Computer Engineering 4DN4
Laboratory 1
Network Scanning and Packet Sniffing

2023-02-07

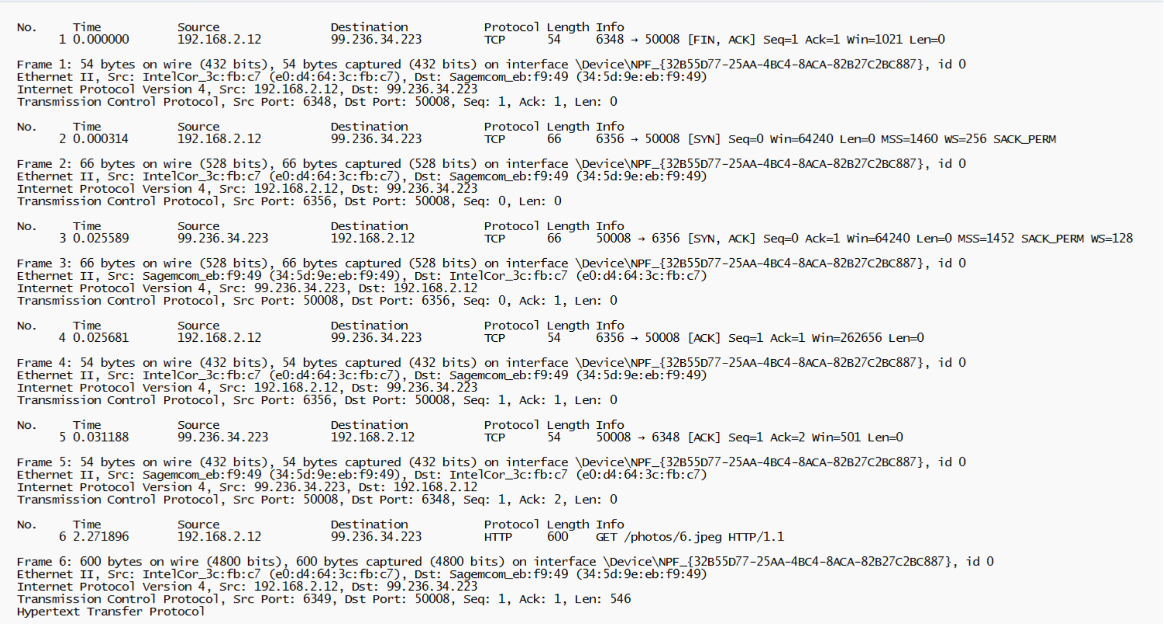
400195279 | Yinwen Xu | xuy212 | xuy212@mcmaster.ca

400241747 | Hengbo Huang| huanh3| huanh3@mcmaster.ca

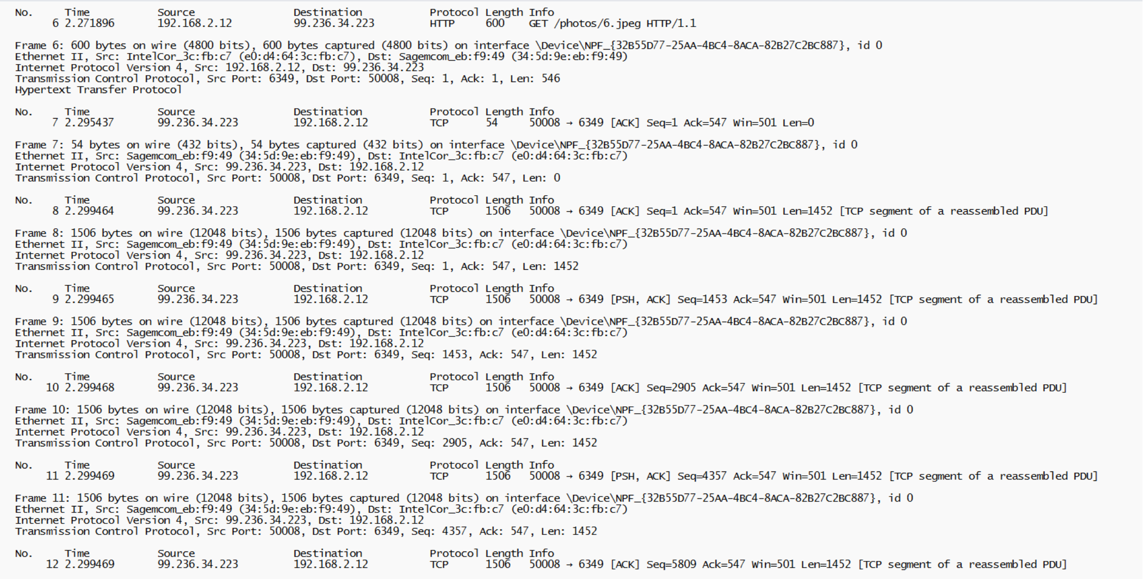
Experiments

TCP:

The picture download is 6.jpg

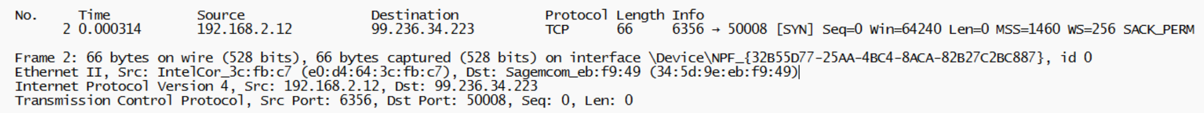


```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       192.168.2.12          99.236.34.223         TCP      54     6348 → 50008 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6348, Dst Port: 50008, Seq: 1, Ack: 1, Len: 0

No.     Time           Source                Destination           Protocol Length Info
      2 0.000314       192.168.2.12          99.236.34.223         TCP      66     6356 → 50008 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6356, Dst Port: 50008, Seq: 0, Len: 0

No.     Time           Source                Destination           Protocol Length Info
      3 0.025589       99.236.34.223         192.168.2.12          TCP      66     50008 → 6356 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6356, Seq: 0, Ack: 1, Len: 0

No.     Time           Source                Destination           Protocol Length Info
      4 0.025681       192.168.2.12          99.236.34.223         TCP      54     6356 → 50008 [ACK] Seq=1 Ack=1 Win=262656 Len=0

Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6356, Dst Port: 50008, Seq: 1, Ack: 1, Len: 0

No.     Time           Source                Destination           Protocol Length Info
      5 0.031188       99.236.34.223         192.168.2.12          TCP      54     50008 → 6348 [ACK] Seq=1 Ack=2 Win=501 Len=0

Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6348, Seq: 1, Ack: 2, Len: 0

No.     Time           Source                Destination           Protocol Length Info
      6 2.271896       192.168.2.12          99.236.34.223         HTTP     600    GET /photos/6.jpeg HTTP/1.1

Frame 6: 600 bytes on wire (4800 bits), 600 bytes captured (4800 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6349, Dst Port: 50008, Seq: 1, Ack: 1, Len: 546
Hypertext Transfer Protocol
```



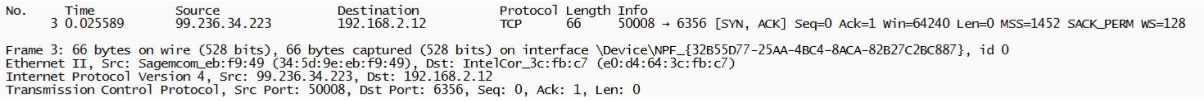
```
No.     Time           Source                Destination           Protocol Length Info
      6 2.271896       192.168.2.12          99.236.34.223         HTTP     600    GET /photos/6.jpeg HTTP/1.1

Frame 6: 600 bytes on wire (4800 bits), 600 bytes captured (4800 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6349, Dst Port: 50008, Seq: 1, Ack: 1, Len: 546
Hypertext Transfer Protocol

No.     Time           Source                Destination           Protocol Length Info
      7 2.295437       99.236.34.223         192.168.2.12          TCP      54     50008 → 6349 [ACK] Seq=1 Ack=547 Win=501 Len=0

Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6349, Seq: 1, Ack: 547, Len: 0

No.     Time           Source                Destination           Protocol Length Info
      8 2.299464       99.236.34.223         192.168.2.12          TCP      1506   50008 → 6349 [ACK] Seq=1 Ack=547 Win=501 Len=1452 [TCP segment of a reassembled PDU]

Frame 8: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6349, Seq: 1, Ack: 547, Len: 1452

No.     Time           Source                Destination           Protocol Length Info
      9 2.299465       99.236.34.223         192.168.2.12          TCP      1506   50008 → 6349 [PSH, ACK] Seq=1453 Ack=547 Win=501 Len=1452 [TCP segment of a reassembled PDU]

Frame 9: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6349, Seq: 1453, Ack: 547, Len: 1452

No.     Time           Source                Destination           Protocol Length Info
     10 2.299468       99.236.34.223         192.168.2.12          TCP      1506   50008 → 6349 [ACK] Seq=2905 Ack=547 Win=501 Len=1452 [TCP segment of a reassembled PDU]

Frame 10: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6349, Seq: 2905, Ack: 547, Len: 1452

No.     Time           Source                Destination           Protocol Length Info
     11 2.299469       99.236.34.223         192.168.2.12          TCP      1506   50008 → 6349 [PSH, ACK] Seq=4357 Ack=547 Win=501 Len=1452 [TCP segment of a reassembled PDU]

Frame 11: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6349, Seq: 4357, Ack: 547, Len: 1452

No.     Time           Source                Destination           Protocol Length Info
     12 2.299469       99.236.34.223         192.168.2.12          TCP      1506   50008 → 6349 [ACK] Seq=5809 Ack=547 Win=501 Len=1452 [TCP segment of a reassembled PDU]
```

Discussion:
From the first picture of the wireshark data, we can see the three hand shake between my computer (IP 192.168.2.12) and the IP address of compeng4dn4.mooo.com (99.236.34.223). First hand shake :



