Ciphertext CTF 2020

Digital Forensics

Undefined_leakage

Description:

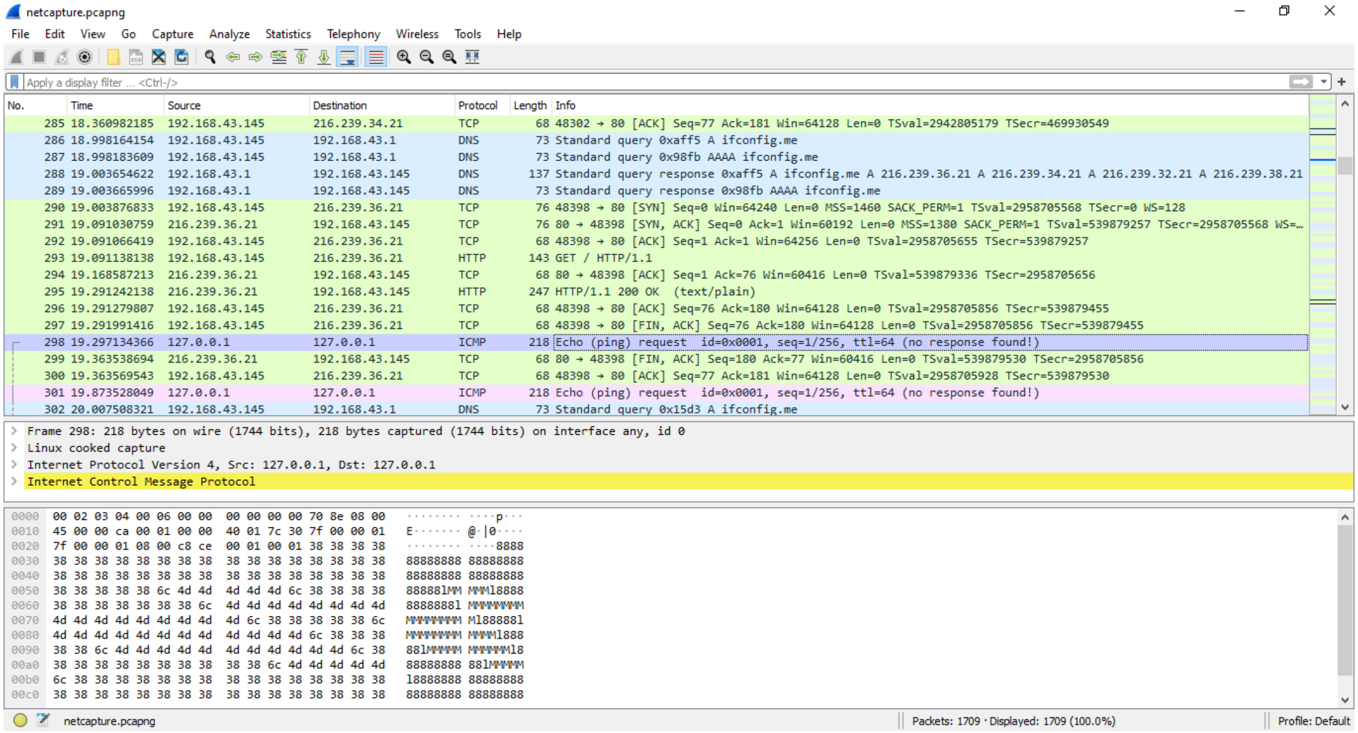
omg another leakage... and this time we don't understand what is happening at alll!.

Files:

netcapture.pcapng Size: 226.23 KB MD5: d44973b60ac1ebd58be6b627b109c2be

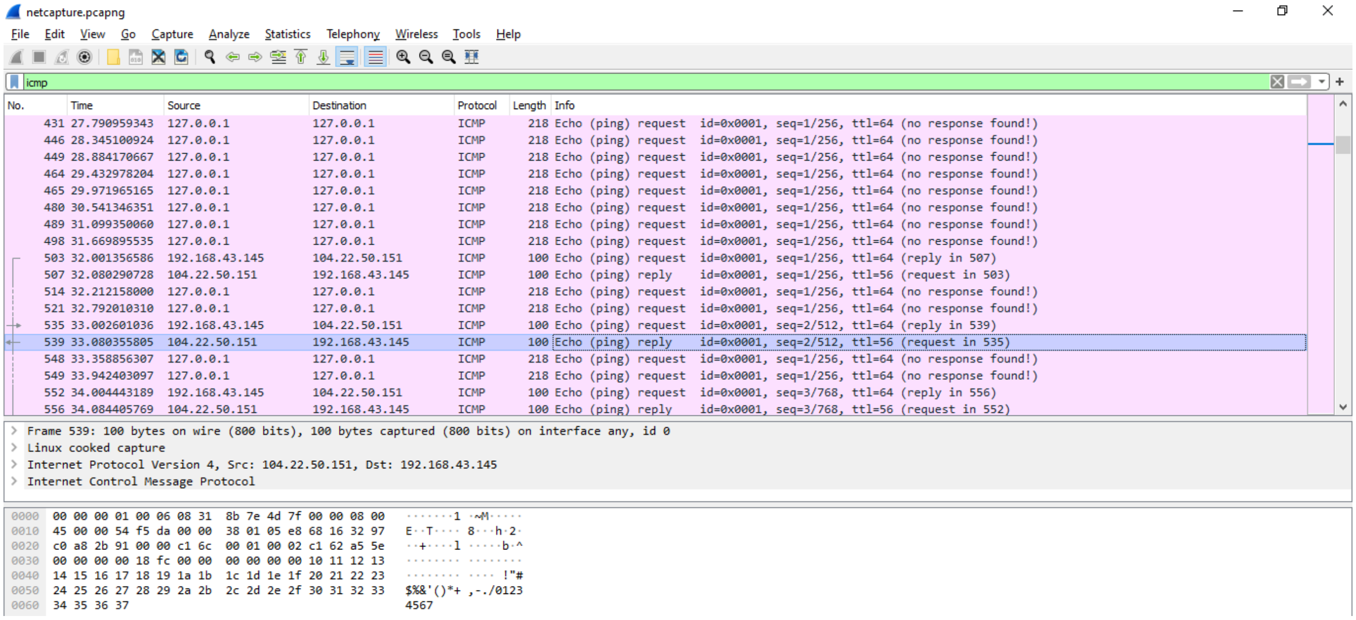
Solution:

Let's see what is happening on that network… after browsing the capture for some time we notice unusual ICMP packets that carry some weird data.



