

Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

# **TUGAS JARINGAN KOMPUTER**

## **TASK V**



Disusun Oleh

Nama : Gonewaje

NIM : 09011181419005

Kelas : SK5A

Dosen Pembimbing : Dr. Deris Stiawan, M.T

**JURUSAN SISTEM KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**

Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

## TASK V

### Computer Networking

#### Using Wireshark and Command "*netstat -a*" to Know About Network Traffic

- What is the protocol ?

**Protokol** dalam ilmu komputer berarti seperangkat peraturan atau prosedur untuk mengirimkan data antara perangkat elektronik (mis. komputer).

Agar komputer satu dan komputer lain dapat mempertukarkan informasi, harus sudah ada persetujuan sebelumnya antarperangkat bagaimana struktur informasi dipertukarkan (dikirim dan diterima).[1]

- What is the ICMP (Internet Control Message Protocol) ?

**Internet Control Message Protocol (ICMP)** adalah salah satu protokol inti dari keluarga protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.[2]

- What is the port?

**Port** adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasi aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasi sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan Port Number dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah.[3]

- What is the HTTP Methods?

HTTP mendefinisikan metode (kadang-kadang disebut sebagai kata kerja) untuk menunjukkan tindakan yang diinginkan yang akan dilakukan pada sumber daya yang akan diidentifikasi. Apakah sumber daya ini mewakili, apakah data yang sudah ada atau data yang dihasilkan secara dinamis, tergantung pada pelaksanaan server.[4]

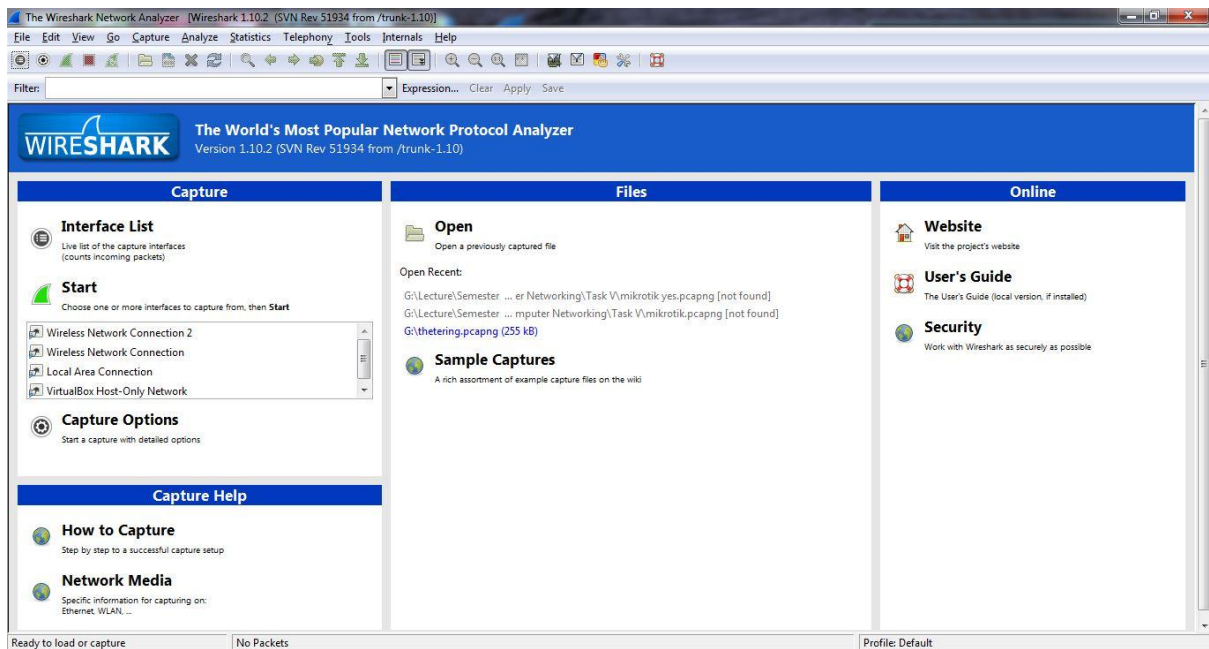
Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

S.N.	Method and Description
1	<b>GET</b> The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.
2	<b>HEAD</b> Same as GET, but transfers the status line and header section only.
3	<b>POST</b> A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
4	<b>PUT</b> Replaces all current representations of the target resource with the uploaded content.
5	<b>DELETE</b> Removes all current representations of the target resource given by a URI.
6	<b>CONNECT</b> Establishes a tunnel to the server identified by a given URI.
7	<b>OPTIONS</b> Describes the communication options for the target resource.
8	<b>TRACE</b> Performs a message loop-back test along the path to the target resource.

