Writeups by

PENGGODAMN

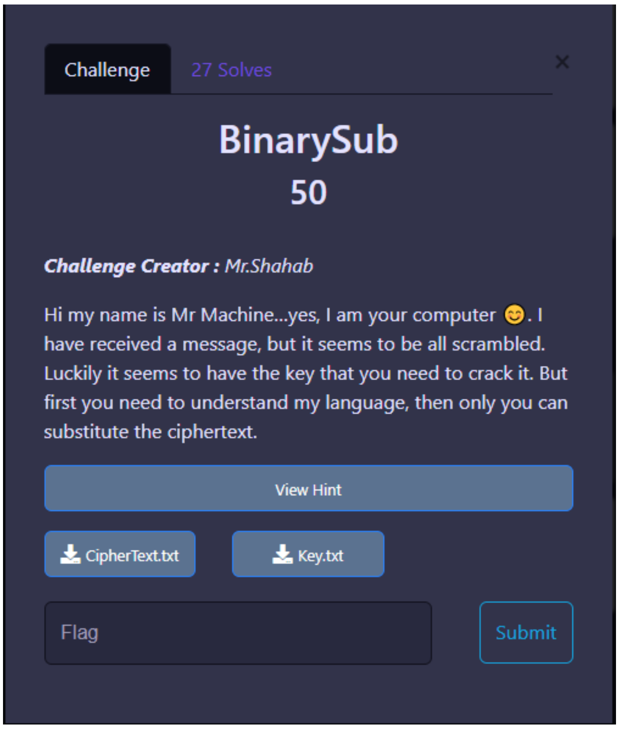
Table of Contents

Acknowledgement

Full appreciation is given to the organizers of APU Battle of Hackers 2022 because organizing the very great event that make us learn more things about cyber security. Thanks also to all sponsors that willing to give some souvenirs and knowledge to all of us. Not forgotten either all Pegg0damn teammates, all UniKL MIIT teams, UniKL MIIT Lecturers that willing to guide and take care of us during this competition, all APU BOH staffs, and our new friends from all universities. We hope that this event will remain to be contested on every year.

Cryptography

BinarySub



Challenge 27 Solves

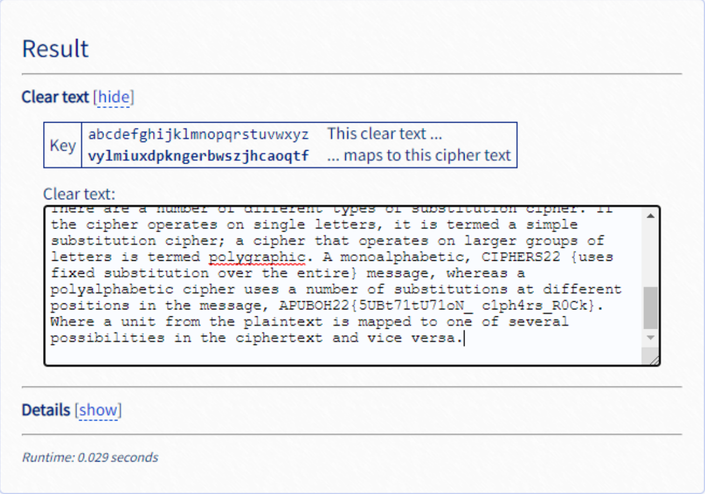
BinarySub

50

Challenge Creator : *Mr.Shahab*

Hi my name is Mr Machine...yes, I am your computer 😊. I have received a message, but it seems to be all scrambled. Luckily it seems to have the key that you need to crack it. But first you need to understand my language, then only you can substitute the ciphertext.

Starting the day with the easy level in cryptography section, we got the cipher text and the key to decode the cipher. The cipher has many alphabets so its indicate that the cipher is may just a substitution cipher also based on the challenge name. So, we just use online substitution tools to decode the cipher text and we got the flag. Pretty easy right 😊.



Result

Clear text [hide]

Key	abcdefghijklmnopqrstuvwxyz	This clear text ...
	vylmiuxdpkngerbwszjhcaoqtf	... maps to this cipher text

Clear text:

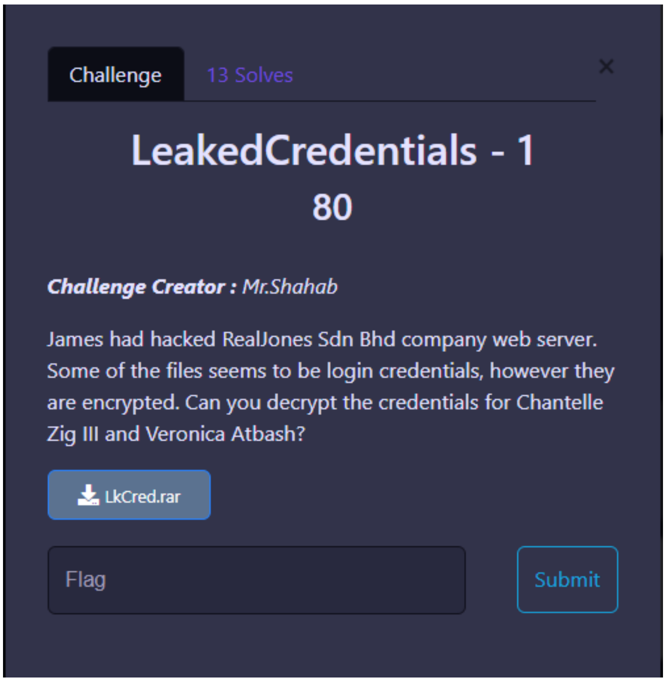
```
There are a number of different types of substitution cipher. If
the cipher operates on single letters, it is termed a simple
substitution cipher; a cipher that operates on larger groups of
letters is termed polygraphic. A monoalphabetic, CIPHERS22 {uses
fixed substitution over the entire} message, whereas a
polyalphabetic cipher uses a number of substitutions at different
positions in the message, APUBOH22{5UBt71tU71oN_ c1ph4rs_R0Ck}.
Where a unit from the plaintext is mapped to one of several
possibilities in the ciphertext and vice versa.
```

Details [show]

Runtime: 0.029 seconds

Flag: APUBOH22{5UBt71tU71oN_ c1ph4rs_R0Ck}

LeakedCredentials 1 & 2



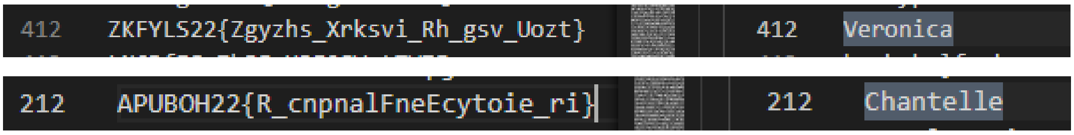
LeakedCredentials - 1

80

Challenge Creator : *Mr.Shahab*

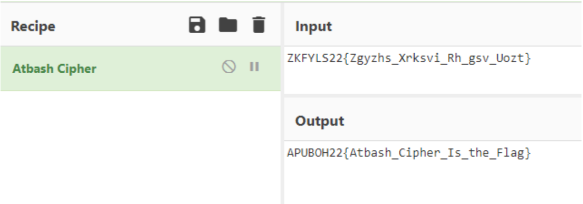
James had hacked RealJones Sdn Bhd company web server. Some of the files seems to be login credentials, however they are encrypted. Can you decrypt the credentials for Chantelle Zig III and Veronica Atbash?

This challenge gives us two txt file that's contain usernames and password for each user. To make us easy to find which password belong to the user, we open the text file in code editor to show the line numbers. Next, we need to find the password for Chantelle and Veronica.



```
412    ZKFYLS22{Zgyzhs_Xrksvi_Rh_gsv_Uozt}        412    Veronica

212    APUBOH22{R_cnpnalFneEcytoie_ri}            212    Chantelle
```

Nice now we have the password for the Veronica and Chantelle, but both is decrypted. So, let's decode the password. The clue we got is based on the question itself where Chantelle related to Zig III and Veronica related to atbash. So, its clear that we need to decode Chantelle password using Rail Fence cipher that refer to Zig III and Veronica password using Atbash cipher which refer to Atbash itself. The decode process is straightforward so we just use CyberChef to decode the ciphertext and we got both flags.



Recipe

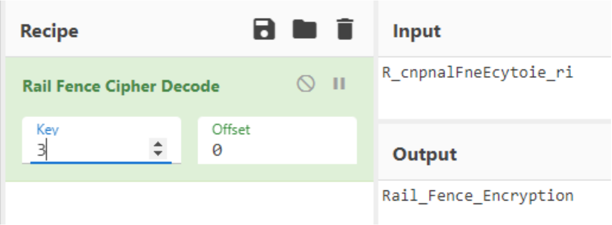
Atbash Cipher

Input

```
ZKFYLS22{Zgyzhs_Xrksvi_Rh_gsv_Uozt}
```

Output

```
APUBOH22{Atbash_Cipher_Is_the_Flag}
```



Recipe

Rail Fence Cipher Decode

Key 3

Offset 0

Input

```
R_cnpnalFneEcytoie_ri
```

Output

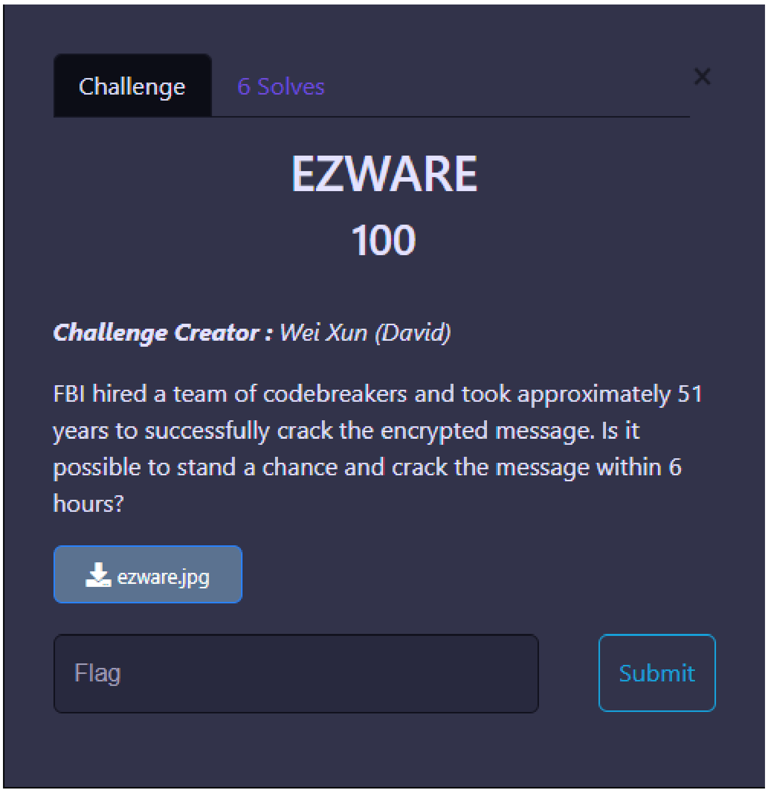
```
Rail_Fence_Encryption
```

Flag:

APUBOH22{Atbash_Cipher_Is_the_Flag}

APUBOH22{Rail_Fence_Encryption}

EZWARE



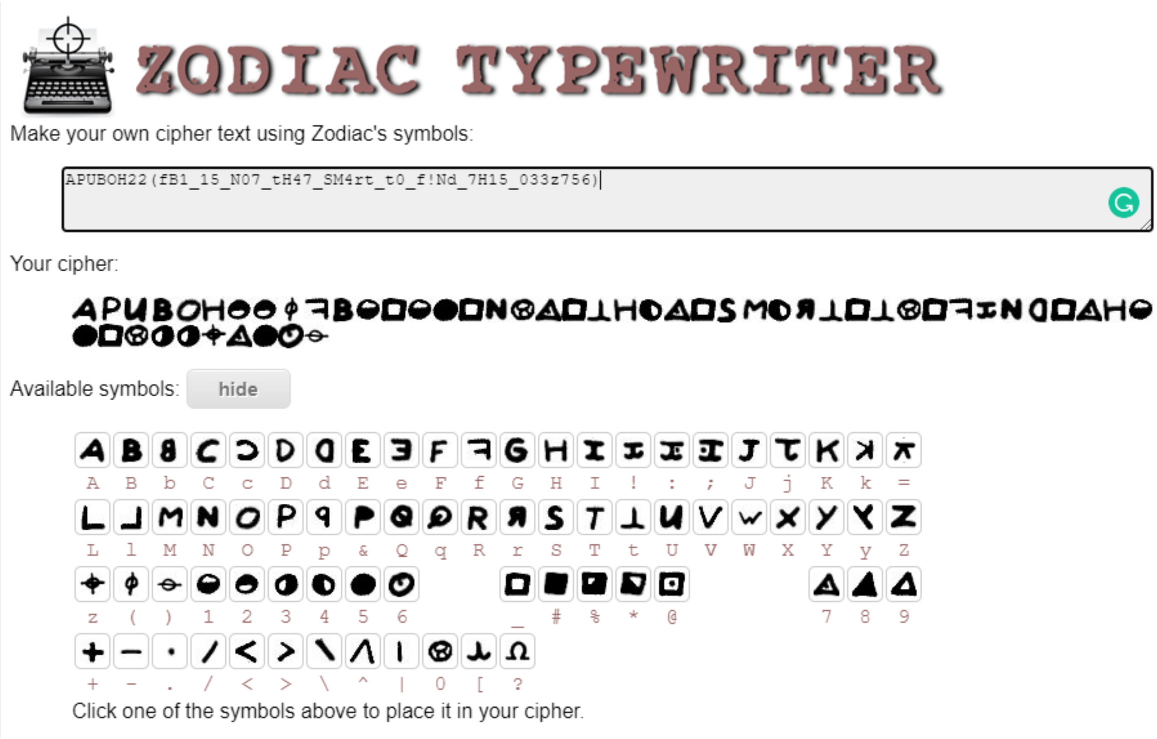
EZWARE

100

Challenge Creator : *Wei Xun (David)*

FBI hired a team of codebreakers and took approximately 51 years to successfully crack the encrypted message. Is it possible to stand a chance and crack the message within 6 hours?

The next crypto challenge is quite straight forward, we are given an image with a cipher, we have seen this cipher quite a lot and it called zodiac cipher. Name by the killer named zodiac. To solve these challenges, we can use an online useful tool called Zodiac Typewriter to decode the cipher then we automatically got the flag.



Make your own cipher text using Zodiac's symbols:

```
APUBOH22(fB1_15_N07_tH47_SM4rt_t0_f!Nd_7H15_033z756)
```

Your cipher:

Available symbols: hide

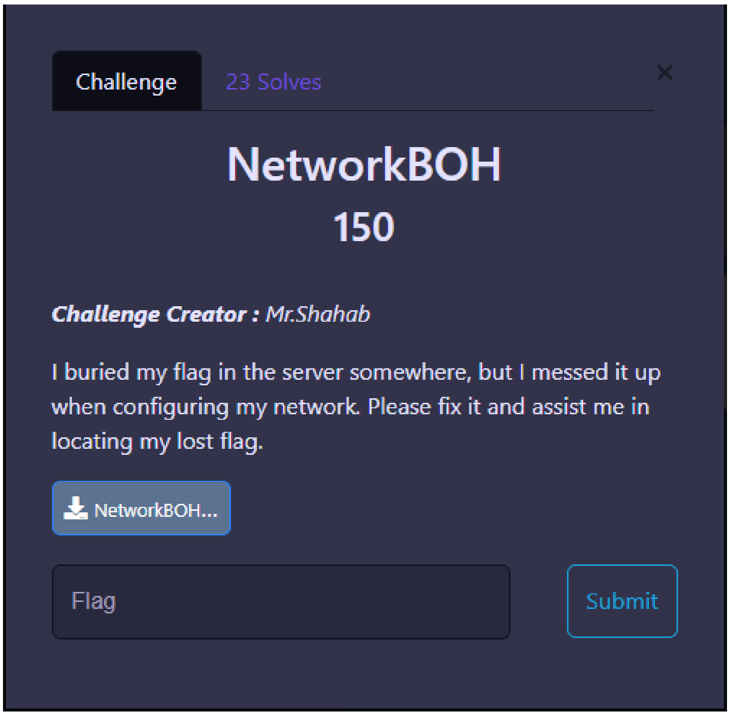
A B b C c D d E e F f G H I ! : ; J j K k =
L l M N O P p & Q q R r S T t U V W X Y y Z
z ( ) 1 2 3 4 5 6 _ # % * @ 7 8 9
+ - . / < > \ ^ | 0 [?

Click one of the symbols above to place it in your cipher.

Flag: APUBOH22(fB1_15_N07_tH47_SM4rt_t0_f!Nd_7H15_033z756)

Network

NetworkBOH



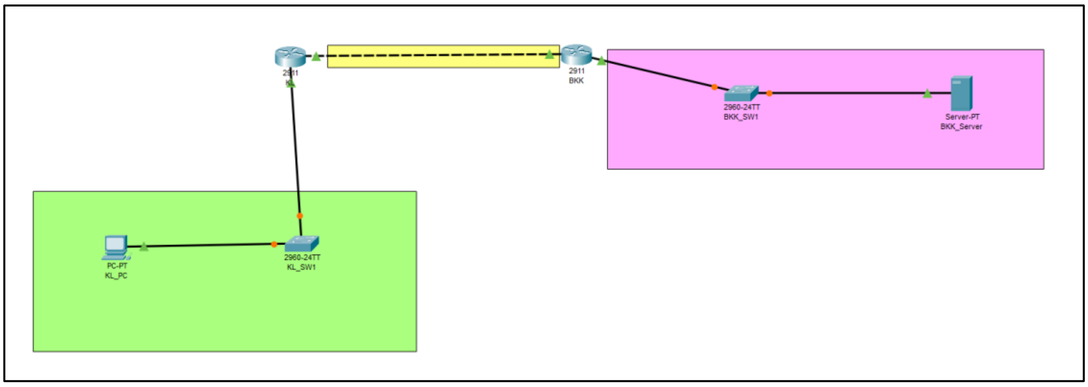
NetworkBOH

150

Challenge Creator : *Mr.Shahab*

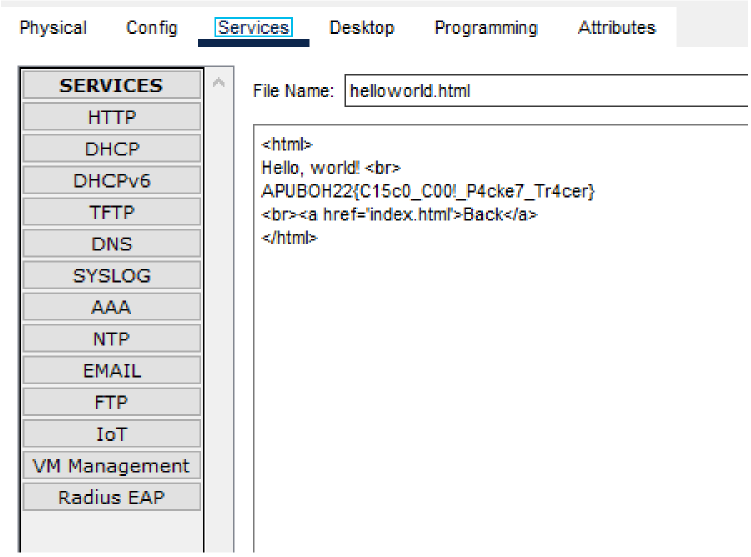
I buried my flag in the server somewhere, but I messed it up when configuring my network. Please fix it and assist me in locating my lost flag.

The NetworkBOH challenge give us a pkt extension file which need us to open the file using network simulation software, so we use Cisco Packet Tracer to open this file. In the file, it shows us the network mapping for small networks configuration that contains PC, server, routers and switches.



Network mapping in the challenge file

In the challenge question, it states that the challenge was in the server, so our idea is to look on the server and search for the flag manually, eventually we found the flag in the http file of the server itself.



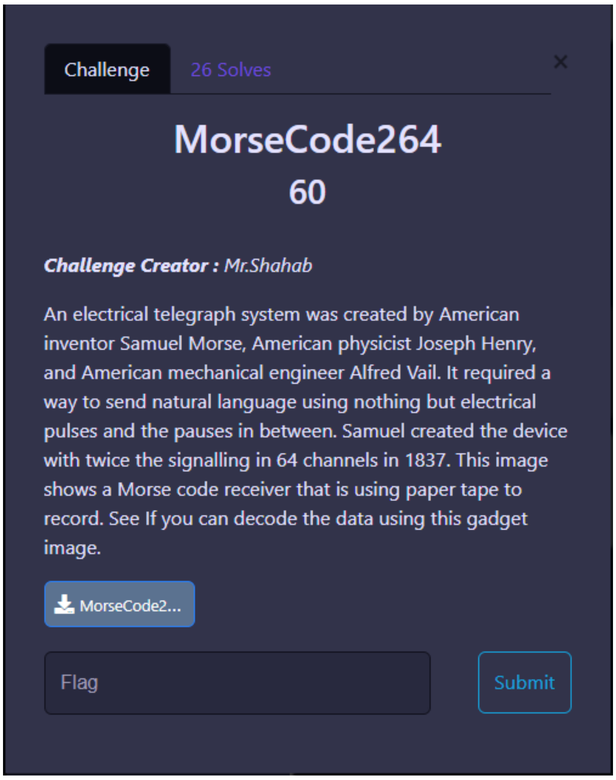
File Name: helloworld.html

```
<html>
Hello, world! <br>
APUBOH22{C15c0_C00!_P4cke7_Tr4cer}
<br><a href='index.html'>Back</a>
</html>
```

Flag: APUBOH22{C15c0_C00!_P4cke7_Tr4cer}

MISC

MorseCode264



Challenge

26 Solves

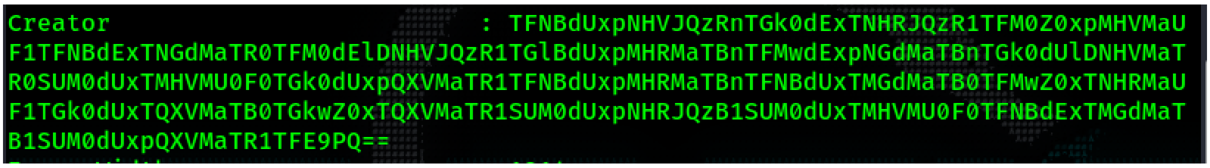
MorseCode264

60

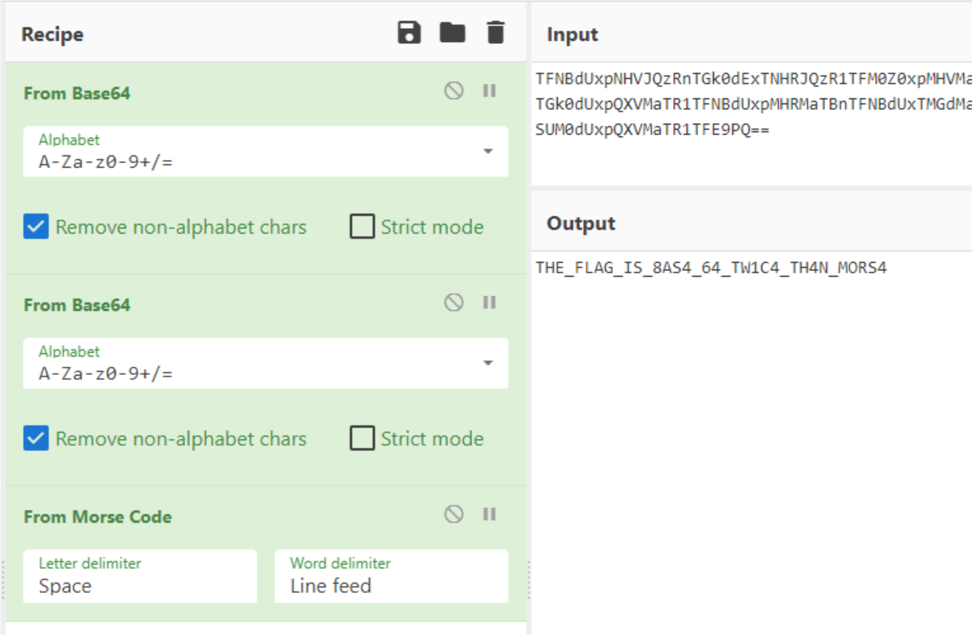
Challenge Creator : *Mr.Shahab*

An electrical telegraph system was created by American inventor Samuel Morse, American physicist Joseph Henry, and American mechanical engineer Alfred Vail. It required a way to send natural language using nothing but electrical pulses and the pauses in between. Samuel created the device with twice the signalling in 64 channels in 1837. This image shows a Morse code receiver that is using paper tape to record. See If you can decode the data using this gadget image.

