

“Analisa Packet Jaringan dengan Wireshark menggunakan Colosoft caps dan Bandingkan dengan Visual Route”

Wireshark merupakan aplikasi yang berguna untuk melihat atau menganalisa paket jaringan. Format protokol apapun dapat dengan mudah ditangkap menggunakan aplikasi ini, dalam kesempatan ini saya akan menganalisa paket yang tercapture saat membuka website ilkom.unsri.ac.id.



```
Wireshark - Follow TCP Stream (tcp.stream eq 23) - wireshark_44806349-0C0D-4F99-8E0A-61C0C0A32430_20180221192424_a06140

GET / HTTP/1.1
Host: ilkom.unsri.ac.id
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.167 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: ga=GA1.3.1949039789.1493196719; _gid=GA1.3.867224137.1519210968; wordfence_verifiedhuman=9abca4798d77a57e07e3993e0lea7b6; wfvit_613827598=5a8d648f1aad4; _pk_ref.1.da38-B38%2282282C%2282282C1519215771%228228221http%3A%2F%2Fderis.unsri.ac.id%2F%2282282D; _pk_ses.1.da38-*; sc_is_visitor_unique=rx10733571.1519215771.D968176363714f434404780287828FFD.4.4.3.3.3.3.3.2; _pk_id.1.da38=9e428c9efa2204e3.1595068488.4.1519216044.1519215771.

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 21 Feb 2018 12:27:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: wfvit_613827598=5a8d65a904ac4; expires=Wed, 21-Feb-2018 12:57:21 GMT; Max-Age=1800; path=/; httpOnly
Referrer-Policy: unsafe-url
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Link: <http://ilkom.unsri.ac.id/wp-json/>; rel="https://api.w.org/"
Content-Encoding: gzip
```

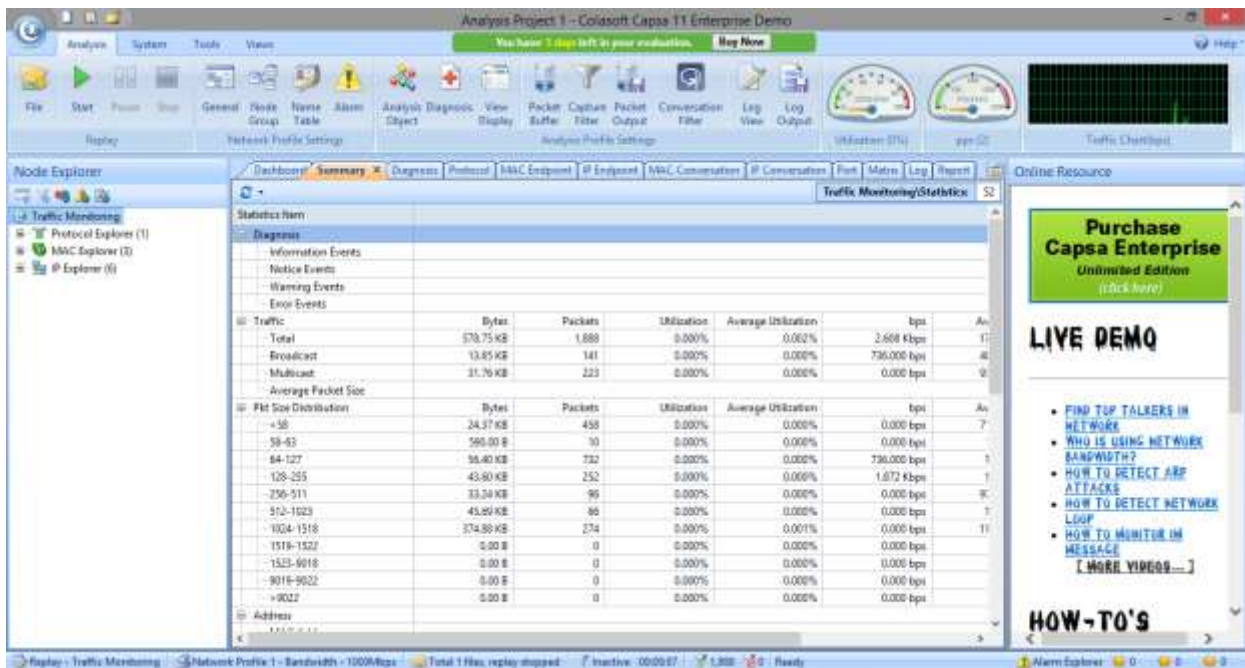
Ini adalah gambar paket data yang tercapture pada saat membuka website [ilkom](http://ilkom.unsri.ac.id), protokol yang saya screenshot di atas adalah TCP. Pada gambar diatas ada begitu banyak informasi yang bisa kita dapatkan, seperti :

1. Web yang kita kunjungi = ilkom.unsri.ac.id.
2. Koneksi pada saat akses tetap Hidup.
3. Browser yang digunakan kemungkinan Mozilla, Chrome, Safari.
4. Server Ubuntu.
5. Data terakhir dimodifikasi kamis, 21 Februari pada jam 12:27:22 GMT.
6. Content Encoding nya Gzip.

