

TUGAS JARINGAN KOMPUTER



DISUSUN OLEH :

Nama : Dera Gustina
Nim : 09011181419003
Nama dosen : Dr. Deris Stiawan,M.T
Jurusan : Sistem Komputer
Fakultas : Ilmu Komputer

Universitas Sriwijaya

Menggunakan software wireshark dan command untuk mengetahui tentang network traffic

PENJELASAN :

Pengertian protokol : Protokol adalah aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan sehingga komputer-komputer anggota jaringan dan komputer berbeda platform dapat saling berkomunikasi.

Pengertian GET : Get adalah Sebuah permintaan GET mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan. Jika Anda memeriksa contoh permintaan HTTP bawah ini, kami minta index.html, dan melewati report_id parameter.

Pengertian POST : post adalah Sebuah permintaan HTTP POST memanfaatkan badan pesan untuk mengirim data ke server web.

Pengertian PUT : PUT adalah mirip dengan POST memanfaatkan badan pesan untuk mentransfer data. Namun, ada beberapa perbedaan mendasar antara keduanya. Pertama PUT dianggap idempotent, kedua tindakan seorang PUT ini selalu ditetapkan untuk URI tertentu, akhirnya PUT adalah untuk memuat data untuk sumber daya itu. Dengan kata lain Anda harus tahu lokasi yang tepat dari mana data yang Anda kirimkan akan diambil nanti.

Pengertian HEAD : head adalah HTTP Metode yang digunakan untuk mengambil informasi tentang URL dari web server.

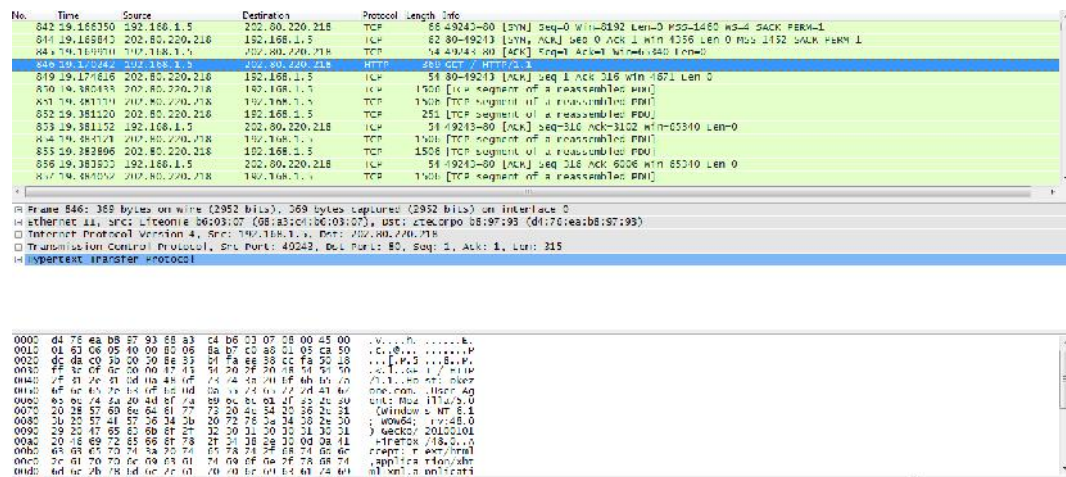
Pengertian DELETE : Menghapus sumber daya tertentu dari web server.

Pengertian TRACE : Metode ini menggemakan kembali permintaan yang diterima sehingga klien HTTP dapat melihat apa server menengah menambahkan atau mengubah permintan.

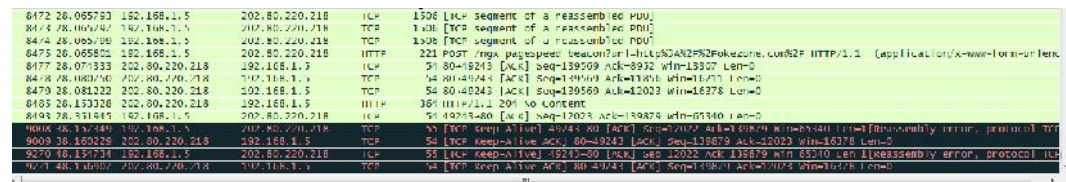
Pengertian OPTIONS : Metode ini membantu menentukan fungsi server seperti menentukan metode mana yang mendukung web server.

