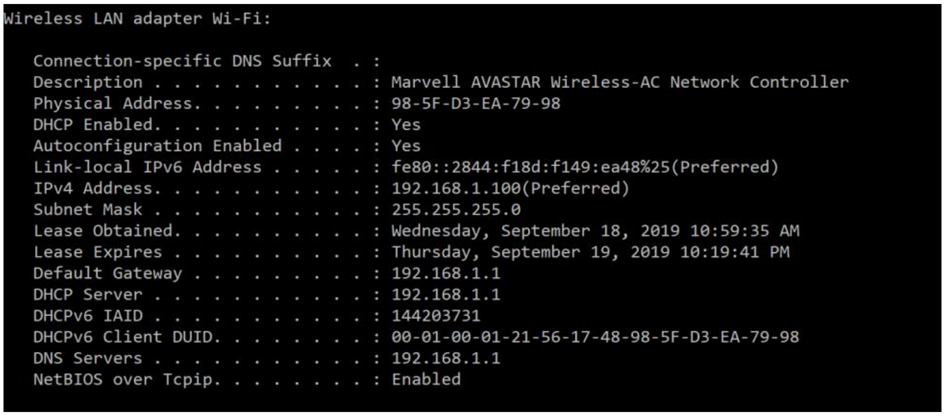
# Lab 3: Packet Analysis (Part 2)

- This is an individual assignment, and is worth 20 points.
- The due date and time is 1:00 / 5:30, Sep 19.
- You should provide the answers using the accompanying outcome file. Change the file name following the naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab 1_ImG.docx).
- Do not copy any of the sample screenshots provided as illustrations.
- You should not scan any live servers using Nmap and hping3. For violation, you may be expelled from the school (not a joke!).

## Task 1. Identify the IP addresses

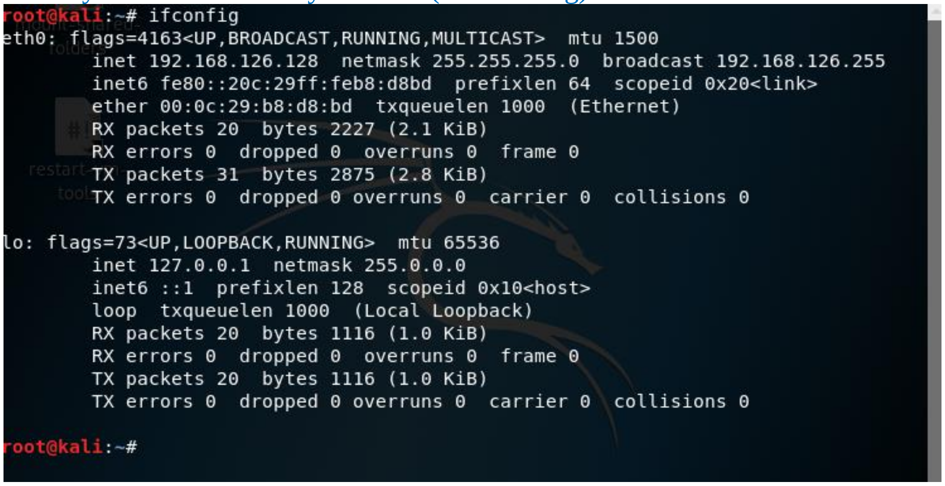
- Task

1) Idenity the IP address of your **host** and the subnet mask (use ipconfig /all). If you use wireless, the IP address of "Wireless LAN adapter Wi-Fi" is the active physical interface. Provide a screenshot for this.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Marvell AVASTAR Wireless-AC Network Controller
   Physical Address. . . . . . . . . : 98-5F-D3-EA-79-98
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2844:f18d:f149:ea48%25(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 18, 2019 10:59:35 AM
   Lease Expires . . . . . . . . . . : Thursday, September 19, 2019 10:19:41 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 144203731
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-56-17-48-98-5F-D3-EA-79-98
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2) Identify the IP address of your **Kali** (use ifconfig). Provide a screenshot for this.

