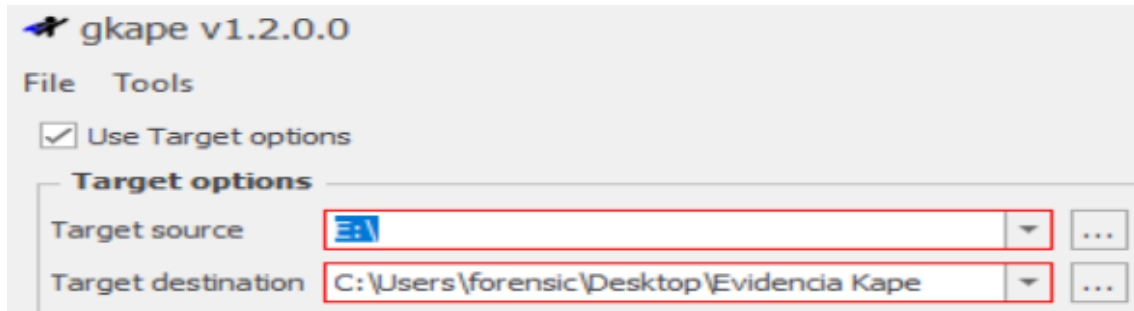




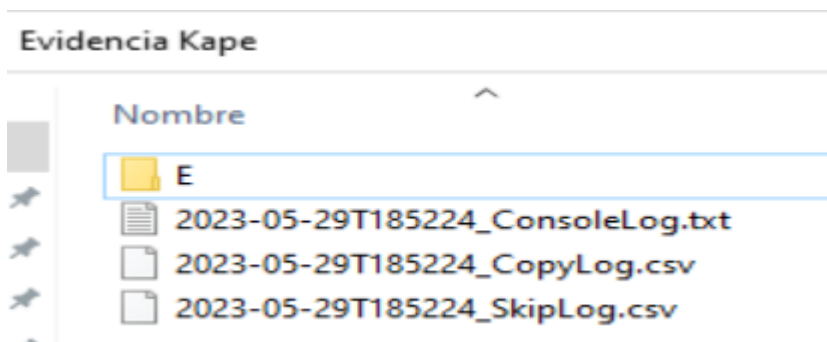
Digital Forensics and Incident Response

Práctica Windows

Obtención de evidencias con Kape:



Se genera el archivo en esta ruta. Nos genera varios archivos:



Análisis de unidad con Loki usando el siguiente comando:

```
C:\Herramientas\04_loki_0.44.2\loki>loki.exe -p E:\ --noprocsan --logfolder C:\Users\forensic\Desktop\Practica\Procesados\Loki
```

-p Indica el destino.

--noprocsan Se pide que no escanee procesos ya que es una máquina “muerta”.

--logfolder Indica la ruta de salida del procesado.

Se procede a parsear el evento Security (extraído previamente o Kape):

```
C:\Herramientas\02_ZimmermanTools\EvtxECmd>EvtxECmd.exe -f "C:\Users\forensic\Desktop\Evidencia_Kape\E\Windows\System32\winevt\logs\Security.evtx" --csv "C:\Users\forensic\Desktop\Practica\Procesados\Eventos" --csvf evento_security_parseado.csv
```

Para conseguir esto se usa la aplicación de Eric Zimmerman llamada EvtxECmd con la estructura siguiente:

-f “RUTA ABSOLUTA” Se especifica la ruta donde se ubica el archivo que se busca.

--csv “RUTA ABSOLUTA” Carpeta destino del parseado.

--csvf nombre.csv Indica el nombre que se va a asignar al archivo resultante.

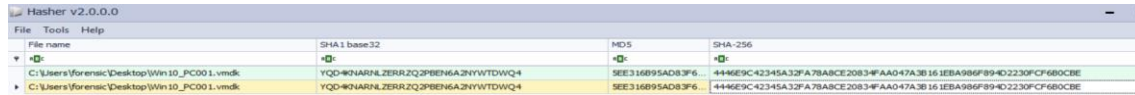
```
C:\Herramientas\chainsaw_allplatformrules&samples\chainsaw\chainsaw_x86_64-pc-windows-msvc.exe hunt C:\Users\forensic\Desktop\Evidencia_Kape\E\Windows\System32\winevt\logs -s sigma/ -r rules/mapping_mappings/sigma-event-logs-all.yml >> c:\Users\forensic\Desktop\Practica\chainsaw.txt
```

Aplicado Chainsaw para obtener más datos de los eventos.

