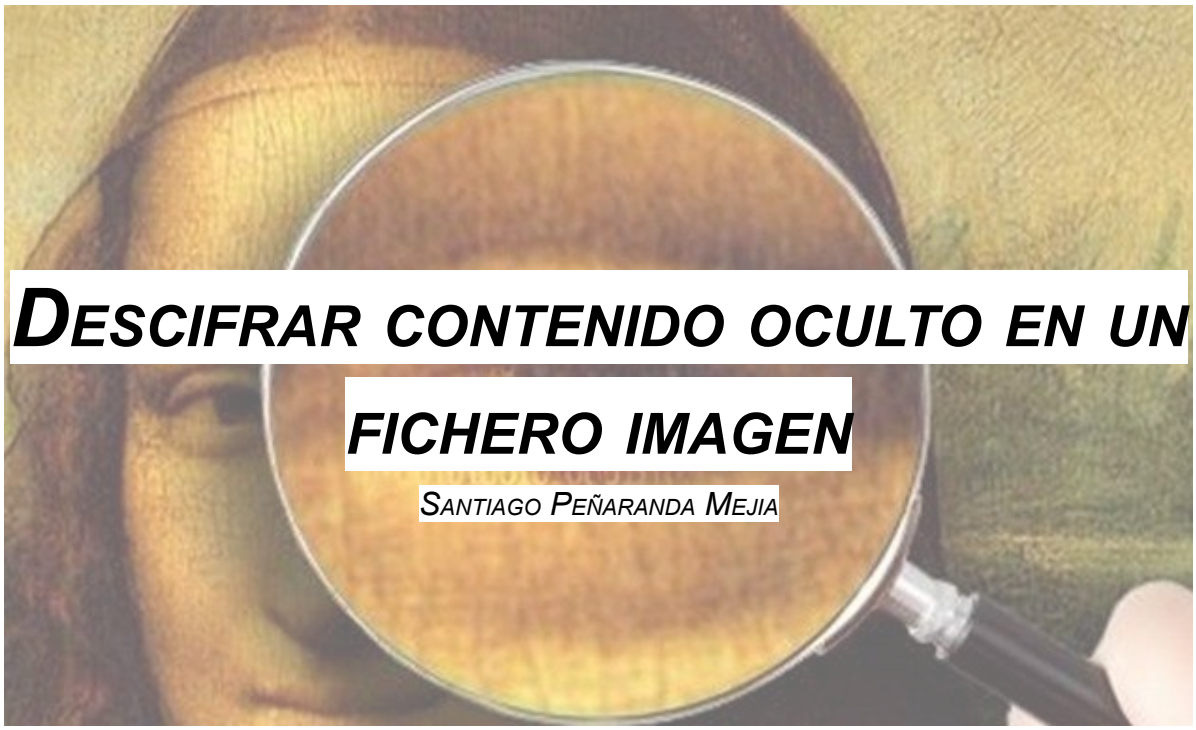
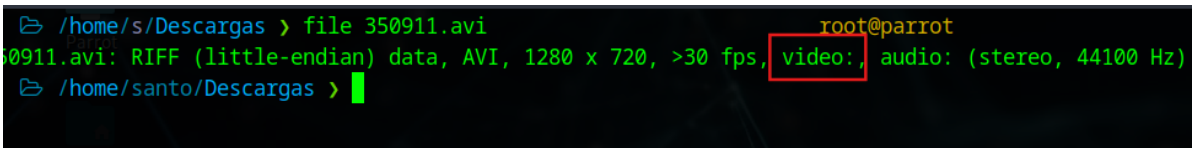


DESCIFRAR CONTENIDO OCULTO EN UN FICHERO IMAGEN

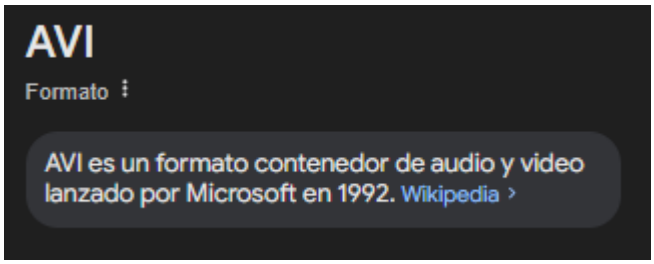
SANTIAGO PEÑARANDA MEJIA

En este informe lo que vamos hacer es una técnica muy conocida que se llama esteganografía, esta práctica trata de ocultar información dentro de otro mensaje, archivo u objeto físico para evitar su detección. Aunque cabe recalcar que las técnicas de esteganografía lo que hacen es ocultar, no proteger, cierta información sensible delante de la vista.

