

KOMUNIKASI DATA



Disusun Oleh:

Nama : Rahman Ramadhan

Kelas : SK 4 A

NIM : 09011381621082

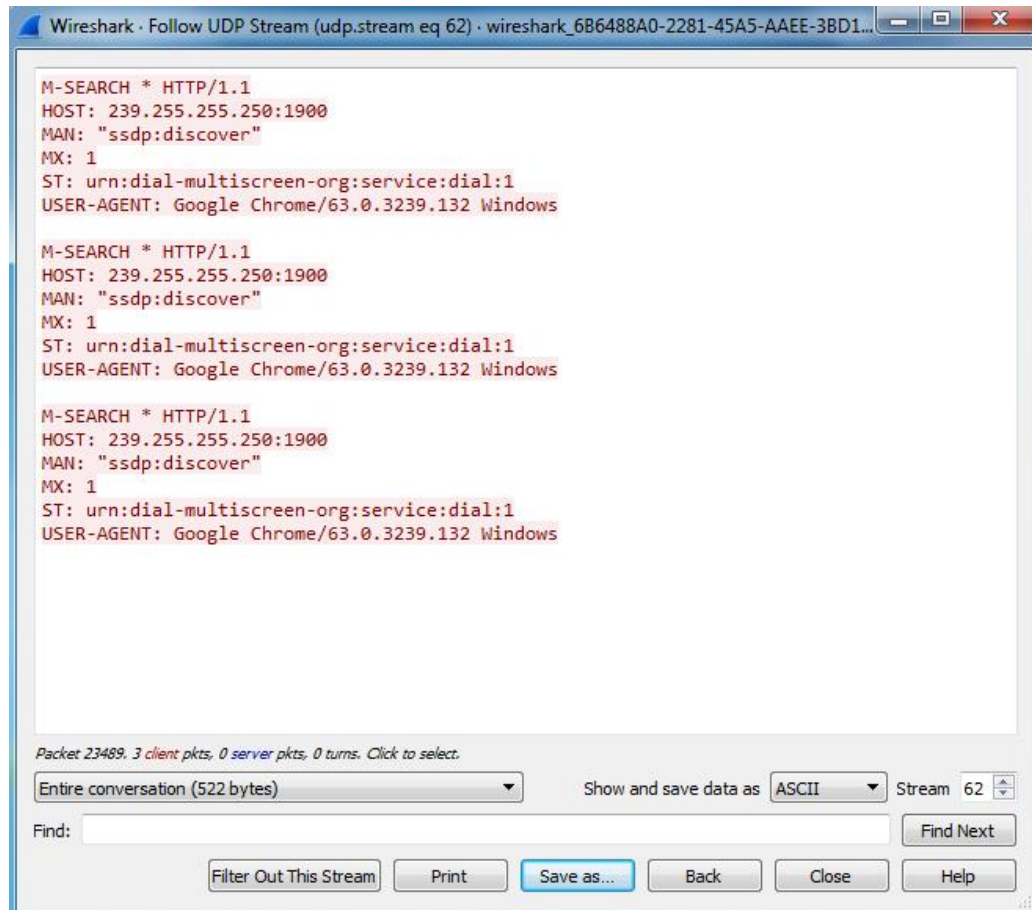
**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

No.	Time	Source	Destination	Protocol	Length	Info
37	4.4414...	104.193.80.60	192.168.43.19	TCP	54	443 → 49412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	4.4420...	104.193.80.60	192.168.43.19	TCP	54	443 → 49413 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	5.8797...	192.168.43.19	172.217.160.35	TCP	66	49477 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
88	5.9486...	172.217.160.35	192.168.43.19	TCP	66	443 → 49477 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
89	5.9487...	192.168.43.19	172.217.160.35	TCP	54	49477 → 443 [ACK] Seq=1 Ack=1 Win=16800 Len=0
90	5.9504...	192.168.43.19	172.217.24.106	TCP	66	49478 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
91	5.9513...	192.168.43.19	74.125.68.95	TCP	66	49479 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
92	5.9523...	192.168.43.19	74.125.200.94	TCP	66	49480 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
93	5.9532...	192.168.43.19	172.217.160.35	TLSv1.2	253	Client Hello
97	6.0218...	172.217.160.35	192.168.43.19	TCP	54	443 → 49477 [ACK] Seq=1 Ack=200 Win=4396 Len=0
98	6.0239...	172.217.24.106	192.168.43.19	TCP	66	443 → 49478 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
99	6.0240...	192.168.43.19	172.217.24.106	TCP	54	49478 → 443 [ACK] Seq=1 Ack=1 Win=16800 Len=0
100	6.0244...	74.125.200.94	192.168.43.19	TCP	66	443 → 49480 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
101	6.0246...	192.168.43.19	74.125.200.94	TCP	54	49480 → 443 [ACK] Seq=1 Ack=1 Win=16800 Len=0
102	6.0329...	74.125.68.95	192.168.43.19	TCP	66	443 → 49479 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=256
103	6.0331...	192.168.43.19	74.125.68.95	TCP	54	49479 → 443 [ACK] Seq=1 Ack=1 Win=16560 Len=0
104	6.0340...	192.168.43.19	172.217.24.106	TLSv1.2	269	Client Hello
105	6.0347...	192.168.43.19	74.125.200.94	TLSv1.2	267	Client Hello
106	6.0354...	192.168.43.19	74.125.68.95	TLSv1.2	262	Client Hello

