

APU BOH 2022 WRITEUP

WHITE HAT PIONEER



1. BinarySub

File given: Key.txt, CipherText.txt

Key is given in binary format, time to use cyberchef.

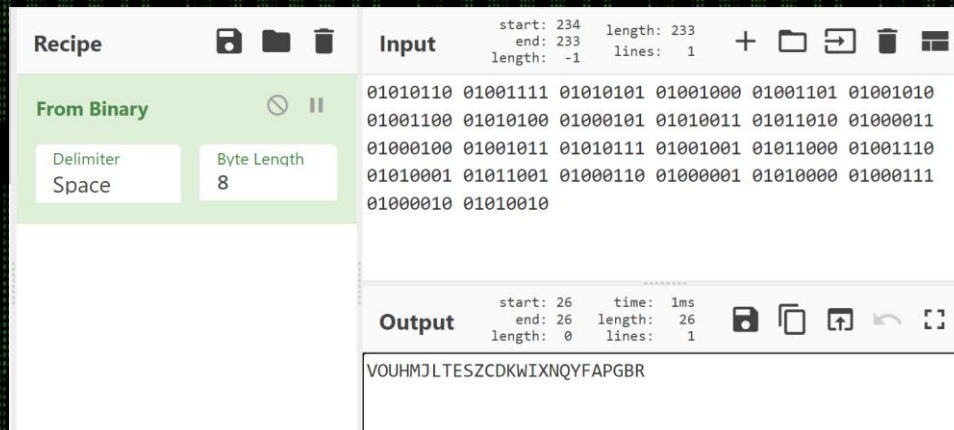


Diagram 1 – Key.txt in CyberChef

Using the key, decrypt the cipher text by substitution cipher.

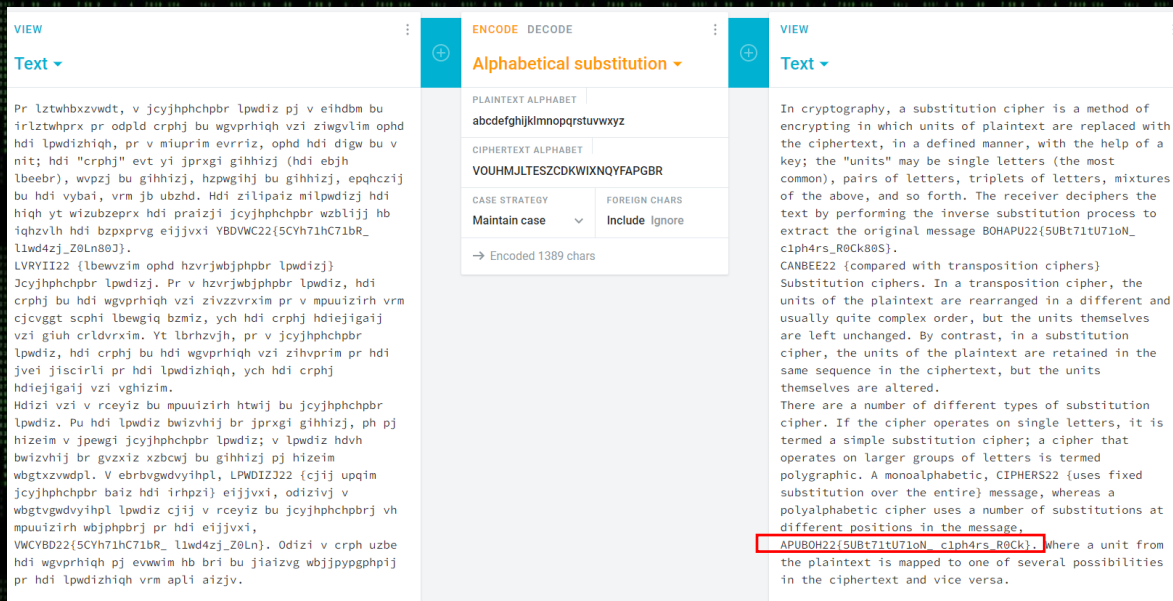


Diagram 2 – CipherText.txt in Cryptii.com

Now here is the flag, but we are required to capitalize.



```
> "APUBOH22{5UBt71tU71oN_c1ph4rs_R0cK}".toUpperCase()  
< 'APUBOH22{5UBT71TU71ON_C1PH4RS_R0CK}'  
> |
```

Done.

Flag: APUBOH22{5UBT71TU71ON_C1PH4RS_R0CK}

2. LeakedCredentials – 1

From the question, we can know that we want to find Chantelle Zig II and Veronica Atbash.

LeakedCredentials - 1

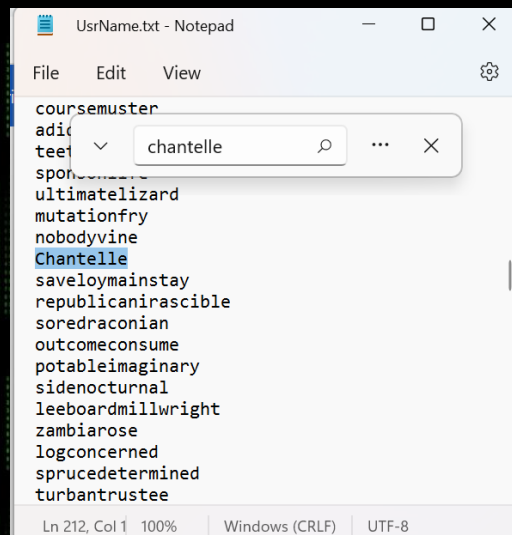
80

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?

[LkCred.rar](#)

We can see Chantelle in UserName.txt at line 212. Let see the line 212 in Passwd.txt.



