JARINGAN KOMPUTER

"CAPTURING DATA"

Nama : Siti Pebsya Roisatun Sholihah

NIM : 09011281520102

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

JURUSAN SISTEM KOMPUTER

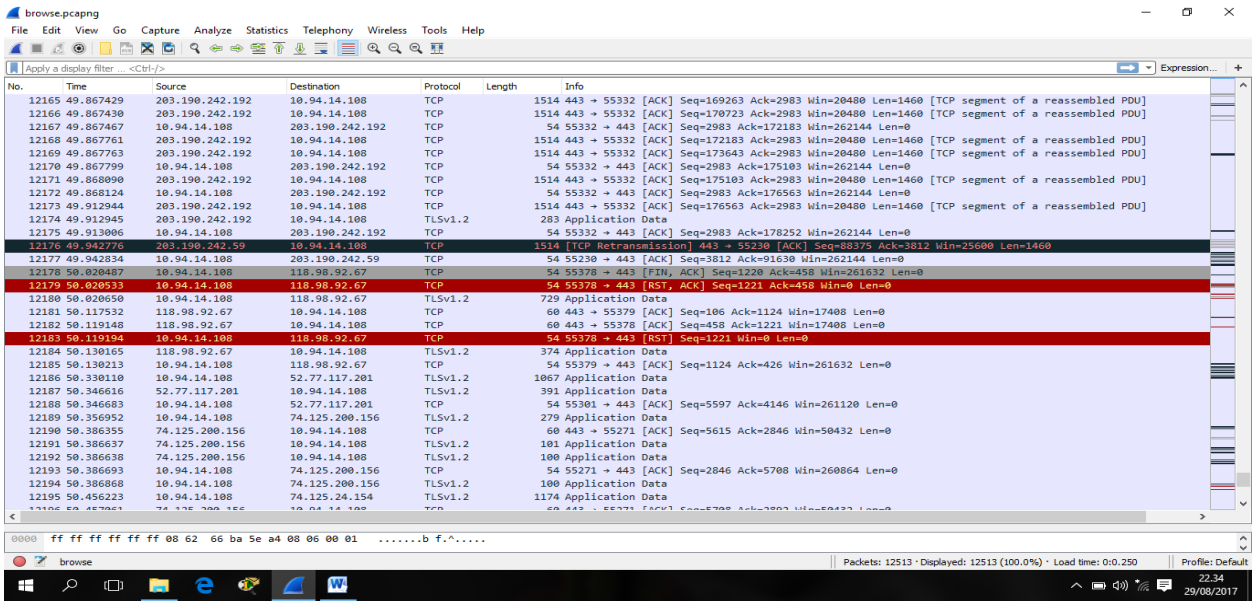
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

CAPTURING DATA

1. Browsing Data
   a. WIRESHARK



IP Source : 74.125.24.101 IP Destination : 10.94.14.108
MAC Source : (d4:ca:6d:44:6b:35) MAC Destination : (40:b0:34:0b:16:36)

- Source

IP	INFO
103.241.4.2	Standard query 0x4fce A www.detik.com
103.241.4.2	Standard query 0xf1ad A cdnstatic.detik.com
103.241.4.2	Standard query 0x2962 A www.google-analytics.com
103.241.5.2	Standard query 0xf1ae A cloudfront-labs.amazonaws.com
203.190.242.172	Client Hello
10.94.14.108	Certificate, Server Key Exchange, Server Hello Done
74.125.24.139	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

