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 protocol yang menggunakan layar 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 menjalanakan 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.

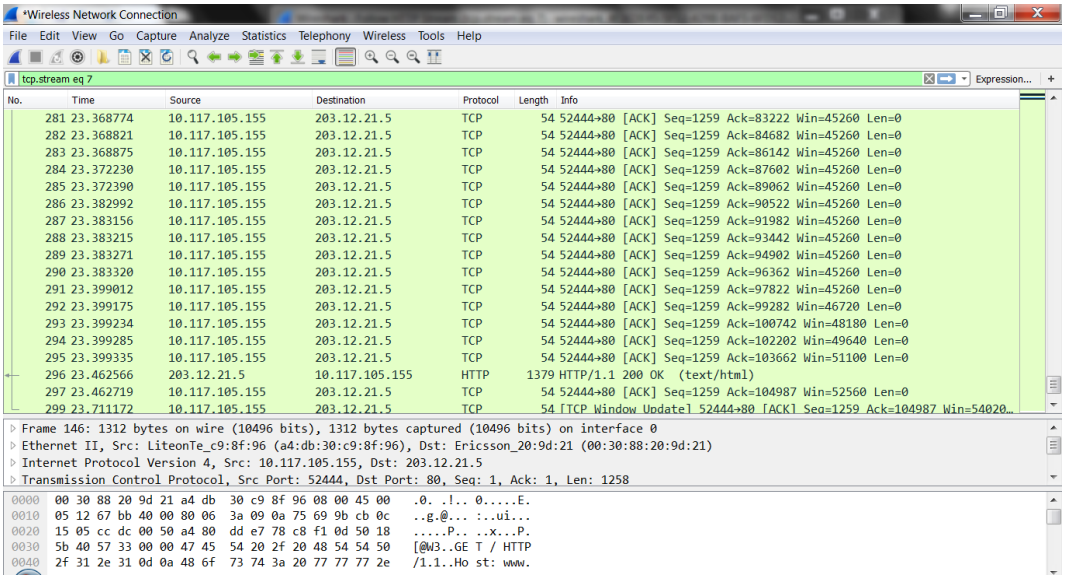
Wireshark adalah tool yang ditujukan untuk melakukan analisa paket data jaringan. Wireshark melalukan monitoring paket secara real-time selanjutnya Wireshark melakukan penangkapan data dan menampilkannya selengkap mungkin.

PENJELASAN CAPTURE PAKET DATA PADA WIRESHARK

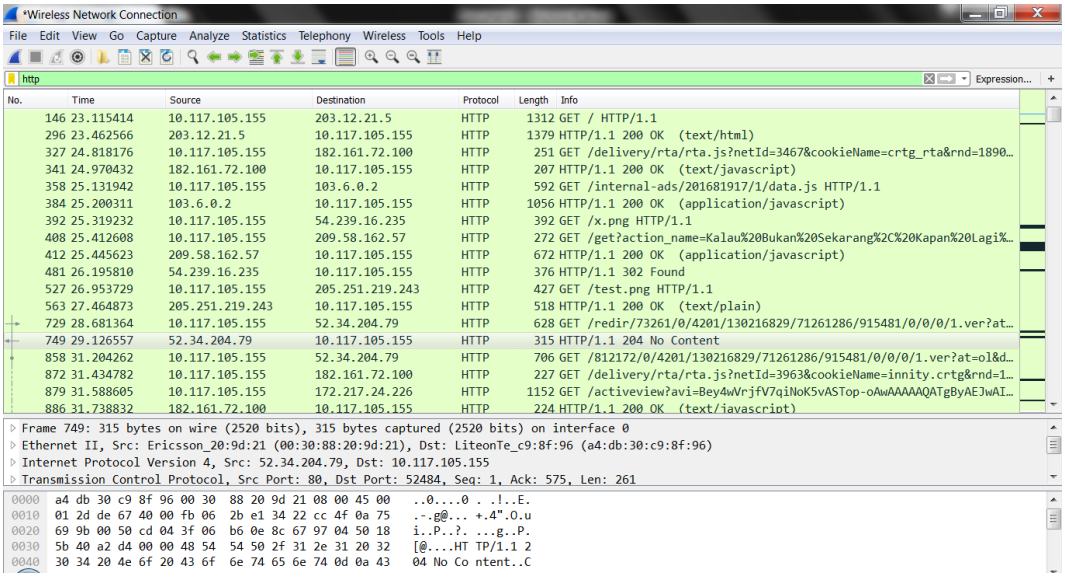
Berikut, saya menggunakan wireshark untuk menganalisa TCP/IP Port pada website kapanlagi.com. Setelah memilih network adapter yang akan digunakan untuk monitoring packet maka kita akan mendapatkan paket jaringan seperti ini.