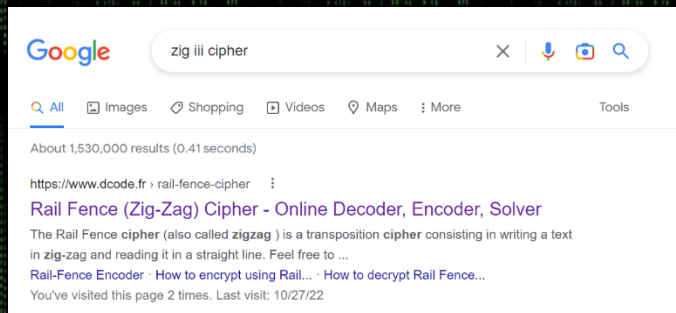


WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

There is only one Chantelle in UserName.txt. If that so, what does the “Zig III” means?

After searching for zig III cipher, the result is shown.



Using dcode.fr and type 3 as the parameter, the answer is shown.



flag: APUBOH22{Rail_Fence_Encryption}

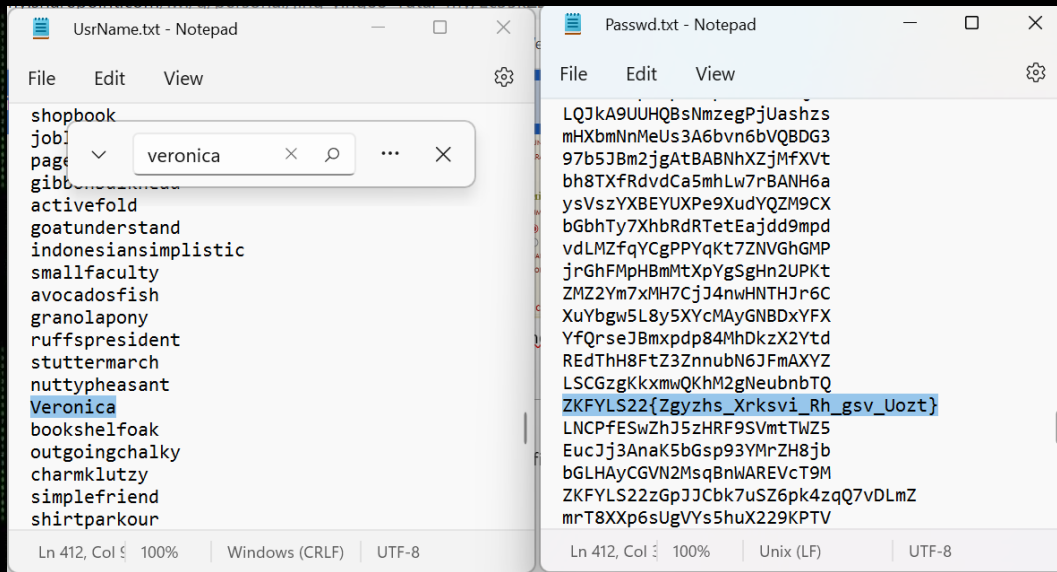


WHITE HAT PIONEER

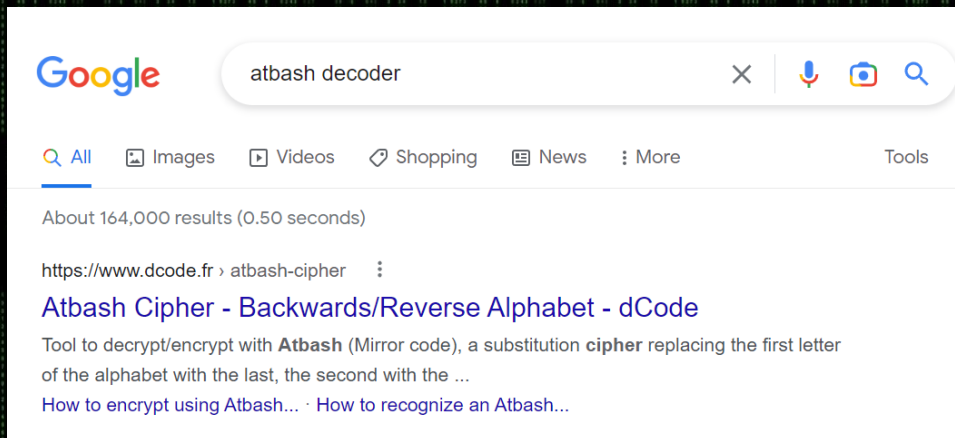
Universiti Tunku Abdul Rahman

3. Crypto – LeakedCredentials – 2

Using the same concept above, we can find Veronica at UsrName.txt and her corresponding password.



Google search for AtBash decoder.

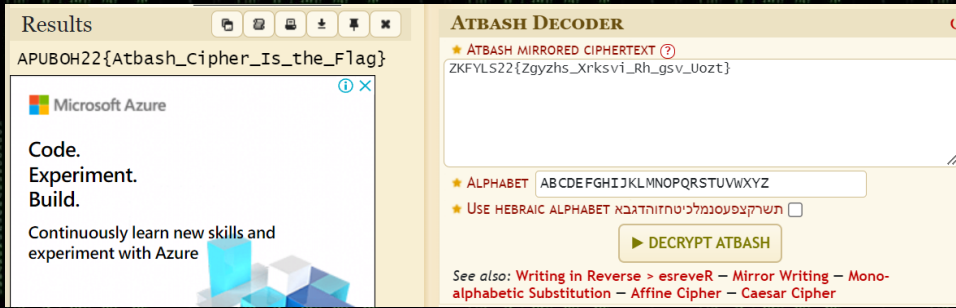




WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

Type the password and choose decrypt. The result is printed.

