

25 DE ABRIL DE 2024



## 2 APP CON ADF AVILA FORENSICS

ANÁLISIS FORENSE INFORMÁTICO

ERIC SERRANO MARÍN

I.E.S MARTINEZ MONTAÑES  
CETI

**Contenido**

Downgrade de Whatsapp..... 2

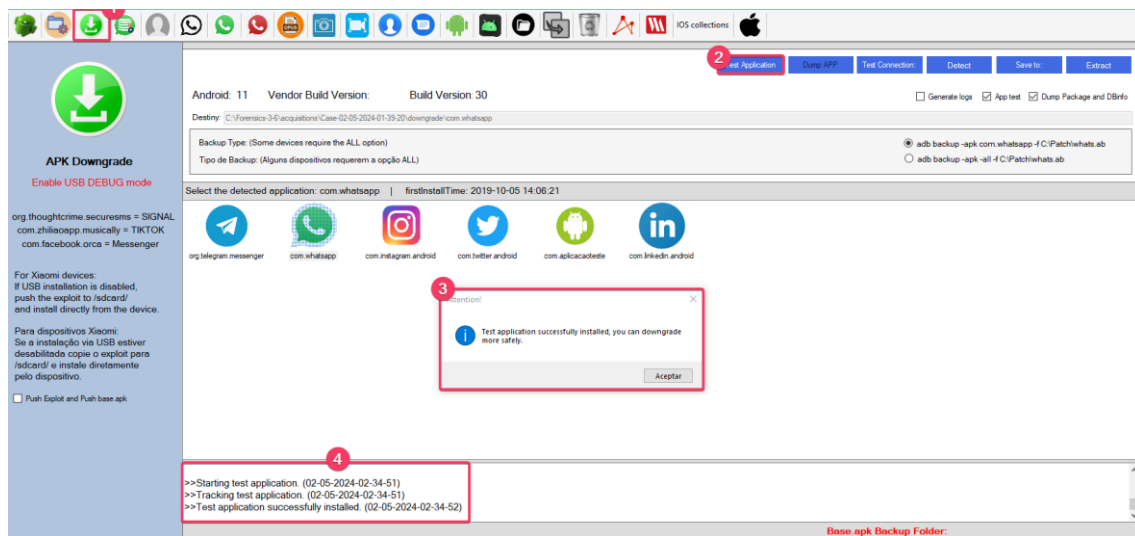
Downgrade de Telegram..... 11

Downgrade de Twitter. .... 12

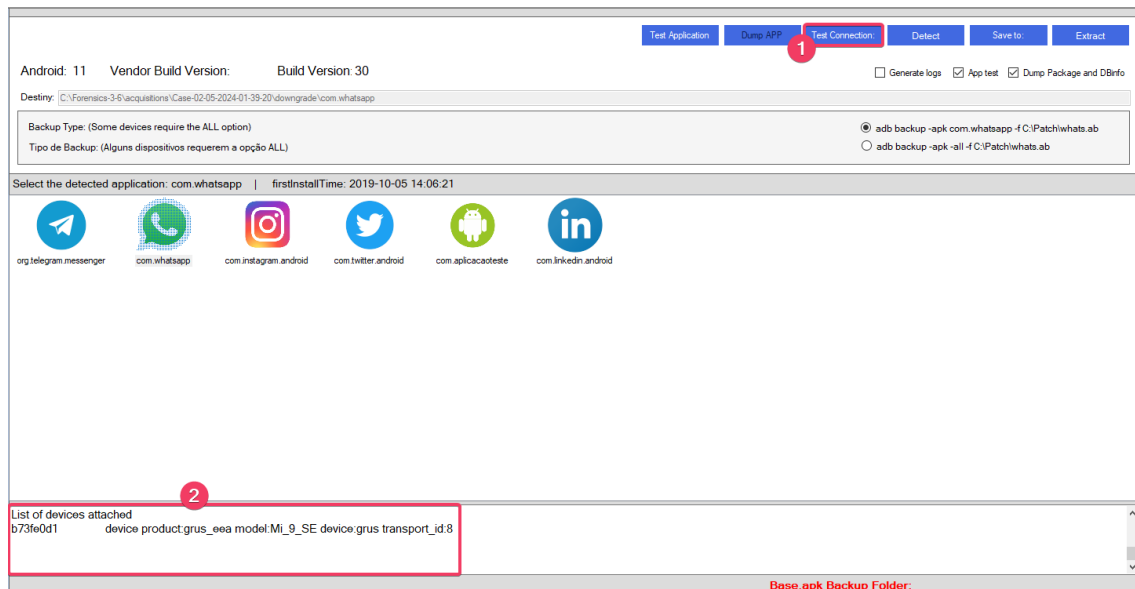
## Downgrade de Whatsapp.

Para que el primer paso funcione, tendremos que habilitar la depuración USB y la instalación por USB.

Al darle clic a Test Application se nos instalará una APP en el móvil, tendremos que darle a aceptar, esta aplicación comprobará si el downgrade es aplicable.

