

PRACTICA DFIR- win10

En la máquina tsurugi, adquisición de la imagen con **guymager**.

Acquire image of /dev/sdb (as superuser)

File format

☐ Linux dd raw image (file extension .dd or .xxx)

☒ Expert Witness Format, sub-format Guymager (file extension .Exx)

☒ Split image files

Split size: 2047 MiB

Case number: Practica Final

Evidence number: dm001

Examiner: Adrian Armesto

Description: Disco Practica Final

Notes:

Destination

Image directory: /home/tsurugi/Evidencias/

Image filename (without extension): dm002

Info filename (without extension): dm002

Hash calculation / verification

☒ Calculate MD5 ☐ Calculate SHA-1 ☐ Calculate SHA-256

☐ Re-read source after acquisition for verification (takes twice as long)

☒ Verify image after acquisition (takes twice as long)

Cancel Duplicate image... Start

Información del software y máquina utilizados.

```
Guymager
=====
Version                : 0.8.13-beta-tsurugi-1
Version timestamp      : 2021-08-27-21.46.29 UTC
Compiled with          : gcc 9.3.0
Using Guymager's own EWF module
libguytools version    : 2.1.0
Host name              : lab
Domain name            : (none)
System                 : Linux lab 5.15.12-tsurugi #1 SMP Thu Dec 30 17:06:21 CET 2021 x86_64
```

Información del disco.

```
=== START OF INFORMATION SECTION ===
Vendor: VMware,
Product: VMware Virtual S
Revision: 1.0
User Capacity: 42,949,672,960 bytes [42.9 GB]
Logical block size: 512 bytes
Rotation Rate: Solid State Device
Device type: disk
Local Time is: Wed May 18 16:22:41 2022 EDT
SMART support is: Unavailable - device lacks SMART capability.
```

Hash del disco e imagen.

```

Acquisition
=====

Linux device      : /dev/sdb
Device size      : 42949672960 (42.9GB)
Format           : Expert Witness Format, sub-format Guymager - file extension is .Exx
Image meta data
  Case number     : Practica Final
  Evidence number : dm001
  Examiner       : Adrian Armesto
  Description     : Disco practica final
  Notes          :
Image path and file name: /home/tsurugi/Evidencias/dm002.Exx
Info path and file name: /home/tsurugi/Evidencias/dm002.info
Hash calculation  : MD5 and SHA-1
Source verification : off
Image verification : on

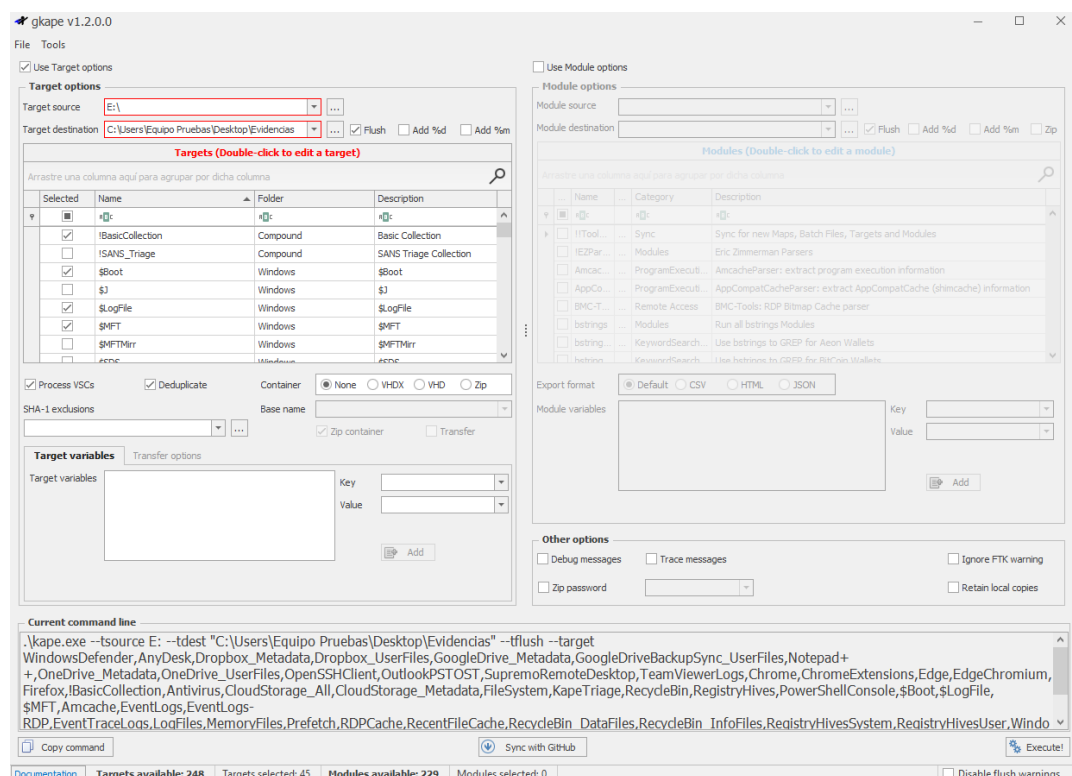
No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash          : 0ad2b998a5dcfb825d01e29b64a46121
MD5 hash verified source : --
MD5 hash verified image : 0ad2b998a5dcfb825d01e29b64a46121
SHA1 hash         : ab7f6987e2f3e7fd800901dc12eba53784e498d6
SHA1 hash verified source : --
SHA1 hash verified image : ab7f6987e2f3e7fd800901dc12eba53784e498d6
SHA256 hash       : --
SHA256 hash verified source : --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.

Acquisition started : 2022-05-18 16:22:41 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2022-05-18 16:25:25
Ended               : 2022-05-18 16:28:23 (0 hours, 5 minutes and 42 seconds)
Acquisition speed   : 249.76 MByte/s (0 hours, 2 minutes and 44 seconds)
Verification speed   : 230.11 MByte/s (0 hours, 2 minutes and 58 seconds)

