**LAPORAN VI (ENAM)**

**KEAMANAN KOMPUTER**

****

**Disusun Oleh:**

**Nama : M Rizal Maulididani**

**NIM : 1400631020**

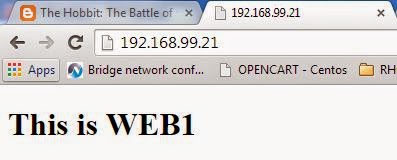
**PROGRAM STUDI MANAJEMEN INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

1. 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)

[root@web1 ~]# tcpdump -nn -l -s 2000 -w http\_packet.pcap -i eth0 'port 80' -v

tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 2000 bytes

13 packets captured

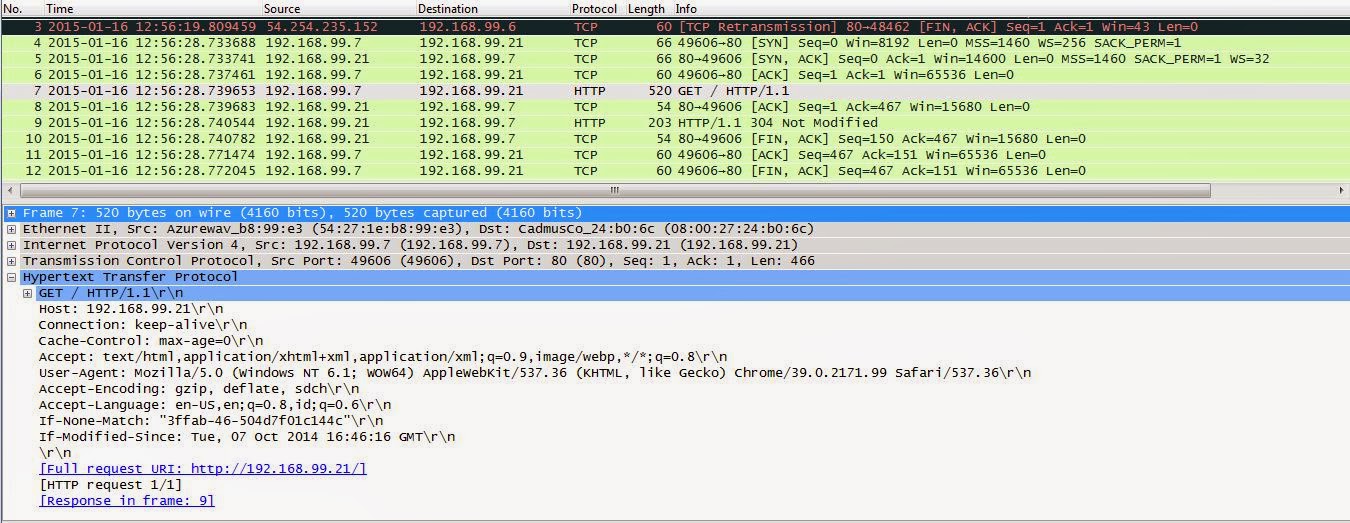
13 packets received by filter

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)

