Task V

Jaringan Komputer

Disusun Oleh :

Nama : Sigit Wijaya Pramono

Nim : 09011181419012

Kelas : SK.5A

Dosen Pengampuh : Dr. Deris Stiawan, M.T.

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

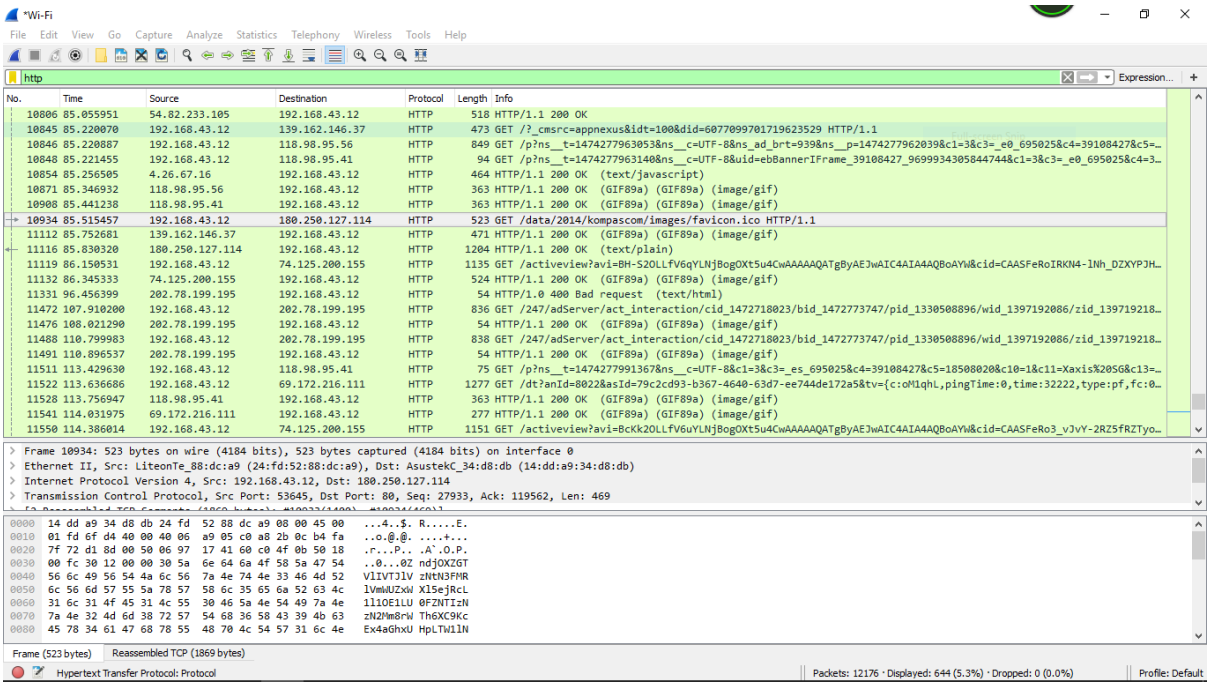
UNIVERSITAS SRIWIJAYA

2016

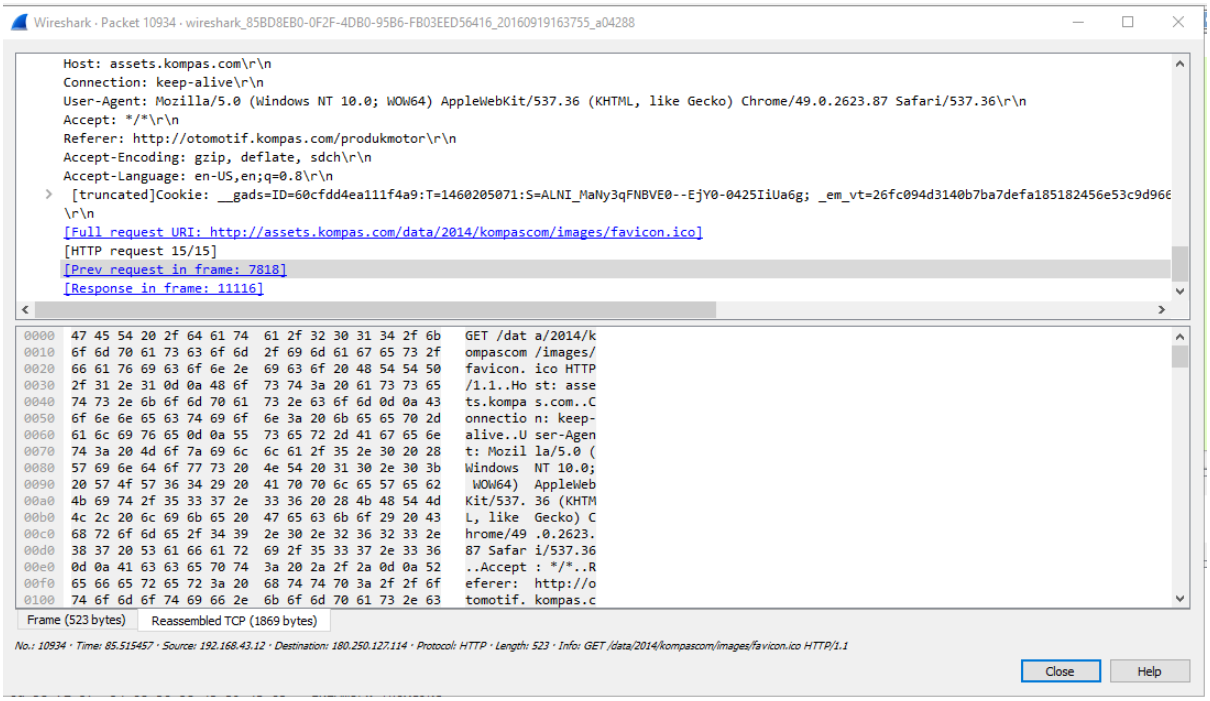
Capturing dan Analisa Protokol Jaringan Menggunakan Wireshark dan CMD

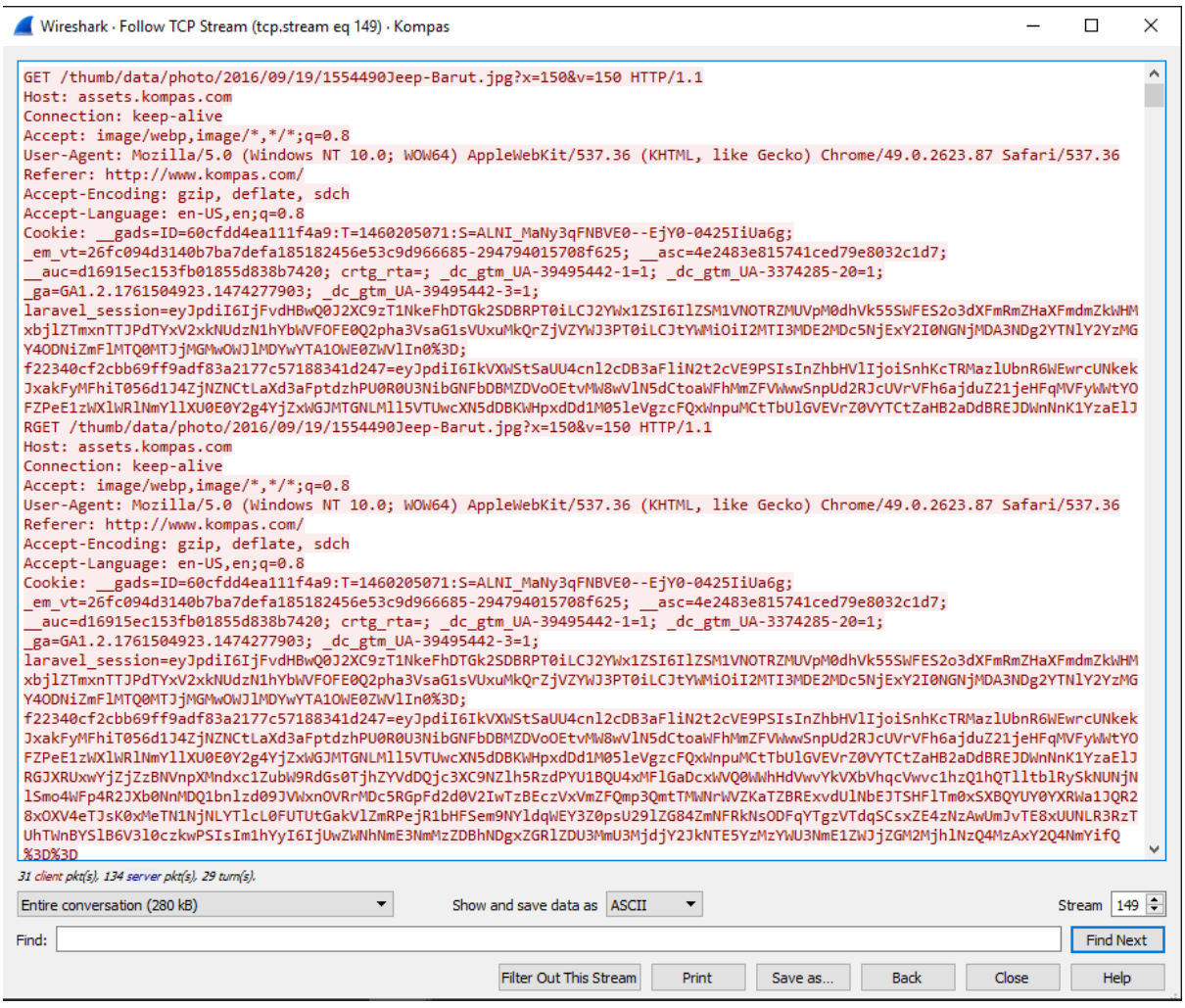
Pada tugas kali ini yaitu mengcapture traffic atau paket-paket data pada suatu jaringan yang menggunakan software wireshark, setelah mengcapture terdapat banyak sekali IP - IP dan protokol muncul dalam software wireshark. Setelah memulai mengcapture kita membuka browser dan browsing suatu website dengan tujuan agar tercapture oleh aplikasi wireshark dan untuk selanjutnya akan dianalisa lalu dibangingkan dengan hasil capture menggunakan cmd. Selain menggunakan wireshark, capturing juga menggunakan cmd dengan command netstat –a.

