

NAMA : MUHAMMAD DIVO TRINANDA

NIM : 09011381722103

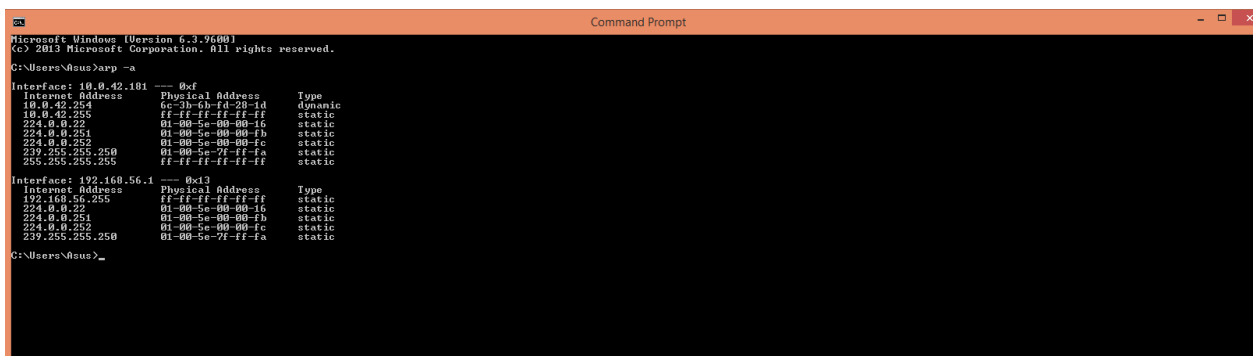
KELAS : SK4A

MATA KULIAH: KOMUNIKASI DATA

Analisis Packet Dengan Menggunakan Aplikasi Wireshark, Colasoft Capsa 11, dan Visual Route

A. Wireshark

WIRESHARK adalah satu dari sekian banyak tool Network Analyzer yang dipakai oleh orang-orang yang bekerja di bidang jaringan yang ingin melihat atau menganalisa paket jaringan, pengembangan protokol jaringan serta edukasi bagi yang ingin memperdalam ilmunya dalam jaringan komputer. Aplikasi ini juga dapat menangkap paket-paket data/informasi yang ada dalam jaringan yang kita ingin lihat. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Kali ini saya akan menganalisa packet protocol yang ter-capture saat membuka situs website Fasilkom Unsri (fasilkom.unsri.ac.id).



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

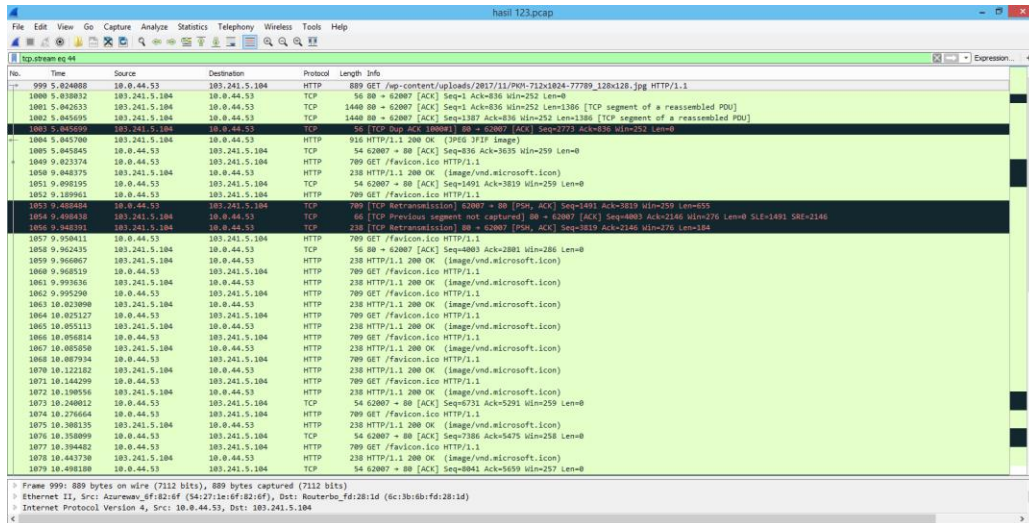
C:\Users\Asus>arp -a

Interface: 10.0.42.101 --- 0xf
