



ZERO_PRIME9

— You are seen or you will be seen —



APU_BOH
WRITEUPS



@zero_prime9



@zero_prime9

WWW.ZEROPRIME9.COM



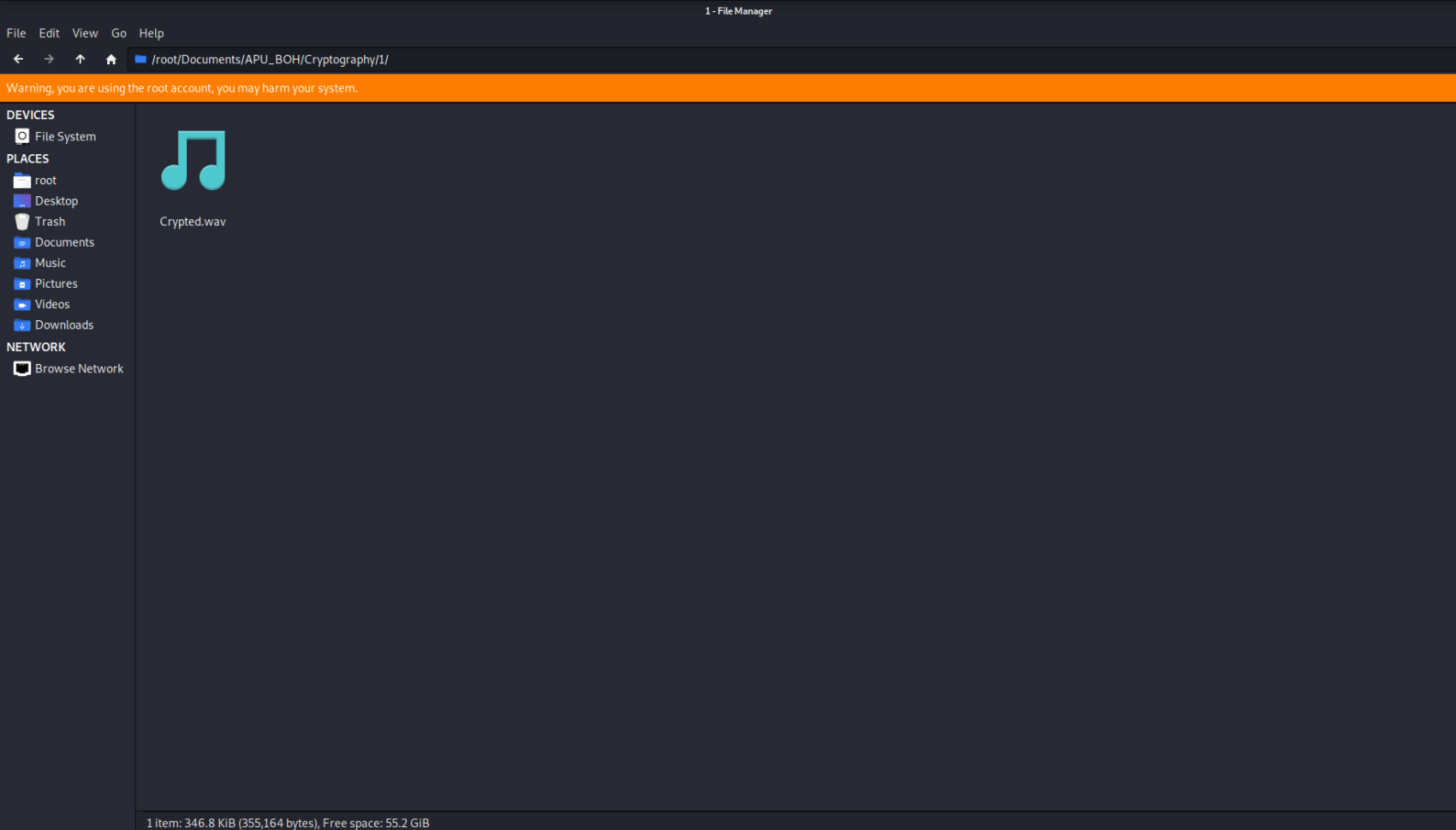
ZERO_PRIME9

— You are seen or you will be seen —

1

CRYPTOGRAPHY

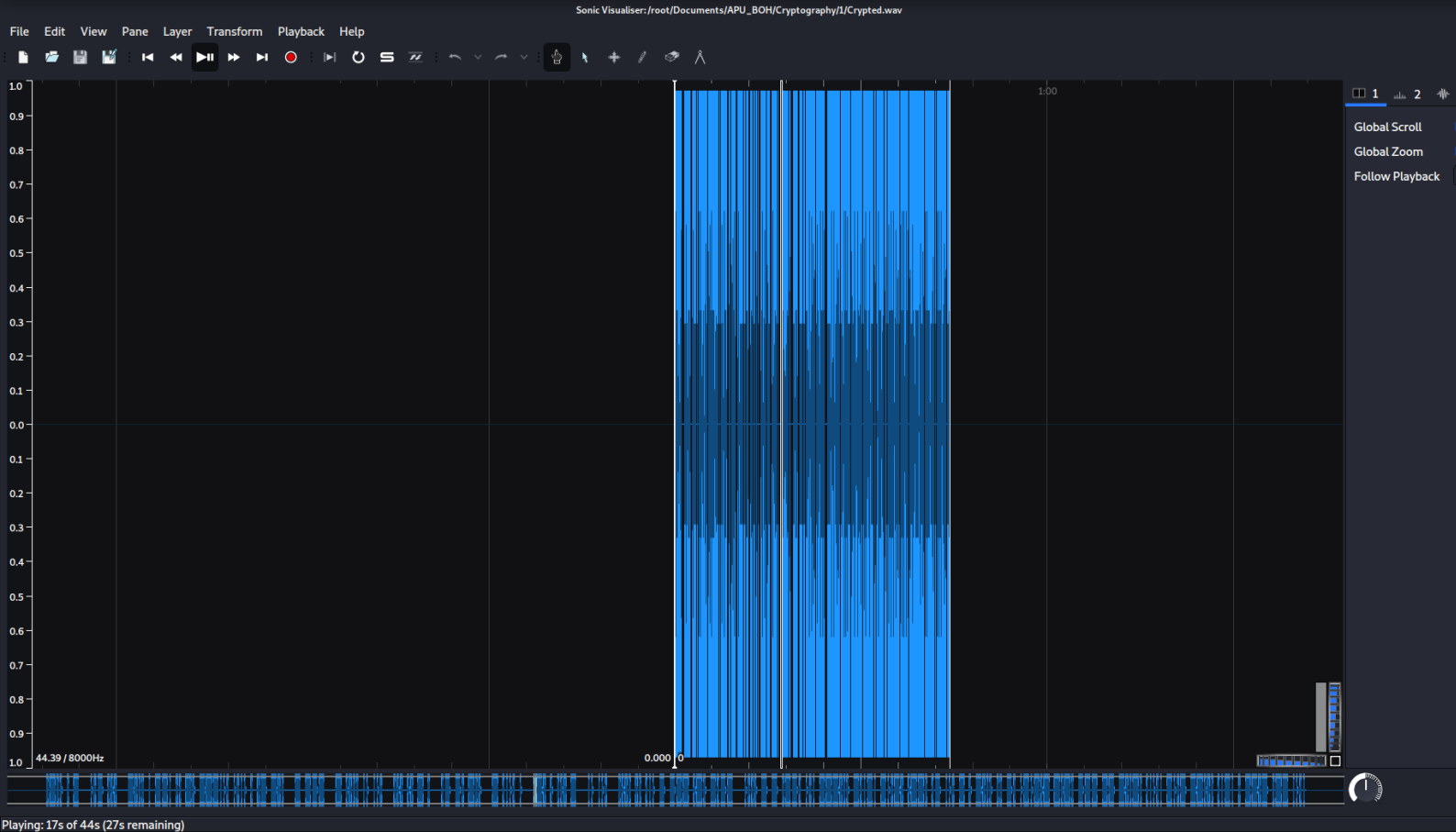
Lost In
Transalation



OEX00: 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

