TUGAS II
JARINGAN KOMPUTER

Nama : Rofby Hidayadi

NIM : 09011281520132

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

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

I. JUDUL TUGAS

Capturing Data Browsing dan Online Streaming menggunakan Wireshark dan Command Prompt.

II. PROSEDUR

Adapun prosedur dalam melakukan capturing data kali ini adalah sebagai berikut:

1. Install aplikasi Wireshark.
2. Capturing data :
   a. Web browsing.
   b. Online streaming (selain youtube).
3. Capturing data menggunakan aplikasi Wireshark.
4. Capturing data menggunakan Command Prompt (*netsat -a*) lalu gunakan Ctrl + C untuk perintah break.
5. Analisa IP dan MAC address source dan destination.
6. Filter berdasarkan IP address kita.
7. Buatlah tabel yang berisikan IP dan Info dari paket data yang di capture setelah di filter.

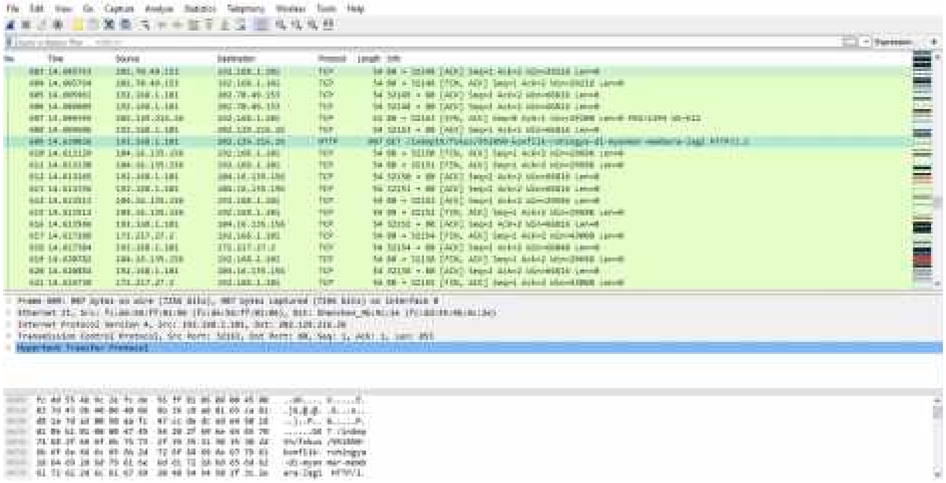
III. DASAR TEORI

Wireshark merupakan salah satu program untuk menganalisis suatu jaringan, baik jaringan kabel ataupun nirkabel. Wireshark sering digunakan untuk troubleshooting, memeriksa keamanan jaringan dan lain-lain. Wireshark akan menangkap paket data pada jaringan yang kemudian, data yang ditangkap tersebut ditampilkan sedetail mungkin. Sedangkan Command Prompt atau CMD merupakan command line interpreter pada sebuah Operating System yang digunakan untuk mengeksekusi suatu hal tertentu dengan cara menuliskan perintahnya pada Command Prompt.

IV. ANALISA PAKET DATA : WEB BROWSING MENGGUNAKAN WIRESHARK DAN CMD

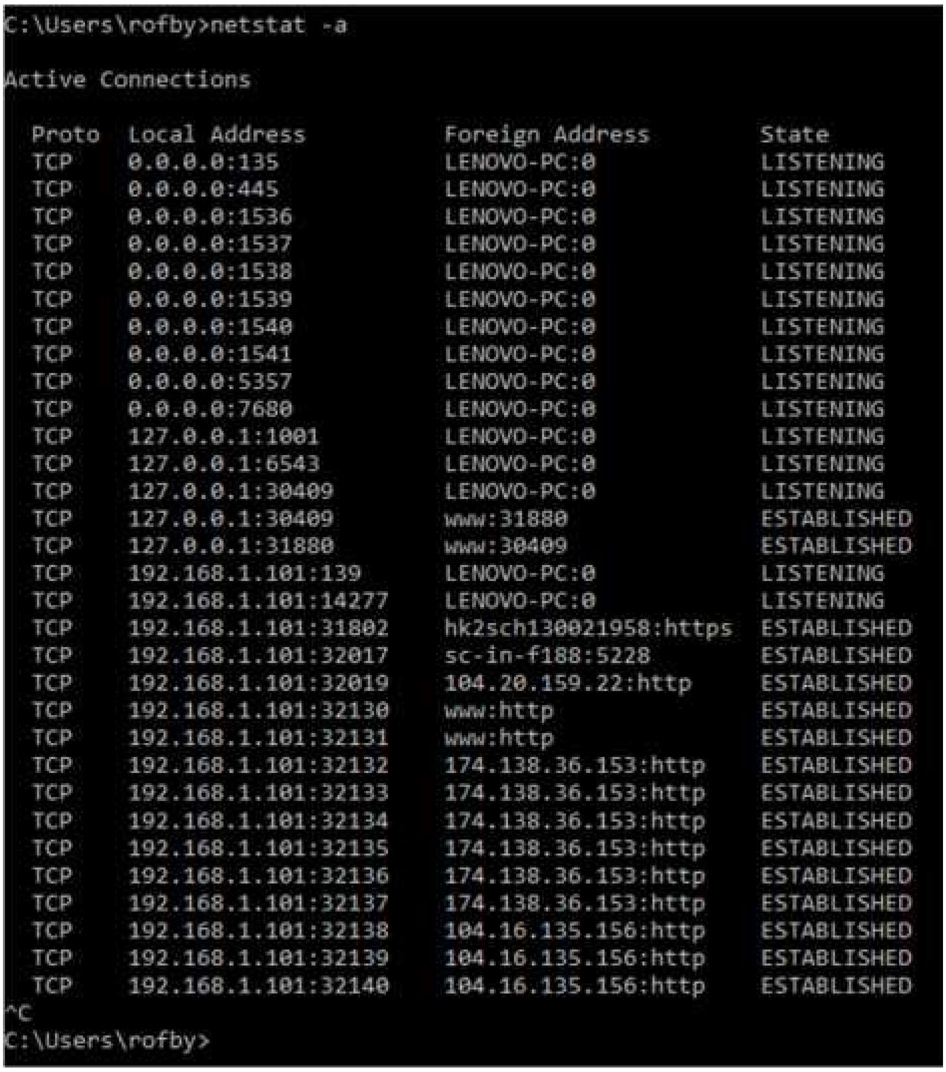
Adapun website yang akan dibrowsing yang kemudian paket datanya di analisa adalah www.viva.co.id yang merupakan salah satu situs berita online Indonesia.