[5]

Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A  
ANALYSIS

Analisa yang dilakukan pada task 5 kali ini adalah menggunakan software “WireShark” yang mana software ini termasuk software terbaik yang dapat digunakan untuk meng-capture lalu lintas data pada suatu jaringan, selain “Wireshark” masih ada beberapa software lain yang berfungsi sama contohnya adalah “Colasoft”. Sebagai tambahan ataupun pelengkap untuk mengamati lalu lintas jaringan tersebut, digunakan pula command “netstat – a” pada *command prompt* yang bertujuan untuk melihat lalu lintas data secara keseluruhan pada suatu jaringan (-a/all/semua).



*tampilan awal software wireshark*

Analisa kali ini berguna untuk mengetahui metode 3 ways hand shake dalam lalu lintas data dan pertukaran data, dimana pada task sebelumnya digunakan analisa menggunakan software “Visual Route” untuk melihat beberapa *hop* yang dilewati dari source to destination. Website yang digunakan sebagai contoh adalah “mikrotik.co.id” yang mempunyai server di IIX. Sebelumnya cek terlebih dahulu IP komputer kita yang mana nanti nya akan disebut sebagai *source*, gunakan command *ipconfig* pada *command prompt*

Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

```
C:\Users\x450cc>ipconfig

Windows IP Configuration

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::c400:64a:2f35:446a%12
    IPv4 Address. . . . . : 10.117.29.48
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.117.0.1

Ethernet adapter Local Area Connection:

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

Ethernet adapter UirtualBox Host-Only Network:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::3818:ca1:e869:7469%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.{B2213103-667D-4F63-9A8F-419907FD1E00}:

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

Tunnel adapter isatap.{651A5DB8-BB63-49F0-A417-5DCACB07DA79}:

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

Tunnel adapter isatap.{BDEC27B2-FA18-4A8E-B601-89B09B4B642C}:

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

Tunnel adapter isatap.{18917512-4A62-4EAD-803D-E81F47FF0447}:



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

Tunnel adapter Teredo Tunneling Pseudo-Interface:


    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:2456:3fb4:2c63:1bcf:f58a:e2cf
    Link-local IPv6 Address . . . . . : fe80::2c63:1bcf:f58a:e2cf%14
    Default Gateway . . . . . : ::
```


Terlihat pada gambar diatas bahwa Ipv4 Address kita adalah **10.117.29.48** , kemudian cek pula IP website tujuan kita tadi yaitu “mikrotik.co.id” dengan menggunakan bantuan website *check-host.net* dan hasilnya ialah sebagai berikut


Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

**CHECK-HOST**   
IP: 36.84.62.176 Country:  Indonesia (North Sumatra, Pandau Hulu II)

Info Ping HTTP TCP port UDP port DNS

**IP and website location: mikrotik.co.id** 

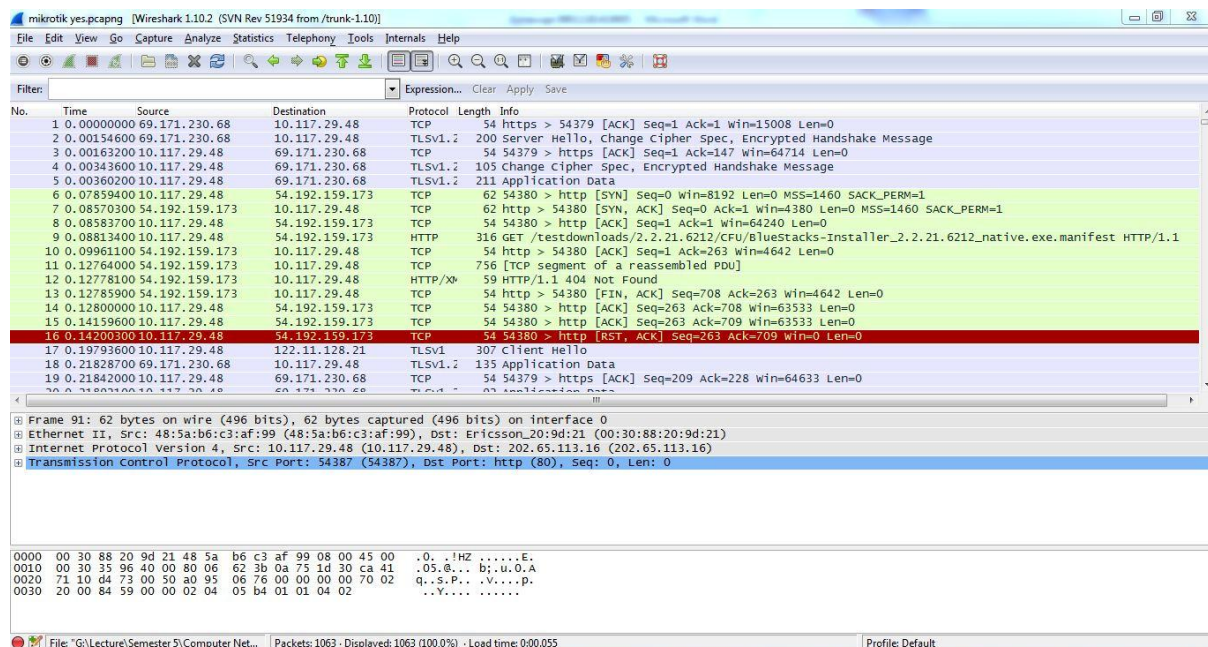
DB-IP	
IP address	<b>202.65.113.16</b>
Host name	www.mikrotik.co.id
IP range	202.65.113.0-202.65.113.255 CIDR
ISP	PT Jembatan Citra Nusantara
Organization	
Country	 <b>Indonesia (ID)</b>
Region	Yogyakarta
City	Catur Tunggal
Time zone	Asia/Jakarta, GMT+0700
Local time	13:31:31 (WIB) / 2016.08.28
Postal Code	



Map Satellite  
Jakarta Bandung EAST-JAVA  
Java Sea  
SOUTH KALIMANTAN  
Christmas Island  
Google Map data ©2016 Google Terms of Use

IP address dari website “mikrotik.co.id” adalah **202.65.113.16** dan dapat kita katakan sebagai *destination*.

Langkah awal adalah meng-capture lalu lintas data menggunakan wireshark dan command “netstat -a” pada command prompt, kemudian kita dapat langsung mengunjungi website yang dituju yang secara otomatis akan di capture oleh wireshark maupun command “netstat -a”.



mikrotik.yes.pcapng [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	69.171.230.68	10.117.29.48	TCP	54	https > 54379 [ACK] Seq=1 Ack=1 win=15008 Len=0
2	0.00154600	69.171.230.68	10.117.29.48	TLSv1.2	200	Server Hello, Change Cipher Spec, Encrypted Handshake Message
3	0.00163200	10.117.29.48	69.171.230.68	TCP	54	54379 > https [ACK] Seq=1 Ack=147 win=64714 Len=0
4	0.00343600	10.117.29.48	69.171.230.68	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
5	0.00360200	10.117.29.48	69.171.230.68	TLSv1.2	211	Application Data
6	0.07859400	10.117.29.48	54.192.159.173	TCP	62	54380 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
7	0.08570300	54.192.159.173	10.117.29.48	TCP	62	http > 54380 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
8	0.08583700	10.117.29.48	54.192.159.173	TCP	54	54380 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
9	0.08813400	10.117.29.48	54.192.159.173	HTTP	316	GET /testdown/loads/2.2.21.6212/CFU/bluestacks-Installer_2.2.21.6212_native.exe.manifest HTTP/1.1
10	0.09961100	54.192.159.173	10.117.29.48	TCP	54	http > 54380 [ACK] Seq=1 Ack=263 Win=4642 Len=0
11	0.12764000	54.192.159.173	10.117.29.48	TCP	756	[TCP segment of a reassembled PDU]
12	0.12778100	54.192.159.173	10.117.29.48	HTTP/1.1	59	404 Not Found
13	0.12785900	54.192.159.173	10.117.29.48	TCP	54	http > 54380 [FIN, ACK] Seq=708 Ack=263 Win=4642 Len=0
14	0.12800000	10.117.29.48	54.192.159.173	TCP	54	54380 > http [ACK] Seq=263 Ack=708 Win=63533 Len=0
15	0.14159600	10.117.29.48	54.192.159.173	TCP	54	54380 > http [ACK] Seq=263 Ack=709 Win=63533 Len=0
16	0.14200300	10.117.29.48	54.192.159.173	TCP	54	54380 > http [RST, ACK] Seq=263 Ack=709 Win=0 Len=0
17	0.19793600	10.117.29.48	122.11.128.21	TLSv1	307	Client Hello
18	0.21828700	69.171.230.68	10.117.29.48	TLSv1.2	135	Application Data
19	0.21842000	10.117.29.48	69.171.230.68	TCP	54	54379 > https [ACK] Seq=209 Ack=228 Win=64633 Len=0