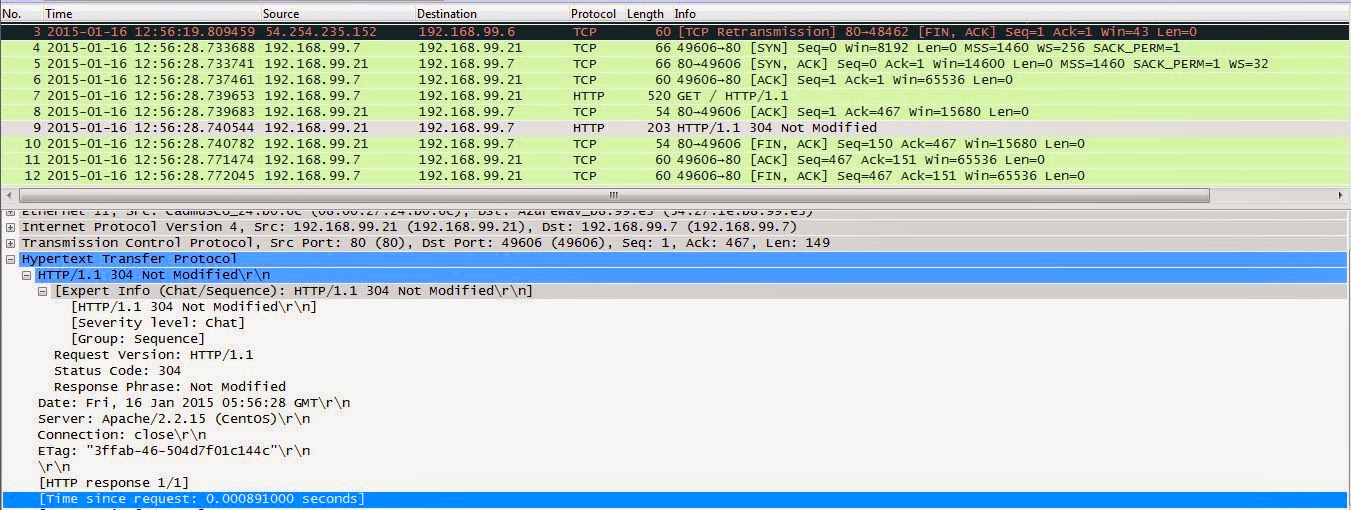
Notes :

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.

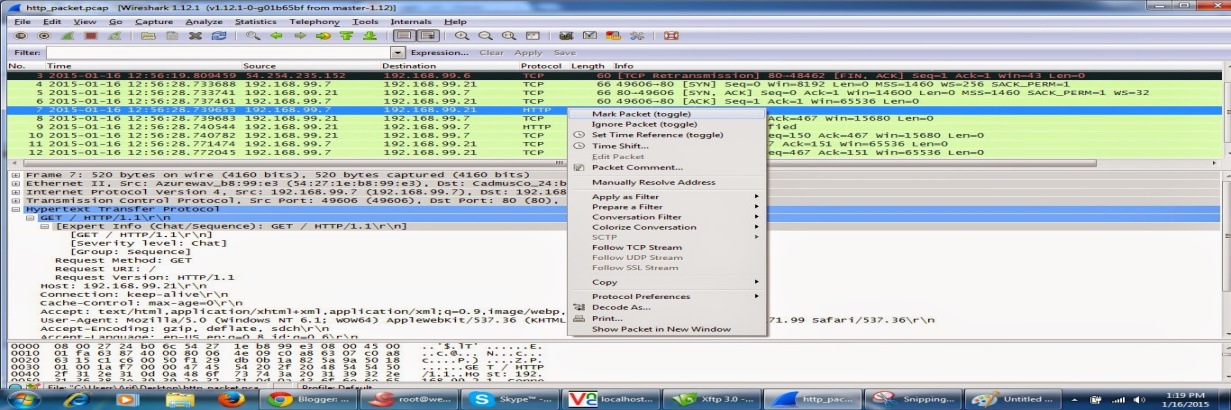
Sekarang kita buka frame no 9, terlihat dari frame tsb response time nya.

[](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.

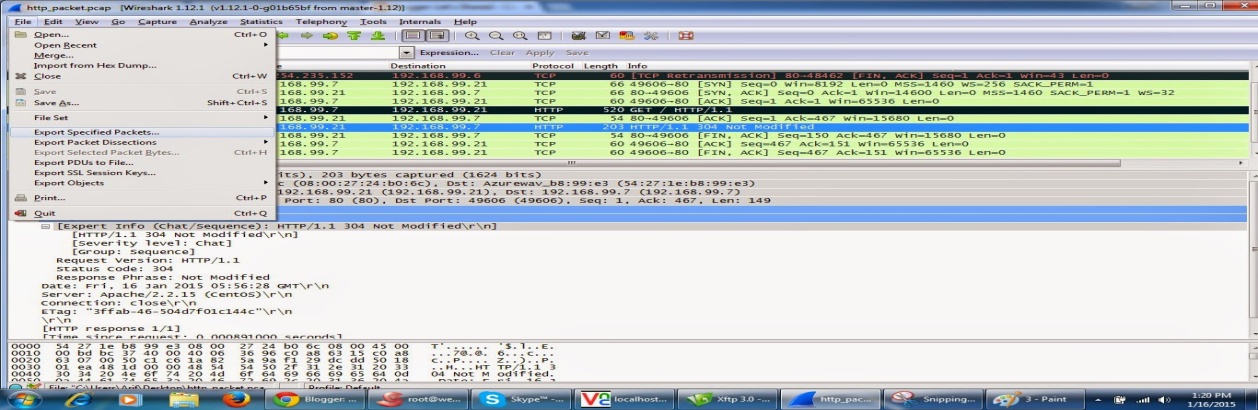
- Mark Packet HTTP dari file dump yang kita buka.