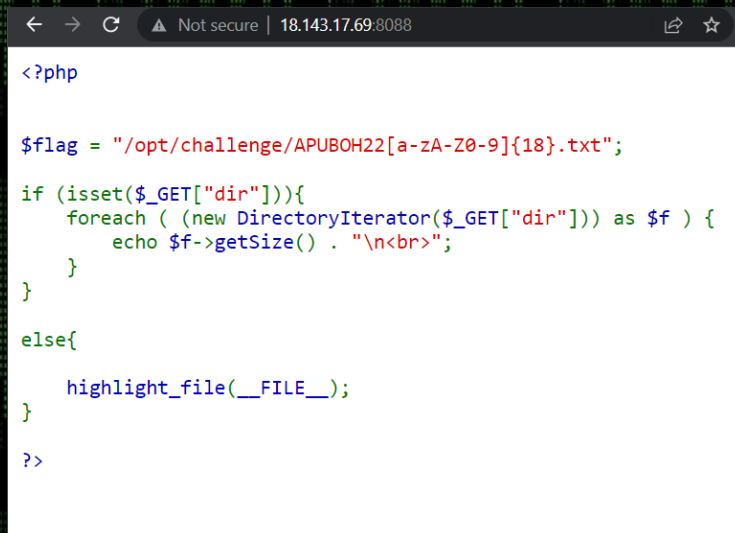


Flag: APUBOH22{Atbash_Cipher_Is_the_Flag}

WEB

1. Sensitive Data

I didn't manage to solve this during the CTF, I was thinking of how to perform RCE, I must be thinking too much :)



The index.php receive GET request and show all file size of the files inside the requested directory. Let's see how it works.



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman



In this /var/www/html directory, there are 4 files, where one of them is index.php.

I notice that there is a hint saying “special protocol”, I suspect this is the one.

https://www.cnblogs.com/littlehann/p/3665062.html#_label3_3_2_0

1、glob://伪协议

glob:// 查找匹配的文件路径模式

```
<?php
// 循环 ext/spl/examples/ 目录里所有 *.php 文件
// 并打印文件名和文件尺寸
$it = new DirectoryIterator("glob://E:\\wamp\\www\\test\\*.php");
foreach($it as $f)
{
    printf("%s: %.1FK\n", $f->getFilename(), $f->getSize()/1024);
}
?>
```

Yes! It is suspicious, just like searching filename containing “aa*” in the directory, which is how you search a file in windows file explorer :). Based on the php code, the txt filename starts with “APUBOH2022”.

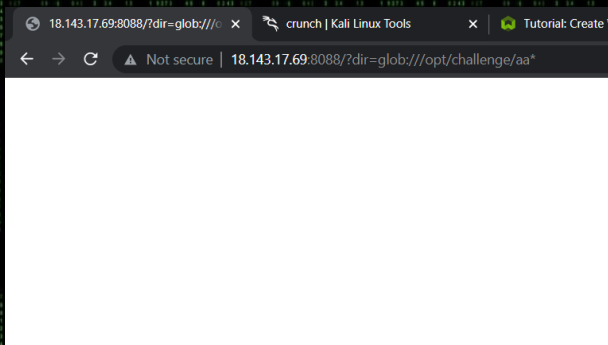


Diagram – File not found

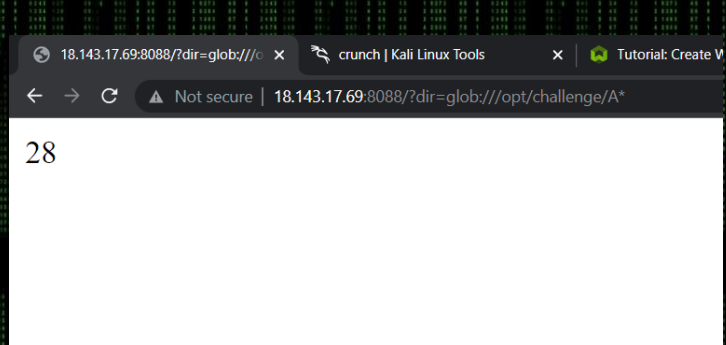


Diagram – 1 File found



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

```
$flag = "/opt/challenge/APUBOH22[a-zA-Z0-9]{18}.txt";
```

The format of the filename is actually given so I decided to trial and error one character by one character.

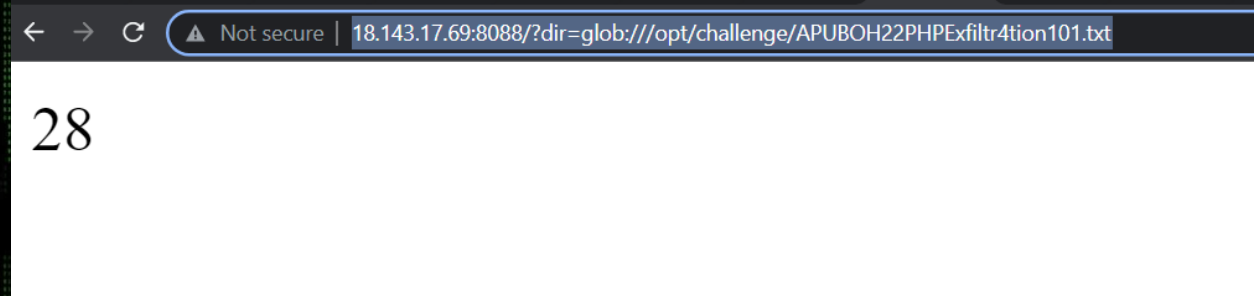
```
(kali@MSI)-[~]
$ crunch 38 38 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 -t ?dir=glob:///opt/ch
allenge/APUBOH22P@* -o test3.txt
Crunch will now generate the following amount of data: 2418 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 62
crunch: 100% completed generating output

(kali@MSI)-[~]
$ gobuster dir -u http://18.143.17.69:8088/ -w test3.txt | grep "Size: 7"
/?dir=glob:///opt/challenge/APUBOH22PH* (Status: 200) [Size: 7]

(kali@MSI)-[~]
$ crunch 40 40 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 -t ?dir=glob:///opt/ch
allenge/APUBOH22PH@* -o test4.txt
Crunch will now generate the following amount of data: 2542 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 62
crunch: 100% completed generating output

(kali@MSI)-[~]
$ gobuster dir -u http://18.143.17.69:8088/ -w test4.txt | grep "Size: 7"
/?dir=glob:///opt/challenge/APUBOH22PHPE* (Status: 200) [Size: 7]
```

With the help of gobuster and crunch(wordlist generator), I manually iterate the last 18 characters. For every iteration, successful request with size 7 means it is the right i-th character.