Berikut adalah hasil capturing data ke www.viva.co.id menggunakan Wireshark:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info

Gambar 1. Hasil capturing data ke www.viva.co.id menggunakan Wireshark

Dan berikut adalah hasil capturing data ke www.viva.co.id menggunakan CMD (netstat -a):



```
C:\Users\rofby>netstat -a

Active Connections

  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    0.0.0.0:1536           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1537           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1538           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1539           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1540           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1541           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:5357           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:7680           LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:1001         LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:6543         LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:30409        LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:30409        www:31880              ESTABLISHED
  TCP    127.0.0.1:31880        www:30409              ESTABLISHED
  TCP    192.168.1.101:139      LENOVO-PC:0            LISTENING
  TCP    192.168.1.101:14277    LENOVO-PC:0            LISTENING
  TCP    192.168.1.101:31802    hk2sch130021958:https  ESTABLISHED
  TCP    192.168.1.101:32017    sc-in-f188:5228        ESTABLISHED
  TCP    192.168.1.101:32019    104.20.159.22:http     ESTABLISHED
  TCP    192.168.1.101:32130    www:http               ESTABLISHED
  TCP    192.168.1.101:32131    www:http               ESTABLISHED
  TCP    192.168.1.101:32132    174.138.36.153:http    ESTABLISHED
  TCP    192.168.1.101:32133    174.138.36.153:http    ESTABLISHED
  TCP    192.168.1.101:32134    174.138.36.153:http    ESTABLISHED
  TCP    192.168.1.101:32135    174.138.36.153:http    ESTABLISHED
  TCP    192.168.1.101:32136    174.138.36.153:http    ESTABLISHED
  TCP    192.168.1.101:32137    174.138.36.153:http    ESTABLISHED
  TCP    192.168.1.101:32138    104.16.135.156:http    ESTABLISHED
  TCP    192.168.1.101:32139    104.16.135.156:http    ESTABLISHED
  TCP    192.168.1.101:32140    104.16.135.156:http    ESTABLISHED
^C
C:\Users\rofby>
```

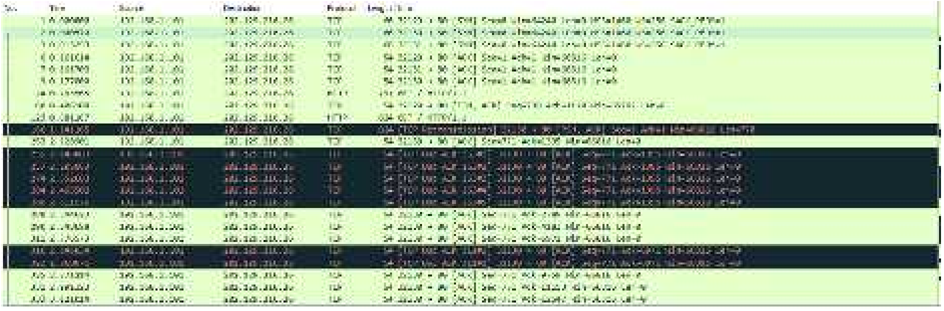
Gambar 2. Hasil capturing data ke www.viva.co.id menggunakan CMD

Setelah dilakukan capturing data proses ke www.viva.co.id kita dapat mengetahui IP dan MAC Address milik perangkat kita dan IP dan MAC address milik perangkat website yang menjadi tujuan kita.

