MODUL 1
WIRESHARK

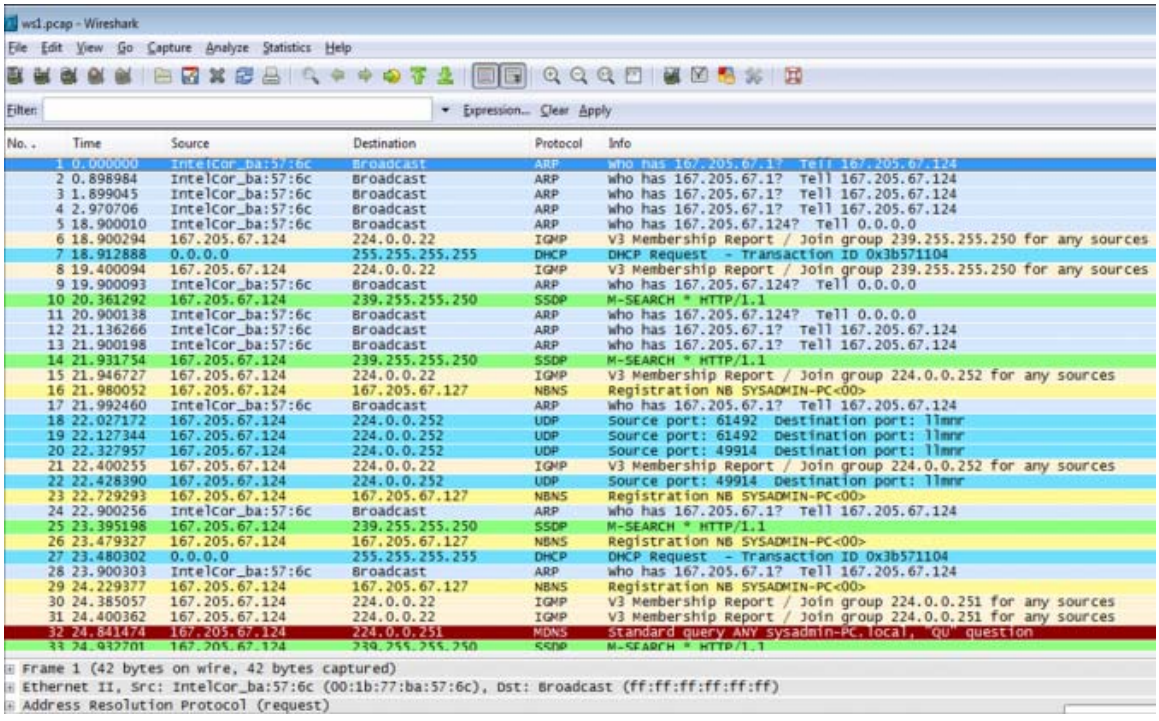
TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep wireshark
2. Mahasiswa memahami konsep pengiriman dengan traceroute
3. Mahasiswa memahami proses fragmentasi

DASAR TEORI

Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

Wireshark dapat membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN , dan koneksi ATM.

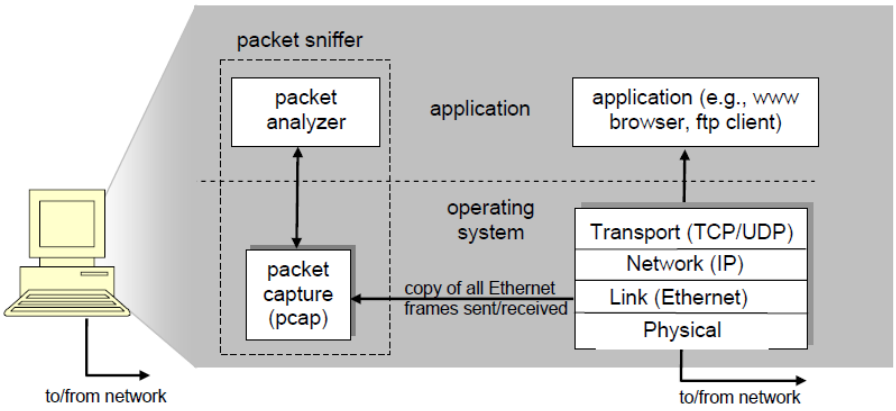


Gambar 1. Tampilan wireshark

Tools ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan

menangkap paket-paket yang berjalan di dalam jaringan dan menganalisanya. Namun tools ini hanya bisa bekerja didalam dalam jaringan melalui LAN/Ethernet Card yang ada di PC

