

JARINGAN KOMPUTER
(Capturing Data Menggunakan Wireshark dan CMD)



Nama : Rahmi Khoirani

NIM : 09011281520104

Kelas : SK 5C

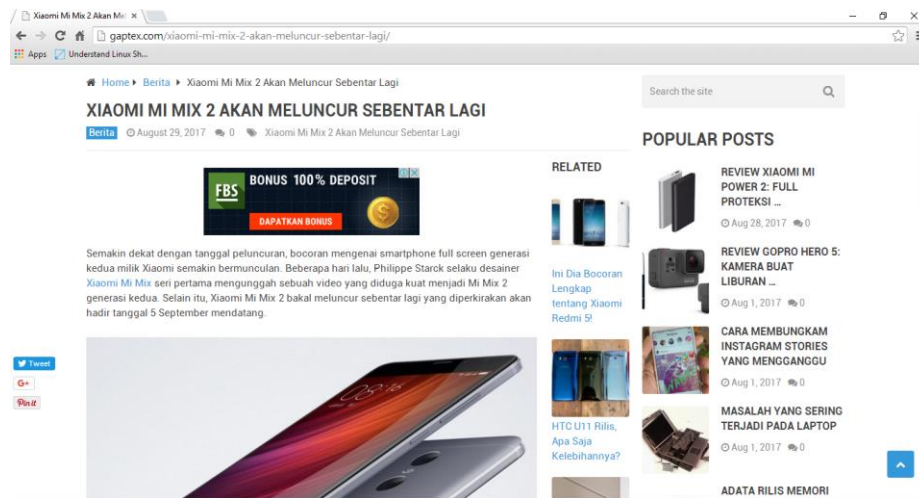
Dosen Pengampuh : Deris Stiawan, M.T., Ph.D.

Jurusan Sistem Komputer
Fakultas Ilmu Komputer
Universitas Sriwijaya

2017

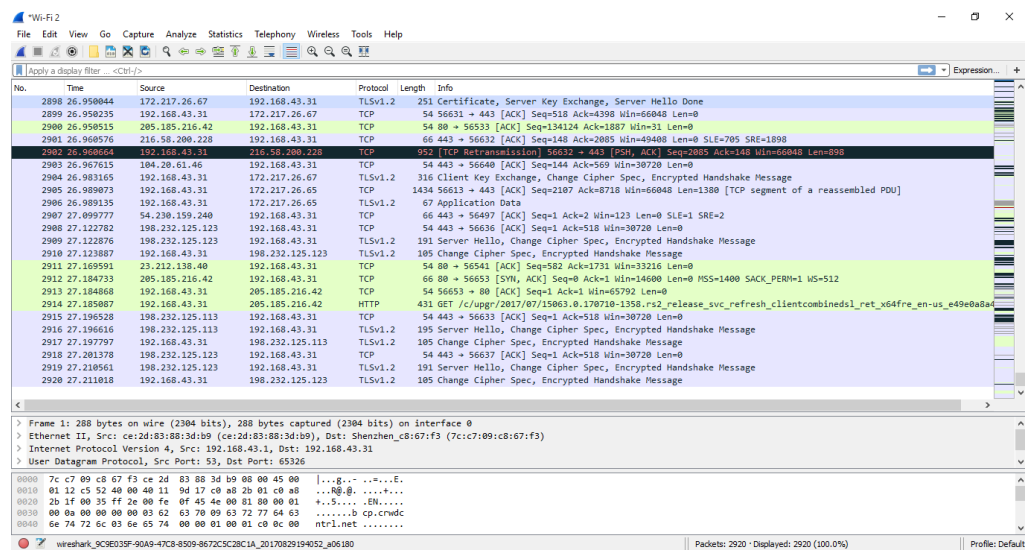
A. Web Browsing

Web Browsing yang saya buka adalah www.gaptex.com selama satu menit.



1. Wireshark

Berikut ini merupakan sebagian dari hasil capturing data web browsing pada wireshark yang dilakukan selama satu menit.



