JARINGAN KOMPUTER

Capture Data Web Browser Dan Online Streaming Menggunakan Wireshark Dan Netstat –a

Nama : Alfiansyah
Nim : 09011281520131
Dosen Pengampuh : Deris Setiawan

Jurusan Sistem Komputer
Fakultas Ilmu Komputer
Universitas Sriwijaya
2017

1. Capture data WEB Browser (http://wiki.teamliquid.net/)

Sebelum mulai melakukan capture data, terlebih dahulu kita harus mengetahui IP address komputer kita (source) dan juga IP address dari web browser yang kita tuju (destination), hal ini nantinya akan dapat kita gunakan untuk mempermudah memfilter hasil capture data.

- IP Address Source : 10.178.10.18

  (Dapat kita ketahui dengan mengetikan perintah ipconfig/all melalui cmd)

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Atheros AR9485WB-EG Wireless Network Adap
ter
   Physical Address. . . . . . . . . : 18-67-B0-7A-83-0B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9da9:a4e7:48dc:d5a4%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.178.10.18(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, August 29, 2017 4:47:55 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 30, 2017 4:47:55 PM
   Default Gateway . . . . . . . . . : 10.178.10.1
   DHCP Server . . . . . . . . . . . : 10.178.10.1
   DHCPv6 IAID . . . . . . . . . . . : 286812080
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-A0-A2-FA-18-67-B0-7A-83-0B

   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- IP Adress Destination : 144.217.237.5

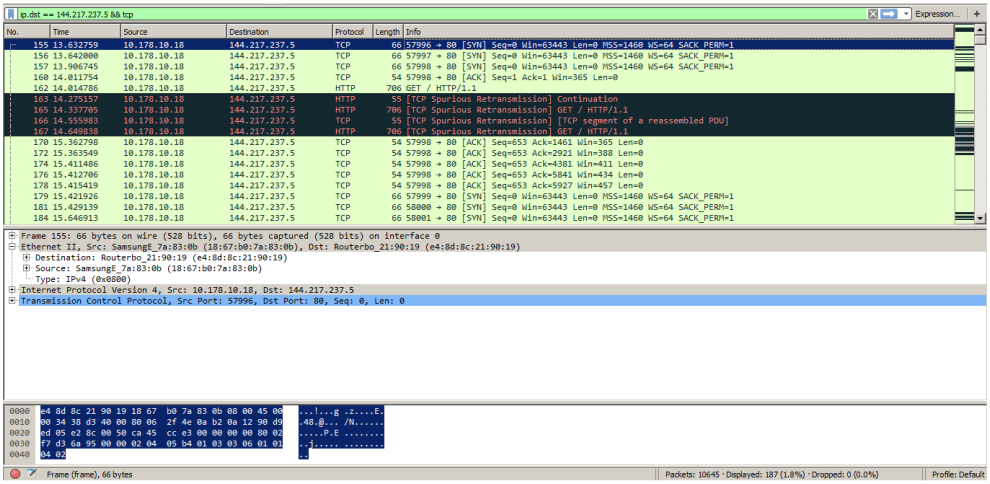
  (Dapat kita ketahui dengan melakukan ping ke web yang kita tuju melalui cmd)

```
C:\Users\Samsung>ping wiki.teamliquid.net

Pinging wiki.teamliquid.net [144.217.237.5] with 32 bytes of data:
Reply from 144.217.237.5: bytes=32 time=348ms TTL=43
Reply from 144.217.237.5: bytes=32 time=337ms TTL=43
Reply from 144.217.237.5: bytes=32 time=376ms TTL=43
Request timed out.

Ping statistics for 144.217.237.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 337ms, Maximum = 376ms, Average = 353ms
```

- Hasil capture data dengan menggunakan wireshark yang sudah di filter berdasarkan IP destination dan protokol FTP



