



Mission Name

Reassembling

Background

Ethan and Claire discuss their confusion and speculate reasons why Atali would want to investigate his own company / order the release of code snippets. Dr Pinche shows the evidence that Atali ordered Jailnor to be killed. This evidence needs to be decrypted to check it.

Technical High-Level Overview

An unknown file is provided to the player. This file is XORed. Once decrypted, player has to depyxel in order to get the Camera code shown in the PNG file.

Short Description

Your goal is to try to get the first 7 numbers of the camera code.

Mission Description

A camera fragment based on Jailnor murder is provided to you. Your goal is to try to get the first 7 numbers of the camera code.

Location

- RECON CAR - AIR



Tools

- <https://github.com/beurtschipper/Depix>
- CyberChef

Questions

- Which program was used to put the camera code?
- Notepad

Hints

1. Bruteforce the file
2. Bruteforce to get a XOR key
3. Use any tool to show the image in the correct format.

Write Up

Upload the file provided to CyberChef:



Figure 1

Use "XOR Brute Force" recipe:

The screenshot shows the CyberChef interface with the 'XOR Brute Force' recipe selected. The 'Input' panel shows a file named 'final.dat' with a size of 688 bytes. The 'Output' panel displays a list of keys found during the brute force search. The output text is as follows:

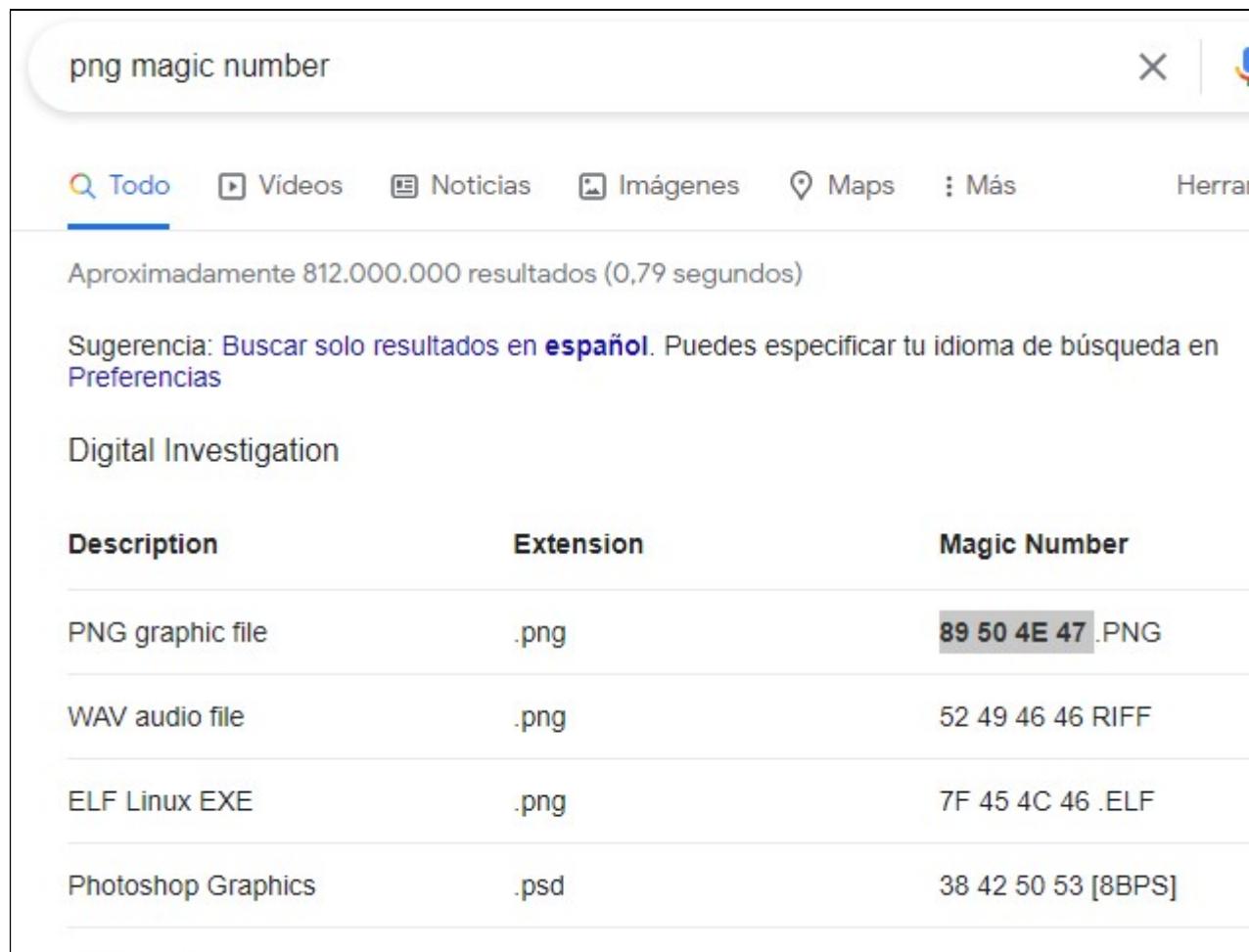
```
start: 28538    time: 532ms
end: 28538    length: 1769444
length: 0    lines: 65535
Key = 041c: b2 73 75 64 36
Key = 041d: b2 72 75 65 36
Key = 041e: b2 71 75 66 36
Key = 041f: b2 70 75 67 36
Key = 0420: b2 4f 75 58 36
Key = 0421: b2 4e 75 59 36
Key = 0422: b2 4d 75 5a 36
Key = 0423: b2 4c 75 5b 36
```

