

Informe Final Pericial – MCS520 Informática Forense																				
Investigador/a: Ángel Peña	ID Investigador/a: 1094214																			
ID caso: DO-IF-A000	Fecha, hora: 23/04/2021 19:28 AST																			
<p><b>Descripción:</b></p> <p>Este documento describe paso a paso la realización de las prácticas de la asignatura “<b>MCS520 – informática Forense</b>” basado en el contexto de un informe pericial de cómputo forense.</p> <p>El levantamiento de información indica que el 17 de marzo del año 2021 el Sr. Ángel Peña (Ing. En Sistemas de Computación) realizó el procedimiento de captura de los datos pertinentes al activo de información listado en la siguiente tabla:</p> <table border="1"> <tbody> <tr> <td>Nombre PC:</td> <td>RESISTANCEB</td> </tr> <tr> <td>Usuario PC:</td> <td>VPN_user</td> </tr> <tr> <td>Dirección IPv4</td> <td>169.254.11.13</td> </tr> <tr> <td>Dirección MAC:</td> <td>08-00-27-9E-3F-E2</td> </tr> <tr> <td>Sistema Operativo, versión, arquitectura:</td> <td>MS Windows 10 LTSC, 1809, 64-bits</td> </tr> <tr> <td>Memoria RAM</td> <td>3048 MB</td> </tr> <tr> <td>Cantidad y capacidad disco duro:</td> <td>1 disco, 50 GB SATA III 5400 rpm</td> </tr> <tr> <td>Procesador, generación, velocidad Hz</td> <td>Intel Core i7, 8750H, 2.20GHz</td> </tr> </tbody> </table> <p><b>Detalle del evento:</b></p> <p>Para la realización de la <u>practica 1</u>: Se realizó búsqueda de un aplicativo web el cual genere tarjetas de crédito ficticias. En las siguientes capturas se muestra el paso a paso de esta actividad.</p> <table border="1"> <tbody> <tr> <td><b>Título:</b> Practica #1</td> </tr> <tr> <td><b>Objetivo:</b> Identificar el origen de un BIN</td> </tr> </tbody> </table> <table border="1"> <tbody> <tr> <td>Ingreso de datos ficticios requeridos por el aplicativo:</td> </tr> </tbody> </table>		Nombre PC:	RESISTANCEB	Usuario PC:	VPN_user	Dirección IPv4	169.254.11.13	Dirección MAC:	08-00-27-9E-3F-E2	Sistema Operativo, versión, arquitectura:	MS Windows 10 LTSC, 1809, 64-bits	Memoria RAM	3048 MB	Cantidad y capacidad disco duro:	1 disco, 50 GB SATA III 5400 rpm	Procesador, generación, velocidad Hz	Intel Core i7, 8750H, 2.20GHz	<b>Título:</b> Practica #1	<b>Objetivo:</b> Identificar el origen de un BIN	Ingreso de datos ficticios requeridos por el aplicativo:
Nombre PC:	RESISTANCEB																			
Usuario PC:	VPN_user																			
Dirección IPv4	169.254.11.13																			
Dirección MAC:	08-00-27-9E-3F-E2																			
Sistema Operativo, versión, arquitectura:	MS Windows 10 LTSC, 1809, 64-bits																			
Memoria RAM	3048 MB																			
Cantidad y capacidad disco duro:	1 disco, 50 GB SATA III 5400 rpm																			
Procesador, generación, velocidad Hz	Intel Core i7, 8750H, 2.20GHz																			
<b>Título:</b> Practica #1																				
<b>Objetivo:</b> Identificar el origen de un BIN																				
Ingreso de datos ficticios requeridos por el aplicativo:																				

CC GENERATOR		BIN GENERATOR	
BRAND		COUNTRY	
VISA		ARGENTINA	
BANK			
CITIBANK			
CVV/CVV2	PIN	DATE (MM-YYYY)	
RANDOM	<input checked="" type="checkbox"/>	Random	Random
MONEY (\$)	QUANTITY	FORMAT	
\$500 - \$1000	5	TEXT	
GENERATE			

Datos ficticios generados:



CARD DETAILS
1 ) CARD BRAND : VISA CARD NUMBER : 4808523030464165 BANK : CITIBANK NAME : Johannes Gaukrogers ADDRESS : 33 Tonbridge Rd COUNTRY : ARGENTINA MONEY : \$790 CVV/CVV2 : 677 EXPIRY DATE : 06/2021 CARD PIN : 7168

Fuente: <https://www.vccgenerator.com/result/>

Ingreso de datos requeridos en aplicativo web:

Our **BIN database** software updates daily to give you a comprehensive list of Bank Identification Numbers. Unlike our competitors, who use computer-based algorithms to generate BIN lists, our BIN checker contains genuine entries. You can see this for yourself and we are convinced that you won't find any blank entries in it. All Bank Identification Numbers are supplied with complete and accurate information.

The online demo binchecker allows you to explore the powerful features of this binchecker.

Please enter first 6 digit of your Credit / Debit / Charge card	<input type="text" value="480852"/>
<div><div> I'm not a robot</div><div> reCAPTCHA <a href="#">Privacy</a> · <a href="#">Terms</a></div></div>	
<input type="button" value="Search Bin"/>	

Search the BIN database for Visa, Mastercard and Amex BIN numbers..

**BIN: 480852**

Your answer was correct. Please copy and paste text in this textbox in to the box below.

fQC UyFqCIMwqY5HOEQTA2QBu7DxJwPeZ72eFfGi8vnxRPLgtfCuNYOWqLaEGisHO46ooGAj72hloe  
FxpYzB0mv5E6piQOqALtilaW7efe03iM6aqwL2X76h219VY3XclQtArwrwTrXEqJ121eSWmcf5aNe7Xoq  
IN7cVnCOyEDss4C7sf5mMdyPclLo1vLo0IPVwl6mZU

fQC UyFqCIMwqY5HOEQTA2QBu7DxJwPeZ72eFfGi8vnxRPLgtfCuNYOWqLaEGisHO46ooGAj72hloe  
FxpYzB0mv5E6piQOqALtilaW7efe03iM6aqwL2X76h219VY3XclQtArwrwTrXEqJ121eSWmcf5aNe7Xoq  
IN7cVnCOyEDss4C7sf5mMdyPclLo1vLo0IPVwl6mZU

**Resultados de búsqueda en aplicativo web:**

**Your search results for BIN 480852 return**

BIN :	480852
Card Brand :	VISA
Issuing Organization :	CITIBANK
Card Type (DEBIT/CREDIT/CHARGE) :	CREDIT
Card SubType :	PURCHASING WITH FLEET
Issuing Country :	ARGENTINA

Report incorrect information

Search Again

Fuente: <http://exactbins.com/bin-lookup/>

Posteriormente para la práctica #2, estos fueron los pasos y resultados:

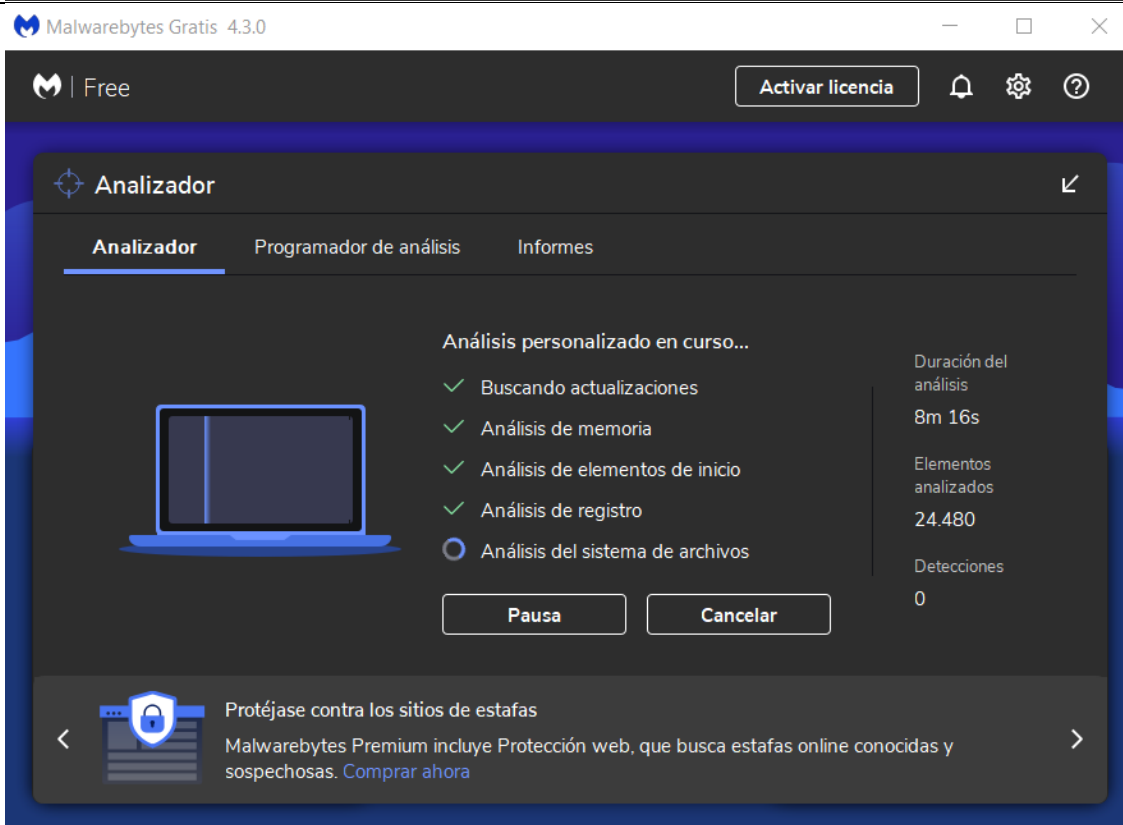
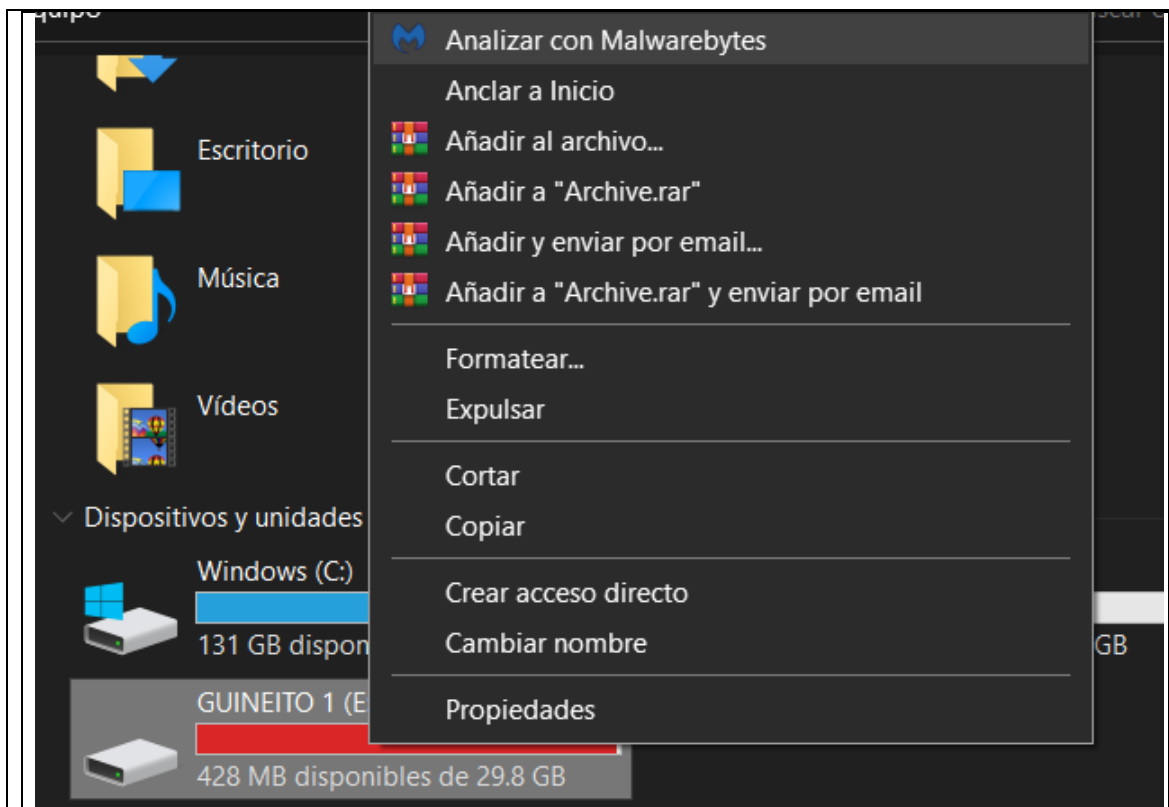
**Título:** Practica #2

