**LAPORAN PRAKTIKUM**

**KEAMANAN KOMPUTER**

**“Analisa File PCAP”**



**Disusun oleh:**

**NAMA : Riskiawati Fransiska**

**NIM : 1400631012**

**PROGRAM STUDI MANAJEMEN INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

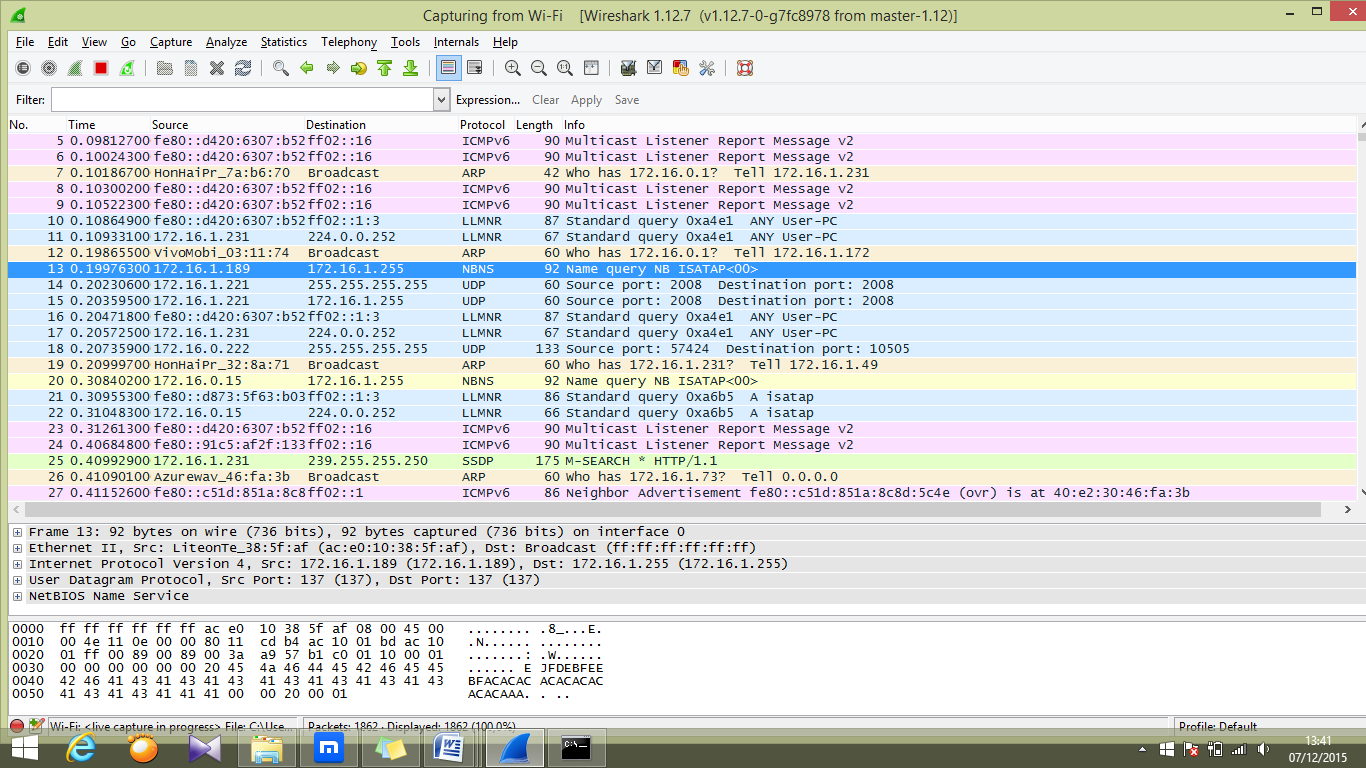
1. Dasar Teori

Wireshark adalah salah satu dari sekian banyak *tool*Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