Dibawah berikut merupakan screenshoot dari hasil capturing menggunakan aplikasi wireshark dengan destisani web kompas.com :



Terlihat dari gambar diatas beberapa dari hasil capture traffic / paket-paket data yang termasuk dalam satu jaringan tersebut. Selanjutnya ini merupakan capture dari *GET* yang terdapat dalam salah satu IP pada hasil capture di wireshark yang mana IP tersebut sama seperti web yang saya cari dalam broser :

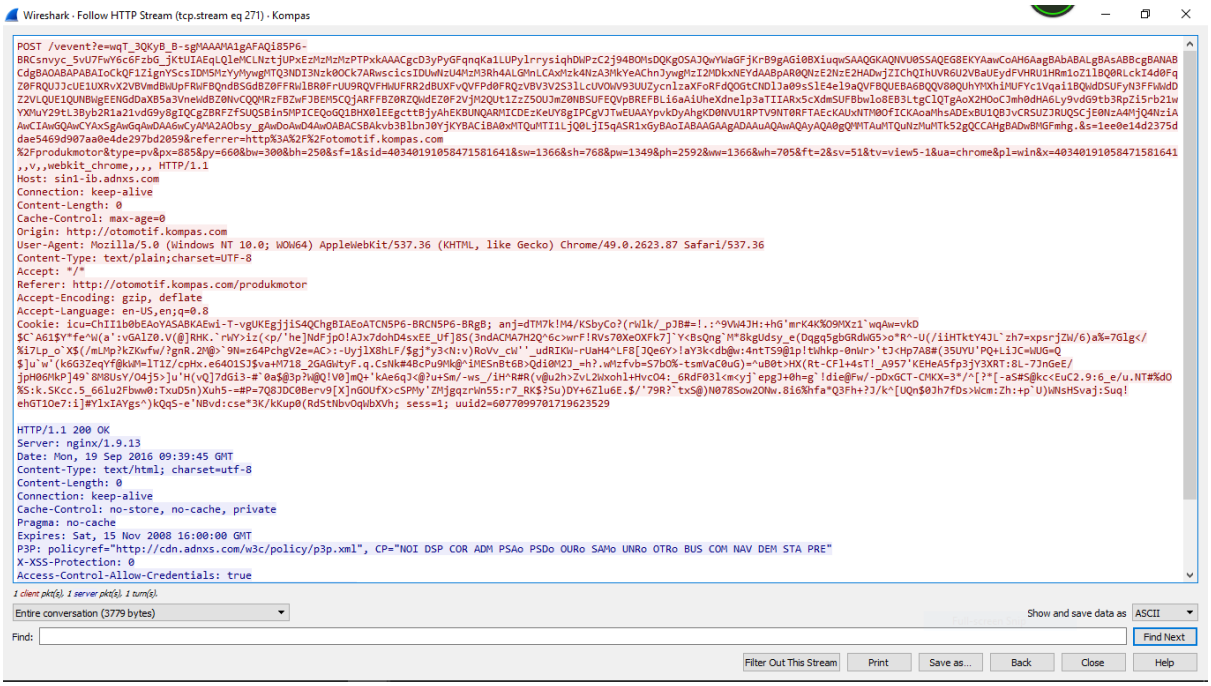




Dua gambar diatas memperlihatkan *GET* pada salah satu protokol dalam jaringan tersebut, disana tergambar ada beberapa diantaranya yang menuliskan *full request url* dengan

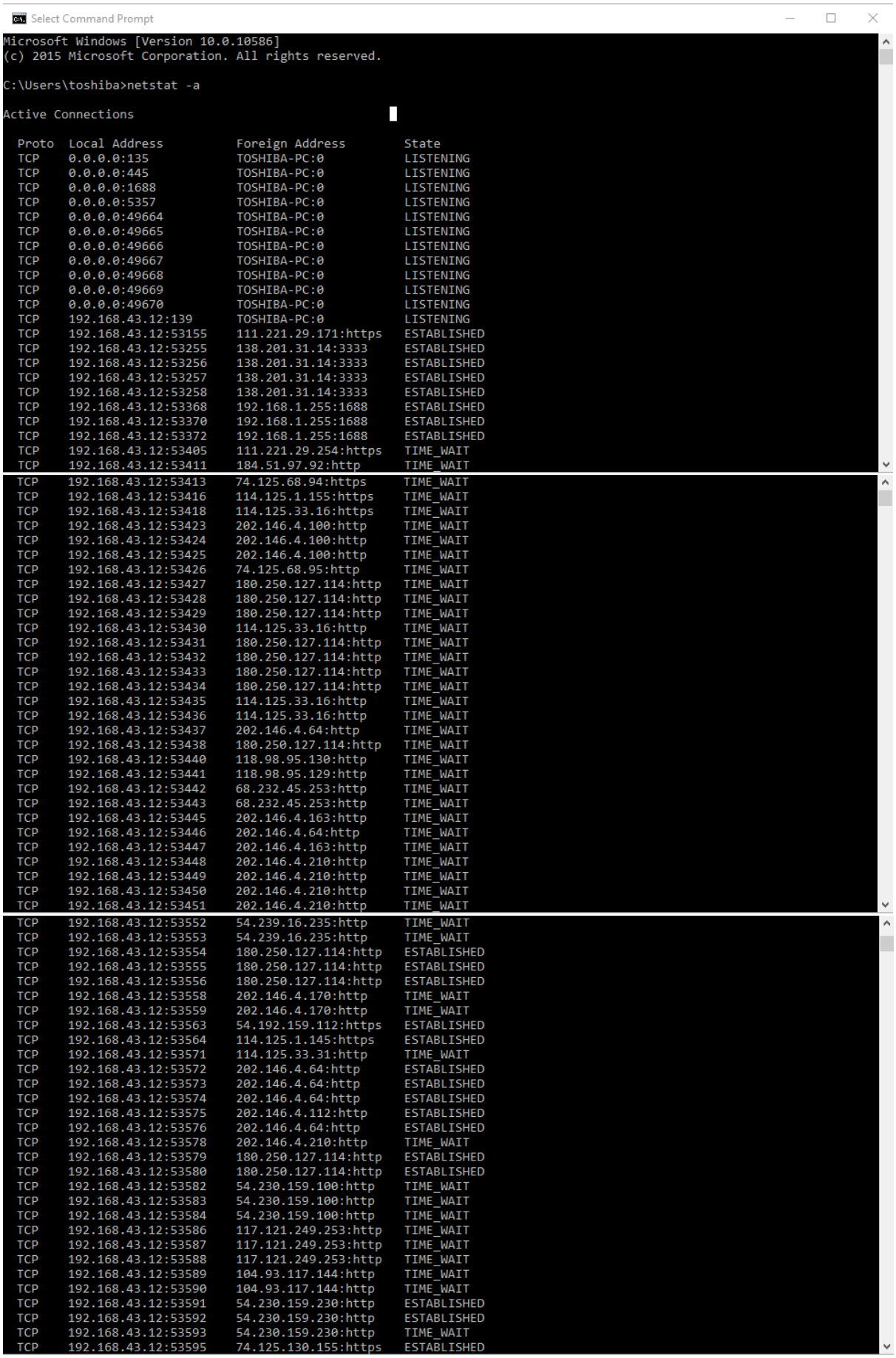
menyebutkan website yang saya buka. Sebuah permintaan *GET* mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan

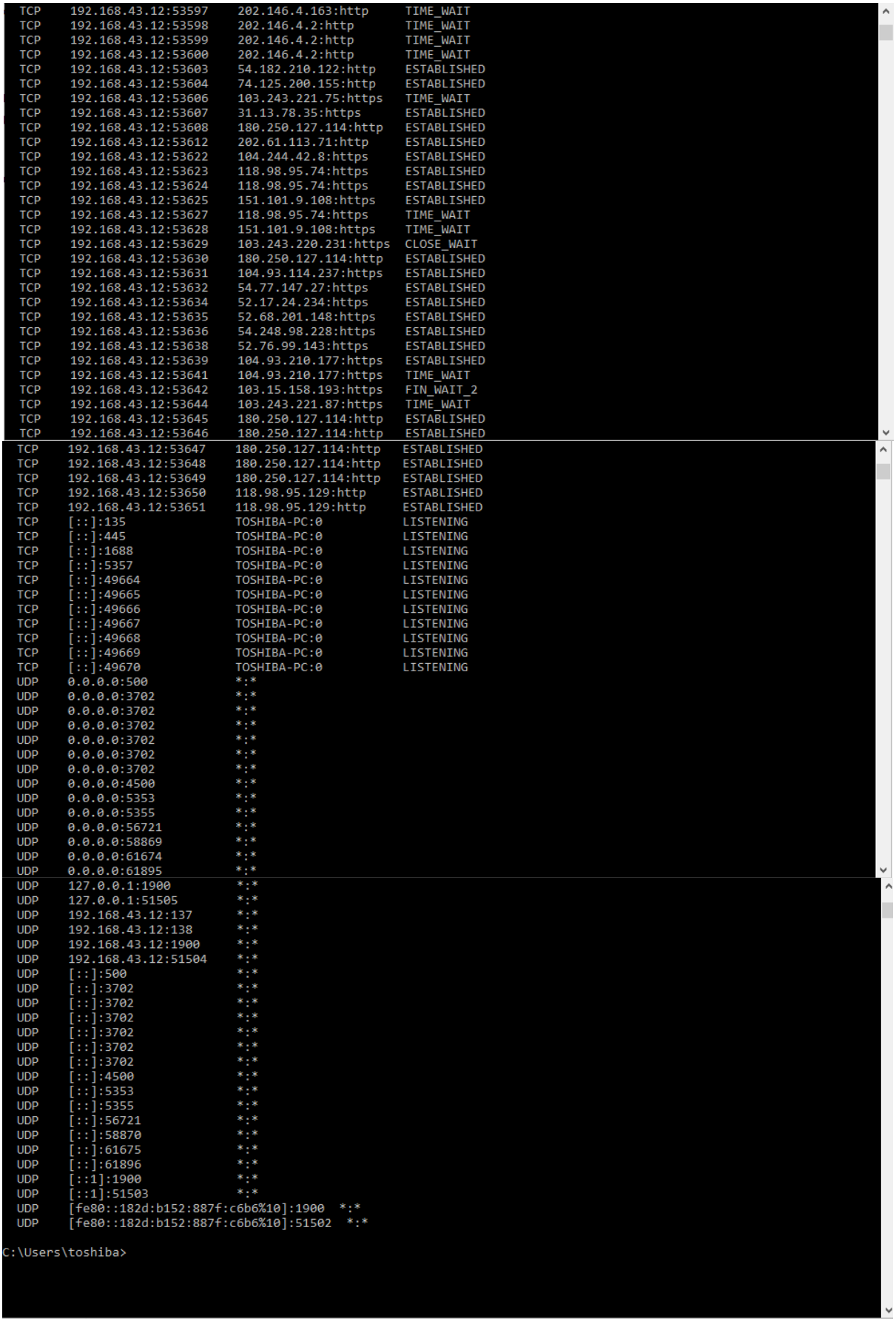
Gambar selanjutnya merupakan capture dari *POST* pada salah satu IP yang tercapture pada wireshark yamg menunjukkan web yang saya tuju :



Seperti yang telihat dalam gambar diatas yang menggambarkan isi *POST* dari IP yang masih berhubungan dengan web dengan protokol *http*. Sebuah permintaan *HTTP POST* memanfaatkan badan pesan untuk mengirim data ke server web.