Tabel Source

IP	MAC	INFO
172.217.26.70	ce:2d:83:88:3d:b9	192.168.43.31 TLSv1.2 1253 Application Data
172.217.26.67	ce:2d:83:88:3d:b9	TLSv1.2 251 Certificate, Server Key Exchange, Server Hello Done
192.168.43.31	7c:c7:09:c8:67:f3	TCP 952 [TCP Retransmission] 56632 → 443 [PSH, ACK] Seq=2085 Ack=148 Win=66048 Len=898
205.185.216.42	ce:2d:83:88:3d:b9	TCP 66 80 → 56653 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1

		WS=512
216.58.200.228	ce:2d:83:88:3d:b9	TCP 66 443 → 56632 [ACK] Seq=148 Ack=2085 Win=49408 Len=0 SLE=705 SRE=1898
104.20.61.46	ce:2d:83:88:3d:b9	TCP 54 443 → 56640 [ACK] Seq=144 Ack=569 Win=30720 Len=0
54.230.159.240	ce:2d:83:88:3d:b9	TCP 66 443 → 56497 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
198.232.125.123	ce:2d:83:88:3d:b9	TLSv1.2 191 Server Hello, Change Cipher Spec, Encrypted Handshake Message
23.212.138.40	ce:2d:83:88:3d:b9	TCP 54 80 → 56541 [ACK] Seq=582 Ack=1731 Win=33216 Len=0
198.232.125.113	ce:2d:83:88:3d:b9	TLSv1.2 195 Server Hello, Change Cipher Spec, Encrypted Handshake Message

Tabel Destination

IP	MAC	INFO
192.168.43.31	7c:c7:09:c8:67:f3	TLSv1.2 1253 Application Data
192.168.43.31	7c:c7:09:c8:67:f3	TLSv1.2 251 Certificate, Server Key Exchange, Server Hello Done
216.58.200.228	ce:2d:83:88:3d:b9	TCP 952 [TCP Retransmission] 56632 → 443 [PSH, ACK] Seq=2085 Ack=148 Win=66048 Len=898
192.168.43.31	7c:c7:09:c8:67:f3	TCP 66 80 → 56653 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1 WS=512
192.168.43.31	7c:c7:09:c8:67:f3	TCP 66 443 → 56632 [ACK] Seq=148 Ack=2085 Win=49408 Len=0 SLE=705 SRE=1898
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 56640 [ACK] Seq=144 Ack=569 Win=30720 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TCP 66 443 → 56497 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
192.168.43.31	7c:c7:09:c8:67:f3	TLSv1.2 191 Server Hello, Change Cipher Spec, Encrypted Handshake Message
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 80 → 56541 [ACK] Seq=582 Ack=1731 Win=33216 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TLSv1.2 195 Server Hello, Change Cipher Spec, Encrypted Handshake Message

2. CMD

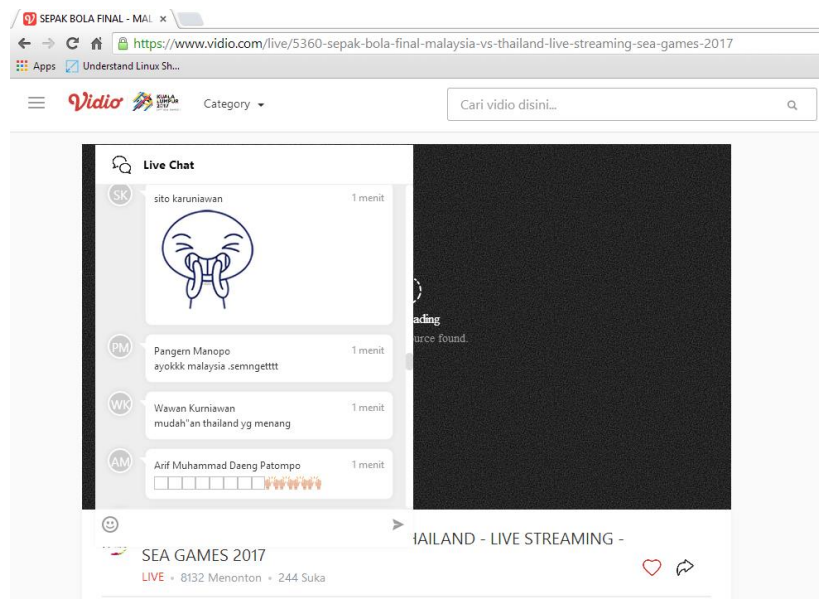
Berikut ini merupakan hasil dari capturing data web browsing pada CMD yang dilakukan selama satu menit.

```
Command Prompt

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 WIN10:0 LISTENING
TCP 0.0.0.0:445 WIN10:0 LISTENING
TCP 0.0.0.0:5357 WIN10:0 LISTENING
TCP 0.0.0.0:7680 WIN10:0 LISTENING
TCP 0.0.0.0:49408 WIN10:0 LISTENING
TCP 0.0.0.0:49409 WIN10:0 LISTENING
TCP 0.0.0.0:49410 WIN10:0 LISTENING
TCP 0.0.0.0:49411 WIN10:0 LISTENING
TCP 0.0.0.0:49412 WIN10:0 LISTENING
TCP 0.0.0.0:49414 WIN10:0 LISTENING
TCP 127.0.0.1:1001 WIN10:0 LISTENING
TCP 127.0.0.1:53860 WIN10:0 LISTENING
TCP 127.0.0.1:53860 WIN10:56684 ESTABLISHED
TCP 127.0.0.1:56368 WIN10:53860 TIME_WAIT
TCP 127.0.0.1:56684 WIN10:53860 ESTABLISHED
TCP 192.168.43.31:139 WIN10:0 LISTENING
TCP 192.168.43.31:56419 hk2sch130021432:https ESTABLISHED
TCP 192.168.43.31:56476 sin10s02-in-f78:https TIME_WAIT
TCP 192.168.43.31:56478 sc-in-f154:https TIME_WAIT
TCP 192.168.43.31:56479 104.20.61.46:https TIME_WAIT
TCP 192.168.43.31:56480 104.20.61.46:https TIME_WAIT
TCP 192.168.43.31:56490 sin10s02-in-f78:https TIME_WAIT
TCP 192.168.43.31:56492 sin10s02-in-f78:https TIME_WAIT
TCP 192.168.43.31:56497 server-54-230-159-240:https TIME_WAIT
TCP 192.168.43.31:56508 sin10s02-in-f78:https TIME_WAIT
TCP 192.168.43.31:56514 sin10s02-in-f78:https TIME_WAIT
TCP 192.168.43.31:56515 sin10s02-in-f78:https TIME_WAIT
```

