

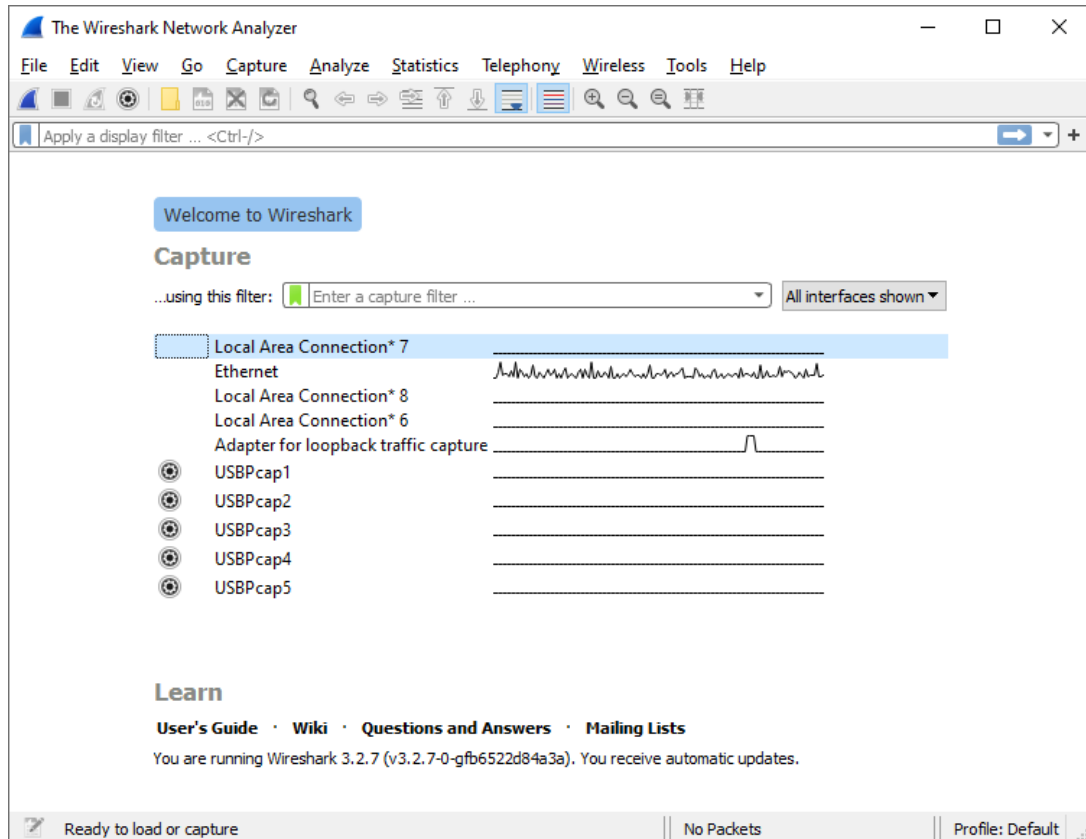
Nama : Loadtriani Oktavia

NIM : 215314172

MENGGUNAKAN WIRESHARK.

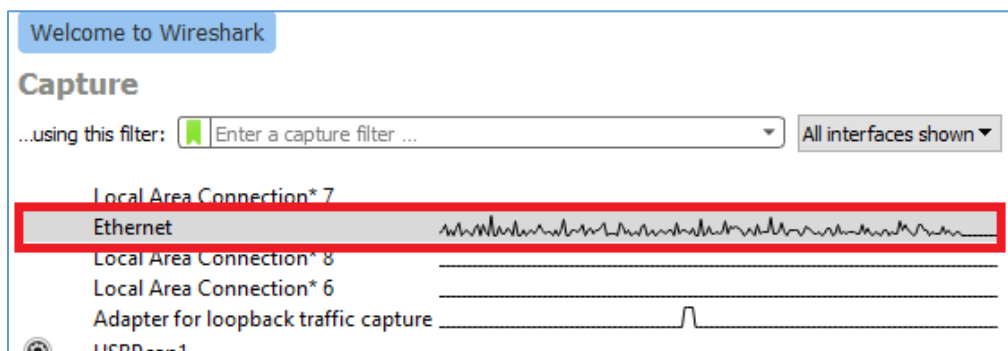
1. Mengamati Traffic Jaringan dengan WireShark