Frame 91: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0  
Ethernet II, Src: 48:5a:b6:c3:af:99 (48:5a:b6:c3:af:99), Dst: Ericsson\_20:9d:21 (00:30:88:20:9d:21)  
Internet Protocol Version 4, Src: 10.117.29.48 (10.117.29.48), Dst: 202.65.113.16 (202.65.113.16)  
Transmission Control Protocol, Src port: 54387 (54387), Dst port: http (80), Seq: 0, Len: 0

```
0000 00 30 88 20 9d 21 48 5a b6 c3 af 99 08 00 45 00 .0. .!HZ . . . . .E.
0010 00 30 35 96 40 00 80 06 62 3b 0a 75 1d 30 ca 41 .05.e... b;u.O.A
0020 71 10 d4 73 00 50 a0 95 06 76 00 00 00 70 02 q..s.P..v....p.
0030 20 00 84 59 00 00 02 04 05 b4 01 01 04 02 ..v....
```

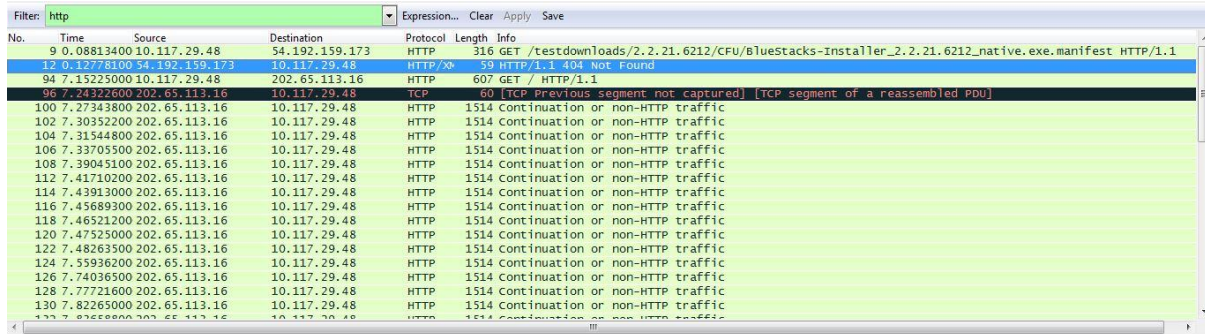
File: "G:\Lecture\Semester 5\Computer Net..." Packets: 1063 - Displayed: 1063 (100.0%) - Load time: 0:00.055 Profile: Default

hasil capture dengan wireshark hingga proses loading website selesai.



Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

Agar lebih memudahkan kita untuk mengetahui lalu lintas data yang hanya berada pada komputer yang kita gunakan adalah dengan cara mem-filter protokol yang ter-capture. Protokol yang kita gunakan adalah protokol HTTP (Hypertext Transfer Protocol) yaitu sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia[6].



