



3108CTF: BANGKIT DARI DASAR



3108CTF is a first Cybersecurity event held by “Bahtera Siber MY”. This CTF is a local based CTF event with storyline of the Theme of “Kemerdekaan” Malaysia. It is not only challenge for the Cybersecurity skills, but also the knowledge of our country, Malaysia. Thus, this event is only open for Malaysian and it is a single player.

▼ Tugasan 1

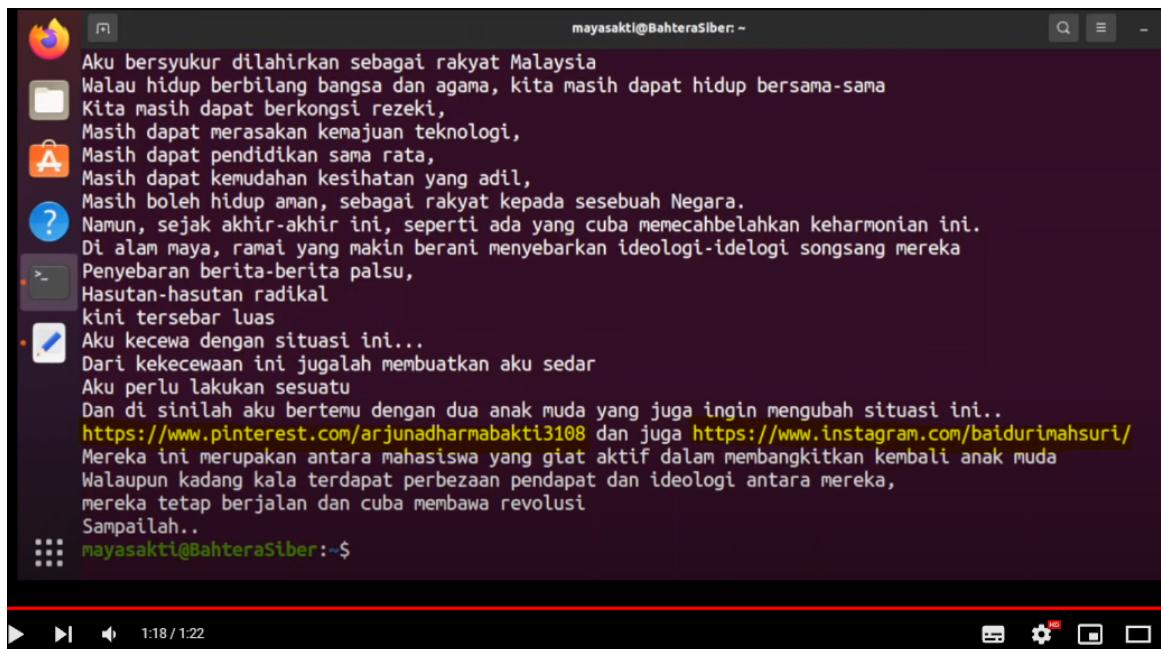


In this challenge, we are given a YouTube Link - <https://youtu.be/-Pso9e6cJNE> .

Navigate to the link given, play the video and it give us two information link.

1st link - <https://www.pinterest.com/arjunadharmaabakti3108/>

2nd link - <https://www.instagram.com/baidurimahsuri/>



Aku bersyukur dilahirkan sebagai rakyat Malaysia
Walau hidup berbilang bangsa dan agama, kita masih dapat hidup bersama-sama
Kita masih dapat berkongsi rezeki,
Masih dapat merasakan kemajuan teknologi,
Masih dapat pendidikan sama rata,
Masih dapat kemudahan kesihatan yang adil,
Masih boleh hidup aman, sebagai rakyat kepada sesebuah Negara.
Namun, sejak akhir-akhir ini, seperti ada yang cuba memecahbelahkan keharmonian ini.
Di alam maya, ramai yang makin berani menyebarkan ideologi-ideologi songsang mereka
Penyebaran berita-berita palsu,
Hasutan-hasutan radikal
kini tersebar luas
Aku kecewa dengan situasi ini...
Dari kekecewaan ini jugalah membuatkan aku sedar
Aku perlu lakukan sesuatu
Dan di sinilah aku bertemu dengan dua anak muda yang juga ingin mengubah situasi ini..
<https://www.pinterest.com/arjunadharmabakti3108> dan juga <https://www.instagram.com/baidurimahsuri/>
Mereka ini merupakan antara mahasiswa yang giat aktif dalam membangkitkan kembali anak muda
Walaupun kadang kala terdapat perbezaan pendapat dan ideologi antara mereka,
mereka tetap berjalan dan cuba membawa revolusi
Sampailah..

```
mayasakti@BahteraSiber:~$
```

At the first link, we are navigate to Arjuna Dharmabakti pinterest user profile.

I noticed that Arjuna posted a morse code image.

Decoded the morse code above and I got the message:

WAHAI PESERTA, ALANGKAH INDAHNYA JIKA KALIAN DAPAT MEMBANTU HAMBA. TOLONG OSINT HAMBA DAN CARI JAWAPAN DI PLATFORM MEDIA SOSIAL BURUNG BIRU.