Setelah software wireshark di install, tampilan pertama wireshark saat di jalankan pertama kali :



Gambar 1. The Wireshark Network Analyzer

Klik pada Interface yang memiliki trafik data :

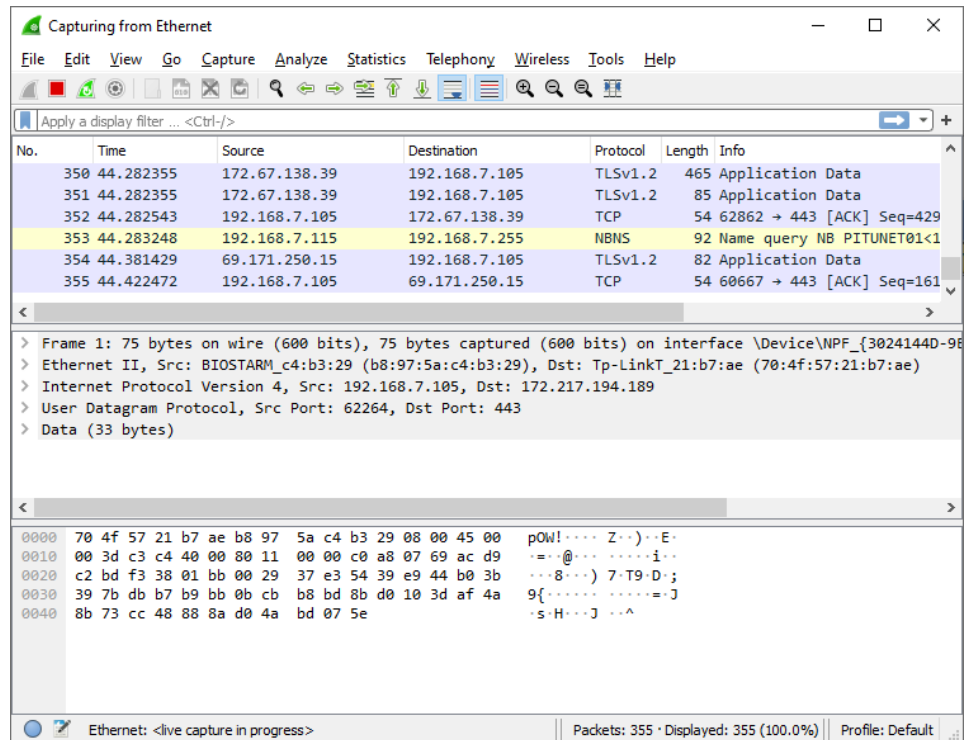


Gambar 2. Wireshark: Capture Interfaces

Nama : Loadtriani Oktavia

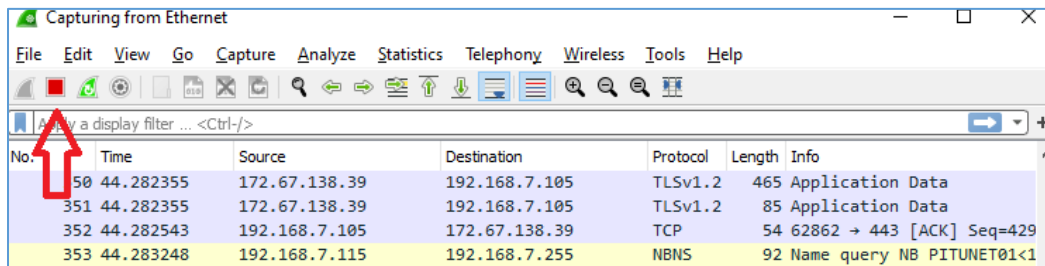
NIM : 215314172

Double klik pada interface yang dipilih maka akan ditampilkan layar scrolling yang berisikan paket-paket yang ditangkap.



Gambar 3 Proses Wireshark Analyzer

Untuk selesai menangkap paket, maka tinggal klik pada tombol yang ditunjukkan oleh panah berikut



Gambar 4. Stop proses Analyzer

Nama : Loadtriani Oktavia

NIM : 215314172

2. Percobaan Pengiriman Data TCP

- 1). Buka web browser, dan arahkan ke :

<http://gaia.cs.umass.edu/wireshark-labs/alice.txt>

- 2). Simpan file **alice.txt** pada folder yang anda tentukan.