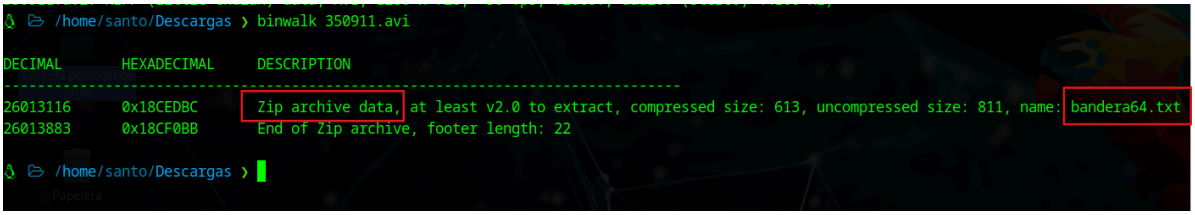
Lo primero que vamos hacer es analizar el archivo que tenemos, para ellos escribimos el siguiente comando



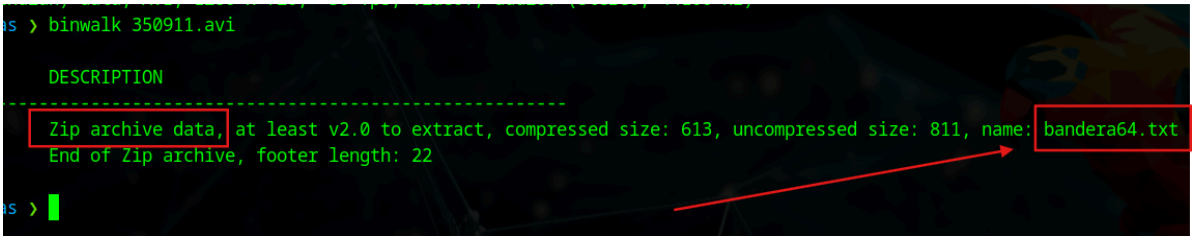
Y como podemos observar es un fichero con formato ".avi" esto quiere decir que es un formato de Audio y video, como podemos ver aquí en la busca que hicimos en internet.



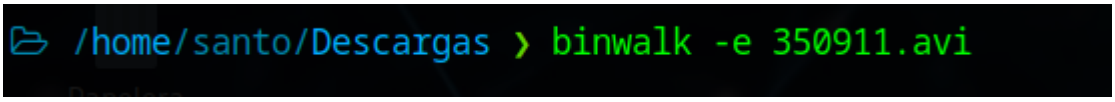
Ahora vamos a extraer datos del archivo, para ello vamos a usar la herramienta Binwalk que es una herramienta destinada a la extracción de datos de imágenes, esto lo hacemos con el siguiente comando.



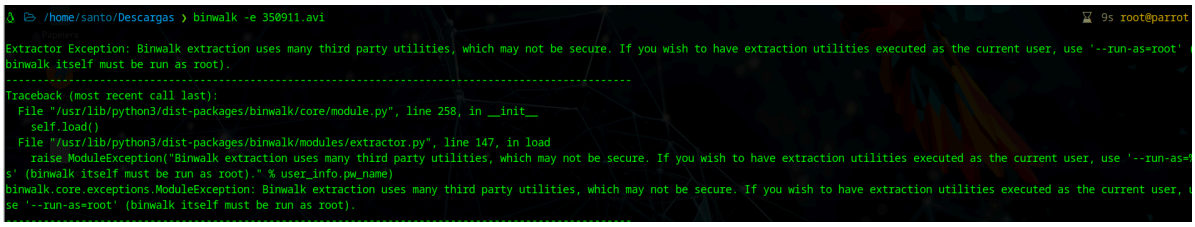
Y así es como nos podemos dar cuenta de que este "supuesto video contiene un fichero ZIP el cual adentro tiene un archivo llamado "bandera64.txt".



Como ya sabemos que el "supuesto video" contiene un fichero ZIP vamos a proceder a extraerlo, esto lo hacemos con el siguiente comando.



