Zero_Prime9

— You are seen or you will be seen —

ZP9

@zero_prime9

@zero_prime9

APU_BOH WRITEUPS

WWW.ZEROPRIME9.COM

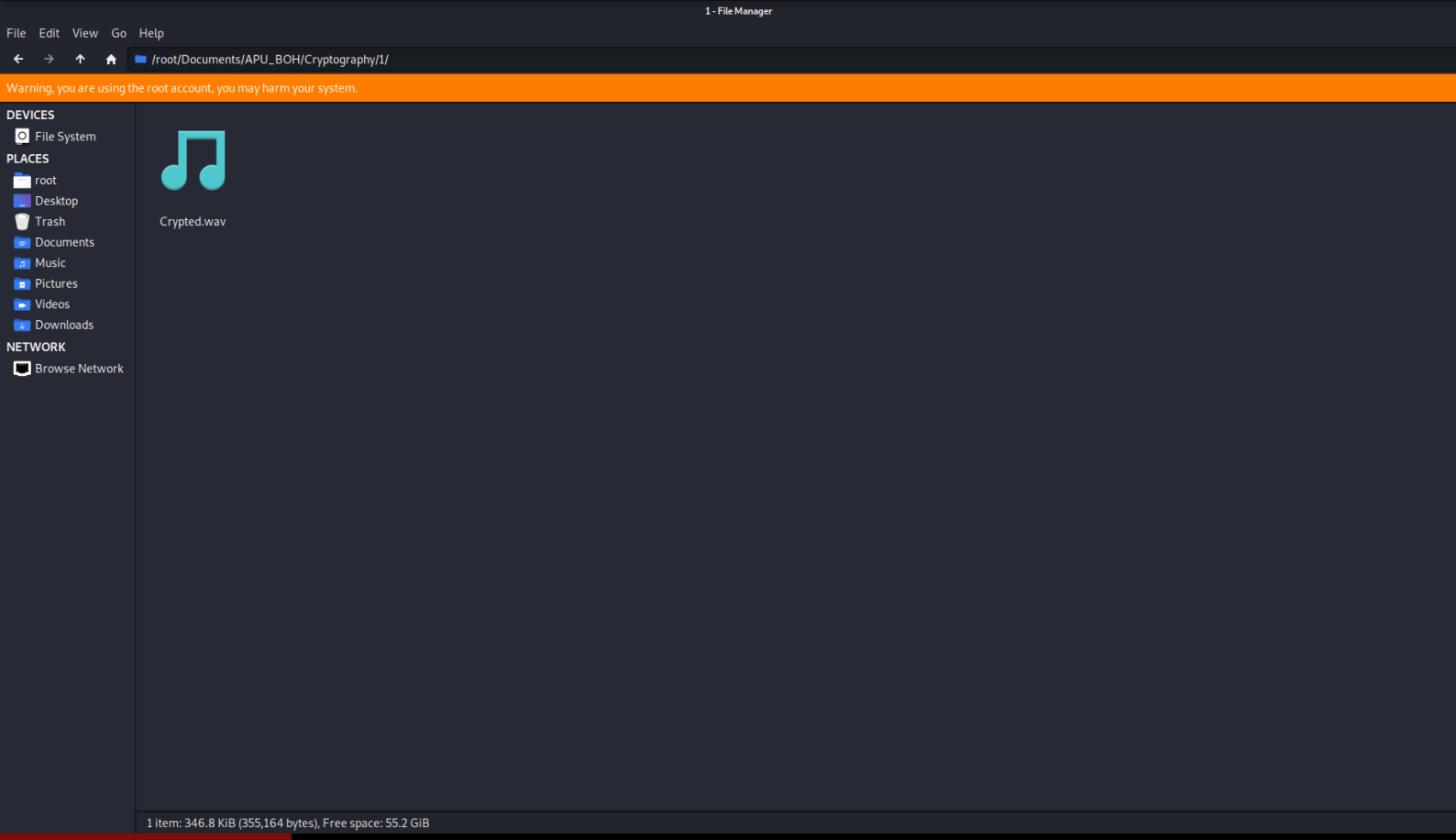
ZERO_PRIME9

— You are seen or you will be seen —

1

CRYPTOGRAPHY

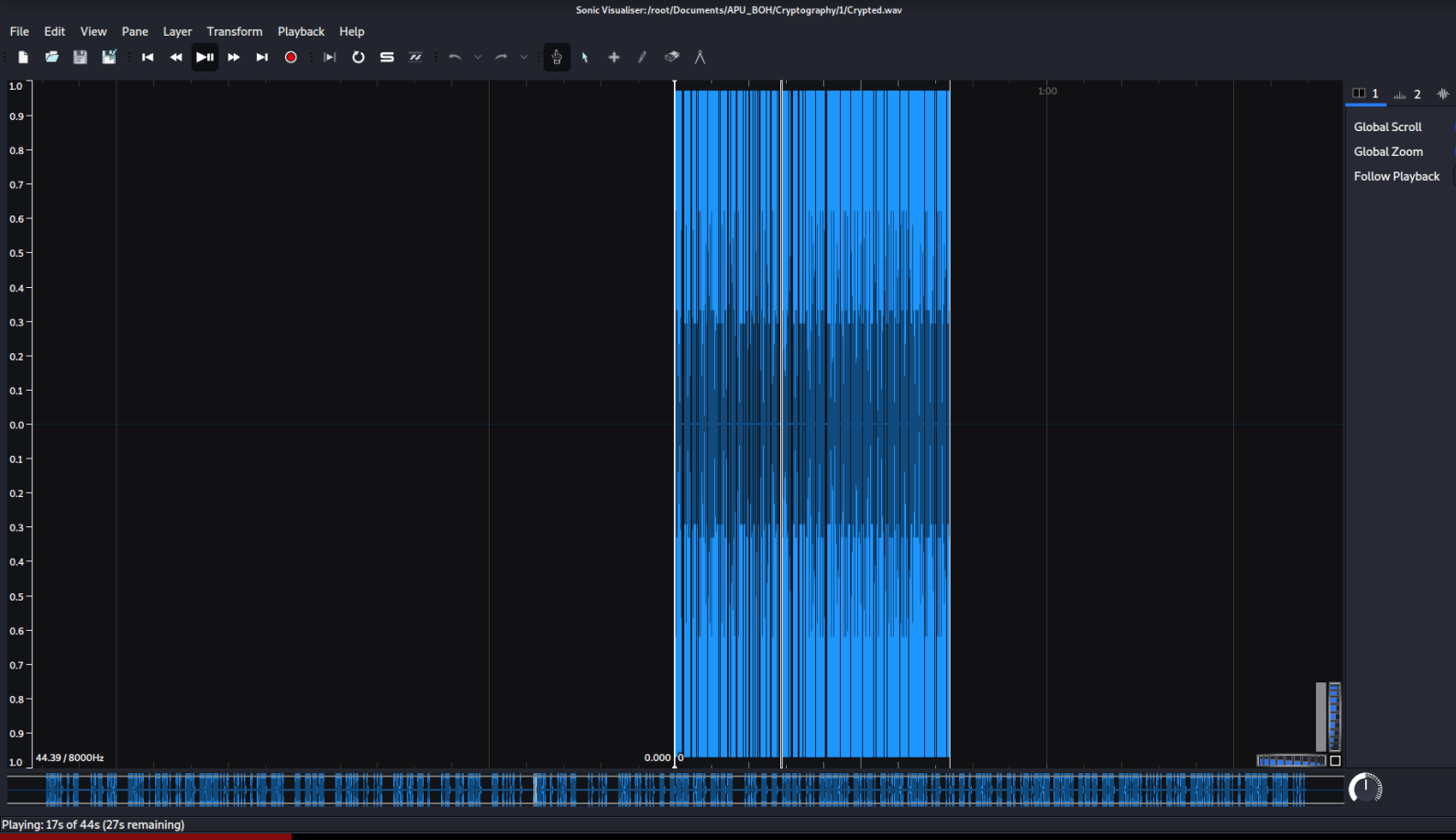
Lost In Transalation



0EX00: PROLOGUE

Welcome to Lost in Transalation, This is a moderate challenge yet. If done well will give you good insights of the multitude of crypts around the world. Especially for certain Capture The Flags. Hope you all enjoyed this one and we shall proceed.