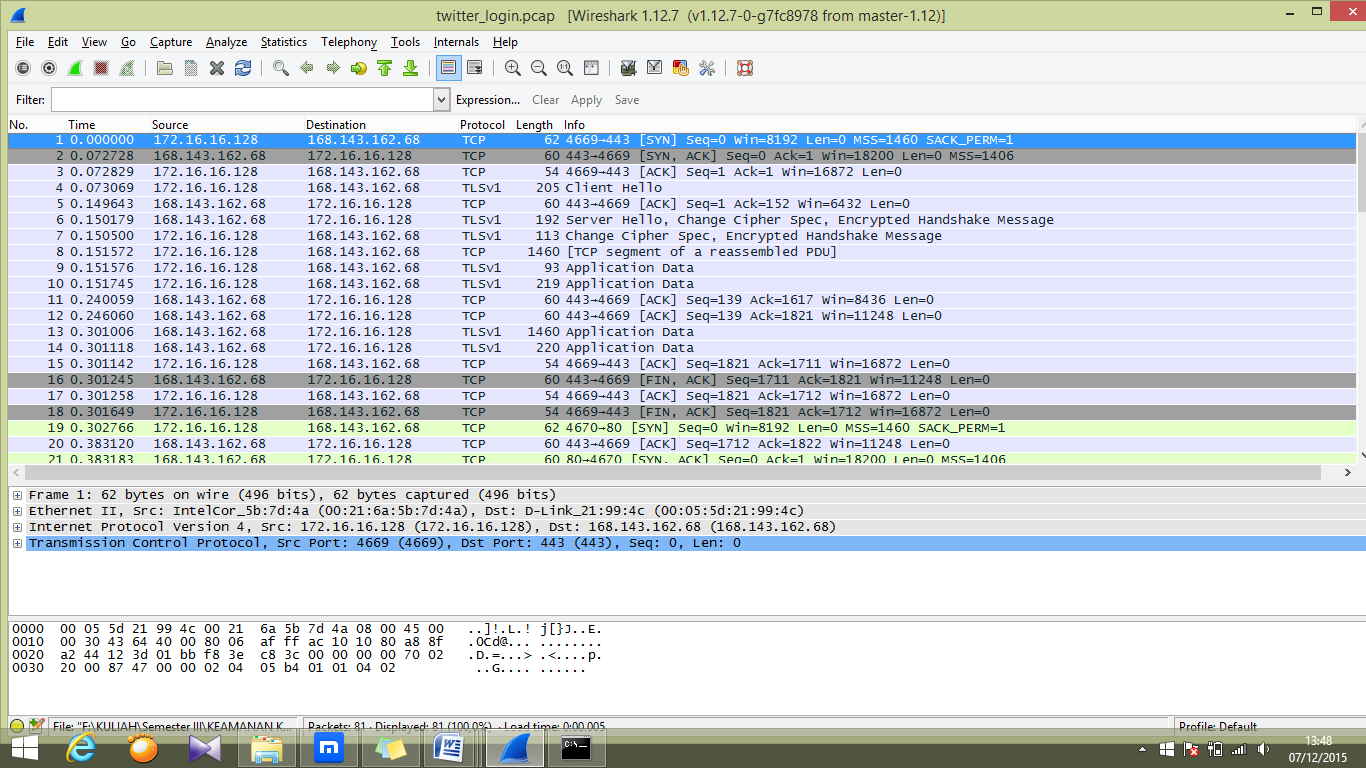
Fungsi dari software Wireshark

Wireshark digunakan untuk troubleshooting jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Wireshark banyak digunakan oleh network admin untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap data/informasi yang melewati suatu jaringan yang kita amati. Dengan kata lain wireshark digunakan untuk mengetahui kejadian yang terjadi pada saat kita melakukan interaksi dengan internet. Dengan wireshark dapat dilihat proses pengiriman data dari komputer ke web yang dituju. 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 spt password email atau account lain) dengan menangkap paket-paket yang lalu lalang di dalam jaringan dan menganalisanya . Wireshark dapat berjalan pada berbagai sistem operasi mirip Unix termasuk Linux, Mac OS X, BSD, dan Solaris, dan Microsoft Windows (Windows XP64 / Vista64 / Windows7 64).