Se especifica la ruta de sigma, rules y mappings y todas ellas están dentro de la propia carpeta donde se lanza el ejecutable.

Con estos procesos se puede afrontar los retos.

Hash:



File name	SHA-1 base32	MD5	SHA-256
C:\Users\forensic\Desktop\Win10_PC001.vmdk	YQD-WNARNLZERRZQ2PBEH6A2NYWTDWQ4	SEE316B95A0B3F6	4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE
C:\Users\forensic\Desktop\Win10_PC001.vmdk	YQD-WNARNLZERRZQ2PBEH6A2NYWTDWQ4	SEE316B95A0B3F6	4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE

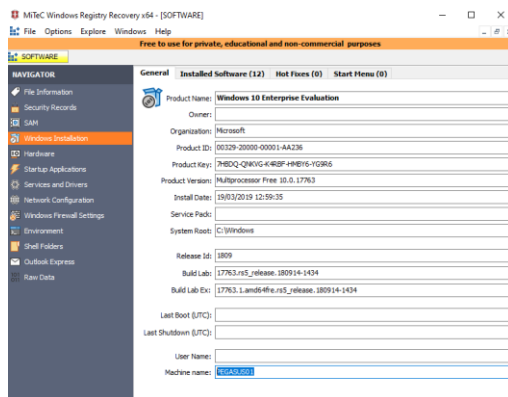
Usando la aplicación hasher se aplica sobre la imagen y tras un momento nos genera los hashes solicitados. En nuestro caso nos quedamos con el SHA-256 que tiene un valor

4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE.

Esto genera que el primer reto sea correcto:



Nombre de la máquina:



Usando el archivo Software obtenido de Kape y aplicado en la aplicación WRR.

La respuesta correcta es PEGASUS01.

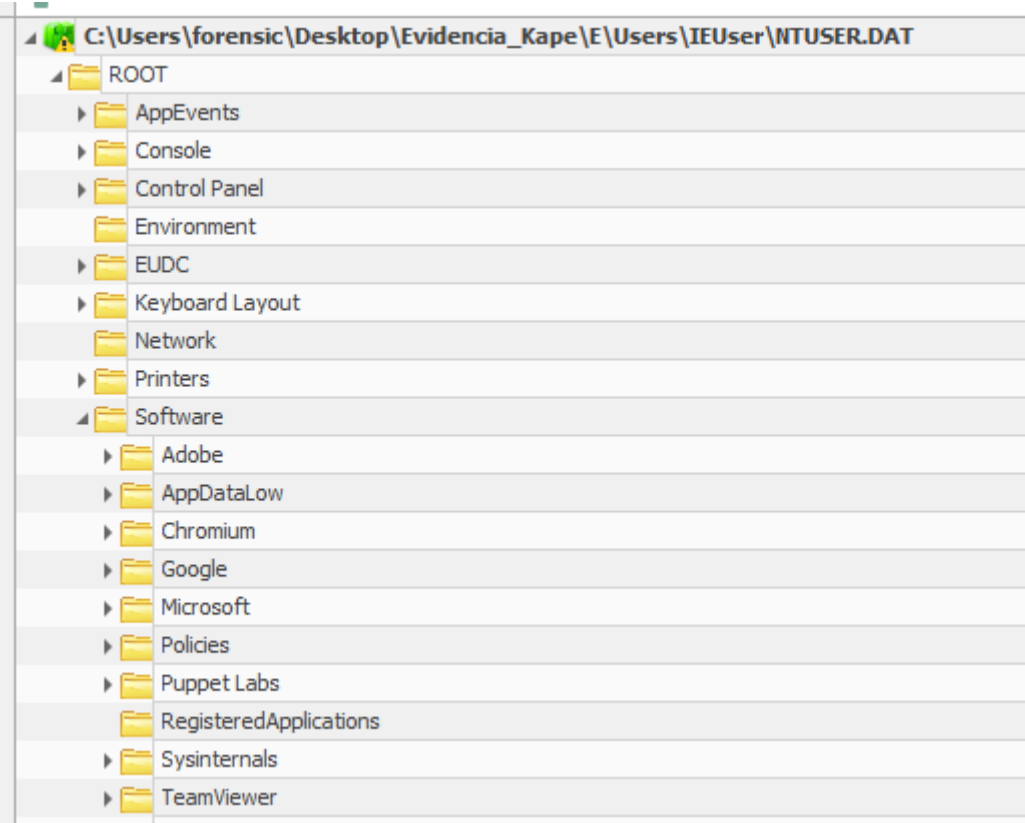
Ficheros maliciosos:

```
20230601T19:53:56Z WINFORENSIC10 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: E:\TMP\nbtscan.exe SCORE: 160
20230601T19:53:56Z WINFORENSIC10 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: E:\TMP\p.exe SCORE: 105 TYPE:
20230601T19:53:56Z WINFORENSIC10 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: E:\TMP\xCmd.exe SCORE: 60 T
IM\vr3\vr6IT\vh\vf2'
```

