

Write Up Olimpiade Hacking ITTS - Week 2

Daftar Isi :

1. Osint
 - Find-Me
2. Network Analysis
 - HIU KAWAT
 - Object
3. Web Hacking
 - Not Easy
 - Bau Bawang
4. File Structure
 - De(compress)
5. Application Service
 - DNS pt. 1
 - DNS pt. 2

[OSINT]

Find Me

Description

Hint : Burung Biru

Recon

Diberikan sebuah gambar seperti berikut



Aku menulisnya di ulasan

gambar tersebut berisi sebuah Tugu Jogja dengan bertuliskan "Aku menulisnya di ulasan"

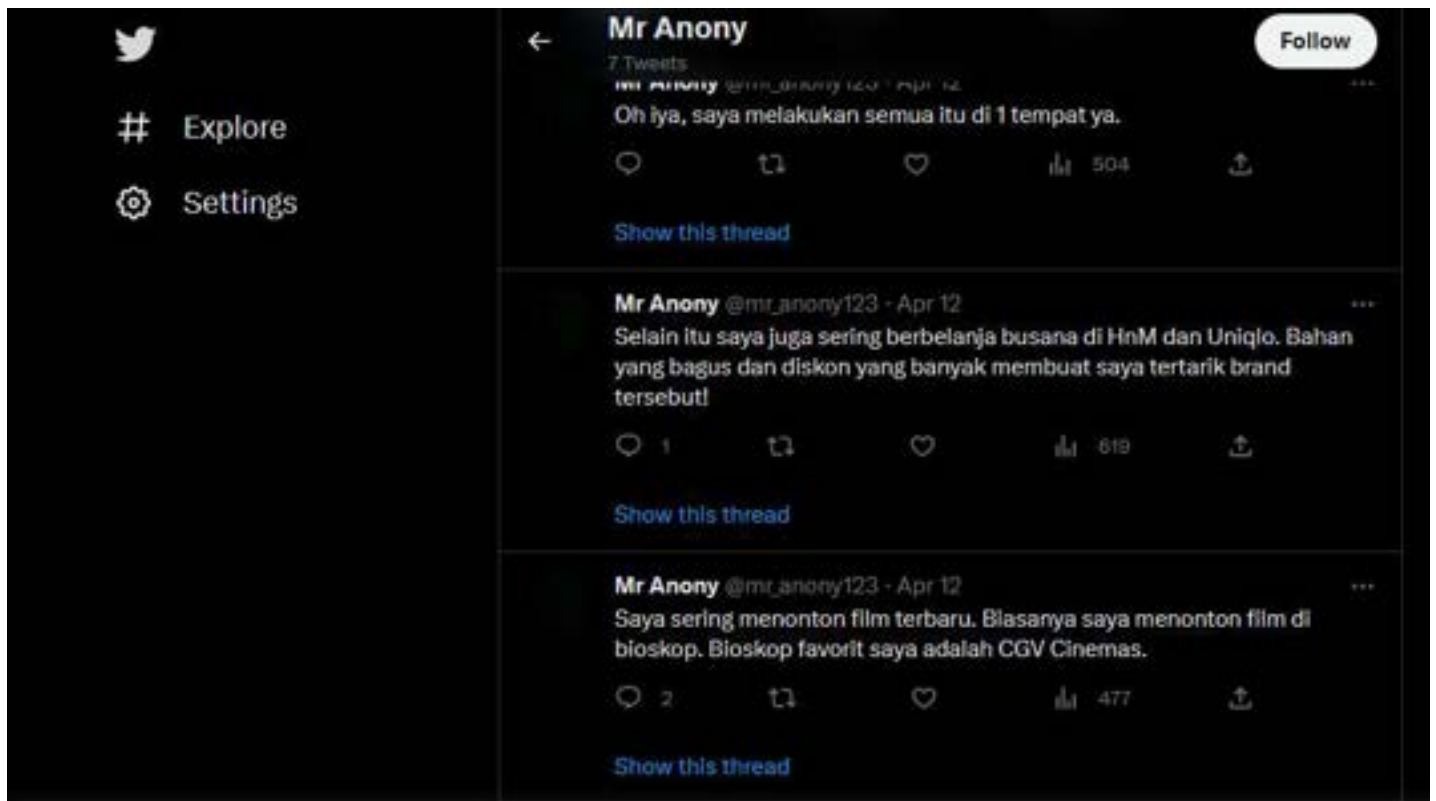
Solve

Asumsi saya awalnya flag tersebut terdapat pada suatu gambar Tugu Jogja yang ada di aplikasi Twitter, Namun setelah lama mencari tidak mendapatkan hasil apa-apa

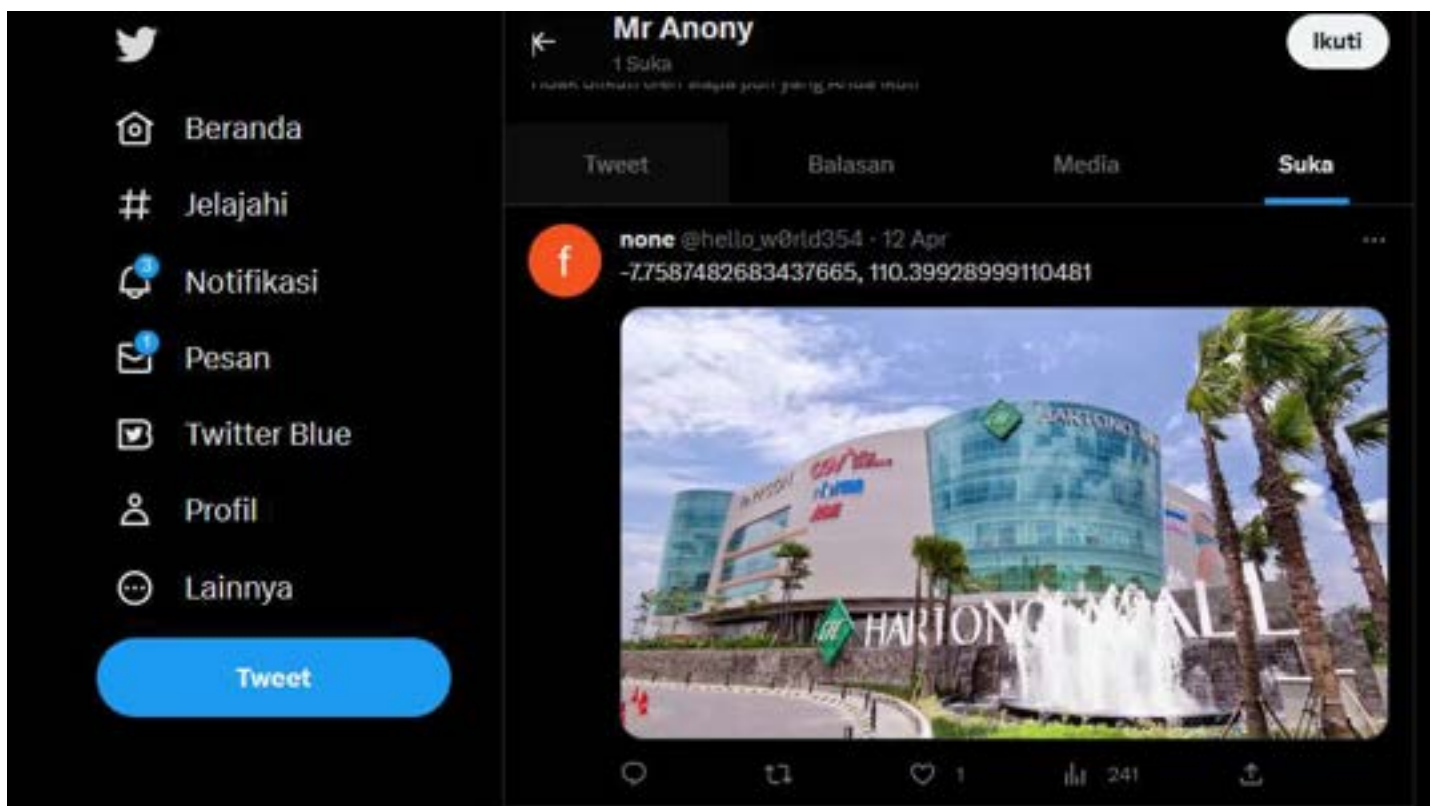
Setelah itu saya mencoba menganalisa metadata dari foto tersebut menggunakan **Exiftool**

```
(anomali@MAYYY)-[~/ITTS]
$ exiftool flag-osint.jpg
ExifTool Version Number      : 12.52
File Name                    : flag-osint.jpg
Directory                   : .
File Size                    : 545 kB
File Modification Date/Time  : 2023:04:12 23:02:21+07:00
File Access Date/Time       : 2023:04:17 23:58:39+07:00
File Inode Change Date/Time  : 2023:04:13 11:21:36+07:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
DCT Encode Version          : 100
APP14 Flags 0                : (none)
APP14 Flags 1                : (none)
Color Transform              : Unknown (RGB or CMYK)
Exif Byte Order              : Big-endian (Motorola, MM)
XP Comment                   : Temukan saya di Twitter ya!
Padding                      : (Binary data 2060 bytes, use -b option to extract)
X Resolution                 : 72
Displayed Units X             : inches
Y Resolution                 : 72
Displayed Units Y             : inches
XMP Toolkit                  : Adobe XMP Core 7.1-c000 79.b0f8be9, 2021/12/08-19:11:22
Format                       : image/jpeg
Title                        : flag-osint
Description                   : Find me on Twitter ya!
Creator                      : mr_anony123
Subject                      : OSINT, Twitter
Creator Tool                  : Adobe Illustrator 26.2 (Windows)
Create Date                  : 2023:04:12 11:01:21+07:00
Modify Date                  : 2023:04:12 04:01:29Z
Metadata Date                : 2023:04:12 11:01:21+07:00
Rating                       : 5
```

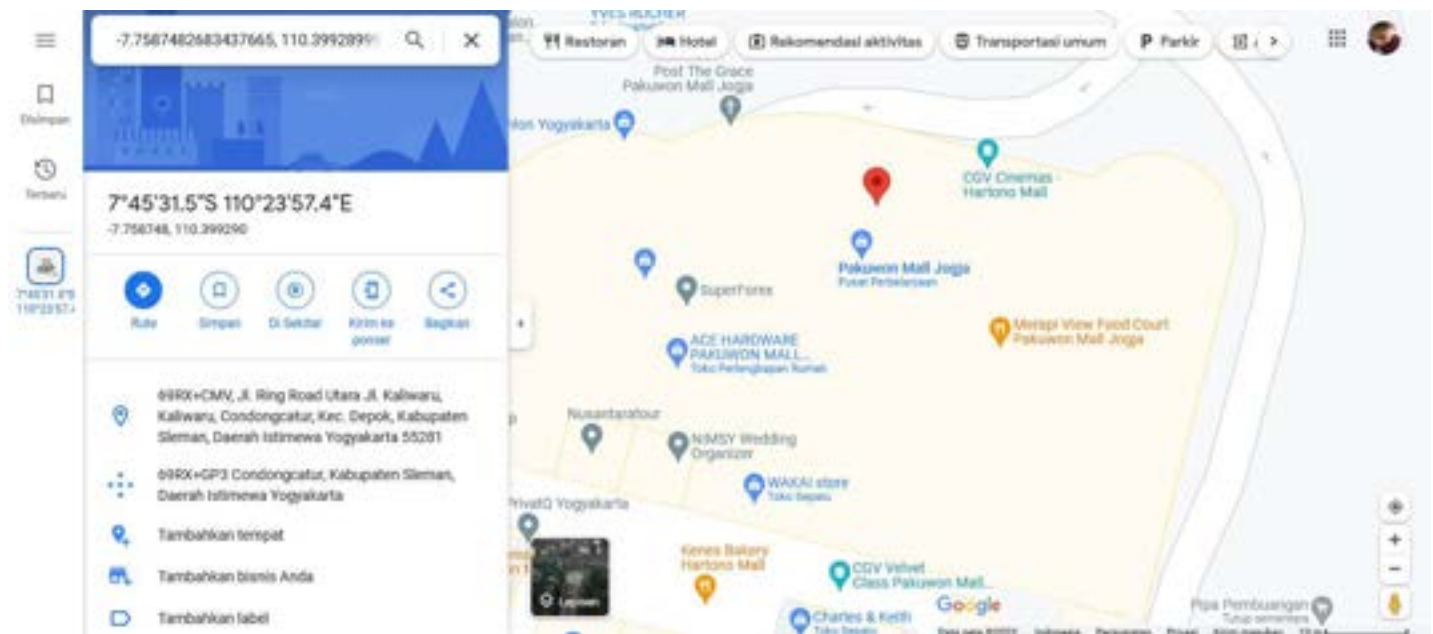
kita dapatkan sebuah akun twitter dengan username **mr_anony123**, langsung saja kita cek twitter



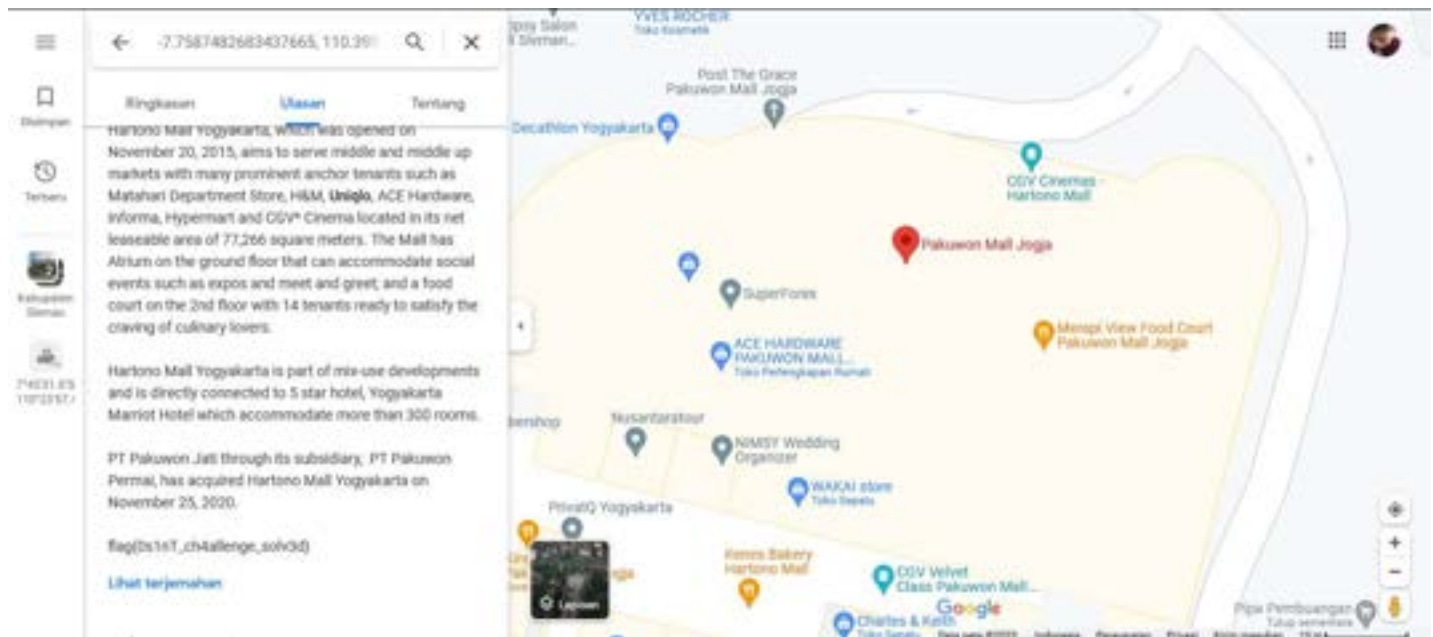
pada cuitan tweet tersebut merujuk ke suatu tempat yang ada di Mall Jogja, Kita eksplor akunnya lebih dalam



Pada bagian likes terdapat gambar serta Koordinat yang merujuk pada Mall yang ada di Jogja, Langsung kita buka Google Maps



Ternyata Koordinat tsb menunjukkan ke Pakuwon Mall Jogja



ditemukan sebuah flag berada pada kolom ulasan

Flag

flag{0s1nT_ch4allenge_sol3d}

[Network Analysis]

Hiu Kawat









Deskripsi

Dengan menganalisis packet capture yang ada di lampiran, sebutkan TCP source port yang digunakan saat :

Diakses pada May 14, 2022 18:42:09.457360000 SE Asia Standard Time dan Alamat yang diakses <http://180.214.246.108:8000/login> (<http://180.214.246.108:8000/login>)

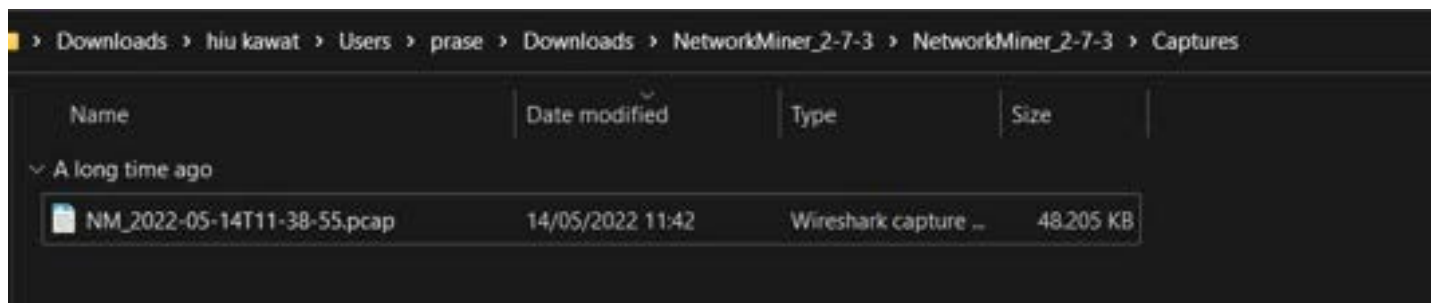
Recon

Diberikan beberapa file, dan ada 1 file berupa file .7z dan bisa diekstrak

 NM_2022-05-14T11-38-55.7z.002	12/04/2023 23:16	002 File	5.120 KB
 NM_2022-05-14T11-38-55.7z.005	12/04/2023 23:16	005 File	5.120 KB
 NM_2022-05-14T11-38-55.7z.003	12/04/2023 23:16	003 File	5.120 KB
 NM_2022-05-14T11-38-55.7z.004	12/04/2023 23:16	004 File	5.120 KB
 NM_2022-05-14T11-38-55.7z.006	12/04/2023 23:16	006 File	5.120 KB
 NM_2022-05-14T11-38-55.7z.007	12/04/2023 23:16	007 File	5.120 KB
 NM_2022-05-14T11-38-55.7z.001	12/04/2023 23:16	WinRAR archive	5.120 KB
 NM_2022-05-14T11-38-55.7z.008	12/04/2023 23:16	008 File	1.528 KB

Solve

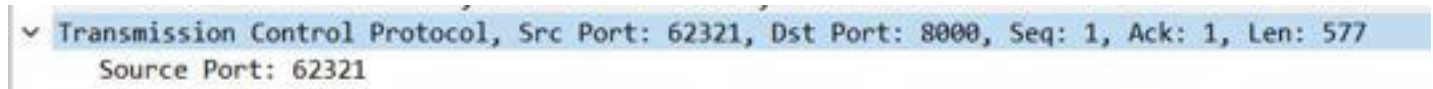
Langsung ekstrak file tersebut, dan hasilnya adalah sebuah folder, dan kita mengeceknya nanti akan ketemu dengan file **.pcap**



Langsung buka dengan wireshark, dan sesuai dengan deskripsi harus mencari **TCP Source Port** yang sesuai. Pertama langsung filter dengan protocol **http**, lalu mencari path **/login** dengan waktu dan tanggal yang sesuai

56804	2022-05-14 18:42:09.457360000	180.214.246.108	192.168.10.11	HTTP	5/ Continuation
56816	2022-05-14 18:42:09.457360000	192.168.10.11	180.214.246.108	HTTP	617 GET /login HTTP/1.1
56872	2022-05-14 18:42:09.707211000	192.168.10.11	180.214.246.108	HTTP	506 GET /events HTTP/1.1

Dan menemukan hasil yang sesuai, langsung saja cek TCP Source Port nya dengan cara klik 2 kali dan cek pada Transmission Protocol



Bisa dilihat source port nya adalah **62321**, ini adalah port yang sesuai

Flag

flag{62321}

Object

Description

ambil file mu di 2lyhefzbt4kep6wpzwuloshnetuzrfbpjlnpnmq4cfdh4diz7xivsad.onion/export

Recon

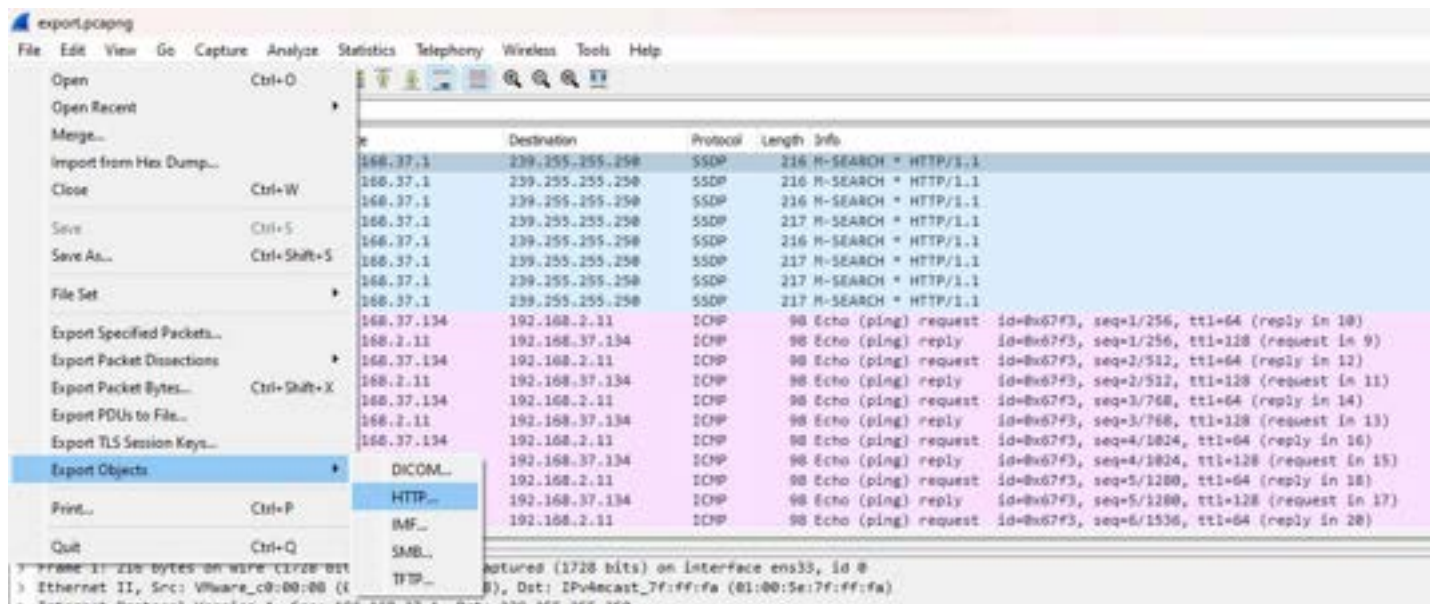
Diberikan sebuah soal dan juga sebuah link dengan domain mengandung **.onion**, kita bisa menggunakan **Tor Browser** untuk menyelesaikan

Solve

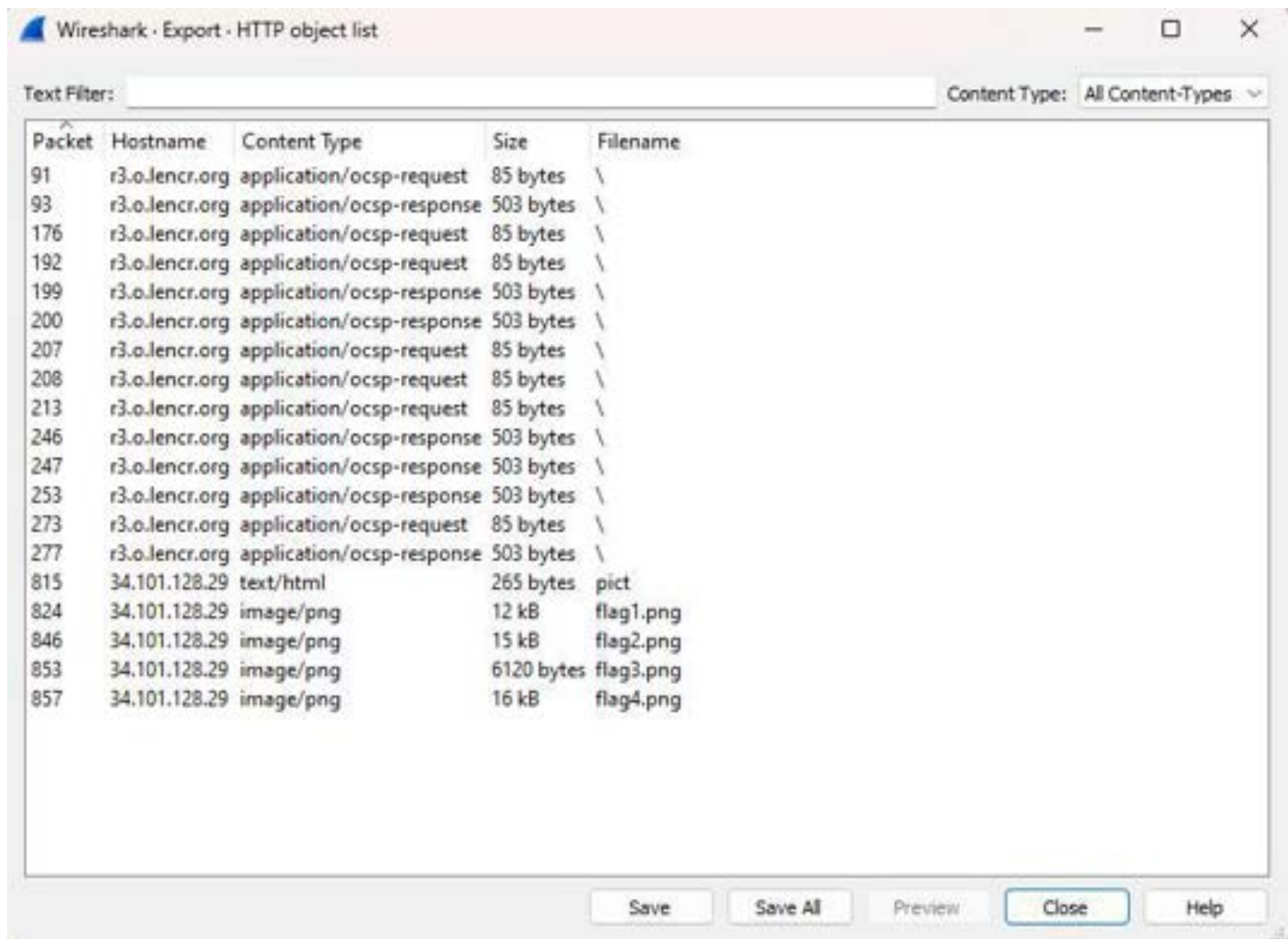
Ternyata link tersebut berisi file **export** dan kita download file nya



kita identifikasi apa file tersebut, ternyata sebuah file **pcapng**, langsung kita buka di Wireshark

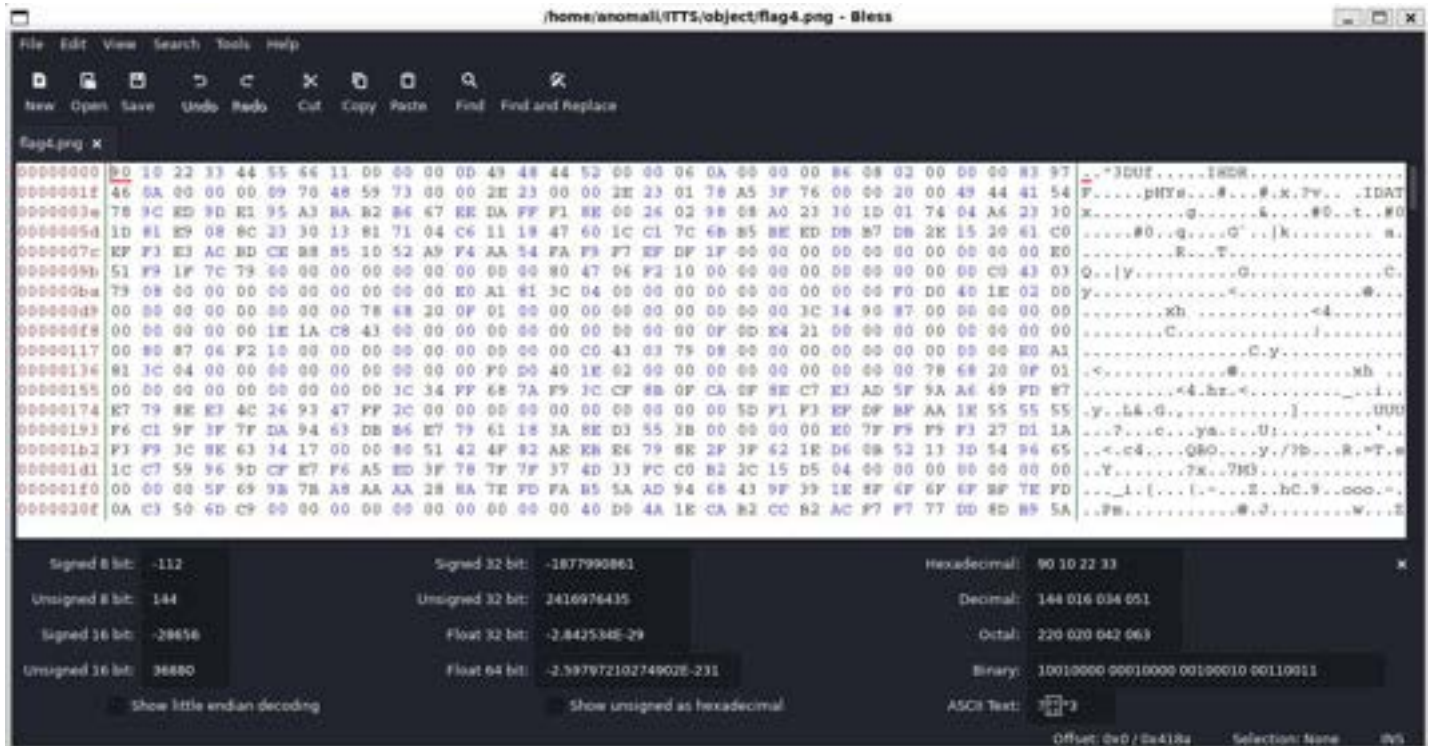


file tersebut berisi respon http yang mengandung file didalamnya, kita coba export object yang ada di protocol http



kita save file ke dalam computer kita flag1.png sampai flag4.png

saya curiga flag 1-3 itu decay saja, karena flag4 corrupt saya coba recover header file png tersebut dengan **bleess/hexedit**



Ternyata benar Header file png tersebut salah dan kita betulkan menggunakan https://en.wikipedia.org/wiki/List_of_file_signatures (https://en.wikipedia.org/wiki/List_of_file_signatures)

kita rubah dari 90 10 22 33 44 55 66 11 menjadi 89 50 4E 47 0D 0A 1A 0A

flag{3xp0rt_0bject_Wir3sh4rk}

betul saja setelah dibetulkan header nya kita temukan flagnya

Flag

flag{3xp0rt_0bject_Wir3sh4rk}

[Web Hacking]

Not Easy

Description

Masukkan jawabanmu di <http://180.214.246.108:9081/ssrf.php> (<http://180.214.246.108:9081/ssrf.php>)

Recon

Diberikan sebuah link website, sesuai yang ada dilink tersebut yaitu **ssrf.php** sepertinya website ini vulnerable terhadap **SSRF (Server Side Request Forgery)**

Solve

Ketika dibuka, web tersebut mengharuskan untuk submit sebuah url, karena ini adalah **SSRF** lalu mencoba untuk menggunakan website <https://webhook.site> (<https://webhook.site>) untuk mengcapture requestnya.

Tinggal submit saja url yang diberikan pada halaman <https://webhook.site> (<https://webhook.site>) tersebut. Dan setelah berhasil lihat hasilnya nya kembali di <https://webhook.site> (<https://webhook.site>)



Bisa dilihat flagnya ada di headaer **user-agent**

Flag

flag{penggunaan_URL_berbahaya_jika_tidak_dibatasi}

Bau Bawang

Description

Buka halamanmu di 21yhefzbt4kep6wpzwuloshnetuzrfbpjlnpnqmq4cfdh4diz7xivsad.onion/kmpstbs

Recon

Diberikan sebuah soal dan juga sebuah link dengan domain mengandung **.onion**, kita bisa menggunakan **Tor Browser** untuk menyelesaikan

Solve

Langsung saja buka link tersebut di Tor Browser, setelah terbuka langsung page source nya (ctrl + u). Pada bagian bawah akan ditemukan sesuatu

```
<!-- Template Main JS File -->
<script src="assets/js/main.js"></script>

<!-- Silahkan decode part per-part, jangan di gabung! -->
<!-- ini adalah flag (1/3) : ZmxhZ3tzMHVYyzNzXwo= -->
```

Itu adalah flag, tapi masih potongan, dan harus mencari potongan yang lainnya.

Setelah dicari potongan kedua ada di **assets/css/style.css**

```
/*-----
# Silahkan decode part per-part, jangan di gabung!
ini adalah flag (2/3) : ZDRsYW1fCg==
-----*/

#footer {
```

Dan flag yang terakhir ada di **assets/js/main.js**

```
/**
 * Silahkan decode part per-part, jangan di gabung!
 * ini adalah flag (3/3) : MW5zcDNjdH0=
 */
new PureCounter();
```

Setelah mendapatkan semuanya, jangan lupa didecode dengan **Base64**



Setelah itu gabungkan flagnya agar menjadi utuh

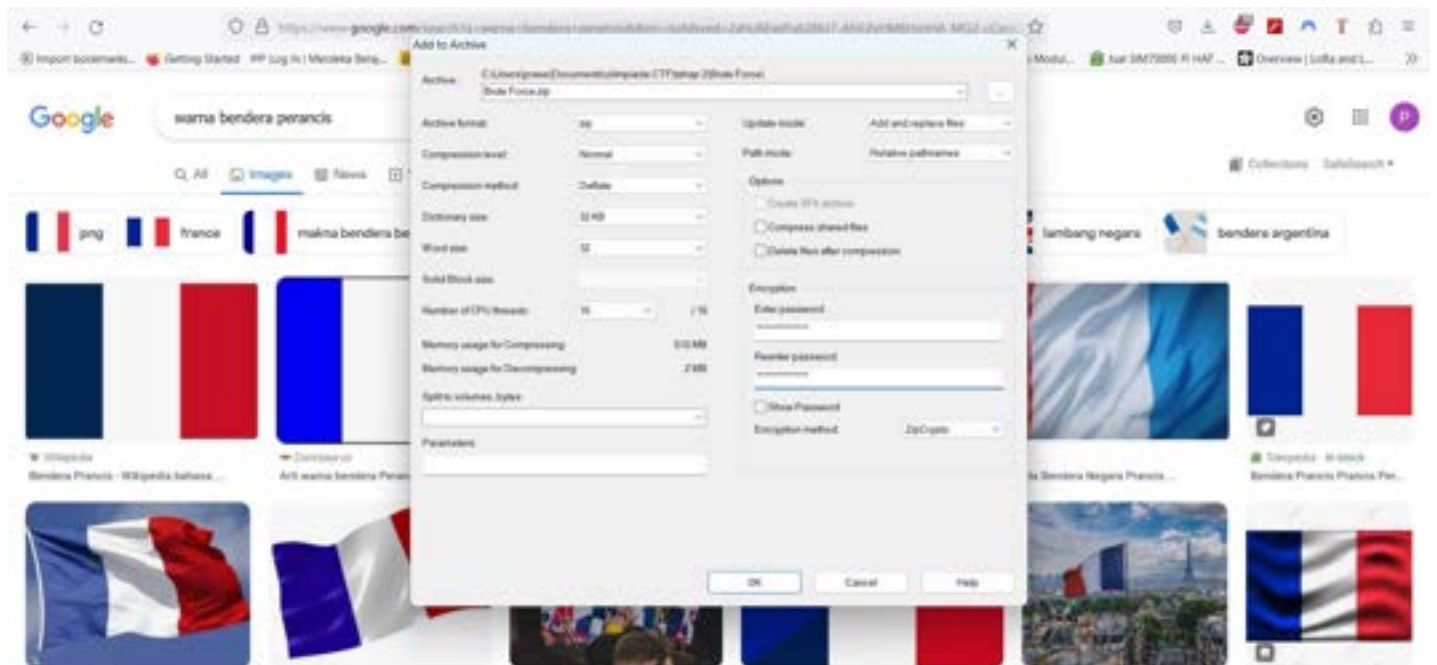
Flag

flag{s0urc3s_d4l4m_1nsp3ct}

[File Structure]

De(compress)

Description



Recon

Diberikan sebuah file Brute_Force.zip yang terkunci, kita harus bisa menebak password nya agar bisa melakukan extract file zip tersebut

Solve

Dari gambar yang ada dideskripsi ini bisa jadi clue passwordnya, hal yang mencurigakan adalah warna benderanya,
langsung mencoba passwordnya yaitu **biruputihmerah**

```

(root@sijastemba2202) - [~/itts/week2/decom]
# unzip Brute_Force.zip
Archive:  Brute_Force.zip
[Brute_Force.zip] Decompress me to find hint.txt password:
extracting: Decompress me to find hint.txt
inflating: flag.zip

(root@sijastemba2202) - [~/itts/week2/decom]
# ls
Brute_Force.zip  'Decompress me to find hint.txt'  flag.zip

```

Berhasil keluar 2 file, untuk file **flag.zip** masih terkunci. Saya curiga dengan file .txt nya itu bukanlah file .txt asli

```

(root@sijastemba2202) - [~/itts/week2/decom]
# file Decompress\ me\ to\ find\ hint.txt
Decompress me to find hint.txt: XZ compressed data, checksum CRC64

```

Dan benar sekali, itu adalah file **XZ**, lalu kami coba decompress, namun diubah dulu menjadi ekstensi yang sesuai

```

(root@sijastemba2202) - [~/itts/week2/decom]
# mv Decompress\ me\ to\ find\ hint.txt Decompress\ me\ to\ find\ hint.xz

(root@sijastemba2202) - [~/itts/week2/decom]
# xz -d Decompress\ me\ to\ find\ hint.xz

(root@sijastemba2202) - [~/itts/week2/decom]
# ls
Brute_Force.zip  'Decompress me to find hint'  flag.zip

(root@sijastemba2202) - [~/itts/week2/decom]
# file Decompress\ me\ to\ find\ hint
Decompress me to find hint: lzip compressed data, version: 1

```

Berhasil, namun lagi - lagi, yang dihasilkan adalah file compress data, dan akan terus seperti itu sampe menemukan file ASCII. Jadi berikut screenshot hingga ketemu file ASCII


```

(root@siyastemba2202) - [~/itts/week2/decom]
# file Decompress\ me\ to\ find\ hint
Decompress me to find hint: lzip-compressed data, version 1

(root@siyastemba2202) - [~/itts/week2/decom]
# mv Decompress\ me\ to\ find\ hint Decompress\ me\ to\ find\ hint.lzip

(root@siyastemba2202) - [~/itts/week2/decom]
# lzip -d Decompress\ me\ to\ find\ hint.lzip

(root@siyastemba2202) - [~/itts/week2/decom]
# ls
Brute_Force.zip 'Decompress me to find hint.lzip.out' flag.zip

(root@siyastemba2202) - [~/itts/week2/decom]
# file Decompress\ me\ to\ find\ hint.lzip.out
Decompress me to find hint.lzip.out: gzip compressed data, was "wordlist.txt", last modified: Tue Feb 14 02:11:03 2023, from Unix, original size modulo 2^32 272

(root@siyastemba2202) - [~/itts/week2/decom]
# mv Decompress\ me\ to\ find\ hint.lzip.out Decompress\ me\ to\ find\ hint.gz

(root@siyastemba2202) - [~/itts/week2/decom]
# gzip -d Decompress\ me\ to\ find\ hint.gz

(root@siyastemba2202) - [~/itts/week2/decom]
# ls
Brute_Force.zip 'Decompress me to find hint' flag.zip

(root@siyastemba2202) - [~/itts/week2/decom]
# file Decompress\ me\ to\ find\ hint
Decompress me to find hint: bzip2 compressed data, block size = 900k

(root@siyastemba2202) - [~/itts/week2/decom]
# mv Decompress\ me\ to\ find\ hint Decompress\ me\ to\ find\ hint.bz2

(root@siyastemba2202) - [~/itts/week2/decom]
# bzip2 -d Decompress\ me\ to\ find\ hint.bz2

(root@siyastemba2202) - [~/itts/week2/decom]
# ls
Brute_Force.zip 'Decompress me to find hint' flag.zip

(root@siyastemba2202) - [~/itts/week2/decom]
# file Decompress\ me\ to\ find\ hint
Decompress me to find hint: ASCII text

(root@siyastemba2202) - [~/itts/week2/decom]
# cat Decompress\ me\ to\ find\ hint
123456
password
12345678
1234
pussy
12345
dragon

```

Dan berhasil mendapatkan ASCII code yang berupa wordlists, kemudian dari sini langsung gunakan untuk melakukan crack file flag.zip nya menggunakan **fcrackzip**

```
(root@sijastemba2202) - [~/itts/week2/decom]
# fcrackzip -u -D -p ./Decompress\ me\ to\ find\ hint flag.zip

PASSWORD FOUND!!!!: pw == gunakaniniya
```

Berhasil dapat passwordnya yaitu **gunakaniniya**, langsung saja gunakan untuk mengekstrak file **flag.zip**

```
(root@sijastemba2202) - [~/itts/week2/decom]
# unzip flag.zip
Archive:  flag.zip
[flag.zip] flag.txt password:
  inflating: flag.txt

(root@sijastemba2202) - [~/itts/week2/decom]
# cat flag.txt
flag{f1l3_typ3s_3asy}

(root@sijastemba2202) - [~/itts/week2/decom]
#
```

Dapat flagnya

Flag

flag{f1l3_typ3s_3asy}

[Application Service]

DNS pt. 1

Description

Ambil filemu di ftp://01100111+10010010+10110110+11100011
(ftp://01100111+10010010+10110110+11100011)

Recon

Diberikan sebuah alamat ftp, namun itu adalah angka binary, jadi harus diubah dulu menjadi angka decimal biasa

```
(root@sijastemba2202) - [~/itts/week2]
# python3
Python 3.11.2 (main, Feb 12 2023, 00:48:52) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0b01100111
103
>>> 0b10010010
146
>>> 0b10110110
182
>>> 0b11100011
227
>>> █
```

Berarti alamatnya adalah ftp://103.146.182.227 (ftp://103.146.182.227)

Solve

Langsung saja kita masuk ke ftp tersebut, karena tidak diberikan user untuk masuk, saya coba masuk dengan ftp cli menggunakan user anonymous dan password kosong

```
(root@sijastemba2202) - [~/itts/week2]
# ftp 103.146.182.227
Connected to 103.146.182.227.
220 (vsFTPD 2.3.4)
Name (103.146.182.227:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Langsung cek file nya

```
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||9105|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 1095 Apr 10 05:01 DNS pt. 1
-rw-r--r-- 1 0 0 799 Apr 10 05:11 DNS pt. 2
-rw-r--r-- 1 0 0 0 Apr 10 04:37 Hax0r
226 Directory send OK.
ftp> █
```

Ada file DNS pt. 1, langsung kami get dan buka filenya

```

226 Directory send OK.
ftp> get DNS\ pt.\ 1
local: DNS pt. 1 remote: DNS pt. 1
229 Entering Extended Passive Mode (|||38976|).
150 Opening BINARY mode data connection for DNS pt. 1 (1095 bytes).
100% |*****
226 Transfer complete.
1095 bytes received in 00:00 (40.03 KiB/s)
ftp> exit
221 Goodbye.

```

```

(root@aljaanba2202) (~/.lstra/week2)
# cat DNS\ pt.\ 1
*****

# dig id.

; <<> BIND 9.16.1-Ubuntu <<> id.
;; global options: +cmd
;; Got answer:
;;->HEADER<-> opcode: QUERY, status: NOERROR, id: 39238
;; flags: qr rd ra ad: QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0, flags: udp: 1232
;; QUESTION SECTION:
;id. IN A

;; AUTHORITY SECTION:
id. 66400 IN DCA b.dns.id. hostmaster.pandi.id. 202208151 28800 7200 604800 172800

;; Query time: 184 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Thu Mar 09 03:04:27 UTC 2023
;; MSG SIZE rcvd: 90

68 97 114 105 32 105 110 102 111 114 109 97 115 105 32 100 105 32 97 116 97 115 32 100 105 32 107 101 116 97 104 117 105 32 98 97 104 119 97 32 119 97 107 116 117 32 121 97 110 103 32 100 105 32
116 117 32 121 97 110 103 32 100 105 32 112 101 114 108 117 107 97 110 32 115 101 114 118 101 114 32 117 110 116 117 107 32 109 101 114 101 115 112 111 1
10 32 112 101 114 109 105 110 116 97 110 32 113 117 101 114 121 32 65 110 100 97 32 97 100 97 108 97 104 32 46 46 46

```

Terlihat dibagian bawah ada sebuah angka, asumsinya adalah ASCII Code, langsung saja dekripsi angka tersebut

Recipe

From Charcode

Delimiter

Space

Base

10

Input

```

68 97 114 105 32 105 110 102 111 114 109 97 115 105 32 100 105 32 97 116 97 115 32 100 105 32 107
101 116 97 104 117 105 32 98 97 104 119 97 32 119 97 107 116 117 32 121 97 110 103 32 100 105 32
112 101 114 108 117 107 97 110 32 115 101 114 118 101 114 32 117 110 116 117 107 32 109 101 114
101 115 112 111 110 32 112 101 114 109 105 110 116 97 110 32 113 117 101 114 121 32 65 110 100 97
32 97 100 97 108 97 104 32 46 46 46

```

Output

Dari informasi di atas di ketahui bahwa waktu yang di perlukan server untuk merespon permintan query Anda adalah ...

Hasilnya adalah pertanyaan, langsung saja dijawab sesuai isi log file tadi

```
;; Query time: 184 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Thu Mar 09 03:04:27 UTC 2023
;; MSG SIZE rcvd: 90
```

Pada bagian query time terlihat ada value **184 msec**, berarti itu adalah jawaban yang valid

Flag

flag{184}

DNS pt. 2

Deskripsi

Ambil filemu di ftp://01100111+10010010+10110110+11100011

(ftp://01100111+10010010+10110110+11100011)

Recon

Langkah awal sama dengan soal **DNS pt. 1**, ip yang digunakan pun juga sama

Solve

Ketika berhasil masuk ke ftp nya, ada file **DNS pt. 2** langsung get lalu lihat isinya


```
Using binary mode to transfer files.
ftp> get DNS\ pt.\ 2
local: DNS pt. 2 remote: DNS pt. 2
229 Entering Extended Passive Mode (||||18599|).
150 Opening BINARY mode data connection for DNS pt. 2 (799 bytes).
100% |*****| 799
226 Transfer complete.
799 bytes received in 00:00 (30.20 KiB/s)
ftp> exit
221 Goodbye.

(root@siyastamba2202) - [~/1ttt/week2]
# cat DNS\ pt.\ 2
dig NS id.

Hasil yang di peroleh adalah,

; <<>> Dig 9.18.1-lubuntu1.3-Ubuntu <<>> NS id.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61486
;; flags: qr rd ra: QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

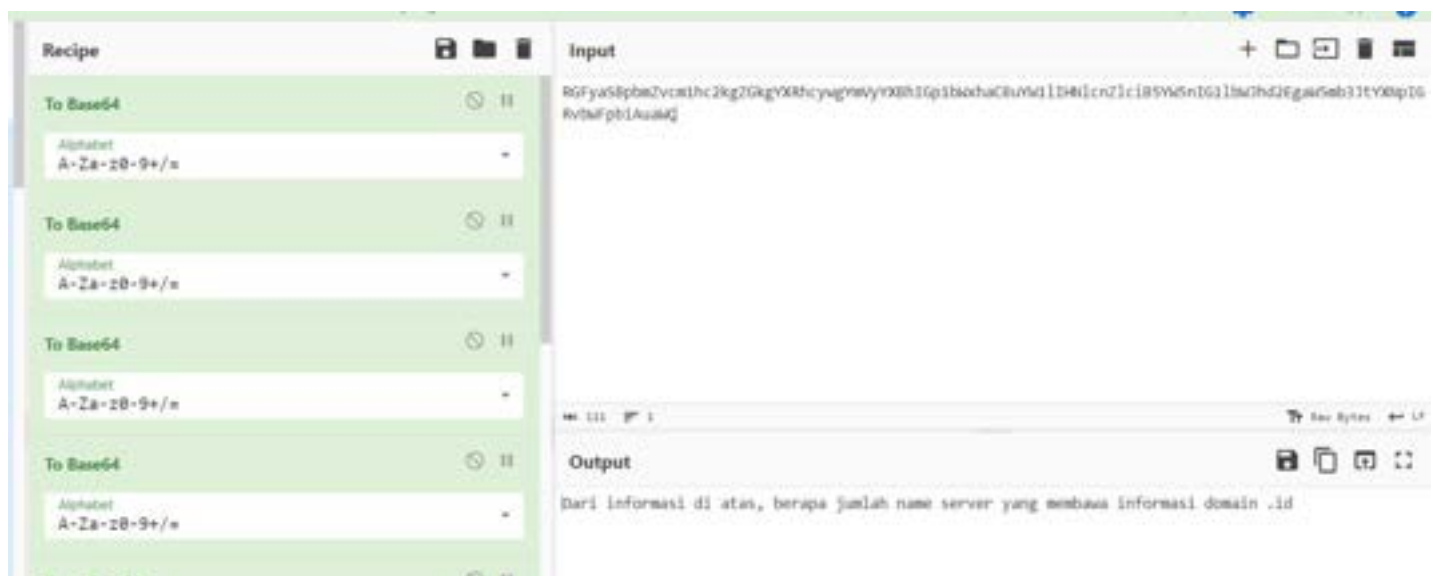
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
;; QUESTION SECTION:
;id.                IN      NS

;; ANSWER SECTION:
id.                7139    IN      NS      d.dns.id.
id.                7139    IN      NS      c.dns.id.
id.                7139    IN      NS      b.dns.id.
id.                7139    IN      NS      ns4.apnic.net.
id.                7139    IN      NS      e.dns.id.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Feb 18 09:31:39 WIB 2023
;; MSG SIZE rcvd: 126

RGFyaSBpbmZvcmlhc2kgZGkgYXRoYyYXBiIGp1bW9kaCBuYXN1IHBlcnRlc1B5YW5nIG1lbWJhd2EgaW5mb3J0YXNpIGRvdWVpbiAuaWQ/
```

Ada sebuah teks dibagian bawah, sepertinya itu adalah **Base64**, langsung saja didecode



Ternyata **Base64** nya sangat sangat dalam, dan harus dilakukan beberapa kali decode untuk mendapatkan plaintext nya.

Hasilnya adalah pertanyaan, langsung saja dijawab sesuai dengan hasil log nya

```
;; ANSWER SECTION:
```

```
id.          7139      IN       NS       d.dns.id.  
id.          7139      IN       NS       c.dns.id.  
id.          7139      IN       NS       b.dns.id.  
id.          7139      IN       NS       ns4.apnic.net.  
id.          7139      IN       NS       e.dns.id.
```

Jika dilihat nameserver dengan domain **.id** hanya ada 4 saja, berarti jawabannya adalah 4

Flag

flag{4}