No.	Time	Source	Destination	Protocol	Length	Info
9	0.08813400	10.117.29.48	54.192.159.173	HTTP	316	GET /testdownloads/2.2.21.6212/CFU/bluestacks-installer_2.2.21.6212_native.exe.manifest HTTP/1.1
12	0.12778100	54.192.159.173	10.117.29.48	HTTP/x	59	HTTP/1.1 404 Not Found
94	7.15225000	10.117.29.48	202.65.113.16	HTTP	607	GET / HTTP/1.1
96	7.24322000	202.65.113.16	10.117.29.48	TCP	60	[TCP previous segment not captured] [TCP segment of a reassembled PDU]
100	7.27343800	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
102	7.30352200	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
104	7.31544800	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
106	7.33705500	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
108	7.39045100	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
112	7.41710200	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
114	7.43913000	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
116	7.45689300	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
118	7.46521200	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
120	7.47525000	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
122	7.48263500	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
124	7.55936200	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
126	7.74036500	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
128	7.77216000	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
130	7.82265000	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic

hasil filter http

Setelah selesai difilter, disana kita dapat melihat seluruh paket data yang menggunakan protokol HTTP dan disinilah kegunaan dari IP *source* dan IP *destination* yang telah kita cari tahu sebelumnya.

IP *source* atau IP komputer kita adalah **10.117.29.48** dan IP *destination* adalah **202.65.113.16** yang secara tidak langsung memberikan kita filter tersendiri terhadap paket-paket maupun data-data yang ter-capture. Pada wireshark yang telah difilter tadi dapat dilihat IP *source* maupun IP *destination* serta menggunakan protokol HTTP yang pertama kali muncul pada nomor 94 dan kuat dugaan sebagai paket data yang ter-capture di komputer kita yang mengunjungi website *mikrotik.co.id*