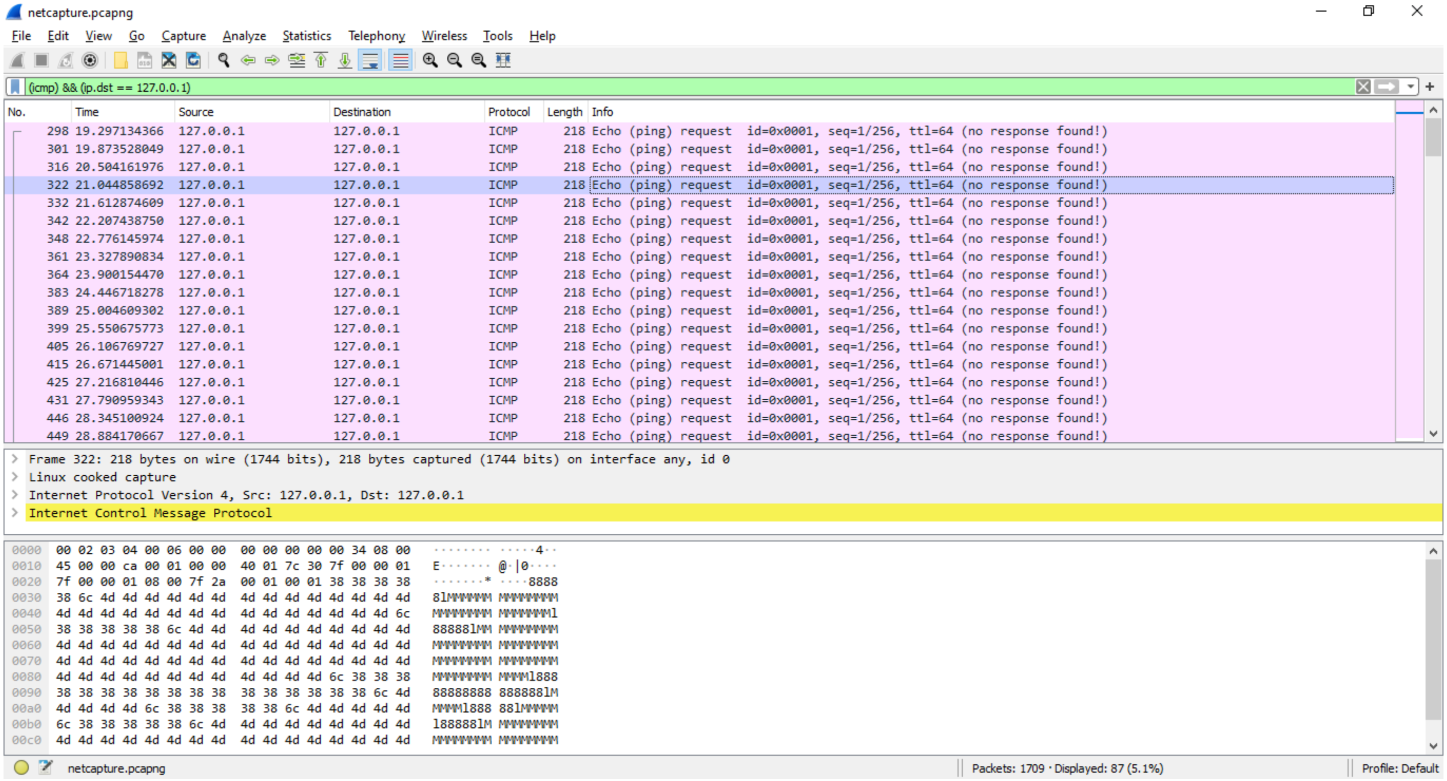
```
No.  Time         Source          Destination     Protocol Length Info
 285 18.360982185 192.168.43.145  216.239.34.21   TCP       68 48302 → 80 [ACK] Seq=77 Ack=181 Win=64128 Len=0 TSval=2942805179 TSecr=469930549
 286 18.998164154 192.168.43.145  192.168.43.1    DNS       73 Standard query 0xaff5 A ifconfig.me
 287 18.998183609 192.168.43.145  192.168.43.1    DNS       73 Standard query 0x98fb AAAA ifconfig.me
 288 19.003654622 192.168.43.1    192.168.43.145  DNS      137 Standard query response 0xaff5 A ifconfig.me A 216.239.36.21 A 216.239.34.21 A 216.239.32.21 A 216.239.38.21
 289 19.003665996 192.168.43.1    192.168.43.145  DNS       73 Standard query response 0x98fb AAAA ifconfig.me
 290 19.003876833 192.168.43.145  216.239.36.21   TCP       76 48398 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2958705568 TSecr=0 WS=128
 291 19.091030759 216.239.36.21   192.168.43.145  TCP       76 80 → 48398 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=539879257 TSecr=2958705568 WS=…
 292 19.091066419 192.168.43.145  216.239.36.21   TCP       68 48398 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2958705655 TSecr=539879257
 293 19.091138138 192.168.43.145  216.239.36.21   HTTP     143 GET / HTTP/1.1
 294 19.168587213 216.239.36.21   192.168.43.145  TCP       68 80 → 48398 [ACK] Seq=1 Ack=76 Win=60416 Len=0 TSval=539879336 TSecr=2958705656
 295 19.291242138 216.239.36.21   192.168.43.145  HTTP     247 HTTP/1.1 200 OK  (text/plain)
 296 19.291279807 192.168.43.145  216.239.36.21   TCP       68 48398 → 80 [ACK] Seq=76 Ack=180 Win=64128 Len=0 TSval=2958705856 TSecr=539879455
 297 19.291991416 192.168.43.145  216.239.36.21   TCP       68 48398 → 80 [FIN, ACK] Seq=76 Ack=180 Win=64128 Len=0 TSval=2958705856 TSecr=539879455
 298 19.297134366 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 299 19.363538694 216.239.36.21   192.168.43.145  TCP       68 80 → 48398 [FIN, ACK] Seq=180 Ack=77 Win=60416 Len=0 TSval=539879530 TSecr=2958705856
 300 19.363569543 192.168.43.145  216.239.36.21   TCP       68 48398 → 80 [ACK] Seq=77 Ack=181 Win=64128 Len=0 TSval=2958705928 TSecr=539879530
 301 19.873528049 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 302 20.007508321 192.168.43.145  192.168.43.1    DNS       73 Standard query 0x15d3 A ifconfig.me

> Frame 298: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface any, id 0
> Linux cooked capture
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Internet Control Message Protocol

0000  00 02 03 04 00 06 00 00  00 00 00 00 70 8e 08 00   ········ ····p···
0010  45 00 00 ca 00 01 00 00  40 01 7c 30 7f 00 00 01   E······· @·|0····
0020  7f 00 00 01 08 00 c8 ce  00 01 00 01 38 38 38 38   ········ ····8888
0030  38 38 38 38 38 38 38 38  38 38 38 38 38 38 38 38   88888888 88888888
0040  38 38 38 38 38 38 38 38  38 38 38 38 38 38 38 38   88888888 88888888
0050  38 38 38 38 38 6c 4d 4d  4d 4d 4d 6c 38 38 38 38   88888lMM MMMl8888
0060  38 38 38 38 38 38 38 6c  4d 4d 4d 4d 4d 4d 4d 4d   8888888l MMMMMMMM
0070  4d 4d 4d 4d 4d 4d 4d 4d  4d 6c 38 38 38 38 38 6c   MMMMMMMM Ml88888l
0080  4d 4d 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 6c 38 38 38   MMMMMMMM MMMMl888
0090  38 38 6c 4d 4d 4d 4d 4d  4d 4d 4d 4d 4d 4d 6c 38   88lMMMMM MMMMMMl8
00a0  38 38 38 38 38 38 38 38  38 38 6c 4d 4d 4d 4d 4d   88888888 88lMMMMM
00b0  6c 38 38 38 38 38 38 38  38 38 38 38 38 38 38 38   l8888888 88888888
00c0  38 38 38 38 38 38 38 38  38 38 38 38 38 38 38 38   88888888 88888888
```