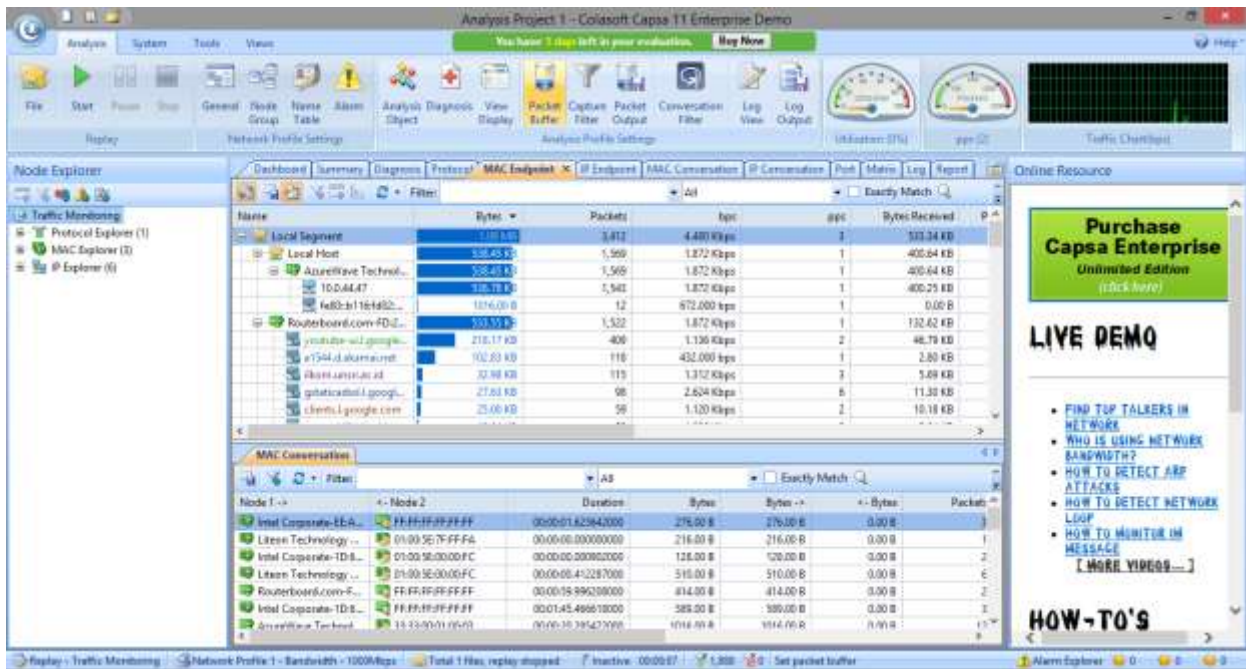
Kemudian buka file wireshark yang berisi paket data saat akses llkom.unsri.ac.id dengan menggunakan Colosoft Capsa 11.