Setelah beberapa gambar diatas yang menjelaskan sedikit proses dari capturing pada wireshark dan beberapa juga penjelasan tentang *post* dan *get* yang terdapat dalam capturing, selanjutnya ada proses capturing jaringan menggunakan cmd dan menggunakan command *netstat –a* yang bersamaan dengan capturing menggunakan wireshark. Berikut merupajan capture gambar hasil menggunakan cmd :


Select Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\toshiba>netstat -a
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:445 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:1688 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:5357 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49664 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49665 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49666 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49667 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49668 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49669 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49670 TOSHIBA-PC:0 LISTENING
TCP 192.168.43.12:139 TOSHIBA-PC:0 LISTENING
TCP 192.168.43.12:53155 111.221.29.171:https ESTABLISHED
TCP 192.168.43.12:53255 138.201.31.14:3333 ESTABLISHED
TCP 192.168.43.12:53256 138.201.31.14:3333 ESTABLISHED
TCP 192.168.43.12:53257 138.201.31.14:3333 ESTABLISHED
TCP 192.168.43.12:53258 138.201.31.14:3333 ESTABLISHED
TCP 192.168.43.12:53368 192.168.1.255:1688 ESTABLISHED
TCP 192.168.43.12:53370 192.168.1.255:1688 ESTABLISHED
TCP 192.168.43.12:53372 192.168.1.255:1688 ESTABLISHED
TCP 192.168.43.12:53405 111.221.29.254:https TIME_WAIT
TCP 192.168.43.12:53411 184.51.97.92:http TIME_WAIT
TCP 192.168.43.12:53413 74.125.68.94:https TIME_WAIT
TCP 192.168.43.12:53416 114.125.1.155:https TIME_WAIT
TCP 192.168.43.12:53418 114.125.33.16:https TIME_WAIT
TCP 192.168.43.12:53423 202.146.4.100:http TIME_WAIT
TCP 192.168.43.12:53424 202.146.4.100:http TIME_WAIT
TCP 192.168.43.12:53425 202.146.4.100:http TIME_WAIT
TCP 192.168.43.12:53426 74.125.68.95:http TIME_WAIT
TCP 192.168.43.12:53427 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53428 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53429 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53430 114.125.33.16:http TIME_WAIT
TCP 192.168.43.12:53431 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53432 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53433 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53434 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53435 114.125.33.16:http TIME_WAIT
TCP 192.168.43.12:53436 114.125.33.16:http TIME_WAIT
TCP 192.168.43.12:53437 202.146.4.64:http TIME_WAIT
TCP 192.168.43.12:53438 180.250.127.114:http TIME_WAIT
TCP 192.168.43.12:53440 118.98.95.130:http TIME_WAIT
TCP 192.168.43.12:53441 118.98.95.129:http TIME_WAIT
TCP 192.168.43.12:53442 68.232.45.253:http TIME_WAIT
TCP 192.168.43.12:53443 68.232.45.253:http TIME_WAIT
TCP 192.168.43.12:53445 202.146.4.163:http TIME_WAIT
TCP 192.168.43.12:53446 202.146.4.64:http TIME_WAIT
TCP 192.168.43.12:53447 202.146.4.163:http TIME_WAIT
TCP 192.168.43.12:53448 202.146.4.210:http TIME_WAIT
TCP 192.168.43.12:53449 202.146.4.210:http TIME_WAIT
TCP 192.168.43.12:53450 202.146.4.210:http TIME_WAIT
TCP 192.168.43.12:53451 202.146.4.210:http TIME_WAIT
TCP 192.168.43.12:53552 54.239.16.235:http TIME_WAIT
TCP 192.168.43.12:53553 54.239.16.235:http TIME_WAIT
TCP 192.168.43.12:53554 180.250.127.114:http ESTABLISHED
TCP 192.168.43.12:53555 180.250.127.114:http ESTABLISHED
TCP 192.168.43.12:53556 180.250.127.114:http ESTABLISHED
TCP 192.168.43.12:53558 202.146.4.170:http TIME_WAIT
TCP 192.168.43.12:53559 202.146.4.170:http TIME_WAIT
TCP 192.168.43.12:53563 54.192.159.112:https ESTABLISHED
TCP 192.168.43.12:53564 114.125.1.145:https ESTABLISHED
TCP 192.168.43.12:53571 114.125.33.31:http TIME_WAIT
TCP 192.168.43.12:53572 202.146.4.64:http ESTABLISHED
TCP 192.168.43.12:53573 202.146.4.64:http ESTABLISHED
TCP 192.168.43.12:53574 202.146.4.64:http ESTABLISHED
TCP 192.168.43.12:53575 202.146.4.112:http ESTABLISHED
TCP 192.168.43.12:53576 202.146.4.64:http ESTABLISHED
TCP 192.168.43.12:53578 202.146.4.210:http TIME_WAIT
TCP 192.168.43.12:53579 180.250.127.114:http ESTABLISHED
TCP 192.168.43.12:53580 180.250.127.114:http ESTABLISHED
TCP 192.168.43.12:53582 54.230.159.100:http TIME_WAIT
TCP 192.168.43.12:53583 54.230.159.100:http TIME_WAIT
TCP 192.168.43.12:53584 54.230.159.100:http TIME_WAIT
TCP 192.168.43.12:53586 117.121.249.253:http TIME_WAIT
TCP 192.168.43.12:53587 117.121.249.253:http TIME_WAIT
TCP 192.168.43.12:53588 117.121.249.253:http TIME_WAIT
TCP 192.168.43.12:53589 104.93.117.144:http TIME_WAIT
TCP 192.168.43.12:53590 104.93.117.144:http TIME_WAIT
TCP 192.168.43.12:53591 54.230.159.230:http ESTABLISHED
TCP 192.168.43.12:53592 54.230.159.230:http ESTABLISHED
TCP 192.168.43.12:53593 54.230.159.230:http TIME_WAIT
TCP 192.168.43.12:53595 74.125.130.155:https ESTABLISHED