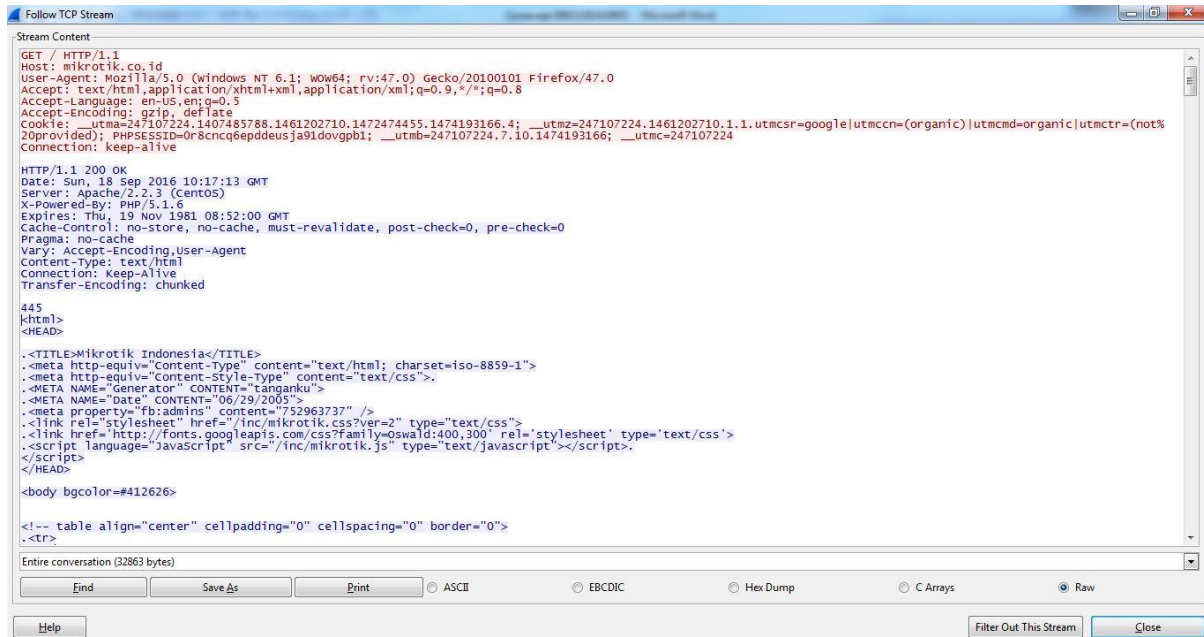


9	0.08813400	10.117.29.48	54.192.159.173	HTTP	316	GET /testdownloads/2.2.21.6212/CFU/bluestacks-installer_2.2.21.6212_native.exe.manifest HTTP/1.1
12	0.12778100	54.192.159.173	10.117.29.48	HTTP/x	59	HTTP/1.1 404 Not Found
94	7.15225000	10.117.29.48	202.65.113.16	HTTP	607	GET / HTTP/1.1
96	7.24322000	202.65.113.16	10.117.29.48	TCP	60	[TCP previous segment not captured] [TCP segment of a reassembled PDU]
100	7.27343800	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
102	7.30352200	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
104	7.31544800	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic
106	7.33705500	202.65.113.16	10.117.29.48	HTTP	1514	Continuation or non-HTTP traffic

data/paket terduga

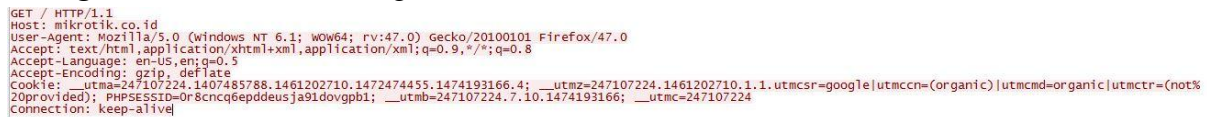
data tersebut mempunyai protokol HTTP dengan panjang paket/data 607 dan HTTP Method nya adalah GET yang mana GET digunakan untuk mengambil informasi dari server yang diberikan menggunakan URL yang diberikan. Sebuah permintaan GET mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan. Ini adalah metode utama yang digunakan untuk pengambilan dokumen. Untuk melihat isi dari HTTP Method GET yaitu dengan cara *right click* pada paket/data no.94 yang diduga sebelumnya dan kemudian pilih *Follow TCP Stream* dan akan dimunculkan info sebagai berikut

Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A



The screenshot shows a network traffic capture window titled "Follow TCP Stream". The main content area displays the raw data of an HTTP GET request. The request starts with "GET / HTTP/1.1" and includes various headers such as "Host: mikrotik.co.id", "User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0", "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", and a long "Cookie" string. The status line is "HTTP/1.1 200 OK". The response headers include "Date: Sun, 18 Sep 2016 10:17:13 GMT", "Server: Apache/2.2.3 (CentOS)", "X-Powered-By: PHP/5.1.6", "Expires: Thu, 19 Nov 1981 08:52:00 GMT", "Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0", "Pragma: no-cache", "Vary: Accept-Encoding, User-Agent", "Content-Type: text/html", "Connection: Keep-Alive", and "Transfer-Encoding: chunked". The body of the response starts with "445" and "<html><HEAD>". The HTML content includes a title "Mikrotik Indonesia", meta tags for content type and style, generator, date, and fb:admins, and links to CSS and JavaScript files. The body background color is "#412626".

Dapat dilihat pada paket/data mentah (raw) diatas bahwa HTTP Method GET mencoba “mengambil” / HTTP/1.1 dengan host *mikrotik.co.id*



This is a duplicate of the screenshot above, showing the raw data of an HTTP GET request to mikrotik.co.id.

#### Method GET

Kemudian server akan merespon terhadap permintaan GET tersebut sebagai berikut



The screenshot shows the raw data of an HTTP GET response from mikrotik.co.id. The status line is "HTTP/1.1 200 OK". The response headers include "Date: Sun, 18 Sep 2016 10:17:13 GMT", "Server: Apache/2.2.3 (CentOS)", "X-Powered-By: PHP/5.1.6", "Expires: Thu, 19 Nov 1981 08:52:00 GMT", "Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0", "Pragma: no-cache", "Vary: Accept-Encoding, User-Agent", "Content-Type: text/html", "Connection: Keep-Alive", and "Transfer-Encoding: chunked". The body of the response starts with "445" and "<html><HEAD>". The HTML content includes a title "Mikrotik Indonesia", meta tags for content type and style, generator, date, and fb:admins, and links to CSS and JavaScript files. The body background color is "#412626".

#### Respons GET

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.



Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

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.

```
C:\Users\x450cc>netstat -a
Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	GoUi-PC:0	LISTENING
TCP	0.0.0.0:445	GoUi-PC:0	LISTENING
TCP	0.0.0.0:2861	GoUi-PC:0	LISTENING
TCP	0.0.0.0:2869	GoUi-PC:0	LISTENING
TCP	0.0.0.0:5665	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12025	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12110	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12119	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12143	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12465	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12563	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12993	GoUi-PC:0	LISTENING
TCP	0.0.0.0:12995	GoUi-PC:0	LISTENING
TCP	0.0.0.0:27275	GoUi-PC:0	LISTENING
TCP	0.0.0.0:49152	GoUi-PC:0	LISTENING
TCP	0.0.0.0:49153	GoUi-PC:0	LISTENING
TCP	0.0.0.0:49154	GoUi-PC:0	LISTENING
TCP	0.0.0.0:49155	GoUi-PC:0	LISTENING
TCP	0.0.0.0:49157	GoUi-PC:0	LISTENING
TCP	10.117.29.48:139	GoUi-PC:0	LISTENING
TCP	10.117.29.48:52297	sc-in-f95:https	TIME_WAIT
TCP	10.117.29.48:52412	2:https	TIME_WAIT
TCP	10.117.29.48:52418	3:https	TIME_WAIT
TCP	10.117.29.48:52422	23:https	TIME_WAIT
TCP	10.117.29.48:52468	14:https	ESTABLISHED
TCP	10.117.29.48:52514	89:http	TIME_WAIT
TCP	10.117.29.48:52515	89:http	TIME_WAIT
TCP	10.117.29.48:52519	19:http	TIME_WAIT
TCP	10.117.29.48:52521	19:http	TIME_WAIT
TCP	10.117.29.48:54312	122.11.128.21:https	TIME_WAIT
TCP	10.117.29.48:54336	42:https	ESTABLISHED
TCP	10.117.29.48:54338	www:http	TIME_WAIT
TCP	10.117.29.48:54352	52:https	TIME_WAIT
TCP	10.117.29.48:54357	sc-in-f132:https	ESTABLISHED
TCP	10.117.29.48:54360	36.86.63.180:http	TIME_WAIT
TCP	10.117.29.48:54362	36.86.63.180:http	TIME_WAIT
TCP	10.117.29.48:54363	36.86.63.180:http	TIME_WAIT
TCP	10.117.29.48:54364	36.86.63.180:http	TIME_WAIT
TCP	10.117.29.48:54365	36.86.63.180:http	TIME_WAIT
TCP	10.117.29.48:54367	122.11.128.21:https	TIME_WAIT
TCP	10.117.29.48:54368	sc-in-f83:http	TIME_WAIT
TCP	10.117.29.48:54369	104.20.23.127:http	TIME_WAIT
TCP	10.117.29.48:54370	122.11.128.21:https	TIME_WAIT
TCP	10.117.29.48:54371	122.11.128.21:https	TIME_WAIT
TCP	10.117.29.48:54379	edge-star-mini-shv-17-prn1:https	ESTABLISHED

hasil capture menggunakan command netstat -a di command prompt (a)

Nama : Gonewaje  
NIM : 09011181419005  
Kelas : SK5A