The miscellaneous challenge starts with MorseCode264 challenge. So, obviously this challenge is about morse code, right? But what we got only the image of morse code machine. As it gives jpg file, we try to steghide and binwalk the file, but nothing came out. So, after inspecting the image using strings and exiftool, we saw that there are some interesting texts inside the metadata of the file which on the creator tags, there are cipher text which looks like base64, so we try to decode the text.



```
Creator                         : TFNBdUxpNHVJQzRnTGk0dExTNHRJQzR1TFM0Z0xpMHVMaU
F1TFNBdExTNGdMaTR0TFM0dElDNHVJQzR1TGlBdUxpMHRMaTBnTFMwdExpNGdMaTBnTGk0dUlDNHVMaT
R0SUM0dUxTMHVMU0F0TGk0dUxpQXVMaTR1TFNBdUxpMHRMaTBnTFNBdUxTMGdMaTB0TFMwZ0xTNHRMaU
F1TGk0dUxTQXVMaTB0TGkwZ0xTQXVMaTR1SUM0dUxpNHRJQzB1SUM0dUxTMHVMU0F0TFNBdExTMGdMaT
B1SUM0dUxpQXVMaTR1TFE9PQ==
```



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

From Morse Code

Letter delimiter
Space

Word delimiter
Line feed

Input

```
TFNBdUxpNHVJQzRnTGk0dExTNHRJQzR1TFM0Z0xpMHVMa
TGk0dUxpQXVMaTR1TFNBdUxpMHRMaTBnTFNBdUxTMGdMa
SUM0dUxpQXVMaTR1TFE9PQ==
```

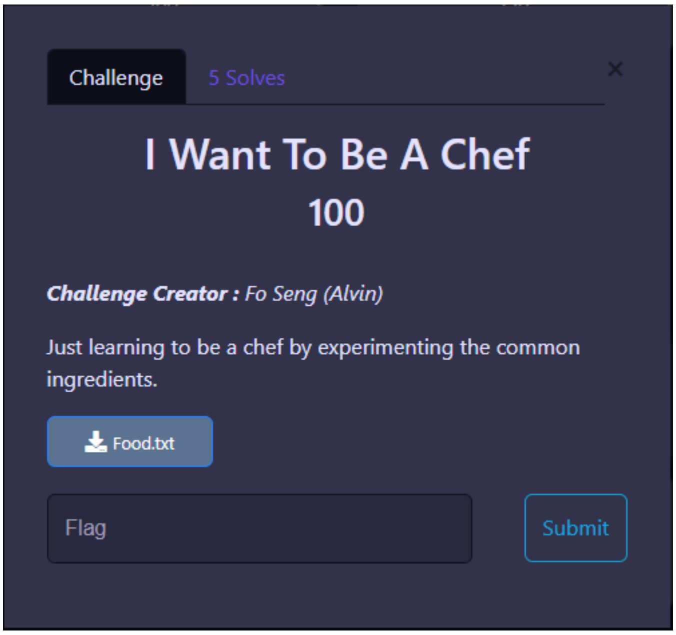
Output

```
THE_FLAG_IS_8AS4_64_TW1C4_TH4N_MORS4
```

After decoding the cipher text using base64, we got the morse code and we can automatically decode the morse code using CyberChef and got the flag.

Flag: APUBOH{8AS4_64_TW1C4_TH4N_MORS4}

I Want To Be A Chef



Challenge

5 Solves

I Want To Be A Chef

100

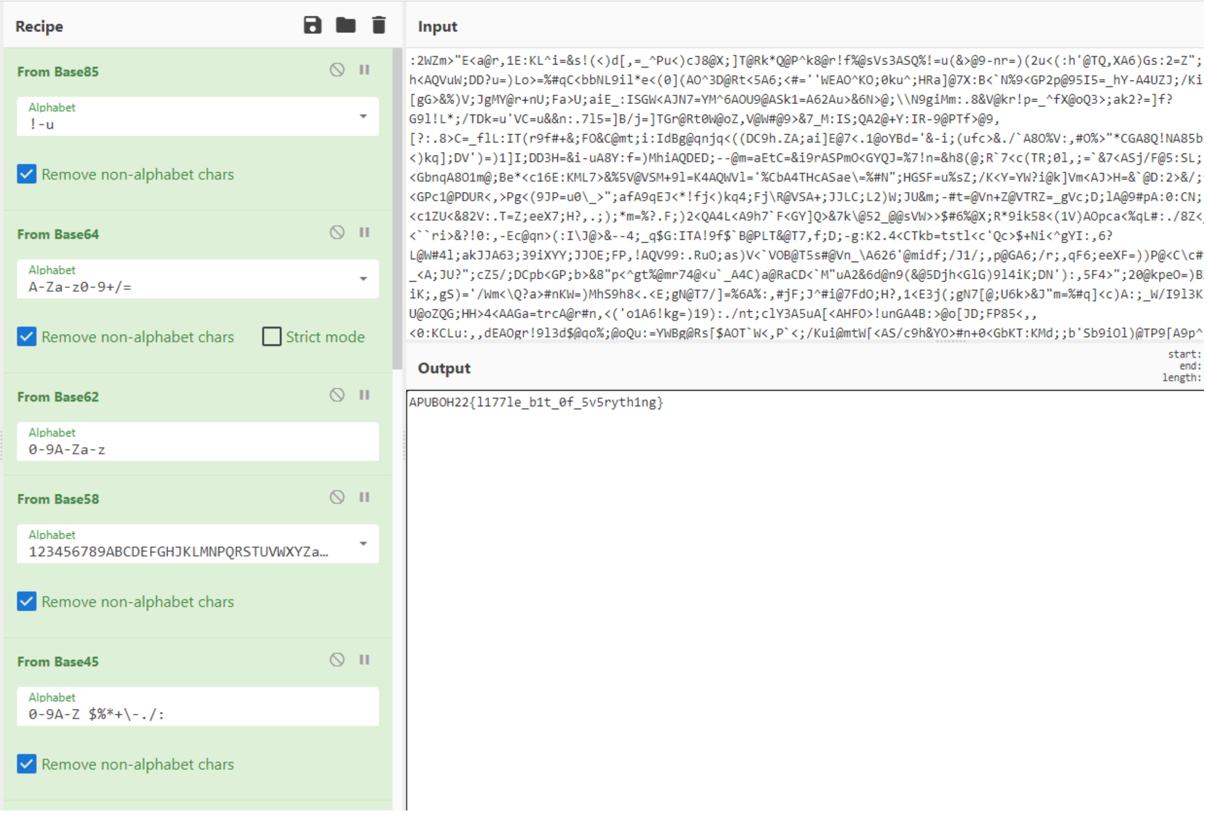
Challenge Creator : *Fo Seng (Alvin)*

Just learning to be a chef by experimenting the common ingredients.

I Want To Be A Chef is one of the challenging questions in this competition, the file we got contains bunch of random alphabet, numbers and symbols. We can't even think what type of the cipher this kind of text uses. So, we try to identify the cipher. We use https://www.dcode.fr/cipher-identifier to identify the cipher text, but each time we decode the cipher text, the other cipher text with other cipher will produce, so we need to keep identify the cipher and decode it to get the flag. The combination to decode the cipher is like below:

Base85 --> Base64 --> Base62 --> Base58 --> Base45 --> Base32 --> Base 85 --> Base64

--> Base62 --> Base58 --> Base45 --> Base32



Recipe

From Base85

Alphabet
!-u

☑ Remove non-alphabet chars

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

From Base62

Alphabet
0-9A-Za-z

From Base58

Alphabet
123456789ABCDEFGHJKLMNPQRSTUVWXYZa...

☑ Remove non-alphabet chars

From Base45

Alphabet
0-9A-Z $%*+\-./:

☑ Remove non-alphabet chars

Input

```
:2WZm>"E<a@r,1E:KL^i=&s!(<)d[,=_^Pu<)cJ8@X;]T@Rk*Q@P^k8@r!f%@sVs3ASQ%!=u(&>@9-nr=)(2u<(:h'@TQ,XA6)Gs:2=Z";
h<AQVuW;DD?u=)Lo>=%#qC<bbNL9il*e<(0](AO^3D@Rt<5A6;<#=''WEAO^KO;0ku^;HRa]@7X:B<`N%9<GP2p@95I5=_hY-A4UZJ;/Ki
[gG>&%)V;JgMY@r+nU;Fa>U;aiE_:ISGW<AJN7=YM^6AOU9@ASk1=A62Au>&6N>@;\\N9giMm:.8&V@kr!p=_^fX@oQ3>;ak2?=]f?
G9l!L*;/TDk=u'VC=u&&n:.7l5=]B/j=]TGr@Rt0W@oZ,V@W#@9>&7_M:IS;QA2@+Y:IR-9@PTf>@9,
[?:.8>C=_flL:IT(r9f#+&;FO&C@mt;i:IdBg@qnjq<((DC9h.ZA;ai]E@7<.1@oYBd='&-i;(ufc>&./`A8O%V:,#O%>"*CGA8Q!NA85b
<)kq];DV')=)1]I;DD3H=&i-uA8Y:f=)MhiAQDED;--@m=aEtC=&i9rASPmO<GYQJ=%7!n=&h8(@;R`7<c(TR;0l,;=`&7<ASj/F@5:SL;
<GbnqA8O1m@;Be*<c16E:KML7>&%5V@VSM+9l=K4AQWVl='%CbA4THcASae\=%#N";HGSF=u%sZ;/K<Y=YW?i@k]Vm<AJ>H=&`@D:2>&/;
<GPc1@PDUR<,>Pg<(9JP=u0\_>";afA9qEJ<*!fj<)kq4;Fj\R@VSA+;JJLC;L2)W;JU&m;-#t=@Vn+Z@VTRZ=_gVc;D;lA@9#pA:0:CN;
<c1ZU<&82V:.T=Z;eeX7;H?,.;);*m=%?.F;)2<QA4L<A9h7`F<GY]Q>&7k\@52_@@sVW>>$#6%@X;R*9ik58<(1V)AOpca<%qL#:./8Z<
<``ri>&?!0:,-Ec@qn>(:I\J@>&--4;_q$G:ITA!9f$`B@PLT&@T7,f;D;-g:K2.4<CTkb=tstl<c'Qc>$+Ni<^gYI:,6?
L@W#4l;akJJA63;39iXYY;JJOE;FP,!AQV99:.RuO;as)V<`VOB@T5s#@Vn_\A626'@midf;/J1/;,p@GA6;/r;,qF6;eeXF=))P@<C\c#
_<A;JU?";cZ5/;DCpb<GP;b>&8"p<^gt%@mr74@<u`_A4C)a@RaCD<`M"uA2&6d@n9(&@5Djh<GlG)9l4iK;DN'):,5F4>";20@kpeO=)B
iK;,gS)='/Wm<\Q?a>#nKW=)MhS9h8<.<E;gN@T7/]=%6A%:,#jF;J^#i@7FdO;H?,1<E3j(;gN7[@;U6k>&J"m=%#q]<c)A:;_W/I9l3K
U@oZQG;HH>4<AAGa=trcA@r#n,<('o1A6!kg=)19):./nt;clY3A5uA[<AHFO>!unGA4B:>@o[JD;FP85<,,
<0:KCLu:,,dEAOgr!9l3d$@qo%;@oQu:=YWBg@Rs[$AOT`W<,P`<;/Kui@mtW[<AS/c9h&YO>#n+0<GbKT:KMd;;b'Sb9iOl)@TP9[A9p^
```