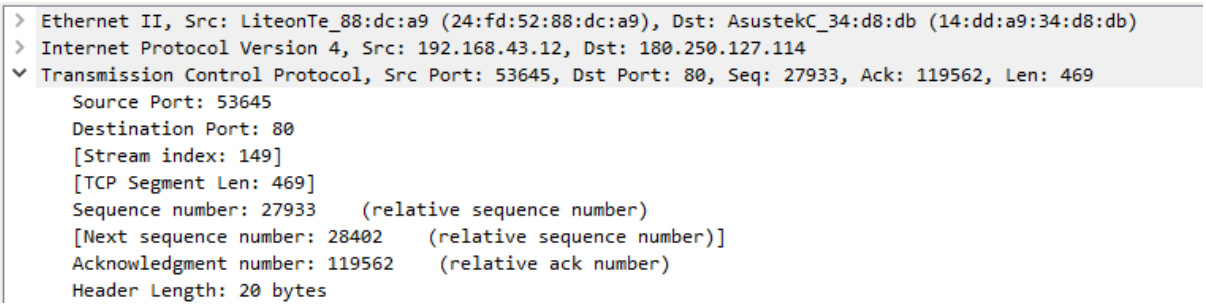
```
  TCP    192.168.43.12:53597    202.146.4.163:http     TIME_WAIT
  TCP    192.168.43.12:53598    202.146.4.2:http       TIME_WAIT
  TCP    192.168.43.12:53599    202.146.4.2:http       TIME_WAIT
  TCP    192.168.43.12:53600    202.146.4.2:http       TIME_WAIT
  TCP    192.168.43.12:53603    54.182.210.122:http    ESTABLISHED
  TCP    192.168.43.12:53604    74.125.200.155:http    ESTABLISHED
  TCP    192.168.43.12:53606    103.243.221.75:https   TIME_WAIT
  TCP    192.168.43.12:53607    31.13.78.35:https      ESTABLISHED
  TCP    192.168.43.12:53608    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53612    202.61.113.71:http     ESTABLISHED
  TCP    192.168.43.12:53622    104.244.42.8:https     ESTABLISHED
  TCP    192.168.43.12:53623    118.98.95.74:https     ESTABLISHED
  TCP    192.168.43.12:53624    118.98.95.74:https     ESTABLISHED
  TCP    192.168.43.12:53625    151.101.9.108:https    ESTABLISHED
  TCP    192.168.43.12:53627    118.98.95.74:https     TIME_WAIT
  TCP    192.168.43.12:53628    151.101.9.108:https    TIME_WAIT
  TCP    192.168.43.12:53629    103.243.220.231:https  CLOSE_WAIT
  TCP    192.168.43.12:53630    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53631    104.93.114.237:https   ESTABLISHED
  TCP    192.168.43.12:53632    54.77.147.27:https     ESTABLISHED
  TCP    192.168.43.12:53634    52.17.24.234:https     ESTABLISHED
  TCP    192.168.43.12:53635    52.68.201.148:https    ESTABLISHED
  TCP    192.168.43.12:53636    54.248.98.228:https    ESTABLISHED
  TCP    192.168.43.12:53638    52.76.99.143:https     ESTABLISHED
  TCP    192.168.43.12:53639    104.93.210.177:https   ESTABLISHED
  TCP    192.168.43.12:53641    104.93.210.177:https   TIME_WAIT
  TCP    192.168.43.12:53642    103.15.158.193:https   FIN_WAIT_2
  TCP    192.168.43.12:53644    103.243.221.87:https   TIME_WAIT
  TCP    192.168.43.12:53645    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53646    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53647    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53648    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53649    180.250.127.114:http   ESTABLISHED
  TCP    192.168.43.12:53650    118.98.95.129:http     ESTABLISHED
  TCP    192.168.43.12:53651    118.98.95.129:http     ESTABLISHED
  TCP    [::]:135               TOSHIBA-PC:0           LISTENING
  TCP    [::]:445               TOSHIBA-PC:0           LISTENING
