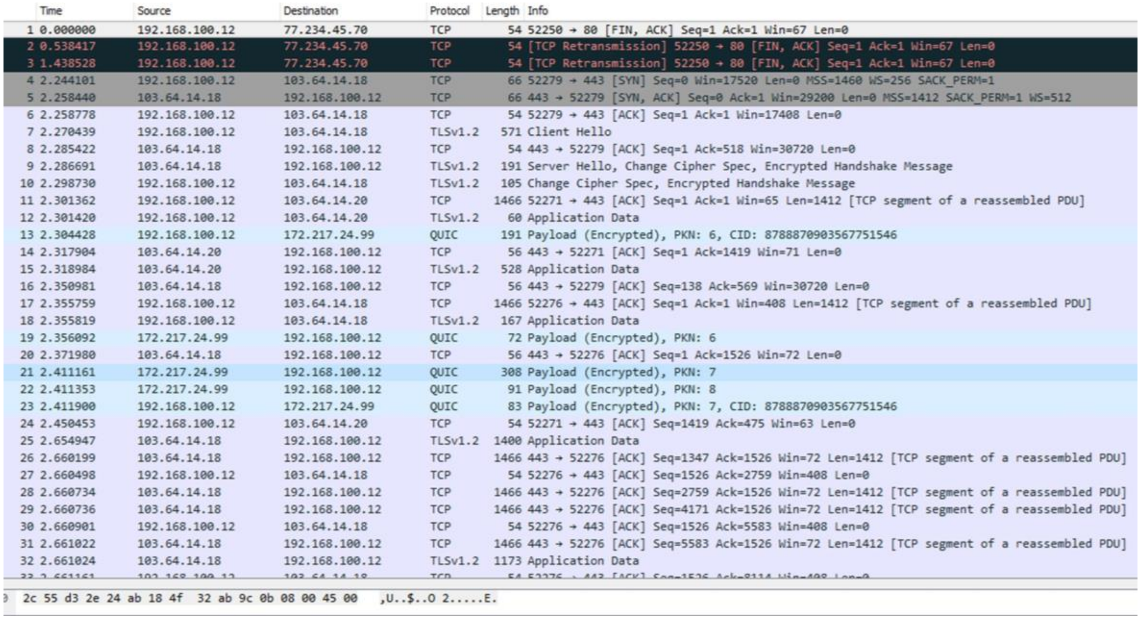
Nama: Muhammad Tamlikho

NIM : 09011281621031

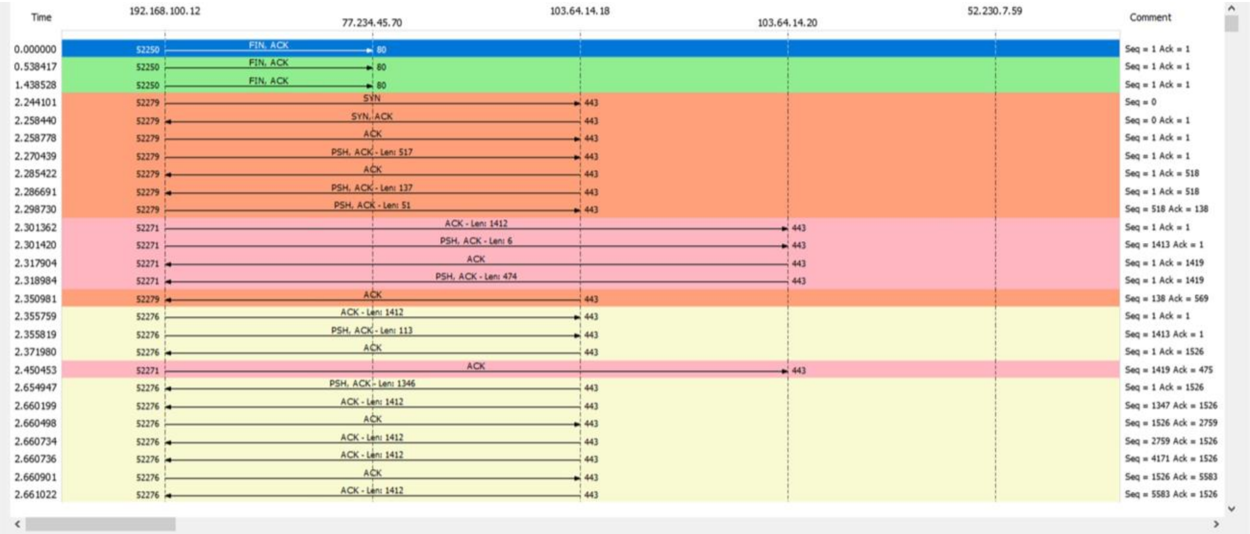
1. Analisis Wireshark



```
   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 0.538417  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 1.438528  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=29200 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     TLSv1.2   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   TLSv1.2   191 Server Hello, Change Cipher Spec, Encrypted Handshake Message
10 2.298730  192.168.100.12   103.64.14.18     TLSv1.2   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     TLSv1.2    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   TLSv1.2   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     TLSv1.2   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   TLSv1.2  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   TLSv1.2  1173 Application Data
33 2.661161  192.168.100.12   103.64.14.18     TCP        54 52276 → 443 [ACK] Seq=1526 Ack=8114 Win=408 Len=0

0  2c 55 d3 2e 24 ab 18 4f  32 ab 9c 0b 08 00 45 00   ,U..$..O 2.....E.
```

