

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

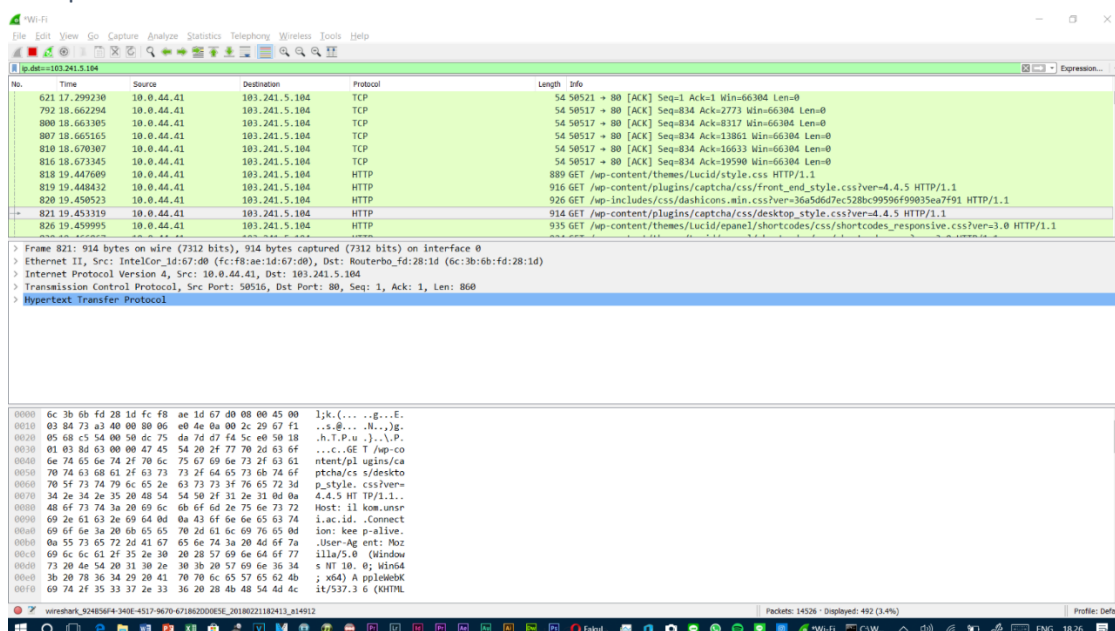
```
C:\Users\Sony>ping ilkom.unsri.ac.id

Pinging ilkom.unsri.ac.id [103.241.5.104] with 32 bytes of data:
Reply from 103.241.5.104: bytes=32 time=15ms TTL=59
Reply from 103.241.5.104: bytes=32 time=9ms TTL=59
Reply from 103.241.5.104: bytes=32 time=6ms TTL=59
Reply from 103.241.5.104: bytes=32 time=6ms TTL=59

Ping statistics for 103.241.5.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 15ms, Average = 9ms

C:\Users\Sony>
```

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_id: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
```

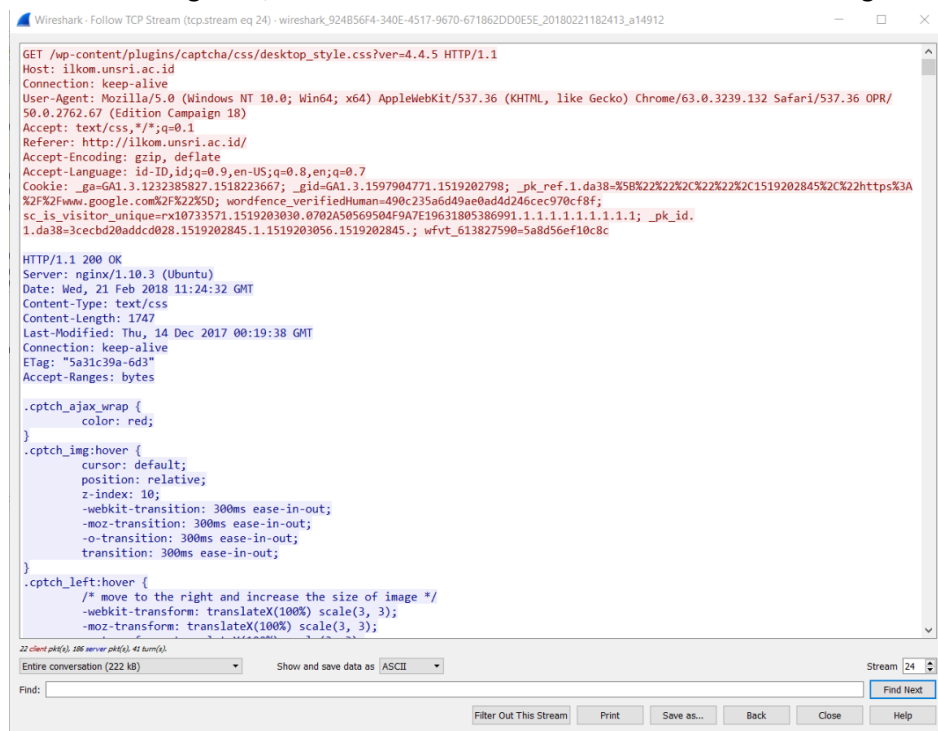
Pada baris pertama, terdapat penjelasan frame tersebut mengcapture sebanyak 914 byte. Pada baris kedua, terdapat keterangan router wifi dan adapter wifi yang terhubung ke source dan destinasi hingga alamat MAC Address.

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