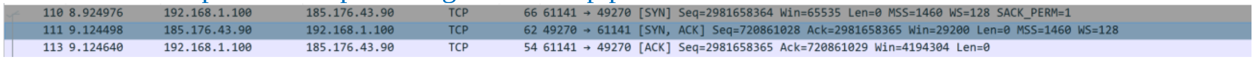


```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.126.128  netmask 255.255.255.0  broadcast 192.168.126.255
        inet6 fe80::20c:29ff:feb8:d8bd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b8:d8:bd  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 2227 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 2875 (2.8 KiB)
        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 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

## Task 2. Analyzing FTP Signatures

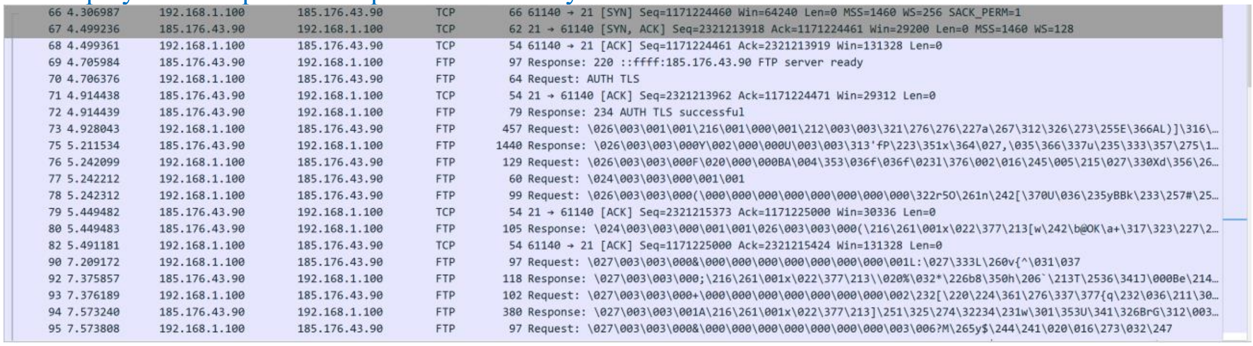
- Task

1) Identify the TCP packets used for the initial three-way handshaking. Take a screenshot of that TCP packets.
   - **Hint**: These packets are placed right before ftp packets.



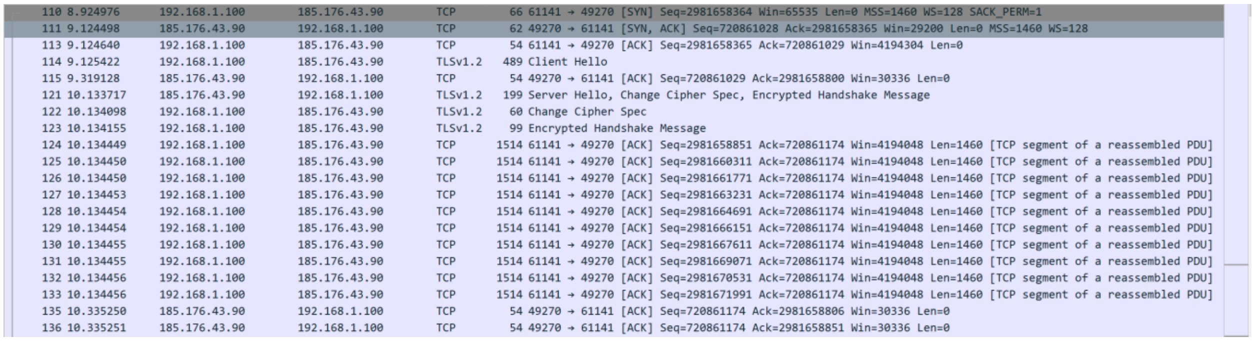
```
110 8.924976   192.168.1.100   185.176.43.90   TCP   66 61141 → 49270 [SYN] Seq=2981658364 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
111 9.124498   185.176.43.90   192.168.1.100   TCP   62 49270 → 61141 [SYN, ACK] Seq=720861028 Ack=2981658365 Win=29200 Len=0 MSS=1460 WS=128
113 9.124640   192.168.1.100   185.176.43.90   TCP   54 61141 → 49270 [ACK] Seq=2981658365 Ack=720861029 Win=4194304 Len=0
```

2) Identify the TCP stream used for authentication to the FTP server. The packets are encrypted and so we should guess. Take a screenshot of the TCP stream.
   - **Hint**: Use the IP address of the ftp server to recognize the relevant TCP stream. Use the display filter "tcp.stream eq xx" as necessary.