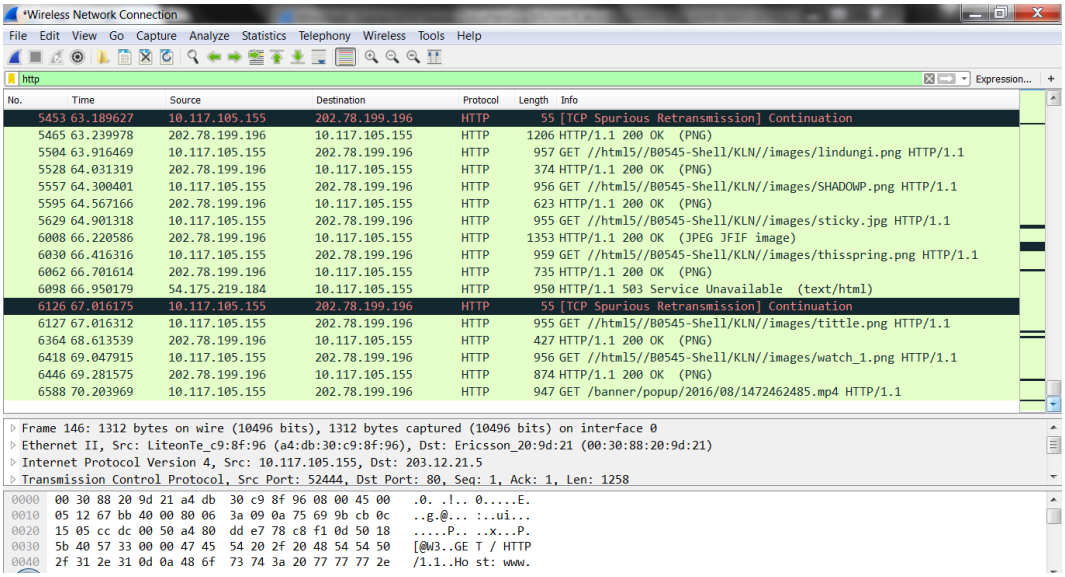
Selanjutnya di capture yg akan menampilkan bentuk traffic yg warna-warni di mana terdapat keterangan seperti :

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).

