Writeup of K.P.A

This is a zip file containing two zipped files.

```
└─$ 7z l very_easy_challenge.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD Ryzen 7 5800X3D 8-Core Processor            (A20F12),ASM,AES-NI)

Scanning the drive for archives:
1 file, 119850 bytes (118 KiB)

Listing archive: very_easy_challenge.zip
--
Path = very_easy_challenge.zip
Type = zip
Physical Size = 119850

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2023-05-06 06:59:52 .....          695          643  not_a_rickroll_lyrics.zip
2023-05-06 06:59:12 .....          690          637  rickroll_lyrics.zip
------------------- ----- ------------ ------------  ------------------------
2023-05-06 06:59:52               1385         1280  2 files
```

By using bkcrack, we can find a file containing lyrics from Never Gonna Give You Up.
This is the bin file used to attack :

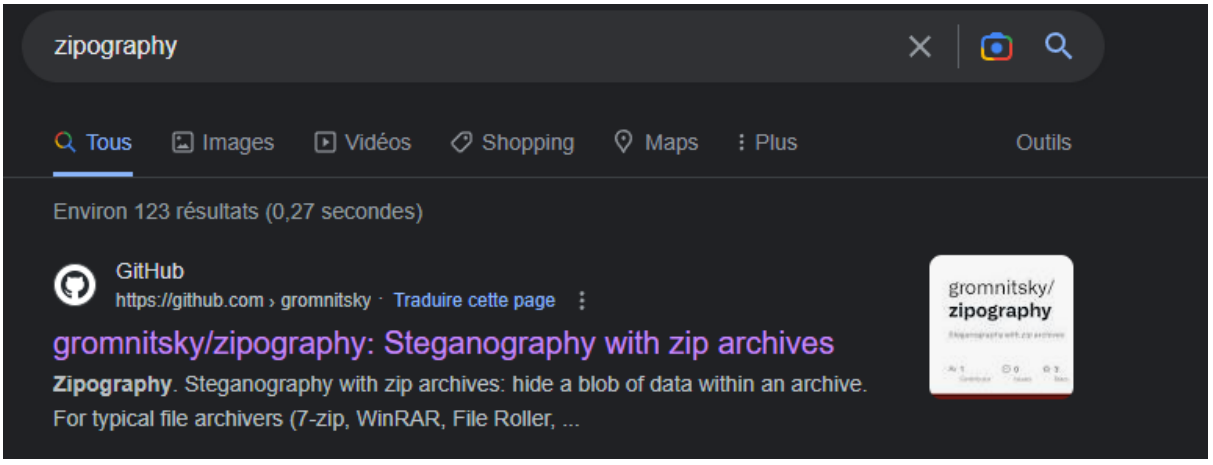
```
┌──(kali㉿kali)-[~/Desktop/KPA]
└─$ cat 'plain (copy 1).bin'
You know the rules and so do I
```

At the end of each files, we can find two hints :

```
HINT ⇒ Z I P O
```

```
NOT A HINT ⇒ YHPARG
```

This is ZIPOGRAPHY !



This is a steganography used to hide files in zip. using this technique we can find a hidden file :

```
└─$ zipography-extract very_easy_challenge.zip > challenge

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
bkcrack  challenge  KPA  very_easy_challenge.zip

┌──(kali㉿kali)-[~/Desktop]
└─$ 7z l challenge

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD Ryzen 7 5800X3D 8-Core Processor          (A20F12),ASM,AES-NI)

Scanning the drive for archives:
1 file, 118227 bytes (116 KiB)

Listing archive: challenge

--
Path = challenge
Type = zip
Physical Size = 118227

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2023-05-05 17:35:13 .....       118033       118045  flag.svg
------------------- ----- ------------ ------------  ------------------------
2023-05-05 17:35:13             118033       118045  1 files
```

Again we are against a zip with a password :

```
└─$ unzip challenge.zip
Archive:  challenge.zip
[challenge.zip] flag.svg password:
```

And it contains only a svg file.

```
└─$ 7z l challenge.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 118226 bytes (116 KiB)

Listing archive: challenge.zip

--
Path = challenge.zip
Type = zip
Physical Size = 118226

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2023-05-03 15:11:14 .....       118032       118044  flag.svg
------------------- ----- ------------ ------------  ------------------------
2023-05-03 15:11:14             118032       118044  1 files
```

```
└─$ 7z l -slt challenge.zip | grep Method
Method = ZipCrypto Store
```

We can use bkcrack again to find the keys.

To do that, we need to understand what's used every time in svg files :

```
<?xml version="1.0"
```

Now we can attack :

```
└─$ ./bkcrack -C "challenge.zip" -c "flag.svg" -p plain.bin
bkcrack 1.5.0 - 2022-07-07
[15:14:37] Z reduction using 30 bytes of known plaintext
100.0 % (30 / 30)
[15:14:37] Attack on 246570 Z values at index 6
Keys: 996312c9 d8d9a415 b5b3634e
7.9 % (19595 / 246570)
[15:15:37] Keys
996312c9 d8d9a415 b5b3634e
```

```
└─$ ./bkcrack -C "challenge.zip" -c "flag.svg" -k 996312c9 d8d9a415 b5b3634e -d "enfin.svg"
bkcrack 1.5.0 - 2022-07-07
[15:16:30] Writing deciphered data enfin.svg (maybe compressed)
Wrote deciphered data.
```

Finally we have the flag :

PS: Here are the passwords used :
I_love_R1ckRoll1ng
th1s_1s_N0t_a_R1ckRoll
P455_50_5Tr0nG_U_c4n'T_Gu355_IT