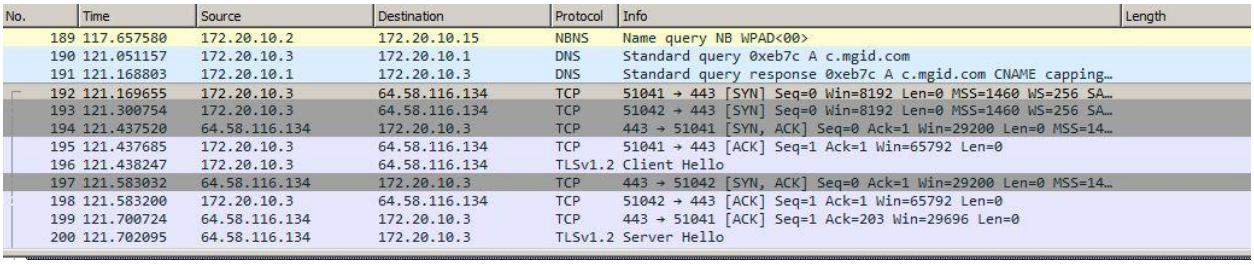
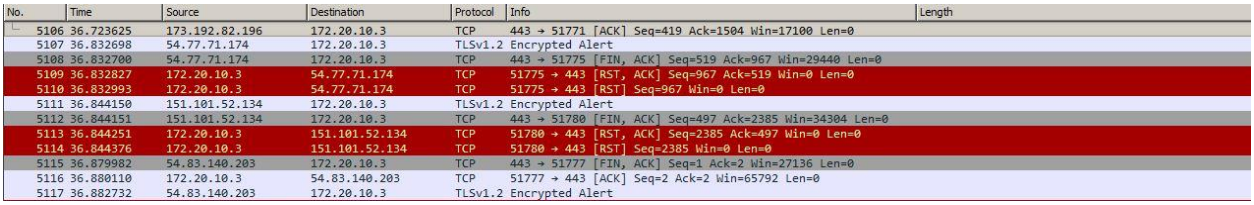
ANALISIS PERBANDINGAN CAPTURING NETWORK TRAFFIC MENGGUNAKAN WIRESHARK DAN NETSTAT

Meidi Dwi Hafiz | 09011281520097

Hasil Capture Wireshark dapat dilihat dibawah ini:



No.	Time	Source	Destination	Protocol	Info	Length
189	117.657580	172.20.10.2	172.20.10.15	NBNS	Name query NB WPAD<00>	
190	121.051157	172.20.10.3	172.20.10.1	DNS	Standard query 0xeb7c A c.mgid.com	
191	121.168803	172.20.10.1	172.20.10.3	DNS	Standard query response 0xeb7c A c.mgid.com CNAME capping…	
192	121.169655	172.20.10.3	64.58.116.134	TCP	51041 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA…	
193	121.300754	172.20.10.3	64.58.116.134	TCP	51042 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA…	
194	121.437520	64.58.116.134	172.20.10.3	TCP	443 → 51041 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14…	
195	121.437685	172.20.10.3	64.58.116.134	TCP	51041 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0	
196	121.438247	172.20.10.3	64.58.116.134	TLSv1.2	Client Hello	
197	121.583032	64.58.116.134	172.20.10.3	TCP	443 → 51042 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14…	
198	121.583200	172.20.10.3	64.58.116.134	TCP	51042 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0	
199	121.700724	64.58.116.134	172.20.10.3	TCP	443 → 51041 [ACK] Seq=1 Ack=203 Win=29696 Len=0	
200	121.702095	64.58.116.134	172.20.10.3	TLSv1.2	Server Hello	