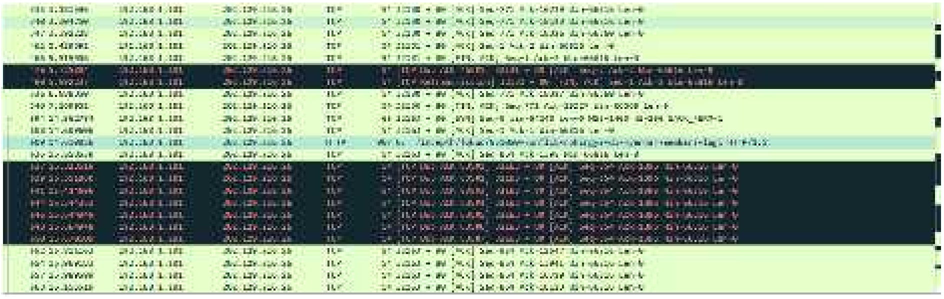
Tabel 1. IP dan MAC Address

Source		Destination	
IP	**MAC**	**IP**	**MAC**
192.168.1.101	FC:DE:56:FF:01:06	202.129.216.26	FC:DD:55:4B:9C:2E

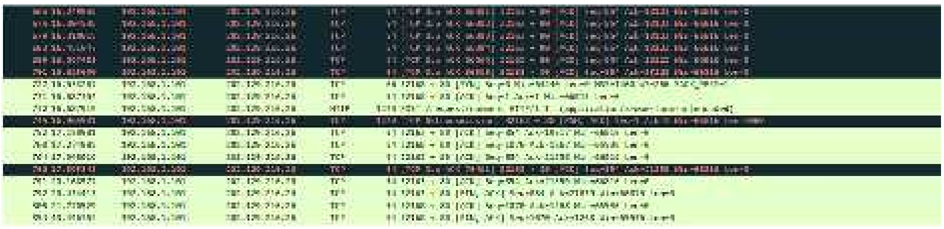
Kemudian, hasil capturing data yang telah diperoleh, kita filter berdasarkan IP dan MAC address pada tabel 1. Didapatlah hasilnya sebagai berikut:



Gambar 3.1. Hasil capturing data setelah di filter



Gambar 3.2. Hasil capturing data setelah di filter



Gambar 3.3. Hasil capturing data setelah di filter

Dari ketiga gambar tersebut dapat kita ketahui bahwa paket data berdasarkan IP dan MAC address source dan destination adalah sebanyak 66 paket data dari 932 paket data secara keseluruhan.

Tabel 2. Info paket data setelah di filter

IP Source	IP Destination	Info
192.168.1.101	202.129.216.26	32129 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	202.129.216.26	32130 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	202.129.216.26	32131 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	202.129.216.26	32129 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	202.129.216.26	32131 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	202.129.216.26	GET / HTTP/1.1
192.168.1.101	202.129.216.26	32129 → 80 [FIN, ACK] Seq=738 Ack=1120 Win=65792 Len=0
192.168.1.101	202.129.216.26	GET / HTTP/1.1
192.168.1.101	202.129.216.26	[TCP Retransmission] 32130 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66816 Len=770
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 253#1] 32130 → 80 [ACK] Seq=771 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 253#2] 32130 → 80 [ACK] Seq=771 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 253#3] 32130 → 80 [ACK] Seq=771 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 253#4] 32130 → 80 [ACK] Seq=771 Ack=1395 Win=66816 Len=0

192.168.1.101	202.129.216.26	[TCP Dup ACK 253#5] 32130 → 80 [ACK] Seq=771 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=2789 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=4183 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=6971 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 311#1] 32130 → 80 [ACK] Seq=771 Ack=6971 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 311#2] 32130 → 80 [ACK] Seq=771 Ack=6971 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=9759 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=11153 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=12547 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=16729 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=18326 Win=66816 Len=0
192.168.1.101	202.129.216.26	32131 → 80 [ACK] Seq=1 Ack=2 Win=66816 Len=0
192.168.1.101	202.129.216.26	32131 → 80 [FIN, ACK] Seq=1 Ack=2 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 462#1] 32131 → 80 [ACK] Seq=2 Ack=2 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Retransmission] 32131 → 80 [FIN, ACK] Seq=1 Ack=2 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 → 80 [ACK] Seq=771 Ack=18327 Win=66560 Len=0

192.168.1.101	202.129.216.26	32130 → 80 [FIN, ACK] Seq=771 Ack=18327 Win=66560 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	202.129.216.26	GET /indepth/fokus/951050-konflik-rohingya-di-myanmar-membara-lagi HTTP/1.1
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#1] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#2] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#3] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#4] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#5] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#6] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 635#7] 32163 → 80 [ACK] Seq=854 Ack=1395 Win=66816 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=12547 Win=66816 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=13941 Win=66816 Len=0