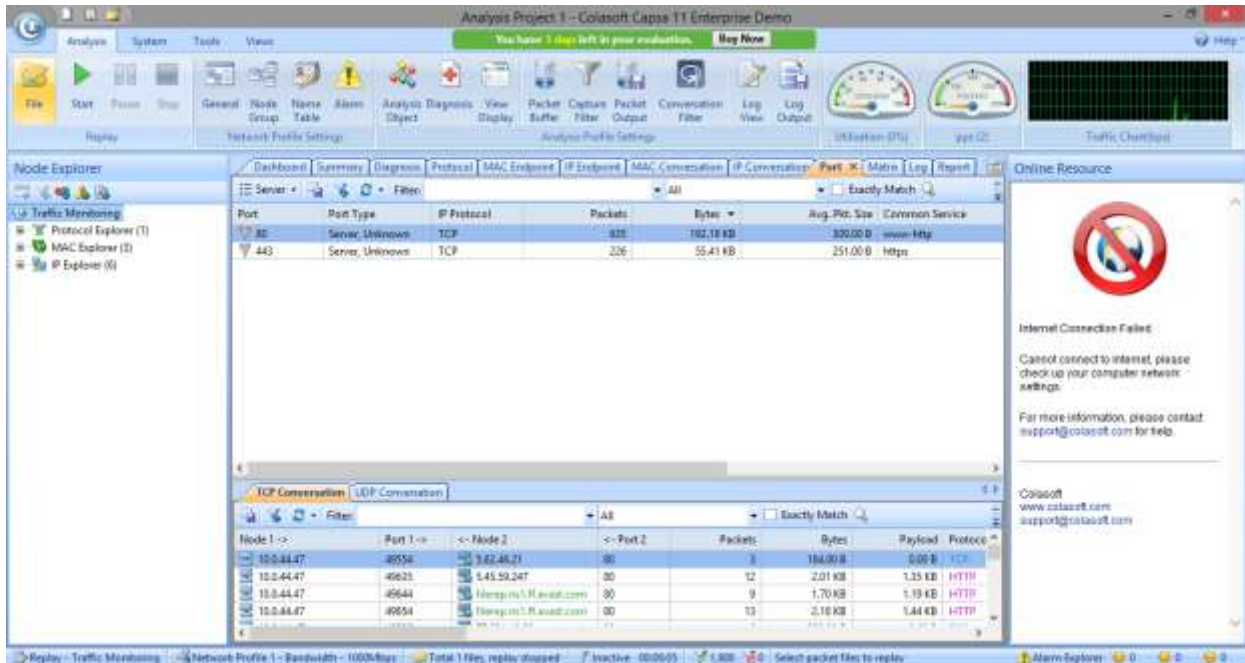
Ini adalah tampilan dashboard dari packet yang kita capture dengan wireshark, pada rentang waktu antara 19:27:23 sampai 19:27:23 total lalu lintas berdasarkan bytes pada paket yang kita akses adalah 175.56 KB.



Pada gambar kedua kita bisa melihat lalu lintas jaringan, total bytes yang dihabiskan untuk mengirim 1888 paket data adalah 578,75 KB.



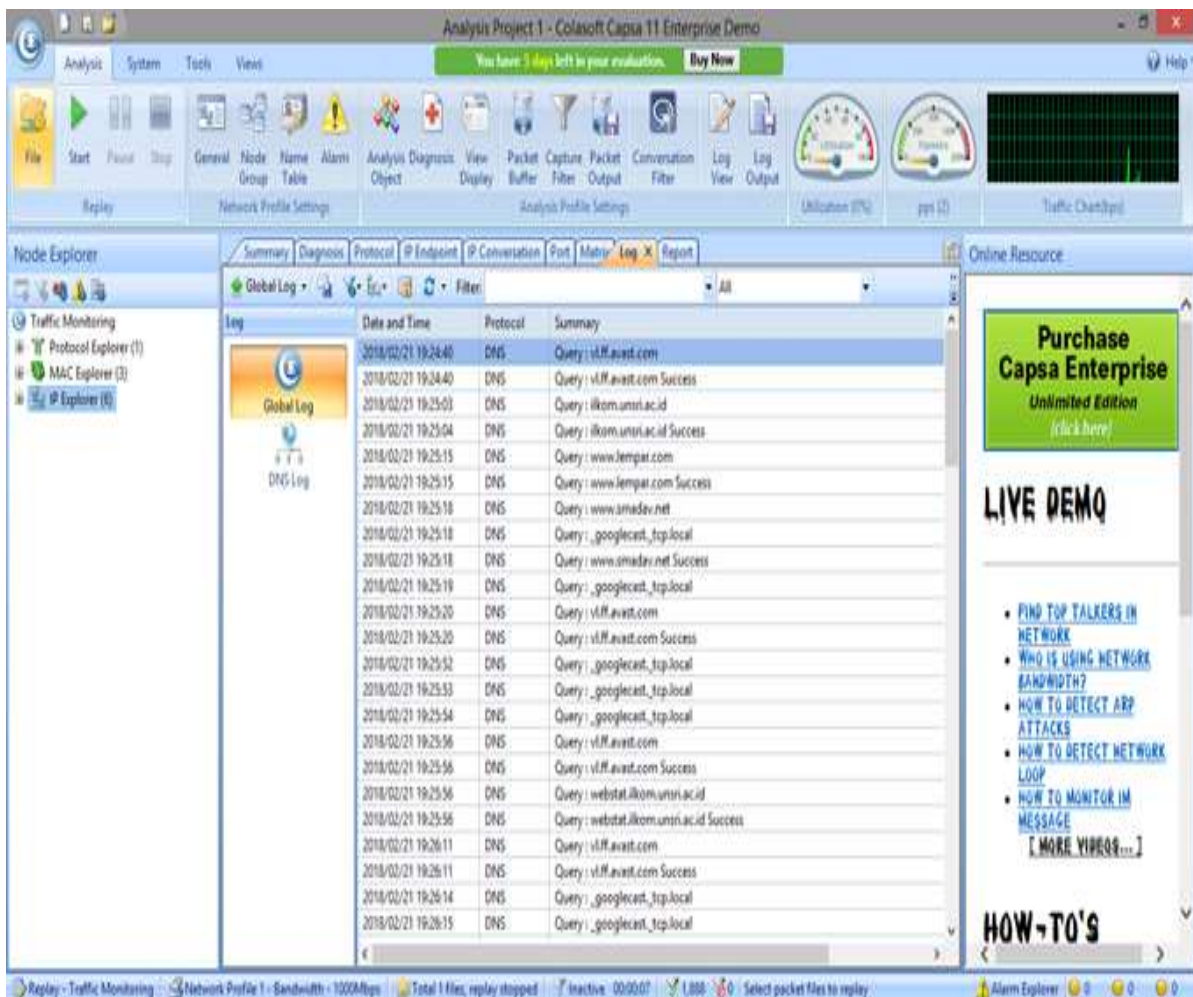
Dua gambar diatas adalah Protokol dan Mac endpoint paket data kita

