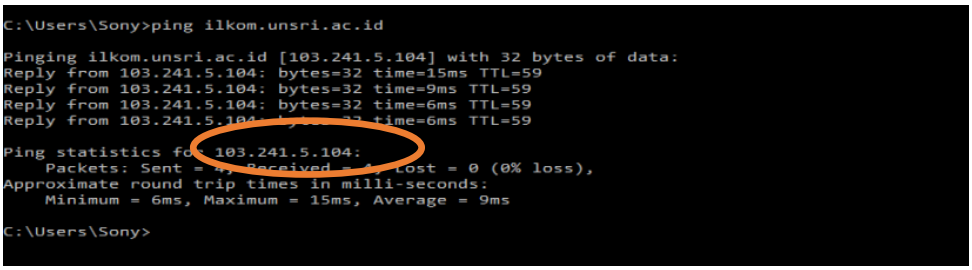
Nama : Ryan Darmawan Siregar
NIM : 09011381722091
Kelas : SK4A
MK : Komunikasi Data

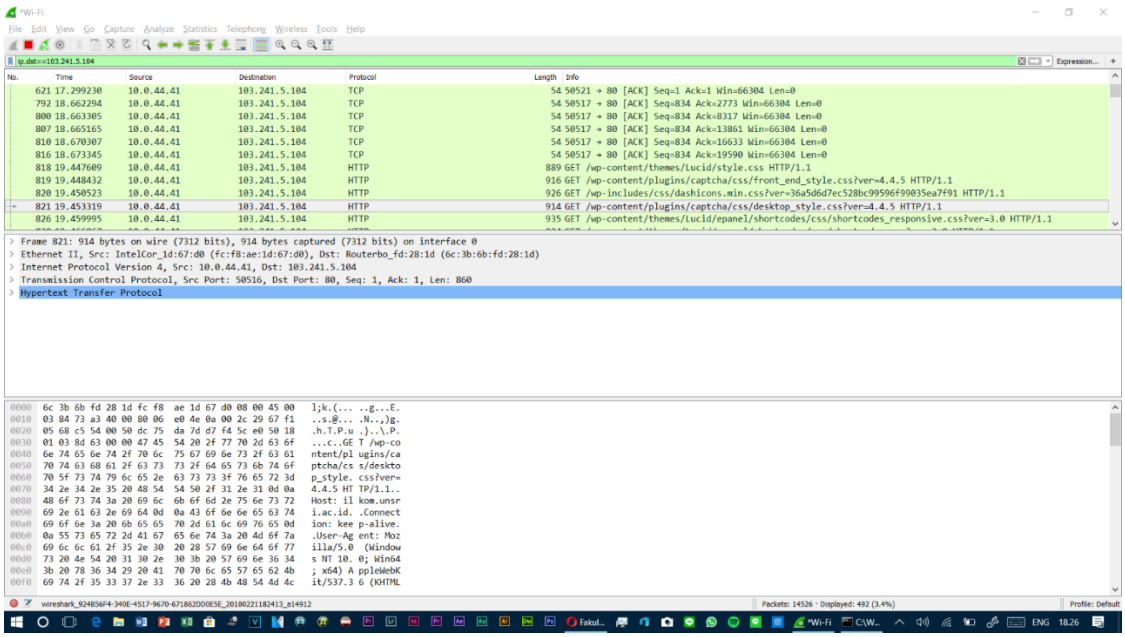
Analisis dan Perbandingan Paket Data di Aplikasi Wireshark, VisualRoute, dan Colasoft

1. Analisis Paket Wireshark

Pertama, buka aplikasi wireshark dan lakukan trace di jaringan wi-fi. Pada kasus ini saya menggunakan jaringan Unsri-Net yang berada di Fasilkom Unsri Bukit.
Setelah melakukan tracing, untuk melihat aktivitas data sebagai contoh akses data ke ilkom.unsri.ac.id pertama mengecek ip server dahulu, dengan menggunakan command prompt



Setelah dapat IP server ilkom.unsri.ac.id yakni 103.241.5.104, kemudian baru masukkan di wireshark yang sudah melakukan tracing dengan tulisan di kotak filter/pencarian yakni ip.dst==103.241.5.104



Kemudian pilih target, sebagai contoh target yang dipilih di wireshark yang berprotokol http, dikotak kedua pada gambar kedua (trace yang sudah di filter ke ip server ilkom) kemudian ada penjelasan segmen koneksi osi layer-nya sebagai berikut:

```
> Frame 821: 914 bytes on wire (7312 bits), 914 bytes captured (7312 bits) on interface 0
> Ethernet II, Src: IntelCor_1d:67:d0 (fc:f8:ae:1d:67:d0), Dst: Routerbo_fd:28:1d (6c:3b:6b:fd:28:1d)
> Internet Protocol Version 4, Src: 10.0.44.41, Dst: 103.241.5.104
> Transmission Control Protocol, Src Port: 50516, Dst Port: 80, Seq: 1, Ack: 1, Len: 860
> Hypertext Transfer Protocol
```

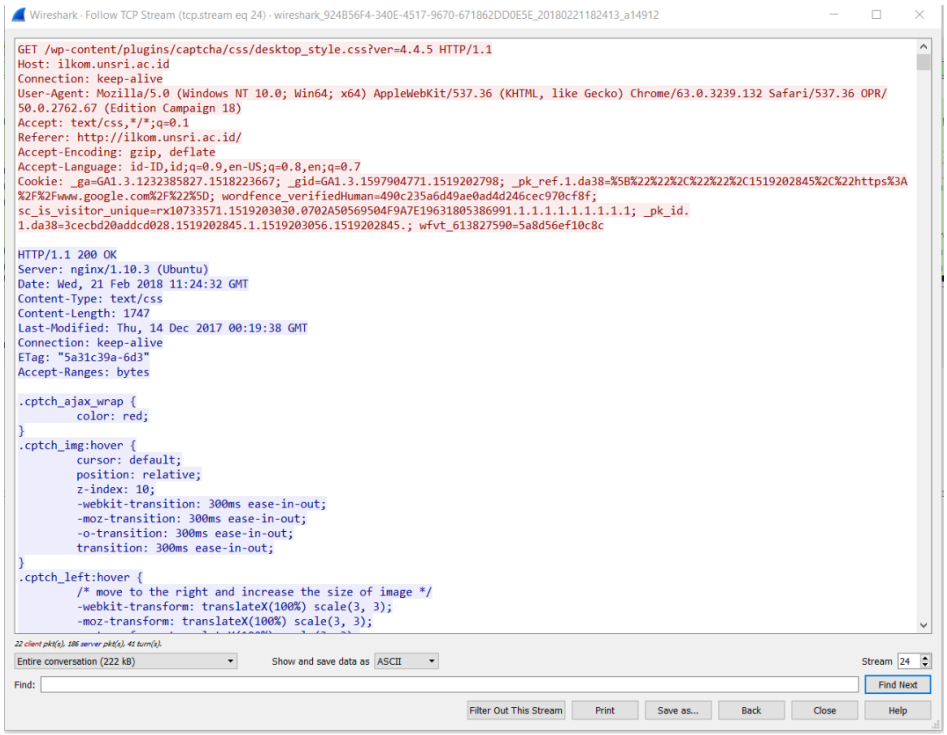
Pada baris pertama, terdapat penjelasan frame tersebut mengcapture sebanyak 914 byte. Pada baris kedua, terdapat keterangan router wifi dan adapter wifi yang terhubung ke source dan destinasi hingga alamat MAC Address.

Pada baris ketiga terdapat penjelasan protocol yang digunakan, yaitu IPv4 dengan source 10.0.44.41 dan destinasi 103.241.5.104 dimana ip source Adalah ip yang ada di laptop dan ip destinasi Adalah ip server ilkom.unsri.ac.id .

Pada baris keempat terdapat alamat port TCP (Transmission Control Protocol) dimana port source yakni 50516 dan port destinasi 80.

Pada baris kelima terdapat tipe protocol yang discan yakni HTTP (hypertext transfer protocol).

