2025

CTF INTERNACIONAL METARED ETAPA MEXICO

WRITEUP

CHALLENGE

Survival

ANUIES

ANUIES - TIC

meta red MÉXICO

Description

Title:	Survival
Description:	The worst criminal can be caught simply by trash
Flag:	flagmx{pl4y1ng_w1th_d4t4_r3c0v3r7}
File:	File.7z
Dificultad:	Intermedio
Tags	Forensic

Solution:

The file.img file is a clone of a USB made with dd. Contains a txt file with the flag removed, but no data recovery is required.

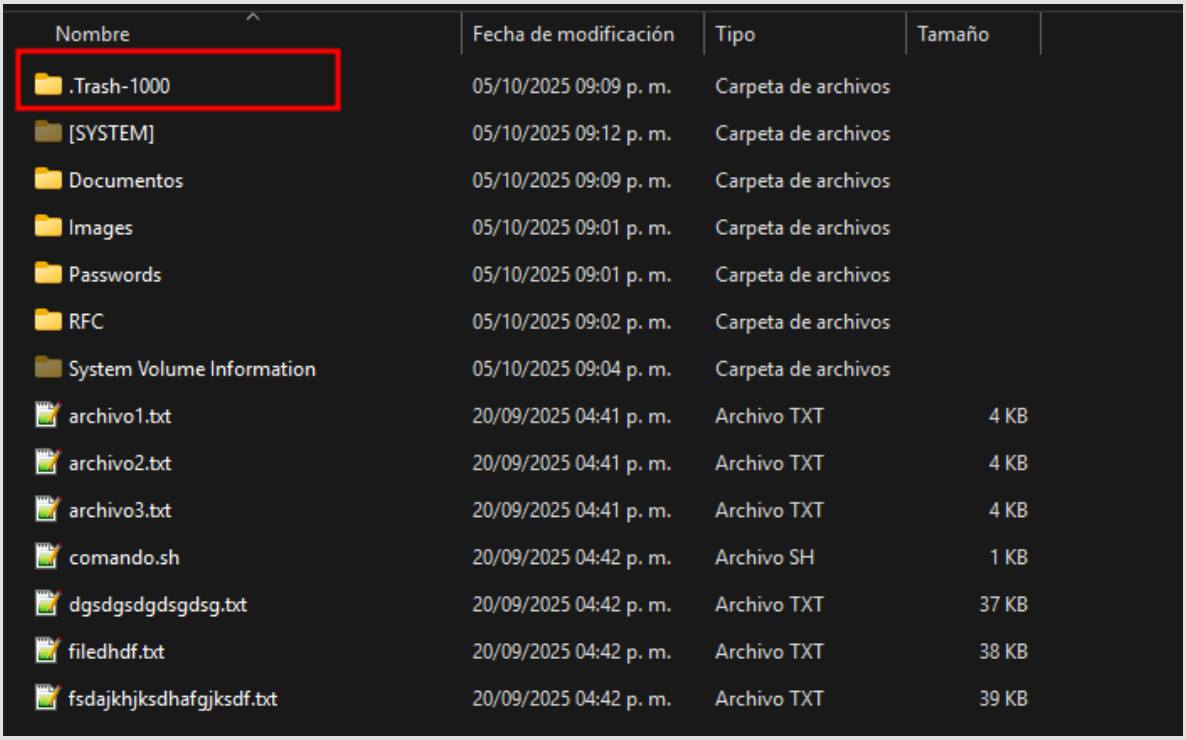
The challenge is ultimately easy to solve. You must analyze the file "file" to determine if it is a disk image.

