TUGAS JARINGAN KOMPUTER

Nama	:	Yonatan Riyadhi
NIM	:	09011181419009
Kelas	:	SK 5A
Nama Dosen	:	Dr. Deris Stiawan M.T

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

CAPTURE DAN ANALISIS PROTOKOL JARINGAN DENGAN WIRESHARK

HTTP (HyperText Transfer Protocol) adalah protocol pada layer aplikasi baik TCP/IP maupun OSI yang digunakan untuk mengakses web pages dari suatu website. Secara spesifik dalam penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan yang disebut hiperteks, yang kemudian membentuk WWW (Word Wide Web). Sebuah client HTTP seperti web browser, biasanya memulai permintaan dengan membuat hubungan ke port tertentu di suatu webhosting (biasanya port 80). Sebuah server HTTP yang mendengarkan di port tersebut menunggu client mengirim kode permintaan (request) yang akan meminta halaman yang sudah ditentukan, diikuti dengan pesan MIME yang memiliki beberapa informasi kode kepala yang menjelaskan aspek dari permintaan tersebut, diikut dengan badan dari data tertentu. Data yang diambil dari server tersebut dapat berupa teks HTML (HyperText Markup Language), PHP script, CSS, resource-nya, dan lain lain.

Hingga kini, ada dua versi mayor dari protokol HTTP, yakni HTTP/1.0 yang menggunakan koneksi terpisah untuk setiap dokumen, dan HTTP/1.1 yang dapat menggunakan koneksi yang sama untuk melakukan transaksi. Dengan demikian, HTTP/1.1 bisa lebih cepat karena memang tidak perlu membuang waktu untuk pembuatan koneksi berulang-ulang.

DNS (Domain Name System) adalah protocol yang digunakan untuk mentranslate hostname ke IP address dan sebaliknya. Karena di dunia manusia ini, lebih susah menghafalkan IP dibanding dengan deretan tulisan yang membentuk nama host. Untuk itu aplikasi ini ada, yang berjalan di protocol aplikasi. Dalam server DNS ada database (IP ßà hosname) yang saling terdistribusi. Sebagai analogi ketika kita mengakseswww.google.com maka oleh server DNS akan ditranslate ke IP dari server google itu sendiri. Kenapa ditranslate ke IP? Jawabanya adalah perangkat jaringan lain seperti router, switch tidak memahami hostname, yang berarti pernyataan kebalikan dali pernyataan pertama. DNS juga bekerja pada layer aplikasi