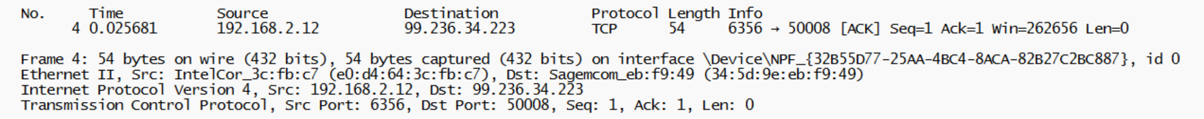
```
No.     Time           Source                Destination           Protocol Length Info
      2 0.000314       192.168.2.12          99.236.34.223         TCP      66     6356 → 50008 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)|
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6356, Dst Port: 50008, Seq: 0, Len: 0
```

Client (my computer) sends a SYN packet (SEQ=0) to the server (compeng4dn4.mooo.com).
Second hand shake:



```
No.     Time           Source                Destination           Protocol Length Info
      3 0.025589       99.236.34.223         192.168.2.12          TCP      66     50008 → 6356 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 99.236.34.223, Dst: 192.168.2.12
Transmission Control Protocol, Src Port: 50008, Dst Port: 6356, Seq: 0, Ack: 1, Len: 0
```

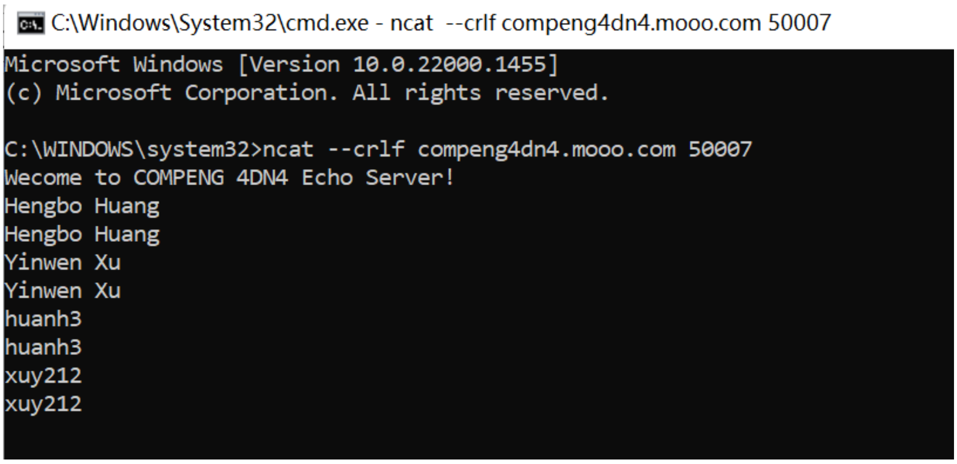
The server receives the SYN packet, confirms the client's SYN (ack=0+1), and at the same time sends a SYN packet (SEQ=0), that is, the SYN+ACK packet. At this time, the server enters the SYN_RECV state.
Third hand shake:



```
No.     Time           Source                Destination           Protocol Length Info
      4 0.025681       192.168.2.12          99.236.34.223         TCP      54     6356 → 50008 [ACK] Seq=1 Ack=1 Win=262656 Len=0

Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 99.236.34.223
Transmission Control Protocol, Src Port: 6356, Dst Port: 50008, Seq: 1, Ack: 1, Len: 0
```

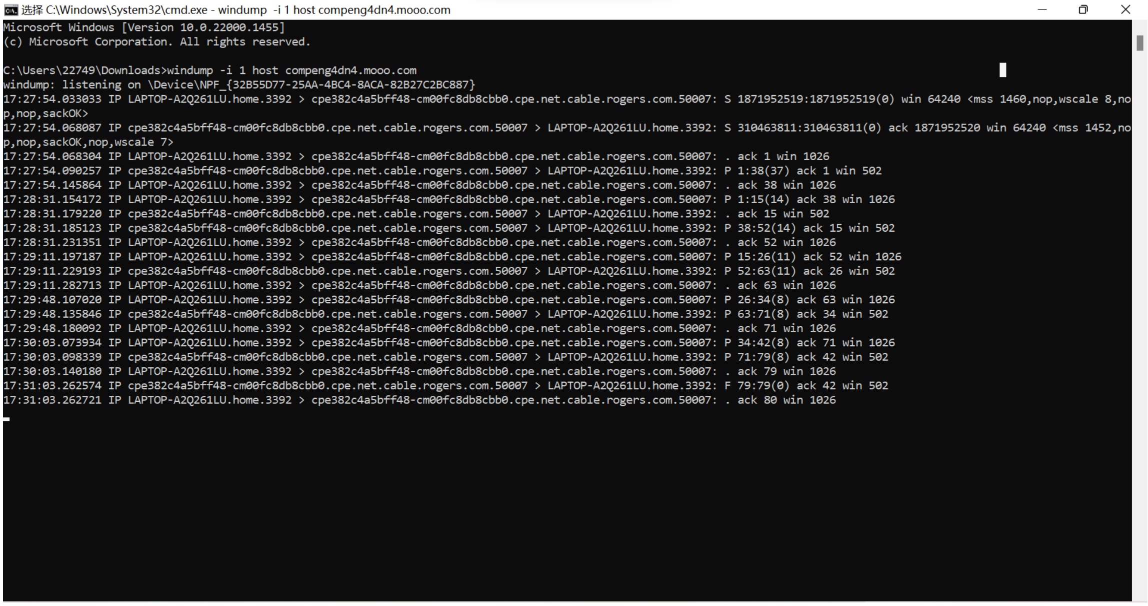
Client receives the SYN+ACK packet from the server and sends an ACK (ack=0+1) to the client. After the packet is sent, client and server enter the Established state and complete the three-way handshake.
The else data of wire shark is about transmission of the picture.

TCP:



C:\Windows\System32\cmd.exe - ncat --crlf compeng4dn4.mooo.com 50007

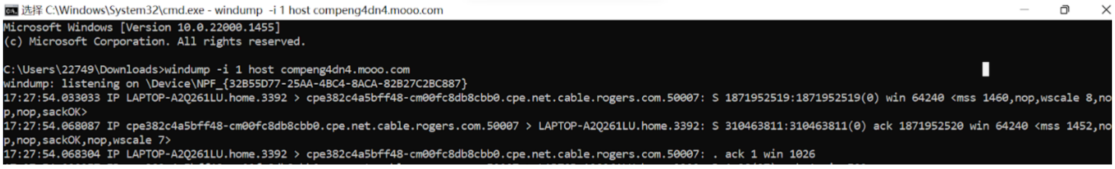
```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ncat --crlf compeng4dn4.mooo.com 50007
Wecome to COMPENG 4DN4 Echo Server!
Hengbo Huang
Hengbo Huang
Yinwen Xu
Yinwen Xu
huanh3
huanh3
xuy212
xuy212
```



选择 C:\Windows\System32\cmd.exe - windump -i 1 host compeng4dn4.mooo.com

```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\Users\22749\Downloads>windump -i 1 host compeng4dn4.mooo.com
windump: listening on \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}
17:27:54.033033 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: S 1871952519:1871952519(0) win 64240 <mss 1460,nop,wscale 8,no
p,nop,sackOK>
17:27:54.068087 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: S 310463811:310463811(0) ack 1871952520 win 64240 <mss 1452,no
p,nop,sackOK,nop,wscale 7>
17:27:54.068304 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 1 win 1026
17:27:54.090257 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: P 1:38(37) ack 1 win 502
17:27:54.145864 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 38 win 1026
17:28:31.154172 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: P 1:15(14) ack 38 win 1026
17:28:31.179220 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: . ack 15 win 502
17:28:31.185123 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: P 38:52(14) ack 15 win 502
17:28:31.231351 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 52 win 1026
17:29:11.197187 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: P 15:26(11) ack 52 win 1026
17:29:11.229193 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: P 52:63(11) ack 26 win 502
17:29:11.282713 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 63 win 1026
17:29:48.107020 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: P 26:34(8) ack 63 win 1026
17:29:48.135846 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: P 63:71(8) ack 34 win 502
17:29:48.180092 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 71 win 1026
17:30:03.073934 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: P 34:42(8) ack 71 win 1026
17:30:03.098339 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: P 71:79(8) ack 42 win 502
17:30:03.140180 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 79 win 1026
17:31:03.262574 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: F 79:79(0) ack 42 win 502
17:31:03.262721 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 80 win 1026
```

Discussion:

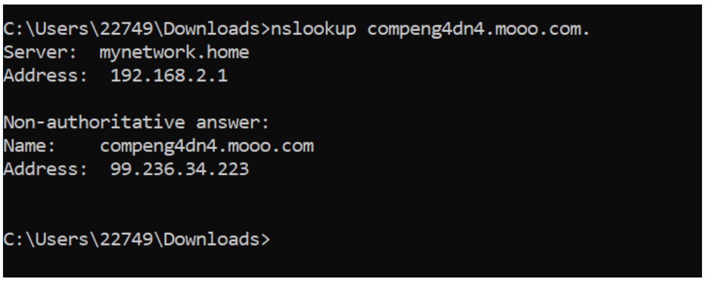


选择 C:\Windows\System32\cmd.exe - windump -i 1 host compeng4dn4.mooo.com

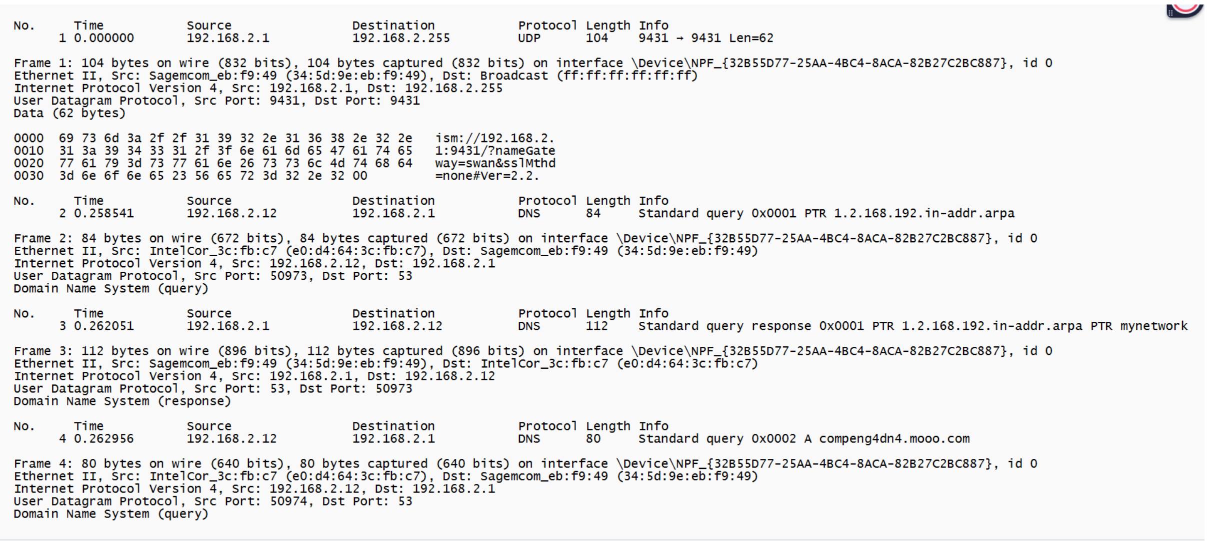
```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\Users\22749\Downloads>windump -i 1 host compeng4dn4.mooo.com
windump: listening on \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}
17:27:54.033033 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: S 1871952519:1871952519(0) win 64240 <mss 1460,nop,wscale 8,no
p,nop,sackOK>
17:27:54.068087 IP cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007 > LAPTOP-A2Q261LU.home.3392: S 310463811:310463811(0) ack 1871952520 win 64240 <mss 1452,no
p,nop,sackOK,nop,wscale 7>
17:27:54.068304 IP LAPTOP-A2Q261LU.home.3392 > cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com.50007: . ack 1 win 1026
```

This is the picture of the three handshakes. The first handshake is at 17:27:54 from the IP of my computer to compng4dn4.mooo.com, Port 50007. My computer sent a SYN request with sequence number 1871952519.
The second handshake is at 17:27:54 , from compng4dn4.mooo.com to my computer. It shows compng4dn4.mooo.com confirms my TCP connection request. Ack 187195250 is the confirmation sequence number, which is the initial sequence number of the request that is increased by 1.
The third handshake is at 17:27:54, the client returns ack 1. The three handshakes end and TCP connection is established.
At 17:31:03 we receive a flag [F] which indicates the connection ends.

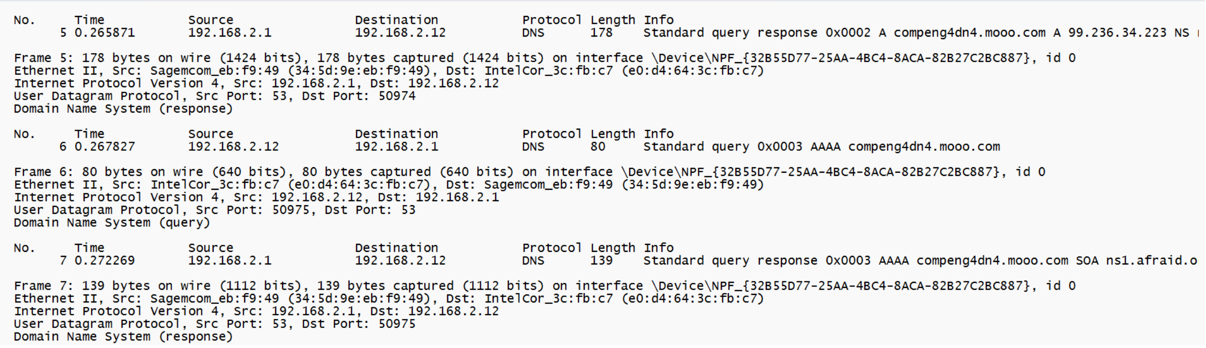
DNS



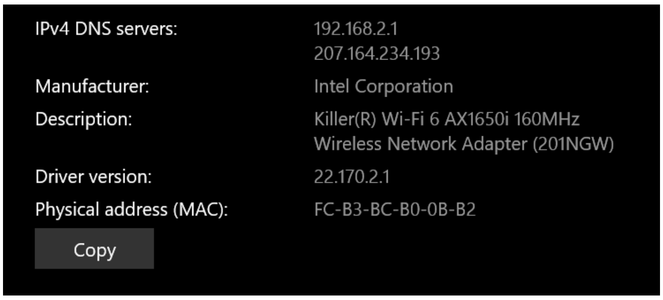
```
C:\Users\22749\Downloads>nslookup compeng4dn4.mooo.com.
Server:  mynetwork.home
Address:  192.168.2.1

Non-authoritative answer:
Name:    compeng4dn4.mooo.com
Address:  99.236.34.223


C:\Users\22749\Downloads>
```



```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       192.168.2.1           192.168.2.255         UDP      104    9431 → 9431 Len=62

Frame 1: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.255
User Datagram Protocol, Src Port: 9431, Dst Port: 9431
Data (62 bytes)

0000  69 73 6d 3a 2f 2f 31 39 32 2e 31 36 38 2e 32 2e   ism://192.168.2.
0010  31 3a 39 34 33 31 2f 3f 6e 61 6d 65 47 61 74 65   1:9431/?nameGate
0020  77 61 79 3d 73 77 61 6e 26 73 73 6c 4d 74 68 64   way=swan&sslMthd
0030  3d 6e 6f 6e 65 23 56 65 72 3d 32 2e 32 00         =none#Ver=2.2.

No.     Time           Source                Destination           Protocol Length Info
      2 0.258541       192.168.2.12          192.168.2.1           DNS      84     Standard query 0x0001 PTR 1.2.168.192.in-addr.arpa

Frame 2: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 50973, Dst Port: 53
Domain Name System (query)

No.     Time           Source                Destination           Protocol Length Info
      3 0.262051       192.168.2.1           192.168.2.12          DNS      112    Standard query response 0x0001 PTR 1.2.168.192.in-addr.arpa PTR mynetwork

Frame 3: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.12
User Datagram Protocol, Src Port: 53, Dst Port: 50973
Domain Name System (response)

No.     Time           Source                Destination           Protocol Length Info
      4 0.262956       192.168.2.12          192.168.2.1           DNS      80     Standard query 0x0002 A compeng4dn4.mooo.com

Frame 4: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 50974, Dst Port: 53
Domain Name System (query)
```



```
No.     Time           Source                Destination           Protocol Length Info
      5 0.265871       192.168.2.1           192.168.2.12          DNS      178    Standard query response 0x0002 A compeng4dn4.mooo.com A 99.236.34.223 NS

Frame 5: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.12
User Datagram Protocol, Src Port: 53, Dst Port: 50974
Domain Name System (response)

No.     Time           Source                Destination           Protocol Length Info
      6 0.267827       192.168.2.12          192.168.2.1           DNS      80     Standard query 0x0003 AAAA compeng4dn4.mooo.com

Frame 6: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7), Dst: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49)
Internet Protocol Version 4, Src: 192.168.2.12, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 50975, Dst Port: 53
Domain Name System (query)

No.     Time           Source                Destination           Protocol Length Info
      7 0.272269       192.168.2.1           192.168.2.12          DNS      139    Standard query response 0x0003 AAAA compeng4dn4.mooo.com SOA ns1.afraid.o

Frame 7: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface \Device\NPF_{32B55D77-25AA-4BC4-8ACA-82B27C2BC887}, id 0
Ethernet II, Src: Sagemcom_eb:f9:49 (34:5d:9e:eb:f9:49), Dst: IntelCor_3c:fb:c7 (e0:d4:64:3c:fb:c7)
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.12
User Datagram Protocol, Src Port: 53, Dst Port: 50975
Domain Name System (response)
```



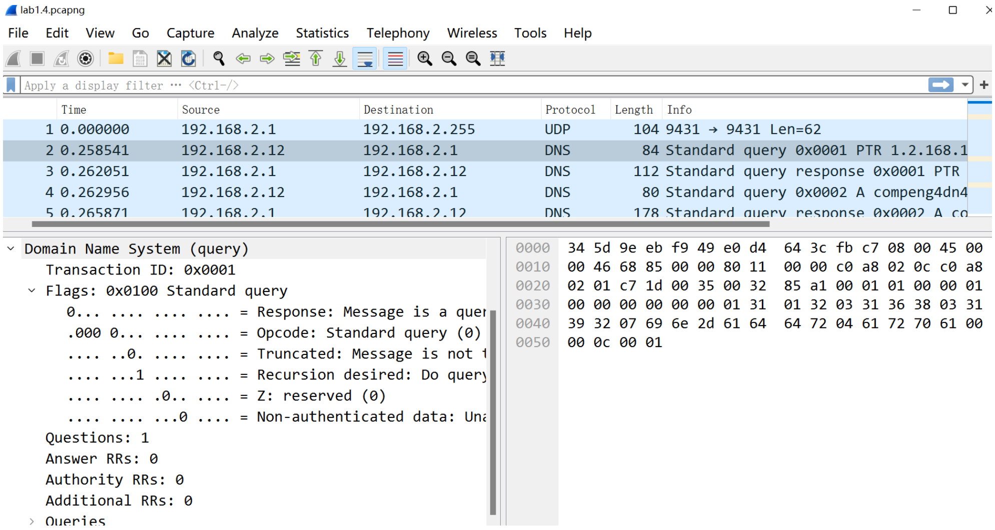
IPv4 DNS servers: 192.168.2.1
207.164.234.193

Manufacturer: Intel Corporation

Description: Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)