Kemudian dari target itu, lakukan TCP stream. Maka akan keluar hasil sebagai berikut



Penjelasan dari gambar diatas sebagai berikut

Pada baris pertama dijelaskan bahwa source berusa merequest untuk mendapatkan sebuah versi css/desktop.style yakni dengan versi 4.4.5 dan tipe http/1.1

Pada baris kedua, host yang dituju yakni ilkom.unsri.ac.id (destinasi).

Pada baris ketiga, diberi tahu bahwa koneksi masih aktif.

Pada baris keempat, dijelaskan bahwa pengguna diperkirakan menggunakan Mozilla versi 5.0 dengan operasi Windows x64 ataupun menggunakan Chrome ataupun Safari.

Pada baris ke delapan, file yang diakses berupa gzip.

Pada baris ke Sembilan yaitu pengaturan Bahasa, Bahasa yang diterima yakni Indonesia dan Inggris.

Pada bari kesepuluh terdapat bahwa server menerapkan cookie.

Digambar kedua penjelasan sebagai berikut:

Pada baris pertama, versi web yang digunakan http/1.1.

Pada baris kedua, server destinasi menggunakan nginx versi 1.10.3 berbasis Ubuntu.

Pada baris ketiga terdapat jam server.

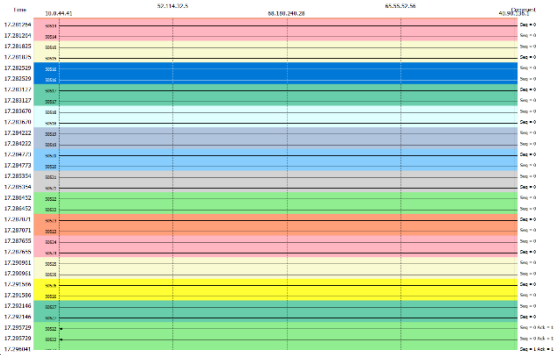
Pada baris keempat dijelaskan data yang diakses berupa text/css

Pada baris keenam diberitahu tanggal server diperbaruhi yakni 14 Desember 2017.

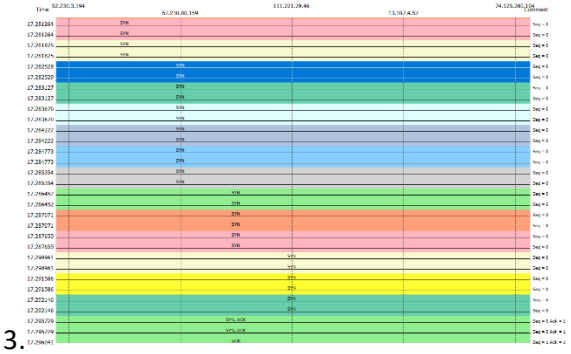
Pada baris ketujuh dinyatakan bahwa koneksi sedang aktif.

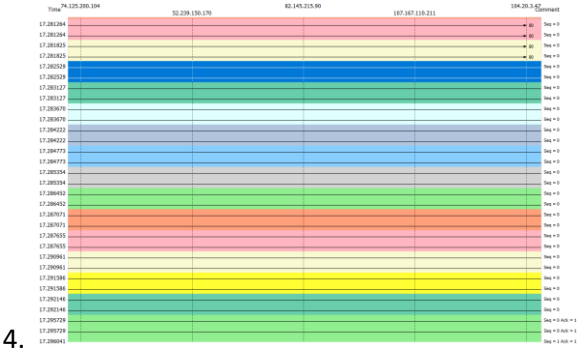
2. Analisis Paket Yang Ada di Nomor 1 pada bagian FlowGraph

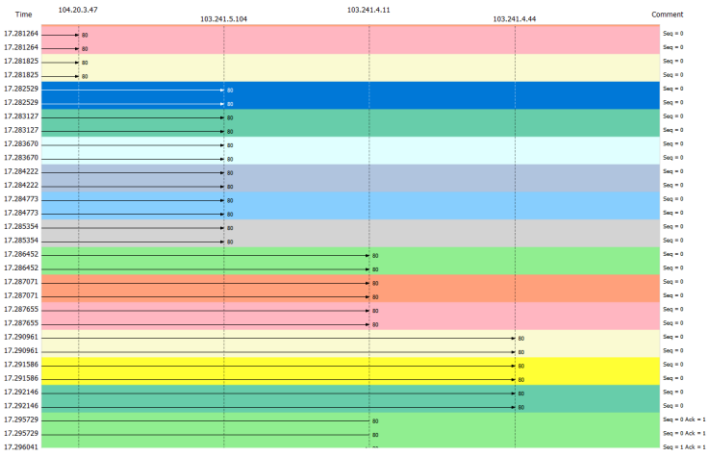
Pada aplikasi wireshark, terdapat sebuah fungsi aplikasi, dimana dapat menunjukan sebuah paket data dikirimkan ke IP mana saja atau yang biasa dikenal IP tersebut melakukan *handshake* kemana saja. Pada aplikasi wireshark, IP terdapat di bagian paling atas dan bagian panah merupakan alur komunikasi datanya. Pada kasus ini, IP yang difokuskan yakni pada ip source dan IP destination.Gambar sebagai berikut:

1.


2.


3.


4.


5.


Dari data di atas, dapat disimpulkan bahwa koneksi antara IP Source ke IP Destination memiliki sambungan IP dengan penjelasan sebagai berikut:

No.	ALAMAT IP	KETERANGAN
1.	10.0.44.41	IP Source
2.	52.114.32.5	N/A
3.	68.180.240.28	
4.	65.55.52.56	
5.	40.90.136.1	
6.	204.79.197.213	
7.	184.27.18.158	
8.	52.230.3.194	
9.	52.230.80.159	
10.	111.221.29.46	
11.	13.107.4.52	
12.	74.125.200.104	
13.	52.239.150.170	
14.	82.145.215.90	
15.	107.167.110.211	
16.	104.20.3.47	
17.	103.241.5.104	IP Destination

Sebelum IP Source terhubung ke IP Destination, maka antara kedua IP tersebut harus melewati beberapa IP lainnya yang ada di Router yang menghubungkan keduanya.

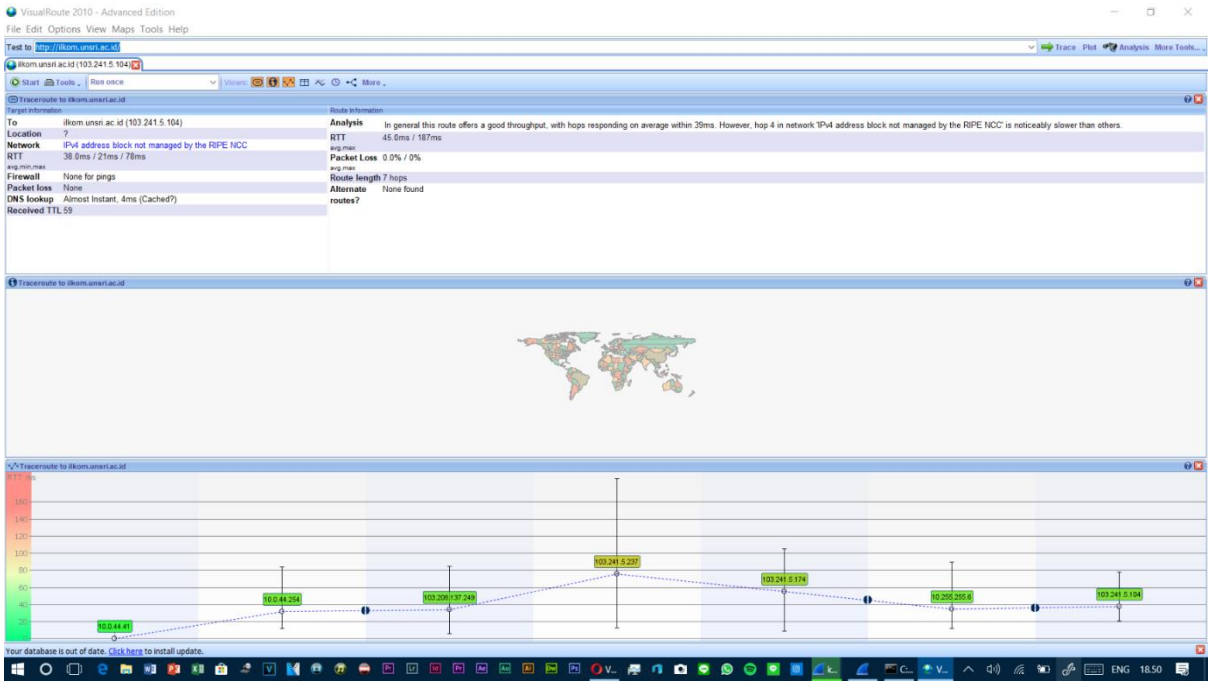
Di Flowgraph juga terdapat keterangan lain seperti port yang digunakan antara Ip Source dan IP Destination.