The hint that show on the above morse code message is we need to find the information from a social media platform that consist blue color bird, which is

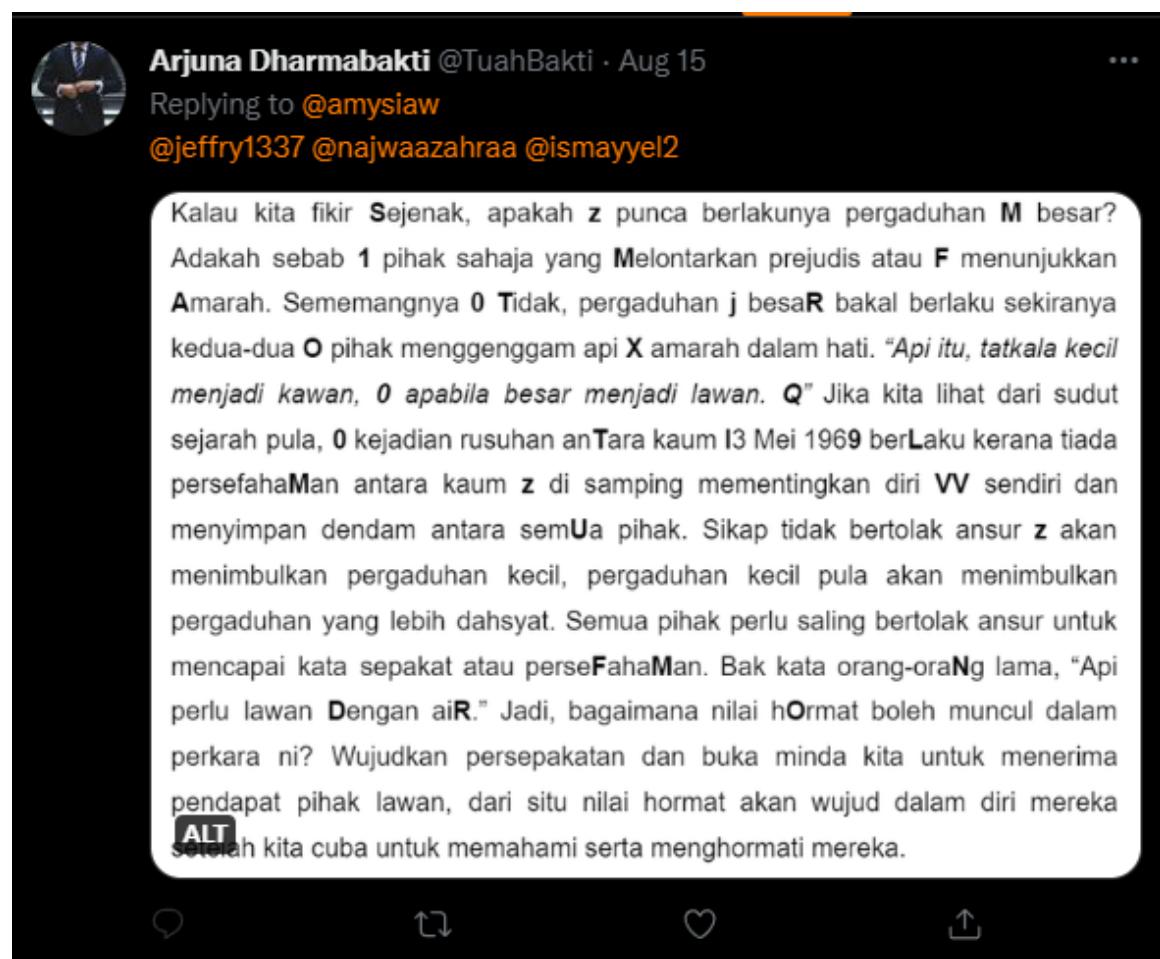
called “Twitter”.

Lets type the same username as pinterest we got above, we can search for Arjuna Twitter account.

Twitter Account - <https://twitter.com/TuahBakti>

Lets start reconnaissance on Arjuna’s Twitter profile.

I noticed that there is a weird tweet post from Arjuna. The image contains a lot of words with Bold Text.



