TUGAS JARINGAN KOMPUTER

TUGAS 5

Nama : M.Nizal

Nim : 09011181419025

Nama dosen : Dr. Deris Setiawan, M.T

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

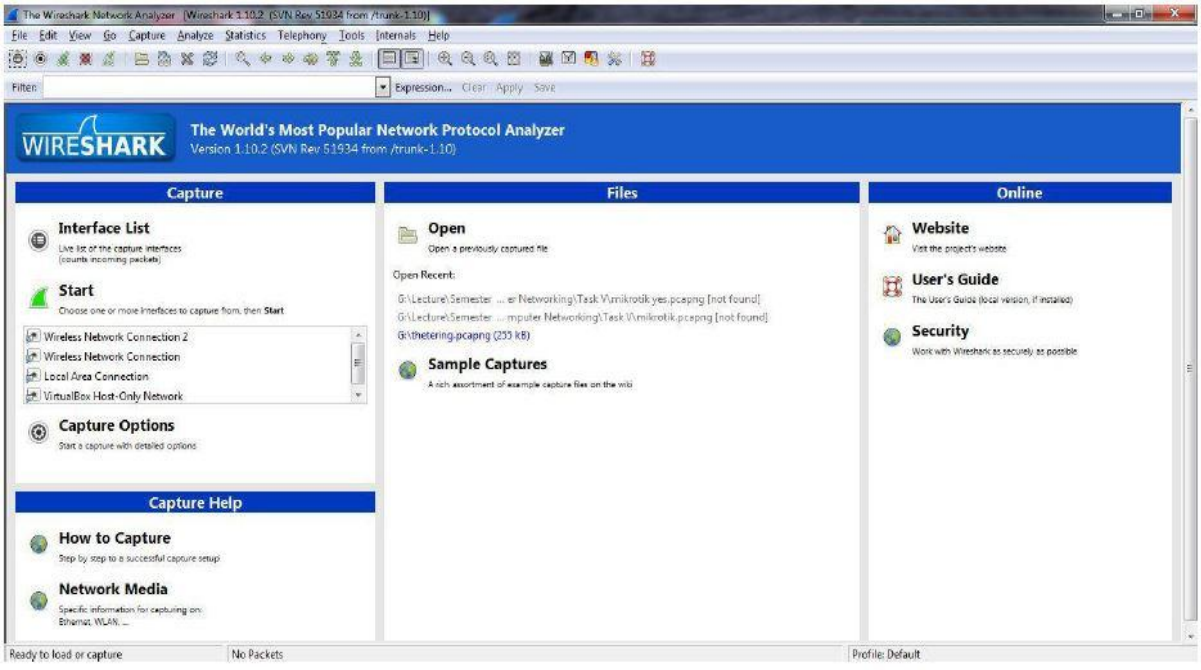
USING WIRESHARK AND COMMAND NESTAT -A

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

Wireshark mampu menangkap paket-paket data atau informasi yang berseliweran 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 spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya.

