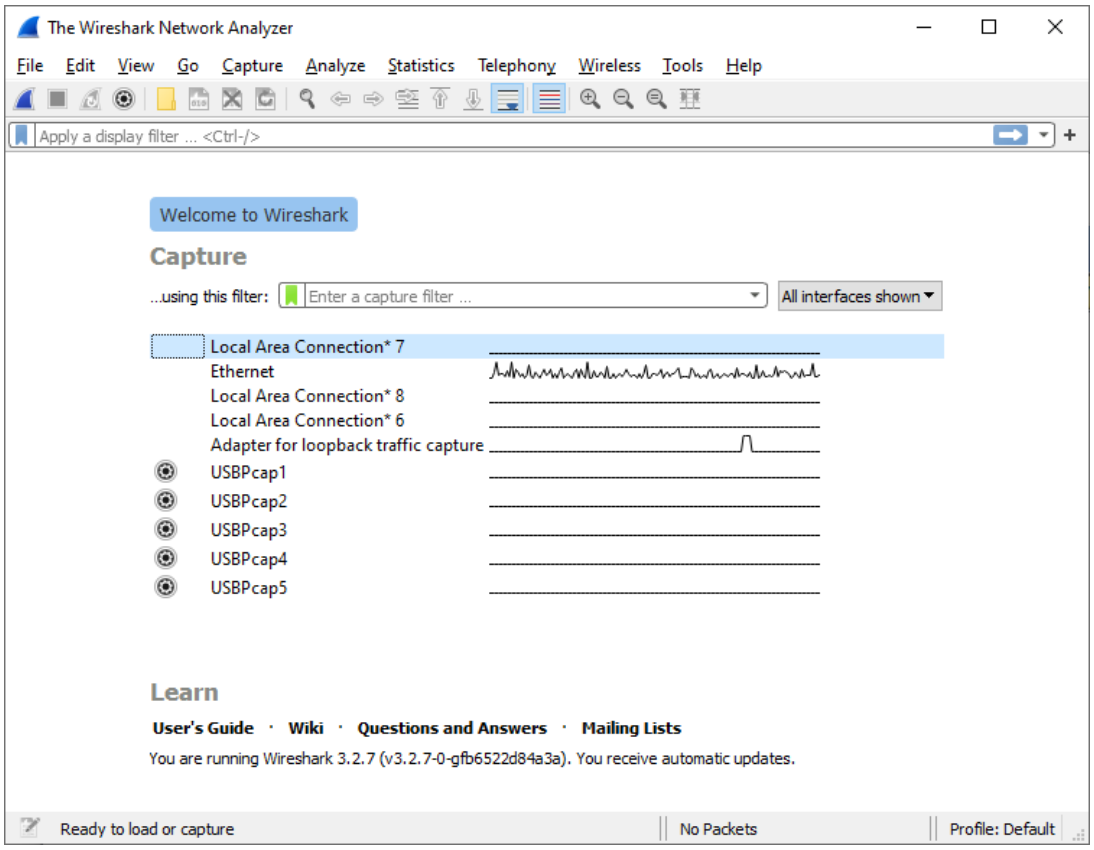
Nama : Loadtriani Oktavia
NIM : 215314172

MENGGUNAKAN WIRESHARK.

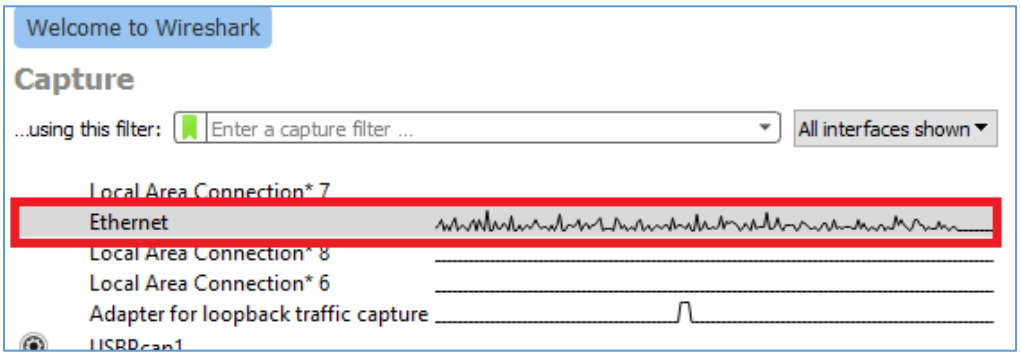
1. Mengamati Traffic Jaringan dengan WireShark