Pengertian CONNECT : Metode connect mengubah Permintaan koneksi ke terowongan TCP / IP transparan. Hal ini membantu memfasilitasi Secure Socket Layer (SSL) berkomunikasi (HTTPS) melalui proxy HTTP yang tidak terenkripsi

Gambar dibawah ini adalah analisis captture menganalisis traffic websate www.okezone.com menggunakan software wirkshark :



Okezone.com



Okezone.com

```
Follow TCP Stream (tcp.stream eq 27)

Stream Content
GET / HTTP/1.1
Host: okezone.com
User-Agent: Mozilla/5.0 (windows NT 6.1; wow64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: OKZ-LB-SRVCS
Date: Mon, 19 Sep 2016 11:45:14 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Vary: Accept-Encoding
Pragma: no-cache
X-Page-Speed: 1.11.33.0-0
Cache-Control: max-age=0, no-cache, no-store
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Link: <http://okezone.com/>; rel="canonical"
Connection: Keep-Alive
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2246e7c6cd9c1a72d838808c3fa42c0480%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A13%3A%22192.168.3.199%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A72%3A%22Mozilla%2F5.0+%28windows+NT+6.1%3B+wow64%3B+rv%3A48.0%29+Gecko%2F20100101+Firefox%2F48.0%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1474285514%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D5923865ea2c494eca649041ccfc7397c; expires=Mon, 19-Sep-2016 13:45:14 GMT; Max-Age=7200; path=/; domain=.okezone.com
Set-Cookie: PHPSESSID=vv8rh09nb3kcl3ieiminn2vcv3: nath=/

Entire conversation (189877 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
```

Software Wireshark memiliki kemampuan untuk menangkap lalu lalang kegiatan yang terjadi pada jaringan milik kita. Selain itu juga bisa mem-filter protokol lain selain ICMP, seperti HTTP dan lain-lain.

Panel pertama merupakan daftar dari data packet yang telah dicapture. Biasanya diurutkan berdasarkan waktu. Panel ini berisi no packet, waktu saat packet di capture, tujuan dan sumber dari packet, protocol yang digunakan dan panjangnya. Hasil yang difilter merupakan hasil dari filter dari packet yang berisi method 'GET'.

Panel ini berisi detail data dari packet yang dipilih di daftar packet. Di baris pertama terdapat frame 93 yang pada umumnya berisi data dari waktu dan panjang paket. Baris Kedua yang terdapat tulisan Ethernet II berisi informasi hardware dari pengirim dan penerima paket. Baris Ketiga berisi versi Internet Protocol. Dari screenshot diatas terlihat IP yang digunakan IPv4 dan jug terlihat IP pengirim dan penerima. Baris Keempat berisi Transmission Control Protocol,

ini berisi daftar port pengirim dan port penerima dan flag yang diset untuk paket yang menandakan apakah paket itu sekuensial atau request acknowledgment.

Baris Kelima berisi Hyper Text Transfer Protocol yaitu packet tersebut menggunakan protocol HTTP.

Panel ketiga merupakan Bytes dari paket. Panel ini berisi data yang diterima atau dikirim dalam bentuk hexadecimal. Karena kita tidak bisa membaca hexadecimal secara langsung maka dibagian kanan dari data hexadcimal terdapat 'terjemahan' nya.

Ip yang ada pada komputer saya adalah 192.168.1.5 dan ip destination adalah 202.80.220.218 . Terlihat bahwa 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 sedangkan dalam kasus ini hanya ditugaskan untuk mengunjungi sebuah situs kemudian dicapture dan method POST tidak terbaca karena kita tidak melakukan login,search pada website maupun login ke website tersebut. Sedangkan untuk method RESPONS dapat dilihat pada bagian GET yang didalamnya merupakan respon dari server yang dituju dalam kasus ini jika website berhasil dikunjungi maka akan menghasilkan RESPONS OK.