Contoh kasus yang diambil dari gambar yang berada pada urutan waktu ke-17.296775 dimana IP Destination mengirim Packet ke IP Source berupa “SYN-ACK” dimana packet ini berada pada urutan 608 pada flowgraph trace tersebut.

Tetapi data diatas belum bisa dikatakan sebagai hops dikarenakan data terdapat kejanggalan pada soal nomor 3 dengan visualroute, sehingga kemungkinan IP tersebut Adalah daftar Riwayat sambungan yang ada di jaringan yang disusun secara satu persatu berdasarkan waktu sambungan.

3. Analisis Paket Flowgraph Wireshark dengan VisualRoute

Pada soal sebelumnya, telah dibahas flowgraph yang ada di wireshark. Perbandfngan kali ini akan menggunakan visualroute sebagai data perbandingan. Data sebagai berikut:

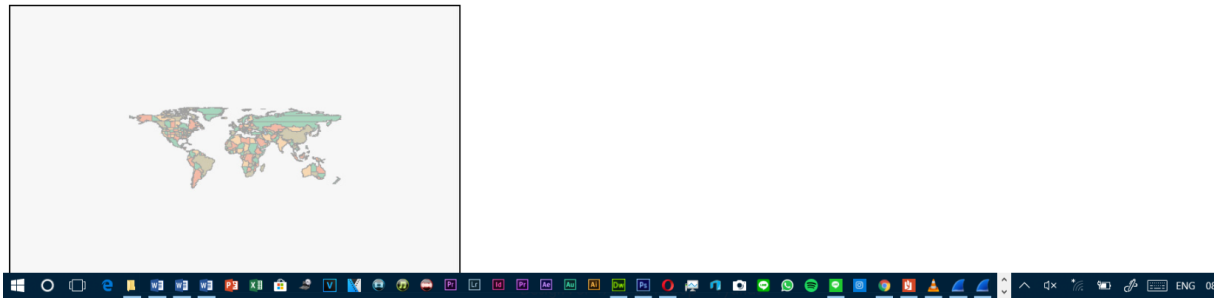


Pada VisualRoute, dilakukan trace ke server ilkom.unsri.ac.id dimana dari aplikasi VisualRoute ditemukan bahwa hanya terdapat 7hops untuk terhubung antara IP Source dengan IP Destination. Penjelasan detail apa saja hops-nya sebagai berikut:

Traceroute to ilkom.unsri.ac.id

This trace was started on Feb 21, 2018 6:37:58 PM. The host 'ilkom.unsri.ac.id' (known as ip-103-241-5-104.unsri.ac.id) has been found, and is reachable in 8 hops. The TTL value of packets received from it is 59.
In general this route offers a good throughput, with hops responding on average within 39ms. However, hop 4 in network 'IPv4 address block not managed by the RIPE NCC' is noticeably slower than others. The DNS lookup was completed almost instantaneously (less than 2ms - this may be the result of caching).

Hops	Loss	IP	Name	Location	Tzone	Avg ms	Min ms	Max ms	Network
0	0	10.0.44.41	VAIO	-	-	0.0	0	0	[Local Network]
1	0	10.0.44.254	-	-	-	32.0	12	84	[Local Network]
2	0	103.208.137.249	ip-103-208-137-249.unsri.ac.id	-	-	34.0	6	85	IPv4 address block not managed by the RIPE NCC
3	0	103.241.5.237	ip-103-241-5-237.unsri.ac.id	-	-	76.0	13	187	IPv4 address block not managed by the RIPE NCC
4	0	103.241.5.174	ilkom-idl.unsri.ac.id	-	-	55.0	9	105	IPv4 address block not managed by the RIPE NCC
5	0	10.255.255.6	-	-	-	35.0	12	90	[Local Network]
6	0	103.241.5.104	ilkom.unsri.ac.id	-	-	38.0	21	78	IPv4 address block not managed by the RIPE NCC



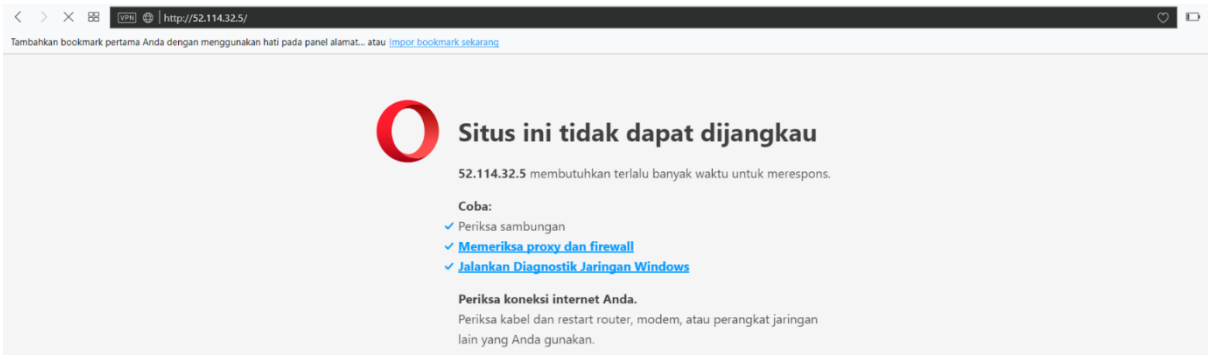
Terdapat penjelasan dimana lokasi server yang tidak diketahui, dan jika dibandingkan dengan aplikasi wireshark terhadap IP hops-nya, maka data tersebut terdapat kejanggalan dimana pada flowgraph wireshark terdapat 17sambungan IP, sedangkan visualroute terdapat 7sambungan IP yang mana jika kita komparasi antara kedua hasil tersebut Adalah sebagai berikut:

No.	ALAMAT IP (WIRESHARK)	KETERANGAN	ALAMAT IP (VISUAL ROUTE)	KETERANGAN
1.	10.0.44.41	IP Source	10.0.44.41	[LOCAL NETWORK] IP SOURCE HOPS 1
2.	52.114.32.5	N/A	10.0.44.254	HOPS 2
3.	68.180.240.28			
4.	65.55.52.56			
5.	40.90.136.1		103.208.137.249	HOPS 3
6.	204.79.197.213			
7.	184.27.18.158			
8.	52.230.3.194		103.241.5.237	HOPS 4
9.	52.230.80.159			
10.	111.221.29.46			
11.	13.107.4.52		103.241.5.174	HOPS 5
12.	74.125.200.104			
13.	52.239.150.170			
14.	82.145.215.90		10.255.255.6	HOPS 6
15.	107.167.110.211			
16.	104.20.3.47			
17.	103.241.5.104	IP Destination	10.241.5.104	[LOCAL NETWORK] IP DESTINATION HOPS 7

Maka dari data diatas dapat dipastikan bahwa hipotesis dari data ke-2 benar, dikarenakan 17 IP yang ada di wireshark, merupakan IP riwayat dari proses trace di wireshark yang diurutkan secara waktu interval kapan terhubungnya, dan data ini juga membuktikan bahwa setiap sambungan IP untuk mengirimkan data, tidak dapat secara bersamaan, melainkan secara satu persatu dimana delay-nya hanya hitungan millisecond (ms).
Yang menariknya Adalah beberapa sambungan IP terdapat ke akses server lain seperti ip wireshark nomor 12 yang ternyata Adalah IP ke server google. Kemudian terdapat peringatan bahwa Akses ditolak di IP wireshark nomor 10 dimana kemungkinan ke jaringan yang sangat vital, hal ini juga terdapat di beberapa IP server lainnya akan tetapi peringatan yang muncul tidak seperti yang ada pada IP nomor 12. Ada juga pada IP di nomor 15, dimana jika diakses terdapat sambutan bahwa berhasil ke server nginx dimana server tersebut berbasis ubuntu. Dan pada IP nomor 16, terdapat peringatan yang mirip dengan IP 12 dan pada hal ini terdapat keterangan lebih detail dimana akses ditolak dan server merupakan bagian dari cloudflare.