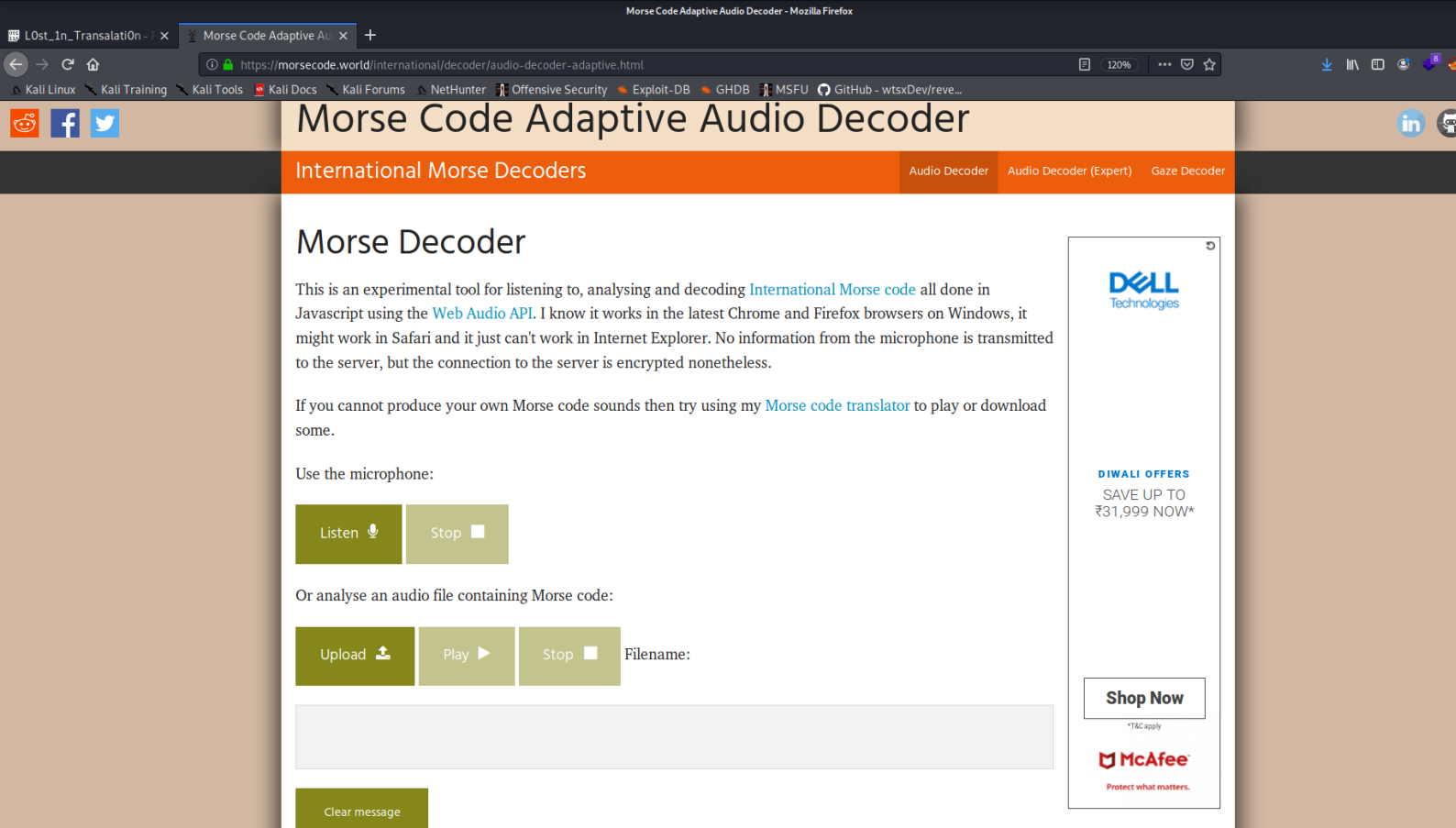


~ ZERO_PRIME9

0EX01: MORSE CODE

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.

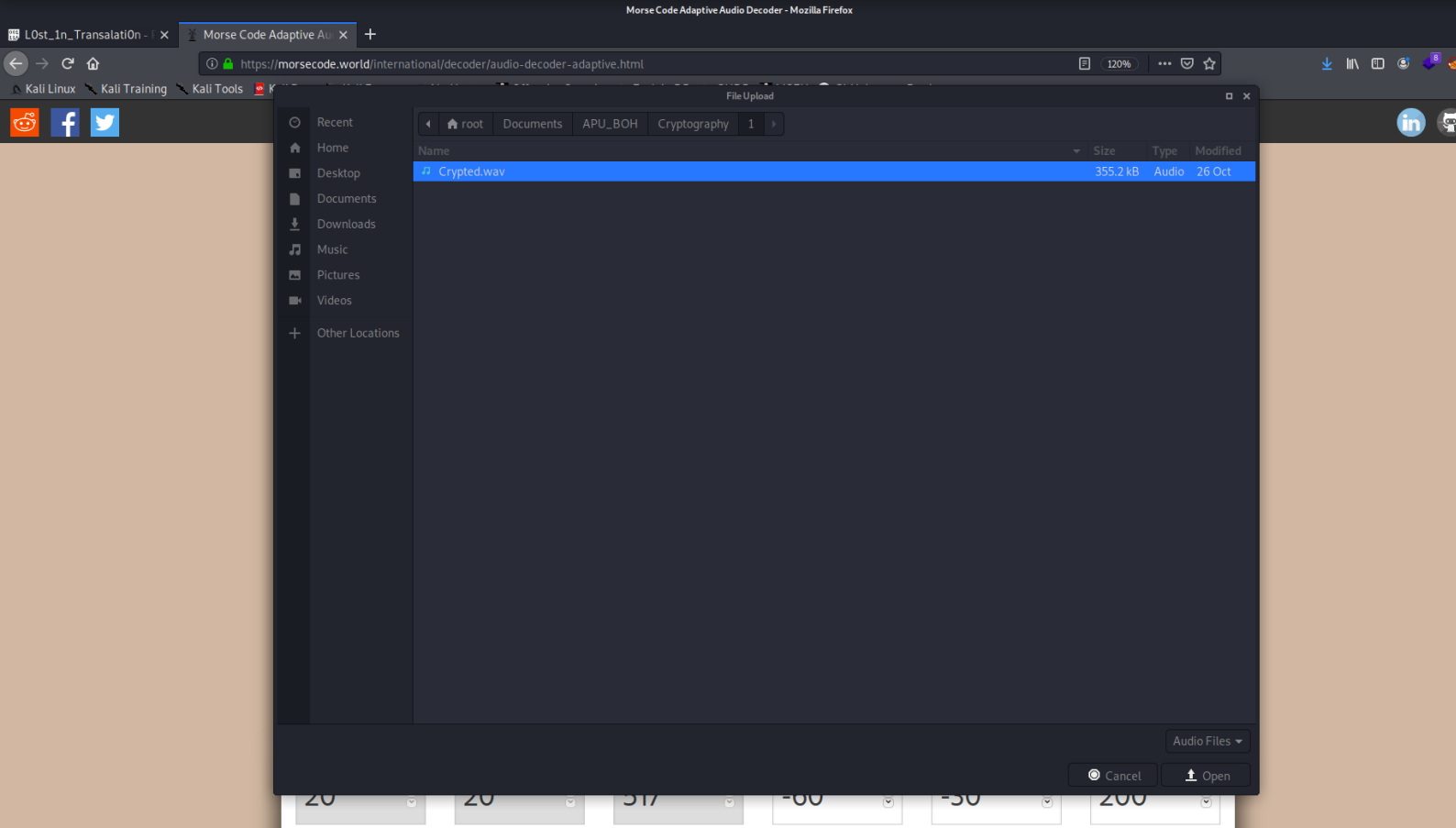


OEX02: MORSE WORLD

~ 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

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

Morse Code Adaptive Audio Decoder - Mozilla Firefox

https://morsecode.world/international/decoder/audio-decoder-adaptive.html

International Morse Decoders

Audio Decoder Audio Decoder (Expert) Gaze Decoder

Upload Play Stop Filename: "morse.wav"

WE SHALL BEGIN, TO DO SO HEAD TO THIS SITE: [HTTPS://PASTEBIN.COM/5X7FEQWH](https://PASTEBIN.COM/5X7FEQWH). THE LETTERS F,E AND W ARE SMALL LETTERS.