Driver version: 22.170.2.1

Physical address (MAC): FC-B3-BC-B0-0B-B2



lab1.4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

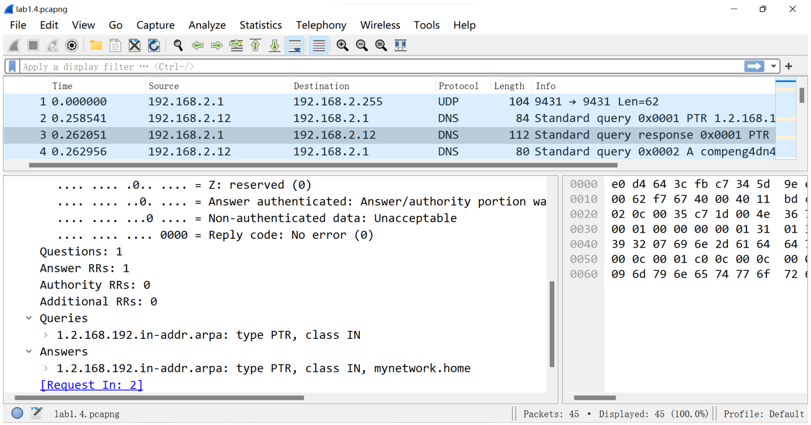
```
  Time         Source          Destination      Protocol  Length  Info
1 0.000000     192.168.2.1     192.168.2.255    UDP          104  9431 → 9431 Len=62
2 0.258541     192.168.2.12    192.168.2.1      DNS           84  Standard query 0x0001 PTR 1.2.168.1
3 0.262051     192.168.2.1     192.168.2.12     DNS          112  Standard query response 0x0001 PTR
4 0.262956     192.168.2.12    192.168.2.1      DNS           80  Standard query 0x0002 A compeng4dn4
5 0.265871     192.168.2.1     192.168.2.12     DNS          178  Standard query response 0x0002 A co
```

```
˅ Domain Name System (query)
    Transaction ID: 0x0001
  ˅ Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a quer
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not t
        .... ...1 .... .... = Recursion desired: Do query
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Una
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  › Queries
```

```
0000  34 5d 9e eb f9 49 e0 d4  64 3c fb c7 08 00 45 00
0010  00 46 68 85 00 00 80 11  00 00 c0 a8 02 0c c0 a8
0020  02 01 c7 1d 00 35 00 32  85 a1 00 01 01 00 00 01
0030  00 00 00 00 00 00 01 31  01 32 03 31 36 38 03 31
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00
0050  00 0c 00 01
```

From No.2 it shows that a standard query is sent to 192.168.2.1, we check the internet and it shows this IP address is DNS server. The Opcode is 0 means this is a standard query. There is only questions is 1 means only one query sequence, the other three is 0. This message is encapsulated on the UDP protocol, sent to the DNS server with port 53.

There are three questions and three answers.



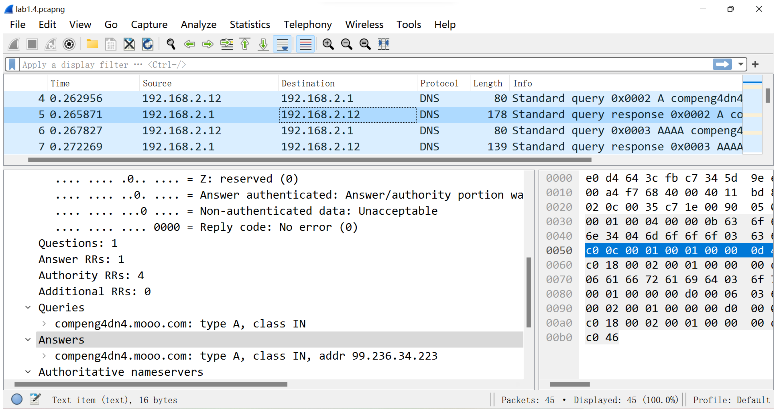
lab1.4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
  Time         Source          Destination      Protocol  Length  Info
1 0.000000     192.168.2.1     192.168.2.255    UDP          104  9431 → 9431 Len=62
2 0.258541     192.168.2.12    192.168.2.1      DNS           84  Standard query 0x0001 PTR 1.2.168.1
3 0.262051     192.168.2.1     192.168.2.12     DNS          112  Standard query response 0x0001 PTR
4 0.262956     192.168.2.12    192.168.2.1      DNS           80  Standard query 0x0002 A compeng4dn4
```

```
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion wa
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    › 1.2.168.192.in-addr.arpa: type PTR, class IN
  ˅ Answers
    › 1.2.168.192.in-addr.arpa: type PTR, class IN, mynetwork.home
    [Request In: 2]
```

```
0000  e0 d4 64 3c fb c7 34 5d  9e
0010  00 62 f7 67 40 00 40 11  bd
0020  02 0c 00 35 c7 1d 00 4e  36
0030  00 01 00 00 00 00 01 31  01
0040  39 32 07 69 6e 2d 61 64  64
0050  00 0c 00 01 c0 0c 00 0c  00
0060  09 6d 79 6e 65 74 77 6f  72
```

lab1. 4. pcapng | Packets: 45 • Displayed: 45 (100.0%) | Profile: Default



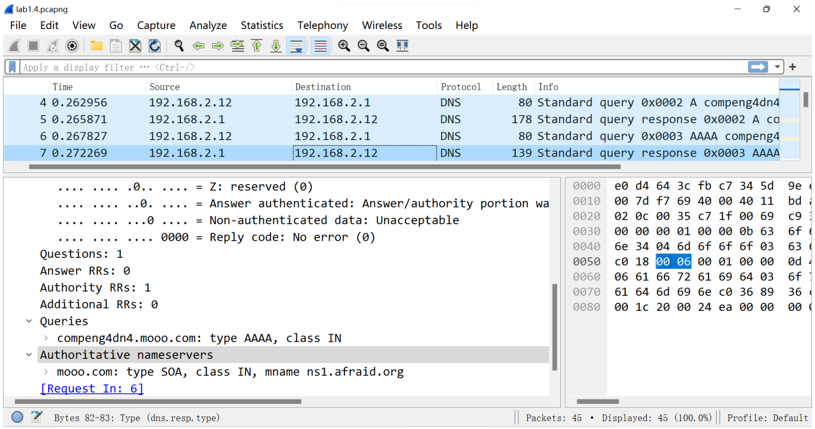
lab1.4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
  Time         Source          Destination      Protocol  Length  Info
4 0.262956     192.168.2.12    192.168.2.1      DNS           80  Standard query 0x0002 A compeng4dn4
5 0.265871     192.168.2.1     192.168.2.12     DNS          178  Standard query response 0x0002 A co
6 0.267827     192.168.2.12    192.168.2.1      DNS           80  Standard query 0x0003 AAAA compeng4
7 0.272269     192.168.2.1     192.168.2.12     DNS          139  Standard query response 0x0003 AAAA
```

```
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion wa
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 0
  ˅ Queries
    › compeng4dn4.mooo.com: type A, class IN
  ˅ Answers
    › compeng4dn4.mooo.com: type A, class IN, addr 99.236.34.223
  ˅ Authoritative nameservers
```

```
0000  e0 d4 64 3c fb c7 34 5d  9e
0010  00 a4 f7 68 40 00 40 11  bd
0020  02 0c 00 35 c7 1e 00 90  05
0030  00 01 00 04 00 00 0b 63  6f
0040  6e 34 04 6d 6f 6f 6f 03  63
0050  c0 0c 00 01 00 01 00 00  0d
0060  c0 18 00 02 00 01 00 00  00
0070  06 61 66 72 61 69 64 03  6f
0080  00 01 00 00 00 d0 00 06  03
0090  00 02 00 01 00 00 00 d0  00
00a0  c0 18 00 02 00 01 00 00  00
00b0  c0 46
```

Text item (text), 16 bytes | Packets: 45 • Displayed: 45 (100.0%) | Profile: Default



lab1.4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

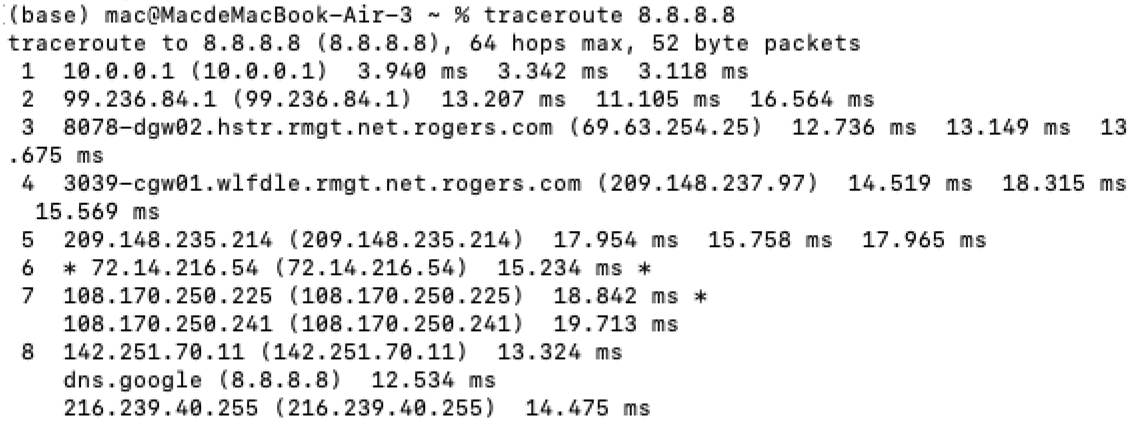
```
  Time       Source         Destination    Protocol  Length  Info
4 0.262956   192.168.2.12   192.168.2.1    DNS        80 Standard query 0x0002 A compeng4dn4
5 0.265871   192.168.2.1    192.168.2.12   DNS       178 Standard query response 0x0002 A co
6 0.267827   192.168.2.12   192.168.2.1    DNS        80 Standard query 0x0003 AAAA compeng4
7 0.272269   192.168.2.1    192.168.2.12   DNS       139 Standard query response 0x0003 AAAA
```

```
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion wa
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
⌄ Queries
  › compeng4dn4.mooo.com: type AAAA, class IN
⌄ Authoritative nameservers
  › mooo.com: type SOA, class IN, mname ns1.afraid.org
  [Request In: 6]
```

