

Nama: Muhammad Nawwar Athalaza

NIM : 09011381621073

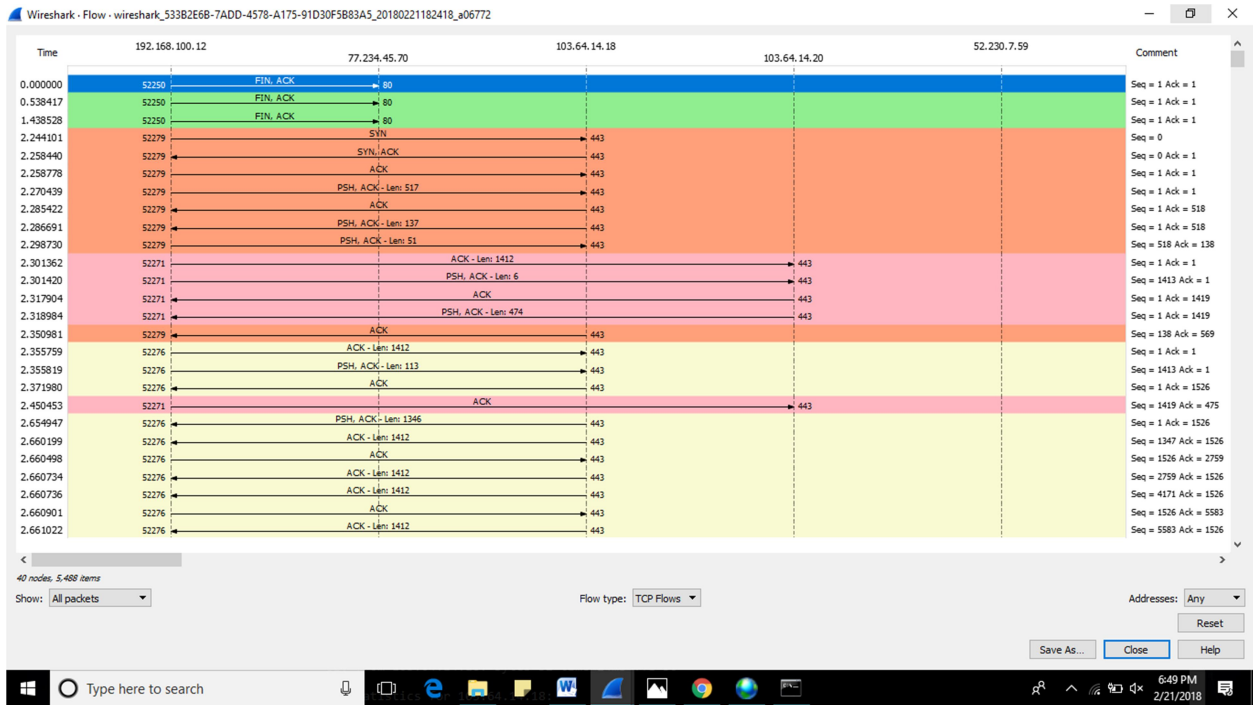
Flow Graph website komikid.com

ANALISIS WIRESHARK

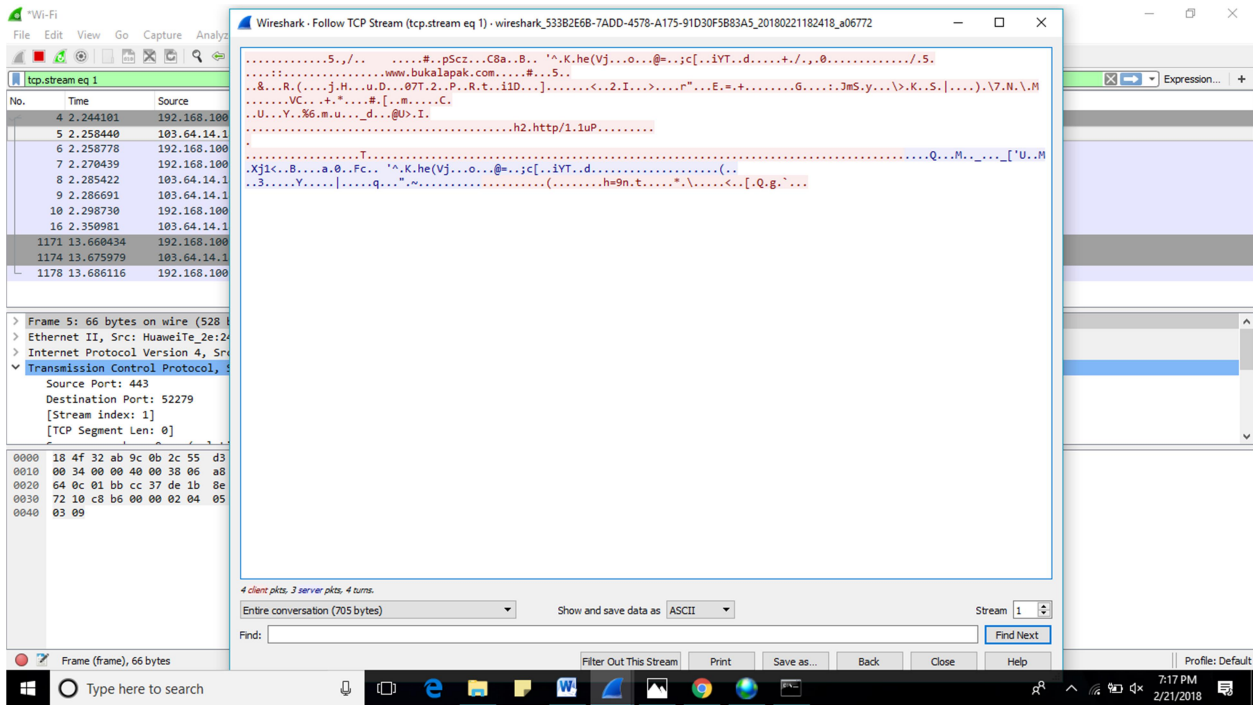
The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The traffic is between source IP 192.168.100.12 and destination IP 77.234.45.70. The capture shows a complete TLS handshake (SYN, ACK, Client Hello, Server Hello, Change Cipher Spec, Encrypted Handshake Message) followed by the transmission of encrypted application data (QUIC) and several TCP segments of reassembled PDUs. The status bar at the bottom indicates 8690 packets displayed (100.0%) and the system time is 6:41 PM on 2/21/2018.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.12	77.234.45.70	TCP	54	52250 → 80 [FIN, ACK] Seq=1 Ack=1 Win=67 Len=0
2	0.530417	192.168.100.12	77.234.45.70	TCP	54	[TCP Retransmission] 52250 → 80 [FIN, ACK] Seq=1 Ack=1 Win=67 Len=0
3	1.439326	192.168.100.12	77.234.45.70	TCP	54	[TCP Retransmission] 52250 → 80 [FIN, ACK] Seq=1 Ack=1 Win=67 Len=0
4	2.244101	192.168.100.12	103.64.14.18	TCP	66	52279 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	2.258440	103.64.14.18	192.168.100.12	TCP	66	443 → 52279 [SYN, ACK] Seq=0 Ack=1 Win=17408 Len=0 MSS=1412 SACK_PERM=1 WS=512
6	2.258778	192.168.100.12	103.64.14.18	TCP	54	52279 → 443 [ACK] Seq=1 Ack=1 Win=17408 Len=0