Figure 2

Player has to know, typical headers of image file, like PNG:

Key = 3f3a: 09 52 4e 45 0d
Key = 3f3e: 89 51 4e 46 0d
Key = 3f3f: 89 50 4e 47 0d
Key = 3f40: 89 2f 4e 38 0d
Key = 3f41: 89 2e 4e 39 0d
Key = 3f42: 89 2d 4e 3a 0d

Figure 3



A screenshot of a search results page from a search engine. The search query "png magic number" is entered in the search bar. Below the search bar, there are navigation links: Todo, Videos, Noticias, Imágenes, Maps, Más, and Herramientas. The search results indicate approximately 812,000,000 results found in 0.79 seconds. A suggestion is shown: "Sugerencia: Buscar solo resultados en [español](#). Puedes especificar tu idioma de búsqueda en Preferencias". Below the suggestion, there is a section titled "Digital Investigation" which lists file types and their magic numbers. The table is as follows:

Description	Extension	Magic Number
PNG graphic file	.png	89 50 4E 47 .PNG
WAV audio file	.png	52 49 46 46 RIFF
ELF Linux EXE	.png	7F 45 4C 46 .ELF
Photoshop Graphics	.psd	38 42 50 53 [8BPS]

Figure 4



If player tries the key located, will see the PNG header:

The screenshot shows the CyberChef XOR tool interface. The top navigation bar includes 'Recipe' (selected), 'Input', 'Output', and various file operations like 'Save', 'Copy', 'Print', and 'Exit'. The 'Input' tab is active, showing a file icon and the details: Name: final.dat, Size: 688 bytes, Type: unknown, Loaded: 100%. The 'Output' tab is also visible, showing the resulting text output.

Input

Name: final.dat
Size: 688 bytes
Type: unknown
Loaded: 100%

Output

```
.PNG
.
.
.
IHDR.....?`U....sRGB.@"é....gAMA..±..üa....
pHYs...Ä...Ä.Co~d...!tEXtCreation Time.2021:07:18 09:12:32E
'....IDATHCíÜKK.a.ÆÑÁX/ÉÄ&M%H VÄRØ.RQ.
bW.Rë~?.].è|u£.0-^åe%..^@...
ÍX.ðÀc9ºÝ.ß&y.,I8.í.ñPPð(ðÌ.ðøð³±_±þýÅ[Z.ý.¢
¡Ñ!.].°Qðøà¢Èßj;"XÌ£"°=.%SCQ.\DQ%".E>%>.ù.
¢Bð...2ë(J.%AÑØ.E'{É(...CÑ..µ..^ú..t%jCÑí..}ýü.E.û.E¥...>M.
£heu.E.yùÙ.o_PuzÅRFè`#t°...:XÉ.úá'r..4..CQì¢(%).
¢iÖ..^wÈ.Ø7Ù.Eñh.EÃiå;jiv.Ettí(J.t¢(%,...k¹;çxRi.EÓS.(JåäÁçå<.
¢æ.y8îiÈ.á|$..x..æ³Z+.â ù{]G.S.h.EäÉ.(ú1ç.¢.%.
±P.ý..%b)#t°...:XÉ..,eÄ.Í
.±ä]Ý`è..»âÙ
```

Figure 5



Once the image was deciphered, player will get the following image:

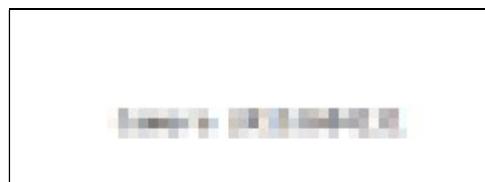


Figure 6

To depixel it, player must install the following tool:

```
git clone https://github.com/beurtschipper/Depix  
cd Depix  
pip3 install -r requirements.txt
```

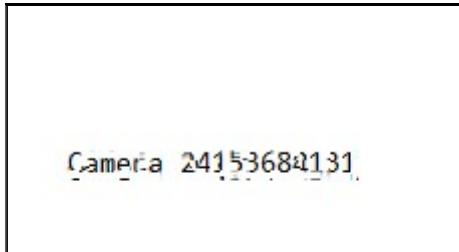
And the following command:

```
python3 depix.py -p image_from_CyberChef.png -s  
images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o path/final.png
```

```
(kali㉿kali)-[~/Depix]  
└─$ python3 depix.py -p /mnt/hgfs/Maquina/pre_image.png -s images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o /mnt/hgfs/Maquina/salida.png  
INFO:root:Loading pixelated image from /mnt/hgfs/Maquina/pre_image.png  
INFO:root:Loading search image from images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png  
INFO:root:Finding color rectangles from pixelated space  
INFO:root:Found 120 same color rectangles  
INFO:root:84 rectangles left after moot filter  
INFO:root:Found 2 different rectangle sizes  
INFO:root:Finding matches in search image  
INFO:root:Scanning 81 blocks with size (5, 5)
```

Figure 7

The image depyxeled:





Flag Information

flag{2415368}