Let's filter for ICMP packets:



```
No.  Time         Source          Destination     Protocol Length Info
 431 27.790959343 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 446 28.345100924 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 449 28.884170667 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 464 29.432978204 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 465 29.971965165 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 480 30.541346351 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 489 31.099350060 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 498 31.669895535 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 503 32.001356586 192.168.43.145  104.22.50.151   ICMP     100 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (reply in 507)
 507 32.080290728 104.22.50.151   192.168.43.145  ICMP     100 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 503)
 514 32.212158000 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 521 32.792010310 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 535 33.002601036 192.168.43.145  104.22.50.151   ICMP     100 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (reply in 539)
 539 33.080355805 104.22.50.151   192.168.43.145  ICMP     100 Echo (ping) reply    id=0x0001, seq=2/512, ttl=56 (request in 535)
 548 33.358856307 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 549 33.942403097 127.0.0.1       127.0.0.1       ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
 552 34.004443189 192.168.43.145  104.22.50.151   ICMP     100 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (reply in 556)
 556 34.084405769 104.22.50.151   192.168.43.145  ICMP     100 Echo (ping) reply    id=0x0001, seq=3/768, ttl=56 (request in 552)

> Frame 539: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
> Linux cooked capture
> Internet Protocol Version 4, Src: 104.22.50.151, Dst: 192.168.43.145
> Internet Control Message Protocol

0000  00 00 00 01 00 06 08 31  8b 7e 4d 7f 00 00 08 00   ·······1 ·~M·····
0010  45 00 00 54 f5 da 00 00  38 01 05 e8 68 16 32 97   E··T···· 8···h·2·
0020  c0 a8 2b 91 00 00 c1 6c  00 01 00 02 c1 62 a5 5e   ··+····l ·····b·^
0030  00 00 00 00 18 fc 00 00  00 00 00 00 10 11 12 13   ········ ········
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ········ ···· !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0060  34 35 36 37                                        4567
```

There is another ICMP flow which seem to ping 104.22.58.151, this doesn’t look interesting for use, lets filter it out and leave only those that has destination IP 127.0.01:


netcapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

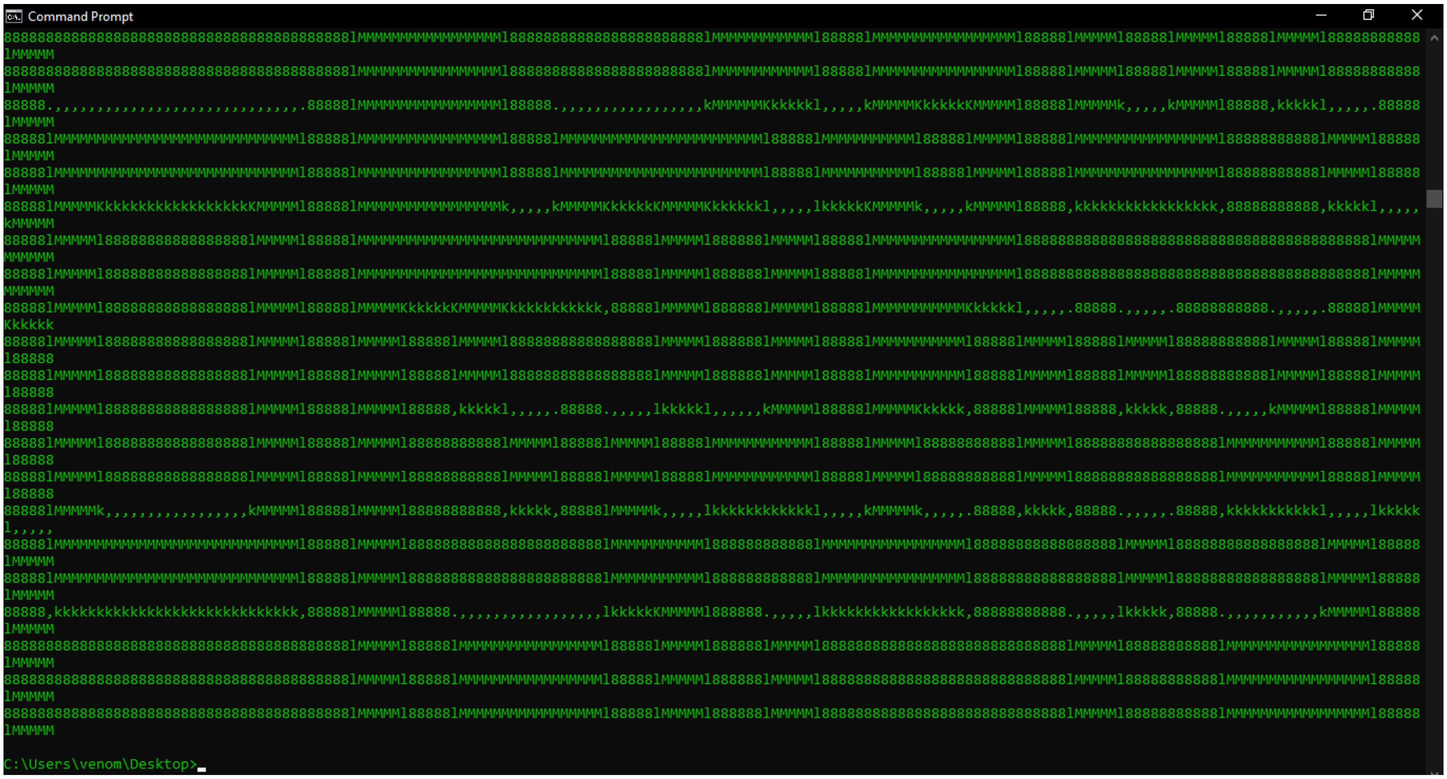
```
(icmp) && (ip.dst == 127.0.0.1)

No.   Time          Source      Destination  Protocol Length Info
  298 19.297134366  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  301 19.873528049  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  316 20.504161976  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  322 21.044858692  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  332 21.612874609  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  342 22.207438750  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  348 22.776145974  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  361 23.327890834  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  364 23.900154470  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  383 24.446718278  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  389 25.004609302  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  399 25.550675773  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  405 26.106769727  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  415 26.671445001  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  425 27.216810446  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  431 27.790959343  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  446 28.345100924  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)
  449 28.884170667  127.0.0.1   127.0.0.1    ICMP     218 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (no response found!)

> Frame 322: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface any, id 0
> Linux cooked capture
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Internet Control Message Protocol

0000  00 02 03 04 00 06 00 00  00 00 00 00 00 34 08 00   ········ ·····4··
0010  45 00 00 ca 00 01 00 00  40 01 7c 30 7f 00 00 01   E······· @·|0····
0020  7f 00 00 01 08 00 7f 2a  00 01 00 01 38 38 38 38   ·······* ····8888
0030  38 6c 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 4d 4d 4d 4d   8lMMMMMM MMMMMMMM
0040  4d 4d 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 4d 4d 4d 6c   MMMMMMMM MMMMMMMl
0050  38 38 38 38 38 6c 4d 4d  4d 4d 4d 4d 4d 4d 4d 4d   88888lMM MMMMMMMM
0060  4d 4d 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 4d 4d 4d 4d   MMMMMMMM MMMMMMMM
0070  4d 4d 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 4d 4d 4d 4d   MMMMMMMM MMMMMMMM
0080  4d 4d 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 6c 38 38 38   MMMMMMMM MMMMl888
0090  38 38 38 38 38 38 38 38  38 38 38 38 38 38 6c 4d   88888888 888888lM
00a0  4d 4d 4d 4d 6c 38 38 38  38 38 6c 4d 4d 4d 4d 4d   MMMMl888 88lMMMMM
00b0  6c 38 38 38 38 38 6c 4d  4d 4d 4d 4d 4d 4d 4d 4d   l88888lM MMMMMMMM
00c0  4d 4d 4d 4d 4d 4d 4d 4d  4d 4d 4d 4d 4d 4d 4d 4d   MMMMMMMM MMMMMMMM

netcapture.pcapng    Packets: 1709 · Displayed: 87 (5.1%)    Profile: Default
```

Now we have 87 packets, and the data inside them doesn’t seem to make any sense…

Let’s extract this data to get more flexibility manipulating it, unfortunately there is no good way to do that using wireshark, hence we will use tshark.