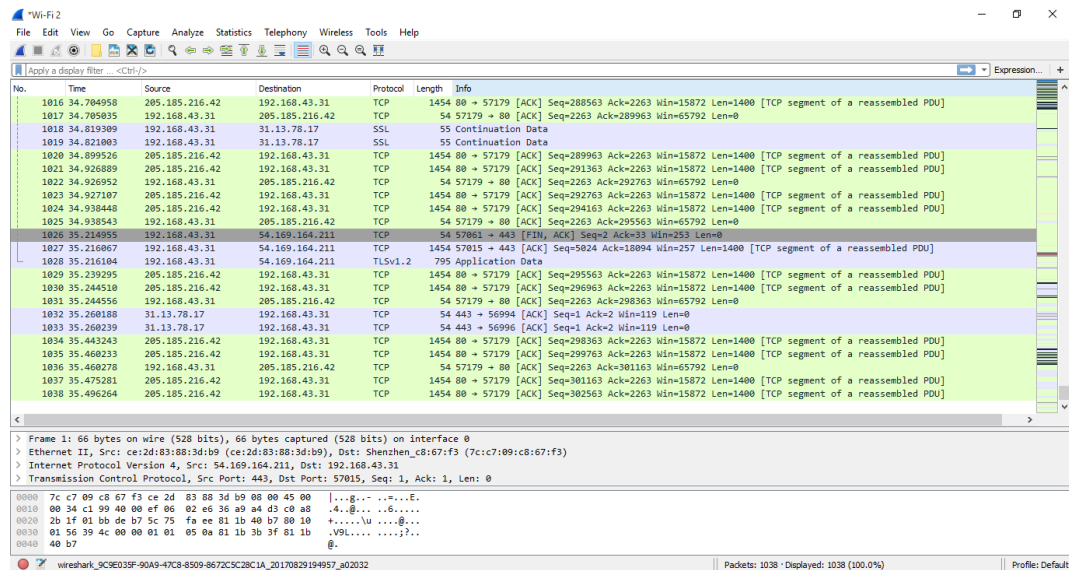
B. Online Streaming

Online Streaming yang saya buka adalah www.vidio.com selama satu menit.



1. Wireshark

Berikut ini merupakan sebagian dari hasil capturing data online streaming pada wireshark yang dilakukan selama satu menit.



Tabel Source

IP	MAC	INFO
205.185.216.42	ce:2d:83:88:3d:b9	TCP 1454 80 → 57179 [ACK] Seq=226925 Ack=1509 Win=15872 Len=1400 [TCP segment of a reassembled PDU]
192.168.43.31	7c:c7:09:c8:67:f3	TCP 66 [TCP Dup ACK 871#1] 57179 → 80 [ACK] Seq=1509 Ack=229725 Win=111872 Len=0 SLE=232525 SRE=233786
54.230.156.222	ce:2d:83:88:3d:b9	TCP 54 443 → 57035 [ACK] Seq=33 Ack=2 Win=127 Len=0
54.169.164.211	ce:2d:83:88:3d:b9	TCP 54 443 → 57124 [ACK] Seq=33 Ack=3 Win=175 Len=0
172.217.26.67	ce:2d:83:88:3d:b9	TCP 66 443 → 57011 [ACK] Seq=1 Ack=2 Win=176 Len=0 SLE=1 SRE=2
66.117.25.55	ce:2d:83:88:3d:b9	TCP 54 443 → 57157 [ACK] Seq=55 Ack=2 Win=40958 Len=0
172.217.26.80	ce:2d:83:88:3d:b9	TCP 54 443 → 56895 [FIN, ACK] Seq=1 Ack=2 Win=180 Len=0
216.58.200.227	ce:2d:83:88:3d:b9	TCP 66 443 → 56867 [ACK] Seq=1 Ack=2 Win=288 Len=0 SLE=1 SRE=2
157.240.13.35	ce:2d:83:88:3d:b9	TCP 54 443 → 57049 [ACK] Seq=1 Ack=2 Win=220 Len=0
31.13.78.17	ce:2d:83:88:3d:b9	TCP 54 443 → 56994 [ACK] Seq=1 Ack=2 Win=119 Len=0