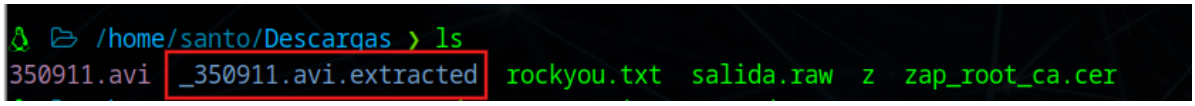
En definitiva este seria el comando, pero como podemos ver me da error, porque la herramienta usa herramientas de terceros y podrían no ser seguras.



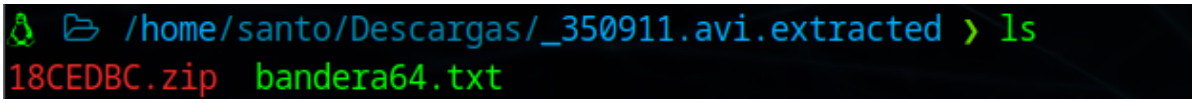
POR ENDE TENEMOS QUE ESCRIBIR EL SIGUIENTE COMANDO A POSTERIOR PARA PODER EJECUTARLA.

```
❯ sudo binwalk -e --run-as=root 350911.avi
```

ESTO NOS GENERA UN FICHERO



Y ASÍ ES COMO HEMOS EXTRAÍDO LA INFORMACIÓN QUE CONTENÍA EL ARCHIVO QUE "APARENTEMENTE SÓLO ERA UN VIDEO"



AL ABRIR EL ARCHIVO .TXT PODEMOS VER QUE HAY CREDENCIALES CIFRADAS, PERO NO SABEMOS EN QUÉ FORMATO DE CIFRADO ESTÁ CIFRADA LAS CREDENCIALES

```
/home/santo/Descargas/_350911.avi.extracted ❯ cat bandera64.txt
UEsDBAoACQBjALpE5UyE1fPolAEAAHgBAAALAAsAYmFuZGVyYS5wbmcBmQcAAQBBRQMAAPKu8K6x
c7GJh/VmKva+f8JqD7Pe3X95ttenp+LwVVKiTrs1N450IIK7cjKsIYwqYBWiSwcClH2S51vh+L6/
xnICJFdIYuqD+sB282j0guUmoXbdIwU3dMtkYeUs/tOm7yd4TxHMfEQ2wM+i64R/iuhx9xvvh5PV
jnyPiKnjKPTQf9tH1XflKezQ8lHDAFPeEWZSMlRBaOwVWLywkiopyEYSuJGzJchCoRtiMX3fmfJX
8bD3SozBFIOPMjje/3/Xn6tVdmaaAVpAt8+iXu05VwXmmg8Ub7isi2KJBljiGMTQ+knFndW3gCEr
V3pk1OfNOGWAI09l5QXe6I+UKJZ5p9bpLi0fBbTHJCFcFu5y/IJHr9Vr5rzi6vpPU7p0ZtNJyYoK
EUB18DsmONtxc+xuqloJtzhRUQ5ZHRWumnfMk9Cw1tYT/KHa4gWh/GOVHLEAkizskRobAfanZ0OY
TfmYtjl/60UaL/sFkDYH4+uNt9MKLLiLR4WomoTq2Qi4o+EyzLDO0drgZXjsd1aN9s3EYkNY+Ug6
UEsHCITV8+iUAQAAeAEAAFBLAQIfAAoACQBjALpE5UyE1fPolAEAAHgBAAALAC8AAAAAAAAAIAAA
AAAAAABiYW5kZXJhLnBuZwoAIAAAAAAAAQAYAABwYYR+FNQBD0sSrJY51AHbTw9ChznUAQGZBwAB
AEFFAwAAUEsFBgAAAAABAAEAaAAAANgBAAAAA==
/home/santo/Descargas/_350911.avi.extracted ❯
```

PERO AL LLAMARSE BANDERA64.TXT PODEMOS INTUIR QUE ESTÉ CIFRADA EN EL FORMATO ***BASE 64****, ASÍ QUE PODRÍAMOS HACER UN ATAQUE DE DICCIONARIO EN BASE 64 Y ASÍ PODER OBTENER LAS CONTRASEÑAS EN TEXTO CLARO.*

ESTO SERÍA TODO, CHAO Y GRACIAS.