Analisis hasil Capture, Follow Stream, dan Flow Graph Jaringan menggunakan aplikasi Wireshark dan VisualRoute

Disusun Oleh:

Mohammad Cahyadi

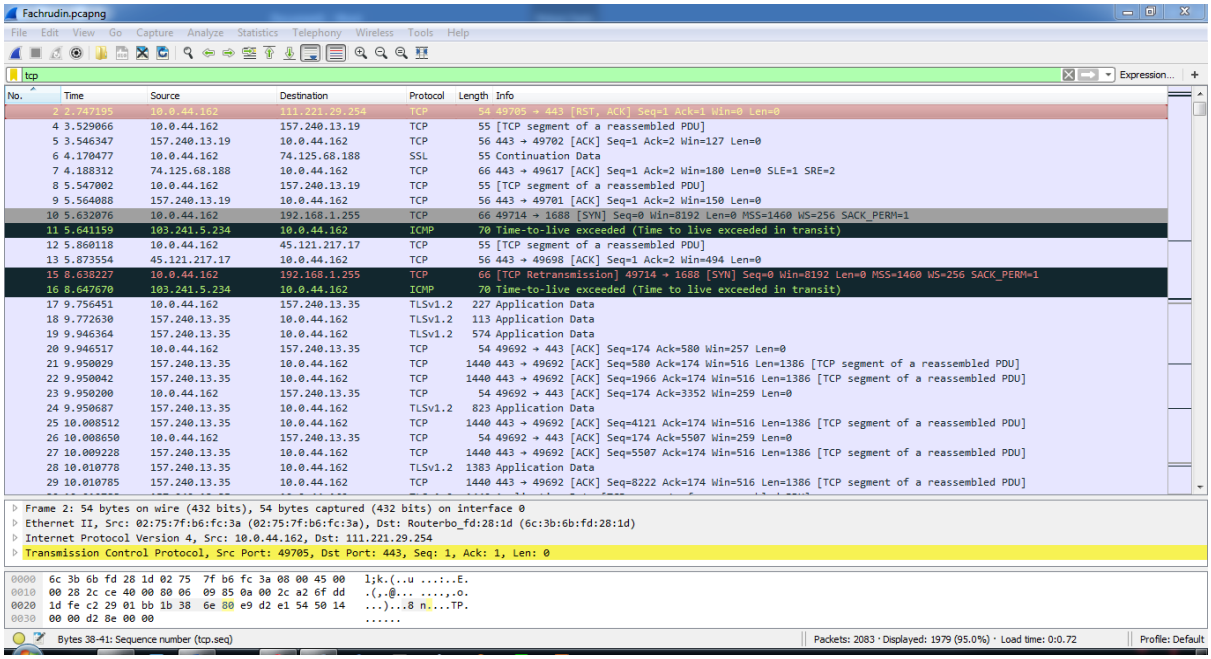
(09011381621065)