~ Zero_Prime9

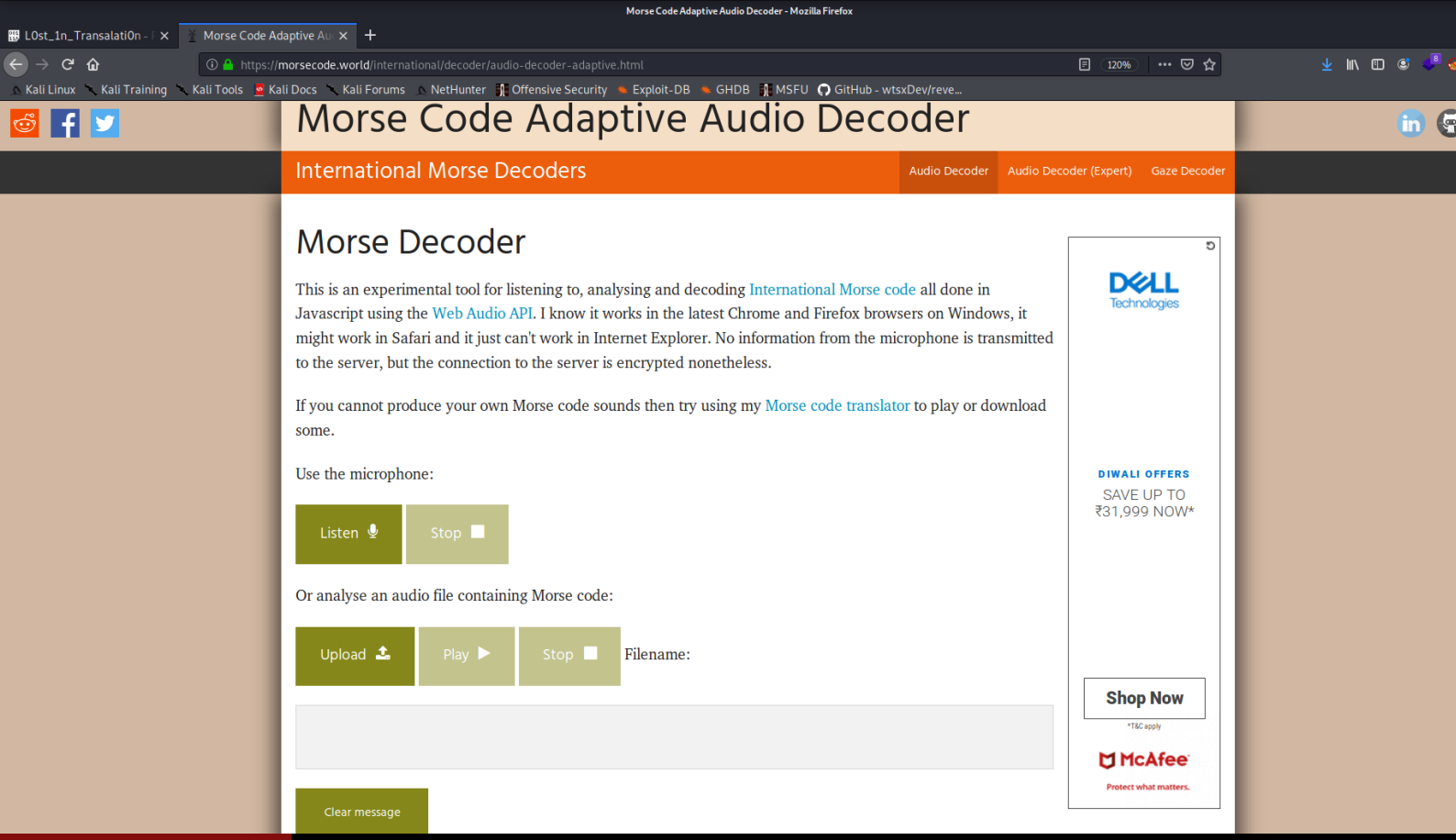


0EX01: MORSE CODE

~ ZERO_PRIME9

On clicking and hearing the **Crypted.wav**, You hear a distinct pauses of dots and slash. This type of distinct sound is known as Morse Code. It can be represented in Text, Voice and Light.

To proceed we head to google and type in Morse audio decoder.

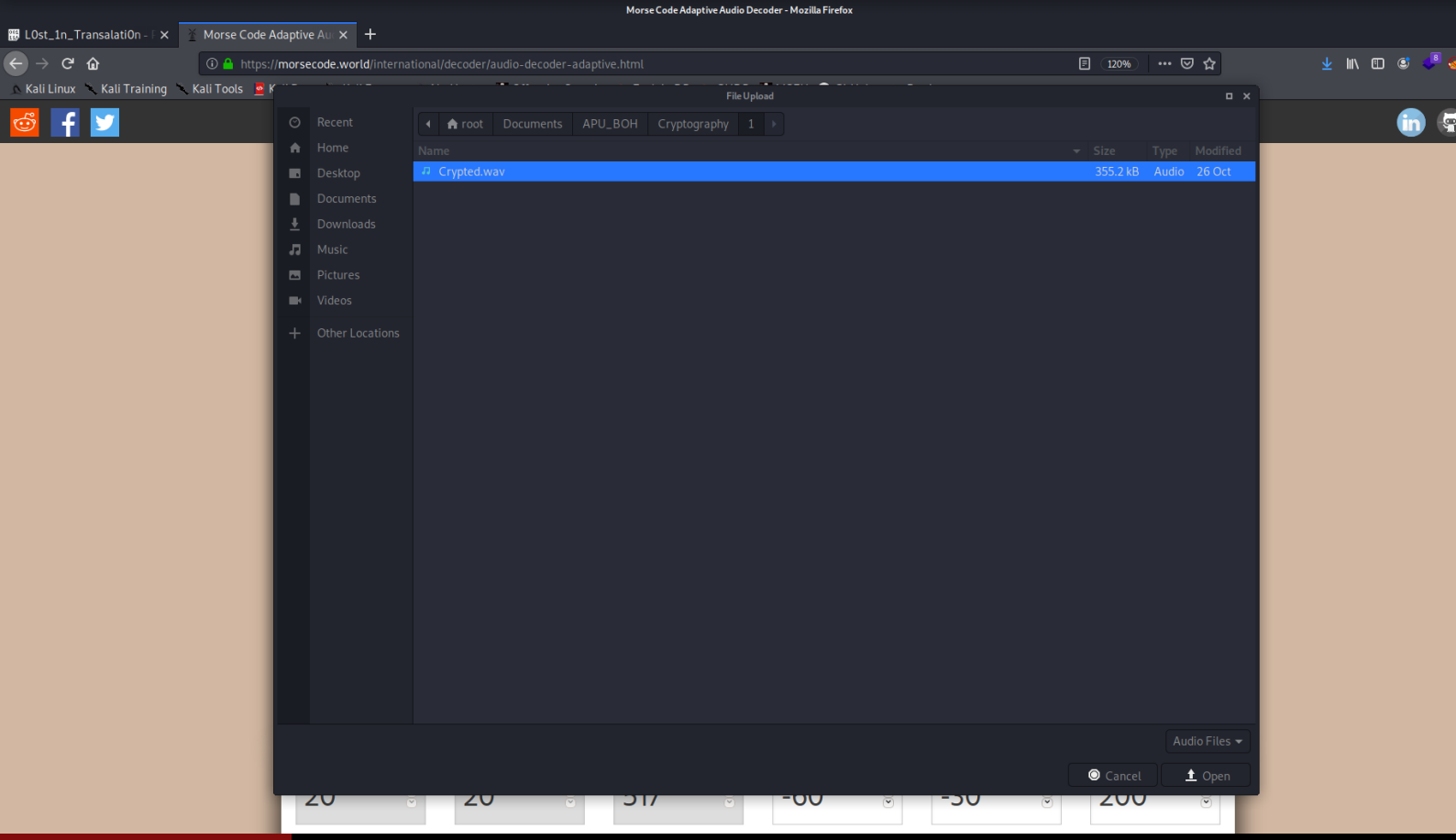


0EX02: MORSE WORLD

~ ZERO_PRIME9

Head to any morse audio decoder website. The one used here is https://morsecode.world/