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

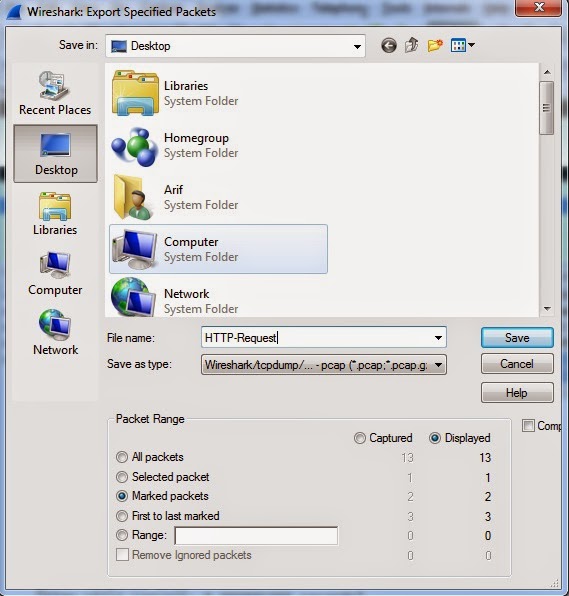
Klik kanan tekan mark packet (toggle)

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

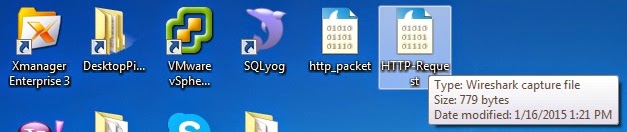
- Apabila sudah maka frame/packet yang di mark akan bewarna hitam, klik file di tab wireshark lalu pilih export specified packets

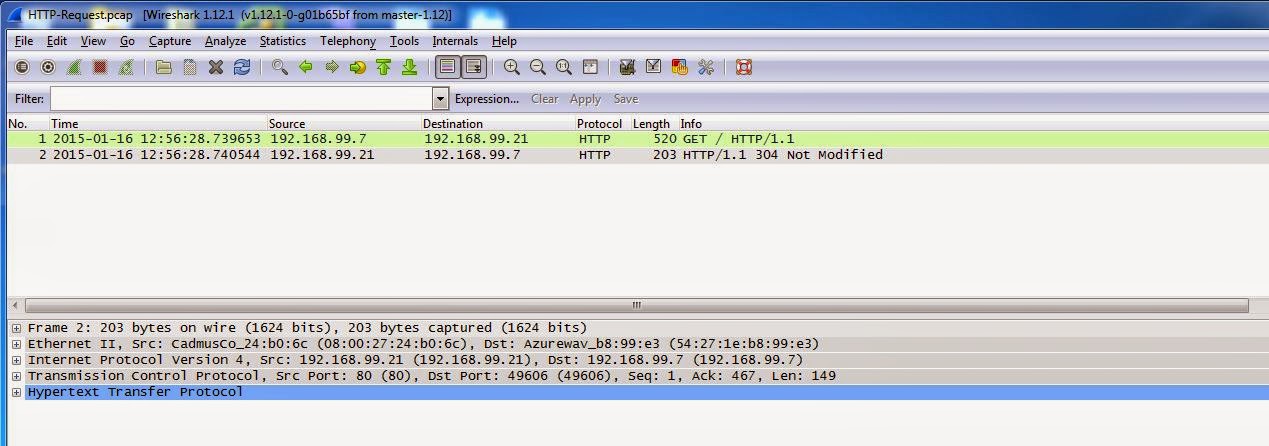
[](http://1.bp.blogspot.com/-P-QKo30ZrY0/VLiuhXcm4SI/AAAAAAAAATg/fqDeR2D1dkk/s1600/4.jpg)

- 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)