- Destination

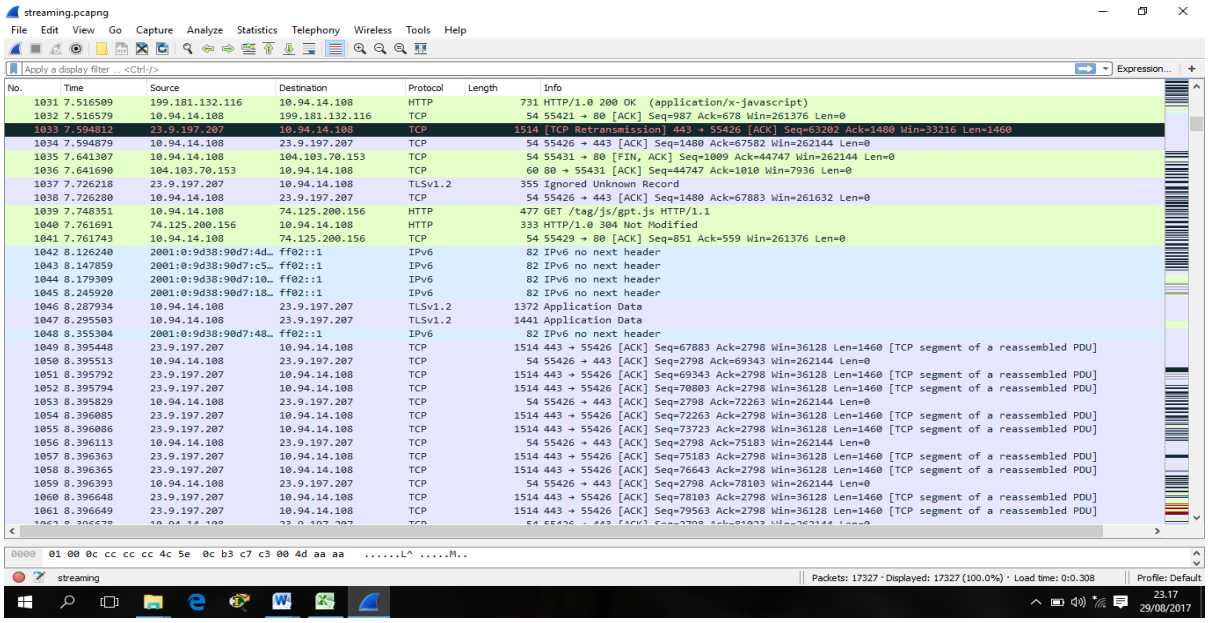
IP	INFO
10.94.14.108	Standard query 0xf1ad A cdnstatic.detik.com
10.94.14.108	Standard query 0x2962 A www.google-analytics.com
10.94.14.108	Standard query 0xf1ae A cloudfront-labs.amazonaws.com
10.94.14.108	Client Hello
74.125.24.139	Certificate, Server Key Exchange, Server Hello Done
10.94.14.108	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
54.230.156.138	Server Hello