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



Gambar 1. The Wireshark Network Analyzer

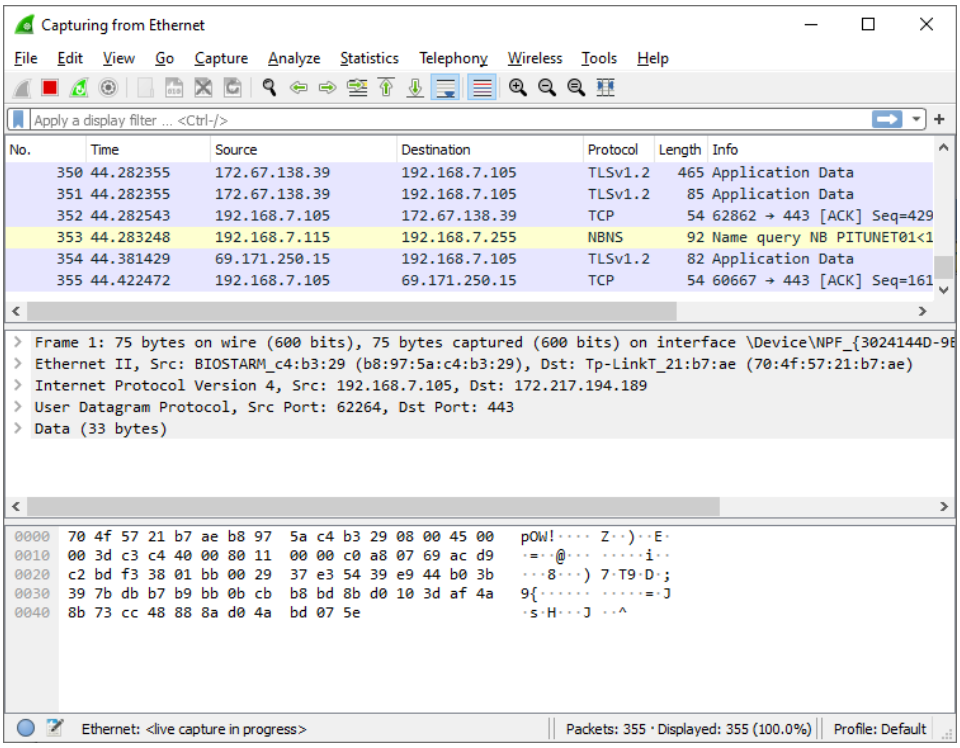
Klik pada Interface yang memiliki trafik data :



Gambar 2. Wireshark: Capture Interfaces

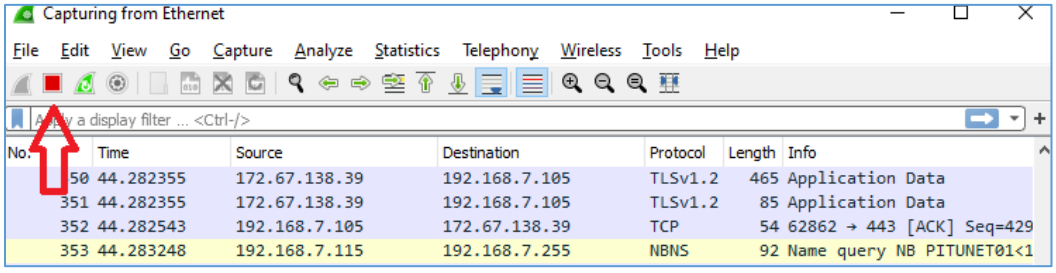
Nama : Loadtriani Oktavia
NIM : 215314172