Analizando el fichero obtenido con Loki, se pueden ver algunas aplicaciones maliciosas ubicadas en la carpeta TMP.

Descarga del fichero control remoto:

Se puede observar accediendo al registro del usuario (Ntuser.dat) que existe una aplicación de control remoto llamada TeamViewer:



El nombre del fichero con extensión .exe que se descarga es: TeamViewer_Setup_x64.exe.

Ficheros eliminados:

evidenciapapelera.csv		
Introduzca texto a buscar		
	File Type	File Name
	REC	REC
321011808-37...	\$I	C:\Users\IEUser\Documents\02_AnejoII_EstrucyContTFG_a.pdf
321011808-37...	\$I	C:\Users\IEUser\AppData\Local\Temp\cosas.zip
321011808-37...	\$I	C:\Users\IEUser\Documents\CONFIDENTIAL document list.pdf
321011808-37...	\$I	C:\Users\IEUser\Documents\Documento Seguridad HipoSEMG.doc

Usando la aplicación RBCmd y la ruta de la papelera obtenida con Kape se pueden obtener estos archivos eliminados. En nuestro caso necesitamos el archivo zip para resolver el reto llamado cosas.zip.

Puerto de conexión máquina atacante:

evento_security_parsed.csv			
Arrastre una columna aquí para agrupar por dicha columna			
description	User Name	Remote Host	Payload Data1
tial Manager credentials were read	IEUser		SID: S-1-5-21-321011808-3761883066-353627080-1000
tial Manager credentials were read	IEUser		SID: S-1-5-21-321011808-3761883066-353627080-1000
n was attempted using explicit credentials	PEGASUS01\IEUser	192.168.183.134:445	Target: PEGASUS01\user1
n was attempted using explicit credentials	PEGASUS01\IEUser	192.168.183.134:445	Target: PEGASUS01\user1

Usando TimeLine Explorer y cargando el fichero parseado de eventos de seguridad se puede filtrar la ip obtenida (192.168.183.134) para conocer el puerto desde el que hacen la conexión que es el 445.

Fecha ejecución TeamViewer:

Sobre la captura mostrada en el apartado “Nombre del fichero de control remoto” se puede obtener la fecha en el registro:

▶ Sysinternals	0	2	2019-03-19 13:28:16
▶ TeamViewer	13	2	2022-04-29 10:30:10
▶ The Document Foundation	0	1	2022-04-29 08:33:16

La fecha con el formato requerido es -> 29/04/2022.