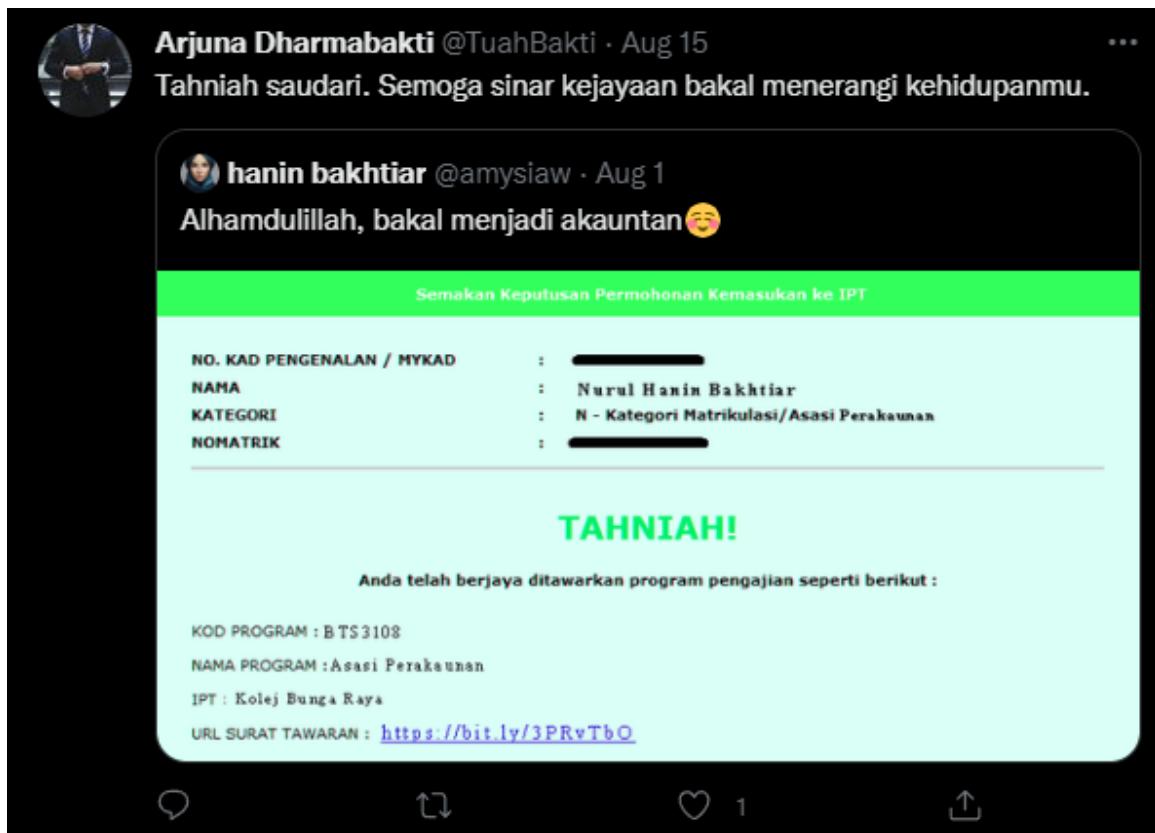
Arjuna Dharmabakti @TuahBakti · Aug 15

Replies to @amysiaW

@jeffry1337 @najwaazahraa @ismayyel2

Kalau kita fikir **Sejenak**, apakah **z** punca berlakunya pergaduhan **M** besar? Adakah sebab **1** pihak sahaja yang **Melontarkan** prejudis atau **F** menunjukkan **Amarah**. Sememangnya **0** **Tidak**, pergaduhan **j** **besaR** bakal berlaku sekiranya kedua-dua **O** pihak menggenggam api **X** amarah dalam hati. *“Api itu, tatkala kecil menjadi kawan, 0 apabila besar menjadi lawan. Q”* Jika kita lihat dari sudut sejarah pula, **0** kejadian rusuhan anTara kaum I3 Mei 1969 berLaku kerana tiada persefahaMan antara kaum **z** di samping mementingkan diri **VV** sendiri dan menyimpan dendam antara semUa pihak. Sikap tidak bertolak ansur **z** akan menimbulkan pergaduhan kecil, pergaduhan kecil pula akan menimbulkan pergaduhan yang lebih dahsyat. Semua pihak perlu saling bertolak ansur untuk mencapai kata sepakat atau perseFahaMan. Bak kata orang-oraNg lama, “Api perlu lawan **Dengan** aiR.” Jadi, bagaimana nilai **hOrmat** boleh muncul dalam perkara ni? Wujudkan persepakatan dan buka minda kita untuk menerima pendapat pihak lawan, dari situ nilai hormat akan wujud dalam diri mereka **ALT** setelah kita cuba untuk memahami serta menghormati mereka.

He also retweeted a tweet post from another user. I sus to the link inside the tweet post.



Arjuna Dharmabakti @TuahBakti · Aug 15

Tahniah saudari. Semoga sinar kejayaan bakal menerangi kehidupanmu.

hanin bakhtiar @amysiaw · Aug 1

Alhamdulillah, bakal menjadi akauntan 😊

Semakan Keputusan Permohonan Kemasukan ke IPT

NO. KAD PENGENALAN / MYKAD	:	[REDACTED]
NAMA	:	Nurul Hanin Bakhtiar
KATEGORI	:	N - Kategori Matrikulasi/Asasi Perakaunan
NOMATRIK	:	[REDACTED]

TAHNIAH!