192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=16729 Win=66816 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 663#1] 32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 663#2] 32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 663#3] 32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 663#4] 32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 663#5] 32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 663#6] 32163 → 80 [ACK] Seq=854 Ack=18123 Win=66816 Len=0
192.168.1.101	202.129.216.26	32168 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	202.129.216.26	32168 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	202.129.216.26	POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded)
192.168.1.101	202.129.216.26	[TCP Retransmission] 32168 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66816 Len=1069
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=19517 Win=66816 Len=0
192.168.1.101	202.129.216.26	32168 → 80 [ACK] Seq=1070 Ack=1267 Win=65536 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=21858 Win=66816 Len=0

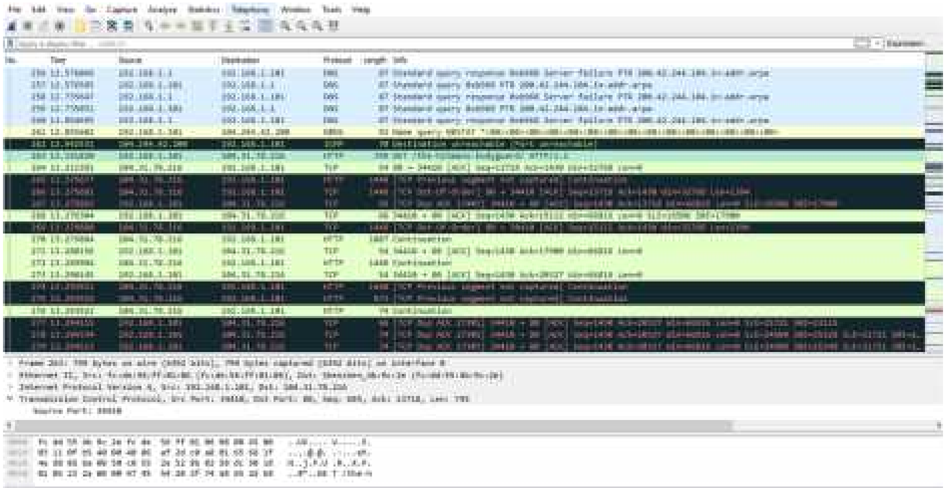
192.168.1.101	202.129.216.26	[TCP Dup ACK 764#1] 32163 → 80 [ACK] Seq=854 Ack=21858 Win=66816 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [ACK] Seq=854 Ack=21859 Win=66816 Len=0
192.168.1.101	202.129.216.26	32163 → 80 [FIN, ACK] Seq=854 Ack=21859 Win=66816 Len=0
192.168.1.101	202.129.216.26	32168 → 80 [ACK] Seq=1070 Ack=1268 Win=65536 Len=0
192.168.1.101	202.129.216.26	32168 → 80 [FIN, ACK] Seq=1070 Ack=1268 Win=65536 Len=0

Dari tabel tersebut dapat kita ketahui bahwa, tabel yang berwarna hitam merupakan paket data yang bermasalah. Sedangkaan tabel yang berwarna hijau merupakan paket data dengan protokol HTTP, dan tabel yang putih merupakan paket data dengan protokol TCP.

V. ANALISA PAKET DATA : ONLINE STREAMING MENGGUNAKAN WIRESHARK DAN CMD

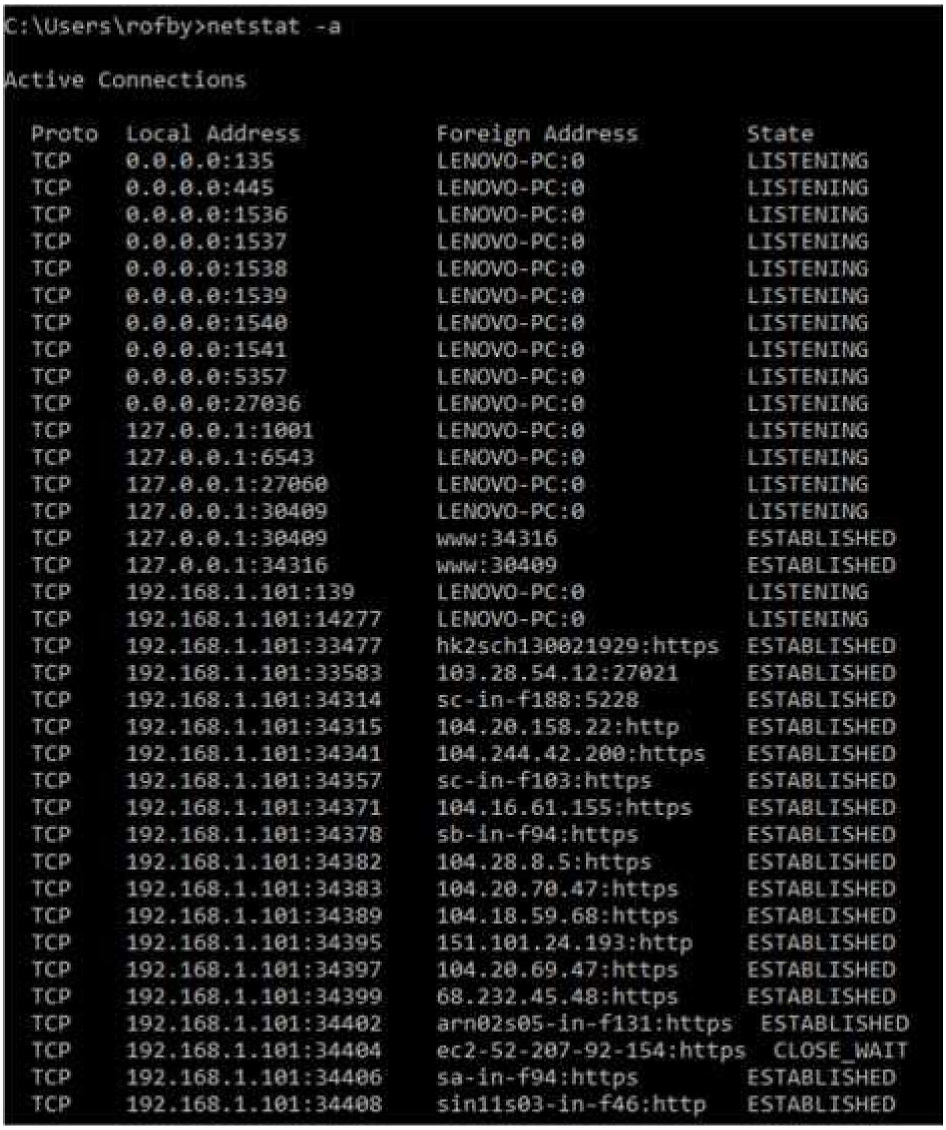
Adapun website online streaming yang akan dibrowsing yang kemudian paket datanya di analisa adalah www.indomovie.tv yang merupakan salah satu situs online streaming Indonesia.

