

**Visualisasi dan Analisis PCAP File Menggunakan Rumint  
2.4**

**(Tugas Mata Kuliah Jaringan Komputer)**



**Nama: Azwar Hidayat**

**NIM: 09011281520126**

**Kelas: SK 5 C**

**Jurusan Sistem Komputer**

**Fakultas Ilmu Komputer Universitas Sriwijaya**

**2017**

## Kasus 1

( [www. Kompas.com](http://www.Kompas.com) )

Sebagai kasus pertama, akan dilakukan tracing data packet dari source ke destination. Penjelajahan situs dilakukan selama 2 menit dan didapatkan hasil kurang lebih sebagai berikut. PCAP file nya didapatkan dari proses tracing menggunakan wireshark

Time	Source	Destination	Protocol	Length	Info
3 0.000132	192.168.0.100	202.70.49.168	TCP	54	51963 → 80 [ACK] Seq=1 A
5 0.000504	192.168.0.100	202.70.49.168	TCP	54	51963 → 80 [ACK] Seq=1 A
8 0.000919	192.168.0.100	202.70.49.168	TCP	54	51963 → 80 [ACK] Seq=1 A
11 2.001499	192.168.0.100	202.70.49.168	TCP	66	51963 → 80 [ACK] Seq=1 A
13 2.001774	192.168.0.100	202.70.49.168	TCP	54	51963 → 80 [ACK] Seq=1 A
14 2.533641	192.168.0.100	216.58.221.67	QUIC	190	Payload (Encrypted), PKN
15 2.724415	192.168.0.100	216.58.221.67	QUIC	81	Payload (Encrypted), PKN
17 2.728660	192.168.0.100	216.58.221.67	QUIC	77	Payload (Encrypted), PKN
18 2.730153	192.168.0.100	216.58.221.67	QUIC	190	Payload (Encrypted), PKN
19 2.961078	192.168.0.100	216.58.221.67	QUIC	81	Payload (Encrypted), PKN
20 2.963896	192.168.0.100	216.58.221.67	QUIC	191	Payload (Encrypted), PKN
23 2.997661	192.168.0.100	216.58.221.67	QUIC	80	Payload (Encrypted), PKN
24 3.205302	192.168.0.100	216.58.221.67	QUIC	81	Payload (Encrypted), PKN
25 3.207227	192.168.0.100	216.58.221.67	QUIC	192	Payload (Encrypted), PKN
28 3.234847	192.168.0.100	216.58.221.67	QUIC	80	Payload (Encrypted), PKN