```
GET /wp-content/plugins/captcha/css/desktop_style.css?ver=4.4.5 HTTP/1.1
Host: ilkom.unsri.ac.id
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36 OPR/50.0.2762.67 (Edition Campaign 18)
Accept: text/css,*/*;q=0.1
Referer: http://ilkom.unsri.ac.id/
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _ga=GA1.3.1232385827.1518223667; _gid=GA1.3.1597904771.1519202798; _pk_ref.1.da38=%5B%22%2C%22%2C1519202845%2C%22https%3A%2F%2Fwww.google.com%2F%22%5D; wordfence_verifiedHuman=490c235a6d49ae0add246cec970cf8f; sc_is_visitor_unique=rx10733571.1519203030.0702A50569504F9A7E19631805386991.1.1.1.1.1.1.1.1; _pk_id.1.da38=3cecbd20addcd028.1519202845.1.1519203056.1519202845.; wfvt_613827590=5a8d56ef10c8c
```

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.

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 21 Feb 2018 11:24:32 GMT
Content-Type: text/css
Content-Length: 1747
Last-Modified: Thu, 14 Dec 2017 00:19:38 GMT
Connection: keep-alive
ETag: "5a31c39a-6d3"
Accept-Ranges: bytes
```

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.

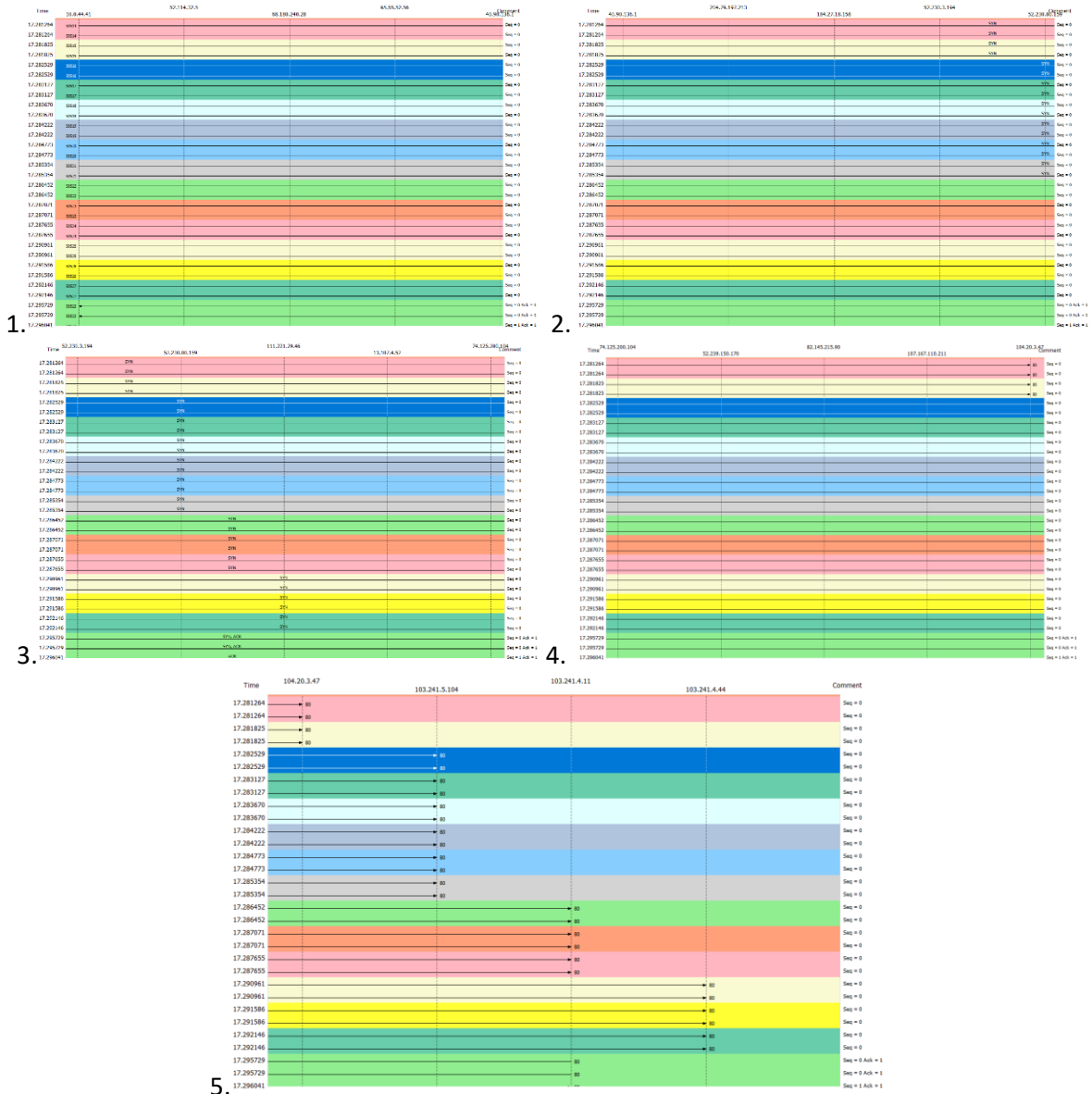
Pada baris keempat dijelaskan data yang diakses berupa text/css

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 menunjukkan 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:



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.