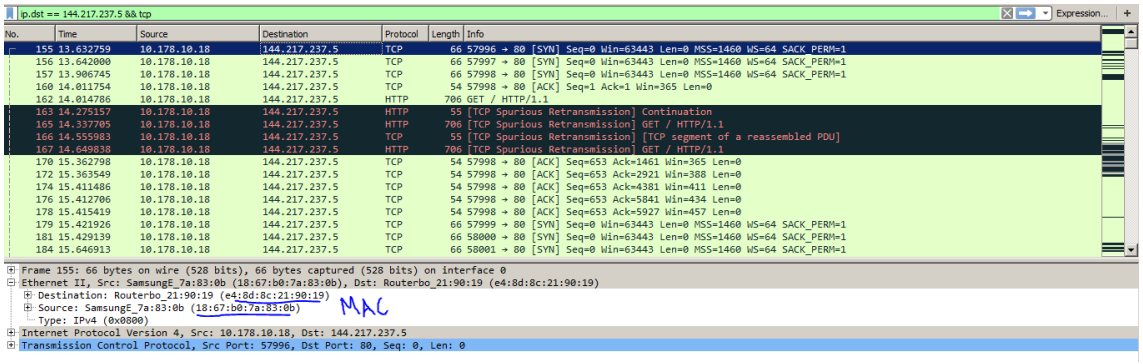
- Tabel hasil capture data

IP Source	IP Destination	Info
10.178.10.18	144.217.237.5	57996 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	57997 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	57998 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=1 Ack=1 Win=365 Len=0
10.178.10.18	144.217.237.5	GET / HTTP/1.1
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] Continuation
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] GET / HTTP/1.1
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] [TCP segment of a reassembled PDU]
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] GET / HTTP/1.1
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=1461 Win=365 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=2921 Win=388 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=4381 Win=411 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=5841 Win=434 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=5927 Win=457 Len=0
10.178.10.18	144.217.237.5	57999 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	58000 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	58001 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	[TCP Window Update] 57998 > 80 [ACK] Seq=653 Ack=5927 Win=480 Len=0
10.178.10.18	144.217.237.5	58000 > 80 [ACK] Seq=1 Ack=1 Win=365 Len=0

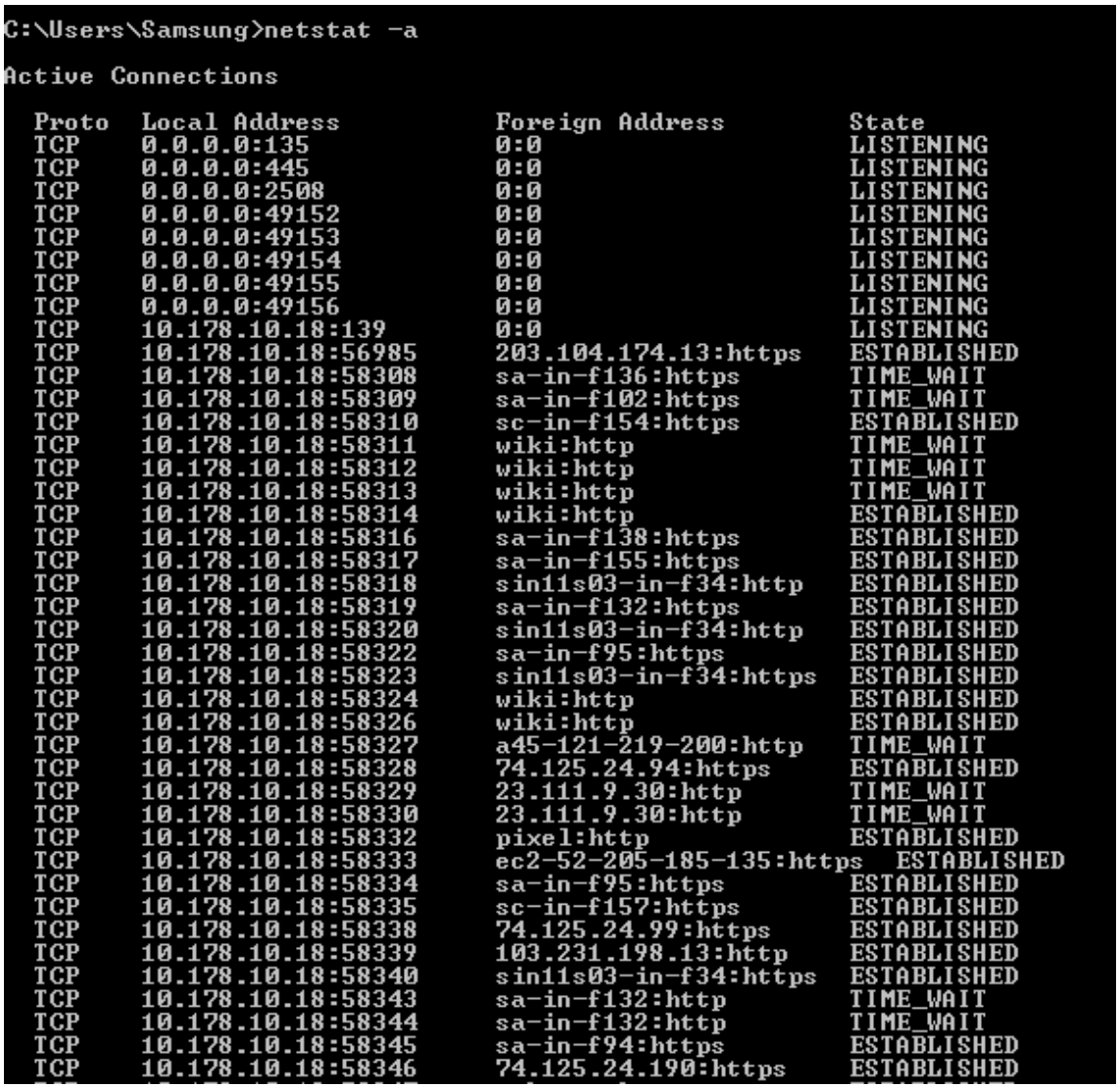
- Setelah melakukan capture data menggunakan wireshark kita dapat melihat detail dari tiap data yang telah kita capture, yang mana diantaranya kita dapat mengetahui MAC address source dan juga destination.

