

Welcome (5) Easy

Challenge

Player Solve

Contoh flag yang kami gunakan, dan flag adalah CTF{1ni_C0n7oh_Fla9}

Hint :-

Submit

- Disini saya langsung mendapatkan flagnya : **CTF{1ni_C0n7oh_Fla9}**

Detektif Bingung (10) Easy

- Diberikan link untuk menjelaskan apa itu CTF di <https://www.dropbox.com/s/hz3l7xe9rpgc67h/Detektif%20Bingung.txt?dl=0>

Detektif Bingung.txt

capture the flag atau sering di sebut ctf adalah sebuah hacking competition dimana para pesertanya bebas melakukan eksplorasi maupun eksploitasi terhadap su meningkatkan skill dalam bidang hacking.

capture artinya adalah mendapatkan sedangkan flag adalah bendera. secara keseluruhan arti dari ctf adalah mendapatkan sebuah "kata kunci" dalam ajang kompetisi dalam sebuah web scoring. jika "kata kunci" yang disubmit sudah benar, maka peserta akan berlanjut ke level selanjutnya.

ctf hacking competition biasanya di selenggarakan dalam 2 mode, yaitu online dan offline. kompetisi secara online peserta harus terhubung dengan jaringan yang sedang mengeksploitasi sebuah target. sedangkan offline, panitia akan menyediakan sebuah jaringan kecil dan peserta dikumpulkan dalam sebuah ruangan.

apakah anda siap bermain? mari temukan flagnya!

- Saya langsung tertuju pada huruf besar yang jika diurutkan maka menjadi "INIBUKANFLAG"
Ternyata setelah menghabiskan waktu setengah jam saya tertawa karna berhasil mendapatkan flag nya : **CTF{bendera}**

Verification File Whistling (20pts)

- Pada soal ini, di berikan berkas yang bernama VerificationFileWhistling.mp3
- cek md5 hash dan sha1 hash file tersebut

```
File Edit View Search Terminal Help
root@Hexa:~/Desktop/CTF/P5# md5sum VerificationFileWhistling.mp3
79af38dc3f8b9f584e599ab5ab93c0c9 VerificationFileWhistling.mp3
root@Hexa:~/Desktop/CTF/P5# shasum VerificationFileWhistling.mp3
2f54f23b92eb31505151ddede275f2401ebcc1fa VerificationFileWhistling.mp3
root@Hexa:~/Desktop/CTF/P5#
```

- Flag :
CTF{79af38dc3f8b9f584e599ab5ab93c0c9_2f54f23b92eb31505151ddede275f2401ebcc1fa}

Grep the World (25) Easy

- Diberikan sebuah file <https://www.dropbox.com/s/6kfeyfkyxd5m07s/Greps.zip?dl=0>
- ekstrak file tersebut, didapatkan banyak file dalam direktori tersebut
- Sesuai dengan clue yang diberikan yaitu grep, kami mencari menggunakan command “grep -ri “flag” untuk mencari string flag pada direktori tersebut

```
root@hendro: ~/Downloads/Greps
File Edit View Search Terminal Help
'fJ0rUeGw6vKafoJe4WgfZpA==' 'fZC6S77eUIXNIgbUAHhsYtg=='
'fj1MpWn0HhJTpvI3Ww8cQTW==' 'fzcDW5jqo5ByJaJ9UlwuzXw=='
'fj32AfH9T7BX5775cuBCQAw==' 'fZCI8z3C7tlo6Ss6sNAIQFg=='
'fj4VReWd5Xu72bCJfEI09yw==' 'fZd7VNTxe5I0LfUjFkbj0MA=='
'fjAAJ07MNB4wxR0vQdk5qwA==' 'fZgIpSAkQsePEVxvZjE1UHA=='
'fjAyyCBezHqZuz3jmmCaBg==' 'fZHu6NE0W58gXCQK88uFVUQ=='
'fJbKCLC9aMjCrAt1HbosEyQ==' 'fZjaCcPBVFBjsWL15Py2bGw=='
'fjBn1ceJR5hy43TYS8m1ezw==' 'fzLCYlmIhH2Htri4m1Y6pLw=='
'fJCH8sSY7lTDfiPfwAueOpQ==' 'fzLHUX7dvfFoL9hn5ecbPNg=='
'fjCNfiagU0i1hlgZAlZ3YWA==' 'fzMCqG4GBgeFsZ23bl3xYgQ=='
'fJd3AAMnT4i4D0wdvmNg8sg==' 'fznjR2iVMCEPrI5Ua4HfBXw=='
'fjdSNai4srSExa0ZLAvlPA==' 'fZoCOMn3HnRNboY4FFnPZBg=='
'fjfcHqUj6wbSgAXqlVIhuyA==' 'fzQBpLDvAWSZ9XsAsUxAobA=='
'fjGdEydQuwsueiIW1TBdEOA==' 'fZRK9Q9nKpuAsmQsKgmUtyg=='
'fJGgZKEJfWpEzUE3laPX23w==' 'fzt67bocvU5vvjDARmHTp1w=='
'fjHu7upXBAl15Uj06G363A==' 'fzuYxEhwuySMv0i8CitXImw=='
'fJI6EQzZ5fsmEePhedibeSg==' 'fZvBB4WpgkosFpAIoqJw3mQ=='
'fjilqBno3VjNw3tBfwjvz7A==' 'fZw6KQ7JGgByh6sqXsAGRiQ=='
'fJIlusMZSY1bMEnhSQT6jtA==' 'fzwBP3Hb6Gk8l9i40tSYcow=='
'fJjNzU7eWLIM9eMdiNzszGA==' 'fZWWP3lirPCTuUTKjn658uQ=='
'fJkCPAnA6cuisARfnStRvMw=='
root@hendro:~/Downloads/Greps# grep -ri "flag"
FmKKnwmnLLHkX4gIQAAIyM=:Flag : CTF{In1_adalAh_Fun6sI_Gr3p}
root@hendro:~/Downloads/Greps#
```

- Dan flagnya pun didapat : **CTF{In1_adalAh_Fun6Si_Gr3p}**

Boomz (30) Easy

- Diberikan link menuju <https://drive.google.com/file/d/1RwWxDiDZOYVaTK6mmv4SqptVeH-INKv7/view>
- extract file dan lihat isi pada file tersebut

```
root@hendro:~/Downloads# cat Boomz
flag is : Booooo0mzzzz_To00o_D4mn__Bi9_Hah!
```

- dan flag didapat: **CTF{Booooo0mzzzz_To00o_D4mn__Bi9_Hah!}**

Rusaksak (45) Easy

- Awalnya saya mencoba dengan strings, exiftool, binwalk dll, ternyata tidak membuahkan hasil apapun.
- Saya coba copy hex dari gambar tersebut dan paste pada hexeditor dan jalankan
- Didapat flag : **CTF{scr3333333333333333333333nsh0000000000ts}**

Tenesys Lab (150) Hacker

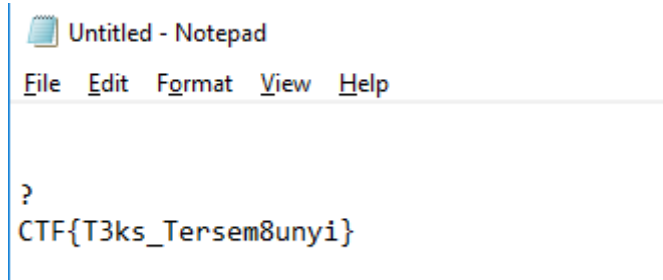
- Disini saya belum paham setting DHCPnya dan fungsi nmap, jadi saya bypass saja password root linuxnya, maaf ya kak jadi mohon bimbingannya :v

Flag : **CTF{amazing_story_of_life}**

#Forensic

View & Copy (15) Easy

- Diberikan file pdf dengan nama View & Copy.pdf
- Ctrl+a dan paste pada text editor



- Flag : **CTF{T3ks_Tersem8unyi}**

View The String (20pts)

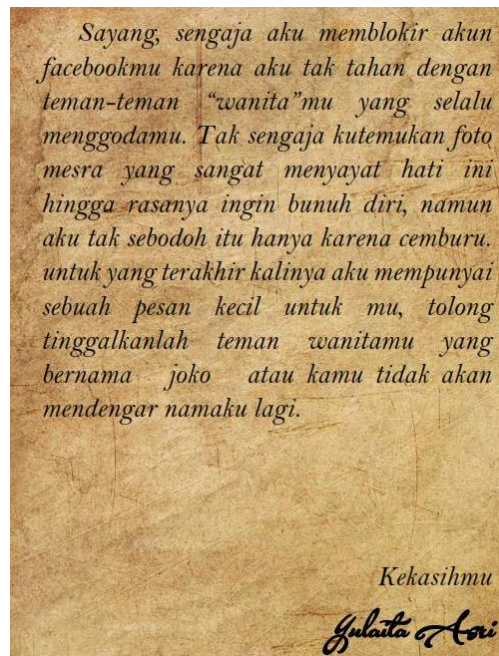
- Diberikan berkas dengan nama ViewTheString.jpg, lihat pada propertiesnya atau bisa juga di linux dengan exiftool

Property	Value
Description	
Title	
Subject	
Rating	☆☆☆☆☆
Tags	
Comments	
Origin	
Authors	CTF{C3k_Met4data}
Date taken	
Program name	
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	500 x 373
Width	500 pixels
Height	373 pixels

- Flag : **CTF{C3k_Met4data}**

Smile, View and Copy (20) Easy

- Diberikan file pdf dengan nama Smile, View & Copy
- Cukup copy image tersebut dan pastekan pada paint