Sistem Komputer

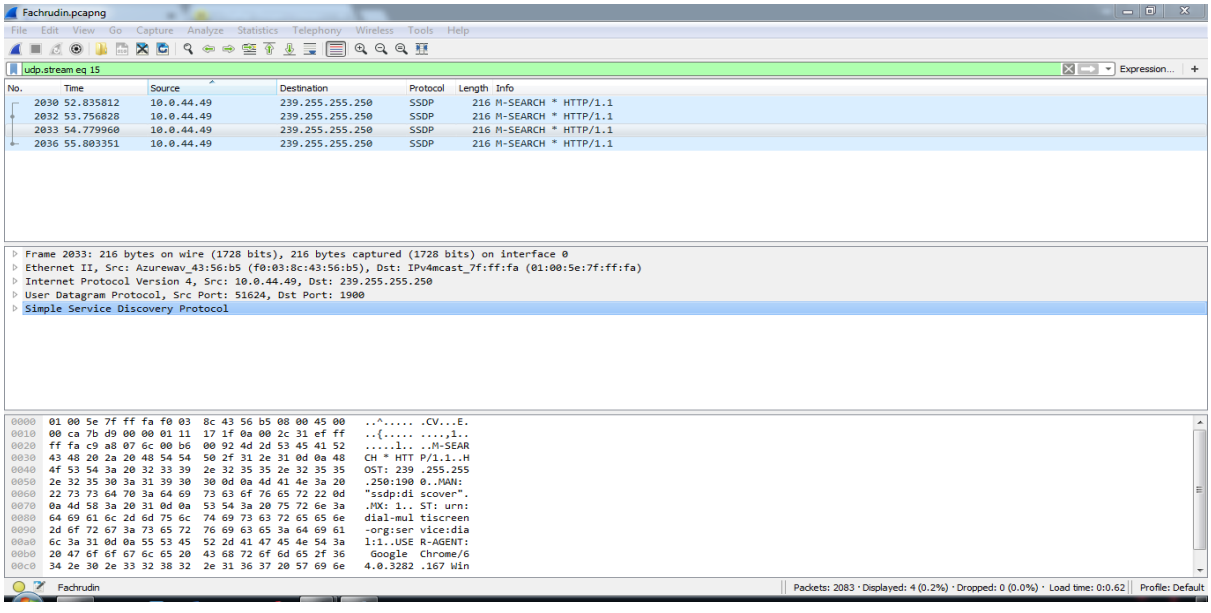
Fakultas Ilmu Komputer

Universitas Sriwijaya

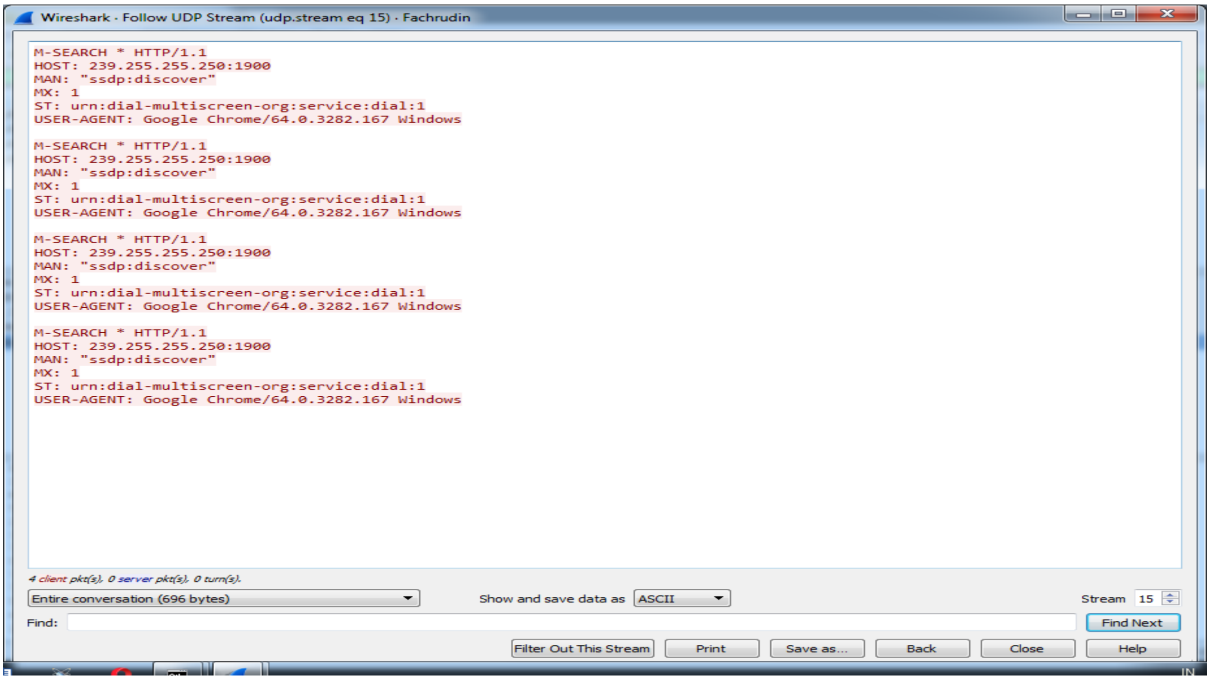
2017/2018



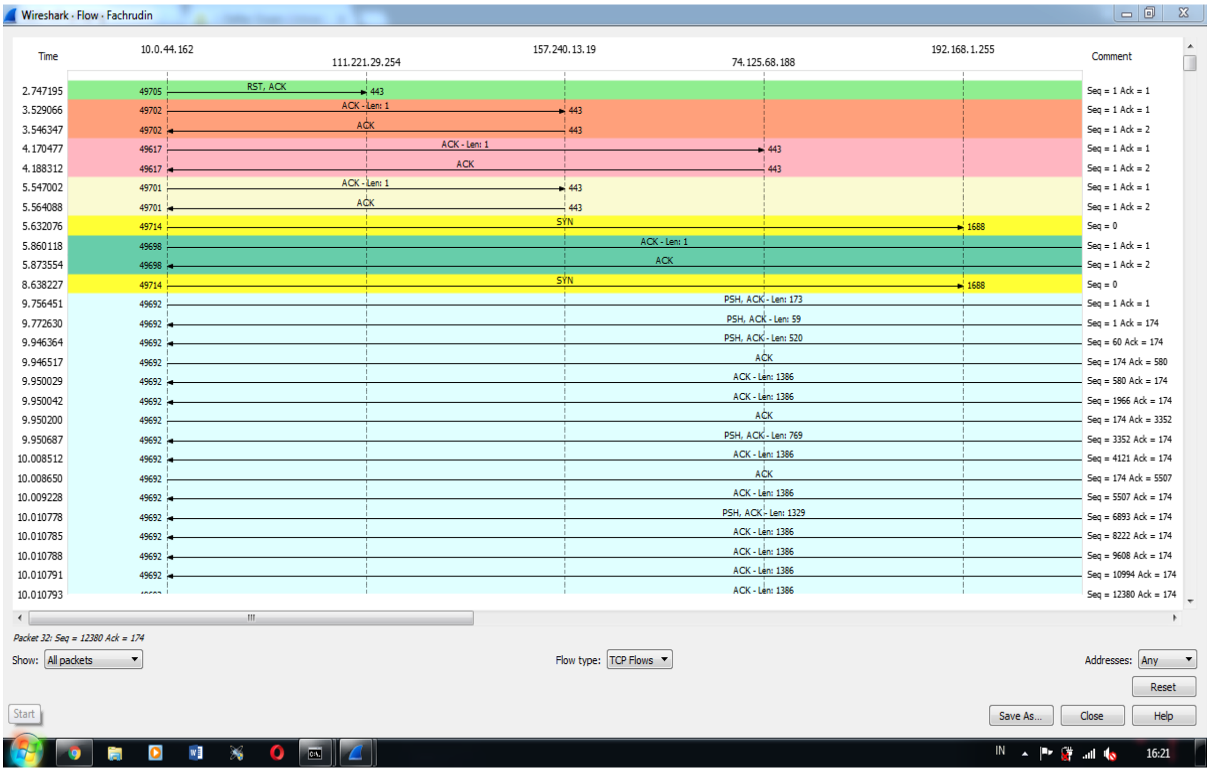
Pada gambar diatas dapat dilihat bahwa banyak sekali ip yang mengakses situs facebook.com dan unsri.ac.id, sebagian kecil ip tersebut hanyalah filter yang menggunakan protocol TCP/IP. Bahkan jika filter dikosongkan, data yang ditampilkan dapat mencapai 3500+ dalam sekali capture dengan rentang waktu 5-10 detik.



Untuk daftar ip diatas adalah filter protocol SSDP/UDP, komputer pada jaringan yang sama dengan komputer pengujian ini hanya dapat di capture pada UDP protocol. Sedangkan pada protocol TCP/IP address komputer tersebut tidak ditemukan.

