ANÁLISIS FORENSE

Unidad 1. Actividad 2

4 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

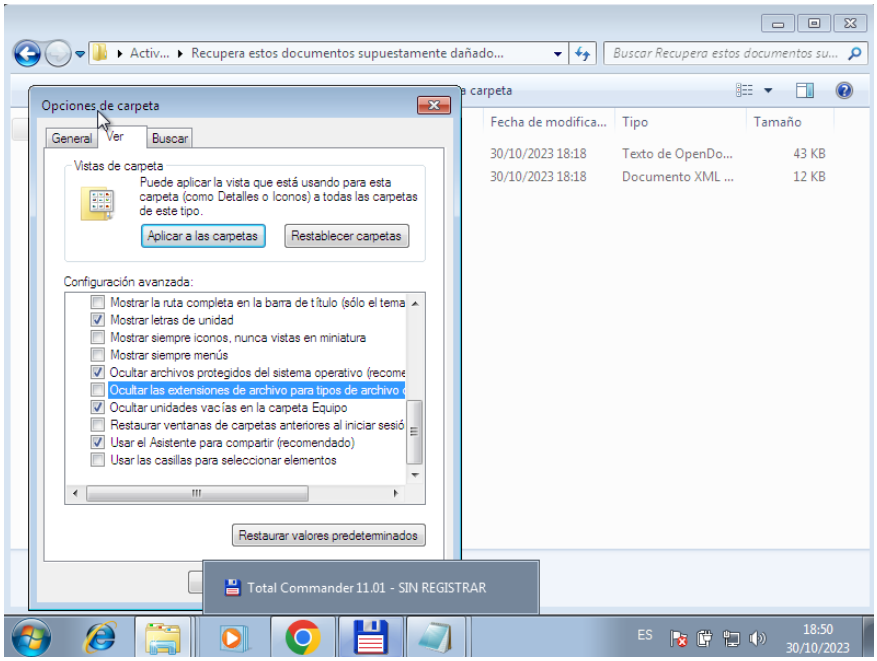
Índice

Ejercicio 1. 2
Ejercicio 2 ..... **¡Error! Marcador no definido.**
Ejercicio 3 ..... **¡Error! Marcador no definido.**
Ejercicio 4 13

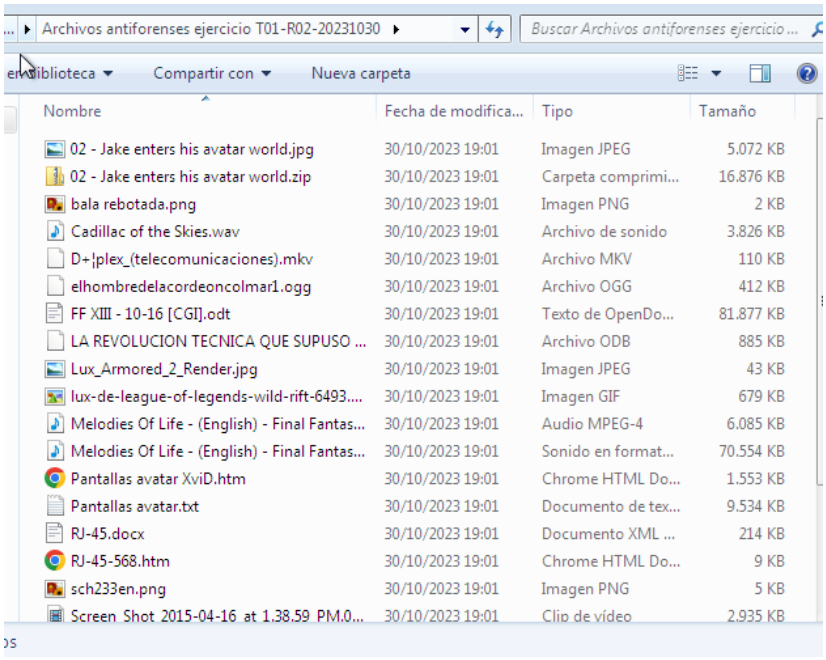
Ejercicio 1.

Instalamos total commander:

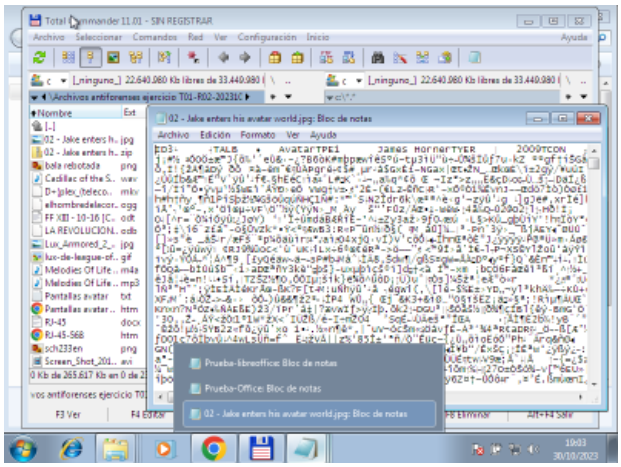
Para que no se nos oculten las extensiones de los archivos:



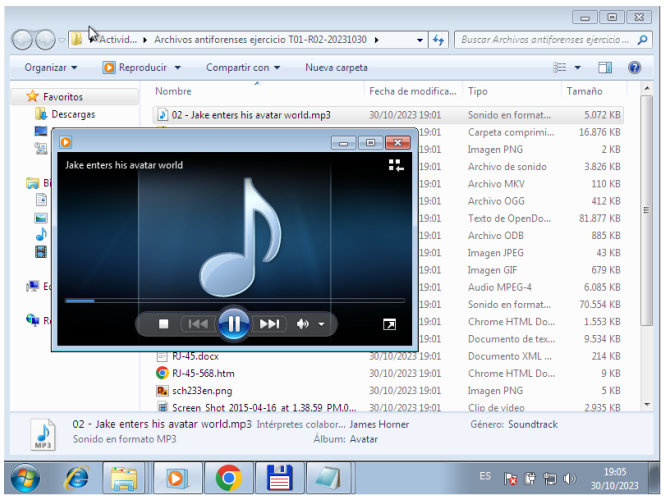
Al extraerlo podemos ver todos estos archivos:



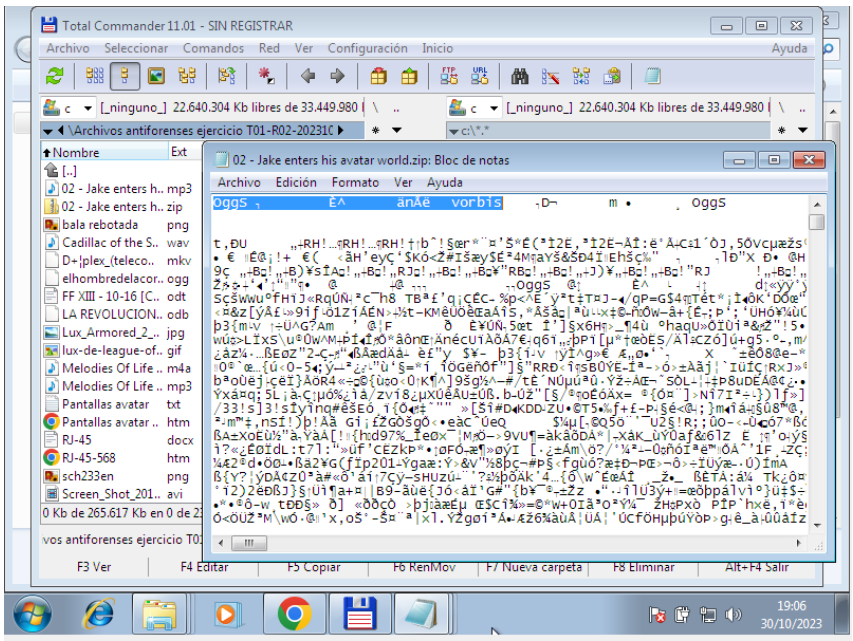
Vamos a empezar por el primero:



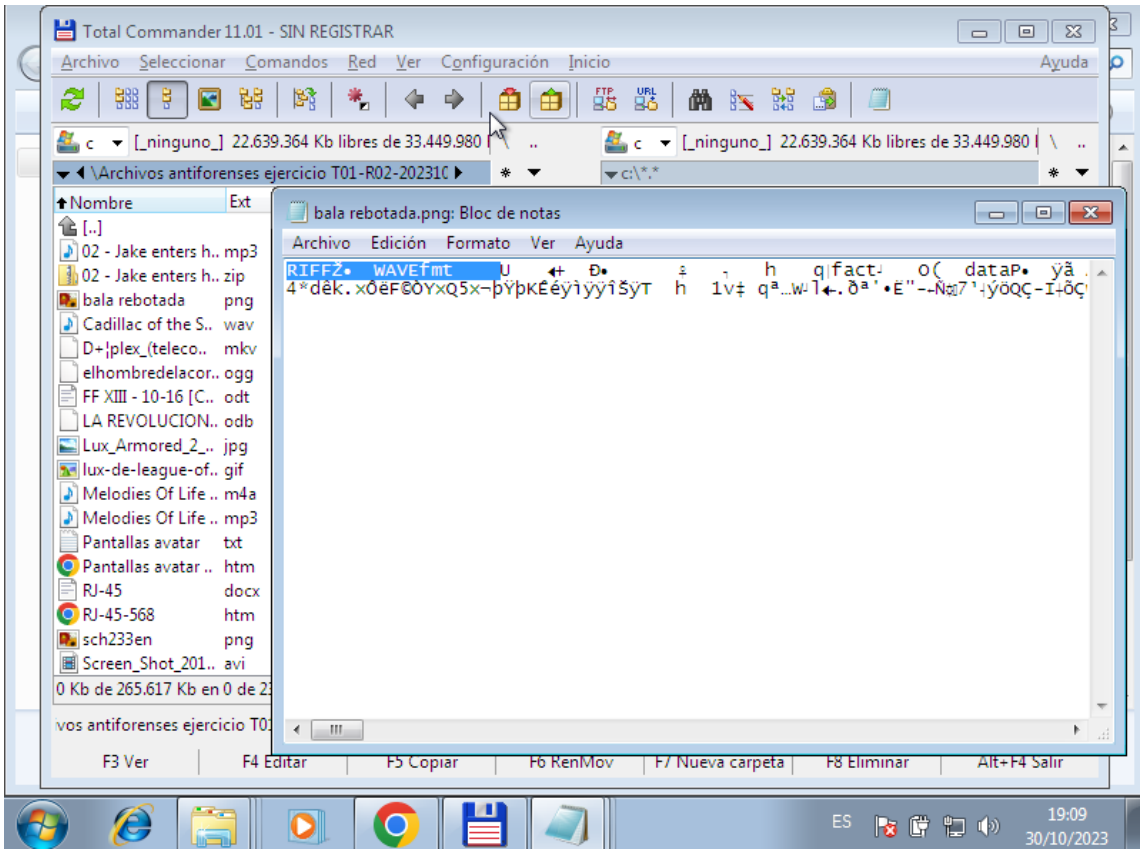
Como vemos tiene de cabecera ID3, por tanto es un MP3, se puede comprobar cambiándole la extensión:



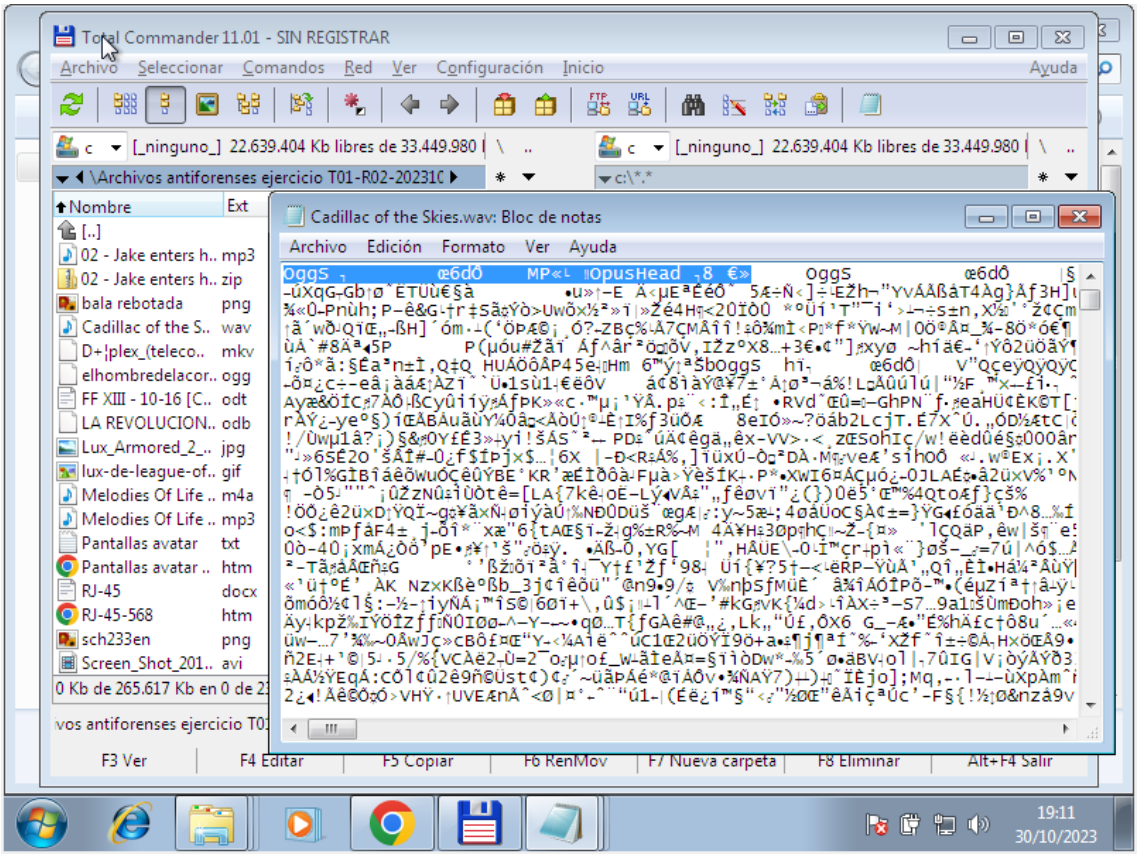
El siguiente es un archivo .ogg, ya que en su comienzo lleva el identificador OggS seguido de un número variable de datos binarios y la palabra vorbis:



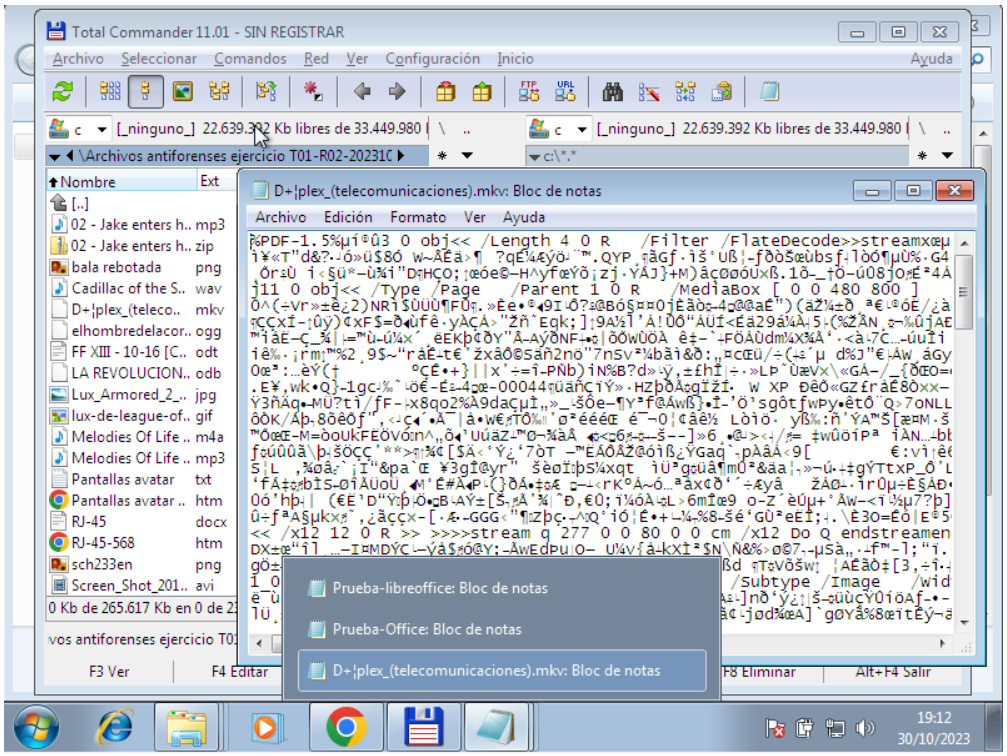
El siguiente tiene una Cabecera de archivos .wav ya que en el comienzo lleva los identificadores RIFF y la palabra WAVE separadas por un grupo de datos binarios:



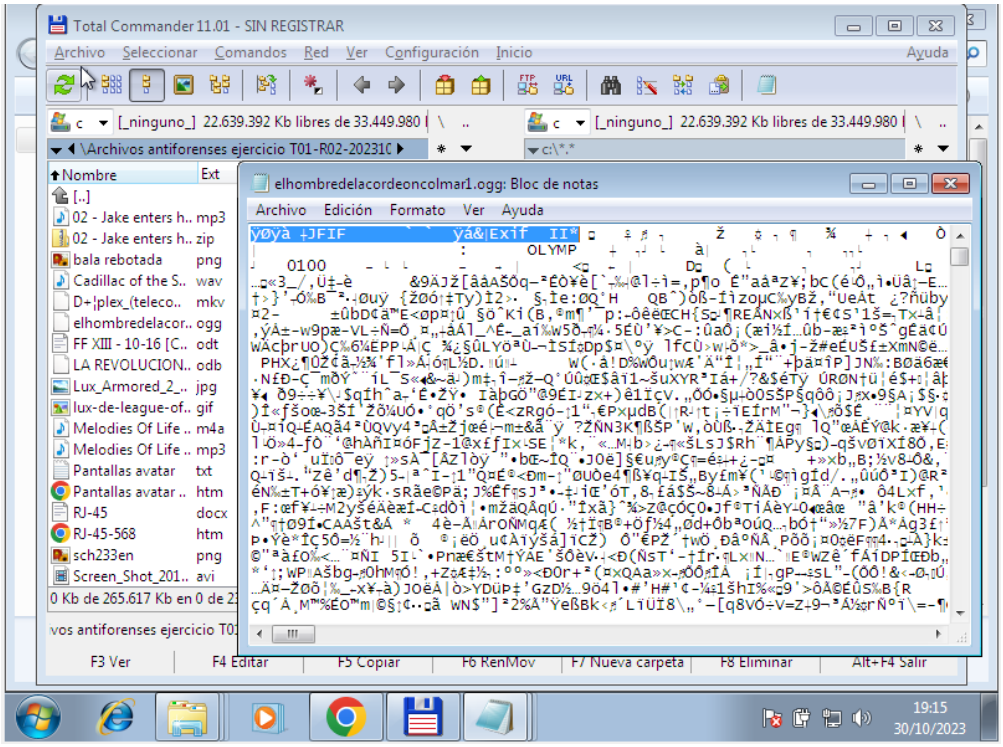
El siguiente es de una cabecera de archivos .opus ya que en su comienzo lleva el identificador OggS seguido de un número variable de datos binarios y la palabra OpusHead



