

TASK V

**OBSERVING TCP/IP, PORT USING COMMAND PROMPT
AND WIRESHARK**



Disusun oleh:

NAMA : ARUM CANTIKA PUTRI

NIM : 09011181419022

DOSEN : DERIS STIAWAN, M.T., Ph.D.

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWAJAYA

MENGANALISA TCP/IP, PORT MENGGUNAKAN COMMAND PROMPT DAN WIRESHARK

Transport Layer Protocol adalah lapisan keempat dari model referensi OSI dan jantung dari hierarki protokol secara keseluruhan karena protokol ini berfungsi untuk menyediakan data transport dari komputer asal atau sumber menuju ke komputer tujuan, yang tidak bergantung pada jaringan fisik atau jaringan-jaringan yang digunakan. Tanpa adanya Transport Layer Protocol ini maka seluruh konsep protokol yang menggunakan layer menjadi tidak ada fungsinya.

Transport layer protocol inilah yang juga mengatur koneksi dari suatu komputer pengirim ke komputer penerima serta juga yang membangun koneksi logic antara host pengirim dengan client penerima dalam sebuah jaringan. Layer ini juga mengatur dan mengaplikasikan layanan transport yang efektif antar jaringan untuk layer-layer di atasnya.

Dalam TCP/IP Transport Layer digunakan 2 macam protokol, yakni TCP dan UDP. TCP (Transmission Control Protocol) adalah protokol yang bertugas untuk membentuk koneksi antar node. Sifat TCP adalah connection-oriented. TCP baru akan membuat koneksi jika kedua belah pihak telah setuju. Karenanya, TCP dianggap reliable (dapat diandalkan). Berbeda dengan UDP (User Datagram Protocol) yang connectionless, transmisi data yang berbasis UDP akan langsung mengirimkan paket karena tidak ada kesepakatan dulu antar node yang bertransmisi.

Masing-masing protokol memiliki karakteristik tertentu dan mendukung protokol-protokol pada layer di atasnya. Misalnya TCP mendukung HTTP dan FTP, sementara UDP mendukung DNS dan TFTP. Perbedaan antara kedua protokol tersebut ada pada reliabilitasnya. Untuk menjalankan tugasnya baik TCP dan UDP menambahkan header pada data yang akan dikirim. Isi header antara kedua protokol tersebut berbeda, sesuai dengan karakteristik masing-masing protokol. Header yang dipasang oleh kedua protokol tersebut dapat

identifikasi dan dianalisis dengan menggunakan network analyzer tool, salah satunya adalah Wireshark.

Wireshark adalah tool yang ditujukan untuk melakukan analisa paket data jaringan. Wireshark melakukan monitoring paket secara real-time selanjutnya Wireshark melakukan penangkapan data dan menampilkannya selengkap mungkin.

PENJELASAN CAPTURE PAKET DATA PADA WIRESHARK

Berikut, saya menggunakan wireshark untuk menganalisa TCP/IP Port pada website kapanlagi.com. Setelah memilih network adapter yang akan digunakan untuk monitoring packet maka kita akan mendapatkan paket jaringan seperti ini.

Selanjutnya di capture yg akan menampilkan bentuk traffic yg warna-warni di mana terdapat keterangan seperti :

1. Time (menampilkan diwaktu waktu paket tersebut tertangkap);
2. Source (menampilkan IP Source dari paket tersebut).
3. Destination (menampilkan IP Destination dari paket tersebut);
4. Protocol (menampilkan protokol yg difungsikan paket data tersebut);
5. Info(menampilkan info dettail paket tersebut).