Filename: APUBOH22PHPExfiltr4tion101



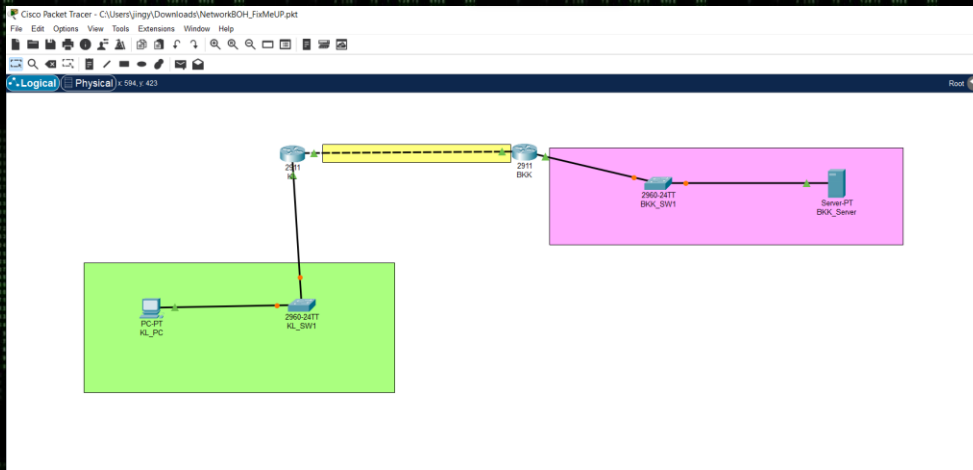
WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

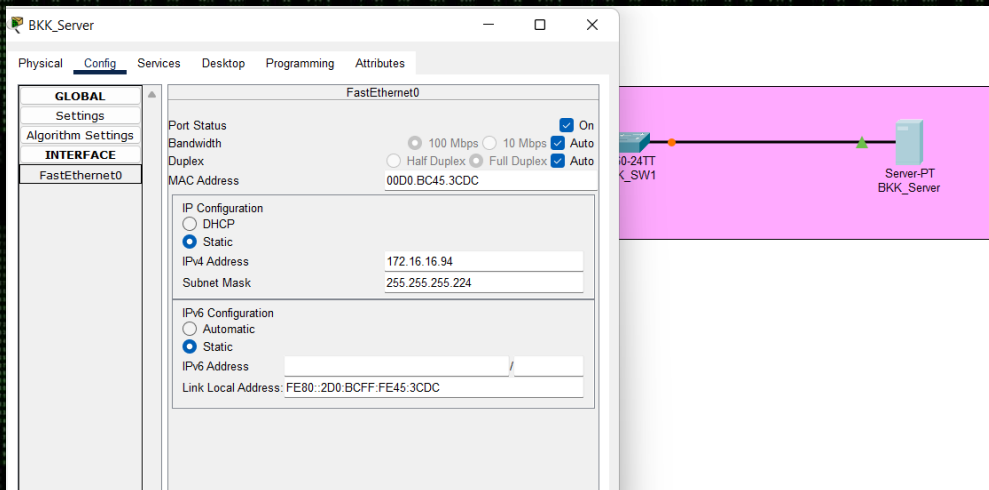
Network

1. NetworkBOH

It is a pkt file, so obviously just open it in Cisco Packet Tracer. Now you see two simple networks. Maybe there is something in the web server?



So we check the IP address of the server, and surf it through browser.

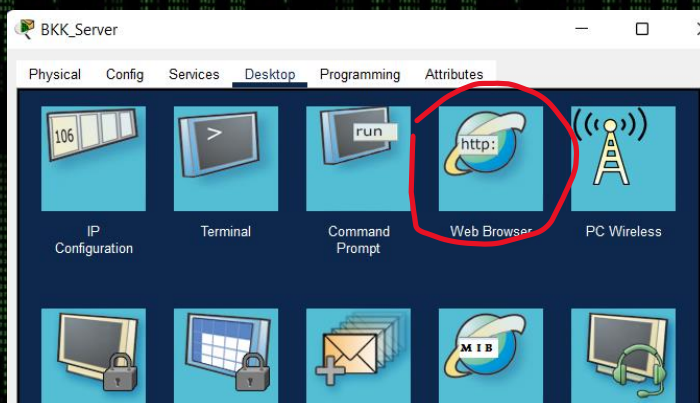
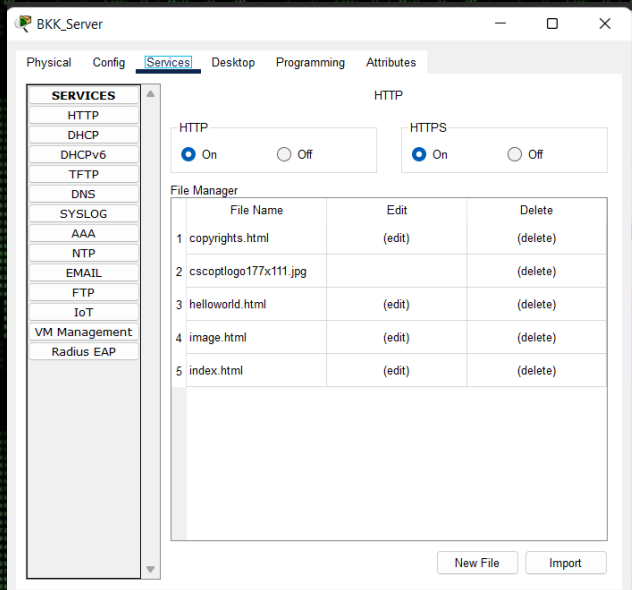




WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

Let's see what files are inside this server first.

