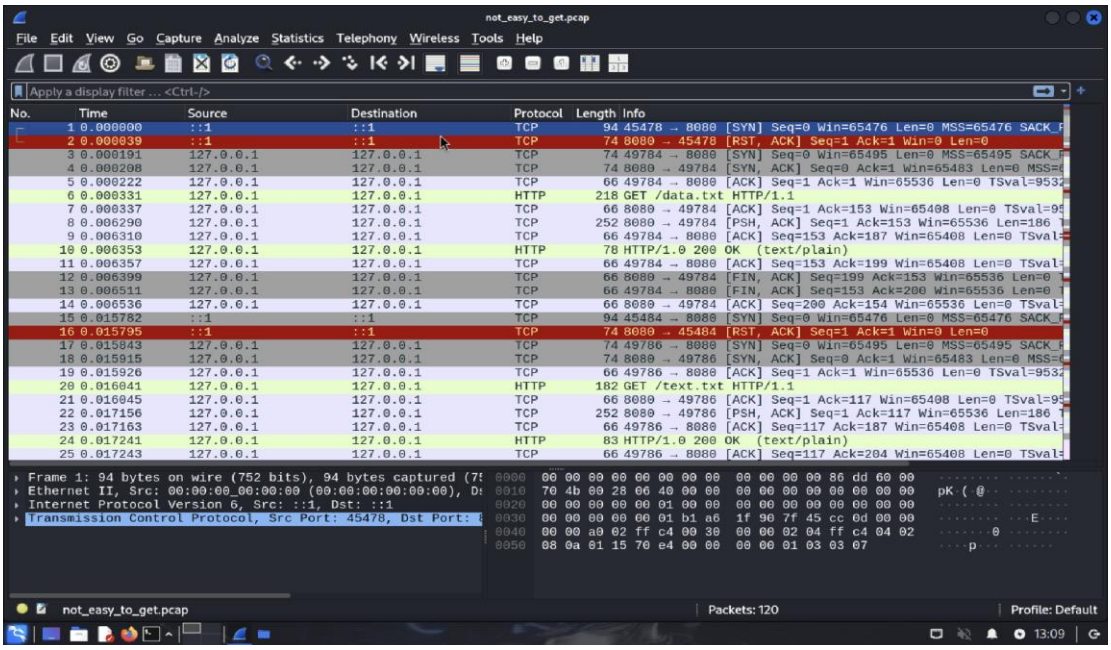
Network Security CTF Write-Ups

Not_easy_to_get.pcap

Steps:

- Opened the pcap file and followed the tcp stream

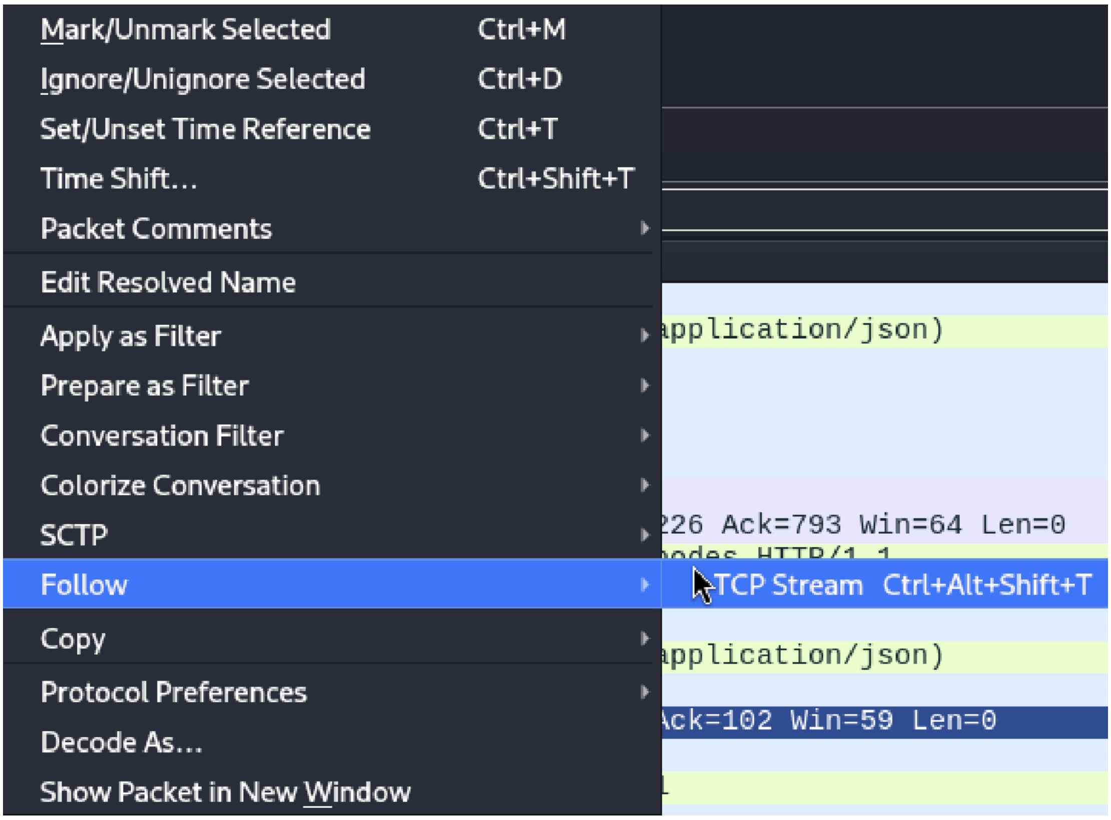


not_easy_to_get.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

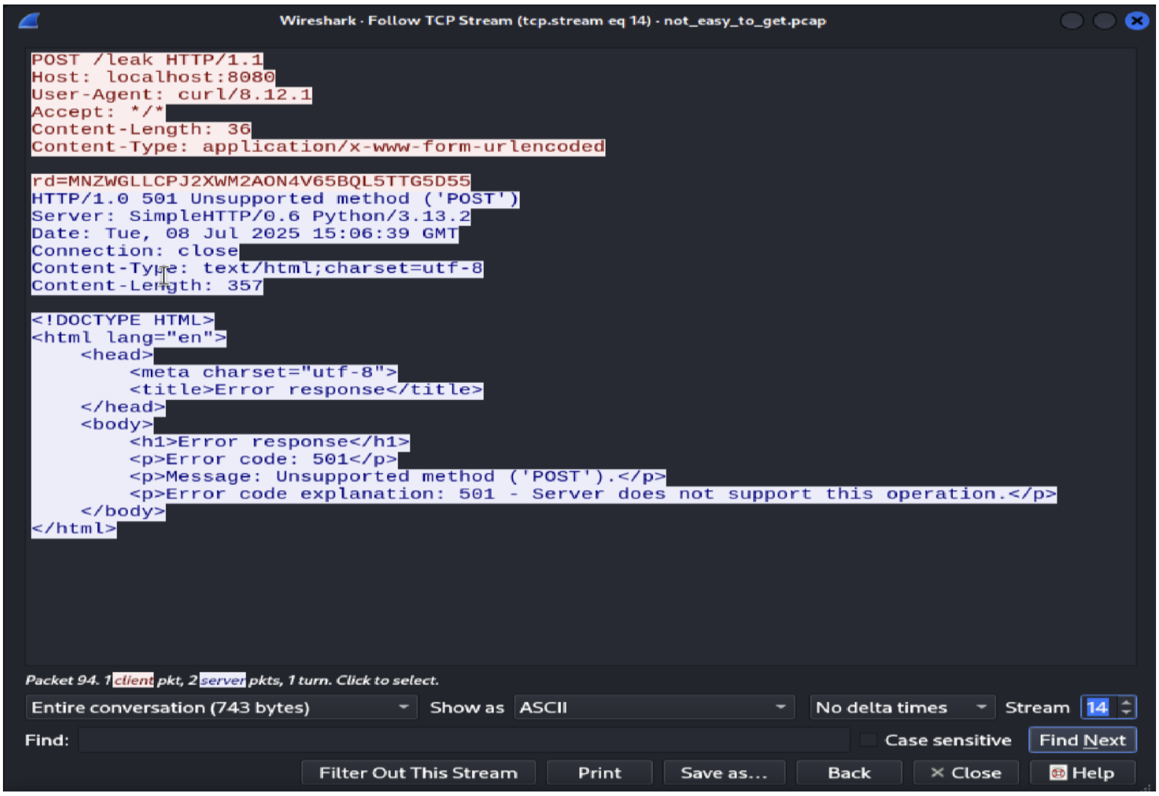
```
No.  Time        Source      Destination  Protocol Length Info
   1 0.000000    ::1         ::1          TCP        94 45478 → 8080 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_P
   2 0.000039    ::1         ::1          TCP        74 8080 → 45478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   3 0.000191    127.0.0.1   127.0.0.1    TCP        74 49784 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_P
   4 0.000208    127.0.0.1   127.0.0.1    TCP        74 8080 → 49784 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=6
   5 0.000222    127.0.0.1   127.0.0.1    TCP        66 49784 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=9532
   6 0.000331    127.0.0.1   127.0.0.1    HTTP      218 GET /data.txt HTTP/1.1
   7 0.000337    127.0.0.1   127.0.0.1    TCP        66 8080 → 49784 [ACK] Seq=1 Ack=153 Win=65408 Len=0 TSval=95
   8 0.006290    127.0.0.1   127.0.0.1    TCP       252 8080 → 49784 [PSH, ACK] Seq=1 Ack=153 Win=65536 Len=186 T
   9 0.006310    127.0.0.1   127.0.0.1    TCP        66 49784 → 8080 [ACK] Seq=153 Ack=187 Win=65408 Len=0 TSval=
  10 0.006353    127.0.0.1   127.0.0.1    HTTP       78 HTTP/1.0 200 OK  (text/plain)
  11 0.006357    127.0.0.1   127.0.0.1    TCP        66 49784 → 8080 [ACK] Seq=153 Ack=199 Win=65408 Len=0 TSval=
  12 0.006399    127.0.0.1   127.0.0.1    TCP        66 8080 → 49784 [FIN, ACK] Seq=199 Ack=153 Win=65536 Len=0 T
  13 0.006511    127.0.0.1   127.0.0.1    TCP        66 49784 → 8080 [FIN, ACK] Seq=153 Ack=200 Win=65536 Len=0 T
  14 0.006536    127.0.0.1   127.0.0.1    TCP        66 8080 → 49784 [ACK] Seq=200 Ack=154 Win=65536 Len=0 TSval=
