

CAPTURE DAN ANALISIS PAKET PROTOKOL MENGUNAKAN WIRESHARK



Nama : FADLI NURHUDA

NIM : 09011181419001

Kelas : SK 5A

Dosen Pengampuh : Dr. Deris Stiawan,M.T,Ph D.

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2016

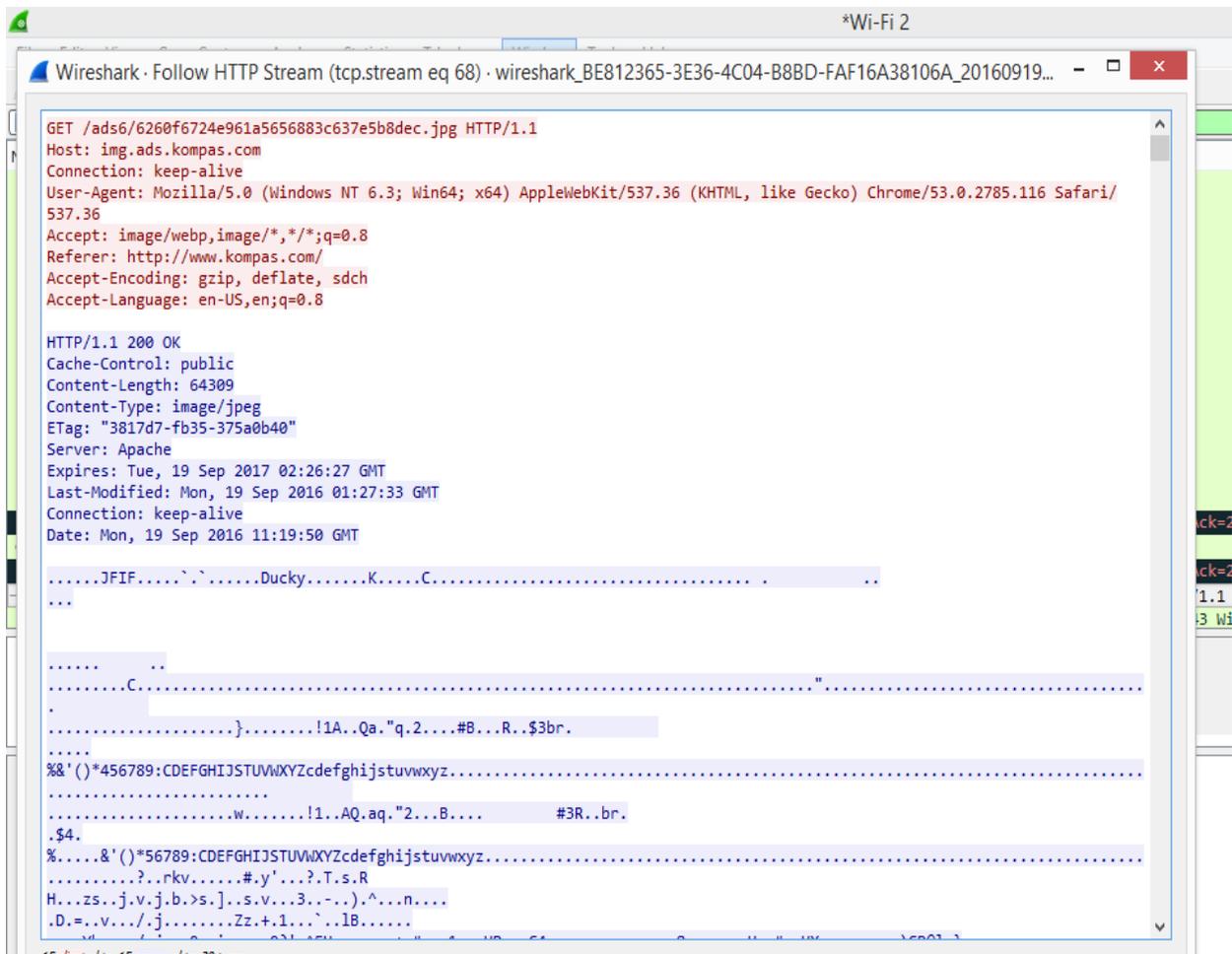
GET adalah method HTTP paling sederhana dan digunakan sebagian besar untuk meminta resource tertentu dari server, apakah berupa halaman web, file gambar grafis, atau sebuah dokumen, dan lain-lain. GET dapat juga digunakan untuk mengirim data di atas server, meskipun demikian hal itu mempunyai batasan-batasan. salah satu contoh menggunakan perintah Get yaitu saat Anda mengakses URL murni demi melihat data. Anda bisa menganggapnya sebagai menggunakan pernyataan select SQL. Anda meminta data dari server web tanpa maksud memperbarui data apapun. Anda perlu URL untuk menjadi 'bookmarkable'. Pada dasarnya HTTP GET dianggap diulangi, yang memungkinkan permintaan untuk dicoba aman dan tanggapan-cache. Anda tidak keberatan permintaan diulang. Misalnya pengguna mengunjungi URL yang sama lebih dari sekali. Sedangkan yang tidak menggunakan perintah get yaitu saat Anda lewat data sensitif seperti username, password, nomor jaminan sosial, dan lain-lain. Anda mengirimkan data dalam jumlah besar. Meskipun tidak ada batas karakter didefinisikan dalam spesifikasi HTTP untuk panjang URL, IE 4 misalnya hanya mendukung URL panjang maksimum ~ 2000 karakter menggunakan permintaan GET. Anda perlu memperbarui sesuatu pada server, misalnya mengirimkan formulir yang akan memperbarui alamat pengguna atau keranjang belanja.