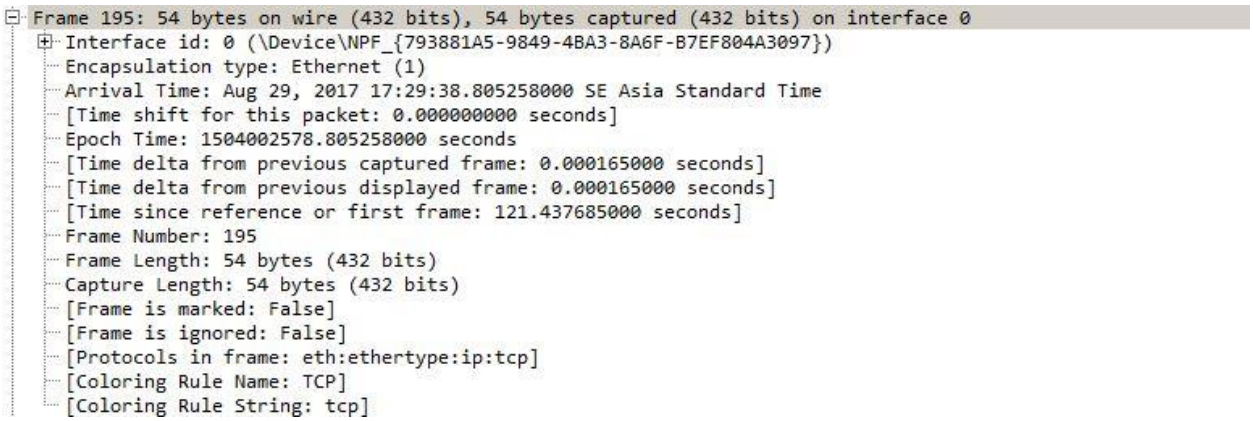
No.	Time	Source	Destination	Protocol	Info	Length
5106	36.723625	173.192.82.196	172.20.10.3	TCP	443 → 51771 [ACK] Seq=419 Ack=1504 Win=17100 Len=0	
5107	36.832698	54.77.71.174	172.20.10.3	TLSv1.2	Encrypted Alert	
5108	36.832700	54.77.71.174	172.20.10.3	TCP	443 → 51775 [FIN, ACK] Seq=519 Ack=967 Win=29440 Len=0	
5109	36.832827	172.20.10.3	54.77.71.174	TCP	51775 → 443 [RST, ACK] Seq=967 Ack=519 Win=0 Len=0	
5110	36.832993	172.20.10.3	54.77.71.174	TCP	51775 → 443 [RST] Seq=967 Win=0 Len=0	
5111	36.844150	151.101.52.134	172.20.10.3	TLSv1.2	Encrypted Alert	
5112	36.844151	151.101.52.134	172.20.10.3	TCP	443 → 51780 [FIN, ACK] Seq=497 Ack=2385 Win=34304 Len=0	
5113	36.844251	172.20.10.3	151.101.52.134	TCP	51780 → 443 [RST, ACK] Seq=2385 Ack=497 Win=0 Len=0	
5114	36.844376	172.20.10.3	151.101.52.134	TCP	51780 → 443 [RST] Seq=2385 Win=0 Len=0	
5115	36.879982	54.83.140.203	172.20.10.3	TCP	443 → 51777 [FIN, ACK] Seq=1 Ack=2 Win=27136 Len=0	
5116	36.880110	172.20.10.3	54.83.140.203	TCP	51777 → 443 [ACK] Seq=2 Ack=2 Win=65792 Len=0	
5117	36.882732	54.83.140.203	172.20.10.3	TLSv1.2	Encrypted Alert	

Pada wireshark terdapat berbagai macam informasi yang didapat yaitu:

- No, menampilkan urutan paket data yang direkam
- Time, menampilkan waktu pada saat mengakses paket ke tujuan
- Source, menampilkan alamat ip pengguna/pengakses
- Destination, menampilkan alamat ip dari tujuan data
- Protocol, menampilkan informasi protocol pada saat mengakses data tsb
- Info, menampilkan informasi yang ditampilkan pada proses capture data tsb

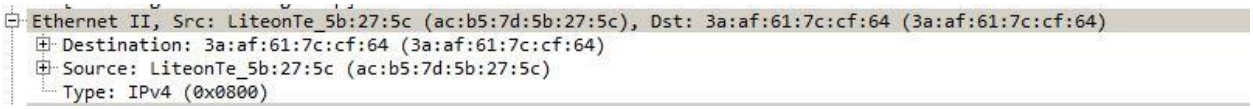
Protocol yang digunakan yaitu TCP.

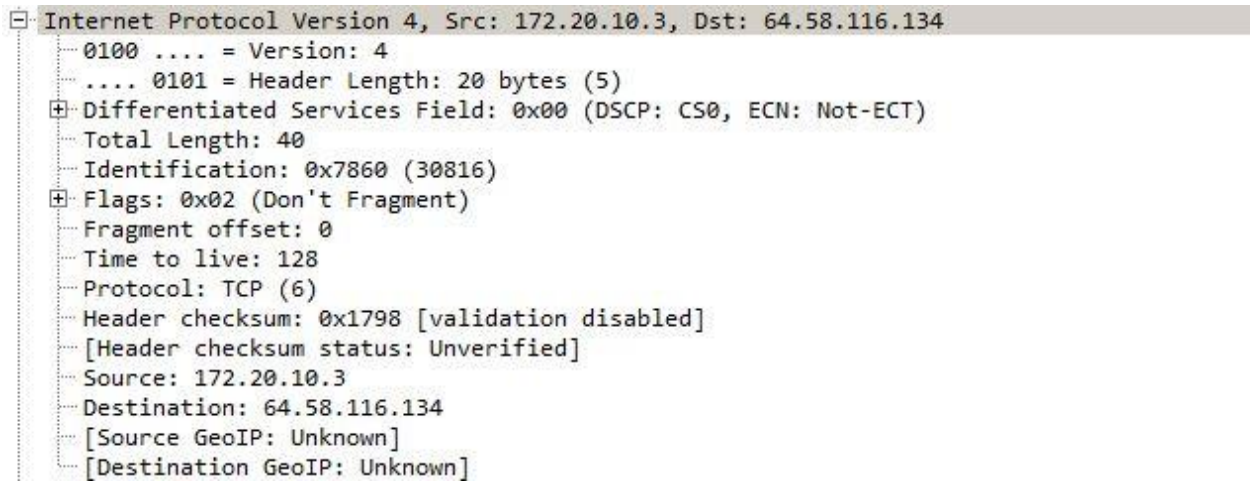
Frame:



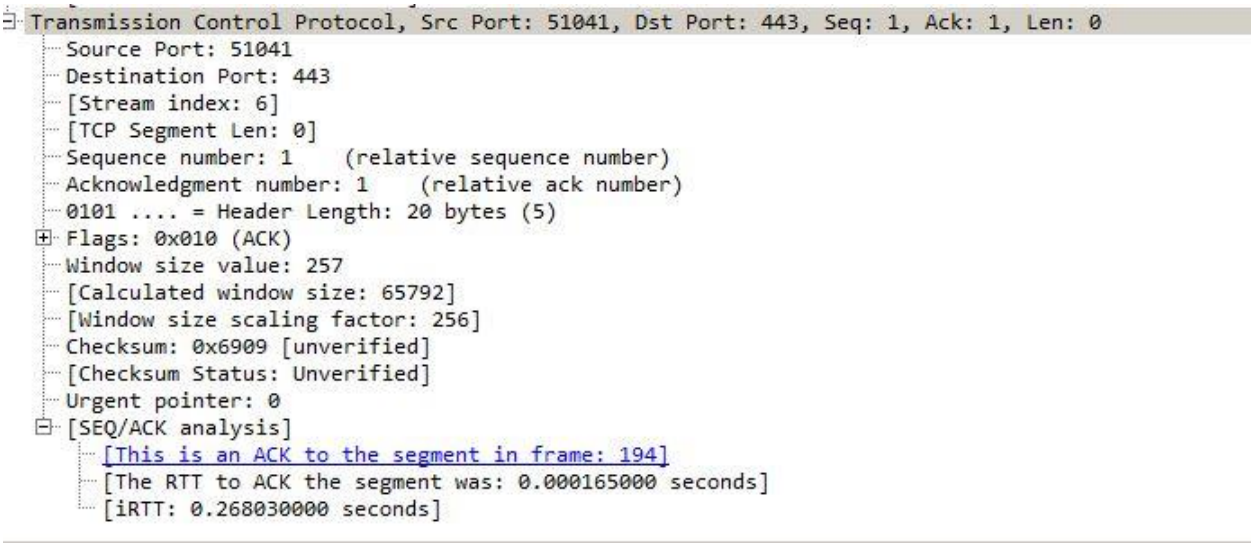
frame menampilkan eksekusi, jumlah, lebar protokol yang digunakan oleh frame yaitu **ethernet:ip:tcp:http.**