- Nama kekasihnya pun terlihat bernama joko?
- Flag : **CTF{joko}**

You can see me ? (20) Easy

- dengan menggunakan perintah “strings Flag.jpg”

```
root@hendro: ~/Downloads
File Edit View Search Terminal Help
jLbFA
&[e4
AyFVM
Flag terpecah
BI`,
%BdU
b8#<
oH\`
fL-0
Format Flag CTF{}
-BUWD"
CA6{d<
XP5 7
38`fB4
%yu[
[B,A
l(W*
T>CTF{Str1ng_15_
*8(&
TXBi
,HD)P.k
!=I1
Du@`
root@hendro:~/Downloads#
```

- Didapatkan setengah flag yaitu : CTF{Str1ng_15_
- Dengan clue flag yg terpecah, saya dapatkan flag setengahnya pada metadata gambar dengan “exiftool Flag.jpg”


```

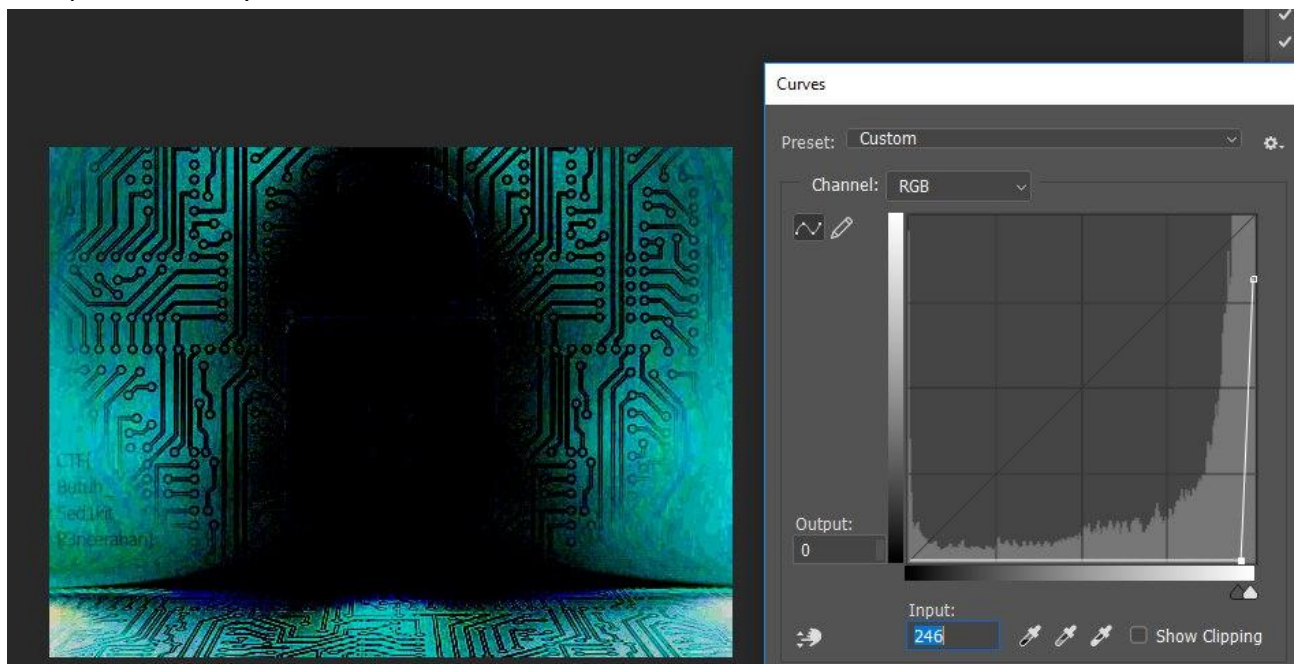
File Type           : JPEG
File Type Extension : jpg
MIME Type           : image/jpeg
JFIF Version        : 1.01
Resolution Unit     : inches
X Resolution        : 72
Y Resolution        : 72
Exif Byte Order     : Big-endian (Motorola, MM)
XP Comment          : V3ry_E45y_R1ght}
Padding             : (Binary data 2060 bytes, use -b
act)
Image Width         : 1024
Image Height        : 768
Encoding Process    : Progressive DCT, Huffman coding
Bits Per Sample     : 8
Color Components    : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size          : 1024x768
Megapixels          : 0.786
@hendro:~/Downloads#

```

- Dan jika digabungkan didapatkan lah sebuah flag : **CTF{Str1ng_15_V3ry_E45y_R1ght}**

Exposure (30) Easy

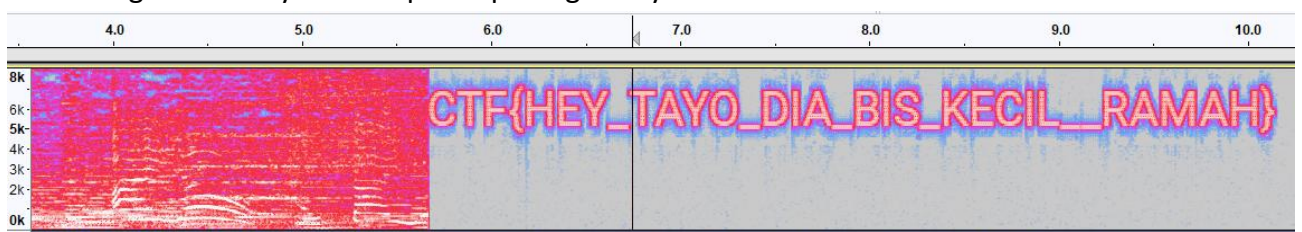
- Diberikan berkas, dengan nama Exposure.jpg
- Saya coba dengan stegsolve tapi kurang jelas flagnya, lalu dengan photoshop saya coba atur pada curvesnya



- Flag : **CTF{Butuh_5ed1kit_P3ncerahan}**

Spectro (30) Easy

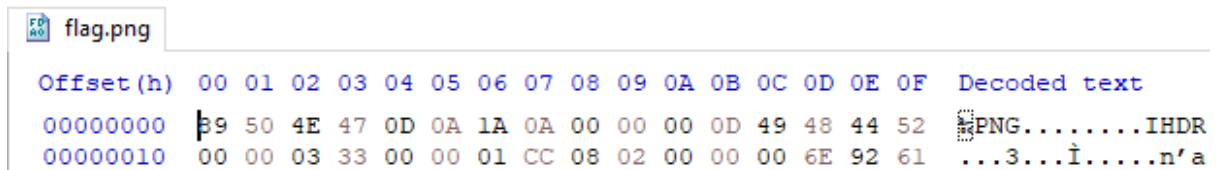
- Diberikan berkas, dengan nama hey.mp3
- Buka dengan audacity kita cek pada spektogramnya



- Flag : **CTF{HEY_TAYO_DIA_BIS_KECIL__RAMAH}**

Exten (30)

- Saya coba cek file dengan HxD



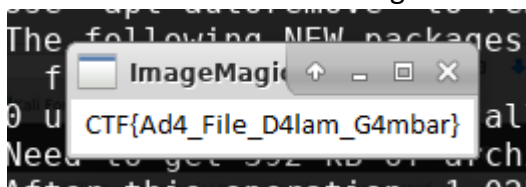
- Format file ternyata berupa PNG, Lalu saya ubah ekstensi menjadi .png
- Flag pun didapat : **CTF{In1_h4ny4_3xt3nsi}**

Insert The Flag (35) Easy

- Diberikan file zip dengan nama InsertTheFlag.zip
- Dengan binwalk diketahui didalamnya terdapat file image lagi

```
root@flint:~/Downloads# unzip Insert\ The\ Flag.zip
Archive:  Insert The Flag.zip
  inflating: Insert The Flag.jpg
root@flint:~/Downloads# binwalk -e Insert\ The\ Flag.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          JPEG image data, JFIF standard 1.01
30            0x1E         TIFF image data, big-endian, offset of first
directory: 8
73564         0x11F5C      Zip archive data, at least v1.0 to extract,
compressed size: 905, uncompressed size: 905, name: flag
74553         0x12339      End of Zip archive
```

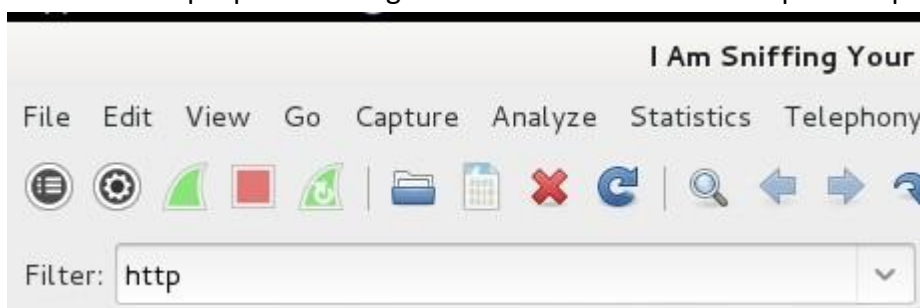
- Coba ekstrak dan buka file flag tersebut



- Flag : **CTF{Ad4_File_D4lam_G4mbar}**

I Am Sniffing Your Activity (40) Easy

- Diberikan file pcap. Buka dengan wireshark kemudian filter pada http



- Cek pada bagian POST login, dan follow TCP stream didapatkan password

```
Wireshark · Follow TCP Stream (tcp.stream eq 55) · I Am Sniffing Your Activity.pcap

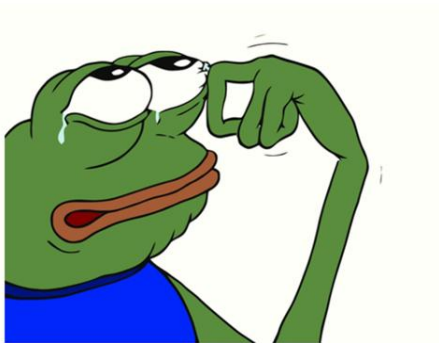
POST /cek-login.php HTTP/1.1
Host: ctf.tenesys.id
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0
Iceweasel/31.5.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://ctf.tenesys.id/login.php
Content-Length: 48
Cookie: PHPSESSID=20d67bb6f85374adb988be1247d2f212
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

username=JogetSanaSini&xXx=Jan9an_Di5al4h9unak4nHTTP/1.1 200 OK
Date: Wed, 27 Jul 2016 09:18:52 GMT
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4
X-Powered-By: PHP/5.4.45
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
```