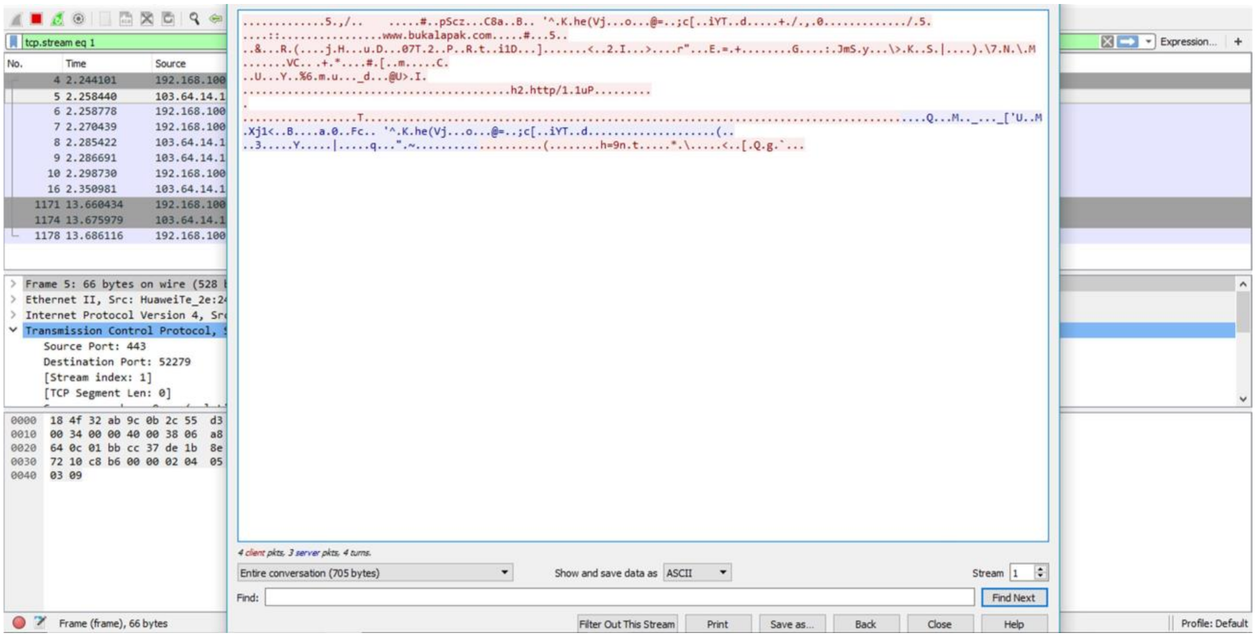
Gambar di atas merupakan hasil capture aplikasi wireshark yang dilakukan dengan TCP yang berfungsi untuk mentransfer data antara IP addres .