  MAC address source : 18-67-B0-7A-83-0B

  MAC address destination : E4-8D-8C-21-90-19



- Hasil capture data menggunakan netstat –a



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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0:0                    LISTENING
  TCP    0.0.0.0:445            0:0                    LISTENING
  TCP    0.0.0.0:2508           0:0                    LISTENING
  TCP    0.0.0.0:49152          0:0                    LISTENING
  TCP    0.0.0.0:49153          0:0                    LISTENING
  TCP    0.0.0.0:49154          0:0                    LISTENING
  TCP    0.0.0.0:49155          0:0                    LISTENING
  TCP    0.0.0.0:49156          0:0                    LISTENING
  TCP    10.178.10.18:139       0:0                    LISTENING
  TCP    10.178.10.18:56985     203.104.174.13:https   ESTABLISHED
  TCP    10.178.10.18:58308     sa-in-f136:https       TIME_WAIT
  TCP    10.178.10.18:58309     sa-in-f102:https       TIME_WAIT
  TCP    10.178.10.18:58310     sc-in-f154:https       ESTABLISHED
  TCP    10.178.10.18:58311     wiki:http              TIME_WAIT
  TCP    10.178.10.18:58312     wiki:http              TIME_WAIT
  TCP    10.178.10.18:58313     wiki:http              TIME_WAIT
  TCP    10.178.10.18:58314     wiki:http              ESTABLISHED
  TCP    10.178.10.18:58316     sa-in-f138:https       ESTABLISHED
  TCP    10.178.10.18:58317     sa-in-f155:https       ESTABLISHED
  TCP    10.178.10.18:58318     sin11s03-in-f34:http   ESTABLISHED
  TCP    10.178.10.18:58319     sa-in-f132:https       ESTABLISHED
  TCP    10.178.10.18:58320     sin11s03-in-f34:http   ESTABLISHED
  TCP    10.178.10.18:58322     sa-in-f95:https        ESTABLISHED
  TCP    10.178.10.18:58323     sin11s03-in-f34:https  ESTABLISHED
  TCP    10.178.10.18:58324     wiki:http              ESTABLISHED
  TCP    10.178.10.18:58326     wiki:http              ESTABLISHED
  TCP    10.178.10.18:58327     a45-121-219-200:http   TIME_WAIT
  TCP    10.178.10.18:58328     74.125.24.94:https     ESTABLISHED
  TCP    10.178.10.18:58329     23.111.9.30:http       TIME_WAIT
