

Day 3 Challenge 2

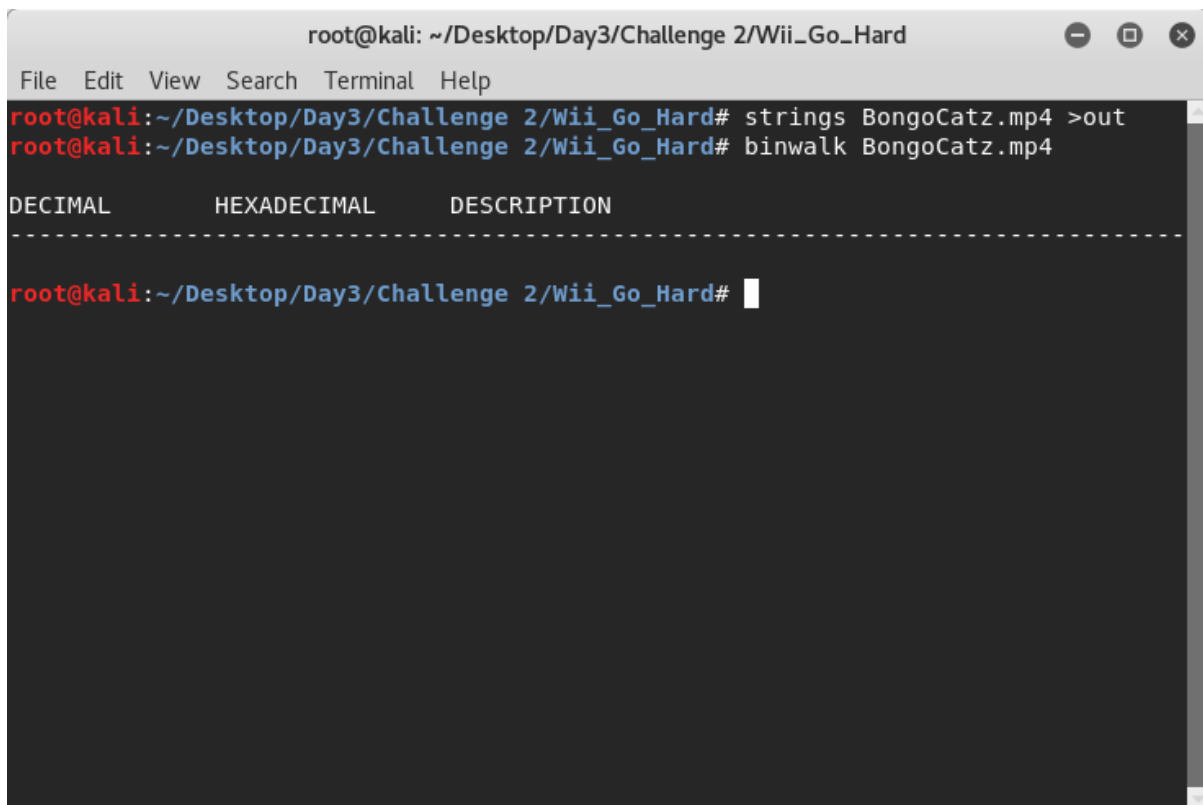
By Bingsu Strawberry from IIUM

Step 1 :

We received a zip file and a mp4 file. First thing first, we watched the video to look for anything in the video itself. Then we watched it again and again because it's a fun video to watch. It says kn0wy0uRalpha837. We tried using it as the zip file password but to no avail.

Step 2 :

Time to bring out the big guns. We did some analysis on the mp4 file. We ran binwalk and strings tool on the video .



```
root@kali: ~/Desktop/Day3/Challenge 2/Wii_Go_Hard
File Edit View Search Terminal Help
root@kali:~/Desktop/Day3/Challenge 2/Wii_Go_Hard# strings BongoCatz.mp4 >out
root@kali:~/Desktop/Day3/Challenge 2/Wii_Go_Hard# binwalk BongoCatz.mp4

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
root@kali:~/Desktop/Day3/Challenge 2/Wii_Go_Hard#
```

Binwalk didn't show anything useful. Lets check the strings.

Step 3 :

Checking the strings lead us to something!

```
Open  out  Save  ~/Desktop/Day3/Challenge 2/Wii_Go_Hard
Zmeta
!hdlr
mdirappl
-ilst
data
Lavf57.41.100
FFFFFFFFKMYUETSSGNZTAYSWHB4FQ6TEN5GTCOLNKRCFE3TGKE6T2===FFFFFFFFFeb63Y4L+0B/
1r7ofIwslqP9MFtgZXcEWpyNRdJSxzDikC5=A82jGaVUqhKuH0mTnvFFFFFFFFFu7NxH9IzG+XpeUr0baLyCYZQ6VsKndKfgBmo5h0MJ1PRv
lq4FE3jWDvcASit8FFFFFFFFFb9de6haAN1uMU0FoTYzR+BXxn8KCKLj2PmGqHDZpyIgWvrEfS4wJ/
0cQ75iV3st=FFFFFFFFFch1ck3nd1nn3rFFFFFFFFF
```

This is the last part of the strings. It doesn't seem natural in any way. First we see at the last part something that says ch1ck3nd1nn3r which means chicken dinner. We tried that as the zip file password but that's not it. Maybe it's just something fun that KPMG left us.

The first line of the strings look suspicious. Removing some clutters from the line leave us with this line "KMYUETSSGNZTAYSWHB4FQ6TEN5GTCOLNKRCFE3TGKE6T2=". It doesn't look to be base64 but the = at the end makes us think its encoded using base system.\

Step 4:

We tried decoding the line using base32

Base32 Decode Online - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Base32 Decode Online x Kali Linux, an Offensive S... x Base64 Decode and E... x +

https://emn178.github.io/online-tools/base32_decode.html

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

Base32 Decode

Base32 online decode function

KMYUETSSGNZTAYSWHB4FQ6TEN5GTCOLNKRCFE3TGKE6T2=

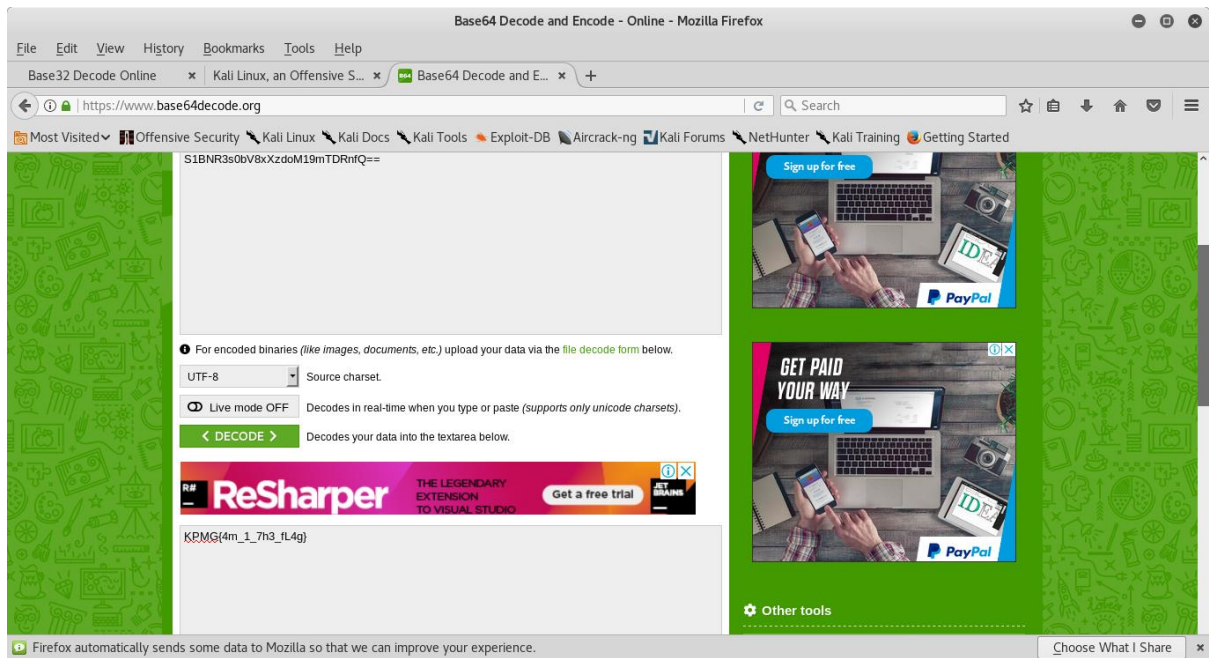
Decode ☒ Auto Update

S1BNR3s0bV8xXzdoM19mTDRnfQ==

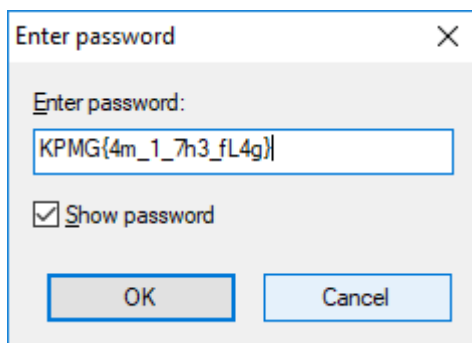
Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

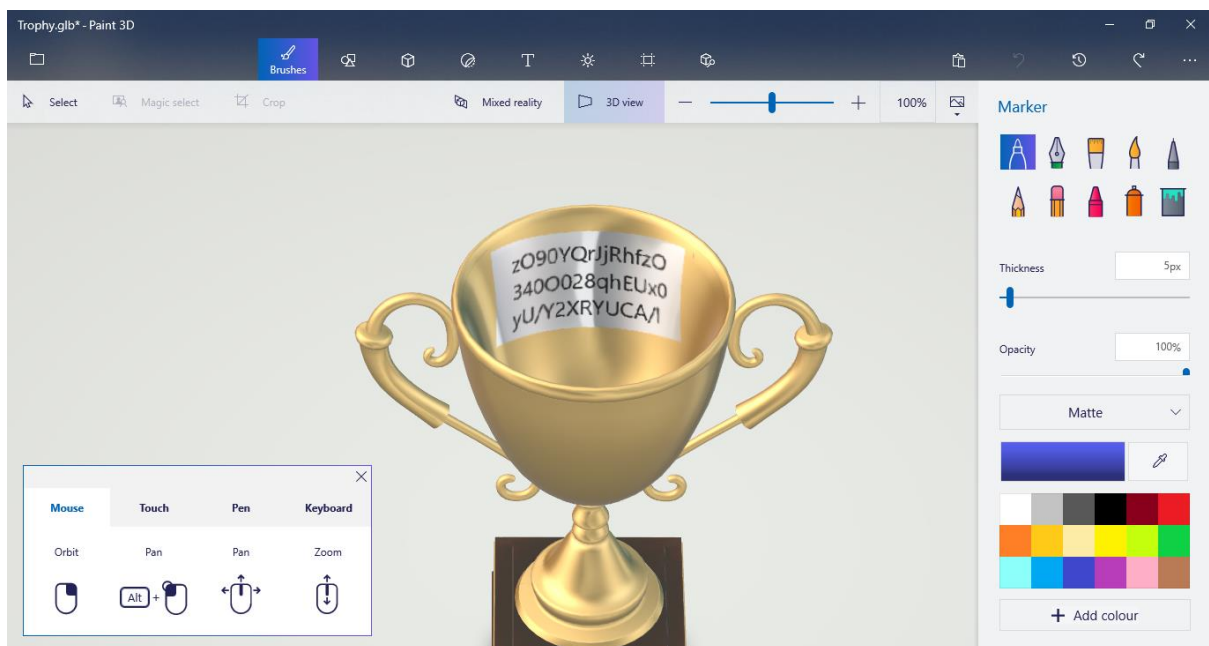
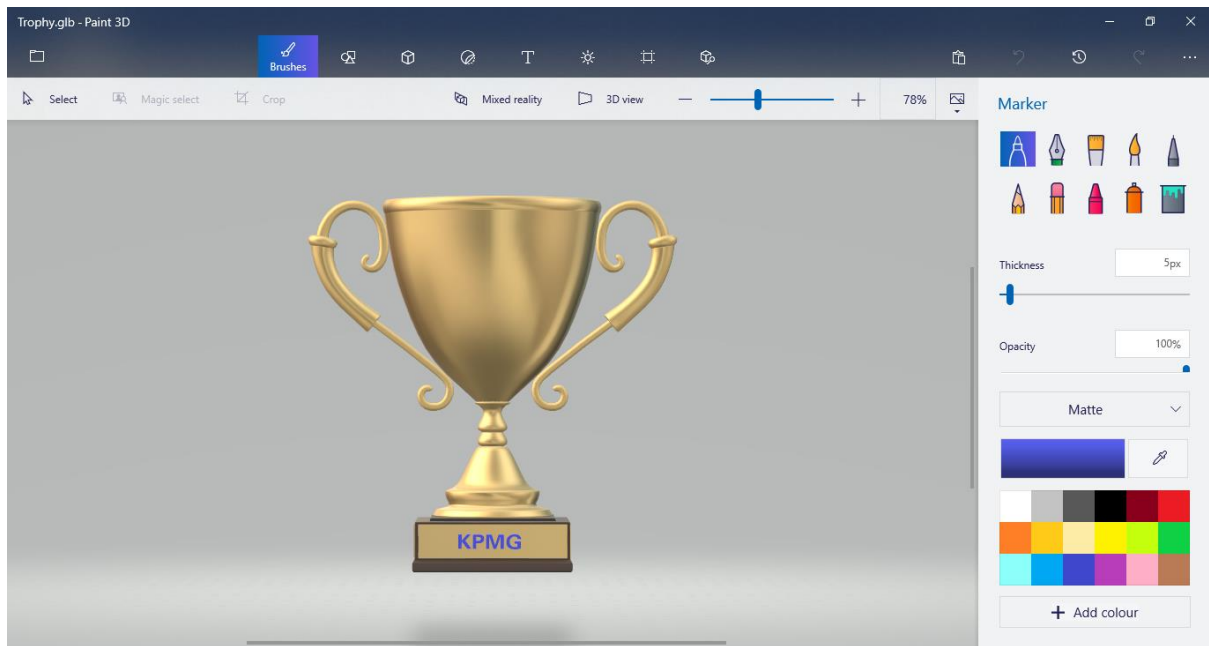
Now to convert it from base64 to plain text.



We found it! This looks to be the flag. KPMG{4m_1_7h3_fL4g}. To verify, we tried using the text as the zip file password and it worked



The zip file contained this



The text on the trophy does make us think. Did we get the right flag?

Flag = KPMG{4m_1_7h3_fl4g}