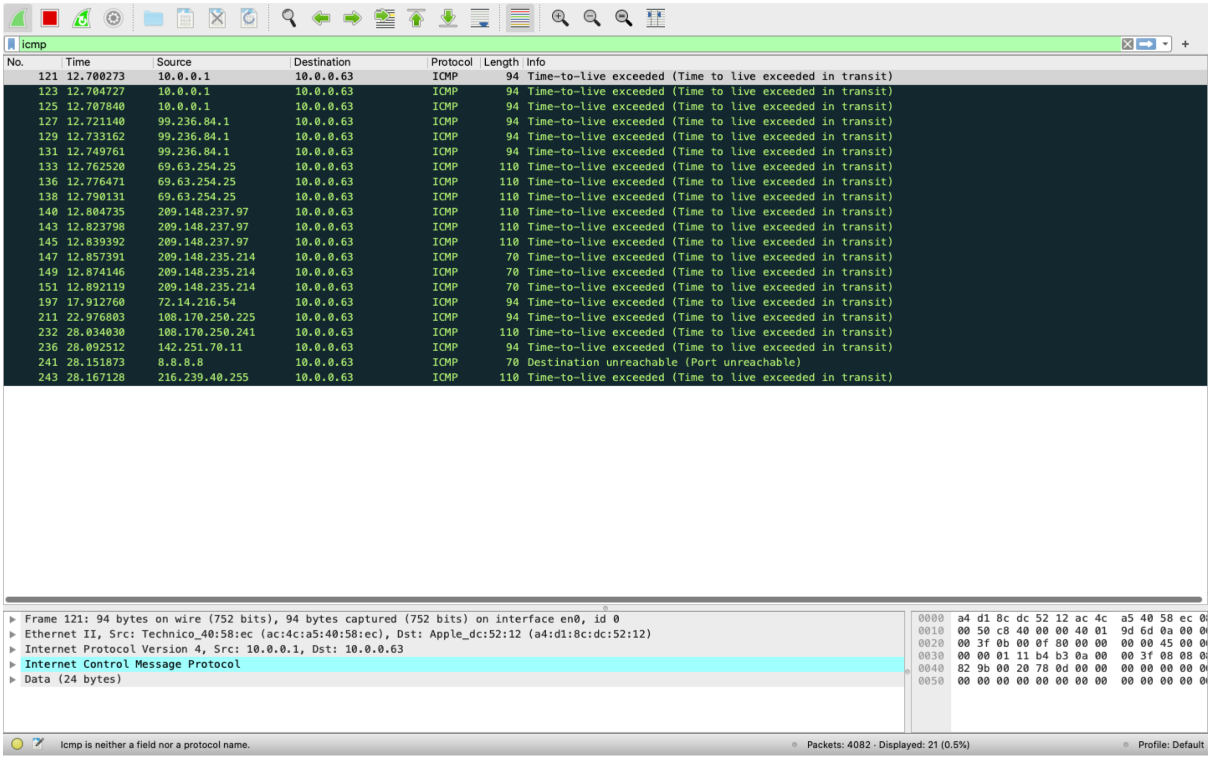
```
0000  e0 d4 64 3c fb c7 34 5d  9e
0010  00 7d f7 69 40 00 40 11  bd
0020  02 0c 00 35 c7 1f 00 69  c9
0030  00 00 00 01 00 00 0b 63  6f
0040  6e 34 04 6d 6f 6f 6f 03  63
0050  c0 18 00 06 00 01 00 00  0d
0060  06 61 66 72 61 69 64 03  6f
0070  61 64 6d 69 6e c0 36 89  36
0080  00 1c 20 00 24 ea 00 00  00
```

Bytes 82-83: Type (dns.resp.type) | Packets: 45 • Displayed: 45 (100.0%) | Profile: Default

Traceroute



```
(base) mac@MacdeMacBook-Air-3 ~ % traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
 1  10.0.0.1 (10.0.0.1)  3.940 ms  3.342 ms  3.118 ms
 2  99.236.84.1 (99.236.84.1)  13.207 ms  11.105 ms  16.564 ms
 3  8078-dgw02.hstr.rmgt.net.rogers.com (69.63.254.25)  12.736 ms  13.149 ms  13
.675 ms
 4  3039-cgw01.wlfdle.rmgt.net.rogers.com (209.148.237.97)  14.519 ms  18.315 ms
  15.569 ms
 5  209.148.235.214 (209.148.235.214)  17.954 ms  15.758 ms  17.965 ms
 6  * 72.14.216.54 (72.14.216.54)  15.234 ms *
 7  108.170.250.225 (108.170.250.225)  18.842 ms *
    108.170.250.241 (108.170.250.241)  19.713 ms
 8  142.251.70.11 (142.251.70.11)  13.324 ms
    dns.google (8.8.8.8)  12.534 ms
    216.239.40.255 (216.239.40.255)  14.475 ms
```



```
No.  Time       Source           Destination  Protocol  Length  Info
121  12.700273  10.0.0.1         10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
123  12.704727  10.0.0.1         10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
125  12.707840  10.0.0.1         10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
127  12.721140  99.236.84.1      10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
129  12.733162  99.236.84.1      10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
131  12.749761  99.236.84.1      10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
133  12.762520  69.63.254.25     10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
136  12.776471  69.63.254.25     10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
138  12.790131  69.63.254.25     10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
140  12.804735  209.148.237.97   10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
143  12.823798  209.148.237.97   10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
145  12.839392  209.148.237.97   10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
147  12.857391  209.148.235.214  10.0.0.63    ICMP       70  Time-to-live exceeded (Time to live exceeded in transit)
149  12.874146  209.148.235.214  10.0.0.63    ICMP       70  Time-to-live exceeded (Time to live exceeded in transit)
151  12.892119  209.148.235.214  10.0.0.63    ICMP       70  Time-to-live exceeded (Time to live exceeded in transit)
197  17.912760  72.14.216.54     10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
211  22.976803  108.170.250.225  10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
232  28.034030  108.170.250.241  10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
236  28.092512  142.251.70.11    10.0.0.63    ICMP       94  Time-to-live exceeded (Time to live exceeded in transit)
241  28.151873  8.8.8.8          10.0.0.63    ICMP       70  Destination unreachable (Port unreachable)
243  28.167128  216.239.40.255   10.0.0.63    ICMP      110  Time-to-live exceeded (Time to live exceeded in transit)
```

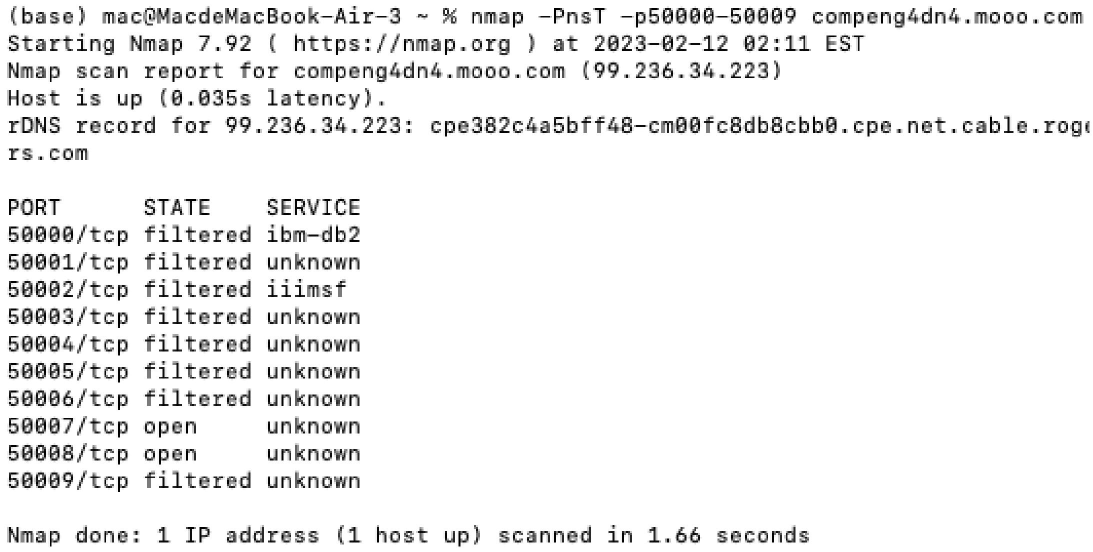
```
▶ Frame 121: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface en0, id 0
▶ Ethernet II, Src: Technico_40:58:ec (ac:4c:a5:40:58:ec), Dst: Apple_dc:52:12 (a4:d1:8c:dc:52:12)
▶ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.63
▶ Internet Control Message Protocol
▶ Data (24 bytes)
```

```
0000  a4 d1 8c dc 52 12 ac 4c  a5 40 58 ec
0010  00 50 c8 40 00 00 40 01  9d 6d 0a 00
0020  00 3f 0b 00 0f 80 00 00  00 00 45 00
0030  00 00 01 11 b4 b3 0a 00  00 3f 08 08
0040  82 9b 00 20 78 0d 00 00  00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00
```

Icmp is neither a field nor a protocol name. · Packets: 4082 · Displayed: 21 (0.5%) · Profile: Default

we filter icmp to see how traceroute works. As shown above, each source ip address in my wireshark is corresponding to my path of route in terminal. According to this, we can see traceroute will send 3 packets to the first router and then return to original positon. After that, it will send 3 packets to the second router and then return to original positon. Then, it will send 3 packets to the next router and then return to original positon. This mode repeats until it reaches destination server which in my code is 8.8.8.8(one of the public DNS of Google).