```
TCP 10.117.29.48:54381 127.0.0.1:https SYN_SENT
TCP 127.0.0.1:1001 GoUi-PC:0 LISTENING
TCP 127.0.0.1:5037 GoUi-PC:0 LISTENING
TCP 127.0.0.1:7037 GoUi-PC:0 LISTENING
TCP 127.0.0.1:10400 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12025 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12110 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12119 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12143 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12465 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12563 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12993 GoUi-PC:0 LISTENING
TCP 127.0.0.1:12995 GoUi-PC:0 LISTENING
TCP 127.0.0.1:27275 GoUi-PC:0 LISTENING
TCP 127.0.0.1:49158 GoUi-PC:0 LISTENING
TCP 127.0.0.1:49260 GoUi-PC:49261 ESTABLISHED
TCP 127.0.0.1:49261 GoUi-PC:49260 ESTABLISHED
TCP 127.0.0.1:50911 GoUi-PC:0 LISTENING
TCP 127.0.0.1:54354 GoUi-PC:54355 ESTABLISHED
TCP 127.0.0.1:54355 GoUi-PC:54354 ESTABLISHED
TCP 127.0.0.1:54383 GoUi-PC:9999 SYN_SENT
TCP 192.168.56.1:139 GoUi-PC:0 LISTENING
TCP [::]:135 GoUi-PC:0 LISTENING
TCP [::]:445 GoUi-PC:0 LISTENING
TCP [::]:2861 GoUi-PC:0 LISTENING
TCP [::]:2869 GoUi-PC:0 LISTENING
TCP [::]:49152 GoUi-PC:0 LISTENING
TCP [::]:49153 GoUi-PC:0 LISTENING
TCP [::]:49154 GoUi-PC:0 LISTENING
TCP [::]:49155 GoUi-PC:0 LISTENING
TCP [::]:49157 GoUi-PC:0 LISTENING
TCP [::1]:12025 GoUi-PC:0 LISTENING
TCP [::1]:12110 GoUi-PC:0 LISTENING
TCP [::1]:12119 GoUi-PC:0 LISTENING
TCP [::1]:12143 GoUi-PC:0 LISTENING
TCP [::1]:12465 GoUi-PC:0 LISTENING
TCP [::1]:12563 GoUi-PC:0 LISTENING
TCP [::1]:12993 GoUi-PC:0 LISTENING
TCP [::1]:12995 GoUi-PC:0 LISTENING
TCP [::1]:27275 GoUi-PC:0 LISTENING
TCP [::1]:49156 GoUi-PC:0 LISTENING
UDP 0.0.0.0:68 *:*
```

hasil capture menggunakan command netstat -a di command prompt (b)

```
UDP 0.0.0.0:68 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5355 *:*
UDP 0.0.0.0:9986 *:*
UDP 0.0.0.0:11572 *:*
UDP 0.0.0.0:50900 *:*
UDP 0.0.0.0:54161 *:*
UDP 10.117.29.48:137 *:*
UDP 10.117.29.48:138 *:*
UDP 10.117.29.48:1900 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:50901 *:*
UDP 127.0.0.1:52102 *:*
UDP 127.0.0.1:60122 *:*
UDP 192.168.56.1:137 *:*
UDP 192.168.56.1:138 *:*
UDP 192.168.56.1:1900 *:*
UDP [::]:500 *:*
UDP [::]:4500 *:*
UDP [::]:5355 *:*
UDP [::1]:1900 *:*
UDP [::1]:52101 *:*
UDP [fe80::3818:ca1:e869:7469%25]:1900 *:*
UDP [fe80::e4cc:64c:2f35:446a%12]:1900 *:*

C:\Users\x450cc>
```

hasil capture menggunakan command netstat -a di command prompt (c)

**Nama : Gonewaje**

**NIM : 09011181419005**

**Kelas : SK5A**

Selain menggunakan software wireshark, capture juga dilakukan menggunakan command *netstat -a* pada command prompt dan muncul tampilan seperti diatas. Port yang digunakan pada praktikum kali ini menggunakan Port 80 dikarenakan port tersebut digunakan untuk mengakses World Wide Web (WWW). Protokol yang digunakan adalah protokol TCP **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*).[6] 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.

**Nama : Gonewaje**  
**NIM : 09011181419005**  
**Kelas : SK5A**  
**Reference**

[1][https://id.wikipedia.org/wiki/Protokol\\_\(komputer\)](https://id.wikipedia.org/wiki/Protokol_(komputer))

[2][https://id.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](https://id.wikipedia.org/wiki/Internet_Control_Message_Protocol)

[3][https://id.wikipedia.org/wiki/Port\\_\(Jaringan\\_Komputer\)](https://id.wikipedia.org/wiki/Port_(Jaringan_Komputer))

[4][https://en.wikipedia.org/wiki/Hypertext\\_Transfer\\_Protocol](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol)

[5] [https://www.tutorialspoint.com/http/http\\_methods.htm](https://www.tutorialspoint.com/http/http_methods.htm)

[6] [https://id.wikipedia.org/wiki/Protokol\\_Transfer\\_Hiperteks](https://id.wikipedia.org/wiki/Protokol_Transfer_Hiperteks)

[7] [https://id.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://id.wikipedia.org/wiki/Transmission_Control_Protocol)