7	2.270439	192.168.100.12	103.64.14.18	TLV1.2	571	Client Hello
8	2.285422	103.64.14.18	192.168.100.12	TCP	54	443 → 52279 [ACK] Seq=1 Ack=518 Win=30720 Len=0
9	2.286691	103.64.14.18	192.168.100.12	TLV1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10	2.298730	192.168.100.12	103.64.14.18	TLV1.2	105	Change Cipher Spec, Encrypted Handshake Message
11	2.301362	192.168.100.12	103.64.14.20	TCP	1466	52271 → 443 [ACK] Seq=1 Ack=1 Win=65 Len=1412 [TCP segment of a reassembled PDU]
12	2.301420	192.168.100.12	103.64.14.20	TLV1.2	60	Application Data
13	2.304428	192.168.100.12	172.217.24.99	QUIC	191	Payload (Encrypted), PKN: 6, CID: 8788870903567751546
14	2.317904	103.64.14.20	192.168.100.12	TCP	56	443 → 52271 [ACK] Seq=1 Ack=1419 Win=71 Len=0
15	2.318984	103.64.14.20	192.168.100.12	TLV1.2	528	Application Data
16	2.350981	103.64.14.18	192.168.100.12	TCP	56	443 → 52279 [ACK] Seq=138 Ack=569 Win=30720 Len=0
17	2.355759	192.168.100.12	103.64.14.18	TCP	1466	52276 → 443 [ACK] Seq=1 Ack=1 Win=408 Len=1412 [TCP segment of a reassembled PDU]
18	2.355819	192.168.100.12	103.64.14.18	TLV1.2	167	Application Data
19	2.356092	172.217.24.99	192.168.100.12	QUIC	72	Payload (Encrypted), PKN: 6
20	2.371980	103.64.14.18	192.168.100.12	TCP	56	443 → 52276 [ACK] Seq=1 Ack=1526 Win=72 Len=0
