



---

# ANÁLISIS FORENSE

---

Unidad 1. Actividad 2



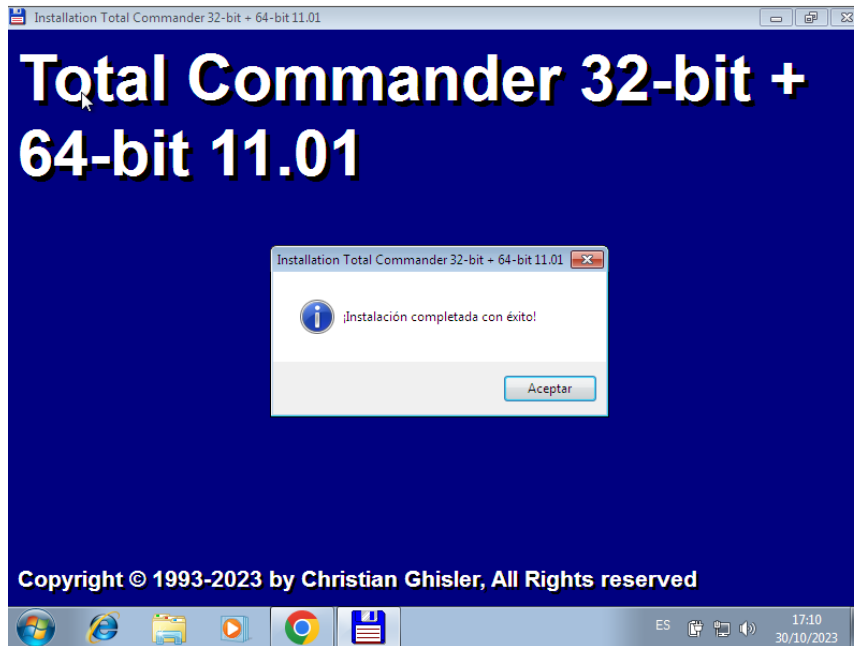
4 DE OCTUBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

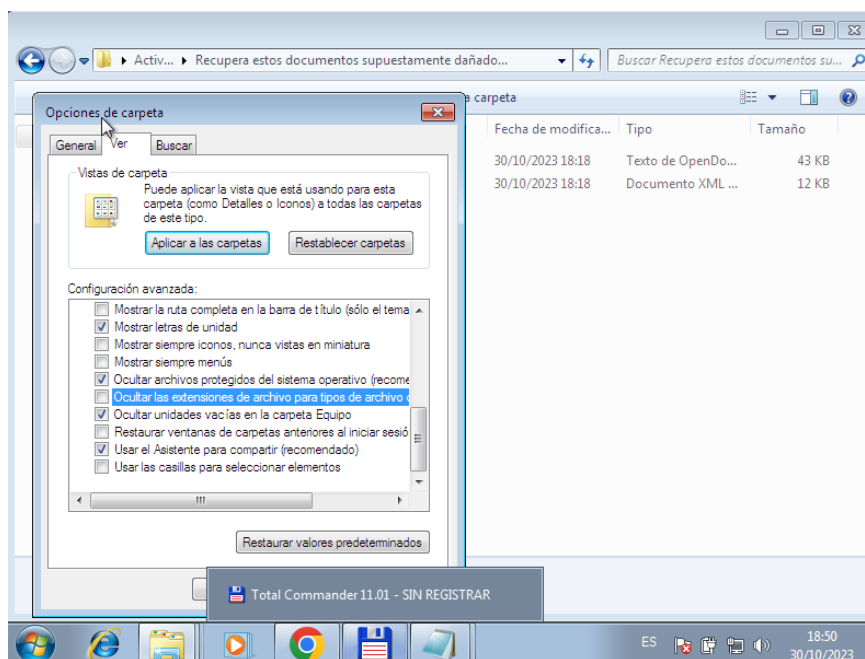
Ejercicio 1 .....	2
Ejercicio 2 .....	<b>¡Error! Marcador no definido.</b>
Ejercicio 3 .....	<b>¡Error! Marcador no definido.</b>
Ejercicio 4 .....	13

## Ejercicio 1.

Instalamos total commander:



Para que no se nos oculten las extensiones de los archivos:



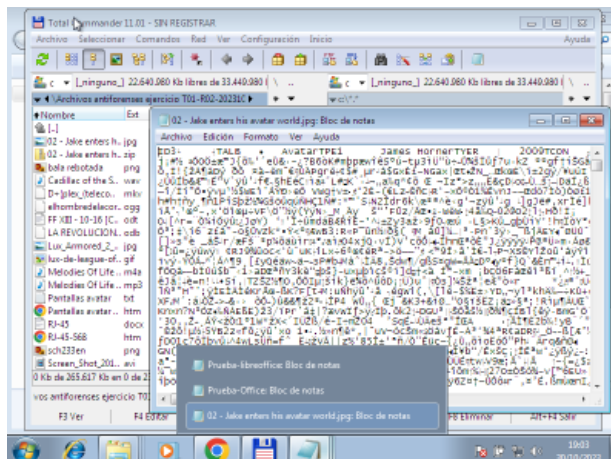
Al extraerlo podemos ver todos estos archivos:

Archivos antiforenses ejercicio T01-R02-20231030

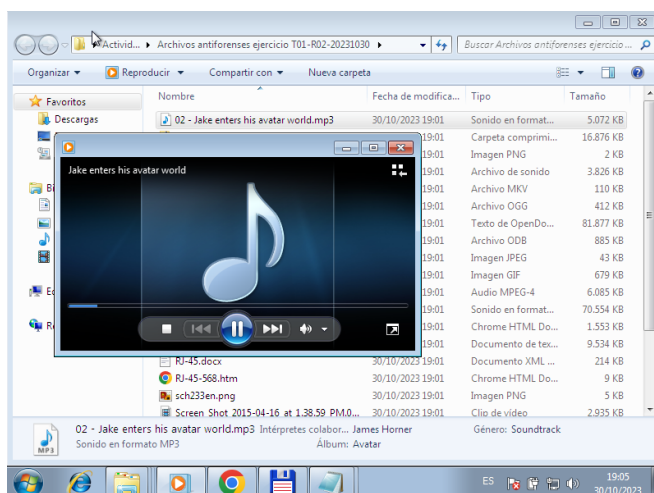
Buscar Archivos antiforenses ejercicio ...