**Objetivo:** Formatear (Sanear) un Periférico de Almacenamientos

Nota: Sanear un dispositivo o periférico de almacenamiento conlleva dos métodos.

- 1- Inicializar el proceso de análisis, búsqueda, identificación y remoción de artefactos maliciosos identificados por la solución Anti-Malware de su preferencia.
- 2- Inicializar un borrado de todos los archivos localizados dentro del periférico de almacenamiento, haciendo uso de la opción "formatear".

**Seleccionar la solución Anti-Malware de su preferencia**



**Resultados del proceso de saneamiento finalizado por solución Anti-Malware**

Analizador

Analizador

Programador de análisis

Informes

### Análisis personalizado resumen

25/4/21 13:01

Hora del análisis	8m 22s
Elementos analizados	146.087
Amenazas detectadas	0
PUP detectados	0
PUM detectadas	0
Detecciones ignoradas	0
Detecciones en cuarentena	0

Ver informe

Hecho

Fuente: Mecanismo de control Anti-Malware Malwarebytes

#### Proceso de saneamiento, mediante opción "Formatear"

131 GB disponibles d

GUINEITO 1 (E:)

428 MB disponibles d

Analizar con Malwarebytes

Anclar a Inicio

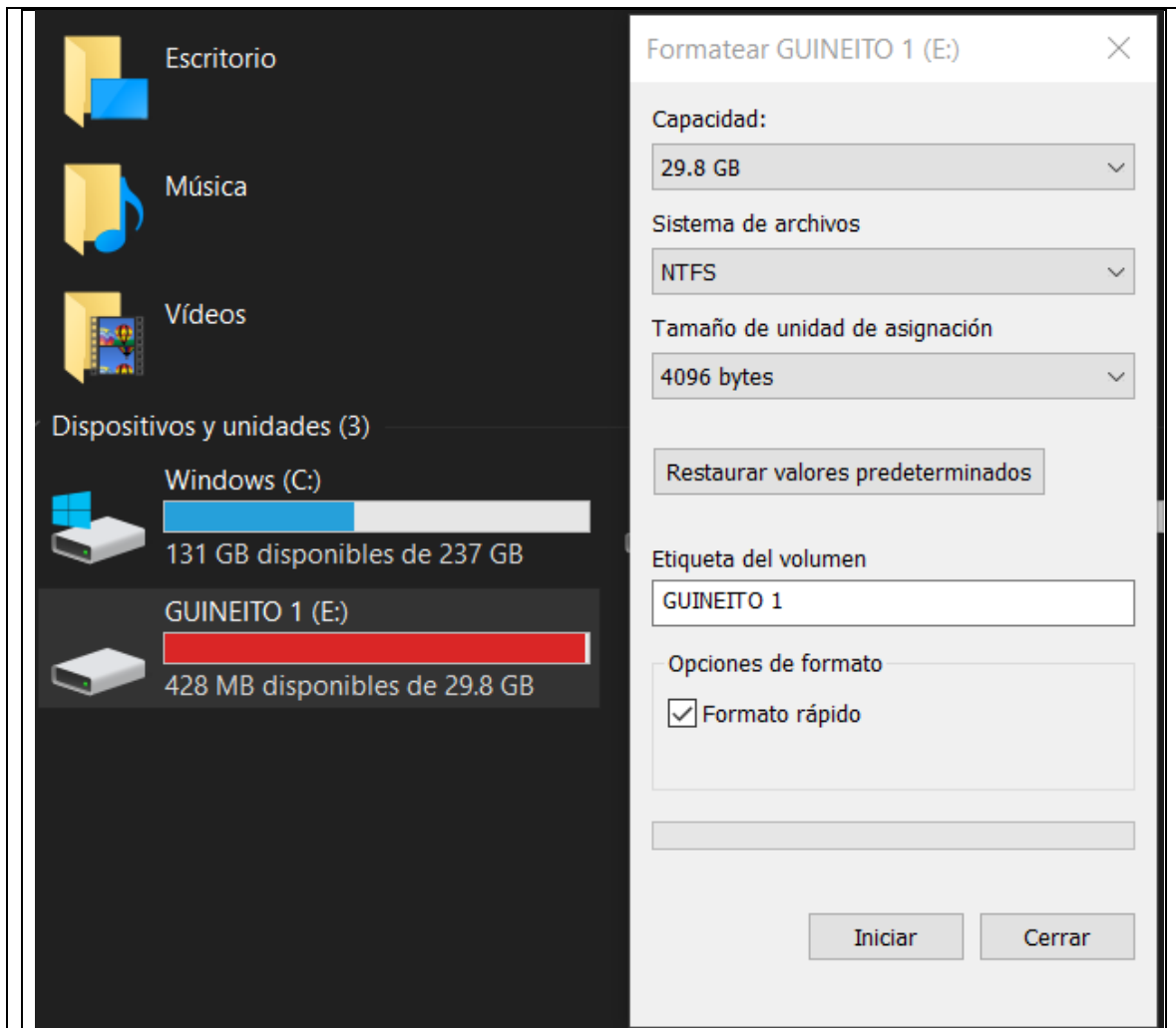
Añadir al archivo...

Añadir a "Archive.rar"

Añadir y enviar por email...

Añadir a "Archive.rar" y enviar por email

Formatear...