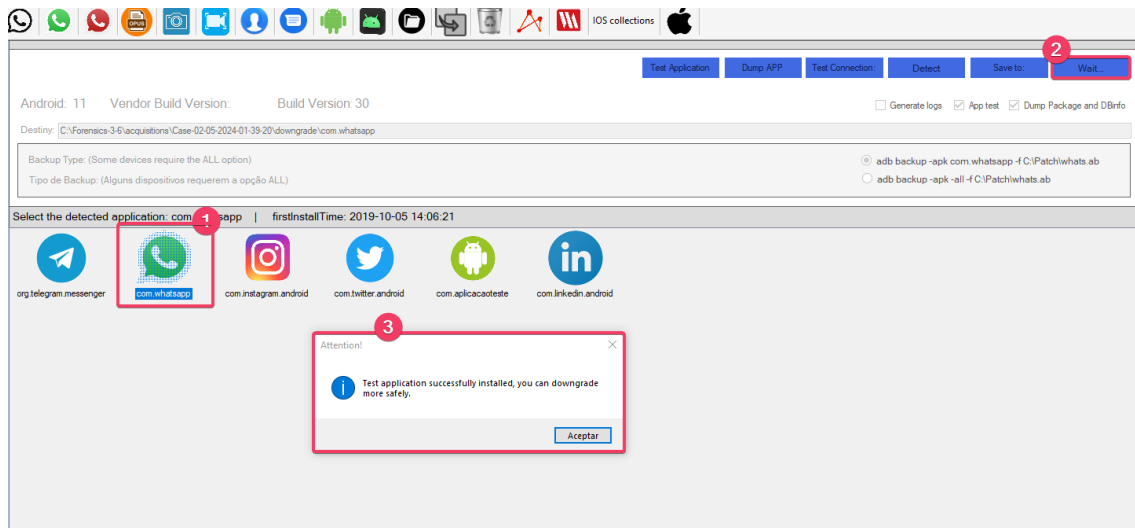


Ahora comprobaremos la conexión.

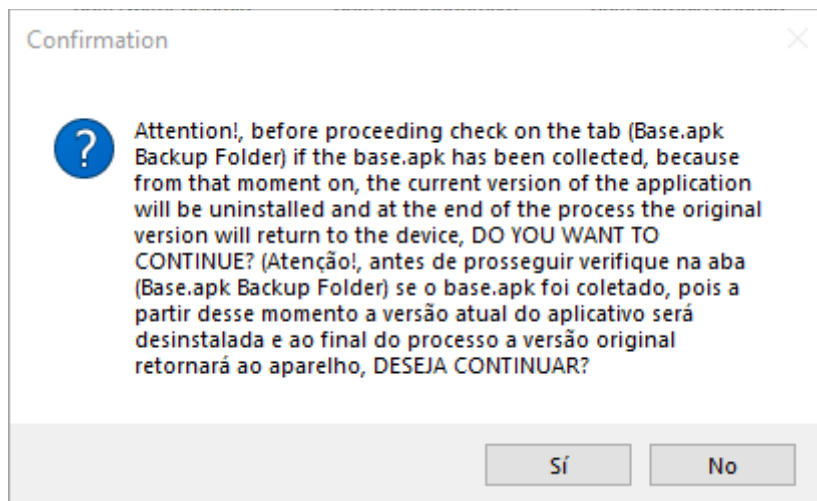


Las aplicaciones que nos aparezcan (al darle al detect), son las que tienen posibilidad de hacer la técnica de downgrade.

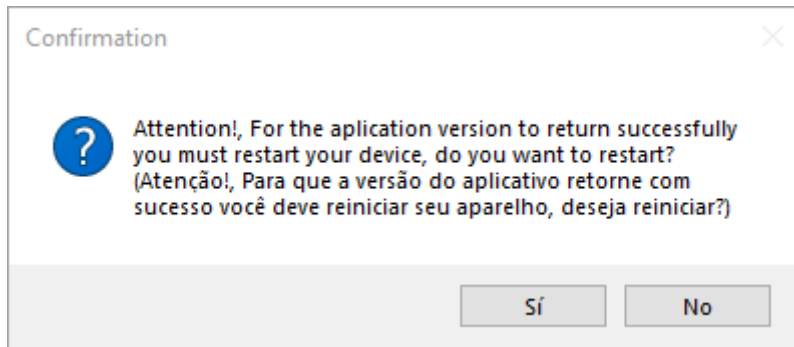
En nuestro caso seleccionaremos Whatsapp y acto seguido haremos clic en Extract.



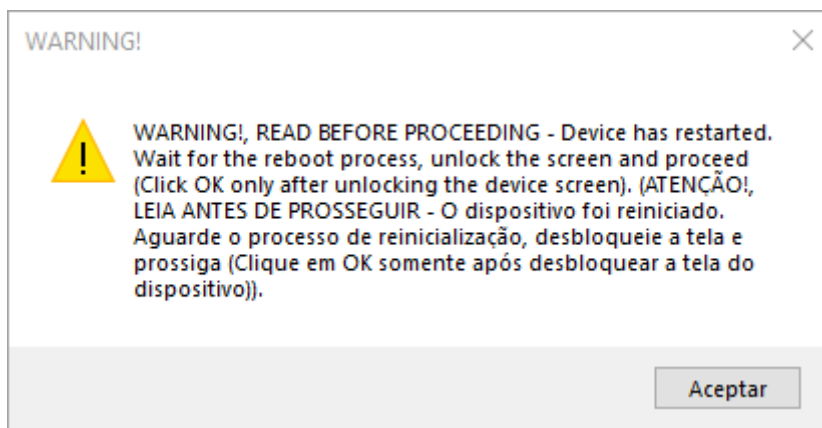
Aceptaremos la siguiente ventana también.