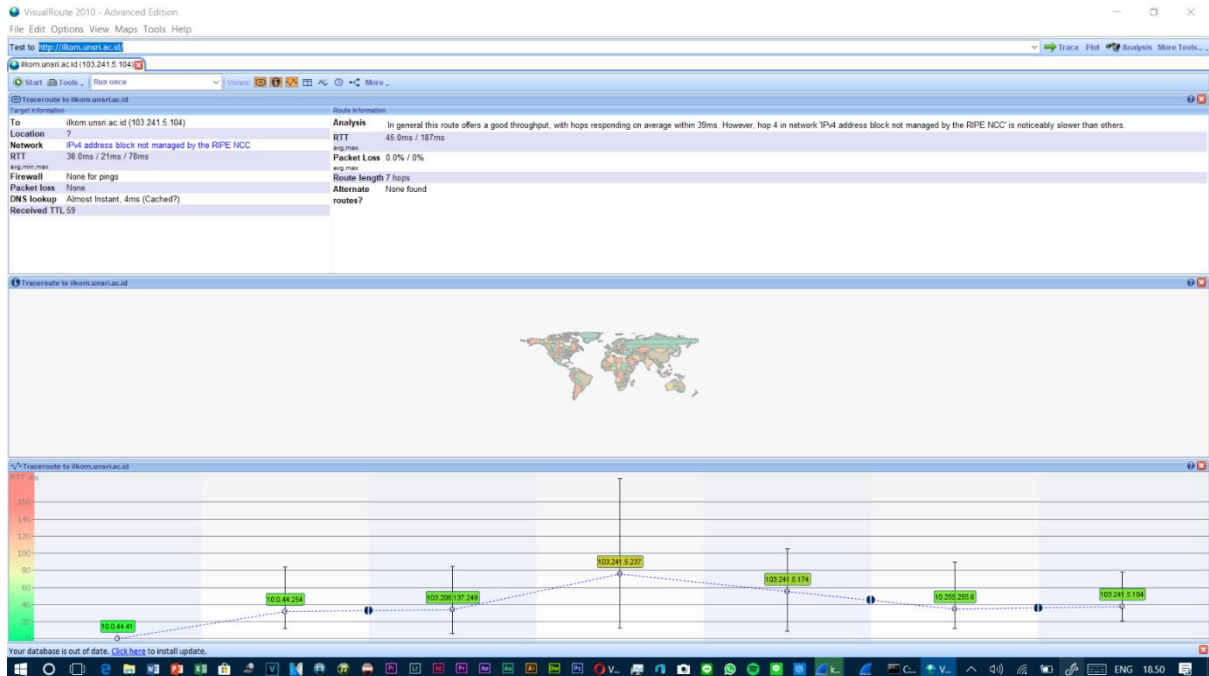
Di Flowgraph juga terdapat keterangan lain seperti port yang digunakan antara Ip Source dan IP Destination.

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. Perbandingan 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-id.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		103.208.137.249	HOPS 3
5.	40.90.136.1			
6.	204.79.197.213			
7.	184.27.18.158		103.241.5.237	HOPS 4
8.	52.230.3.194			
9.	52.230.80.159		103.241.5.174	HOPS 5
10.	111.221.29.46			
11.	13.107.4.52			
12.	74.125.200.104			
13.	52.239.150.170		10.255.255.6	HOPS 6
14.	82.145.215.90			
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

The screenshot shows a browser window with the address bar containing `http://52.114.32.5/`. The main content area displays a red circular icon with a white 'O' and the text "Situs ini tidak dapat dijangkau". Below this, it states "52.114.32.5 membutuhkan terlalu banyak waktu untuk merespons." Under the heading "Coba:", there are three items with checkmarks: "Periksa sambungan", "Memeriksa proxy dan firewall", and "Jalankan Diagnostik Jaringan Windows". A section titled "Periksa koneksi internet Anda." provides instructions to check cables and restart network hardware.

## 3. 68.180.240.28

The screenshot shows a browser window with the address bar containing `68.180.240.28`. The main content area displays a red circular icon with a white 'O' and the text "Situs ini tidak dapat dijangkau". Below this, it states "68.180.240.28 membutuhkan terlalu banyak waktu untuk merespons." Under the heading "Coba:", there are three items with checkmarks: "Periksa sambungan", "Memeriksa proxy dan firewall", and "Jalankan Diagnostik Jaringan Windows".

## 4. 65.55.52.56

The screenshot shows a browser window with the address bar containing `65.55.52.56`. The main content area displays a red circular icon with a white 'O' and the text "Situs ini tidak dapat dijangkau". Below this, it states "65.55.52.56 membutuhkan terlalu banyak waktu untuk merespons." Under the heading "Coba:", there are three items with checkmarks: "Periksa sambungan", "Memeriksa proxy dan firewall", and "Jalankan Diagnostik Jaringan Windows".

## 5. 40.90.136.1

The screenshot shows a browser window with the address bar containing `http://40.90.136.1/`. The main content area displays a red circular icon with a white 'O' and the text "Halaman 40.90.136.1 ini tidak dapat ditemukan". Below this, it states "Tidak ada halaman web yang ditemukan untuk alamat web: `http://40.90.136.1/`". At the bottom, there is a Google search bar with the text "40.90.136.1" entered.

## 6. 204.79.197.213

The screenshot shows a browser window with the address bar containing `http://204.79.197.213/`. The main content area displays a message: "Our services aren't available right now. We're working to restore all services as soon as possible. Please check back soon." followed by reference IDs: "Ref A: 183486BEA4F044659AACB54048B6CAE1 Ref B: SGESCHEDGE0111 Ref C: 2018-02-23T01:16:59Z".



## 7. 184.27.18.158

< > C http://184.27.18.158/

Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [Impor bookmark sekarang](#)

### Invalid URL

The requested URL "[no URL]", is invalid.  
Reference #9.24da387d.1519356352.b662e32

## 8. 52.230.3.194

< > C http://52.230.3.194/

Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [Impor bookmark sekarang](#)



### Situs ini tidak dapat dijangkau

52.230.3.194 membutuhkan terlalu banyak waktu untuk merespons.

**Coba:**

- ✓ Periksa sambungan
- ✓ [Memeriksa proxy dan firewall](#)
- ✓ [Jalankan Diagnostik Jaringan Windows](#)

## 9. 52.230.80.159

< > C 52.230.80.159

Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [Impor bookmark sekarang](#)



### Situs ini tidak dapat dijangkau

52.230.80.159 membutuhkan terlalu banyak waktu untuk merespons.