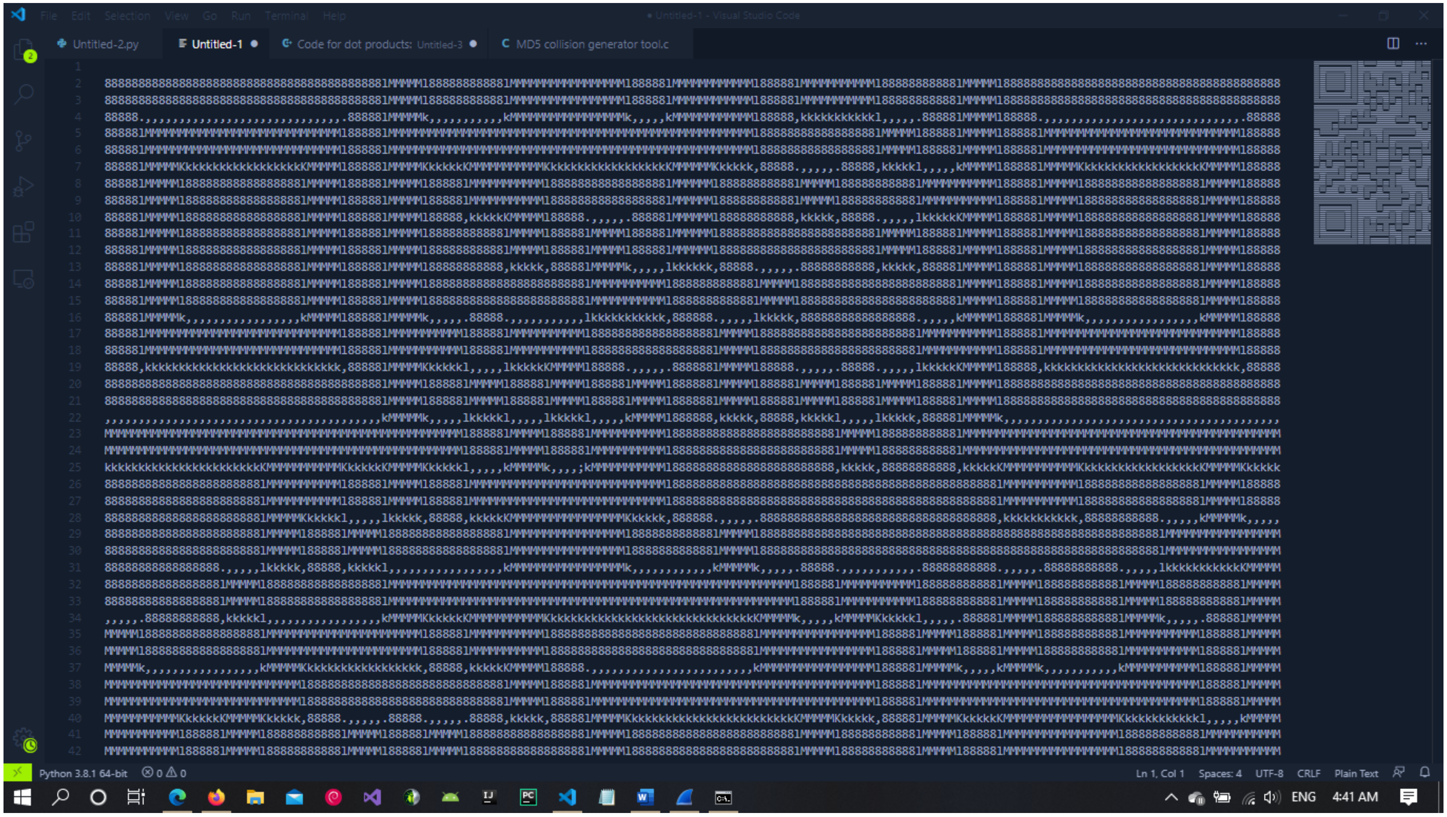
Use the following tshark command to extract the data we need:

tshark -2 -r netcapture.pcapng -R "(icmp) && (ip.dst == 127.0.0.1)" -o data.show_as_text:TRUE -T fields -e data.text