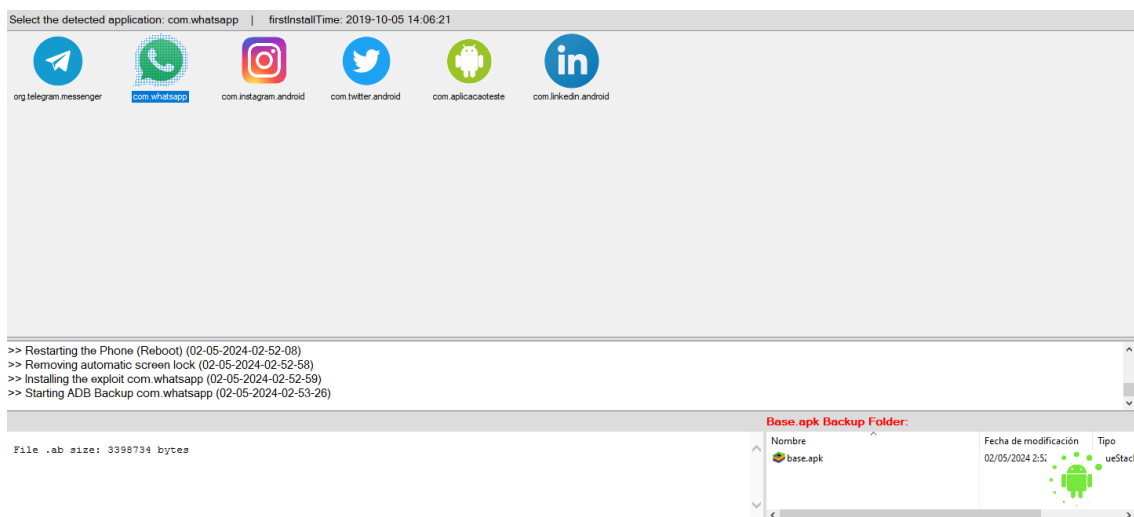
Aceptaremos también este paso, en cuando le daremos a ok, el móvil se reiniciará.



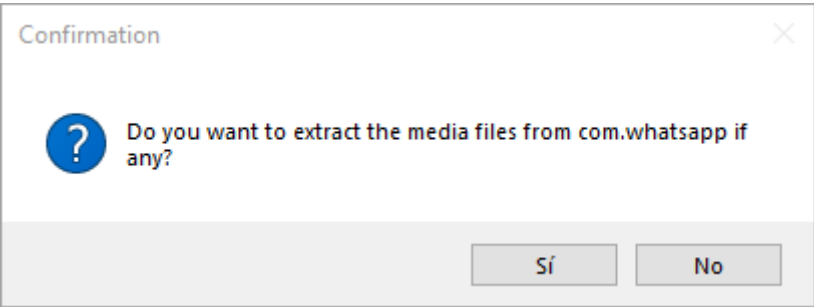
Importante no darle a aceptar al siguiente hasta que el móvil no se haya reiniciado correctamente.



Podemos observar cómo se está copiando toda la APP y sus datos.

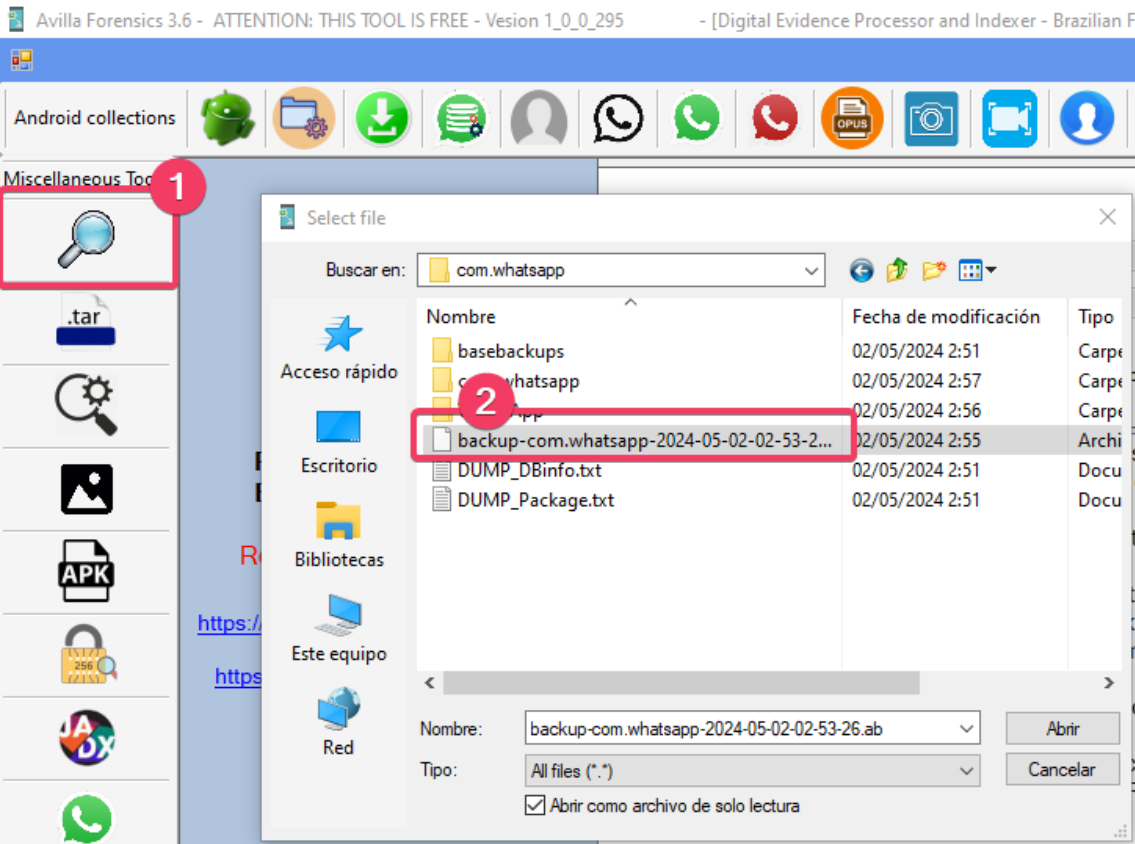


Diremos que si para extraer los archivos.



Se ha realizado correctamente.