  15 0.015782    ::1         ::1          TCP        94 45484 → 8080 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_P
  16 0.015795    ::1         ::1          TCP        74 8080 → 45484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  17 0.015843    127.0.0.1   127.0.0.1    TCP        74 49786 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_P
  18 0.015915    127.0.0.1   127.0.0.1    TCP        74 8080 → 49786 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=6
  19 0.015926    127.0.0.1   127.0.0.1    TCP        66 49786 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=9532
  20 0.016041    127.0.0.1   127.0.0.1    HTTP      182 GET /text.txt HTTP/1.1
  21 0.016045    127.0.0.1   127.0.0.1    TCP        66 8080 → 49786 [ACK] Seq=1 Ack=117 Win=65408 Len=0 TSval=95
  22 0.017156    127.0.0.1   127.0.0.1    TCP       252 8080 → 49786 [PSH, ACK] Seq=1 Ack=117 Win=65536 Len=186 T
  23 0.017163    127.0.0.1   127.0.0.1    TCP        66 49786 → 8080 [ACK] Seq=117 Ack=187 Win=65408 Len=0 TSval=
  24 0.017241    127.0.0.1   127.0.0.1    HTTP       83 HTTP/1.0 200 OK  (text/plain)
  25 0.017243    127.0.0.1   127.0.0.1    TCP        66 49786 → 8080 [ACK] Seq=117 Ack=204 Win=65408 Len=0 TSval=
```

```
› Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (75
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Ds
› Internet Protocol Version 6, Src: ::1, Dst: ::1
› Transmission Control Protocol, Src Port: 45478, Dst Port: 8
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 00   ··········`·
0010  70 4b 00 28 06 40 00 00  00 00 00 00 00 00 00 00   pK·(·@··········
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ················
0030  00 00 00 00 00 01 b1 a6  1f 90 7f 45 cc 0d 00 00   ···········E····
0040  00 00 a0 02 ff c4 00 30  00 00 02 04 ff c4 04 02   ·······0········
0050  08 0a 01 15 70 e4 00 00  00 00 01 03 03 07         ····p·········
```