Berikut adalah hasil capturing data ke www.indomovie.tv menggunakan Wireshark:



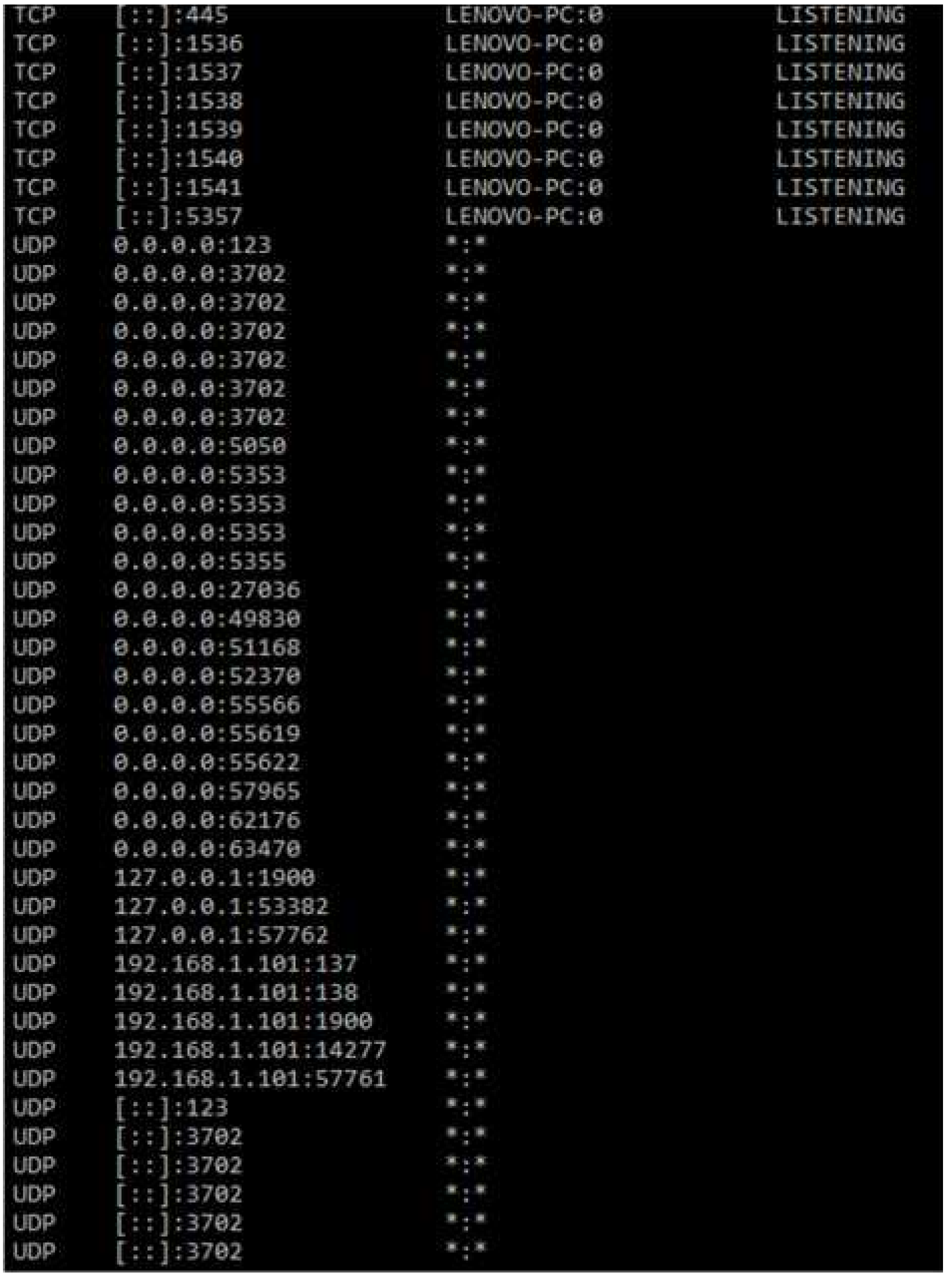
Gambar 4. Hasil capturing data ke www.indomovie.tv menggunakan Wireshark