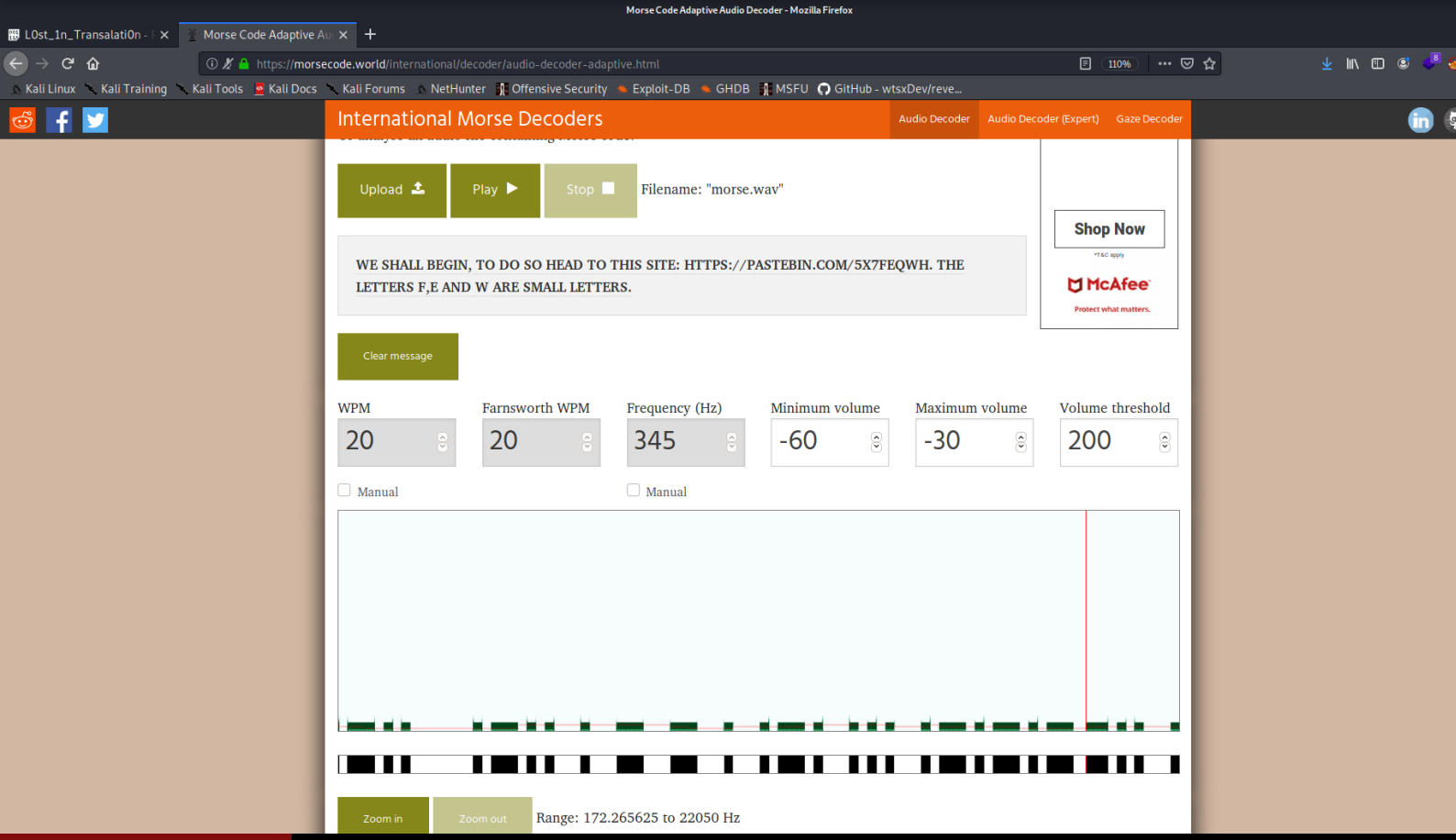
This website is dedicated to Morse and Morse only so anything to encode or decode.



0EX03: UPLOAD

~ ZERO_PRIME9

Select on the upload button and upload the Crypted.wav file on to the website.

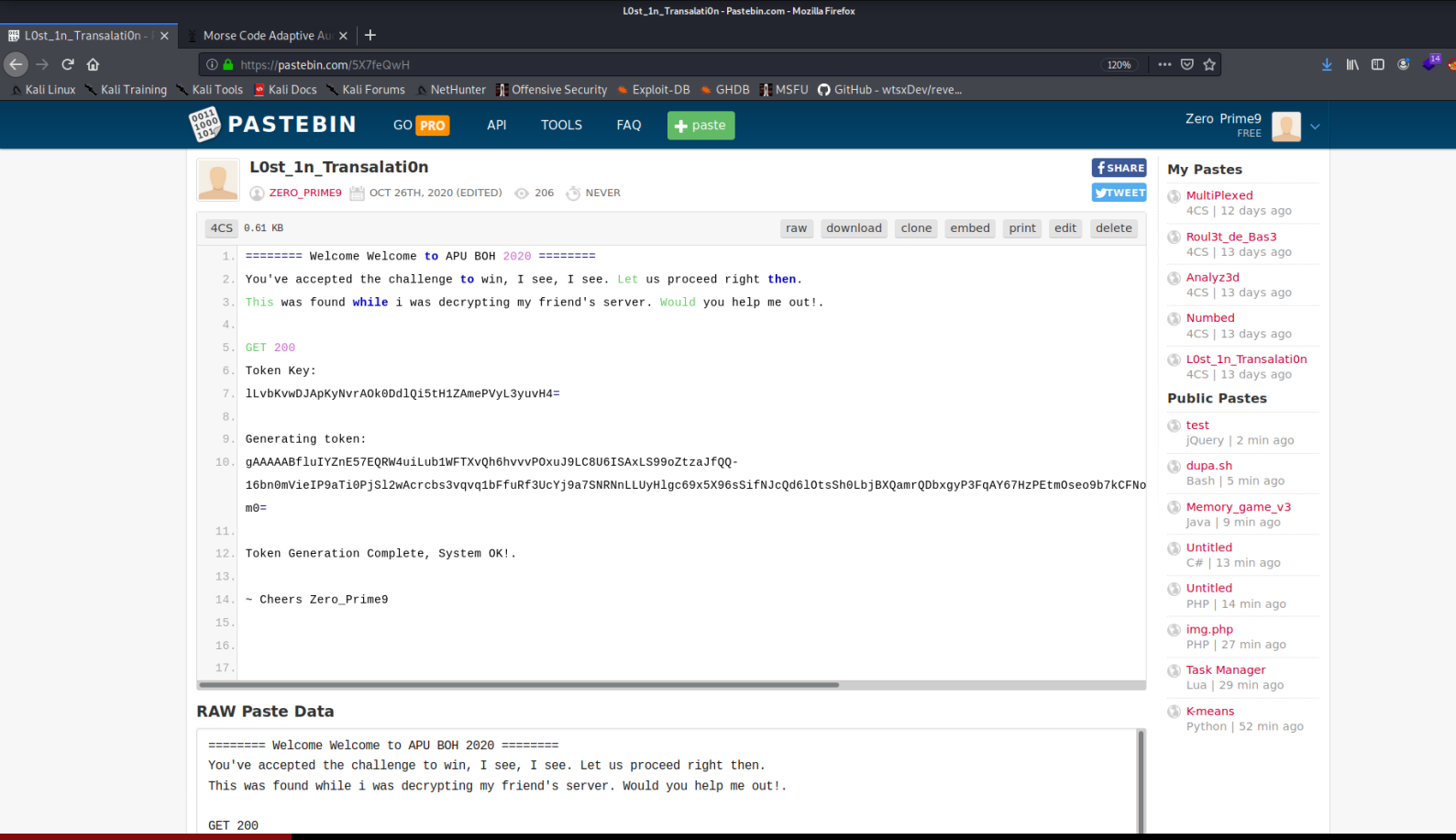


~ ZERO_PRIME9

0EX04: DECODE ... --- ...

Now the best bit, Click on play and the website actually takes the frequency of the sounds both high and low then converts them into ASCII. On doing that you should be greeted with a paste bin page specifically telling about the Capitalization .