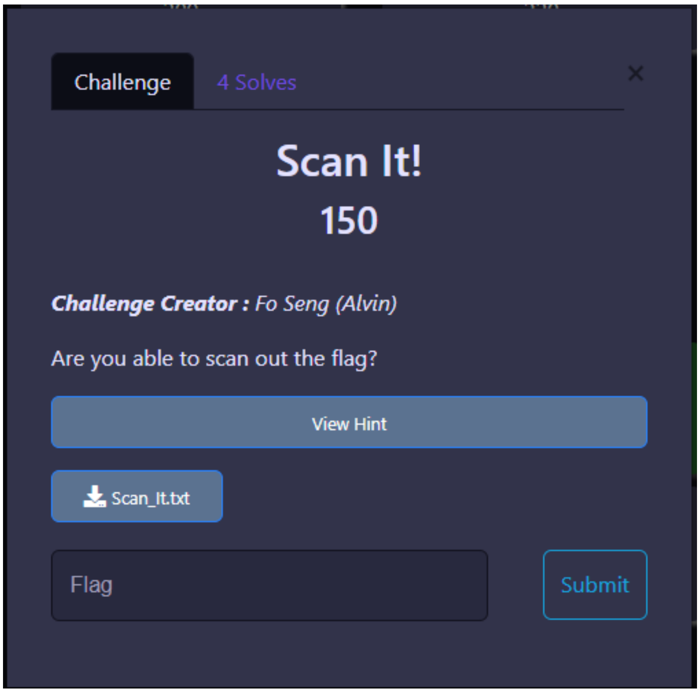
start:
end:
length:

Output

```
APUBOH22{l177le_b1t_0f_5v5ryth1ng}
```

Flag: APUBOH22{l177le_b1t_0f_5v5ryth1ng}

Scan It!


Challenge 4 Solves

Scan It!

150

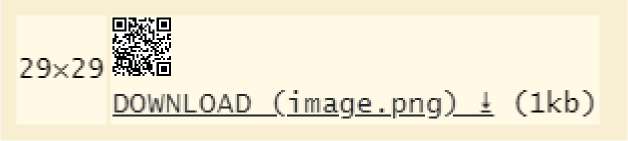
***Challenge Creator :** Fo Seng (Alvin)*

Are you able to scan out the flag?

Scan It! Is one of the interesting challenges that we got to solve, the text file contains base64 cipher text, so we just need to decode it right? But after two times we decode the cipher text got the binary and the binary does not represent any readable text.

We stuck awhile when doing this challenge, after the hint came out, we got some ideas to solve the problem. The hint says we can try to colour the binary, and the ideas is to represent the binary with black and white colour, but how to sort the colour?

After some research we found the tools that can help to convert binary to images, we use https://www.dcode.fr/binary-image to convert the binary. The image produce is black and white pixel like the QR code, but we cannot scan the code yet because the position of the pixel is not correct. We try and error to adjust the size of the image and the size of 29, we got the perfect QR code images, we scan the QR and got the flag. Hooray.

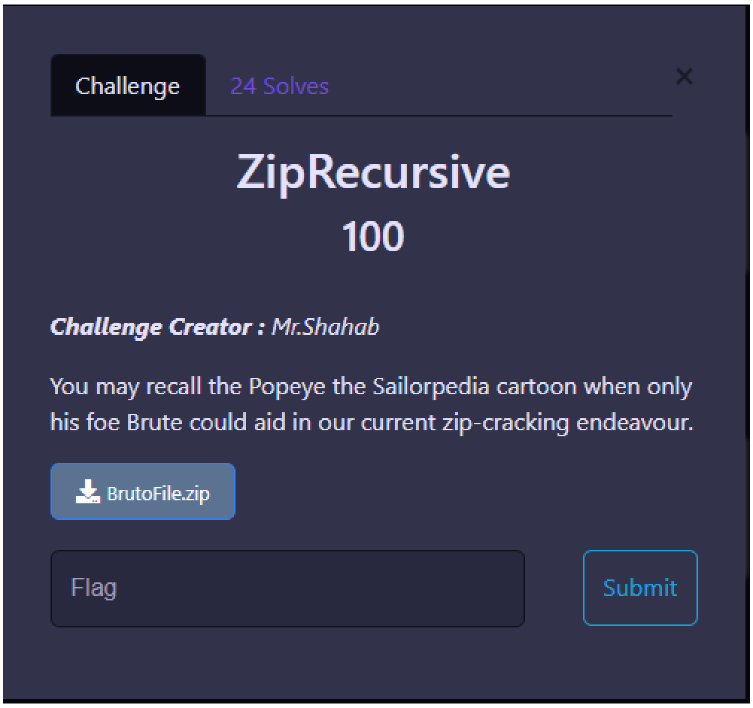

29×29

DOWNLOAD (image.png) ⤓ (1kb)

Flag: APUBOH22{7h1s_1s_7h5_QR_y0u_n55d_7o_Sc@n}

Forensics

ZipRecursive



ZipRecursive

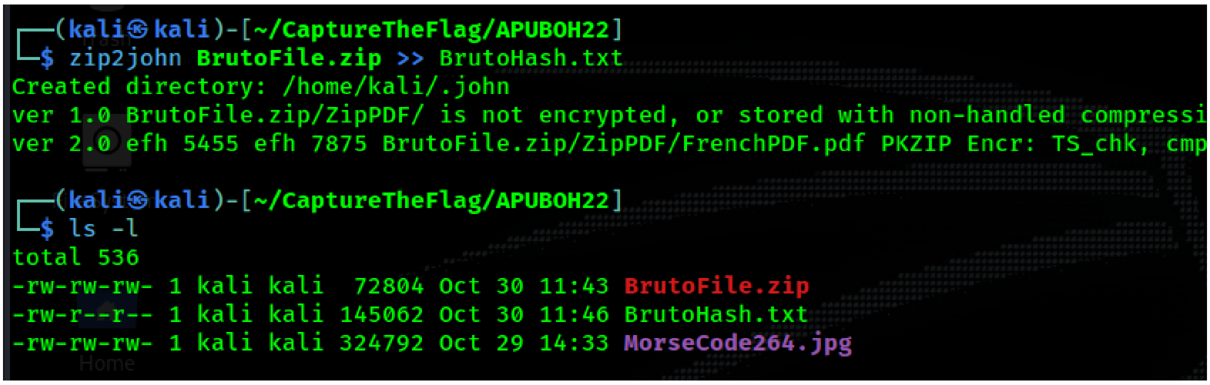
100

Challenge Creator : *Mr.Shahab*

You may recall the Popeye the Sailorpedia cartoon when only his foe Brute could aid in our current zip-cracking endeavour.

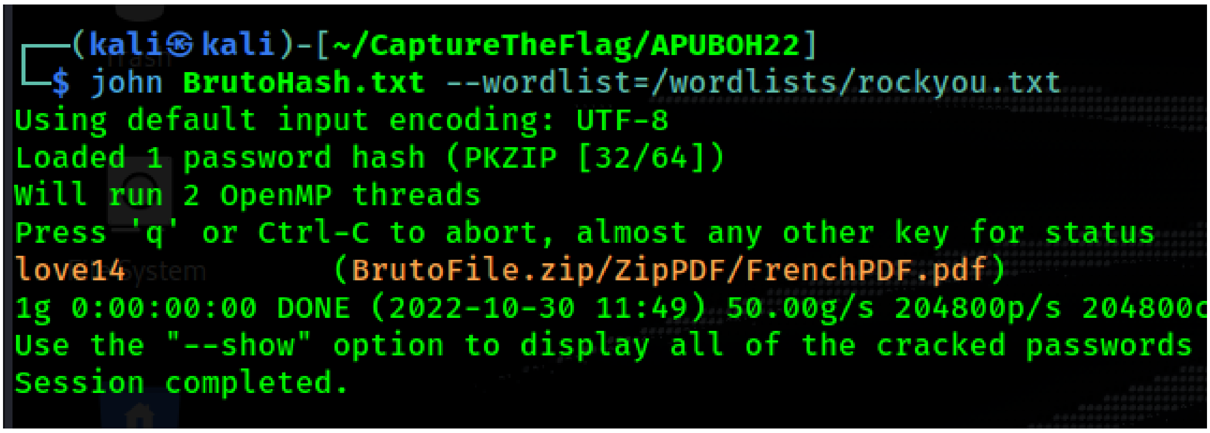
The first forensics challenge is about file zipping, we have been supplied with the zip file called BrutoFile.zip, we try to extract the content of the file, but it need password. So, let's just brute force the password using john.

First, create zip hash using zip2john tools.