Sedangkan Post merupakan Sebuah permintaan HTTP POST memanfaatkan badan pesan untuk mengirim data ke server web. Jika Anda memeriksa contoh permintaan HTTP POST di bawah ini, Anda akan melihat bahwa kita mengirimkan permintaan HTTP POST dengan tubuh pesan 'userid = mo & password = mypassw' untuk login.jsp (login.jsp akan menjadi sebuah aplikasi yang ke depan server web permintaan untuk). Salah satu contoh yang menggunakan perintah post yaitu Anda memiliki sejumlah besar data untuk mengirim ke server web (ukuran data akan melebihi batas URL dari metode GET). Anda mengirim data sensitif seperti uesrnames, password, nomor jaminan sosial dan lain-lain Anda mengubah keadaan data dalam aplikasi web. Misalnya, keranjang belanja melacak item yang Anda beli.

Sedangkan contoh yang tidak menggunakan post yaitu URL yang Anda melewati memiliki persyaratan menjadi 'bookmarkable'. Jika keadaan perubahan URL, maka pengguna tidak akan dapat mengambil, atau melihat data itu itu adalah mantan negara. Permintaan Anda perlu idempotent. Perhatikan bahwa permintaan POST bisa idempotent, namun itu praktik yang lebih baik untuk menggunakan PUT (jika metode permintaan HTTP ini didukung oleh web server dan client)

MAC merupakan singkatan dari Media Access Control Address adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasi sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address.

Nama NetBIOS adalah sebuah nama yang berukuran 16-byte yang digunakan oleh keluarga sistem operasi Windows NT untuk sebuah fungsi atau layanan jaringan. Nama NetBIOS digunakan oleh aplikasi-aplikasi yang memakai jasa protokol dan API NetBIOS. Menggunakan nama NetBIOS jauh lebih mudah dan lebih bersahabat untuk mengidentifikasi sebuah host komputer dalam sebuah jaringan daripada menggunakan angka-angka (dalam hal ini adalah alamat IP). Nama NetBIOS dapat digunakan dalam aplikasi Windows NT, mulai dari Windows Explorer, Network Neighborhood, dan juga perintah command-line net (net start, net stop, net send, dan lain-lain). Sama seperti halnya alamat IP, nama NetBIOS haruslah unik dalam sebuah jaringan; jika tidak, maka konflik akan terjadi dan sistem jaringan tidak akan dapat berjalan dengan baik. Dalam Windows 2000/XP/Server 2003 beberapa layanan jaringan (seperti halnya NetLogon) tidak menggunakan nama NetBIOS lagi, akan tetapi telah menggunakan Domain Name System (DNS). Meskipun demikian, aplikasi-aplikasi warisan Windows NT dapat berjalan di atas Windows 2000 ke atas dengan masih menggunakan nama NetBIOS untuk mengakses layanan-layanan tersebut.



