**LAPORAN PRAKTIKUM**

**KEAMANAN KOMPUTER**



**Disusun oleh:**   
 M Trio Prastyo Billy W

(1400631022)

**PROGRAM STUDI MANAJEMEN INFORMATIKA FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

**Modul Praktikum Keamanan Komputer**

Pada pertemuan pertama, saya ingin menjelaskan fungsi dari software / perangkat lunak Wireshark. Wireshark merupakan perangkat lunak yang spesifik untuk melakukan

analisa paket data pada jaringan secara real time dan menampilkan hasil analisa paket

data tersebut dalam format yang dipahami oleh pengguna. Wireshark dapat melakukan

paket filtering, paket color coding, dan fitur-fitur lain yang dapat mengizinkan untuk

melihat detail network traffic dan inspeksi paket data secara individu.

Untuk mengunduh software wireshark, Anda dapat mengunjungi alamat website official

wireshark di http://www.wireshark.org/download.html. Wireshark dapat digunakan pada

sistem operasi Windows, Mac OS X, dan Linux.

Ada banyak hal yang dilakukan menggunakan wireshark. Berikut ini merupakan contoh

kasus yang mungkin dibutuhkan tools wireshark :

1. Melakukan troubleshoot permasalahan jaringan

2. Melakukan pengujian masalah keamanan

3. Melakukan debugging implementasi protokol

4. Belajar protokol jaringan

Wireshark ini dapat kita sebut sebagai tools yang powerfull, karena dengan

menggunakan tools ini, kita bisa saja dapat menggunakannya untuk mencuri informasi

yang sensitif pada jaringan, seperti password, cookie, dan lain sebagainya.

Wireshark mempunyai fitur yang lengkap, diantaranya adalah :

1. Multiplatform - Dapat digunakan untuk beberapa platform sistem operasi (Unix,

**Dasar-dasar Penggunaan Wireshark**

**Tools**

**Kapan Menggunakan Wireshark**

**Fitur**

Modul Praktikum Keamanan Komputer

Bab 1 Dasar-Dasar Penggunaan Wireshark 3

Mac, Windows, dan Linux)

2. Dapat melakukan capture paket data jaringan secara real time

3. Dapat menampilkan informasi protokol jaringan dari paket data secara lengkap

4. Paket data dapat disimpan menjadi file dan nantinya dapat dibuka kembali untuk

analisis lebih lanjut

5. Filtering paket data jaringan

6. Pencarian paket data dengan kriteria spesifik

7. Pewarnaan tampilan paket data untuk mempermudah analisa paket data

8. Menampilkan data statistik

Untuk melakukan capture paket data yang keluar ataupun masuk pada jaringan,

wireshark memerlukan perangkat fisik NIC (Network Interface Card).

Wireshark dapat melakukan analisis terhadap beberapa protokol paket data jaringan.

Sampai wireshark versi 1.12.6, sudah mendukung 1482 protokol, seperti terlihat pada

gambar dibawah ini:

Gambar 1.1 - Protokol yang disupport Wireshark

Pada gambar diatas sudah mendukung 1482 protokol, tentunya jumlah protokol yang

**Protokol**

Modul Praktikum Keamanan Komputer

Bab 1 Dasar-Dasar Penggunaan Wireshark 4

didukung wireshark akan bertambah lagi pada tiap versinya.

Wireshark dapat menganalisis paket data secara real time. Artinya, aplikasi wireshark

akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah

ditentukan dan selanjutnya akan menampilkan hasil paket datanya. Contoh aplikasi

wireshark yang sedang melakukan pengawasan dapat dilihat pada gambar 2, berikut ini:

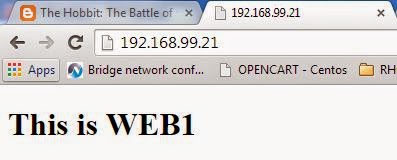
Gambar 1.2 - Tampilan Data Wireshark Real Time

Jika komputer kita terhubung dengan jaringan kecepatan tinggi dan pada komputer

sedang dijalankan banyak aplikasi berbasis jaringan, aplikasi wireshark akan

menampilkan banyak sekali paket data

Terlihat diatas masih belum ada paket yang masuk, Lalu coba akses web server dari browser kamu.