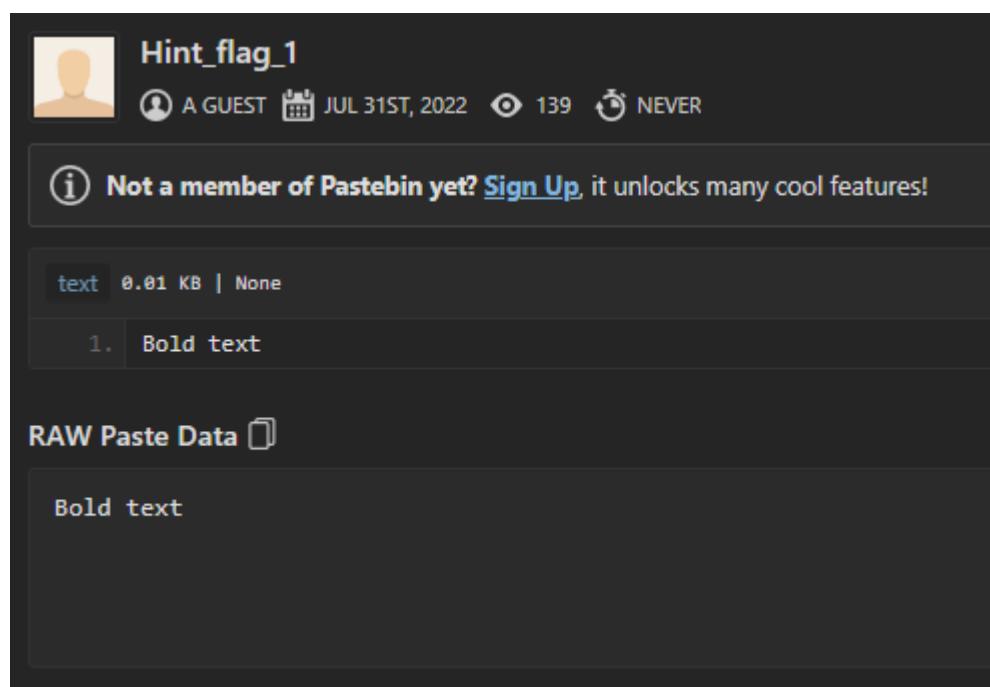
Anda telah berjaya ditawarkan program pengajian seperti berikut :

KOD PROGRAM : B TS3108
NAMA PROGRAM : Asasi Perakaunan
IPT : Kolej Bunga Raya
URL SURAT TAWARAN : <https://bit.ly/3PRvTbO>

1 reply 1 like

Lets navigate to the link that show inside the tweet post, I got the hint flag 1.

Link - <https://pastebin.com/bEfyt8fQ>



Hint_flag_1

A GUEST JUL 31ST, 2022 139 NEVER

1. Bold text

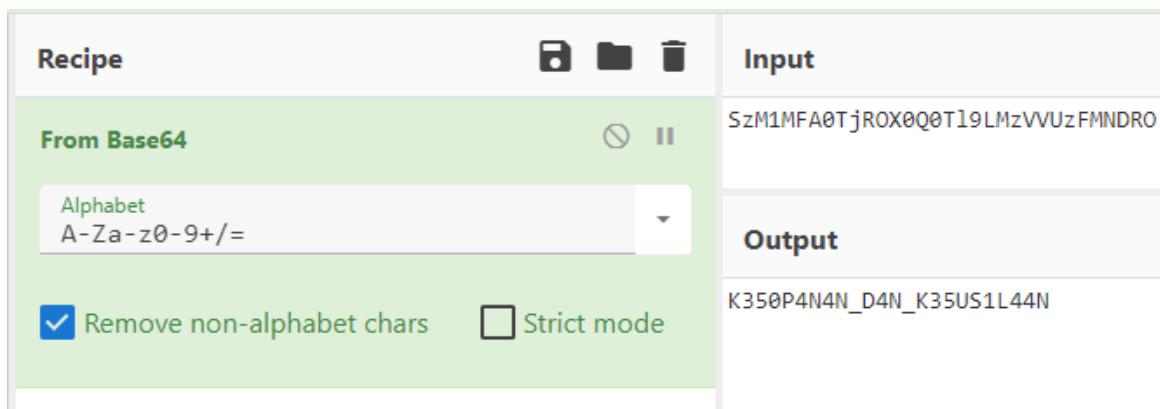
RAW Paste Data

Bold text

Then, lets combine all the Bold Text together and we got this.