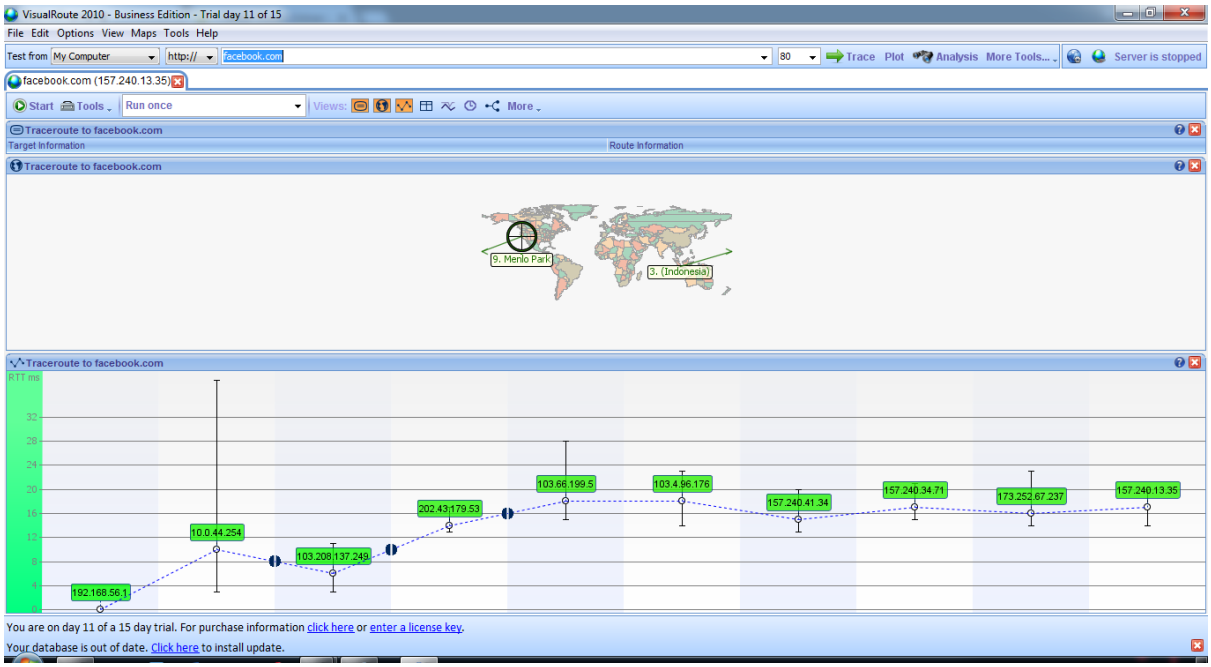


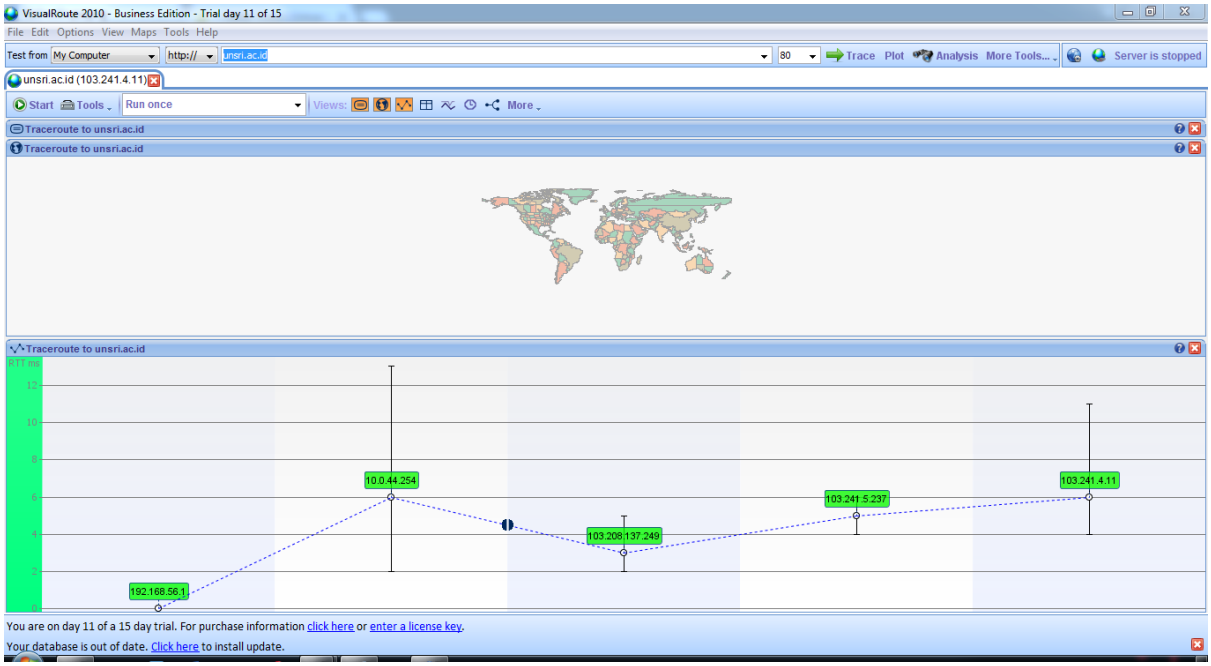
Ketika address komputer yang satu jaringan tersebut di follow stream, maka akan didapat data seperti diatas, tertuang beberapa data yang dapat di analisa. Seperti pada "MAN: ssdp:discover ", dapat kita ketahui bahwa jaringan yang digunakan menggunakan protocol SSDP/UDP yang mana disitu tertulis "discover" sehingga dapat disimpulkan bahwa jaringan tersebut terbuka atau bisa disebut juga jaringan publik. Selain itu, pada user-agent bisa juga diketahui browser yang digunakan komputer tersebut adalah google Chrome.