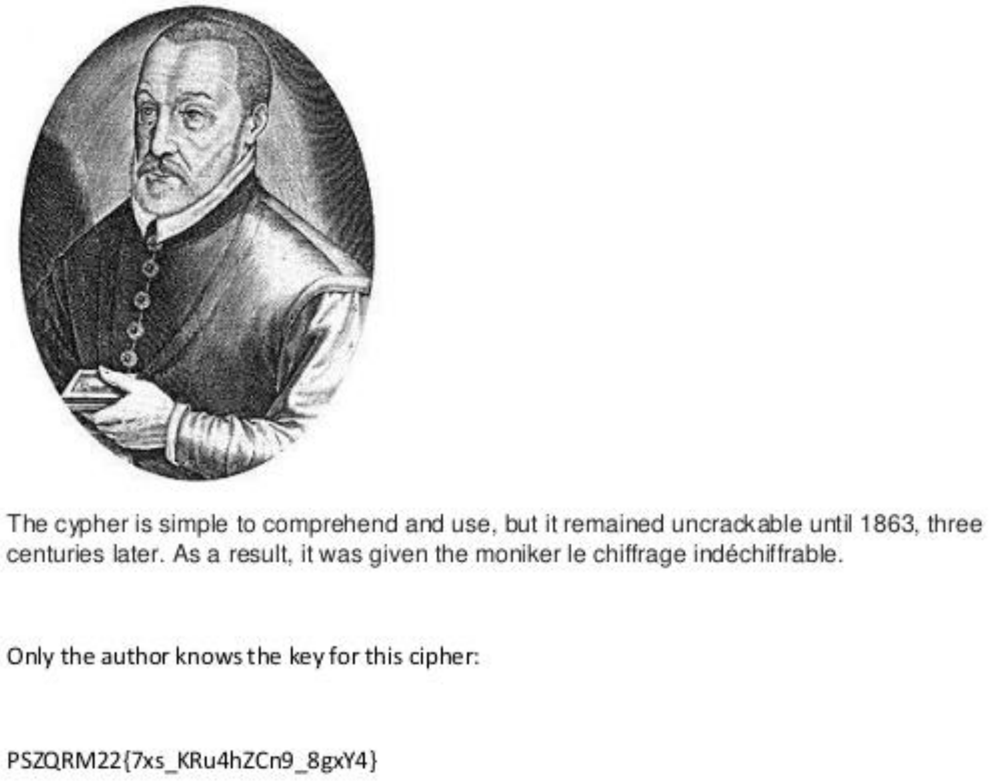
```
┌──(kali㉿kali)-[~/CaptureTheFlag/APUBOH22]
└─$ zip2john BrutoFile.zip >> BrutoHash.txt
Created directory: /home/kali/.john
ver 1.0 BrutoFile.zip/ZipPDF/ is not encrypted, or stored with non-handled compressi
ver 2.0 efh 5455 efh 7875 BrutoFile.zip/ZipPDF/FrenchPDF.pdf PKZIP Encr: TS_chk, cmp

┌──(kali㉿kali)-[~/CaptureTheFlag/APUBOH22]
└─$ ls -l
total 536
-rw-rw-rw- 1 kali kali  72804 Oct 30 11:43 BrutoFile.zip
-rw-r--r-- 1 kali kali 145062 Oct 30 11:46 BrutoHash.txt
-rw-rw-rw- 1 kali kali 324792 Oct 29 14:33 MorseCode264.jpg
```

Then use john to brute force the zip password using common password list "Rockyou".



```
┌──(kali㉿kali)-[~/CaptureTheFlag/APUBOH22]
└─$ john BrutoHash.txt --wordlist=/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
love14           (BrutoFile.zip/ZipPDF/FrenchPDF.pdf)
1g 0:00:00:00 DONE (2022-10-30 11:49) 50.00g/s 204800p/s 204800c
Use the "--show" option to display all of the cracked passwords
Session completed.
```

The password for the zip file is “love14”, after we extract the zip, it will provide us with pdf called FrenchPDF. The content of this pdf is about cryptography, and we can see there are decrypted flag at the bottom of the text.

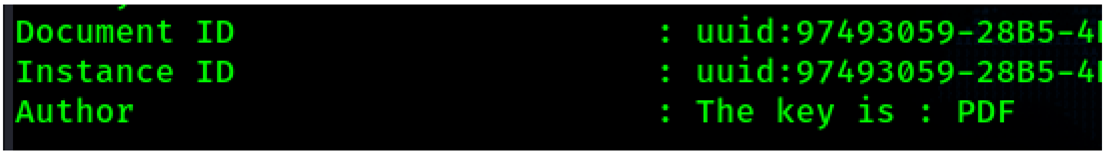


The cypher is simple to comprehend and use, but it remained uncrackable until 1863, three centuries later. As a result, it was given the moniker le chiffrage indéchiffrable.

Only the author knows the key for this cipher:

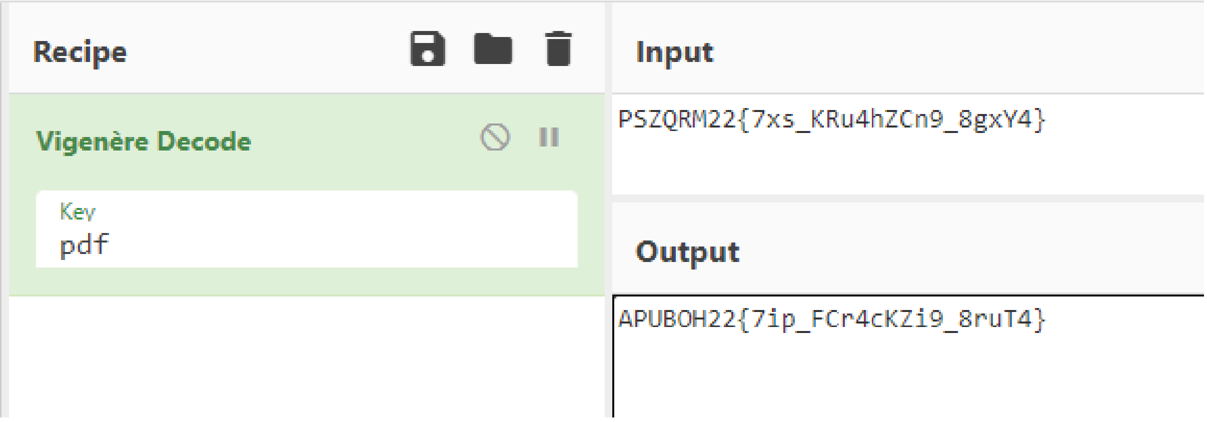
PSZQRM22{7xs_KRu4hZCn9_8gxY4}

The clue for the cipher is on the text given, so the cipher this ciphertext use is Vigenère cipher, but we need the key. The text said only author know the key to decode the ciphertext. Maybe the author of the file is the clue that we need. We can use Exif tool to see the information of the file. And the key of the Vigenère cipher is PDF based on the author tags of the file.



```
Document ID                                      : uuid:97493059-28B5-4
Instance ID                                      : uuid:97493059-28B5-4
Author                                           : The key is : PDF
```

Using key “PDF” we can decode the cipher text and get the flag.



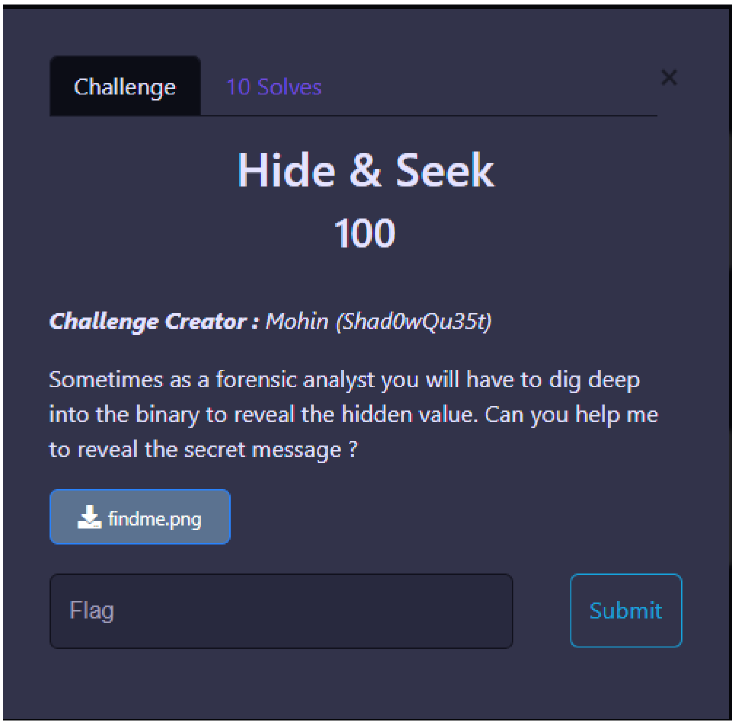
Key
pdf

```
PSZQRM22{7xs_KRu4hZCn9_8gxY4}
```

```
APUBOH22{7ip_FCr4cKZi9_8ruT4}
```

Flag: APUBOH22{7ip_FCr4cKZi9_8ruT4}

Hide & Seek



Challenge 10 Solves

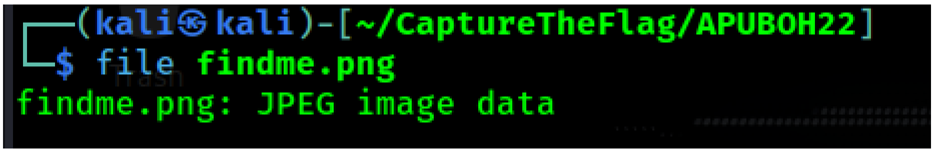
Hide & Seek

100

Challenge Creator : *Mohin (Shad0wQu35t)*

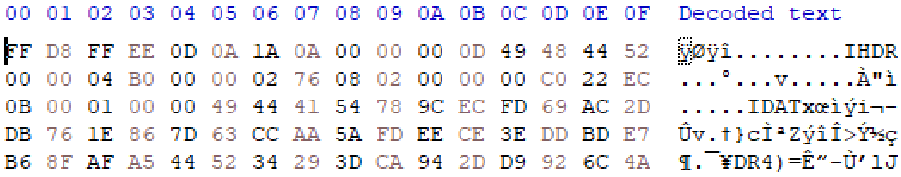
Sometimes as a forensic analyst you will have to dig deep into the binary to reveal the hidden value. Can you help me to reveal the secret message ?

In the challenge, we get the image called findme.png, but the problem is the image is corrupted and cannot be open, after some observations, we noticed that the file is in jpeg, but the extension of the file is png.



```
┌──(kali㉿kali)-[~/CaptureTheFlag/APUBOH22]
└─$ file findme.png
findme.png: JPEG image data
```

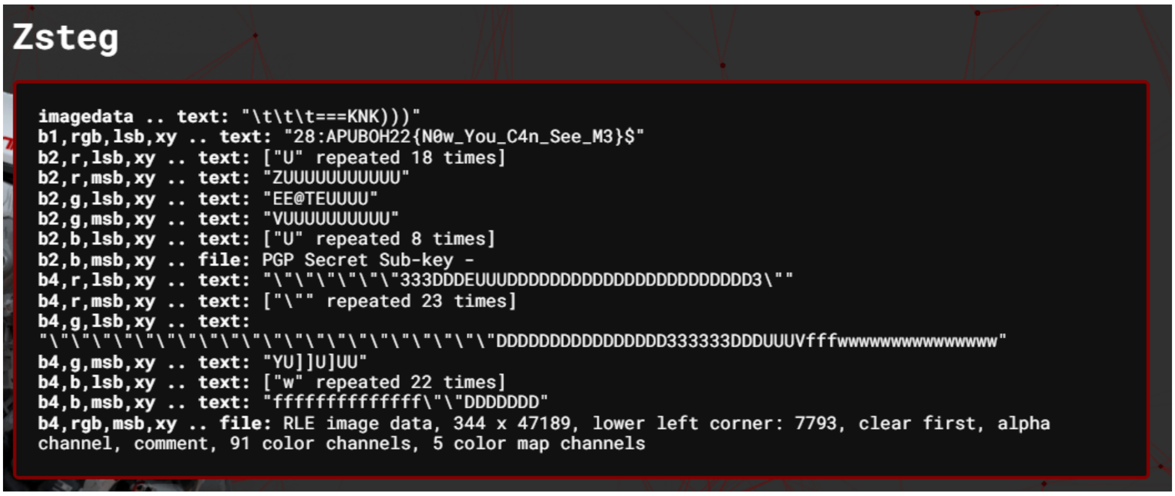
So, it is possible that the file header has been changed to jpeg, so the file will be detected as jpeg. We open the file using hex editor to inspect the file hex and clearly it show the header of the file is in jpeg, so we just need to edit the header to png header.



```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

FF D8 FF EE 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ÿØÿî........IHDR
00 00 04 B0 00 00 02 76 08 02 00 00 00 C0 22 EC  ...°...v.....À"ì
0B 00 01 00 00 49 44 41 54 78 9C EC FD 69 AC 2D  .....IDATxœìýi¬-
DB 76 1E 86 7D 63 CC AA 5A FD EE CE 3E DD BD E7  Ûv.†}cÌªZýîÎ>Ý½ç
B6 8F AF A5 44 52 34 29 3D CA 94 2D D9 92 6C 4A  ¶.¯¥DR4)=Ê”-Ù’lJ
```

Change FF D8 FF EE 0D 0A 1A 0A to 89 50 4E 47 0D 0A 1A 0A and save the file.