**Coba:**

- ✓ Periksa sambungan
- ✓ [Memeriksa proxy dan firewall](#)
- ✓ [Jalankan Diagnostik Jaringan Windows](#)

## 10. 111.221.29.46

< > C http://111.221.29.46/

Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [Impor bookmark sekarang](#)

## Server Error

**403 - Forbidden: Access is denied.**

**You do not have permission to view this directory or page using the credentials that you supplied.**

## 11. 13.107.4.52

< > C http://13.107.4.52/

Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [Impor bookmark sekarang](#)

<h2>Our services aren't available right now</h2><p>We're working to restore all services as soon as possible. Please check back soon.</p><p>Ref A: 6917E8AAE05485E8980015D7FFD2BA5 Ref B: 5GESCHEDGE0113 Ref C: 2018-02-23T03:28:09Z

## 12. 74.125.200.104

< > C 74.125.200.104

Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [Impor bookmark sekarang](#)

Gmail Gambar [Masuk](#)

Google

Penelusuran Google [Saya Lagi Beruntung](#)

Google menawarkan: [English](#) [Basa Jawa](#) [Basa Bali](#)

### 13. 52.239.150.170

The screenshot shows a browser window with the address bar containing `http://52.239.150.170/`. Below the address bar, there is a message: "Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [impor bookmark sekarang](#)". The main content area displays the message: "This XML file does not appear to have any style information associated with it. The document tree is shown below." Below this message is an XML error structure:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>InvalidUri</Code>
  <Message>
    The requested URI does not represent any resource on the server. RequestId:3381579c-001e-00ec-6044-ac49b3000000 Time:2018-02-23T01:20:41.6411581Z
  </Message>