Shop Now

McAfee

Protect what matters.

Clear message

WPM 20 Farnsworth WPM 20 Frequency (Hz) 345 Minimum volume -60 Maximum volume -30 Volume threshold 200

☐ Manual ☐ Manual

Zoom in Zoom out Range: 172.265625 to 22050 Hz



OEX04: 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

Browser tabs: L0st_1n_Translati0n - Morse Code Adaptive Au -

Address bar: https://pastebin.com/5X7feQwH

Navigation: Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, MSFU, GitHub - wtsxDev/reve...

PASTEBIN GO PRO API TOOLS FAQ + paste

User: Zero Prime9 FREE

L0st_1n_Translati0n

4CS 0.61 KB raw download clone embed print edit delete

```
1. ===== Welcome Welcome to APU BOH 2020 =====
2. You've accepted the challenge to win, I see, I see. Let us proceed right then.
3. This was found while i was decrypting my friend's server. Would you help me out!.
4.
5. GET 200
6. Token Key:
7. 1LvbKvwDJApyNvrA0k0Dd1Q15tH1ZAmePVyL3yuvH4=
8.
9. Generating token:
10. gAAAAABf1uIYZnE57EQRW4u1Lub1WFTXvqh6hvvvPOxuJ9LC8U6ISAxLS99oZtzaJfQQ-
    16bn0mVieIP9aTi0PjSl2wAcrcbs3vqvq1bFfuRf3UcYj9a7SNRNnLLUyHlgc69x5X96sSifNjCqd610tsSh0LbjBXQamrQDbxgyP3FqAY67HzPETm0seo9b7kCFNo
    m0=
11.
12. Token Generation Complete, System OK!.
13.
14. ~ Cheers Zero_Prime9
15.
16.
17.
```

RAW Paste Data

```
===== Welcome Welcome to APU BOH 2020 =====
You've accepted the challenge to win, I see, I see. Let us proceed right then.
This was found while i was decrypting my friend's server. Would you help me out!.

GET 200
```

My Pastes

- MultiPlexed 4CS | 12 days ago
- Roul3t_de_Bas3 4CS | 13 days ago
- Analyz3d 4CS | 13 days ago
- Numbed 4CS | 13 days ago
- L0st_1n_Translati0n 4CS | 13 days ago

Public Pastes

- test jQuery | 2 min ago
- dupa.sh Bash | 5 min ago
- Memory_game_v3 Java | 9 min ago
- Untitled C# | 13 min ago
- Untitled PHP | 14 min ago
- img.php PHP | 27 min ago
- Task Manager Lua | 29 min ago
- Kmeans Python | 52 min ago