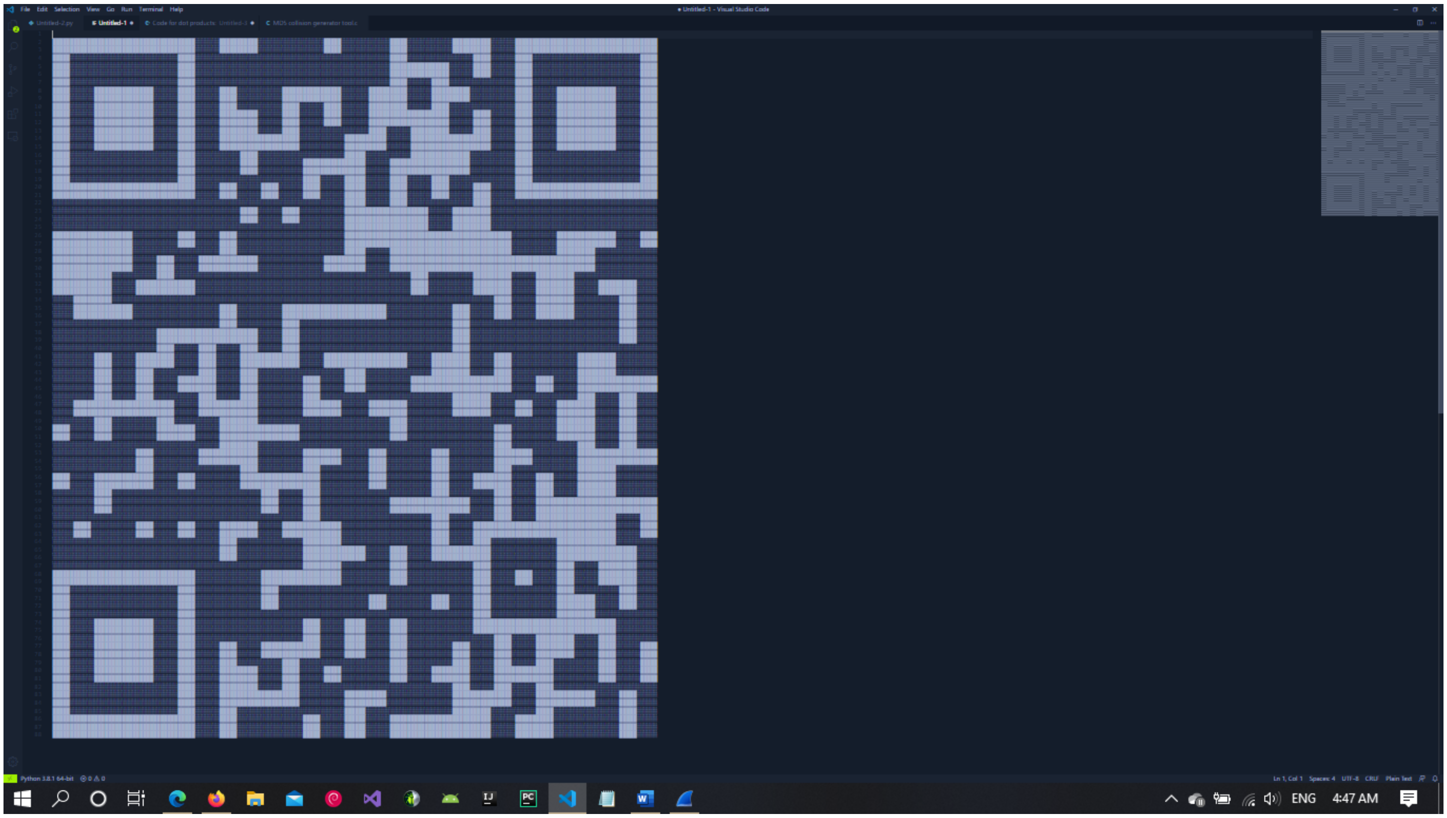


```
8888888888888888888888888888888888888888lMMMMMMMMMMMMMMMMMl8888888888888888888888888lMMMMMMMMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMl88888lMMMMMl88888lMMMMMl88888888888
lMMMMM
8888888888888888888888888888888888888888lMMMMMMMMMMMMMMMMMl8888888888888888888888888lMMMMMMMMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMl88888lMMMMMl88888lMMMMMl88888888888
lMMMMM
88888.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.88888lMMMMMMMMMMMMMMMMMMl88888.,,,,,,,,,,,,,,,,,kMMMMMMKkkkkl,,,,,kMMMMMKkkkkKMMMMMl88888lMMMMMk,,,,,kMMMMMl88888,kkkkkl,,,,,.88888
lMMMMM
88888lMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMMMMMMMl88888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888888888lMMMMMl88888
lMMMMM
88888lMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMMMMMMMl88888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888888888lMMMMMl88888
lMMMMM
88888lMMMMMKkkkkkkkkkkkkkkkkKMMMMMl88888lMMMMMMMMMMMMMMMMMMk,,,,,kMMMMMKkkkkkKMMMMMKkkkkkkl,,,,,lkkkkkKMMMMMk,,,,,kMMMMMl88888,kkkkkkkkkkkkkkkk,8888888888,kkkkkl,,,,,
kMMMMM
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMl888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl8888888888888888888888888888888888888888lMMMMM
MMMMMM
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMl888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl8888888888888888888888888888888888888888lMMMMM
MMMMMM
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMKkkkkkKMMMMMKkkkkkkkkkkk,88888lMMMMMl888888lMMMMMl88888lMMMMMMMMMMMKkkkkkl,,,,,.88888.,,,,,,.88888888888.,,,,,,.88888lMMMMM
Kkkkkk
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMl88888lMMMMMl88888888888888888lMMMMMl888888lMMMMMl88888lMMMMMMMMMMMl88888lMMMMMl88888lMMMMMl88888888888lMMMMMl88888lMMMMM
l88888
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMl88888lMMMMMl88888888888888888lMMMMMl888888lMMMMMl88888lMMMMMMMMMMMl88888lMMMMMl88888lMMMMMl88888888888lMMMMMl88888lMMMMM
l88888
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMl88888,kkkkkl,,,,,.88888.,,,,,lkkkkkl,,,,,kMMMMMl88888lMMMMMKkkkkk,88888lMMMMMl88888,kkkkk,88888.,,,,,kMMMMMl88888lMMMMM
l88888
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMl88888888888lMMMMMl88888lMMMMMl88888lMMMMMMMMMMMMl88888lMMMMMl88888888888lMMMMMl88888888888888888lMMMMMMMMMMMl88888lMMMMM