21	2.411161	172.217.24.99	192.168.100.12	QUIC	308	Payload (Encrypted), PKN: 7
22	2.411353	172.217.24.99	192.168.100.12	QUIC	91	Payload (Encrypted), PKN: 8
23	2.411900	192.168.100.12	172.217.24.99	QUIC	83	Payload (Encrypted), PKN: 7, CID: 8788870903567751546
24	2.450453	192.168.100.12	103.64.14.20	TCP	54	52271 → 443 [ACK] Seq=1419 Ack=475 Win=63 Len=0
25	2.654947	103.64.14.18	192.168.100.12	TLV1.2	1400	Application Data
26	2.660199	103.64.14.18	192.168.100.12	TCP	1466	443 → 52276 [ACK] Seq=1347 Ack=1526 Win=72 Len=1412 [TCP segment of a reassembled PDU]
27	2.660498	192.168.100.12	103.64.14.18	TCP	54	52276 → 443 [ACK] Seq=1526 Ack=2759 Win=408 Len=0
28	2.660734	103.64.14.18	192.168.100.12	TCP	1466	443 → 52276 [ACK] Seq=2759 Ack=1526 Win=72 Len=1412 [TCP segment of a reassembled PDU]
29	2.660736	103.64.14.18	192.168.100.12	TCP	1466	443 → 52276 [ACK] Seq=4171 Ack=1526 Win=72 Len=1412 [TCP segment of a reassembled PDU]
30	2.660901	192.168.100.12	103.64.14.18	TCP	54	52276 → 443 [ACK] Seq=1526 Ack=5583 Win=408 Len=0
31	2.661022	103.64.14.18	192.168.100.12	TCP	1466	443 → 52276 [ACK] Seq=5583 Ack=1526 Win=72 Len=1412 [TCP segment of a reassembled PDU]
32	2.661024	103.64.14.18	192.168.100.12	TLV1.2	1173	Application Data
33	2.661161	103.64.14.18	192.168.100.12	TCP	54	52276 → 443 [ACK] Seq=1526 Ack=8114 Win=408 Len=0