<< Forensics-3-6 > acquisitions > Case-02-05-2024-02-51-24 > downgrade > com.whatsapp					Bus
	Nombre	Fecha de modificación	Tipo	Tamaño	
ido	basebackups	02/05/2024 2:51	Carpeta de archivos		
	com.whatsapp	02/05/2024 2:57	Carpeta de archivos		
	WhatsApp	02/05/2024 2:56	Carpeta de archivos		
tos	backup-com.whatsapp-2024-05-02-02-5...	02/05/2024 2:55	Archivo AB	312.009 KB	
	DUMP_DBInfo.txt	02/05/2024 2:51	Documento de te...	1 KB	
DO	DUMP_Package.txt	02/05/2024 2:51	Documento de te...	56 KB	





Select	C:\Forensics-3-6\acquisitions\Case-02-05-2024-02-51-24\downgrade\com.whatsapp\backup-com.whatsapp-2024-05-02-02-53-26.ab
Save to	C:\Users\Usuario\Desktop\Práctica Avila

Vamos a generar un informe completo del backup de la base de datos de whatsapp. Una vez acabado obtenemos lo siguiente.

se-02-05-2024-02-51-24

Nombre	Fecha de modificación	Tipo	Tamaño
iped	02/05/2024 3:06	Carpeta de archivos	11 KB
FileList.csv	02/05/2024 3:07	Archivo de valores...	11 KB
IPED-SearchApp.exe	02/05/2024 3:06	Aplicación	145 KB

Propiedades: iped

General

Tipo: Carpeta de archivos

Ubicación: C:\Users\Usuario\Desktop\Práctica Avila

Tamaño: 693 MB (727.241.763 bytes)

Tamaño en disco: 697 MB (731.230.208 bytes)

Contiene: 1.714 archivos, 159 carpetas

Abrimos el informe.

Este equipo > Escritorio > Práctica Avilla				
	Nombre	Fecha de modificación	Tipo	Tamaño
	iped	02/05/2024 3:06	Carpeta de archivos	
	FileList.csv	02/05/2024 3:07	Archivo de valores...	11 KB
	IPED-SearchApp.exe	02/05/2024 3:06	Aplicación	145 KB
	IPED-SearchApp.log	02/05/2024 3:09	Documento de te...	0 KB

Indicador e Procesador de Evidências Digitais 4.1.3

Case: C:\Users\Usuario\Desktop\Prática Avila\

[No filter]

Filter Listed Duplicates

Clear Filter

Search: (Type or choose the search expression)

Options

Help

F/32

Categories

Evidences

Table

Gallery

Map

Timeline

Links

32

Score

Bookmark

Name

Ext

Type

Size (KB/MB)

Deleted

Category

Created

Modified

Accessed

MetaChanged

TimeRt

1

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

2

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

3

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

4

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

5

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

6

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

7

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

8

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

9

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

10

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

11

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

12

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

13

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

14

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

15

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

16

2%

backup-com.whatsapp-2024...

ab

ab

310.496.513

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

17

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

18

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

19

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

20

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

21

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

22

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

23

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

24

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

25

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

26

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

27

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

28

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

29

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

30

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

31

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

32

2%

backup-com.whatsapp-2024...