- 3). Selanjutnya arahkan web browser ke :

<http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>

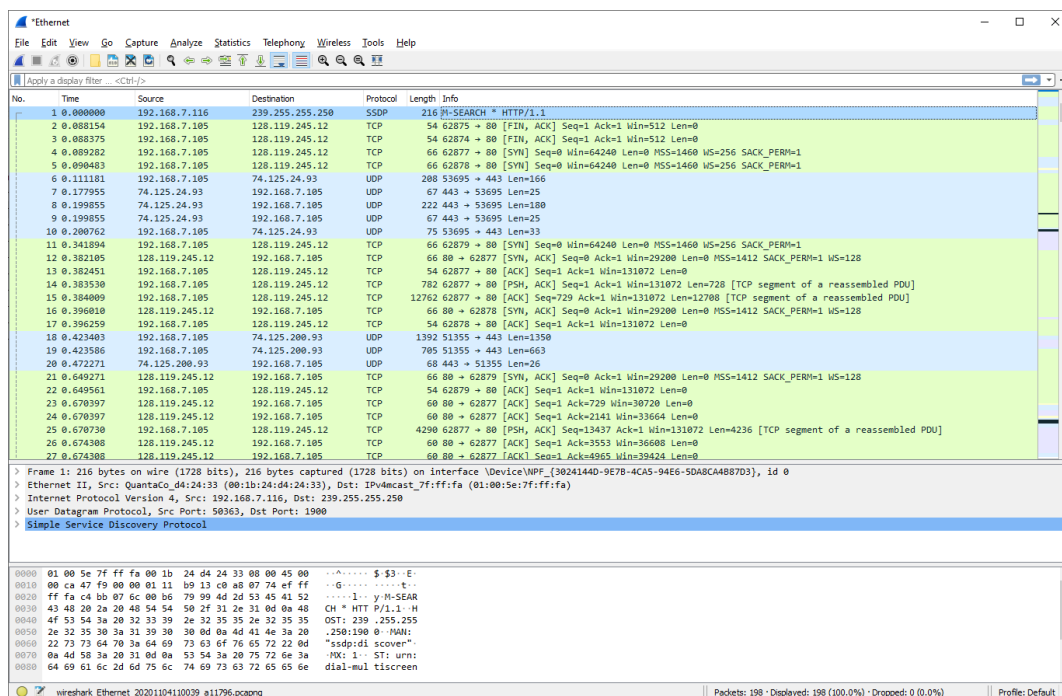
Web tersebut untuk mengupload file alice.txt ke sisi server tersebut. **Jangan diklik upload terlebih dahulu.**

- 4). Jalankan wireshark untuk memulai menangkap paket data yang lewat. **Stop dahulu capture jaringan yang aktif saat ini.**

- 5). Klik upload pada langkah 3 untuk memulai proses pengiriman data dari client ke server.

Setelah ter-upload, maka akan ada pesan keberhasilan proses.

- 6). Stop wireshark. Sehingga akan terlihat seperti berikut :



Gambar 5 Hasil Capture

- 7). Filterlah wireshark diatas dengan mengetikkan "tcp" pada bagian filter.

Nama : Loadtriani Oktavia

NIM : 215314172

3. Jawab Pertanyaan Dasar Protokol TCP berikut:

1. Berapa no IP dan port number TCP yang digunakan oleh client dan server
 - No IP client: 192.168.1.9
 - No IP server : 54.85.100.197
 - Port Number client : 60077
 - Port Number server : 80
2. Berapa sequence number dari TCP SYN segmen yang digunakan untuk memulai koneksi TCP antara client dan server ?
SYN : 0(2129608727)

3. Berapa sequence number dari segmen SYNACK yang dikirim oleh server ke client ?
SYN : 0(3704761662)

Berapa nilai dari ACK dari segmen SYNACK tersebut ?

ACK : 1(3680367623)

4. Carilah 6 segmen pertama dalam koneksi TCP setelah terjadinya 3-way handshake ?

Amati perbedaan dari tiap segmen TCP dikirim sampai ACK diterima. Berapa nilai RTT dari masing-masing 6 segmen yang pertama tersebut ?

Client Hello : iRTT(0.044247000)

Application Data : iRTT(0.026918000)

[ACK] : iRTT (0.044247000)

Server Hello : (0.044247000)

TCP Previous segment (0.044247000)

TCP Previous segment (0.044247000)

Berapa panjang (byte) dari masing-masing 6 segmen TCP yang pertama ?

