Wireshark

Program wireshark merupakan salah satu program networking yang digunakan untuk monitoring traffic networking, sniffing dsb, lebih umum dikenal sebagai sniffing (mengendus) tools. Wireshark secara interaktif dapat mem-browse paket data dari network realtime atau dari file yang telah di capture sebelumnya. User dapat menggunakan ini untuk berbagai macam keperluan seperti instrusion detection, traffic monitoring, debug protocol implementation. Wireshark dapat digunakan sebagai peer di dalam suatu jaringan dan mengamati trafik secara detail dala berbagai level mulai dari header packet hingga bit yang menyusun suatu paket

Netstat

Netstat adalah perintah di command prompt yang berfungsi untuk menampilkn statistik koneksi jaringan dari dan ke komputer yang sedang kita pakai. Netstat bisa disamakan dengan taskmanager, perbedaannya taskmanager menampilkan proses dan aplikasi yang sedang berjalan sedangkan netstat menampilkan layanan jaringan yang sedang dipakai beserta informasi tambahan seperti ip dan portnya.

Netstat (network statistics) adalah program berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik itu jaringan lokal (LAN) maupun jaringan internet. Kapan saya membutuhkan netstat ? misalkan suatu ketika anda sedang internetan kemudian tiba tiba koneksi menjadi sangat lambat dan anda mencurigai ada program di komputer anda yang jadi penyebabnya. Jika hal itu yang anda alami maka anda perlu memanggil program netstat untuk melakukan pengecekan

Berikut ini keterangan dari output netstat diatas :

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 anda yang mana saat itu sedang aktif melakukan koneksi. Contoh diatas fatality adalah nama host dari komputer saya dan 1772 adalah nomor port di komputer saya yang sedang melakukan koneksi.

3. **Foreign Address**. Kolom ini menunjukan koneksi yang dituju oleh local address beserta nomor portnya. Contoh diatas saya sedang menghubungi server google melalui http (port 80) yang artinya saya sedang browsing google.
4. **State**. Kolom ini menunjukan status dari koneksi yang sedang terjadi.

5. **Established** artinya sudah terhubung dengan komputer lain dan siap mengirimkan data.

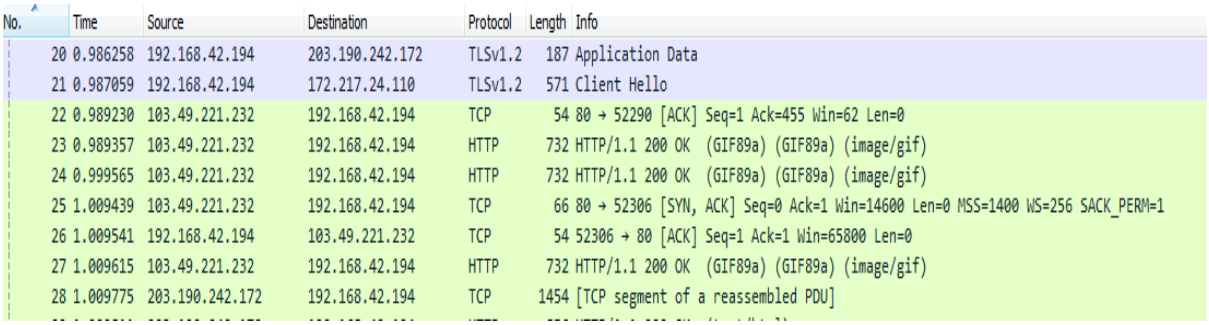
State yang terjadi

- **LISTENING** -> siap untuk melakukan koneksi.
- **SYN_SENT** -> mengirimkan paket SYN
- **SYN_RECEIVED** -> menerima paket SYN
- **ESTABLISHED** -> koneksi terjadi dan siap mengirimkan data.
- **TIME_WAIT** -> sedang menunggu koneksi