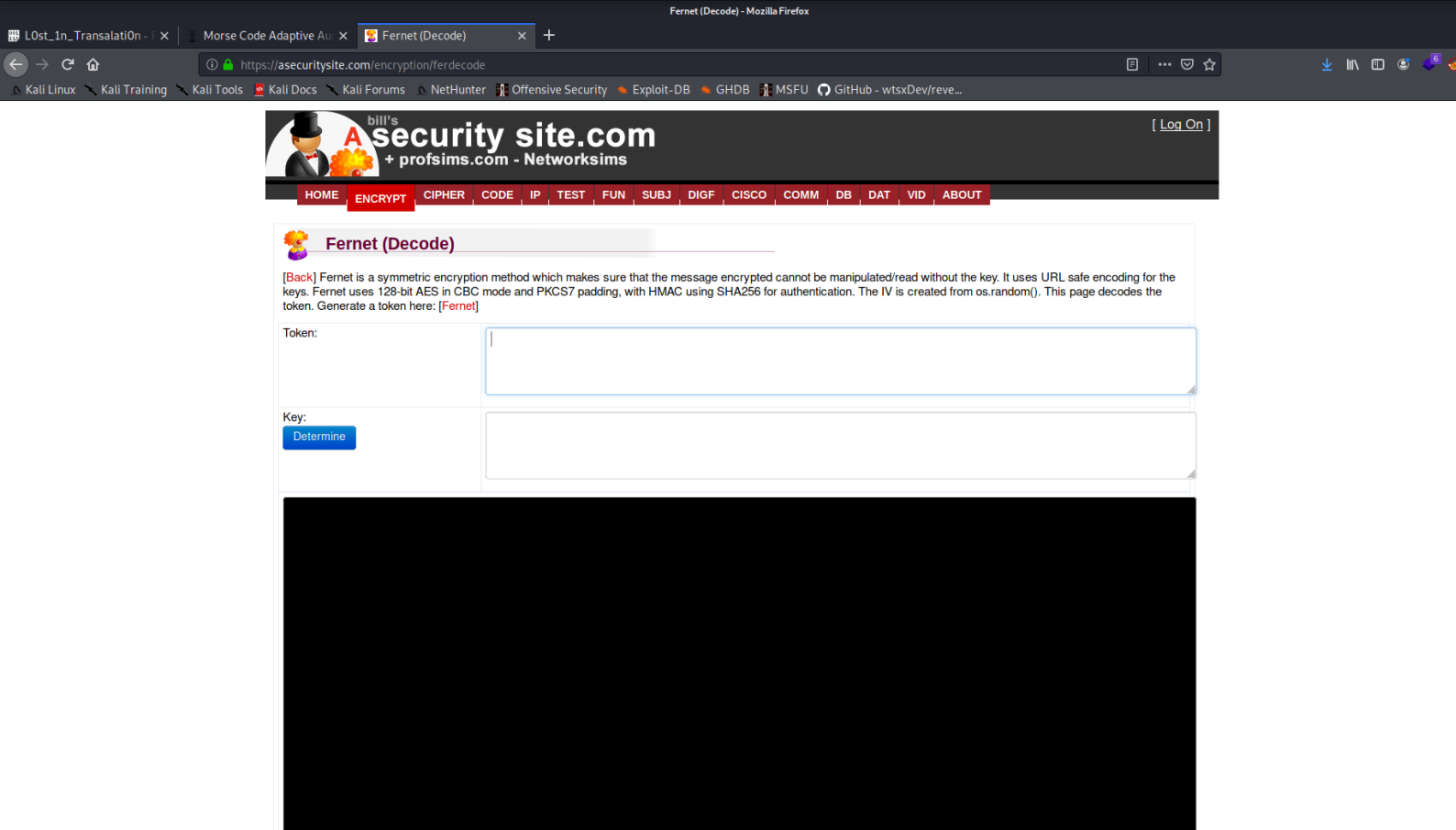


OEX05: PASTEBINED

~ ZERO_PRIME9

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



~ ZERO_PRIME9

OEX06: FERNET WHO?

You will see two boxes, one for token 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>

[L0st_In_Translati0n](#)
[Morse Code Adaptive Au](#)
[Fernet \(Decode\)](#)

[HOME](#)
[ENCRYPT](#)
[CIPHER](#)
[CODE](#)
[IP](#)
[TEST](#)
[FUN](#)
[SUBJ](#)
[DIGF](#)
[CISCO](#)
[COMM](#)
[DB](#)
[DAT](#)
[VID](#)
[ABOUT](#)

Fernet (Decode)

[Back] Fernet is a symmetric encryption method which makes sure that the message encrypted cannot be manipulated/read without the key. It uses URL safe encoding for the keys. Fernet uses 128-bit AES in CBC mode and PKCS7 padding, with HMAC using SHA256 for authentication. The IV is created from os.random(). This page decodes the token. Generate a token here: [\[Fernet\]](#)

Token: `gAAAAABf1uIYZnE57EQRW4u1Lub1WFTXvQh6hvvvP0xuJ9LC8U6ISAxLS99oZtzaJfQQ-16bn0mVieIP9aT10PjS12wAcrcbs3vqvq1bFfuRf3UcYj9a7SNRNLuYHlGc69x5X96sS1fNjCqd610tsSh0LbjBXQamrQD
bxgYP3FqAY67HzPETm0seo9b7kCFNoaxm5Mav0i1Hw88UisPZE4yNwvRBS51tkMrF6moH0KRM0HdB-m0=`

Key: `1LvbkVwDJApKyNvrA0k0Dd1Q15tH1ZAmPVyL3yuvH4=`

[Determine](#)

```

Decoded: aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2ZpbG9vZC8xenplL29xbURwbjQ2VFd5VW1ic1I6RTB6Vmc1am9Memwvdmlldz91c3A9c2hhcm1uZw==
Date created: Mon Oct 26 14:50:00 2020
Current time: Mon Nov 9 13:34:56 2020

=====Analysis=====
Decoded data:
80000000005f96e218667139ec44115b8ba22ee6f55854d7bd087a86fbef3cec6e27d2c2f14e88480c4b4bdf6866dcda25f410fb5e9b9f499589e20ff5a4e2d0f8d2976c0
072b71bb37beabead5b15fb917f751c623f5aed23513672cb5321e581cebdc795fdeac4a27cd25c41dea53adb128742db8c15d06a6ad00dbc60c8fdc5a8063aec7ccf12d9
8eb1ea3d6fb90214da1af719b931abf48a51f0f3c52248f644e3235656b0794a5b64a8cac5ea6a07d0a44c387741fa6d
Version: 80
Date created: 000000005f96e218
IV: 667139ec44115b8ba22ee6f55854d7bd
Cipher:
087a86fbef3cec6e27d2c2f14e88480c4b4bdf6866dcda25f410fb5e9b9f499589e20ff5a4e2d0f8d2976c0072b71bb37beabead5b15fb917f751c623f5aed23513672cb5
321e581cebdc795fdeac4a27cd25c41dea53adb128742db8c15d06a6ad00dbc60c8fdc5a8063aec7ccf12d98eb1ea3d6fb90214da1af719b931abf4
HMAC: 8a51f0f3c52248f644e3235656b0794a5b64a8cac5ea6a07d0a44c387741fa6d

=====Converted=====
IV: 667139ec44115b8ba22ee6f55854d7bd
Time stamp: 1603723800
Date created: Mon Oct 26 14:50:00 2020
  
```



~ ZERO_PRIME9

OEX07: FERNET DECODED

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

Base64 Decode and Encode - Online - Mozilla Firefox

Base64 Decode and Encode - Online - Mozilla Firefox

Decode from Base64 format

Simply enter your data then push the decode button.

aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29lL2ZpbGUvZC8xenpLZ29xbURWbjQ2VFd5VW11c1I6RTB0Vmc1am9Memwvdmldz91c3A9c2hhcmLuZw==

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for multiple entries).