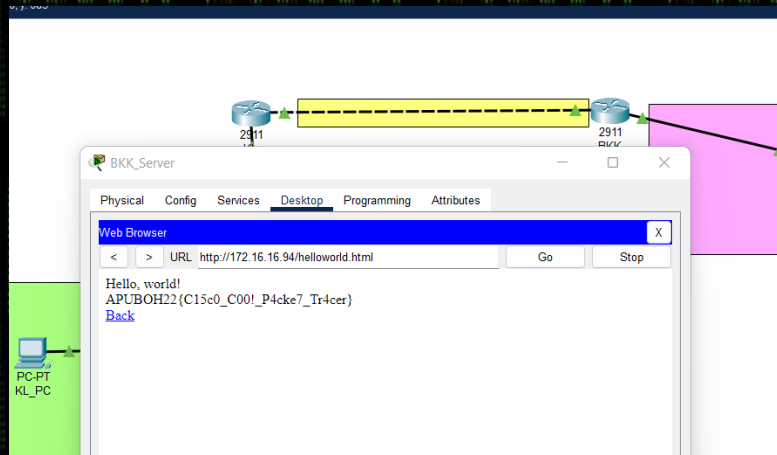


Try to browse this server.



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman



Surf the server, trial and error, voila the flag is here!

Flag: APUBOH22{C15c0_C00!_P4cke7_Tr4cer}



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

MISC

1. MorseCode264

1. Use exiftool to investigate the provided picture.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ exiftool MorseCode264.jpg
ExifTool Version Number      : 12.44
File Name                    : MorseCode264.jpg
Directory                    : .
File Size                    : 325 kB
File Modification Date/Time  : 2022:10:27 02:02:35-04:00
File Access Date/Time       : 2022:10:28 12:49:06-04:00
File Inode Change Date/Time  : 2022:10:28 12:49:05-04:00
File Permissions             : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                  : 288
Y Resolution                  : 288
Creator                      : TFNbDUXpNHVJQzRnTGk0dExTNRHJQzR1TFM0Z0xpMHV
MaUF1TFNBdExTNGdMaTR0TFM0dELDNHVJQzR1TGLBdUxpMHRMaTBnTFMwdExpNGdMaTBnTGk0dULD
NHVMaTR0SUM0dUxTMHVMU0F0TGk0dUxpQXVMaTR1TFNBdUxpMHRMaTBnTFNBdUxTMGdMaTB0TFMwZ
0xTNRHMaUF1TGk0dUxTQXVMaTB0TGk0dUxTQXVMaTR1SUM0dUxpNHRJQzB1SUM0dUxTMHVMU0F0TF
NBdExTMGdMaTB1SUM0dUxpQXVMaTR1TFE9PQ==
Image Width                  : 1814
Image Height                 : 1482
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1814x1482
Megapixels                   : 2.7
```




WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

- II. We found some suspicious texts at Creator. Let's throw it into cyberchef and see what it would be.

- III. Click the magic wand continuously. Then the flag is obtained.

Flag: APUBOH22{THE_FLAG_IS_8AS4_64_TW1C4_TH4N_MORS4}

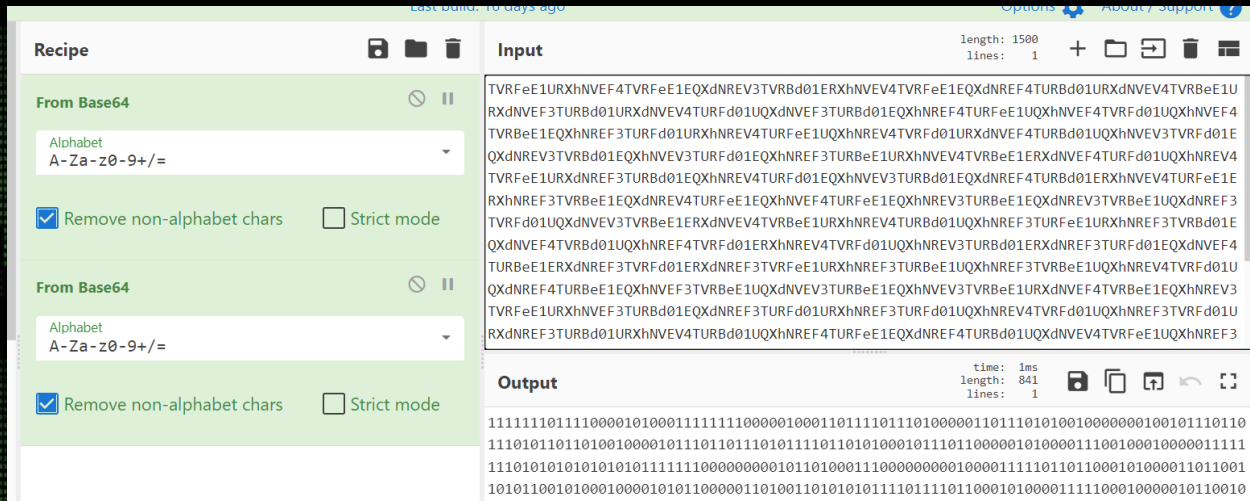


WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

2. Scan It!

Open the text file, apply base64 decode for twice.



With the help of binary to image generator in dcode.fr, choose a suitable size (29x29), now can see a QR code.



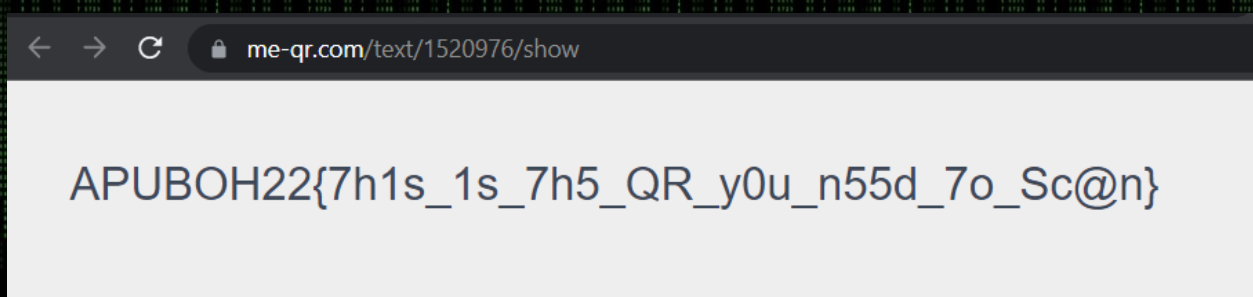


WHITE HAT PIONEER

Universiti Tunku Abdul Rahman



Scan it using your phone, and you will be redirected to a website.



Flag: APUBOH22{7h1s_1s_7h5_QR_y0u_n55d_7o_Sc@n}



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

Forensic

ZipRecursive

We are given a protected zip file. From the challenge description, we knew that BruteForce is required, hence time to ask zip2john for help.