tcp.stream eq 7

No.	Time	Source	Destination	Protocol	Length	Info
281	23.368774	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=83222 Win=45260 Len=0
282	23.368821	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=84682 Win=45260 Len=0
283	23.368875	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=86142 Win=45260 Len=0
284	23.372230	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=87602 Win=45260 Len=0
285	23.372390	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=89062 Win=45260 Len=0
286	23.382992	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=90522 Win=45260 Len=0
287	23.383156	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=91982 Win=45260 Len=0
288	23.383215	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=93442 Win=45260 Len=0
289	23.383271	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=94902 Win=45260 Len=0
290	23.383320	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=96362 Win=45260 Len=0
291	23.399012	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=97822 Win=45260 Len=0
292	23.399175	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=99282 Win=45260 Len=0
293	23.399234	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=100742 Win=48180 Len=0
294	23.399285	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=102202 Win=49640 Len=0
295	23.399335	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=103662 Win=51100 Len=0
296	23.462566	203.12.21.5	10.117.105.155	HTTP	1379	HTTP/1.1 200 OK (text/html)
297	23.462719	10.117.105.155	203.12.21.5	TCP	54	52444→80 [ACK] Seq=1259 Ack=104987 Win=52560 Len=0
299	23.711172	10.117.105.155	203.12.21.5	TCP	54	[TCP Window Update] 52444→80 [ACK] Seq=1259 Ack=104987 Win=54020

Frame 146: 1312 bytes on wire (10496 bits), 1312 bytes captured (10496 bits) on interface 0
 Ethernet II, Src: LiteonTe_c9:8f:96 (a4:db:30:c9:8f:96), Dst: Ericsson_20:9d:21 (00:30:88:20:9d:21)
 Internet Protocol Version 4, Src: 10.117.105.155, Dst: 203.12.21.5
 Transmission Control Protocol, Src Port: 52444, Dst Port: 80, Seq: 1, Ack: 1, Len: 1258

```

0000 00 30 88 20 9d 21 a4 db 30 c9 8f 96 00 00 45 00  .0...0...E.
0010 05 12 67 bb 40 00 80 06 3a 09 0a 75 69 9b cb 0c  ..g@...+.4".0.u
0020 15 05 cc dc 00 50 a4 80 dd e7 78 c8 f1 0d 50 18  ....P...x...P.
0030 5b 40 57 33 00 00 47 45 54 20 2f 20 48 54 50 50  [@W3..GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: www.

```

Menampilkan “GET” untuk http terhadap host www.kapanlagi.com caranya dengan memfilter http.host www.kapanlagi.com

http

No.	Time	Source	Destination	Protocol	Length	Info
146	23.115414	10.117.105.155	203.12.21.5	HTTP	1312	GET / HTTP/1.1
296	23.462566	203.12.21.5	10.117.105.155	HTTP	1379	HTTP/1.1 200 OK (text/html)
327	24.818176	10.117.105.155	182.161.72.100	HTTP	251	GET /delivery/rta/rta.js?netId=3467&cookieName=crtg_rta&rnd=1890...
341	24.970432	182.161.72.100	10.117.105.155	HTTP	207	HTTP/1.1 200 OK (text/javascript)
358	25.131942	10.117.105.155	103.6.0.2	HTTP	592	GET /internal-ads/201681917/1/data.js HTTP/1.1
384	25.200311	103.6.0.2	10.117.105.155	HTTP	1056	HTTP/1.1 200 OK (application/javascript)
392	25.319232	10.117.105.155	54.239.16.235	HTTP	392	GET /x.png HTTP/1.1
408	25.412608	10.117.105.155	209.58.162.57	HTTP	272	GET /get?action_name=Kalau%20Bukan%20Sekarang%2C%20Kapan%20Lagi%...
412	25.445623	209.58.162.57	10.117.105.155	HTTP	672	HTTP/1.1 200 OK (application/javascript)
481	26.195810	54.239.16.235	10.117.105.155	HTTP	376	HTTP/1.1 302 Found
527	26.953729	10.117.105.155	205.251.219.243	HTTP	427	GET /test.png HTTP/1.1
563	27.464873	205.251.219.243	10.117.105.155	HTTP	518	HTTP/1.1 200 OK (text/plain)
729	28.681364	10.117.105.155	52.34.204.79	HTTP	628	GET /redir/73261/0/4201/130216829/71261286/915481/0/0/0/1.ver?at...
749	29.126557	52.34.204.79	10.117.105.155	HTTP	315	HTTP/1.1 204 No Content
858	31.204262	10.117.105.155	52.34.204.79	HTTP	706	GET /812172/0/4201/130216829/71261286/915481/0/0/0/1.ver?at=ol&d...
872	31.434782	10.117.105.155	182.161.72.100	HTTP	227	GET /delivery/rta/rta.js?netId=3963&cookieName=innity.crtg&rnd=1...
879	31.588605	10.117.105.155	172.217.24.226	HTTP	1152	GET /activeview?avi=Bey4wVrjFV7qiNoK5vASTop-oAWAAAAAQATByAE3wAI...
886	31.738832	182.161.72.100	10.117.105.155	HTTP	224	HTTP/1.1 200 OK (text/javascript)