Internet Address      Physical Address      Type
10.0.42.254           6c-2b-91-fd-28-1d    static
10.0.42.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-1b    static
224.0.0.252           01-00-5e-00-00-1c    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x13
Internet Address      Physical Address      Type
192.168.56.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-1b    static
224.0.0.252          01-00-5e-00-00-1c    static
239.255.255.250     01-00-5e-7f-ff-fa    static

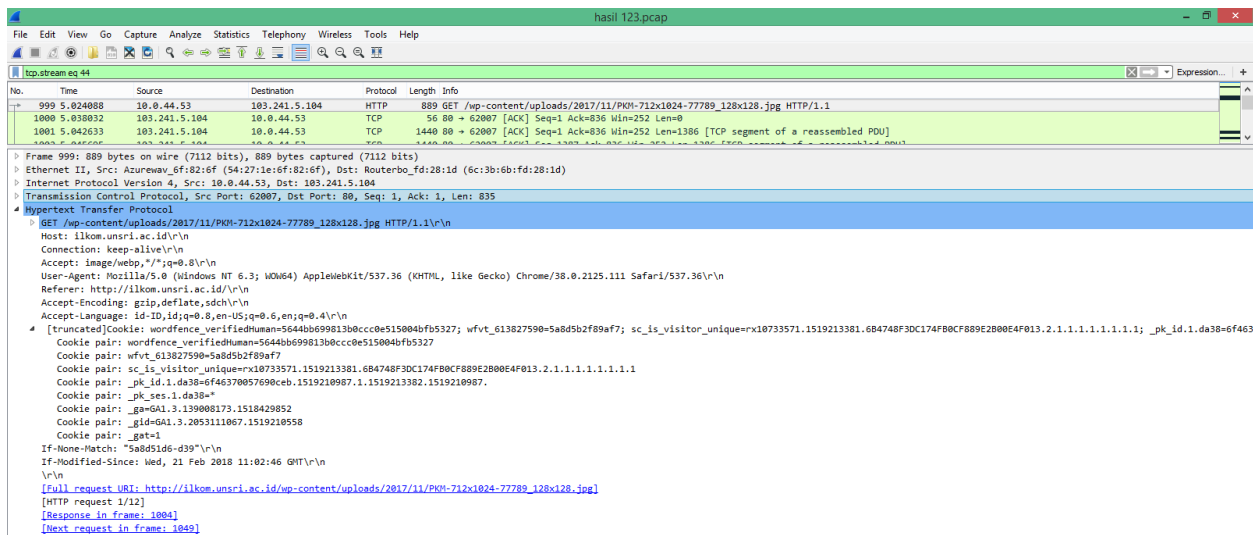
C:\Users\Asus>_
```

Pertama kita harus mengecek terlebih dahulu ip yang kita gunakan dengan cara membuka cmd. Setelah cmd terbuka ketik `arp -a` untuk menampilkan nomor ip kita seperti pada gambar di atas.



Setelah itu buka wireshark dan masukkan keyword `ip.dst==103.241.5.104` pada kolom filter maka akan timbul capture seperti di atas. Kemudian saya akan menjelaskan protocol yang terdapat dalam gambar tersebut.

1. HTTP

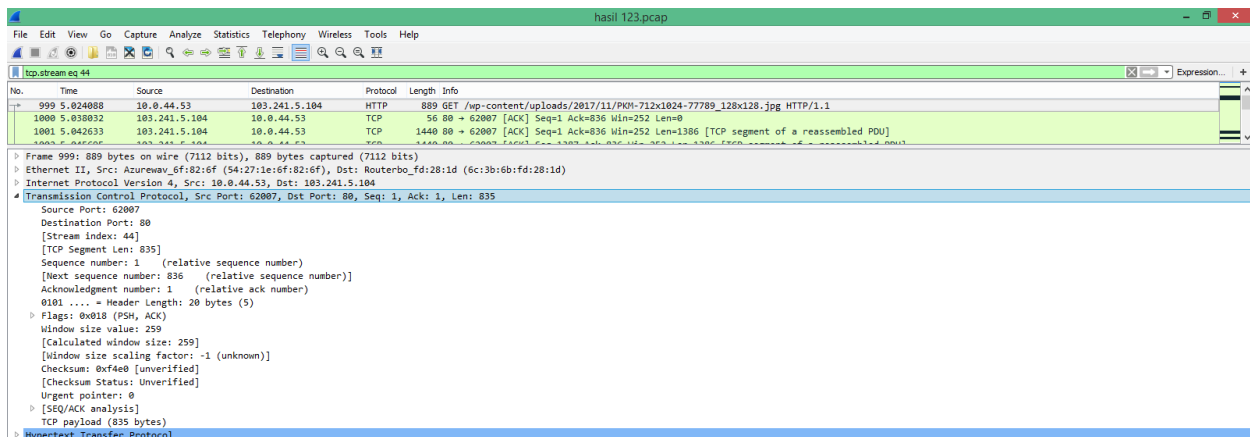


Dari data yang dicapture di atas Dari kita dapat menganalisis beberapa informasi sebagai berikut:

1. Alamat yang sedang diakses `ilkom.unsri.ac.id` dan koneksinya tetap terjaga
2. Kemungkinan Web Browser yang digunakan adalah Mozilla 5.0/Chrome 38.0.2125.111/Safari 543.36

3. Bahasa yang digunakan adalah bahasa Indonesia
4. Akses ke ilkom.unsri.ac.id browser ini sudah pernah dilakukan hingga terdapat cookie tersimpan di browser user.
5. Hari/Tanggal diaksesnya adalah Rabu/21 Februari 2018 pada pukul 11:42:46 GMT

2. TCP



Transport layer menjelaskan dimana aplikasi berkomunikasi melalui port yang digunakan. Melihat capture ditunjukkan pada gambar diatas, kita dapat melihat bahwa port sumber adalah 62007, sedangkan port tujuan adalah 80, dan panjang header (44 byte) dan nomor urut. Nomor urut umumnya akan berubah untuk setiap paket.

B. Colasoft Capsa

Colasoft Capsa adalah alat analisis dan alat analisis kinerja jaringan portabel, memberikan solusi penangkapan dan analisis paket yang sangat hebat dan komprehensif dengan antarmuka yang mudah digunakan yang memungkinkan pengguna veteran dan pemula mendapatkan kemampuan untuk melindungi dan memantau jaringan di lingkungan bisnis yang kritis. Bantuan Capsa dalam menjaga Anda menilai ancaman yang dapat menyebabkan pemadaman bisnis yang signifikan. Masih sama seperti Wireshark tadi yang menggunakan alamat website Fasilkom Unsri (ilkom.unsri.ac.id)

1. Analisis dengan menggunakan IP conversation pada Colasoft Capsa 11

10.0.44.53	l.sharethis.com	00:01:05.032618000	2.35 KB	1.50 KB	876.00 B	21	12	9
10.0.44.53	scontent.xx.fbcdn.net	00:01:06.308785000	79.53 KB	2.88 KB	76.65 KB	103	36	67
10.0.44.53	star-mini.c10r.faceb...	00:01:05.409806000	8.40 KB	1.94 KB	6.46 KB	35	16	19
10.0.44.122	224.0.0.251	00:01:06.971776000	1.28 KB	1.28 KB	0.00 B	16	16	0
10.0.44.53	ilkom.unsri.ac.id	00:01:11.231686000	16.53 KB	9.76 KB	6.78 KB	47	24	23
10.0.44.122	239.255.255.250	00:01:20.588232000	1.79 KB	1.79 KB	0.00 B	11	11	0
10.0.44.53	74.125.24.188	00:00:45.022105000	176.00 B	110.00 B	66.00 B	3	2	1
10.0.44.47	224.0.0.252	00:00:00.002847000	256.00 B	256.00 B	0.00 B	4	4	0
10.0.44.41	239.255.255.250	00:01:24.575059000	6.88 KB	6.88 KB	0.00 B	23	23	0
10.0.44.47	10.0.44.255	00:00:01.133639000	276.00 B	276.00 B	0.00 B	3	3	0

Gambar di atas adalah sebagian gambar dari hasil pengoperasian analisis dengan colasoft dimana hasil pada IP conversation diperoleh sebanyak 38 IP. Disini, saya hanya akan melakukan analisis terhadap IP saya sendiri, dan juga IP 2 teman saya.

Adapun ruang lingkup analisis yang saya lakukan itu hanya pada IP Conversation dan Marks saja. Berikut hasil analisis saya di IP conversation:

- Hasil analisis pada colasoft bagian IP Conversation diketahui bahwa IP saya yang bernomor 10.0.44.53 melakukan destination request ke domain ilkom.unsri.ac.id dengan durasi perjalanan 00:00:1.1123160 dengan tingkat kecepatan request 9.76 KB yang membawa packet data sebanyak 47 dan kecepatan reply dari domain ilkom.unsri.ac.id yaitu 6.78 KB dengan membawa 24 paket data. Dengan rincian analisis, yaitu:

No.	Absolute Time	Source	Destination	Protocol	Size	Payload	Decode	Summary	File Name
999	18:43:04.10588000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	889	835		GET /wp-content/uploads/2017/11/PKM-7...	C:\Users\Asus\Do...
1000	18:43:04.11983000	ilkom.unsri.ac.id:80	10.0.44.53:62007	TCP	56	0		SeqNumber=4290232719,AckNumber=680...	C:\Users\Asus\Do...
1001	18:43:04.12443000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	1,440	1,386		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1002	18:43:04.12749600	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	1,440	1,386		HTTP data packet	C:\Users\Asus\Do...
1003	18:43:04.12750000	ilkom.unsri.ac.id:80	10.0.44.53:62007	TCP	56	0		SeqNumber=4290235491,AckNumber=680...	C:\Users\Asus\Do...
1004	18:43:04.127501000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	916	862		HTTP data packet	C:\Users\Asus\Do...
1005	18:43:04.127546000	10.0.44.53:62007	ilkom.unsri.ac.id:80	TCP	54	0		SeqNumber=68080341,AckNumber=4290...	C:\Users\Asus\Do...
1049	18:43:08.105175000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1050	18:43:08.130176000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1051	18:43:08.179996000	10.0.44.53:62007	ilkom.unsri.ac.id:80	TCP	54	0		SeqNumber=68080996,AckNumber=4290...	C:\Users\Asus\Do...
1052	18:43:08.271762000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1053	18:43:08.570285000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		[Retransmission] GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1054	18:43:08.580239000	ilkom.unsri.ac.id:80	10.0.44.53:62007	TCP	66	0		[TCP Previous packet lost] SeqNumber=42...	C:\Users\Asus\Do...
1056	18:43:09.030192000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		[Retransmission] HTTP/1.1 200 OK	C:\Users\Asus\Do...
1057	18:43:09.03212000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1058	18:43:09.044236000	ilkom.unsri.ac.id:80	10.0.44.53:62007	TCP	56	0		SeqNumber=4290236721,AckNumber=680...	C:\Users\Asus\Do...
1059	18:43:09.047868000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1060	18:43:09.050320000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1061	18:43:09.075437000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1062	18:43:09.07791000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1063	18:43:09.104891000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1064	18:43:09.106828000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1065	18:43:09.136814000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1066	18:43:09.136815000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1067	18:43:09.167651000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1068	18:43:09.169735000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1070	18:43:09.203883000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1071	18:43:09.226100000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1072	18:43:09.272370000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1073	18:43:09.321813000	10.0.44.53:62007	ilkom.unsri.ac.id:80	TCP	54	0		SeqNumber=680812236,AckNumber=4290...	C:\Users\Asus\Do...
1074	18:43:09.338465000	10.0.44.53:62007	ilkom.unsri.ac.id:80	HTTP	709	655		GET /favicon.ico HTTP/1.1	C:\Users\Asus\Do...
1075	18:43:09.389936000	ilkom.unsri.ac.id:80	10.0.44.53:62007	HTTP	238	184		HTTP/1.1 200 OK	C:\Users\Asus\Do...
1076	18:43:09.439900000	10.0.44.53:62007	ilkom.unsri.ac.id:80	TCP	54	0		SeqNumber=680812891,AckNumber=4290...	C:\Users\Asus\Do...

- Selanjutnya hasil analisis pada colasoft bagian IP Conversation diketahui bahwa IP 10.0.44.122 melakukan destination request ke IP 224.0.0.251 dengan durasi perjalanan 00:01:06.97176000 dengan tingkat kecepatan request 1.28 KB yang membawa packet data

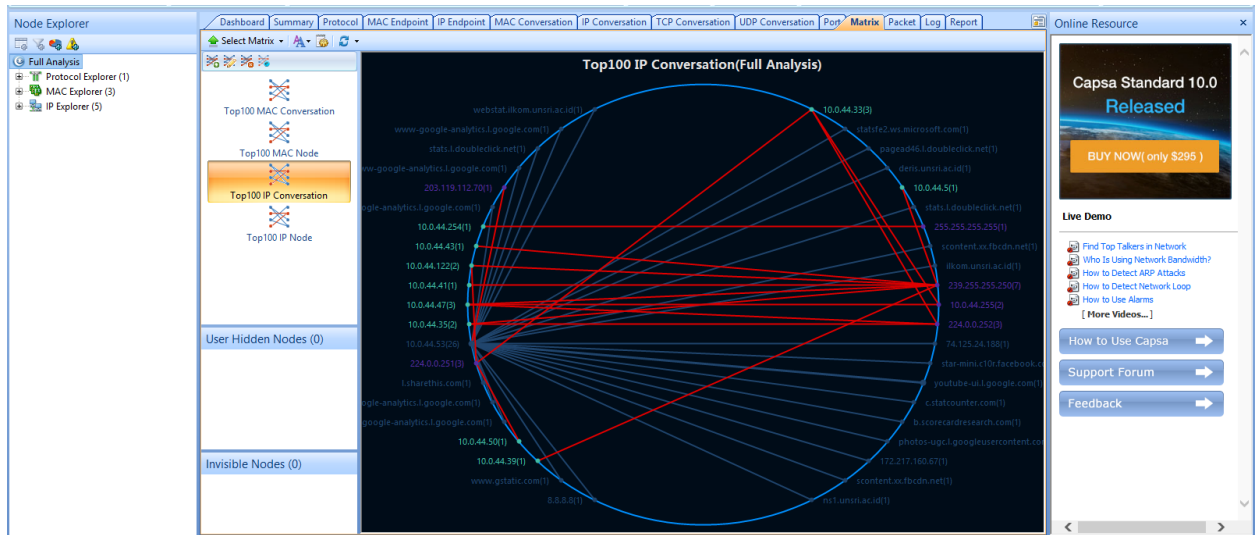
sebanyak 16 dan kecepatan reply dari IP 224.0.0.251 yaitu 1.28 KB dengan membawa 16 paket data. Dengan rincian analisis, yaitu:

No.	Absolute Time	Source	Destination	Protocol	Size	Payload	Decode	Summary	File Name
997	18:43:04.022480000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
998	18:43:04.023327000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1036	18:43:05.966712000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1037	18:43:05.967747000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1332	18:43:25.936890000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1333	18:43:25.938585000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1334	18:43:26.959610000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1336	18:43:27.986359000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1337	18:43:27.987396000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1364	18:43:47.954418000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1365	18:43:47.956360000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1369	18:43:48.976176000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1439	18:44:09.960811000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1440	18:44:09.969810000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1446	18:44:10.993193000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...
1447	18:44:10.994256000	10.0.44.122:5353	224.0.0.251:5353	MDNS	82	40		C: Qs_googlecast_tcp.local(PTR)	C:\Users\Asus\Do...

- c. Dilanjutkan dengan IP 10.0.44.254 melakukan destination request ke IP 239.255.255.250 dengan durasi perjalanan 00:01:0.0041970 dengan tingkat kecepatan request 414.00 B yang membawa packet data sebanyak 2 dan kecepatan reply dari domain ilkom.unsri.ac.id yaitu 414.00 B dengan membawa 2 paket data. Dengan rincian analisis, yaitu:

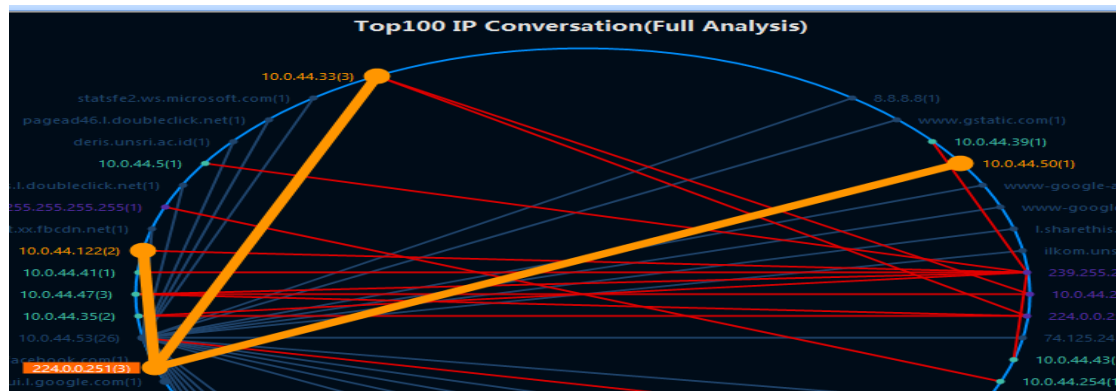
No.	Absolute Time	Source	Destination	Protocol	Size	Payload	Decode	Summary	File Name
621	18:43:01.770550000	10.0.44.254:57095	255.255.255.250:5678	MNDP	207	165		Header Unknown=19070,Sequence Numbe...	C:\Users\Asus\Do...
1397	18:44:01.774747000	10.0.44.254:57095	255.255.255.250:5678	MNDP	207	165		Header Unknown=19582,Sequence Numbe...	C:\Users\Asus\Do...

2. Analisis dengan menggunakan Matriks pada Colasoft Capsa 11

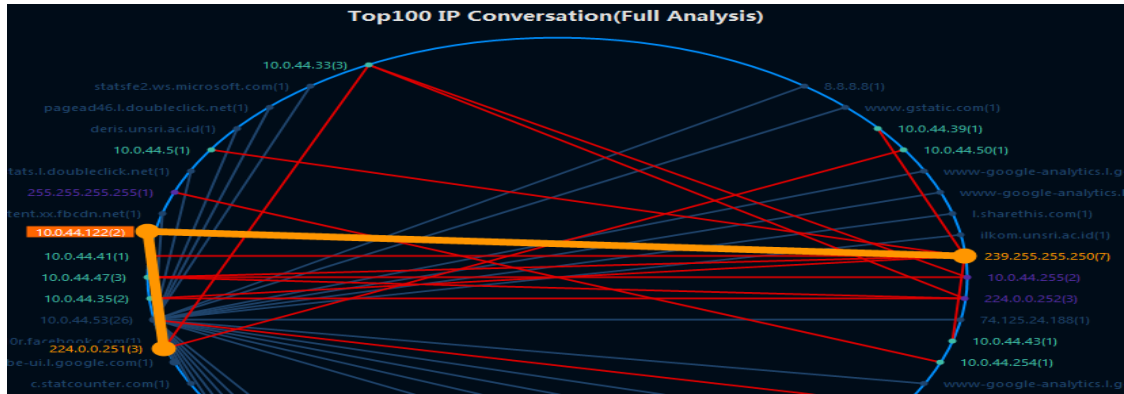


Gambar diatas adalah matriks analisis dari domain ilkom.unsri.ac.id dengan TOP 100 Ipv4 Conwertation sebagai acuan analisis. Penganalisisan hanya dilakukan terhadap 2 IP saja. Berikut hasil analisis yang saya lakukan:

- IP 224.0.0.251 melakukan proses pengaksesan terhadap 3 IP lain yaitu 10.44.50, 10.0.44.122, dan 10.0.44.33 dengan packet received 24 dan bytes received 2.04 KB.

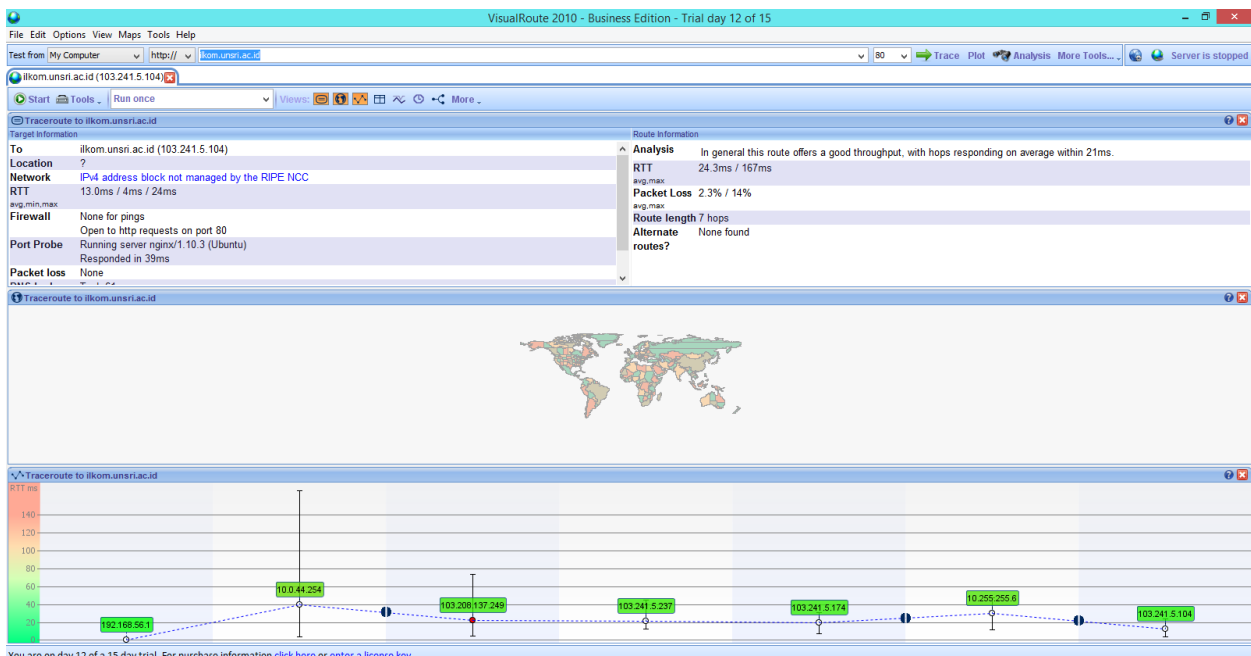


- IP 10.0.44.122 melakukan prosen pengaksesan terhadap 2 IP lain yaitu 224.0.0.251, dan 239.255.255.250 dengan packet sent 27 dan bytes sent 3.08 KB



C. Analisis Dengan Menggunakan Visual Route

VisualRoute adalah sebuah aplikasi yang dapat mengimplementasikan packet tracer, ping, dan juga reverse DNS kedalam sebuah tampilan grafis yang terhubung dengan koneksi internet sehingga dapat mengetahui fungsi dari suatu koneksi internet yang kita jalankan untuk menemukan suatu kondisi yang terjadi saat kita beraktifitas sehingga dapat mengetahui apabila terjadi pelambatan, juga dapat mengidentifikasi lokasi geografis dan IP address dan web server yang akan menunjukkan path dari sebuah koneksi internet pada peta global.



Berdasarkan hasil pengukuran jaringan internet menggunakan wifi UnsriNet disertai dengan aplikasi visualroute bahwa nilai yang di peroleh adalah sebesar 13 ms. Selain itu diperoleh bahwa jarak antara user dan server route sebanyak 7 hop, dimana setiap router mengalami koneksi internet yang baik hal ini ditandai pada setiap hop berwarna hijau. Berdasarkan hasil uji coba, koneksi internet yang didapatkan cukup baik, begitupun dari segi kualitasnya, karena paket loss yang didapat dari hasil pengukuran sebesar 2.3% untuk kualitas jaringan yang baik (mencapai taraf dibawah rata-rata 5%).