1. Pada gambar di atas merupakan hasil capture dari app wireshark yang merupakan langkah demi langkah yang dilakukan oleh koneksi dengan TPC atau biasa disebut Transmission Control protocol yang bertujuan mentransfer data antara IP address. Website yang digunakan adalah buka lapak yang merupakan situs jual beli online.

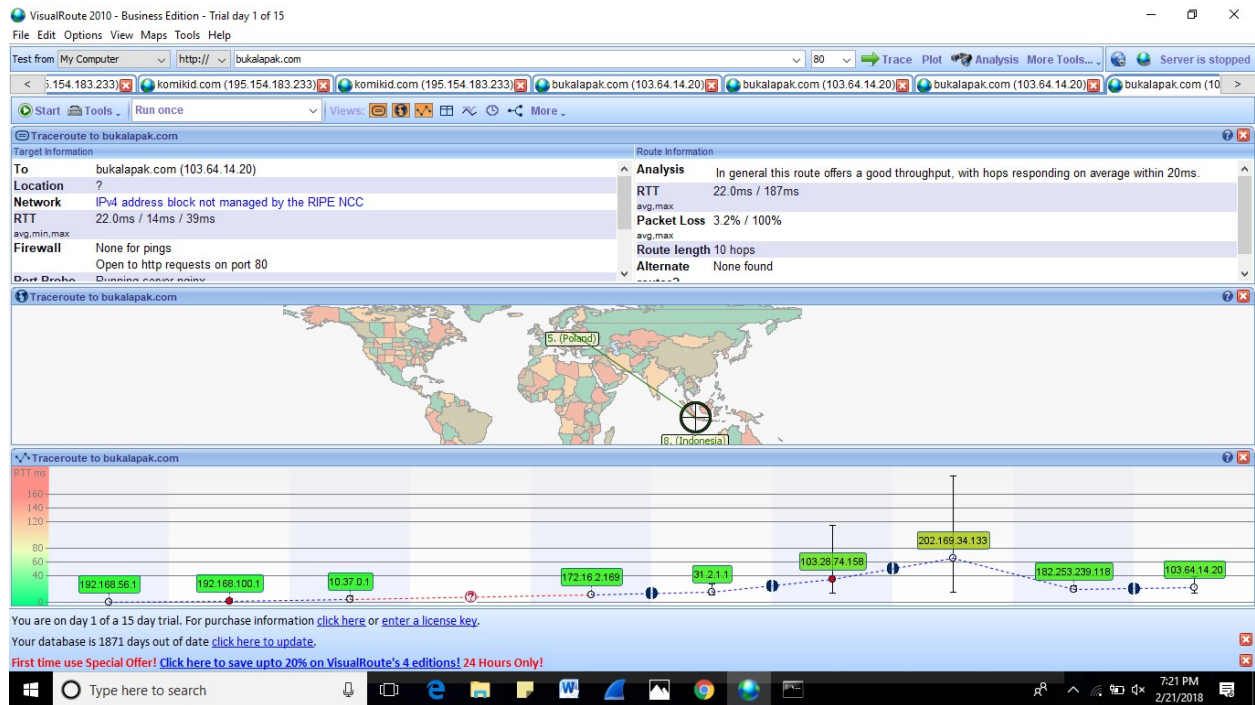


2. Lalu pada Flow Graph TPC tersebut, terdapat semua alur yang dilakukan oleh TPC untuk mentransfer data.
 1. line 1 dan 3 IP address komputer melakukan transfer data kepada menuju IP server dan mengakhiri koneksi.
 2. Pada line ke 4 IP source ingin memulai koneksi dengan IP website
 3. Pada line ke 5 IP website juga merespon dan menginginkan koneksi dengan IP source.
 4. Pada line ke 6 IP mengirimkan Octet yang diharapkan pada koneksi
 5. Pada line ke 7 IP source memberikan data dalam receive buffer dan tidak boleh kehilangan data ketika mengirimkan ke tujuan
 6. Pada line ke 8-9 IP website melakukan hal yang sama dengan IP source untuk mengirimkan data menuju source
 7. Pada line ke 10 source melakukan pengiriman lagi tetapi SEQ number menjadi tinggi karena urutan IP kita berubah.
 8. Pada line ke 11-14 IP source melakukan hal yang sama dengan satu website tetapi memiliki IP yang berbeda.