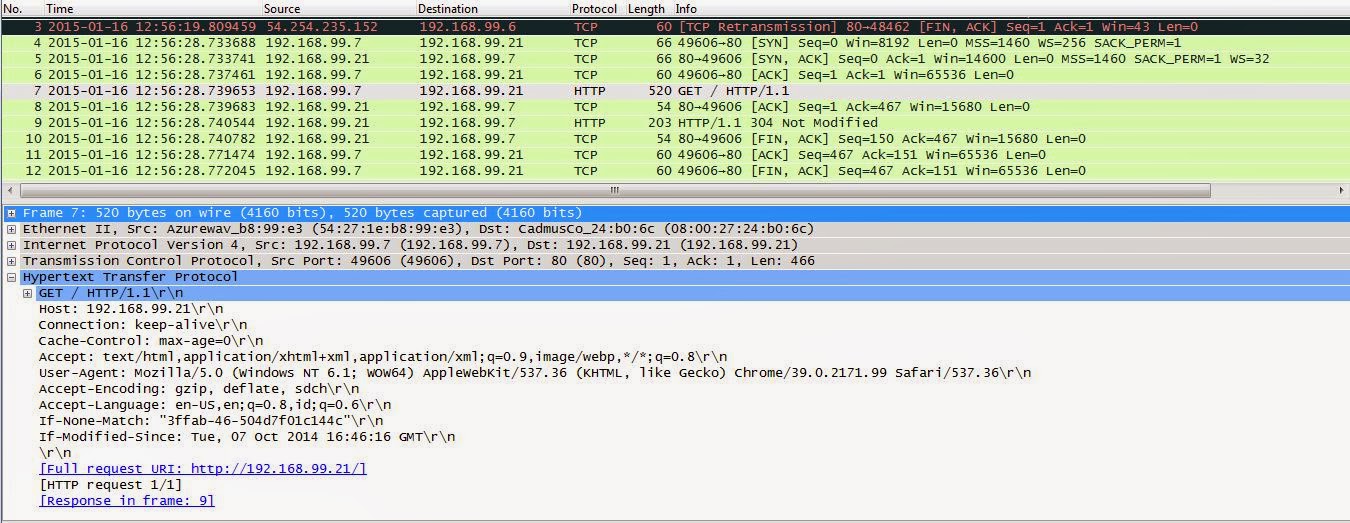
[](http://3.bp.blogspot.com/-yiiCPxBk49Q/VLipv6XfJLI/AAAAAAAAASk/rKYRkfRRgIE/s1600/Capture.JPG)

Dari gambar diatas, saya ambil paket tersebut ke laptop saya lalu saya buka paket tsb dengan menggunakan wireshark.

[](http://3.bp.blogspot.com/-nYYrCxCZr1s/VLisTWxi23I/AAAAAAAAATA/nDoYWspsfII/s1600/Capture.JPG)