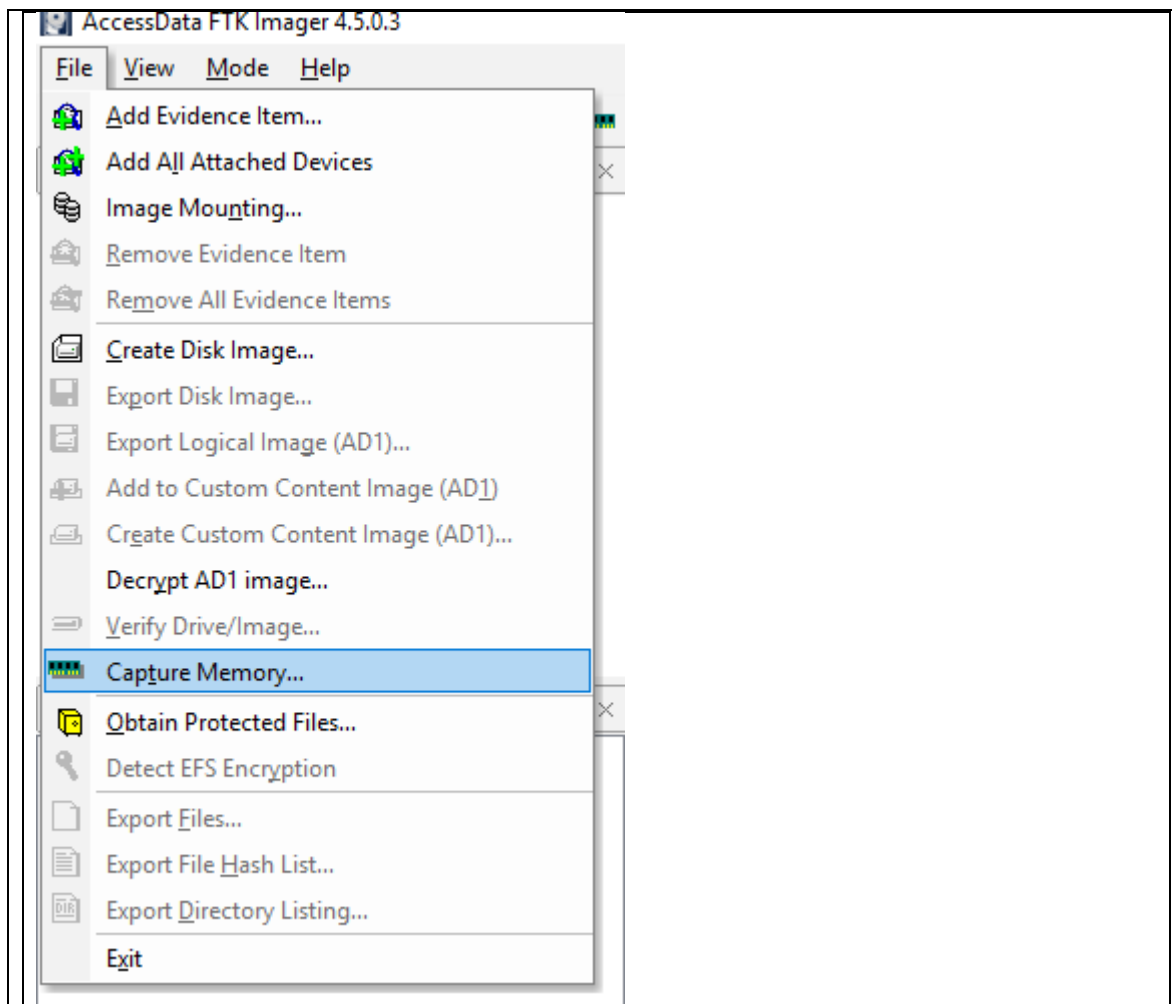


*Fuente: Opción de saneamiento "Formatear"*

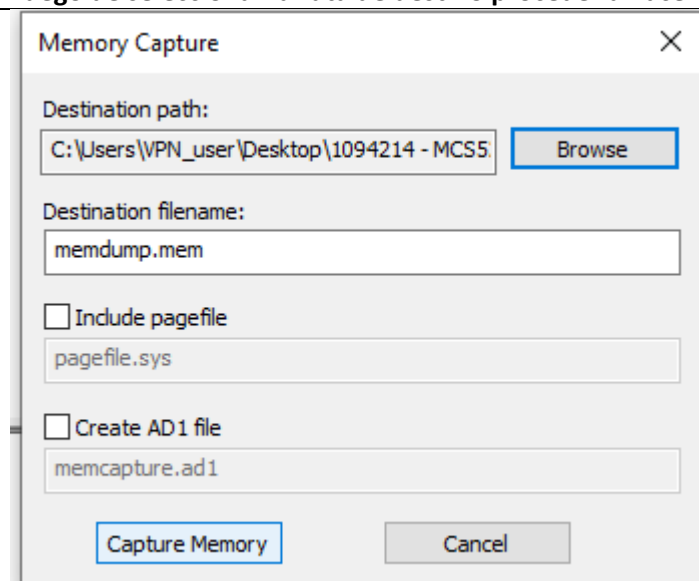
**Título:** Practica #3

**Objetivo:** Capturar volcado de memoria RAM – FTK Imager

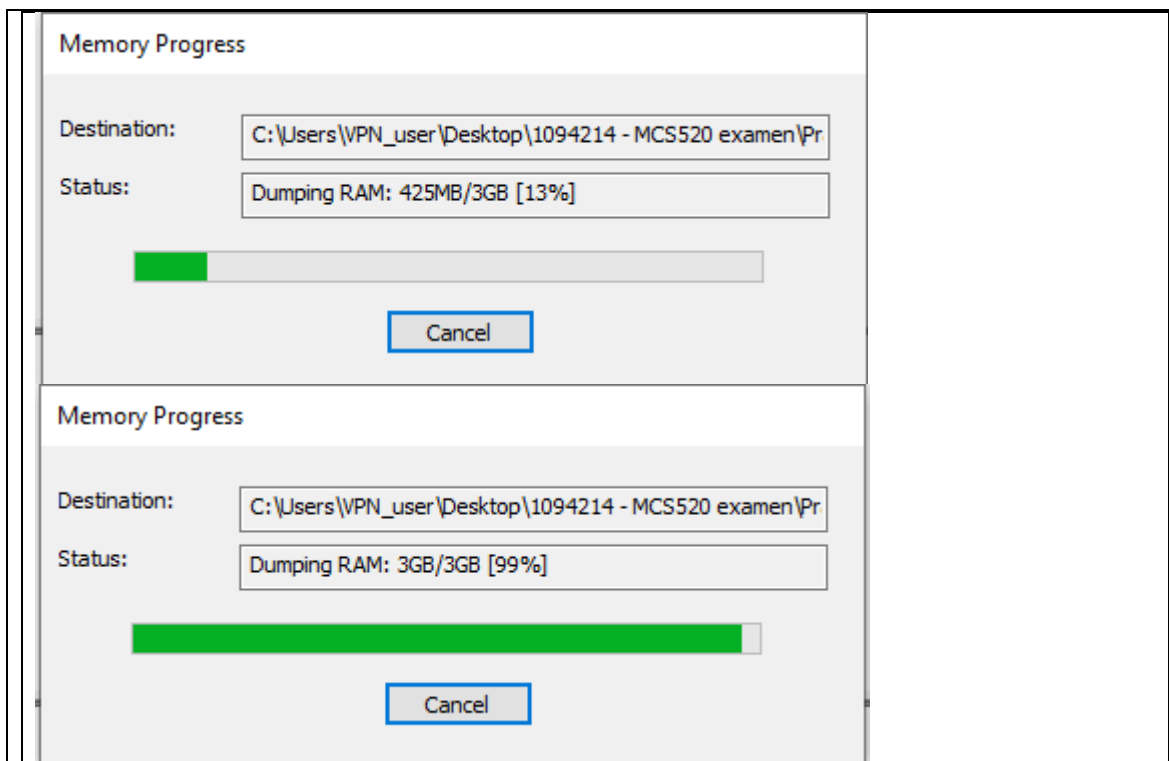
Seleccionar opción "Capture memory..."



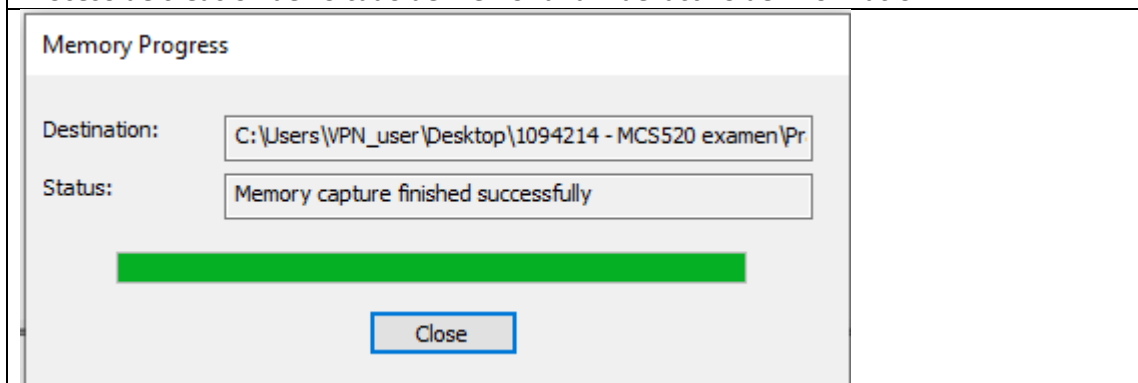
Luego de seleccionar la ruta de destino proceder a hacer clic en el boton "Capture Memory"



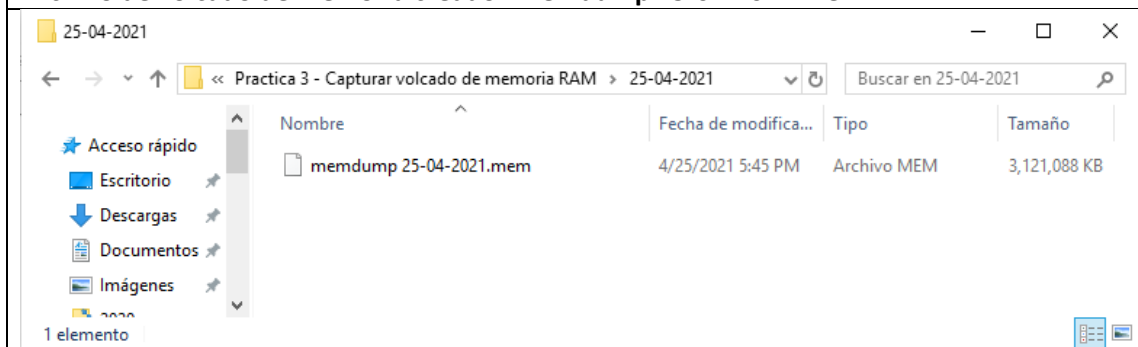




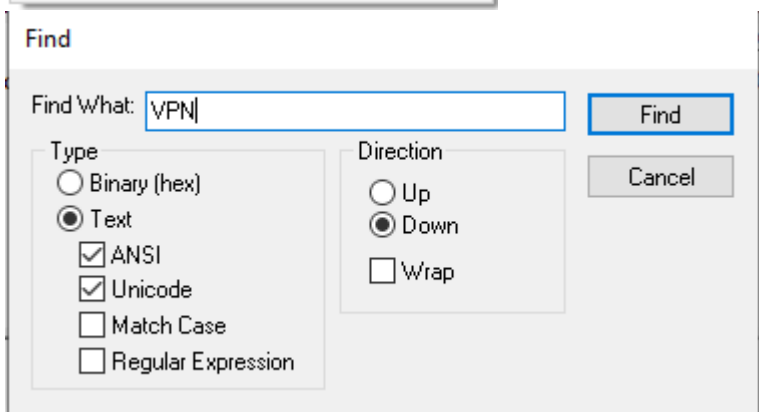
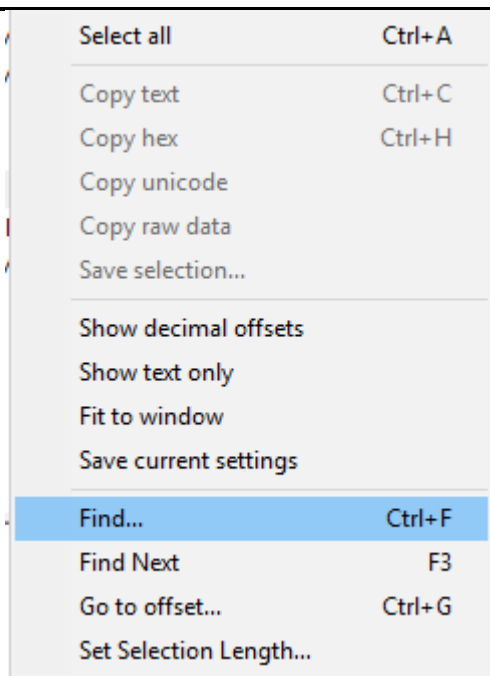
#### Proceso de creacion de volcado de memoria ram del activo de información



#### Archivo de volcado de memoria creado “memdump 25-04-2021.mem”



Hacer clic en la opción “Find...” y colocar el nombre del usuario del activo para validar que el volcado se haya realizado de manera correcta.