Frame 749: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0
 Ethernet II, Src: Ericsson_20:9d:21 (00:30:88:20:9d:21), Dst: LiteonTe_c9:8f:96 (a4:db:30:c9:8f:96)
 Internet Protocol Version 4, Src: 52.34.204.79, Dst: 10.117.105.155
 Transmission Control Protocol, Src Port: 80, Dst Port: 52484, Seq: 1, Ack: 575, Len: 261

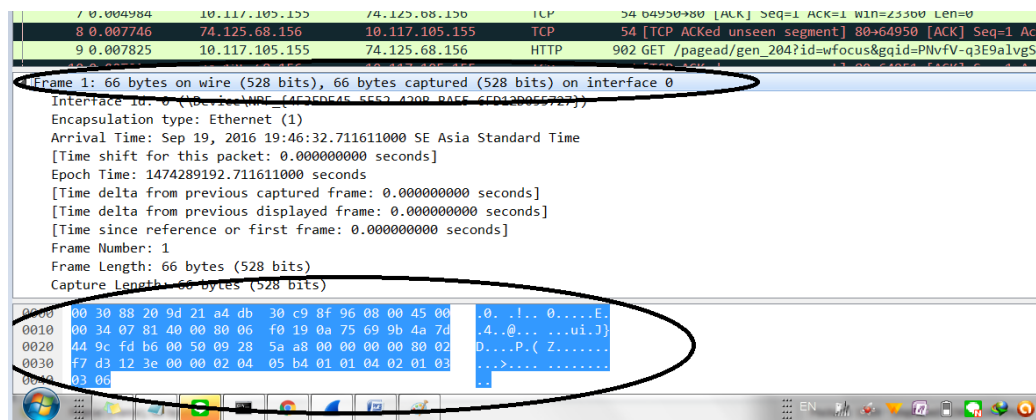
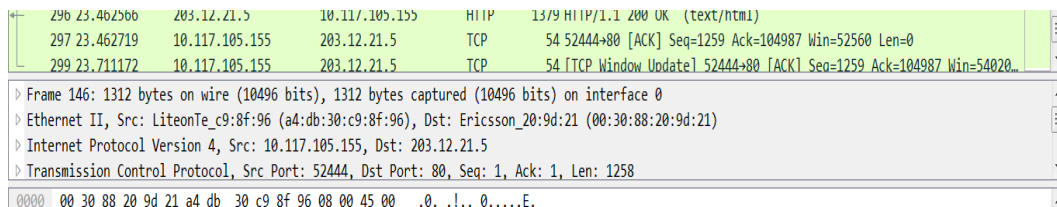
```

0000 a4 db 30 c9 8f 96 00 30 88 20 9d 21 08 00 45 00  .0...0...E.
0010 01 2d de 67 40 00 fb 06 2b e1 34 22 cc 4f 0a 75  ..g@...+.4".0.u
0020 69 9b 00 50 cd 04 3f 06 b6 0e 8c 67 97 04 50 18  i..P..?....g..P.
0030 5b 40 a2 d4 00 00 48 54 54 50 2f 31 2e 31 20 32  [@...HT TP/1.1 2
0040 30 34 20 4e 6f 20 43 6f 6e 74 65 6e 74 0d 0a 43  04 No Co ntent...C

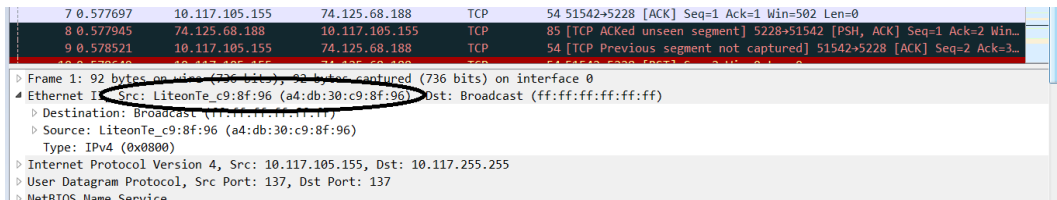
```