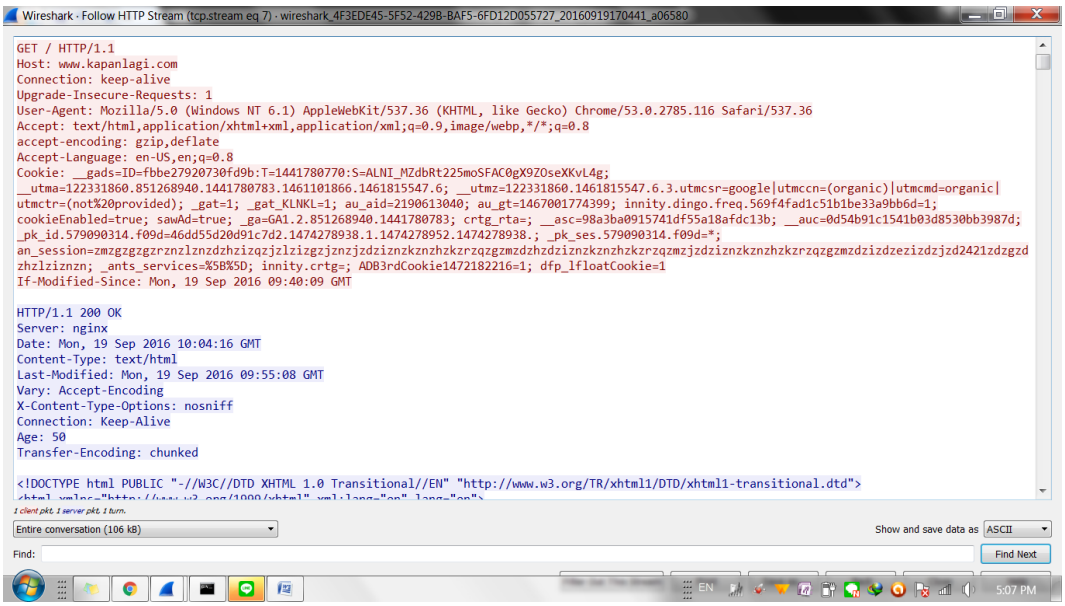


Menampilkan “GET” untuk http terhadap host www.kapanlagi.com caranya dengan memfilter http.host www.kapanlagi.com

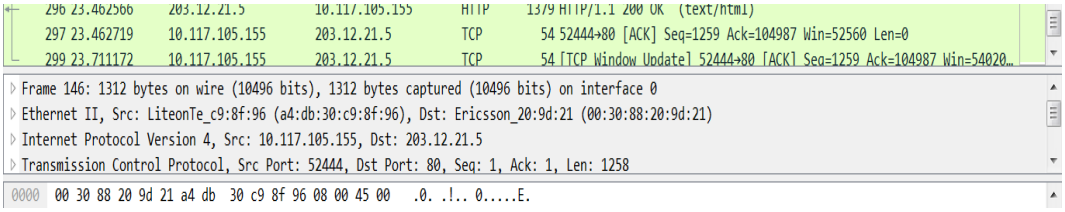


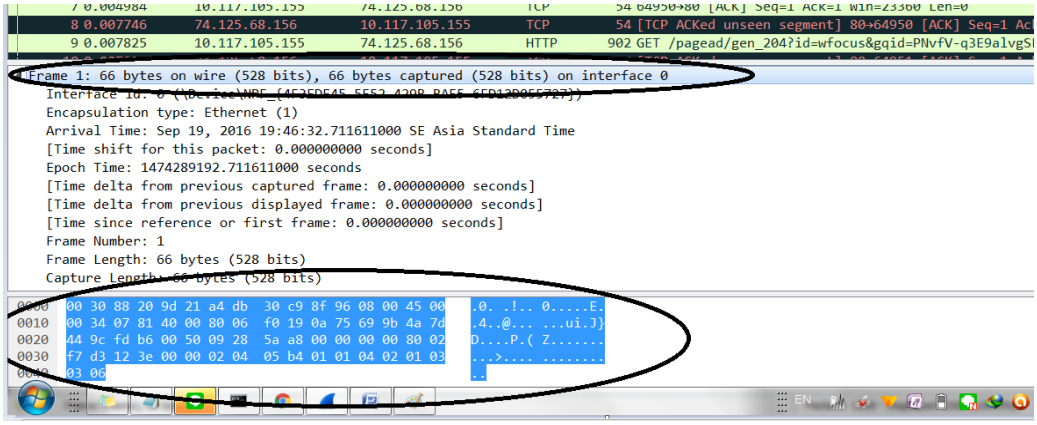


Dan hasil http Stream yang saya ikuti sebagai berikut

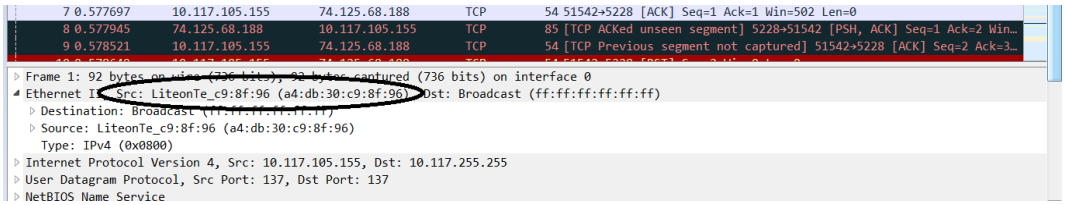


Capture di bawah merupakan IP dan port number TCP yang digunakan oleh client dan server