Name	Size	Type	Date Modified
AUTHORS.txt	1	Regular File	12/27/2016 1:44:32 PM
CREDITS.txt	4	Regular File	12/27/2016 1:52:54 PM
LEGAL.txt	1	Regular File	7/7/2016 1:16:42 AM
LICENSE.txt	15	Regular File	7/7/2016 1:16:42 AM
memdump 25-04-2021.mem	3,121,088	Regular File	4/25/2021 9:45:09 PM
README.txt	32	Regular File	12/24/2016 12:14:00 PM
volatility_2.6_win64_standalone.exe	15,424	Regular File	12/27/2016 2:02:42 PM

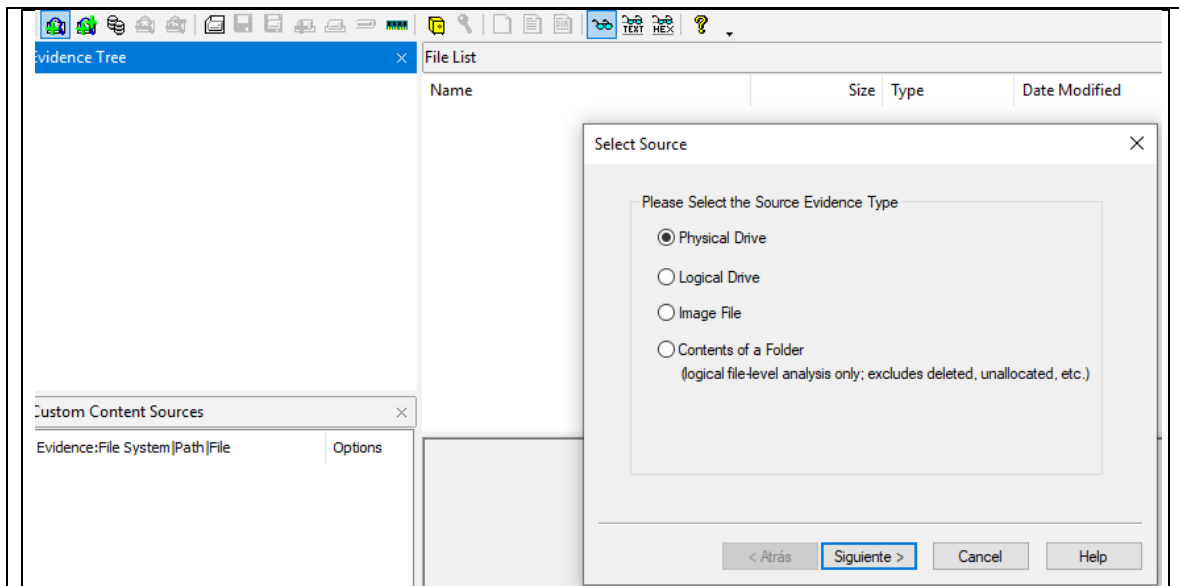
8f952610	00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
8f952620	00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
8f952630	00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
8f952640	00 00 00 00 00 00 00 00 00-02 00 00 00 00 00 00	.....
8f952650	5C 00 44 00 65 00 76 00-69 00 63 00 65 00 5C 00	\.D.e.v.i.c.e.\.
8f952660	48 00 61 00 72 00 64 00-64 00 69 00 73 00 6B 00	H.a.r.d.d.i.s.k.
8f952670	56 00 6F 00 6C 00 75 00-6D 00 65 00 32 00 5C 00	V.o.l.u.m.e-2.\.
8f952680	55 00 73 00 65 00 72 00-73 00 5C 00 56 00 50 00	U.s.e.r.s.\ V.P.
8f952690	4E 00 5F 00 75 00 73 00-65 00 72 00 5C 00 41 00	N_.u.s.e.r.\.A.
8f9526a0	70 00 70 00 44 00 61 00-74 00 61 00 5C 00 52 00	p.p.D.a.t.a.\.R.
8f9526b0	6F 00 61 00 6D 00 69 00-6E 00 67 00 5C 00 4D 00	o.a.m.i.n.g.\.M.
8f9526c0	69 00 63 00 72 00 6F 00-73 00 6F 00 66 00 74 00	i.c.r.o.s.o.f.t.
8f9526d0	5C 00 57 00 69 00 6E 00-64 00 6F 00 77 00 73 00	\.W.i.n.d.o.w.s.

Fuente: FTK Imager

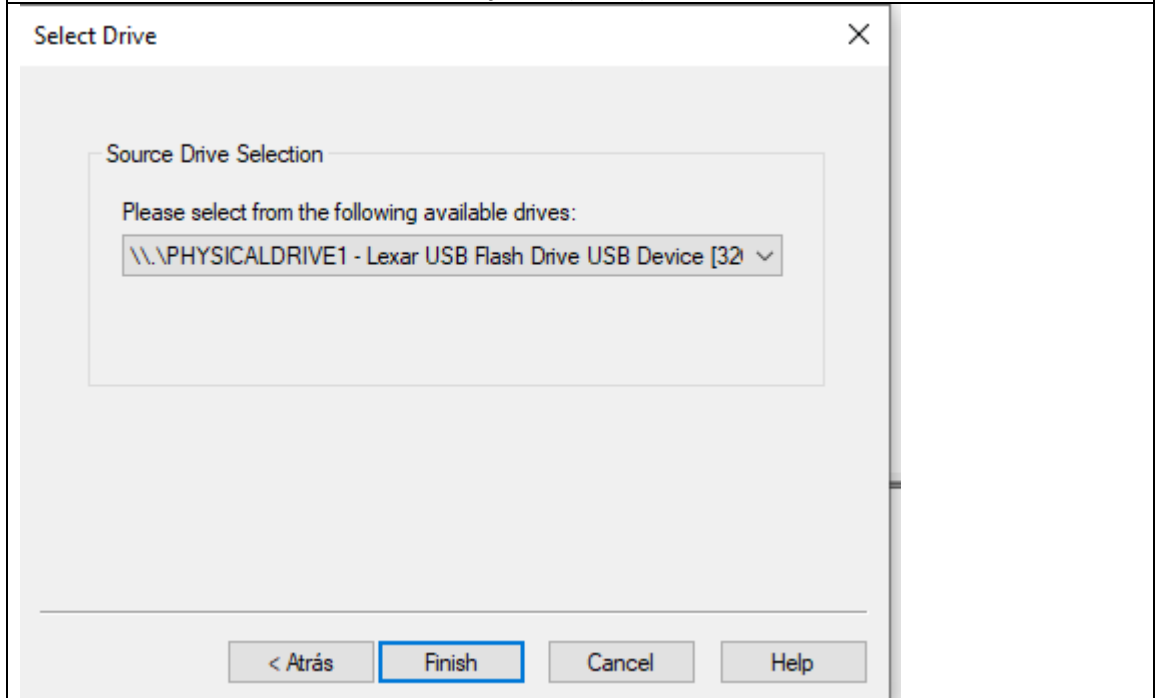
**Título:** Practica #4

**Objetivo:** Montar una memoria USB – FTK Imager

Durante el proceso investigativo se identificó que el 17 de marzo del 2021 fue realizado un volcado de memoria de un dispositivo extraíble localizado en la ruta de disco (E:\) el cual posee una capacidad de almacenamiento total de 32 GB.



### Seleccionar el disco extraíble o USB objetivo (32GB)



Evidence Tree

\\PHYSICALDRIVE1

Partition 1 [30535MB]

GUINEITO 1 [NTFS]

[orphan]

[root]

\$BadClus

\$Extend

\$Secure

\$UpCase

Beginning ASP .NET 4.5 In C#.pdf

BK USB AP

es\_windows\_10\_enterprise\_itsc\_2019\_...

Knight Rider (2008)

Maestrias

MEGA-RECOVERYKEY (1).txt

MEGA-RECOVERYKEY.txt

Music

Nueva carpeta

Presentaciones

Software utilidades

System Volume Information

tportable

White App Chat - M. Y. & Marthal Sierra

Custom Content Sources

Evidence:File System[Path|File]

Options

New

Edit

Remove

Remove All

Create Image

Properties

Hex Value Interp...

Custom Content ...