```

En una maquina Windows 10, se ha montado la imagen en **Arsenal Image Mounter**, actos eguido se ha utilizado **Kape** para la adquisición de artefactos.



Comandos utilizados:

```

.\kape.exe --tsource E: --tdest "C:\Users\Equipo Pruebas\Desktop\Evidencias" --tflush --target
WindowsDefender,AnyDesk,Dropbox_Metadatas,Dropbox_UserFiles,GoogleDrive_Metadatas,GoogleDriveBackupSync_UserFiles,Notepad++

```


,OneDrive_Metadata,OneDrive_UserFiles,OpenSSHClient,OutlookPSTOST,SupremoRemoteDesktop,TeamViewerLogs,Chrome,ChromeExtensions,Edge,EdgeChromium,Firefox,!BasicCollection,Antivirus,CloudStorage_All,CloudStorage_Metadata,FileSystem,KapeTriage,RecycleBin,RegistryHives,PowerShellConsole,\$Boot,\$LogFile,\$MFT,Amcache,EventLogs,EventLogs-RDP,EventTraceLogs,LogFiles,MemoryFiles,Prefetch,RDPCache,RecentFileCache,RecycleBin_DataFiles,RecycleBin_InfoFiles,RegistryHivesSystem,RegistryHivesUser,WindowsFirewall,WindowsTimeline --vss -gui

Por medio de **WRR (MiTeC Windows Registry Recovery)** se procede a analizar los archivos obtenidos.













Analizando SYSTEM, ubicado en *\Windows\System32\config, se consigue información acerca de la máquina. Nombres, ultima vez encendida y apagada, así como el hardware.

Build Lab:	17763.rs5_release.180914-1434
Build Lab Ex:	17763.1.amd64fre.rs5_release.180914-1434
Last Boot (UTC):	29/04/2022 11:45:38
Last Shutdown (UTC):	29/04/2022 10:30:16
User Name:	
Machine name:	PEGASUS01
CPU:	Intel Core i7-7700HQ 2.80GHz
Monitor:	
Graphics:	VMware SVGA 3D
Sound:	
Network:	Intel(R) PRO/1000 MT Network Connection
Product:	VMware, Inc. VMware Virtual Platform
BIOS:	Phoenix Technologies LTD 6.00 (07/22/2020)

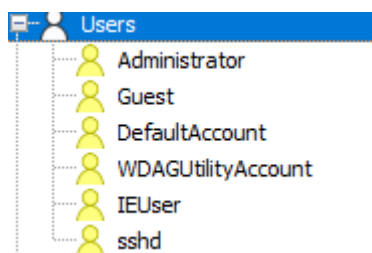
Analizando SOFRWARE se puede sacar información de programas instalados y datos del sistema operativo.