ab

ab

10.485.760

false

Other files

05/02/2024 00:53:26 UTC

05/02/2024 00:55:02 UTC

05/02/2024 01:06:59 UTC

2024-04-25 04:00

Bookmarks

Metadata

No hits

Attachments/Subitems

Parent Item

Duplicates

Referencing

Referenced By

Hex

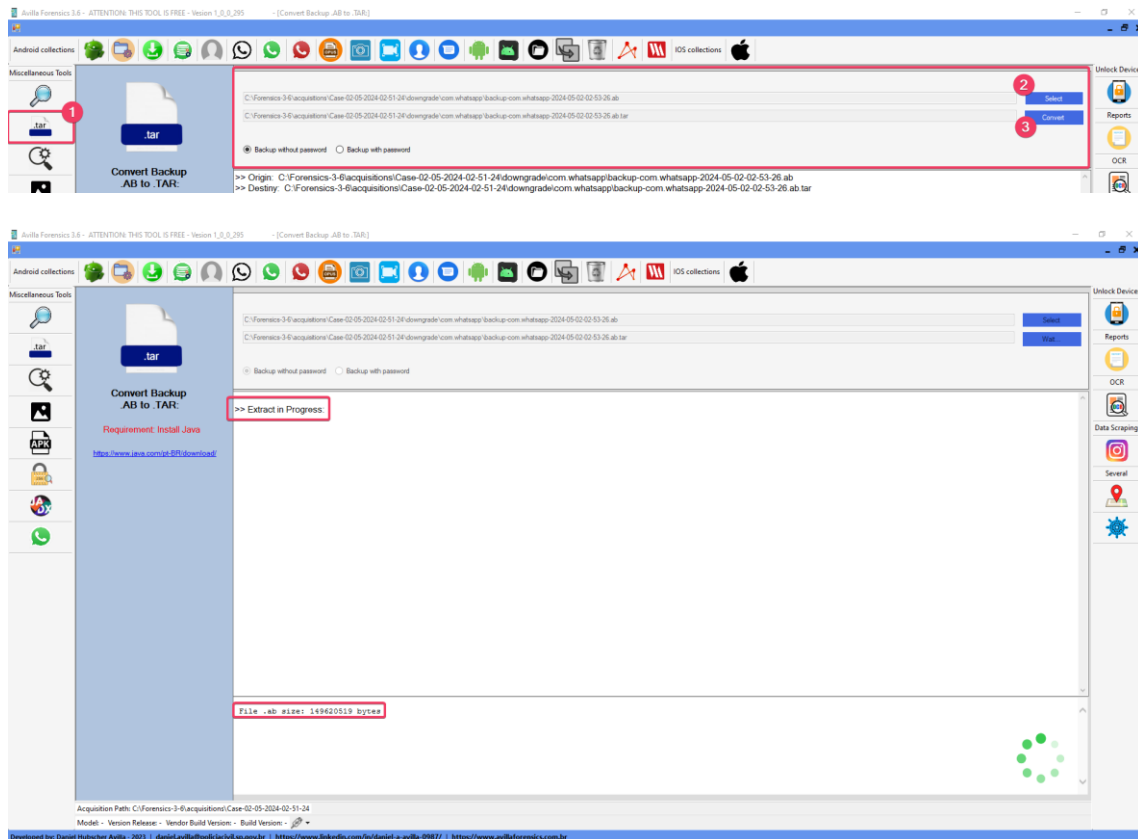