Berikut screenshoot dari akses ke IP 2~6

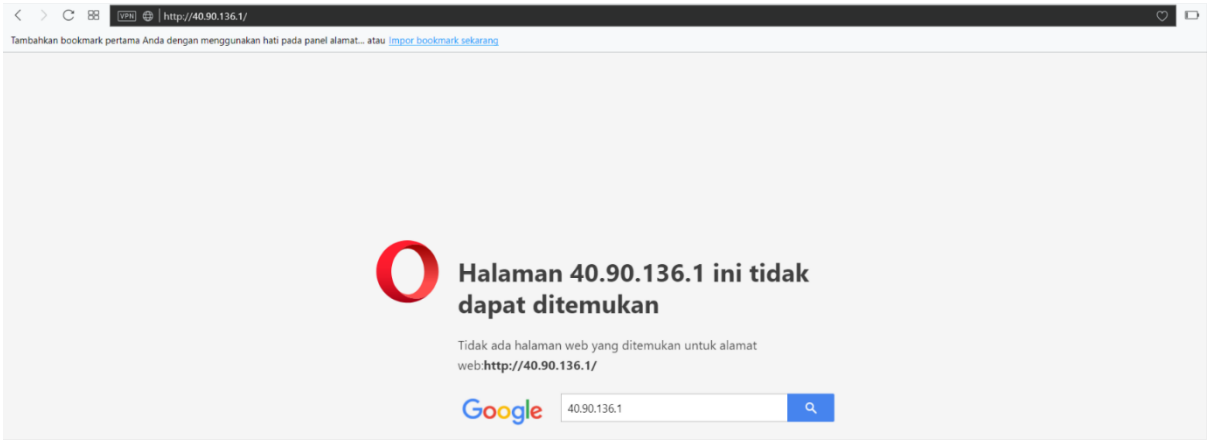
2. 52.114.32.5



3. 68.180.240.28

4. 65.55.52.56

5. 40.90.136.1



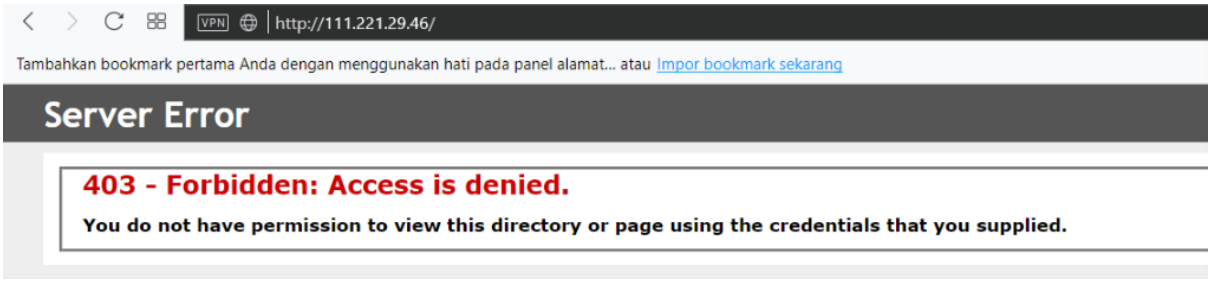
6. 204.79.197.213

7. 184.27.18.158

8. 52.230.3.194

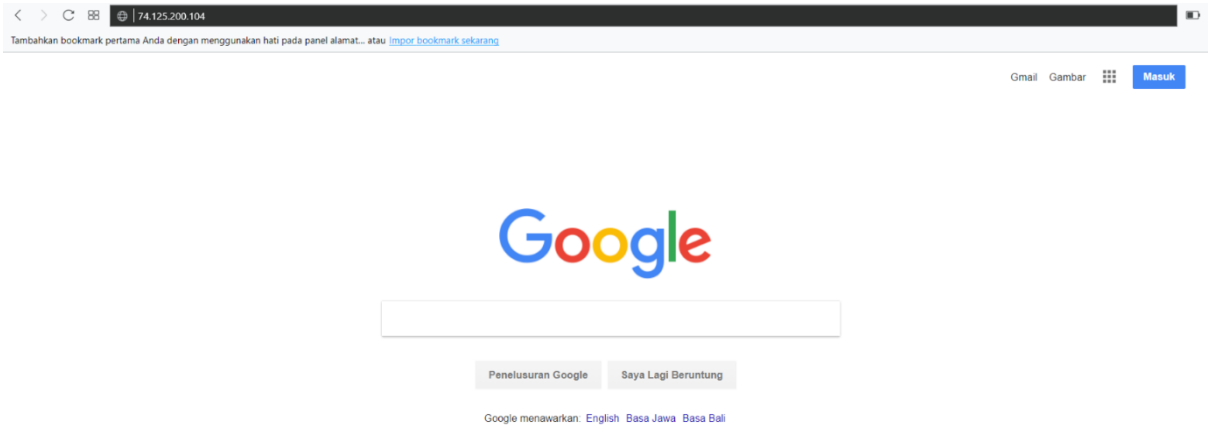
9. 52.230.80.159

10. 111.221.29.46



11. 13.107.4.52

12. 74.125.200.104

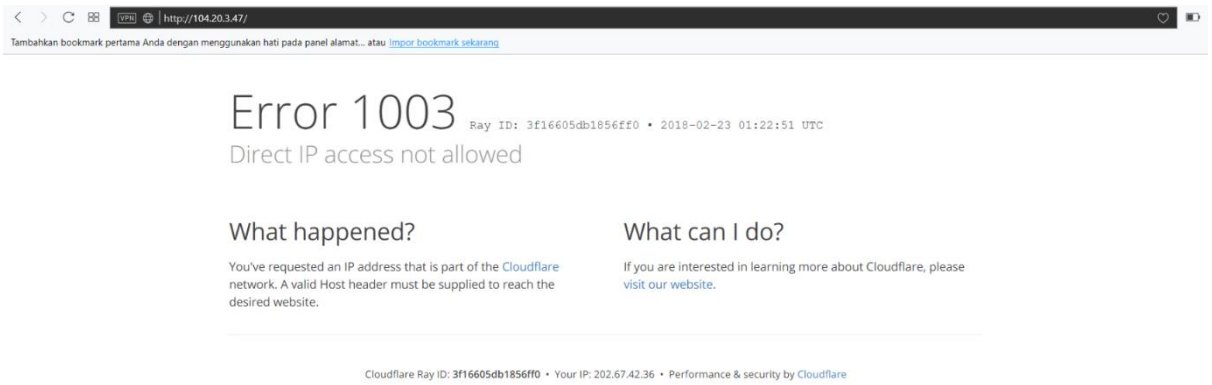


13. 52.239.150.170

14. 82.145.215.90

15. 107.167.110.211

16. 104.20.3.47

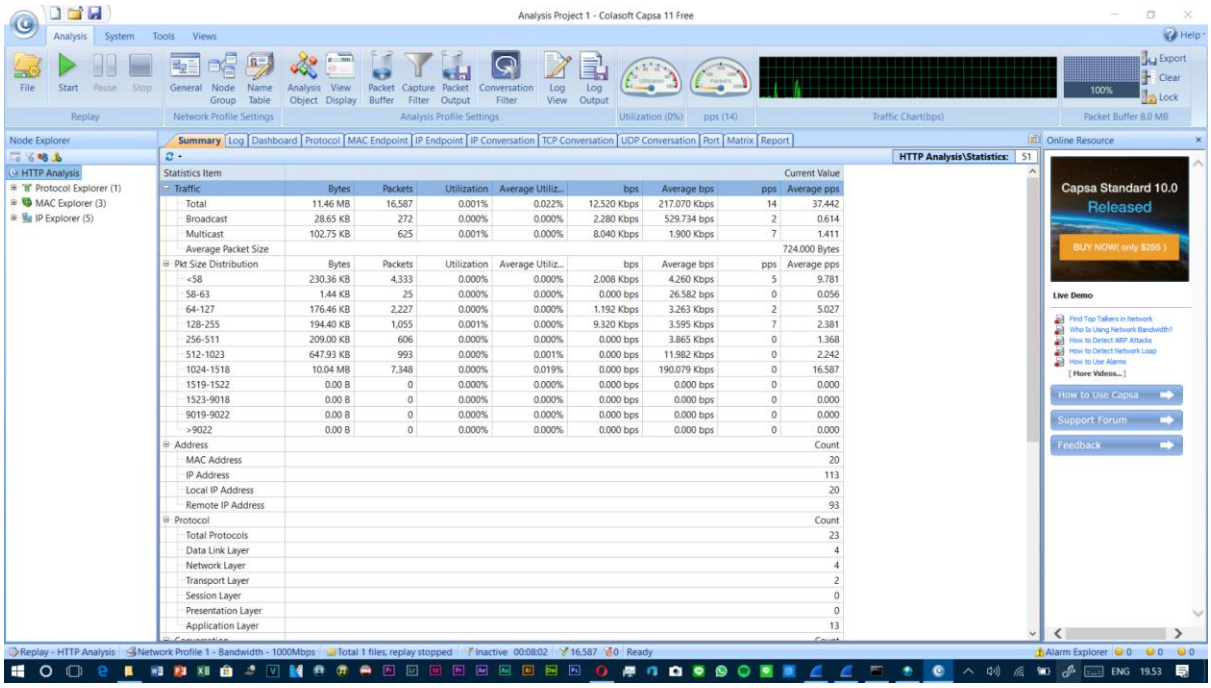


Ini menandakan jika sambungan IP pada wireshark tidak dapat disamakan dengan IP yang didapat di visualroute, karena pada wireshark, flowgraph tersebut merupakan hasil scan jaringan di router yang sama, yang berarti IP 2~16 