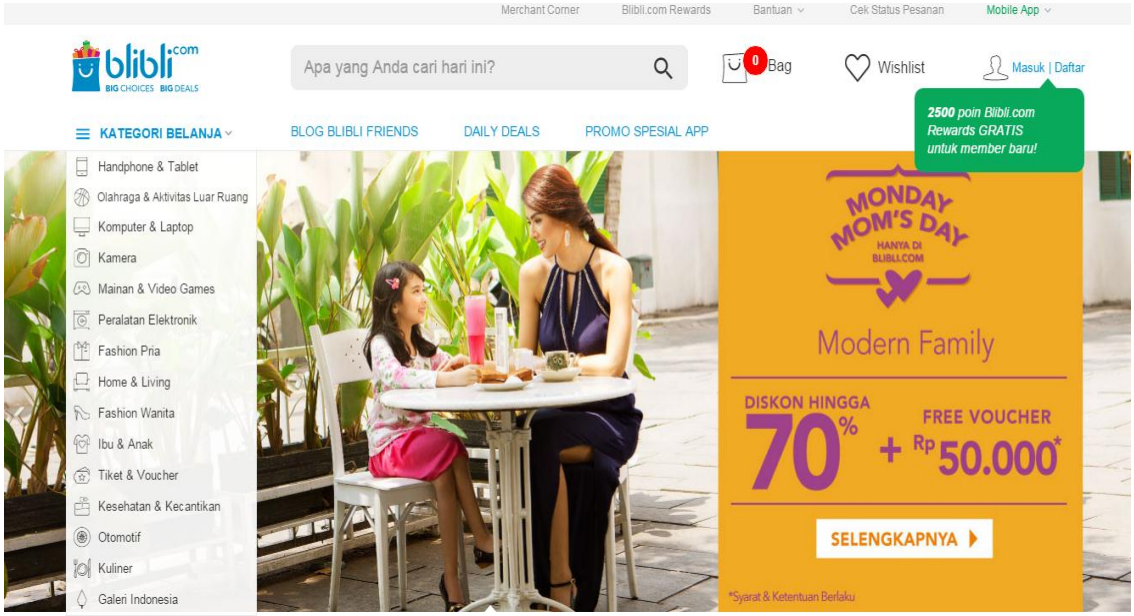
Capture Packet

Wireshark akan menampilkan semua informasi tentang packet yang keluar dan masuk dalam interface yang telah dipilih. Beberapa tampilan hasil capture Wireshark meliputi Frame, Ethernet, Internet rotokol, User-Datagram Protokol, Link-local Multicast Name Resolution.

1. Buka web browser

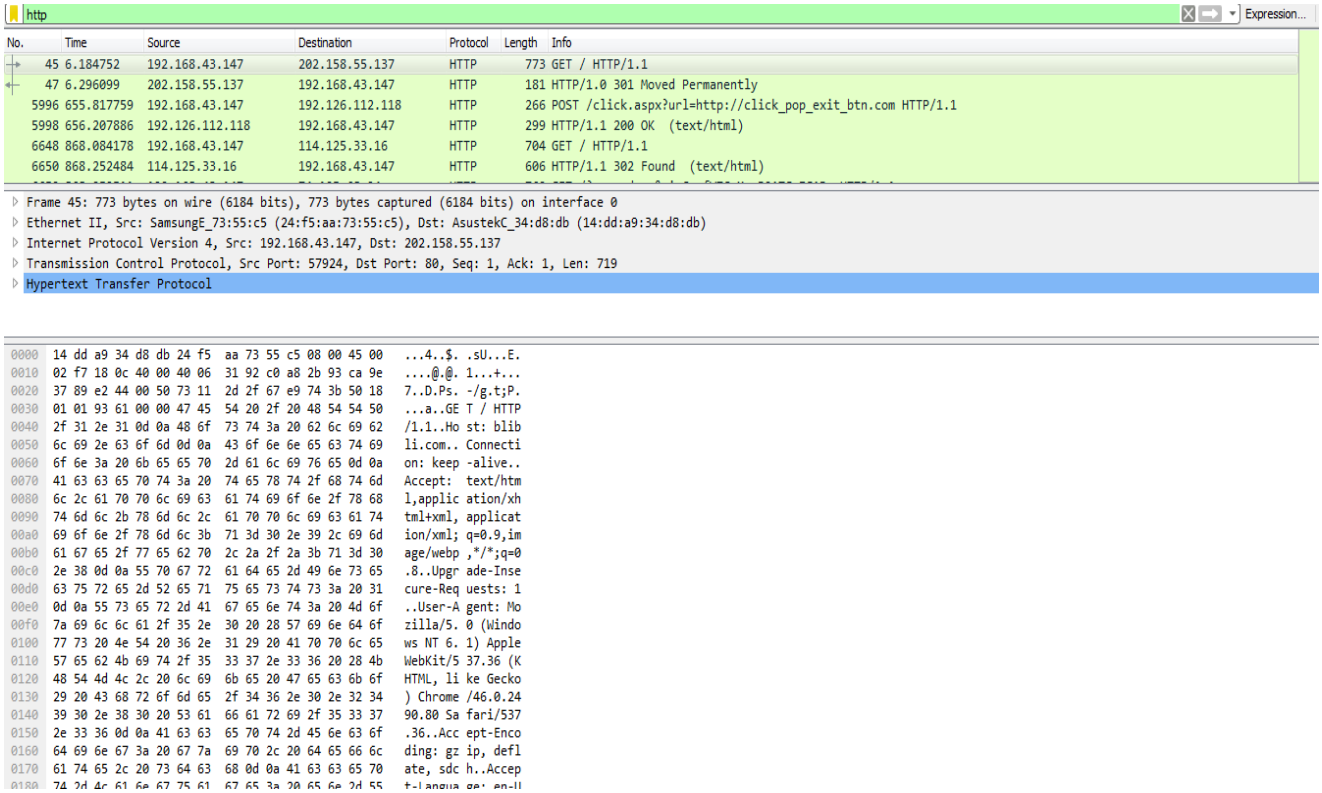
2. Buka wireshark kemudian pilih interface yang akan dicapture, klik start.