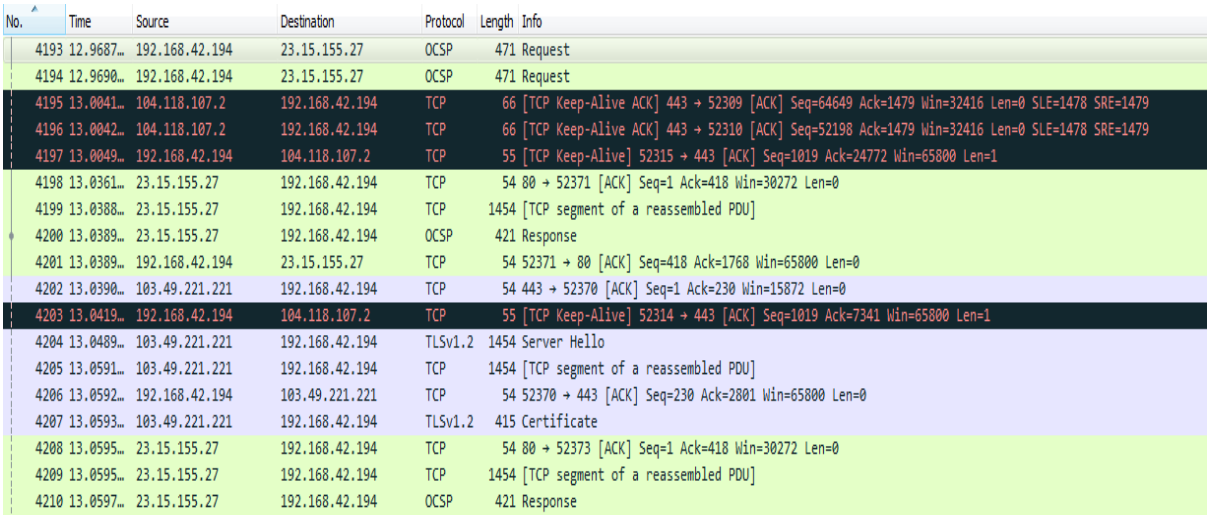
Yang perlu diperhatikan jika muncul state SYN_SENT adalah data dalam jumlah yang banyak dan terus menerus, efeknya koneksi internet anda menjadi sangat lambat.

Pada Langkah ini menjelaskan pada saat Bagian Web Browsing (CnnIndonesia.com) Menggunakan WireShark

Pada langkah ini saya telah melakukan web browsing dengan situs yang dituju ialah www.cnnindonesia.com , pada bagian yang ini saya menggunakan WireShark untuk melihat proses dari source ke destination serta sebaliknya proses dari destination ke source.



No.	Time	Source	Destination	Protocol	Length	Info
20	0.986258	192.168.42.194	203.190.242.172	TLSv1.2	187	Application Data
21	0.987059	192.168.42.194	172.217.24.110	TLSv1.2	571	Client Hello
22	0.989230	103.49.221.232	192.168.42.194	TCP	54	80 → 52290 [ACK] Seq=1 Ack=455 Win=62 Len=0
23	0.989357	103.49.221.232	192.168.42.194	HTTP	732	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
24	0.999565	103.49.221.232	192.168.42.194	HTTP	732	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
25	1.009439	103.49.221.232	192.168.42.194	TCP	66	80 → 52306 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 WS=256 SACK_PERM=1
26	1.009541	192.168.42.194	103.49.221.232	TCP	54	52306 → 80 [ACK] Seq=1 Ack=1 Win=65800 Len=0
27	1.009615	103.49.221.232	192.168.42.194	HTTP	732	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
28	1.009775	203.190.242.172	192.168.42.194	TCP	1454	[TCP segment of a reassembled PDU]