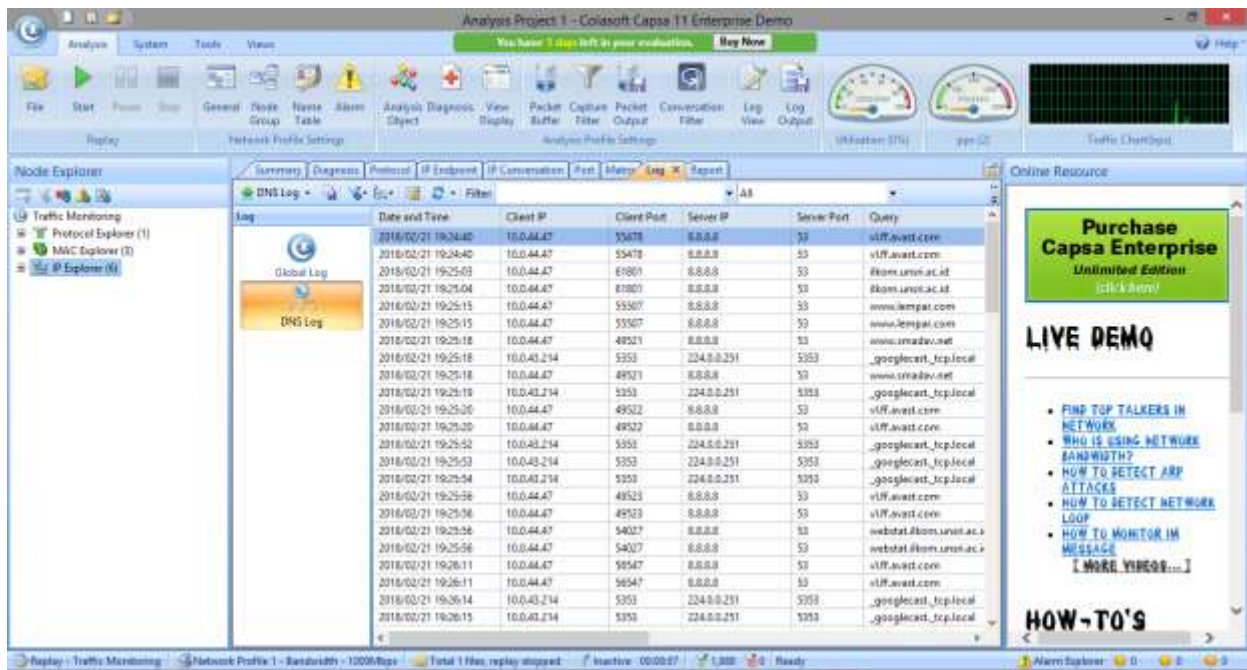


Pada Tab port kita bisa melihat port yang dipakai sever pada saat kita mengakses web yang kita tuju, port 80 adalah port yang dipakai web browser untuk melihat ip pada saat kita mengetikan hostname di web browser.

Sedangkan port 443 biasa disebut SSL atau Secure Socket Layer dimana port ini adalah port yang berfungsi untuk server yang terenkripsi.

Dari gambar diatas bisa dilihat kedua port menggunakan protokol TCP.





Gambar diatas merupakan tab log yang berisi log DNS dan log GLOBAL, pada log DNS kita bisa mendapatkan beberapa informasi sebagai berikut :

1. Waktu dan Tanggal akses
2. IP client
3. Port yang digunakan client
4. IP server
5. Port yang digunakan server
6. Query atau web yang melakukan komunikasi dengan kita

Contohnya pada tanggal 21, bulan 2, 2018, IP 10.0.44.47 (ip kita) mengakses lkom.unsri.ac.id melalui port client 61801, 8.8.8.8 adalah ip Google artinya kita akses menggunakan google melalui port 53.