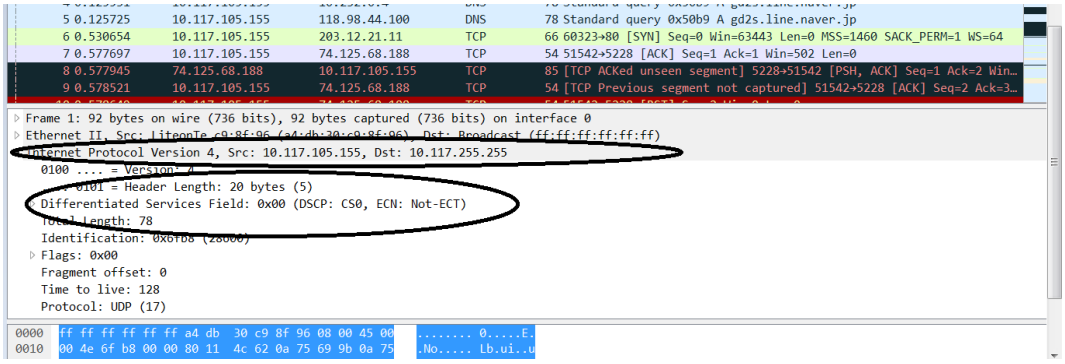




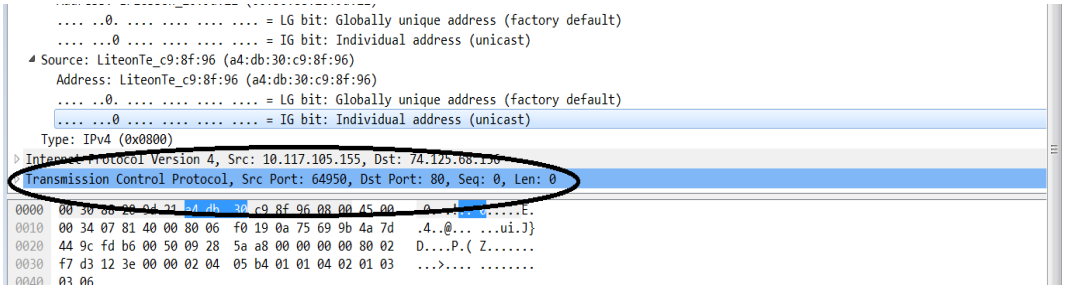
Pada gambar diatas merupaka ringkasan dari paket data. Untuk baris yang lainnya menunjukkan data link layer, network layer , dan transport layer . Pada dasarnya paket data yang telah dicapture terbungkus didalam frame sepeti gambar diatas.



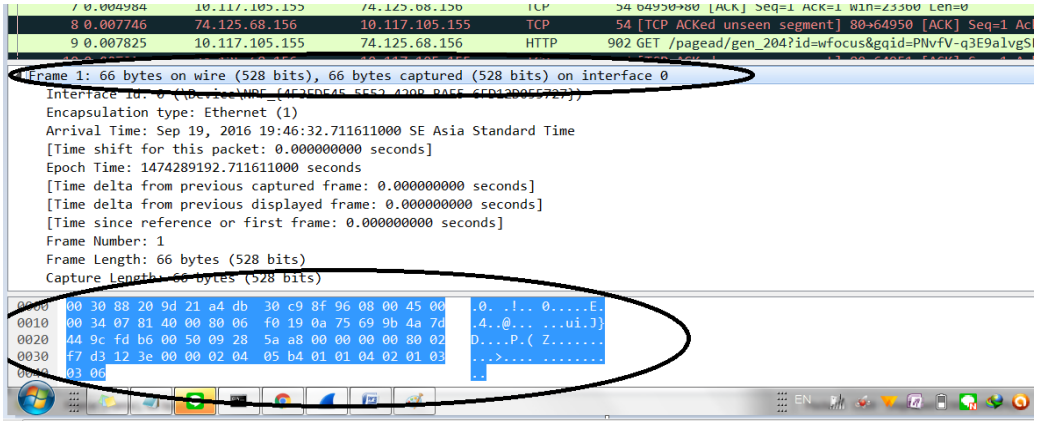
Pada gambar diatas menunjukan alamat tujuan dan alamat asalnya dalam bentuk mac address.