Powershell maliciosa:

AccessData FTK Imager 4.2.1.4			
File View Mode Help			
Evidence Tree			
Partition 1 [40958MB]	File List		
Windows 10 [NTFS]	Name	Size	Type Date Modified
[orphan]	\$I30	4	NTFS Index All... 08/05/2022 19:...
[root]	127.0.0.1.txt	1	Regular File 11/10/2014 3:0...
\$BadClus	d.txt	10	Regular File 11/10/2014 3:4...
\$Extend	nbtscan.exe	36	Regular File 04/02/2018 19:...
\$Recycle.Bin	p.exe	373	Regular File 27/04/2010 10:...
\$Secure	p.exe.FileSlack	4	File Slack
\$UpCase	scan1.tmp	0	Regular File 08/05/2022 19:...
BGinfo	scan2.tmp	0	Regular File 08/05/2022 19:...
Boot	scan3.tmp	0	Regular File 08/05/2022 19:...
Documents and Settings	sys.txt	8	Regular File 08/05/2022 19:...
inetpub	WMIBackdoor.ps1	20	Regular File 10/08/2015 13:...
PerfLogs	xCmd.exe	824	Regular File 29/07/2014 15:...
Program Files			
Program Files (x86)			
ProgramData			
Recovery			
System Volume Information			

Para llegar a la solución de este reto ha sido necesario montar la evidencia con FTK Imager y navegar hasta la carpeta TMP ubicada dentro de Partition 1 – Windows 10 – [root] – TMP. Al abrirla aparece un archivo llamado WMIBackdoor.ps1 que es requerido para completar el reto.

Contraseña débil:

Usando la aplicación Mimikatz y el siguiente comando obtenemos las contraseñas hasheadas:

```
mimikatz # lsadump::sam /system:C:\Users\forensic\Desktop\Evidencia_Kape\E\Windows\System32\config\SYSTEM /sam:C:\Users\forensic\Desktop\Evidencia_Kape\E\Windows\System32\config\SAM
```

En el comando hay que añadir la ruta del fichero SAM y SYSTEM, ambos obtenidos con Kape previamente y almacenados en la ruta E\Windows\System32\config\.

Al ejecutar el comando nos aparece toda la información de las contraseñas, para la evidencia es necesario buscar lo que se pide, el usuario IEUser

```
RID : 000003e8 (1000)
User : IEUser
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf
```

Su Hash es 2d20d252a479f485cdf5e171d93985bf.

Para decodificarla se ha usado la aplicación online [Crackstation](https://crackstation.net/) y el resultado es:



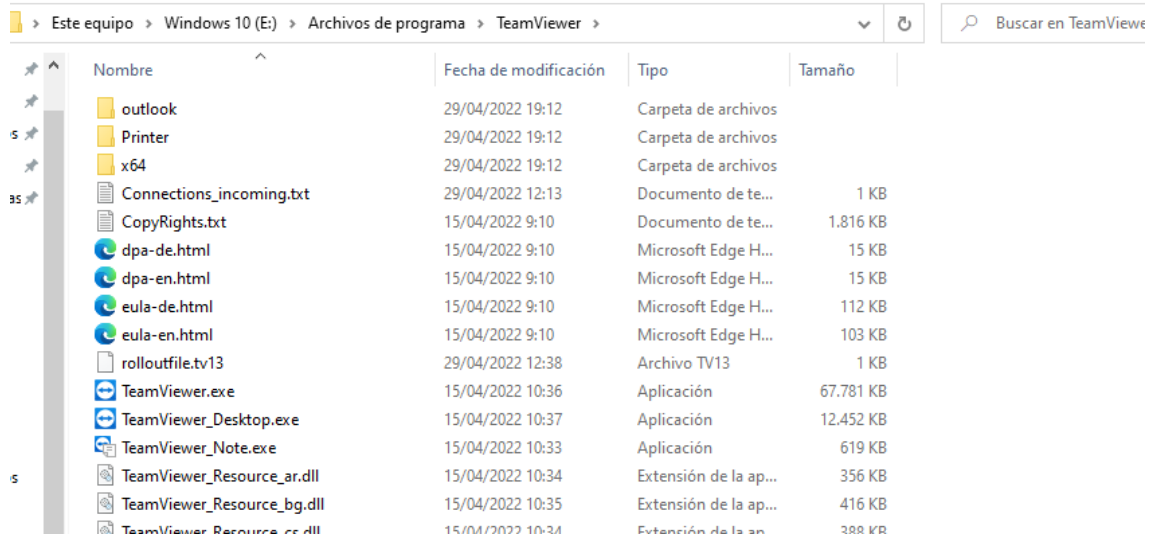
The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links like 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below this, there's a text input field containing the hash '2d20d252a479f485cdf5e171d93985bf'. To the right of the input field is a CAPTCHA challenge with the text 'No soy un robot' and a 'Crack Hashes' button. Below the input field, there's a list of supported hash types: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults. Below this, there's a table with three columns: 'Hash', 'Type', and 'Result'. The table contains one row with the hash '2d20d252a479f485cdf5e171d93985bf', the type 'NTLM', and the result 'qwerty'. At the bottom, there's a legend for color codes: Green for 'Exact match', Yellow for 'Partial match', and Red for 'Not found'.