No.	Time	Source	Destination	Protocol	Length	Info
4193	12.9687…	192.168.42.194	23.15.155.27	OCSP	471	Request
4194	12.9690…	192.168.42.194	23.15.155.27	OCSP	471	Request
4195	13.0041…	104.118.107.2	192.168.42.194	TCP	66	[TCP Keep-Alive ACK] 443 → 52309 [ACK] Seq=64649 Ack=1479 Win=32416 Len=0 SLE=1478 SRE=1479
4196	13.0042…	104.118.107.2	192.168.42.194	TCP	66	[TCP Keep-Alive ACK] 443 → 52310 [ACK] Seq=52198 Ack=1479 Win=32416 Len=0 SLE=1478 SRE=1479
4197	13.0049…	192.168.42.194	104.118.107.2	TCP	55	[TCP Keep-Alive] 52315 → 443 [ACK] Seq=1019 Ack=24772 Win=65800 Len=1
4198	13.0361…	23.15.155.27	192.168.42.194	TCP	54	80 → 52371 [ACK] Seq=1 Ack=418 Win=30272 Len=0
4199	13.0388…	23.15.155.27	192.168.42.194	TCP	1454	[TCP segment of a reassembled PDU]
4200	13.0389…	23.15.155.27	192.168.42.194	OCSP	421	Response
4201	13.0389…	192.168.42.194	23.15.155.27	TCP	54	52371 → 80 [ACK] Seq=418 Ack=1768 Win=65800 Len=0
4202	13.0390…	103.49.221.221	192.168.42.194	TCP	54	443 → 52370 [ACK] Seq=1 Ack=230 Win=15872 Len=0
4203	13.0419…	192.168.42.194	104.118.107.2	TCP	55	[TCP Keep-Alive] 52314 → 443 [ACK] Seq=1019 Ack=7341 Win=65800 Len=1
4204	13.0489…	103.49.221.221	192.168.42.194	TLSv1.2	1454	Server Hello
4205	13.0591…	103.49.221.221	192.168.42.194	TCP	1454	[TCP segment of a reassembled PDU]
4206	13.0592…	192.168.42.194	103.49.221.221	TCP	54	52370 → 443 [ACK] Seq=230 Ack=2801 Win=65800 Len=0
4207	13.0593…	103.49.221.221	192.168.42.194	TLSv1.2	415	Certificate
4208	13.0595…	23.15.155.27	192.168.42.194	TCP	54	80 → 52373 [ACK] Seq=1 Ack=418 Win=30272 Len=0
4209	13.0595…	23.15.155.27	192.168.42.194	TCP	1454	[TCP segment of a reassembled PDU]
4210	13.0597…	23.15.155.27	192.168.42.194	OCSP	421	Response

Bisa dilihat pada gambar di atas terlihat proses **REQUEST** yang meminta paket data ke Destination yaitu alamat website www.cnnindonesia.com , bisa kita lihat proses request yang dilakukan tidak langsung menuju destination melainkan request dilakukan melalui beberapa port ocsp.

Setelah melakukan proses request ke server selanjutnya server menggirimkan kembali paket data source bahwa paket data yang diminta terdapat pada server tersebut. Akhirnya server Merespon data yang kita request tadi dan mengirimkannya kembali ke Source.

Pada Langkah ini menjelaskan pada saat Bagian Web Browsing (CnnIndonesia.com) Menggunakan Netstat