merupakan akses pengguna lain di jaringan router tersebut. Sedangkan visualroute digunakan untuk melakukan tracing antara IP Source ke IP Destination untuk melihat banyaknya hops.

4. **Membaca Hasil Paket Data pada Nomor Satu dengan Menggunakan Aplikasi Colasoft Capsa**

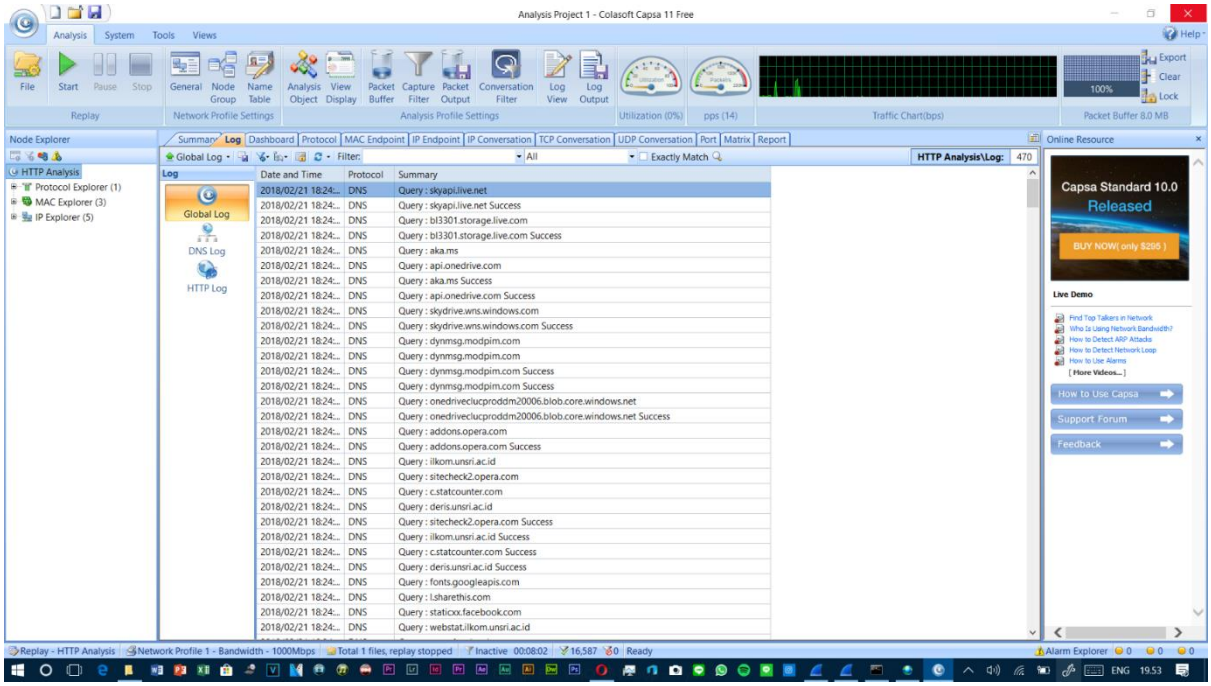
Setelah nomor satu tadi selesai dijalankan, maka yang dilakukan Adalah memberhentikan tracing dan menyimpan file tersebut ke format “pcap”. Kemudian dibuka di aplikasi colasoft yang akan mendapatkan hasil dalam beberapa bentuk, yakni:

1. **Summary**



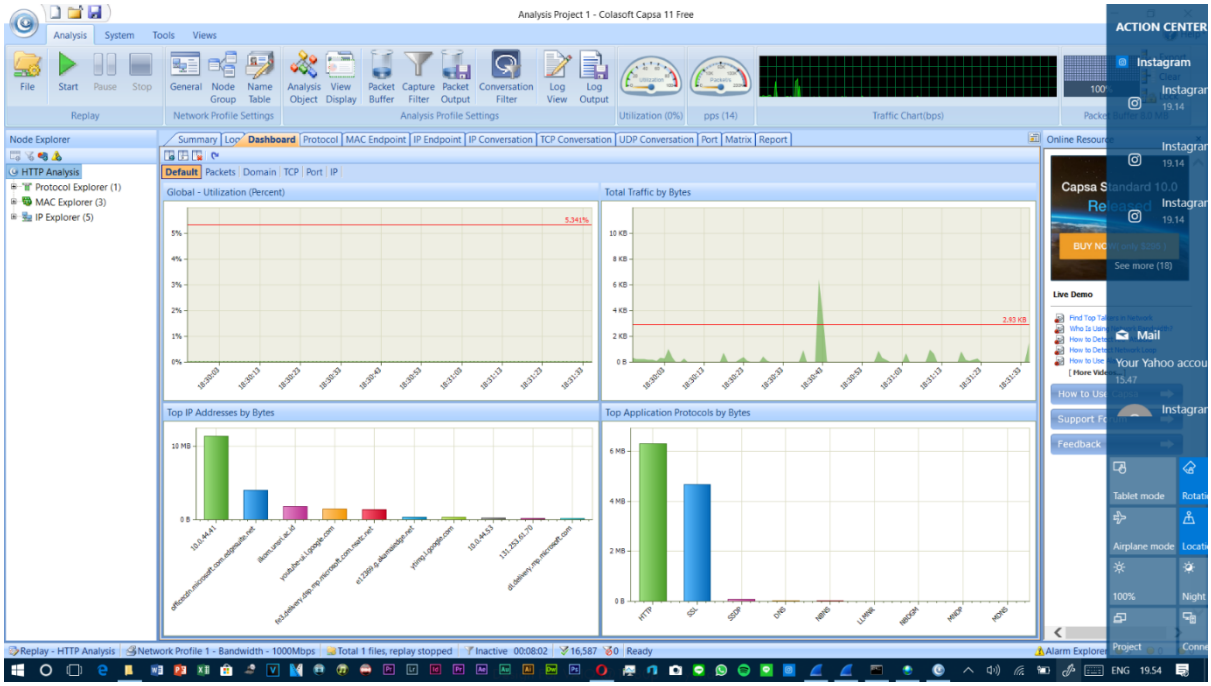
Hasil dari summary yang didapat yakni: Data yang berhasil di trace di wireshark sebelumnya yaitu sebesar 11,46 MB dengan total packet sebanyak 16.587.