This is the real image of findme.png. So now we need to find the flag that hidden inside the image. This is png image so steghide is not applicable for this image. We try to use online steganography to detect the steganography inside the file and we found the flag was embedded into the image using zsteg.



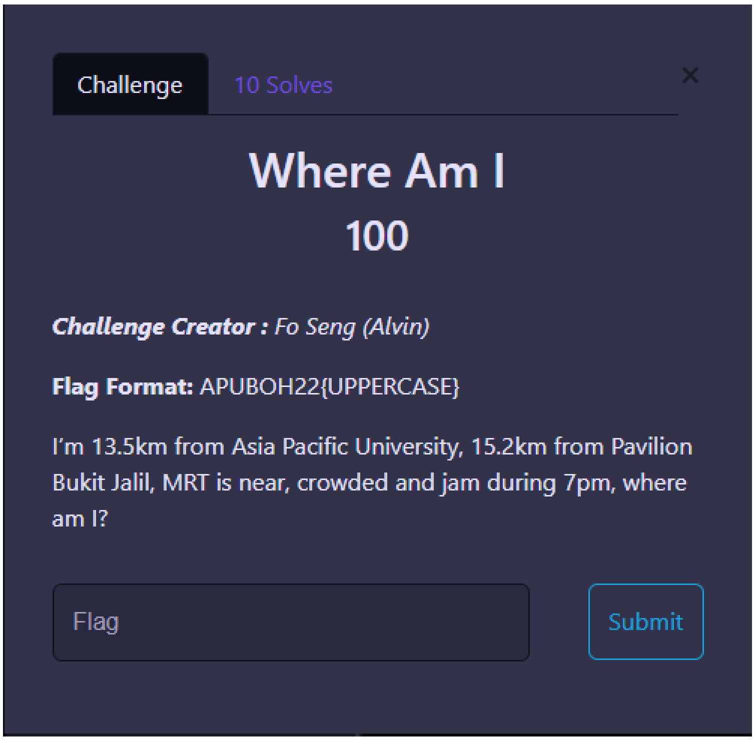
Zsteg

```
imagedata .. text: "\t\t\t===KNK)))"
b1,rgb,lsb,xy .. text: "28:APUBOH22{N0w_You_C4n_See_M3}$"
b2,r,lsb,xy .. text: ["U" repeated 18 times]
b2,r,msb,xy .. text: "ZUUUUUUUUUUU"
b2,g,lsb,xy .. text: "EE@TEUUUU"
b2,g,msb,xy .. text: "VUUUUUUUUUU"
b2,b,lsb,xy .. text: ["U" repeated 8 times]
b2,b,msb,xy .. file: PGP Secret Sub-key -
b4,r,lsb,xy .. text: "\"\"\"\"\"\"333DDDEUUUDDDDDDDDDDDDDDDDDDDDDD3\""
b4,r,msb,xy .. text: ["\"" repeated 23 times]
b4,g,lsb,xy .. text:
"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"DDDDDDDDDDDDDDDD333333DDDUUUVfffwwwwwwwwwwwwwww"
b4,g,msb,xy .. text: "YU]]U]UU"
b4,b,lsb,xy .. text: ["w" repeated 22 times]
b4,b,msb,xy .. text: "fffffffffffff\"\"DDDDDDD"
b4,rgb,msb,xy .. file: RLE image data, 344 x 47189, lower left corner: 7793, clear first, alpha
channel, comment, 91 color channels, 5 color map channels
```

Flag: APUBOH22{N0w_You_C4n_See_M3}

OSINT

Where Am I



Where Am I

100

Challenge Creator : *Fo Seng (Alvin)*

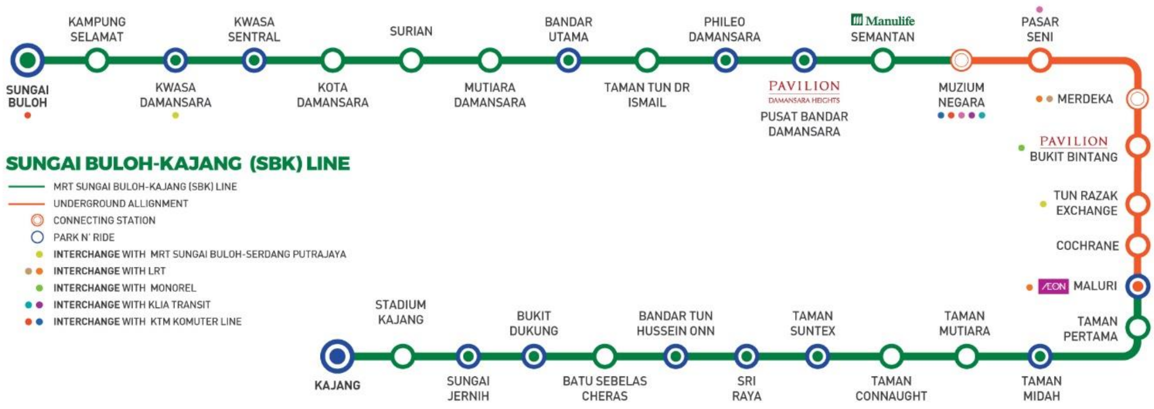
Flag Format: APUBOH22{UPPERCASE}

I'm 13.5km from Asia Pacific University, 15.2km from Pavilion Bukit Jalil, MRT is near, crowded and jam during 7pm, where am I?

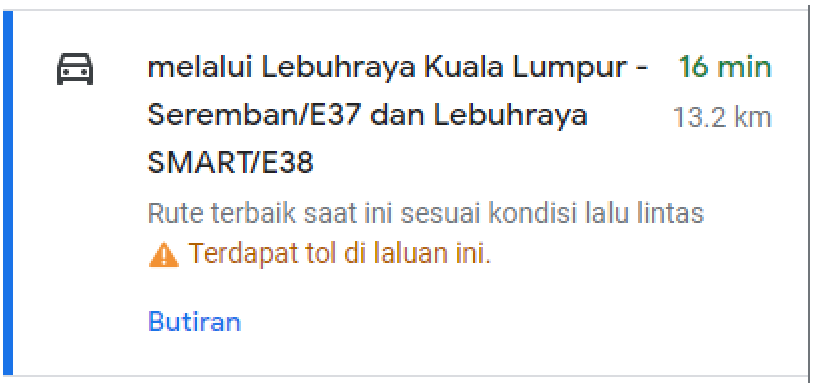
Flag

This OSINT challenge is quite hard when we try to attempt it, we need to find the location from two point which is APU and Pavilion Bukit Jalil, we thought that we need to find the interception between these two points, but we did not find any place that intercept each other, the distance also is different so how can this point intercept.

Our next strategies are to find the MRT station and measure distance between the station and the point given.



First, we try to measure the distance from each MRT station toward APU and match it with 13.5 km distance. After little bit of measuring, we found that MRT Bukit Bintang is the nearest accurate distance from APU that is 13.2 km.



melalui Lebuhraya Kuala Lumpur - Seremban/E37 dan Lebuhraya SMART/E38

16 min

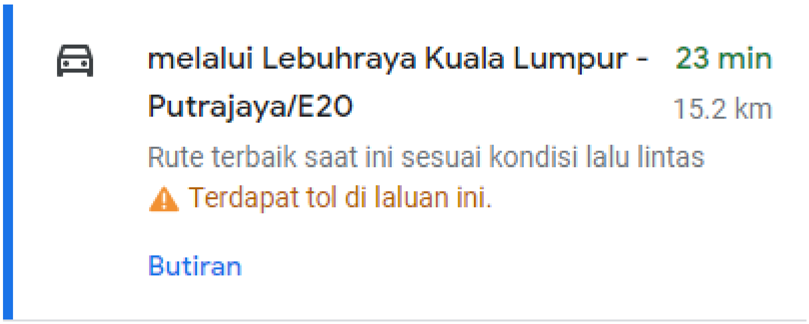
13.2 km

Rute terbaik saat ini sesuai kondisi lalu lintas

⚠ Terdapat tol di laluan ini.

Butiran

The next point is from Pavilion Bukit Jalil. The distance we got is also nearest to the given distance.



melalui Lebuhraya Kuala Lumpur - Putrajaya/E20

23 min

15.2 km

Rute terbaik saat ini sesuai kondisi lalu lintas

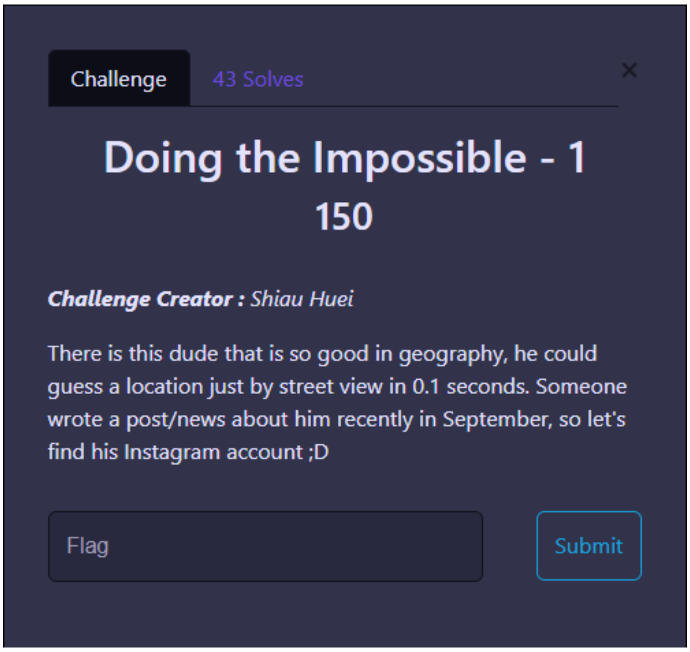
⚠ Terdapat tol di laluan ini.

Butiran

Now come the most challenging phase is to find the place that the question wants, we use a lot of time to figure out where is the place that crowded and jam during 7 p.m. After many tries, we found the answer and the flag. The place that we need to find is actually Pavilion Kuala Lumpur at Bukit Bintang. We tried many times to figure out what format is the flag and we got it with full of joy.

Flag: APUBOH22{PAVILIONKUALALUMPUR}

Doing the Impossible – 1



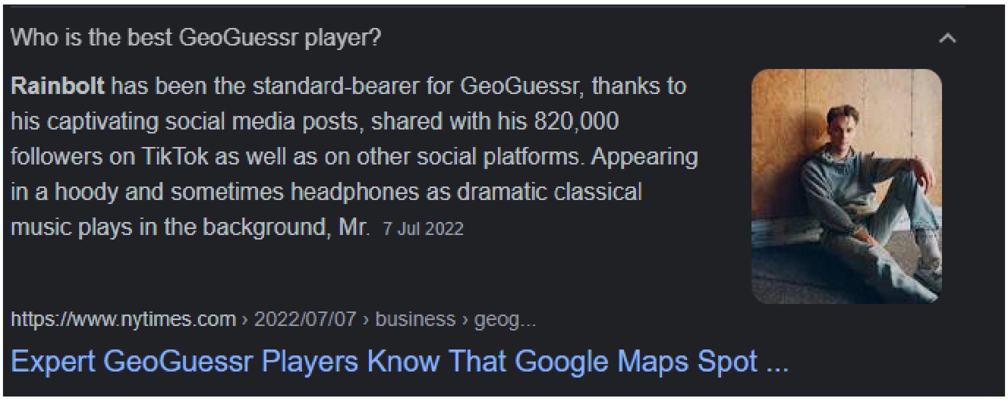
Doing the Impossible - 1

150

Challenge Creator : *Shiau Huei*

There is this dude that is so good in geography, he could guess a location just by street view in 0.1 seconds. Someone wrote a post/news about him recently in September, so let's find his Instagram account ;D

This OSINT challenges start with asking us to find the Instagram of person who professional in geo-guesser. Using some googling, we found that the name of the professional geo-guesser was Rainbolt, so we try to find his Instagram.



