

Writeup HackToday 2019

Zer0Byte ID X SiapaYa?

1001

Rexy Fahrezi

Gayu Gumelar

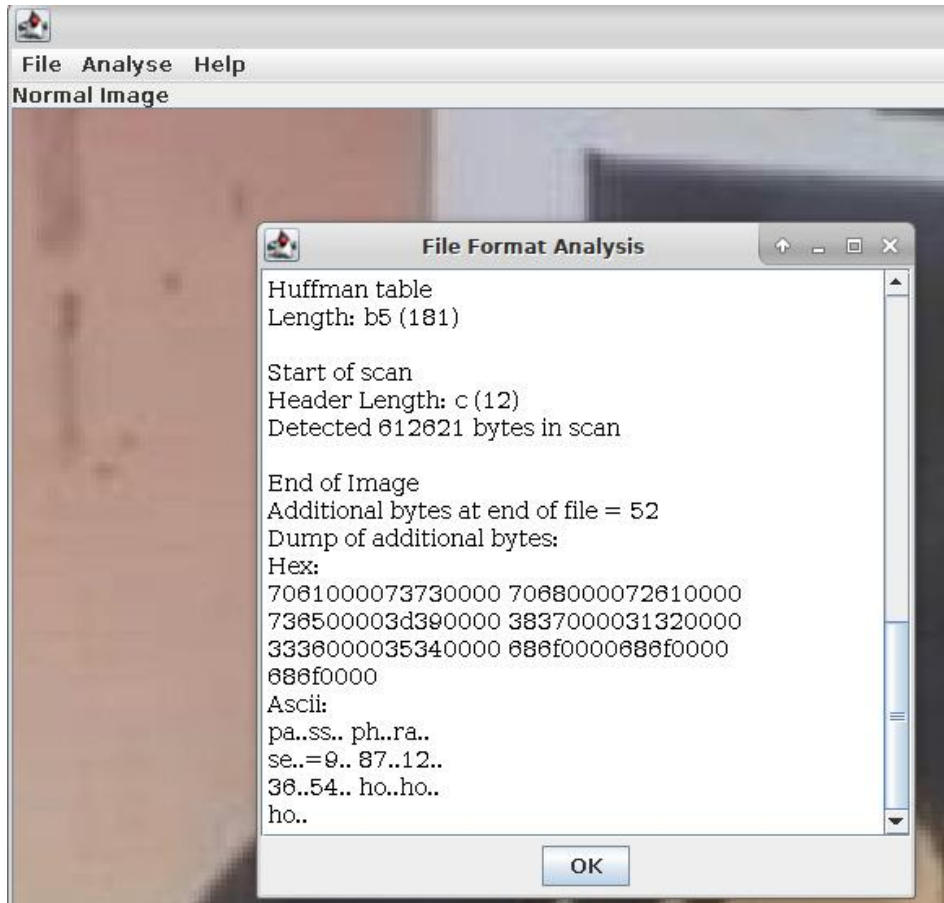
M Hendro Junawarko

M Nurhasan Aprilian

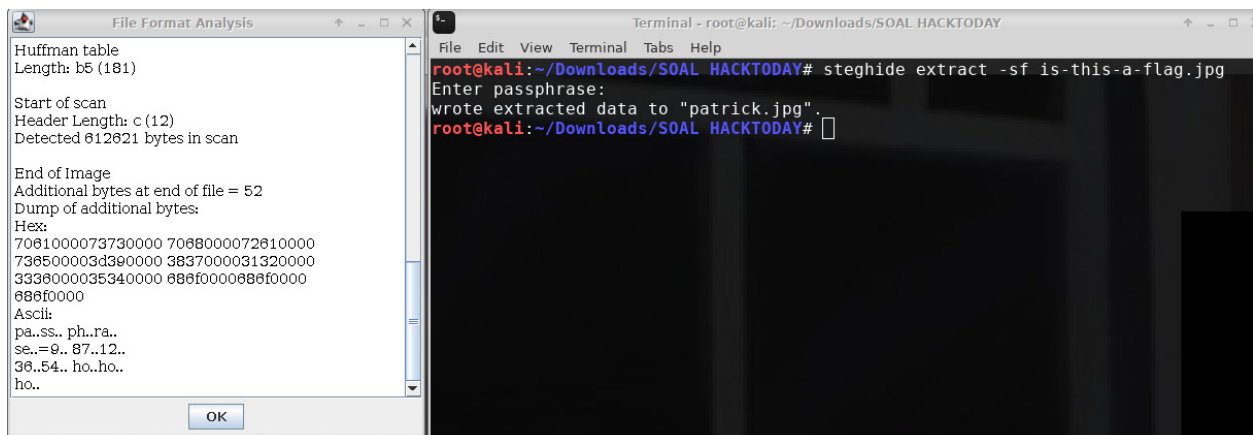
FORENSIC

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.