Pada gambar diatas dapat dilihat bahwa banyak IP yang mengakses facebook.com. Pada gambar tersebut juga IP telah difilter hanya menampilkan protocol TCP/IP.

No.	Time	Source	Destination	Protocol	Length	Info
23487	604.73...	192.168.43.13	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
23488	605.96...	192.168.43.13	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
23489	606.78...	192.168.43.13	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Untuk daftar IP digambar tersebut adalah IP dari seseorang yang berada disamping saya yang di filter untuk menampilkan protocol SSDP/UDP, sedangkan pada protocol TCP/IP tidak sama sekali bisa ditemukan.



The image shows a Wireshark window titled "Follow UDP Stream (udp.stream eq 62) · wireshark_6B6488A0-2281-45A5-AAEE-3BD1...". The main content area displays three identical M-SEARCH HTTP requests. Each request has the following fields: M-SEARCH * HTTP/1.1, HOST: 239.255.255.250:1900, MAN: "ssdp:discover", MX: 1, ST: urn:dial-multiscreen-org:service:dial:1, and USER-AGENT: Google Chrome/63.0.3239.132 Windows. Below the text, there is a status bar indicating "Packet 23489, 3 client pkts, 0 server pkts, 0 turns. Click to select." and a dropdown menu set to "Entire conversation (522 bytes)". To the right, there are controls for "Show and save data as" (set to ASCII) and "Stream" (set to 62). At the bottom, there is a "Find:" input field and a "Find Next" button. Below these are several action buttons: "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help".

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/63.0.3239.132 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/63.0.3239.132 Windows