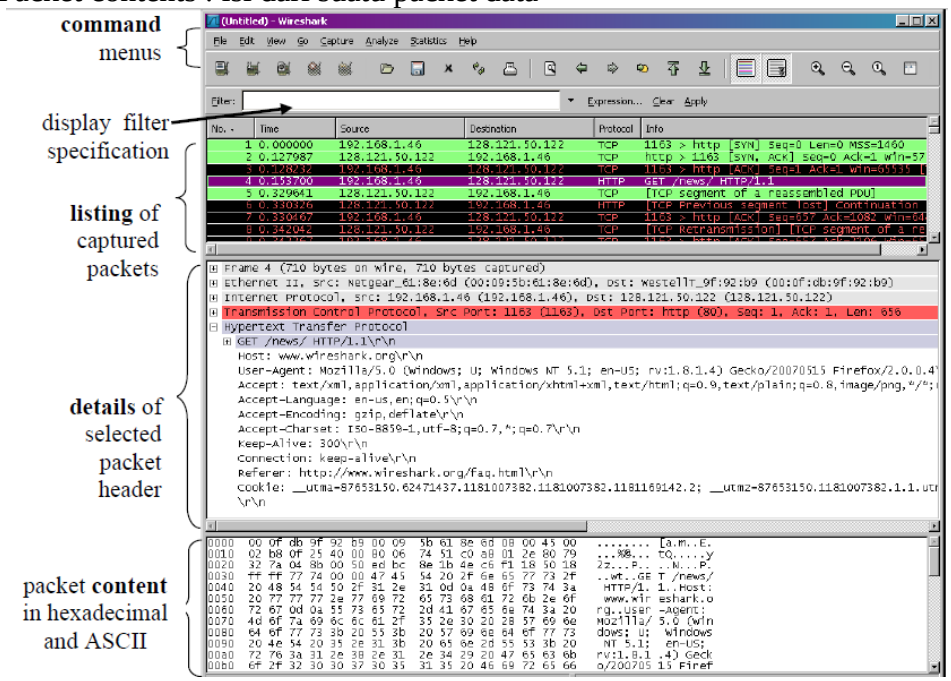
Untuk struktur dari packet sniffer terdiri dari 2 bagian yaitu packet analyzer pada layer application dan packet capture pada layer operating system (kernel).



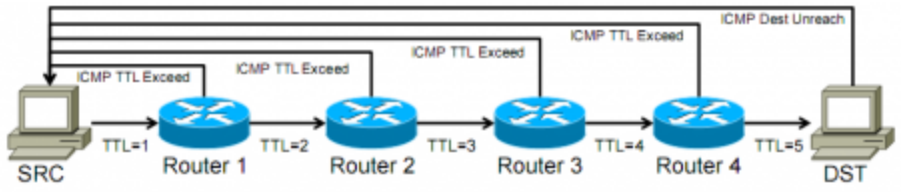
Gambar 2. Struktur Packet Sniffer

Struktur dari wireshark graphical user interface adalah sebagai berikut :

a. Command menu
b. Display filter specification : untuk memfilter packet data
c. Listing of captured packets : paket data yang tertangkap oleh wireshark
d. Details of selected packet header : data lengkap tentang header dari suatu packet
e. Packet contents : isi dari suatu packet data



Gambar 3. Struktur Wireshark



Untuk mengetahui jalur yang ditempuh untuk mencapai suatu node, traceroute mengirimkan 3 buah paket probe tipe UDP dari port sumber berbeda, dengan TTL bernilai 1. Saat paket tersebut mencapai router next-hop, TTL paket akan dikurangi satu sehingga menjadi 0, dan router next-hop akan menolak paket UDP tersebut sembari mengirimkan paket ICMP Time-to-Live Exceeded ke node asal traceroute tersebut. Dengan cara ini, pengirim traceroute tahu alamat IP pertama dari jalur yang ditempuh.