Nombre	Fecha de modifica...	Tipo	Tamaño
02 - Jake enters his avatar world.jpg	30/10/2023 19:01	Imagen JPEG	5.072 KB
02 - Jake enters his avatar world.zip	30/10/2023 19:01	Carpeta compri...	16.876 KB
bala rebotada.png	30/10/2023 19:01	Imagen PNG	2 KB
Cadillac of the Skies.wav	30/10/2023 19:01	Archivo de sonido	3.826 KB
D+Jplex_(telecomunicaciones).mkv	30/10/2023 19:01	Archivo MKV	110 KB
elhombredelacordeoncolmar1.ogg	30/10/2023 19:01	Archivo OGG	412 KB
FF XIII - 10-16 [CGI].odt	30/10/2023 19:01	Texto de OpenDo...	81.877 KB
LA REVOLUCION TECNICA QUE SUPUSO ...	30/10/2023 19:01	Archivo ODB	885 KB
Lux_Armored_2_Render.jpg	30/10/2023 19:01	Imagen JPEG	43 KB
lux-de-league-of-legends-wild-rift-6493....	30/10/2023 19:01	Imagen GIF	679 KB
Melodies Of Life - (English) - Final Fantas...	30/10/2023 19:01	Audio MPEG-4	6.085 KB
Melodies Of Life - (English) - Final Fantas...	30/10/2023 19:01	Sonido en format...	70.554 KB
Pantallas avatar XviD.htm	30/10/2023 19:01	Chrome HTML Do...	1.553 KB
Pantallas avatar.txt	30/10/2023 19:01	Documento de tex...	9.534 KB
RJ-45.docx	30/10/2023 19:01	Documento XML ...	214 KB
RJ-45-568.htm	30/10/2023 19:01	Chrome HTML Do...	9 KB
sch233en.png	30/10/2023 19:01	Imagen PNG	5 KB
Screen Shot 2015-04-16 at 1.38.59 PM.0...	30/10/2023 19:01	Clip de vídeo	2.935 KB

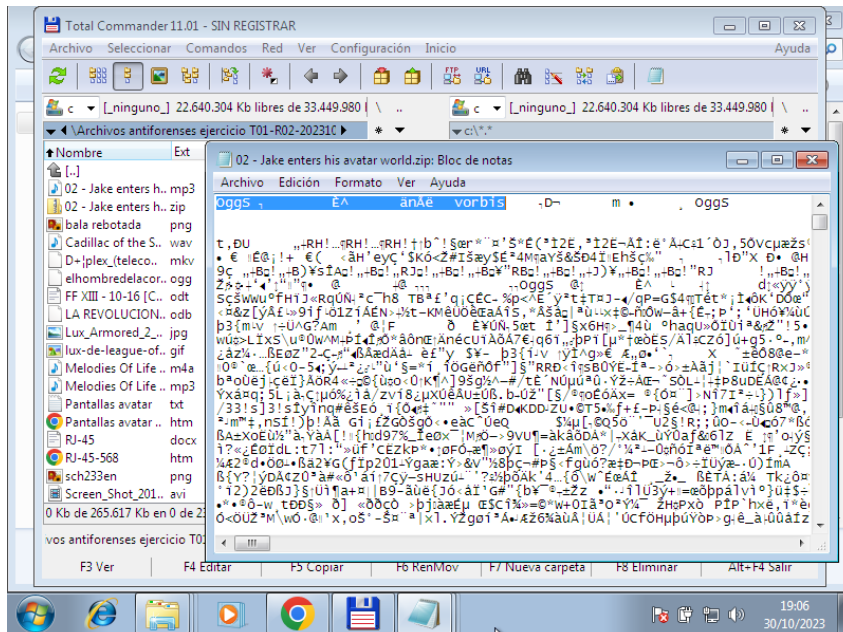
Vamos a empezar por el primero:



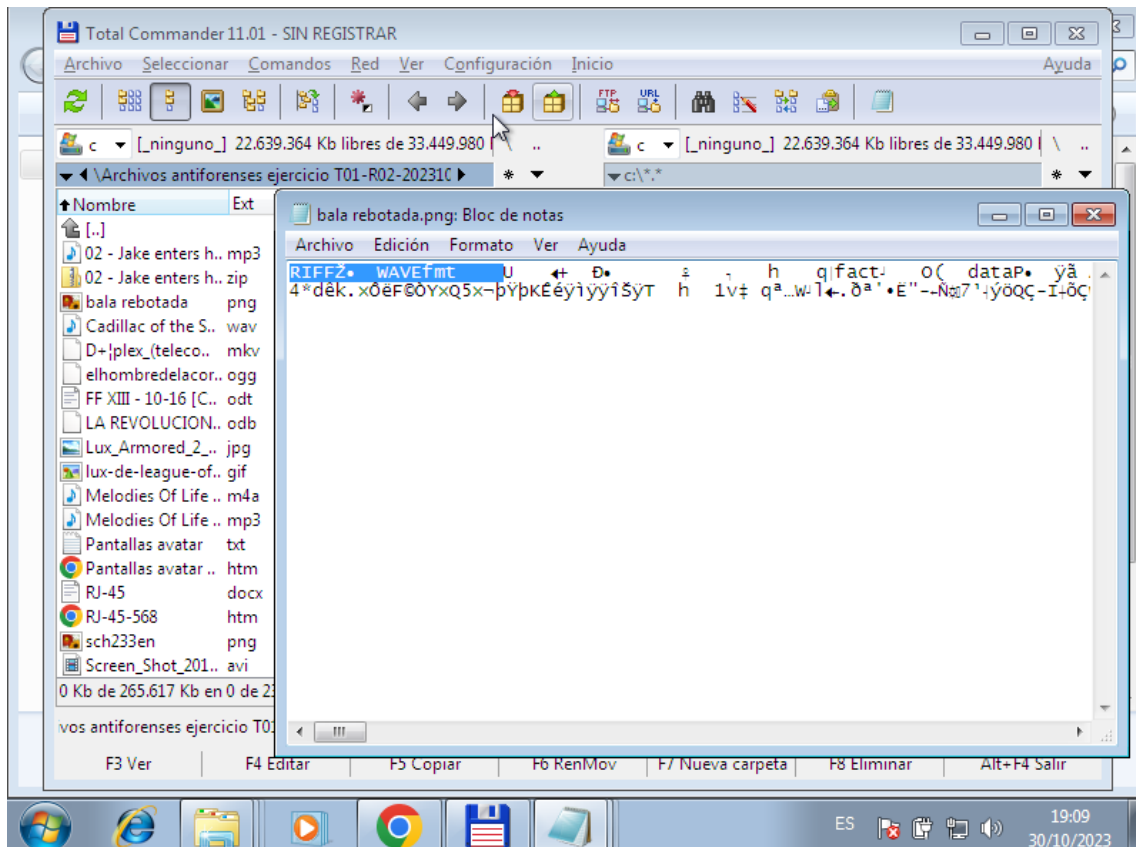
Como vemos tiene de cabecera ID3, por tanto es un MP3, se puede comprobar cambiándole la extensión:



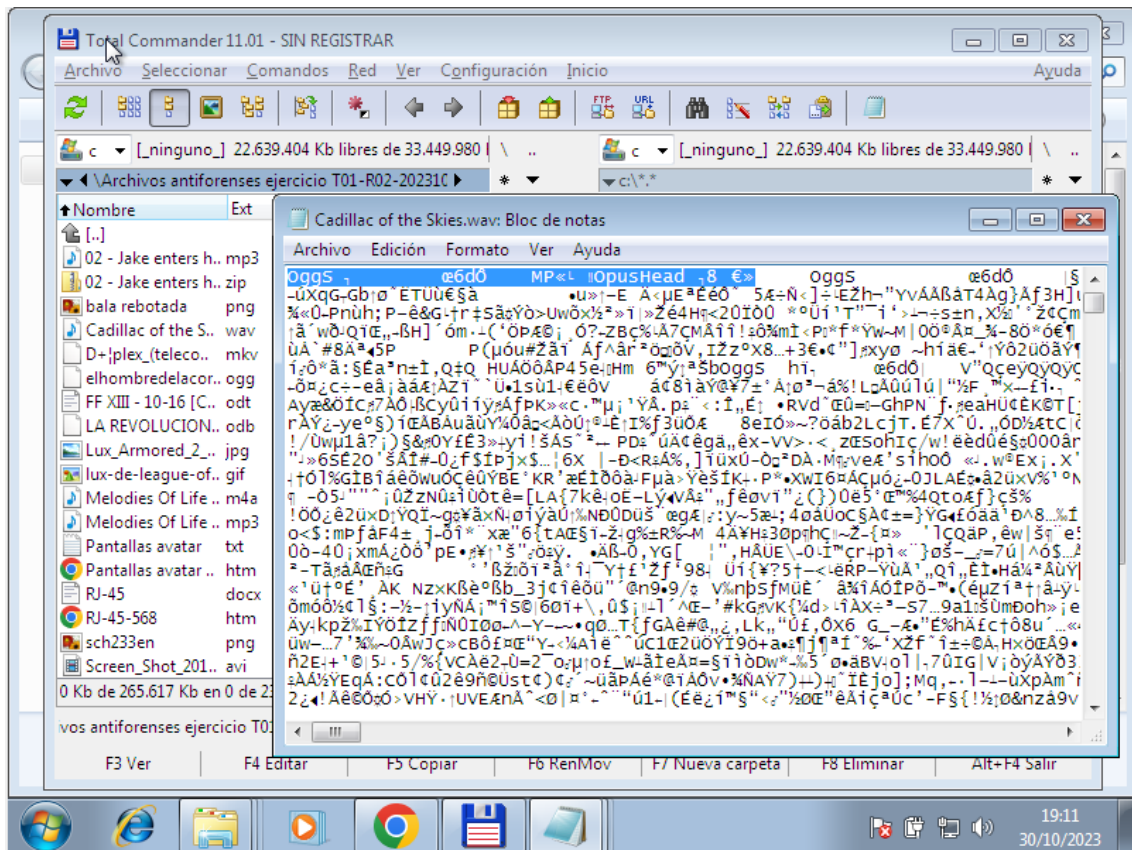
El siguiente es un archivo .ogg, ya que en su comienzo lleva el identificador OggS seguido de un número variable de datos binarios y la palabra vorbis:



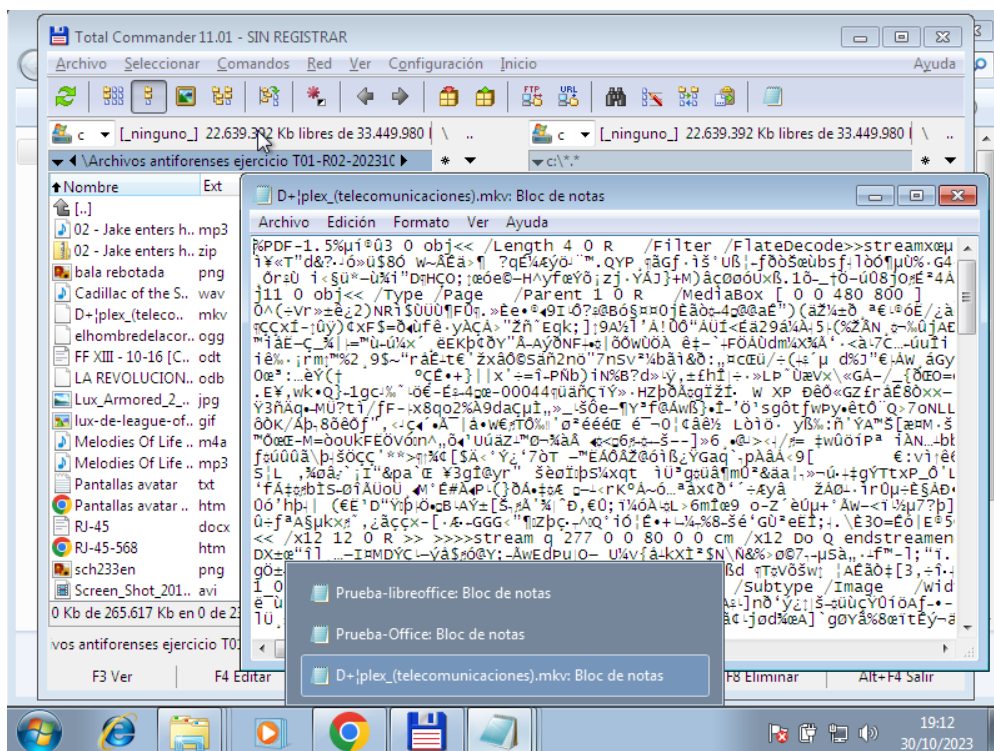
El siguiente tiene una Cabecera de archivos .wav ya que en el comienzo lleva los identificadores RIFF y la palabra WAVE separadas por un grupo de datos binarios:



El siguiente es de una cabecera de archivos .opus ya que en su comienzo lleva el identificador OggS seguido de un número variable de datos binarios y la palabra OpusHead