- found a suspicious packet text, copied it and checked it with cyberchef


Wireshark · Follow TCP Stream (tcp.stream eq 14) · not_easy_to_get.pcap

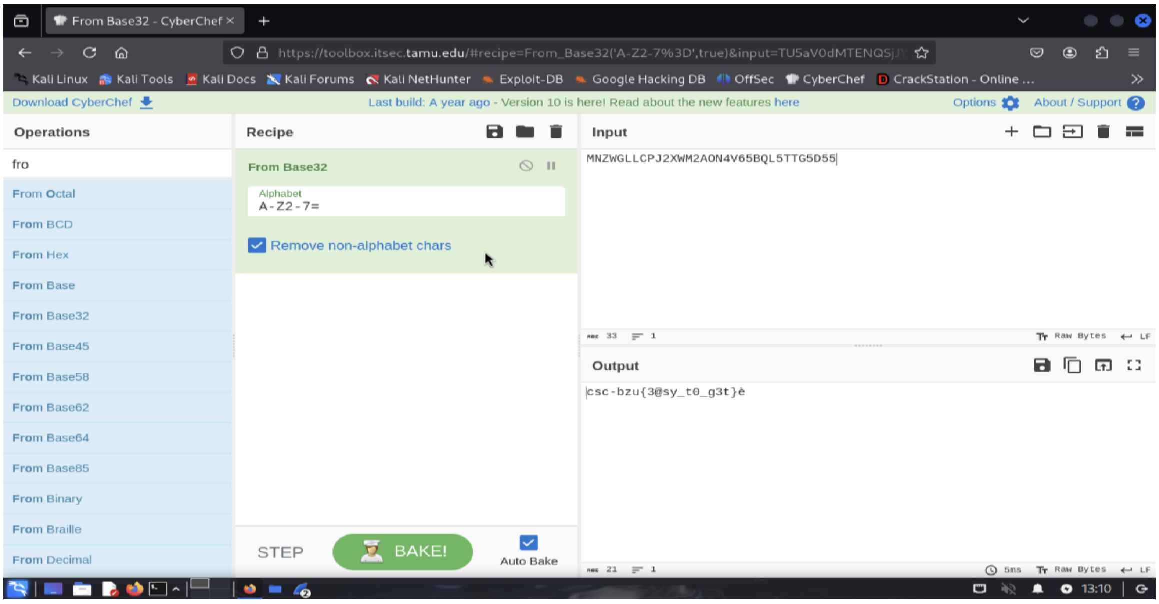
```
POST /leak HTTP/1.1
Host: localhost:8080
User-Agent: curl/8.12.1
Accept: */*
Content-Length: 36
Content-Type: application/x-www-form-urlencoded

rd=MNZWGLLCPJ2XWM2AON4V65BQL5TTG5D55
HTTP/1.0 501 Unsupported method ('POST')
Server: SimpleHTTP/0.6 Python/3.13.2
Date: Tue, 08 Jul 2025 15:06:39 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 357

<!DOCTYPE HTML>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 501</p>
        <p>Message: Unsupported method ('POST').</p>
        <p>Error code explanation: 501 - Server does not support this operation.</p>
    </body>
</html>
```

Packet 94. 1 client pkt, 2 server pkts, 1 turn. Click to select.