Let us move on to the pastebin page

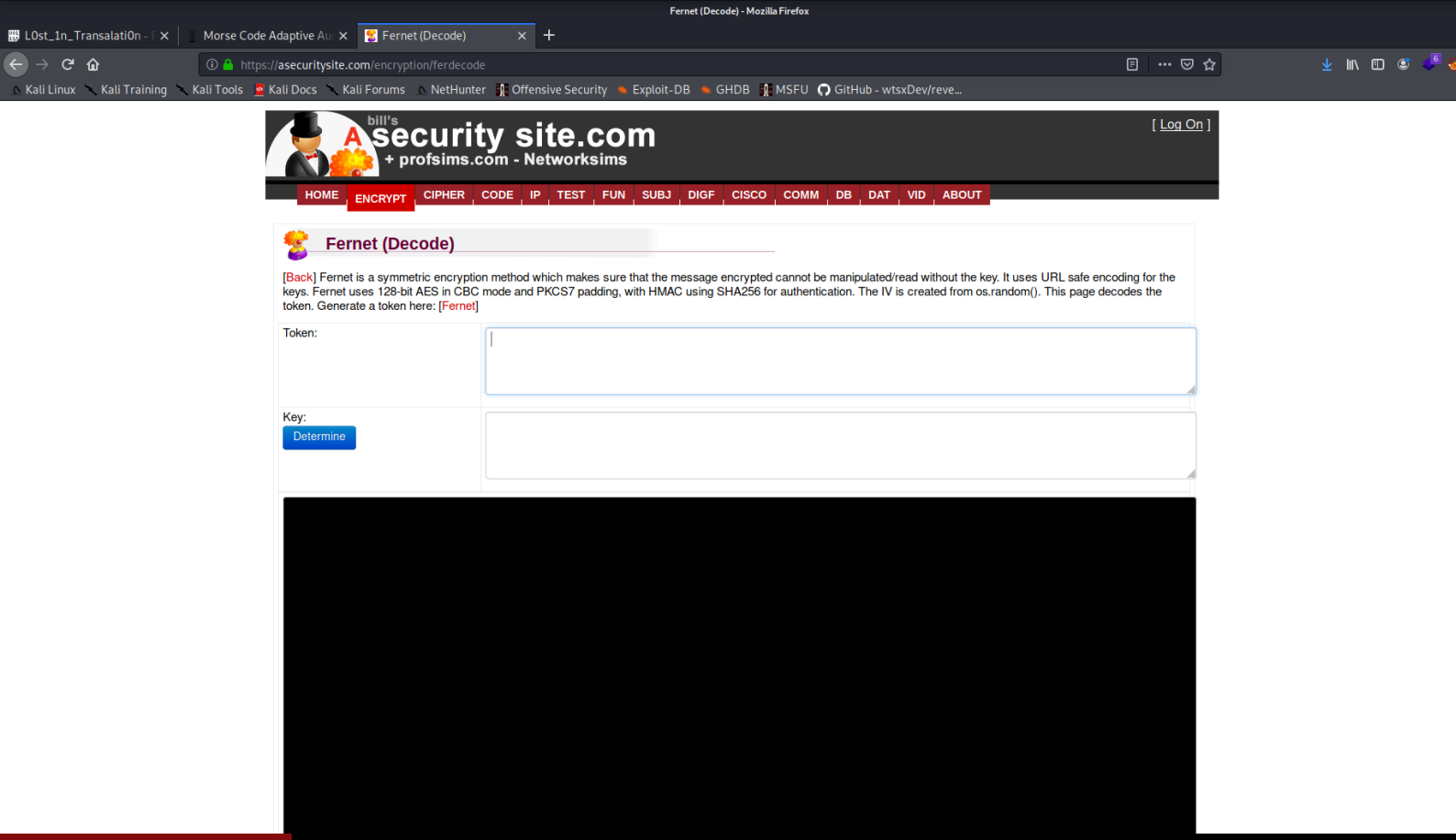


~ ZERO_PRIME9

0EX05: PASTEBINED

We are greeted with a story followed by a Token and Key.
The token seems like a URL based encoding and as it starts with "gAAA" The only encryption of that sort is Fernet.

Head to Google and type in Fernet decoder and look for any Fernet Decoder present



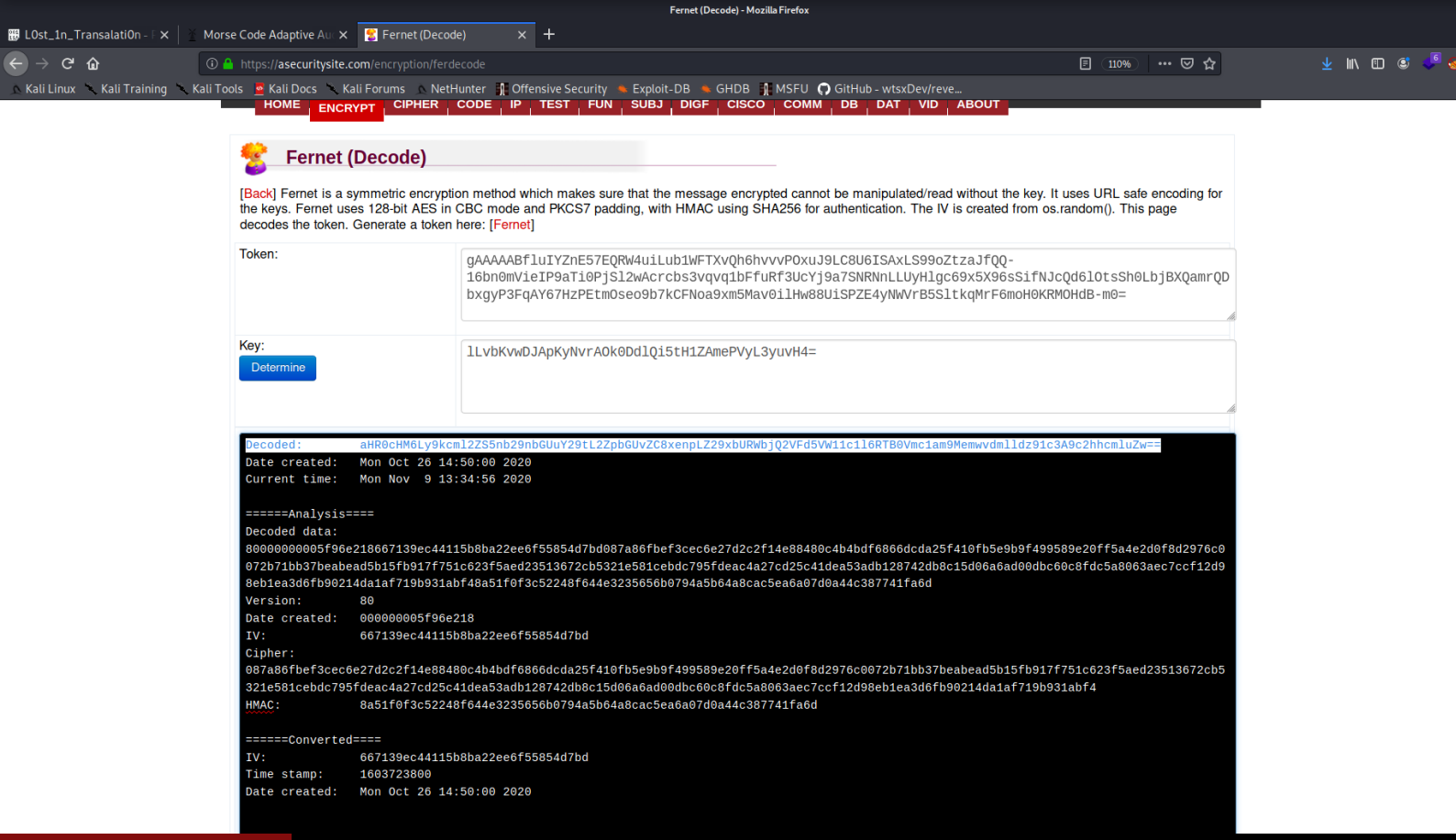
0EX06: FERNET WHO?

~ ZERO_PRIME9

You will see two boxes, one foken and the other key. When we look back at paste-bin we see the same two crypts. Copy and paste it in the appropriate box and press decode.

Fernet is a Symmetric Encryption.