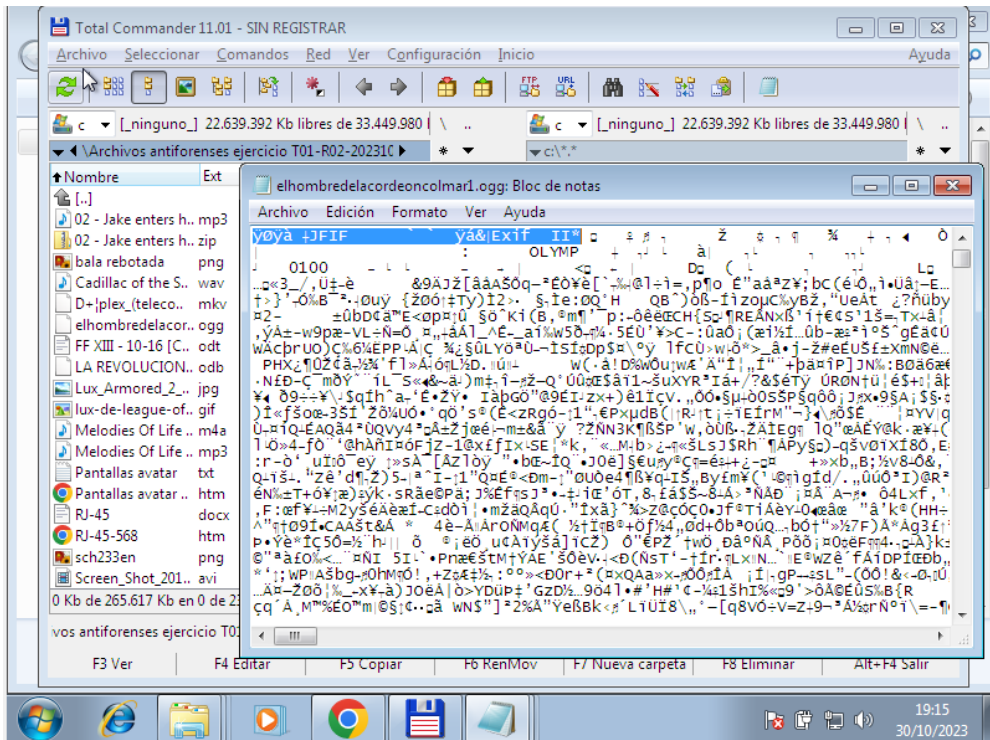


El siguiente es una cabecera de archivos .pdf realizada con Libreoffice Writer. En su comienzo lleva el identificador PDF seguido de un número indicando la versión del codificador usado por writer para crear el pdf, en este ejemplo es la versión 1.5

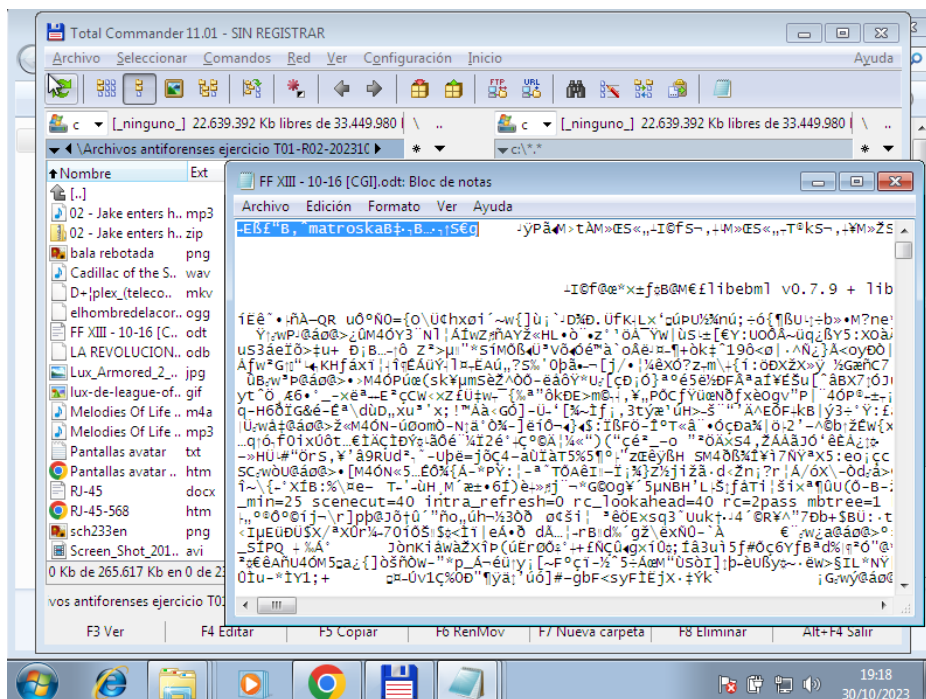




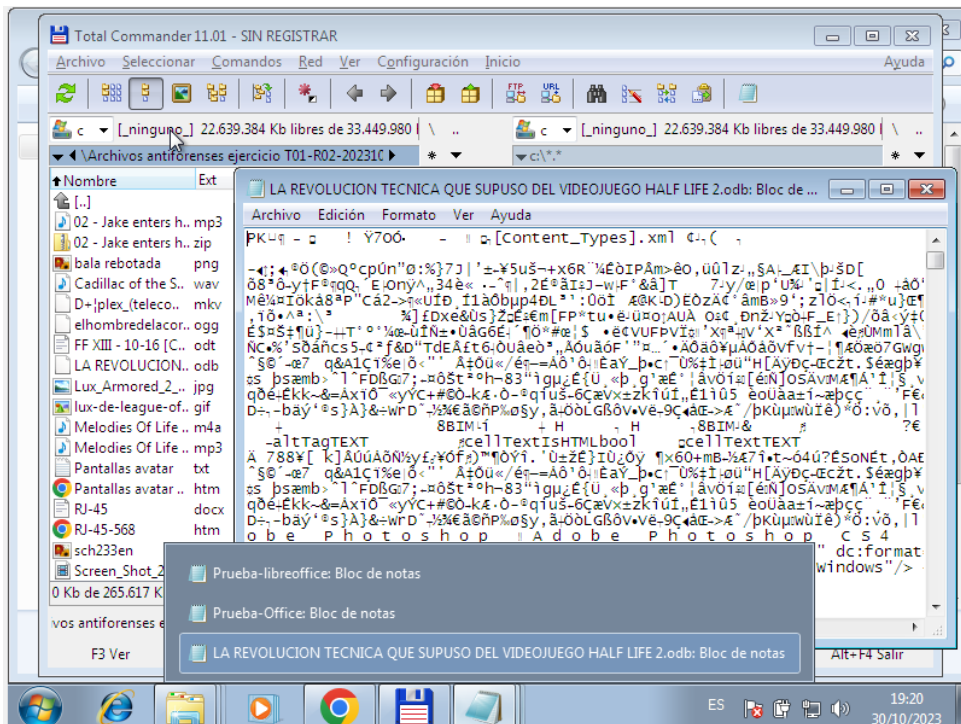
El siguiente es una cabecera de archivos .jpg y también .jpeg . En su comienzo lleva el identificador JFIF y puede que datos acerca del programa que lo creó, la calidad de la imagen, etc.