☒ Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE > Decodes your data into the textarea below.

https://drive.google.com/file/d/1zzKgoqmDVn46TWyUmusYzE0tVg5j0LzI/view?usp=sharing

Decode files from Base64 format

Select a file to upload and process, then you can download the decoded result.

Bonus tip: Bookmark us!

Other tools

- URL Decode
- URL Encode
- JSON Minify
- JSON Beautify
- JS Minify
- JS Beautify
- CSS Minify
- CSS Beautify

Partner sites

- Decimal to Hex converter
- Hex to Decimal converter
- Secure Chat



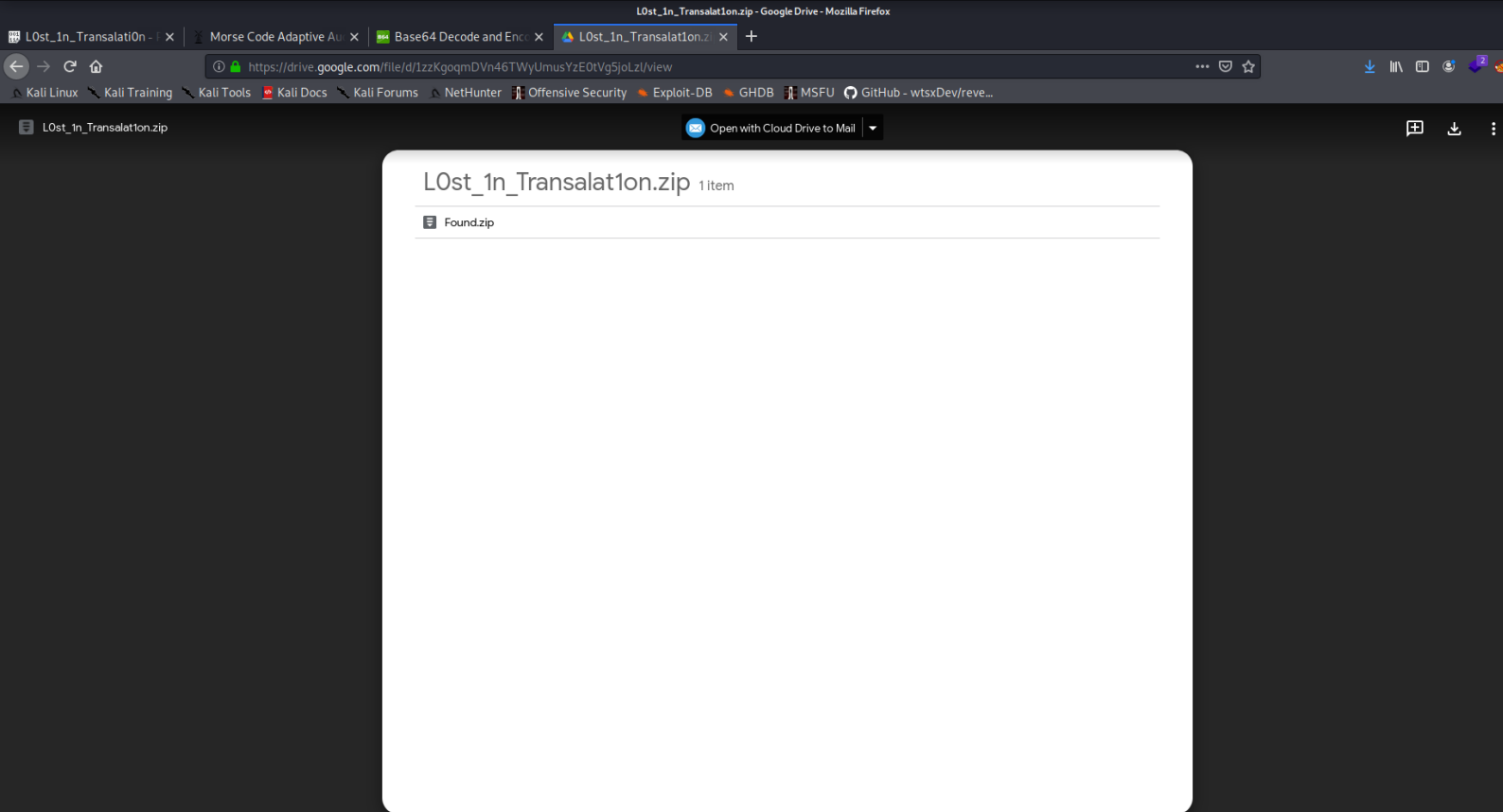
0EX08: BASE DECODED

~ 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/>



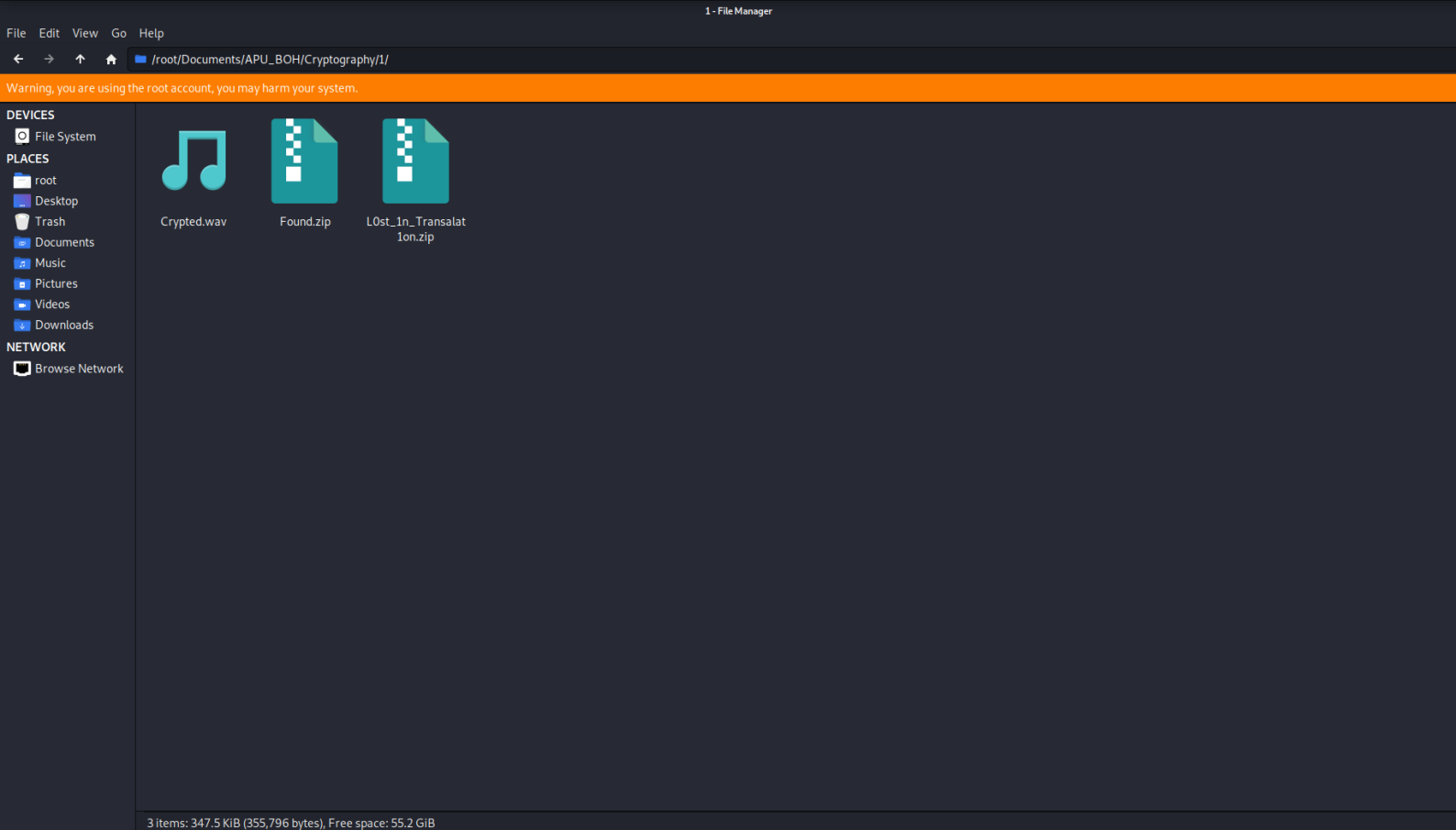
~ ZERO_PRIME9

0EX09: LOST IN TRANSLATION

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.