Bold Text - SzM1MFA0TjROX0Q0T19LMzVVUzFMNDRO

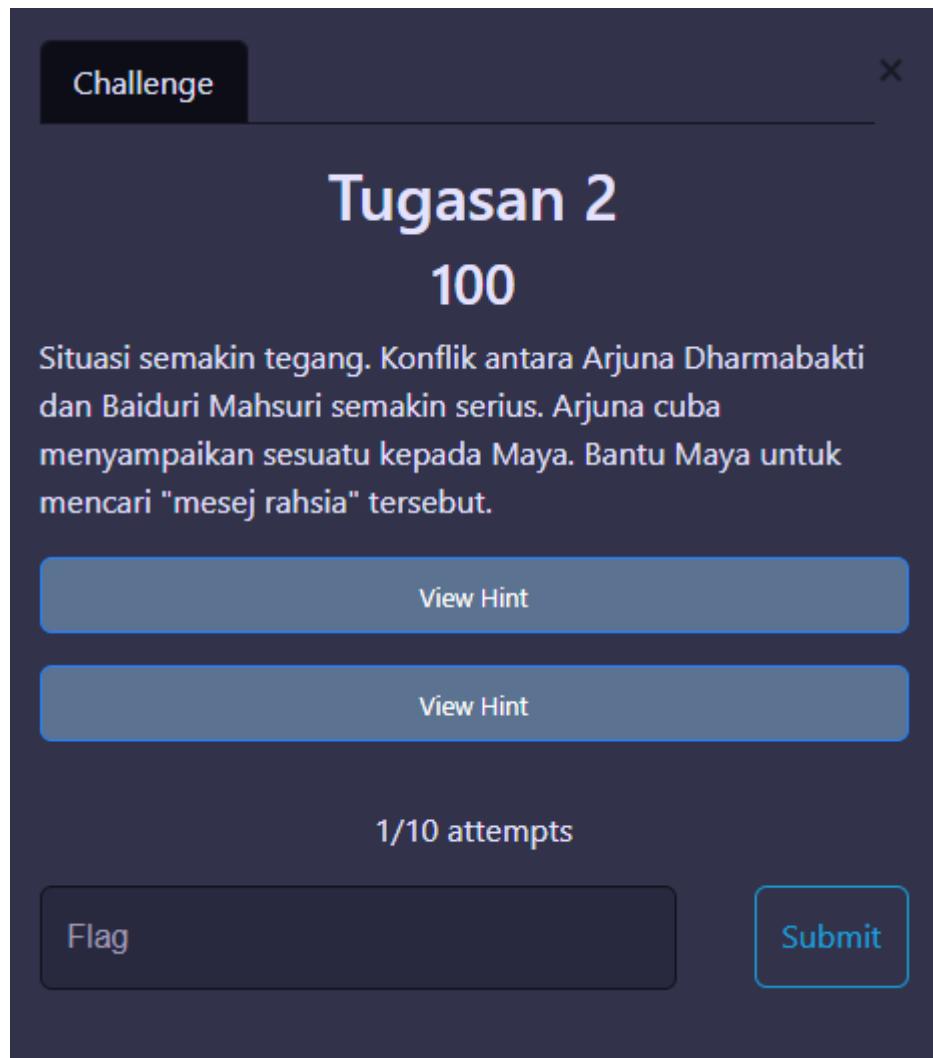
It seems like a Base64 encoded message. Let decode it using [CyberChef](#) and there the flag 1 !



The screenshot shows the CyberChef interface. The 'Recipe' section is set to 'From Base64'. The 'Input' field contains the Base64 encoded string: SzM1MFA0TjROX0Q0T19LMzVVUzFMNDRO. The 'Output' field shows the decoded result: K350P4N4N_D4N_K35US1L44N. The 'Alphabet' dropdown is set to 'A-Za-z0-9+/=' and the 'Remove non-alphabet chars' checkbox is checked.

Flag 1: 3108{K350P4N4N_D4N_K35US1L44N}

▼ Tugasan 2



In second challenge, we are asked to find out the “mesej rahsia”, which is a secret message from Arjuna. Since it is a storyline CTF event, lets continue find the information from the Arjuna Twitter profile.

We are given 2 hints:

1st (free) - OSINT > SECRET MESSAGE > DECODE > CHANNEL > FLAG
Got it!

2nd (-50points) - Mungkin dapat membantu 🤔🤔 Pembayang

Reference - <https://darthnull.org/poem-codes/>

Go to the like tab, I noticed Arjuna liked a weird Tweet with a number of secret code.

There is a poem and a secret code posted by madah4rjuna. I assume it is another account for Arjuna.

← Thread



😎 @madah4rjuna · Aug 19

Dedaunan yang menghijau dan rendang
menyuburkan maruah dan semangat waja
memartabatkan bahasa dan keluhuran perlumbagaan
membendung tekad dan keazaman
membasmi hujan petualangan
menaungi mentari keganasan
yang merobek nurani bangsa.

1 1



😎 @madah4rjuna

GBQDU AGAMM TSBGU ANGLN UEJLT ULGXI ANLSN
EAUIH DNEIM EAAEU TEATI EANHA ASNCA ALDAS
UTMIA RXYIR YDBCA ANIGA SLYNH YR---

[Translate Tweet](#)

4:02 AM · Aug 24, 2022 · Twitter Web App

According to the hints given, the secret code can be decoded with Poem Code.

To decode the secret code, we need to generate the key based on the poem code and the indicator group from the secret code. The first 5 letters of the secret code was the “GBQDU”.

It means that the key words is “maruah yang tekad dan hujan”.