3. Pada browser saya memilih blibli.com



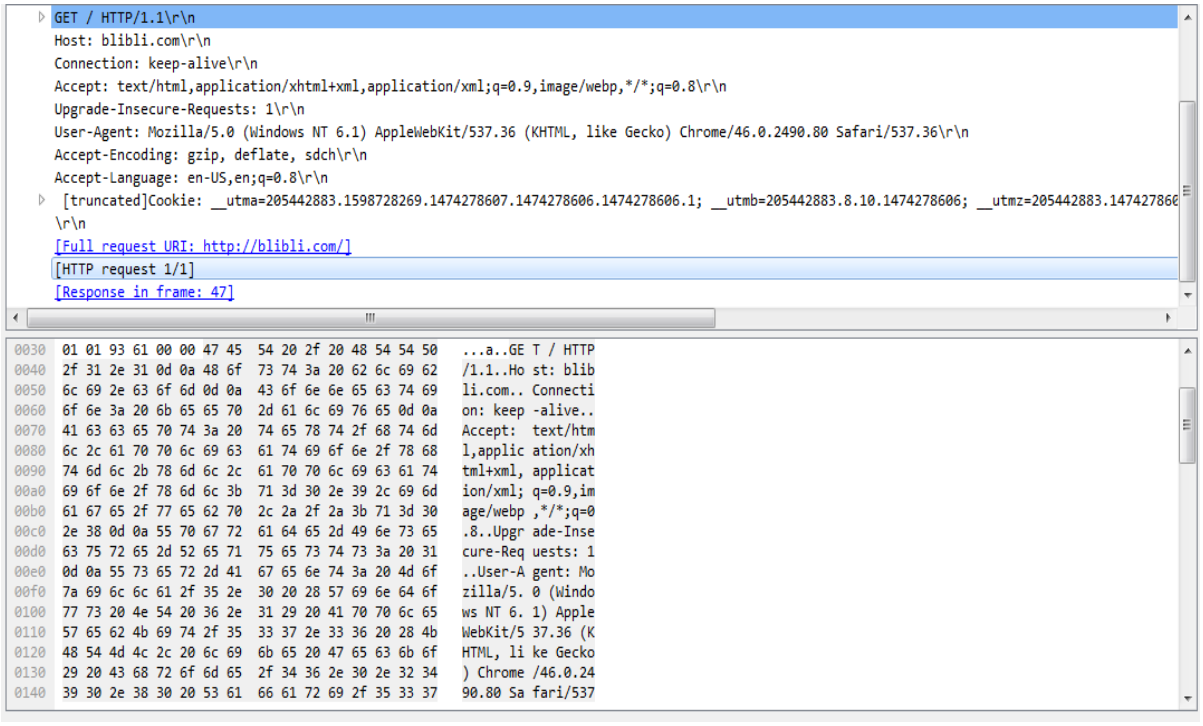
4. Setelah Web browser selesai meload Page dari situs blibli.com, pada wireshrark lakukan stop capture (menu Capture >> Stop) maka langsung tertampil paket-paket data yang tertangkap selama meload situs blibli.com.

5. Karena yang akan kita analisis adalah protokol HTTP maka buatlah filter “http” pada menu filter.



Ini adalah gambar pada saat tampilan paket pada blibli.com

Metode Get adalah metode pengiriman data menggunakan query string, jadi seluruh nilai pada form akan di kirim ke sisi server/file dan nilai dari form anda akan tampil pada barus URL/ Address bar