Text

Metadata

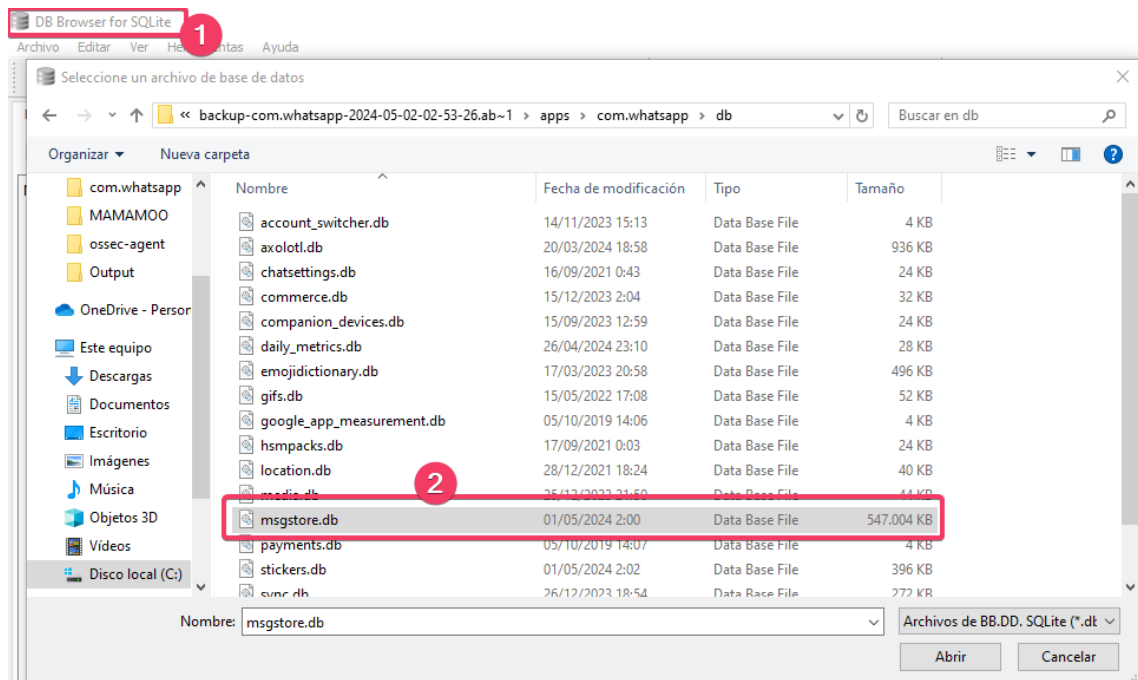
Preview

Bookmarks

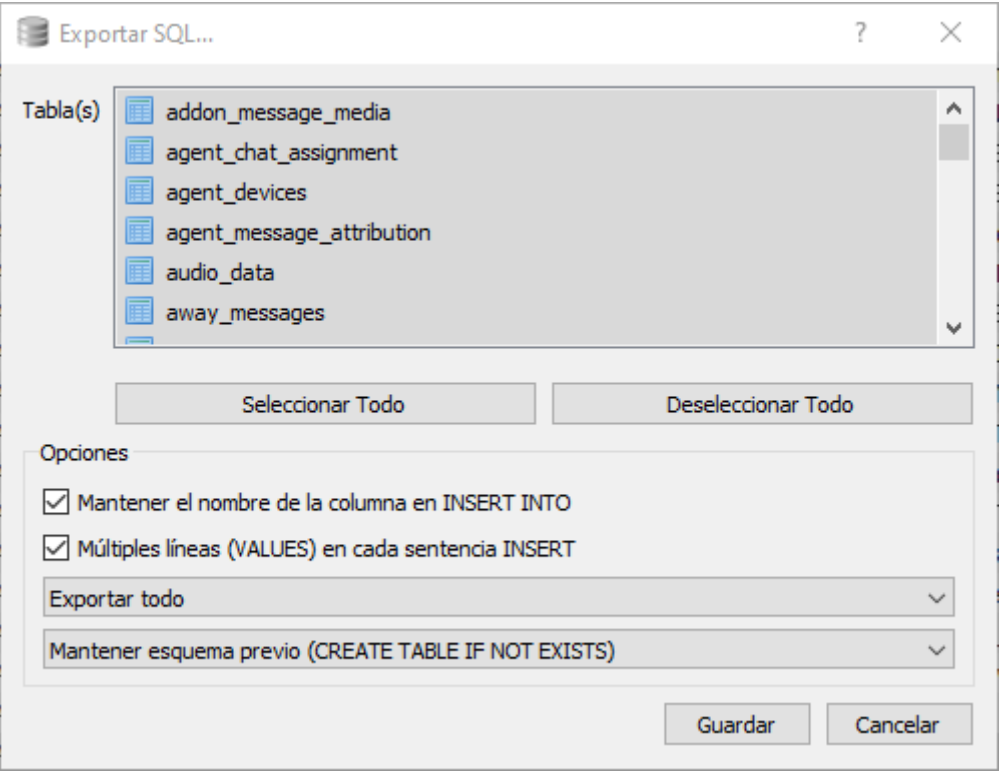
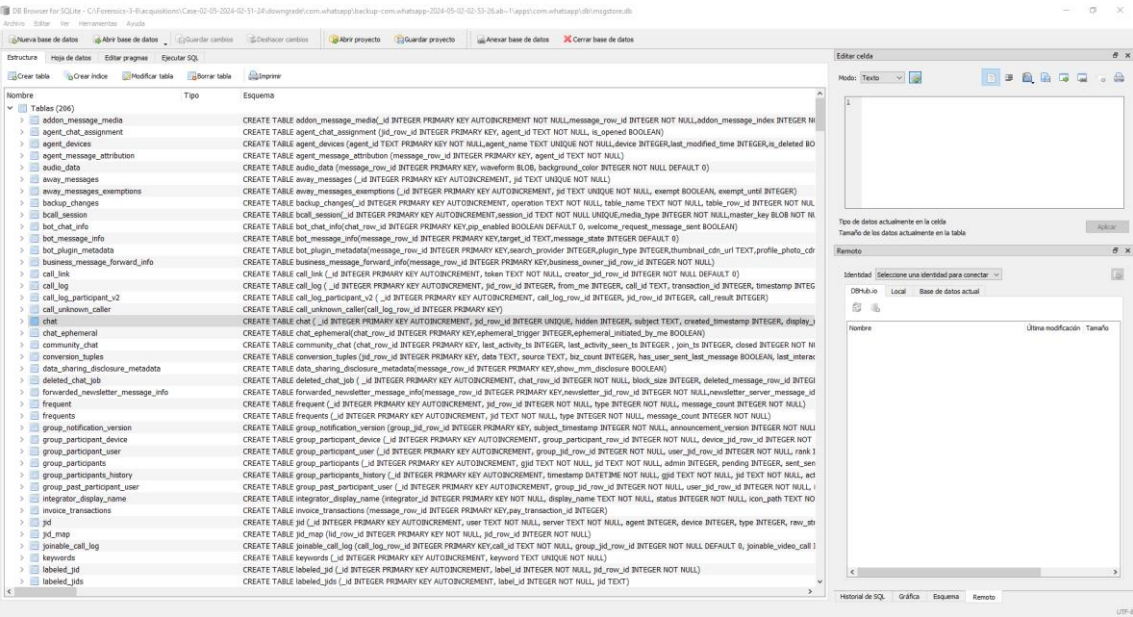
[No Bookmarks]

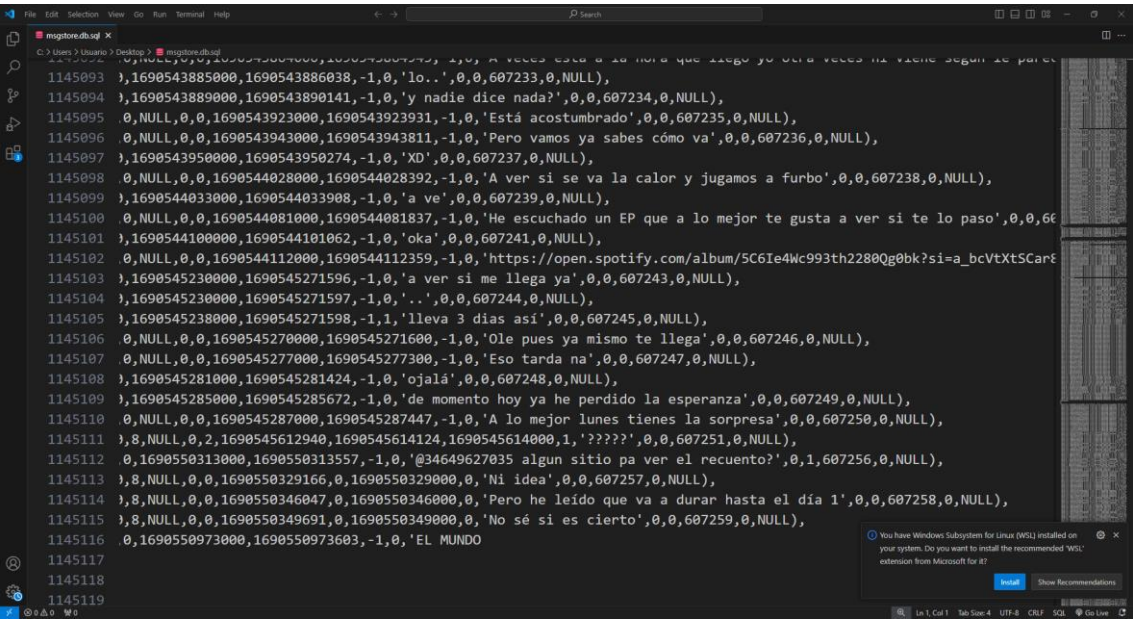


Vamos a abrir la base de datos con SQLite browser.