```
zip2john BrutoFile.zip > zip.txt
ver 1.0 BrutoFile.zip/ZipPDF/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 BrutoFile.zip/ZipPDF/FrenchPDF.pdf PKZIP Encr: TS_chk, cmplen=72456, decmplen=78157, crc=DBD56
C07 ts=46A0 cs=46a0 type=8
```

Next, we use hashcat to bruteforce the zip password in incremental mode.

```
./hashcat.exe -a 3 -m 17220 -O -o cracked.txt zip.txt -1 ?l?u?d ?1?1?1?1?1?1
--increment
```

```
Candidate.Engine.: Device Generator
Candidates.#1....: sSzFz -> XQzFz
Hardware.Mon.#1..: Temp: 51c Util: 91% Core:1811MHz Mem:4996MHz Bus:16
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 17220 (PKZIP (Compressed Multi-File))
Hash.Target....: $pkzip$1*1*2*0*11b08*1314d*dbd56c07*41*4e*8*11b08*4...pkzip$
Time.Started...: Sat Oct 29 19:56:55 2022 (7 secs)
Time.Estimated...: Sat Oct 29 19:57:02 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?1?1?1?1?1 [6]
Guess.Charset...: -1 ?l?u?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue....: 6/6 (100.00%)
Speed.#1.....: 679.6 MH/s (42.30ms) @ Accel:192 Loops:256 Thr:32 Vec:1
Speed.##.....: 679.6 MH/s
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 4559732736/56800235584 (8.03%)
Rejected.....: 0/4559732736 (0.00%)
Restore.Point...: 1179648/14776336 (7.98%)
Restore.Sub.#1...: Salt:0 Amplifier:0-256 Iteration:0-256
Candidate.Engine.: Device Generator
Candidates.#1....: saRhZE -> prsq43
Hardware.Mon.#1..: Temp: 53c Util:100% Core:1859MHz Mem:4995MHz Bus:16
```