Entire conversation (743 bytes) Show as ASCII No delta times Stream 14


From Base32 - CyberChef

https://toolbox.itsec.tamu.edu/#recipe=From_Base32('A-Z2-7%3D',true)&input=TU5aV0dMTENQSjJY

Recipe: From Base32

Alphabet: A-Z2-7=

☑ Remove non-alphabet chars

Input

```
MNZWGLLCPJ2XWM2AON4V65BQL5TTG5D55
```

Output

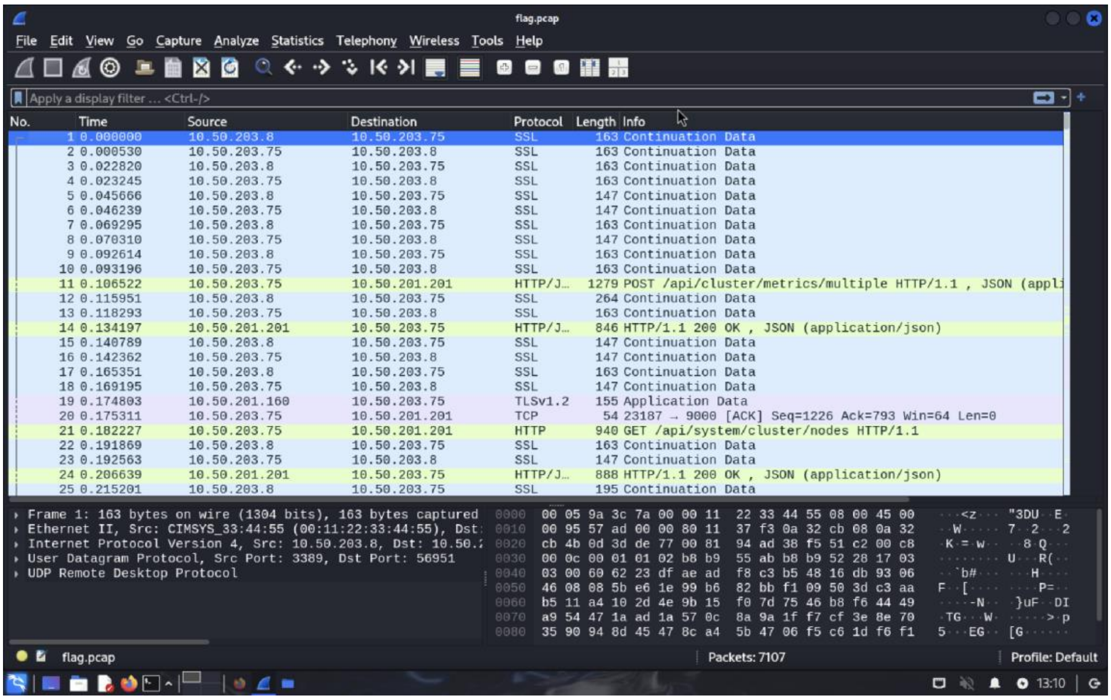
```
csc-bzu{3@sy_t0_g3t}è
```

Flag: csc-bzu{3@sy_t0_g3t}

flag.pcap

Steps:

- Same as before after checking the tcp stream we found a suspicious text in the packet