Dan berikut adalah hasil capturing data ke www.indomovie.tv menggunakan CMD (netstat -a):



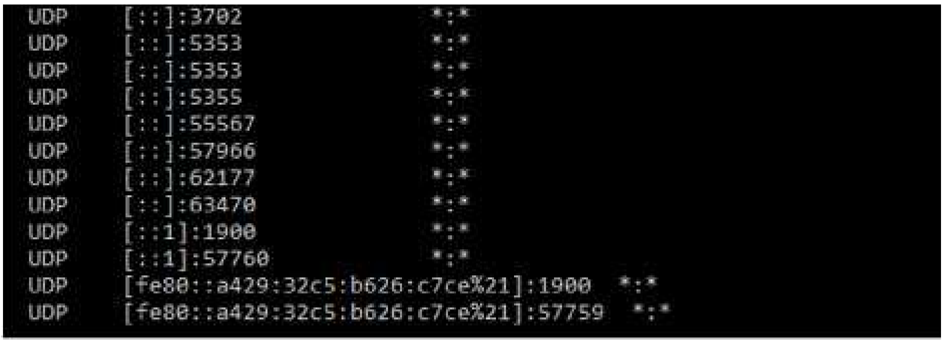
```
C:\Users\rofby>netstat -a

Active Connections

  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    0.0.0.0:1536           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1537           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1538           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1539           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1540           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:1541           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:5357           LENOVO-PC:0            LISTENING
  TCP    0.0.0.0:27036          LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:1001         LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:6543         LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:27060        LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:30409        LENOVO-PC:0            LISTENING
  TCP    127.0.0.1:30409        www:34316              ESTABLISHED
  TCP    127.0.0.1:34316        www:30409              ESTABLISHED
  TCP    192.168.1.101:139      LENOVO-PC:0            LISTENING
  TCP    192.168.1.101:14277    LENOVO-PC:0            LISTENING
  TCP    192.168.1.101:33477    hk2sch130021929:https  ESTABLISHED
  TCP    192.168.1.101:33583    103.28.54.12:27021     ESTABLISHED
  TCP    192.168.1.101:34314    sc-in-f188:5228        ESTABLISHED
  TCP    192.168.1.101:34315    104.20.158.22:http     ESTABLISHED
  TCP    192.168.1.101:34341    104.244.42.200:https   ESTABLISHED
  TCP    192.168.1.101:34357    sc-in-f103:https       ESTABLISHED
  TCP    192.168.1.101:34371    104.16.61.155:https    ESTABLISHED
  TCP    192.168.1.101:34378    sb-in-f94:https        ESTABLISHED
  TCP    192.168.1.101:34382    104.28.8.5:https       ESTABLISHED
  TCP    192.168.1.101:34383    104.20.70.47:https     ESTABLISHED
  TCP    192.168.1.101:34389    104.18.59.68:https     ESTABLISHED
  TCP    192.168.1.101:34395    151.101.24.193:http    ESTABLISHED
  TCP    192.168.1.101:34397    104.20.69.47:https     ESTABLISHED
  TCP    192.168.1.101:34399    68.232.45.48:https     ESTABLISHED
  TCP    192.168.1.101:34402    arn02s05-in-f131:https  ESTABLISHED
  TCP    192.168.1.101:34404    ec2-52-207-92-154:https  CLOSE_WAIT
  TCP    192.168.1.101:34406    sa-in-f94:https        ESTABLISHED
  TCP    192.168.1.101:34408    sin11s03-in-f46:http   ESTABLISHED
```