Hash	Type	Result
2d20d252a479f485cdf5e171d93985bf	NTLM	qwerty

“qwerty”.

Conexión programa control remoto:

Para solucionar este reto ha sido necesario navegar un poco en el explorador de archivos. Dentro de la carpeta de TeamViewer (ubicada en E:\Program Files\TeamViewer\), hay un archivo llamado Connections_incoming.txt:



En dicho archivo figuran varios datos de las conexiones realizadas:

765418952	WIN-MORENIN	29-04-2022 10:09:14	29-04-2022 10:10:10	IEUser	RemoteControl	{adb13c9a-796c-438c-af8b-2079077f0a4f}
765418952	WIN-MORENIN	29-04-2022 10:10:34	29-04-2022 10:13:21	IEUser	RemoteControl	{301db382-67ac-4b5a-9bec-d1a44aa0ad30}

La ID con la que el atacante se conecta es: 765418952.

RDP:

+ Suspicious Rejected SMB Guest Logon From IP	1	Microsoft-Windows-SMBClient	31017	1	PEGASUS01	ServerName: \192.168.183.134 ServerNameLength: 16 UserName: '' UserNameLength: 0
---	---	-----------------------------	-------	---	-----------	---

Usando un bloc de notas para la información parseada con Chainsaw, podemos ver que hay una dirección IP persistente.

La ip desde la que proviene el ataque es 192.168.183.134.

Práctica RAM

Hay que descargar la aplicación WinpMem:

<https://github.com/Velocidex/WinPmem/releases>

En nuestro caso usamos esta versión porque nuestra CPU admite 64 bits.

Release 4.0 RC2 Latest

This release fixes an issue with the drivers loading on recent Windows versions.

For this release we make available the old "mini" pmem imager based on the old 1.6 branch. This imager is very simple - it can only make raw images. The AFF4 based imager may be back in the future but for now we can produce RAW images.


We started to distribute Winpmem releases directly from this project as it is now separated from the Rekall project (which has been discontinued).

The new drivers implement Fast IO mode so should be faster than before.

Thanks

We would like to thank Emre Tinaztepe and Mehmet GÖKSU at Binalyze as well as Viviane Zwanger for making this release possible.

Assets 4

 winpmem_mini_x64_rc2.exe	515 KB	Oct 13, 2020
--	--------	--------------

Es necesario usar la consola de comandos (ejecutando como administrador).

El comando que he seguido es el siguiente:

```
c:\Herramientas>winpmem_mini_x64_rc2.exe c:\Herramientas\memoria_local_adquisition.mem
```

Winpmem_mini_x64_rc2.exe c:\Herramientas\memoria_local_adquisition.mem. La primera parte invoca a la aplicación y la segunda parte es la ruta absoluta donde se va a almacenar el archivo obtenido.