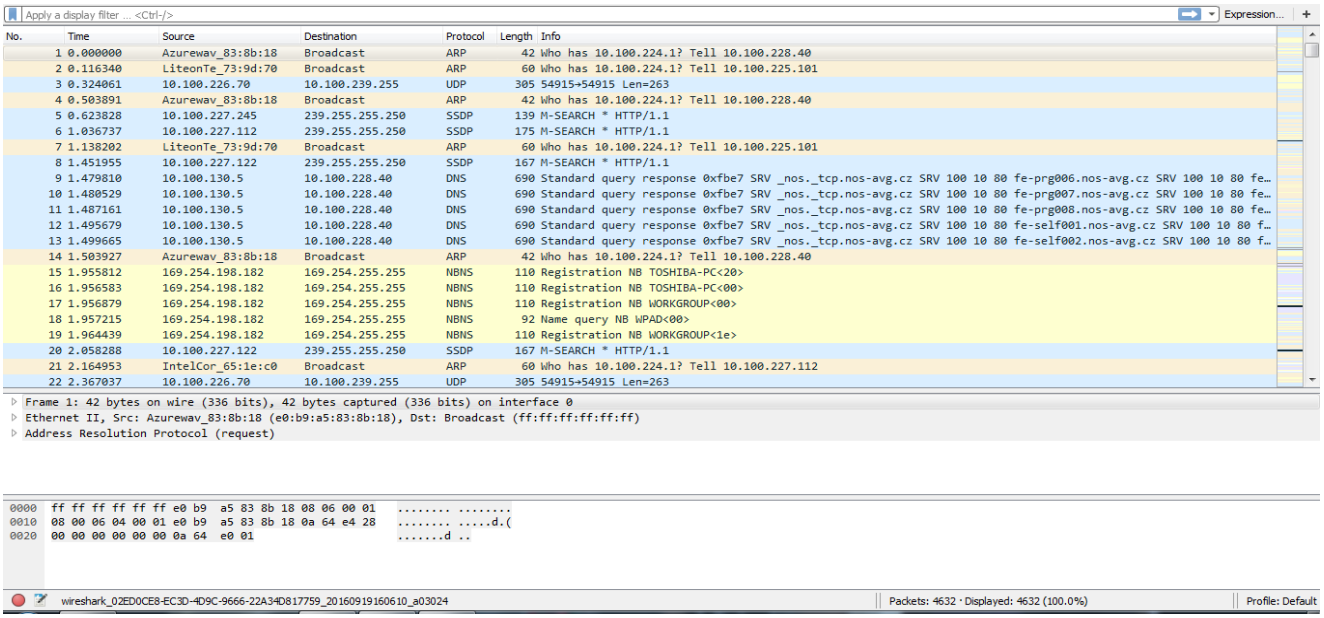
Wireshark dipakai oleh network administrator untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang terlihat dan semua jenis informasi ini dapat dengan mudah dianalisa yaitu dengan memakai sniffing , dengan sniffing diperoleh informasi penting seperti password email account lain.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 dan SLIP), 802.11 wireless LAN, dan koneksi ATM. Program ini juga sering digunakan oleh chatters untuk mengetahui ip korban maupun para chatter lainnya lewat typingan room.Tool wireshark dapat menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer.Selama kita bisa mendapatkan paket langsung dari jaringan, dengan tools seperti wireshark, maka kita juga bisa memanfaatkan wireshark untuk ‘menyadap’ pembicaraan Voice over IP.



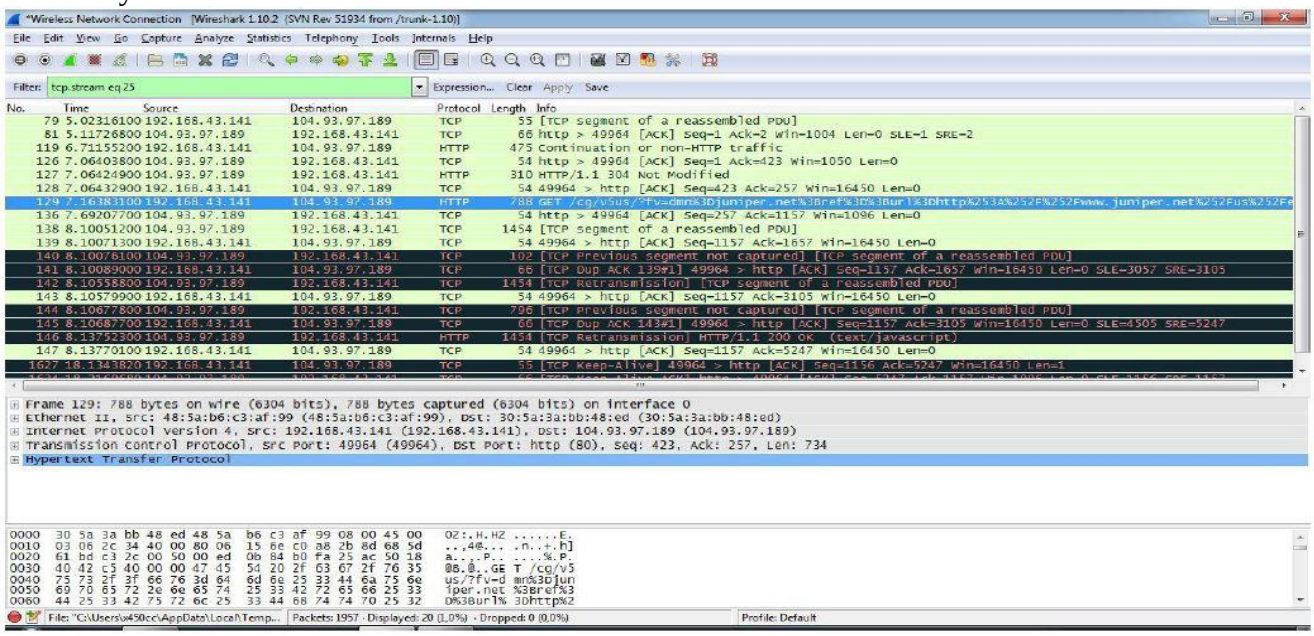
Tampilan Awal pada program WIRESHARK

Selanjutnya adalah meng-capture lalu lintas data menggunakan wireshark dan command “netstat –a” pada command prompt, kemudian kita dapat langsung mengunjungi website yang dituju yang secara otomatis akan di capture oleh wireshare maupun command “netstat –a”.