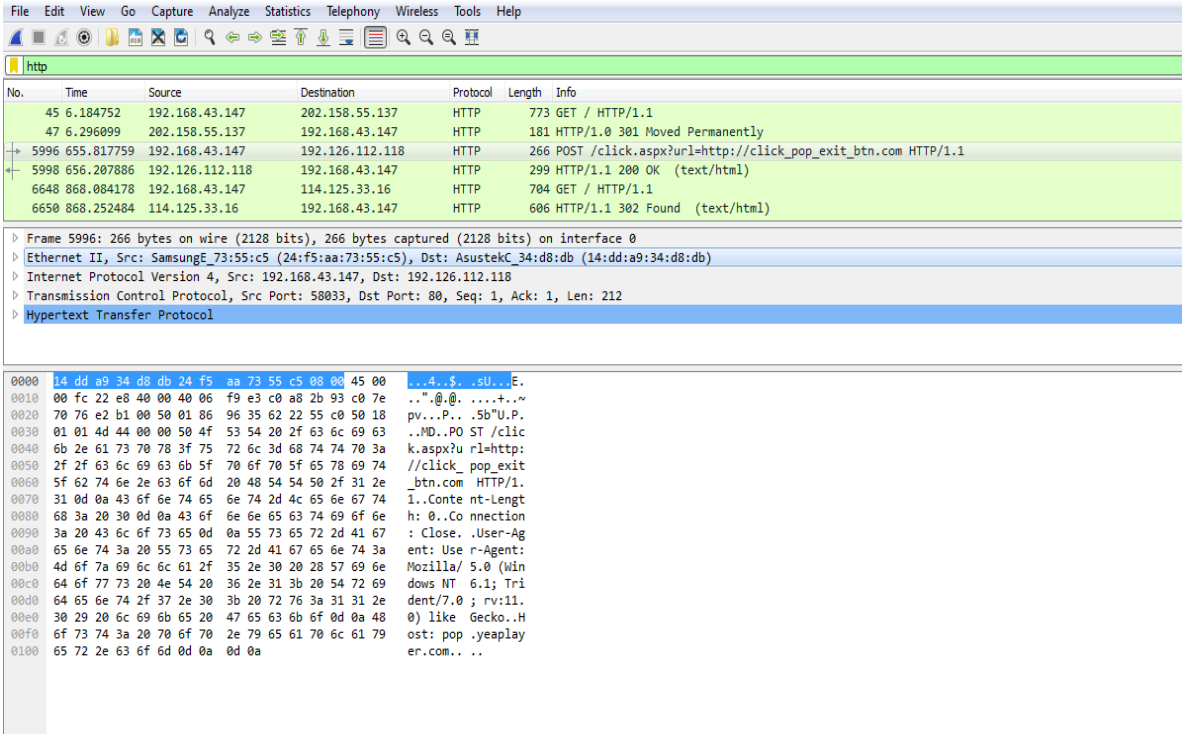


```
GET / HTTP/1.1
Host: blibli.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: __utma=205442883.1598728269.1474278607.1474278606.1474278606.1; __utmb=205442883.8.10.1474278606;
__utmz=205442883.1474278606.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
rr_rcs=eF5j4cotK8lMETA0MjDVNdQ1ZClN9kgxskg1tTAw07U0M0jWNUkyNdVNNDQz000yMDVNMTA3SUkyNQEAiBkNzw; _vz=viz_57dfb4d76ee9f;
_ga=GA1.2.1598728269.1474278607; _gat_UA-21718848-13=1

HTTP/1.0 301 Moved Permanently
Location: https://www.blibli.com/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

Pada gambar diatas merupakan gambar dari metode GET pada situs blibli.com

Metode Post adalah metode pengiriman yang tidak akan terlihat oleh user yang mengakases, dikarenakan informasi yang dikirim akan tidak ditampilkan di Address Bar Web Browser. Selain $_POST juga tidak memiliki batasan pada jumlah informasi yang dikirim.



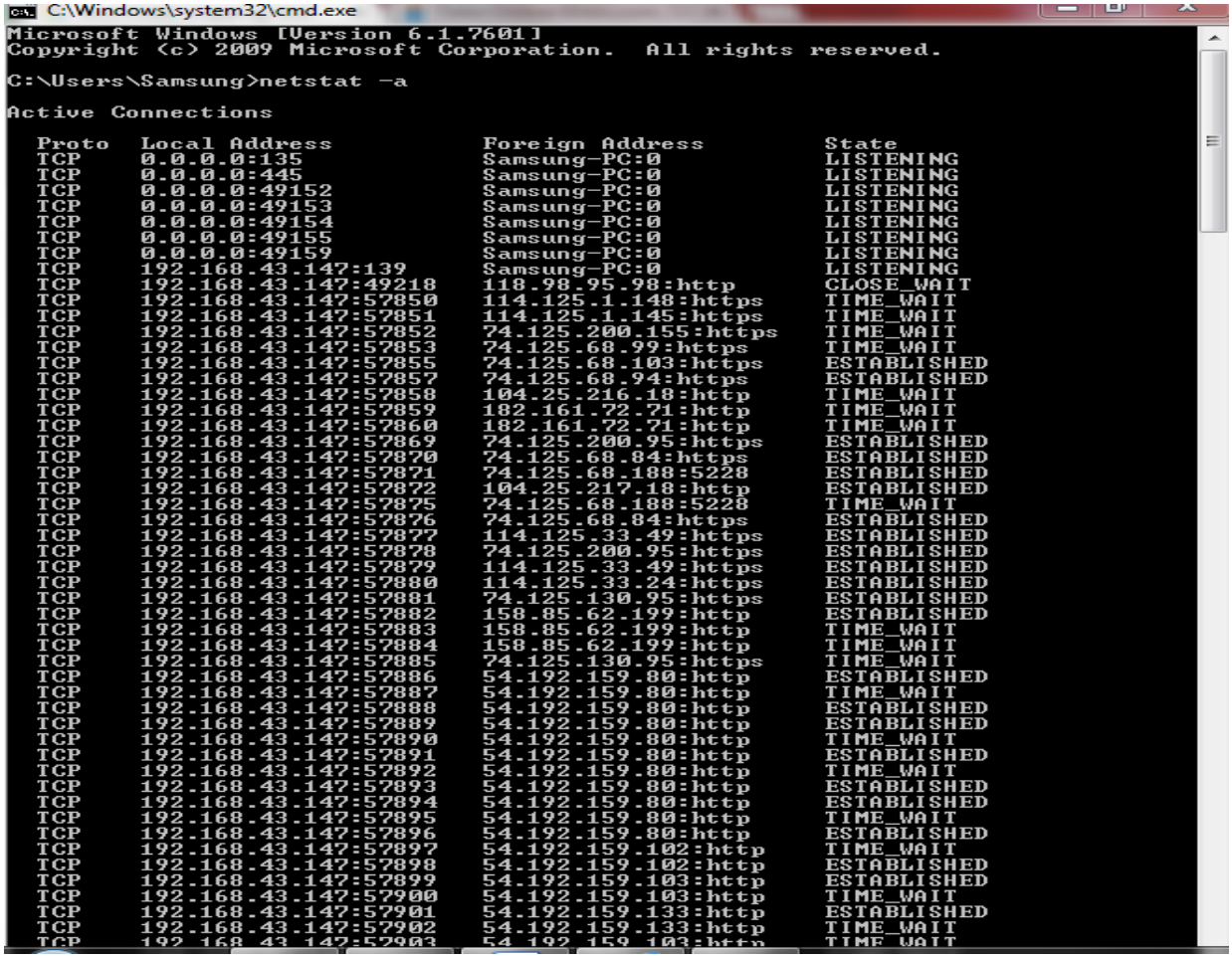
Gambar diatas merupakan gambar dari wireshark pada metode POST pada situs blibli.com

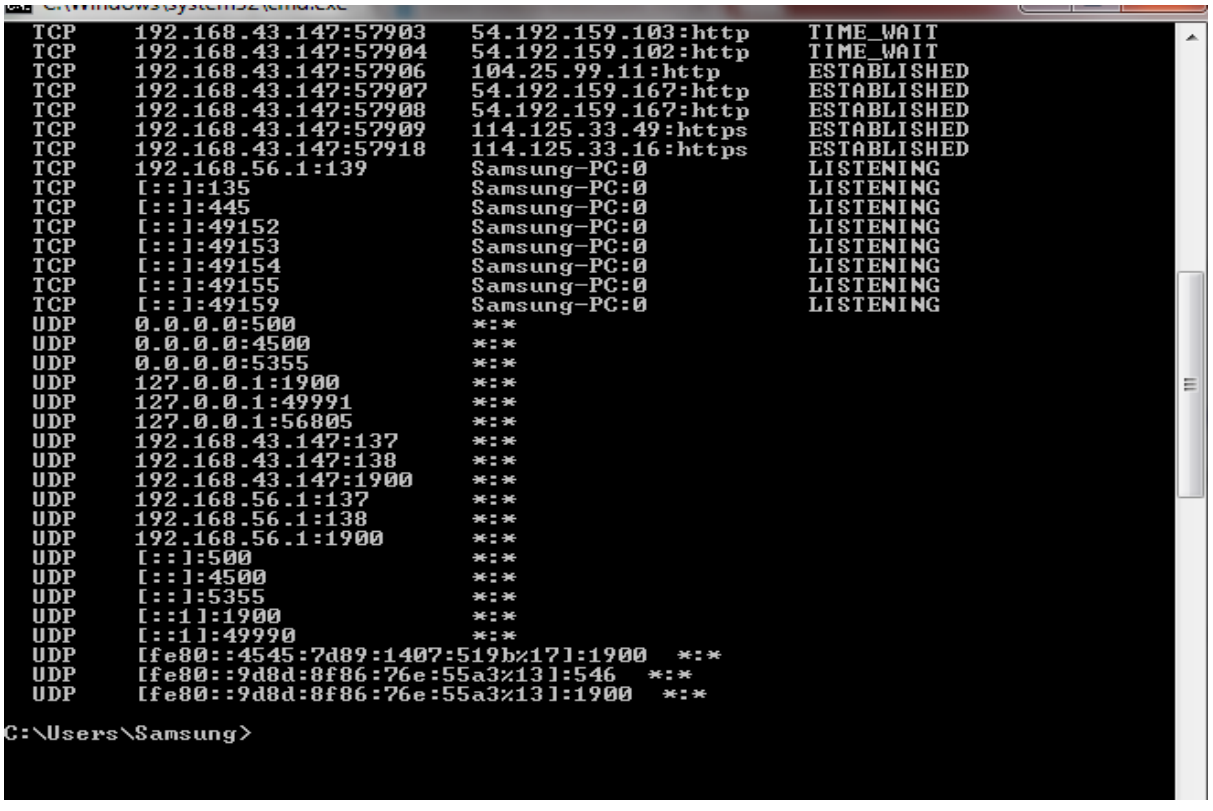
Pada gambar diatas menunjukan bahwa banyak sekali HTTP Messages yang ditangkap saat meload situs Blibli.com. Berdasarkan sumbernya ada dua macam HTTP Messages yang ditangkap yaitu dari browser kita ke server Blibli dan sebaliknya, hal tersebut dapat dilihat dari IP source dan destination.