Aquí se puede apreciar el resultado:

```
c:\Herramientas>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5860-5AF5

Directorio de c:\Herramientas

28/05/2023  20:52    <DIR>          .
28/05/2023  20:52    <DIR>          ..
06/05/2022  12:10    <DIR>          01_Artefactos
25/04/2023  16:49    <DIR>          02_ZimmermanTools
27/04/2022  14:36    <DIR>          03_kape
05/05/2022  20:12    <DIR>          04_loki_0.44.2
27/04/2022  12:34    <DIR>          Arsenal-Image-Mounter-v3.3.138
04/05/2022  20:03             5.440.291 LogFileParser-master.zip
05/05/2022  20:12             22.073.249 loki_0.44.2.zip
28/05/2023  20:52             4.779.409.408 memoria_local_adquisition.mem
27/04/2022  14:26    <DIR>          SysinternalsSuite
28/05/2023  20:40             527.640 winpmem_mini_x64_rc2.exe
               4 archivos  4.807.450.588 bytes
               8 dirs  136.047.276.032 bytes libres
```

Usando Volatility:

Es necesario tener instalado el plugin para poder ejecutar la aplicación Volatility, el método usado para este caso ha sido escribir Python en el terminal de Windows y re dirige a la tienda de Windows donde nos permite instalarlo.

Salvando este paso procedemos a ejecutar comandos con la aplicación para poder ver contenido en la RAM y comprender mejor su uso:

```
C:\Herramientas\01_Artefactos\RAM\volatility3-1.0.0\volatility3-1.0.0>vol.py -f C:\Users\forensic\Desktop\Practica\RAM\memoria_local_adquisition.mem windows.pslist >> c:\Users\forensic\Desktop\pslist.txt
Progress: 93.02 Scanning memory_layer using BytesScanner
```

Con este comando nos genera una lista de archivos almacenados.

```
C:\Herramientas\01_Artefactos\RAM\volatility3-1.0.0\volatility3-1.0.0>vol.py -f C:\Users\forensic\Desktop\Practica\RAM\memoria_local_adquisition.mem windows.psscan >> c:\Users\forensic\Desktop\psscan.csv
Progress: 100.00 PDB scanning finished
```

Psscan hace un escaneo de procesos y los muestra en el archivo indicado.

```
C:\Herramientas\01_Artefactos\RAM\volatility3-1.0.0\volatility3-1.0.0>vol.py -f C:\Users\forensic\Desktop\Practica\RAM\memoria_local_adquisition.mem windows.filescan >> c:\Users\forensic\Desktop\filescan.csv
Progress: 100.00 PDB scanning finished
```

Se lanza filescan para detectar posibles archivos malicioso.

Metadatos

Para esta práctica nos basamos en la siguiente imagen de un ratón:



```
File Name           : Original.jpg
Directory           : C:/Users/forensic/Desktop/Practica/Metadatos
File Size           : 1788 kB
File Modification Date/Time : 2023:06:04 19:21:24+02:00
File Access Date/Time   : 2023:06:05 17:38:09+02:00
File Creation Date/Time  : 2023:06:04 19:21:24+02:00
File Permissions      : -rw-rw-rw-
File Type           : JPEG
File Type Extension   : jpg
MIME Type           : image/jpeg
Exif Byte Order      : Little-endian (Intel, II)
Make                : Google
Camera Model Name    : Pixel 7 Pro
Orientation         : Horizontal (normal)
X Resolution        : 72
Y Resolution        : 72
Resolution Unit      : inches
Software            : HDR+ 1.0.529100733zd
Modify Date         : 2023:06:04 19:17:30
Y Cb Cr Positioning  : Centered
Exposure Time       : 1/41
F Number           : 1.9
```

Se aprecian datos específicos del terminal con el que fue tomada la imagen, así como datos específicos propios de la imagen tales como tiempo de exposición y diafragma.

WhatsApp:

```
File Name           : WhatsApp.jpg
Directory           : C:/Users/forensic/Desktop/Practica/Metadatos
File Size           : 173 kB
File Modification Date/Time : 2023:06:04 19:37:23+02:00
File Access Date/Time   : 2023:06:05 17:40:58+02:00
File Creation Date/Time  : 2023:06:04 19:37:23+02:00
File Permissions      : -rw-rw-rw-
File Type           : JPEG
File Type Extension   : jpg
MIME Type           : image/jpeg
JFIF Version         : 1.01
Resolution Unit      : inches
X Resolution        : 96
Y Resolution        : 96
Image Width         : 900
Image Height        : 1600
Encoding Process     : Baseline DCT, Huffman coding
Bits Per Sample     : 8
Color Components     : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size          : 900x1600
Megapixels          : 1.4
```

Esta es toda la información que muestra, se puede apreciar que en WhatsApp la imagen ha sido redimensionada y aplicado un proceso de compresión.