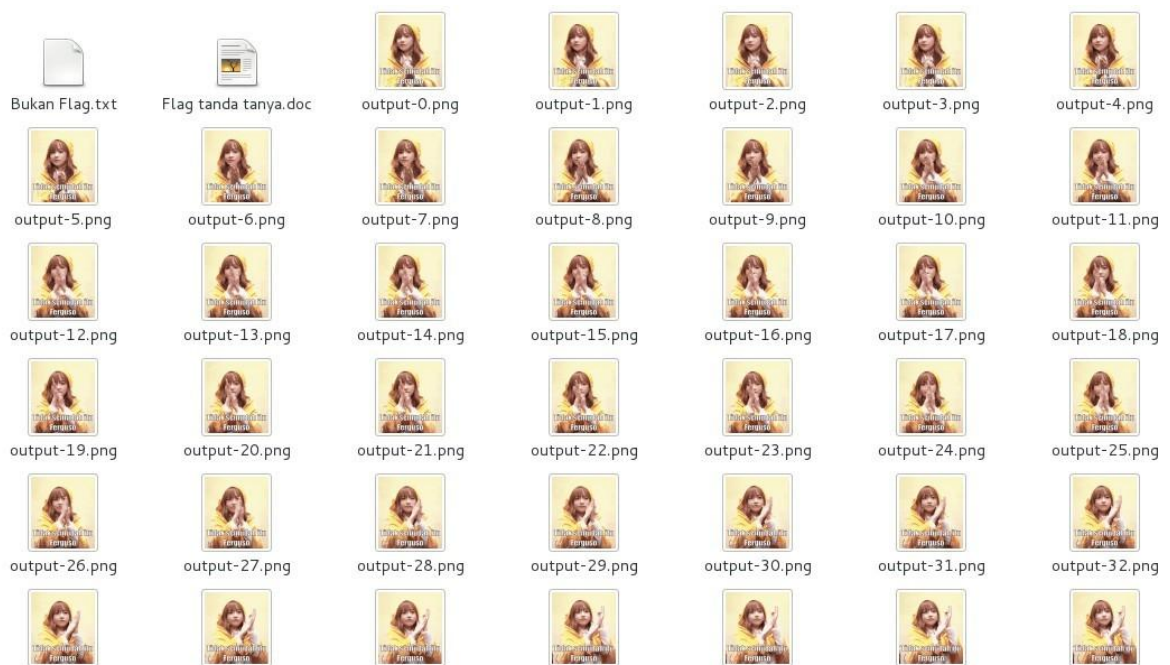
- Flag : **CTF{Jan9an_Di5al4h9unak4n}**

Gift from Yuri (40pts)

- Diberikan sebuah file gif
Dibilangin Disini gak ada Flag cari tahu yang lain ya siapa tau nemu kan wkwk



- Sial awalnya saya ketipu disini :’v
- Saya coba ubah file tersebut dengan ‘convert HmMMM.gif HmMMM.png’



- Cek hasil gambar png tersebut terdapat potongan flag dan susun
- Flag : **CTF{P354n_d1_d4l4m_g1f}**

Check My Image (60)

- Download file
https://drive.google.com/file/d/16lwjWOBpaUE3J3hC39p1AXcDR_OVSbC7/view
- kita lihat ada 3 gambar didalamnya, yg ternyata file signature nya tidak sesuai.

1.jpg

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	58	58	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	SoXyà..JFIF....
00000010	00	00	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02	...yû.C.....
00000020	02	02	02	02	02	02	03	05	03	03	03	03	03	06	04	
00000030	04	03	05	07	06	07	07	07	08	09	0B	09	08			

- Saya edit file signaturenya dengan list disini
https://en.wikipedia.org/wiki/List_of_file_signatures
- Dan gabungkan string pada gambar menjadi sebuah flag
:CTF{7ahu_T3nt4ng_F1le_Si9nature_!}

Ferguso Jahad (60)

- cek file gambar merupakan asli jpg, coba liat dengan hex editor dan terdapat file rar dan txt disana

00019070	CA	D4	1F	FF	D9	52	61	72	21	1A	07	01	00	33	92	B5	ËÖ.yÛRar!....3'µ
00019080	E5	0A	01	05	06	00	05	01	01	80	80	00	A9	F6	6E	B6	å.....ëë.öñq
00019090	5D	02	03	3C	B0	00	04	98	00	20	AB	E0	92	5E	80	03]..<°...~. «à'^ë.
000190A0	00	10	66	6C	61	67	2F	62	65	6E	64	65	72	61	2E	74	..flag/bendera.t
000190B0	78	74	30	01	00	03	0F	59	E0	D1	FC	A6	EA	3E	22	02	xt0....YàÑü!è>".

- Coba dengan binwalk dan unrar anehnya ga bisa
- saya coba open di windows with winrar dan ternyata bisa, dan ternyata txtnya dipassword , teringat deskripsi soal saya inputkan 'ferguso' dan didapat flag :
CTF{S3mud4h_1n1_f3rgus0}

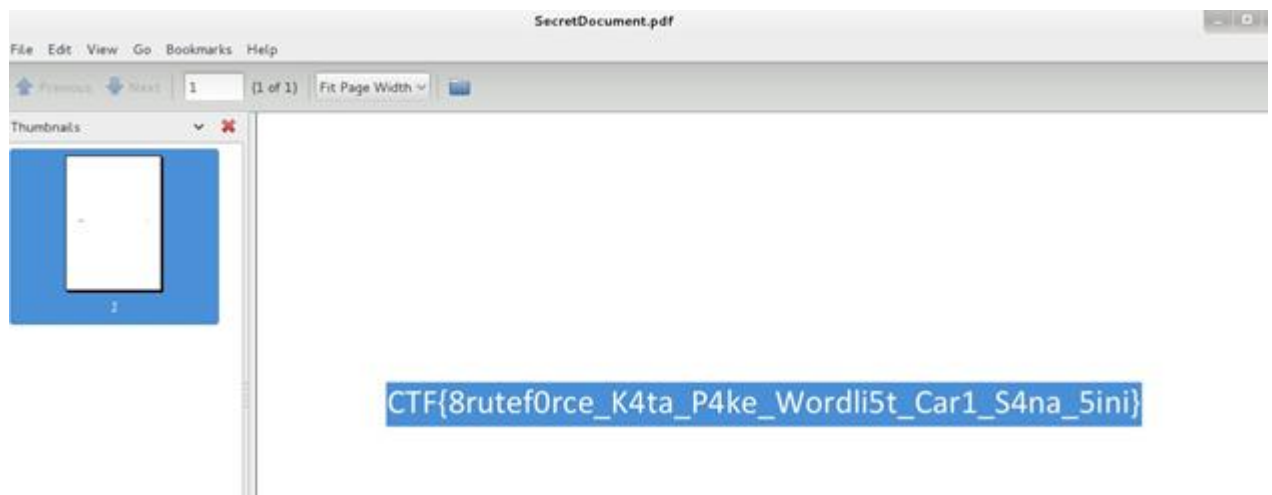
- Diberikan sebuah file image
- Coba coba dengan strings didalamnya ada file rar dan txt. Extract gambar tersebut dan didapat sebuah password.txt

- coba dengan steghide 'steghide extract -sf nani.jpg'
- kemudian masukan password yang sudah di dapat tadi, dan muncul Bendera.txt

- Flag : **CTF{S1mp4n_s3bu4h_p3s4n_w1th_St3gh1d3}**

- Diberikan file pdf dengan nama SecretDocument.pdf yang terpassword.
- saya coba bruteforce pakai pdfcrackdengan wordlist rockyou

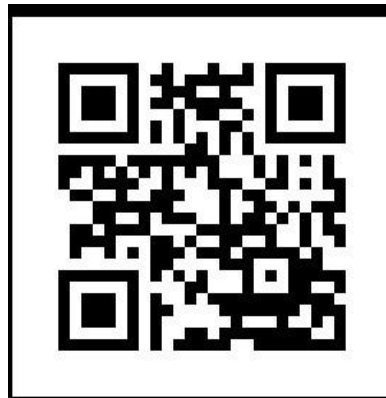
- Didapatlah password pdf tersebut 'survivor' dan inputkan



- Flag : `CTF{8rutef0rce_K4ta_P4ke_Wordli5t_Car1_S4na_5ini}`

The Message From Planet QR (70pts)

- Diberikan sebuah qrcode yang tengahnya ilang ntah kemana.
- liat source code nya, dan cek terdapat perbedaan pada #q
- find #q dan rubah menjadi #p kemudian replace all.