Ethernet



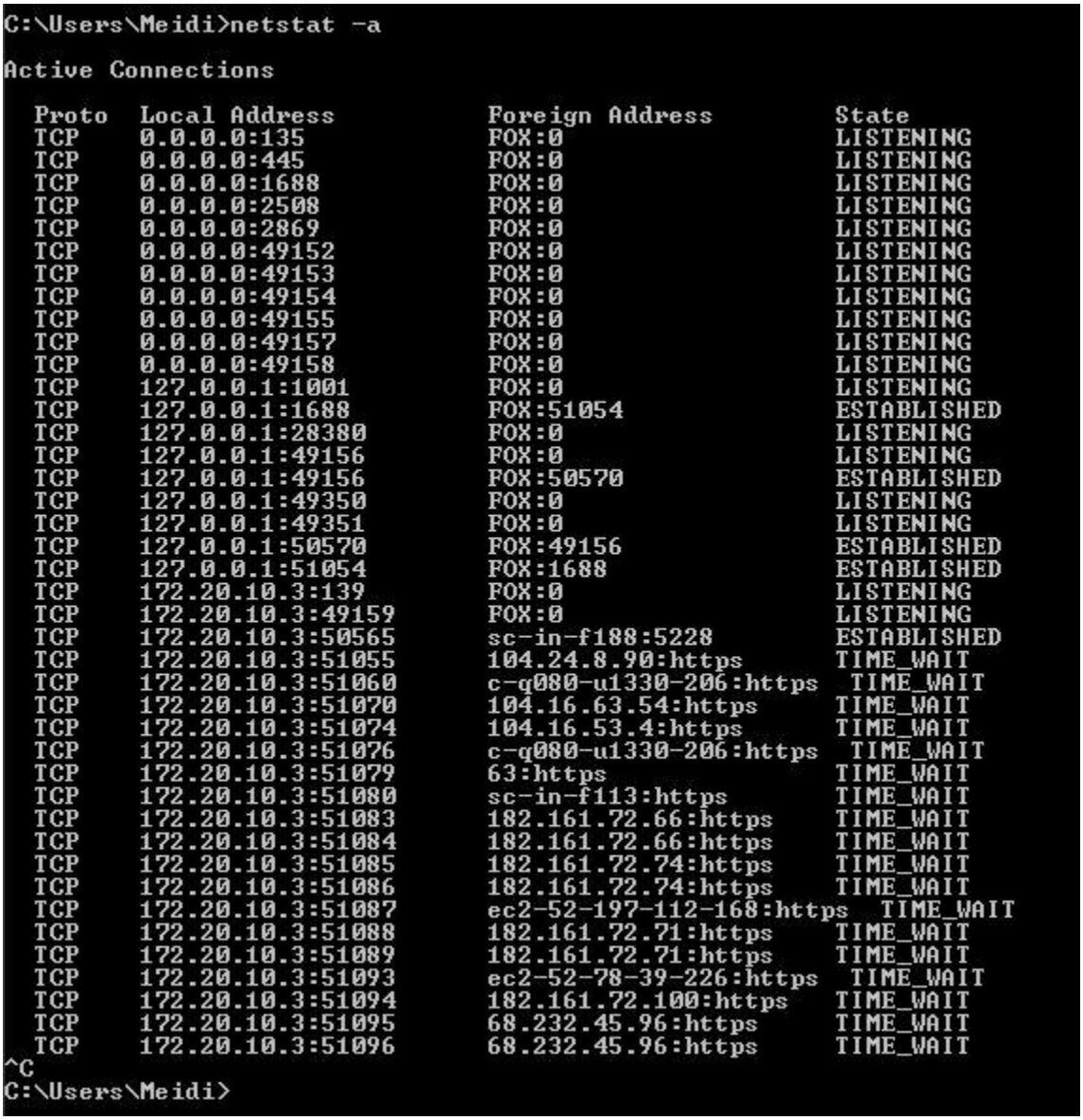


Menampilkan mac address pada proses yang dilakukan antara keduanya.



Menampilkan informasi TCP

Dan berikut ini adalah capture yang menggunakan netstat –a :



```
C:\Users\Meidi>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            FOX:0                  LISTENING
  TCP    0.0.0.0:445            FOX:0                  LISTENING
  TCP    0.0.0.0:1688           FOX:0                  LISTENING
  TCP    0.0.0.0:2508           FOX:0                  LISTENING
  TCP    0.0.0.0:2869           FOX:0                  LISTENING
  TCP    0.0.0.0:49152          FOX:0                  LISTENING
  TCP    0.0.0.0:49153          FOX:0                  LISTENING
  TCP    0.0.0.0:49154          FOX:0                  LISTENING
  TCP    0.0.0.0:49155          FOX:0                  LISTENING
  TCP    0.0.0.0:49157          FOX:0                  LISTENING
  TCP    0.0.0.0:49158          FOX:0                  LISTENING
  TCP    127.0.0.1:1001         FOX:0                  LISTENING
  TCP    127.0.0.1:1688         FOX:51054              ESTABLISHED
  TCP    127.0.0.1:28380        FOX:0                  LISTENING
  TCP    127.0.0.1:49156        FOX:0                  LISTENING
  TCP    127.0.0.1:49156        FOX:50570              ESTABLISHED
  TCP    127.0.0.1:49350        FOX:0                  LISTENING
  TCP    127.0.0.1:49351        FOX:0                  LISTENING
  TCP    127.0.0.1:50570        FOX:49156              ESTABLISHED
  TCP    127.0.0.1:51054        FOX:1688               ESTABLISHED
  TCP    172.20.10.3:139        FOX:0                  LISTENING
  TCP    172.20.10.3:49159      FOX:0                  LISTENING
  TCP    172.20.10.3:50565      sc-in-f188:5228        ESTABLISHED
  TCP    172.20.10.3:51055      104.24.8.90:https      TIME_WAIT
  TCP    172.20.10.3:51060      c-q080-u1330-206:https  TIME_WAIT
  TCP    172.20.10.3:51070      104.16.63.54:https     TIME_WAIT
  TCP    172.20.10.3:51074      104.16.53.4:https      TIME_WAIT
  TCP    172.20.10.3:51076      c-q080-u1330-206:https  TIME_WAIT
  TCP    172.20.10.3:51079      63:https               TIME_WAIT
  TCP    172.20.10.3:51080      sc-in-f113:https       TIME_WAIT
  TCP    172.20.10.3:51083      182.161.72.66:https    TIME_WAIT
  TCP    172.20.10.3:51084      182.161.72.66:https    TIME_WAIT
  TCP    172.20.10.3:51085      182.161.72.74:https    TIME_WAIT
  TCP    172.20.10.3:51086      182.161.72.74:https    TIME_WAIT
  TCP    172.20.10.3:51087      ec2-52-197-112-168:https  TIME_WAIT
  TCP    172.20.10.3:51088      182.161.72.71:https    TIME_WAIT
  TCP    172.20.10.3:51089      182.161.72.71:https    TIME_WAIT
  TCP    172.20.10.3:51093      ec2-52-78-39-226:https  TIME_WAIT
  TCP    172.20.10.3:51094      182.161.72.100:https   TIME_WAIT
  TCP    172.20.10.3:51095      68.232.45.96:https     TIME_WAIT
  TCP    172.20.10.3:51096      68.232.45.96:https     TIME_WAIT
^C
C:\Users\Meidi>
```