Product Name:	Windows 10 Enterprise Evaluation
Owner:	
Organization:	Microsoft
Product ID:	00329-20000-00001-AA236
Product Key:	7HBDQ-QNKVG-K4RBF-HMBY6-YG9R6
Product Version:	Multiprocessor Free 10.0.17763
Install Date:	19/03/2019 12:59:35
Service Pack:	
System Root:	C:\Windows
Release Id:	1809
Build Lab:	17763.rs5_release.180914-1434
Build Lab Ex:	17763.1.amd64fre.rs5_release.180914-1434
Last Boot (UTC):	
Last Shutdown (UTC):	
User Name:	
Machine name:	PEGASUS01

	Adobe Acrobat DC (64-bit)	22.001.2...	Adobe	20220429
	Google Chrome	101.0.49...	Google LLC	20220429
	Google Drive	57.0.5.0	Google LLC	
	LibreOffice 7.3.2.2	7.3.2.2	The Document ...	20220429
	Microsoft Silverlight	5.1.50918.0	Microsoft Corp...	20190319
	Microsoft Visual C++ 2008 Redistributable - x64 9.0....	9.0.3072...	Microsoft Corp...	20190319
	Microsoft Visual C++ 2008 Redistributable - x86 9.0....	9.0.3072...	Microsoft Corp...	20190319
	Microsoft Visual C++ 2015-2019 Redistributable (x64...	14.24.28...	Microsoft Corp...	
	Microsoft Visual C++ 2015-2019 Redistributable (x86...	14.24.28...	Microsoft Corp...	
	Puppet (64-bit)	3.8.7	Puppet Labs	20190319
	TeamViewer	15.29.4	TeamViewer	
	VMware Tools	11.1.5.16...	VMware, Inc.	20220429

Analizando SAM, se obtienen los usuarios.



Por medio de **Mft2Csv** se convierte el archivo MFT y **LogFileParser** para el LogFile, para posteriormente una mejor exploración.

Mft2Csv 2.0.0.43

Scan Physical Scan Shadows Rescan Mounted Drives <-- Test it

Set decoded timestamps to specific region: UTC: 0.00 ☐ Skip Fixups

Set output format: ☐ log2timeline ☐ Broken \$MFT ☐ bodyfile ☐ Scan slack ☒ dump everything Extract resident: ☐ Slack ☐ Data

Set separator: ☐ 0x7C ☐ Quotation mark ☐ Unicode ☐ split csv

Timestamp format: 6 Precision: NanoSec Timestamp ErrorVal: 0000-00-00 00:00:00

Precision separator: . Precision separator2: 2012-08-07 17:41:16.4389560

Decoding \$MFT
NTFS drives detected
Selected \$MFT file: C:\Users\Equipo Pruebas\Desktop\Evidencias\E\\$.MFT

Choose Image
Choose \$MFT
Set Output Path
Start Processing

\$LogFile: C:\Users\Equipo Pruebas\Desktop\Evidencias\E\\$.LogFile Select \$LogFile

Fragment: Broken transaction fragment (optional) Select fragment

MFT: Output of latest mft2csv (optional) Get MFT csv

Timestamp format: 6 Precision: NanoSec ☐ split csv Precision separator: .