```
66 4.306987   192.168.1.100   185.176.43.90   TCP     66 61140 → 21 [SYN] Seq=1171224460 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67 4.499236   185.176.43.90   192.168.1.100   TCP     62 21 → 61140 [SYN, ACK] Seq=2321213918 Ack=1171224461 Win=29200 Len=0 MSS=1460 WS=128
68 4.499361   192.168.1.100   185.176.43.90   TCP     54 61140 → 21 [ACK] Seq=1171224461 Ack=2321213919 Win=131328 Len=0
69 4.705984   185.176.43.90   192.168.1.100   FTP     97 Response: 220 ::ffff:185.176.43.90 FTP server ready
70 4.706376   192.168.1.100   185.176.43.90   FTP     64 Request: AUTH TLS
71 4.914438   185.176.43.90   192.168.1.100   TCP     54 21 → 61140 [ACK] Seq=2321213962 Ack=1171224471 Win=29312 Len=0
72 4.914439   185.176.43.90   192.168.1.100   FTP     79 Response: 234 AUTH TLS successful
73 4.928043   192.168.1.100   185.176.43.90   FTP    457 Request: \026\003\001\001\216\001\000\001\212\003\003\321\276\276\227a\267\312\326\273\255E\366AL)]\316\…
75 5.211534   185.176.43.90   192.168.1.100   FTP   1440 Response: \026\003\003\000Y\002\000\000U\003\003\313'fP\223\351x\364\027,\035\366\337u\235\333\357\275\1…
76 5.242099   192.168.1.100   185.176.43.90   FTP    129 Request: \026\003\003\000F\020\000\000BA\004\353\036f\036f\0231\376\002\016\245\005\215\027\330Xd\356\26…
77 5.242212   192.168.1.100   185.176.43.90   FTP     60 Request: \024\003\003\000\001\001
78 5.242312   192.168.1.100   185.176.43.90   FTP     99 Request: \026\003\003\000(\000\000\000\000\000\000\000\000\322r5O\261n\242[\370U\036\235yBBk\233\257#\25…
79 5.449482   185.176.43.90   192.168.1.100   TCP     54 21 → 61140 [ACK] Seq=2321215373 Ack=1171225000 Win=30336 Len=0
80 5.449483   185.176.43.90   192.168.1.100   FTP    105 Response: \024\003\003\000\001\001\026\003\003\000(\216\261\001x\022\377\213[w\242\b@OK\a+\317\323\227\2…
82 5.491181   192.168.1.100   185.176.43.90   TCP     54 61140 → 21 [ACK] Seq=1171225000 Ack=2321215424 Win=131328 Len=0
90 7.209172   192.168.1.100   185.176.43.90   FTP     97 Request: \027\003\003\000&\000\000\000\000\000\000\000\001L:\027\333L\260v{^\031\037
92 7.375857   185.176.43.90   192.168.1.100   FTP    118 Response: \027\003\003\000;\216\261\001x\022\377\213\\020%\032*\226b8\350h\206`\213T\2536\341J\000Be\214…
93 7.376189   192.168.1.100   185.176.43.90   FTP    102 Request: \027\003\003\000+\000\000\000\000\000\000\000\002\232[\220\224\361\276\337\377{q\232\036\211\30…
94 7.573240   185.176.43.90   192.168.1.100   FTP    380 Response: \027\003\003\001A\216\261\001x\022\377\213]\251\325\274\32234\231w\301\353U\341\326BrG\312\003…
95 7.573808   192.168.1.100   185.176.43.90   FTP     97 Request: \027\003\003\000&\000\000\000\000\000\000\000\003\006?M\265y$\244\241\020\016\273\032\247
```

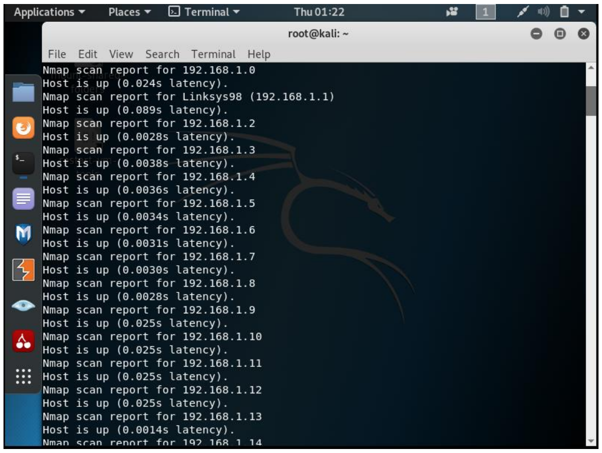
3) Identify the TCP stream used for the uploading. Take a screenshot of that TCP stream.