  <UriPath>http://52.239.150.170/</UriPath>
</Error>
```

### 14. 82.145.215.90

The screenshot shows a browser window with the address bar containing `http://82.145.215.90/`. Below the address bar, there is a message: "Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [impor bookmark sekarang](#)". The main content area displays the error: "403 Forbidden" and "nginx/1.6.2".

### 15. 107.167.110.211

The screenshot shows a browser window with the address bar containing `http://107.167.110.211/`. Below the address bar, there is a message: "Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [impor bookmark sekarang](#)". The main content area displays the message: "Welcome to nginx!". Below this message, there is a paragraph: "If you see this page, the nginx web server is successfully installed and working. Further configuration is required." Below this paragraph, there is a paragraph: "For online documentation and support please refer to [nginx.org](#). Commercial support is available at [nginx.com](#)." Below this paragraph, there is a paragraph: "Thank you for using nginx."

### 16. 104.20.3.47

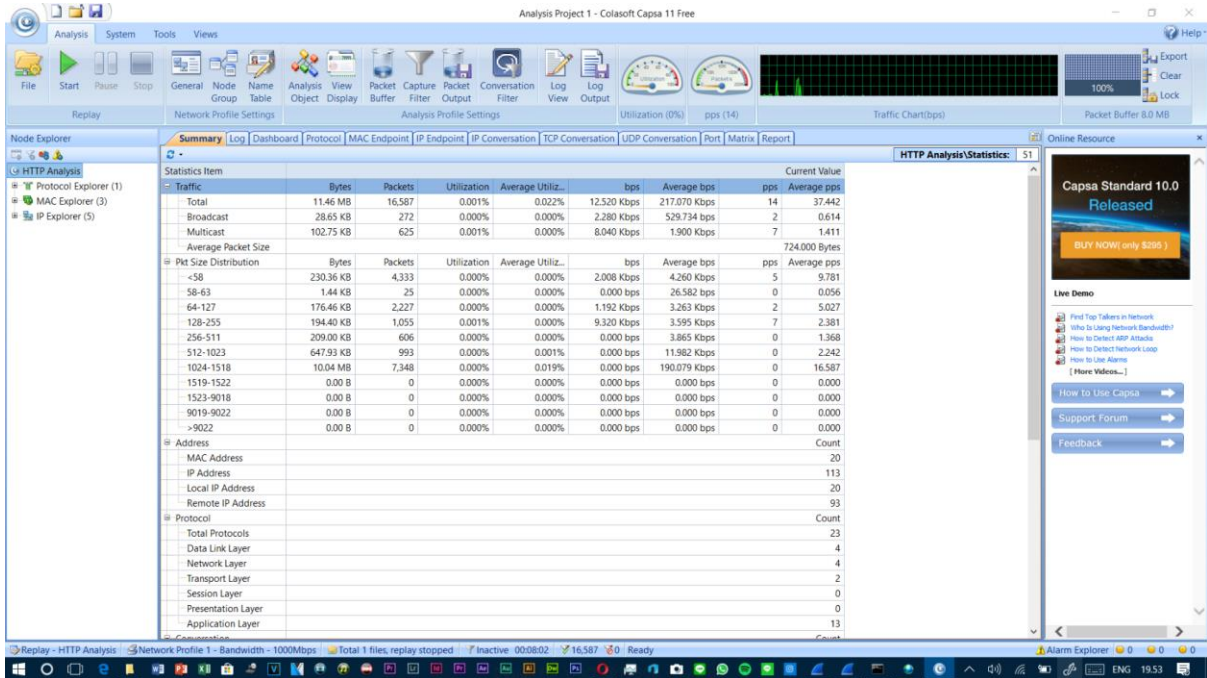
The screenshot shows a browser window with the address bar containing `http://104.20.3.47/`. Below the address bar, there is a message: "Tambahkan bookmark pertama Anda dengan menggunakan hati pada panel alamat... atau [impor bookmark sekarang](#)". The main content area displays the error: "Error 1003" and "Direct IP access not allowed". Below this error, there is a paragraph: "Ray ID: 3f16605db1856ff0 • 2018-02-23 01:22:51 UTC". Below this paragraph, there are two columns of text: "What happened?" and "What can I do?". Below these columns, there is a paragraph: "Cloudflare Ray ID: 3f16605db1856ff0 • Your IP: 202.67.42.36 • Performance & security by Cloudflare".