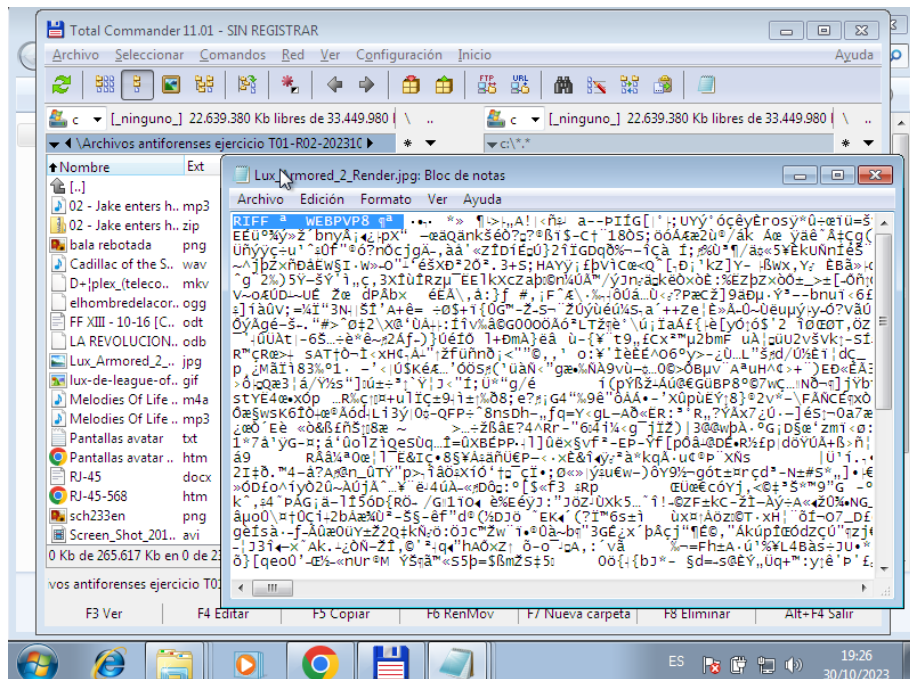
El siguiente es una cabecera de archivos .mkv. Precedida de un número indeterminado de datos binarios, encontraremos la palabra matroska ya que mkv es la abreviatura de Matroska Video:



La siguiente es una cabecera de archivos .docx de Microsoft Word. En el comienzo lleva los identificadores PK y la palabra doc precedida de un grupo de puntos suspensivos

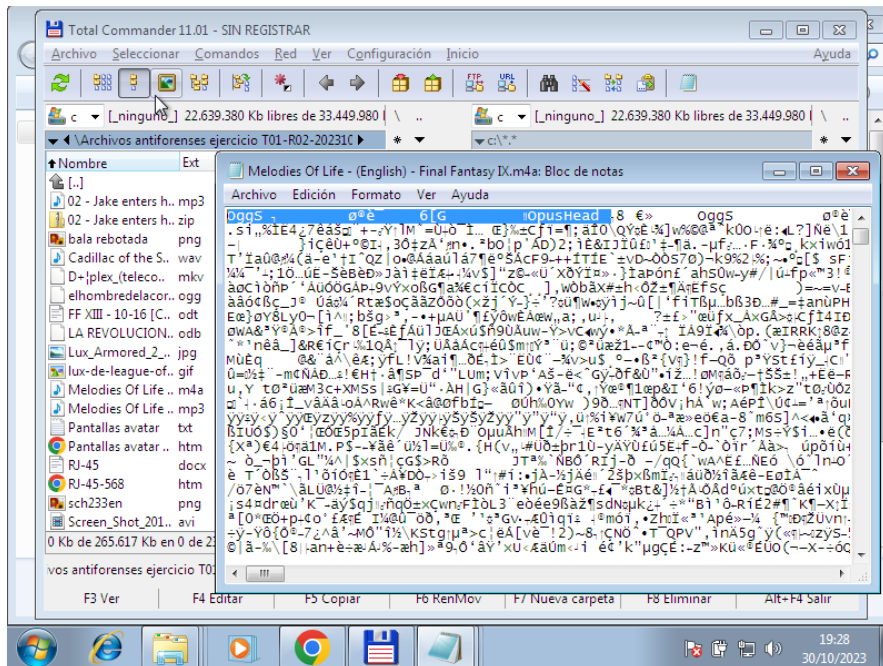


El siguiente tiene una Cabecera de archivos .wav ya que en el comienzo lleva los identificadores RIFF y la palabra WAVE separadas por un grupo de datos binarios:

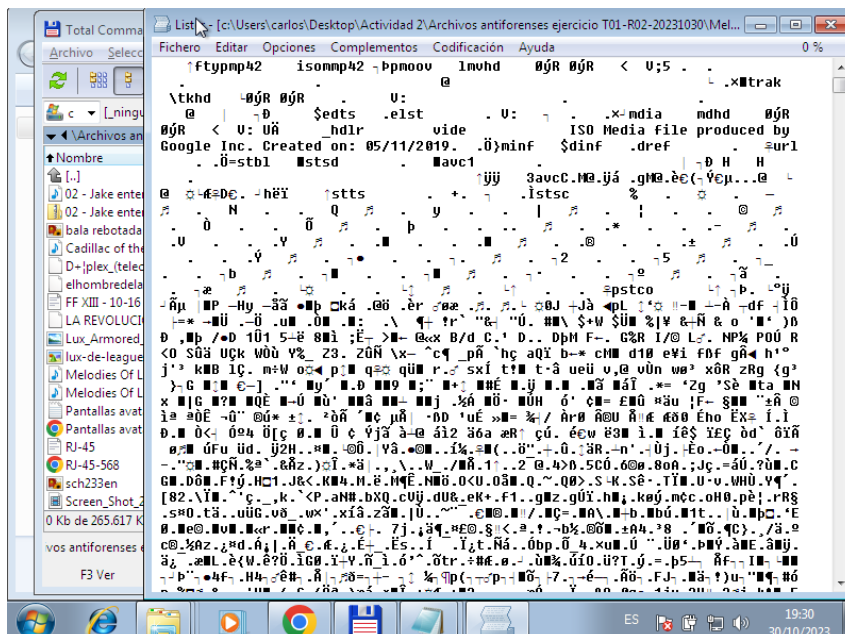




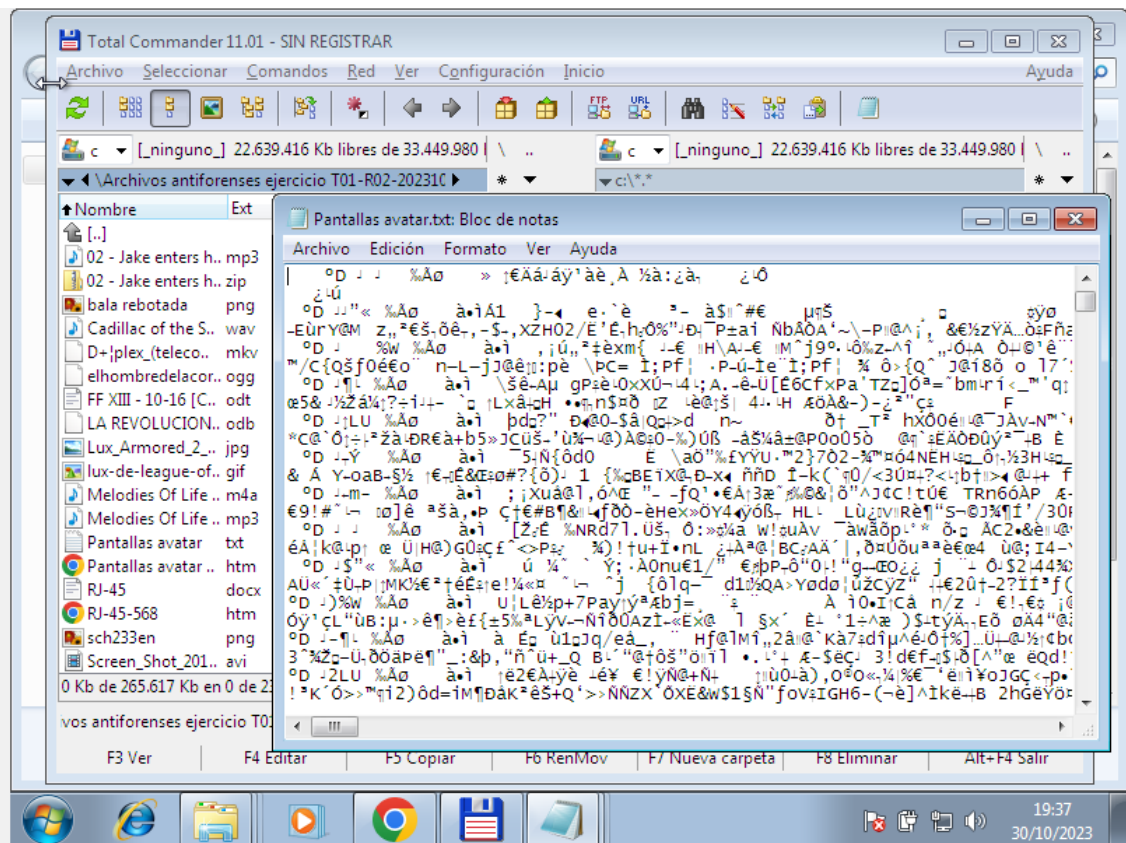
El siguiente es de una cabecera de archivos .opus ya que en su comienzo lleva el identificador OggS seguido de un número variable de datos binarios y la palabra OpusHead:



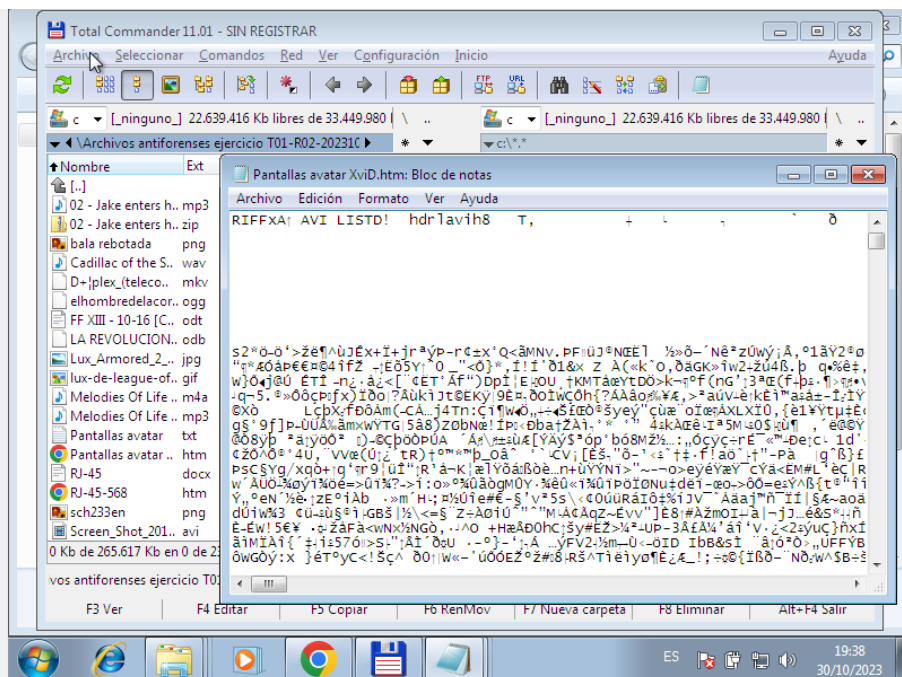
El siguiente es una cabecera de archivos .mp4 En su comienzo, acompañada de otras palabras, lleva el identificador isonmp42 donde avc1 es el nombre técnico que recibe el codificador mp4.