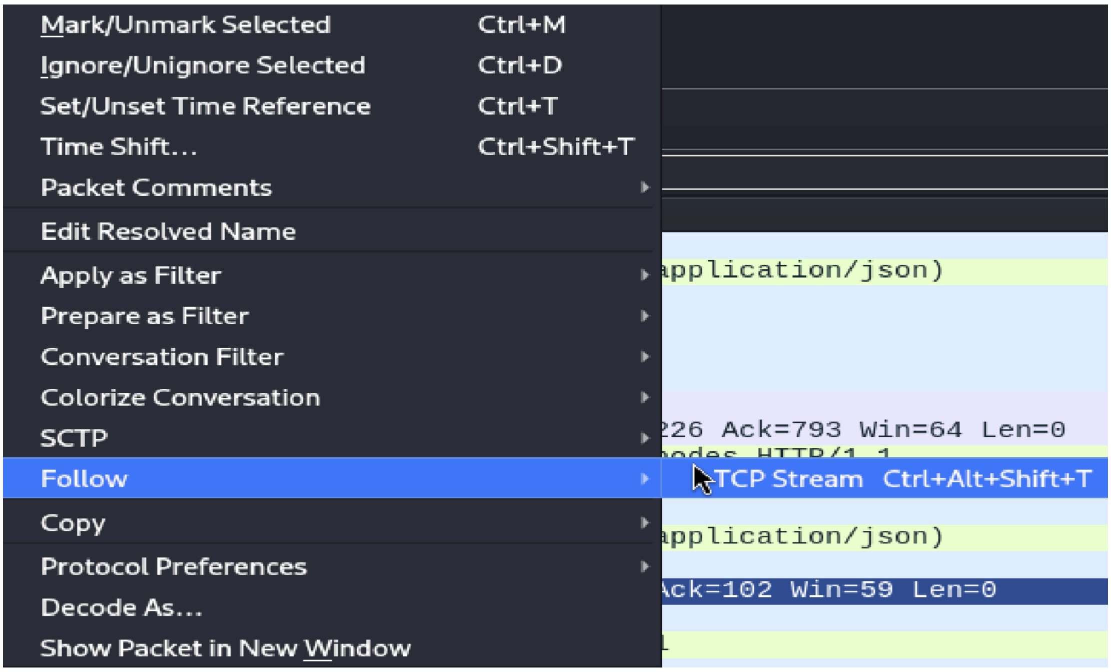


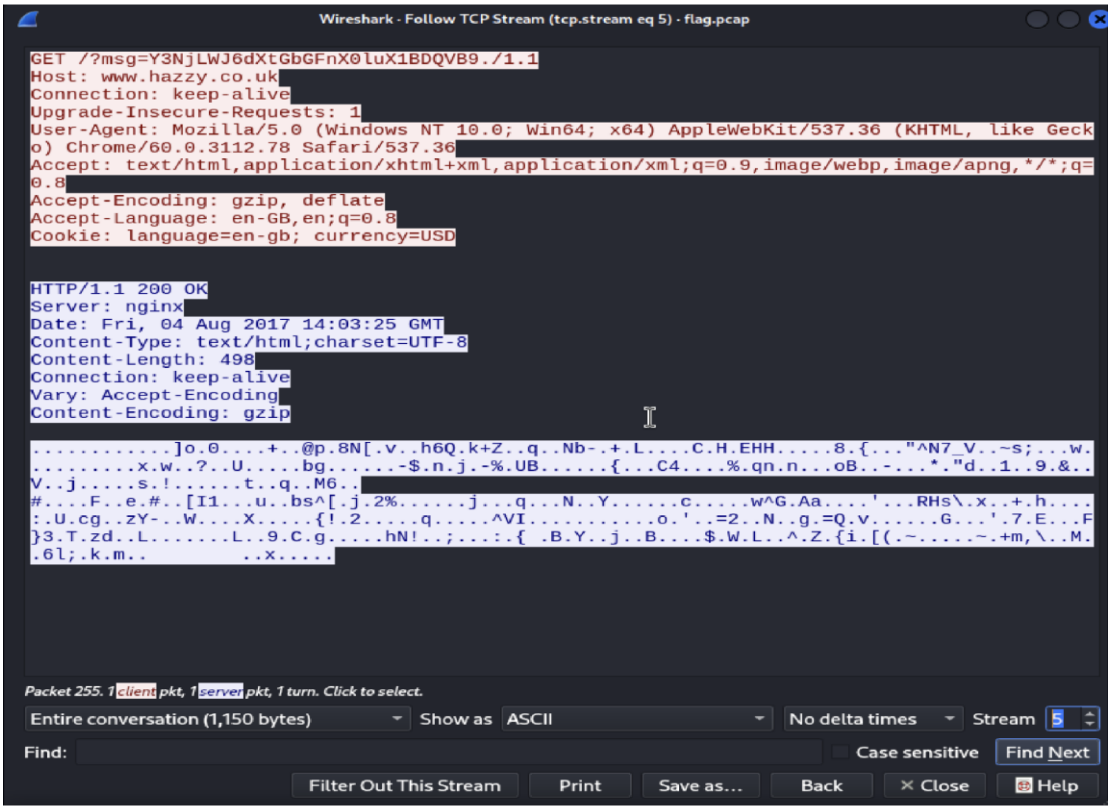
flag.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source          Destination     Protocol  Length Info
    1 0.000000   10.50.203.8     10.50.203.75    SSL        163 Continuation Data
    2 0.000530   10.50.203.75    10.50.203.8     SSL        163 Continuation Data
    3 0.022820   10.50.203.8     10.50.203.75    SSL        163 Continuation Data
    4 0.023245   10.50.203.75    10.50.203.8     SSL        163 Continuation Data
    5 0.045666   10.50.203.8     10.50.203.75    SSL        147 Continuation Data
    6 0.046239   10.50.203.75    10.50.203.8     SSL        147 Continuation Data
    7 0.069295   10.50.203.8     10.50.203.75    SSL        163 Continuation Data
    8 0.070310   10.50.203.75    10.50.203.8     SSL        147 Continuation Data
    9 0.092614   10.50.203.8     10.50.203.75    SSL        163 Continuation Data
   10 0.093196   10.50.203.75    10.50.203.8     SSL        163 Continuation Data
   11 0.106522   10.50.203.75    10.50.201.201   HTTP/J…   1279 POST /api/cluster/metrics/multiple HTTP/1.1 , JSON (appli
   12 0.115951   10.50.203.8     10.50.203.75    SSL        264 Continuation Data