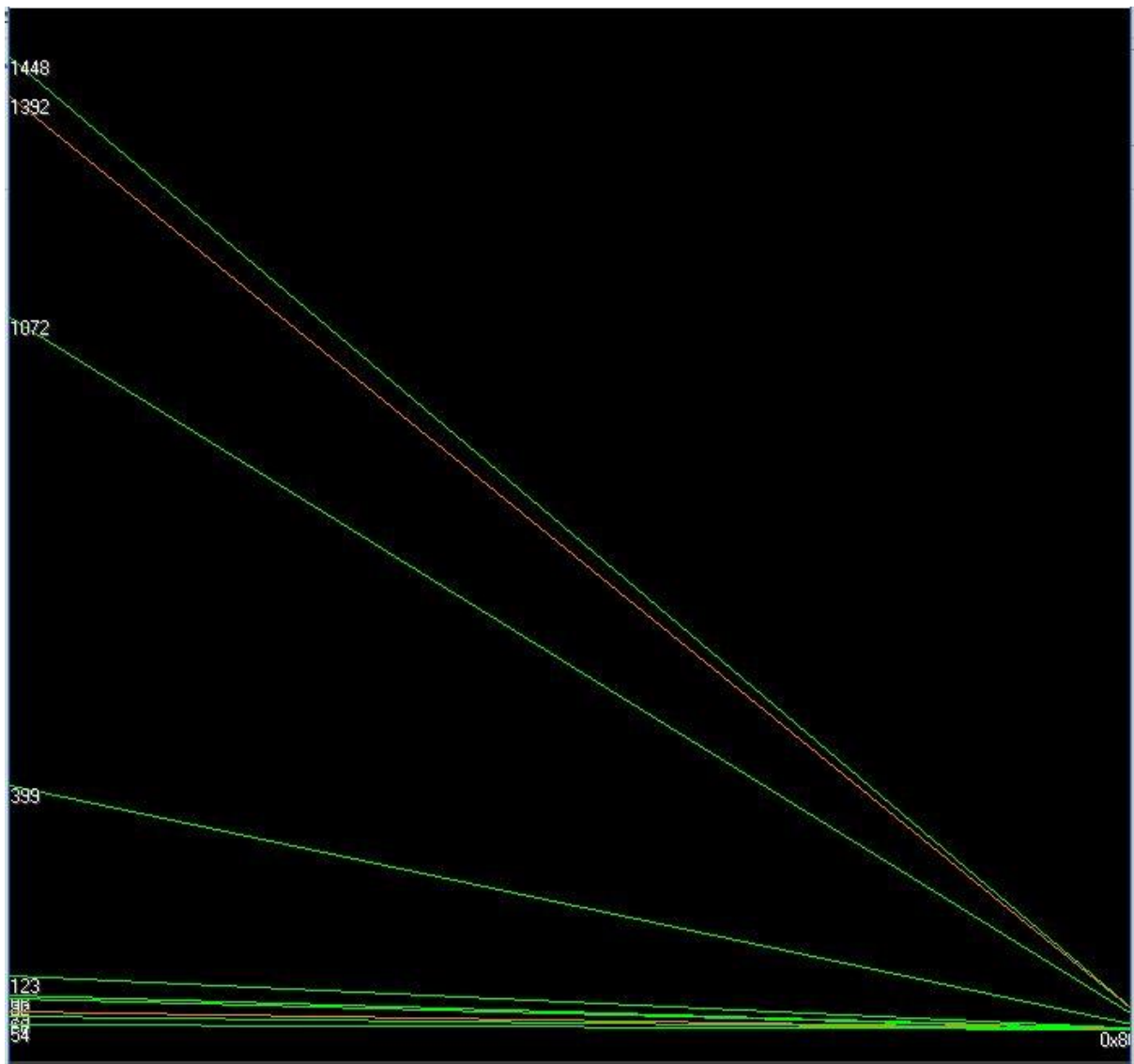
Gambar 1. Hasil Tracing Kompas.com menggunakan Wireshark[1]

Setelah di dapat data tadi kemudian file.pcap kemudian di load dan di visualisasikan menggunakan rumint.