Set decoded timestamps to specific region: UTC: 0.00 Precision separator2: ☐ skip sqlite3

Timestamp ErrorVal: 0000-00-00 00:00:00 2012-08-07 17:41:16.4389560 ☐ Skip Fixups

Set separator: ☐ 0x7C ☐ Unicode ☐ Reconstruct data runs ☐ Rebuild headers (in slack) ☐ Broken \$LogFile

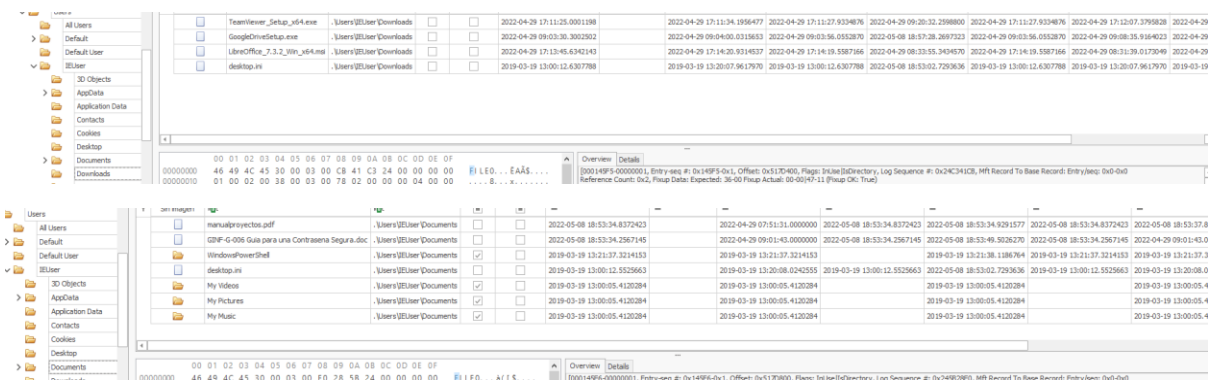
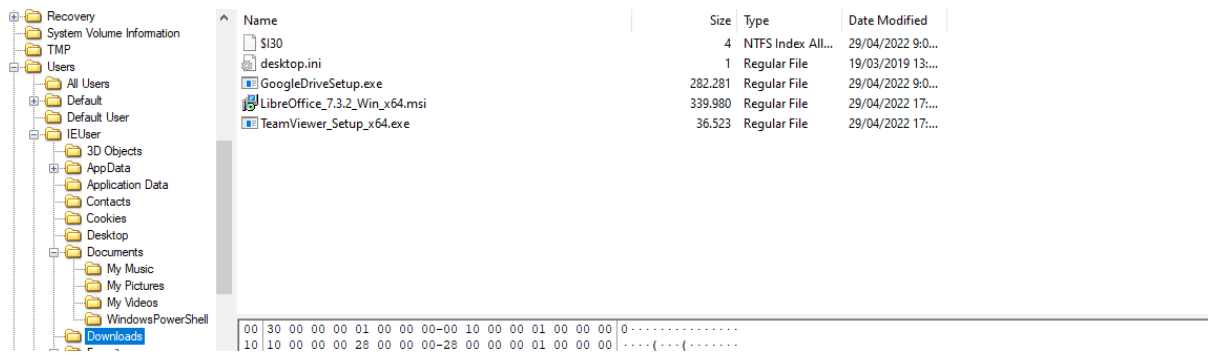
Sectors per cluster: 8 MFT record size: 1024 LSN error level: 0.1 10 % (up/down)

☐ Source is from 32-bit OS ☐ Extract non + resident updates of min size: 2

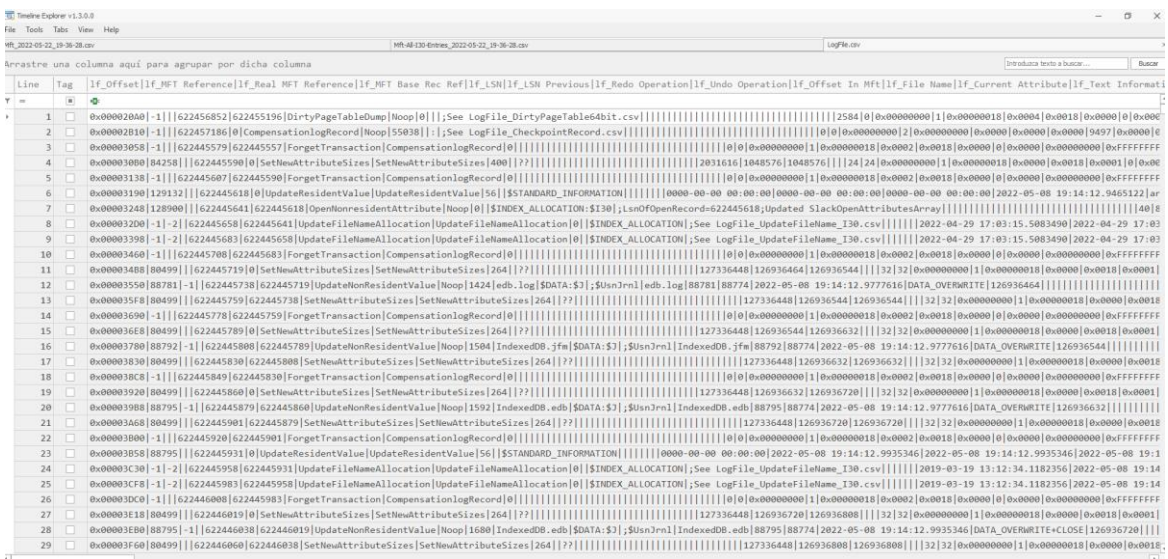
LSN's to trigger verbose output (comma separate): Start Exit