Dari gambar diatas dapat diperoleh beberapa informasi, yaitu:

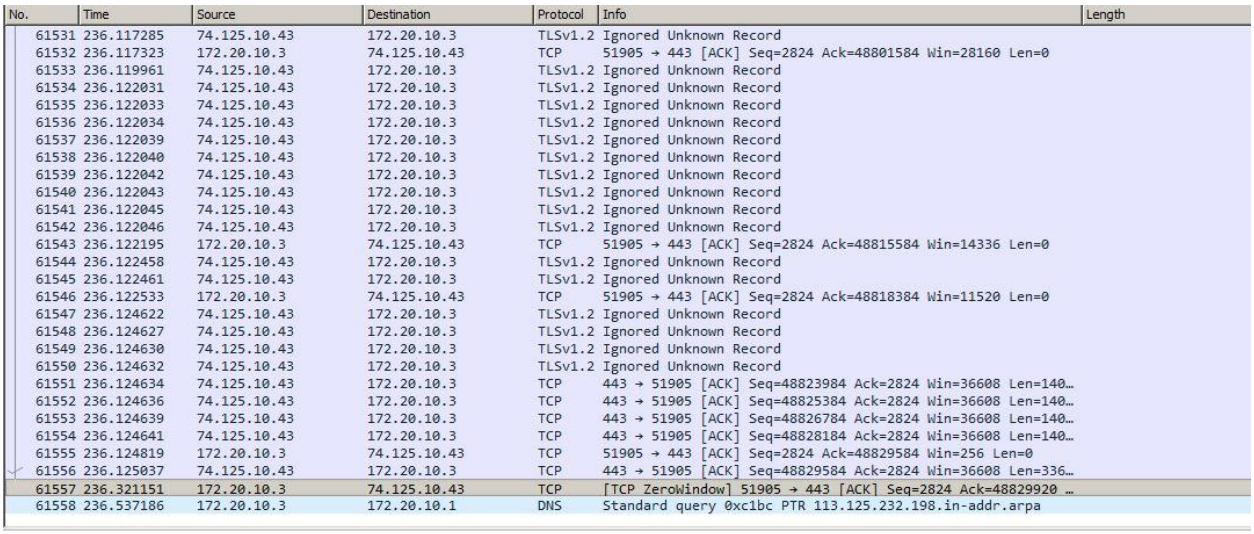
- Proto, menmpilkan protokol yang digunakan pengguna
- Local address, menampilkan alamat ip pengguna/user
- Foreign address, menampilkan penjelasan proses menuju alamat IP yang dituju
- State, menampilkan keadaan proses data yang dilakakukan

Jika pada wireshark proses data dijelaskan mendetail, namun berbeda dengan netstat, netstat hanya menjelaskan suatu keadaan proses seperti listening, estabilished, time wait.

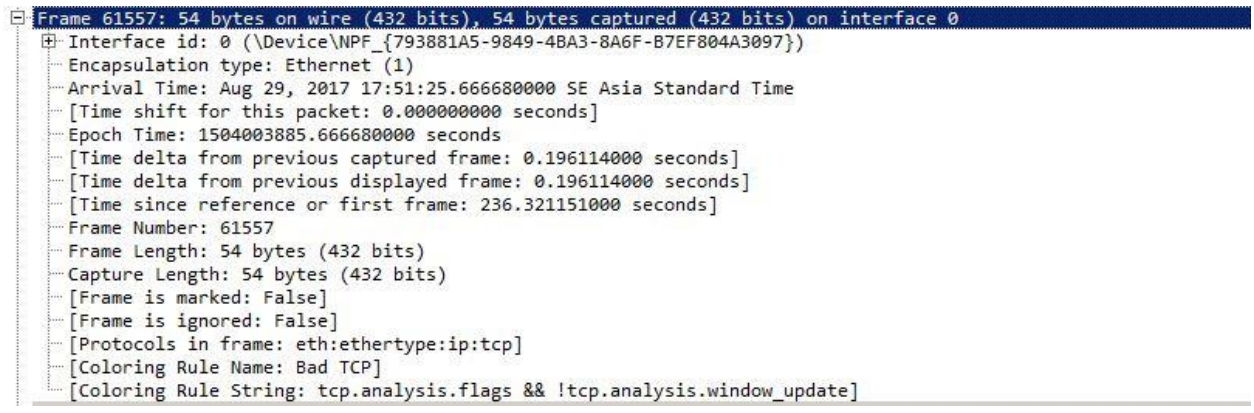
Source IP address	Destination IP address	Protocol	INFO
172.20.10.3	64.58.116.134	TCP	5104 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.20.10.3	64.58.116.134	TCP	51042 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
64.58.116.134	172.20.10.3	TCP	443 → 51041 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=512
172.20.10.3	64.58.116.134	TCP	51041 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0