Dapat kita lihat proses yang terjadi pada saat saya ingin melakukan Web Browsing yang memiliki alamat **IP 117.18.237.29** melalui port http dimulai dari proses **TIME_WAIT** maksudnya Source sedang menunggu koneksi dari Destination

```
TCP    169.254.151.174:139    User-PC:0              LISTENING
TCP    192.168.42.194:139     User-PC:0              LISTENING
TCP    192.168.42.194:52796   ec2-52-38-199-186:https  ESTABLISHED
TCP    192.168.42.194:52798   117.18.237.29:http     ESTABLISHED
TCP    192.168.42.194:52799   117.18.237.29:http     ESTABLISHED
TCP    192.168.42.194:52800   117.18.237.29:http     TIME_WAIT
TCP    192.168.42.194:52801   117.18.237.29:http     TIME_WAIT
TCP    192.168.42.194:52802   117.18.237.29:http     TIME_WAIT
TCP    192.168.42.194:52803   117.18.237.29:http     TIME_WAIT
TCP    192.168.42.194:52804   203.190.242.254:https  ESTABLISHED
TCP    192.168.42.194:52807   a23-15-155-27:http     ESTABLISHED
TCP    192.168.42.194:52808   203.190.242.102:https  ESTABLISHED
TCP    192.168.42.194:52809   103.49.221.172:https   SYN_SENT
TCP    192.168.42.194:52810   103.49.221.232:https   ESTABLISHED
TCP    192.168.42.194:52811   103.49.221.172:https   SYN_SENT
TCP    192.168.42.194:52812   edge-star-mini-shv-01-sin6:https  ESTABLISHED
TCP    192.168.42.194:52813   sb-in-f102:https       ESTABLISHED
TCP    192.168.42.194:52814   74.125.24.157:https    ESTABLISHED
TCP    192.168.42.194:52815   203.190.242.244:https  ESTABLISHED
TCP    192.168.42.194:52816   server-54-230-156-60:https  ESTABLISHED
TCP    192.168.42.194:52817   74.125.24.157:https    ESTABLISHED
TCP    192.168.42.194:52818   edge-z-1-p2-shv-02-sin6:https  ESTABLISHED
TCP    192.168.42.194:52819   sin10s07-in-f110:https  ESTABLISHED
TCP    192.168.42.194:52820   103.49.221.221:https   ESTABLISHED
TCP    192.168.42.194:52821   xx-fbcdn-shv-02-sin6:https  ESTABLISHED
TCP    192.168.42.194:52822   103.3.56.92:https      ESTABLISHED
TCP    192.168.42.194:52823   203.190.242.120:https  ESTABLISHED
TCP    192.168.42.194:52824   7c:https               ESTABLISHED
```

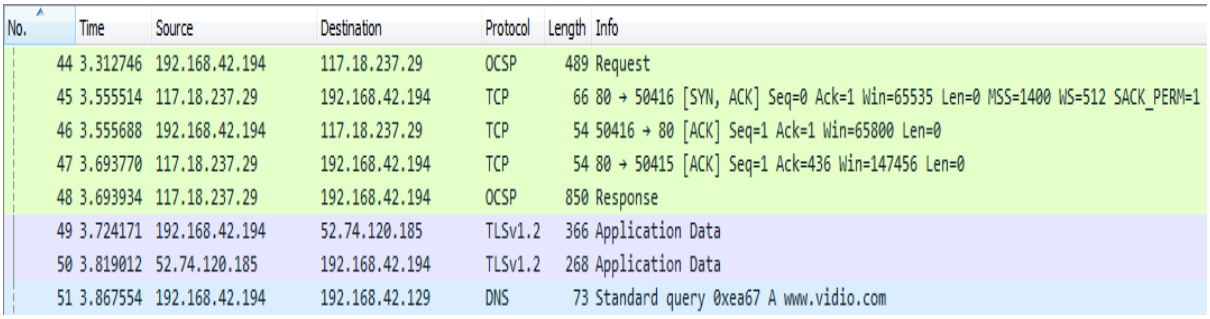
Setelah proses maka akan tercipta psoes **ESTABLISHED** setelah itu bisa kita lihat di bawah ini Proses State **SYN_SENT** ini merupakan data yang dalam jumlah yang banyak dan terus menerus

Pada Langkah ini menjelaskan pada saat Bagian Online Streaming (Vidio.com) Menggunakan WireShark

Pada langkah ini saya telah melakukan online streaming dengan situs yang dituju ialah www.vidio.com , pada bagian ini saya menggunakan WireShark untuk melihat proses dari source ke destination serta sebaliknya proses dari destination ke source.