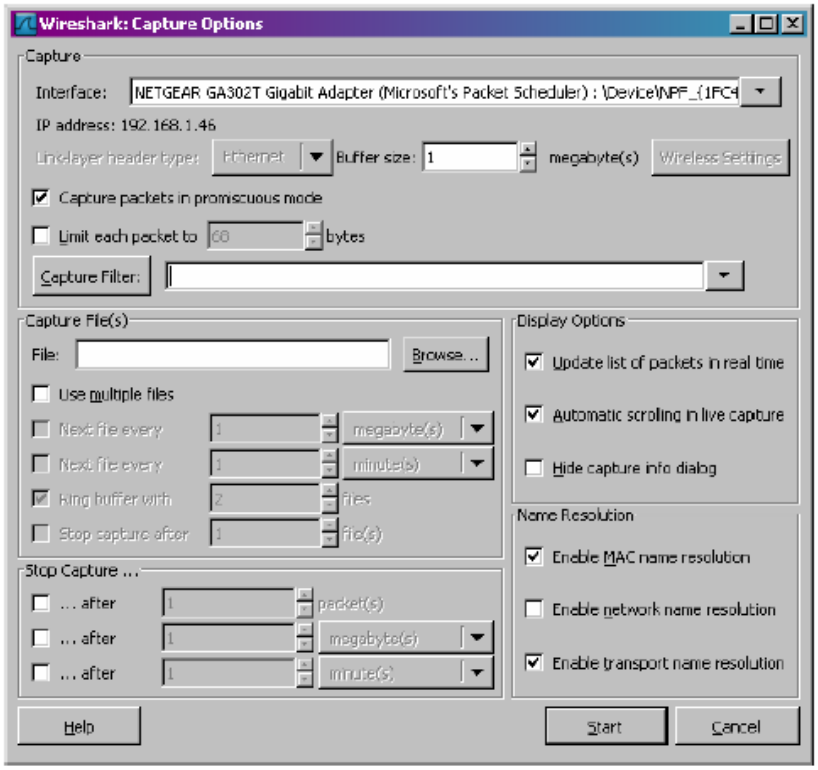
TUGAS PENDAHULUAN

1. Download paket wireshark dan pingplotter dari http://lecturer.eepis-its.edu/~zenhadi/kuliah/NGN

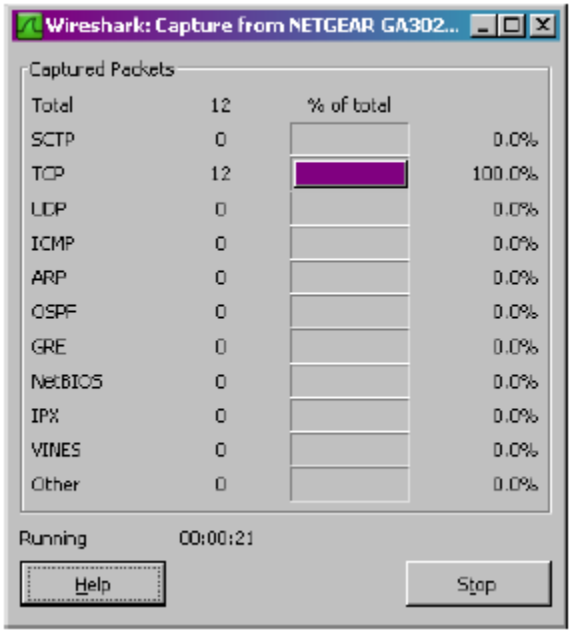
PERCOBAAN

A. Pengenalan Wireshark

1. Bukalah wireshark. Dan mulai mengcapture paket data dengan memilih Capture | Options. Pilihlah interface card yang digunakan untuk menangkap paket data yang lewat seperti gambar berikut.