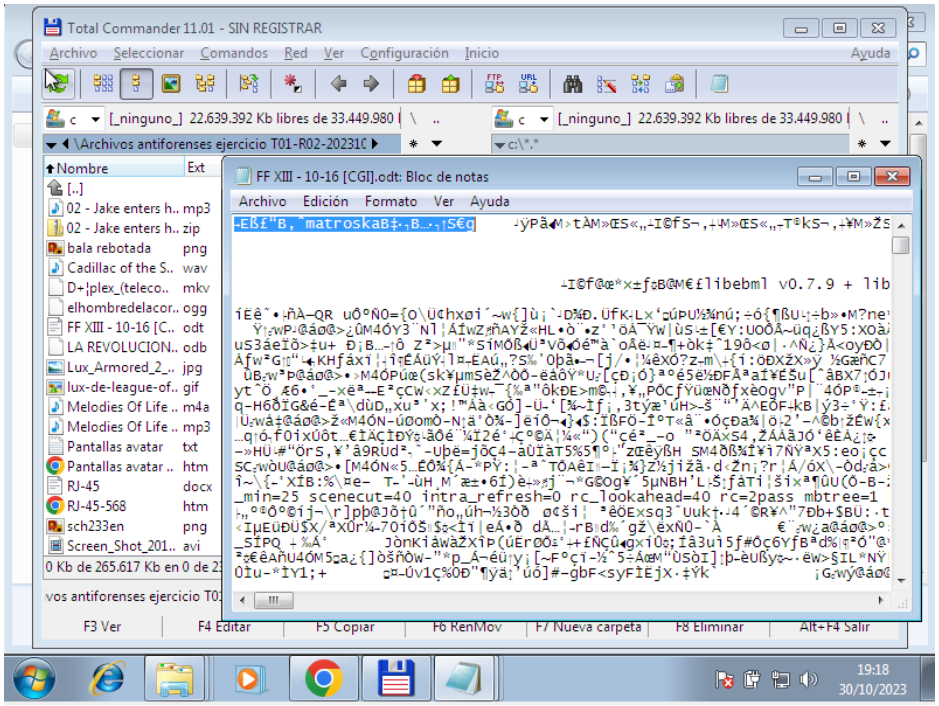
El siguiente es una cabecera de archivos .pdf realizada con Libreoffice Writer. En su comienzo lleva el identificador PDF seguido de un número indicando la versión del codificador usado por writer para crear el pdf, en este ejemplo es la versión 1.5



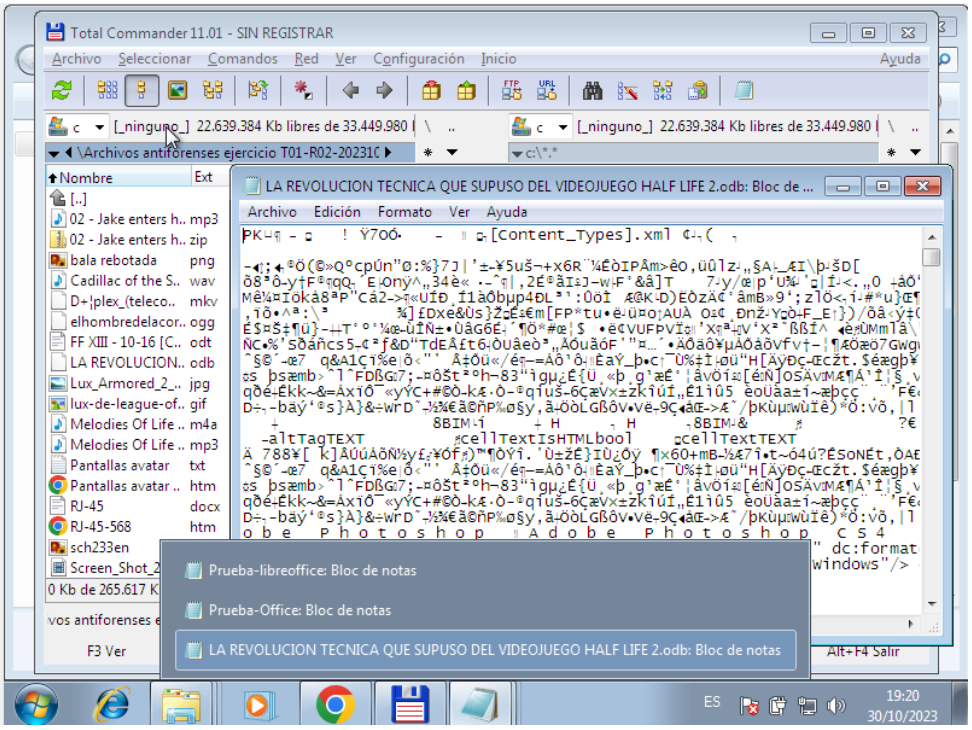
El siguiente es una cabecera de archivos .jpg y también .jpeg . En su comienzo lleva el identificador JFIF y puede que datos acerca del programa que lo creó, la calidad de la imagen, etc.



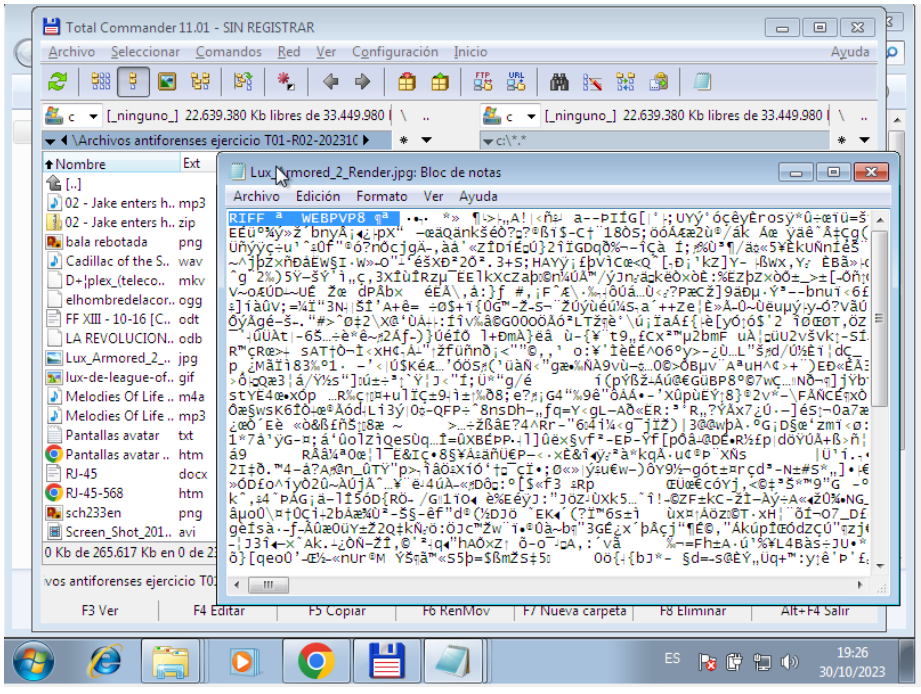
El siguiente es una cabecera de archivos .mkv. Precedida de un número indeterminado de datos binarios, encontraremos la palabra matroska ya que mkv es la abreviatura de MatrosKa Video:



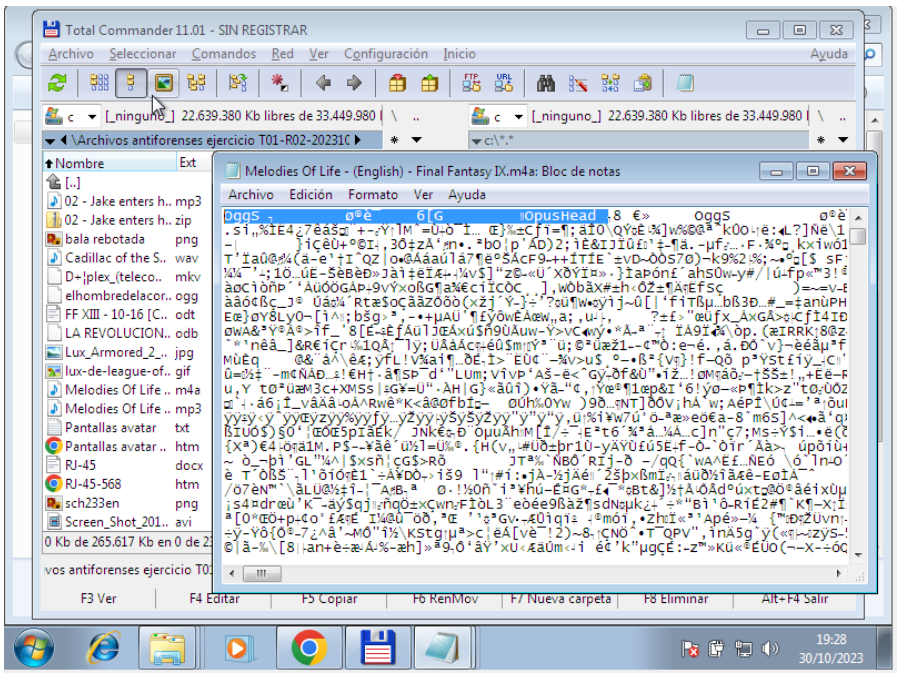
La siguiente es una cabecera de archivos .docx de Microsoft Word. En el comienzo lleva los identificadores PK y la palabra doc precedida de un grupo de puntos suspensivos



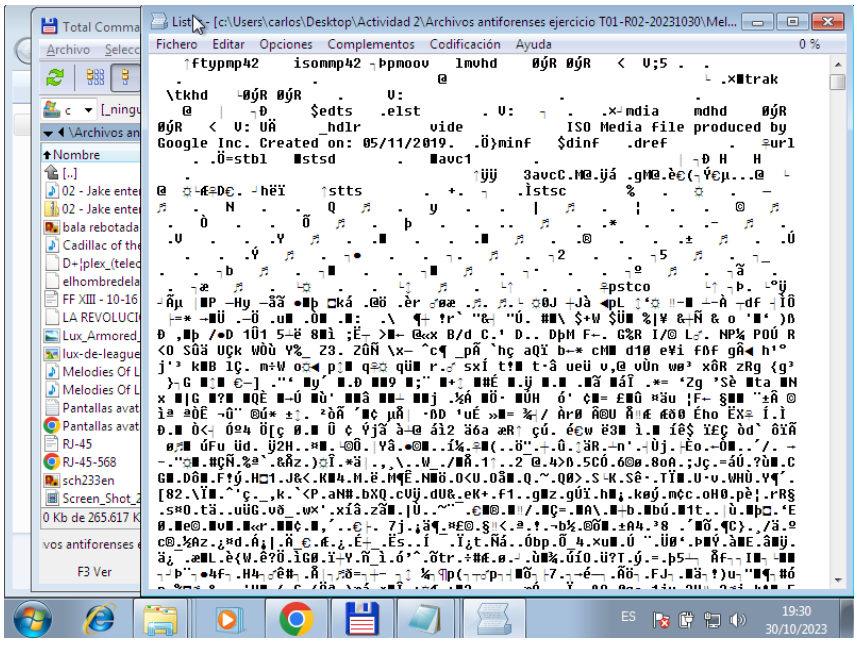
El siguiente tiene una Cabecera de archivos .wav ya que en el comienzo lleva los identificadores RIFF y la palabra WAVE separadas por un grupo de datos binarios:



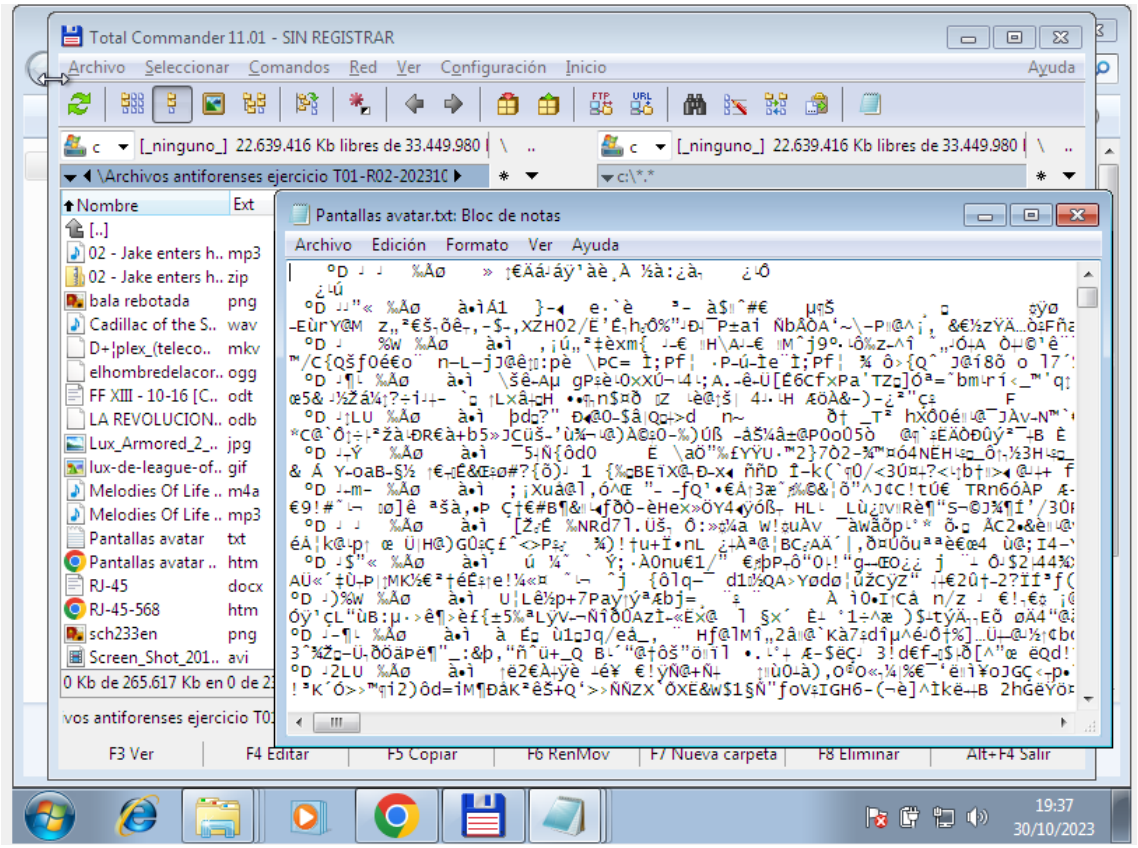
El siguiente es de una cabecera de archivos .opus ya que en su comienzo lleva el identificador OggS seguido de un número variable de datos binarios y la palabra OpusHead:



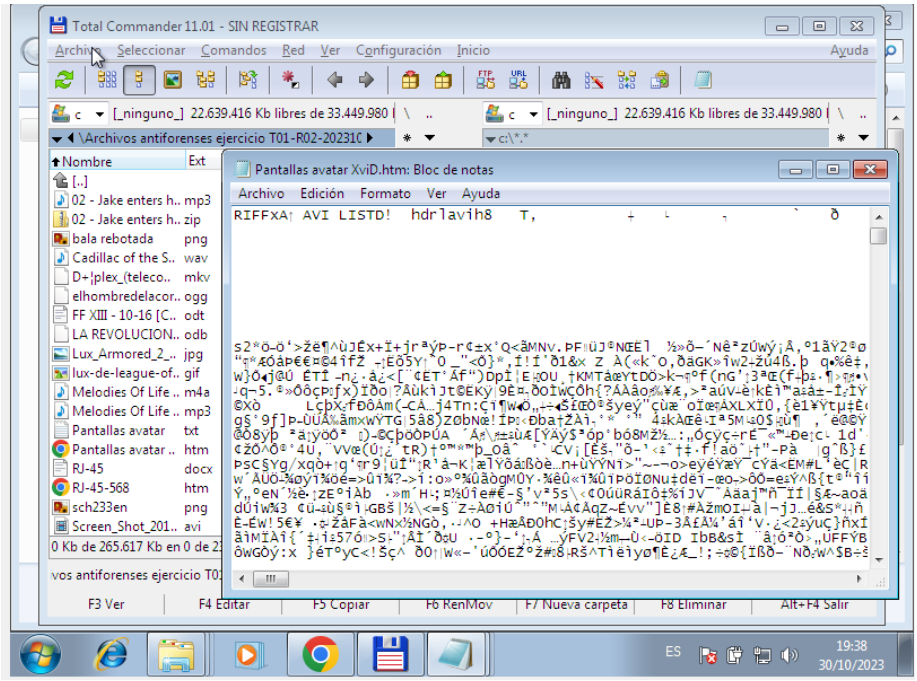
El siguiente es una cabecera de archivos .mp4 En su comienzo, acompañada de otras palabras, lleva el identificador isonmp42 donde avc1 es el nombre técnico que recibe el codificador mp4.



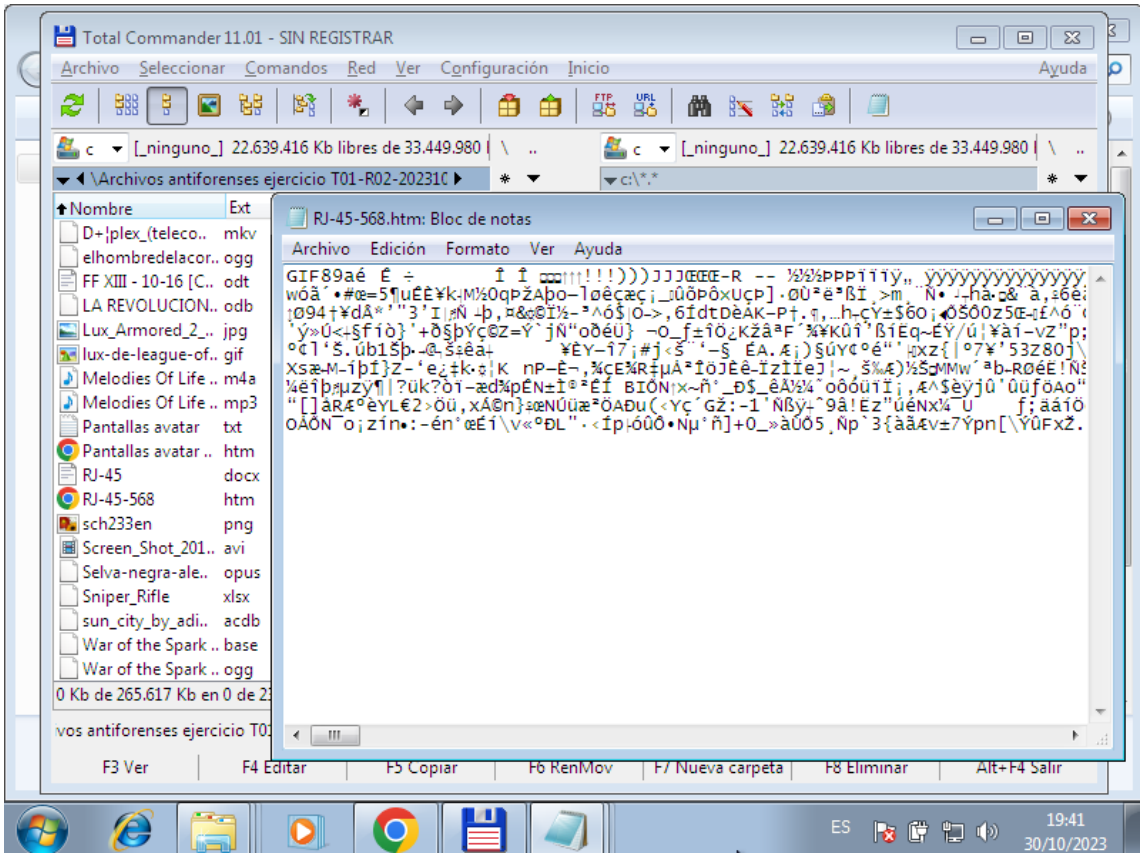
El siguiente es una abecera de archivos .bmp En el comienzo lleva el identificador BM