Por medio de **MFT Explorer** y **FTK Imager**, se pueden observar archivos descargados, accedidos o modificados.

System Volume Information	name	size	type	Date modified
Users	My Music	1	Reparse Point	19/03/2019 13:...
Users	My Pictures	1	Reparse Point	19/03/2019 13:...
Users	My Videos	1	Reparse Point	19/03/2019 13:...
Users	WindowsPowerShell	1	Directory	19/03/2019 13:...
Users	\$I30	4	NTFS Index All...	08/05/2022 18:...
Users	desktop.ini	1	Regular File	19/03/2019 13:...
Users	GINF-G-006 Guia para una Contraseña Segura.doc	234	Regular File	29/04/2022 9:0...
Users	GINF-G-006 Guia para una Contraseña Segura.doc.FileSlack	2	File Slack	
Users	manualproyectos.pdf	3,531	Regular File	29/04/2022 7:5...
Users	manualproyectos.pdf.FileSlack	2	File Slack	



He estado investigando con **TimeLine Explorer** los diferentes archivos csv conseguidos anteriormente. Pero aun no los controlo muy bien y tampoco se muy bien como seguir buscando mas datos. Me pareció ver una conexión externa a otro equipo con otro nombre, pero he sido capaz de encontrarlo otra vez.



Me interesa seguir aprendiendo sobre esto, a ver si me puedes aconsejar un poco sobre que he hecho mal y si faltaba por sacar más archivos para explorar mejor.

METADATOS

La foto ha sido enviada por email, whatsapp, discord y Messenger de Facebook. Se puede observar que por medio de email(Outlook) no se modifican los metadatos, mientras que las otras plataformas eliminan la información acerca del software y el dispositivo utilizados.

Metadatos de la original.


```
ExifTool Version Number      : 12.41
File Name                    : 20210109_170310.jpg
Directory                    : .
File Size                    : 1908 KiB
File Modification Date/Time   : 2021:01:09 11:03:11-05:00
File Access Date/Time        : 2022:05:22 18:29:29-04:00
File Inode Change Date/Time   : 2022:05:22 18:29:22-04:00
File Permissions              : -rwxrw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Little-endian (Intel, II)
Make                         : samsung
Camera Model Name             : SM-G975F
Orientation                   : Horizontal (normal)
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Software                      : G975FXXU9DTJA
Modify Date                   : 2021:01:09 17:03:10
Y Cb Cr Positioning           : Centered
Exposure Time                 : 1/672
F Number                      : 2.4
Exposure Program              : Program AE
ISO                           : 50
Exif Version                  : 0220
Date/Time Original            : 2021:01:09 17:03:10
Create Date                   : 2021:01:09 17:03:10
Shutter Speed Value           : 1
Aperture Value                : 2.4
Brightness Value              : 19.71
Exposure Compensation         : 0
Max Aperture Value            : 2.4
Metering Mode                 : Center-weighted average
Flash                         : No Flash
Focal Length                  : 4.3 mm
Color Space                   : sRGB
Exif Image Width              : 4032
Exif Image Height             : 3024
Exposure Mode                 : Auto
White Balance                  : Auto
Digital Zoom Ratio            : 1
Focal Length In 35mm Format   : 26 mm
Scene Capture Type            : Standard
Image Unique ID               : L12XLLD00SM
Compression                   : JPEG (old-style)
Thumbnail Offset              : 774
Thumbnail Length              : 16677
```