The website i use here is: https://asecuritysite.com/encryption/ferdecode



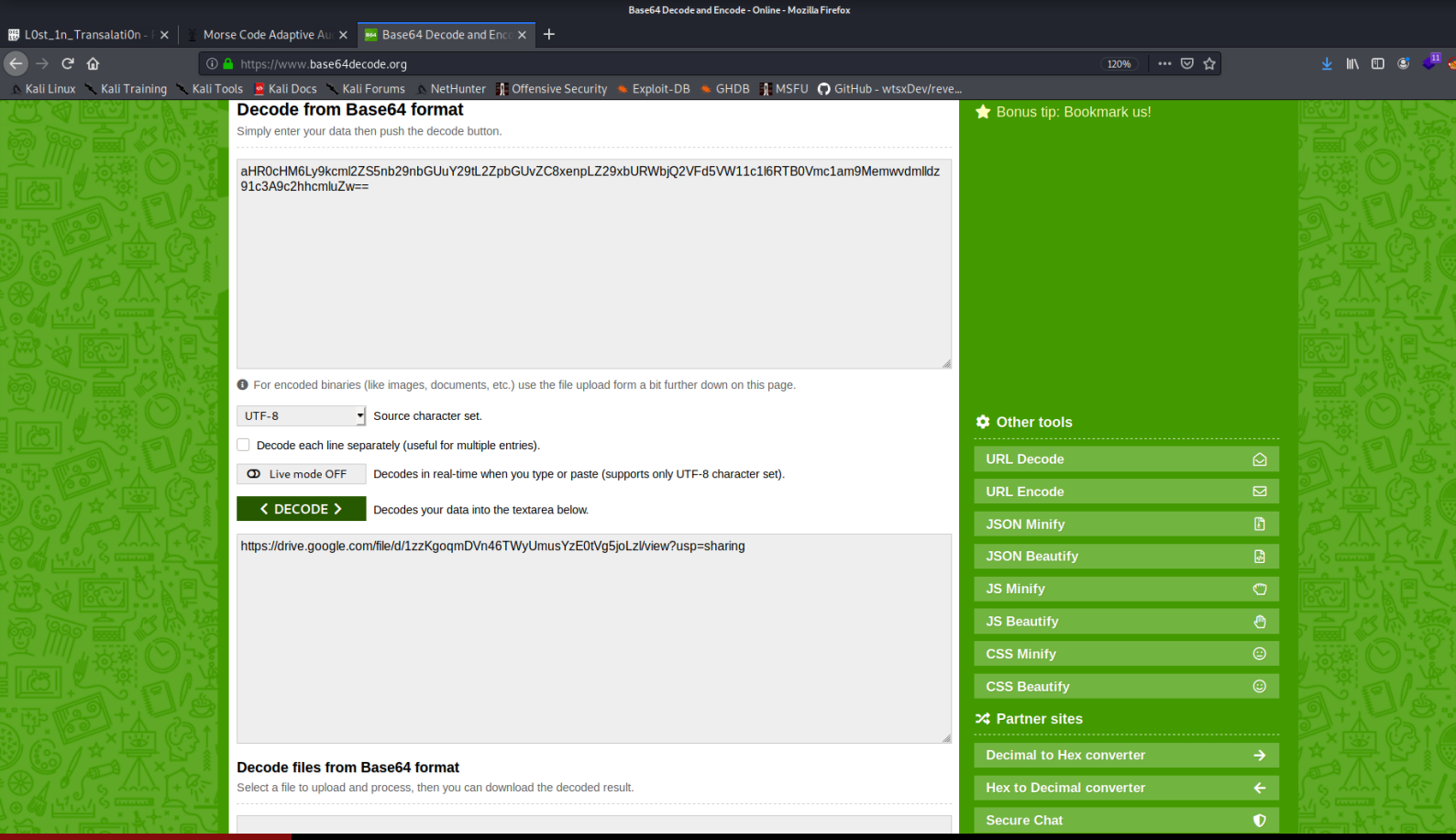
0EX07: FERNET DECODED

~ ZERO_PRIME9

On pressing Decode you will see a lot of data. Most of it telling the Analysis part of the Decryption that took place.

When you look at the top portion you will see Decoded: and a Base64 hash. How do we know its Base64? It ends with 2 "=" signs.

We have thus de-crypted Fernet



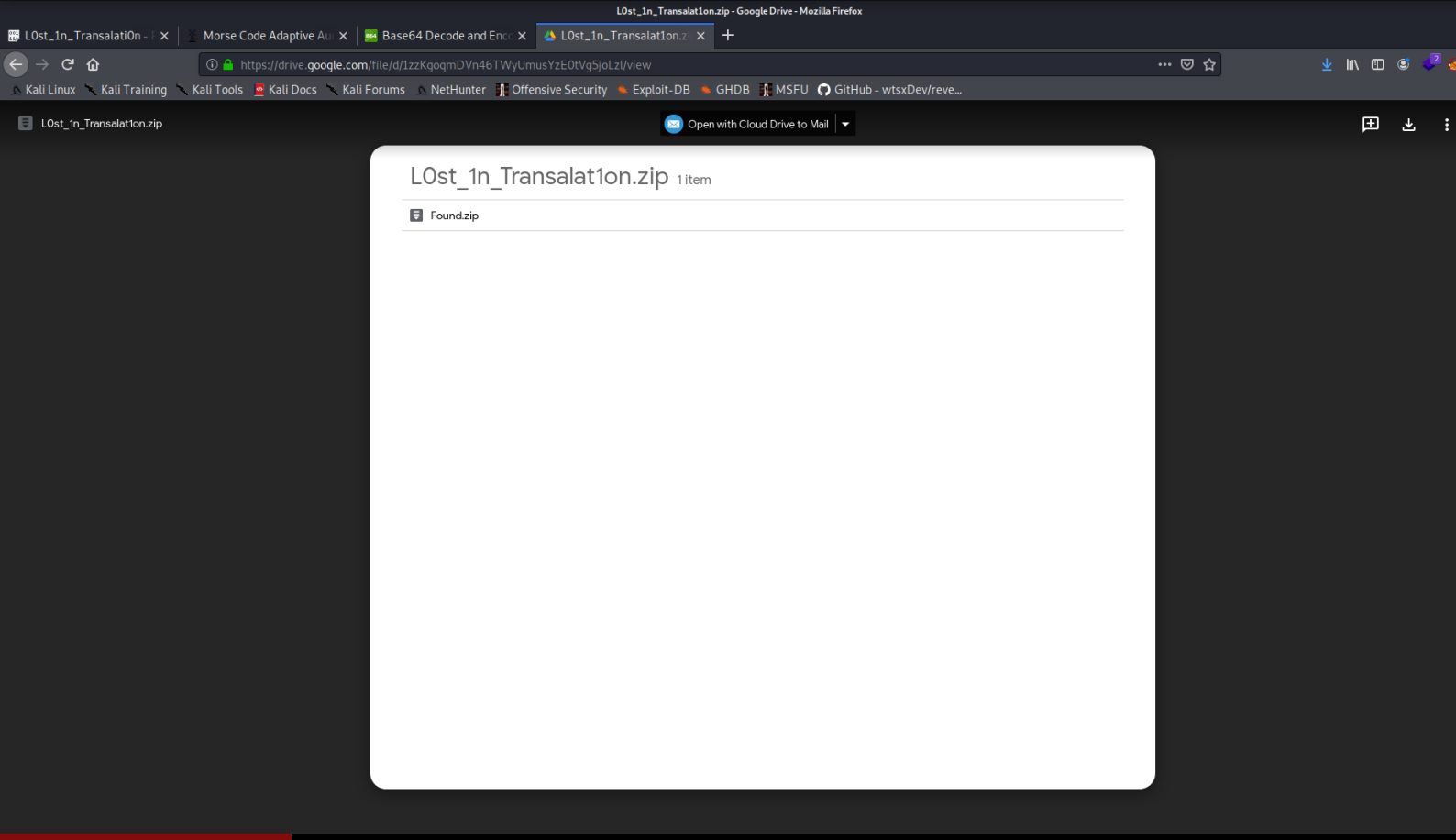
0EX08: BASE DECODED

~ ZERO_PRIME9

Now we have the Base64 hash we copy it and head to our dear friend google. Then we search for Base64 decoder.

Select any of the base64 decoder sites and decode the hash. It should give you a Google Drive Link.

The website used here is: https://www.base64decode.org/



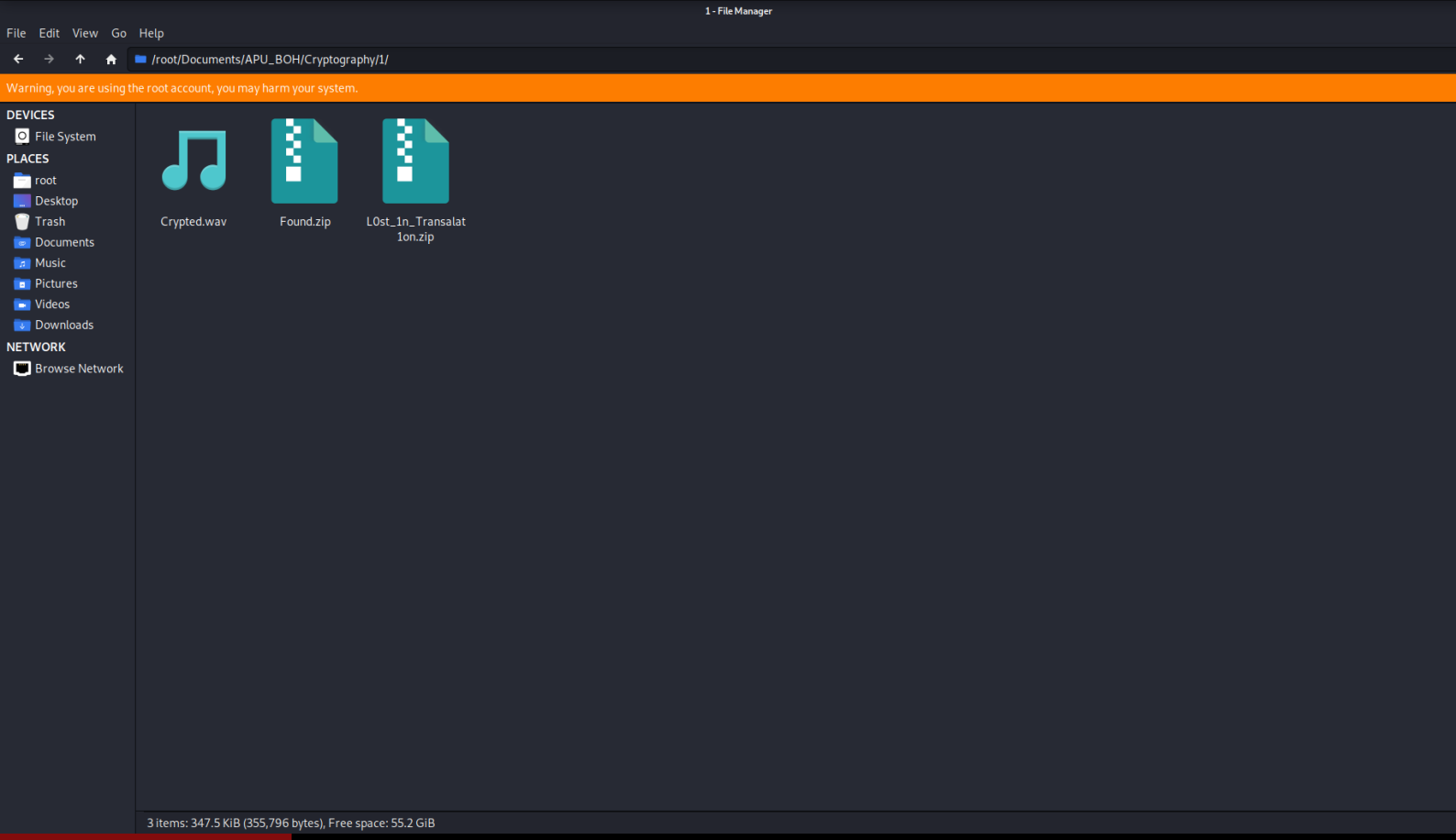
0EX09: LOST IN TRANSALATION

~ ZERO_PRIME9

Aha, we are getting close can we get a Yeehaw!.