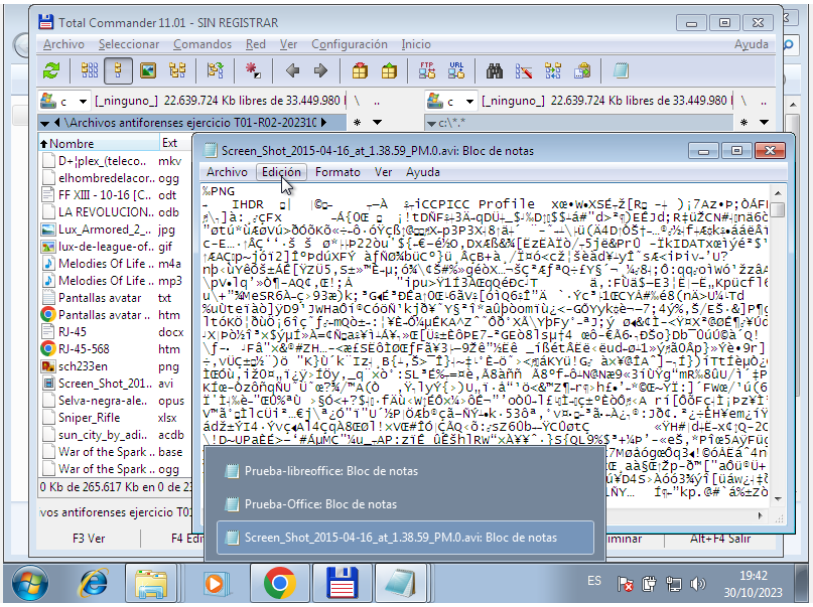
El siguiente es una cabecera de archivos .avi En el comienzo lleva los identificadores RIFF y la palabra AVI precedida de un grupo más o menos grande de datos binarios.



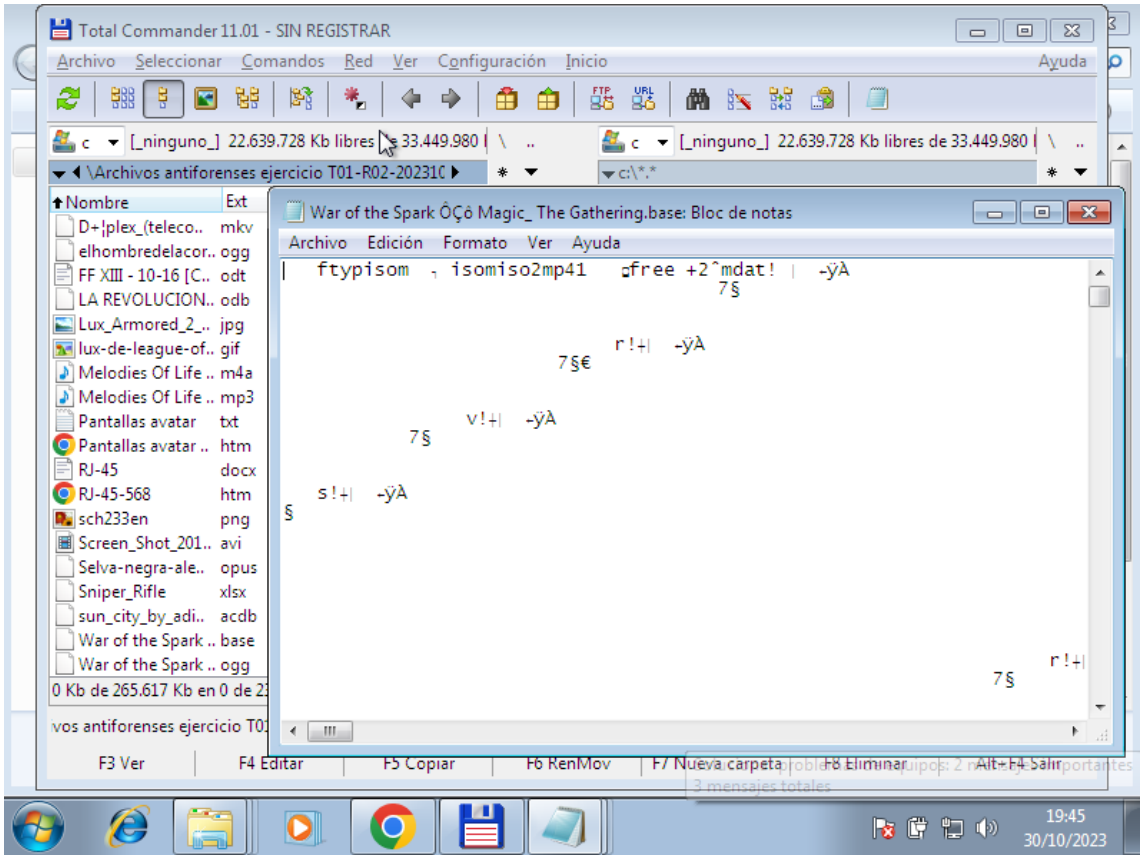
El siguiente es una cabecera de archivos .gif En su comienzo llevan el identificador GIF89a aunque también es posible ver el GIF87a :



El siguiente es una cabecera de archivos .png En su comienzo lleva el identificador PNG seguido de un grupo de datos en binario y el identificador IHDR

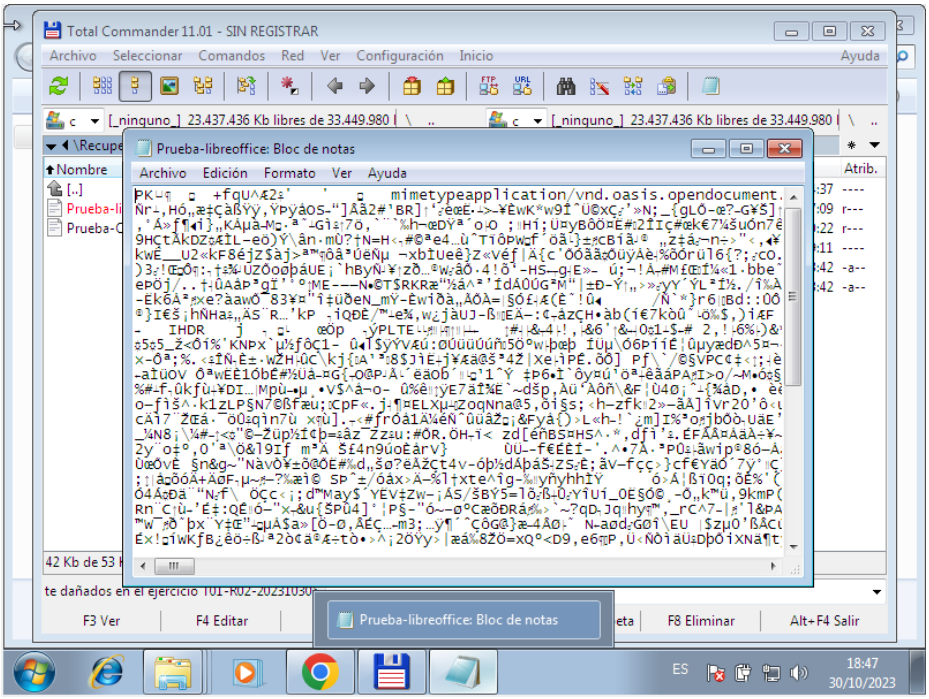


El siguiente es una cabecera de archivos .mp4 En su comienzo, acompañada de otras palabras, lleva el identificador isomiso2mp41 donde avc1 es el nombre técnico que recibe el codificador mp4.