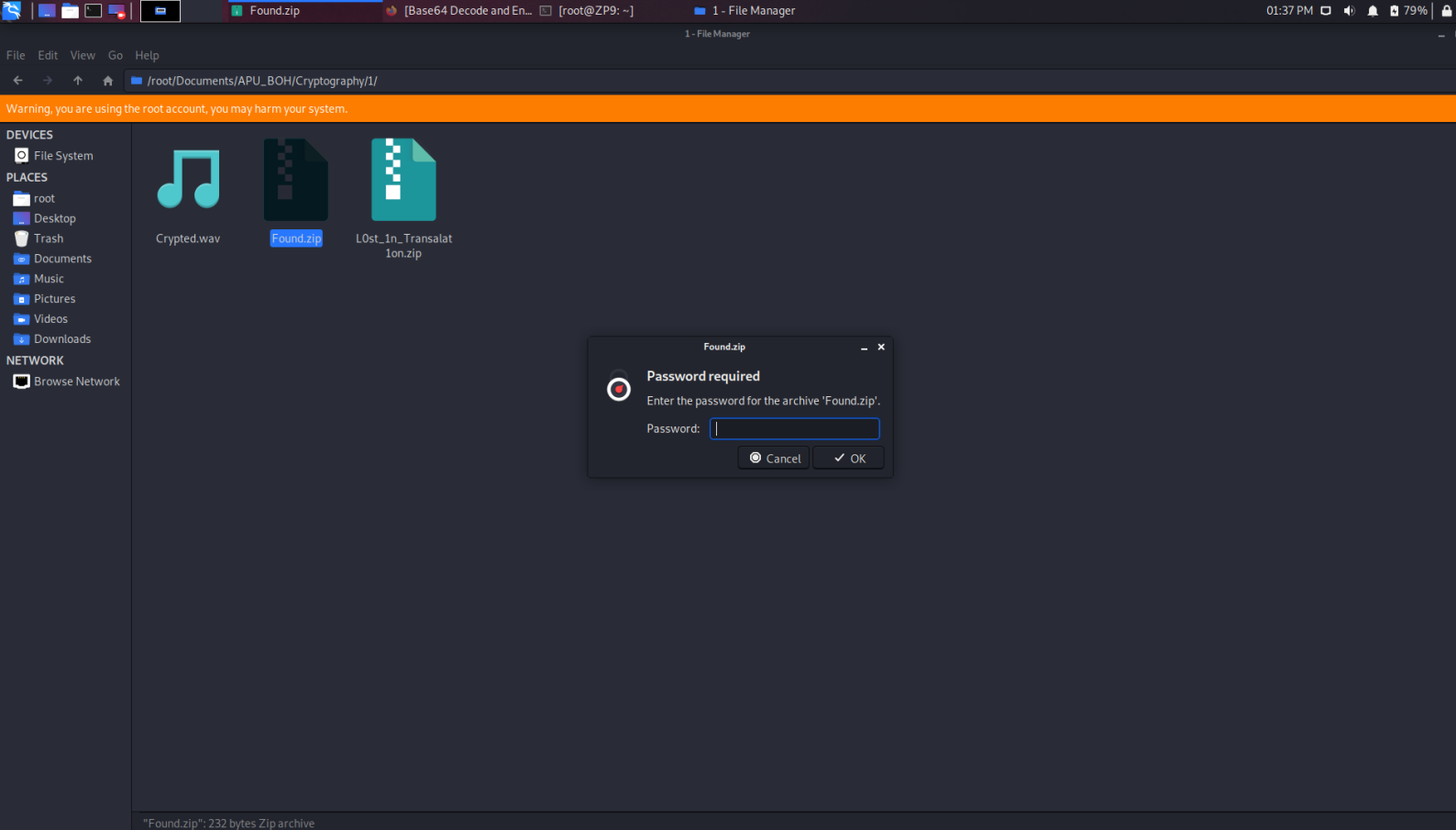


OEX0A: WE ARE CLOSE

~ 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



OEXOB: 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-encrypt the hash using custom word-list.

```
File Actions Edit View Help
root@ZP9: ~/Documents/APU_BOH/Cryptography/1

(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]
# zip2john Found.zip > hash.txt
ver 1.0 efh 5455 efh 7875 Found.zip/flag.txt PKZIP Encr: 2b chk, TS_chk, cmplen=50, decmplen=38,
c=E4C7BE3B

(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]
#
```



~ ZERO_PRIME9

OEXOC: ARE WE CLOSE?

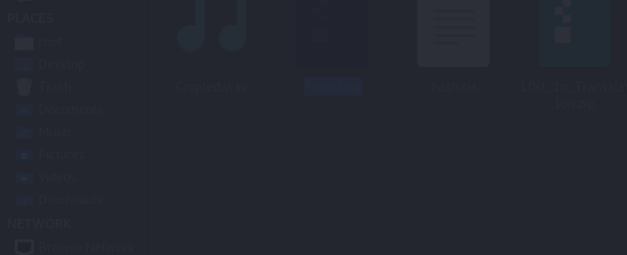
By Default Zip2John is installed on Kali. If it is not installed you can search for it in google and download it through one of the GitHub repositories .

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

```
(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]  
# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```



~ ZERO_PRIME9

OEXOD: HASHED

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.


```
(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kitty1 (Found.zip/flag.txt)
1g 0:00:00:00 DONE (2020-11-09 08:38) 14.28g/s 117028p/s 117028c/s 117028C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]
#
```



~ ZERO_PRIME9

OEXOE: 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

```
(root👤 ZP9)-[~/Documents/APU_BOH/Cryptography/1]
# unzip Found.zip
Archive: Found.zip
[Found.zip] flag.txt password:
extracting: flag.txt
```

```
(root👤 ZP9)-[~/Documents/APU_BOH/Cryptography/1]
#
```

NETWORK

📺 Local Network



~ ZERO_PRIME9

OEXOF: 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.

```
(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]
# cat flag.txt
apuboh{_$$_Y0u_G0t_it_Transalat3d_$$_}

(root@ZP9)-[~/Documents/APU_BOH/Cryptography/1]
#
```



~ ZERO_PRIME9

OEX10: FLAGGED

Once you type in "cat flag.txt"
The flag is mentioned and it is
apuboh{_\$\$_Y0U_G0T_1T_Transalat3
d_\$\$_}

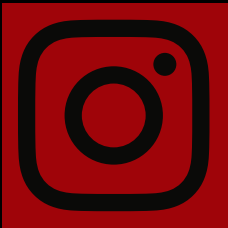
Congratulations you just completed
the challenge

~ Cheers Zero_Prime9

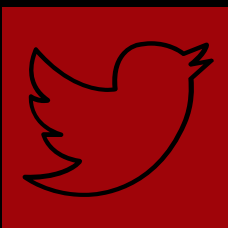


ZERO_PRIME9

— You are seen or you will be seen —



@zero_prime9



@zero_prime9



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