```
110 8.924976    192.168.1.100   185.176.43.90   TCP       66 61141 → 49270 [SYN] Seq=2981658364 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
111 9.124498    185.176.43.90   192.168.1.100   TCP       62 49270 → 61141 [SYN, ACK] Seq=720861028 Ack=2981658365 Win=29200 Len=0 MSS=1460 WS=128
113 9.124640    192.168.1.100   185.176.43.90   TCP       54 61141 → 49270 [ACK] Seq=2981658365 Ack=720861029 Win=4194304 Len=0
114 9.125422    192.168.1.100   185.176.43.90   TLSv1.2  489 Client Hello
115 9.319128    185.176.43.90   192.168.1.100   TCP       54 49270 → 61141 [ACK] Seq=720861029 Ack=2981658800 Win=30336 Len=0
121 10.133717   185.176.43.90   192.168.1.100   TLSv1.2  199 Server Hello, Change Cipher Spec, Encrypted Handshake Message
122 10.134098   192.168.1.100   185.176.43.90   TLSv1.2   60 Change Cipher Spec
123 10.134155   192.168.1.100   185.176.43.90   TLSv1.2   99 Encrypted Handshake Message
124 10.134449   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981658851 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
125 10.134450   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981660311 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
126 10.134450   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981661771 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
127 10.134453   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981663231 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
128 10.134454   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981664691 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
129 10.134454   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981666151 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
130 10.134455   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981667611 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
131 10.134455   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981669071 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
132 10.134456   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981670531 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
133 10.134456   192.168.1.100   185.176.43.90   TCP     1514 61141 → 49270 [ACK] Seq=2981671991 Ack=720861174 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
135 10.335250   185.176.43.90   192.168.1.100   TCP       54 49270 → 61141 [ACK] Seq=720861174 Ack=2981658806 Win=30336 Len=0
136 10.335251   185.176.43.90   192.168.1.100   TCP       54 49270 → 61141 [ACK] Seq=720861174 Ack=2981658851 Win=30336 Len=0
```

## Task 3. Ping Sweeping

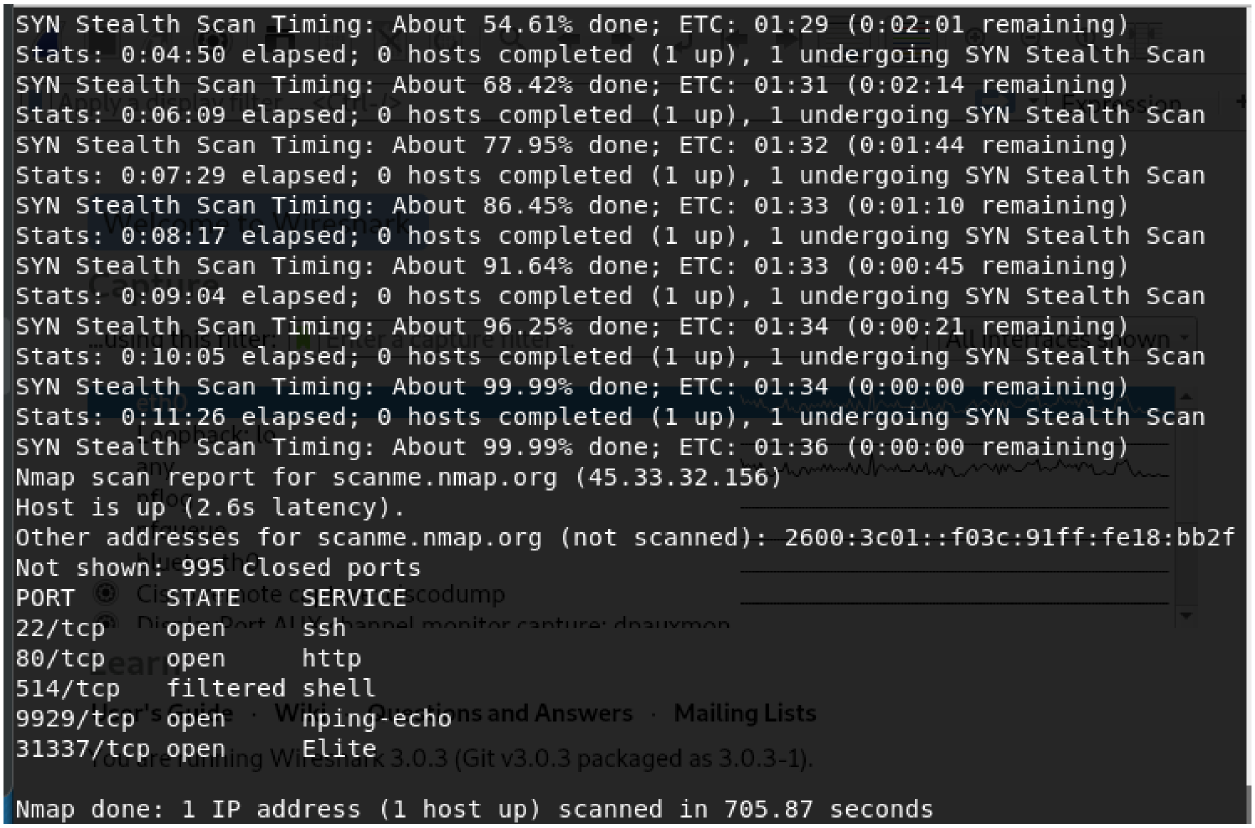
- Report the result with a screenshot.