Source IP address	Destination IP address
172.20.10.3	64.58.116.134
MAC address	MAC address
ac:b5:7d:5b:27:5c	3a:af:61:7c:cf:64

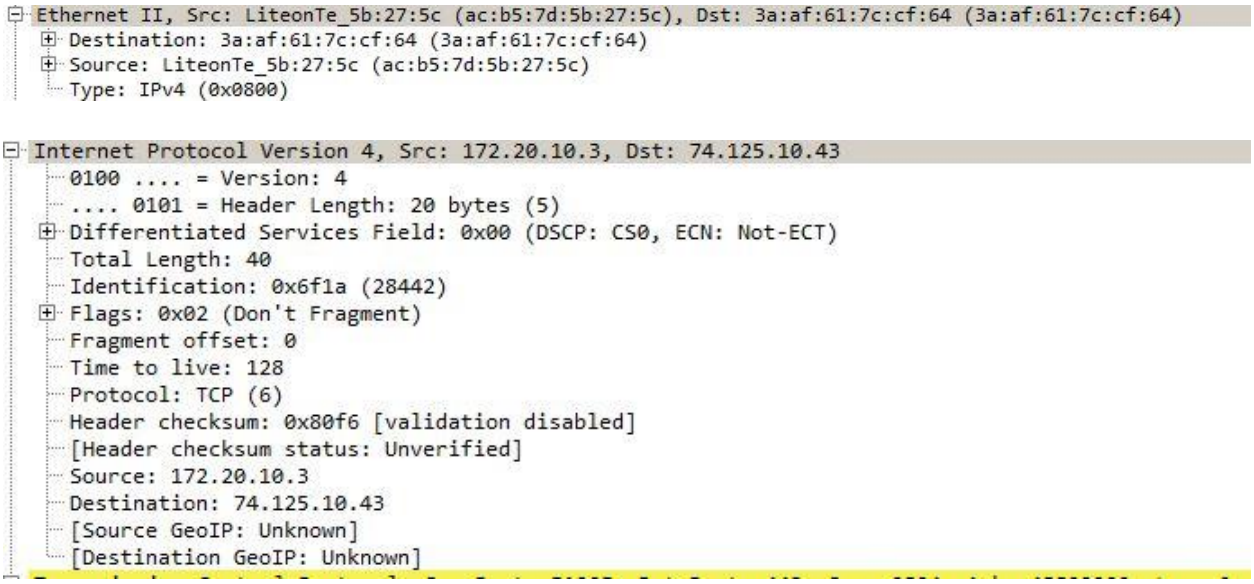
Streaming:

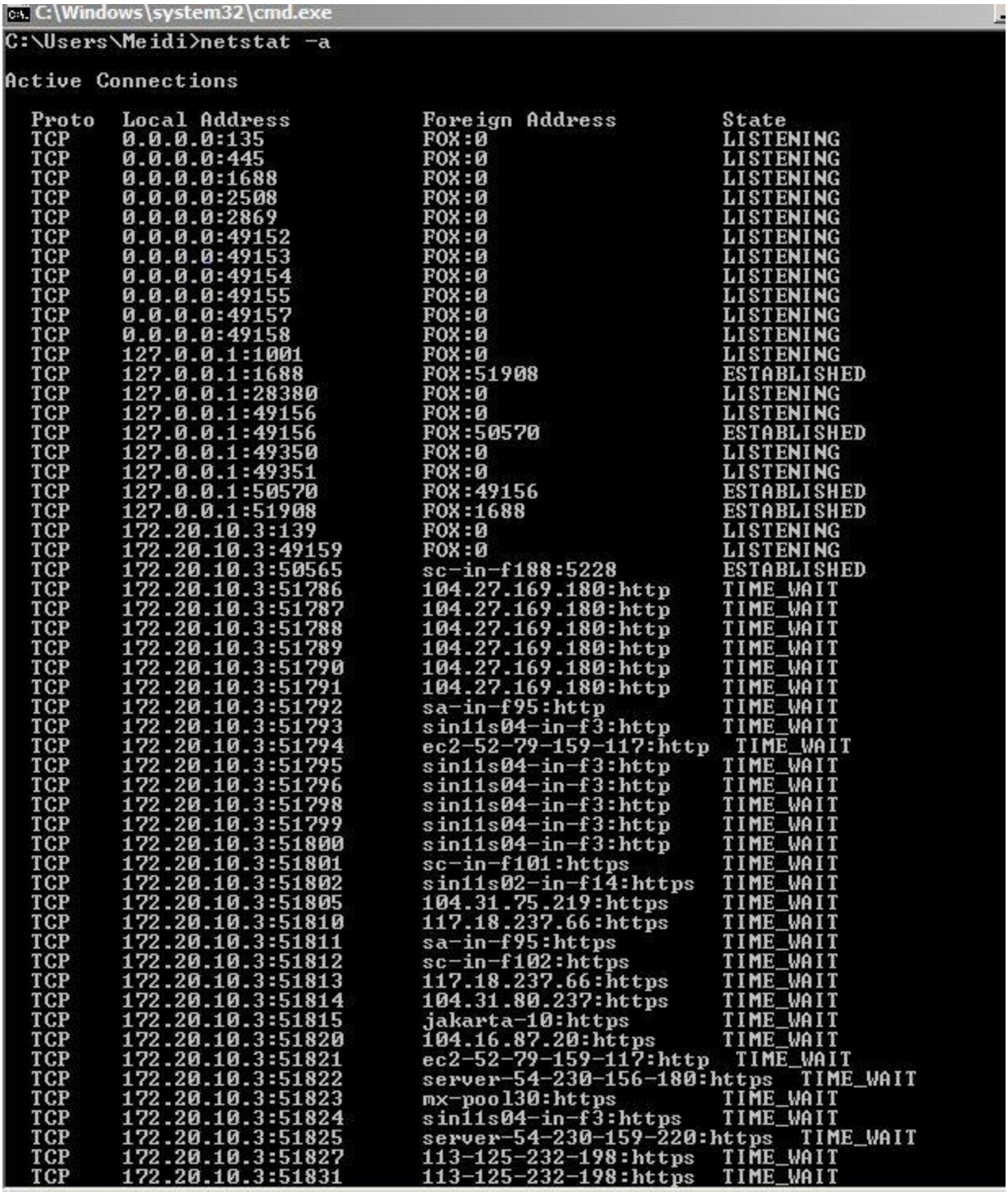


No.	Time	Source	Destination	Protocol	Info	Length
61531	236.117285	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61532	236.117323	172.20.10.3	74.125.10.43	TCP	51905 → 443 [ACK] Seq=2824 Ack=48801584 Win=28160 Len=0	
61533	236.119961	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61534	236.122031	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61535	236.122033	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61536	236.122034	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61537	236.122039	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61538	236.122040	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61539	236.122042	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61540	236.122043	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61541	236.122045	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61542	236.122046	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61543	236.122195	172.20.10.3	74.125.10.43	TCP	51905 → 443 [ACK] Seq=2824 Ack=48815584 Win=14336 Len=0	
61544	236.122458	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61545	236.122461	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61546	236.122533	172.20.10.3	74.125.10.43	TCP	51905 → 443 [ACK] Seq=2824 Ack=48818384 Win=11520 Len=0	
61547	236.124622	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61548	236.124627	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61549	236.124630	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61550	236.124632	74.125.10.43	172.20.10.3	TLSv1.2	Ignored Unknown Record	
61551	236.124634	74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48823984 Ack=2824 Win=36608 Len=140…	
61552	236.124636	74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48825384 Ack=2824 Win=36608 Len=140…	
61553	236.124639	74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48826784 Ack=2824 Win=36608 Len=140…	
61554	236.124641	74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48828184 Ack=2824 Win=36608 Len=140…	
61555	236.124819	172.20.10.3	74.125.10.43	TCP	51905 → 443 [ACK] Seq=2824 Ack=48829584 Win=256 Len=0	
61556	236.125037	74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48829584 Ack=2824 Win=36608 Len=336…	
61557	236.321151	172.20.10.3	74.125.10.43	TCP	[TCP ZeroWindow] 51905 → 443 [ACK] Seq=2824 Ack=48829920 …	
61558	236.537186	172.20.10.3	172.20.10.1	DNS	Standard query 0xc1bc PTR 113.125.232.198.in-addr.arpa	



```
Frame 61557: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
  Interface id: 0 (\Device\NPF_{793881A5-9849-4BA3-8A6F-B7EF804A3097})
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug 29, 2017 17:51:25.666680000 SE Asia Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1504003885.666680000 seconds
  [Time delta from previous captured frame: 0.196114000 seconds]
  [Time delta from previous displayed frame: 0.196114000 seconds]
  [Time since reference or first frame: 236.321151000 seconds]
  Frame Number: 61557
  Frame Length: 54 bytes (432 bits)
  Capture Length: 54 bytes (432 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: Bad TCP]
  [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update]
```


Ethernet II, Src: LiteonTe_5b:27:5c (ac:b5:7d:5b:27:5c), Dst: 3a:af:61:7c:cf:64 (3a:af:61:7c:cf:64)
Destination: 3a:af:61:7c:cf:64 (3a:af:61:7c:cf:64)
Source: LiteonTe_5b:27:5c (ac:b5:7d:5b:27:5c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.20.10.3, Dst: 74.125.10.43
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x6f1a (28442)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x80f6 [validation disabled]
[Header checksum status: Unverified]
Source: 172.20.10.3
Destination: 74.125.10.43
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]