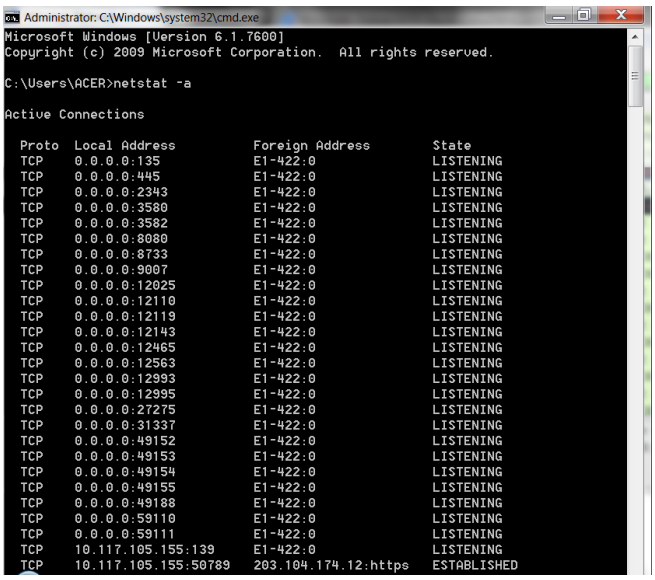
Pada gambar diatas menunjukan alamat tujuan dan alamat asal dalam bentuk IP. Dari gambar diatas juga terlihat bahwa bytes Header 20 bytes

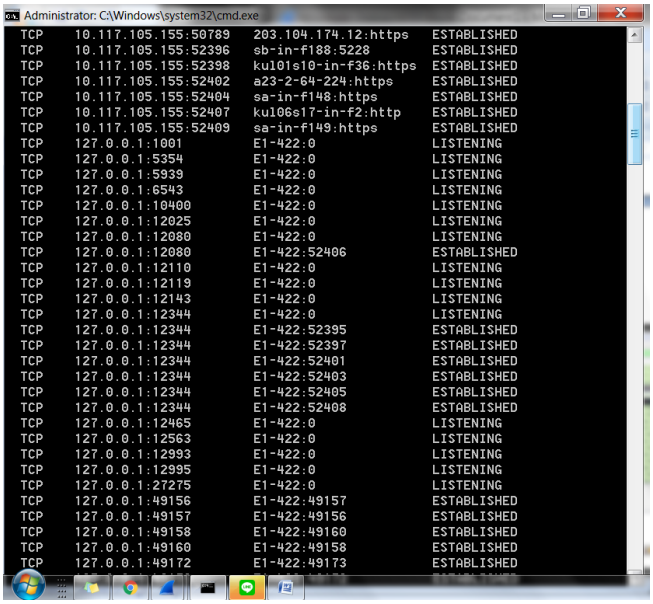


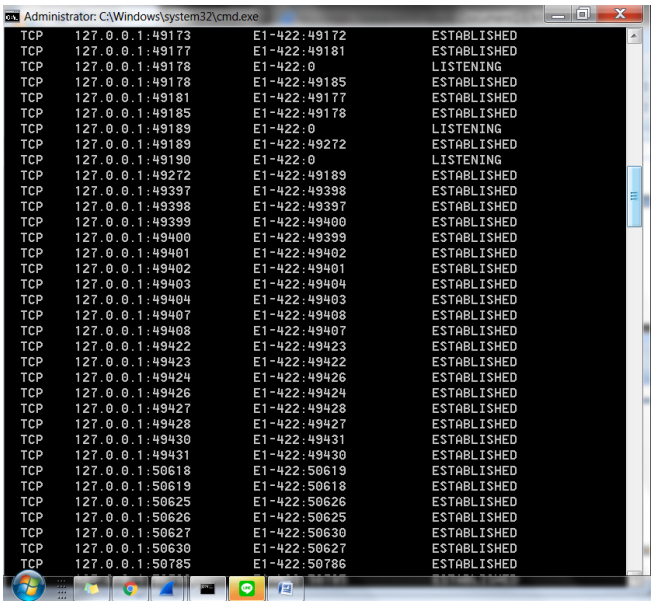
Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (64950) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