Tabel Destination

IP	MAC	INFO
192.168.43.31	7c:c7:09:c8:67:f3	TCP 1454 80 → 57179 [ACK] Seq=226925 Ack=1509 Win=15872 Len=1400 [TCP segment of a reassembled PDU]
205.185.216.42	ce:2d:83:88:3d:b9	TCP 66 [TCP Dup ACK 871#1] 57179 → 80 [ACK] Seq=1509 Ack=229725 Win=111872 Len=0 SLE=232525 SRE=233786
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 57035 [ACK] Seq=33 Ack=2 Win=127 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 57124 [ACK] Seq=33 Ack=3 Win=175 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TCP 66 443 → 57011 [ACK] Seq=1 Ack=2 Win=176 Len=0 SLE=1 SRE=2
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 57157 [ACK] Seq=55 Ack=2 Win=40958 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 56895 [FIN, ACK] Seq=1 Ack=2 Win=180 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TCP 66 443 → 56867 [ACK] Seq=1 Ack=2 Win=288 Len=0 SLE=1 SRE=2
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 57049 [ACK] Seq=1 Ack=2 Win=220 Len=0
192.168.43.31	7c:c7:09:c8:67:f3	TCP 54 443 → 56994 [ACK] Seq=1 Ack=2 Win=119 Len=0

2. CMD

Berikut ini merupakan hasil dari capturing data online streaming pada CMD yang dilakukan selama satu menit.

```

C:\Users\Asus>netstat -a
Active Connections
Proto Local Address           Foreign Address         State
TCP 0.0.0.0:135             WIN10:0                LISTENING
TCP 0.0.0.0:445            WIN10:0                LISTENING
TCP 0.0.0.0:5357          WIN10:0                LISTENING
TCP 0.0.0.0:7680          WIN10:0                LISTENING
TCP 0.0.0.0:49408        WIN10:0                LISTENING
TCP 0.0.0.0:49409        WIN10:0                LISTENING
TCP 0.0.0.0:49410        WIN10:0                LISTENING
TCP 0.0.0.0:49411        WIN10:0                LISTENING
TCP 0.0.0.0:49412        WIN10:0                LISTENING
TCP 0.0.0.0:49414        WIN10:0                LISTENING
TCP 127.0.0.1:10801       WIN10:0                LISTENING
TCP 127.0.0.1:53860       WIN10:0                LISTENING
TCP 127.0.0.1:53860       WIN10:56859            ESTABLISHED
TCP 127.0.0.1:56859       WIN10:53860            ESTABLISHED
TCP 192.168.43.31:139     WIN10:0                LISTENING
TCP 192.168.43.31:56419   hk2sch130021432:https  ESTABLISHED
TCP 192.168.43.31:56676   hk2sch130021236:https  ESTABLISHED
TCP 192.168.43.31:56858   tsa03s01-in-f3:https  ESTABLISHED
TCP 192.168.43.31:56863   sa-in-f100:https      ESTABLISHED
TCP 192.168.43.31:56866   tsa03s01-in-f3:https  ESTABLISHED
TCP 192.168.43.31:56867   tsa03s01-in-f3:https  ESTABLISHED
TCP 192.168.43.31:56868   tsa03s01-in-f3:https  ESTABLISHED
TCP 192.168.43.31:56883   sin10s07-in-f14:https ESTABLISHED
TCP 192.168.43.31:56891   a23-0-180-247:https   ESTABLISHED
TCP 192.168.43.31:56892   a23-212-107-24:https  ESTABLISHED
TCP 192.168.43.31:56894   sin10s02-in-f8:https  ESTABLISHED
TCP 192.168.43.31:56901   a23-212-139-249:https ESTABLISHED
TCP 192.168.43.31:56917   sin10s07-in-f19:https ESTABLISHED
^C
C:\Users\Asus>

```