El siguiente es una abecera de archivos .bmp En el comienzo lleva el identificador BM



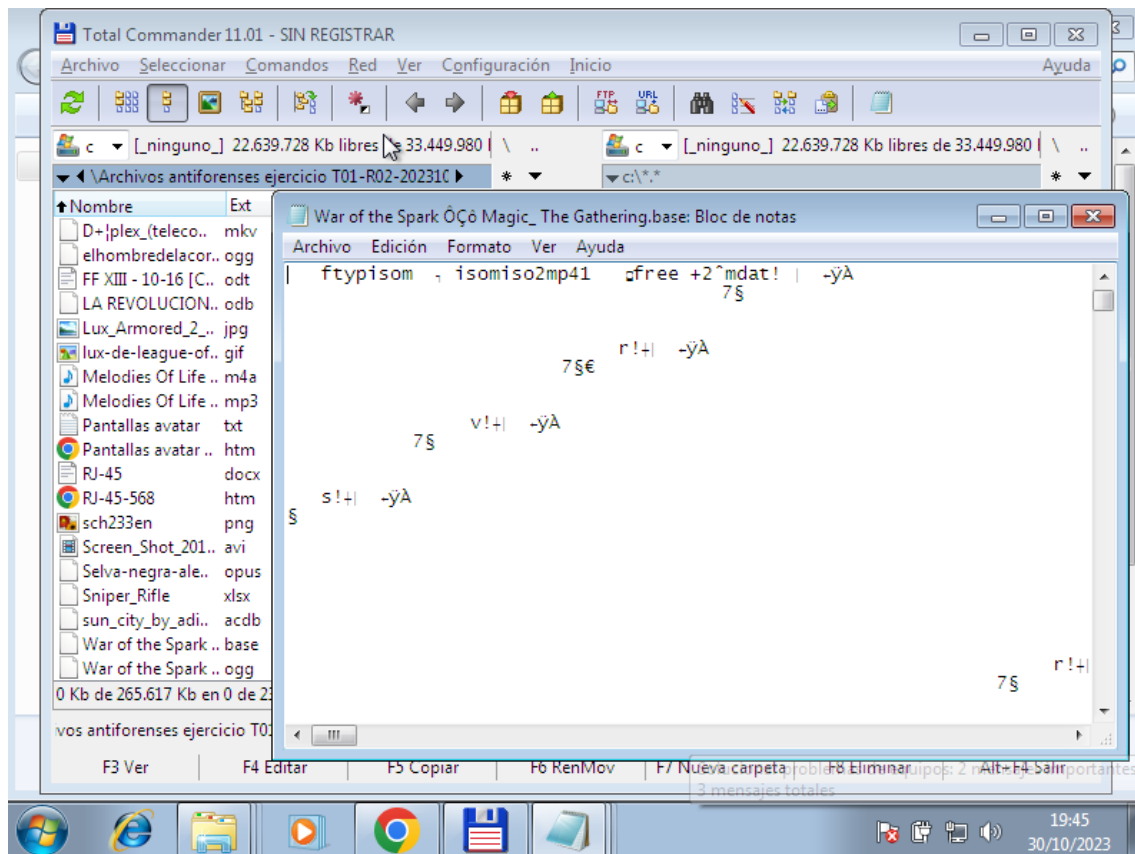
El siguiente es una cabecera de archivos .avi En el comienzo lleva los identificadores RIFF y la palabra AVI precedida de un grupo más o menos grande de datos binarios.



The screenshot shows a Windows XP desktop environment. The primary application is Total Commander 11.01, which is displaying a directory listing of files and folders. The files include various image formats (jpg, png, avi), audio files (mp3, ogg), and documents (txt, docx, htm). A secondary window, titled 'RJ-45-568.htm: Bloc de notas', is open in the foreground, displaying a block of text that appears to be a mix of characters, possibly a mix of Spanish and English, with some characters appearing to be encoded or garbled. The taskbar at the bottom shows the Start button, several open application icons, and the system clock indicating the time as 19:41 on 30/10/2023.

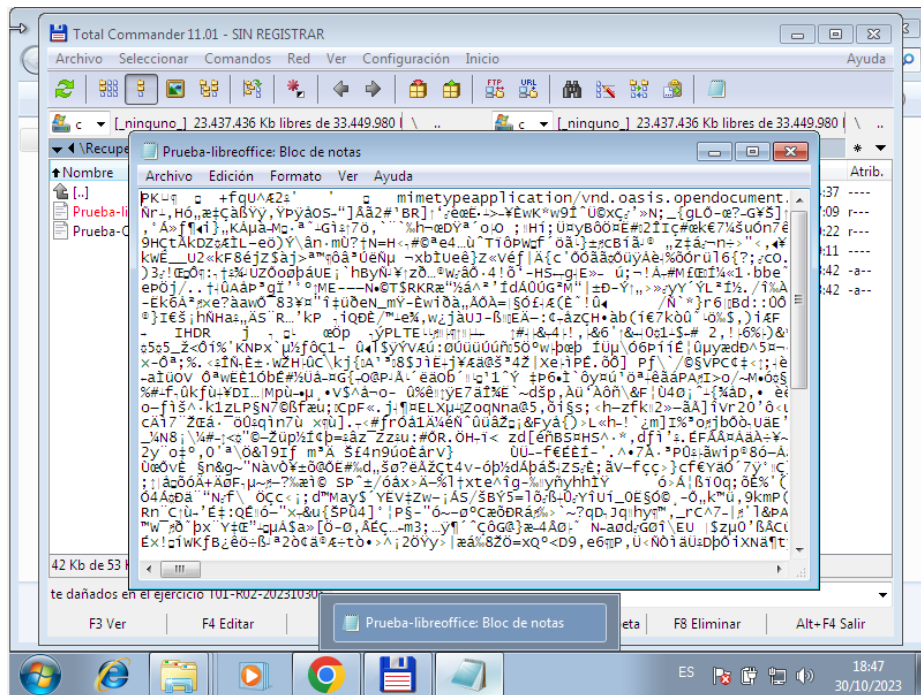
[illegible]

El siguiente es una cabecera de archivos .mp4 En su comienzo, acompañada de otras palabras, lleva el identificador isomiso2mp41 donde avc1 es el nombre técnico que recibe el codificador mp4.

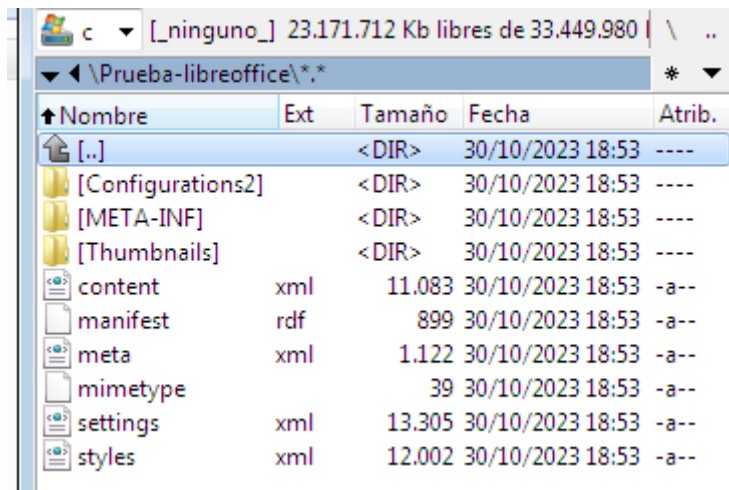


## Ejercicio 2

Los archivos PK son archivos .zip, por tanto vamos a cambiarles la extensión y a exportarlos.