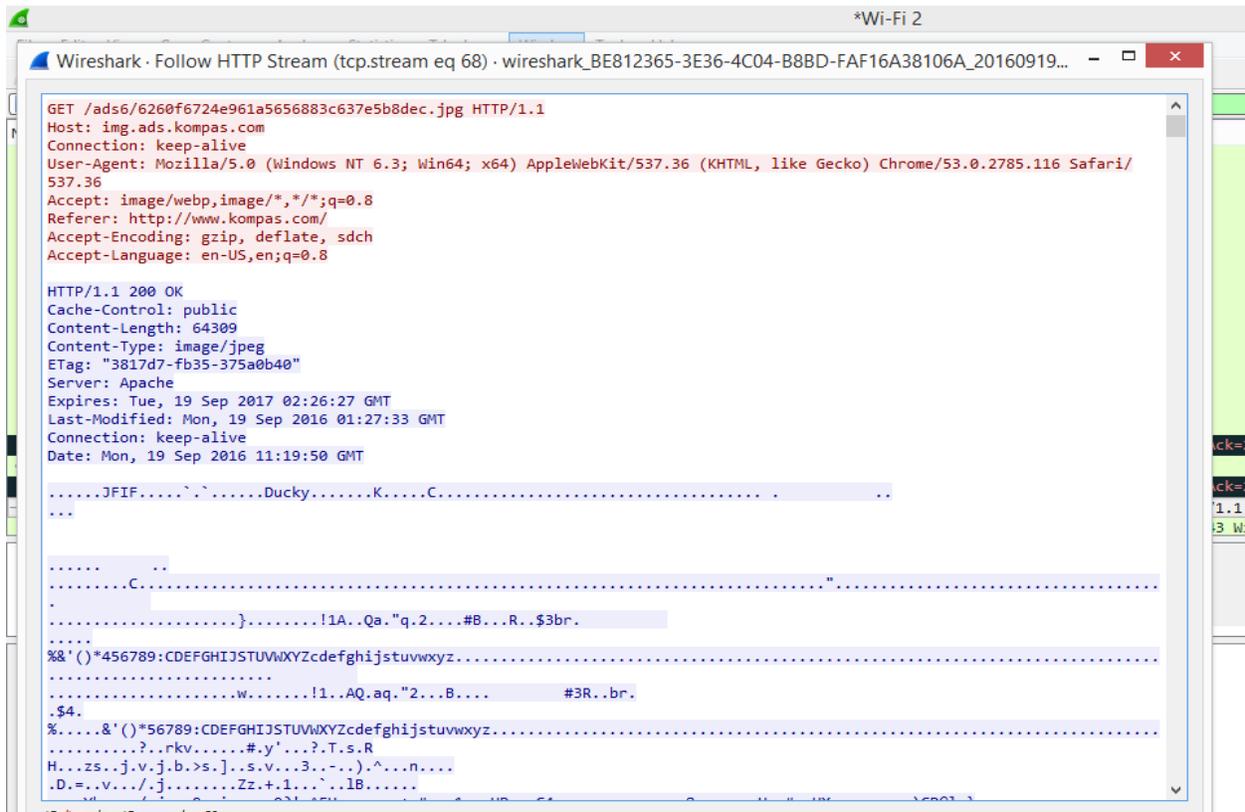
```
Wireshark · Follow HTTP Stream (tcp.stream eq 68) · wireshark_BE812365-3E36-4C04-B8BD-FAF16A38106A_20160919...
GET /ads6/6260f6724e961a5656883c637e5b8dec.jpg HTTP/1.1
Host: img.ads.kompas.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.116 Safari/537.36
Accept: image/webp,image/*,*/*;q=0.8
Referer: http://www.kompas.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Cache-Control: public
Content-Length: 64309
Content-Type: image/jpeg
ETag: "3817d7-fb35-375a0b40"
Server: Apache
Expires: Tue, 19 Sep 2017 02:26:27 GMT
Last-Modified: Mon, 19 Sep 2016 01:27:33 GMT
Connection: keep-alive
Date: Mon, 19 Sep 2016 11:19:50 GMT

.....JFIF.....`.....Ducky.....K.....C.....
.....
.....C....."
.....}.....!1A..Qa."q.2....#B...R..$3br.
.....
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxzy.....
.....
.....w.....!1..AQ.aq."2...B.... #3R..br.
.$4.
%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxzy.....
.....?.rkv.....#y'...?.T.s.R
H...zs..j.v.j.b.>s.].s.v...3...).^..n....
.D...v.../.j.....Zz.+1...^1B.....
```