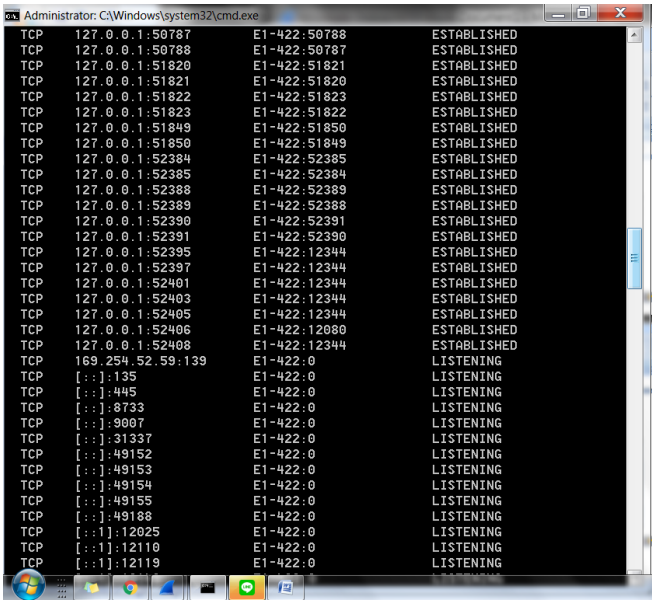


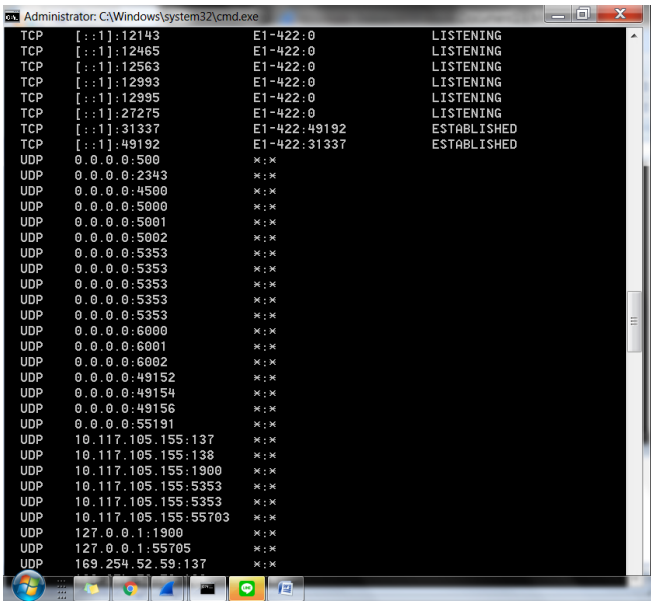
PENJELASAN CAPTURE PAKET DATA PADA COMMAND