l88888
88888lMMMMMl88888888888888888lMMMMMl88888lMMMMMl88888888888lMMMMMl88888lMMMMMl88888lMMMMMMMMMMMMl88888lMMMMMl88888888888lMMMMMl88888888888888888lMMMMMMMMMMMl88888lMMMMM
l88888
88888lMMMMMk,,,,,,,,,,,,,,,,kMMMMMl88888lMMMMMl88888888888,kkkkk,88888lMMMMMk,,,,,lkkkkkkkkkkkkl,,,,,kMMMMMk,,,,,.88888,kkkkk,88888.,,,,,,.88888,kkkkkkkkkkl,,,,,lkkkkk
l,,,,,
88888lMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMl8888888888888888888888888lMMMMMMMMMMMl888888888888lMMMMMMMMMMMMMMMMMMl88888888888888888lMMMMMl88888888888888888lMMMMMl88888
lMMMMM
88888lMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMl88888lMMMMMl8888888888888888888888888lMMMMMMMMMMMl888888888888lMMMMMMMMMMMMMMMMMMl88888888888888888lMMMMMl88888888888888888lMMMMMl88888
lMMMMM
88888,kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk,88888lMMMMMl88888.,,,,,,,,,,,,,,,,,lkkkkkKMMMMMl888888.,,,,,lkkkkkkkkkkkkkkkkk,88888888888.,,,,,lkkkkk,88888.,,,,,,,,,,,,kMMMMMl88888
lMMMMM
8888888888888888888888888888888888888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMl888888lMMMMMl8888888888888888888888888888888lMMMMMl88888888888lMMMMMMMMMMMMMMMMMMl88888
lMMMMM
8888888888888888888888888888888888888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMl888888lMMMMMl8888888888888888888888888888888lMMMMMl88888888888lMMMMMMMMMMMMMMMMMMl88888
lMMMMM
8888888888888888888888888888888888888888lMMMMMl88888lMMMMMMMMMMMMMMMMMMl88888lMMMMMl888888lMMMMMl8888888888888888888888888888888lMMMMMl88888888888lMMMMMMMMMMMMMMMMMMl88888
lMMMMM

C:\Users\venom\Desktop>
```

We got what we need, now let's copy and paste it in some nice text editor (I used VScode, sublime is a good choice as well):


File Edit Selection View Go Run Terminal Help
● Untitled-1 - Visual Studio Code
Untitled-2.py
Untitled-1 ●
Code for dot products: Untitled-3 ●
MD5 collision generator tool.c
Python 3.8.1 64-bit
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF Plain Text
ENG 4:41 AM

OMG! What do we see here? That's a QR code! Lets use some Unicode characters for box drawing to make it scannable (░ and █), will change all occurrences of 8 to █ and the rest to ░, then make it smaller to fit the screen:



Now just scan it, and the flag is in your hands: CTCTF{l3ak1ng_QRs_7hr0u6h_1CMP_tunn3l$}.