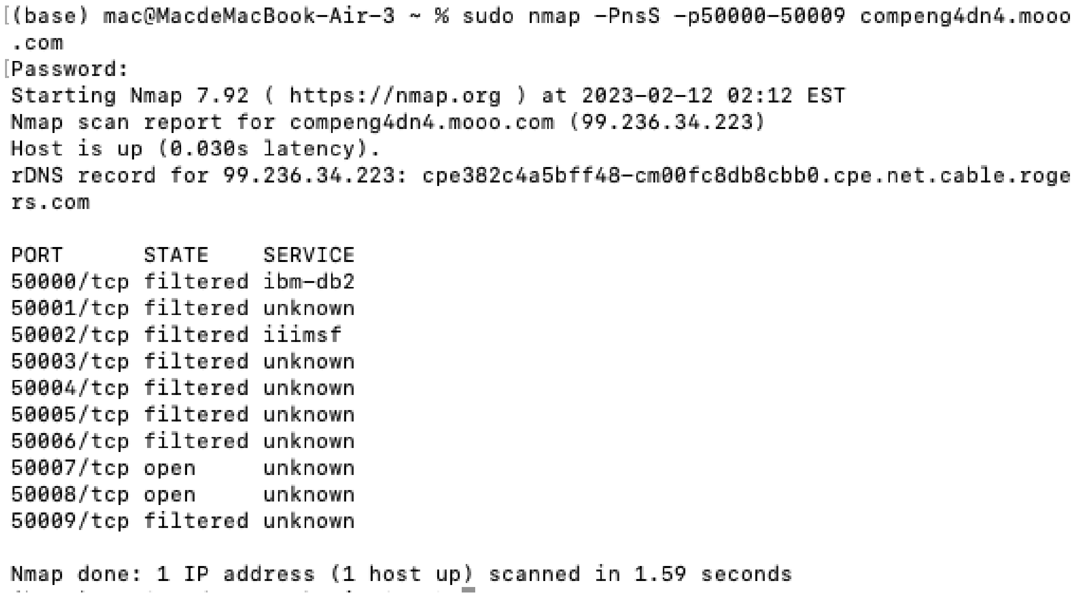
nmap：



```
(base) mac@MacdeMacBook-Air-3 ~ % nmap -PnsT -p50000-50009 compeng4dn4.mooo.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-12 02:11 EST
Nmap scan report for compeng4dn4.mooo.com (99.236.34.223)
Host is up (0.035s latency).
rDNS record for 99.236.34.223: cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.roge
rs.com

PORT      STATE    SERVICE
50000/tcp filtered ibm-db2
50001/tcp filtered unknown
50002/tcp filtered iiimsf
50003/tcp filtered unknown
50004/tcp filtered unknown
50005/tcp filtered unknown
50006/tcp filtered unknown
50007/tcp open     unknown
50008/tcp open     unknown
50009/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Port 50000 to 50009 are filtered(close) except 50007 and 50008.

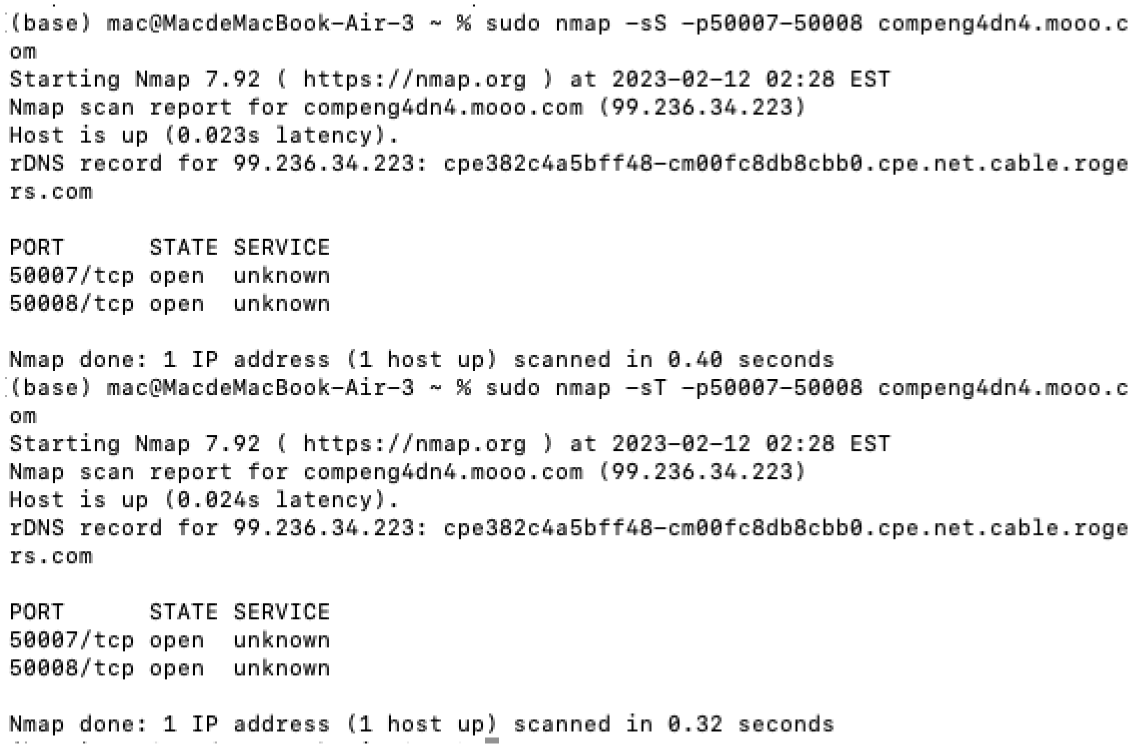
nmap -p 50000 -sS compeng4dn4.mooo.com



```
[(base) mac@MacdeMacBook-Air-3 ~ % sudo nmap -PnsS -p50000-50009 compeng4dn4.mooo
.com
[Password:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-12 02:12 EST
Nmap scan report for compeng4dn4.mooo.com (99.236.34.223)
Host is up (0.030s latency).
rDNS record for 99.236.34.223: cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.roge
rs.com

PORT      STATE    SERVICE
50000/tcp filtered ibm-db2
50001/tcp filtered unknown
50002/tcp filtered iiimsf
50003/tcp filtered unknown
50004/tcp filtered unknown
50005/tcp filtered unknown
50006/tcp filtered unknown
50007/tcp open     unknown
50008/tcp open     unknown
50009/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

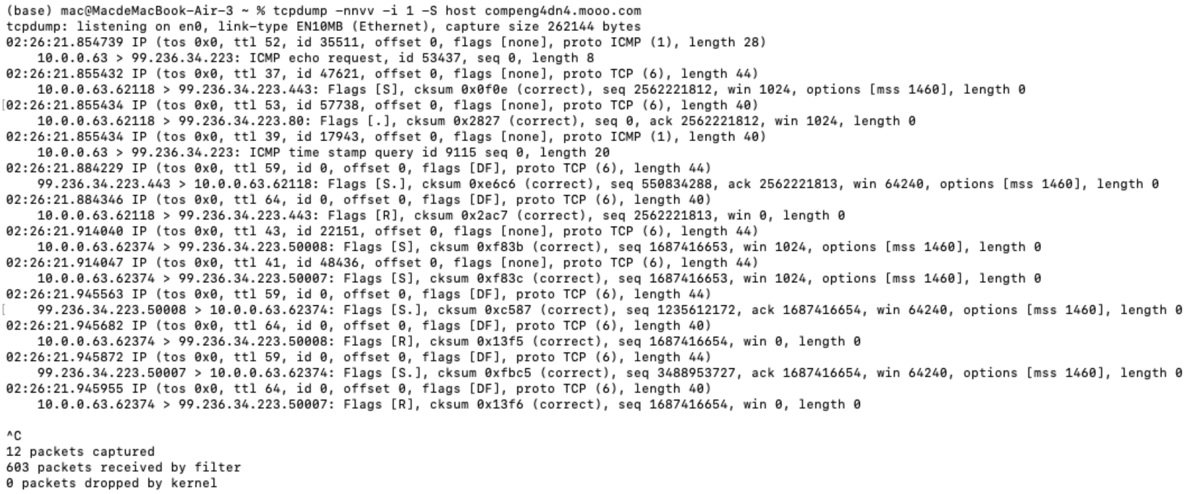
Same as Nmap problem 1. All the ports between 50000 and 50009 are all filtered(close) except 50007 and 50008.

3.



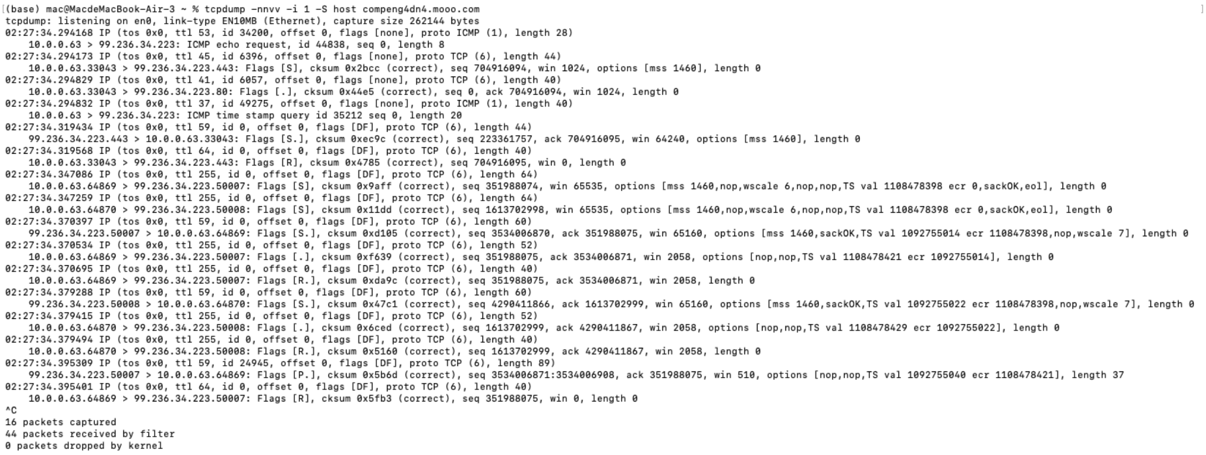
```
(base) mac@MacdeMacBook-Air-3 ~ % sudo nmap -sS -p50007-50008 compeng4dn4.mooo.c
om
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-12 02:28 EST
Nmap scan report for compeng4dn4.mooo.com (99.236.34.223)
Host is up (0.023s latency).
rDNS record for 99.236.34.223: cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.roge
rs.com

PORT      STATE SERVICE
50007/tcp open  unknown
50008/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
(base) mac@MacdeMacBook-Air-3 ~ % sudo nmap -sT -p50007-50008 compeng4dn4.mooo.c
om
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-12 02:28 EST
Nmap scan report for compeng4dn4.mooo.com (99.236.34.223)
Host is up (0.024s latency).
rDNS record for 99.236.34.223: cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.roge
rs.com

PORT      STATE SERVICE
50007/tcp open  unknown
50008/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

-sS