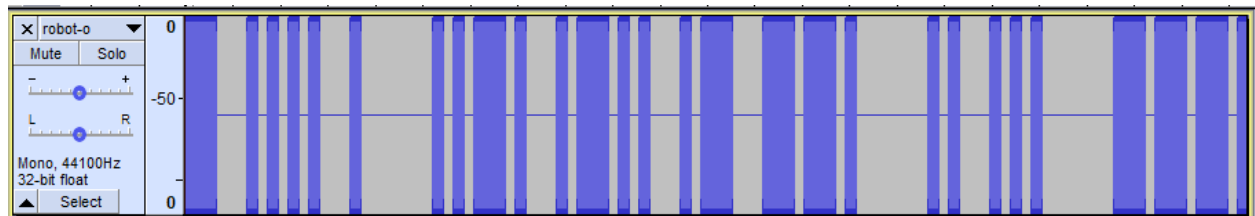
```
Comment : JJ2XG5BANNUIWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYLHHIQGQYLDNN2G6ZDBPF5V6NDMNRPWQNDJNRPV6NLUGM4WQ2LEMVPTC  
ZJSG5RWKM35
```

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

```
>>> import base64  
>>> data = 'JJ2XG5BANNUIWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYLHHIQGQYLDNN2G6ZDBPF5V6NDMNRPWQNDJNRPV6NLUGM4WQ2LEMVPTCZJSG5RWKM35'  
>>> dcode = base64.b32decode(data)  
>>> print dcode  
Just kidding. Here's your flag: hacktoday{_4ll_h4il_5t39hide_1e27ce3}
```