Time	192.168.100.12		77.234.45.70	103.64.14.18	103.64.14.20	52.230.7.59	Comment
0.000000	52250	FIN, ACK →	80				Seq = 1 Ack = 1
0.538417	52250	FIN, ACK →	80				Seq = 1 Ack = 1
1.438528	52250	FIN, ACK →	80				Seq = 1 Ack = 1
2.244101	52279	SYN →		443			Seq = 0
2.258440	52279	← SYN, ACK		443			Seq = 0 Ack = 1
2.258778	52279	ACK →		443			Seq = 1 Ack = 1
2.270439	52279	PSH, ACK - Len: 517 →		443			Seq = 1 Ack = 1
2.285422	52279	← ACK		443			Seq = 1 Ack = 518
2.286691	52279	← PSH, ACK - Len: 137		443			Seq = 1 Ack = 518
2.298730	52279	PSH, ACK - Len: 51 →		443			Seq = 518 Ack = 138
2.301362	52271	ACK - Len: 1412 →			443		Seq = 1 Ack = 1
2.301420	52271	PSH, ACK - Len: 6 →			443		Seq = 1413 Ack = 1
2.317904	52271	← ACK			443		Seq = 1 Ack = 1419
2.318984	52271	← PSH, ACK - Len: 474			443		Seq = 1 Ack = 1419
2.350981	52279	← ACK		443			Seq = 138 Ack = 569
2.355759	52276	ACK - Len: 1412 →		443			Seq = 1 Ack = 1
2.355819	52276	PSH, ACK - Len: 113 →		443			Seq = 1413 Ack = 1
2.371980	52276	← ACK		443			Seq = 1 Ack = 1526
2.450453	52271	ACK →			443		Seq = 1419 Ack = 475
2.654947	52276	← PSH, ACK - Len: 1346		443			Seq = 1 Ack = 1526
2.660199	52276	← ACK - Len: 1412		443			Seq = 1347 Ack = 1526
2.660498	52276	ACK →		443			Seq = 1526 Ack = 2759
2.660734	52276	← ACK - Len: 1412		443			Seq = 2759 Ack = 1526
2.660736	52276	← ACK - Len: 1412		443			Seq = 4171 Ack = 1526
2.660901	52276	ACK →		443			Seq = 1526 Ack = 5583
2.661022	52276	← ACK - Len: 1412		443			Seq = 5583 Ack = 1526

Pada Flow Graph TCP, terdapat semua alur yang dilakukan oleh TCP untuk mentransfer data.

1. Line 1 dan 3 -> IP addres komputer melakukan transfer data menuju IP server dan mengakhiri koneksi.
2. Line ke 4 -> IP source memulai koneksi dengan IP website.
3. Line ke 5 -> IP website mulai merespon dan menginginkan koneksi dengan IP source.
4. Line ke 6 -> IP mengirimkan Octet.
5. Line ke 7 -> IP source memberikan data dalam receive buffer.
6. Line ke 8 dan 9 -> IP website mengirimkan data menuju source.
7. Line ke 10 -> source melakukan pengiriman tetapi kali ini, SEQ number menjadi tinggi karena IP kita berubah.



tcp.stream eq 1

```
No.   Time        Source
   4 2.244101     192.168.100
   5 2.258440     103.64.14.1
   6 2.258778     192.168.100
   7 2.270439     192.168.100
   8 2.285422     103.64.14.1
   9 2.286691     103.64.14.1
  10 2.298730     192.168.100
  16 2.350981     103.64.14.1
1171 13.660434    192.168.100
1174 13.675979    103.64.14.1
1178 13.686116    192.168.100
```

```
> Frame 5: 66 bytes on wire (528 
> Ethernet II, Src: HuaweiTe_2e:2
> Internet Protocol Version 4, Sr
v Transmission Control Protocol, 
    Source Port: 443
    Destination Port: 52279
    [Stream index: 1]
    [TCP Segment Len: 0]
```

```
0000  18 4f 32 ab 9c 0b 2c 55  d3
0010  00 34 00 00 40 00 38 06  a8
0020  64 0c 01 bb cc 37 de 1b  8e
0030  72 10 c8 b6 00 00 02 04  05
0040  03 09
```

```
............5.,/..    .....#..pScz...C8a..B.. '^.K.he(Vj...o...@=..;c[..iYT..d.....+./.,.0............/.5.
....::................www.bukalapak.com.....#...5..
..&...R.(....j.H...u.D...07T.2..P..R.t..i1D...].......<..2.I...>....r"...E.=.+........G....:.JmS.y...\>.K..S.|....).\7.N.\.M
.......VC.. .+.*....#.[..m.....C.
..U...Y..%6.m.u..._d...@U>.I.
.....................................h2.http/1.1uP.........
.
.................T..................................................................................Q...M.._...._['U..M
.Xj1<..B....a.0..Fc.. '^.K.he(Vj...o...@=..;c[..iYT..d...................(..
..3.....Y.....|.....q...".~...........................(........h=9n.t.....*.\.....<..[.Q.g.`...
```