  TCP    [::]:1688              TOSHIBA-PC:0           LISTENING
  TCP    [::]:5357              TOSHIBA-PC:0           LISTENING
  TCP    [::]:49664             TOSHIBA-PC:0           LISTENING
  TCP    [::]:49665             TOSHIBA-PC:0           LISTENING
  TCP    [::]:49666             TOSHIBA-PC:0           LISTENING
  TCP    [::]:49667             TOSHIBA-PC:0           LISTENING
  TCP    [::]:49668             TOSHIBA-PC:0           LISTENING
  TCP    [::]:49669             TOSHIBA-PC:0           LISTENING
  TCP    [::]:49670             TOSHIBA-PC:0           LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:56721          *:*
  UDP    0.0.0.0:58869          *:*
  UDP    0.0.0.0:61674          *:*
  UDP    0.0.0.0:61895          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:51505        *:*
  UDP    192.168.43.12:137      *:*
  UDP    192.168.43.12:138      *:*
  UDP    192.168.43.12:1900     *:*
  UDP    192.168.43.12:51504    *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:56721             *:*
  UDP    [::]:58870             *:*
  UDP    [::]:61675             *:*
  UDP    [::]:61896             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:51503            *:*
  UDP    [fe80::182d:b152:887f:c6b6%10]:1900  *:*
  UDP    [fe80::182d:b152:887f:c6b6%10]:51502  *:*

C:\Users\toshiba>
```

Gambar diatas merupakan hasil dari capturing jaringan melalui cmd dengan command

netstat –a yang prosesnya bersamaan dengan capturing menggunakan wireshark. Pada gambar diatas terdapat beberapa protokol yang berbeda, ada TCP dan ada juga UDP. Transmission Control Protocol (TCP) adalah salah satu jenis protokol yang memungkinkan kumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu network (jaringan). TCP merupakan suatu protokol yang berada di lapisan transpor (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (connection-oriented) dan dapat diandalkan (reliable). Lalu ada UDP, UDP singkatan dari User Datagram Protocol, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP.

Port IP :

Dari beberapa IP yang saya cek disitu menjelaskan bahwa Destination Port terdapat pada port 80, seperti yang di gambarkan oleh capture dibawah ini :



Dari gambar diatas saya menggunakan IP yang saya ambil untuk melihat *get* sebelumnya, disana di tuliskan Source Port : 53645 dan Destination Port : 80. Setelah saya melihat beberapa IP dengan protokol http Get lain juga menerangkan bahwa destination port juga dituliskan 80.