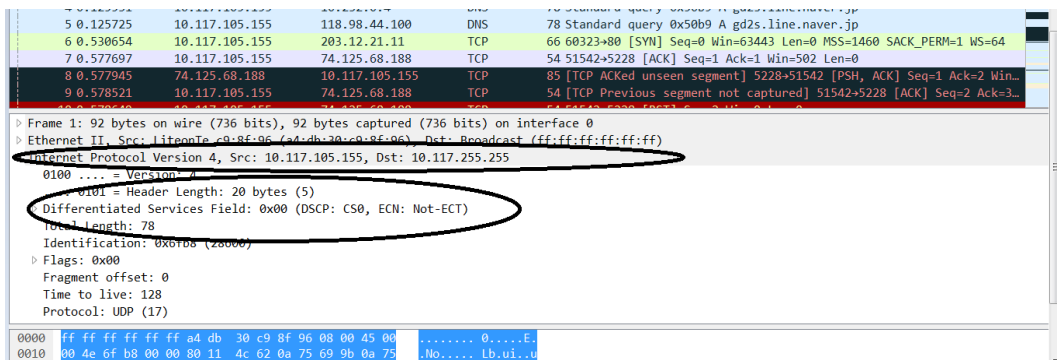

Capture di bawah merupakan IP dan port number TCP yang digunakan oleh client dan server



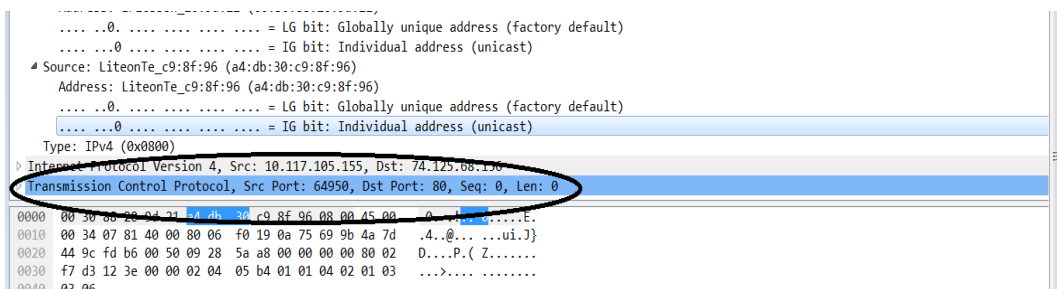
Pada gambar diatas merupakan ringkasan dari paket data. Untuk baris yang lainnya menunjukkan data link layer, network layer , dan transport layer . Pada dasarnya paket data yang telah dicapture terbungkus didalam frame seperti gambar diatas.