We can see within the Lost_In_Transalation Zip File, there is one more zip file called Found.zip.

We will download the Zip file on to our system and proceed forward.

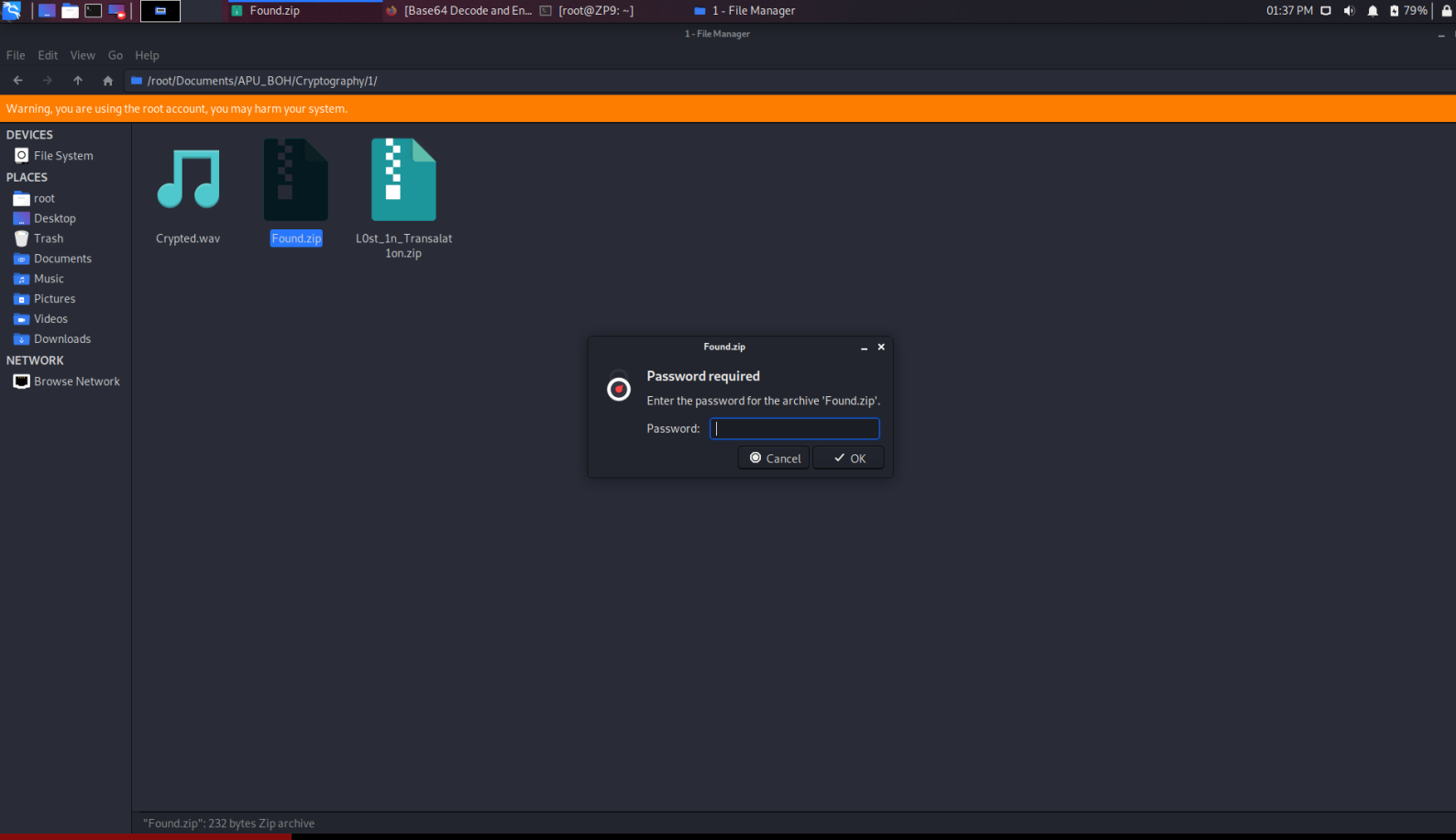


0EX0A: WE ARE CLOSE

~ ZERO_PRIME9

After we download Lost_In_Transalation and then unzip the file. We get one more Zip file which is Found.zip

We know we are going to unzip this one more time right

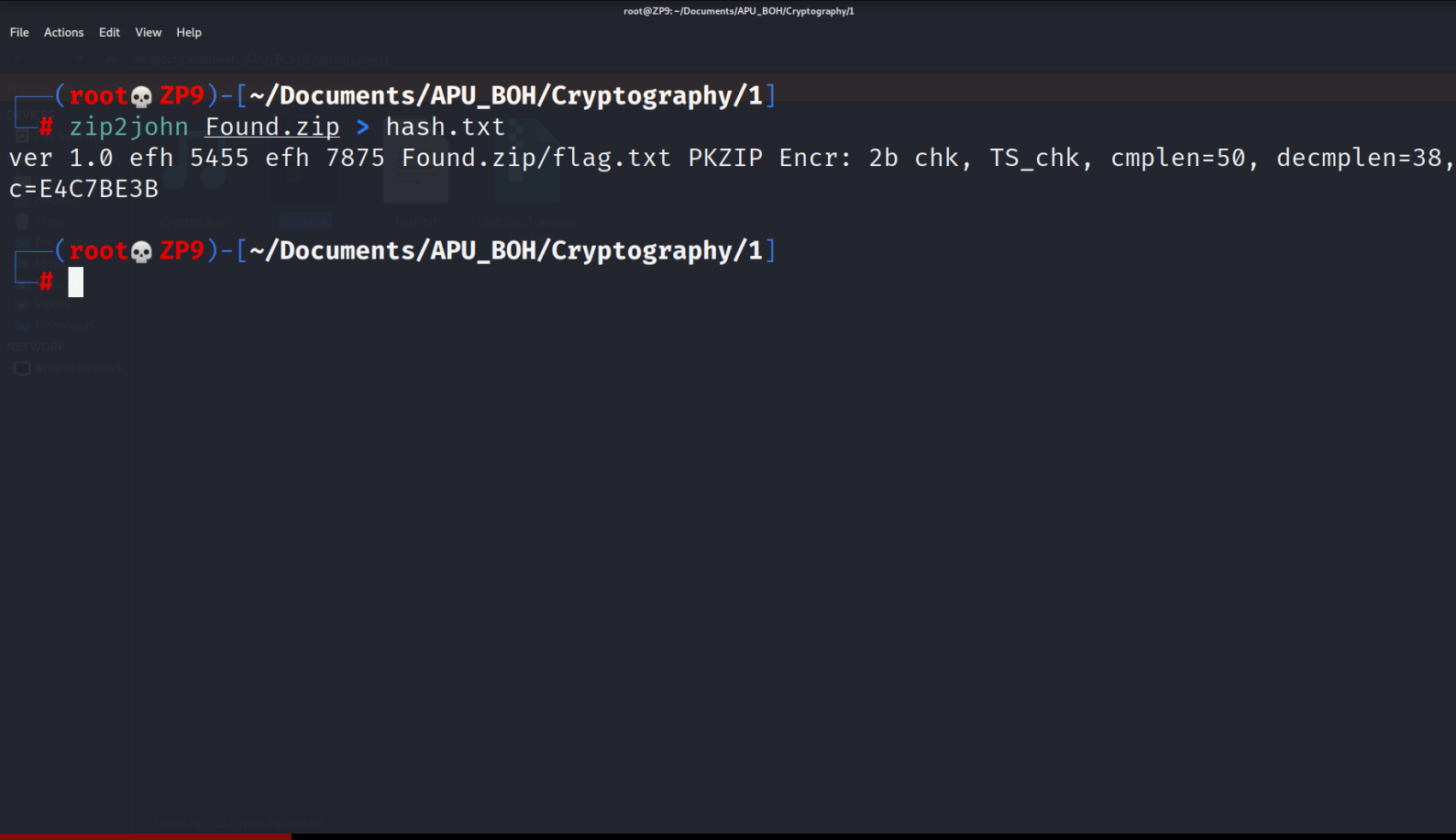


0EX0B: BAMBOOZLED

~ ZERO_PRIME9

OH SHOOTS!.
On clicking unzip its asking for a password. Well then we will use our handy dandy tools called zip2john.