  TCP    10.178.10.18:58330     23.111.9.30:http       TIME_WAIT
  TCP    10.178.10.18:58332     pixel:http             ESTABLISHED
  TCP    10.178.10.18:58333     ec2-52-205-185-135:https  ESTABLISHED
  TCP    10.178.10.18:58334     sa-in-f95:https        ESTABLISHED
  TCP    10.178.10.18:58335     sc-in-f157:https       ESTABLISHED
  TCP    10.178.10.18:58338     74.125.24.99:https     ESTABLISHED
  TCP    10.178.10.18:58339     103.231.198.13:http    ESTABLISHED
  TCP    10.178.10.18:58340     sin11s03-in-f34:https  ESTABLISHED
  TCP    10.178.10.18:58343     sa-in-f132:http        TIME_WAIT
  TCP    10.178.10.18:58344     sa-in-f132:http        TIME_WAIT
  TCP    10.178.10.18:58345     sa-in-f94:https        ESTABLISHED
  TCP    10.178.10.18:58346     74.125.24.190:https    ESTABLISHED
```

Setelah kita menggunakan netstat –a untuk melakukan capture data terdapat beberapa informasi yang kita dapatkan dari koneksi yang terjadi seperti protocol yang digunakan kemudian local dan foreign address dan juga state.

2. Capture data online streaming (http://indoxxi.net/)

- IP Source : 192.168.43.36

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Atheros AR9485WB-EG Wireless Network Adap
ter
   Physical Address. . . . . . . . . : 18-67-B0-7A-83-0B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9da9:a4e7:48dc:d5a4%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.36(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 30, 2017 1:12:07 AM
   Lease Expires . . . . . . . . . . : Wednesday, August 30, 2017 2:12:07 AM
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 286812080
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-A0-A2-FA-18-67-B0-7A-83-0B

   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

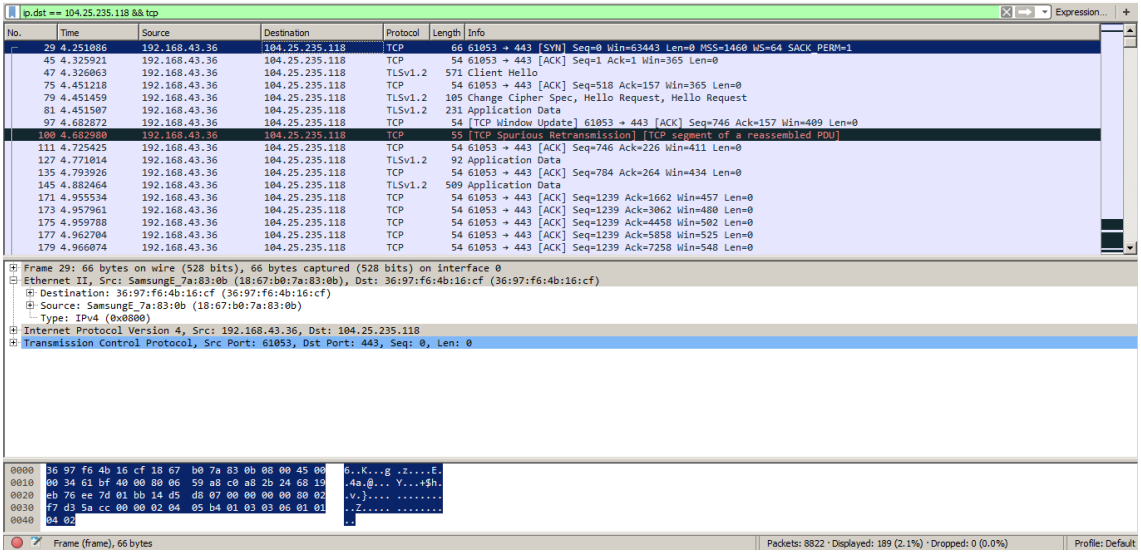
- IP Destination : 104.25.235.118

```
C:\Users\Samsung>ping indoxxi.net

Pinging indoxxi.net [104.25.235.118] with 32 bytes of data:
Reply from 104.25.235.118: bytes=32 time=408ms TTL=54
Reply from 104.25.235.118: bytes=32 time=79ms TTL=54
Reply from 104.25.235.118: bytes=32 time=71ms TTL=54
Reply from 104.25.235.118: bytes=32 time=77ms TTL=54