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

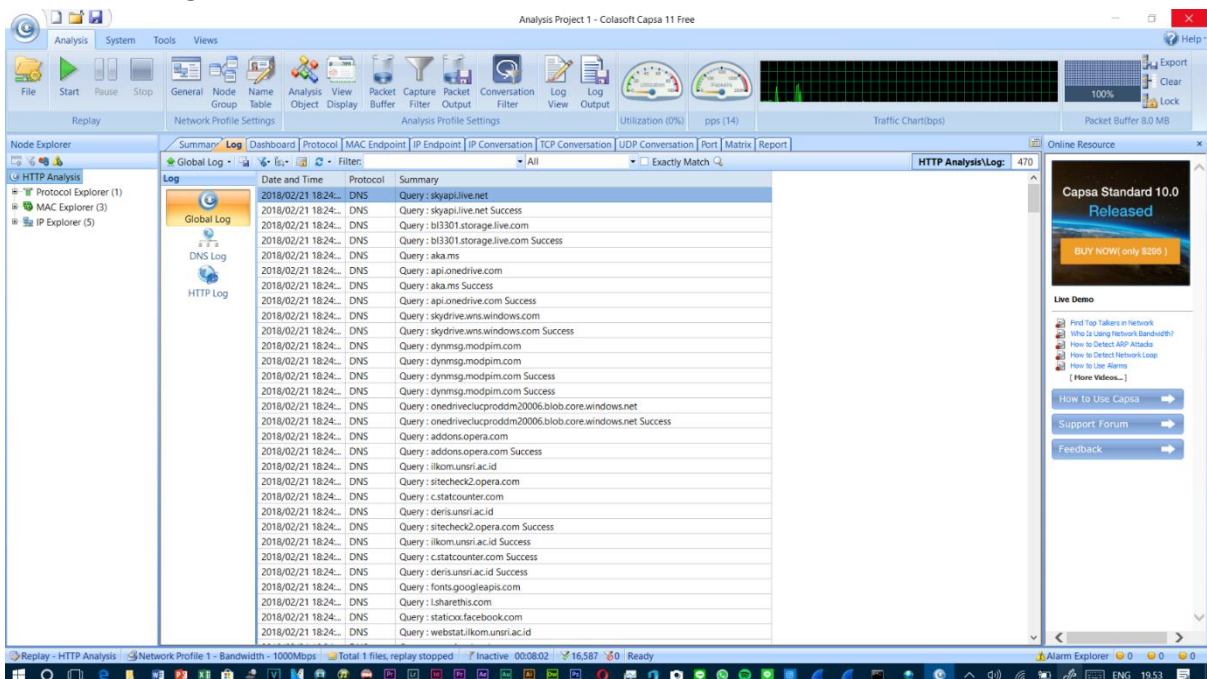
Setelah nomor satu tadi selesai dijalankan, maka yang dilakukan Adalah memberhentikan tracing dan menyimpan file tersebut ke format “pcap”. Kemudian dibuka di aplikasi colasoft yang akan mendapatkan hasil dalam beberapa bentuk, yakni:

##### 1. Summary



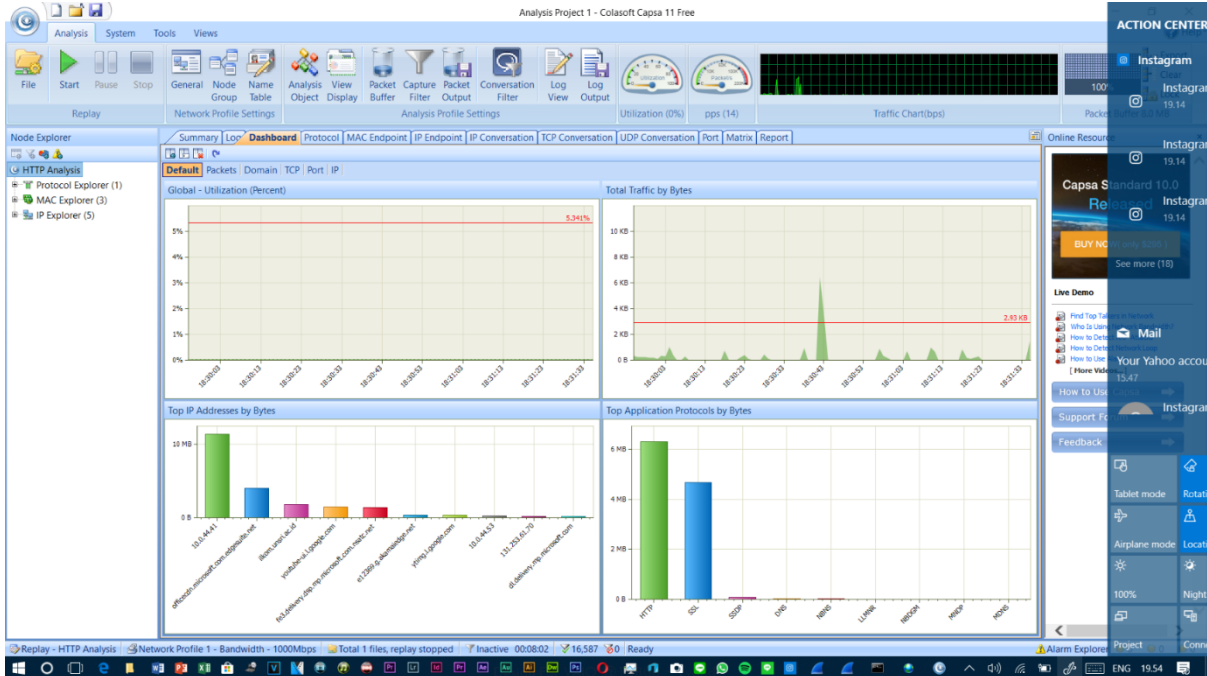
Hasil dari summary yang didapat yakni: Data yang berhasil di trace di wireshark sebelumnya yaitu sebesar 11,46 MB dengan total packet sebanyak 16.587.

##### 2. Log



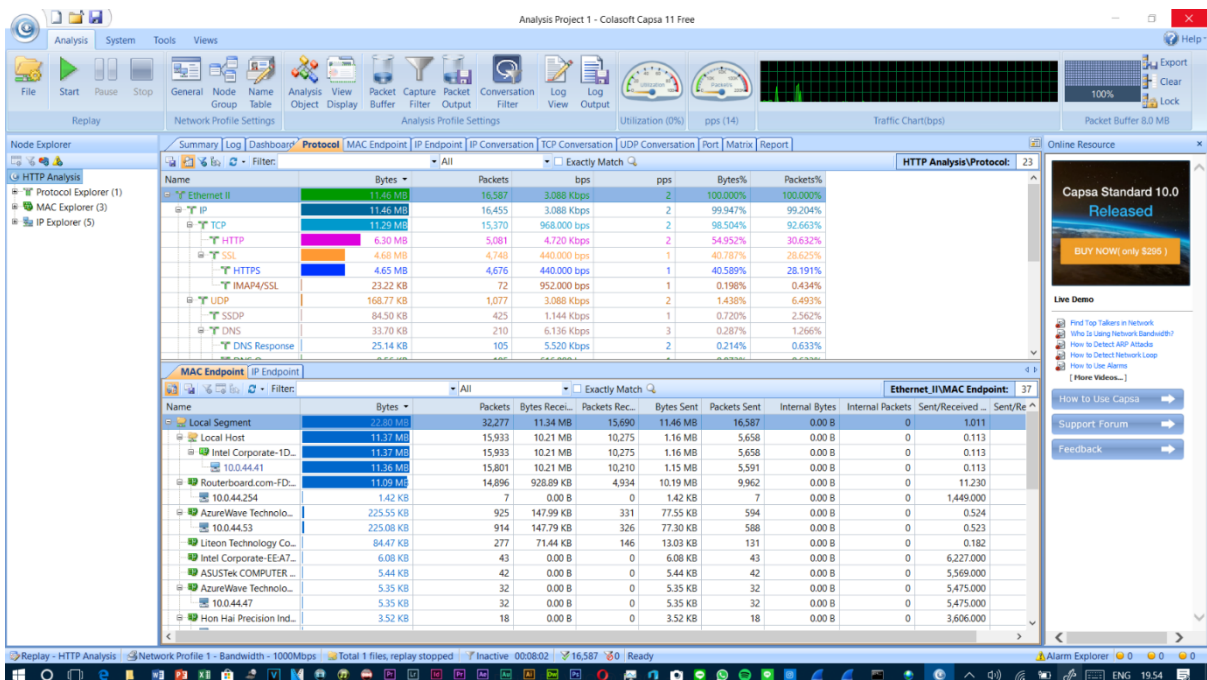
Dari data diatas, terdapat banyak data pencarian, yang sebelumnya teracak di wireshark, dan dapat kita ketahui bahwa ilkom.unsri.ac.id ada di riwayat berdasarkan gambar tersebut terletak pada baris ke-19

### 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.

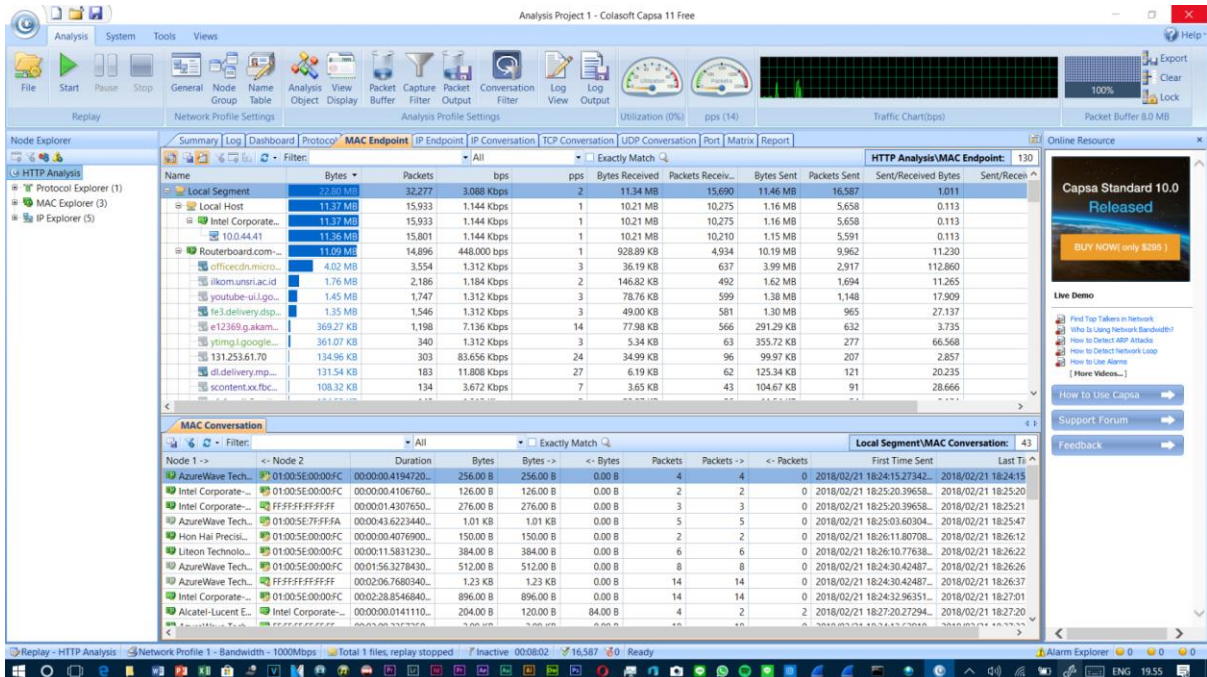
### 4. Protocol



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

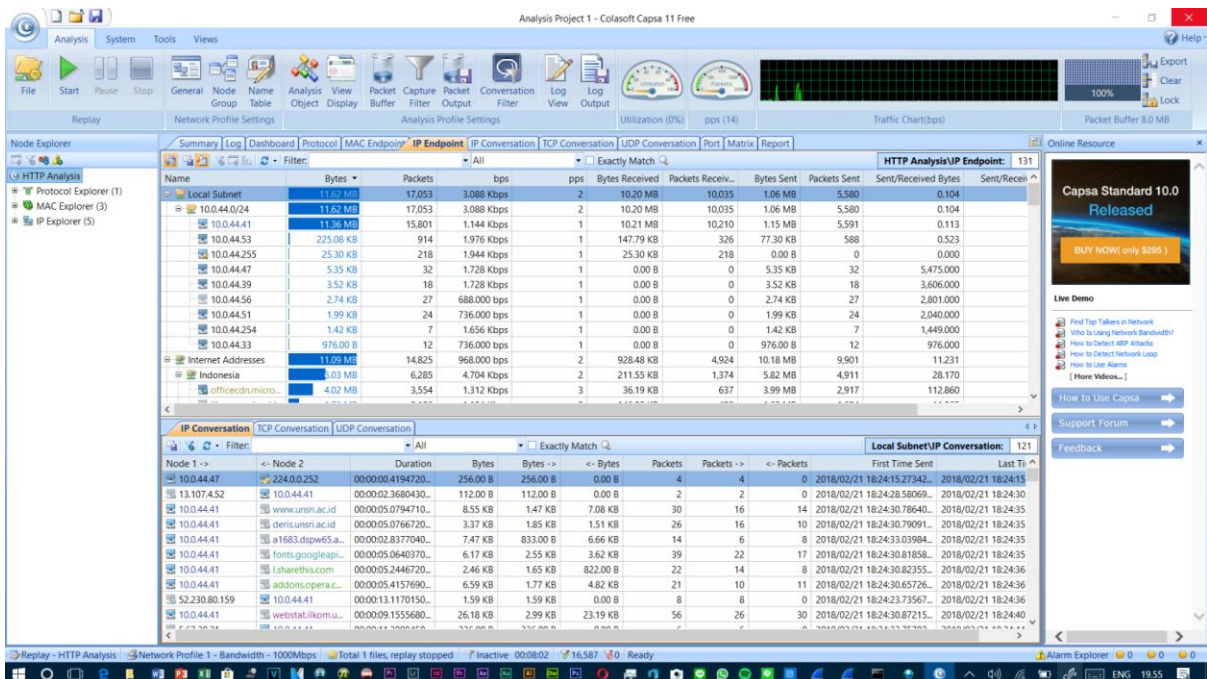
Di bagian bawah (MAC Endpoint) terdapat penjelasan jumlah data seperti protocol yang ada di HTTP Analysis, akan tetapi secara menyeluruh yang berarti seluruh pengguna di router penggunaan data terlihat berapa jumlahnya.

## 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

Node 1 ->	Port 1 ->	Node 2	Port 2	Packets	Bytes	Payload	Protocol	Interaction Diagram	Duration
10.044.47	224.0.0.252	00:00:00:4194720...		256.00 B	256.00 B	0.00 B			
13.107.452	10.0.44.41	00:00:02:3680490...		112.00 B	112.00 B	0.00 B			
10.0.44.41	www.unsri.ac.id	00:00:05:0794710...		8.55 KB	1.47 KB	7.08 KB			
10.0.44.41	denis.unsri.ac.id	00:00:05:0766720...		3.37 KB	1.85 KB	1.51 KB			