Ahora vamos a indexar y procesar evidencias del ab.tar

Indexador e Processador de Evidências Digitais 4.1.3				Processing 68469 / 69263 - Finish in 0h 0m 0s		Preview Case	Pause
Statistics		Task Times		Parser Times		Current Items	
Processing Time	0h 2m 29s	SkipCommittedTask	0s 0%	CompressorParser	0s 0%	Worker-0	Parsin
Estimated Finish	-	IgnoreHardLinkTask	0s 0%	EXEParse	0s 1%	Worker-1	Parsin
Average Speed	14 GB/h	TempFileTask	- -	HtmlParser	1s 4%	Worker-2	Graph
Current Speed	1 GB/h	HashTask	3s 3%	ImageParser	0s 0%	Worker-3	Langu
Volume Found	631 MB	SignatureTask	2s 2%	JPEGParser	1s 6%	Worker-4	Regex
Volume Processed	631 MB	SetTypeTask	0s 0%	PackageParser	6s 21%	Worker-5	Langu
Items Found	69,321	SetCategoryTask	0s 0%	RawStringParser	6s 19%	Worker-6	Parsin
Items Processed	68,516	RefineCategoryTask	4s 5%	SQLite3Parser	1s 4%	Worker-7	Index
Actual Items Processed	1	HashDBLookupTask	- -	TextAndCSVParser	1s 4%		
Subitems Processed	69,319	DuplicateTask	0s 0%	VCardParser	0s 0%		
Carved Items	0	AudioTranscriptTask	- -	WebpParser	1s 4%		
Carved Discarded	0	VideoThumbTask	0s 0%	WhatsAppParser	4s 15%		
Exported Items	68,519	ParsingTask	31s 37%	XMLParser	0s 1%		
Ignored Items	0	QRCodeTask	- -				

## Conversación de Whatsapp.

The screenshot displays the 'Indicador e Procesador de Evidencias Digitales 4.1.3' software interface. The top section shows a list of files with columns for Name, Ext, Type, Size (KB/MB), Deleted, Category, Created, Modified, Accessed, MetaChanged, and Hash. The files are categorized under 'WhatsApp Group - nos vemos'. Below the file list, the 'Bookmarks' section shows 'Probably Shared By WhatsApp (283)'. The main preview area shows a chat conversation with a contact named 'Nathan (34673135717@cs.whatsapp.net)'. The chat includes a text message '[Chat continuation.]', a date separator '2022-09-02', and a photo of a person. The bottom status bar shows the file path: 'back-up-whatsapp-2024-05-02-03-29-07.ab.tar=appscom.whatsapp\miguelpere-120363038130649385'.

## Multimedia.

The screenshot displays the 'Indicador e Procesador de Evidencias Digitales 4.1.3' software interface. The top section shows a list of files with columns for Name, Ext, Type, Size (KB/MB), Deleted, Category, Created, Modified, Accessed, MetaChanged, and Hash. The files are categorized under 'WhatsApp Group - nos vemos'. Below the file list, the 'Bookmarks' section shows 'Probably Shared By WhatsApp (283)'. The main preview area shows a large image of a cat. The bottom status bar shows the file path: 'back-up-whatsapp-2024-05-02-03-29-07.ab.tar=appscom.whatsapp\miguelpere-120363038130649385'.





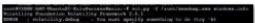




Downgrade de Telegram.

Ahora vamos a hacer exactamente lo mismo para la aplicación telegram, en este caso no documentaré los pasos, ya que los voy a repetir, simplemente sacaré captura de algunos momentos clave.

← → ↕ ⬆ ⬇ « acquisitions » Case-02-05-2024-04-13-31 » downgrade » org.telegram.messenger 🔍 Buscar en c				
★ Acceso rápido Escritorio Descargas Documentos Imágenes	Nombre	Fecha de modificación	Tipo	Tamaño
	basebackups	02/05/2024 4:14	Carpeta de archivos	
	org.telegram.messenger	02/05/2024 4:16	Carpeta de archivos	
	backup-org.telegram.messenger-2024-0...	02/05/2024 4:15	Archivo AB	27.544 KB
	DUMP_DBinfo.txt	02/05/2024 4:14	Documento de te...	1 KB
	DUMP_Package.txt	02/05/2024 4:14	Documento de te...	37 KB

Después de convertirlo en tar

← → ↕ ⬆ ⬇ « apps » org.telegram.messenger » db 🔍 Buscar en db				
★ Acceso rápido Escritorio Descargas	Fecha de modificación	Nombre	Tipo	Tamaño
	16/10/2023 21:38	com.google.android.datatransport.events	Archivo EVENTS	56 KB
	16/10/2023 21:38	com.google.android.datatransport.events-journal	Archivo EVENTS-J...	9 KB

← → ↕ ⬆ ⬇ « apps » org.telegram.messenger » ef » Telegram » Telegram Images 🔍 Buscar en Telegram Images				
★ Acceso rápido Escritorio Descargas Documentos Imágenes com.whatsapp MAMAMOO ossec-agent Output OneDrive - Personal Este equipo Descargas Documentos Escritorio Imágenes Música Objetos 3D Videos Disco local (C:) HDD (E:) Nuevo vol (K:)				
	-5879672626518015399_121.jpg	-5879672626518015400_121.jpg	-5900276903191888506_121.jpg	
				
	-5900276903191888511_121.jpg	-5900276903191888522_120.jpg	-5900276903191888523_109.jpg	
				
	-5900276903191888527_121.jpg	-5900276903191888529_120.jpg	-5900276903191888533_121.jpg	

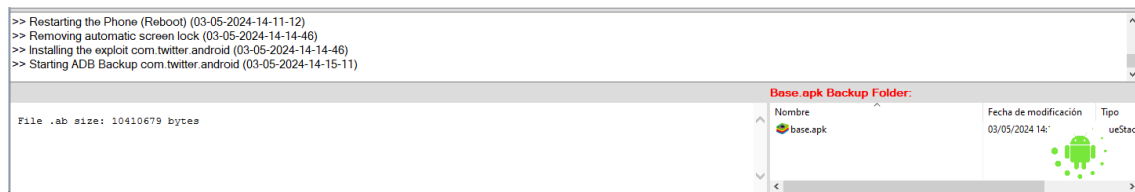
He decidido que no voy a usar telegram, ya que creo que no está funcionando, no me está sacando la base de datos.