2. **Log**



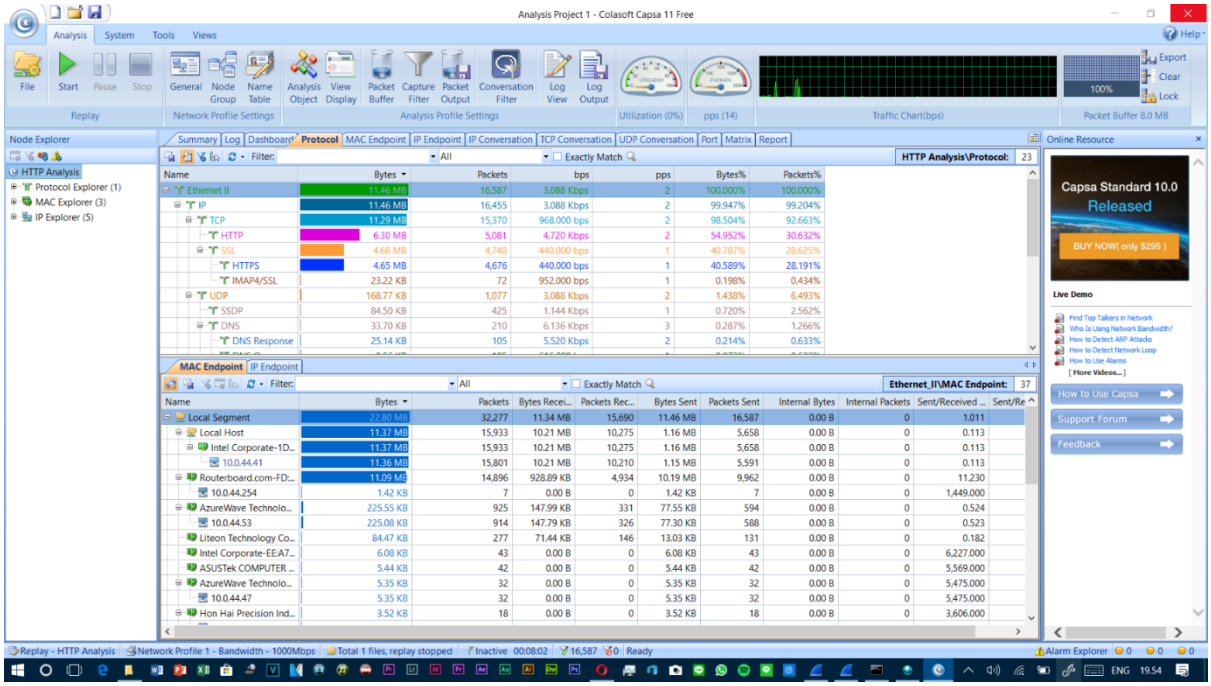
Dari data diatas, terdapat banyak data pencarian, yang sebelumnya teracak di wireshark, dan dapat kita ketahui bahwa ilkom.unsri.ac.id ada di riwayat berdasarkan gambar tersebut terletak pada baris ke-19

3. Dashboard



Di bagian dashboard, dapat dilihat jika bahwa akses ke server ilkom memakan lebih dari ¼ dari 10 MB, dengan akses data tertinggi pada IP Source. Tampak juga pada grafik di kanan server ilkom menggunakan tipe aplikasi protocol berbasis SSDP.

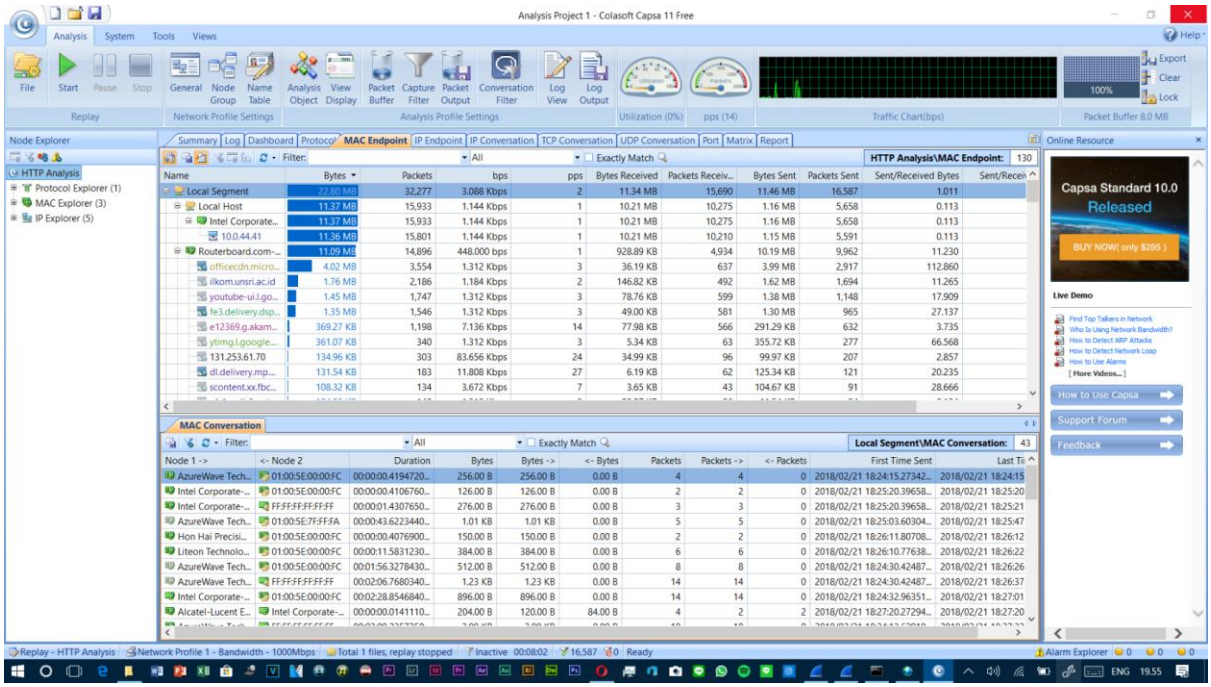
4. Protocol



Pada bagian protocol grafik atas (HTTP Analysis) tercatat berapa jumlah bytes, packets, bps, pps, dan persentasi terhadap bytes dan packets.

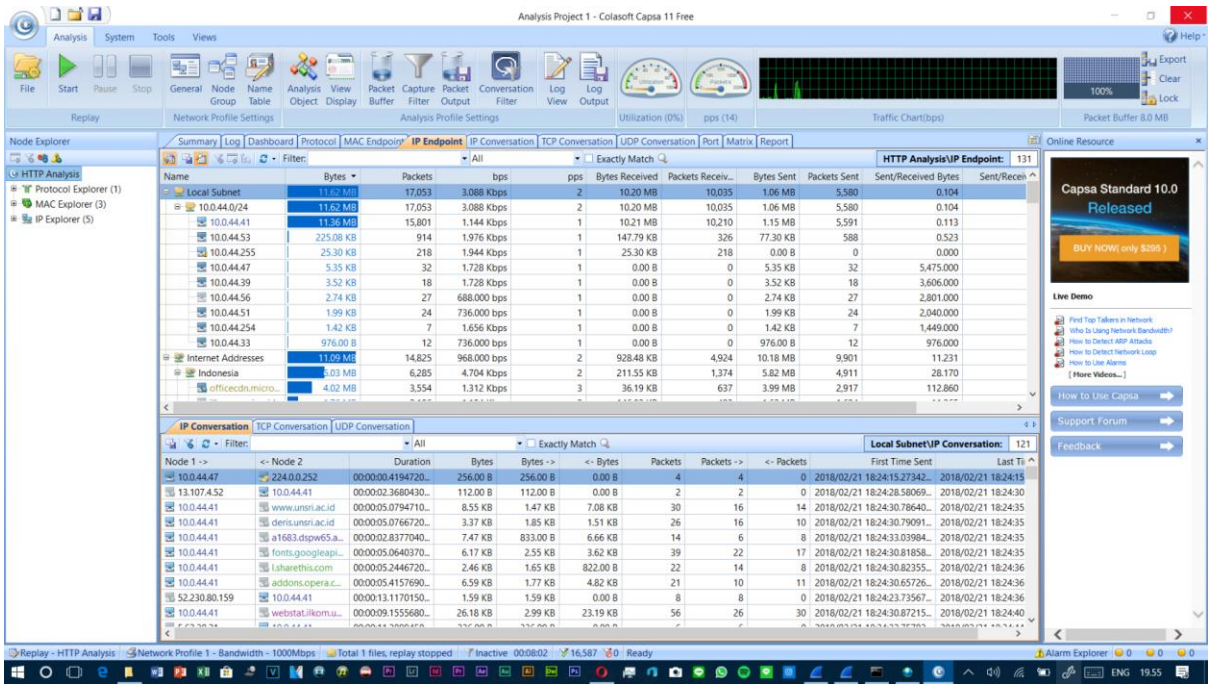
Di bagian bawah (MAC Endpoint) terdapat penjelasan jumlah data seperti protocol yang ada di HTTP Analysis, akan tetapi secara menyeluruh yang berarti seluruh pengguna di router penggunaan data terlihat berapa jumlahnya.

5. MAC Endpoint



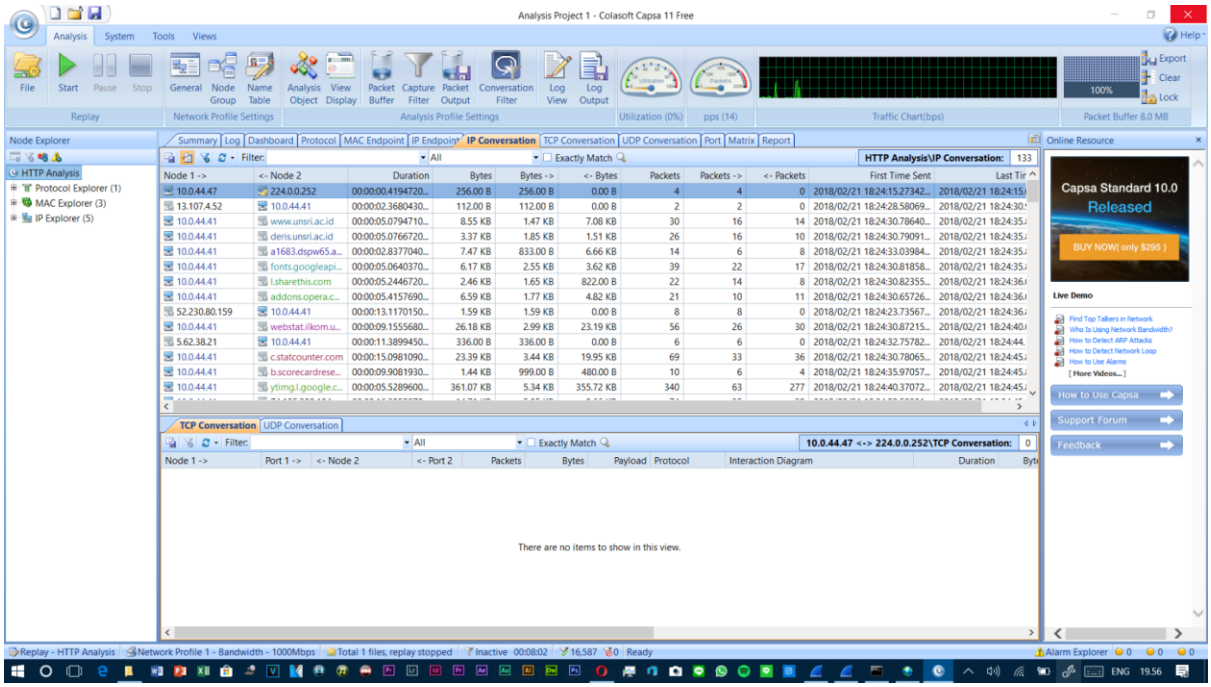
Hampir sama pada bagian protocol, akan tetapi lebih menyeluruh.

6. IP Endpoint



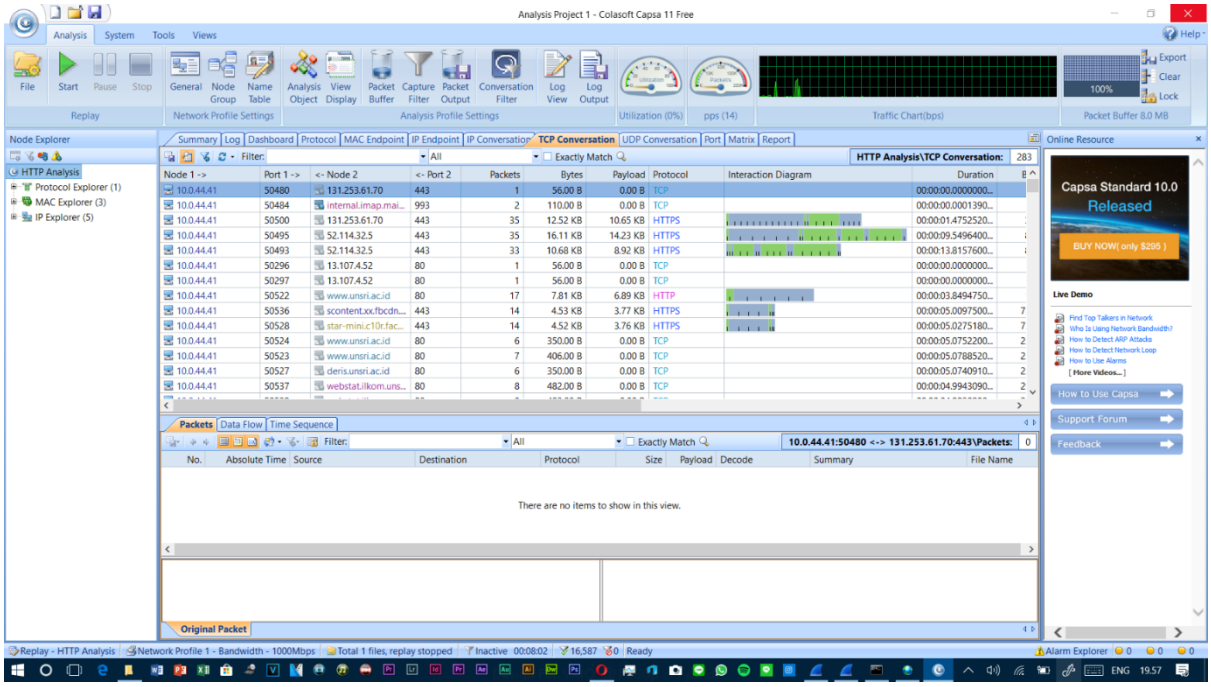
Pada IP endpoint, terdapat kemana saja IP tersebut berinteraksi.

7. IP Conversation



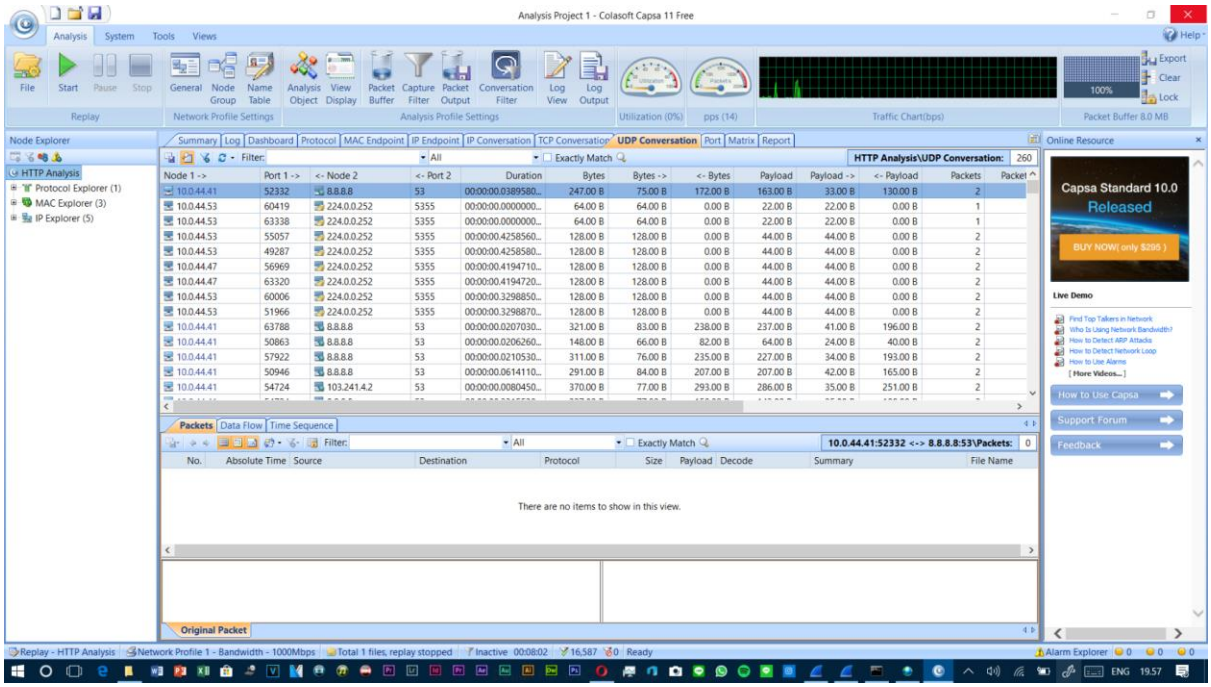
Tab IP Conversation ini sama hal kerjanya dengan IP EndPoint.