10.0.44.41	a1683.dspw65.a...	00:00:02:8377040...		7.47 KB	833.00 B	6.66 KB			
10.0.44.41	fonts.googleapp...	00:00:05:0640370...		6.17 KB	2.55 KB	3.62 KB			
10.0.44.41	lsharethis.com	00:00:05:2446720...		2.46 KB	1.65 KB	822.00 B			
10.0.44.41	addons.opera.c...	00:00:05:4157690...		6.59 KB	1.77 KB	4.82 KB			
52.230.80.159	10.0.44.41	00:00:13:1170150...		1.59 KB	1.59 KB	0.00 B			
10.0.44.41	webstat.likom.u...	00:00:09:1555680...		26.18 KB	2.99 KB	23.19 KB			
5.62.38.21	10.0.44.41	00:00:11:3899450...		336.00 B	336.00 B	0.00 B			
10.0.44.41	cstatcounter.com	00:00:15:0981090...		23.39 KB	3.44 KB	19.95 KB			
10.0.44.41	bacorecardrese...	00:00:09:9081930...		1.44 KB	999.00 B	480.00 B			
10.0.44.41	yimg.l.google.c...	00:00:05:5289600...		361.07 KB	5.34 KB	355.72 KB			

Tab IP Conversation ini sama hal kerjanya dengan IP EndPoint.

## 8. TCP Conversation

Node 1 ->	Port 1 ->	Node 2	Port 2	Packets	Bytes	Payload	Protocol	Interaction Diagram	Duration
10.044.41	50480	131.253.61.70	443	1	56.00 B	0.00 B	TCP		00:00:00.000000...
10.044.41	50484	internal.imap.mai...	993	2	110.00 B	0.00 B	TCP		00:00:00.0001390...
10.044.41	50500	131.253.61.70	443	35	12.52 KB	10.65 KB	HTTPS		00:00:01.4752520...
10.044.41	50495	52.114.32.5	443	35	16.11 KB	14.23 KB	HTTPS		00:00:05.5496400...
10.044.41	50493	52.114.32.5	443	33	10.68 KB	8.92 KB	HTTPS		00:00:13.8157600...
10.044.41	50296	13.107.452	80	1	56.00 B	0.00 B	TCP		00:00:00.0000000...
10.044.41	50297	13.107.452	80	1	56.00 B	0.00 B	TCP		00:00:00.0000000...
10.044.41	50522	www.unsri.ac.id	80	17	7.81 KB	6.89 KB	HTTP		00:00:03.6494750...
10.044.41	50536	scorintex.fbcdn...	443	14	4.53 KB	3.77 KB	HTTPS		00:00:05.0097500...
10.044.41	50528	star-mini.c10r.fac...	443	14	4.52 KB	3.76 KB	HTTPS		00:00:05.0275180...