Bytes Client Hello: 591

Application Data : 139

{ACK} : 74

Nama : Loadtriani Oktavia

NIM : 215314172

Server Hello : 1294

TCP Previous segment : 1294

TCP Previous segment : 1294

5. Apakah ada segmen yang dikirim ulang ? Bagaimana anda mengeceknya ?

Dengan menggunakan tcp.analysis.retransmission

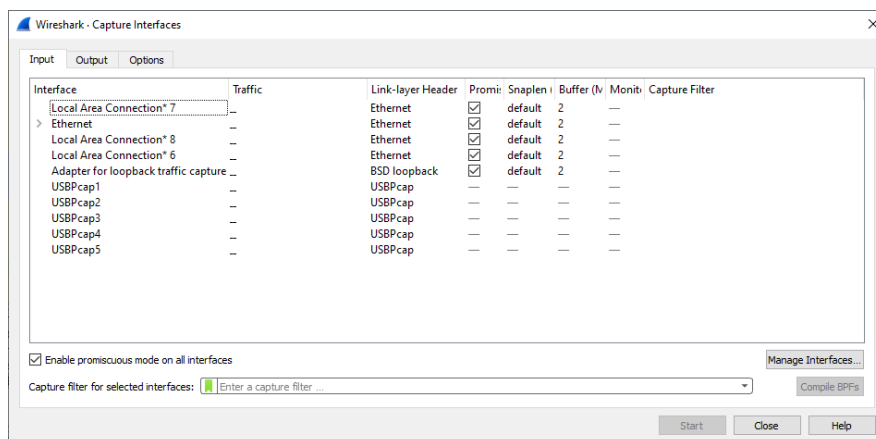
No.	Time	Source	Destination	Protocol	Length	Info
197.20.364932	162.159.134.234	192.168.1.9	TCP	130	[TCP Spurious Retransmission]	443 → 58230 [PSH, ACK] Seq=1935 Ack=55 Win=8 Len=76
261.31.750158	162.159.134.234	192.168.1.9	TCP	105	[TCP Spurious Retransmission]	443 → 58230 [PSH, ACK] Seq=3085 Ack=55 Win=8 Len=51
281.36.287007	162.159.134.234	192.168.1.9	TCP	132	[TCP Spurious Retransmission]	443 → 58230 [PSH, ACK] Seq=3136 Ack=55 Win=8 Len=78
641.94.203706	162.159.136.234	192.168.1.9	TCP	137	[TCP Spurious Retransmission]	443 → 56797 [PSH, ACK] Seq=5716 Ack=2672 Win=65536 Len=83
965.133.892568	137.221.106.103	192.168.1.9	TCP	1434	[TCP Spurious Retransmission]	443 → 56835 [PSH, ACK] Seq=1 Ack=206 Win=22080 Len=1380
1267.173.506005	2001:448a:404b:1d32	2003:2880:f25c:c3:f...	TCP	1466	[TCP Retransmission]	56854 → 443 [PSH, ACK] Seq=1521 Ack=489 Win=66304 Len=1392
1278.173.806038	2001:448a:404b:1d32	2003:2880:f25c:c3:f...	TCP	1466	[TCP Retransmission]	56854 → 443 [PSH, ACK] Seq=4800 Ack=489 Win=66304 Len=1392
3865.370.384011	162.159.136.234	192.168.1.9	TCP	132	[TCP Spurious Retransmission]	443 → 56797 [PSH, ACK] Seq=25493 Ack=3656 Win=65536 Len=78
4382.428.589263	20.198.118.190	192.168.1.9	TCP	227	[TCP Spurious Retransmission]	443 → 52251 [PSH, ACK] Seq=1904 Ack=1237 Win=8192 Len=173
4598.429.784824	2001:448a:404b:1d32	2060:1901:11:c36::	TCP	655	[TCP Retransmission]	50958 → 443 [PSH, ACK] Seq=1 Ack=1 Win=64768 Len=581
5691.451.708744	137.221.105.136	192.168.1.9	TLSv1.2	1434	[TCP Fast Retransmission]	, Server Hello
6232.456.790201	192.168.1.9	162.159.138.234	TCP	139	[TCP Retransmission]	52665 → 443 [PSH, ACK] Seq=2610 Ack=4948 Win=65824 Len=85
8012.469.955961	192.168.1.9	162.159.136.234	TCP	108	[TCP Retransmission]	56797 → 443 [PSH, ACK] Seq=5157 Ack=37374 Win=65280 Len=54
10507.487.623428	162.159.136.234	192.168.1.9	TCP	480	[TCP Spurious Retransmission]	443 → 56797 [PSH, ACK] Seq=38308 Ack=5211 Win=65536 Len=426
12337.501.701517	192.168.1.9	162.159.138.234	TCP	139	[TCP Retransmission]	52665 → 443 [PSH, ACK] Seq=5744 Ack=5176 Win=64768 Len=85
12807.507.023688	162.159.136.234	192.168.1.9	TCP	139	[TCP Spurious Retransmission]	443 → 56797 [PSH, ACK] Seq=41650 Ack=5314 Win=65536 Len=85
14092.517.277232	137.221.105.136	192.168.1.9	TCP	54	[TCP Retransmission]	443 → 59327 [FIN, ACK] Seq=3472 Ack=3013 Win=63480 Len=0
14959.527.437522	192.168.1.9	20.212.86.199	TCP	212	[TCP Retransmission]	59353 → 443 [PSH, ACK] Seq=216 Ack=7142 Win=262144 Len=158
15227.529.645522	104.16.119.50	192.168.1.9	TLSv1.3	1506	[TCP Fast Retransmission]	, Application Data