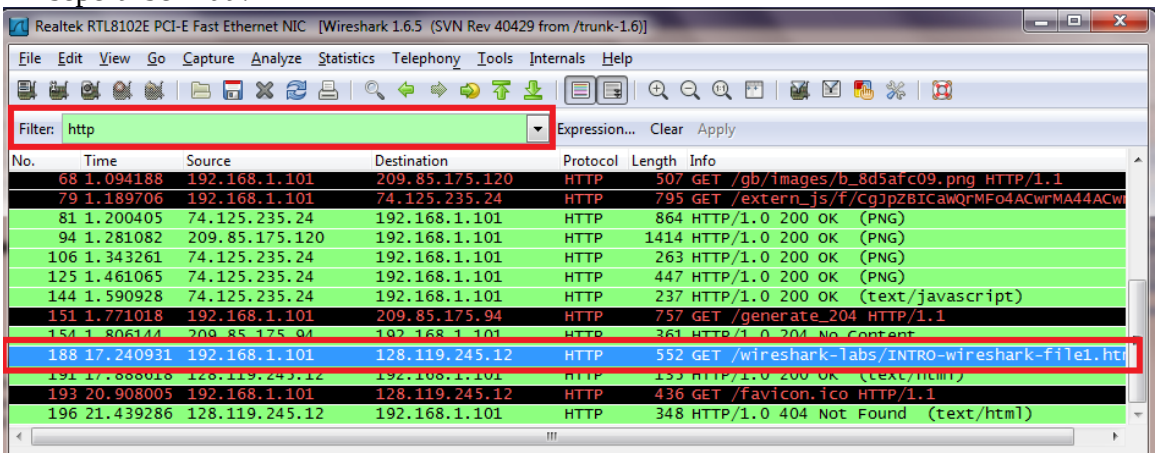


2. Mulai lakukan pengamatan data dengan menekan tombol start :



3. Sementara wireshark jalan, lakukan koneksi ke :
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

   Setelah muncul tampilan pada browser kemudian stop wireshark, Capture | Stop. Perhatikan pada bagian Protocol, ada banyak protocol yang ditampilkan.
   Untuk memfilter hanya protocol http saja yang ditampilkan lakukan filtering seperti berikut :



   Catat dan amati header paket dan content datanya.

4. Dari HTTP GET message diatas yang dikirim dari komputer anda ke gaia HTTP server. Amatilah data berikut pada informasi header packet dan juga content informasi yang dikandungnya :
   a. Ethernet frame
   b. IP datagram