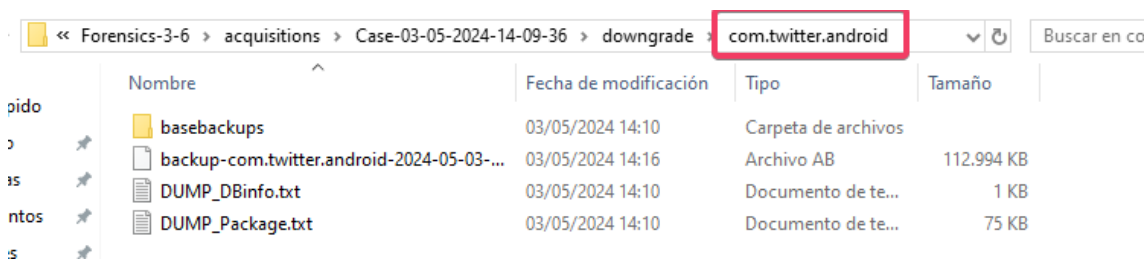
## Downgrade de Twitter.



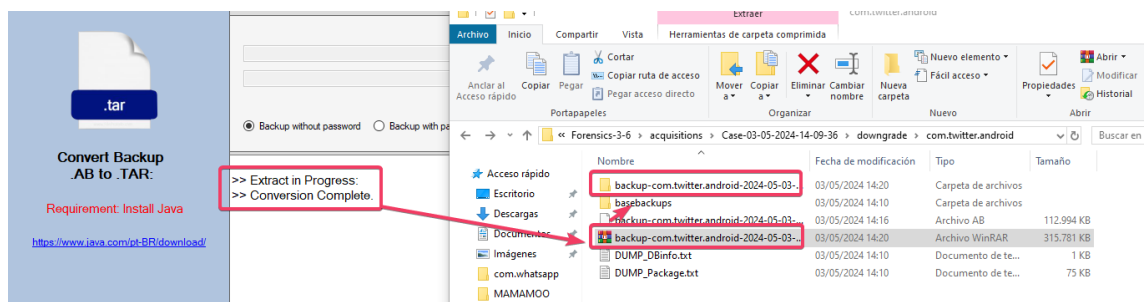
Estamos copiando los datos después del reinicio y de dar permisos a la aplicación.



Aquí tenemos ya los archivos.



Extracción completada.



No he encontrado nada relevante de información en las bases de datos, hay muchísimas y casi todas no tienen información: <https://i.imgur.com/KadJEb6.gif>

Al sacar el informe del .tar tampoco encuentra nada relevante.

SelectC:\Forensics-3-6\acquisitions\Case-03-05-2024-14-09-36\downgrade\com.twitter.android\backup-com.twitter.android-2024-05-03-14-15-11.ab.tar

Saves toC:\Users\Usuario\Desktop\AvilaTwitter

What...Index fileIndex folderDefault folderC:\Forensics-3-6\IPED-4.1.3\_and\_plugins\iped-4.1.3Change

IPED - Digital Evidence Processor and Indexer (translated from Portuguese) is a tool implemented in java and originally and still developed by digital forensic experts from Brazilian Federal Police since 2012. Although it was always open source, only in 2019 its code was officially published.

Since the beginning, the goal of the tool was efficient data processing and stability. Some key characteristics of the tool are:

Command line data processing for batch case  
Multiplatform support, tested on Windows and Linux  
Portable cases without installation, you can run it from a USB drive  
Integrated and intuitive analysis interface  
High multithread performance and support for large files

Currently IPED uses the Sleuthkit Library only to process raw images and UDF (Cellebrite format) AD1 (AccessData) and UDFR (Cellebrite format) files.

>> Origin: C:\Forensics-3-6\acquisitions\Case-03-05-2024-14-09-36\downgrade\com.twitter.android\backup-com.twitter.android-2024-05-03-14-15-11.ab.tar  
>> Destiny: C:\Users\Usuario\Desktop\AvilaTwitter\report.html  
>> IPED indexing started.

on items in a (multi) case as of 12/12/2019

RAW/DD, E01, EX01, ISO9660, AFF, VHD, VMDK. Also there is support for UDF(ISO), Sleuthkit.

2024-05-03-14-15-11.ab.tar

Nombre	Fecha de modificación	Tipo	Tamaño
iped	03/05/2024 14:18	Carpeta de archivos	5 KB
FileList.csv	03/05/2024 14:19	Archivo de valores...	145 KB
IPED-SearchApp.exe	03/05/2024 14:18	Aplicación	18 KB
IPED-SearchApp.log	03/05/2024 14:33	Documento de te...	

Indicador e Processador de Evidências Digitais 4.1.3 [Case: C:\Users\Usuario\Desktop\AvilaTwitter]

[No filter]

Filter Listed Duplicates

Clear Filter

Search [Type or choose the search expression]

Options

Help

Categories

Other files (13)

	Score	Bookmark	Name	Ext	Type	Size (110MB)	Deleted	Category	Created	Modified	Accessed	MetaChanged	TimeStamp
1	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
2	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
3	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
4	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
5	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
6	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
7	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
8	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
9	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
10	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
11	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11
12	4%		backup-com.twitter.android-2...	ab	ab	10,485,760	false	Other files	05/03/2024 12:15:11 UTC	05/03/2024 12:16:23 UTC	05/03/2024 12:18:50 UTC		2024-05-03 14:15:11

Bookmarks

Metadata

[No Bookmarks]

Basic Properties

namebackup-com.twitter.android-2024-05-03-14-15-11.ab\_9

size10,485,760

extab\_9

typetwitter

deletedfalse

category[Other files]

createdFri May 03 14:16:11 CEST 2024

modifiedFri May 03 14:16:23 CEST 2024

accessedFri May 03 14:18:50 CEST 2024

pathbackup-com.twitter.android-2024-05-03-14-15-11.ab>backup-com.twitter.android-2024-05-03-14-15-11.ab\_9