No.	Time	Source	Destination	Protocol	Length	Info
13	2.186566	192.168.42.194	52.74.120.185	HTTP	337	GET / HTTP/1.1
14	2.186783	192.168.42.129	192.168.42.194	DNS	262	Standard query response 0x1cff AAAA vidio.com AAAA 64:ff9b::344d:87b9 AAAA 64:ff9c::344d:87b9 NS ns-2043.awsdns-63.…
15	2.329696	52.74.120.185	192.168.42.194	TCP	54	80 → 50412 [ACK] Seq=1 Ack=284 Win=28160 Len=0
16	2.335244	52.74.120.185	192.168.42.194	HTTP	224	HTTP/1.1 302 Found
17	2.383596	192.168.42.194	52.74.120.185	TCP	66	50414 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
18	2.445429	52.74.120.185	192.168.42.194	TCP	66	443 → 50414 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 WS=256 SACK_PERM=1
19	2.445631	192.168.42.194	52.74.120.185	TCP	54	50414 → 443 [ACK] Seq=1 Ack=1 Win=65800 Len=0
20	2.453271	192.168.42.194	52.74.120.185	TLSv1.2	237	Client Hello
21	2.521198	52.74.120.185	192.168.42.194	TCP	54	443 → 50414 [ACK] Seq=1 Ack=184 Win=28160 Len=0
22	2.533947	52.74.120.185	192.168.42.194	TLSv1.2	1454	Server Hello

Pada langkah kali ini bisa kita lihat di trafik yang didapat dari Wireshark menujukkan proses **GET/HTTP/1.1 pada No 13** yang menjelaskan bahwa kita sedang mencari situs online streaming (Vidio.com)setelah melakukan proses pencarian akhirnya kita mendapatkan **HTTP/1.1 302 Found pada No 16** yang mengartikan bahwa kita menemukan situs Vidio.com yang kita cari sebelumnya. IP laptop yang saya gunakan disini ialah **192.168.42.194** sebagai Source , dan IP Vidio.com ialah **52.74.120.185** sebagai Destinationnya. Setelah mendapatkan data bisa diliat pada **No 20 dan 22** antara source dan destination telah terhubung. Setelah melakukan proses GET ke server Vidio.com akhirnya server mengirimkan kembali paket data ke source

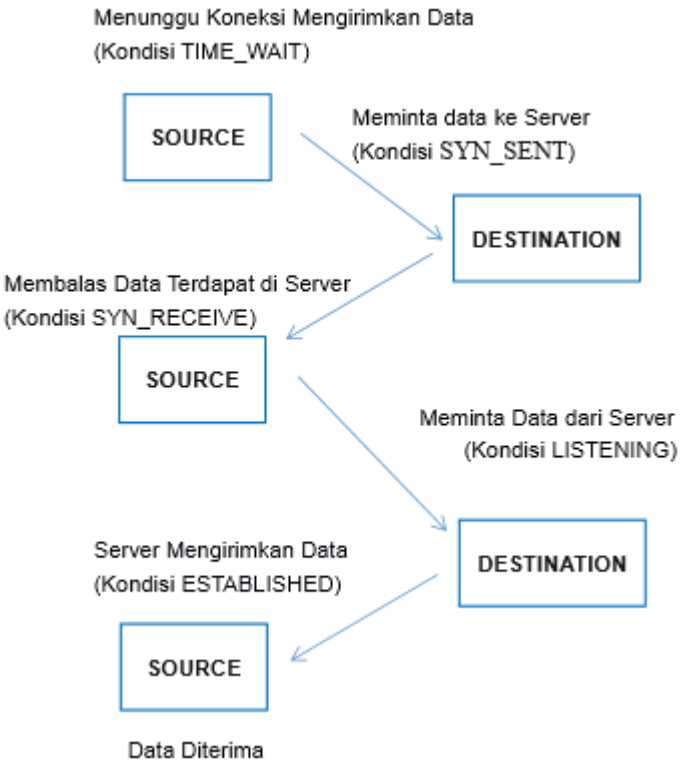


No.	Time	Source	Destination	Protocol	Length	Info
44	3.312746	192.168.42.194	117.18.237.29	OCSP	489	Request
45	3.555514	117.18.237.29	192.168.42.194	TCP	66	80 → 50416 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=512 SACK_PERM=1
46	3.555688	192.168.42.194	117.18.237.29	TCP	54	50416 → 80 [ACK] Seq=1 Ack=1 Win=65800 Len=0
47	3.693770	117.18.237.29	192.168.42.194	TCP	54	80 → 50415 [ACK] Seq=1 Ack=436 Win=147456 Len=0
48	3.693934	117.18.237.29	192.168.42.194	OCSP	850	Response
49	3.724171	192.168.42.194	52.74.120.185	TLSv1.2	366	Application Data
50	3.819012	52.74.120.185	192.168.42.194	TLSv1.2	268	Application Data
51	3.867554	192.168.42.194	192.168.42.129	DNS	73	Standard query 0xea67 A www.vidio.com