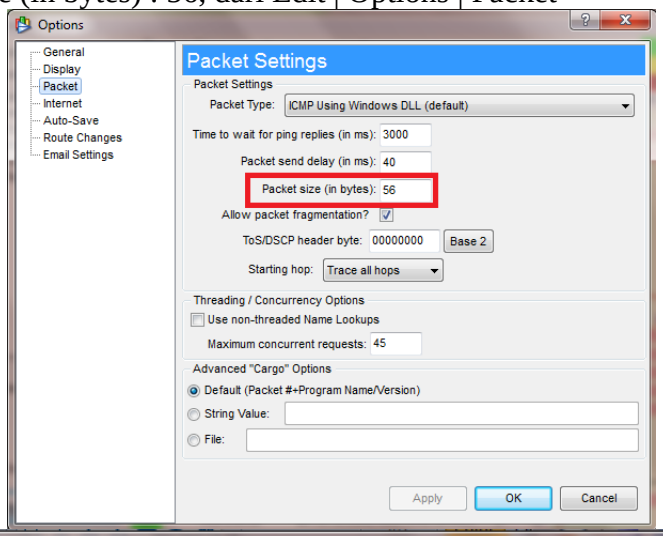
c. TCP segment
d. HTTP message

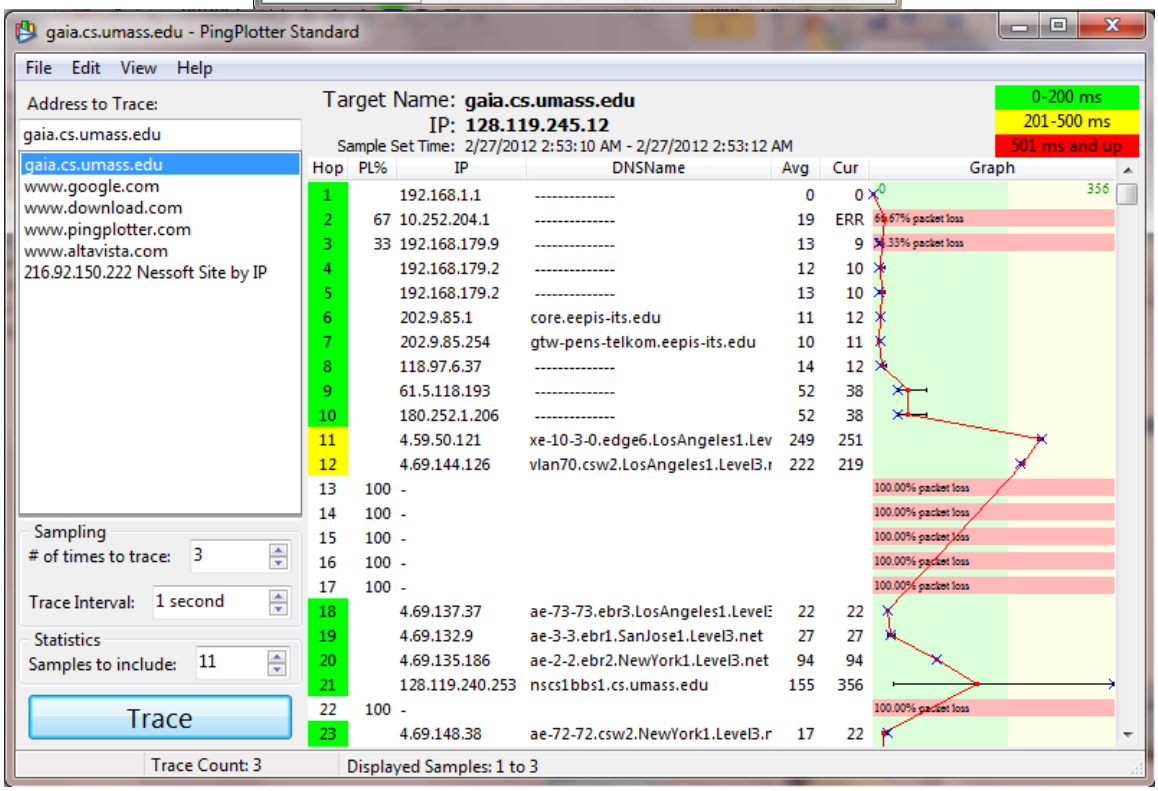
B. Pengamatan Traceroute IP

1. Download program pingplotter, dan gunakan dengan MS. Windows.
2. Setting sebagai berikut :

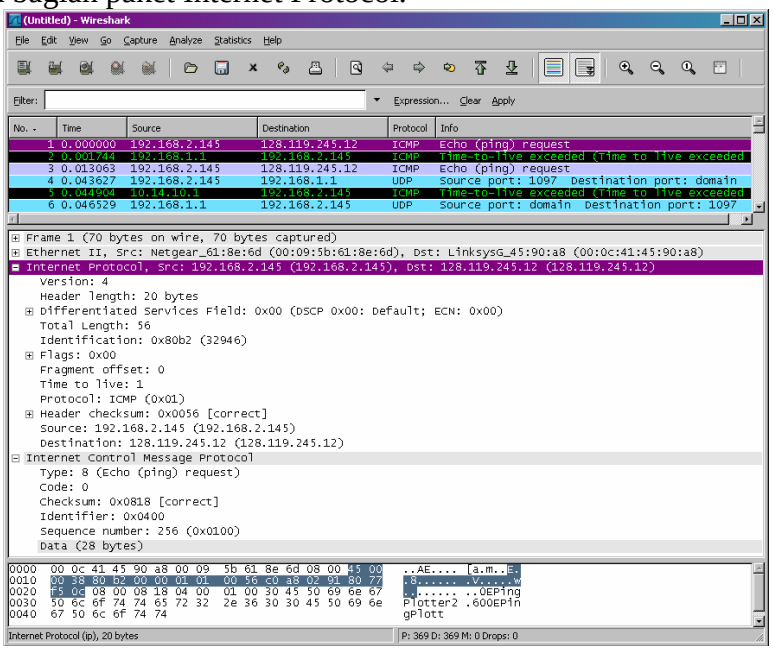
   Address to trace : gaia.cs.umass.edu
   # of time to trace : 3 (3 kali pengiriman paket)
   Trace Interval : 1 second

   Atur packet size (in bytes) : 56, dari Edit | Options | Packet





3. Aktifkan wireshark untuk mulai mengcapture paket, dan tekan tombol Trace pada pingplotter.
4. Matikan wireshark jika sudah selesai, lakukan filter paket ICMP agar hanya paket ICMP yang ditampilkan.
5. Pilih ICMP Echo Request message yang pertama yang dikirim oleh komputer anda, dan expand bagian paket Internet Protocol.