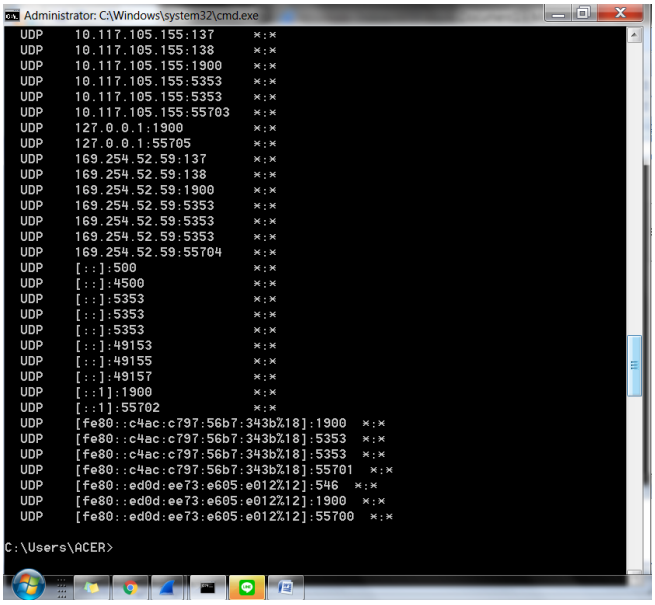



Administrator: C:\Windows\system32\cmd.exe
TCP 10.117.105.155:50789 203.104.174.12:https ESTABLISHED
TCP 10.117.105.155:52396 sb-in-f188:5228 ESTABLISHED
TCP 10.117.105.155:52398 ku101s10-in-f36:https ESTABLISHED
TCP 10.117.105.155:52402 a23-2-64-224:https ESTABLISHED
TCP 10.117.105.155:52404 sa-in-f148:https ESTABLISHED
TCP 10.117.105.155:52407 ku106s17-in-f2:http ESTABLISHED
TCP 10.117.105.155:52409 sa-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 127.0.0.1:49408 E1-422:49407 ESTABLISHED
TCP 127.0.0.1:49422 E1-422:49423 ESTABLISHED
TCP 127.0.0.1:49423 E1-422:49422 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
TCP 127.0.0.1:50787 E1-422:50788 ESTABLISHED
TCP 127.0.0.1:50788 E1-422:50787 ESTABLISHED
TCP 127.0.0.1:51820 E1-422:51821 ESTABLISHED
TCP 127.0.0.1:51821 E1-422:51820 ESTABLISHED
TCP 127.0.0.1:51822 E1-422:51823 ESTABLISHED
TCP 127.0.0.1:51823 E1-422:51822 ESTABLISHED
TCP 127.0.0.1:51849 E1-422:51850 ESTABLISHED
TCP 127.0.0.1:51850 E1-422:51849 ESTABLISHED
TCP 127.0.0.1:52384 E1-422:52385 ESTABLISHED
TCP 127.0.0.1:52385 E1-422:52384 ESTABLISHED
TCP 127.0.0.1:52388 E1-422:52389 ESTABLISHED
TCP 127.0.0.1:52389 E1-422:52388 ESTABLISHED
TCP 127.0.0.1:52390 E1-422:52391 ESTABLISHED
TCP 127.0.0.1:52391 E1-422:52390 ESTABLISHED
TCP 127.0.0.1:52395 E1-422:12344 ESTABLISHED
TCP 127.0.0.1:52397 E1-422:12344 ESTABLISHED
TCP 127.0.0.1:52401 E1-422:12344 ESTABLISHED
TCP 127.0.0.1:52403 E1-422:12344 ESTABLISHED
TCP 127.0.0.1:52405 E1-422:12344 ESTABLISHED
TCP 127.0.0.1:52406 E1-422:12080 ESTABLISHED
TCP 127.0.0.1:52408 E1-422:12344 ESTABLISHED
TCP 169.254.52.59:139 E1-422:0 LISTENING
TCP [::]:135 E1-422:0 LISTENING
TCP [::]:445 E1-422:0 LISTENING
TCP [::]:8733 E1-422:0 LISTENING
TCP [::]:9007 E1-422:0 LISTENING
TCP [::]:31337 E1-422:0 LISTENING
TCP [::]:49152 E1-422:0 LISTENING
TCP [::]:49153 E1-422:0 LISTENING
TCP [::]:49154 E1-422:0 LISTENING
TCP [::]:49155 E1-422:0 LISTENING
TCP [::]:49188 E1-422:0 LISTENING
TCP [::1]:12025 E1-422:0 LISTENING
TCP [::1]:12110 E1-422:0 LISTENING
TCP [::1]:12119 E1-422:0 LISTENING


Administrator: C:\Windows\system32\cmd.exe
TCP [::1]:12143 E1-422:0 LISTENING
TCP [::1]:12465 E1-422:0 LISTENING
TCP [::1]:12563 E1-422:0 LISTENING
TCP [::1]:12993 E1-422:0 LISTENING
TCP [::1]:12995 E1-422:0 LISTENING
TCP [::1]:27275 E1-422:0 LISTENING
TCP [::1]:31337 E1-422:49192 ESTABLISHED
TCP [::1]:49192 E1-422:31337 ESTABLISHED
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:2343 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5000 *:*
UDP 0.0.0.0:5001 *:*
UDP 0.0.0.0:5002 *:*
UDP 0.0.0.0:5353 *:*
UDP 0.0.0.0:5353 *:*
UDP 0.0.0.0:5353 *:*
UDP 0.0.0.0:5353 *:*
UDP 0.0.0.0:5353 *:*
UDP 0.0.0.0:6000 *:*
UDP 0.0.0.0:6001 *:*
UDP 0.0.0.0:6002 *:*
UDP 0.0.0.0:49152 *:*
UDP 0.0.0.0:49154 *:*
UDP 0.0.0.0:49156 *:*
UDP 0.0.0.0:55191 *:*
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 *:*



Keterangan output netstat:

1. **Proto**. Kolom proto menunjukan 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 menunjukan koneksi yang dituju oleh local address beserta nomor port tujuannya.
4. **State**. Kolom ini menunjukan 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.