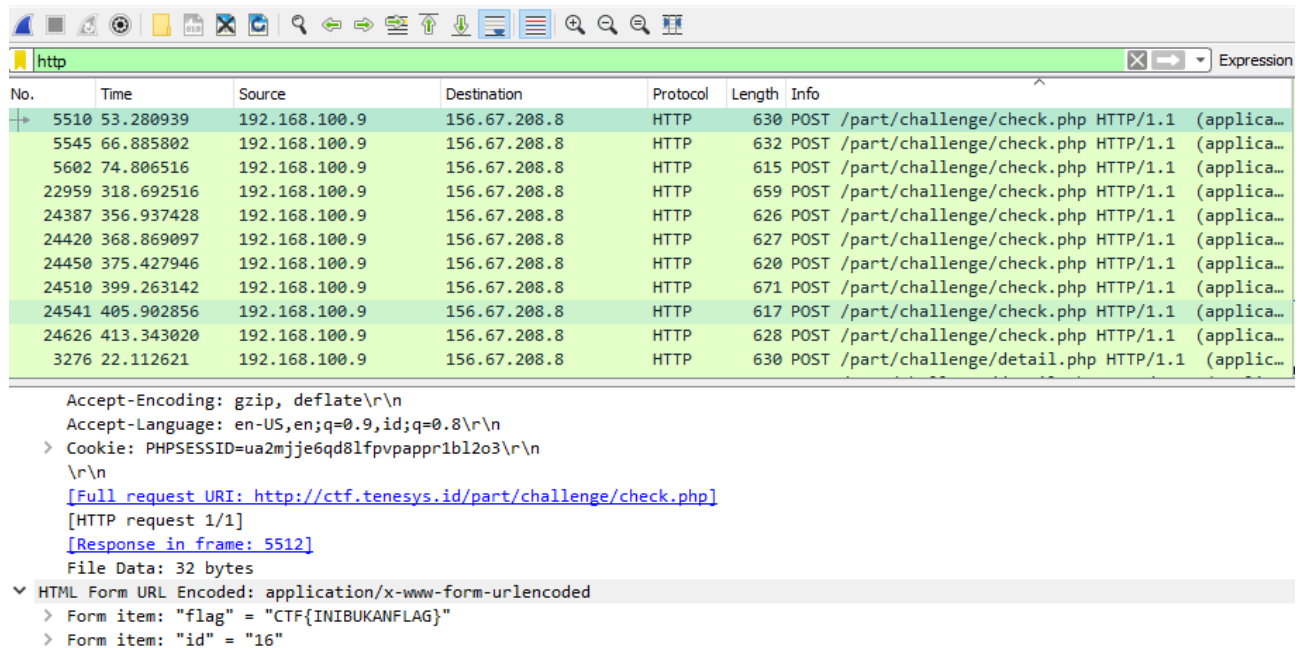
- Decode qrcode tersebut dan menghasilkan sebuah link <http://pastebin.com/WpgkZFuk>
- Buka linknya, didapat sebuah base64, decode lalu hasilnya merupakan sebuah hex dan cobadecode kembali.

```
File Edit View Terminal Tabs Help
root@flint:~/Downloads# echo NTQ2ZjZjNmY2ZTY3MjA2OTczNjk2YjYxNmUyMDZkNjE2ZDYxMjA
3MDc1NmM3MzYxMjAzNTMwMmUzMMDwMzAyMDczNjU2YjYxNzI2MTZlNjcyZTIwNGQ2MTZkNjEyMDZjNjE
2NzY5MjA2NDY5MjA2YjYxNmU3NDZmNzIyMDcwNmY2YzY5NzM2OTIwNmQ2MTczNjE2YjYxNzI2NTZlNjQ
2MTZlNjcyZjYxNmU2MTZlNzQ2OTIwNmQ2MTZkNjEyMDc0NjU2YzY5NzY2ZTIwNjI2MTZjNjk2YjYxNmI
2MTZjNmYyMDcyNjU2ZTY0NjE2ZTY3NmU3OTYxMjA3NTY0NjE2ODIwNjI2MTczNjk2YjYxNjI2ZTY5MjA
2MTY0NjEyMDc0NjE2NDY5NzA2MTZlMjA2NjZjNjE2NzIwNjI3NTYxNzQyMDZiNjE2ZDc1MjA2YTlWNDM
1NDQ2N2I2Zjdk | base64 -d
546f6c6f6e7206973696b616e206d616d612070756c73612035302e3030302073656b6172616e67
2e204d616d61206c616769206469206b616e746f7220706f6c697369206d6173616b2072656e6461
6e672c206e616e7469206d616d612074656c706f6e2062616c696b206b616c6f2072656e64616e67
6e7961207564616820626173692e20696e6920616461207469746970616e20666c61672062756174
206b616d75203a204354467b6f7droot@flint:~/Downloads#
root@flint:~/Downloads# echo 546f6c6f6e7206973696b616e206d616d612070756c7361203
5302e3030302073656b6172616e672e204d616d61206c616769206469206b616e746f7220706f6c6
97369206d6173616b2072656e64616e672c206e616e7469206d616d612074656c706f6e2062616c6
96b206b616c6f2072656e64616e676e7961207564616820626173692e20696e69206164612074697
46970616e20666c61672062756174206b616d75203a204354467b6f7d | xxd -r -p
Tolong isikan mama pulsa 50.000 sekarang. Mama lagi di kantor polisi masak renda
ng, nanti mama telpon balik kalo rendangnya udah basi. ini ada titipan flag buat
kamu : CTF{o}root@flint:~/Downloads#
```

- Flag : **CTF{o}**

Tersadap (70) Medium

- diberikan file pcapng, buka dengan wireshark dan filter pada 'http'
- cek pada bagian post challenge dan Follow TCP stream

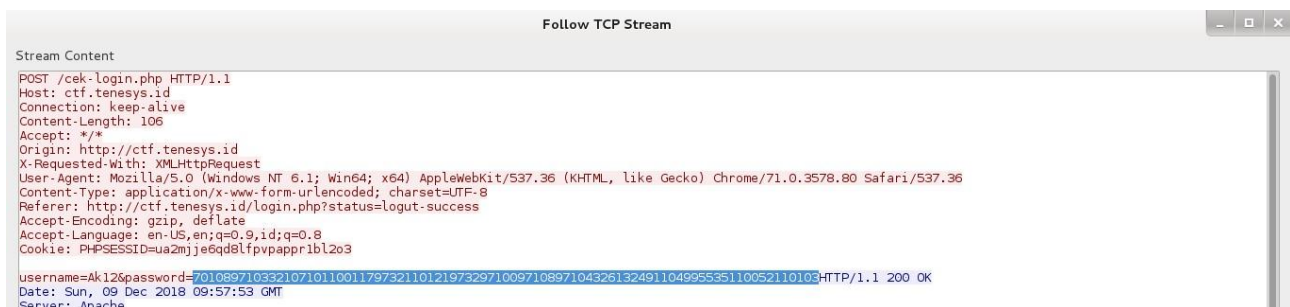


No.	Time	Source	Destination	Protocol	Length	Info
5510	53.280939	192.168.100.9	156.67.208.8	HTTP	630	POST /part/challenge/check.php HTTP/1.1 (applica...
5545	66.885802	192.168.100.9	156.67.208.8	HTTP	632	POST /part/challenge/check.php HTTP/1.1 (applica...
5602	74.806516	192.168.100.9	156.67.208.8	HTTP	615	POST /part/challenge/check.php HTTP/1.1 (applica...
22959	318.692516	192.168.100.9	156.67.208.8	HTTP	659	POST /part/challenge/check.php HTTP/1.1 (applica...
24387	356.937428	192.168.100.9	156.67.208.8	HTTP	626	POST /part/challenge/check.php HTTP/1.1 (applica...
24420	368.869097	192.168.100.9	156.67.208.8	HTTP	627	POST /part/challenge/check.php HTTP/1.1 (applica...
24450	375.427946	192.168.100.9	156.67.208.8	HTTP	620	POST /part/challenge/check.php HTTP/1.1 (applica...
24510	399.263142	192.168.100.9	156.67.208.8	HTTP	671	POST /part/challenge/check.php HTTP/1.1 (applica...
24541	405.902856	192.168.100.9	156.67.208.8	HTTP	617	POST /part/challenge/check.php HTTP/1.1 (applica...
24626	413.343020	192.168.100.9	156.67.208.8	HTTP	628	POST /part/challenge/check.php HTTP/1.1 (applica...
3276	22.112621	192.168.100.9	156.67.208.8	HTTP	630	POST /part/challenge/detail.php HTTP/1.1 (applica...

Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
 > Cookie: PHPSESSID=ua2mjje6qd8lfpvpappr1bl2o3\r\n
 \r\n
 [Full request URI: http://ctf.tenesys.id/part/challenge/check.php]
 [HTTP request 1/1]
 [Response in frame: 5512]
 File Data: 32 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded
 > Form item: "flag" = "CTF{INIBUKANFLAG}"
 > Form item: "id" = "16"

- terdapat sebuah string, coba decode didapat flag kelima adalah n4m4nya_Sn1ff1ng_hehe_:D}



Stream Content

```
POST /cek-login.php HTTP/1.1
Host: ctf.tenesys.id
Connection: keep-alive
Content-Length: 106
Accept: */*
Origin: http://ctf.tenesys.id
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.80 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://ctf.tenesys.id/login.php?status=logut-success
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: PHPSESSID=ua2mjje6qd8lfpvpappr1bl2o3

username=Ak12&password=70108971033210710110011797321101219732971009710897104326132491104995535110052110103
Date: Sun, 09 Dec 2018 09:57:53 GMT
Server: Apache

HTTP/1.1 200 OK
```

- flag terpecah di dalam file tersadap.pcapng tersebut, cari satu persatu pada filter http kemudian decode, dan gabungkan semua flag


```

Applications  Places  Thu Dec 13, 4:39 AM
tersadap.txt (~/Desktop/P6) - gedit
File Edit View Search Tools Documents Help
Open Save Undo Cut Copy Paste Find
tersadap.txt x
1n1_53d4ng
flag=Dimana+sih+flagnya&id=28
Apa+sih+ini&id=58
flag=koksalah&id=72
flag=ohh+harus+CTF%7B%7D&id=72
password-reset=&team-reset=Temukan+Aku+%3A)
Flag kedua nya adalah = 1n1_53d4ng
flag ketiga adalah m3lakuk4n_
flag keempat adalah y4ng_
flag kelima adalah n4m4nya_Sn1ff1ng_hehe_:D}7'1'

1 = aku
2 = 1n1_53d4ng
3 = m3lakuk4n_
4 = y4ng_
5 = n4m4nya_Sn1ff1ng_hehe_:D}
CTF{aku_1n1_53d4ngm3lakuk4n_y4ng_n4m4nya_Sn1ff1ng_hehe_:D}