Ping statistics for 104.25.235.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 71ms, Maximum = 408ms, Average = 158ms
```

- Hasil capture data dengan menggunakan wireshark yang sudah di filter berdasarkan IP destination dan protokol FTP

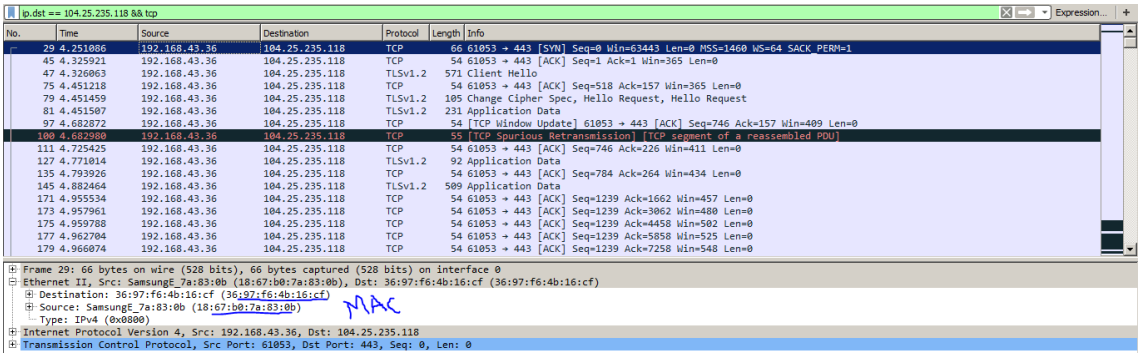


- Tabel hasil capture data

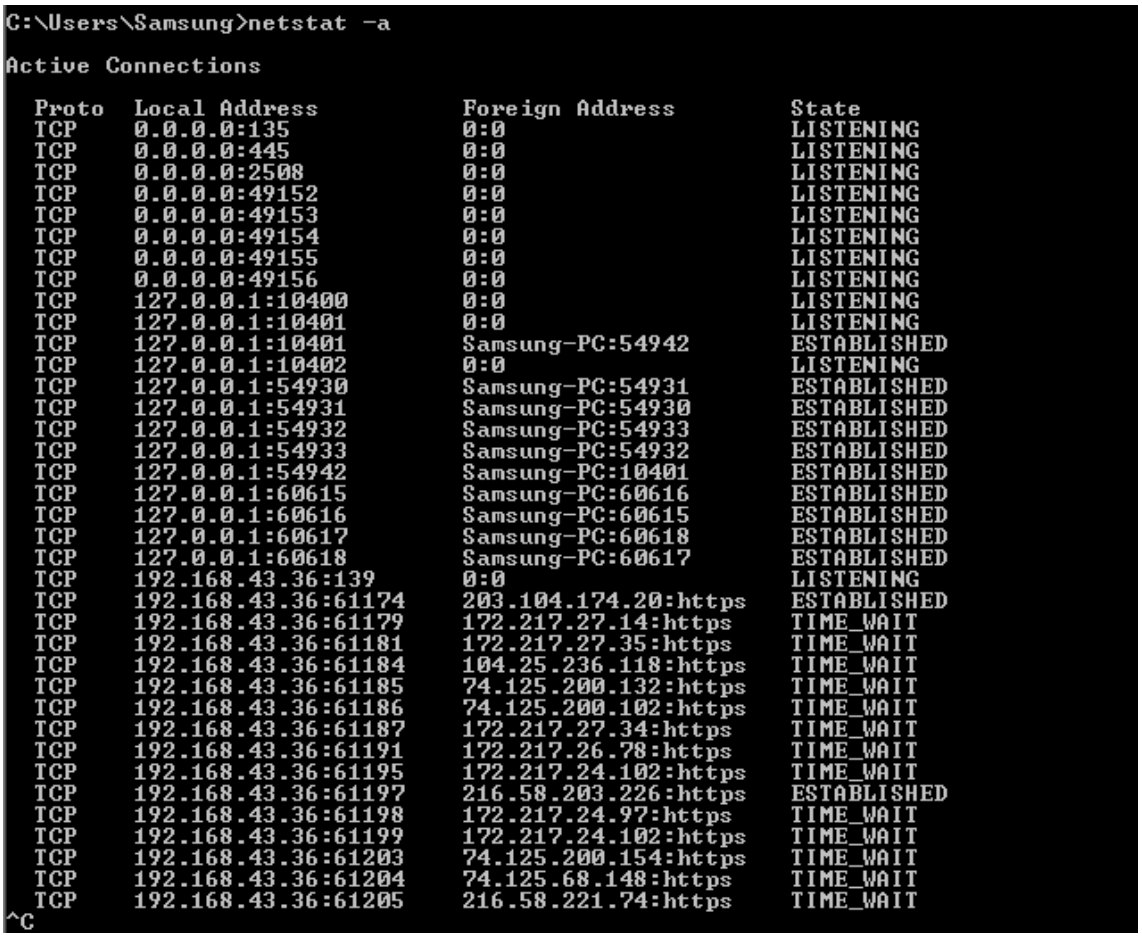
Source	Destination	Info
192.168.43.36	104.25.235.118	61053 > 443 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1 Ack=1 Win=365 Len=0
192.168.43.36	104.25.235.118	Client Hello
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=518 Ack=157 Win=365 Len=0
192.168.43.36	104.25.235.118	Change Cipher Spec, Hello Request, Hello Request
192.168.43.36	104.25.235.118	Application Data
192.168.43.36	104.25.235.118	[TCP Window Update] 61053 > 443 [ACK] Seq=746 Ack=157 Win=409 Len=0
192.168.43.36	104.25.235.118	[TCP Spurious Retransmission] [TCP segment of a reassembled PDU]
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=746 Ack=226 Win=411 Len=0
192.168.43.36	104.25.235.118	Application Data
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=784 Ack=264 Win=434 Len=0
192.168.43.36	104.25.235.118	Application Data
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=1662 Win=457 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=3062 Win=480 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=4458 Win=502 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=5858 Win=525 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=7258 Win=548 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=8658 Win=571 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=10058 Win=594 Len=0

- MAC address source : 18-67-B0-7A-83-0B

  MAC address destination : 36-97-F6-4B-16-CF



- Hasil capture data menggunakan netstat –a



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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0:0                    LISTENING
  TCP    0.0.0.0:445            0:0                    LISTENING
  TCP    0.0.0.0:2508           0:0                    LISTENING
  TCP    0.0.0.0:49152          0:0                    LISTENING
  TCP    0.0.0.0:49153          0:0                    LISTENING
  TCP    0.0.0.0:49154          0:0                    LISTENING
  TCP    0.0.0.0:49155          0:0                    LISTENING
