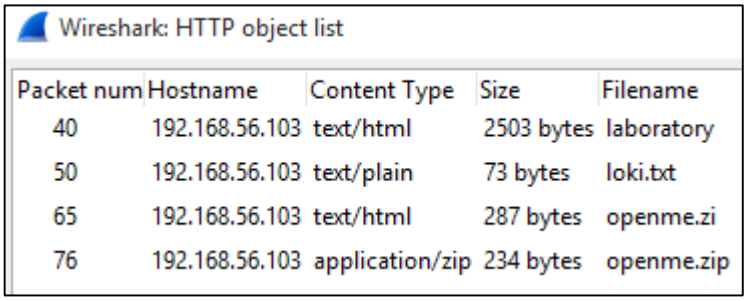
TENESYS

"FINAL ITOBAFEST 2017"

Universitas Teknokrat Indonesia

1. Archive - 75

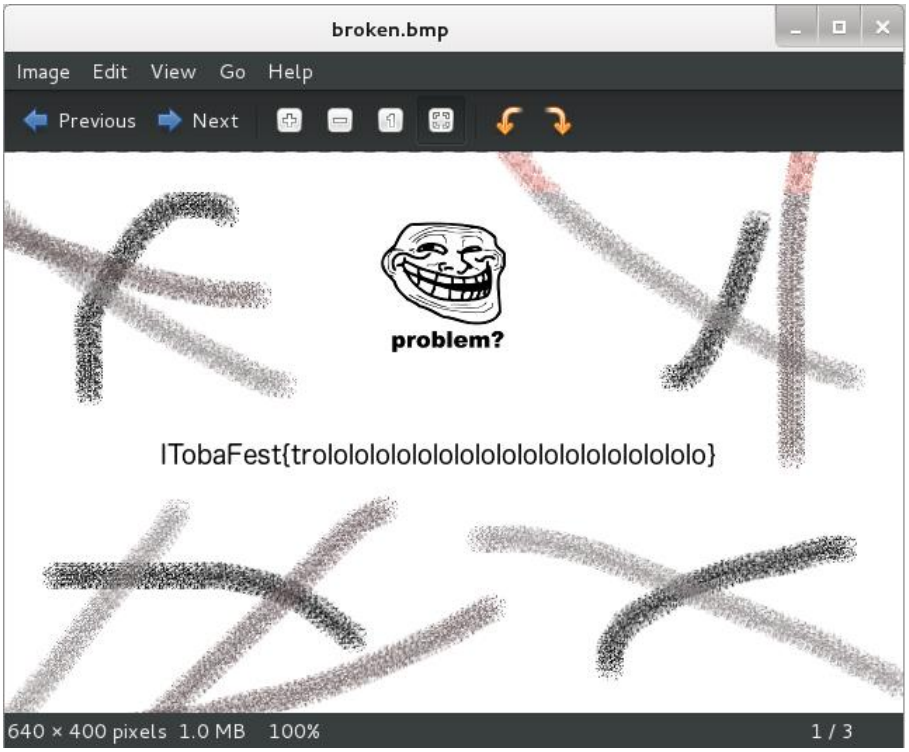
- Didapat sebuah file *network trafic* dan kami buka menggunakan aplikasi *Wireshark*.
- Langkah awal kami langsung melihat apakah ada file mencurigakan yang dikirim pada jaringan tersebut melalui *File > Export Objects > HTTP* maka akan tampak beberapa file mencurigakan, seperti berikut,



- Dua file mencurigakan terdapat pada file loki.txt dan openme.zip, dimana ternyata file openme.zip tersebut diberi password dan pasword terdapat pada file loki.txt, hanya saja password di encode kedalam bentuk *base64* yang harus di decode sebanyak 5x.
- Setelah dibuka maka akan terdapat flag adalah **ITobaFest{__just_carving_request__}**.

2. Broken BMP - 100

- Didapat sebuah file gambar berekstensi .bmp apabila dibuka menggunakan *Windows* gambar tersebut tidak akan ter-load, saat kami coba buka gambar tersebut di *Linux* ternyata gambar tersebut dapat ter-load (sudah gitu doang :S poinnya lumayan padahal) disertai sebuah flag seperti berikut,

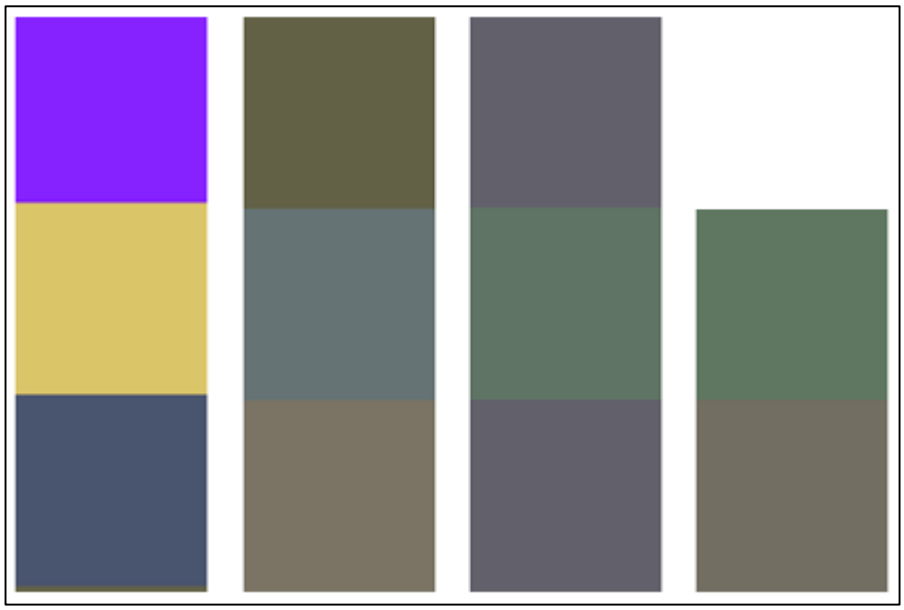


- Flag adalah **ITobaFest{trololololololololololololololololo}**.

MISCELLANEOUS

1. Color - 50

- Didapat sebuah file .html dimana setelah dibuka hanya menampilkan beberapa blok warna secara horisontal seperti berikut,



- Tidak ada hal khusus dari file ini karena misi yang diberikan langsung berupa file .html saja, begitupun pada *source code* yang hanya menampilkan beberapa baris kode html dan css, maka kami beranggapan satu-satunya yang mencurigakan adalah pada bagian baris css kode warna yang berupakan rangkaian dari bilangan heksa desimal, setelah dikumpulkan dan di decode akan terdapat beberapa *strings* sampah yang disertai dengan flag pada bagian akhir seperti berikut,

```
>>> "8621ffdbc56949546f6261466573747b746562616b5f746562616b5f7761726e61".decode('hex')
'\x86!\xff\xdb\xc5iITobaFest{tebak_tebak_warna'
```

- Flag adalah **ITobaFest{tebak_tebak_warna}**.

2. Acar - 50

- Didapat beberapa *strings* aneh pada misi ini, kami sendiri pun bingung harus “ngapain” sampai akhirnya panitia memberikan beberapa clue (lupa :D),

```
(lp0 S'p' p1 aS'r' p2 aS'o' p3 aS't' p4 ag3 aS'n' p5 aS'_' p6 aS'e'
p7 aS'a' p8 ag2 ag4 aS'h' p9 ag6 aS'k' p10 ag2 aS'y' p11 ag1
ag4 ag3 ag5 ag6 ag1 aS'i' p12 aS'c' p13 ag10 aS'l' p14 ag7 ag6
ag12 aS's' p15 ag6 ag8 ag13 ag8 ag2 ag6 aS'm' p16 ag7 ag5
ag4 ag12 ag16 aS'u' p17 ag5 a.
```

- Agar lebih mudah menganalisis kami susun menjadi seperti berikut,

```
(lp0
aS'p' p1
aS'r' p2
aS'o' p3
aS't' p4  ag3
aS'n' p5
aS'_' p6
aS'e' p7
aS'a' p8  ag2 ag4
aS'h' p9  ag6
aS'k' p10 ag2
aS'y' p11 ag1 ag4 ag3 ag5 ag6 ag1
aS'i' p12
aS'c' p13 ag10
aS'l' p14 ag7 ag6 ag12
aS's' p15 ag6 ag8 ag13 ag8 ag2 ag6
aS'm' p16 ag7 ag5 ag4 ag12 ag16
aS'u' p17 ag5
a.
```

- Kami coba memberikan istilah untuk beberapa huruf yang tersusun diatas menjadi seperti berikut,
  - **"aS"** adalah huruf yang digunakan untuk acuan penentuan huruf dalam flag.
  - **"p"** adalah huruf yang digunakan untuk penentuan posisi.
  - **"ag"** adalah huruf yang digunakan sebagai penentuan posisi setelah "**p"** sedangkan nilai dari **"ag"** sama dengan **"p"**.
  - Huruf pada bagian teratas dan terbawah abaikan saja.
- Sehingga apabila disusun huruf-per-huruf seperti *p1('p'), p2('r'), p3('o'), p4('t'), ag3=p3('o'), p5('n'), p6('_'), p7('e'), p8('a'), ag2=p2(r), ag4=p4('t'), p9('h'),* dan seterusnya maka akan didapat flag yaitu **ITobaFest{proton_earth_krypton_pickle_is_acar_mentimun}**.

3. WannaCry - 50

- Didapat sebuah file berekstensi .jpg dimana sebenarnya file tersebut adalah sebuah file program *ELF 64-bit*, setelah kami coba buka menggunakan aplikasi *IDA Pro* ternyata tidak terdapat apa-apa mengingat ini merupakan misi kategori *Miscellaneous*.
- Setelah kami cek file tersebut menggunakan *Binwalk* ternyata terdapat file zip yang bernama "a.wnry".

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             ELF 64-bit LSB shared object, AMD x86-64, version
1 (SYSV)
7312          0x1C90          LZMA compressed data, properties: 0x8A, dictionary
 size: 16777216 bytes, uncompressed size: 100663296 bytes
8016          0x1F50          LZMA compressed data, properties: 0x93, dictionary
 size: 16777216 bytes, uncompressed size: 50331648 bytes
8464          0x2110          Zip encrypted archive data, at least v2.0 to extra
ct, compressed size: 45,  uncompressed size: 36, name: "a.wnry"
8665          0x21D9          End of Zip archive
```

- Setelah di ekstrak file tersebut meminta sebuah password dan bisa didapat hanya dengan melakukan strings saja, maka akan mendapatkan strings berupa "WNcry@2oH" dimana huruf "H" pada strings tersebut hanya sebuah pengecoh saja, kami coba submit password tersebut ternyata salah, lalu kami coba dengan menambahkan huruf "l7" sehingga menjadi "Wncry2ol7" dan bumz password benar.
- Buka file hasil ekstrak dan didapatlah flag yaitu **ITobaFest{wanna_cry_wanna_get_girl}**.

1. WarmUp - 150

- Didapat sebuah file program *ELF 64-bit*, apabila program tersebut di running di linux, maka akan menampilkan strings *"push"* dan *"up"* sampai 40000000011000 dengan jeda 1 detik per strings.
- Kami coba analisa prgoram tersebut menggunakan *IDA Pro*, dan coba membuka fungsi sub_7C0.
- Beberapa hal yang kita dapat ketahui bahwa:
  - Strings flag berjumlah 30 karakter.
  - Format flag adalah "ITobaFest{}".
  - Flag dihasilkan dari operasi *xor* dengan variable "i".
  - Setiap 2 karakter di *xor* dengan nilai yang sama.
  - Flag akan muncul apabila program sudah menampilkan strings *"push"* dan *"up"* hingga ke 40000000011000.
- Pembuktian bahwa tiap 2 karakter di *xor* dengan nilai yang sama yaitu,

```
>>> 2545 ^ ord('I') == 2540 ^ ord('T')
True
>>> 2735 ^ ord('o') == 2722 ^ ord('b')
True
>>>
```

- Dari cara diatas kami hanya mendapatkan strings **ITobaFest{ ?}**.
- Untuk mendapatkan beberapa strings yang lain, kami mencoba melakukan bruteforce terhadap flag.

```
import sys
flag = [2545,2540,2735,2722,3481,3518,3685,3699,316,307,610,626,679,663,612,
623,775,813,607,613,942,957,622,607,804,801,614,628,759,693]
flag_dec = "ITobaFest{"
for a in range(1,4000):
    if flag[10]^a >94 and flag[10]^a <123 and flag[11]^a >94 and flag[11]^a
    <123:
        for b in range(1,4000):
            if flag[12]^b >94 and flag[12]^b <123 and flag[13]^b >94 and
            flag[13]^b <123:
                for c in range(1,4000):
                    if flag[14]^c >94 and flag[14]^c <123 and flag[15]^c >94
                     and flag[15]^c <123:
                        for d in range(1,4000):
                            if flag[16]^d >94 and flag[16]^d <123 and flag[
                            17]^d >94 and flag[17]^d <123:
                                for e in range(1,4000):
                                    if flag[18]^e >94 and flag[19]^e <123
                                    and flag[19]^e >94 and flag[19]^e <123:
                                        sys.stdout.write(flag_dec+chr(flag[
                                        10]^a)+chr(flag[11]^a)+chr(flag[12]^
                                        b)+chr(flag[13]^b)+chr(flag[14]^c)+
                                        chr(flag[15]^c)+chr(flag[16]^d)+chr(
                                        flag[17]^d)+chr(flag[18]^e)+chr(flag
                                        [19]^e))
                                        print ""
```

- Didapatlah strings seperti berikut,

```
1   ITobaFest{bro_do_u_e
2   ITobaFest{bro_do_ue_
3   ITobaFest{bro_dou__e
4   ITobaFest{bro_dou_e_
5   ITobaFest{bro_en_u_e
6   ITobaFest{bro_en_ue_
7   ITobaFest{bro_enu__e
8   ITobaFest{bro_enu_e_
9   ITobaFest{bro_fm_u_e
0   ITobaFest{bro_fm_ue_
1   ITobaFest{bro_fmu__e
2   ITobaFest{bro_fmu_e_
3   ITobaFest{bro_gl_u_e
4   ITobaFest{bro_gl_ue_
5   ITobaFest{bro_glu__e
```

- Pada tahap pertama brute kami mendapatkan strings yang kemungkinan adalah flagnya yaitu **ITobaFest{bro_do_u_e**,

```
import sys
flag = [2545,2540,2735,2722,3481,3518,3685,3699,316,307,610,626,679,663,612,
623,775,813,607,613,942,957,622,607,804,801,614,628,759,693]
flag_dec = "ITobaFest{bro_do_u_e"
for a in range(1,4000):
    if flag[20]^a >94 and flag[20]^a <123 and flag[21]^a >94 and flag[21]^a
    <123:
        for b in range(1,4000):
            if flag[22]^b >94 and flag[22]^b <123 and flag[23]^b >94 and
            flag[23]^b <123:
                for c in range(1,4000):
                    if flag[24]^c >94 and flag[24]^c <123 and flag[25]^c >94
                     and flag[25]^c <123:
                        for d in range(1,4000):
                            if flag[26]^d >94 and flag[26]^d <123 and flag[
                            27]^d >94 and flag[27]^d <123:
                                sys.stdout.write(flag_dec+chr(flag[20]^a)+
                                chr(flag[21]^a)+chr(flag[22]^b)+chr(flag[23
                                ]^b)+chr(flag[24]^c)+chr(flag[25]^c)+chr(
                                flag[26]^d)+chr(flag[27]^d))
                                print ""
```

- Didapatlah strings seperti berikut,

```
14959   ITobaFest{bro_do_u_even_cfxj
14960   ITobaFest{bro_do_u_even_cfyk
14961   ITobaFest{bro_do_u_even_lift
14962   ITobaFest{bro_do_u_even_ligu
14963   ITobaFest{bro_do_u_even_lidv
14964   ITobaFest{bro_do_u_even_liew
```

- Lalu kami mencari strings yang kemungkinan adalah flagnya, didapatlah sebuah strings yang merupakan flag yaitu **ITobaFest{bro_do_u_even_lift?}.**