```
(base) mac@MacdeMacBook-Air-3 ~ % tcpdump -nnvv -i 1 -S host compeng4dn4.mooo.com
tcpdump: listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
02:26:21.854739 IP (tos 0x0, ttl 52, id 35511, offset 0, flags [none], proto ICMP (1), length 28)
    10.0.0.63 > 99.236.34.223: ICMP echo request, id 53437, seq 0, length 8
02:26:21.855432 IP (tos 0x0, ttl 37, id 47621, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.63.62118 > 99.236.34.223.443: Flags [S], cksum 0x0f0e (correct), seq 2562221812, win 1024, options [mss 1460], length 0
02:26:21.855434 IP (tos 0x0, ttl 53, id 57738, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.63.62118 > 99.236.34.223.80: Flags [.], cksum 0x2827 (correct), seq 0, ack 2562221812, win 1024, length 0
02:26:21.855434 IP (tos 0x0, ttl 39, id 17943, offset 0, flags [none], proto ICMP (1), length 40)
    10.0.0.63 > 99.236.34.223: ICMP time stamp query id 9115 seq 0, length 20
02:26:21.884229 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 44)
    99.236.34.223.443 > 10.0.0.63.62118: Flags [S.], cksum 0xe6c6 (correct), seq 550834288, ack 2562221813, win 64240, options [mss 1460], length 0
02:26:21.884346 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.62118 > 99.236.34.223.443: Flags [R], cksum 0x2ac7 (correct), seq 2562221813, win 0, length 0
02:26:21.914040 IP (tos 0x0, ttl 43, id 22151, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.63.62374 > 99.236.34.223.50008: Flags [S], cksum 0xf83b (correct), seq 1687416653, win 1024, options [mss 1460], length 0
02:26:21.914047 IP (tos 0x0, ttl 41, id 48436, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.63.62374 > 99.236.34.223.50007: Flags [S], cksum 0xf83c (correct), seq 1687416653, win 1024, options [mss 1460], length 0
02:26:21.945563 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 44)
    99.236.34.223.50008 > 10.0.0.63.62374: Flags [S.], cksum 0xc587 (correct), seq 1235612172, ack 1687416654, win 64240, options [mss 1460], length 0
02:26:21.945682 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.62374 > 99.236.34.223.50008: Flags [R], cksum 0x13f5 (correct), seq 1687416654, win 0, length 0
02:26:21.945872 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 44)
    99.236.34.223.50007 > 10.0.0.63.62374: Flags [S.], cksum 0xfbc5 (correct), seq 3488953727, ack 1687416654, win 64240, options [mss 1460], length 0
02:26:21.945955 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.62374 > 99.236.34.223.50007: Flags [R], cksum 0x13f6 (correct), seq 1687416654, win 0, length 0

^C
12 packets captured
603 packets received by filter
0 packets dropped by kernel
```

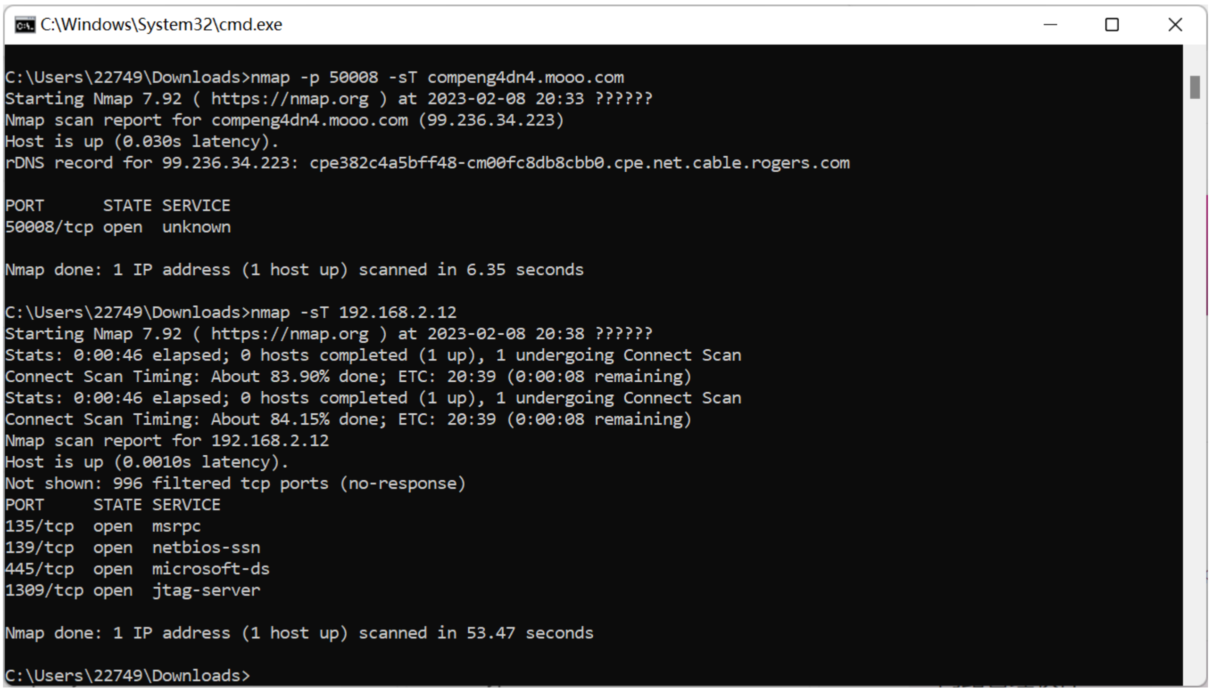
-sT



```
(base) mac@MacdeMacBook-Air-3 ~ % tcpdump -nnvv -i 1 -S host compeng4dn4.mooo.com
tcpdump: listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
02:27:34.294168 IP (tos 0x0, ttl 53, id 34200, offset 0, flags [none], proto ICMP (1), length 28)
    10.0.0.63 > 99.236.34.223: ICMP echo request, id 44838, seq 0, length 8
02:27:34.294173 IP (tos 0x0, ttl 45, id 6396, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.63.33043 > 99.236.34.223.443: Flags [S], cksum 0x2bcc (correct), seq 704916094, win 1024, options [mss 1460], length 0
02:27:34.294829 IP (tos 0x0, ttl 41, id 6057, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.63.33043 > 99.236.34.223.80: Flags [.], cksum 0x44e5 (correct), seq 0, ack 704916094, win 1024, length 0
02:27:34.294832 IP (tos 0x0, ttl 37, id 49275, offset 0, flags [none], proto ICMP (1), length 40)
    10.0.0.63 > 99.236.34.223: ICMP time stamp query id 35212 seq 0, length 20
02:27:34.319434 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 44)
    99.236.34.223.443 > 10.0.0.63.33043: Flags [S.], cksum 0xec9c (correct), seq 223361757, ack 704916095, win 64240, options [mss 1460], length 0
02:27:34.319568 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.33043 > 99.236.34.223.443: Flags [R], cksum 0x4785 (correct), seq 704916095, win 0, length 0
02:27:34.347086 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    10.0.0.63.64869 > 99.236.34.223.50007: Flags [S], cksum 0x9aff (correct), seq 351988074, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1108478398 ecr 0,sackOK,eol], length 0
02:27:34.347259 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    10.0.0.63.64870 > 99.236.34.223.50008: Flags [S], cksum 0x11dd (correct), seq 1613702998, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1108478398 ecr 0,sackOK,eol], length 0
02:27:34.370397 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    99.236.34.223.50007 > 10.0.0.63.64869: Flags [S.], cksum 0xd105 (correct), seq 3534006870, ack 351988075, win 65160, options [mss 1460,sackOK,TS val 1092755014 ecr 1108478398,nop,wscale 7], length 0
02:27:34.370534 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.63.64869 > 99.236.34.223.50007: Flags [.], cksum 0xf639 (correct), seq 351988075, ack 3534006871, win 2058, options [nop,nop,TS val 1108478421 ecr 1092755014], length 0
02:27:34.370695 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.64869 > 99.236.34.223.50007: Flags [R.], cksum 0xda9c (correct), seq 351988075, ack 3534006871, win 2058, length 0
02:27:34.379288 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    99.236.34.223.50008 > 10.0.0.63.64870: Flags [S.], cksum 0x47c1 (correct), seq 4290411866, ack 1613702999, win 65160, options [mss 1460,sackOK,TS val 1092755022 ecr 1108478398,nop,wscale 7], length 0
02:27:34.379415 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.63.64870 > 99.236.34.223.50008: Flags [.], cksum 0x6ced (correct), seq 1613702999, ack 4290411867, win 2058, options [nop,nop,TS val 1108478429 ecr 1092755022], length 0
02:27:34.379494 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.64870 > 99.236.34.223.50008: Flags [R.], cksum 0x5160 (correct), seq 1613702999, ack 4290411867, win 2058, length 0
02:27:34.395309 IP (tos 0x0, ttl 59, id 24945, offset 0, flags [DF], proto TCP (6), length 89)
    99.236.34.223.50007 > 10.0.0.63.64869: Flags [P.], cksum 0x5b6d (correct), seq 3534006871:3534006908, ack 351988075, win 510, options [nop,nop,TS val 1092755040 ecr 1108478421], length 37
02:27:34.395401 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.0.63.64869 > 99.236.34.223.50007: Flags [R], cksum 0x5fb3 (correct), seq 351988075, win 0, length 0
^C
16 packets captured
44 packets received by filter
0 packets dropped by kernel
```

When the Syn is acknowledged the acknowledgement is equal to the sequence number.Eg, at 02:26:21 the sequence number for the Syn is 2562221812. After it is acknowledged, the ack number for the Ack is 2562221812.

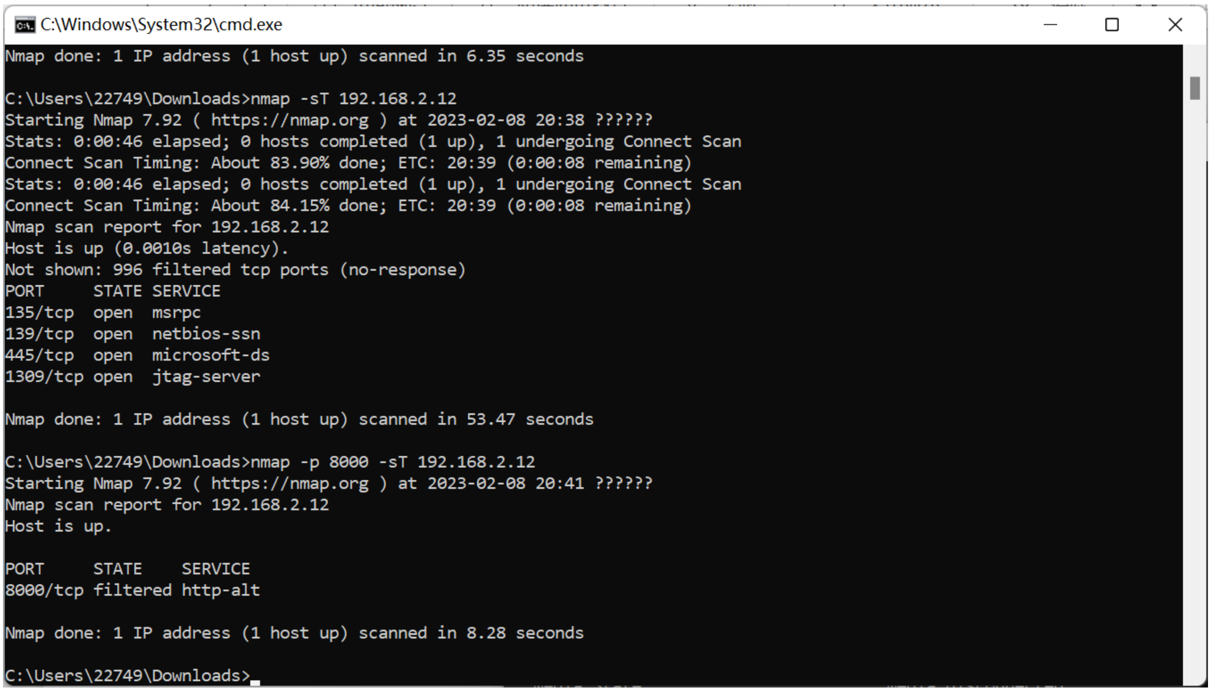
4.