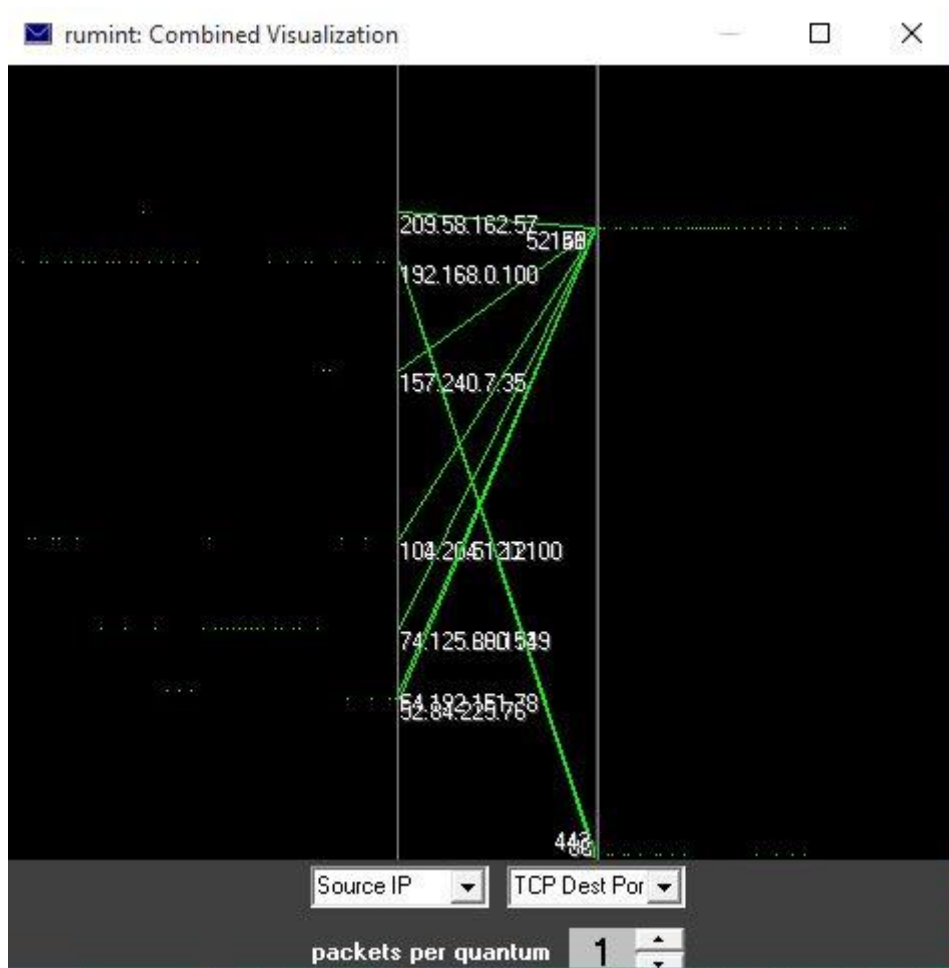


Gambar 2. Proses load file kompas.pcap ke rumint

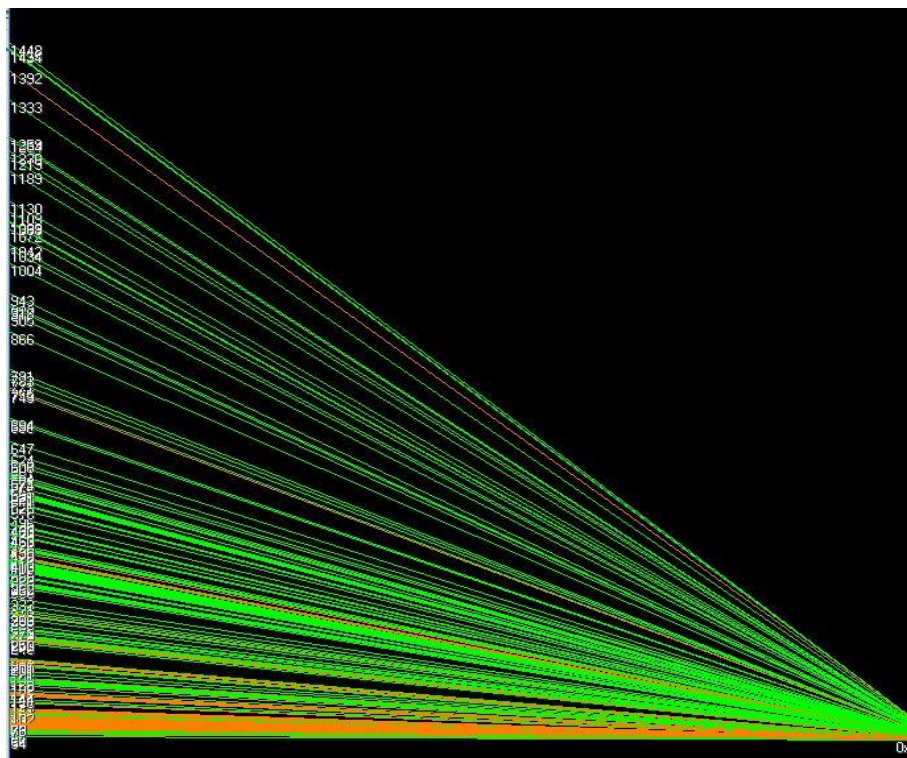
Pada aplikasi ini terlihat bahwa jumlah data yang terdapat di dalam file kompas.pcap itu sebanyak 10668 data dengan buffer 1 dan kecepatan transmisinya 10 packet/second.



Gambar 3. Bentuk visualisasi kompas.pcap kedalam bentuk pararel coordinat plot data ke 150



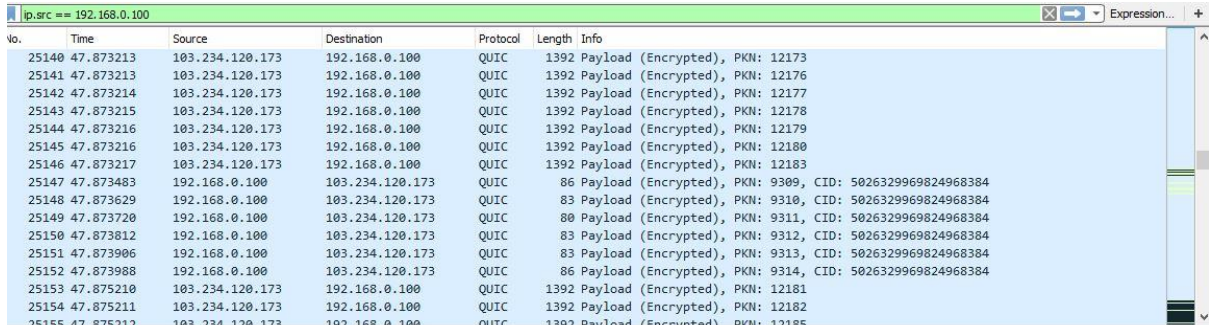
Gambar 4. Bentuk visualisasi kompas.pcap dalam transmisi data



Gambar 5. Bentuk visualisasi kompas.pcap kedalam bentuk pararel koordinat plot data 2000

## Kasus 2 : Streaming (live.tv.ub.ac.id)

Langkah yang dilakukan sama dengan kasus 1, namun bedanya adalah kali ini tracing dilakukan pada web online streaming. Pada kasus ini saya memilih UB TV live.



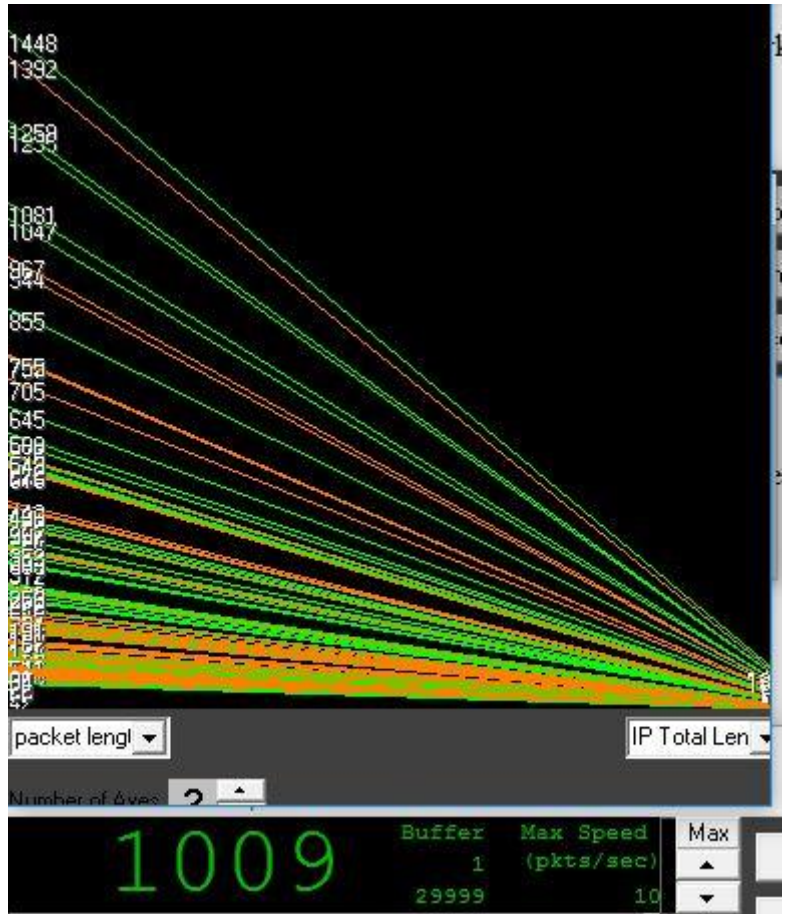
No.	Time	Source	Destination	Protocol	Length	Info
25140	47.873213	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12173
25141	47.873213	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12176
25142	47.873214	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12177
25143	47.873215	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12178
25144	47.873216	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12179
25145	47.873216	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12180
25146	47.873217	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12183
25147	47.873483	192.168.0.100	103.234.120.173	QUIC	86	Payload (Encrypted), PKN: 9309, CID: 5026329969824968384
25148	47.873629	192.168.0.100	103.234.120.173	QUIC	83	Payload (Encrypted), PKN: 9310, CID: 5026329969824968384
25149	47.873720	192.168.0.100	103.234.120.173	QUIC	80	Payload (Encrypted), PKN: 9311, CID: 5026329969824968384
25150	47.873812	192.168.0.100	103.234.120.173	QUIC	83	Payload (Encrypted), PKN: 9312, CID: 5026329969824968384
25151	47.873906	192.168.0.100	103.234.120.173	QUIC	83	Payload (Encrypted), PKN: 9313, CID: 5026329969824968384
25152	47.873988	192.168.0.100	103.234.120.173	QUIC	86	Payload (Encrypted), PKN: 9314, CID: 5026329969824968384
25153	47.875210	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12181
25154	47.875211	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12182
25155	47.875212	103.234.120.173	192.168.0.100	QUIC	1392	Payload (Encrypted), PKN: 12185