  TCP    0.0.0.0:49156          0:0                    LISTENING
  TCP    127.0.0.1:10400        0:0                    LISTENING
  TCP    127.0.0.1:10401        0:0                    LISTENING
  TCP    127.0.0.1:10401        Samsung-PC:54942       ESTABLISHED
  TCP    127.0.0.1:10402        0:0                    LISTENING
  TCP    127.0.0.1:54930        Samsung-PC:54931       ESTABLISHED
  TCP    127.0.0.1:54931        Samsung-PC:54930       ESTABLISHED
  TCP    127.0.0.1:54932        Samsung-PC:54933       ESTABLISHED
  TCP    127.0.0.1:54933        Samsung-PC:54932       ESTABLISHED
  TCP    127.0.0.1:54942        Samsung-PC:10401       ESTABLISHED
  TCP    127.0.0.1:60615        Samsung-PC:60616       ESTABLISHED
  TCP    127.0.0.1:60616        Samsung-PC:60615       ESTABLISHED
  TCP    127.0.0.1:60617        Samsung-PC:60618       ESTABLISHED
  TCP    127.0.0.1:60618        Samsung-PC:60617       ESTABLISHED
  TCP    192.168.43.36:139      0:0                    LISTENING
  TCP    192.168.43.36:61174    203.104.174.20:https   ESTABLISHED
  TCP    192.168.43.36:61179    172.217.27.14:https    TIME_WAIT
  TCP    192.168.43.36:61181    172.217.27.35:https    TIME_WAIT
  TCP    192.168.43.36:61184    104.25.236.118:https   TIME_WAIT
  TCP    192.168.43.36:61185    74.125.200.132:https   TIME_WAIT
  TCP    192.168.43.36:61186    74.125.200.102:https   TIME_WAIT
  TCP    192.168.43.36:61187    172.217.27.34:https    TIME_WAIT
  TCP    192.168.43.36:61191    172.217.26.78:https    TIME_WAIT
  TCP    192.168.43.36:61195    172.217.24.102:https   TIME_WAIT
  TCP    192.168.43.36:61197    216.58.203.226:https   ESTABLISHED
  TCP    192.168.43.36:61198    172.217.24.97:https    TIME_WAIT
  TCP    192.168.43.36:61199    172.217.24.102:https   TIME_WAIT
  TCP    192.168.43.36:61203    74.125.200.154:https   TIME_WAIT
  TCP    192.168.43.36:61204    74.125.68.148:https    TIME_WAIT
  TCP    192.168.43.36:61205    216.58.221.74:https    TIME_WAIT
^C
```

3. Perbandingan capture data menggunakan Wireshark dan Netstat –a

Perbandingan	Wireshark	Netstat -a
Protokol	1482 lebih protokol	TCP & UDP
Filtering paket data jaringan	Ya	Tidak
Menampilkan detail dari hasil capture data	Ya	Tidak
Hasil capture dapat disimpan untuk dianalisa kembali	Ya	Tidak