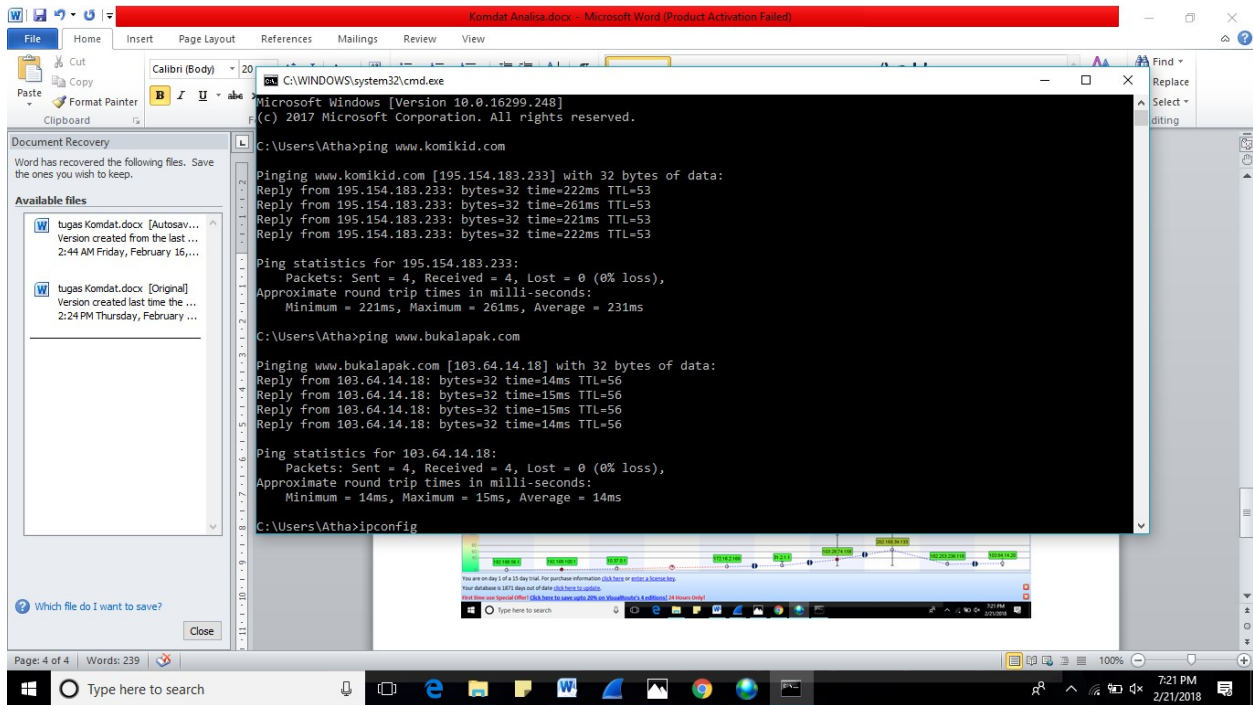


3. Gambar di atas merupakan Follow stream TCP dari Line 4 dimana proses bermulainya untuk mengirimkan data menuju IP tujuan. Tidak ada aktivitas peng-inputan data karena hanya mengakses website tersebut.

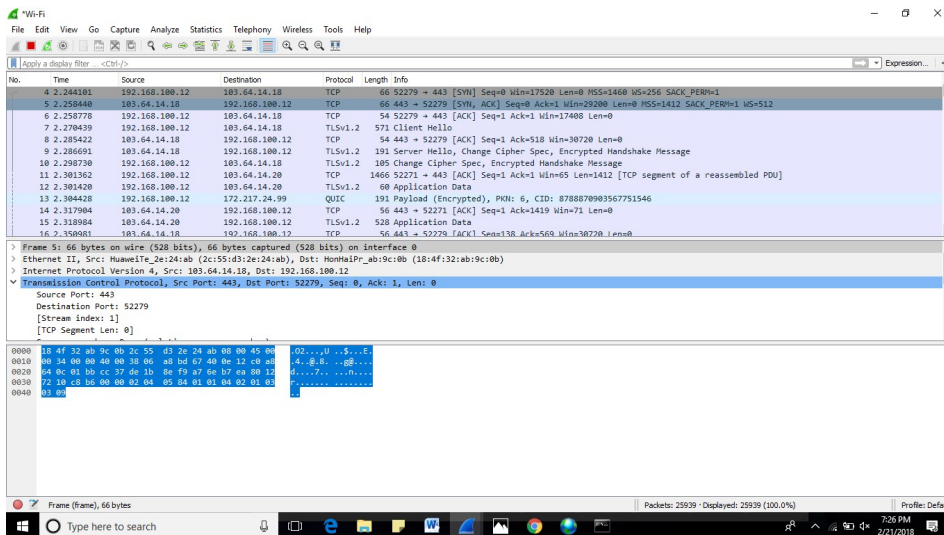
PERBANDINGAN WIRESHARK DAN VISUAL ROUTE



1. Pada Visual route IP website berbeda dengan wireshark, meskipun satu website dan IP yang mirip. Karena setiap mengakses website akan diberi IP yang berbeda untuk setiap orang. Tampilan alur IP pada visual route sangat simple hanya menampilkan langkah IP source menuju IP Server



2. Gambar diatas merupakan hasil mencari IP untuk website bukhalapak.com dan di dapatkan IP : 103.64.14.18 yang berbeda dengan wireshark.



3. Dan pada wireshark mendapatkan 2 IP tersebut, dan 2 IP tersebut melakukan hal yang sama untuk mengirimkan data menuju IP source.

Kesimpulan

1. Pembacaan IP wireshark dan visual route sedikit berbeda tetapi IP yang di dapatkan tetap IP website www.bukalapak.com.
2. Tampilan Visual Route sangat simple, sehingga user dengan mudah melihat langkah pengiriman data IP demi IP
3. Wireshark sangat detail menampilkan langkah pengambilan data dari server menuju IP source