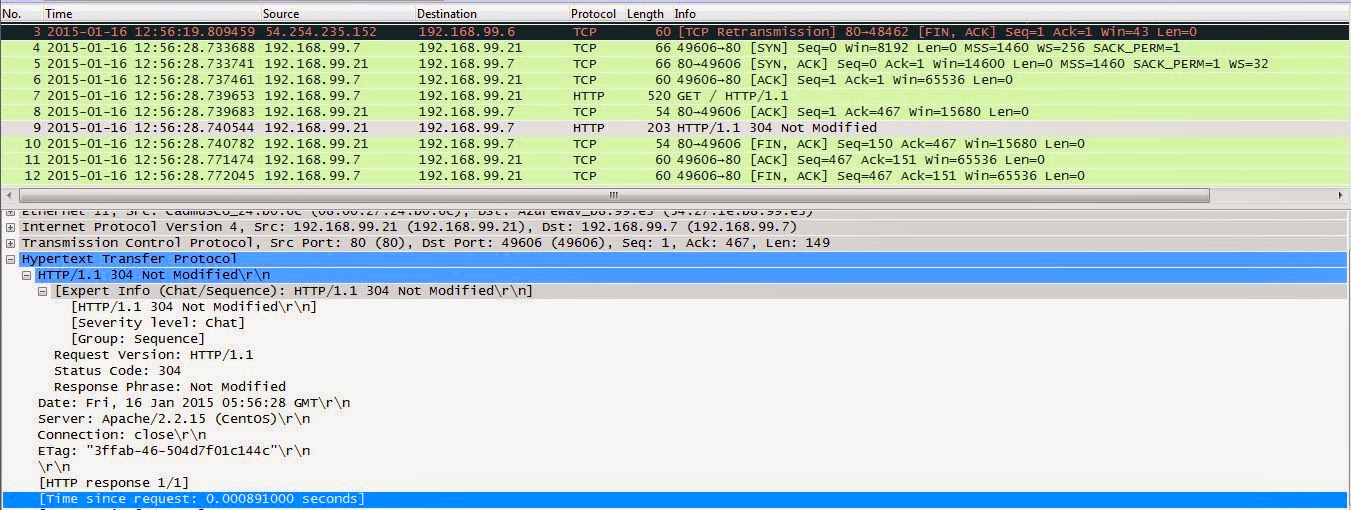
**Notes :**

**Pastikan kamu sudah menginstall wireshark di komputer kamu.**

[](http://1.bp.blogspot.com/-ET2WaqoS094/VLiufKItCdI/AAAAAAAAATM/TS48J5aK490/s1600/1.JPG)

Terlihat diatas request HTTP ada di Frame ke 7 dan Response ada di Frame 9, kalo dilihat lebih detail lagi bahkan kita dapat melihat user agent yang mengakses menggunakan browser apa, jam berapa, dsb.

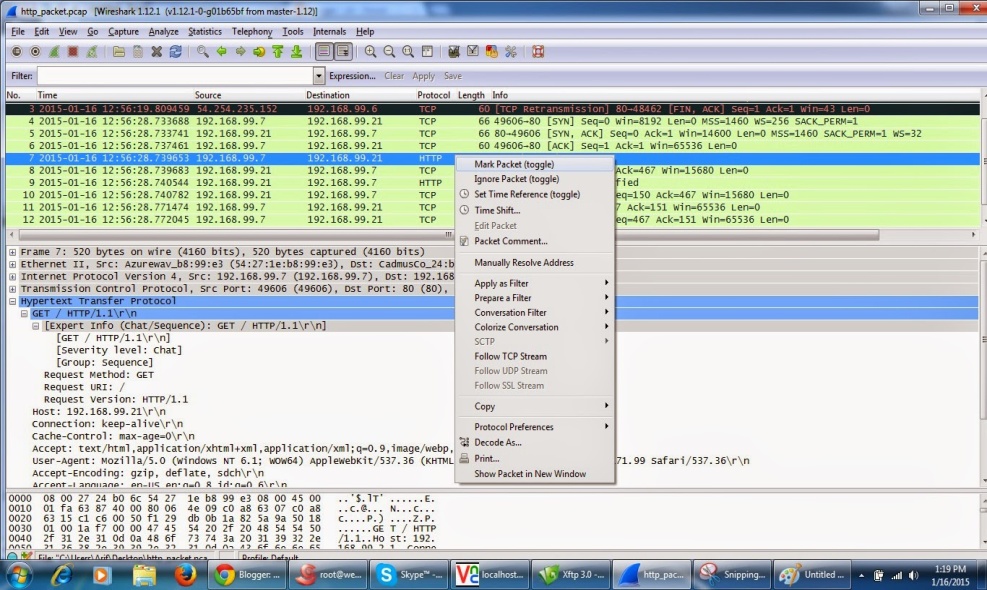
Sekarang kita buka frame no 9, terlihat dari frame tsb response time nya.