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

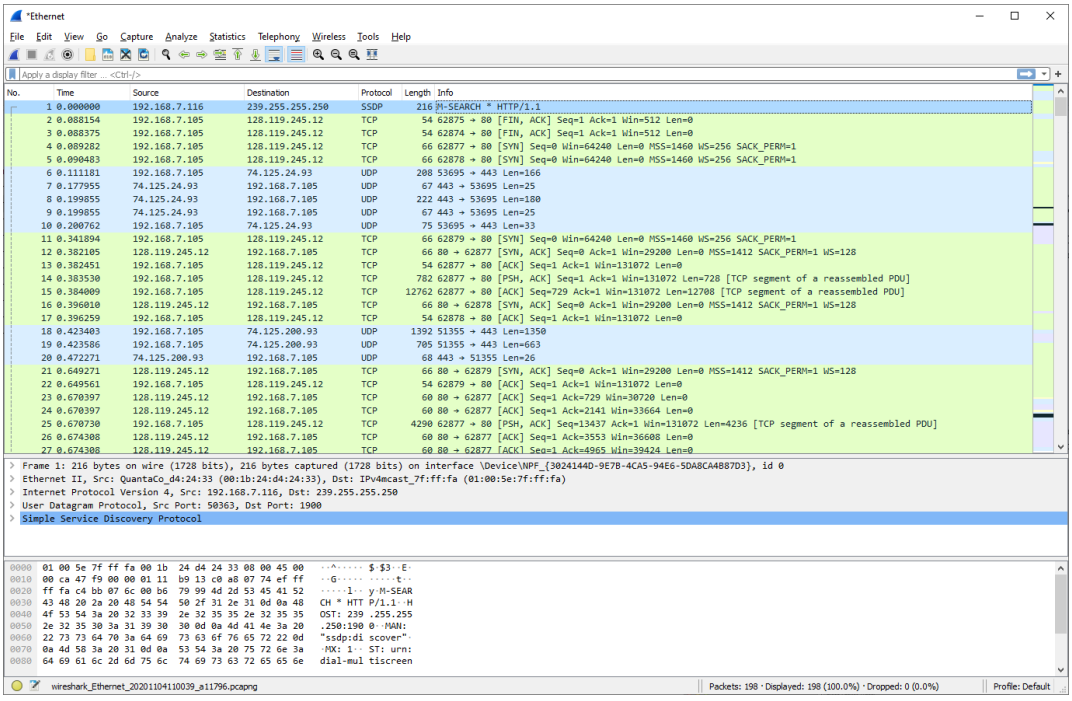
Web tersebut untuk mengupload file alice.txt ke sisi server tersebut. Jangan diklik upload terlebih dahulu.