Selain menggunakan software wirshark analisis yang saya gunakan juga menggunakan commad promnt dimana hasilnya adalah sebagai berikut :

```

ca Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             user-PC:0              LISTENING
TCP   0.0.0.0:445             user-PC:0              LISTENING
TCP   0.0.0.0:554             user-PC:0              LISTENING
TCP   0.0.0.0:2869            user-PC:0              LISTENING
TCP   0.0.0.0:10243           user-PC:0              LISTENING
TCP   0.0.0.0:49152           user-PC:0              LISTENING
TCP   0.0.0.0:49153           user-PC:0              LISTENING
TCP   0.0.0.0:49154           user-PC:0              LISTENING
TCP   0.0.0.0:49155           user-PC:0              LISTENING
TCP   0.0.0.0:49156           user-PC:0              LISTENING
TCP   0.0.0.0:49161           user-PC:0              LISTENING
TCP   127.0.0.1:5354          user-PC:0              LISTENING
TCP   127.0.0.1:5354          user-PC:49157          ESTABLISHED
TCP   127.0.0.1:5354          user-PC:49159          ESTABLISHED
TCP   127.0.0.1:6543          user-PC:0              LISTENING
TCP   127.0.0.1:27015         user-PC:0              LISTENING
TCP   127.0.0.1:27015         user-PC:49150          ESTABLISHED
TCP   127.0.0.1:49157         user-PC:5354           ESTABLISHED
TCP   127.0.0.1:49158         user-PC:27015          ESTABLISHED
TCP   127.0.0.1:49159         user-PC:5354           ESTABLISHED
TCP   169.254.100.44:139     user-PC:0              LISTENING
TCP   192.168.1.5:139        user-PC:0              LISTENING
TCP   192.168.1.5:49160      ip-203-124-98-19:http  ESTABLISHED
TCP   192.168.1.5:49166      29:http                TIME_WAIT
TCP   192.168.1.5:49167      ec2-52-24-117-193:http TIME_WAIT
TCP   192.168.1.5:49168      112:http               TIME_WAIT
TCP   192.168.1.5:49170      ocsip:http            TIME_WAIT
TCP   192.168.1.5:49171      sa-in-f93:https        TIME_WAIT
TCP   192.168.1.5:49172      sa-in-f101:http        TIME_WAIT
TCP   192.168.1.5:49173      sin04s09-in-f14:https  TIME_WAIT
TCP   192.168.1.5:49175      server-54-230-159-210:https TIME_WAIT
TCP   192.168.1.5:49181      kul06s14-in-f4:https   TIME_WAIT
TCP   192.168.1.5:49183      20:https               TIME_WAIT
TCP   192.168.1.5:49184      a23-15-155-27:http     TIME_WAIT
TCP   192.168.1.5:49185      a23-15-155-27:http     TIME_WAIT
TCP   192.168.1.5:49186      20:https               TIME_WAIT
TCP   192.168.1.5:49187      server-54-230-159-112:https TIME_WAIT
TCP   192.168.1.5:49190      sb-in-f100:http        TIME_WAIT
TCP   192.168.1.5:49191      kul01s11-in-f3:http    TIME_WAIT
TCP   192.168.1.5:49192      kul01s11-in-f3:https   TIME_WAIT
TCP   192.168.1.5:49193      sa-in-f132:https       TIME_WAIT
TCP   192.168.1.5:49194      sb-in-f94:https        TIME_WAIT
TCP   192.168.1.5:49195      sa-in-f94:https        TIME_WAIT
TCP   192.168.1.5:49196      sb-in-f102:https       TIME_WAIT
TCP   192.168.1.5:49197      sa-in-f100:https       TIME_WAIT
TCP   192.168.1.5:49198      sin04s05-in-f174:https TIME_WAIT
TCP   192.168.1.5:49201      104.25.11.6:https      CLOSE_WAIT
TCP   192.168.1.5:49202      10:http                ESTABLISHED
TCP   192.168.1.5:49203      114:http               TIME_WAIT