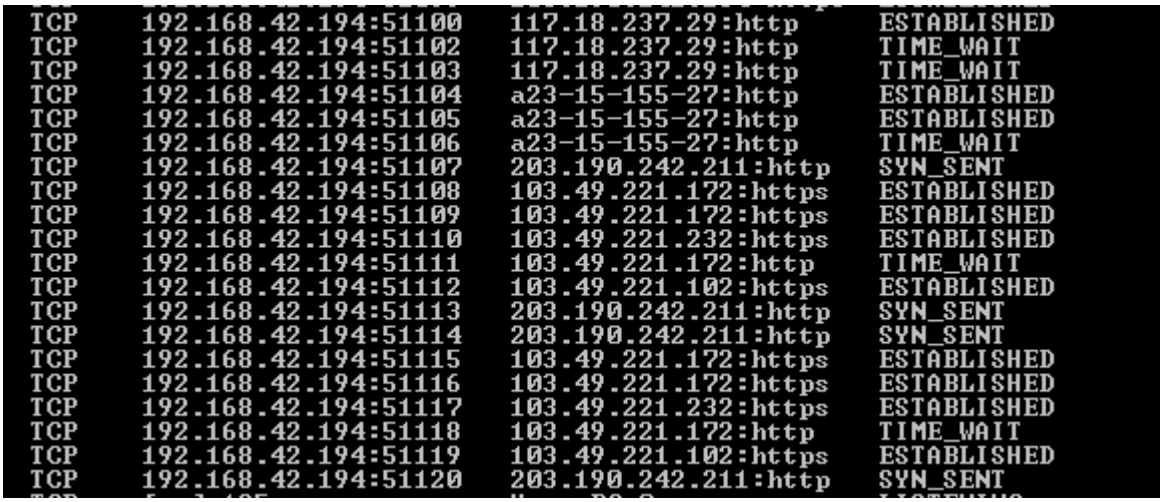
Setelah mendapatkan paket data dari Destination ke Source Lalu setelah itu saya melakukan proses Request ke server Vidio.com untuk melakukan online streaming video dimana video yang ingin saya streaming memiliki **IP 117.18.237.29**, bisa dilihat pada gambar di atas proses yang terjadi dan akhirnya proses yang saya minta untuk melakukan online streaming di Respon oleh Destination pada akhirnya IP Vidio.com menggirimkan data yang saya minta untuk melakukan online streaming ke IP saya.

Pada Langkah ini menjelaskan pada saat Bagian Online Streaming (Vidio.com) Menggunakan Netstat

Dapat kita lihat proses yang terjadi pada saat saya ingin melakukan proses online streaming yang memiliki alamat **IP 117.18.237.29** melalui port http dimulai dari proses **TIME_WAIT** maksudnya Source sedang menunggu koneksi dari Destination bisa kita analogikan sebagai berikut



Setelah proses pada diagram maka akan tercipta psoes **ESTABLISHED** setelah itu bisa kita lihat di bawah ini Proses State **SYN_SENT** ini merupakan data yang dalam jumlah yang banyak dan terus menerus karena kita sedang melakukan Online Streaming



Kesimpulan

Pada Wireshark Informasi yang ditampilkan sangat lengkap dan mendetail mencakup data keseluruhan yang di capturing sedangkan pada penggunaan Netstat informasi yang diberikan hanya sederhana disebut dengan State atau bisa disebut hanya mendeskripsikan suatu keadaang yang data yangdi capturing