```

- Flag :CTF{aku_1n1_53d4ngm3lakuk4n_y4ng_n4m4nya_Sn1ff1ng_hehe_:D}

ZIP RUSAK (85)

- Diberikan sebuah file zip yang didalamnya berisi file initahflagnya.txt Terlihat bahwa file tersebut sehat – sehat saja namun sebenarnya filenya tsb rusak karena tidak dapat dibuka ataupun di extract. Buka dengan hexeditor, coba cek file tsb dan mencari referensi dari zip structure <https://users.cs.jmu.edu/buchhofp/forensics/formats/pkzip.html>, sekian lama masih tetep stuck juga.
- Kembali coba searching lagi kesana sini dan beruntung ketemu writeup mirip ziprusak ini di lapping ctf <https://www.lctf.fun/#writeups>

ZIPRUSAKKKKKK.zip

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	00	00	08	00	9B	AB	7A	4D	58	58	PK.....>zMXX
00000010	58	58	A2	00	00	00	28	00	00	00	58	00	00	00	66	6C	XX<... (...X...fl
00000020	51	67	70	61	6C	73	75	69	6E	69	69	2E	74	78	74	4B	agpalsuinii.txtK
00000030	4A	CD	4B	2D	CA	CC	53	A8	CA	2C	50	28	48	CC	4E	55	J1K-E1S-E,P(H1NU
00000040	70	0E	71	AB	CE	31	48	4E	CC	89	4F	33	CC	49	8D	8F	p.q«11HN1%0311..
00000050	CF	48	35	49	49	0D	AA	05	00	50	4B	01	02	1F	00	14	1H511.^...PK.....
00000060	00	00	00	08	00	9B	AB	7A	4D	1C	8E	B4	69	2A	00	00>zM.Z'i*..
00000070	00	28	00	00	00	11	00	24	00	00	00	00	00	00	00	20	.(.....\$.....
00000080	00	00	00	00	00	00	00	66	6C	61	67	6E	79	61	69	6Eflagnyaain
00000090	69	74	61	68	2E	74	78	74	0A	00	20	00	00	00	00	00	itah.txt..
000000A0	01	00	18	00	FC	2F	FC	5B	94	85	D4	01	3C	8A	9A	05ü/ü["...Ô.<Šš.
000000B0	94	85	D4	01	3C	8A	9A	05	94	85	D4	01	50	4B	05	06	"...Ô.<Šš."...Ô.PK..
000000C0	00	00	00	00	01	00	01	00	63	00	00	00	59	00	00	00c...Y...
000000D0	00	00															..

- Diketahui berdasarkan tabel struktur, letak kesalahan ada pada :
 - Hash CRC32 (mudahnya dapat dilihat langsung dengan menggunakan aplikasi winrar). Dan saya samakan dengan nilai hex yang ada dibawahnya

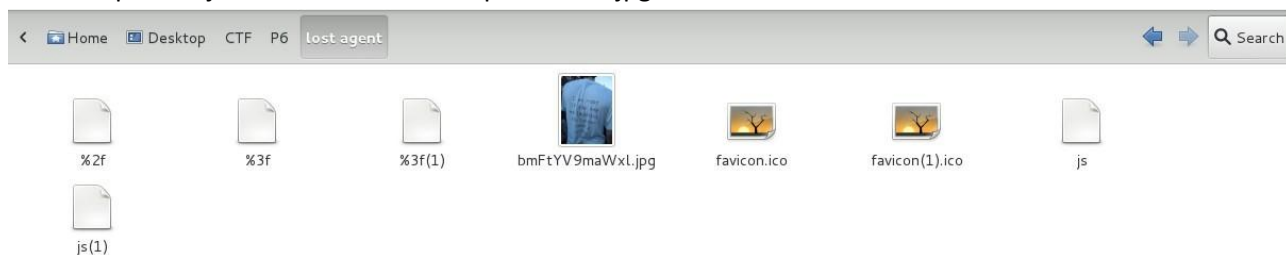
- Nama file yang tersisip dalam file tersebut (seharusnya bernama flagnyainitah.txt bukan flagpalsuinii.txt).
- Edit nilai hex pada file tersebut dan save .

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	00	00	08	00	9B	AB	7A	4D	1C	8E	PK.....>«zM.Ž
00000010	B4	69	2A	00	00	00	28	00	00	00	11	00	00	00	66	6C	'i*... (.....fl
00000020	61	67	6E	79	61	69	6E	69	74	61	68	2E	74	78	74	4B	agnyainitah.txtK
00000030	4A	CD	4B	2D	CA	CC	53	A8	CA	2C	50	28	48	CC	4E	55	JĲK-ĒİS"Ē,P(HĲNU
00000040	70	0E	71	AB	CE	31	48	4E	CC	89	4F	33	CC	49	8D	8F	p.q«ĲlHNİ%03İİ..
00000050	CF	48	35	49	49	0D	AA	05	00	50	4B	01	02	1F	00	14	İH5İİ.*...PK.....
00000060	00	00	00	08	00	9B	AB	7A	4D	1C	8E	B4	69	2A	00	00>«zM.Ž'i*...
00000070	00	28	00	00	00	11	00	24	00	00	00	00	00	00	00	20	. (.....\$.....
00000080	00	00	00	00	00	00	00	66	6C	61	67	6E	79	61	69	6Eflagnyain
00000090	69	74	61	68	2E	74	78	74	0A	00	20	00	00	00	00	00	itah.txt..
000000A0	01	00	18	00	FC	2F	FC	5B	94	85	D4	01	3C	8A	9A	05ü/ü["...Ô.<Šš.
000000B0	94	85	D4	01	3C	8A	9A	05	94	85	D4	01	50	4B	05	06	"...Ô.<Šš."...Ô.PK..
000000C0	00	00	00	00	01	00	01	00	63	00	00	00	59	00	00	00c...Y...
000000D0	00	00															..

- buka dan flag akan didapatkan: **CTF{l0cal_file__he4deR}**

Lost Agent (110) Hard

- Diberikan file pcapng, coba simpan file tersebut dengan cara
- file >> Export Objects >> HTTP dan didapatkan file jpg



- cek dengan exiftool didapat sebuah koordinat dan search pada google map

```

GPS Date/Time          : 2016:07:05 14:01:39Z
GPS Latitude           : 5 deg 22' 33.61" S
GPS Latitude Ref       : South
GPS Longitude          : 105 deg 14' 47.53" E
GPS Longitude Ref      : East
GPS Position           : 5 deg 22' 33.61" S, 105 deg 14' 47.53" E
Image Size             : 296x394
root@Hexa:~/Desktop/CTF/P6/lost agent#

```



- Nama warnet samping Yan Cell adalah FAJAR dan ubah ke sha256
- flag : `CTF{d6deb0c5e0efa2f72f63d7fb805504b54a1962aeaaf45b6eac9ef4d959806717}`

#Crypto

Triple ASCII (10) Easy

- Buka pesan pada link ini <https://drive.google.com/file/d/1ttC744cqxmYuYCO8ViQZSzCEkrnnhowT/view>
- decode dari yg pertama biner, lalu decimal dan terakhir hexa di <https://cryptii.com> dan gabungkan menjadi
- Flag : `CTF{T1ga_Da5ar_Pent0l_Asc1i}`

Base Camp (20) Easy

- Buka link <https://www.dropbox.com/s/kfm6nheounetoa7/Basecamp.txt?dl=0> didapatkan sebuah base64, dengan python kita decode menjadi
`INKEM62CGQ2TGX3CGRZTGX3JGVPM3SPFPWOMBQMRPWE4TPPU=====`
- Hasil didapat sebuah base32 lalu decode kembali

```
>>> x=base64.b64decode(a)
>>> print x
INKEM62CGQ2TGX3CGRZTGX3JGVPM3SPFPWOMBQMRPWE4TPPU=====
>>> b="INKEM62CGQ2TGX3CGRZTGX3JGVPM3SPFPWOMBQMRPWE4TPPU======"
>>> x=base64.b32decode(b)
>>> print x
CTF{B453 b4s3 i5 v3ry g00d bro}
>>>
```

- flag : `CTF{B453_b4s3_i5_v3ry_g00d_bro}`

Caisar (20) Easy

- Disini saya menggunakan tools di <https://cryptii.com>
- string merupakan Caesar chipper jadi tinggal kita geser aja

The screenshot shows the 'CAESAR CIPHER' tool interface. The 'Shift' is set to 13. The 'Transform' dropdown is set to 'Lowercase letters'. The input text is 'OFR{OMQEMD_OUBTQD_UFG_OGYMZ_PU_SQEQD_MVM}' and the output is 'ctf{caesar_cipher_itu_cuman_di_geser_aja}'.

- Taraaa.. flagnya :CTF{caesar_cipher_itu_cuman_di_geser_aja}

Vigen (30) Easy

KEY : INIKUNCI

CIPHER : KGN{Fctgvmem_snh_vpm_omcn_cqswxviu}

- Sesuai judul vigen chipper masukan key "inikunci" dan didapat

The screenshot shows the 'Vigenere cipher' tool interface. The 'KEY' is set to 'inikunci'. The 'Plaintext' dropdown is set to 'Plaintext'. The output is 'ctf{vigenere_itu_the_best_pokoknya}'.