File List

Name	Size	Type	Date Modified
\$AttrDef	3	Regular File	12/2/2019 4:29:33 AM
\$BadClus	0	Regular File	12/2/2019 4:29:33 AM
\$Bitmap	955	Regular File	12/2/2019 4:29:33 AM
\$Bitmap.FileSlack	2	File Slack	
\$Boot	8	Regular File	12/2/2019 4:29:33 AM
\$I30	4	NTFS Index All...	3/20/2021 3:30:34 PM
\$LogFile	42,672	Regular File	12/2/2019 4:29:33 AM
\$MFT	3,440	Regular File	12/2/2019 4:29:33 AM
\$MFTMirr	4	Regular File	12/2/2019 4:29:33 AM
\$Secure	1	Regular File	12/2/2019 4:29:33 AM
\$TXF_DATA	1	NTFS Logged ...	3/20/2021 3:30:34 PM
\$UpCase	128	Regular File	12/2/2019 4:29:33 AM
\$Volume	0	Regular File	12/2/2019 4:29:33 AM
Beginning ASP .NET 4.5 In C#.pdf	22,441	Regular File	6/6/2016 11:13:34 PM
es_windows_10_enterprise_itsc_2019_x64_...	3,800,374	Regular File	8/29/2019 6:32:33 PM
Everything-1.4.1.877.x64-Setup.exe	1,410	Regular File	12/4/2017 12:02:45 PM
MEGA-RECOVERYKEY (1).txt	1	Regular File	3/5/2018 11:25:23 PM
MEGA-RECOVERYKEY.txt	1	Regular File	3/5/2018 11:24:28 PM
Resumen unid 3 - 25ptos.docx	18	Regular File	9/10/2019 2:22:17 AM
SQLPRWT_x64_ENU.exe	686,011	Regular File	6/24/2016 2:30:25 AM

00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00

10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00

20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00

30 00 00 00 00 00 00 00 00-

Cursor pos = 0

Listed: 33 Selected: 0 \\PHYSICALDRIVE1\Partition 1 [30535MB]\GUINEITO 1 [NTFS]\[root]

Posteriormente hacer clic derecho en la carpeta que desee recuperar y luego hacer clic en “Export Files” y la ruta destino.

Nueva carpeta

Presentaciones

Software utilida

Dell-Power

System-Util

System Volume

tportable

White App Chat - M. Y. & Marthal Sierra

Export Files...

Export File Hash List...

Export Logical Image (AD1)...

Add to Custom Content Image (AD1)

Practica 4 - Montar una Memoria USB

Compartir Vista

<< 1094214 - MCS52...

> Practica 4 - Montar una Memoria USB >

Nombre

Fecha de m

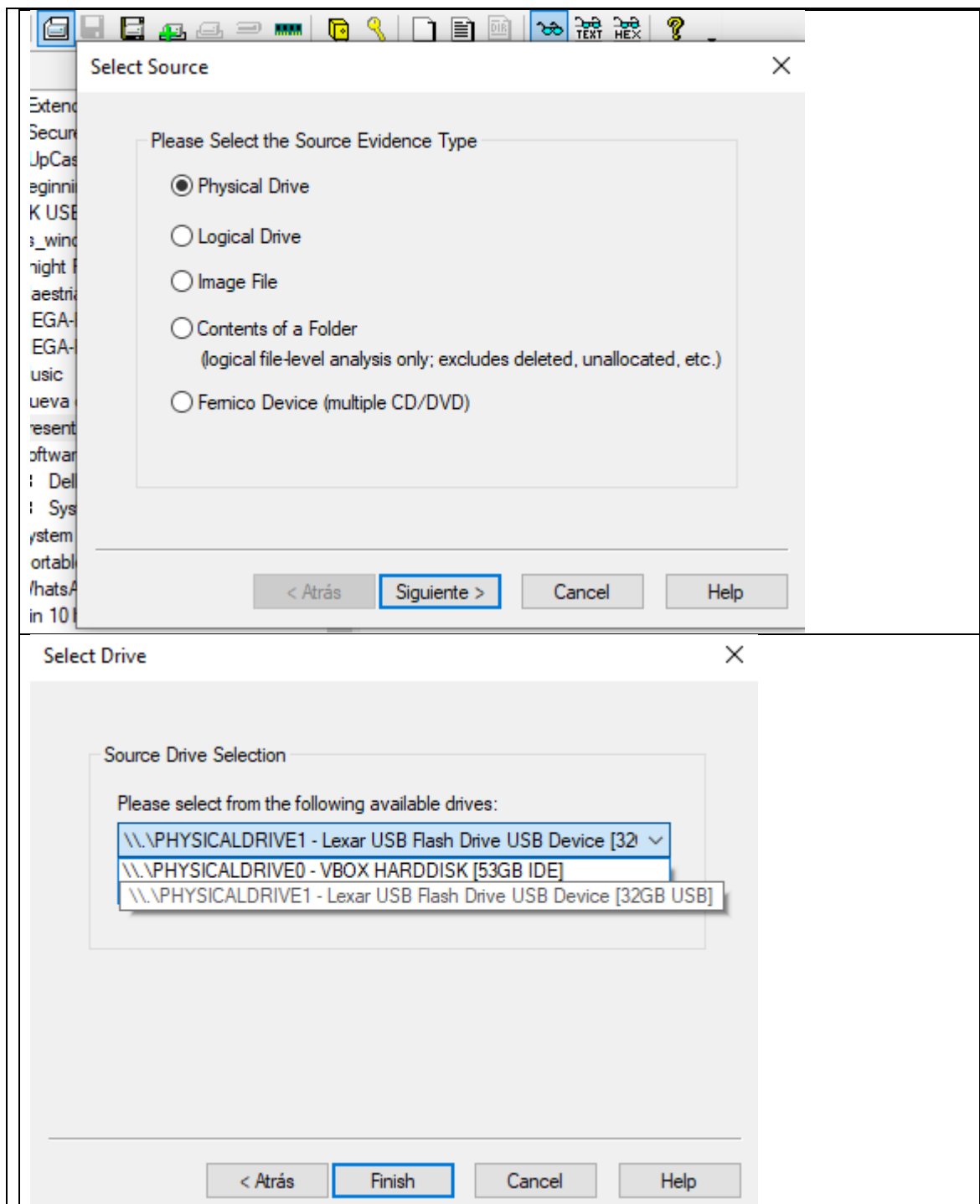
Presentaciones

4/25/2021

Fuente: FTK Imager

Título: Practica #5

Objetivo: Crear una imagen forense de una memoria USB – FTK Imager



Select Image Type

Please Select the Destination Image Type

☒ Raw (dd)  
☐ SMART  
☐ E01  
☐ AFF

< Atrás    **Siguiente >**    Cancelar    Ayuda

En este apartado se ingresan los detalles de la evidencia a analizar, responsable y datos de identificación de la evidencia (Cadena de Custodia).

Create Image

Image Source: \\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

Add...

Add Over

☒ Verify images after they are created  
☐ Create directory listings of all files in

Start

Evidence Item Information

Case Number: DO-IF-A000

Evidence Number: U000

Unique Description: USB: Imagen Forense

Examiner: Angel Peña

Notes: Practica #5. Datos: USB Lexar capc.32GB, c\Naranja

< Atrás    **Siguiente >**    Cancel    Help

01 00 00 00-00 10 00 00 01  
 B0 00 00 00-B0 00 00 00 00  
 00 00 01 00-90 00 80 00 00  
 00 00 01 00-52 82 3E 7E CE

Se procede a ingresar el nombre o título de la imagen de la USB "IMG\_USB\_U000"

Select Image Destination

Image Destination Folder  
C:\Users\VPN\_user\Desktop\1094214 - MCS520 examen\Practi Browse

Image Filename (Excluding Extension)  
IMG\_USB\_U000

Image Fragment Size (MB) 1500  
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☐

< Atrás Finish Cancel Help

Al hacer clic en “Finish”, mostrará una ventana indicando el destino de la imagen. Se debe hacer clic en “Start” para inicializar la construcción de la imagen.

Create Image

Image Source  
\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)  
C:\Users\VPN\_user\Desktop\1094214 - MCS520 examen\Practica 5 - Crear un

Add... Edit... Remove

Add Overflow Location

☒ Verify images after they are created ☒ Precalculate Progress Statistics  
☒ Create directory listings of all files in the image after they are created

Start Cancel

Proceso de construccion de imagen inicializado.



Creating Image [0%]

Image Source: \\.\PHYSICALDRIVE2

Destination: E:\1094214 - MCS520 examen\Practica 5 - Crear una image

Status: Creating image...

Progress

290.00 of 30536.00 MB (24.167 MB/sec)

Elapsed time: 0:00:12

Estimated time left: 0:20:51

Cancel

Imagen creada con formato ".0001"

... > Practica 5 - Crear una imagen forense de una mem...

Buscar en Practica 5 - Crear ...

Nombre	Fecha de modifica...	Tipo	Tamaño
IMG_USB_U000.001	4/25/2021 8:10 PM	Archivo 001	1,536,000 KB
IMG_USB_U000.001	4/25/2021 8:11 PM	Documento de tex...	2 KB
IMG_USB_U000.002	4/25/2021 8:10 PM	Archivo 002	90,624 KB

En la siguiente imagen, se pueden ver los detalles arrojados por el aplicativo FTK Imager acerca de la construccion de la imagen de la USB.

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:

Acquired using: ADI4.5.0.3

Case Number: DO-IF-A000

Evidence Number: U000

Unique description: USB: Imagen Forense

Examiner: Angel Peña

Notes: Practica #5. Datos: USB Lexar capc. 32GB c\Naranja

-----  
Information for E:\1094214 - MCS520 examen\Practica 5 -  
Crear una imagen forense de una memoria USB\IMG\_USB\_U000:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3,892

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 62,537,728

[Physical Drive Information]

Drive Model: Lexar USB Flash Drive USB Device

Drive Serial Number: AANS6F5QZMSKLOX5LASD

Drive Interface Type: USB

Removable drive: True

Source data size: 30536 MB

---

Sector count: 62537728

[Computed Hashes]

MD5 checksum: 454d342541ce5970a62e2272fd185ad1

SHA1 checksum: 0371a8b0eb619b28713eba173fde2b22f35be5f5

Image Information:

Acquisition started: Sun Apr 25 20:09:22 2021

Acquisition finished: Sun Apr 25 20:11:06 2021

Segment list:

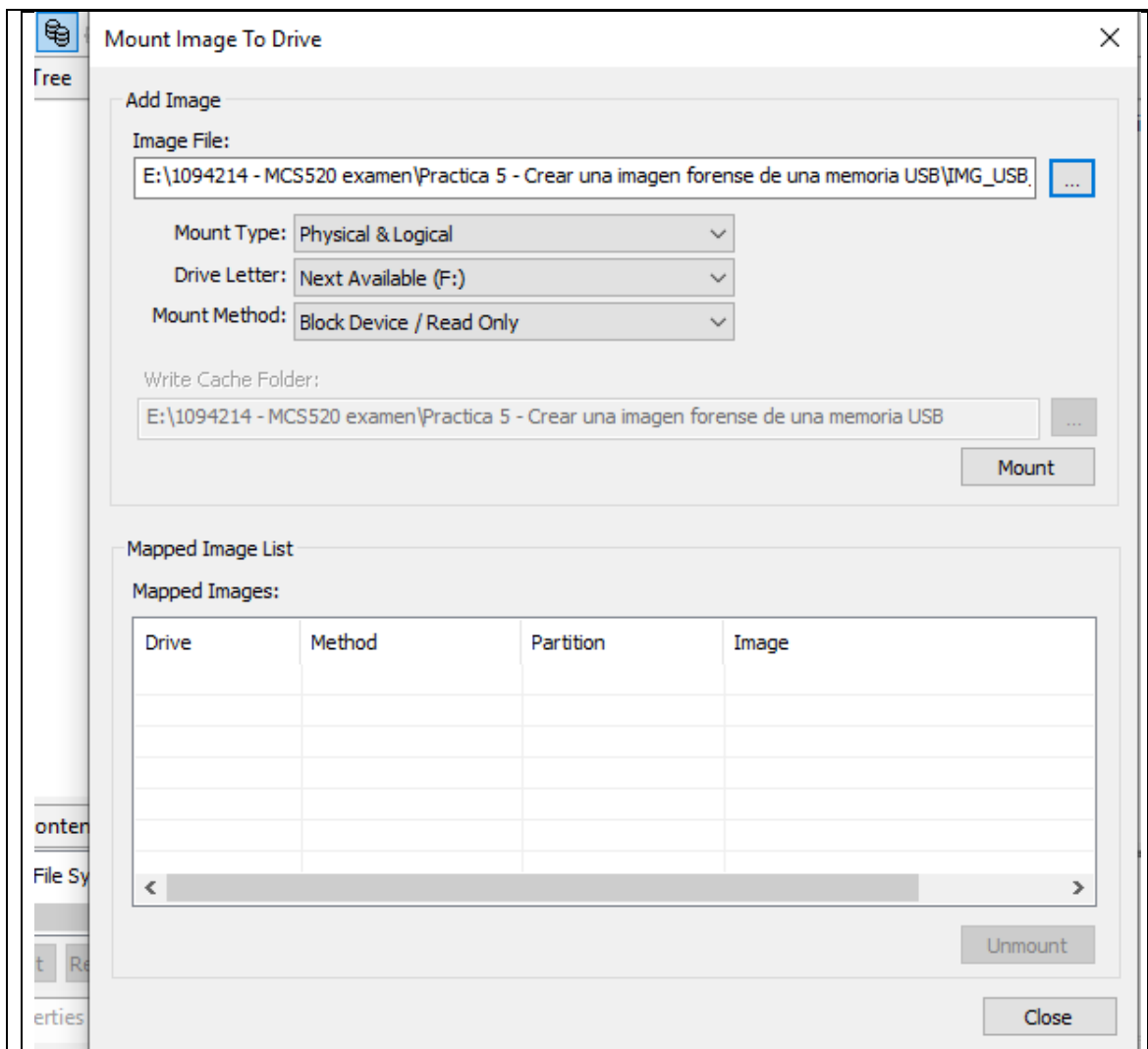
E:\1094214 - MCS520 examen\Practica 5 - Crear una imagen forense de una memoria USB\IMG\_USB\_U000.001

E:\1094214 - MCS520 examen\Practica 5 - Crear una imagen forense de una memoria USB\IMG\_USB\_U000.002

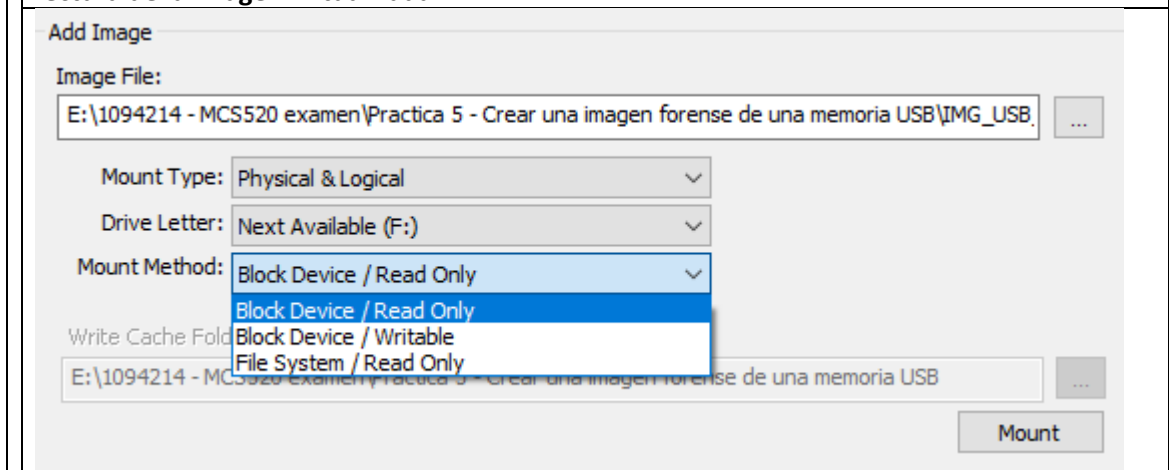
Fuente: FTK Imager

**Título:** Practica #6

**Objetivo:** Virtualizar o Montar imagen forense de memoria USB – FTK Imager

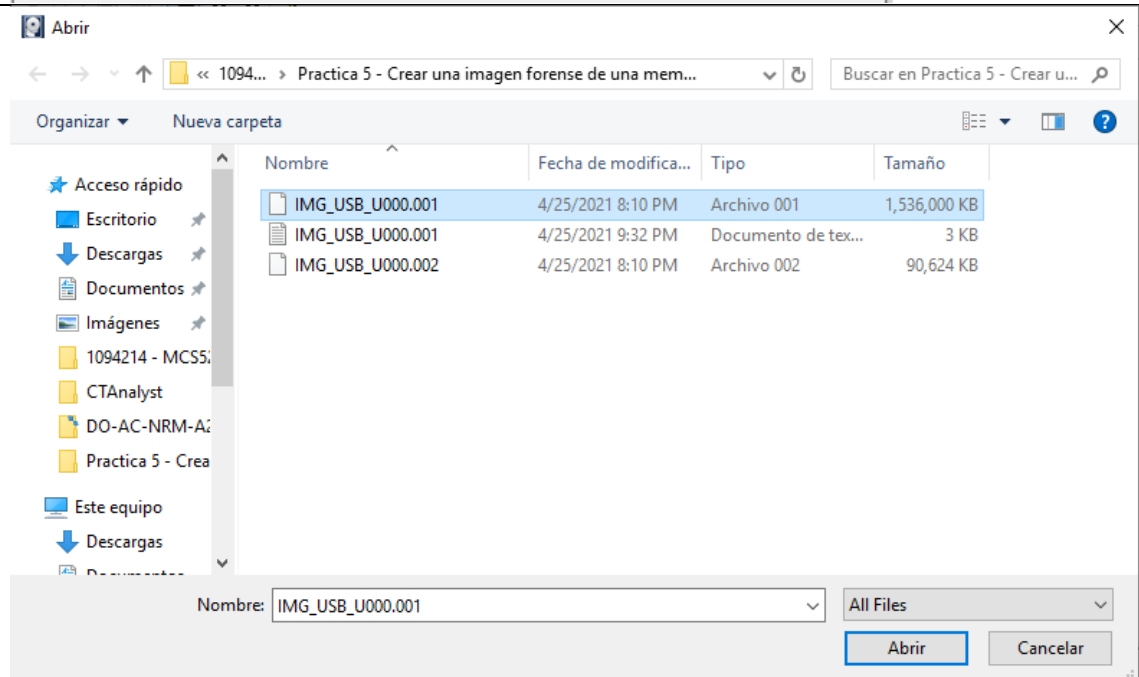
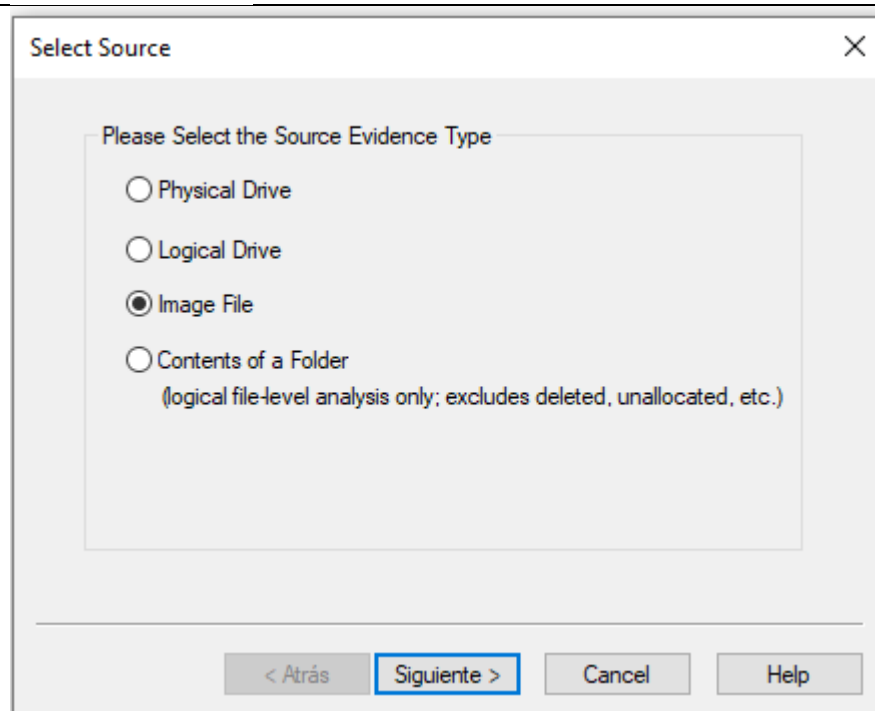
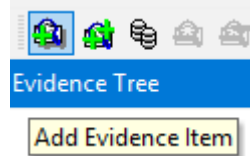


Se debe hacer clic en la opción "Block Device/Read Only" para solo habilitar el uso de lectura de la imagen virtualizada.