C:\Windows\system32\cmd.exe
C:\Users\Meidi>netstat -a
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 FOX:0 LISTENING
TCP 0.0.0.0:445 FOX:0 LISTENING
TCP 0.0.0.0:1688 FOX:0 LISTENING
TCP 0.0.0.0:2508 FOX:0 LISTENING
TCP 0.0.0.0:2869 FOX:0 LISTENING
TCP 0.0.0.0:49152 FOX:0 LISTENING
TCP 0.0.0.0:49153 FOX:0 LISTENING
TCP 0.0.0.0:49154 FOX:0 LISTENING
TCP 0.0.0.0:49155 FOX:0 LISTENING
TCP 0.0.0.0:49157 FOX:0 LISTENING
TCP 0.0.0.0:49158 FOX:0 LISTENING
TCP 127.0.0.1:1001 FOX:0 LISTENING
TCP 127.0.0.1:1688 FOX:51908 ESTABLISHED
TCP 127.0.0.1:28380 FOX:0 LISTENING
TCP 127.0.0.1:49156 FOX:0 LISTENING
TCP 127.0.0.1:49156 FOX:50570 ESTABLISHED
TCP 127.0.0.1:49350 FOX:0 LISTENING
TCP 127.0.0.1:49351 FOX:0 LISTENING
TCP 127.0.0.1:50570 FOX:49156 ESTABLISHED
TCP 127.0.0.1:51908 FOX:1688 ESTABLISHED
TCP 172.20.10.3:139 FOX:0 LISTENING
TCP 172.20.10.3:49159 FOX:0 LISTENING
TCP 172.20.10.3:50565 sc-in-f188:5228 ESTABLISHED
TCP 172.20.10.3:51786 104.27.169.180:http TIME_WAIT
TCP 172.20.10.3:51787 104.27.169.180:http TIME_WAIT
TCP 172.20.10.3:51788 104.27.169.180:http TIME_WAIT
TCP 172.20.10.3:51789 104.27.169.180:http TIME_WAIT
TCP 172.20.10.3:51790 104.27.169.180:http TIME_WAIT
TCP 172.20.10.3:51791 104.27.169.180:http TIME_WAIT
TCP 172.20.10.3:51792 sa-in-f95:http TIME_WAIT
TCP 172.20.10.3:51793 sin11s04-in-f3:http TIME_WAIT
TCP 172.20.10.3:51794 ec2-52-79-159-117:http TIME_WAIT
TCP 172.20.10.3:51795 sin11s04-in-f3:http TIME_WAIT
TCP 172.20.10.3:51796 sin11s04-in-f3:http TIME_WAIT
TCP 172.20.10.3:51798 sin11s04-in-f3:http TIME_WAIT
TCP 172.20.10.3:51799 sin11s04-in-f3:http TIME_WAIT
TCP 172.20.10.3:51800 sin11s04-in-f3:http TIME_WAIT
TCP 172.20.10.3:51801 sc-in-f101:https TIME_WAIT
TCP 172.20.10.3:51802 sin11s02-in-f14:https TIME_WAIT
TCP 172.20.10.3:51805 104.31.75.219:https TIME_WAIT
TCP 172.20.10.3:51810 117.18.237.66:https TIME_WAIT
TCP 172.20.10.3:51811 sa-in-f95:https TIME_WAIT
TCP 172.20.10.3:51812 sc-in-f102:https TIME_WAIT
TCP 172.20.10.3:51813 117.18.237.66:https TIME_WAIT
TCP 172.20.10.3:51814 104.31.80.237:https TIME_WAIT
TCP 172.20.10.3:51815 jakarta-10:https TIME_WAIT
TCP 172.20.10.3:51820 104.16.87.20:https TIME_WAIT
TCP 172.20.10.3:51821 ec2-52-79-159-117:http TIME_WAIT
TCP 172.20.10.3:51822 server-54-230-156-180:https TIME_WAIT
TCP 172.20.10.3:51823 mx-pool30:https TIME_WAIT
TCP 172.20.10.3:51824 sin11s04-in-f3:https TIME_WAIT
TCP 172.20.10.3:51825 server-54-230-159-220:https TIME_WAIT
TCP 172.20.10.3:51827 113-125-232-198:https TIME_WAIT
TCP 172.20.10.3:51831 113-125-232-198:https TIME_WAIT

Source IP address	Destination IP address	Protocol	INFO
74.125.10.43	172.20.10.3	TCP	443 ?→ 51905 [ACK] Seq=48826784 Ack=2824 Win=36608 Len=1400 [TCP segment of a reassembled PDU]
74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48828184 Ack=2824 Win=36608 Len=1400 [TCP segment of a reassembled PDU]
172.20.10.3	74.125.10.43	TCP	51905 → 443 [ACK] Seq=2824 Ack=48829584 Win=256 Len=0
74.125.10.43	172.20.10.3	TCP	443 → 51905 [ACK] Seq=48829584 Ack=2824 Win=36608 Len=336 [TCP segment of a reassembled PDU]

Source IP address	Destination IP address
172.20.10.3	74.125.10.43
MAC address	MAC address
ac:b5:7d:5b:27:5c	3a:af:61:7c:cf:64