8. TCP Conversation



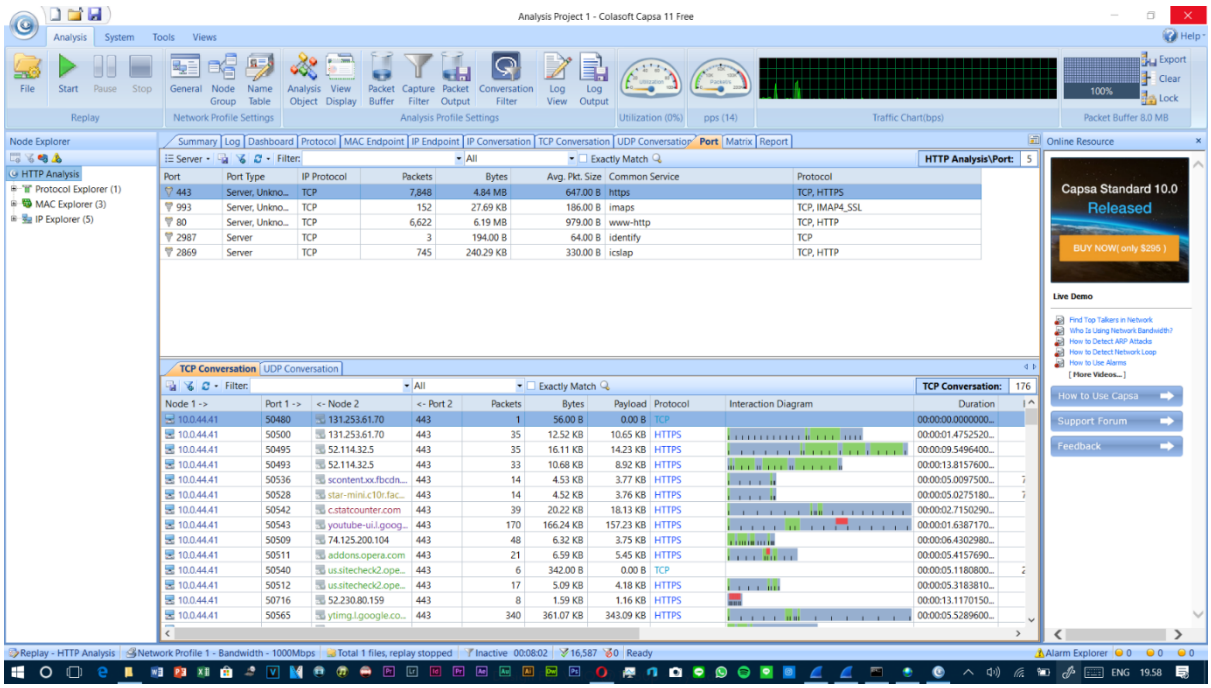
TCP Conversation berfungsi untuk melihat konversasi antar IP dengan melihat protocol dan port yang digunakan. Sebagai contoh pada web unsri.ac.id IP Source dengan IP 10.0.44.41 dengan port 50522 saling berhubungan dengan IP Destination dengan Port 80 dan protocol yang digunakan yakni HTTP dengan jumlah packet sebanyak 17 packet.

9. UDP Conversation



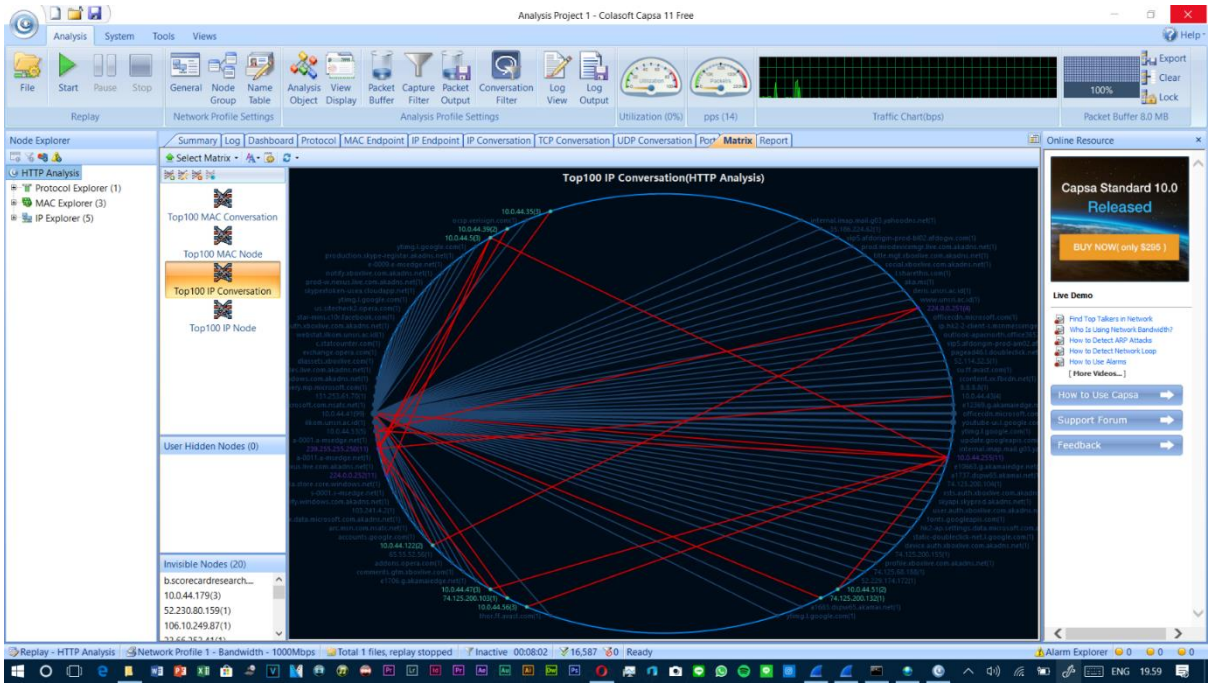
UDP Conversation biasanya digunakan untuk melihat aktivitas IP yang satu router, untuk melihat apa yang digunakan sebagai contoh pada baris kedua terlihat IP Source 10.0.44.53 berusaha menghubungi atau menerima packet data dari IP server yakni 224.0.0.252 dengan packet yang diterima berjumlah satu.

10. Port



Port berfungsi untuk melihat segala aktivitas port, protocol, packet, common service server yang diakses. Sebagai contoh port 443 memiliki IP Protocol berupa TCP dengan jumlah packet yang diterima hingga 7.848 dan Size yang diterima/dikirim sebesar 4,84 MB dengan Common service berupa https (HTML 5) dengan protocol yang digunakan/dilayankan yakni TCP, HTTPS.

11. Matrix



Matriks berfungsi untuk menampilkan IP Konversasi yang sering digunakan (Sebagai gamabaran dimana IP Source yang sering melakukan interaksi). Pada Matriks, dapat terlihat juga IP perangkat yang berada pada satu router sehingga aktivitas IP tersebut terlihat dengan jelas disbanding jika menggunakan wireshark yang notabene menampilkan seluruh tracing. Sebagai contoh IP 10.0.44.41 terhubung ke IP 224.0.0.25 .