6. Dari informasi diatas, jawablah pertanyaan berikut :
   a. Berapa IP address komputer anda ?
   b. Di dalam IP packet header, berapa value pada upper layer protocol field ?
   c. Berapa banyak byte dalam IP header dan payload dari IP datagram ?
   d. Apakah IP datagram di fragmen ? jelaskan.

7. Lakukan pengamatan dari paket ICMP yang pertama dan berikutnya dengan melakukan sorting pada paket ICMP (klik pada bagian source di wireshark), dan amatilah pada bagian paket Internet Protocol. Jawablah pertanyaan berikut:

a. Field mana dari IP datagram yang selalu berubah dari paket yang dikirim dari komputer anda ?

b. Field mana yang selalu konstan ? Field mana yang harus selalu konstan ?

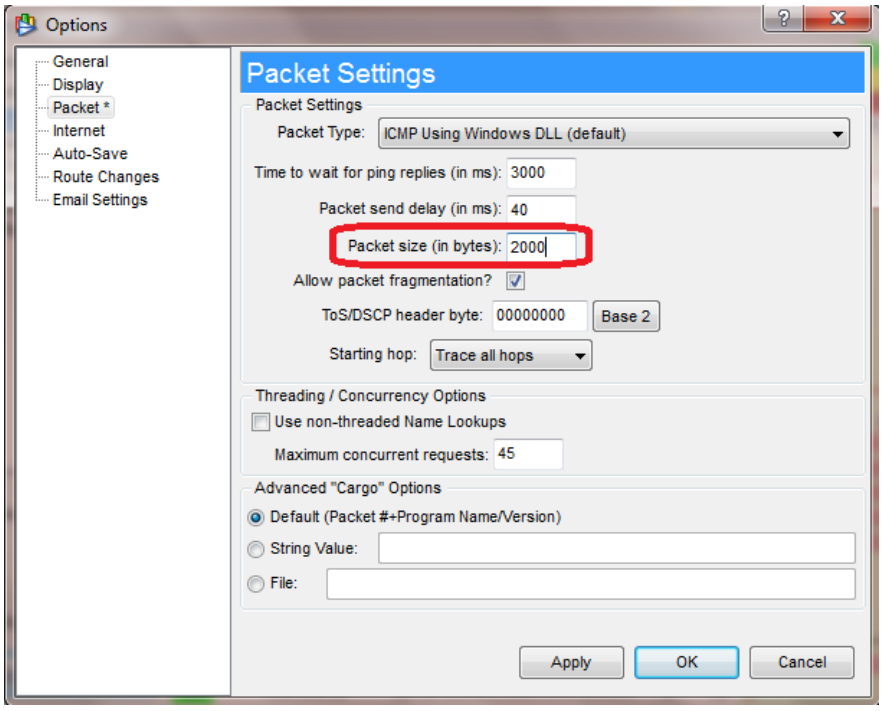
8. Carilah paket ICMP TTL-exceeded replies yang dikirim ke komputer anda oleh router yang pertama, dan jawab pertanyaan berikut :

a. Berapa nilai Identification field dan TTL field ?

b. Apakah nilai tersebut tetap tidak berubah untuk semua ICMP TTL-exceeded replies ? Mengapa ?

C. Pengamatan Fragmentation

1. Ulangi langkah B. 1 – 4, tetapi dengan merubah ukuran paket menjadi 2000.



2. Pada wireshark, amati pada bagian Internet Protocol dan jawab pertanyaan berikut:
   a. Pilih paket pertama yang dikirim ke tujuan, apakah IP datagram mengalami fragmentation ?
   b. Jika iya, informasi apa saja pada IP header yang mengindikasikan datagram telah diframentasi ? Berapa panjang IP datagram ini ?
   c. Lakukan pengamatan pada fragmen kedua dari IP datagram yang terfragmentasi. Informasi apa dalam IP header yang mengindikasikan bahwa ini bukan fragmen datagram yang pertama ? Apakah ada fragmen lainnya ?
   d. Informasi apa yang berubah dari IP header fragmen pertama dan kedua ?

3. Ulangi langkah C. 1 dengan merubah ukuran paket menjadi 3500, dan jawab pertanyaan berikut :
   a. Berapa banyak fragmen yang dihasilkan ?
   b. Field apa yang berubah dalam IP header diantara fragmen-fragmen di atas ?

LAPORAN RESMI

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Bandingkan hasilnya jika dilakukan proses traceroute dari linux dengan merubah-rubah isi paket data.