4 client pkts, 3 server pkts, 4 turns.

Entire conversation (705 bytes)

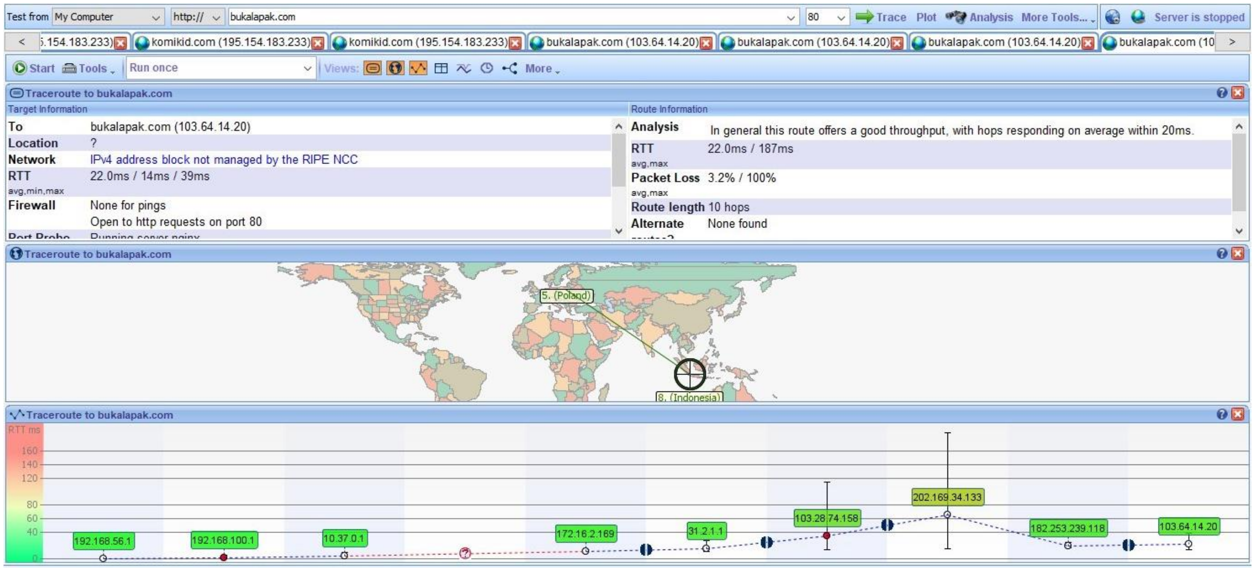
Show and save data as: ASCII

Stream: 1

Find:

Gambar di atas merupakan Follow stream TCP Line 4 dimana proses bermulainya untuk mengirimkan data menuju IP tujuan.

2. Perbandingan Wireshark dan Visual Route



To	bukalapak.com (103.64.14.20)
Location	?
Network	IPv4 address block not managed by the RIPE NCC
RTT avg,min,max	22.0ms / 14ms / 39ms
Firewall	None for pings Open to http requests on port 80
Port Probe	Running server nginx

Analysis	In general this route offers a good throughput, with hops responding on average within 20ms.
RTT avg,max	22.0ms / 187ms
Packet Loss avg,max	3.2% / 100%
Route length	10 hops
Alternate routes?	None found

IP website Visual Route berbeda dengan wireshark, meskipun satu website dan IP yang mirip. Karena setiap mengakses website akan diberi IP yang berbeda untuk setiap orang.