Gambar 5.1. Hasil capturing data ke www.indomovie.tv
menggunakan CMD



```
TCP    [::]:445              LENOVO-PC:0            LISTENING
TCP    [::]:1536             LENOVO-PC:0            LISTENING
TCP    [::]:1537             LENOVO-PC:0            LISTENING
TCP    [::]:1538             LENOVO-PC:0            LISTENING
TCP    [::]:1539             LENOVO-PC:0            LISTENING
TCP    [::]:1540             LENOVO-PC:0            LISTENING
TCP    [::]:1541             LENOVO-PC:0            LISTENING
TCP    [::]:5357             LENOVO-PC:0            LISTENING
UDP    0.0.0.0:123           *:*
UDP    0.0.0.0:3702          *:*
UDP    0.0.0.0:3702          *:*
UDP    0.0.0.0:3702          *:*
UDP    0.0.0.0:3702          *:*
UDP    0.0.0.0:3702          *:*
UDP    0.0.0.0:3702          *:*
UDP    0.0.0.0:5050          *:*
UDP    0.0.0.0:5353          *:*
UDP    0.0.0.0:5353          *:*
UDP    0.0.0.0:5353          *:*
UDP    0.0.0.0:5355          *:*
UDP    0.0.0.0:27036         *:*
UDP    0.0.0.0:49830         *:*
UDP    0.0.0.0:51168         *:*
UDP    0.0.0.0:52370         *:*
UDP    0.0.0.0:55566         *:*
UDP    0.0.0.0:55619         *:*
UDP    0.0.0.0:55622         *:*
UDP    0.0.0.0:57965         *:*
UDP    0.0.0.0:62176         *:*
UDP    0.0.0.0:63470         *:*
UDP    127.0.0.1:1900        *:*
UDP    127.0.0.1:53382       *:*
UDP    127.0.0.1:57762       *:*
UDP    192.168.1.101:137     *:*
UDP    192.168.1.101:138     *:*
UDP    192.168.1.101:1900    *:*
UDP    192.168.1.101:14277   *:*
UDP    192.168.1.101:57761   *:*
UDP    [::]:123              *:*
UDP    [::]:3702             *:*
UDP    [::]:3702             *:*
UDP    [::]:3702             *:*
UDP    [::]:3702             *:*
UDP    [::]:3702             *:*
```

Gambar 5.2. Hasil capturing data ke www.indomovie.tv menggunakan CMD



```
UDP    [::]:3702                *:*
UDP    [::]:5353                *:*
UDP    [::]:5353                *:*
UDP    [::]:5355                *:*
UDP    [::]:55567               *:*
UDP    [::]:57966               *:*
UDP    [::]:62177               *:*
UDP    [::]:63470               *:*
UDP    [::1]:1900               *:*
UDP    [::1]:57760              *:*
UDP    [fe80::a429:32c5:b626:c7ce%21]:1900   *:*
UDP    [fe80::a429:32c5:b626:c7ce%21]:57759   *:*
```

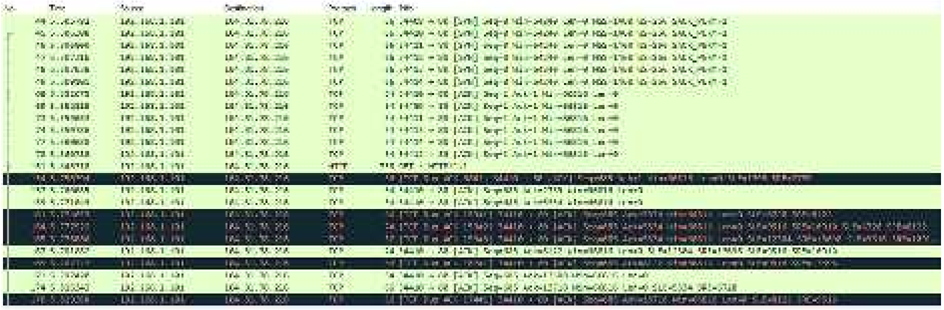
Gambar 5.3. Hasil capturing data ke www.indomovie.tv menggunakan CMD

Setelah dilakukan capturing data proses ke www.indomovie.tv kita dapat mengetahui IP dan MAC Address milik perangkat kita dan IP dan MAC address milik perangkat website online streaaming yang menjadi tujuan kita.

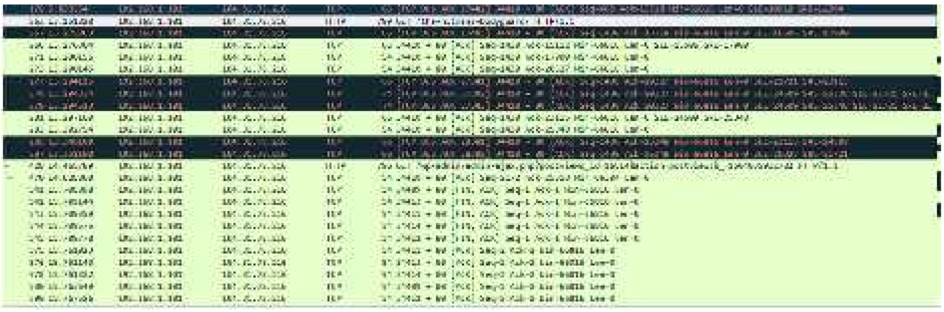
Tabel 3. IP dan MAC Address

Source		Destination	
IP	**MAC**	**IP**	**MAC**
192.168.1.101	FC:DE:56:FF:01:06	104.31.78.216	FC:DD:55:4B:9C:2E

Kemudian, hasil capturing data yang telah diperoleh, kita filter berdasarkan IP dan MAC address pada tabel 3. Didapatlah hasilnya sebagai berikut:



Gambar 6.1. Hasil capturing data setelah di filter



Gambar 6.2. Hasil capturing data setelah di filter

Dari ketiga gambar tersebut dapat kita ketahui bahwa paket data berdasarkan IP dan MAC address source dan destination adalah sebanyak 49 paket data dari 4.888 paket data secara keseluruhan.