Who is the best GeoGuessr player?

Rainbolt has been the standard-bearer for GeoGuessr, thanks to his captivating social media posts, shared with his 820,000 followers on TikTok as well as on other social platforms. Appearing in a hoody and sometimes headphones as dramatic classical music plays in the background, Mr. 7 Jul 2022

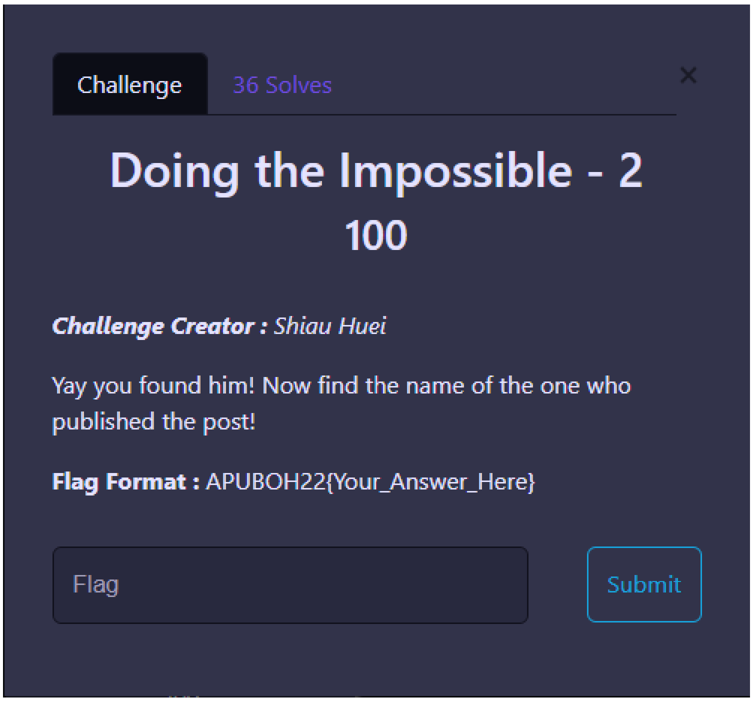
https://www.nytimes.com › 2022/07/07 › business › geog...

Expert GeoGuessr Players Know That Google Maps Spot ...

We found the IG named trevorrainbolt, but that’s not the flag, observing the IG post, we saw that there is the newspaper article about him and there are people tag on the post that led to his famous main account. The IG named georainbolt which is his main account and was the flag of this challenge.

Flag: APUBOH22{georainbolt}

Doing the Impossible – 2



Challenge 36 Solves

Doing the Impossible - 2

100

Challenge Creator : *Shiau Huei*

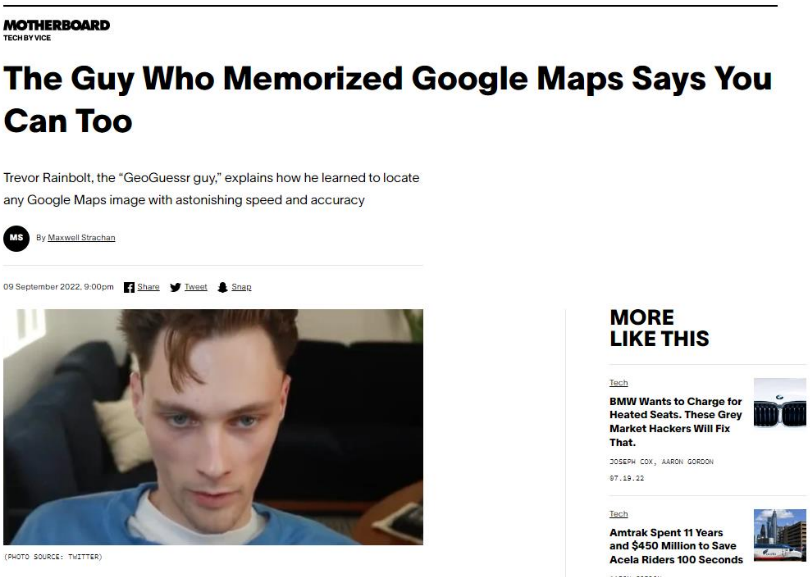
Yay you found him! Now find the name of the one who published the post!

Flag Format : APUBOH22{Your_Answer_Here}

Flag

Submit

This next challenge is quite hard, first we need to find the article about Rainbolt, there are so many articles about him, so we try to check the author's name one by one of the articles we found, one of the articles write by Maxwell Strachan and that is the article writer that we want.



MOTHERBOARD
TECH BY VICE

The Guy Who Memorized Google Maps Says You Can Too

Trevor Rainbolt, the "GeoGuessr guy," explains how he learned to locate any Google Maps image with astonishing speed and accuracy

MS By Maxwell Strachan

09 September 2022, 9:00pm Share Tweet Snap

(PHOTO SOURCE: TWITTER)

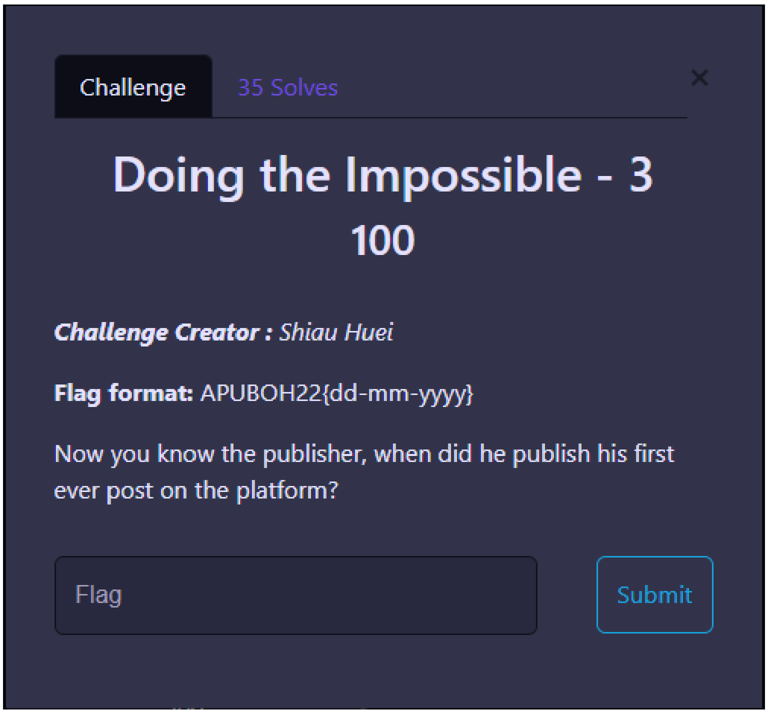
MORE LIKE THIS

Tech
BMW Wants to Charge for Heated Seats. These Grey Market Hackers Will Fix That.
JOSEPH COX, AARON GORDON
07.19.22

Tech
Amtrak Spent 11 Years and $450 Million to Save Acela Riders 100 Seconds

Flag: APUBOH22{Maxwell_Strachan}

Doing the Impossible – 3



Challenge

35 Solves

Doing the Impossible - 3

100

Challenge Creator : *Shiau Huei*

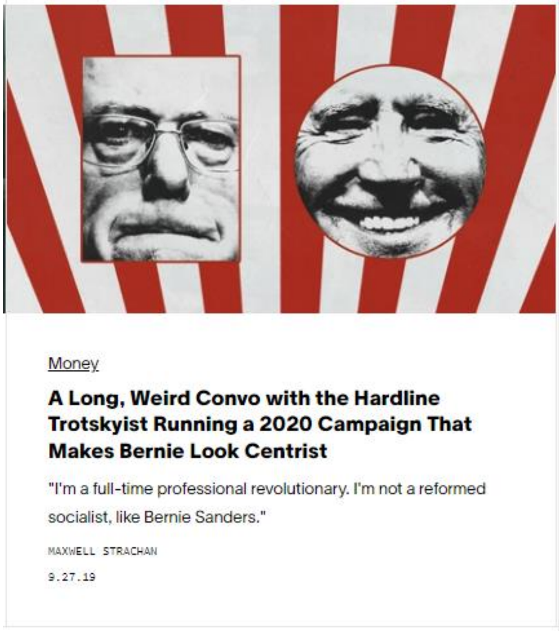
Flag format: APUBOH22{dd-mm-yyyy}

Now you know the publisher, when did he publish his first ever post on the platform?

Flag

Submit

The third challenges of Doing the Impossible is quite easy, we just need to find the date of Maxwell first article on Vice.com. We can open his profile and choose the older sort to view his first ever post. The date of the article is the flag.



Money

A Long, Weird Convo with the Hardline Trotskyist Running a 2020 Campaign That Makes Bernie Look Centrist

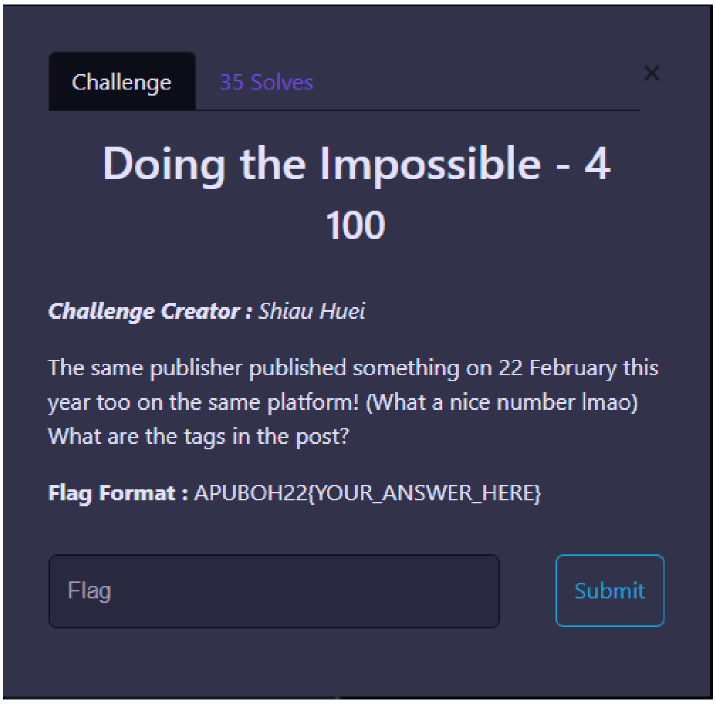
"I'm a full-time professional revolutionary. I'm not a reformed socialist, like Bernie Sanders."