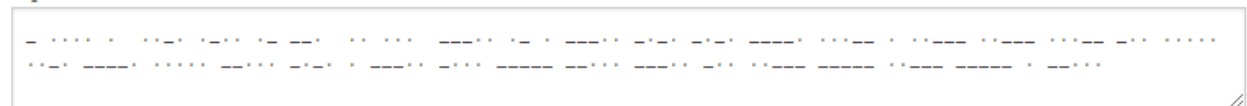
Robot o

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 intro.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', '=' : '1e', '/' : '1f', '{' : '1a', '}' : '1c',
        '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 HUNNGGARIAN RHAPSODIES WHICH TAKKETT
AKKE THEIR FROMM TTIIIS DDANCCE THE FISRISKKA IS GGENERALLY EITHER TURBULLENT OR JUBILANTT INN TONE GRIFF HOLLAND TOGGEHTEERTHEER WITH
ED BOROWN FFOUNDEED TTHE BUSINESSS INN 22090909 BBAASSED ONN A PRRINCIPLLE IOOGFF DDELIVVERINNG FFELL EEL GOOD FOODD MMASDDEE FROMM F
RRES H QUALITY AANDD RRESPONBILITY SIBLUYY SOURCCECCEDD INGREDIENTS BOTH FOUNDDERS ARRE INSSSEDIDDER 442 UNNDDEERR 442 ALUMNNI TTREE COMPA
NY CYURRENTLY OPERATES FLOUR BBRRAANCCEHEHHEES NNEEAARR HIGH DISSENTYENSITY OFFICCE BBUILDINGDDINNGS WHIITHIITH 70 PPERR CENT OOFF II
TS RREVENEUES COMINNG FROM LUNCCHTTIMME TRRADDE I SSAAW 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 KONNNOW HHEE JUUSTT JUST TRRYINNG TT00 CHHANNGE TTHE SUUBJECT THEN AGGAIN MMAYBBEE HHE JUUSTT MEENNEEDED SOE MME FRRES
ATRR TT0 CLLEEAR IHIIIS MDIND SS0 I SSSIID YYES TTREE ENNEST XTT DDAY I SSAAW HHIM WWASHHINNG MY NNEIGHBOURS CCARR ANND WHENN HHEE CCAM
E HHOMME I AASKEDD HHIMM WHY HHEE WOULD DD0 THHAATHHATTHTAHHAATT HHEE JUUSTT SSAIDD HHE TOLD MME TT00 SOO I TOLD HHIM TO TTAKE A B
OATHN ANND DO TTIIIS00S HHIIIS HHOMMEWEORRK HWHHENN HE WWAASS DONNEE I TOLD HIM THHAT HHE DINDNT HHAVE TO WWASHH TT0 E CCAR BBECOAUSE IT
SSAXWWAASS NN00T HHIS RRESPONSIBBILITIEIES HE KJJJUUSTT NN0D
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
CGGCAGAAAAATTGGAATACAATGAGGCAGAGACACAGAAACATGATCCCAAGGAGTACAAAACATTGTAGTACAACAGAACTTTGAATAGAAGGACAATCAAAAGTTTGAATACAATCACGAAAACTTTGCAG
AGAATCACGAGGAAACATAAAATCTTGCTCGCTCGGTTGAAAAATAAAAGTAAAACTTTGCAGACAAGCACAAATCAGACAGTTGAACAGAAATGATAATGAGTACAAGGCCAAGTTTGCGAAAAATCAGTTGATA
ACAATCCGAAGAATAATTAAAATCTTGAATAAAATCTTGATAACAATCCGAAAAATCAATAGATTGAGAAATCCAGCATCACCAAGGCAGAGATTGAGAATCCAGCATCACCAAGGCAGAGATTGACGACAAATC
ACACATAGAAGGAAATTGCAGACACATAGAAAAATTTTGTATGACACAGAAAAATCAGACAGATAACATTGAATAAAATCTTGAACAAAAATCCGAAAAAGGTTGAGCACAATCAGACAGTTGCCCAGACACCCACAG
TTGAGAAATCCAGCATCACCAAGGCAGAGATTGAGAATCCAGCATCACCAAGGCAGAGATTGACGACAAATCAGACATAGAAAGGAAATTTGAGAAATCAGATTGAACACACACATTACACAAAAATCTTGATTACA
ATCCATAGAAATCAGTTGAATAAAAGTAAAAATTTGATTACACACCATCCAAATAACCCAACTAAAAATCATTACACACAGGACAATAAACAAAAATCACGAAAAATCTTGAATAAAATCTTGACCCCAATCAGCGAG
AGATTGATGCACACGAAAAATCAGACAGATAACATTGAATAAAATCTTGCCAGACACCCACAGTTGCTCGCTCGGTTGATAACACACCCCAATTAAGGAAAAATCTTGAAACAGAAAAATTTGATCCCAAGGAGT
ACAAAACATTTGAAACACACACAGAAAAATAAAAAATCTTGAATACAATCAGGAAATCTTGATTACATGCATACAAGAACTTTGAATAAAATCTTGAGGAAACACAAATGACTAGAAATCACAACATTTG

```

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',
    'CTA': 'G',
    'CTC': 'H',
    'CTG': 'I',
    'CTT': 'J',
    'CTA': 'K',
    'CTC': 'L',
    'CTG': 'M',
    'CTT': 'N',
    'CTA': 'O',
    'CTC': 'P',
    'CTG': 'Q',
    'CTT': 'R',
    'CTA': 'S',
    'CTC': 'T',
    'CTG': 'U',
    'CTT': 'V',
    'CTA': 'W',
    'CTC': 'X',
    'CTG': 'Y',
    'CTT': 'Z',
    'CTA': 'a',
    'CTC': 'b',
    'CTG': 'c',
    'CTT': 'd',
    'CTA': 'e',
    'CTC': 'f',
    'CTG': 'g',
    'CTT': 'h',
    'CTA': 'i',
    'CTC': 'j',
    'CTG': 'k',
    'CTT': 'l',
    'CTA': 'm',
    'CTC': 'n',
    'CTG': 'o',
    'CTT': 'p',
    'CTA': 'q',
    'CTC': 'r',
    'CTG': 's',
    'CTT': 't',
    'CTA': 'u',
    'CTC': 'v',
    'CTG': 'w',
    'CTT': 'x',
    'CTA': 'y',
    'CTC': 'z',
    'CTG': 'A',
    'CTT': 'B',
    'CTA': 'C',
    'CTC': 'D',
    'CTG': 'E',
    'CTT': 'F',
    'CTA': 'G',
    'CTC': 'H',
    'CTG': 'I',
    'CTT': 'J',
    'CTA': 'K',
    'CTC': 'L',
    'CTG': 'M',
    'CTT': 'N',
    'CTA': 'O',
    'CTC': 'P',
    'CTG': 'Q',
    'CTT': 'R',
    'CTA': 'S',
    'CTC': 'T',
    'CTG': 'U',
    'CTT': 'V',
    'CTA': 'W',
    'CTC': 'X',
    'CTG': 'Y',
    'CTT': 'Z'
}
```



```
'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' : ' ',
```

```
}  
  
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