[](http://2.bp.blogspot.com/-Ib1ZZV4ZiOc/VLiufwTLmGI/AAAAAAAAATQ/ySRXHqIy6e0/s1600/2.JPG)

Sekarang kita coba mark paket HTTP nya saja sehingga hanya frame yang protokol HTTP saja yang kita lihat, teknik ini sangat berguna buat analisis data dan biasanya dikasi ke customer sebagai bukti otentik dan tshoot.

Caranya seperti dibawah ini.

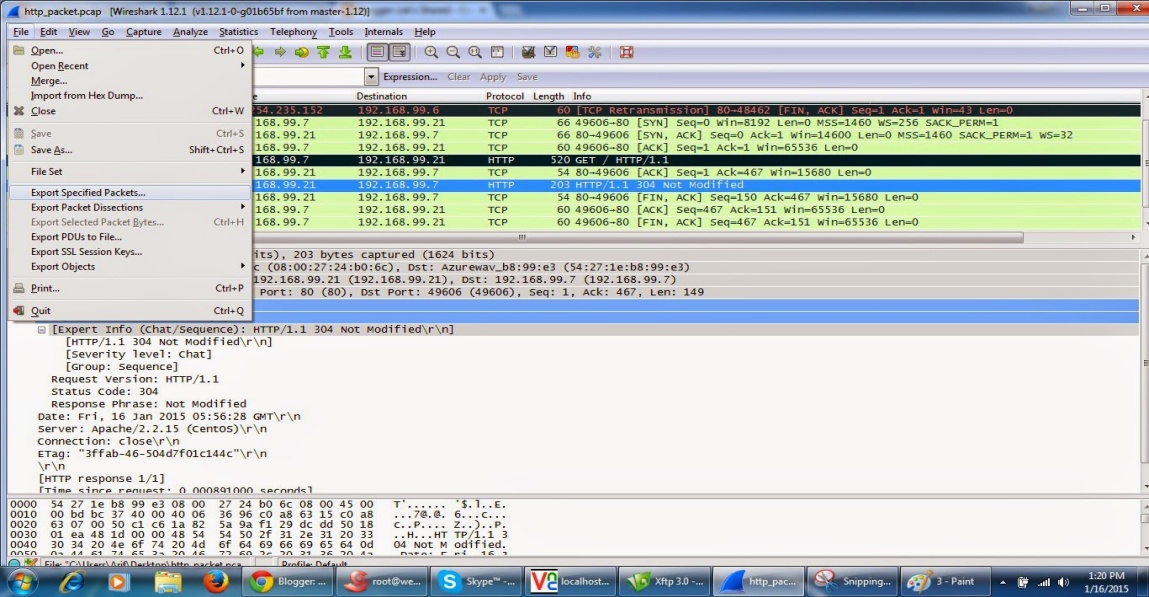
- Mark Packet HTTP dari file dump yang kita buka.

[](http://1.bp.blogspot.com/-hrXpoSrfaNY/VLiugf5UNfI/AAAAAAAAATU/mvzocW4BKLY/s1600/3.jpg)

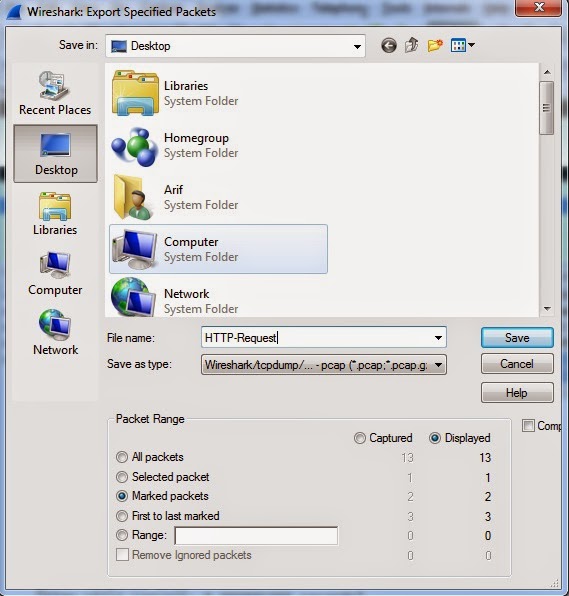
Klik kanan tekan ***mark packet (toggle)***

