






TENESYS

The logo features the word "TENESYS" in a bold, cyan, sans-serif typeface. The letter "T" is uniquely designed with a horizontal bar extending to the left and a vertical stem that continues downwards as a thick line. To the right of the "T", there are two additional thick vertical cyan lines of varying heights, with the taller one positioned behind the word. The entire graphic is set against a solid black background.

– Easy –

<https://codefest-ctf-18.slack.com/>

-  Pinned by @cb1711
-  **cb1711** 7:31 PM
- flag for Freebies CodefestCTF{Phr33B13\$ R L0\3}
-  11

- Dan didapatkan flag : **CodefestCTF{Phr33B13\$ R L0\3}**

– Medium –

download file here

<https://drive.google.com/file/d/10O4w6rtsUiCspM94qdXqvHeTj-4O0RfX/view?usp=sharing>

Output Format

CodefestCTF{flag}

- ```

00000000 A0 D8 FF BE 00 00 44 66 48 46 00 01 01 01 00 F0 0x...DEHF.....8
00000010 00 F0 00 00 FF FE 00 18 41 75 74 68 6F 72 3A 20 .6..yp..Author:
00000020 55 74 73 61 76 20 4B 72 69 73 68 6E 61 6E FF E2 Utsav Krishnanya
00000030 02 40 49 43 43 5F 50 52 4F 46 49 4C 45 01 01 .@CC_PROFILE.....
00000040 00 00 02 30 41 44 42 45 02 10 00 00 6D 6E 74 72 ...0ADBE...mntnr
00000050 52 47 42 20 58 59 5A 20 07 CF 00 06 03 00 00 RGB XYZ .i.....
00000060 00 00 00 00 61 63 73 70 41 50 50 4C 00 00 00 .acspAPPL.....
00000070 6E 6F 6E 65 00 00 00 00 00 00 00 00 00 00 none.....
00000080 00 00 00 00 F6 D6 00 01 00 00 00 00 D3 2D80.....0-
00000090 41 44 42 45 00 00 00 00 00 00 00 00 00 00 ADBE.....
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000B0 00 00 00 00 0A 63 70 72 74 00 00 00 00 00
000000C0 00 00 00 0A 63 70 72 74 00 00 FC 00 00 00 32cprt...d...2
000000D0 64 65 73 63 00 01 30 00 00 6B 77 74 70 74 desc...0..kwpt
000000E0 00 00 01 9C 00 00 14 62 6B 70 74 00 00 01 B0 ...x...bkpt...°
000000F0 00 00 14 72 54 52 43 00 01 C4 00 00 00 0EtRRC...A...
00000100 67 54 52 43 00 01 D4 00 00 E2 54 52 43 gTRC...0...bTRC
00000110 00 00 01 E4 00 00 0E 72 58 59 5A 00 01 F4 ...ä...xXYZ...ö
00000120 00 00 00 14 67 58 59 5A 00 02 08 00 00 14 ...gXYZ.....
00000130 62 58 59 5A 00 02 1C 00 00 14 65 78 74 bXYZ.....text
00000140 00 00 00 00 43 6F 70 79 72 69 67 68 74 31 39Copyright 19
00000150 39 39 20 41 61 6F 62 65 20 53 79 73 65 6D 73 99 Adobe Systems
00000160 20 49 6E 63 6F 72 70 6F 72 61 74 65 64 00 00 Incorporated...
00000170 64 65 73 63 00 00 00 00 00 00 11 41 6F 62 desc.....Adob
00000180 65 20 52 47 42 20 28 31 39 38 28 00 00 00 .e_BGR_(1998)

```

- Karena terdapat RGB, author dan extension mirip dengan JPG lalu saya ubah extension menjadi jpg

```

FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 F0 00 F0 00 00 FF FE 00 18 41 75 74 68 6F 72 3A 20 55 74 73 61 76 20 4B 72 69 73 68 6E 61 6E FF E2 02 40 49 43 43 5F 50 52 4F 46 49 4C 45 00 01 01 00 00 02 30 41 44 42 45 02 10 00 00 6D 6E 74 72
G0yà..JFIF.....8
.8..ÿþ..Author:
Utsav Krishnanyâ
.@ICC_PROFILE...
...0ADBE....mnr

```

- Hasilnya berupa gambar



- Dan didapatkan flag : **CodefestCTF{mAgic\_byTes}**

### 3. Thunder – 250

– Medium –

João was downloading a secret from the internet when it got struck by thunder, which led it to pieces. Help João in recovering the secret.

Captured Packet File

- thunder.pcap

<https://drive.google.com/file/d/1lzIAI4parDtVQ0AdGctZLbNpFedJ0uTJ/view?usp=sharing>

Output Format

**CodefestCTF{flag}**

- Didapatkan sebuah file pcap
- Lalu buka dengan Wireshark
- Terdapat File Image di protocol HTTP

```

HTTP 219 GET /flag.jpg HTTP/1.1
TCP 66 8000→45414 [ACK] Seq=1 Ack=154 Win
TCP 83 [TCP segment of a reassembled PDU]
TCP 66 45414→8000 [ACK] Seq=154 Ack=18 Wi
HTTP 340 HTTP/1.0 200 OK (JPEG JFIF image)

```

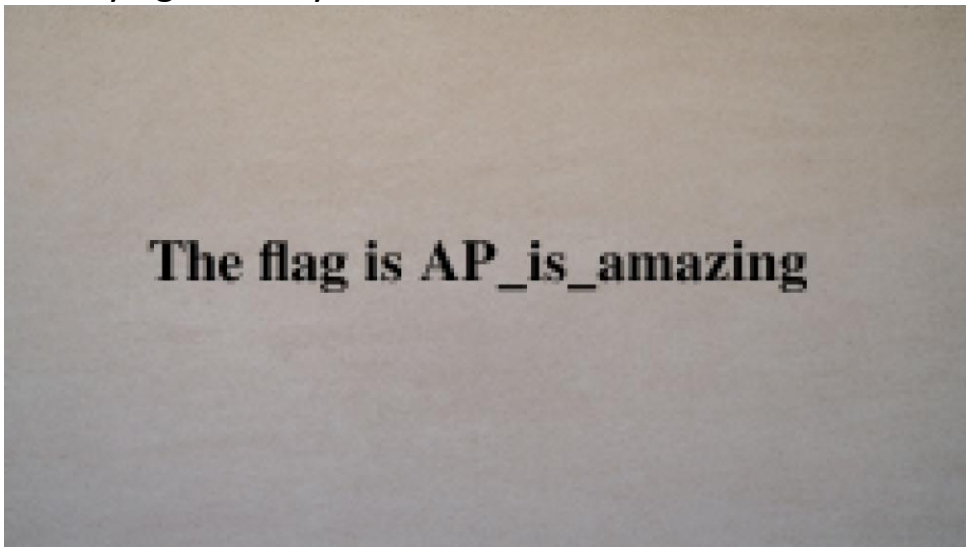
- Ku ambil file nya , File > Export Objects > HTTP dan di save semua

| Packet | Hostname           | Content Type | Size      | Filename |
|--------|--------------------|--------------|-----------|----------|
| 8      | 172.17.42.128:8000 | image/jpeg   | 101 bytes | flag.jpg |
| 20     | 172.17.42.128:8000 | image/jpeg   | 101 bytes | flag.jpg |
| 268    | 172.17.42.128:8000 | image/jpeg   | 139 kB    | flag.jpg |
| 456    | 172.17.42.128:8000 | image/jpeg   | 139 kB    | flag.jpg |
| 775    | 172.17.42.128:8000 | image/jpeg   | 174 kB    | flag.jpg |
| 999    | 172.17.42.128:8000 | image/jpeg   | 174 kB    | flag.jpg |
| 1223   | 172.17.42.128:8000 | image/jpeg   | 174 kB    | flag.jpg |
| 1374   | 172.17.42.128:8000 | image/jpeg   | 35 kB     | flag.jpg |
| 1456   | 172.17.42.128:8000 | image/jpeg   | 35 kB     | flag.jpg |
| 1798   | 172.17.42.128:8000 | image/jpeg   | 279 kB    | flag.jpg |
| 2132   | 172.17.42.128:8000 | image/jpeg   | 279 kB    | flag.jpg |
| 2467   | 172.17.42.128:8000 | image/jpeg   | 279 kB    | flag.jpg |
| 3072   | 172.17.42.128:8000 | image/jpeg   | 209 kB    | flag.jpg |
| 3279   | 172.17.42.128:8000 | image/jpeg   | 105 kB    | flag.jpg |
| 3439   | 172.17.42.128:8000 | image/jpeg   | 105 kB    | flag.jpg |
| 3591   | 172.17.42.128:8000 | image/jpeg   | 105 kB    | flag.jpg |
| 3899   | 172.17.42.128:8000 | image/jpeg   | 244 kB    | flag.jpg |
| 4360   | 172.17.42.128:8000 | image/jpeg   | 70 kB     | flag.jpg |
| 4475   | 172.17.42.128:8000 | image/jpeg   | 70 kB     | flag.jpg |

- Ternyata ku buka satu persatu tidak bisa dibuka dan di lihat extensionnya ternyata ini merupakan sebuah file gambar yang terpecah belah extensinya dan di dapatkan 2 file yang terpisah extensinya dan akhirnya saya satukan

```
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 00 00 00 00 FF E1 0E 54 45 78 69 66 00 00 49 49 2A 00 08 00 00 00 05 00 1A 01 05 00 01 00 00 00 *.....J.....R...4A 00 00 00 1B 01 05 00 01 00 00 00 52 00 00 00 (.1....OC 00 00 00 5A 00 00 00 32 01 02 00 14 00 00 00Z...2.....66 00 00 00 7A 00 00 00 48 00 00 00 01 00 00 00 f...z...H.....48 00 00 00 01 00 00 00 47 49 4D 50 20 32 2E 31 H.....GIMP 2.130 2E 30 00 32 30 31 38 3A 30 38 3A 32 34 20 32 0.0.2018:08:24 232 3A 31 35 3A 33 36 00 08 00 00 01 04 00 01 00 2:15:36.....00 00 00 01 00 00 01 01 04 00 01 00 00 00 90 00à.....00 00 02 01 03 00 03 00 00 00 E0 00 00 00 03 0103 00 01 00 00 00 06 00 00 00 06 01 03 00 01 0000 00 06 00 00 00 15 01 03 00 01 00 00 00 03 0000 00 01 02 04 00 01 00 00 00 E6 00 00 00 02 02æ.....04 00 01 00 00 00 65 0D 00 00 00 00 00 00 08 00e.....08 00 08 00 FF D8 FF E0 00 10 4A 46 49 46 00 01ÿøÿà..JFIF..01 00 00 01 00 01 00 00 FF DB 00 43 00 08 06 06ÿÛ.C...07 06 05 08 07 07 07 09 09 08 0A 0C 14 0D 0C 0B0B 0C 19 12 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 2024 2E 27 20 22 2C 23 1C 1C 28 37 29 2C 30 31 34 $. ' " , # . () , 01434 34 1F 27 39 3D 38 32 3C 2E 33 34 32 FF DB 00 44 . ' 9 = 8 2 < . 342ÿÛ.43 01 09 09 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 C.....2!..!32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 222222222222222232 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 222222222222222232 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 222222222222222232 32 FF C0 00 11 08 00 90 01 00 03 01 22 00 02 22ÿà.....".
```

- Hasilnya gambarnya



- Dan didapatkan flag : **CodefestCTF{AP\_is\_amazing}**