Tabel 4. Info paket data setelah di filter

IP Source	IP Destination	Info
192.168.1.101	104.31.78.216	34409 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	104.31.78.216	34410 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	104.31.78.216	34411 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	104.31.78.216	34412 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	104.31.78.216	34413 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	104.31.78.216	34414 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34409 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0

192.168.1.101	104.31.78.216	34411 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34413 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34414 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34412 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	GET / HTTP/1.1
192.168.1.101	104.31.78.216	[TCP Dup ACK 68#1] 34410 → 80 [ACK] Seq=685 Ack=1 Win=66816 Len=0 SLE=1395 SRE=2789
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=685 Ack=2789 Win=66816 Len=0
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0
192.168.1.101	104.31.78.216	[TCP Dup ACK 159#1] 34410 → 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0 SLE=6728 SRE=8122
192.168.1.101	104.31.78.216	[TCP Dup ACK 159#2] 34410 → 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0 SLE=9516 SRE=10910 SLE=6728 SRE=8122
192.168.1.101	104.31.78.216	[TCP Dup ACK 159#3] 34410 → 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0 SLE=12304 SRE=13698 SLE=9516 SRE=10910 SLE=6728 SRE=8122
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=685 Ack=8122 Win=66816 Len=0 SLE=12304 SRE=13698 SLE=9516 SRE=10910
192.168.1.101	104.31.78.216	[TCP Dup ACK 167#1] 34410 → 80 [ACK] Seq=685 Ack=8122 Win=66816 Len=0 SLE=9516 SRE=13698
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=685 Ack=13698 Win=66816 Len=0
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=685 Ack=13718 Win=66816 Len=0 SLE=5334 SRE=6728

192.168.1.101	104.31.78.216	[TCP Dup ACK 174#1] 34410 → 80 [ACK] Seq=685 Ack=13718 Win=66816 Len=0 SLE=8122 SRE=9516
192.168.1.101	104.31.78.216	[TCP Dup ACK 174#2] 34410 → 80 [ACK] Seq=685 Ack=13718 Win=66816 Len=0 SLE=10910 SRE=12304
192.168.1.101	104.31.78.216	GET /the-hitmans-bodyguard/ HTTP/1.1
192.168.1.101	104.31.78.216	[TCP Dup ACK 174#3] 34410 → 80 [ACK] Seq=1430 Ack=13718 Win=66816 Len=0 SLE=16506 SRE=17900
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=1430 Ack=15112 Win=66816 Len=0 SLE=16506 SRE=17900
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=1430 Ack=17900 Win=66816 Len=0
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0
192.168.1.101	104.31.78.216	[TCP Dup ACK 273#1] 34410 → 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115
192.168.1.101	104.31.78.216	[TCP Dup ACK 273#2] 34410 → 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115
192.168.1.101	104.31.78.216	[TCP Dup ACK 273#3] 34410 → 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SLE=24509 SRE=25348
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0
192.168.1.101	104.31.78.216	[TCP Dup ACK 283#1] 34410 → 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0 SLE=23115 SRE=24509

192.168.1.101	104.31.78.216	[TCP Dup ACK 283#2] 34410 → 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0 SLE=20327 SRE=21721
192.168.1.101	104.31.78.216	GET /wp-admin/admin-ajax.php?postviews_id=16814&action=postviews&_=1504035932782 HTTP/1.1
192.168.1.101	104.31.78.216	34410 → 80 [ACK] Seq=2172 Ack=25818 Win=66304 Len=0
192.168.1.101	104.31.78.216	34409 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34413 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34411 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34414 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34412 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34411 → 80 [ACK] Seq=2 Ack=2 Win=66816 Len=0
192.168.1.101	104.31.78.216	34413 → 80 [ACK] Seq=2 Ack=2 Win=66816 Len=0
192.168.1.101	104.31.78.216	34414 → 80 [ACK] Seq=2 Ack=2 Win=66816 Len=0
192.168.1.101	104.31.78.216	34409 → 80 [ACK] Seq=2 Ack=2 Win=66816 Len=0
192.168.1.101	104.31.78.216	34412 → 80 [ACK] Seq=2 Ack=2 Win=66816 Len=0

Dari tabel tersebut dapat kita ketahui bahwa, tabel yang berwarna hitam merupakan paket data yang bermasalah. Sedangkaan tabel yang berwarna hijau merupakan paket data dengan protokol HTTP, dan tabel yang putih merupakan paket data dengan protokol TCP.