

Melihat URL Yang Sedang Di Akses Dengan Wireshark

Kamaldila Puja Yusnika

kamaldilapujayusnika@gmail.com

http://aldiyusnika.wordpress.com

Lisensi Dokumen:

Copyright © 2003-2013 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

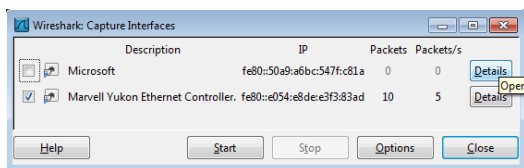
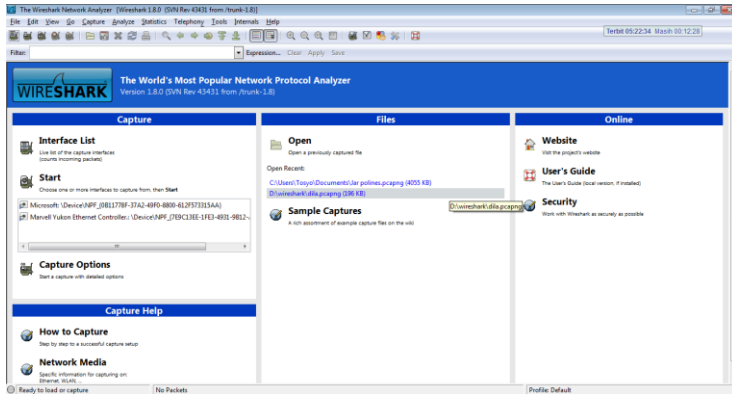
Pendahuluan

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 and SLIP), 802.11 wireless LAN, dan koneksi ATM.

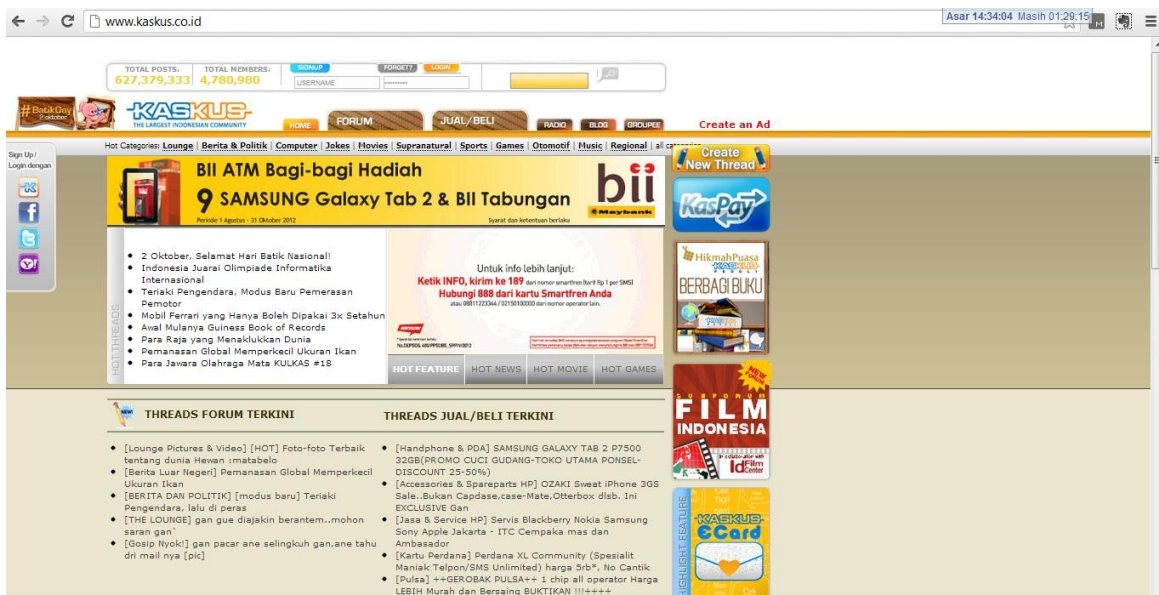
Dalam sebuah jaringan local, terkadang kita ingin melihat situs apa yang sedang di akses oleh klien pada jaringan tersebut, dengan menggunakan wireshark kita bisa melakukan itu

Dalam kasus ini kita misalkan klien sedang mengakses kaskus.co.id

Pertama buka wireshark dan pilih interface dari computer yang terhubung ke jaringan



Lalu pada sisi klien, melakukan akses ke situs yang di tuju



Lalu scan menggunakan wireshark

The screenshot shows the Wireshark interface with a list of network packets. The selected packet (No. 967) is an HTTP GET request for the image `/images/batik_kaskus-LOGO_seasonal.jpg`. The details pane shows the following information:

- Frame 967:** 774 bytes on wire (6192 bits), 774 bytes captured (6192 bits) on interface 0
- Ethernet II:** Src: Hewlett_77:ba:f2 (00:25:b3:77:ba:f2), Dst: Routerbo_e4:86:c5 (00:0c:42:e4:86:c5)
- Internet Protocol Version 4:** Src: 192.168.1.3 (192.168.1.3), Dst: 50.7.245.26 (50.7.245.26)
- Transmission Control Protocol:** Src Port: 64593 (64593), Dst Port: http (80), Seq: 1, Ack: 1, Len: 720
- Hypertext Transfer Protocol:**
 - GET /images/batik_kaskus-LOGO_seasonal.jpg HTTP/1.1\r\n
 - Host: img.kaskus.co.id\r\n
 - Connection: keep-alive\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.79 Safari/537.4\r\n
 - Accept: */*\r\n
 - Referer: http://www.kaskus.co.id/\r\n
 - Accept-Encoding: gzip, deflate, sdch\r\n
 - Accept-Language: id-ID,id;q=0.8,en-US;q=0.6,en;q=0.4\r\n
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

Lalu amati pada protokol HTTP, kemudia lihat detailnya di bawah, akan terlihat situs yang sedang di akses, namun untuk protokol HTTPS belum bisa di amati dengan wireshark

Referensi

Percobaan pribadi (aldiyusnika.wordpress.com)

Biografi Penulis



Kamaldila Puja Yusnika. Mahasiswa tingkat akhir Politeknik Negeri Semarang jurusan telekomunikasi, sedang mendalami hal-hal yang behubungan dengan jaringan komputer. Follow my twitter @Aldi_91 atau di blog saya aldiyusnika.wordpress.com