Telegram:

```
ExifTool Version Number      : 12.62
File Name                    : Telegram.jpg
Directory                   : C:/Users/forensic/Desktop/Practica/Metadatos
File Size                   : 158 kB
File Modification Date/Time  : 2023:06:05 17:40:21+02:00
File Access Date/Time       : 2023:06:05 17:46:26+02:00
File Creation Date/Time     : 2023:06:05 17:40:21+02:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : inches
X Resolution                : 96
Y Resolution                : 96
Profile CMM Type            :
Profile Version             : 2.4.0
Profile Class               : Display Device Profile
Color Space Data            : RGB
Profile Connection Space    : XYZ
Profile Date Time           : 0000:00:00 00:00:00
Profile File Signature      : acsp
Primary Platform            : Unknown ()
CMM Flags                   : Not Embedded, Independent
Device Manufacturer        :
Device Model               :
Device Attributes           : Reflective, Glossy, Positive, Color
Rendering Intent            : Media-Relative Colorimetric
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator             : Unknown (Qt..)
```

Aunque Telegram también comprime la imagen, muestra más información. Dicha información no tiene mucha relación con la original, su sistema de procesado – compresión es más rico a la hora de analizar metadatos.

Email:

```
ExifTool Version Number      : 12.62
File Name                    : Email.jpg
Directory                   : C:/Users/forensic/Desktop/Practica/Metadatos
File Size                   : 1788 kB
File Modification Date/Time  : 2023:06:05 17:43:44+02:00
File Access Date/Time       : 2023:06:05 17:44:03+02:00
File Creation Date/Time     : 2023:06:05 17:43:44+02:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order             : Little-endian (Intel, II)
Make                       : Google
Camera Model Name           : Pixel 7 Pro
Orientation                 : Horizontal (normal)
X Resolution                : 72
Y Resolution                : 72
Resolution Unit             : inches
Software                    : HDR+ 1.0.529100733zd
Modify Date                 : 2023:06:04 19:17:30
Y Cb Cr Positioning        : Centered
Exposure Time               : 1/41
F Number                   : 1.9
Exposure Program            : Program AE
ISO                        : 450
Exif Version               : 0232
Date/Time Original          : 2023:06:04 19:17:30
Create Date                 : 2023:06:04 19:17:30
Offset Time                 : +02:00
Offset Time Original        : +02:00
Offset Time Digitized       : +02:00
Components Configuration    : Y, Cb, Cr, -
Shutter Speed Value         : 1/41
Aperture Value              : 1.9
```

En este caso ha enviado la imagen tal cual es la original, teniendo en cuenta la capacidad en MB de la imagen no nos preguntó el gestor de correo la calidad de envío de la misma.

Discord:

```
ExifTool Version Number      : 12.62
File Name                    : Discord.jpg
Directory                   : C:/Users/forensic/Desktop/Practica/Metadatos
File Size                   : 1733 kB
File Modification Date/Time  : 2023:06:05 17:46:16+02:00
File Access Date/Time       : 2023:06:05 17:46:26+02:00
File Creation Date/Time     : 2023:06:05 17:46:16+02:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Orientation                 : Horizontal (normal)
XMP Toolkit                  : Adobe XMP Core 5.1.0-jc003
Has Extended XMP             : E205DD329496A266D937305042A44D71
JFIF Version                 : 1.02
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
Profile CMM Type             :
Profile Version               : 4.0.0
Profile Class                 : Display Device Profile
Color Space Data             : RGB
```

El tamaño de la imagen es muy similar al de la original, salvo que Discord tiene su propio método de gestionar el intercambio de contenido multimedia.