Thus, we can generate the key and decode the secret code.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
1	M	A	R	U	A	H	Y	A	N	G	T	E	K	A	D	D	A	N	H	U	J	A	
2	15	1	19	21	2	11	23	3	16	20	9	14	4	7	8	S	17	12	22	13	6	18	
3																							
4	S	A	Y	A	M	E	N	G	A	N	D	U	N	G	I	S	E	S	U	A	T	U	
5	N	G	I	N	T	A	H	U	L	E	B	I	H	L	A	N	J	U	T	S	I	L	
6	C	A	R	I	S	A	Y	A	D	I	C	H	A	N	N	E	L	T	E	L	G	R	
7	A	M	Y	G	B	E	R	N	A	M	A	D	A	U	L	A	T	M	A	Y	A	X	
8																							
9	SAYA	MENGANDUNG	SESUATU	INGIN	TAHU	LEBIH	LANJUT	SILA	CARI	SAYA	DI	CHANNEL	TELEGRAM	YG	BERNAMA	DAULATMAYA	XX						

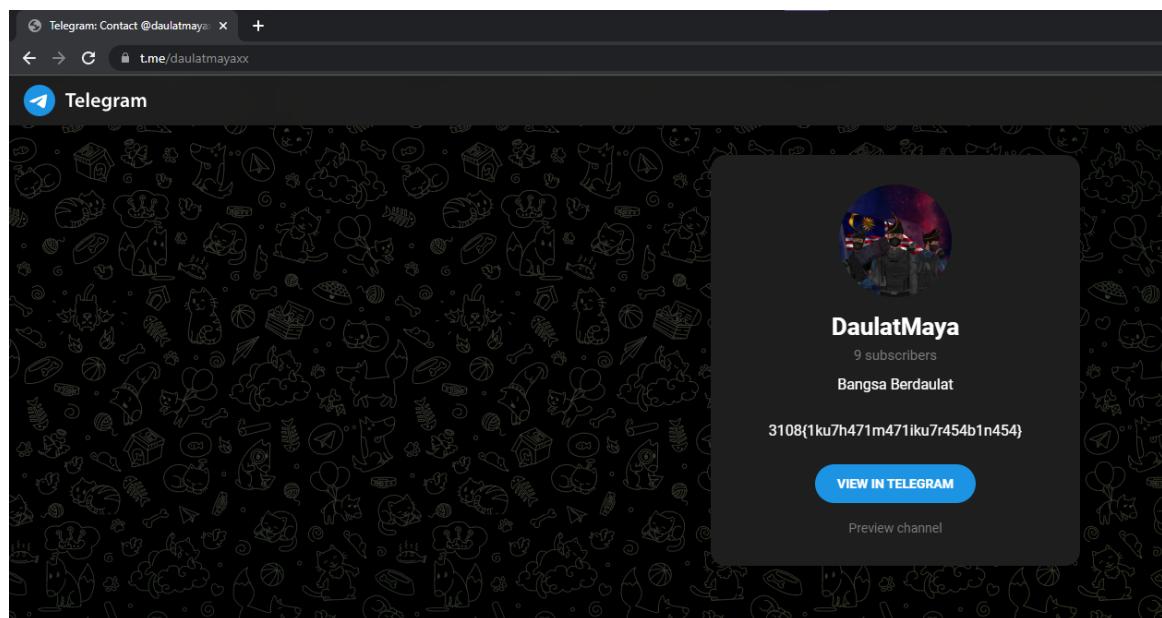
The message I got after decoded is -

**SAYA MENGANDUNGI SESUATU INGIN TAHU LEBIH
LANJUT SILA CARI SAYA DI CHANNEL TELEGRAM YG
BERNAMA DAULATMAYAXX**

It means that we can get something from telegram with the username "DAULATMAYAXX".

Telegram Link - <https://t.me/daulatmayaxx>

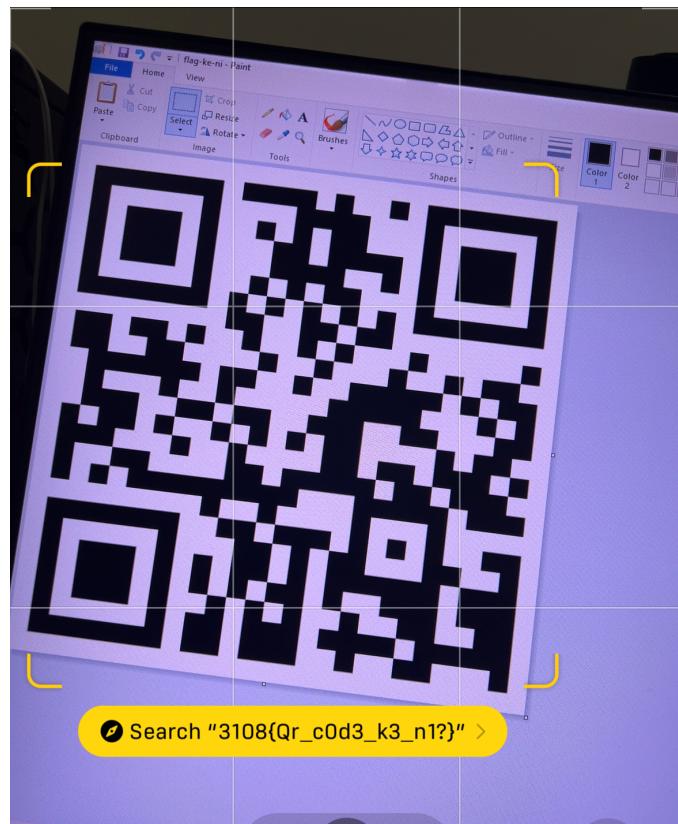
Clink on the link and we got the flag 2 !