MAXWELL STRACHAN

9.27.19

Flag: APUBOH22{27-09-2019}

Doing the Impossible – 4



Doing the Impossible - 4

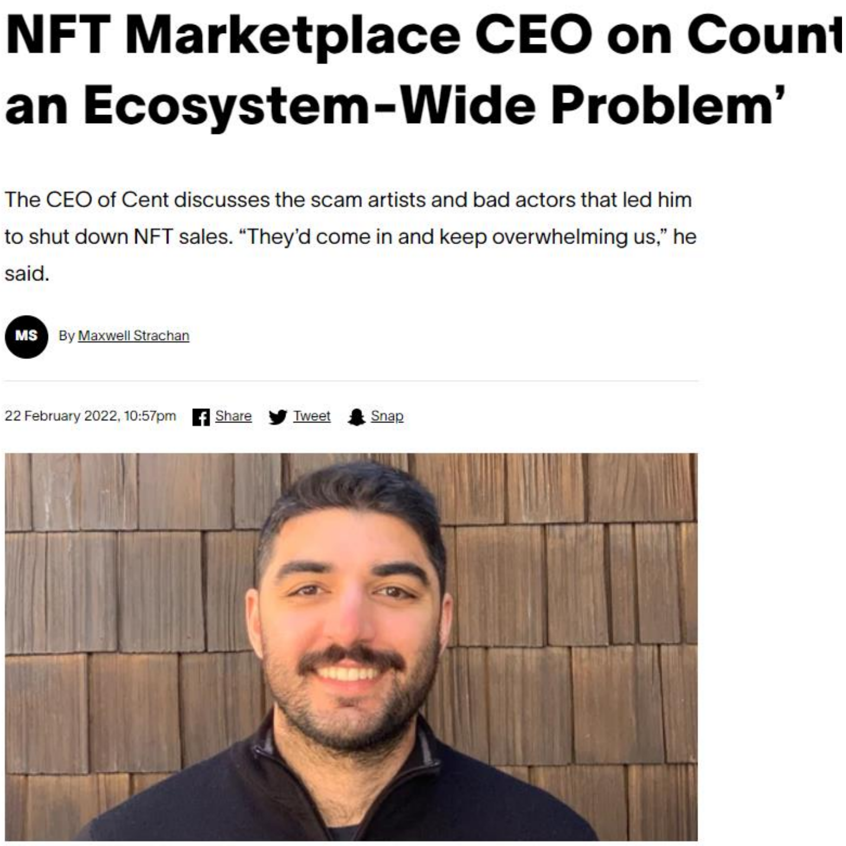
100

Challenge Creator : *Shiau Huei*

The same publisher published something on 22 February this year too on the same platform! (What a nice number lmao) What are the tags in the post?

Flag Format : APUBOH22{YOUR_ANSWER_HERE}

The last challenge for Doing the Impossible is also straight forward. First, we need to find the article with date 22 February 2022.



NFT Marketplace CEO on Count
an Ecosystem-Wide Problem'

The CEO of Cent discusses the scam artists and bad actors that led him to shut down NFT sales. “They'd come in and keep overwhelming us,” he said.

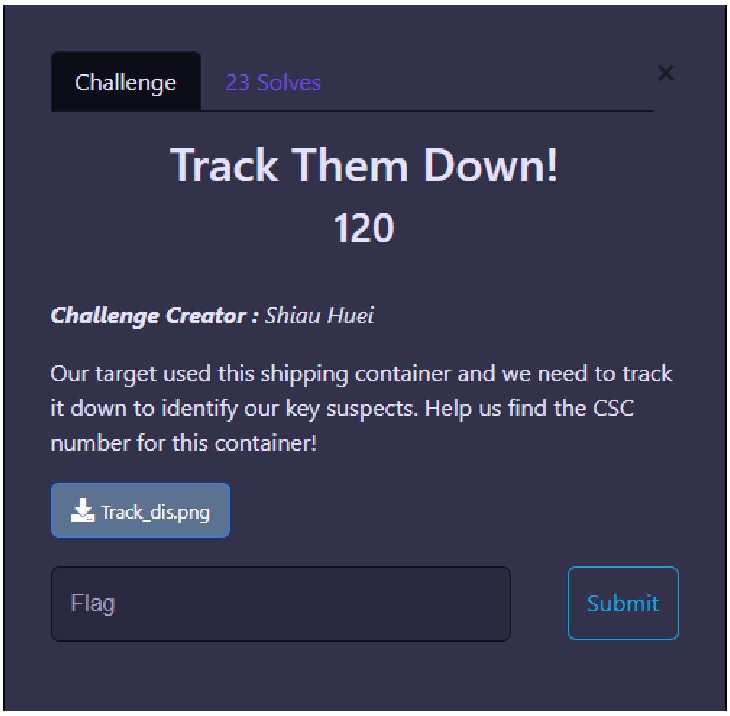
MS By Maxwell Strachan

22 February 2022, 10:57pm Share Tweet Snap

After we found the article, search for the tags at the bottom of the article and we got the flag.

Flag: APUBOH22{BLOCKCHAIN_CRYPTO_OPENSEA}

Track Them Down!



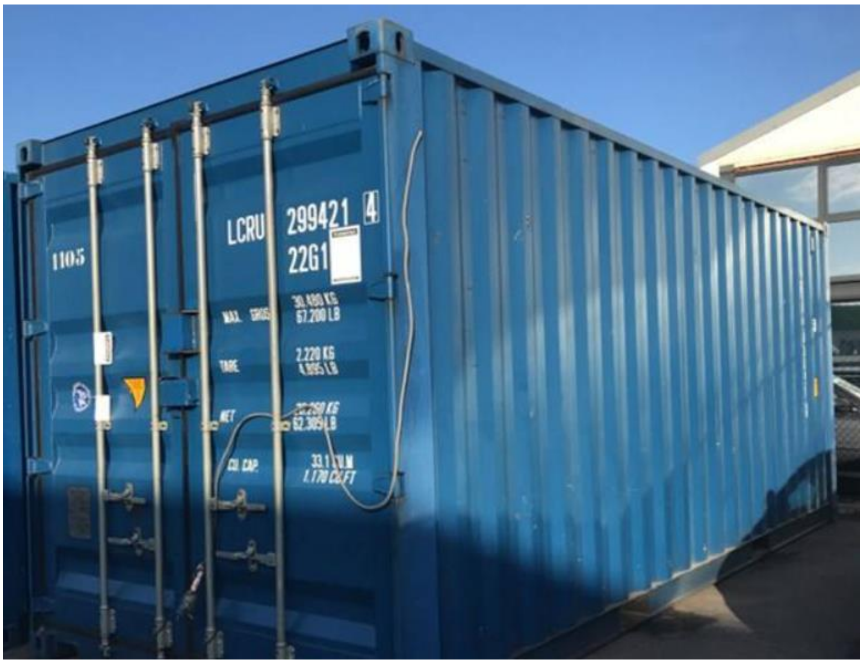
Track Them Down!

120

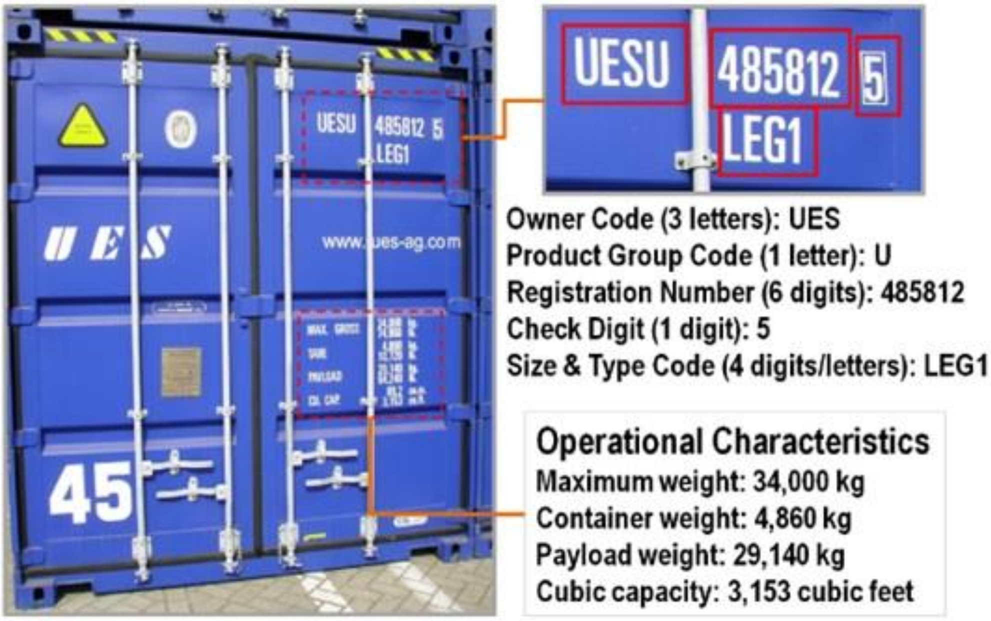
Challenge Creator : *Shiau Huei*

Our target used this shipping container and we need to track it down to identify our key suspects. Help us find the CSC number for this container!

This challenge is quite interesting because it searches the container CSC number. From the challenges, we got the image of container with a information shown on the container.



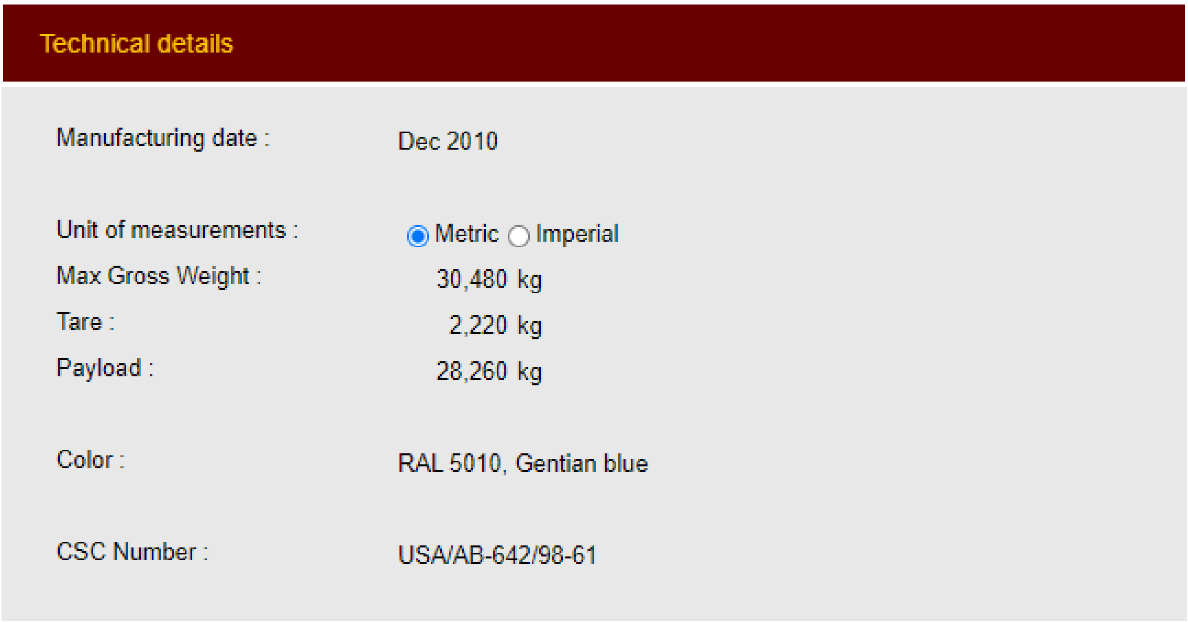
But the problem is we don’t know how to read those numbers and letters, after some research we got to know how to real the container serial numbers.



Owner Code (3 letters): UES
Product Group Code (1 letter): U
Registration Number (6 digits): 485812
Check Digit (1 digit): 5
Size & Type Code (4 digits/letters): LEG1

Operational Characteristics
Maximum weight: 34,000 kg
Container weight: 4,860 kg
Payload weight: 29,140 kg
Cubic capacity: 3,153 cubic feet

So, the container number is LCRU2994214. Next, we need to search for the CSC number of this container. We search for online tools that help us to track the CSC number and we found one site that very useful, it was https://www.track-trace.com/. By entering the container number, we got the CSC number.



Technical details

Manufacturing date :	Dec 2010
Unit of measurements :	● Metric ○ Imperial
Max Gross Weight :	30,480 kg
Tare :	2,220 kg
Payload :	28,260 kg
Color :	RAL 5010, Gentian blue
CSC Number :	USA/AB-642/98-61

Flag: APUBOH2022{ USA/AB-642/98-61}

Memorabilia

Thank You ❤