Perintah Netstat dengan argumen -a.

Netstat **(Net**work **Stat**istics) adalah program berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik itu jaringan lokal (LAN) maupun jaringan internet.

Digunakan untuk menampilkan semua koneksi yang sedang terbuka pada mesin lokal. Hal tersebut meliputi sistem remote dimana koneksi tersebut terjadi, nomor port koneksi tersebut (juga yang pada mesin lokal) dan juga tipe serta status dari koneksi tersebut.


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Samsung>netstat -a
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 Samsung-PC:0 LISTENING
TCP 0.0.0.0:445 Samsung-PC:0 LISTENING
TCP 0.0.0.0:49152 Samsung-PC:0 LISTENING
TCP 0.0.0.0:49153 Samsung-PC:0 LISTENING
TCP 0.0.0.0:49154 Samsung-PC:0 LISTENING
TCP 0.0.0.0:49155 Samsung-PC:0 LISTENING
TCP 0.0.0.0:49159 Samsung-PC:0 LISTENING
TCP 192.168.43.147:139 Samsung-PC:0 LISTENING
TCP 192.168.43.147:49218 118.98.95.98:http CLOSE_WAIT
TCP 192.168.43.147:57850 114.125.1.148:https TIME_WAIT
TCP 192.168.43.147:57851 114.125.1.145:https TIME_WAIT
TCP 192.168.43.147:57852 74.125.200.155:https TIME_WAIT
TCP 192.168.43.147:57853 74.125.68.99:https TIME_WAIT
TCP 192.168.43.147:57855 74.125.68.103:https ESTABLISHED
TCP 192.168.43.147:57857 74.125.68.94:https ESTABLISHED
TCP 192.168.43.147:57858 104.25.216.18:http TIME_WAIT
TCP 192.168.43.147:57859 182.161.72.71:http TIME_WAIT
TCP 192.168.43.147:57860 182.161.72.71:http TIME_WAIT
TCP 192.168.43.147:57869 74.125.200.95:https ESTABLISHED
TCP 192.168.43.147:57870 74.125.68.84:https ESTABLISHED
TCP 192.168.43.147:57871 74.125.68.188:5228 ESTABLISHED
TCP 192.168.43.147:57872 104.25.217.18:http ESTABLISHED
TCP 192.168.43.147:57875 74.125.68.188:5228 TIME_WAIT
TCP 192.168.43.147:57876 74.125.68.84:https ESTABLISHED
TCP 192.168.43.147:57877 114.125.33.49:https ESTABLISHED
TCP 192.168.43.147:57878 74.125.200.95:https ESTABLISHED
TCP 192.168.43.147:57879 114.125.33.49:https ESTABLISHED
TCP 192.168.43.147:57880 114.125.33.24:https ESTABLISHED
TCP 192.168.43.147:57881 74.125.130.95:https ESTABLISHED
TCP 192.168.43.147:57882 158.85.62.199:http ESTABLISHED
TCP 192.168.43.147:57883 158.85.62.199:http TIME_WAIT
TCP 192.168.43.147:57884 158.85.62.199:http TIME_WAIT
TCP 192.168.43.147:57885 74.125.130.95:https TIME_WAIT
TCP 192.168.43.147:57886 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57887 54.192.159.80:http TIME_WAIT
TCP 192.168.43.147:57888 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57889 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57890 54.192.159.80:http TIME_WAIT
TCP 192.168.43.147:57891 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57892 54.192.159.80:http TIME_WAIT
TCP 192.168.43.147:57893 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57894 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57895 54.192.159.80:http TIME_WAIT
TCP 192.168.43.147:57896 54.192.159.80:http ESTABLISHED
TCP 192.168.43.147:57897 54.192.159.102:http TIME_WAIT
TCP 192.168.43.147:57898 54.192.159.102:http ESTABLISHED
TCP 192.168.43.147:57899 54.192.159.103:http ESTABLISHED
TCP 192.168.43.147:57900 54.192.159.103:http TIME_WAIT
TCP 192.168.43.147:57901 54.192.159.133:http ESTABLISHED
TCP 192.168.43.147:57902 54.192.159.133:http TIME_WAIT

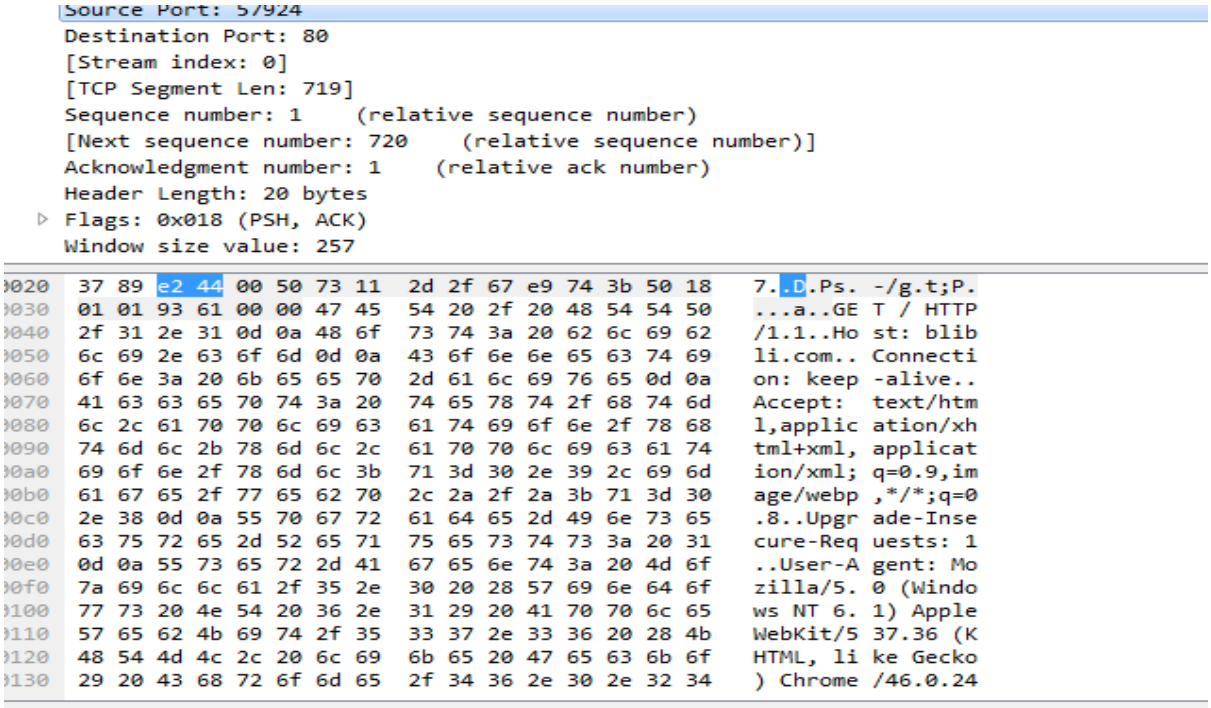

TCP 192.168.43.147:57903 54.192.159.103:http TIME_WAIT
TCP 192.168.43.147:57904 54.192.159.102:http TIME_WAIT
TCP 192.168.43.147:57906 104.25.99.11:http ESTABLISHED
TCP 192.168.43.147:57907 54.192.159.167:http ESTABLISHED
TCP 192.168.43.147:57908 54.192.159.167:http ESTABLISHED
TCP 192.168.43.147:57909 114.125.33.49:https ESTABLISHED
TCP 192.168.43.147:57918 114.125.33.16:https ESTABLISHED
TCP 192.168.56.1:139 Samsung-PC:0 LISTENING
TCP [::]:135 Samsung-PC:0 LISTENING
TCP [::]:445 Samsung-PC:0 LISTENING
TCP [::]:49152 Samsung-PC:0 LISTENING
TCP [::]:49153 Samsung-PC:0 LISTENING
TCP [::]:49154 Samsung-PC:0 LISTENING
TCP [::]:49155 Samsung-PC:0 LISTENING
TCP [::]:49159 Samsung-PC:0 LISTENING
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5355 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:49991 *:*
UDP 127.0.0.1:56805 *:*
UDP 192.168.43.147:137 *:*
UDP 192.168.43.147:138 *:*
UDP 192.168.43.147:1900 *:*
UDP 192.168.56.1:137 *:*
UDP 192.168.56.1:138 *:*
UDP 192.168.56.1:1900 *:*
UDP [::]:500 *:*
UDP [::]:4500 *:*
UDP [::]:5355 *:*
UDP [::1]:1900 *:*
UDP [::1]:49990 *:*
UDP [fe80::4545:7d89:1407:519b%17]:1900 *:*
UDP [fe80::9d8d:8f86:76e:55a3%13]:546 *:*
UDP [fe80::9d8d:8f86:76e:55a3%13]:1900 *:*
C:\Users\Samsung>

Hasil command dengan menggunakan cmd dimana :

1. LISTENING -> siap untuk melakukan koneksi
2. ESTABLISHED -> koneksi terjadi dan siap mengirimkan data
3. TIME_WAIT -> sedang menunggu koneksi

PORT IP

Port adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan Port Number dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP



Dari gambar diatas saya menggunakan IP yang diambil. Disini saya mendapatkan source port 57924 dan destination portnya 80.