best Carding World
<http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/viewtopic.php?f=52&p=21873&sid=e1af32562220f586c264b887ddd492b5>

The screenshot shows a forum post titled "PlasmaHTTP | (VB MALWARE)" on the "Malware" board of the "Best Carding World" forum. The post was made by "Murka LeLe" on July 7, 2022, at 8:52 am. The post content discusses the malware and provides a download link. Below the post, there is a reply from "Murka LeLe" with the password "infected". The forum interface includes a search bar, quick links, and user profile information.

PlasmaHTTP | (VB MALWARE)
by Murka LeLe • Thu Jul 07, 2022 8:52 am
PlasmaHTTP steals passwords from chrome, cookies grabber, data grabber, etc...
CODE: SELECT ALL
<https://anonymouse.com/rfj1Adveyf/PlasmaHTTP.zip>

The password is : infected

Have a nice day !
- Murka LeLe



ARCHIVO UTILIZADO

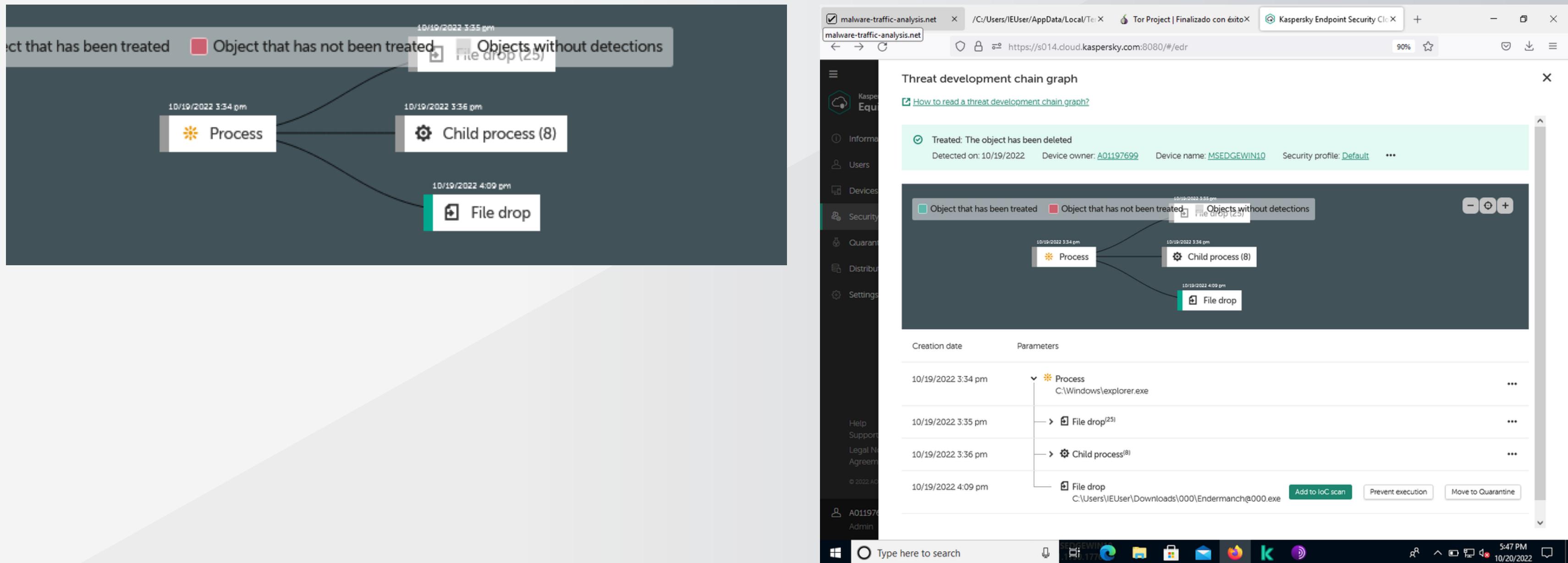
The screenshot shows a dark-themed web browser window. The address bar displays the URL https://anonfiles.com/rfj1Adveyf/PlasmaHTTP_zip. The main content is the AnonFiles landing page, featuring a logo of a person in a suit holding a briefcase. A yellow call-to-action box contains the text "We need your help!" with a link to "Read more here." Below it, a note says "UPDATE: You can now securely donate with your credit card!". A large button labeled "DESCARGAR (557.63 KB)" is prominently displayed. To the right, there's a section titled "Donations:" with Bitcoin and Monero QR codes. At the bottom, links for "Iniciar sesión - Registrarse - Términos de Uso - API - FAQ - Evaluación/Opinión/Comentarios - REPORTAR ABUSO" are visible.

The screenshot shows a Windows File Explorer window with a dark theme. The address bar shows the path https://anonfiles.com/rfj1Adveyf/PlasmaHTTP_zip. The main area displays the contents of the "PlasmaHTTP.zip" archive, which includes several folders and files. A table provides details about the items:

Name	Date modified	Type	Size
Bot	10/20/2022 3:28 PM	File folder	
Bot.sln	10/20/2022 3:28 PM	SLN File	1 KB
InjectionLibrary.dll	10/20/2022 3:28 PM	Application extens...	42 KB

At the bottom of the File Explorer window, links for "Iniciar sesión - Registrarse - Términos de Uso - API - FAQ - Evaluación/Opinión/Comentarios - REPORTAR ABUSO" are visible. The taskbar at the bottom of the screen also shows the AnonFiles icon.

KASPERSKY GRÁFICO DE CADENA



KASPERSKY THREAT INTELLIGENCE PORTAL

The image displays two side-by-side screenshots of the Kaspersky Threat Intelligence Portal. Both screenshots show a 'Report' page for a specific file hash.

Left Screenshot (Report for hash f2b7074e1543720a9a98fda660e02688):

- Overview:**
 - Hits: ≈ 1,000
 - Format: exe x32
 - Size: 6.66 MB (6983680 B)
 - First seen: 2 Oct, 2016 02:14
 - Last seen: 18 Oct, 2022 03:37
 - Signed by: —
 - Packed by: —
- Detection names:**
 - 20 Jun, 2022 10:23: BSS.Trojan.Win32.Generic
 - 6 Oct, 2022 23:10: BSS.Worm.Win32.BSS.ScreenLock
 - 17 Jun, 2021 20:46: HEUR:Trojan.Win32.Agent.gen

Right Screenshot (Report for hash 4ea1f2ecf7eb12896f2cbf8683dae8546d2b8dc43cf7710d68ce99e127c0a966):

- Overview:**
 - Hits: ≈ 1,000
 - Format: exe x32
 - Size: 6.66 MB (6983680 B)
 - First seen: 2 Oct, 2016 02:14
 - Last seen: 18 Oct, 2022 03:37
 - Signed by: —
 - Packed by: —
- Detection names:**
 - 20 Jun, 2022 10:23: BSS.Trojan.Win32.Generic
 - 6 Oct, 2022 23:10: BSS.Worm.Win32.BSS.ScreenLock
 - 17 Jun, 2021 20:46: HEUR:Trojan.Win32.Agent.gen
 - 22 May, 2020 12:22: —
 - 2 Oct, 2016 05:13: —
 - 21 Aug, 2019 16:49: —

Both screenshots show a navigation bar at the top with tabs for Analysis, Requests, Premium Services, and About Portal. The bottom of each screenshot shows a taskbar with various application icons and system status indicators.

CONCLUSIONES

Mantener respaldos tanto físicos como digitales

Tener cuidado sobre dónde se conectan los dispositivos

Tomar medidas necesarias de protección ante amenazas y ataques

Mantener claros los objetivos del análisis forense, no desviarse