Flag 2 : 3108{1ku7h471m471iku7r454b1n454}

▼ Bonus 2

We are given an incomplete QR code. I manually fixed it with replace 2 square on top right and left corner. Then we can get the flag after scan the fixed QR code below.



Flag Bonus 2: 3108{Qr_c0d3_k3_n1?}

▼ Bonus 3

We are given a zip file called “bangkit.zip”.

I've tried to unzip the file but it only provided me a html source of Apache documents.

Check for file type with the command `file bangkit.zip` and it showed me its not a zip file, but a pcapng capture file.

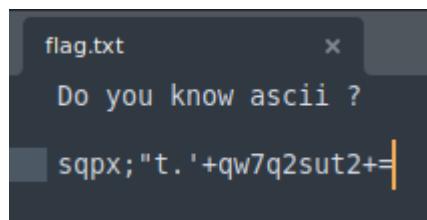
```
L$ file bangkit.zip
bangkit.zip: pcapng capture file - version 1.0
```

Thus, I renamed it into bangkit.pcap and open it with wireshark software.

Let observe for the pcap file. I found a message showed `GET method` is called for the `flag.txt` file.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	127.0.0.1	127.0.0.1	TCP	76	33538 - 88 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TStamp=1286938686 TSectr=0 WS=128
2	0.0000009538	127.0.0.1	127.0.0.1	TCP	76	80 - 33538 [SYN, ACK] Seq=0 Ack=1 Win=65493 Len=0 MSS=65495 SACK_PERM=1 TStamp=1286938686 TSectr=1286938686 WS=128
3	0.0000016231	127.0.0.1	127.0.0.1	TCP	68	33538 - 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TStamp=1286938686 TSectr=1286938686
4	0.0000059872	127.0.0.1	127.0.0.1	HTTP	508	GET / HTTP/1.1
5	0.0000079808	127.0.0.1	127.0.0.1	TCP	68	80 - 33538 [ACK] Seq=1 Ack=441 Win=65152 Len=0 TStamp=1286938687 TSectr=1286938687
6	0.0000079572	127.0.0.1	127.0.0.1	HTTP	3416	HTTP/1.1 200 OK (text/html)
7	0.0000079572	127.0.0.1	127.0.0.1	TCP	68	33538 - 88 [ACK] Seq=441 Ack=3881 Win=63232 Len=0 TStamp=1286938687 TSectr=1286938687
8	0.0000079323	127.0.0.1	127.0.0.1	HTTP	464	GET /Icons/openlogo-75.png HTTP/1.1
9	0.0000095113	127.0.0.1	127.0.0.1	TCP	68	33538 - 88 [ACK] Seq=3381 Ack=837 Win=65152 Len=0 TStamp=1286938755 TSectr=1286938755
10	0.0000099768	127.0.0.1	127.0.0.1	HTTP	317	HTTP/1.1 304 Not Modified
11	0.00000936187	127.0.0.1	127.0.0.1	TCP	68	33538 - 88 [ACK] Seq=837 Ack=3630 Win=65408 Len=0 TStamp=1286938755 TSectr=1286938755
12	3.790307322	127.0.0.1	127.0.0.1	HTTP	483	GET /flag.txt HTTP/1.1
13	3.790325977	127.0.0.1	127.0.0.1	TCP	68	80 - 33538 [ACK] Seq=3630 Ack=1252 Win=65152 Len=0 TStamp=1286942477 TSectr=1286942477
14	3.790488628	127.0.0.1	127.0.0.1	HTTP	315	HTTP/1.1 304 Not Modified
15	3.790502153	127.0.0.1	127.0.0.1	TCP	68	33538 - 88 [ACK] Seq=1252 Ack=3877 Win=65408 Len=0 TStamp=1286942477 TSectr=1286942477

Then, I tried to export the content from Wireshark, and it actually provided me a flag.txt file.



XOR the message at CyberChef and I got the Flag !

Input: sqpx;"t. '+qw7q2sut2+=

Output: 3108{b4ngk17w1r354rk}

Flag Bonus 3: 3108{b4ngk17w1r354rk}

▼ Bonus 5

In this bonus challenge, we are given an audio file.

I assumed it is a Dual Tone Multi-Frequency (DTMF) generated audio file.

We can decode the audio file from this link - <https://unframework.github.io/dtmf-detect/>

Then get the message from the audio.

Message - 2288664277729992

I think that it is a message for us to type in 10key numpad.

Type two time in 2 is B

Type two time in 8 is U

...

until I finish the number from the Message and that's the flag !