Lalu lintas berjalannya ekspedisi informasi dapat divisualisasikan menggunakan Flow Graph seperti gambar diatas. Berikut adalah penjelasan terhadap panah pada flow graph:

1. Panah 1 – komputer user mengirim informasi address atau link ke router jaringan.
2. Panah 2 – ketika router menerima informasi, maka ia akan mengalamatkan data tersebut ke isp sumber terdekat (palembang).
3. Panah 3 – isp akan menanggapi permintaan user tersebut, apakah address yang dituju itu tersedia atau tidak.
4. Panah 4 – apabila address tesedia, maka isp akan mengarahkan informasi tersebut ke isp pusat (mis. Jakarta).
5. Panah 5 – isp pusat pun akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.
6. Panah 6 – ketika informasi tersebut tidak valid atau address tersebut tidak ditemukan, maka user diharuskan mengirim ulang informasi yang valid. Dimana data tersebut akan kembali diperiksa oleh isp terdekat.
7. Panah 7 – jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.
8. Panah 8 – apabila isp pusat menanggapi informasi tersebut valid, maka kita akan diarahkan ke server perusahaan yang memberi isp bandwidth. Yang mana disini kita akan di arahkan ke link server cloud berikutnya.
9. Panah 9 – disini situs yang diakses adalah facebook.com dengan mengambil berita international, sehingga address user akan diarahkan terlebih dahulu ke cloud singapura.
10. Panah 10 – seperti pada isp tadi, server singapura pun akan mengirimkan informasi kepada user apakah address yang dituju tersebut valid atau tidak.





Tampak jelas sekali perbedaan data yang dihasilkan oleh aplikasi wireshark dan visualroute ini.

1. Pada aplikasi wireshark setiap lalu lintas perjalanan data dapat dilihat serta dianalis kemana dan apakah data tersebut memberi timbal balik kepada user, tentu saja dapat diambil satu point untuk aplikasi ini yaitu sangat berguna bagi operator server atau server manager yang memiliki kemampuan expert dan para peneliti jaringan untuk mendapatkan data yang sangat mendetail, karena setiap hop terstruktur dengan rapi. Selain itu, aplikasi wireshark dapat memberikan fasilitas filter protocol sehingga dalam menganalis data lebih effective dan akurat.
2. Sedangkan pada aplikasi visualroute akan dibagi menjadi:
    - Kelemahan
        - Kurang mendetailnya aliran data dari awal sesi hingga sampai ke destination atau tidak tersedianya fasilitas flow graph seperti wireshark.
        - Tidak adanya filter protocol.
        - Kurang mumpuni dalam mencapture data pada sebuah ip.
    - Kelebihan
        - Penggunaan yang mudah.
        - Dapat dimengerti oleh pengguna pemula.
        - Visalisasi tempat source dan destination terlihat jelas.
        - Setiap hope ditampilkan semua.