```
Nmap scan report for 192.168.1.0
Host is up (0.024s latency).
Nmap scan report for Linksys98 (192.168.1.1)
Host is up (0.089s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0028s latency).
Nmap scan report for 192.168.1.3
Host is up (0.0038s latency).
Nmap scan report for 192.168.1.4
Host is up (0.0036s latency).
Nmap scan report for 192.168.1.5
Host is up (0.0034s latency).
Nmap scan report for 192.168.1.6
Host is up (0.0031s latency).
Nmap scan report for 192.168.1.7
Host is up (0.0030s latency).
Nmap scan report for 192.168.1.8
Host is up (0.0028s latency).
Nmap scan report for 192.168.1.9
Host is up (0.025s latency).
Nmap scan report for 192.168.1.10
Host is up (0.025s latency).
Nmap scan report for 192.168.1.11
Host is up (0.025s latency).
Nmap scan report for 192.168.1.12
Host is up (0.025s latency).
Nmap scan report for 192.168.1.13
Host is up (0.0014s latency).
Nmap scan report for 192.168.1.14
```

## Task 4. Port Scanning

- Report the result with a screenshot.

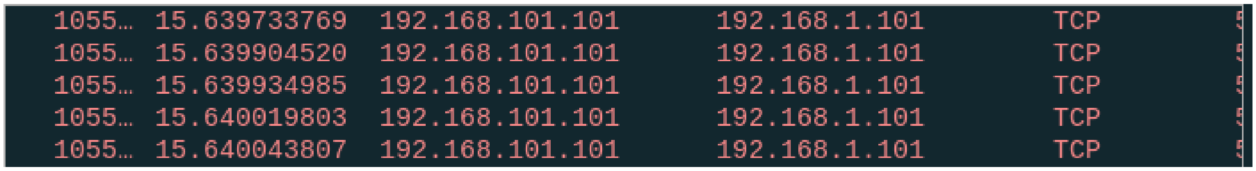


```
SYN Stealth Scan Timing: About 54.61% done; ETC: 01:29 (0:02:01 remaining)
Stats: 0:04:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.42% done; ETC: 01:31 (0:02:14 remaining)
Stats: 0:06:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.95% done; ETC: 01:32 (0:01:44 remaining)
Stats: 0:07:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.45% done; ETC: 01:33 (0:01:10 remaining)
Stats: 0:08:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.64% done; ETC: 01:33 (0:00:45 remaining)
Stats: 0:09:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.25% done; ETC: 01:34 (0:00:21 remaining)
Stats: 0:10:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 01:34 (0:00:00 remaining)
Stats: 0:11:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 01:36 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (2.6s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
514/tcp   filtered shell
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 705.87 seconds
```

## Task 5. SYN Flooding Attack

- Task

1) Report your Wireshark result in a screenshot.



```
1055…  15.639733769  192.168.101.101    192.168.1.101    TCP
1055…  15.639904520  192.168.101.101    192.168.1.101    TCP
1055…  15.639934985  192.168.101.101    192.168.1.101    TCP
1055…  15.640019803  192.168.101.101    192.168.1.101    TCP
1055…  15.640043807  192.168.101.101    192.168.1.101    TCP
```