Vamos a empezar por el archivo 1, llamado Prueba-libreoffice:



En el archivo content podemos ver el contenido del archivo:

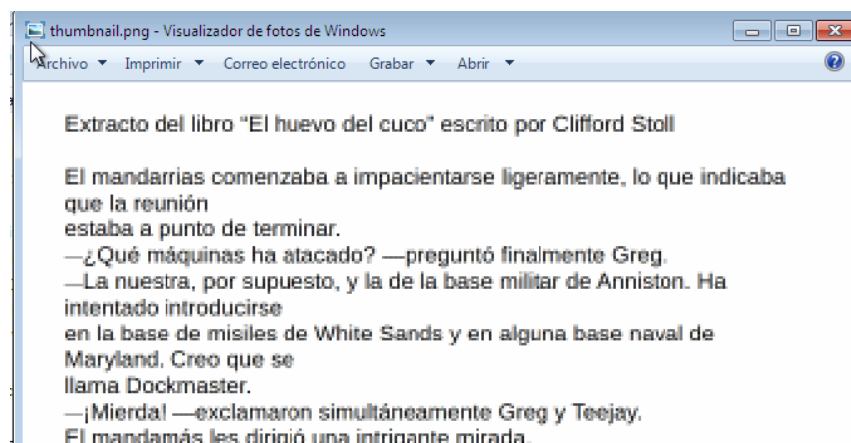


```

<text:span text:style-name="T1">Extracto del libro "El huevo del cuco" escrito por
Clifford Stoll</text:span>
</text:p>
- <text:p text:style-name="P1">
  <text:span text:style-name="T1" />
</text:p>
- <text:p text:style-name="P1">
  <text:span text:style-name="T1">El mandarrias comenzaba a impacientarse
  ligeramente, lo que indicaba que la reunión</text:span>
  <text:line-break />
  <text:span text:style-name="T1">estaba a punto de terminar.</text:span>
  <text:line-break />
  —
  <text:span text:style-name="T1">¿Qué máquinas ha atacado? —preguntó finalmente
  Greg.</text:span>
  <text:line-break />
  —
  <text:span text:style-name="T1">La nuestra, por supuesto, y la de la base militar de
  Anniston. Ha intentado introducirse</text:span>
  <text:line-break />
  <text:span text:style-name="T1">en la base de misiles de White Sands y en alguna
  base naval de Maryland. Creo que se</text:span>
  <text:line-break />
  <text:span text:style-name="T1">llama Dockmaster.</text:span>

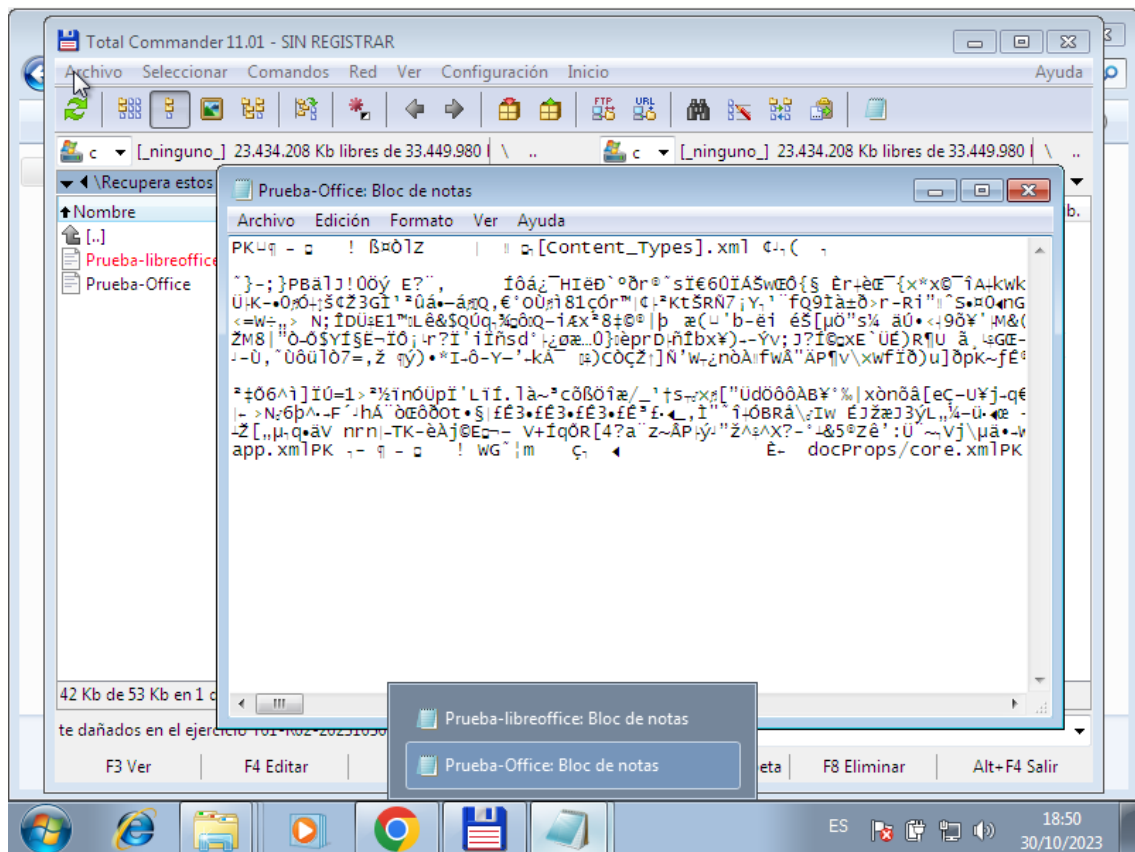
```

Aquí podemos comprobar que esta bien:



### Ejercicio 3

Este es el segundo archivo que venía en el R02, vemos que esta en zip asique lo extraemos y le cambiamos la extensión a zip:



Ahora simplemente investigamos el contenido:

