

TUGAS JARINGAN KOMPUTER



Nama : Yonatan Riyadhhi
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 (World 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, diikuti 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.

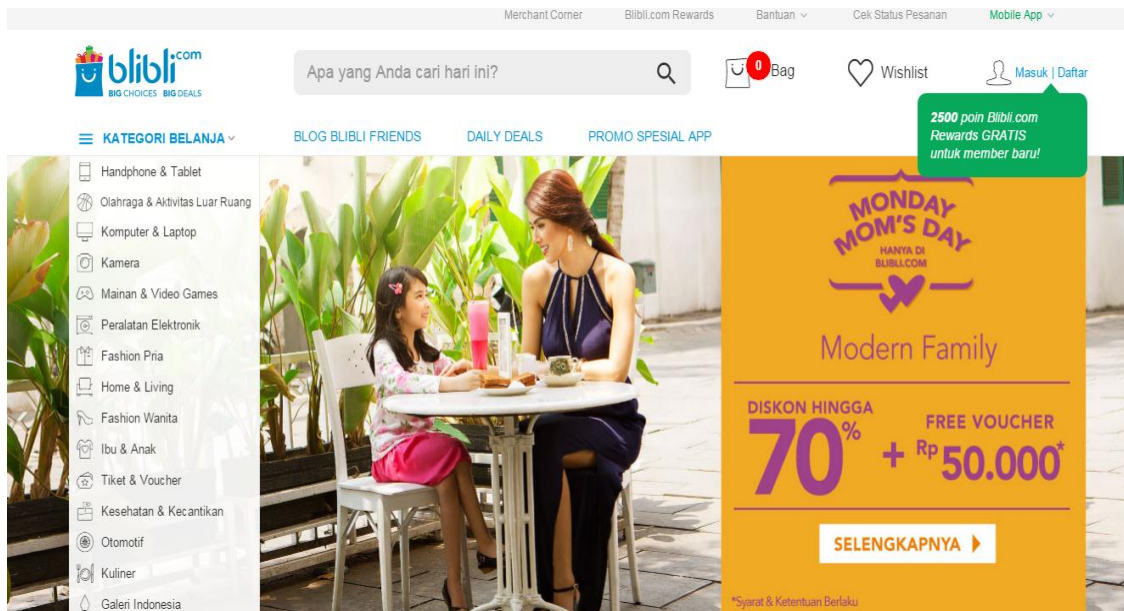
Hingga kini, ada dua versi mayor dari protokol HTTP, yakni HTTP/1.0 yang menggunakan koneksi terpisah untuk setiap dokumen, dan HTTP/1.1 yang dapat menggunakan koneksi yang sama untuk melakukan transaksi. Dengan demikian, HTTP/1.1 bisa lebih cepat karena memang tidak perlu membuang waktu untuk pembuatan 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 & hostname) yang saling terdistribusi. Sebagai analogi ketika kita mengakses www.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 dari 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 wireshark 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.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.184752	192.168.43.147	202.158.55.137	HTTP	773	GET / HTTP/1.1
47	6.296099	202.158.55.137	192.168.43.147	HTTP	181	HTTP/1.0 301 Moved Permanently
5996	655.817759	192.168.43.147	192.126.112.118	HTTP	266	POST /click.aspx?url=http://click_pop_exit_btn.com HTTP/1.1
5998	656.207886	192.126.112.118	192.168.43.147	HTTP	299	HTTP/1.1 200 OK (text/html)
6648	868.004178	192.168.43.147	114.125.33.16	HTTP	704	GET / HTTP/1.1
6650	868.252484	114.125.33.16	192.168.43.147	HTTP	606	HTTP/1.1 302 Found (text/html)

▶ Frame 45: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface 0
 ▶ Ethernet II, Src: SamsungE_73:55:c5 (24:f5:aa:73:55:c5), Dst: AsustekC_34:d8:db (14:dd:a9:34:d8:db)
 ▶ Internet Protocol Version 4, Src: 192.168.43.147, Dst: 202.158.55.137
 ▶ Transmission Control Protocol, Src Port: 57924, Dst Port: 80, Seq: 1, Ack: 1, Len: 719
 ▶ Hypertext Transfer Protocol

```

0000  14 dd a9 34 d8 db 24 f5 aa 73 55 c5 08 00 45 00  ...4.$ .sU...E.
0010  02 f7 18 0c 40 00 40 06 31 92 c0 a8 2b 93 ca 9e  ...@.@.1...+...
0020  37 89 e2 44 00 50 73 11 2d 2f 67 e9 74 3b 50 18  7..D.Ps. -/g.t;P.
0030  01 01 93 61 00 00 47 45 54 20 2f 20 48 54 54 50  ...a..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 62 6c 69 62  /1.1..Ho st: blib
0050  6c 69 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69  li.com.. Connecti
0060  6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a  on: keep -alive..
0070  41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d  Accept: text/htm
0080  6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68  l,applic ation/xh
0090  74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74  tml+xml, applicat
00a0  69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d  ion/xml; q=0.9,im
00b0  61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30  age/webp ,*/;q=0
00c0  2e 38 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65  .8..Upgr ade-Inse
00d0  63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31  cure-Req uests: 1
00e0  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f  ..User-A gent: Mo
00f0  7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f  zilla/5. 0 (Windo
0100  77 73 20 4e 54 20 36 2e 31 29 20 41 70 70 6c 65  ws NT 6. 1) Apple
0110  57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b  WebKit/5 37.36 (K
0120  48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f  HTML, li ke Gecko
0130  29 20 43 68 72 6f 6d 65 2f 34 36 2e 30 2e 32 34  ) Chrome /46.0.24
0140  39 30 2e 38 30 20 53 61 66 61 72 69 2f 35 33 37  90.80 Sa fari/537
0150  2e 33 36 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f  .36..Acc ept-Enco
0160  64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 6e 6c  ding: gz ip, defl
0170  61 74 65 2c 20 73 64 63 68 0d 0a 41 63 63 65 70  ate, sdc h..Accep
0180  74 2d 4e 61 6a 67 75 61 67 65 3a 20 65 6e 2d 55  t-langua ge: en-I
  
```

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 baru URL/ Address bar

```

▶ GET / HTTP/1.1\r\n
Host: blibli.com\r\n
Connection: keep-alive\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
[truncated]Cookie: __utma=205442883.1598728269.1474278607.1474278606.1; __utmb=205442883.8.10.1474278606; __utmz=205442883.1474278606
\r\n
[Full request URI: http://blibli.com/]
[HTTP request 1/1]
[Response in frame: 47]
  
```

```

0030  01 01 93 61 00 00 47 45 54 20 2f 20 48 54 54 50  ...a..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 62 6c 69 62  /1.1..Ho st: blib
0050  6c 69 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69  li.com.. Connecti
0060  6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a  on: keep -alive..
0070  41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d  Accept: text/htm
0080  6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68  l,applic ation/xh
0090  74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74  tml+xml, applicat
00a0  69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d  ion/xml; q=0.9,im
00b0  61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30  age/webp ,*/;q=0
00c0  2e 38 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65  .8..Upgr ade-Inse
00d0  63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31  cure-Req uests: 1
00e0  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f  ..User-A gent: Mo
00f0  7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f  zilla/5. 0 (Windo
0100  77 73 20 4e 54 20 36 2e 31 29 20 41 70 70 6c 65  ws NT 6. 1) Apple
0110  57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b  WebKit/5 37.36 (K
0120  48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f  HTML, li ke Gecko
0130  29 20 43 68 72 6f 6d 65 2f 34 36 2e 30 2e 32 34  ) Chrome /46.0.24
0140  39 30 2e 38 30 20 53 61 66 61 72 69 2f 35 33 37  90.80 Sa fari/537
  
```

```

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=eF5j4cotK8lMETA0MjDVNDQ1ZCln9kgxskg1tAw07U0M0jWNUkyNdVNNQz00yMDVNMtA3SUKyNQEAiBkNzw; _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.

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets. Packet 5996 is highlighted, showing an HTTP POST request to /click.aspx?url=http://click_pop_exit_btn.com. The packet details pane shows the structure of the HTTP message, including the request line, headers, and body. The packet bytes pane shows the raw hexadecimal and ASCII data of the captured packet.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.184752	192.168.43.147	202.158.55.137	HTTP	773	GET / HTTP/1.1
47	6.296099	202.158.55.137	192.168.43.147	HTTP	181	HTTP/1.0 301 Moved Permanently
5996	655.817759	192.168.43.147	192.126.112.118	HTTP	266	POST /click.aspx?url=http://click_pop_exit_btn.com HTTP/1.1
5998	656.207886	192.126.112.118	192.168.43.147	HTTP	299	HTTP/1.1 200 OK (text/html)
6648	868.084178	192.168.43.147	114.125.33.16	HTTP	704	GET / HTTP/1.1
6650	868.252484	114.125.33.16	192.168.43.147	HTTP	606	HTTP/1.1 302 Found (text/html)

Frame 5996: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface 0
 Ethernet II, Src: SamsungE_73:55:c5 (24:f5:aa:73:55:c5), Dst: AsustekC_34:d8:db (14:dd:a9:34:d8:db)
 Internet Protocol Version 4, Src: 192.168.43.147, Dst: 192.126.112.118
 Transmission Control Protocol, Src Port: 58033, Dst Port: 80, Seq: 1, Ack: 1, Len: 212
 Hypertext Transfer Protocol

```

0000 14 dd a9 34 d8 db 24 f5 aa 73 55 c5 08 00 45 00 ..4..$.su..E.
0010 00 fc 22 e8 40 00 40 06 f9 e3 c0 a8 2b 93 c0 7e ..".@. ....~
0020 70 76 e2 b1 00 50 01 86 96 35 62 22 55 c0 50 18 pv...P..5b"U.P.
0030 01 01 4d 44 00 00 50 4f 53 54 20 2f 63 6c 69 63 .MD.xPO ST /clie
0040 6b 2e 61 73 70 78 3f 75 72 6c 3d 68 74 70 70 3a k.aspx?url=http:
0050 2f 2f 63 6c 69 63 6b 5f 70 6f 70 5f 65 78 69 74 //click_pop_exit
0060 5f 62 74 6e 2e 63 6f 6d 20 48 54 54 50 2f 31 2e _btn.com HTTP/1.
0070 31 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 1..Content-Lengt
0080 68 3a 20 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e h: 0..Connection
0090 3a 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 : Close. User-Ag
00a0 65 6e 74 3a 20 55 73 65 72 2d 41 67 65 6e 74 3a ent: Use r-Agent:
00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
00c0 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 54 72 69 dows NT 6.1; Tri
00d0 64 65 6e 74 2f 37 2e 30 3b 20 72 76 3a 31 31 2e dent/7.0 ; rv:11.
00e0 30 29 20 6c 69 6b 65 20 47 65 63 6b 6f 0d 0a 48 0) like Gecko..H
00f0 6f 73 74 3a 20 70 6f 70 2e 79 65 61 70 6c 61 79 ost: pop.yeaplay
0100 65 72 2e 63 6f 6d 0a 0d 0a er.com...

```

```
POST /click.aspx?url=http://click_pop_exit_btn.com HTTP/1.1
Content-Length: 0
Connection: Close
User-Agent: User-Agent:Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Host: pop.yeaplayer.com

HTTP/1.1 200 OK
Connection: close
Date: Mon, 19 Sep 2016 11:12:47 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 8

12092649
```

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

Pada gambar diatas menunjukkan 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 (**Network Statistics**) 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

```

```

C:\Windows\system32\cmd.exe
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 [::]:1900 *:*
UDP [::]:49990 *:*
UDP [fe80::4545:7d89:1407:519b%171]: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 mengidentifikasi aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasi 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

```
Source Port: 57924
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 719]
Sequence number: 1 (relative sequence number)
[Next sequence number: 720 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 257

020 37 89 e2 44 00 50 73 11 2d 2f 67 e9 74 3b 50 18 7.D.Ps. -/g.t;P.
030 01 01 93 61 00 00 47 45 54 20 2f 20 48 54 54 50 ...a..GE T / HTTP
040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 62 6c 69 62 /1.1..Ho st: blib
050 6c 69 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 li.com.. Connecti
060 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..
070 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d Accept: text/htm
080 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 l,application/xh
090 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 tml+xml, applicat
0a0 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d ion/xml; q=0.9,im
0b0 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 age/webp ,*/*;q=0
0c0 2e 38 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 .8..Upgr ade-Inse
0d0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
0e0 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..User-A gent: Mo
0f0 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo
100 77 73 20 4e 54 20 36 2e 31 29 20 41 70 70 6c 65 ws NT 6. 1) Apple
110 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b WebKit/5 37.36 (K
120 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f HTML, li ke Gecko
130 29 20 43 68 72 6f 6d 65 2f 34 36 2e 30 2e 32 34 ) Chrome /46.0.24
```

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