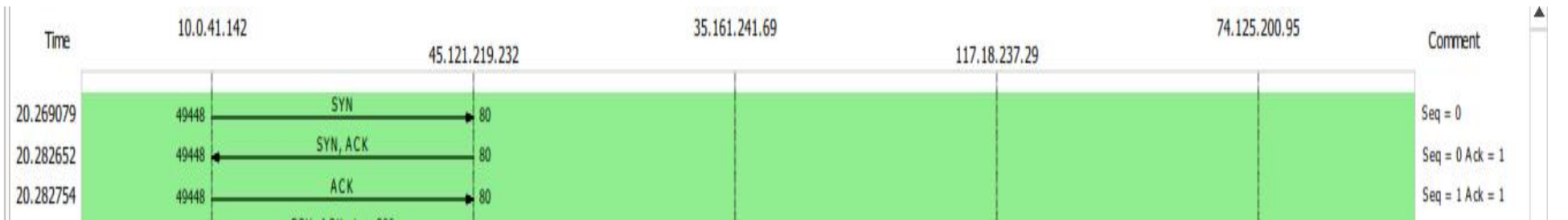
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/63.0.3239.132 Windows
```

Ketika IP Address dari salah satu protocol SSDP/UDP yang ditunjukkan pada gambar sebelumnya dilakukan Follow UDP Steam, maka akan muncul data seperti gambar diatas. Ada beberapa hal yang dapat dianalisa pada data tersebut misalnya “USER AGENT : Google Chrome/63.0.3239.132 Windows”, dapat diketahui bahwa USER yang memiliki IP Address yang di Follow UDP Stream tersebut adalah USER pyang menggunakan OS Windows dan sedang menggunakan aplikasi browser yaitu Google Chrome.



Analisa :

1. IP Address client adalah 10.0.41.142

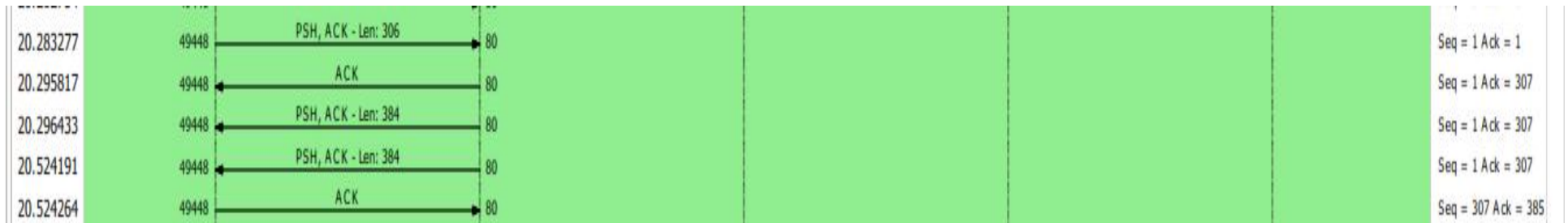


Analisa :

1. Gambar diatas merupakan Connection Establishment. Connection Establishment merupakan proses dimana dua computer menukar tiga segmen TCP untuk menginisialisasi TP header field, dengan demikian mengizinkan program aplikasi pada masing-masing computer dapat berkomunikasi dengan program aplikasi pada computer lain., dengan menggunakan TCP. Client mengirimkan flags SYN menuju server dengan sequence number 0. Kemudian server membalas dengan mengirim flags SYN + ACK ke clinet dengan sequence number 0 dan acknowledgement number 1. Hal ini terjadi karena segmen SYN + ACK tidak bisa membawa data, namun mengonsumsi satu sequence number. Selanjutnya, Client membalas dengan mengirim flags ACK menuju server dengan sequence number 1 dan acknowledgement number 1

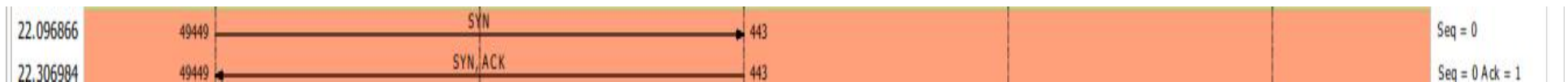
Keterangan :

1. SYN adalah singkatan dari Synchronize
2. ACK adalah Acknowledgement yang merupakan receive data



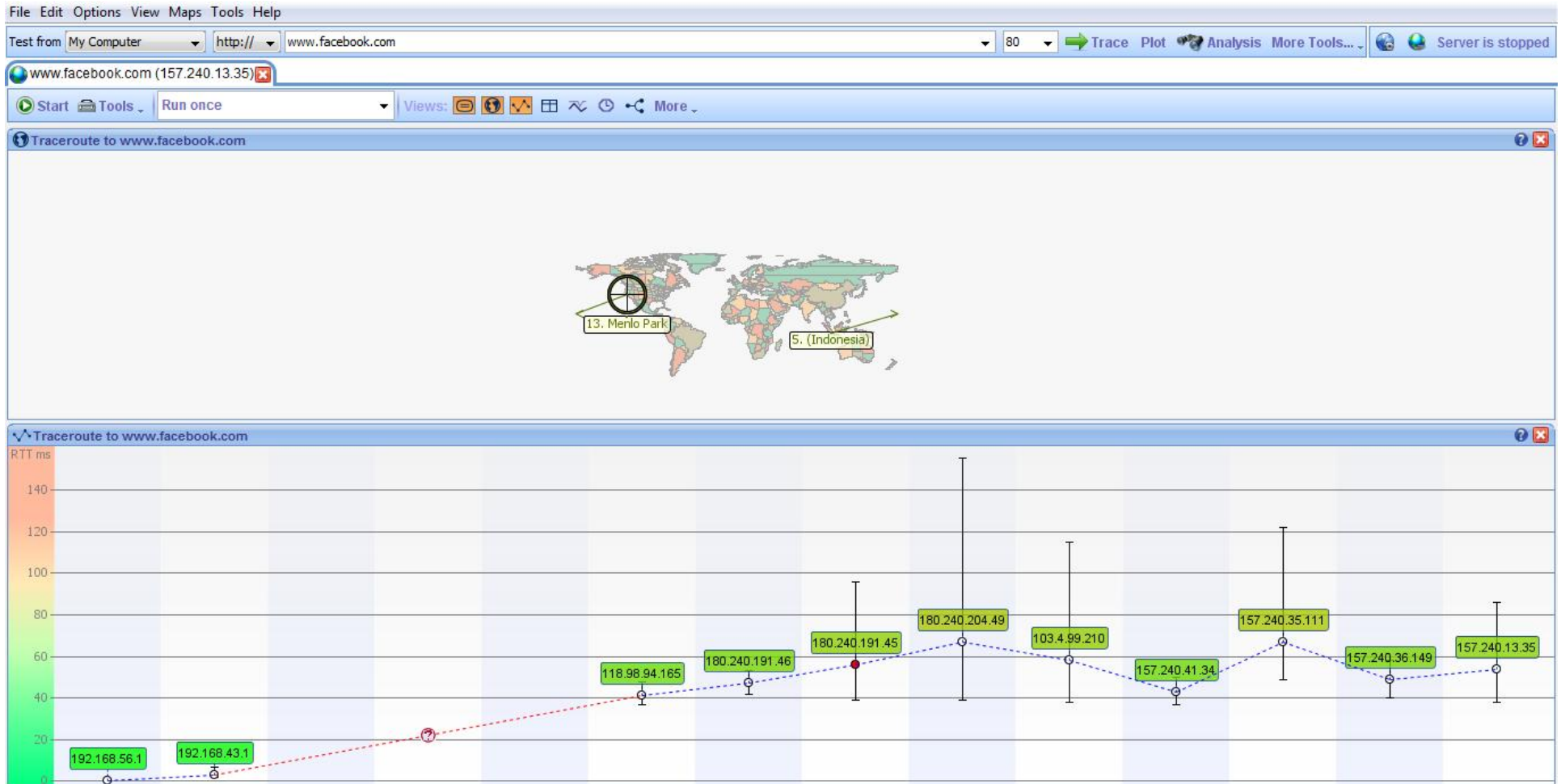
Analisis :

1. Pada panah 1 tersebut melakukan pengiriman data dari client ke server sebesar 306 byte, melalui flags PSH + ACK + len 306. Sequence number dan acknowledgement number tetap 1