Metadatos email(Outlook).


```
ExifTool Version Number      : 12.41
File Name                    : 20210109_170310_mail.jpg
Directory                   : .
File Size                    : 1908 KiB
File Modification Date/Time   : 2022:05:22 18:35:01-04:00
File Access Date/Time        : 2022:05:22 18:40:05-04:00
File Inode Change Date/Time   : 2022:05:22 18:40:05-04:00
File Permissions              : -rwxrw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Little-endian (Intel, II)
Make                         : samsung
Camera Model Name             : SM-G975F
Orientation                  : Horizontal (normal)
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Software                      : G975FXXU9DTJA
Modify Date                   : 2021:01:09 17:03:10
Y Cb Cr Positioning           : Centered
Exposure Time                 : 1/672
F Number                      : 2.4
Exposure Program              : Program AE
ISO                           : 50
Exif Version                  : 0220
Date/Time Original            : 2021:01:09 17:03:10
Create Date                   : 2021:01:09 17:03:10
Shutter Speed Value           : 1
Aperture Value                 : 2.4
Brightness Value              : 19.71
Exposure Compensation         : 0
Max Aperture Value            : 2.4
Metering Mode                 : Center-weighted average
Flash                         : No Flash
Focal Length                  : 4.3 mm
Color Space                   : sRGB
Exif Image Width              : 4032
Exif Image Height             : 3024
Exposure Mode                 : Auto
White Balance                  : Auto
Digital Zoom Ratio            : 1
Focal Length In 35mm Format   : 26 mm
Scene Capture Type            : Standard
Image Unique ID               : L12XLLD00SM
Compression                   : JPEG (old-style)
Thumbnail Offset              : 774
Thumbnail Length              : 16677
Image Width                   : 4032
Image Height                   : 3024
```

Metadatos Whatsapp.

```
└─$ exiftool IMG-20210109-WA0071.jpg
ExifTool Version Number      : 12.41
File Name                    : IMG-20210109-WA0071.jpg
Directory                    : .
File Size                    : 96 KiB
File Modification Date/Time   : 2022:05:22 18:25:59-04:00
File Access Date/Time        : 2022:05:22 18:29:29-04:00
File Inode Change Date/Time   : 2022:05:22 18:29:22-04:00
File Permissions              : -rwxrw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                   : 2016
Image Height                  : 1512
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 2016x1512
Megapixels                   : 3.0
```

Metadatos Facebook Messenger.

```
└─$ exiftool received_427478492076009.jpeg
ExifTool Version Number      : 12.41
File Name                    : received_427478492076009.jpeg
Directory                    : .
File Size                    : 61 KiB
File Modification Date/Time   : 2022:05:22 17:56:31-04:00
File Access Date/Time        : 2022:05:22 18:29:29-04:00
File Inode Change Date/Time   : 2022:05:22 18:29:22-04:00
File Permissions              : -rwxrw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
Current IPTC Digest           : 04858a8d49dbc03dccbcd9c4b762d76a
Special Instructions          : FBMD0f000755010000c03a0000a66a00002a6c00003
06e000087a80000d3e70000f4f20000
Image Width                   : 2016
Image Height                  : 1512
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 2016x1512
Megapixels                   : 3.0
```

Metadatos Discord.

```
└─$ exiftool Discord
ExifTool Version Number      : 12.41
File Name                    : Discord
Directory                    : .
File Size                    : 1891 KiB
File Modification Date/Time   : 2022:05:22 18:29:10-04:00
File Access Date/Time        : 2022:05:22 18:29:29-04:00
File Inode Change Date/Time   : 2022:05:22 18:29:22-04:00
File Permissions              : -rwxrw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Big-endian (Motorola, MM)
Orientation                   : Horizontal (normal)
Image Width                   : 4032
Image Height                  : 3024
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Time Stamp                    : 2021:01:09 11:03:10-05:00
MCC Data                     : 214
Image Size                   : 4032x3024
Megapixels                   : 12.2
```