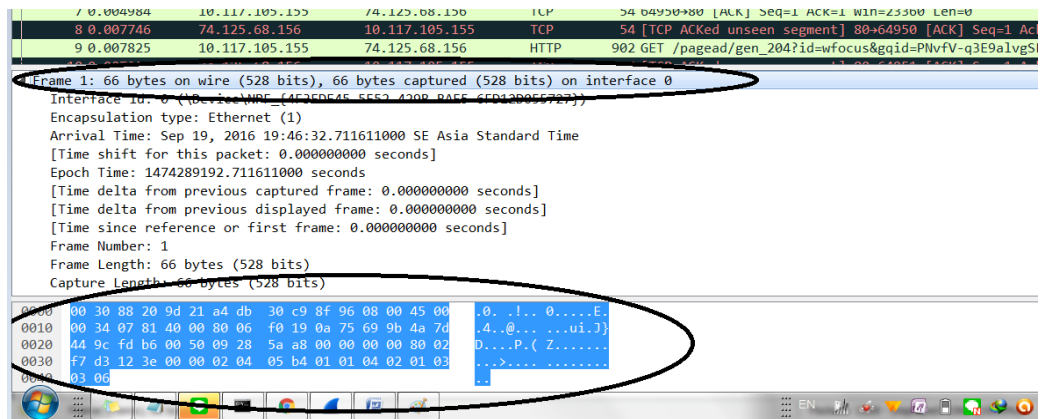
Pada gambar diatas menunjukkan alamat tujuan dan alamat asalnya dalam bentuk mac address.



Pada gambar diatas menunjukkan alamat tujuan dan alamat asal dalam bentuk IP. Dari gambar diatas juga terlihat bahwa bytes Header 20 bytes



Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (64950) dan port tujuannya (80). Port 80 merupakan port untuk TCP.



PENJELASAN CAPTURE PAKET DATA PADA COMMAND

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ACER>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              E1-422:0               LISTENING
TCP    0.0.0.0:445             E1-422:0               LISTENING
TCP    0.0.0.0:2343            E1-422:0               LISTENING
TCP    0.0.0.0:3580            E1-422:0               LISTENING
TCP    0.0.0.0:3582            E1-422:0               LISTENING
TCP    0.0.0.0:8080            E1-422:0               LISTENING
TCP    0.0.0.0:8733            E1-422:0               LISTENING
TCP    0.0.0.0:9007            E1-422:0               LISTENING
TCP    0.0.0.0:12025           E1-422:0               LISTENING
TCP    0.0.0.0:12110           E1-422:0               LISTENING
TCP    0.0.0.0:12119           E1-422:0               LISTENING
TCP    0.0.0.0:12143           E1-422:0               LISTENING
TCP    0.0.0.0:12465           E1-422:0               LISTENING
TCP    0.0.0.0:12563           E1-422:0               LISTENING
TCP    0.0.0.0:12993           E1-422:0               LISTENING
TCP    0.0.0.0:12995           E1-422:0               LISTENING
TCP    0.0.0.0:27275           E1-422:0               LISTENING
TCP    0.0.0.0:31337           E1-422:0               LISTENING
TCP    0.0.0.0:49152           E1-422:0               LISTENING
TCP    0.0.0.0:49153           E1-422:0               LISTENING
TCP    0.0.0.0:49154           E1-422:0               LISTENING
TCP    0.0.0.0:49155           E1-422:0               LISTENING
TCP    0.0.0.0:49188           E1-422:0               LISTENING
TCP    0.0.0.0:59110           E1-422:0               LISTENING
TCP    0.0.0.0:59111           E1-422:0               LISTENING
TCP    10.117.105.155:139      E1-422:0               LISTENING
TCP    10.117.105.155:50789   203.104.174.12:https  ESTABLISHED

```