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

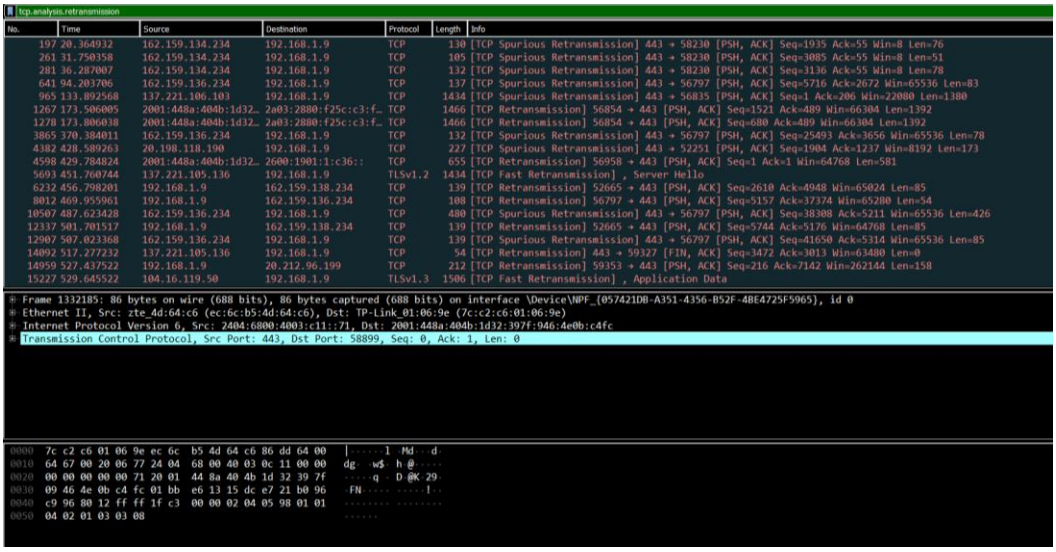
Server Hello : 1294

TCP Previous segment : 1294

TCP Previous segment : 1294

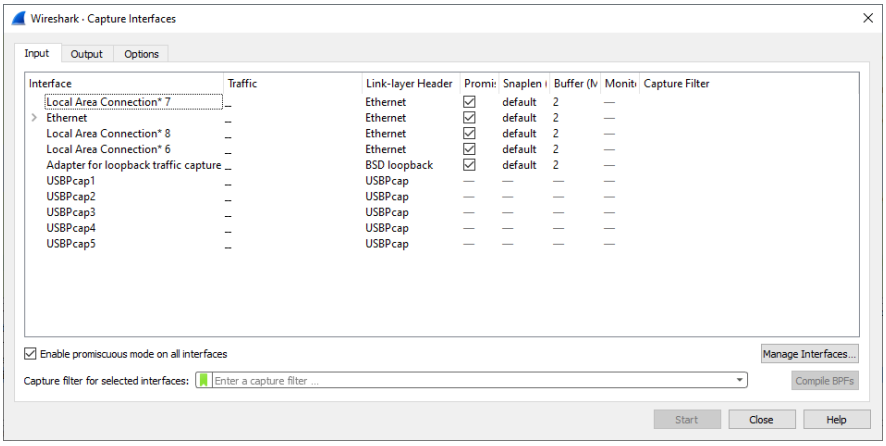
5. Apakah ada segmen yang dikirim ulang ? Bagaimana anda mengeceknya ?

Dengan menggunakan tcp.analysis.retransmission



4. Lebih lanjut tentang Capture Options pada Interface

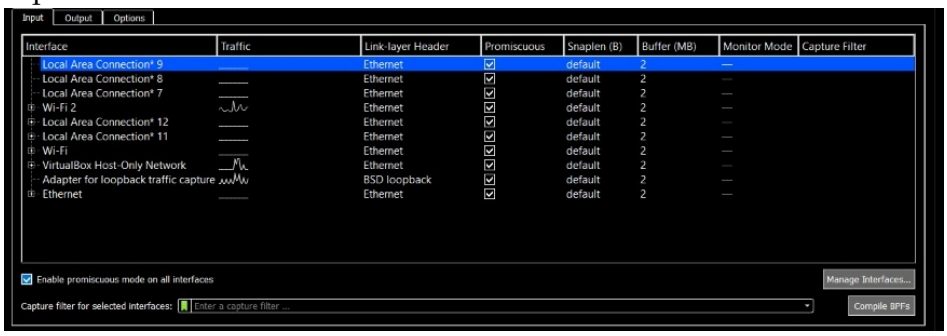
4.1. Pelajari dan jelaskan menu dari Capture --> Options... (Input, Output dan Options) berikut ini



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 semuda paket data jaringan dapat di akses dan dilihat oleh semua adapter jaringan.

- Output

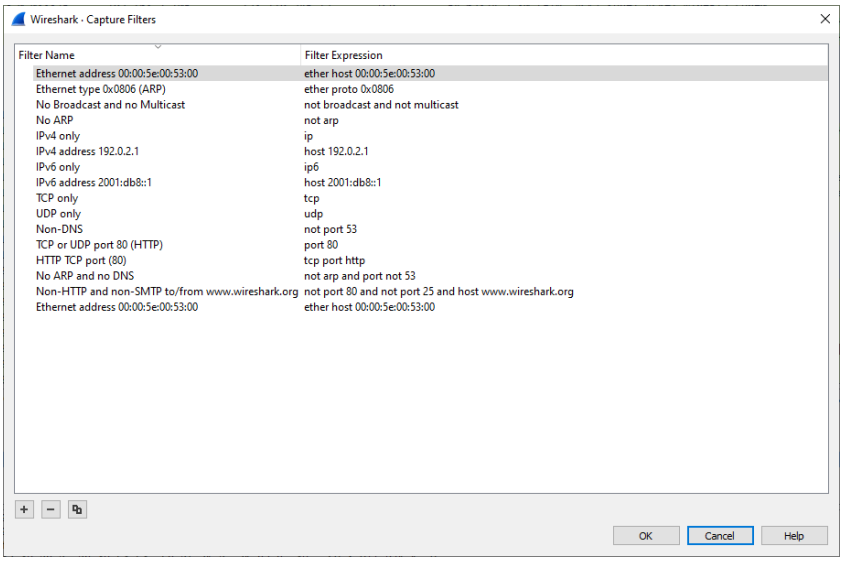
Pada output pengguna dapat memasukan file yang ingin di gunakan kemudian di berikan 2 pilihan format yaitu pcapng atau pcap. Pada out ini juga pengguna dapat membuat hal baru secara otomatis dengan cara mengisi seliruh after sesuai yang di inginkan.

- Options

Nama : Loadtriani Oktavia
NIM : 215314172

Pada options ini berguna untuk pengguna mengatus 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 mengatus ingin menggunakan nama resolusi apa. Pengguna juga bisa menghentikan capture secara otomatis. Missal 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 ekxpresi dari filter name yang ada. Tanda aad 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 ☺