```
Started: Sat Oct 29 19:56:50 2022
Stopped: Sat Oct 29 19:57:03 2022
--
```

```
185efe228d4e64bc69798028ee50e6e8d4a695daa5ad77215d1c9b6a3e45337c6bd91efce3d891990de44c015199b41ca12f1548f68367c2b60c5e14cc0f7b8a9ff8c864e
224ad44783784be5ba9c51463e95c5db343690aa916ebbe148a940af32e918f1ee14a69d9cb8d3e872c739e41067cb854941b26c57229f5b3da930d1431b9276451312b;
1b8bc65b34e7db36cd7a3b3df8c6998d6995d1f648736aeb5d4643c04dbf7bdd98ac33501698722a496ad3d03616180f7707b2a49f4d01c6f04a7d841e21bbc1279bd0f1c
635049d820fbca1ac1e1eae1440fdae1f6f6644ba00fc055204d4402c3fc5e4074190db337db5f493129203d22735ce6ff761deb7fb69be77f38f210cf97f988770d5f
f44f1805b419df48a7a5527df0f8c159d4be8561f9e81d48f4f013478c0955ebc14af08e88a330f6b679570182fa292b45aba146dfd6c3fda71e96a8de567bace647164f
ca6aa8ea078b67a3081726bd37cc6f2cd0e554dd90661cc7b63a88fb0ce3706ad0fc5f1b521772e7cc7f1bbda9b4f48c2930725c983af7ee0579c6267036d3a4232cb0;
723a881770a2ef43e3fa38447d10532059738f6e8105249ebfb6907276da05ad29229f82d2d72f6b8d297497427d5e6eb9dd3b16b919ff1b91d2dc57a5ba83c2555e88af;
89c9fc8345851e94048dc738f56aec58f19a276db2a1fc91096b9c15b85349b3769153d4b591bac2b34392d3a3ea41d6b6ad0c9df8b5263168094884b2a8061e402840f;
d461f10ebdd*/$pkzip$:love14
```

Password is love14



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman



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 **chiffre** indéchiffrable.

Only the author knows the key for this cipher:

PSZQRM22{7xs_KRu4hZCn9_8gxY4}

We are given a cipher in french PDF.pdf, the man on the picture is Vigenere.

← → ↺ 🔒 <https://www.dcode.fr/vigenere-cipher> 🔊 📖 ⭐ 1.00 🔄

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random' 🔍

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

Vigenere ?
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

↑↓	↑↓
LVKCAG	EXPORG22{7mx_APu4bOhd9_8exS4}
PDFPDF	APUBOH22{7ip_FCr4ckZi9_8ruT4}
FBZZUS	KRARXU22{7sr_LSa4pUBo9_8hdG4}
IYJDNM	HUQNEA22{7pu_BOH4vREe9_8dkM4}
YGRFN	RETZM22{7ze_EAP4uBoH9_8psL4}
QSKWQY	ZAPUBO22{7ha_AVe4jJKd9_8khA4}
SSVXTT	XAETYT22{7fa_PUB4oHks9_8jeF4}
WEDQCS	TOWAPU22{7bo_HBs4pDyk9_8qvG4}
JLZBXL	GHAPUB22{7oh_LQx4wQRo9_8faN4}
KIMSQH	FKNYBF22{7nk_YZe4aPub9_8ohR4}
XDQGA	SPJALM22{7ap_UBo4hCZx9_8qrY4}
ZNTFJR	QFGLIV22{7yf_RM14qAPu9_8boH4}
TTSVX	WZHVUT22{7ea_PUB4oHHq9_8neG4}
DRWKRX	MBDGAP22{7ub_OHd4kWLr9_8wgB4}

#14

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ⓘ
PSZQRM22{7xs_KRu4hZCn9_8gxY4}

PARAMETERS

★ PLAINTEXT LANGUAGE English ▼

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

☐ KNOWING THE KEY/PASSWORD: KEY

☐ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

☐ KNOWING ONLY A PARTIAL KEY: KE?

☒ KNOWING A PLAINTEXT WORD: APUBOH

☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: [Beaufort Cipher](#) — [Caesar Cipher](#)

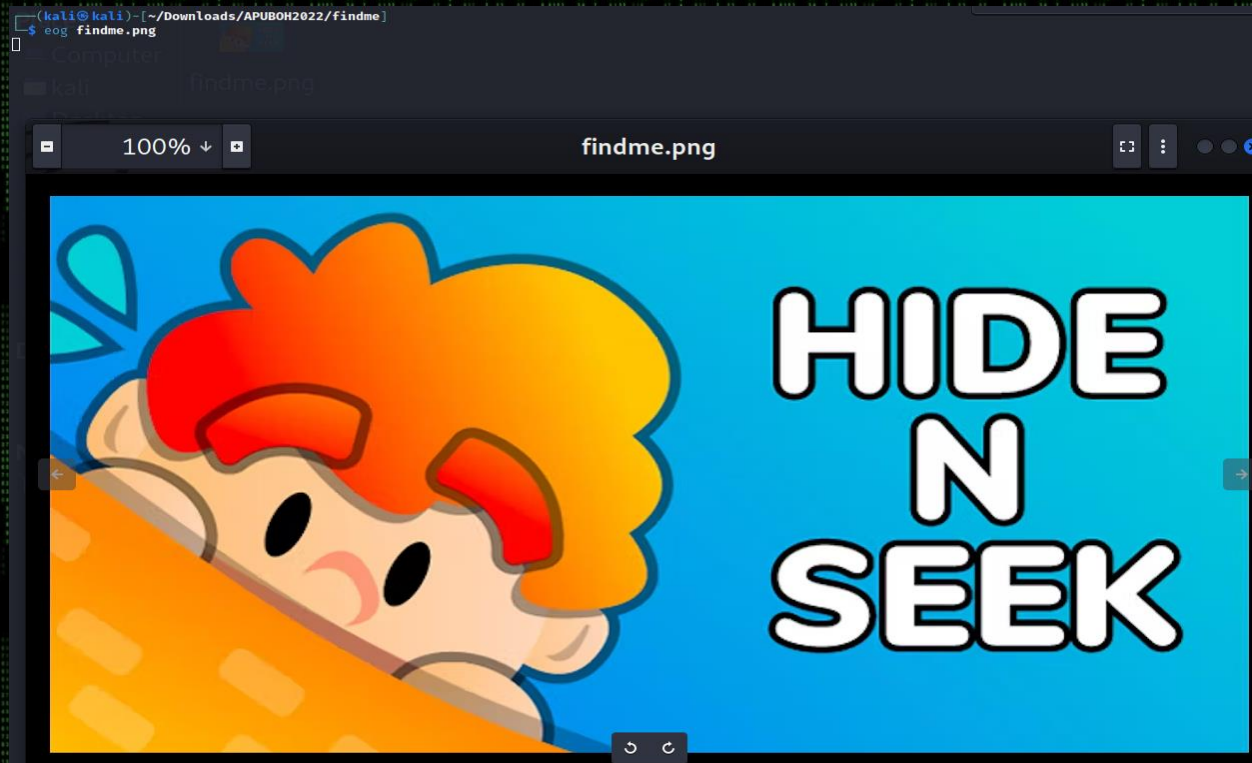
So we try to bruteforce a bit using dcode.fr again. Voila!

Flag: APUBOH22{7ip_FCr4ckZi9_8ruT4}



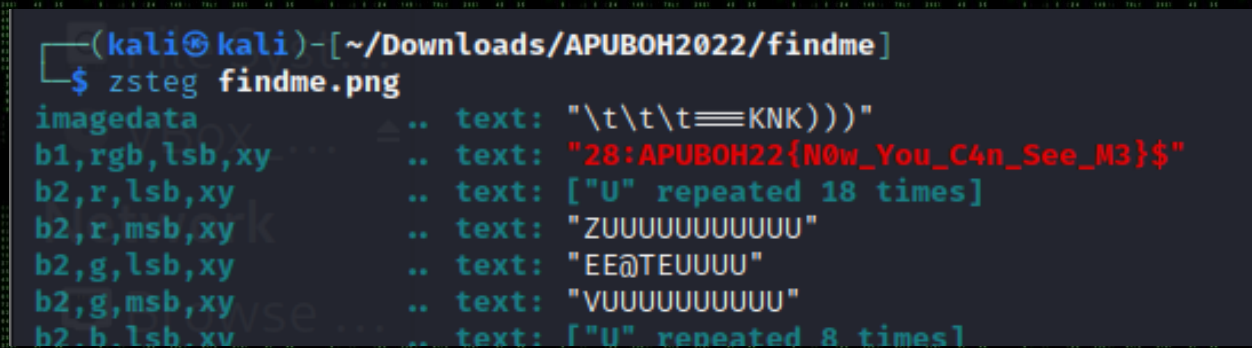
Hide & Seek

Firstly, when we downloaded the file named findme.jpg, we try to view the photo. It looks fine and the file is not corrupted.



Then, we try to open the file using stegsolve and view it in different plane. Unfortunately, the flag is not hiding in any of the planes.

Thinking of hide and seek, maybe the the flag is hidden in the LSB. Thus, we try to use zsteg to detect the LSB Steganography. And boom! The flag is here!



Flag: APUBOH22{N0w_You_C4n_See_M3}




WHITE HAT PIONEER





Universiti Tunku Abdul Rahman


OSINT

Bonus

linkedin.com/company/forensic-security-research-center-student-section-apu/about/







Forensic & Security Research Center Student Section APU

A community at Asia Pacific University that focuses on activities related to Cyber Security including workshops and CTF.

Computer and Network Security · Bukit Jalil, Kuala Lumpur · 362 followers

See all 10 employees on LinkedIn

[+ Follow](#)[Visit website](#)[More](#)

HomeAboutPostsJobsPeopleVideos

Overview

The APU Forensics and Cyber Security Research Center - Student Section (FSeC-SS) is a student chapter of FSec-SS that addresses market demands and future technology needs through nurturing collaborative industry research and developing graduates' employability skills set in the areas of digital forensics, cybersecurity and privacy. By providing a platform for the exchange of ideas, shared challenges and research solutions between academia, industry and the international cybersecurity community, FSeC promotes and supports the development of talent and creative thinking towards cybersecurity.

Website

<https://youtu.be/J9xDyEYJN2c>

Industry

Computer and Network Security

Company size

11-50 employees

Let's check FSECSS APU LinkedIn page. The website sections look sus.



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

"NO TECHNOLOGY THAT'S CONNECTED
TO THE INTERNET IS UNHACKABLE". BEST