Dari gambar diatas saya coba mark frame no 7, lakukan hal yang sama ke frame no.9

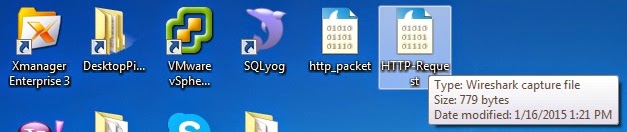
- Apabila sudah maka frame/packet yang di mark akan bewarna hitam, klik file di tab wireshark lalu pilih ***export specified packets***

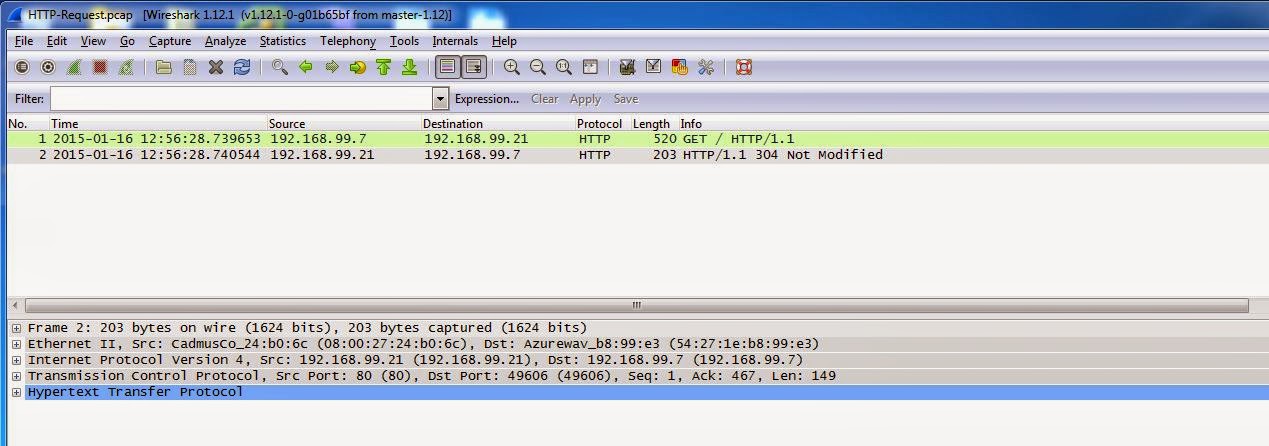
[](http://1.bp.blogspot.com/-P-QKo30ZrY0/VLiuhXcm4SI/AAAAAAAAATg/fqDeR2D1dkk/s1600/4.jpg)

Lalu di tab yang baru ini ketik nama file yang baru, jangan lupa pilih di ***radio button packet range*** yang ***marked packets***

[](http://1.bp.blogspot.com/-mk3n_jTHKxo/VLiuhuNjVuI/AAAAAAAAATk/U3MxajgyB8o/s1600/5.jpg)

Setelah itu akan muncul file baru namanya HTTP-Request yang isinya hanya packet yang tadi kita mark saja, kamu bisa buka lalu bisa dikasi deh ke orang yang memang minta dump file tsb sebagai bukti kalo misalnya aplikasi kita gak salah atau untuk keperluan lainnya.

[](http://3.bp.blogspot.com/-hBIUyKoVsHg/VLiuhouY6wI/AAAAAAAAATo/CmfRLMJGwBY/s1600/6.jpg)

[](http://1.bp.blogspot.com/-12mRirFB7sg/VLiuiwVJDpI/AAAAAAAAATs/yPef-Aw6cYg/s1600/7.JPG)

Kesimpilan: Dapat disimpulkan bahwa kita bisa menganalisa suatu file.pcap yaitu packet picture dengan menggunakan wireshark, dengan wireshark kita lebih bisa mengerti dan mengetahui code – code yang tidak kita ketahui