Pada gambar diatas merupakan hasil capture menggunakan program wireshark. Wireshark merupakan salah satu tools atau aplikasi “Network Analyzer” atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (memperoleh informasi penting seperti password email, dll). Wireshark sendiri merupakan free tools untuk Network Analyzer yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface). Kegunaan wireshark yaitu Menganalisa jaringan yaitu Menangkap paket data atau informasi yang berkeliaran dalam jaringan yang terlihat. Penganalisaan informasi yang didapat dilakukan dengan sniffing, dengan begitu dapat diperoleh informasi penting seperti password, dan lain-lain. Selain itu kegunaannya yaitu Membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM. Selain itu Dapat mengetahui IP seseorang melalui typingan room. Serta Menganalisa transmisi paket data dalam jaringan, proses koneksi, dan transmisi data antar komputer. Pada gambar diatas merupakan hasil capture menggunakan program wireshark. Dan

dapat dianalisa yaitu user-agent yang digunakan yaitu chrome/53.0.2785.116 safari. Dan windows yang digunakan windows NT 6.3 x64. Dan refer yang ditujuh yaitu <http://www.kompas.com>. selain itu dapat diketahui date yaitu pada mon,19 sep 2016 09:52:09 dan via yang digunakan yaitu via 1.1 google. Sehingga post dapat diartikan dimana client mengirimkan data ke web server



Sedangkan gambar diatas merupakan gambar capture pada wireshark yang menampilkan fungsi get. Yaitu dimana client melakukan request pada web server agar web server dapat mengetahui dan menampilkan permintaan client seperti gambar diatas client melakukan request pada web server yang berupa situs www.kompas.com

```

C:\Windows\system32\cmd.exe

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 lenovo-pc:0 LISTENING
TCP 0.0.0.0:445 lenovo-pc:0 LISTENING
TCP 0.0.0.0:5357 lenovo-pc:0 LISTENING
TCP 0.0.0.0:49152 lenovo-pc:0 LISTENING
TCP 0.0.0.0:49153 lenovo-pc:0 LISTENING
TCP 0.0.0.0:49154 lenovo-pc:0 LISTENING
TCP 0.0.0.0:49155 lenovo-pc:0 LISTENING
TCP 0.0.0.0:49162 lenovo-pc:0 LISTENING
TCP 0.0.0.0:49164 lenovo-pc:0 LISTENING
TCP 127.0.0.1:5354 lenovo-pc:0 LISTENING
TCP 192.168.43.181:139 lenovo-pc:0 LISTENING
TCP 192.168.43.181:63596 74.125.68.188:5228 ESTABLISHED
TCP 192.168.43.181:63664 114.125.33.35:https TIME_WAIT
TCP 192.168.43.181:63676 182.253.238.102:https TIME_WAIT
TCP 192.168.43.181:63677 182.253.238.102:https ESTABLISHED
TCP 192.168.43.181:63678 182.253.238.102:https ESTABLISHED
TCP 192.168.43.181:63679 182.253.238.102:https TIME_WAIT
TCP 192.168.43.181:63680 104.244.42.3:https ESTABLISHED
TCP 192.168.43.181:63681 104.244.42.69:https ESTABLISHED
TCP 192.168.43.181:63682 104.25.75.109:https ESTABLISHED
TCP 192.168.43.181:63683 137.116.139.114:https ESTABLISHED
TCP 192.168.43.181:63684 74.125.68.94:https ESTABLISHED
TCP 192.168.43.181:63685 74.125.68.132:https ESTABLISHED

```

```

C:\Windows\system32\cmd.exe

TCP 192.168.43.181:63699 198.199.14.82:https ESTABLISHED
TCP 192.168.43.181:63700 146.88.135.5:https ESTABLISHED
TCP 192.168.43.181:63701 202.61.113.35:http ESTABLISHED
TCP 192.168.43.181:63702 202.61.113.35:http ESTABLISHED
TCP 192.168.43.181:63704 74.125.68.95:http ESTABLISHED
TCP 192.168.43.181:63705 74.125.68.95:http ESTABLISHED
TCP 192.168.43.181:63706 202.77.124.34:http ESTABLISHED
TCP 192.168.43.181:63707 202.77.124.34:http ESTABLISHED
TCP 192.168.43.181:63708 202.77.124.34:http ESTABLISHED
TCP 192.168.43.181:63709 114.125.1.152:http ESTABLISHED
TCP [::]:135 lenovo-pc:0 LISTENING
TCP [::]:445 lenovo-pc:0 LISTENING
TCP [::]:5357 lenovo-pc:0 LISTENING
TCP [::]:49152 lenovo-pc:0 LISTENING
TCP [::]:49153 lenovo-pc:0 LISTENING
TCP [::]:49154 lenovo-pc:0 LISTENING
TCP [::]:49155 lenovo-pc:0 LISTENING
TCP [::]:49162 lenovo-pc:0 LISTENING
TCP [::]:49164 lenovo-pc:0 LISTENING
UDP 0.0.0.0:123 **
UDP 0.0.0.0:3702 **
UDP 0.0.0.0:3702 **
UDP 0.0.0.0:5353 **
UDP 0.0.0.0:5353 **
UDP 0.0.0.0:5353 **