## Generar hash con FTK Imager



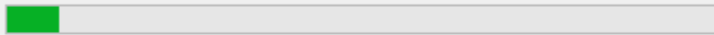
## Evidence Tree

- IMG\_USB\_U000.001
  - Parti
  - Unp
    - Remove Evidence Item
    - Verify Drive/Image...
    - Export Disk Image...
    - Image Mounting...
    - Export Directory Listing...

## Verifying [7%]

Source Drive/Image: IMG\_USB\_U000.001

### Progress



121.97 of 1588.50 MB verified (40.656 MB/sec)

Elapsed time: 0:00:03

Estimated time left: 0:00:36

Cancel

## Drive/Image Verify Results

[-]	
Name	IMG_USB_U000.001
Sector count	3253248
[-] MD5 Hash	
Computed hash	454d342541ce5970a62e2272fd185ad1
Report Hash	454d342541ce5970a62e2272fd185ad1
Verify result	Match
[-] SHA1 Hash	
Computed hash	0371a8b0eb619b28713eba173fde2b22f35be!
Report Hash	0371a8b0eb619b28713eba173fde2b22f35be!
Verify result	Match
[-] Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

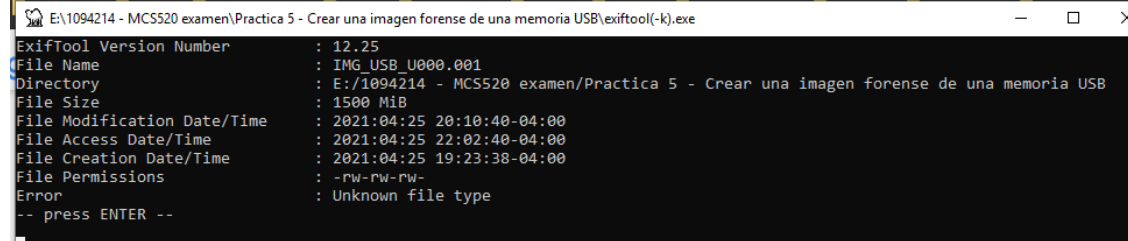
Close

*Fuente: FTK Imager*

**Título:** Practica #8

**Objetivo:** Obtener los Metadatos de un archivo

**La imagen virtualizada “IMG\_USB\_U000” fue analizada con la herramienta “ExifTools”**



```
ExifTool Version Number      : 12.25
File Name                    : IMG_USB_U000.001
Directory                   : E:/1094214 - MCS520 examen/Practica 5 - Crear una imagen forense de una memoria USB
File Size                   : 1500 MiB
File Modification Date/Time  : 2021:04:25 20:10:40-04:00
File Access Date/Time       : 2021:04:25 22:02:40-04:00
File Creation Date/Time     : 2021:04:25 19:23:38-04:00
File Permissions             : -rw-rw-rw-
Error                       : Unknown file type
-- press ENTER --
```

*Fuente: ExifTools*

**Título:** Practica #9

**Objetivo:** ¿Porque debe de ir un experto al levantamiento?

Debido a que los peritos informáticos forenses conocen las normas y reglamentos para el cuidado de las evidencias. Poseen un conocimiento especializado en las herramientas a utilizar, composición de los sistemas y como salvaguardar las evidencias. Tienen la habilidad y responsabilidad de evidenciar que los datos recolectados son íntegros e irrefutables ante cualquier juicio que se encuentre en ejecución.

El perito informatico forense se encarga de extraer informacion tanto de activos de informacion encendidos, como los apagados, dispositivos móviles o cualquier otro dispositivo informatico que se encuentre asociado a una investigación.

El Profesional del computo forense debe asistir a las escenas donde se identifique que fue utilizado un medio informatico para dar origen a un atentado criminalístico.

**Título:** Practica #10

**Objetivo:** Análisis estático – OSForensics (Free Trial)

Edit Case

Help

Basic Case Data

Case Categories

Offense & Custody Data

Description of Evidence

Chain of Custody

Custom Fields

◀ ▶

Case Name

2021-04-25 22-49-24

▼

Investigator

Angel Peña

▼

Organization

▼

Contact Details

▼

Timezone

Local (GMT -4:00)

▼

Default Drive

C:\ [Local]

▼

Acquisition Type

☒ Live Acquisition of Current Machine

☐ Investigate Disk(s) from Another Machine

Enable USB Write-block

☐

Case Folder

☐ Default Location

☒ Custom Location

E:\1094214 - MCS520 examen\Practica 10 - Analisis estatico\Evid\

Browse

Log case activity

☒

OK

Cancel





## Live Acquisition Auto Image

Case Name

Investigator

Case Folder ☐ Default Location ☒ Custom Location

[Browse](#)

### Scan Options

☒ Process List

☒ System Information

☐ Memory Dump

☐ Screen Capture

☒ Detect Bitlocker Encryption

☒ User Activity

☒ Save files to Logical Image [\(Config...\)](#)

☐ Passwords/Logins

☒ File Listing [\(Select drives\)](#)

☒ Generate HTML Report

☒ List of Deleted Files [\(Select drives\)](#)

☐ Generate PDF Report

☒ Clipboard Contents

[Check All](#)

[Uncheck All](#)

Mouse over an item for more information.

[Close](#)

[Start Scan](#)

Case Path

E:\1094214 - MCS520 examen\Practica 10 - Analisis estatico\Evid\

Task Progress

Task	# Results	Status
Process List		In Progress
Physical Memory Dump		In Progress
User Activity Scan		In Progress
Password/Login Scan		In Progress
System Information		In Progress
File Listing		In Progress
List of Deleted Files		In Progress
Collect Clipboard Contents		In Progress
Screen Capture		In Progress
Detect BitLocker		In Progress

Physical Memory Dump

Please refrain from performing other activities while this dialog box is visible.

Est. Time Remaining: 30 Seconds (91.64 MB\s)

Suggested Actions

- Manually search for files
- Manually search for videos
- Manually search for E-mail archives
- Review deleted files found
- Carve deleted files in unallocated clusters
- Image hard drive
- Browse file system
- Edit Case details
- Generate new HTML report
- Generate new PDF report

Progreso de la captura de informacion y/o triaje:

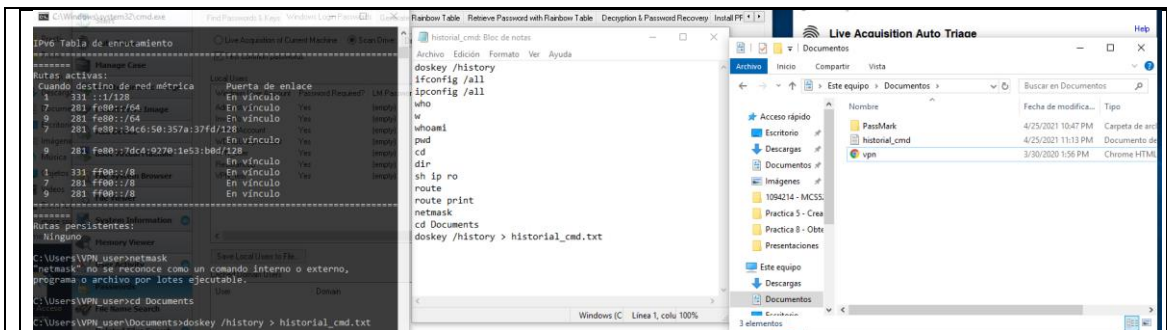
Case Path

E:\1094214 - MCS520 examen\Practica 10 - Analisis estatico\Evid\

Task Progress

Task	# Results	Status
Process List	68 Processes	Finished
Physical Memory Dump	Memory snapshot taken	Finished
User Activity Scan	594 Artifacts	In Progress
Password/Login Scan	7 Passwords/keys and logins	In Progress
System Information	3 commands completed	In Progress
File Listing	5877 files found	In Progress
List of Deleted Files	Running deleted files search	Finished
Collect Clipboard Contents	1 clipboard items exported	Finished
Screen Capture	Screen captures taken	Finished
Detect BitLocker	BitLocker detection complete	Finished

Historial de comandos en consola o terminal de MS Windows



Datos activo de informacion: ResistanceB

## Computer Name (Registry)

Date: domingo, abril 25, 2021, 23:16:04

Registry File: HKEY\_LOCAL\_MACHINE

Key Location: SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Computer Name	RESISTANCEB
---------------	-------------

[Back to Top](#)

## Timezone Info (Registry)

Date: domingo, abril 25, 2021, 23:16:04

Registry File: HKEY\_LOCAL\_MACHINE

Key Location: SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Timezone Name	SA Western Standard Time
Bias	240
Daylight Saving Bias	-60
Active Bias	240



## System Information

List: Basic System Information ▼ Edit... Go Export to Case... Export to File...