```



```

Administrator: C:\Windows\system32\cmd.exe
TCP 192.168.1.5:49201 104.25.11.6:https CLOSE_WAIT
TCP 192.168.1.5:49202 10:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49203 114:80:80:80:80:80:80:80 TIME_WAIT
TCP 192.168.1.5:49204 1c:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49205 crl:80:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49206 114:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49207 36.86.63.180:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49208 106:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49210 1c:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49211 29:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49212 114:80:80:80:80:80:80:80 ESTABLISHED
TCP 192.168.1.5:49213 104.16.90.188:80:80:80:80:80:80:80:80 ESTABLISHED
TCP [::1]:135 user-PC:0 LISTENING
TCP [::1]:445 user-PC:0 LISTENING
TCP [::1]:554 user-PC:0 LISTENING
TCP [::1]:2869 user-PC:0 LISTENING
TCP [::1]:10243 user-PC:0 LISTENING
TCP [::1]:49152 user-PC:0 LISTENING
TCP [::1]:49153 user-PC:0 LISTENING
TCP [::1]:49154 user-PC:0 LISTENING
TCP [::1]:49155 user-PC:0 LISTENING
TCP [::1]:49156 user-PC:0 LISTENING
TCP [::1]:49161 user-PC:0 LISTENING
TCP [::1]:2869 user-PC:49214 TIME_WAIT
TCP [::1]:2869 user-PC:49215 ESTABLISHED
TCP [::1]:49215 user-PC:icslap ESTABLISHED
UDP 0.0.0.0:5000 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5004 *:*
UDP 0.0.0.0:5005 *:*
UDP 0.0.0.0:5355 *:*
UDP 0.0.0.0:57668 *:*
UDP 0.0.0.0:59525 *:*
UDP 0.0.0.0:65430 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:50336 *:*
UDP 127.0.0.1:50337 *:*
UDP 127.0.0.1:56946 *:*
UDP 127.0.0.1:63768 *:*
UDP 127.0.0.1:63769 *:*
UDP 169.254.100.44:137 *:*
UDP 169.254.100.44:138 *:*
UDP 169.254.100.44:1900 *:*
UDP 169.254.100.44:5353 *:*
UDP 192.168.1.5:137 *:*
UDP 192.168.1.5:138 *:*
UDP 192.168.1.5:1900 *:*
UDP 192.168.1.5:5353 *:*
UDP [::1]:500 *:*
UDP [::1]:4500 *:*
UDP [::1]:5004 *:*
UDP [::1]:5005 *:*
UDP [::1]:5355 *:*
UDP [::1]:53162 *:*
UDP [::1]:56138 *:*
UDP [::1]:61561 *:*
UDP [::1]:62342 *:*

```

```

UDP [::1]:500 *:*
UDP [::1]:4500 *:*
UDP [::1]:5004 *:*
UDP [::1]:5005 *:*
UDP [::1]:5355 *:*
UDP [::1]:53162 *:*
UDP [::1]:56138 *:*
UDP [::1]:61561 *:*
UDP [::1]:62342 *:*
UDP [::1]:65431 *:*
UDP [::1]:1900 *:*
UDP [::1]:56945 *:*
UDP [fe80::282f:bc60:98fd:642c%16]:1900 *:*
UDP [fe80::282f:bc60:98fd:642c%16]:5353 *:*
UDP [fe80::943a:b5d8:a476:1648%12]:1900 *:*
C:\Users\user>

```

Pada hasil capture diatas command yang digunakan yaitu “netstat -a” dan muncul tampilan seperti diatas. Cara membaca hasil capture menggunakan

command netstat -a adalah melihat Local Address yang merupakan IP Address komputer kita sendiri atau merupakan source dan untuk Destination dapat dilihat pada bagian Foreign Address. 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.

```
Administrator: C:\Windows\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Bluetooth Network Connection 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Wireless Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::943a:b5d8:a476:1648%12
    IPv4 Address. . . . . : 192.168.1.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%12
                                192.168.1.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::282f:bc60:98fd:642c%16
    Autoconfiguration IPv4 Address. . . : 169.254.100.44
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

Tunnel adapter isatap.{7C1DB121-1DE9-459E-8592-7BF93B15D4FE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter isatap.{4F02C20E-C80F-4948-A38C-23C2431F3672}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter isatap.{FBB06F33-B825-440F-AF31-E5C4ABC8E2EC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:2456:3fb4:1031:3f80:3f57:fefa
    Link-local IPv6 Address . . . . . : fe80::1031:3f80:3f57:fefa%21
    Default Gateway . . . . . : ::
```

Gambar diatas adalah gambar ip yang ada pada komputer yang saya gunakan