```

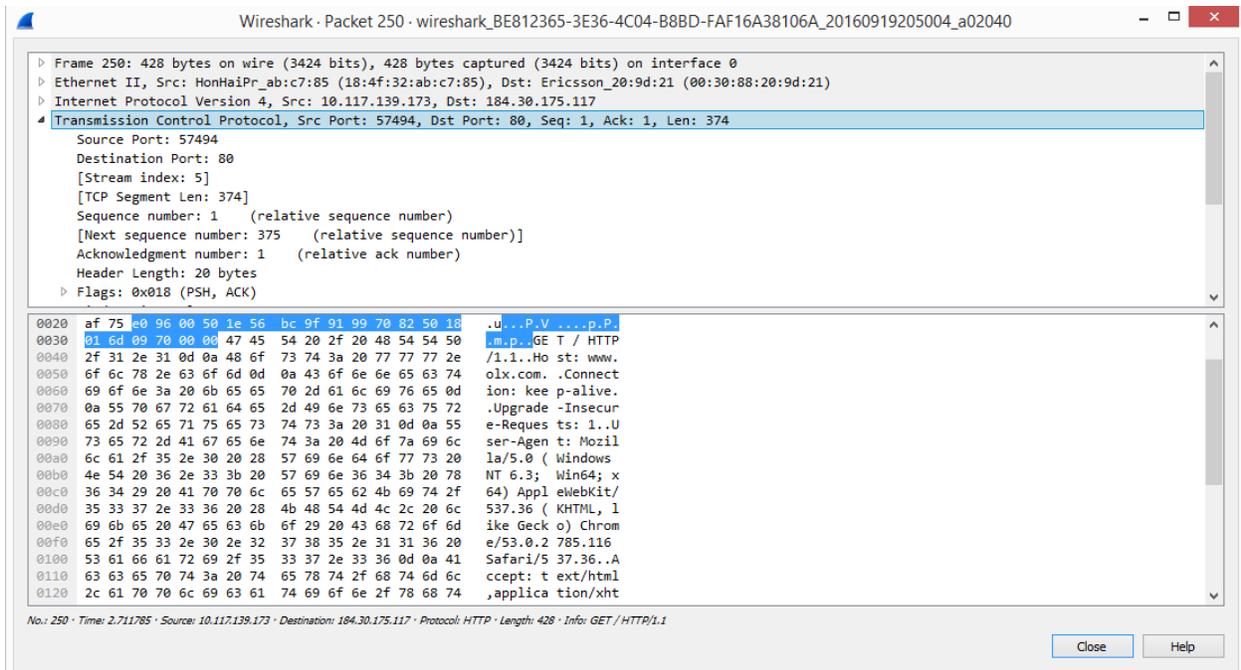
```
C:\Windows\system32\cmd.exe
UDP 0.0.0.0:58451 ***
UDP 127.0.0.1:1900 ***
UDP 127.0.0.1:49228 ***
UDP 192.168.43.181:137 ***
UDP 192.168.43.181:138 ***
UDP 192.168.43.181:1900 ***
UDP 192.168.43.181:5353 ***
UDP [::]:123 ***
UDP [::]:3702 ***
UDP [::]:3702 ***
UDP [::]:5353 ***
UDP [::]:5353 ***
UDP [::]:5355 ***
UDP [::]:51256 ***
UDP [::]:57974 ***
UDP [::]:58452 ***
UDP [::]:1900 ***
UDP [::]:49227 ***
UDP [fe80::28c6:2c3b:3f57:d44a%14]:546 ***
UDP [fe80::ad6e:f06c:84ee:6512%12]:546 ***
UDP [fe80::ad6e:f06c:84ee:6512%12]:1900 ***
C:\Users\G40-45>
```

Ini merupakan Hasil screenshot dari CMD dengan command netstat -a

Terdapat 2 buah protocol yaitu TCP dan UDP

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).

UDP adalah kependekan dari User Datagram Protocol merupakan bagian dari internet protocol. Dengan UDP, aplikasi komputer dapat mengirimkan pesan kepada komputer lain dalam jaringan lain tanpa melakukan komunikasi awal. UDP melakukan komunikasi secara sederhana dengan mekanisme yang sangat minimal.



Ini merupakan hasil screenshot dari destination port yaitu 80. Source port pada wireshark ini yaitu IP address pc si pemilik.