   13 0.118293   10.50.203.75    10.50.203.8     SSL        163 Continuation Data
   14 0.134197   10.50.201.201   10.50.203.75    HTTP/J…    846 HTTP/1.1 200 OK , JSON (application/json)
   15 0.140789   10.50.203.8     10.50.203.75    SSL        147 Continuation Data
   16 0.142362   10.50.203.75    10.50.203.8     SSL        147 Continuation Data
   17 0.165351   10.50.203.8     10.50.203.75    SSL        163 Continuation Data
   18 0.169195   10.50.203.75    10.50.203.8     SSL        147 Continuation Data
   19 0.174803   10.50.201.160   10.50.203.75    TLSv1.2    155 Application Data
   20 0.175311   10.50.203.75    10.50.201.201   TCP         54 23187 → 9000 [ACK] Seq=1226 Ack=793 Win=64 Len=0
   21 0.182227   10.50.203.75    10.50.201.201   HTTP       940 GET /api/system/cluster/nodes HTTP/1.1
   22 0.191869   10.50.203.8     10.50.203.75    SSL        163 Continuation Data
   23 0.192563   10.50.203.75    10.50.203.8     SSL        147 Continuation Data
   24 0.206639   10.50.201.201   10.50.203.75    HTTP/J…    888 HTTP/1.1 200 OK , JSON (application/json)
   25 0.215201   10.50.203.8     10.50.203.75    SSL        195 Continuation Data
```