Frame 1332185: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{057421D0-A351-4356-B52F-4BE4725F5965}, id 0
Ethernet II, Src: zte Ad:64:c6 (ec:6c:b5:4d:64:c6), Dst: TP-Link 01:06:9e (7c:c2:c6:01:06:9e)
Internet Protocol Version 6, Src: 2404:6800:4001:c11:71, Dst: 2001:448a:404b:1d32:397f:946:4e0b:c4fc
Transmission Control Protocol, Src Port: 443, Dst Port: 58989, Seq: 0, Ack: 1, Len: 0

```
0000  7c c2 c6 01 06 9e ec 6c b5 4d 64 c6 86 dd 64 00  |.....1 Hd...d|
0010  64 67 00 20 06 77 24 04 68 00 40 03 0c 11 00 00  |dg..s.h@...|
0020  00 00 00 00 00 71 20 01 44 8a 4b 1d 32 39 7f  |...q.DK.29|
0030  09 46 4e 0b c4 fc 01 bb e6 13 15 de e7 21 b0 96  |FN...I...|
0040  c9 96 80 12 ff ff 1f c3 00 00 02 04 05 98 01 01  |.....|
0050  04 02 01 03 03 00  |.....|
```

4. Lebih lanjut tentang Capture Options pada Interface

4.1. Pelajari dan jelaskan menu dari Capture --> Options... (Input, Output dan Options) berikut ini

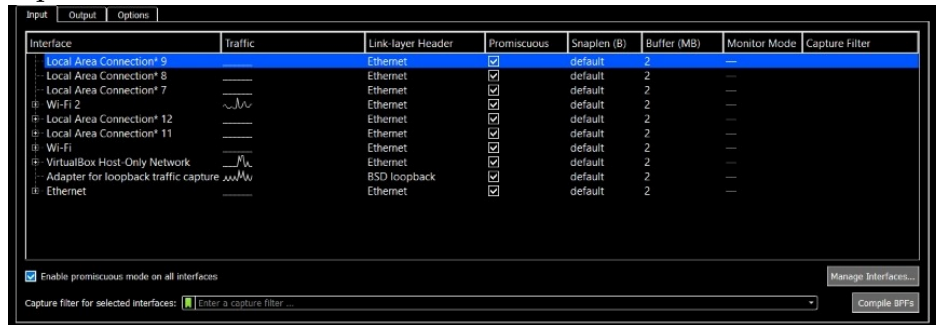


Gambar 6 Opsi Capture

Nama : Loadtriani Oktavia

NIM : 215314172

- Input



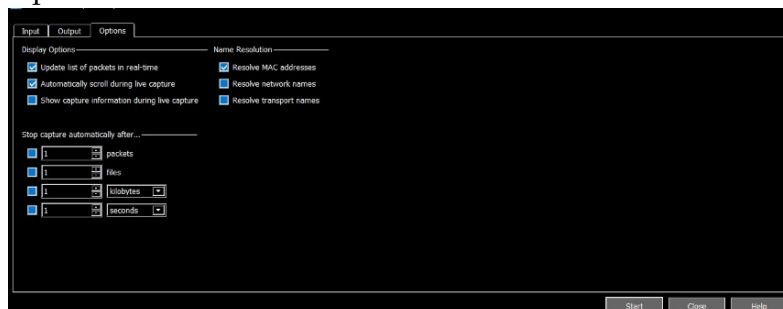
Pada input ini berfungsi untuk menangkap interface yang ada dan kemudian memberikan traffic agar pengguna dapat melihat interface apa saja yang sedang berjalan. Link layer header berguna sebagai pemberitahu dari mana asal dari interface-interface tersebut. Promiscuous adalah mode untuk dimana semua paket data jaringan dapat di akses dan dilihat oleh semua adapter jaringan.

- Output



Pada output pengguna dapat memasukan file yang ingin di gunakan kemudian di berikan 2 pilihan format yaitu pcapng atau pcap. Pada out ini juga pengguna dapat membuat hal baru secara otomatis dengan cara mengisi seluruh after sesuai yang di inginkan.