- Flagnya : CTF{vigenere_itu_the_best_pokoknya}

Emm Dee Lyma (30)

- Decrypt md5 tersebut '4dc4c8bb99cbdf316b3d87c207111718' pada <https://hashkiller.co.uk/md5-decrypter.aspx>
- Flag : CTF{Md5_Md5_y4huuuuud}

Hash For Password (35)

- coba decrypt kembali dengan web tadi ternyata gagal dan saya cari lagi web lainnya, setelah lama searching saya mencoba disini <http://www.md5decrypt.org/>
- yang ternyata mempunyai database yg sama saat string diencrypt
- flag :
CTF{Say4n9_K4mu_T4u_9ak_K4lau_D3kr1p_MD5_1tu_Haru5_S4ma_Den9an_D4ta8as
e_5aat_D1a_Men9enkr1p_?}

I am Fine (40) Easy

Cipher : CTF{hggvub_vhp_gvub_yqhufxzd}

Key 1 : 5

Key 2 : 7

- Dengan menggunakan affine chipper

Affine cipher ▾

SLOPE / A			INTERCEPT / B		
−	5	+	−	7	+

ALPHABET
 abcdefghijklmnopqrstuvwxyz

+

Plaintext ▾

zsk{affine_iam_fine_thankyou}

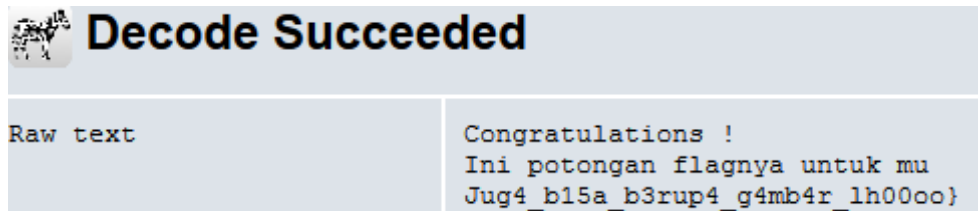
- Flagnya: **CTF{affine_iam_fine_thankyou}**

Just Base Friend (50) Medium

- Diberikan link menuju
<https://www.dropbox.com/s/9jc79p83ucdgg6w/Just%20Base%20Friend.txt?dl=0>
- decode base64 tersebut didapat setengah flag CTF{Base64_
- base64 satunya diduga merupakan file gambar karna terdapat strings PNG dan ternyata benar



- Decode qrcode tersebut dan didapatkan setengah flag nya



- Gabungkan dan Flag didapat : **CTF{Base64_Jug4_b15a_b3rup4_g4mb4r_lh00oo}**

Hari Kebalikan (50) Medium

- Kita reverse saja key substitusinya :

ABCDEFGHIJKLMNOPQRSTUVWXYZ
 ZYXWVUTSRQPONMLKJIHGFEDCBA

- Menjadi
 :fwi{lrl_dgdodk_kdul_nhedolndr_vtxlgzdug_pdnd_d_mdgl_z_vhodpdw_kdul_nhedolndr
 }

- geser dengan caesar dan didapat

Caesar cipher ▾

Plaintext ▾

SHIFT

-

29

+

ctf{ioi_adalah_hari_kebalikao_squidward_maka_a_jadi_w_se
lambat_hari_kebalikao}

- perbaiki sedikit penulisan kata dan Flag nya :
CTF{ini_adalah_hari_kebalikan_squidward_maka_a_jadi_w_selamat_hari_kebalikan}

The Subtitution (55) Medium

- Dengan clue yang ada bahasa merupakan inggris mencoba di <https://quipqiup.com> dengan method dictionary, text pun didapat Albert Einstein quote is "the only source of knowledge is experience"

https://quipqiup.com

quip

quipqiup is a fast and automated cryptogram solver by [Edwin Olson](#). It can solve simple substitution ciphers often found in ne

Puzzle:

Qywsni Scguiscg bohls cu "ixs hgyt uhones hd tghjysazs cu skvancsages"

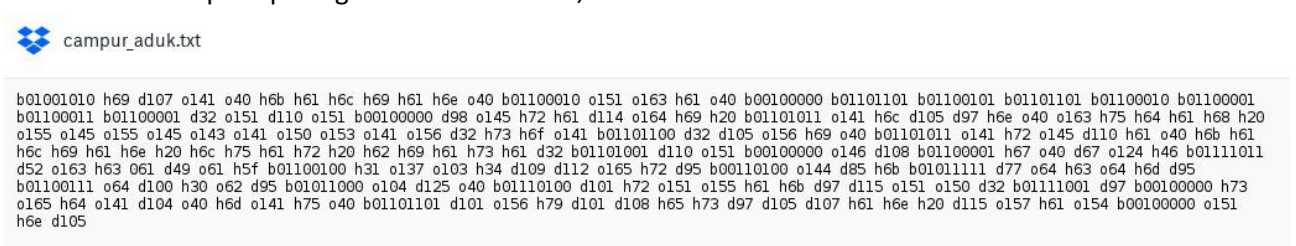
Clues: For example G=R QVW=THE

0 -0.654 Albert Einstein quote is "the only source of knowledge is experience"

- Encrypt isi kutipan dengan sha1 dan flag didapat :
CTF{3021852b58ed30adb8a2eb5058ae1f688e7cb1b1}

Campur Aduk (55)

- Diberikan soal seperti pada gambar di bawah ini,



- Untuk tim toxic terimakasih yang mau susah payah mencoba decode manual 1 per 1 wkwwkw dan berhasil solved awalnya berkat mereka.

- Dan makasih juga untuk yg ngasih scriptnya :v

```
campuraduk.py x
import binascii

chiper = 'b01001010 h69 d107 o141 o40 h6b h61 h6c h69 h61 h6e o40 b01100010 o151 o163 h61 o40 b00100000 b01101101 b01100101 b01100101 b01100010 b01100011 b01100011 b01100011 d32 o151 d110 o151 b00100000 d98 o145 h72 h61 d114 o164 h69 h20 b01101011 o141 h6c d105 d97 h6e o40 o163 h75 h64 h61 h68 h20 o155 o145 o155 o145 o143 o141 o150 o153 o141 o156 d32 h73 h6f o141 b01101100 d32 d105 o156 h69 o40 b01101011 o141 h72 o145 d110 h61 o40 h6b h61 h6c h69 h61 h6e h20 h6c h75 h61 h72 h20 h62 h69 h61 h73 h61 d32 b01101001 d110 o151 b00100000 o146 d108 b01100001 h67 o40 d67 o124 h46 b01111011 d52 o163 h63 o61 d49 o61 h5f b01100100 h31 o137 o103 h34 d109 d112 o165 h72 d95 b00110100 o144 d85 h6b b01011111 d77 o64 h63 o64 h6d d95 b01100111 o64 d100 h30 o62 d95 b01011000 o104 d125 o40 b01110100 d101 h72 o151 o155 h61 h6b d97 d115 o151 o150 d32 b01111001 d97 b00100000 h73 o165 h64 o141 d104 o40 h6d o141 h75 o40 b01101101 d101 o156 h79 d101 d108 h65 h73 d97 d105 d107 h61 h6e h20 d115 o157 h61 o154 b00100000 o151 h6e d105'

plain = ""
for a in chiper.split(' '):
    if a.startswith("h"):
        plain += a[1:].decode('hex')
    if a.startswith("d"):
        plain += chr(int(a[1:]))
    if a.startswith("o"):
        plain += chr(int(a[1:], 8))
    if a.startswith("b"):
        plain += binascii.unhexlify('%x' % int(a[1:],2))

print plain
```

```
File Edit View Search Terminal Help
root@Hexa:~/Desktop/CTF/CRYPTOGRAPHY# python campuraduk.py
Jika kalian bisa membaca ini berarti kalian sudah memecahkan soal ini karena kalian luar biasa ini flag CTF{4sc11_d1_C4mpur_4dUk_M4c4m_g4d02_XD} teri
makasih ya sudah mau menyelesaikan soal ini
root@Hexa:~/Desktop/CTF/CRYPTOGRAPHY#
```

- Flag : CTF{4sc11_d1_C4mpur_4dUk_M4c4m_g4d02_XD}

Ayo main Sandi Pramuka (55) Medium

- Dengan clue sesuai judul, search gambar tentang sandi pramuka dan diketahui menggunakan sandi merah putih

	M	E	R	A	H
P	A	B	C	D	E
U	F	G	H	I	J
T	K	L	M	N	O
I	P	Q	R	S	T
H	U	V	W	X	Y
					Z

- Dengan key1 : CUMANDan key2 : TEMAN saya corat-oret dikertas :v, dengan menambah satu huruf dandidapat flag : CTF{WATASHI_JUST_FRIEND_HIKS}

#Web

Headbang (20) Easy

- Diberikan link
<http://play.ctf.tenesys.id/a6a0004c322a18afe5d1a0eb64a0984e/index.php>
- kemudian cekpada http header dengan curl

```
root@flint:~# curl -I http://play.ctf.tenesys.id/a6a0004c322a18afe5d1a0eb64a0984e/index.php
HTTP/1.1 200 OK
Date: Thu, 27 Dec 2018 04:19:49 GMT
Server: Apache
X-Powered-By: PHP/5.6.38
Z-Flag: CTF{Fl49_4da__d1_H3adER}
Vary: User-Agent
Content-Type: text/html; charset=UTF-8
Connection: Keep-Alive
Content-Length: 0
```

- Flag : CTF{Fl49_4da__d1_H3adER}

Console (30) Easy

- diberikan link
<http://play.ctf.tenesys.id/6cef97b622fe1940d59d65ea07313806/>
- lihat source code web tersebut 'ctrl+u'

```
<p>GIVE ME MY FLAG!!!</p>

<!-- you thought the flag would be in the comments didn't you? nice try we're better than that -->
</div>
<script type="text/javascript" src="script.js"></script>
<script type="text/javascript">if (self==top) {function netbro_cache_analytics(fn, callback) {setTimeou

Prism.languages.scss=Prism.languages.extend("css",{comment:{pattern:/(\s|^[^\\]) (\s|\\*['
Prism.languages.bash=Prism.languages.extend("clike",{comment:{pattern:/(\s|^[^\\]) (#
console.log('Wow, anda luar biasa! Ini flag untuk kamu : Fla9_Bi5a_Ada_D1man4pun');
/*! perfect-scrollbar - v0.5.8
* http://noraesae.github.com/perfect-scrollbar/
```

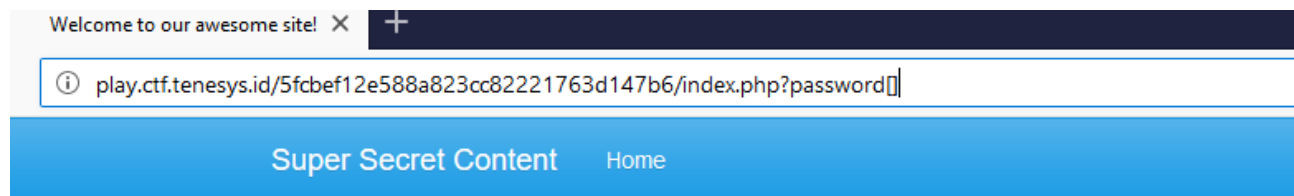
- cek pada javascript file itu dan lihat ditemukan flag : **CTF{Fla9_Bi5a_Ada_D1man4pun}**

Komparasi (35) Easy

- Diberikan link
<http://play.ctf.tenesys.id/5fcbe12e588a823cc82221763d147b6/index.php>
- Kita lihat source code pada index.md celahnya ada pada strcmp(a, b)==0

```
$auth = false;
if (isset($_GET["password"])) {
    if (strcmp($_GET["password"], $pass) == 0) {
        $auth = true;
    }
}
```

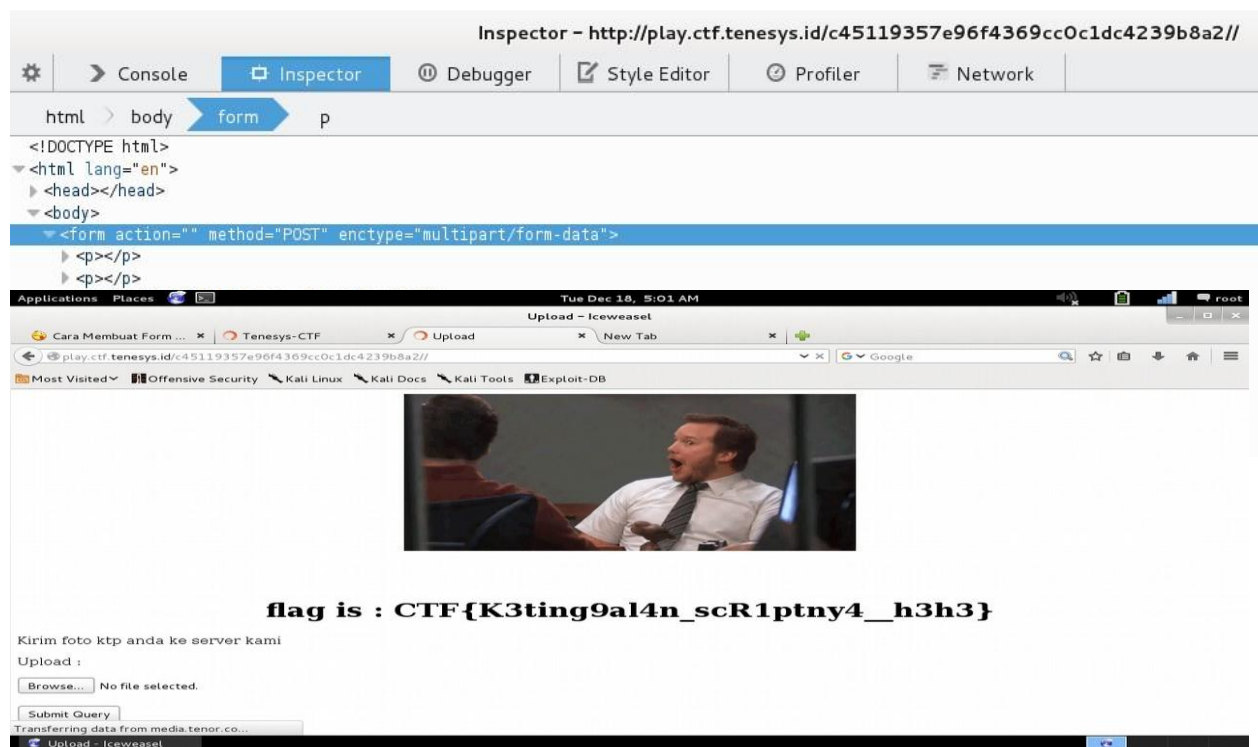
- tambahkan ?password[]= pada akhir linknya



- Flag : **CTF{Don't_7ru5t_5trcmp}**

Loss (40) Easy

- Diberikan link <http://play.ctf.tenesys.id/c45119357e96f4369cc0c1dc4239b8a2//>
- jika dilihat source code pasti paham script tersebut ada yang kurang
- inspect element dan tambahkan pada bagian form : enctype="multipart/form-data"



- flag is : CTF{K3ting9al4n_scR1ptny4_h3h3}

Asal-lasa (45) Easy

- Diberikan link berikut
<http://play.ctf.tenesys.id/330e75f7d451a6889b03029cedd2d771/index.html>
- Kita liat lagi source code web tersebut

```

</body>
<!-- <script>
  var _0xa405 = ["\x4e\x75\x62\x31\x5f", "\x4d\x6f\x68", "\x48\x61", "\x42\x31\x6d\x62\x69", "\x7d", "\x4b", "\x43\x54\x46\x7b", "\x6e\x39\x61\x6e\x79", "\x61\x6b\x34\x6b\x7a\x5f", "\x30\x6e\x5f", "\x78\x30\x72\x5f"];
  var _0xf0a4 = [_0xa405[0], _0xa405[1], _0xa405[2], _0xa405[3], _0xa405[4], _0xa405[5], _0xa405[6], _0xa405[7], _0xa405[8], _0xa405[9], _0xa405[10]];
  var tenesys = _0xf0a4[0];
  var ten3sys = _0xf0a4[7];
  tenesys = _0xa405[3] + _0xa405[6] + _0xa405[1] + _0xa405[8] + _0xa405[10] + _0xa405[4] + tenesys + _0xa405[9];
  ten3sys = _0xa405[5] + ten3sys + _0xa405[2];
</script> -->
</html>

```

- sama seperti hex bisa dibilang javascript obfuscator?bener ato kaga,kemudian decode dan coba susun

```

asalasa.txt
0 "\x4e\x75\x62\x31\x5f",      Nub1_
1 "\x4d\x6f\x68",             Moh
2 "\x48\x61",                  Ha
3 "\x42\x31\x6d\x62\x69",      B1mbi
4 "\x7d",                       }
5 "\x4b",                       K
6 "\x43\x54\x46\x7b",          CTF{
7 "\x6e\x39\x61\x6e\x79\x61",  n9anya
8 "\x61\x6b\x34\x6b\x7a\x5f",  ak4kz_
9 "\x30\x6e\x5f",              0n_
10 "\x78\x30\x72\x5f",         x0r_

var tenesys = _0xf0a4[0];      = Nub1_
var ten3sys = _0xf0a4[7];      = n9anya

tenesys = _0xa405[3] + _0xa405[6] + _0xa405[1] + _0xa405[8] + _0xa405[10] + _0xa405[4] + tenesys + _0xa405[9];

B1mbiCTF{Mohak4kz_x0r_}Nub1_0n_

ten3sys = _0xa405[5] + ten3sys + _0xa405[2];

Kn9anyaHa|

```

- Flag : CTF{Hax0r_Nub1_Kak4kz_Moh0n_B1mbin9anya}

Kakukikeko (45) Easy

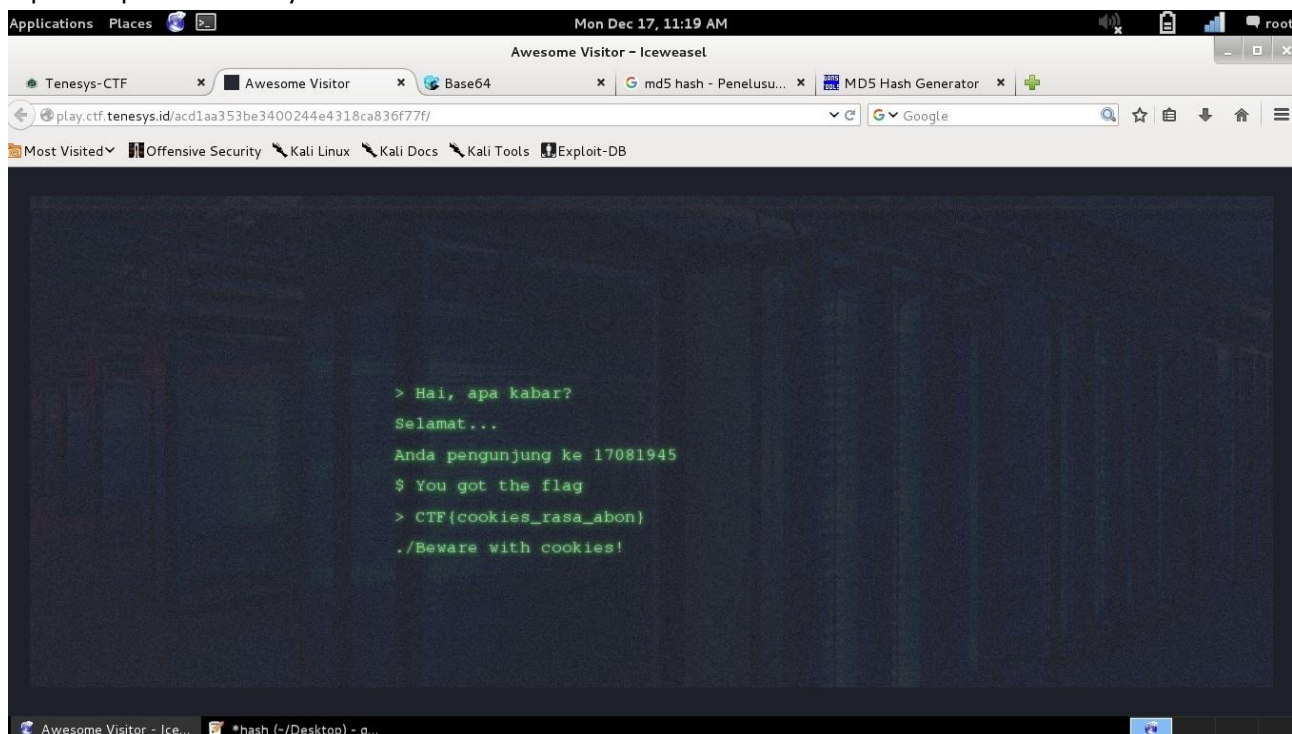
- Diberikan link
<http://play.ctf.tenesys.id/acd1aa353be3400244e4318ca836f77f/>
- langsung saja cek cookie web tersebut

Editor Gaya	Kinerja	Memori	Jaringan	Penyimpanan	Aksesibilitas	Adblock Plus
Domain	Direktori	Kedaluwarsa pada	Terakhir diakses pada	Nilai		
play.ctf.tenesys...	/acd1aa353be3...	Sesi	Wed, 26 Dec 2018 17:12:3...	MzEzMzc6NmYzMjQ5YWEzMDQwNTVkJmM4MjhhZjNiZmFiNzc4ZjY%3D		

string merupakan base64, lalu decode

```
File Edit View Search Terminal Help
root@Hexa:~# python
Python 2.7.3 (default, Mar 14 2014, 11:57:14)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> "MzEzMzc6NmYzMjQ5YWEzMDQwNTVkJmM4MjhhZjNiZmFiNzc4ZjY==" .decode('base64')
'31337:6f3249aa304055d63828af3bfab778f6'
>>>
```

- Hasil decode merupakan angka pengunjung 31337 dan setelahnya merupakan hasil hash md5nya
- Jadi hash saja 17081945 menjadi md5 <https://www.md5hashgenerator.com/>
- hasil hash buat seperti ini =17081945:d41f6c90ac245d93aa2740e083407393
- encode kembali menjadi base64
'MTcwODE5NDU6ZDQxZjZjOTBhYzI0NWQ5M2FhMjc0MGUwODM0MDczOTM'
- inputkan pada cookie nya dan booomz...



- Flag : **CTF{cookies_rasa_abon}**

Number (65) Medium

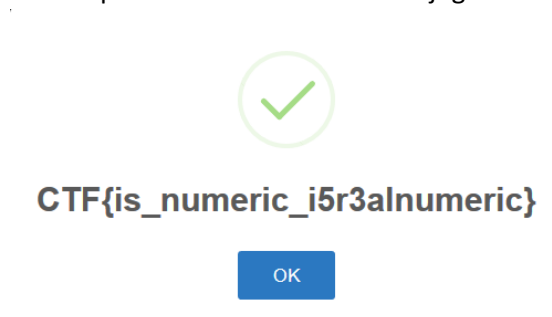
- Diberikan sebuah link dengan clue robot didalamnya
<http://play.ctf.tenesys.id/d89e00b8b4ea97df904450702bd4353e/>



- cek pada robots.txt ada sebuah file backup.zip, download dan buka terdapat script proses.php

```
1 <?php
2 include "flag.php";
3 $stat = "";
4 $notice = "error";
5 $min = 9000;
6 $max = 10000;
7 $password = $_GET['password'];
8 if (isset($password)) {
9     if (is_numeric($password)){
10         if (!strpos($password, ".")){
11             $passw = 0 + $password;
12             if (strlen($passw) > 4){
13                 if ($passw > $min){
14                     if ($passw < $max){
15                         $stat = $flag;
16                         $notice = 'success';
17                     }else{
18                         $stat = 'Oops, terlalu besar!';
19                     }
20                 }
21             }
22             else
23                 $stat = 'Hmmm ,terlalu kecil!';
```

- password adalah angkalebih dari 9000 dan kurang dari 10000, Ditambah strlen harus lebih dari 4??
- Pada php, is_numeric() bisa diberi parameter eksponen misal 9e3=9000
- Coba inputkan 99999e-1 dan solve juga :’v



- Flag :CTF{is_numeric_i5r3alnumeric}

Komparasi 2D (75) Medium

- Diberikan link dengan hint berupa strcmpplagi
<http://play.ctf.tenesys.id/23053b77473074683f52bfa8d97d7125/index.php>
- lihat pada source code bagian index.md

Celah pada strcmp bisa dibypass dengan memasukkan array 2dimensi, apapun isinya bernilai true. Jadi idenya seperti ini saja sebanyak 12

tambahkan pada alamat link dan didapat

- Diberikan gambar, coba search google for image dan...

Google <https://20-h979-rw> x bayerische staatsbibliothek

All **Images** Maps Shopping More Settings Tools

About 25,270,000,000 results (0.72 seconds)





Image size: 997 × 744
Find other sizes of this image: All sizes - Medium

Best guess for this image: [bayerische staatsbibliothek](#)

Bayerische Staatsbibliothek
<https://www.bsb-muenchen.de/> Translate this page
 Die Bayerische Staatsbibliothek (BSB) in München ist die zentrale Landesbibliothek des Freistaates Bayern und eine der bedeutendsten ...

Bayerische Staatsbibliothek - Wikipedia
https://en.wikipedia.org/wiki/Bavarian_State_Library
 The Bavarian State Library in Munich is the central "Landesbibliothek", i. e. the state library of the Free State of Bavaria and one of Europe's most important ...

Visually similar images



Bavarian State Library

The Bavarian State Library in Munich is the central "Landesbibliothek", i. e. the state library of the Free State of Bavaria and one of Europe's most important universal libraries. With its collections currently around 10.36 million books, it ranks among the best research libraries worldwide. [Wikipedia](#)

Construction started: 1832
Height: 24 m
Architectural style: Romanesque Revival architecture
Founded: 1558
Function: Library
Architect: [Friedrich von Gärtner](#)

Profiles

[Facebook](#) [YouTube](#) [Twitter](#)

People also search for

[Berlin State Library](#) [German National Library](#) [Austrian National Library](#) [National Library of the Netherlands](#)

- Flag : **CTF{Bavarian State Library}**

Monumen (30)

- Coba search google dengan keyword 'kipa taman kubus biner' didapat gambar



- Yang ternyata kubus tersebut mempunyai 4 sisi, saya coba Decode semuanya didapat :
 - BEAUTIFUL MALANG 1
 - NGALAM KIPA ILAKES 2
 - PARIS OF EAST JAVA 3
 - KOTA PENDIDIKAN 4
- Kita inputkan salah satunya dan flag : **CTF{KOTA PENDIDIKAN 4}**
 //Sempat frustrasi karna puluhan kali submit gagal dan dikasih clue sama kk Andrian :v

Where The Flag (40)

- Search di google 'mana99 vitt' didapat sebuah blog.

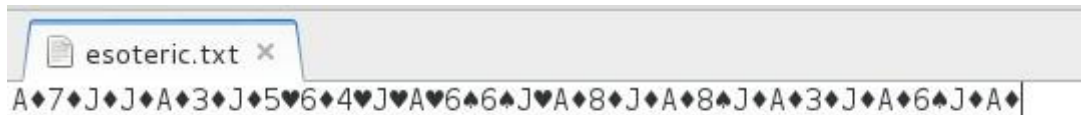
[Home](#)

 Subscribe to: [Posts \(Atom\)](#)

5047537b4334656e5f433361706e65765f537934747d :

- pada bagian footer terdapat string hex, decode menjadi PG5{C4en_C3apnev_Sy4t} , dan geser dengan Caesar. Flag : **CTF{p4ra_p3ncari_fl4g}**

Esoteric (45) Easy



- Sebenarnya saya langsung search google, dan didapat link <https://esolangs.org/wiki/Ante>
- lalu awalnya mau saya coba decrypt :v dan ga mungkin wkww
- Baca cluenya lagi, flag merupakan nama :D

Ante - Esolang - Iceweasel

Tenesys-CTF x Ante - Esolang x +

https://esolangs.org/wiki/Ante#Syntax

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Page [Discussion](#) [Read](#)

Ante

Ante is an [esoteric programming language](#) where all you've got is a deck of playing cards. The interpreter was developed in Ruby, versions in Go, Rust, and Swift are also available.

Contents [\[hide\]](#)

- [1 Operators, Sequential Precedence](#)
- [2 Syntax](#)
- [3 Examples](#)
- [4 External resources](#)

Operators, Sequential Precedence

- ♦ # Add
- ♥ # Multiply
- ♠ # Subtract
- ♣ # Divide

- Flag : **CTF{Ante}**

Broken Link (45)

- Saya kira awalnya string tersebut merupakan link dari mega.nz, ternyata bukan, string merupakan sebuah link googledrive

CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u}
CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u}
CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u} Flag is
CTF{Go0gl3_Dr1v3_is_aw3s0me} CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u}
CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u}
CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u} CTF{In1_Buk4n_FI4g_T4u}

- Scroll dan lihat dengan teliti terdapat flag : **CTF{Go0gl3_Dr1v3_is_aw3s0me}**

Organization Name (5)

- Unit Kegiatan Mahasiswa Programming Teknokrat.
- Saya coba singkatan dari ukm tersebut dan yap benar : **CTF{protek}**

Special Thanks for Kak Andrian, Kak Thomas, Kak Zhansy, Kak Allen, juga Kak Lian dan yang lainnya, yang udah mau bantu solve sehingga terciptanya lah writeup dari saya ini. jugaterimakasih pastinya buat tim FR13NDS dan toxicping, kalianpaten kalee pak~