Zip2John is a tool based of on John The Ripper, it extracts the hash from the Zip file so we can use John to de-crypt the hash using custom word-list.



~ ZERO_PRIME9

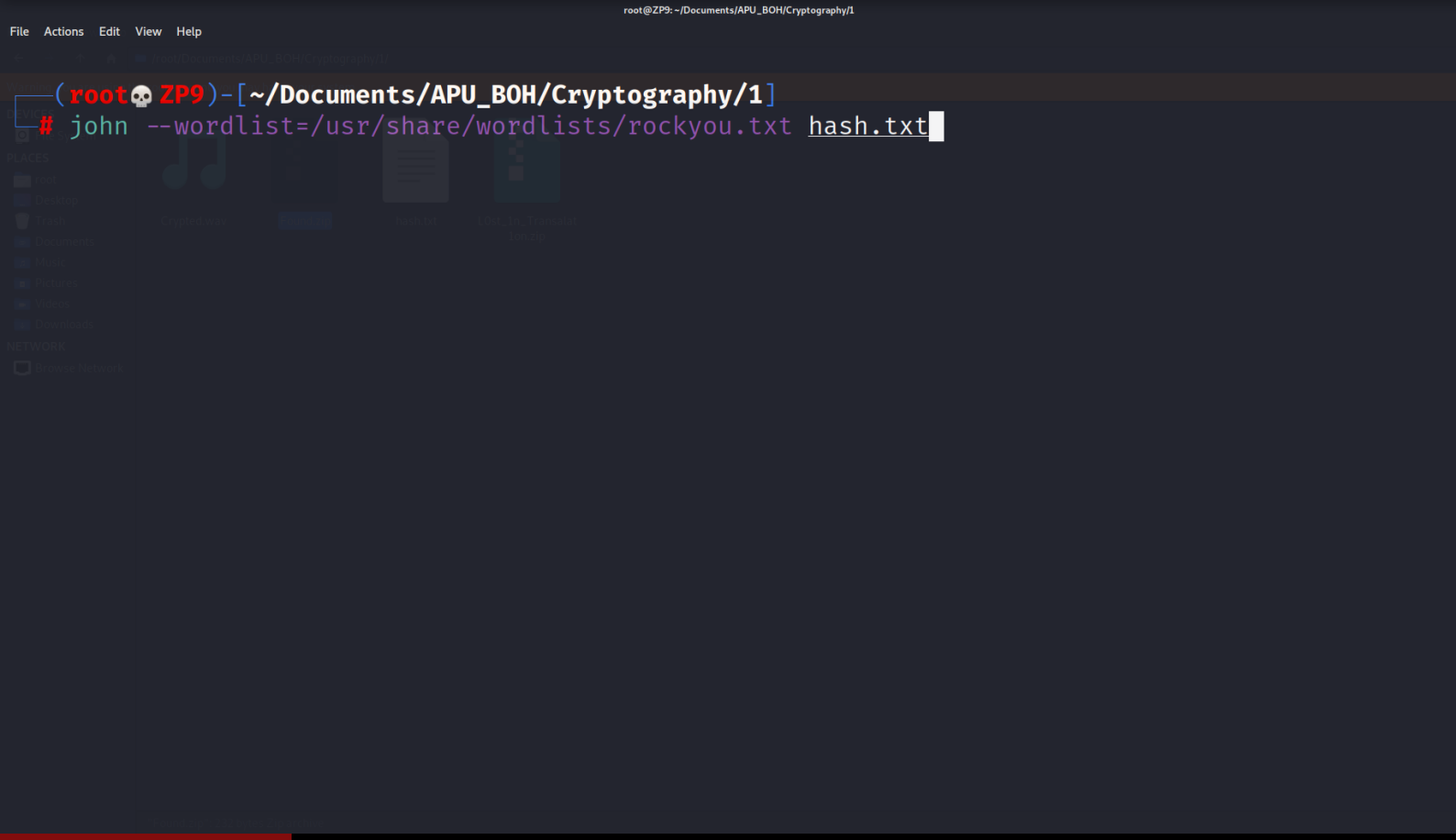
0EX0C: ARE WE CLOSE?

By Default Zip2John is installed on Kali. If it is not installed you can search for it in google and download it through one of the GitHub repositories .

To get the hash out of the zip file type in

zip2john Found.zip > hash.txt

We are telling zip2john to extract the hash then using the ">" to copy the extracted hash into hash.txt

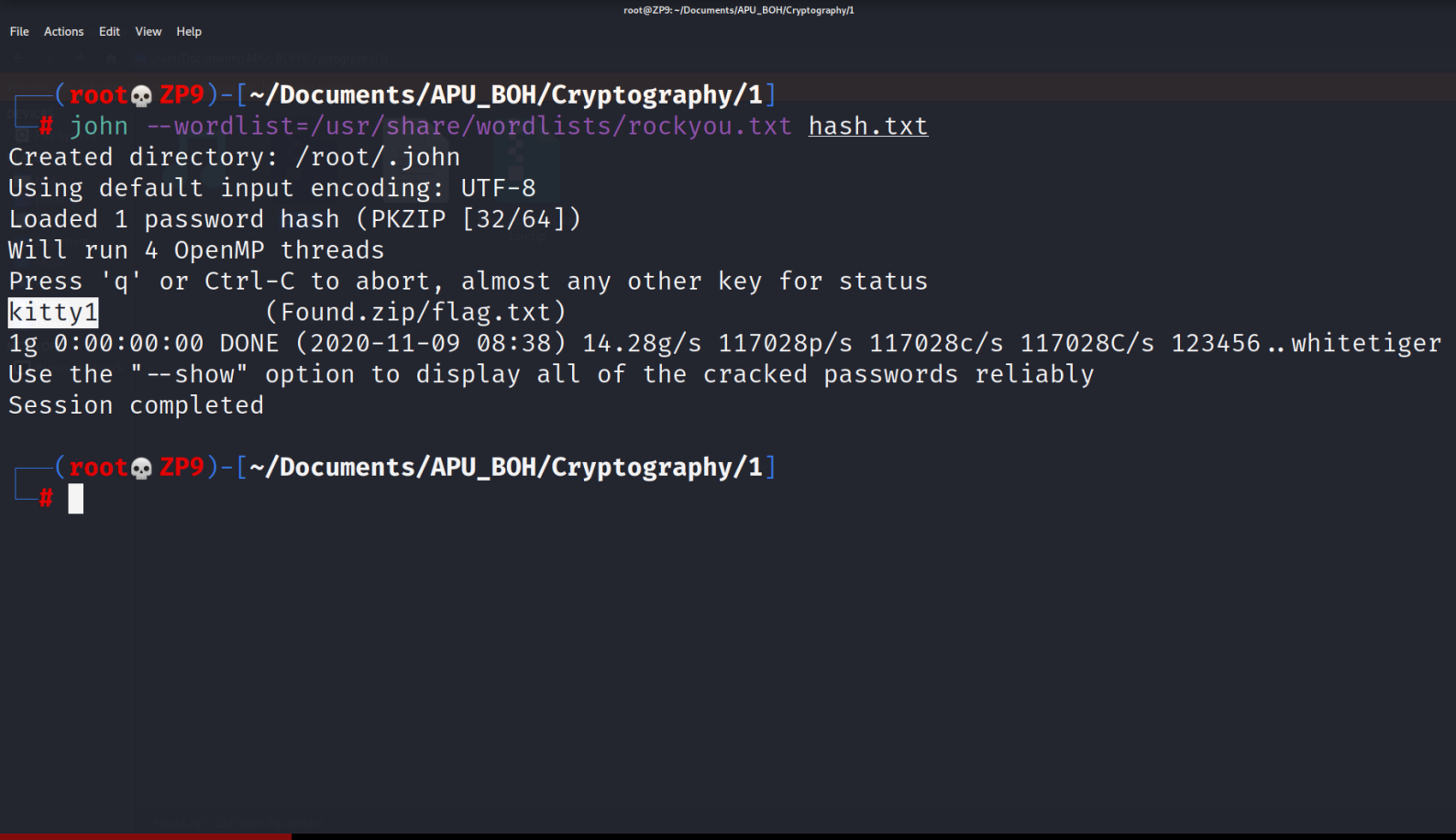


0EX0D: HASHED

~ ZERO_PRIME9

Now we use john to crack the hash.txt
The command is
john --wordlist= /usr/share/wordlists/rockyou.txt hash.txt

--wordlists -> is for telling where the wordlist is
Use rockyou.txt for cracking.