2. Pada panah 2 tersebut dimana server membalas dengan mengirim flags ACK menuju client. Sequence number 1 dan acknowledgement berubah menjadi 307. Acknowledgement number berubah menjadi 307, yang merupakan hasil penjumlahan antara besar data yang diterima yaitu 306 byte dengan sequence number yang sebelumnya dikirim oleh client yaitu 1
3. Pada panah 3 dan 4 tersebut dimana server mengirim data sebesar 384 byte menuju client melalui flags PSH + ACK + len 384. Sequence number dan acknowledgement number tetap.
4. Pada panah ke 5 tersebut dimana client menerima apa yang telah dikirim oleh server dengan cara mengirim flags ACK. Sequence number berubah menjadi 307 yang merupakan acknowledgement number yang sebelumnya dikirim oleh server, dan acknowledgement 385 yang merupakan hasil penjumlahan antara besar data yang diterima yaitu 384 byte dengan sequence number yang sebelumnya dikirim oleh server yaitu 1.



Analisis :

1. Pada panah 1 digambar diatas tersebut melakukan Sinkronisasi client terhadap sever
2. Pada panah 2 tersebut melakukan penerimaan untuk melakukan Sinkronisasi dari client terhadap server.



Sudah jelas perbedaan data yang dihasilkan oleh aplikasi WireShark dan VisualRoute.

1. Pada aplikasi WireShark kita dapat melakukan filter protocol sehingga memudahkan kita untuk mencari protocol yang ingin di analisa, dan juga pada WireShark memberikan fitur yang berupa Flow Graph, dimana kita dapat mengetahui apa yang dilakukan client selama menuju sever yang dituju walaupun sedikit susah untuk dimengerti.
2. Pada aplikasi VisualRoute informasi yang diberikan sedikit kurang detail sehingga sedikit sulit untuk dianalisa apa yang dilakukan client selama menuju server dan juga dikarenakan VisualRoute hanya menampilkan hope secara singkat, tidak semua hope yang dapat kita lihat didalamnya.