```
› Frame 1: 163 bytes on wire (1304 bits), 163 bytes captured
› Ethernet II, Src: CIMSYS_33:44:55 (00:11:22:33:44:55), Dst:
› Internet Protocol Version 4, Src: 10.50.203.8, Dst: 10.50.2
› User Datagram Protocol, Src Port: 3389, Dst Port: 56951
› UDP Remote Desktop Protocol
```

```
0000  00 05 9a 3c 7a 00 00 11  22 33 44 55 08 00 45 00   ···<z···  "3DU··E·
0010  00 95 57 ad 00 00 80 11  37 f3 0a 32 cb 08 0a 32   ··W·····  7··2···2
0020  cb 4b 0d 3d de 77 00 81  94 ad 38 f5 51 c2 00 c8   ·K·=·w··  ··8·Q···
0030  00 0c 00 01 01 02 b8 b9  55 ab b8 b9 52 28 17 03   ········  U···R(··
0040  03 00 60 62 23 df ae ad  f8 c3 b5 48 16 db 93 06   ··`b#···  ···H····
0050  46 08 08 5b e6 1e 99 b6  82 bb f1 09 50 3d c3 aa   F··[····  ····P=··
0060  b5 11 a4 10 2d 4e 9b 15  f0 7d 75 46 b8 f6 44 49   ····-N··  ·}uF··DI
0070  a9 54 47 1a ad 1a 57 0c  8a 9a 1f f7 cf 3e 8e 70   ·TG···W·  ·····>·p
0080  35 90 94 8d 45 47 8c a4  5b 47 06 f5 c6 1d f6 f1   5···EG··  [G······
```





Wireshark · Follow TCP Stream (tcp.stream eq 5) · flag.pcap

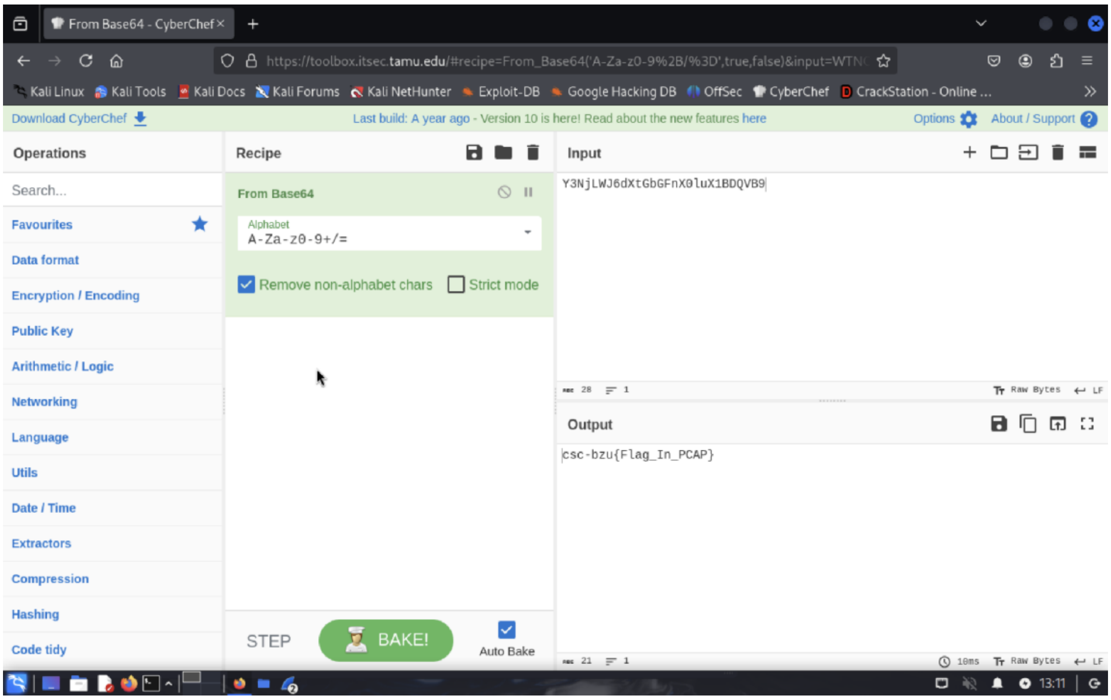
```
GET /?msg=Y3NjLWJ6dXtGbGFnX0luX1BDQVB9./1.1
Host: www.hazzy.co.uk
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/60.0.3112.78 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=
0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.8
Cookie: language=en-gb; currency=USD


HTTP/1.1 200 OK
Server: nginx
Date: Fri, 04 Aug 2017 14:03:25 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 498
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

............]o.0....+..@p.8N[.v..h6Q.k+Z..q..Nb-.+.L....C.H.EHH.....8.{..."^N7_V..~s;...w.
.........x.w..?..U.....bg......-$.n.j.-%.UB......{...C4....%.qn.n...oB..-...*."d..1..9.&..
V..j.....s.!......t..q..M6..
#....F..e.#..[I1...u..bs^[.j.2%......j...q...N..Y......c.....w^G.Aa....'...RHs\.x..+.h....
:.U.cg..zY-..W....X.....{!.2.....q.....^VI...........o.'..=2..N..g.=Q.v......G...'.7.E...F
}3.T.zd..L.......L..9.C.g.....hN!..;...:.{ .B.Y..j..B....$.W.L..^.Z.{i.[(.~.....~.+m,\..M.
.6l;.k.m..        ..x.....
```

Packet 255. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1,150 bytes) | Show as ASCII | No delta times | Stream 5



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

Input

```
Y3NjLWJ6dXtGbGFnX0luX1BDQVB9
```

Output

```
csc-bzu{Flag_In_PCAP}
```

Flag: csc-bzu{Flag_In_PCAP}