- Options

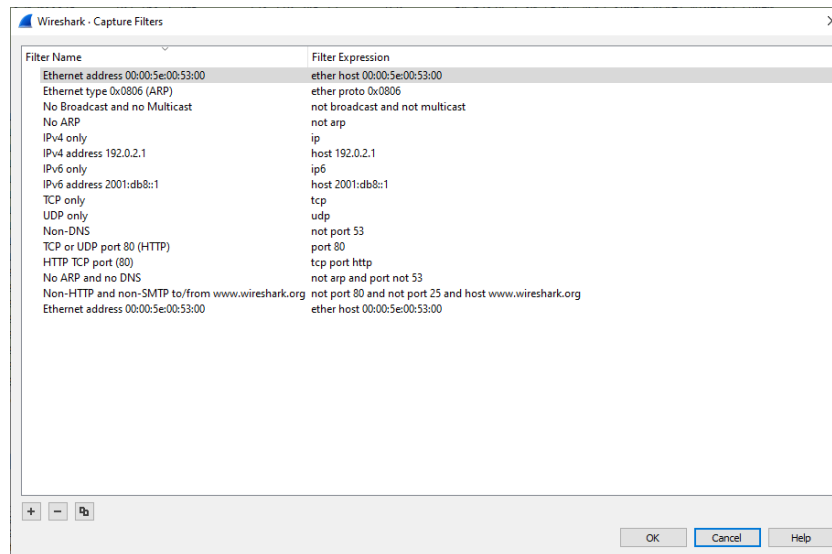


Nama : Loadtriani Oktavia

NIM : 215314172

Pada options ini berguna untuk pengguna mengatur mau seperti apa display optionsnya bisa dengan mengupdate list paket secara real-time, bisa otomatis mengscroll selama live capture, atau juga mau menampilkan informasi capture selama live capture. Pengguna juga bisa mengatur ingin menggunakan nama resolusi apa. Pengguna juga bisa menghentikan capture secara otomatis. Misal pengguna ingin menghentikan ketika packets 2, files 2, 4 kb, 4 second. Setelah capture mencapai angka yang di pilih maka capture akan otomatis berhenti.

4.2. Pelajari dan jelaskan menu dari Capture --> Capture Filter berikut ini (termasuk tombol add, remove, dan copy) :



Gambar 6. Opsi Capture

- Pada capture filters ini berguna untuk melihat, menambahkan, mengurangi atau menyalin nama filter atau ekspresi filter. Filter name berguna untuk menampilkan nama-nama yang terdapat pada filter. Filter expression sebagai ekspresi dari filter name yang ada. Tanda + berguna untuk menambahkan filter name, remove berguna untuk menghapus filter yang tidak di inginkan dan copy berguna untuk menyalin filter yang di inginkan.

2. Mengamati Traffic Jaringan dengan Packet Tracer

- Amati paket TCP dan UDP dari aplikasi WEB, FTP, DNS, dan VoIP dari packet tracer lab8.pkt
- Buatlah analisis lapisan transport dari aplikasi di atas:
 - Nomor Socket, protokol UDP atau TCP dan proses pengawalan koneksi dan data sensitif (misal password dan username)

Selamat belajar ☺