Analysis examples

```
└─$ file  file
file: DOS/MBR boot sector MS-MBR XP "j" "j" "j", disk signature 0×f7aa5; partition 1 : ID=0×7,
active, start-CHS (0×0,1,1), end-CHS (0×e,254,63), startsector 63, 251841 sectors
```

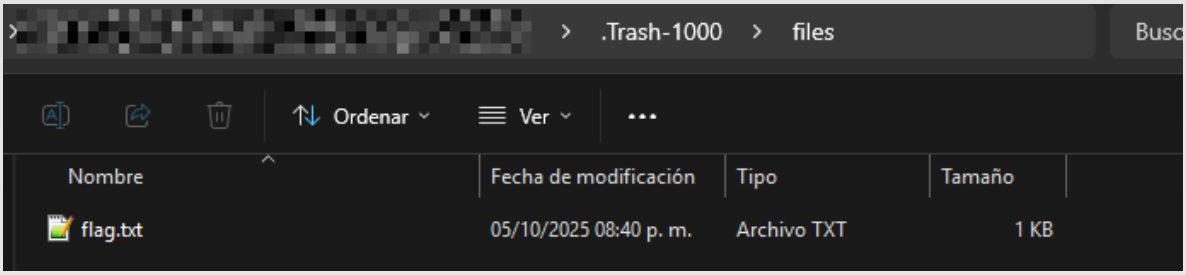
```
> type .\file | more +10
èV
=r#è┴$?ÿèÌè³C¸ÒïÐåÍ▒Ê¯B¸Ô9V
w#r9sÙ╕É╗
|ïNïV
=sQOtN2õèV
=ÙõèV
`╗¬U┤A=r6ü³U¬u0÷┴t+a`j
j
 v
 j
h
|jj┤Bï¶=aasOt
             2õèV
=ÙÍa¨├Invalid partition table
Error loading operating system
Missing operating system
```

After determining that it is a disk image file, we can unzip it with 7zip and analyze the contents.

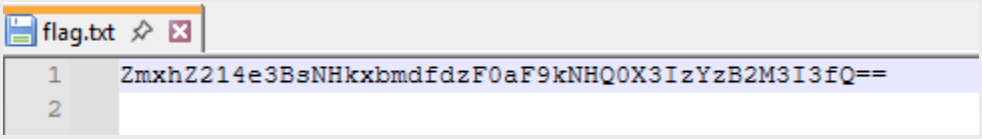


Nombre	Fecha de modificación	Tipo	Tamaño
.Trash-1000	05/10/2025 09:09 p. m.	Carpeta de archivos	
[SYSTEM]	05/10/2025 09:12 p. m.	Carpeta de archivos	
Documentos	05/10/2025 09:09 p. m.	Carpeta de archivos	
Images	05/10/2025 09:01 p. m.	Carpeta de archivos	
Passwords	05/10/2025 09:01 p. m.	Carpeta de archivos	
RFC	05/10/2025 09:02 p. m.	Carpeta de archivos	
System Volume Information	05/10/2025 09:04 p. m.	Carpeta de archivos	
archivo1.txt	20/09/2025 04:41 p. m.	Archivo TXT	4 KB
archivo2.txt	20/09/2025 04:41 p. m.	Archivo TXT	4 KB
archivo3.txt	20/09/2025 04:41 p. m.	Archivo TXT	4 KB
comando.sh	20/09/2025 04:42 p. m.	Archivo SH	1 KB
dgsdgsdgdsgdsg.txt	20/09/2025 04:42 p. m.	Archivo TXT	37 KB
filedhdf.txt	20/09/2025 04:42 p. m.	Archivo TXT	38 KB
fsdajkhjksdhafgjksdf.txt	20/09/2025 04:42 p. m.	Archivo TXT	39 KB

We analyze the contents of the ".Trash-1000" directory and there is a "flag" file.

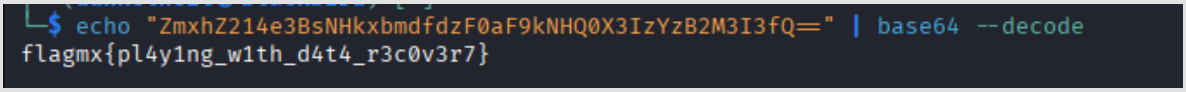


When opening it with the notes editor we see a base64 string



In Linux you can decode to base64 with the following command

echo "ZmxhZ214e3BsNHkxbmdfdzF0aF9kNHQ0X3IzYzB2M3I3fQ==" | base64 –decode



The flag is:

flagmx{pl4y1ng_w1th_d4t4_r3c0v3r7}