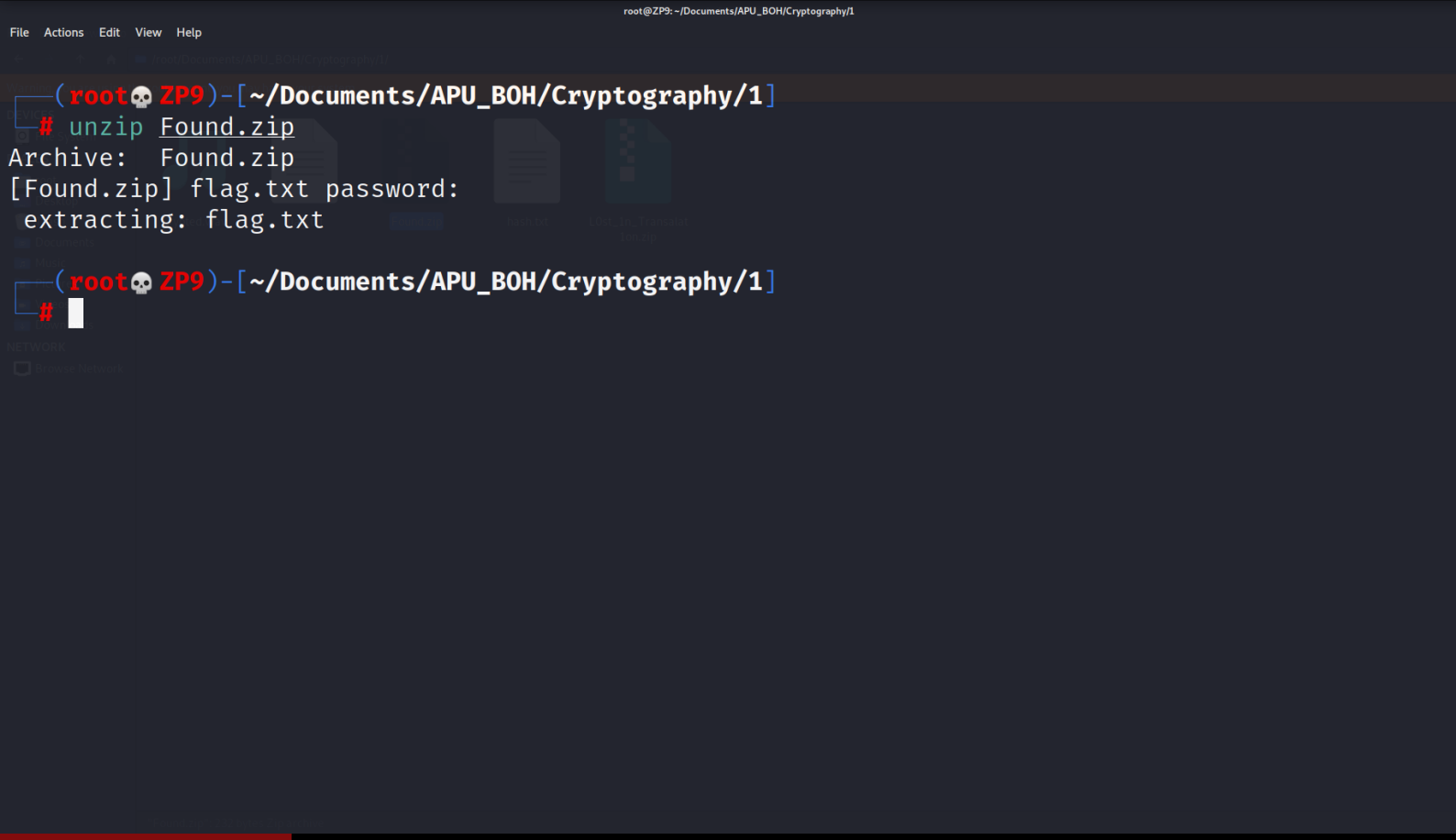
~ ZERO_PRIME9

0EX0E: WE ARE CLOSE II

On typing in the command we can see john starts to do its work. Give it some time and do be patient for this. After 1-4 minutes you will see the decoded password

The decoded password here is kitty1

Use that on the zip file and see if it unlocks

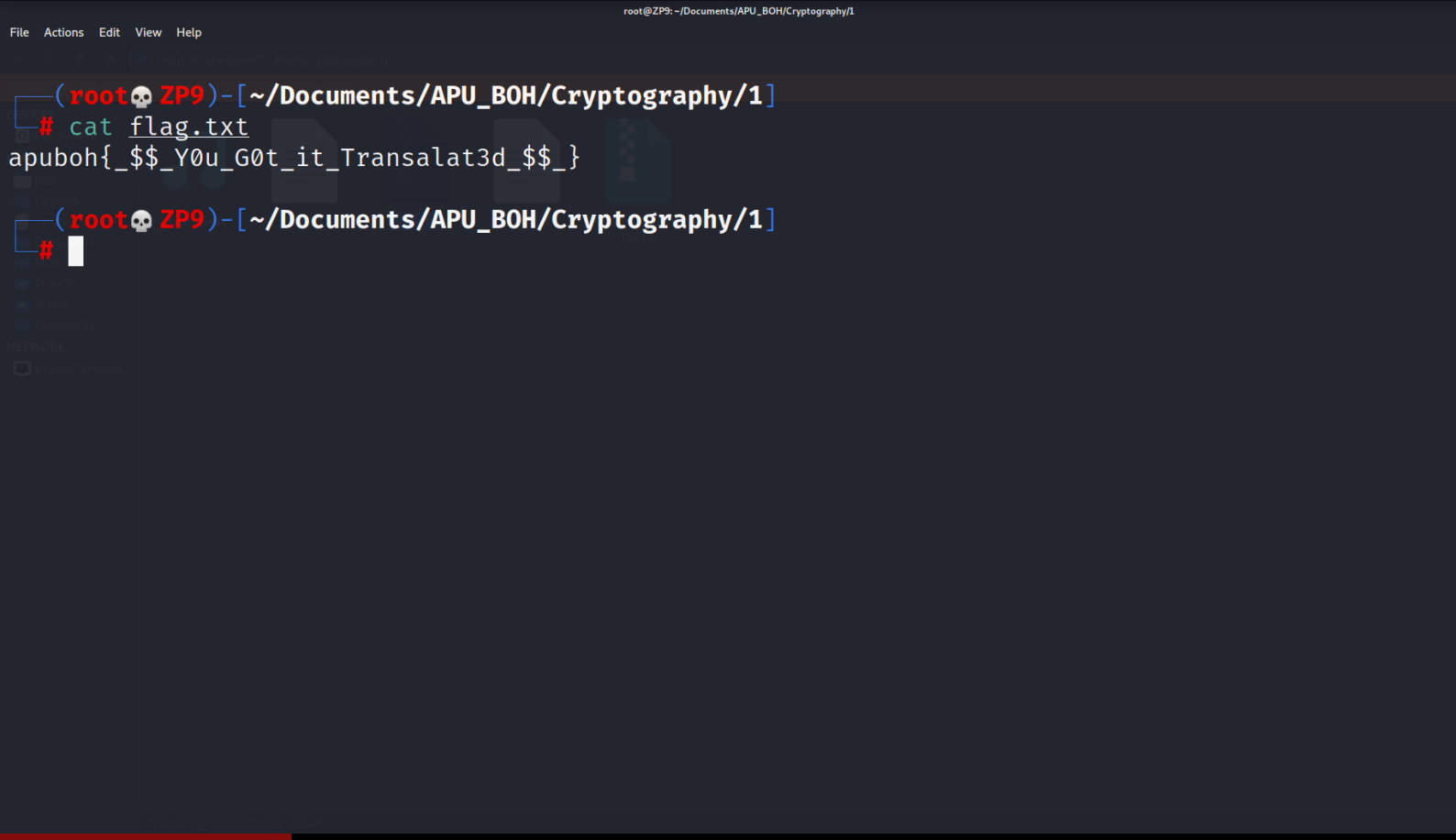


~ ZERO_PRIME9

0EX0F: UNLOCKED

On typing in:
unzip Found.zip
It will ask for the password then type in "kitty1".

You can see the flag.txt unzips successfully.



~ ZERO_PRIME9

0EX10: FLAGGED

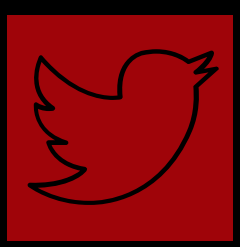
Once you type in "cat flag.txt"
The flag is mentioned and it is apuboh{_$$_Y0U_G0T_1T_Transalat3d_$$_}
Congratulations you just completed the challenge

~ Cheers Zero_Prime9

Zero_Prime9

— You are seen or you will be seen —

@zero_prime9



@zero_prime9

https://www.linkedin.com/in/farzan-nobi/