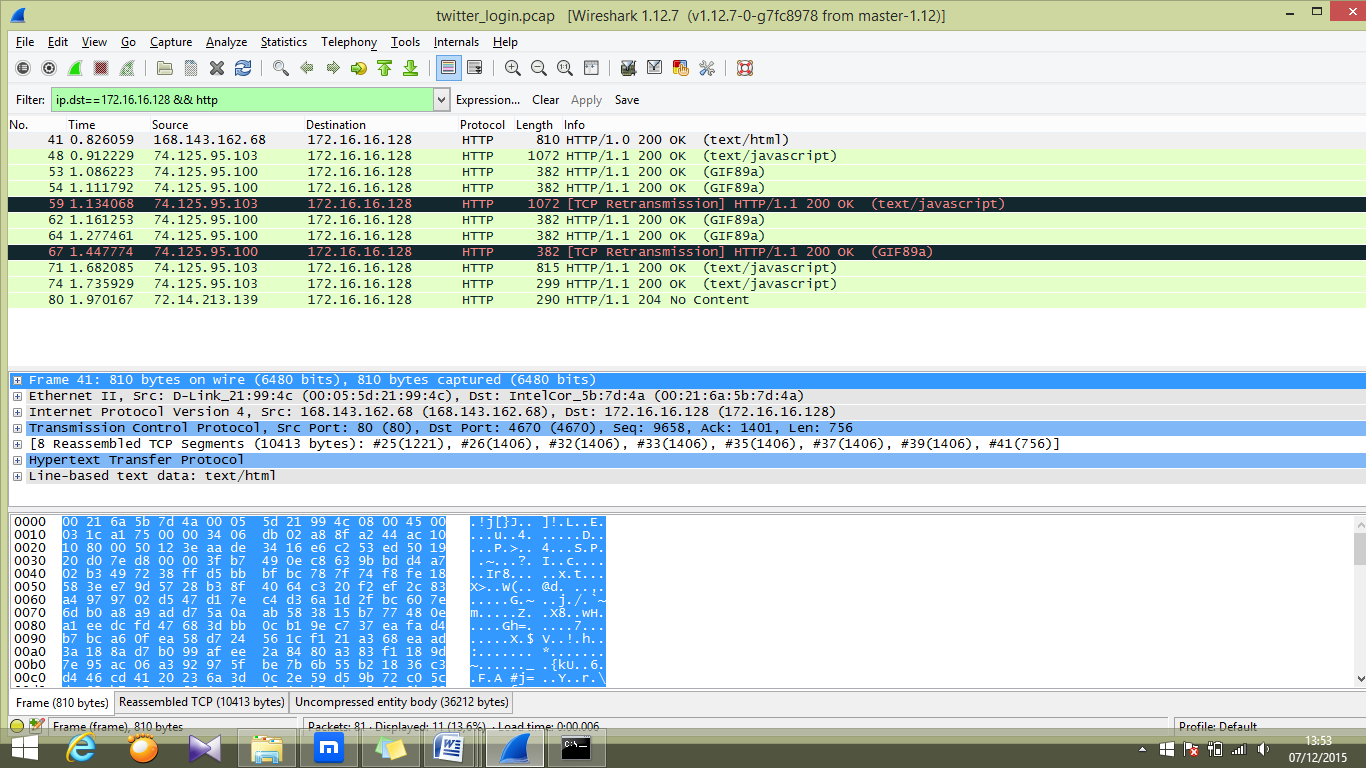
1. Tugas Praktikum
2. Pastikan di komputer sudah terinstal wireshark, langsung centang interface yang sedang aktif kemudian klik start. Maka ip komputer yang sedang aktif akan muncul seperti gambar di bawah, untuk berhenti klik icon yang berwarna merah.



1. Menganalisa file pcap di folder jejaringan-sosial “twitter login”



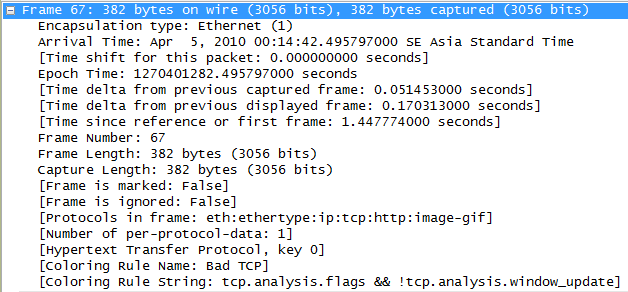
1. Kemudian kita filter, maka akan muncul seperti gambar di bawah ini



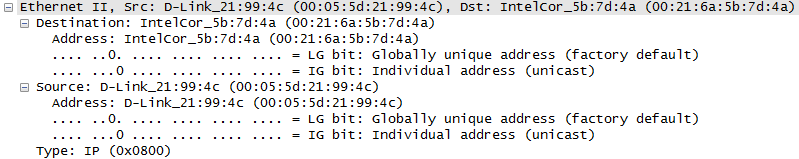
1. Kesimpulan

Dari percobaan di atas terdapat ip twitter yang di ketahui, serta frame yang muncul seperti gambar di bawah

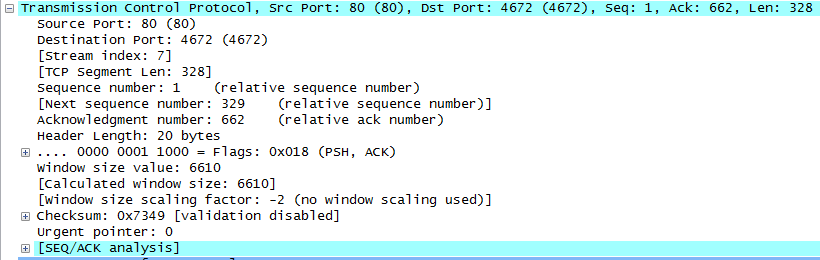
* frame



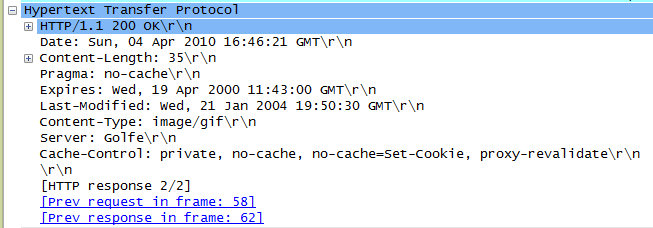
* Ethernet II



* Transmission control protocol



* Hypertext transfer protocol



* Compuserve Giv