Gambar 6. Hasil Tracing data ubtv.pcap menggunakan wireshark[1]

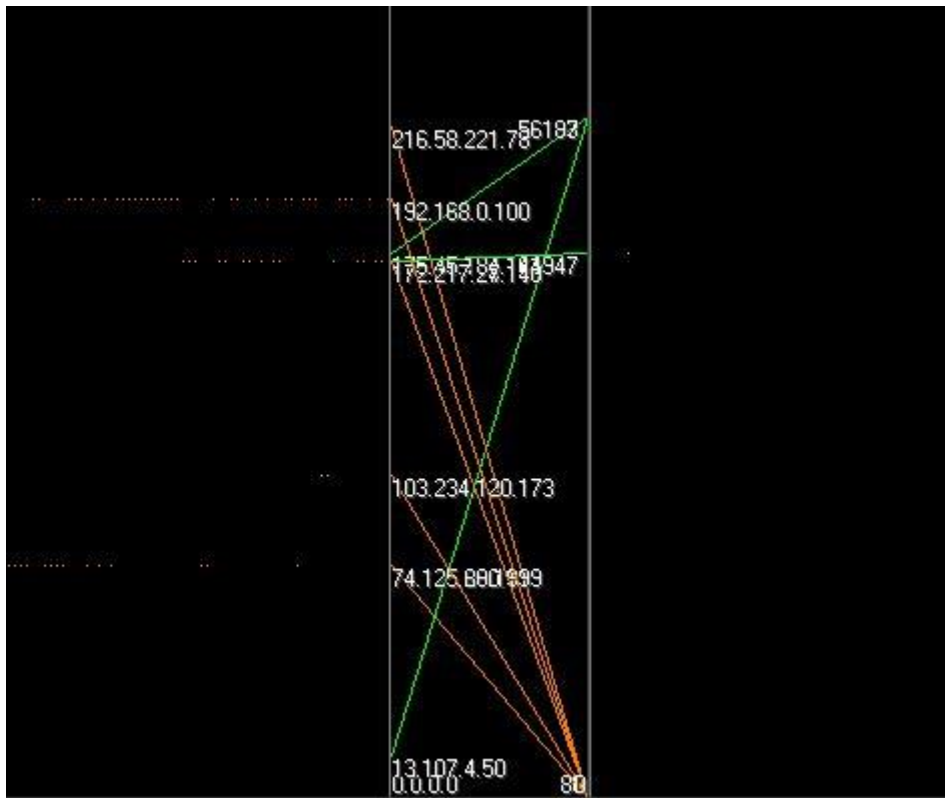


Gambar 7. Proses load file ubtvlive.pcap ke rumint

Terlihat pada aplikasi ini terbaca 30000 data dari ubtvlive.pcap. Hasil ini berbeda jauh dengan tracing pada kompas tadi yang hasil datanya hanya 10.000 data.



Gambar 8. Bentuk visualisasi ubtvlive.pcap ke dalam bentuk paralel koordinat plot data 1009



Gambar 9. Bentuk visualisasi ubtvlive.pcap dalam transmisi data

Analisa :

Dari perbandingan kedua visualisasi diatas, nampak bahwa streaming memiliki jumlah paket data yang lebih besar dibandingkan browsing seperti kompas.com. Ketika melakukan streaming maka jumlah paket data yang dikirim dari source ke destination juga besar dibandingkan proses browsing biasa. Terlihat juga pada gambar visualisasi tersebut beberapa IP address yang digunakan sebagai langkah untuk menemukan rute terbaik untuk transmisi agar data yang dikirim oleh source dapat diterima baik oleh penerima di destination.

## DAFTAR PUSTAKA

- [1] “Azwar Hidayat\_SK 5 C\_Tracer Jaringan dan Paket Data dengan Wireshark dan Netstat.pdf.” .
- [2] Goldstein,Max.2013.Large Packet Visualization.Tufts University.
- [3] Anonim. "2009.Visualisasi pcap dengan rumint.online : <http://rumint.org>. Diakses pada tanggal 3 september 2017