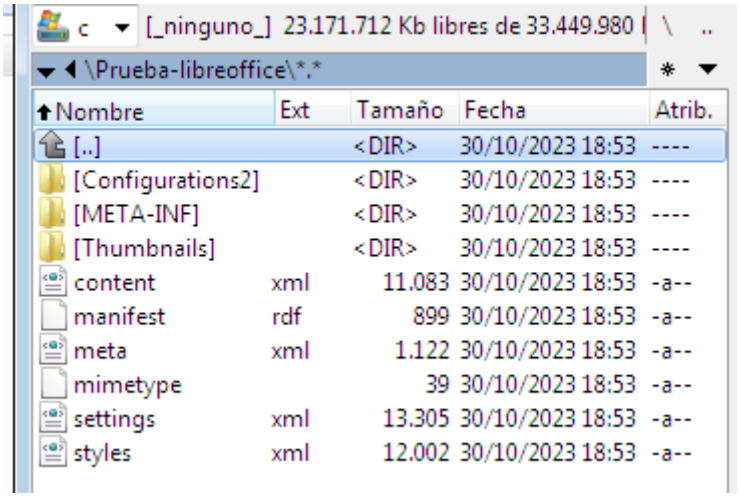


Ejercicio 2

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



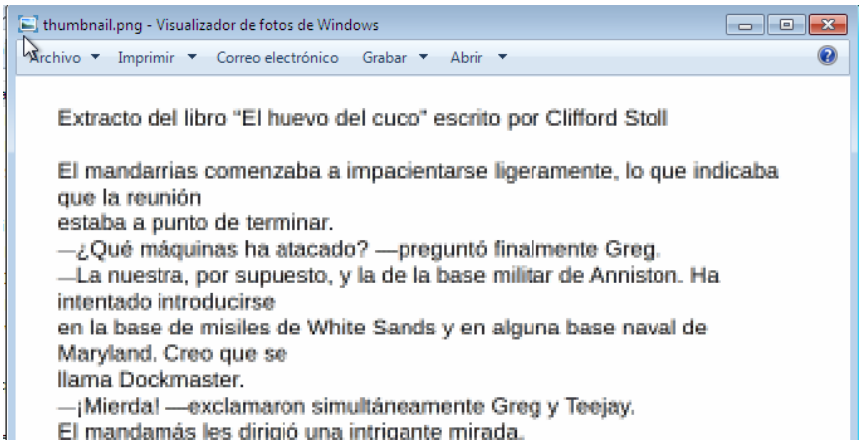
Vamos a empezar por el archivo 1,llamado Prueba-libreoffice:



En el archivo content podemos ver el contenido del archivo:

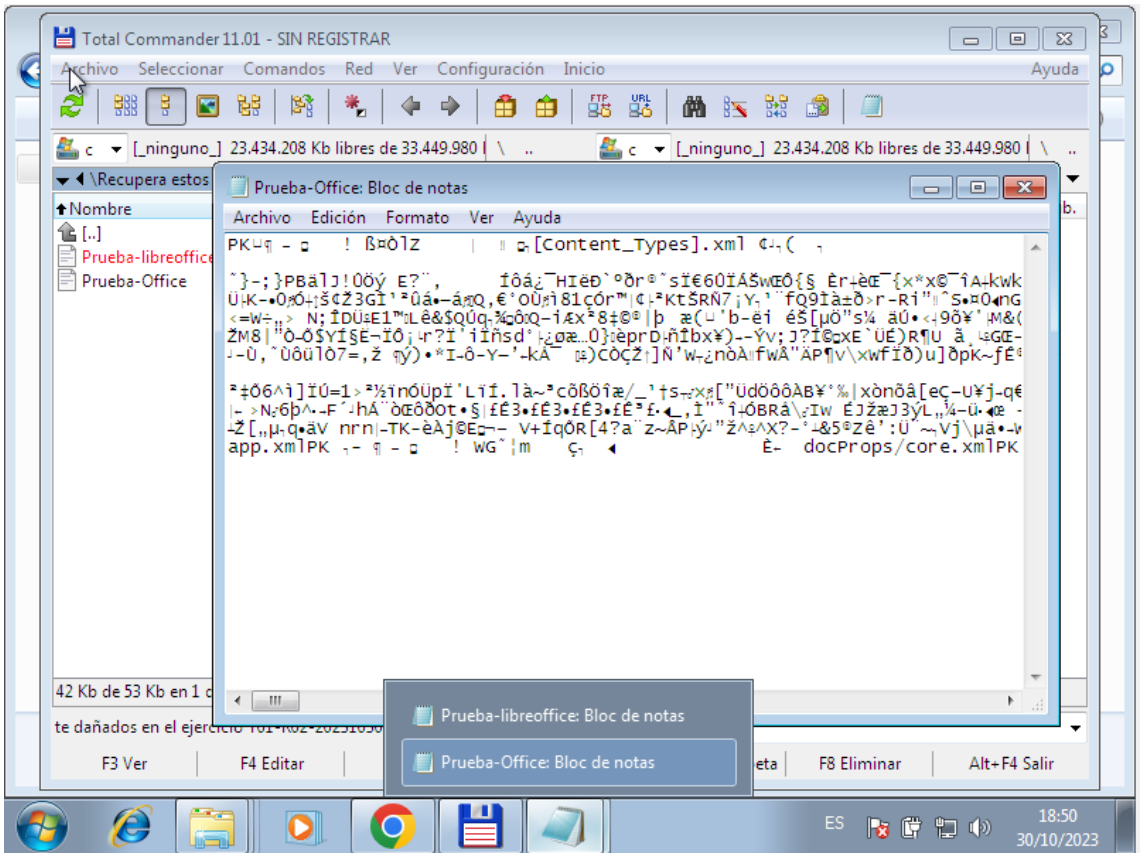
```
    <text:span text:style-name="T1">Extracto del libro "El huevo del cuco" escrito por
      Clifford Stoll</text:span>
  </text:p>
- <text:p text:style-name="P1">
    <text:span text:style-name="T1" />
  </text:p>
- <text:p text:style-name="P1">
    <text:span text:style-name="T1">El mandarrias 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 />
```

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: