**Writeup HackToday 2019**

**Zer0Byte ID X SiapaYa?**

# 1001

**Rexy Fahrezi**

**Gayu Gumelar**

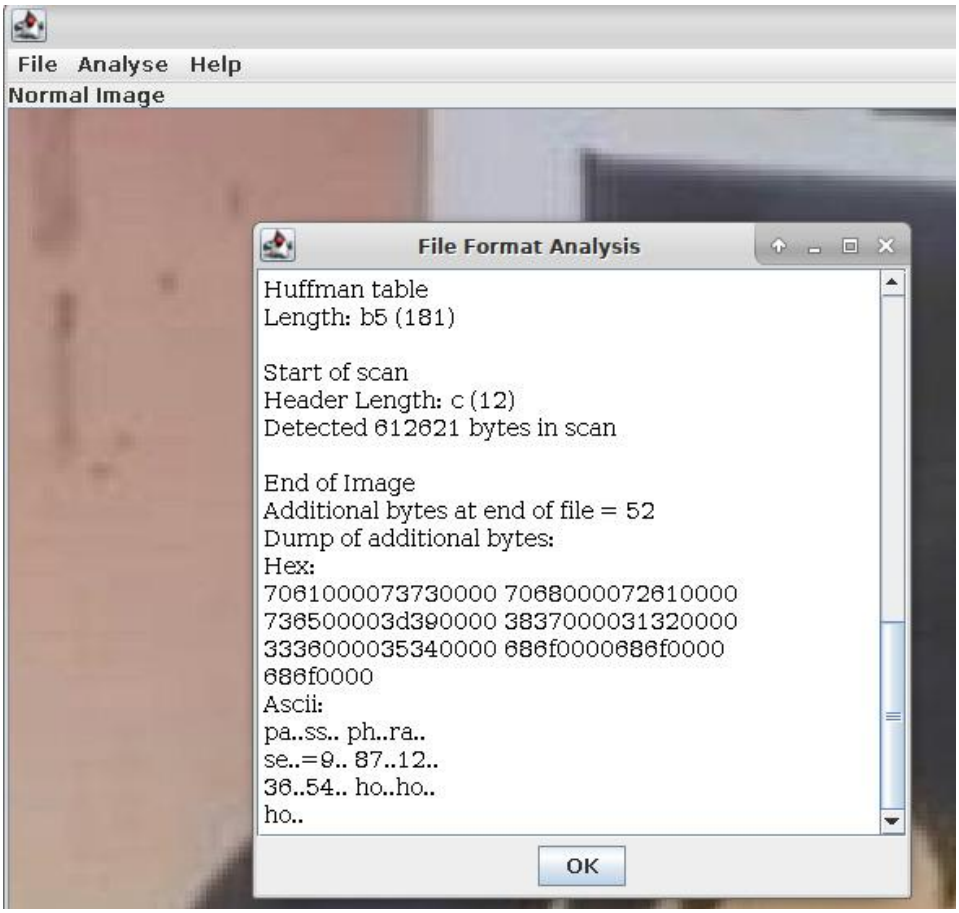
**M Hendro Junawarko**

**M Nurhasan Aprilian**

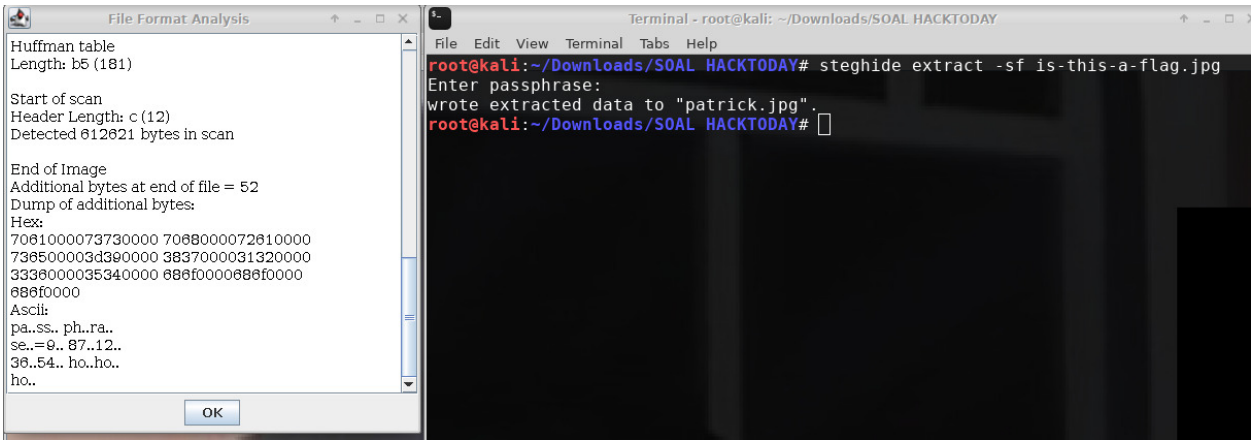
# # FORENSIC

## Know Your Flag

Diberikan sebuah file image, analisis dengan stegsolve pada file format analysis




Terdapat clue yaitu passphrase :**987123654hohoho** maka saya asumsikan terdapat file lagi di dalamnya. Saya coba extract dengan steghide



Kemudian saya analisis lagi file hasil dari steghide tadi, dengan exiftool.

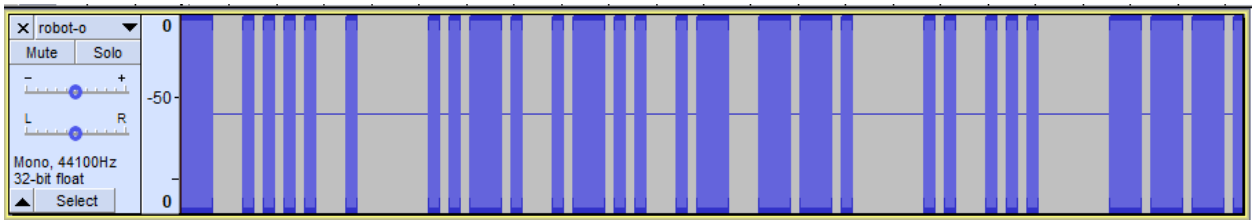
```
Comment                         : JJ2XG5BANNUWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYYLHHIQGQYLDNN2G6ZDBPF5V6NDMNRPWQNDJNRPV6NLUGM4WQ2LEMVPTC
ZJSG5RWKM35
```

Terdapat enkripsi dari base32, lakukan decode dengan python dan di dapatkan flag

```
>>> import base64
>>> data = 'JJ2XG5BANNUWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYYLHHIQGQYLDNN2G6ZDBPF5V6NDMNRPWQNDJNRPV6NLUGM4WQ2LEMVPTCZJSG5RWKM35'
>>> dcode = base64.b32decode(data)
>>> print dcode
Just kidding. Here's your flag: hacktoday{_4ll_h4il__5t39hide_1e27ce3}
```

## Robot o

Diberikan sebuah file berekstensi .voice , lalu saya coba untuk melihat waveform audionya dengan meng- import raw data dari audio tersebut menggunakan audacity




Bentuk waveformnya terlihat seperti morse code, setelah di decode, ternyata itu benar morse code, dan didapatkan flagnya.

Input:

```
_ .... .  ..-. .-.. .- --.  .. ...  ---.. .- . ---.. -.-. -.-. ----. ...-- . ..--- ..--- ...-- -.. .....
..-. ----. ..... --... -.-. . ---.. -... ----- --... ---.. -.. ..--- ----- ..--- ----- . --...
```

Output:

```
THEFLAGIS8AE8CC93E223D5F957CE8B078D2020E7
```

## Intro

Diberikan paket data berupa intro.pcapng yang memuat USB Streams.

Kemudian saya lakukan ekstraksi **usb.capdata** dengan bantuan **tshark**

```
root@kali:~/Downloads/SOAL HACKTODAY# tshark -r intro.pcapng -Y usb.capdata -Tfields -e usb.capdata | head
Running as user "root" and group "root". This could be dangerous.
00:00:09:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:15:00:00:00:00:00
00:00:15:0c:00:00:00:00
00:00:0c:00:00:00:00:00
00:00:16:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:0e:00:00:00:00:00
00:00:04:00:00:00:00:00
00:00:00:00:00:00:00:00
tshark: An error occurred while printing packets: Broken pipe.
root@kali:~/Downloads/SOAL HACKTODAY#
```

Lakukan penyimpanan hasil ekstraksi tadi kedalam file **capdata**

```
root@kali:~/Downloads/SOAL HACKTODAY# tshark -r introo.pcapng -Y usb.capdata -Tfields -e usb.capdata > capdata
Running as user "root" and group "root". This could be dangerous.
root@kali:~/Downloads/SOAL HACKTODAY#
```

Dilakukan pemetaan byte ke-2 terhadap **USB HID Scan codes** untuk mendapatkan key sequences. Berikut scriptnya

```
def usbHID(txt):
  dic = {
    'a' : '04', 'b' : '05', 'c' : '06', 'd' : '07', 'e' : '08',
    'f' : '09', 'g' : '0a', 'h' : '0b', 'i' : '0c', 'j' : '0d',
    'k' : '0e', 'l' : '0f', 'm' : '10', 'n' : '11', 'o' : '12',
    'p' : '13', 'q' : '14', 'r' : '15', 's' : '16', 't' : '17',
    'u' : '18', 'v' : '19', 'w' : '1a', 'x' : '1b', 'y' : '1c',
    'z' : '1d', '=' : '2e', '/' : '38', '{' : '2f', '}' : '30',
    '1' : '1e', '2' : '1f', '3' : '20', '4' : '21', '5' : '22',
    '6' : '23', '7' : '24', '8' : '25', '9' : '26', '0' : '27',
    '_' : '2d', ' ' : '2c', ':' : '33', ',' : '36', '/' : '38',
    '\n' : '58', '.' : '37'
  }
  dic = {dic[i] : i for i in dic}
  plain = ''.join(dic.get(i,'') for i in txt.split(':'))
  return plain

def decodeUSBHID():
  cap = open('capdata').read().rstrip('\r').split('\n')
  cap = [i.split(':')[2] for i in cap if i != '']
  return ''.join(usbHID(i) for i in cap)
```

Run dan di dapatkan flag

```
root@kali:~/Downloads/SOAL HACKTODAY# python testt.py
FRRISKA IIS THHE FAST SSECTIONION OOF THE CSSARDAS A HUNGARIAN FOLK DDANCCE OR OF MOOST OOF LISZT HUNNGGARIIAN RHAPSODIES WHICH TAKKETT
AKKE THEIR FRORM TTHIS DDANCCE THE FISRISKKA IS GGENERRALLY EITHER TURBULLENT OR JUBILANTT INN TONE GRIFF HOLLAND TOGGEHTEERTHEER WITH
ED BOROWN FFOUNDDEED TTHE BUSINESSS INN 22090909 BBAASSED ONN A PRRINCIPLLE IOOGFF DDELIVVERINNG FFELLL EEL GOOD FOOOD MMASDDEE FROMM F
RRES H QUALITY AANDD RRESPONBILITY SIBLUYY SOURCCECCED INGREDIENTS BOTH FOUNDDERS ARRE INSSEDIDDER 442 UNNDDERR 442 ALUMNNI TTHEE COMPA
NY CYURRENTLLY OPERRATES FLOUR BBRRAANCCEHEHHEES NNEEAARR HIGH DISSENTYENSITY OFFICCE BBUILDINGDDINNGS WHIITHIITH 70 PPERR CENT OOFF II
TS RREVVENEUES COMINNG FROM LUNCCHTTIMME TRRADDE I SSAW HIM WWA:LLKINNH H G AROUND THEE BBACKYYARD LIKKE SOMETHINNGS TROUBLINNG HHIMM F
LLAGG IIS  IIS I_L3ARN_US8_C4PTUPTUUR3 II CCALLED HHIM IN ADDNND WHEN III  AASKED WHATS GOINNGG ON HHEE JUST SSAIDD CCAN I GGO OUT FFOO
RR A WHILLE I KONWNNOW HHEE JUUSTT JUST TRRYINNG TTOO CHHANNGGE TTHE SUUBJECT THEN AGGAIN MMAYBBEE HHE JUUSTT MEENNEEDED SOE MME FRRES
AIRR TTO CLLEEAR IHHIIS MDIND SSO I SSSIID YYES TTHEE ENNEST XTT DDAY I SSAW HHIM WWASHHINNG MY NNEIGHBOURS CCARR ANNDD WHENN HHEE CCAM
E HHOMME I AASKEDD HHIMM WHY HHEE WOULLDD DDO THHAATHHATTHTAHHAATT HHEE JUUSTT SSAIIDD HHE TOLD MMEE TTOO SOO I TOLD HHIM TO TTAAKE A B
OATHN ANND DO TTHIISOOS HHIIS HHOMMEWEORKK HWHHENN HE WWASS DONNEE I TOLD HIM THHAT HHE DINDNT HHAVE TO WWASHH TTH E CCAR BBECCAUSSE IT
 SSAXWWAASS NNOOT HIIS RRESPONSIBBILITIEIIEES HE KKJJJUUSTT NNOD
root@kali:~/Downloads/SOAL HACKTODAY#
```

## # KRIPTOGRAFI

## Acid (-_-)

Diberikansebuah file yang isinyasudah di enkripsi

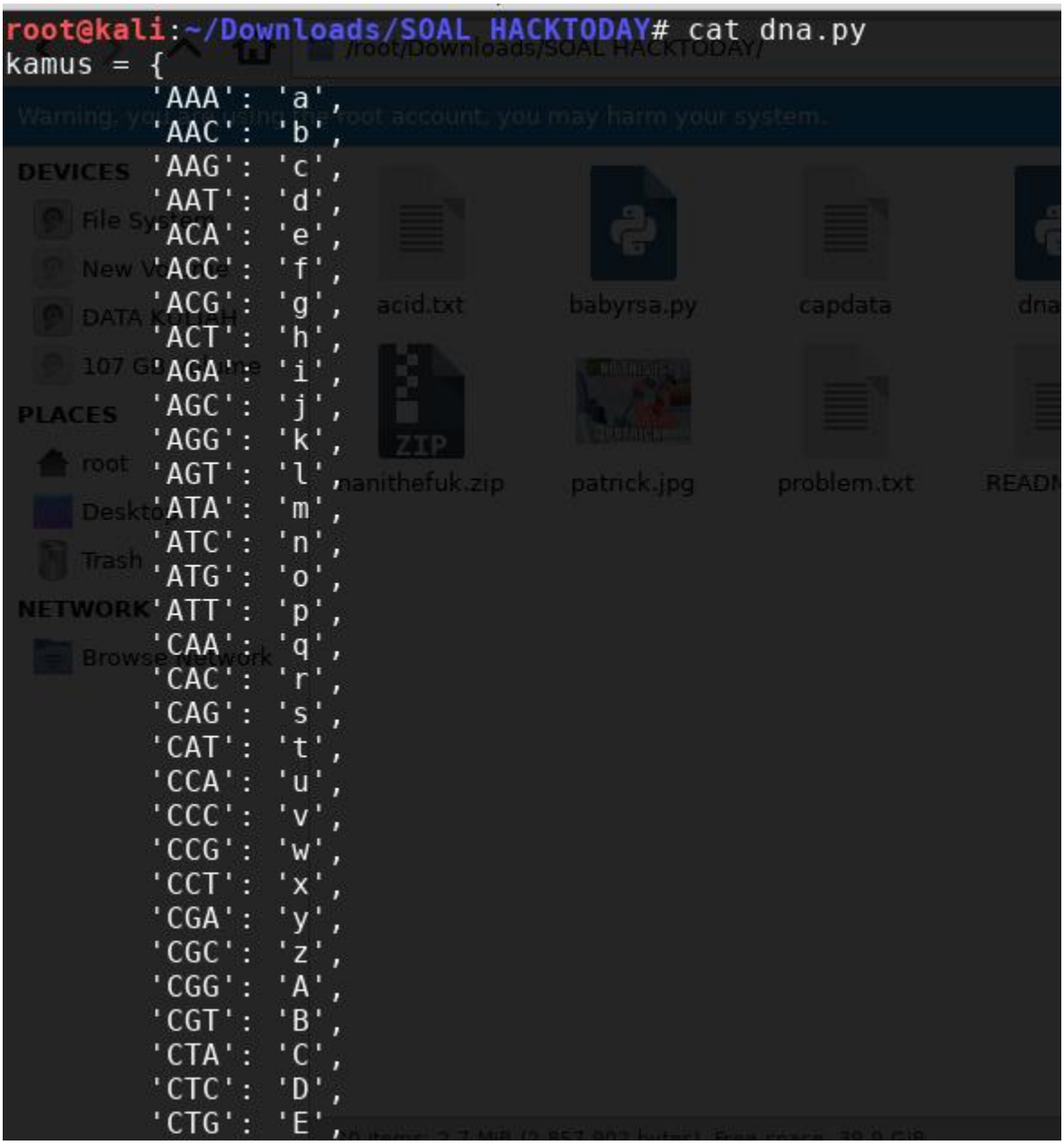
```
File  Edit  View  Terminal  Tabs  Help
root@kali:~/Downloads/SOAL HACKTODAY# cat acid.txt
CGGCAGAAAATATTGAATACAATGAGGCAGAGACACAGAAACATGATCCCAAGGAGTACAAAACATTTGAGTACAAACAGAACTTTGAATAGAAGGACAATCAAAAGTTTGAATACAATCACGAAAATCTTGCAG
AGAATCACGAGGAAACATAAAATCTTGCTCGCTCGGTTGAAAAATAAAAGTAAAACTTTGCAGACAAGCACAATCAGACAGTTGAACAGAATGATAATGAGTACAAGGCCAAGTTTGCGAAAAATCACGTTGATA
ACAATCCGAAGAATAATTAAAATCTTGAATAAAATCTTGATAACAATCCGAAAAATCAATAGATTGAGAATCCAGCATCACCCAAGGCAGAGATTGAGAATCCAGCATCACCCAAGGCAGAGATTGACGACAATC
ACACATAGAAGGAAATTGCAGACACATAGAAAAATTTTGATGCACACGAAAATCAGACAGATAACATTGAATAAAATCTTGAACAAAATCCGAAAAAGGTTGAGCACAATCAGACAGTTGCCCAGACACCCACAG
TTGAGAATCCAGCATCACCCAAGGCAGAGATTGAGAATCCAGCATCACCCAAGGCAGAGATTGACGACAATCACACATAGAAGGAAATTGAGAATCAGATTGAACACACACATTACACACAAAATCTTGATTACA
ATCCATAGAATCACGTTGAATAAAAGTAAAATATTGATTACACACCATCCAATAAACCCAACTAAAATCATTACACACAGGACAATAAACAAAATCACGAAAATCTTGAATAAAATCTTGACCCCAATCACGCAG
AGATTGATGCACACGAAAATCAGACAGATAACATTGAATAAAATCTTGCCCAGACACCCACAGTTGCTCGCTCGGTTGATAACACACCCAATTAAAAGGAAAATCTTGAAACAGAAAATATTGATCCCAAGGAGT
ACAAAACATTTGAACACACACCAGAAAATAAAAAAAATCTTGAATACAATCACGAAAATCTTGATTCACATGCATACAAGAATCTTGAATAAAATCTTGAGGAAACACAACATGACTAGAAATCACAAACATTTG
```

Setelah cari kesana dan kemari dan trololololo… di dapatkan clue enkripsi tersebut merupakan salah satu enkripsi dari esolang **DNA**

DNA#

```
  AT
 T--A
A----T
T-----A
T-----A
G----C
 T--A
  GC
  CG
 C--G
A----T
A-----T
T-----A
A----T
 A--T
  GC
  AT
 C--G
T----A
C-----G
T-----A
G----C
 C--G
  CG
```

Lakukan decode dengan script berikut



```
root@kali:~/Downloads/SOAL HACKTODAY# cat dna.py
kamus = {
        'AAA': 'a',
        'AAC': 'b',
        'AAG': 'c',
        'AAT': 'd',
        'ACA': 'e',
        'ACC': 'f',
        'ACG': 'g',
        'ACT': 'h',
        'AGA': 'i',
        'AGC': 'j',
        'AGG': 'k',
        'AGT': 'l',
        'ATA': 'm',
        'ATC': 'n',
        'ATG': 'o',
        'ATT': 'p',
        'CAA': 'q',
        'CAC': 'r',
        'CAG': 's',
        'CAT': 't',
        'CCA': 'u',
        'CCC': 'v',
        'CCG': 'w',
        'CCT': 'x',
        'CGA': 'y',
        'CGC': 'z',
        'CGG': 'A',
        'CGT': 'B',
        'CTA': 'C',
        'CTC': 'D',
        'CTG': 'E',
```

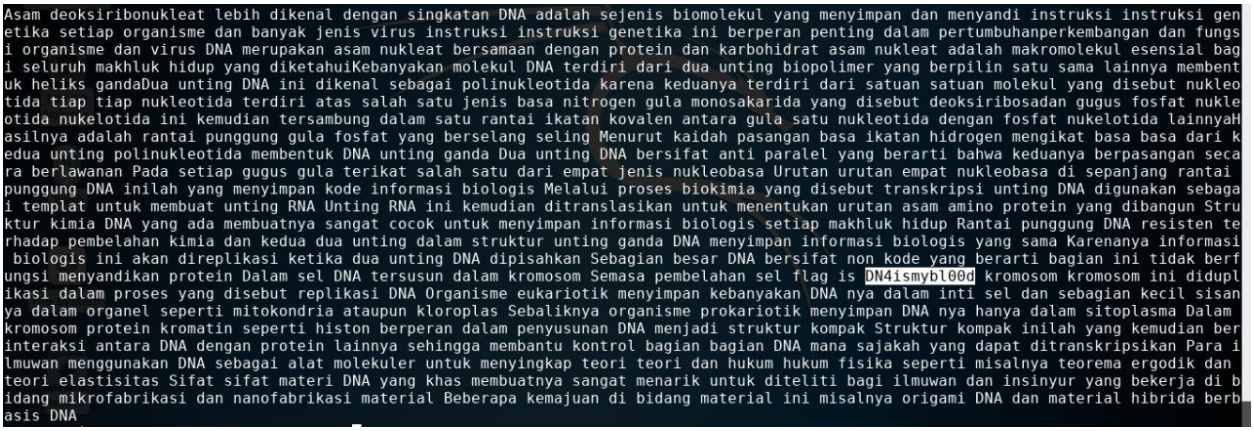
```
        'CTT': 'F',
        'GAA': 'G',
        'GAC': 'H',
        'GAG': 'I',
        'GAT': 'J',
        'GCA': 'K',
        'GCC': 'L',
        'GCG': 'M',
        'GCT': 'N',
        'GGA': 'O',
        'GGC': 'P',
        'GGG': 'Q',
        'GGT': 'R',
        'GTA': 'S',
        'GTC': 'T',
        'GTG': 'U',
        'GTT': 'V',
        'TAA': 'W',
        'TAC': 'X',
        'TAG': 'Y',
        'TAT': 'Z',
        'TCA': '1',
        'TCC': '2',
        'TCG': '3',
        'TCT': '4',
        'TGA': '5',
        'TGC': '6',
        'TGG': '7',
        'TGT': '8',
        'TTA': '9',
        'TTC': '0',
        'TTG': ' ',
        'TTT': '.',
```

```
        'TTT': '.',
}

c = open('acid.txt').read().strip()

flag = []
for x in range(0,len(c), 3):
        aw = c[x:x+3]
        print aw, kamus[aw]
        flag.append(kamus[aw])
```

Run dan didapatkan flag



# # WEB

## Flag.io

Didapatkan sebuah website yang berisi string ini secara berulang-ulang,

```
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
```

Saat dilihat source nya ada fungsi untuk menampilkan message tersebut secara berulang-ulang.

```
    <script>
        var socket = io.connect('http://' + document.domain + ':' + location.port, {
'sync disconnect on unload': true });
        socket.on('connect', function(){
            console.log('Connected to server.');
          });
        socket.on('message', function(msg){
            $( 'div.message_holder' ).append('<div><b style="color: #000">'+msg+'</div>' )
        });
    </script>
```

Setelah di check menggunakan inspect element, ternyata flagnya ada di bagian response pada tab network