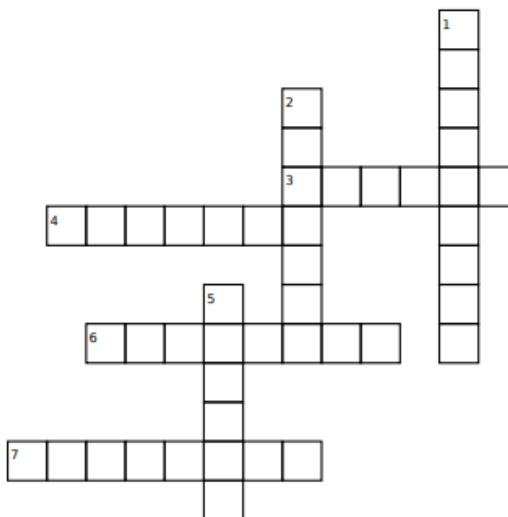
bungaraya

Flag Bonus 5: 3108{bungaraya}

▼ Bonus 6

Bonus 6 challenge is provided us a pdf file. We need to complete all the answer to get the first letter for each of the answer and that's the flag.

Kemerdekaan yang ke-65



Down:

1. Warna Biru pada Jalur Gemilang melambangkan? _____
2. Di manakah tempat pengisytiharan kemerdekaan? Stadium _____
5. Siapakah yang mencipta Bendera Malaysia? Mohamed _____

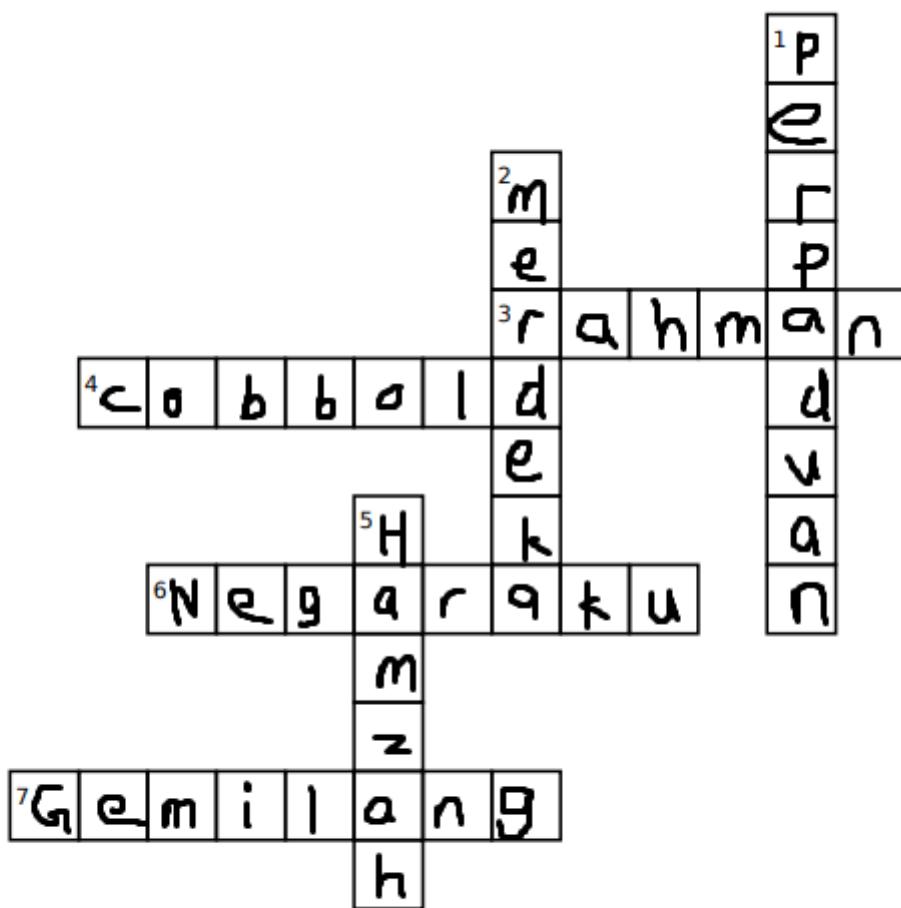
Across:

3. Siapakah bapa kemerdekaan negara? Tunku Abdul _____
4. Apakah suruhanjaya yang meninjau pandangan penduduk negeri-negeri di Borneo Utara dan Sarawak tentang gagasan Malaysia? Suruhanjaya _____
6. Apakah nama lagu kebangsaan Malaysia? Lagu _____
7. Apakah nama lain bagi bendera Malaysia? Jalur _____

Flag untuk soalan ini ialah huruf depan bagi setiap jawapan dalam huruf besar.

Contoh: 3108{ABCDEFG}

Completed Answer:



Flag Bonus 6: 3108{PMRCHNG}

Conclusion

Its a fun and different type of experience while playing this CTF event with the Theme of “Kemerdekaan” Malaysia. Even though I didn’t completed all the challenge, but most importantly I’ve learn something new especially for the Poem Code. LOL