```
Administrator: C:\Windows\system32\cmd.exe
TCP 10.117.105.155:50789 203.104.174.12:https ESTABLISHED
TCP 10.117.105.155:52396 sb-in-f188:5228 ESTABLISHED
TCP 10.117.105.155:52398 ku101s10-in-f36:https ESTABLISHED
TCP 10.117.105.155:52402 a23-2-64-224:https ESTABLISHED
TCP 10.117.105.155:52404 ea-in-f148:https ESTABLISHED
TCP 10.117.105.155:52407 ku106s17-in-f2:http ESTABLISHED
TCP 10.117.105.155:52409 ea-in-f149:https ESTABLISHED
TCP 127.0.0.1:1001 E1-422:0 LISTENING
TCP 127.0.0.1:5354 E1-422:0 LISTENING
TCP 127.0.0.1:5939 E1-422:0 LISTENING
TCP 127.0.0.1:6543 E1-422:0 LISTENING
TCP 127.0.0.1:10400 E1-422:0 LISTENING
TCP 127.0.0.1:12025 E1-422:0 LISTENING
TCP 127.0.0.1:12080 E1-422:0 LISTENING
TCP 127.0.0.1:12080 E1-422:52406 ESTABLISHED
TCP 127.0.0.1:12110 E1-422:0 LISTENING
TCP 127.0.0.1:12119 E1-422:0 LISTENING
TCP 127.0.0.1:12143 E1-422:0 LISTENING
TCP 127.0.0.1:12344 E1-422:0 LISTENING
TCP 127.0.0.1:12344 E1-422:52395 ESTABLISHED
TCP 127.0.0.1:12344 E1-422:52397 ESTABLISHED
TCP 127.0.0.1:12344 E1-422:52401 ESTABLISHED
TCP 127.0.0.1:12344 E1-422:52403 ESTABLISHED
TCP 127.0.0.1:12344 E1-422:52405 ESTABLISHED
TCP 127.0.0.1:12344 E1-422:52408 ESTABLISHED
TCP 127.0.0.1:12465 E1-422:0 LISTENING
TCP 127.0.0.1:12563 E1-422:0 LISTENING
TCP 127.0.0.1:12993 E1-422:0 LISTENING
TCP 127.0.0.1:12995 E1-422:0 LISTENING
TCP 127.0.0.1:27275 E1-422:0 LISTENING
TCP 127.0.0.1:49156 E1-422:49157 ESTABLISHED
TCP 127.0.0.1:49157 E1-422:49156 ESTABLISHED
TCP 127.0.0.1:49158 E1-422:49160 ESTABLISHED
TCP 127.0.0.1:49160 E1-422:49158 ESTABLISHED
TCP 127.0.0.1:49172 E1-422:49173 ESTABLISHED
```