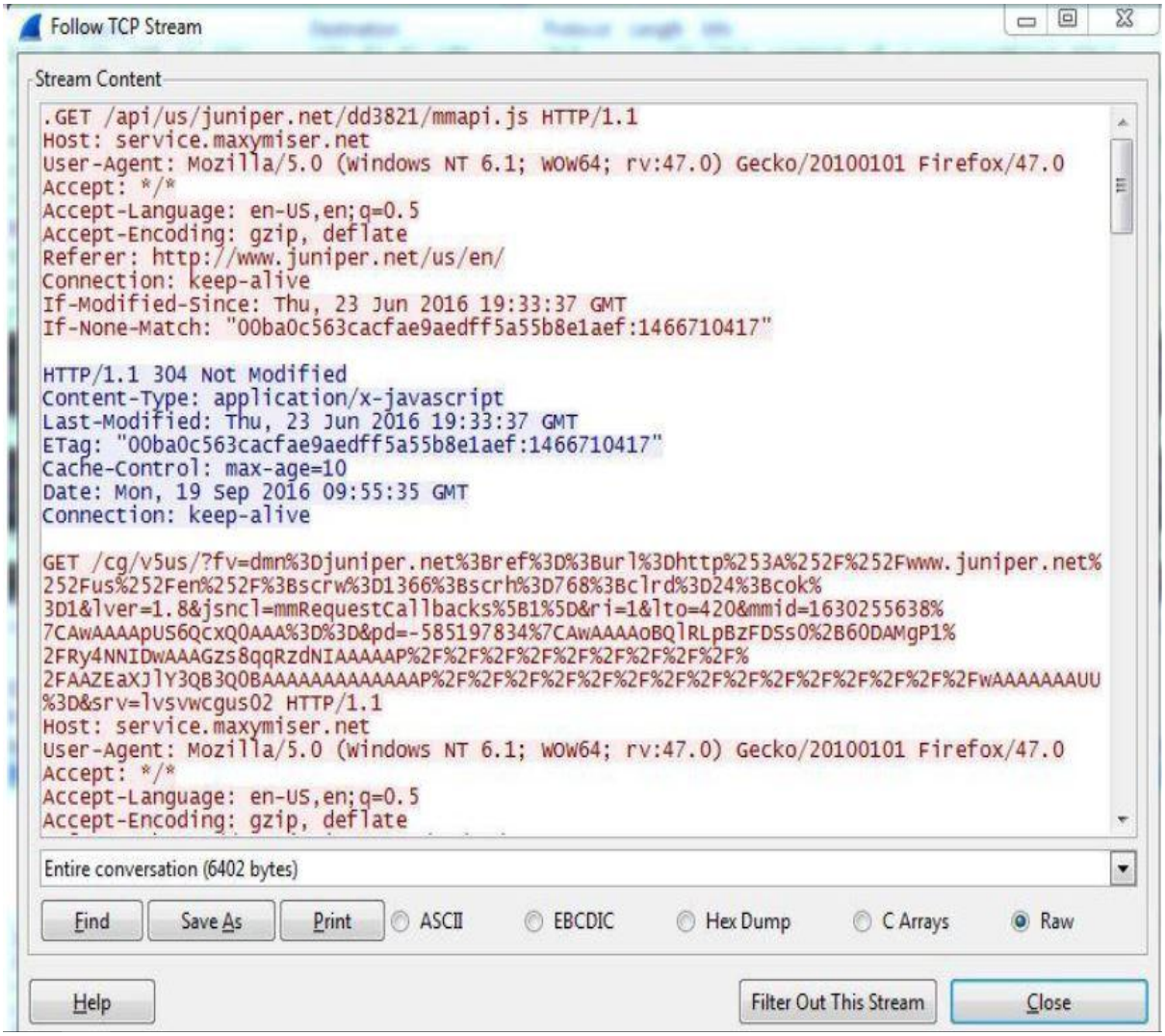


Mengcapture dengan wireshark hingga proses loading website

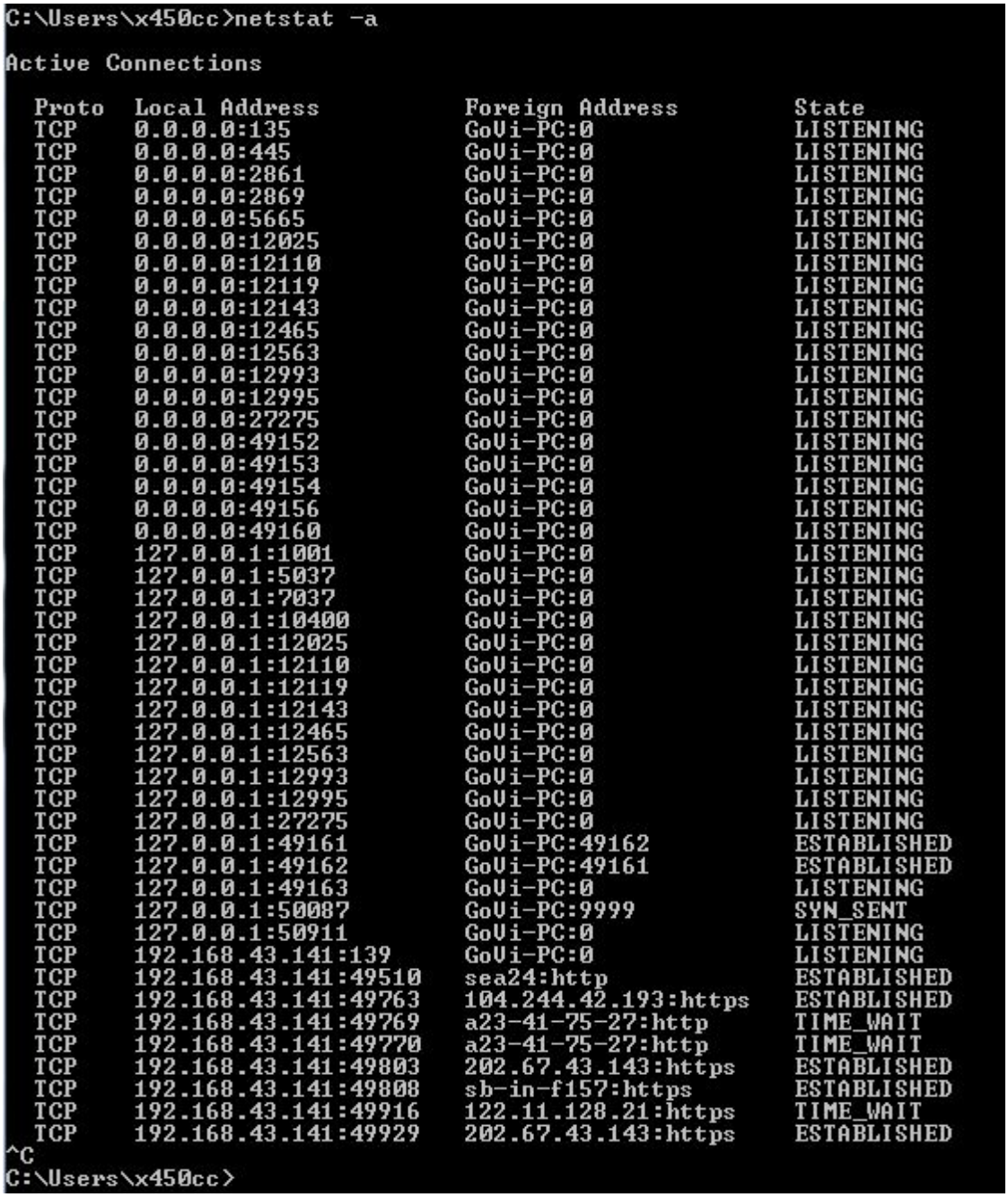
Cara mem-filter protokol yang ter-capture. Protokol yang kita gunakan adalah protokol HTTP (Hypertext Transfer Protocol) yaitu sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia. Setelah selesai difilter, disana kita dapat melihat seluruh paket data yang menggunakan protokol HTTP dan disinilah kegunaan dari IP *source* dan IP *destination* yang telah kita cari tahu sebelumnya



HASIL FILTER HTTP



Respon server terhadap Method GET tersebut adalah OK dan pada bagian bawahnya berisi element website tersebut dengan bahasa html, Namun tidak ditemukan Methode POST maupun RESPONS. Pada method POST sendiri, Permintaan POST digunakan untuk mengirim data ke server, misalnya, informasi pelanggan, file upload, dll menggunakan bentuk HTML



Menggunakan command *netstat –a* pada command prompt dan muncul tampilan seperti diatas. Port yang digunakan pada praktikum kali ini menggunakan Port 80 dikarenakan port tersebut digunakan untuk mengakses World Wide Web (WWW). Protokol yang digunakan adalah protokol TCP **Transmission Control Protocol (TCP)** adalah suatu protokol yang berada di lapisan transport (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (*connection-oriented*) dan dapat diandalkan (*reliable*). Sedangkan untuk *state* merupakan keadaan dari proses lalu lintas data tersebut misalkan listening dapat diartikan menunggu respon user, time wait merupakan proses menunggu respon dari destination.