OF LUCK TO EVERY BATTLE OF HACKERS
2022 PARTICIPANTS!

Oh yeah, and here's the flag: APUBOH22{whErE_D1D_tH3_4Ud1o_9o?}

13:20 / 14:03

VSBOaGuayB0aGUgdGI0bGUgaXMgdGhlIGZsYWw/IFdlbGwgaXQgYWluJ3Q3Qga2Vrdw==

43次观看 · 2022年10月27日

👍 1 🗨 踩 🔗 分享 ⬇ 下载 🎧 剪辑 ➡ 保存 ...

全部

最近上传的内容

已观看

👤 卢卡斯的脱口秀很尴尬! ? 【大

Surprise! The flag is here, didn't really notice it during the opening ceremony :)

Flag: APUBOH22{whErE_D1D_tH3_4Ud1o_9o?}



WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

Doing the Impossible – 1

From the given hint, we try to google search “dude that is so good in geography, he could guess a location just by street view in 0.1 seconds”, and we find the Instagram name of the guy is “georainbolt”

Google

dude that is so good in geography, he could guess a l

All

Images

Videos

Books

Maps

More

Tools

About 23,900,000 results (0.61 seconds)

Videos



How This Guy Can Guess Where He Is In 0.1 Seconds ...

YouTube · Cheddar
18 Aug 2022



google maps but u have to guess in 2 seconds #geo ...

TikTok · georainbolt
24 Mar 2022



georainbolt

Message

Follow

...

94 posts 418K followers 21 following

rainbolt

professional google maps player

[georainbolt.com](https://www.georainbolt.com)



finding str...



tips

Flag: APUBOH22{georainbolt}



Doing the Impossible – 2

From the results of the google search in 1, we observed that there are two posts written of this guy on September, so we click in the post.

<https://www.autoevolution.com> > News > Technology :

Faster Than Google: This Man Needs Just 0.1 Seconds to ...

12 Sept 2022 — Probably the **best** GeoGuessr player in the entire world, Trevor Rainbolt is able to locate any Google Maps image faster than **you** blink.

Missing: geography, | Must include: geography,

<https://www.vice.com> > Home > Tech :

The Guy Who Memorized Google Maps Says You Can Too

9 Sept 2022 — **He** can do **so** after **only** looking at the image for **0.1 seconds**, ... from Google **Street View** and then click the area of the world in which they ...

Luckily, we manage to spot the name of the publisher inside the post.

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, 1:00pm [f Share](#) [t Tweet](#) [s Snap](#)

Flag: APUBOH22{Maxwell_Strachan}



Doing the Impossible – 3

After that, we just click in the profile of the publisher and check all the posts of the publisher. Since the posts are arranged from the latest to the oldest, we navigate to the last page of the posts.



Money

How Baby Boomers Have Killed the Manhattan Power Lunch

Perhaps, and stay with me here, responsibility for the power lunch's death rests with the people who have power and time for lunch.

MAXWELL STRACHAN

10.29.19

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

Newer 11 / 11 Older

From here, we can see the date of the first post is 9.27.19.

Flag: APUBOH22{27-09-2019}



Doing the Impossible – 4

Checking the post of the same publisher in 22 February 2022, there are total of 3 tags in the post.

Do we have challenges to solve? Yeah, but we're smart people. We can come together, and we can fix the problems inherent to the systems that we've created.

TAGGED: BLOCKCHAIN, CRYPTO, OPENSEA

Flag: APUBOH22{BLOCKCHAIN_CRYPTO_OPENSEA}



Track Them Down!

After we downloaded the "Track_dis.png", there are some information in the photo.



Then, we try to google the container information, and found this clear explanation.





WHITE HAT PIONEER

Universiti Tunku Abdul Rahman

Based on the information give, we know that the container number/ID is LCRU299421. Then we google search this container number and discover the company of this container is CARU CONTAINERS.

<https://www.bic-code.org> > container-bic-code > lcru

LCRU - Intermodal Container Details - bic-code.org

Company, CARU CONTAINERS BV. Code, LCRU. Address, SEATTLEWEG 34. Zip Code, 3195 ND. City, ROTTERDAM. State. Country, Netherlands. Telephone, +31 168 387 000.

Zip Code: 3195 ND

Company: CARU CONTAINERS BV

Then, we try to check the CARU CONTAINER website to see if we can search the container details via the container number. After done some research, we found the customer portal of CARU CONTAINER and we can check the container details under unit specification.

Unit specification

Container status	Technical details
Container : LCRU2994214 Type (ISO) : 22G1 (22G1) 20ft Standard Current status : Out of stock Last depot : Containerdepot Moerdijk, NLMOETSMA Locate : Track on Google Maps Booking number : SO 2112061 Date out : 22-03-2011	Manufacturing date : Dec 2010 Unit of measurements : <input checked="" type="radio"/> Metric <input type="radio"/> 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

Attachments

Documents	Images
American Bureau of Shipping PLCS Acceptance Certificate	

The CSC Number is USA/AB-642/98-61.

Flag: APUBOH22{USA/AB-642/98-61}