☒ Live Acquisition of Current Machine ☐ Scan Drive: C:\ ▼

Commands Result 1 - Basic System Information (Live) ✕

Date: domingo, abril 25, 2021, 22:54:30

### CPU

<b>CPU manufacturer:</b>	GenuineIntel
<b>CPU Type:</b>	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz
<b>Codename:</b>	Coffee Lake
<b>CPUID</b>	Family 6, Model 9E, Stepping A
<b>Socket:</b>	LGA 1151
<b>Lithography:</b>	14nm
<b>Physical CPU's:</b>	1
<b>Cores per CPU:</b>	2
<b>Hyperthreading:</b>	Disabled
<b>CPU features:</b>	MMX SSE SSE2 SSE3 SSSE3 SSE4.1 SSE4.2 DEP PAE Intel64 AES AVX AVX2
<b>Clock frequencies:</b>	
- Measured CPU speed:	2208.0 MHz
- Base Clock:	100.0 MHz
- Multiplier range:	Min: x22, Max non turbo: x22

**Registry File:** HKEY\_LOCAL\_MACHINE

**Key Location:** SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces

**Timezone:** -4:00

<b>Network GUID</b>	{4051634c-6e11-41d8-8f81-f7900498a23c}
<b>Network Name</b>	Ethernet
<b>IP (using DHCP)</b>	10.0.2.15 (Yes)
<b>DHCP Server</b>	10.0.2.2
<b>DHCP Name Server</b>	196.3.81.132 200.88.127.22
<b>Lease Obtained</b>	domingo, abril 25, 2021, 19:31:58
<b>Lease Expires</b>	lunes, abril 26, 2021, 19:31:58
<b>Network GUID</b>	{4db7800d-bc97-4270-a61b-1c317c2366e2}
<b>Network Name</b>	Ethernet (depurador de kernel)
<b>IP (using DHCP)</b>	(Yes)
<b>DHCP Server</b>	
<b>DHCP Name Server</b>	
<b>Lease Obtained</b>	
<b>Lease Expires</b>	

**Registry File:** HKEY\_LOCAL\_MACHINE\SAM

**Key Location:** SAM\SAM\Domains\Account\Users

**Using Timezone:** -4:00

<b>Username [ID]</b>	Administrador [500]
<b>Full Name</b>	
<b>Description</b>	Cuenta integrada para la administración del equipo o dominio
<b>Password Hint</b>	
<b>Account Created</b>	domingo, abril 25, 2021, 23:16:04 (can be inaccurate if registry permissions have been updated)
<b>Last Login</b>	Never
<b>Password Reset</b>	Never
<b>Password Fail Date</b>	N/A
<b>Password Fail Count</b>	0 (reset after correct login)
<b>Login Count</b>	0
<b>Notes</b>	*Password never expires*

<b>Username [ID]</b>	VPN_user [1001]
<b>Full Name</b>	
<b>Description</b>	
<b>Password Hint</b>	null
<b>Account Created</b>	domingo, abril 25, 2021, 23:16:04 (can be inaccurate if registry permissions have been updated)
<b>Last Login</b>	domingo, abril 25, 2021, 19:33:03
<b>Password Reset</b>	Never
<b>Password Fail Date</b>	N/A
<b>Password Fail Count</b>	0 (reset after correct login)
<b>Login Count</b>	363
<b>Notes</b>	*Password never expires*
<b>Username [ID]</b>	Resistanceb [1002]
<b>Full Name</b>	
<b>Description</b>	
<b>Password Hint</b>	
<b>Account Created</b>	domingo, abril 25, 2021, 23:16:04 (can be inaccurate if registry permissions have been updated)
<b>Last Login</b>	domingo, marzo 22, 2020, 17:39:56
<b>Password Reset</b>	jueves, marzo 19, 2020, 19:46:15
<b>Password Fail Date</b>	domingo, marzo 22, 2020, 17:40:43
<b>Password Fail Count</b>	1 (reset after correct login)
<b>Login Count</b>	15

# manage-bde.exe -status

Date: domingo, abril 25, 2021, 23:18:53

Cifrado de unidad BitLocker: versión de la herramienta de configuración 10.0.1776

Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

Volumenes del disco que se pueden proteger con el Cifrado de unidad

BitLocker:

Volumen E: [more space]

[Volumen de datos]

Tamaño:	49.98 GB
Versión de BitLocker:	Ninguno
Estado de conversión:	Descifrado completo
Porcentaje cifrado:	0.0%
Método de cifrado:	Ninguno
Estado de protección:	Protección desactivada
Estado de bloqueo:	Desbloqueado
Campo de identificación:	Ninguno
Desbloqueo automático:	Deshabilitado

Historial de navegación



**User Activity**
Help

☒ Live Acquisition of Current Machine  
☐ Scan Drive: C:\

Activity Filters: Off  
 Timeline Filter: Off  
 Quick Filter:  Go Reset

Scan Config...  
Filters

**Total Items: 22866**

Windows Explorer - Recent Items ( 84 )

OSX - Recent Documents ( 0 )

OSX - Recent Items ( 0 )

OSX Media - Recent Files ( 0 )

OSX - Network Drives ( 0 )

Installed Programs ( 80 )

Autorun Commands ( 3 )

Clipboard ( 1 )

Event Logs ( 13828 )

UserAssist ( 136 )

Jump Lists ( 187 )

Shellbags ( 11 )

Windows 10 Timeline ( 428 )

Recycle Bin ( 0 )

Shimcache ( 0 )

SRUM ( 0 )

Prefetch ( 0 )

Windows Search ( 0 )

Downloads ( 31 )

Browser History ( 997 )

Search Terms ( 13 )

Website Logins ( 5 )

Form History ( 6360 )

Bookmarks ( 489 )

Chat Logs ( 0 )

Peer-to-Peer ( 0 )

WLAN ( 0 )

Cookies ( 0 )

USB ( 9 )

Mounted Volumes ( 1 )

Mobile Backups ( 0 )

File Details

File List

Timeline

<input type="checkbox"/>	Title	URL	Date Last Accessed	Visit
<input type="checkbox"/>	OSForensics - Download	https://www.osforensics.c...	4/25/2021, 22:42:06	1
<input type="checkbox"/>	PassMark OSForensics...	https://www.osforensics.c...	4/25/2021, 22:41:51	1
<input type="checkbox"/>	¿Qué es un perito infor...	https://protecciondatos-lop...	4/25/2021, 22:35:56	1
<input type="checkbox"/>	perito informatico foren...	https://www.google.com/s...	4/25/2021, 22:35:49	2
<input type="checkbox"/>	Jeffrey Fried's Image M...	http://exif.regex.info/exif.cgi	4/25/2021, 22:32:46	11
<input type="checkbox"/>	exiftool online - Buscar ...	https://www.google.com/s...	4/25/2021, 22:19:10	3
<input type="checkbox"/>	Magick: ImageMagick...	http://exif-viewer.com/	4/25/2021, 22:19:08	4
<input type="checkbox"/>	exiftool windows online ...	https://www.google.com/s...	4/25/2021, 22:18:07	2
<input type="checkbox"/>	Latest ExiftoolGUI versi...	https://exiftool.org/forum/l...	4/25/2021, 22:04:58	1
<input type="checkbox"/>	ExifToolGUI	https://exiftool.org/gui/	4/25/2021, 22:04:08	1
<input type="checkbox"/>	exiftool windows - Busc...	https://www.google.com/s...	4/25/2021, 22:03:59	2
<input type="checkbox"/>	Installing ExifTool	https://exiftool.org/install.h...	4/25/2021, 21:59:28	1
<input type="checkbox"/>	ExifTool by Phil Harvey	https://exiftool.org/	4/25/2021, 21:59:13	2
<input type="checkbox"/>	exiftool online - Buscar ...	https://www.google.com/s...	4/25/2021, 21:59:04	2
<input type="checkbox"/>	exiftools - Buscar con ...	https://www.google.com/s...	4/25/2021, 21:48:53	2
<input type="checkbox"/>	Bert Moss eforensics ar...	http://www.isebahamas.co...	4/25/2021, 21:44:31	1
<input type="checkbox"/>	HOW TO INVESTIGA...	https://eforensicsmag.com...	4/25/2021, 21:44:09	1
<input type="checkbox"/>	how to obtain metadata...	https://www.google.com/s...	4/25/2021, 21:44:04	2
<input type="checkbox"/>	how to generate hash ...	https://www.google.com/s...	4/25/2021, 21:43:38	3
<input type="checkbox"/>	How to Verify the MD5 ...	https://support.accessdata...	4/25/2021, 21:27:05	1
<input type="checkbox"/>	HashMyFiles: Calculate...	https://www.nirsoft.net/util...	4/25/2021, 21:16:13	2
<input type="checkbox"/>	CurrPorts: Monitoring T...	https://www.nirsoft.net/util...	4/25/2021, 21:15:55	1
<input type="checkbox"/>	RegDllView - Register ...	https://www.nirsoft.net/util...	4/25/2021, 21:14:35	1
<input type="checkbox"/>	ProcessActivityView - S...	https://www.nirsoft.net/util...	4/25/2021, 21:14:22	1
<input type="checkbox"/>	DriverView: Loaded Wi...	https://www.nirsoft.net/util...	4/25/2021, 21:13:54	1
<input type="checkbox"/>	SysExporter: Grab data...	https://www.nirsoft.net/util...	4/25/2021, 21:13:39	1
<input type="checkbox"/>	SpecialFoldersView - S...	https://www.nirsoft.net/util...	4/25/2021, 21:12:36	1
<input type="checkbox"/>	CurrPorts: Monitoring T...	https://www.nirsoft.net/util...	4/25/2021, 21:12:14	1
<input type="checkbox"/>	Download 64-bit (x64) ...	https://www.nirsoft.net/x6...	4/25/2021, 21:12:00	1
<input type="checkbox"/>	hash my files - Buscar c...	https://www.google.com/s...	4/25/2021, 21:11:44	2
<input type="checkbox"/>	Memory dump analysis ...	https://book.hacktricks.xy...	4/25/2021, 21:10:38	0
<input type="checkbox"/>	TryHackMe: vulnversit...	https://latios01.medium.c...	4/25/2021, 21:10:38	0
<input type="checkbox"/>	Ubuntu 20.04 y NETPL...	https://mytcpip.com/netpla...	4/25/2021, 21:10:38	0

## Listado softwares instalados

Administrador: Símbolo del sistema

Microsoft Windows [Versión 10.0.17763.1879]  
 (c) 2018 Microsoft Corporation. Todos los derechos reservados.  
 C:\Windows\system32>wmic /output:E:\Listado\_Software\_Instalado.txt product get name, version  
 C:\Windows\system32>

Listado\_Software\_Instalado: Bloc de notas

Archivo Edición Formato Ver Ayuda

Name	Version
Office 16 Click-to-Run Extensibility Component	16.0.13901.20400
Office 16 Click-to-Run Localization Component	16.0.13901.20336
Office 16 Click-to-Run Extensibility Component 64-bit Registration	16.0.13901.20336
Office 16 Click-to-Run Licensing Component	16.0.13901.20400
Memoryze	3.0.0
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005	12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005	12.0.21005
Teams Machine-Wide Installer	1.3.0.9267
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	9.0.30729.6161
J2SE Runtime Environment 5.0 Update 12	1.5.0.120
AccessData FTK Imager	4.5.0.3
Cisco AnyConnect Secure Mobility Client	4.9.06037

Fuente: OSForensics