Asam deoksiribonukleat lebih dikenal dengan singkatan DNA adalah sejenis biomolekul yang menyimpan dan menyandi instruksi instruksi genetik setiap organisme dan banyak jenis virus instruksi instruksi genetika ini berperan penting dalam pertumbuhan perkembangan dan fungsi organisme dan virus DNA merupakan asam nukleat bersamaan dengan protein dan karbohidrat asam nukleat adalah makromolekul esensial bagi seluruh makhluk hidup yang diketahui. Kebanyakan molekul DNA terdiri dari dua untai biopolimer yang berpilin satu sama lainnya membentuk heliks ganda. Dua untai DNA ini dikenal sebagai polinukleotida karena keduanya terdiri dari satuan-satuan molekul yang disebut nukleotida. Tiap-tiap nukleotida terdiri atas salah satu jenis basa nitrogen gula monosakarida yang disebut deoksiribosa dan gugus fosfat nukleotida. Nukleotida ini kemudian tersambung dalam satu rantai ikatan kovalen antara gula satu nukleotida dengan fosfat nukleotida lainnya. Hasilnya adalah rantai punggung gula fosfat yang berselang seling. Menurut kaidah pasangan basa, ikatan hidrogen mengikat basa-basa dari kedua untai polinukleotida membentuk DNA untai ganda. Dua untai DNA bersifat anti-paralel yang berarti bahwa keduanya berpasangan secara berlawanan. Pada setiap gugus gula terikat salah satu dari empat jenis nukleobasa. Urutan empat nukleobasa di sepanjang rantai punggung DNA inilah yang menyimpan kode informasi biologis. Melalui proses biokimia yang disebut transkripsi, untai DNA digunakan sebagai cetakan untuk membuat untai RNA. Untai RNA ini kemudian ditranslasikan untuk menentukan urutan asam amino protein yang dibangun. Struktur kimia DNA yang ada membuatnya sangat cocok untuk menyimpan informasi biologis setiap makhluk hidup. Rantai punggung DNA resisten terhadap pembelahan kimia dan kedua untai dalam struktur untai ganda DNA menyimpan informasi biologis yang sama. Karenanya informasi biologis ini akan direplikasi ketika dua untai DNA dipisahkan. Sebagian besar DNA bersifat non-kode yang berarti bagian ini tidak berfungsi menyandi protein. Dalam sel, DNA tersusun dalam kromosom. Selama pembelahan sel, flag is DN4ismybl00d kromosom kromosom ini diduplikasi dalam proses yang disebut replikasi DNA. Organisme eukariotik menyimpan kebanyakan DNA nya dalam inti sel dan sebagian kecil sisanya dalam organel seperti mitokondria ataupun kloroplas. Sebaliknya organisme prokariotik menyimpan DNA nya hanya dalam sitoplasma. Dalam kromosom, protein kromatin seperti histon berperan dalam penyusunan DNA menjadi struktur kompak. Struktur kompak inilah yang kemudian berinteraksi antara DNA dengan protein lainnya sehingga membantu kontrol bagian-bagian DNA mana saja yang dapat ditranskripsikan. Para ilmuwan menggunakan DNA sebagai alat molekuler untuk menyingkap teori-teori dan hukum-hukum fisika seperti misalnya teorema ergodik dan teori elastisitas. Sifat-sifat materi DNA yang khas membuatnya sangat menarik untuk diteliti bagi ilmuwan dan insinyur yang bekerja di bidang mikrofabrikasi dan nanofabrikasi material. Beberapa kemajuan di bidang material ini misalnya origami DNA dan material hibrida berbasis DNA.

Flag.io

[illegible]

```
<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>
```

The screenshot shows the Chrome DevTools Network tab. The top toolbar includes icons for Elements, Console, Sources, Network (selected), and Performance. Below the toolbar, there's a filter input and checkboxes for 'Hide data URLs', 'Preserve log', and 'Disable cache'. The 'Network' tab is active, displaying a list of network requests. The first request is selected, and its details are shown in the right pane. The 'Response' pane displays the content of the selected request, which is a JSON object: `{As_you_Humans_say, Im_all_ears}`. The 'Timing' pane shows the request's duration, which is approximately 10000 ms.

Name	Headers	Preview	Response	Cookies	Timing
?EIO=3&transport=polling&t.			1 RET-FLAGGG", "hacktoday{As_you_Humans_say, Im_all_ears}"		10000 ms
?EIO=3&transport=polling&t.					20000 ms
?EIO=3&transport=polling&t.					30000 ms
?EIO=3&transport=polling&t.					40000 ms
?EIO=3&transport=polling&t.					50000 ms
?EIO=3&transport=polling&t.					60000 ms
?EIO=3&transport=polling&t.					70000 ms