```
C:\Users\22749\Downloads>nmap -p 50008 -sT compeng4dn4.mooo.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 20:33 ??????
Nmap scan report for compeng4dn4.mooo.com (99.236.34.223)
Host is up (0.030s latency).
rDNS record for 99.236.34.223: cpe382c4a5bff48-cm00fc8db8cbb0.cpe.net.cable.rogers.com

PORT      STATE SERVICE
50008/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.35 seconds

C:\Users\22749\Downloads>nmap -sT 192.168.2.12
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 20:38 ??????
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 83.90% done; ETC: 20:39 (0:00:08 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.15% done; ETC: 20:39 (0:00:08 remaining)
Nmap scan report for 192.168.2.12
Host is up (0.0010s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1309/tcp open  jtag-server

Nmap done: 1 IP address (1 host up) scanned in 53.47 seconds

C:\Users\22749\Downloads>
```

After scanning, we find that 996 of tcp ports are close and 4 of 1000 ports are open.
Port 135 has service msrpc which is s a protocol that uses the client-server model that enables one program to request a service from a program on another computer, without having to understand the details of that computer's network.
Port 139 has service netbios-ssn which means NetBIOS Session Service (NBSS) is a protocol to connect two computers to transmit heavy data traffic. It is mostly used for printer and file services over a network.
Port 445 has the service microsoft-ds which is the name given to port 445 which is used by SMB (Server Message Block). SMB is a network protocol used mainly in Windows networks for sharing resources (e.g. files or printers) over a network. It can also be used to remotely execute commands
Port 1309 has service jtag-server which allows different applications to share access to JTAG cables (such as the ByteBlaster cable). Clients connect to the server using a TCP/IP connection. You can access JTAG cables connected to a remote computer, which is useful when you use an operating system that has no fast JTAG hardware available.

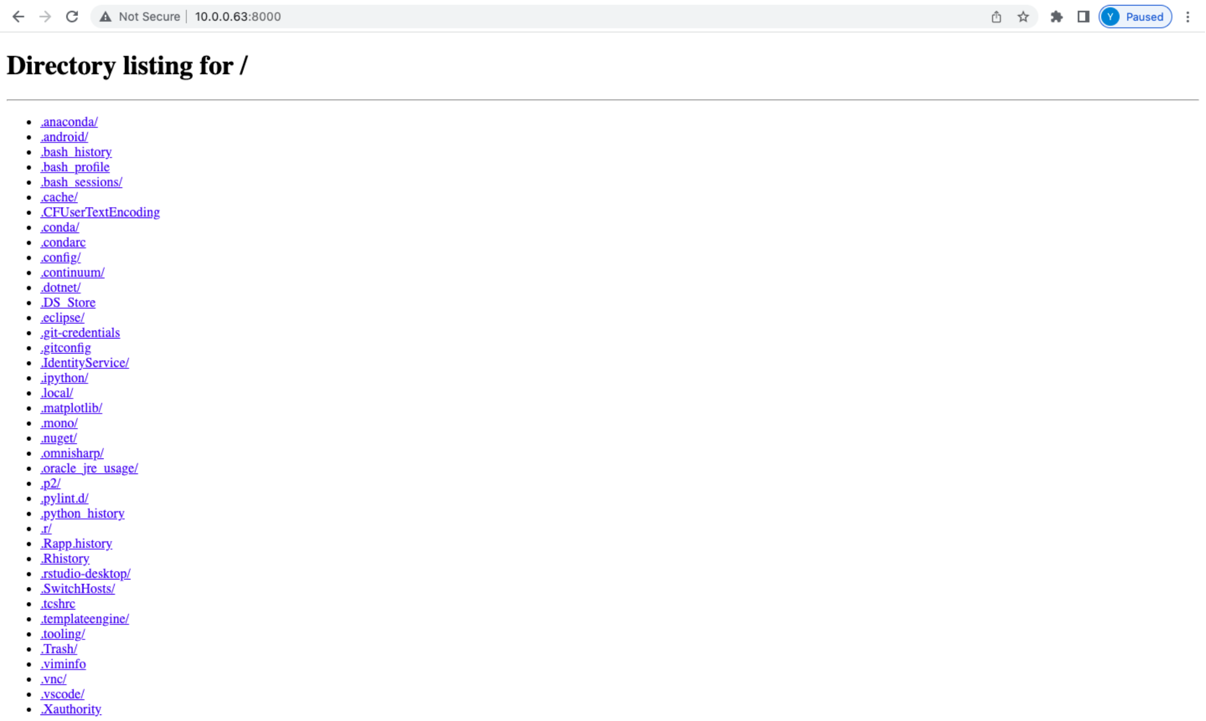
5.



```
Nmap done: 1 IP address (1 host up) scanned in 6.35 seconds

C:\Users\22749\Downloads>nmap -sT 192.168.2.12
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 20:38 ??????
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 83.90% done; ETC: 20:39 (0:00:08 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.15% done; ETC: 20:39 (0:00:08 remaining)
Nmap scan report for 192.168.2.12
Host is up (0.0010s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1309/tcp open  jtag-server

Nmap done: 1 IP address (1 host up) scanned in 53.47 seconds

C:\Users\22749\Downloads>nmap -p 8000 -sT 192.168.2.12
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 20:41 ??????
Nmap scan report for 192.168.2.12
Host is up.

PORT     STATE    SERVICE
8000/tcp filtered http-alt

Nmap done: 1 IP address (1 host up) scanned in 8.28 seconds

C:\Users\22749\Downloads>_
```

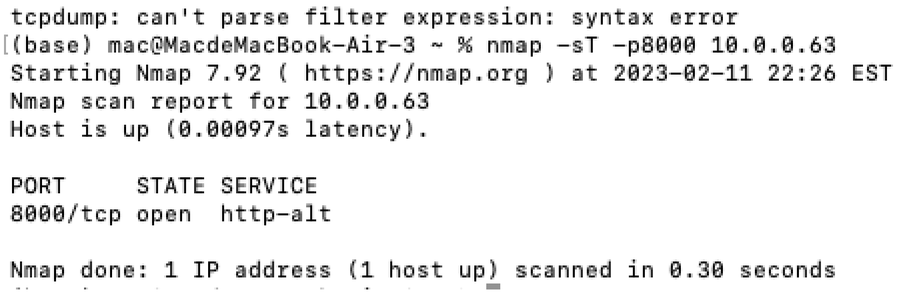
we find port 8000 in our computer is filtered(closed). It has the service http-alt which means HTTP alternate is commonly used for Web proxy and caching server, or for running a Web server as a non-root user

6.



Directory listing for /

- .anaconda/
- .android/
- .bash_history
- .bash_profile
- .bash_sessions/
- .cache/
- .CFUserTextEncoding
- .conda/
- .condarc
- .config/
- .continuum/
- .dotnet/
- .DS_Store
- .eclipse/
- .git-credentials
- .gitconfig
- .IdentityService/
- .ipython/
- .local/
- .matplotlib/
- .mono/
- .nuget/
- .omnisharp/
- .oracle_jre_usage/
- .p2/
- .pylint.d/
- .python_history
- .r/
- .Rapp.history
- .Rhistory
- .rstudio-desktop/
- .SwitchHosts/
- .tcshrc
- .templateengine/
- .tooling/
- .Trash/
- .viminfo
- .vnc/
- .vscode/
- .Xauthority



```
tcpdump: can't parse filter expression: syntax error
[(base) mac@MacdeMacBook-Air-3 ~ % nmap -sT -p8000 10.0.0.63
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-11 22:26 EST
Nmap scan report for 10.0.0.63
Host is up (0.00097s latency).

PORT     STATE SERVICE
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

The directory shows the contents of the directory where python was invoked.