```
Administrator: C:\Windows\system32\cmd.exe
TCP 127.0.0.1:49173 E1-422:49172 ESTABLISHED
TCP 127.0.0.1:49177 E1-422:49181 ESTABLISHED
TCP 127.0.0.1:49178 E1-422:0 LISTENING
TCP 127.0.0.1:49178 E1-422:49185 ESTABLISHED
TCP 127.0.0.1:49181 E1-422:49177 ESTABLISHED
TCP 127.0.0.1:49185 E1-422:49178 ESTABLISHED
TCP 127.0.0.1:49189 E1-422:0 LISTENING
TCP 127.0.0.1:49189 E1-422:49272 ESTABLISHED
TCP 127.0.0.1:49190 E1-422:0 LISTENING
TCP 127.0.0.1:49272 E1-422:49189 ESTABLISHED
TCP 127.0.0.1:49397 E1-422:49398 ESTABLISHED
TCP 127.0.0.1:49398 E1-422:49397 ESTABLISHED
TCP 127.0.0.1:49399 E1-422:49400 ESTABLISHED
TCP 127.0.0.1:49400 E1-422:49399 ESTABLISHED
TCP 127.0.0.1:49401 E1-422:49402 ESTABLISHED
TCP 127.0.0.1:49402 E1-422:49401 ESTABLISHED
TCP 127.0.0.1:49403 E1-422:49404 ESTABLISHED
TCP 127.0.0.1:49404 E1-422:49403 ESTABLISHED
TCP 127.0.0.1:49407 E1-422:49408 ESTABLISHED
TCP 127.0.0.1:49422 E1-422:49407 ESTABLISHED
TCP 127.0.0.1:49423 E1-422:49423 ESTABLISHED
TCP 127.0.0.1:49424 E1-422:49426 ESTABLISHED
TCP 127.0.0.1:49426 E1-422:49424 ESTABLISHED
TCP 127.0.0.1:49427 E1-422:49428 ESTABLISHED
TCP 127.0.0.1:49428 E1-422:49427 ESTABLISHED
TCP 127.0.0.1:49430 E1-422:49431 ESTABLISHED
TCP 127.0.0.1:49431 E1-422:49430 ESTABLISHED
TCP 127.0.0.1:50618 E1-422:50619 ESTABLISHED
TCP 127.0.0.1:50619 E1-422:50618 ESTABLISHED
TCP 127.0.0.1:50625 E1-422:50626 ESTABLISHED
TCP 127.0.0.1:50626 E1-422:50625 ESTABLISHED
TCP 127.0.0.1:50627 E1-422:50630 ESTABLISHED
TCP 127.0.0.1:50630 E1-422:50627 ESTABLISHED
TCP 127.0.0.1:50785 E1-422:50786 ESTABLISHED
```



```
Administrator: C:\Windows\system32\cmd.exe
UDP 10.117.105.155:137 *:*
UDP 10.117.105.155:138 *:*
UDP 10.117.105.155:1900 *:*
UDP 10.117.105.155:5353 *:*
UDP 10.117.105.155:5353 *:*
UDP 10.117.105.155:55703 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:55705 *:*
UDP 169.254.52.59:137 *:*
UDP 169.254.52.59:138 *:*
UDP 169.254.52.59:1900 *:*
UDP 169.254.52.59:5353 *:*
UDP 169.254.52.59:5353 *:*
UDP 169.254.52.59:5353 *:*
UDP 169.254.52.59:55704 *:*
UDP [::]:500 *:*
UDP [::]:4500 *:*
UDP [::]:5353 *:*
UDP [::]:5353 *:*
UDP [::]:5353 *:*
UDP [::]:49153 *:*
UDP [::]:49155 *:*
UDP [::]:49157 *:*
UDP [::]:1900 *:*
UDP [::]:55702 *:*
UDP [fe80::c4ac:c797:56b7:343b718]:1900 *:*
UDP [fe80::c4ac:c797:56b7:343b718]:5353 *:*
UDP [fe80::c4ac:c797:56b7:343b718]:5353 *:*
UDP [fe80::c4ac:c797:56b7:343b718]:55701 *:*
UDP [fe80::ed0d:ee73:e605:e012212]:546 *:*
UDP [fe80::ed0d:ee73:e605:e012212]:1900 *:*
UDP [fe80::ed0d:ee73:e605:e012212]:55700 *:*
C:\Users\ACER>
```

Keterangan output netstat:

1. **Proto.** Kolom proto menunjukkan jenis protokol yang dipakai bisa TCP atau UDP.
2. **Local Address.** Kolom ini menjelaskan alamat dan nomor port yang ada di komputer kita yang mana saat itu sedang aktif melakukan koneksi.
3. **Foreign Address.** Kolom ini menunjukkan koneksi yang dituju oleh local address beserta nomor port tujuannya.
4. **State.** Kolom ini menunjukkan status dari koneksi yang sedang terjadi

Diantara capture wireshark dan command prompt terdapat perbedaan, bahwa pada command memiliki output netstat states yang isinya menjelaskan established dan listening.