10.044.41	50524	www.unsri.ac.id	80	6	350.00 B	0.00 B	TCP		00:00:05.0752200...
10.044.41	50523	www.unsri.ac.id	80	7	406.00 B	0.00 B	TCP		00:00:05.0788520...
10.044.41	50527	denis.unsri.ac.id	80	6	350.00 B	0.00 B	TCP		00:00:05.0740910...
10.044.41	50537	webstat.likom.uns...	80	8	482.00 B	0.00 B	TCP		00:00:04.9943990...

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

The screenshot shows the Wireshark interface with the 'UDP Conversation' pane selected. The main pane displays a list of UDP packets between Node 1 and Node 2. The selected packet (No. 1) shows a source IP of 10.0.44.53 and a destination IP of 224.0.0.252. The packet size is 247 bytes, with a payload of 75 bytes. The interface also shows a 'Packets' pane with a filter for '10.0.44.41:52332 <-> 8.8.8.8:53' and a 'Packets' list that is currently empty.

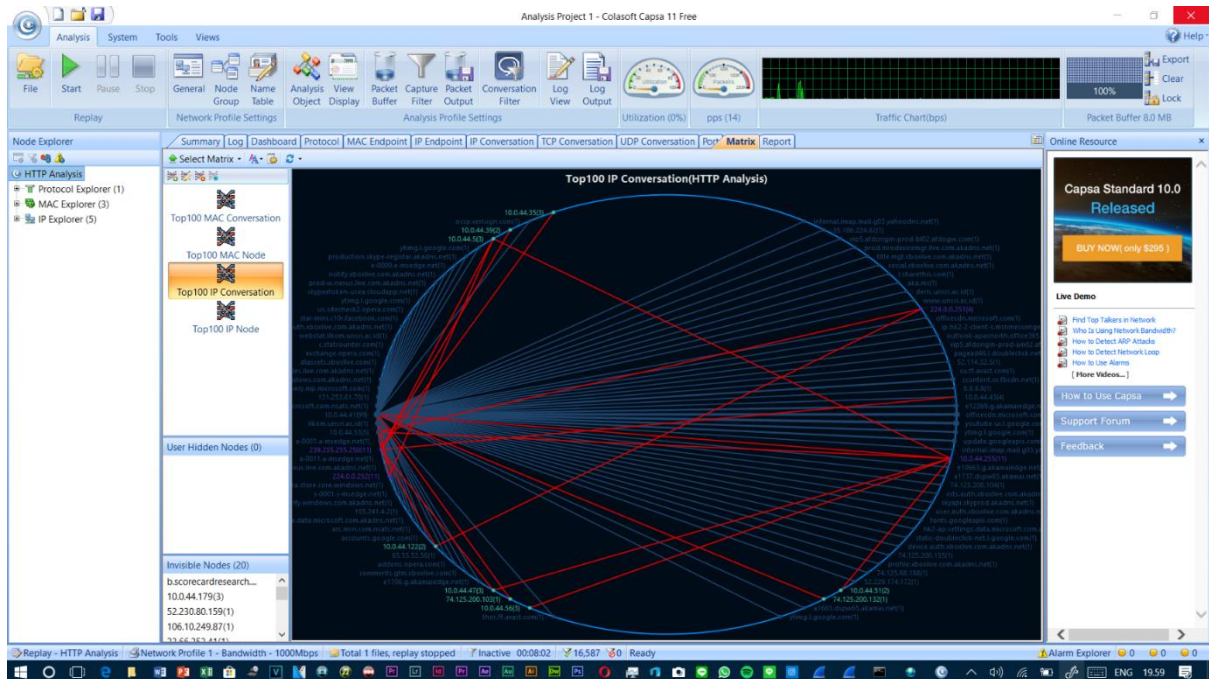
UDP Conversation biasanya digunakan untuk melihat aktivitas IP yang satu router, untuk melihat apa yang digunakan sebagai contoh pada baris kedua terlihat IP Source 10.0.44.53 berusaha menghubungi atau menerima packet data dari IP server yakni 224.0.0.252 dengan packet yang diterima berjumlah satu.

## 10. Port

The screenshot shows the Wireshark interface with the 'Port' pane selected. The main pane displays a list of ports and their associated protocols and services. The selected port (443) shows a server IP of 131.253.61.70, a protocol of TCP, and a common service of https. The interface also shows a 'TCP Conversation' pane with a filter for '10.0.44.41:50480 <-> 131.253.61.70:443' and a 'TCP Conversation' list showing various connections to the selected 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 gambaran 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 .