b. Command

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\10>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:2508           DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:51306          DESKTOP-D8OL0MP:0      LISTENING
  TCP    10.94.14.108:139       DESKTOP-D8OL0MP:0      LISTENING
  TCP    10.94.14.108:55094     no-rdns:https          CLOSE_WAIT
  TCP    10.94.14.108:55095     no-rdns:https          ESTABLISHED
  TCP    10.94.14.108:55208     74.125.24.147:https    TIME_WAIT
  TCP    10.94.14.108:55228     74.125.24.139:https    TIME_WAIT
  TCP    10.94.14.108:55229     203.190.242.172:https  TIME_WAIT
  TCP    10.94.14.108:55230     203.190.242.59:https   TIME_WAIT
  TCP    10.94.14.108:55231     203.190.242.102:https  TIME_WAIT
  TCP    10.94.14.108:55232     203.190.242.102:https  TIME_WAIT
  TCP    10.94.14.108:55243     74.125.24.136:https    TIME_WAIT
  TCP    10.94.14.108:55246     203.190.242.35:https   TIME_WAIT
  TCP    10.94.14.108:55255     203.190.242.244:https  TIME_WAIT
  TCP    10.94.14.108:55256     sa-in-f157:https       TIME_WAIT
  TCP    10.94.14.108:55266     sa-in-f154:https       TIME_WAIT
  TCP    10.94.14.108:55267     sa-in-f154:https       ESTABLISHED
  TCP    10.94.14.108:55271     sa-in-f156:https       TIME_WAIT
  TCP    10.94.14.108:55272     74.125.24.154:https    ESTABLISHED
  TCP    10.94.14.108:55277     74.125.24.132:https    TIME_WAIT
  TCP    10.94.14.108:55279     74.125.24.148:https    TIME_WAIT
  TCP    10.94.14.108:55312     103.49.221.132:http    TIME_WAIT
  TCP    10.94.14.108:55313     74.125.24.102:https    TIME_WAIT
  TCP    10.94.14.108:55316     74.125.24.102:https    TIME_WAIT
^C
```

2. Streaming

a. WIRESHARK



IP Source : 10.94.14.108 IP Destination : 58.26.1.104

MAC Source : (d4:ca:6d:44:6b:35) MAC Destination : (40:b0:34:0b:16:36)

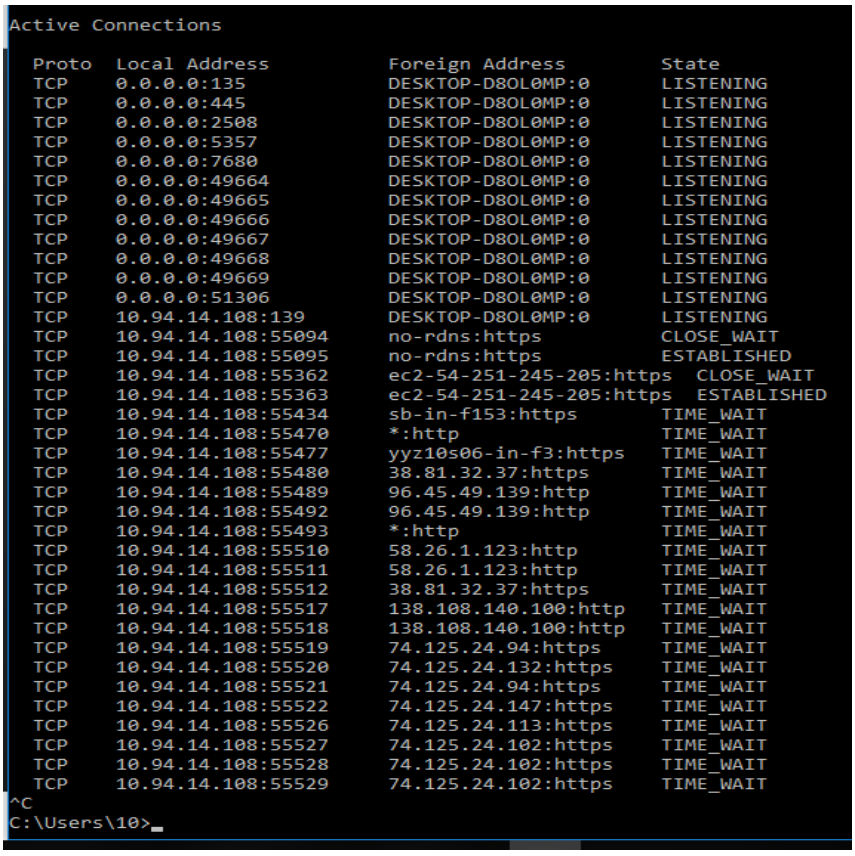
- Source

IP	INFO
10.94.14.108	Server Hello, Change Cipher Spec, Encrypted Handshake Message
74.125.24.102	Client Hello
74.125.24.102	Change Cipher Spec, Encrypted Handshake Message
10.94.14.108	Server Hello, Change Cipher Spec, Encrypted Handshake Message
103.241.4.2	Standard query 0x16f6 A cdn.registerdisney.go.com
103.241.5.2	Standard query 0x16f6 A cdn.registerdisney.go.com
103.241.4.2	Standard query 0x71ed A tredir.go.com

- Destination

IP	INFO
74.125.24.102	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.94.14.108	Client Hello
10.94.14.108	Change Cipher Spec, Encrypted Handshake Message
74.125.24.101	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.94.14.108	Standard query 0x16f6 A cdn.registerdisney.go.com
10.94.14.108	Standard query 0x16f6 A cdn.registerdisney.go.com
10.94.14.108	Standard query 0x71ed A tredir.go.com

b. Command



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:2508           DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-D8OL0MP:0      LISTENING
  TCP    0.0.0.0:51306          DESKTOP-D8OL0MP:0      LISTENING
  TCP    10.94.14.108:139       DESKTOP-D8OL0MP:0      LISTENING
  TCP    10.94.14.108:55094     no-rdns:https          CLOSE_WAIT
  TCP    10.94.14.108:55095     no-rdns:https          ESTABLISHED
  TCP    10.94.14.108:55362     ec2-54-251-245-205:https  CLOSE_WAIT
  TCP    10.94.14.108:55363     ec2-54-251-245-205:https  ESTABLISHED
  TCP    10.94.14.108:55434     sb-in-f153:https       TIME_WAIT
  TCP    10.94.14.108:55470     *:http                 TIME_WAIT
  TCP    10.94.14.108:55477     yyz10s06-in-f3:https   TIME_WAIT
  TCP    10.94.14.108:55480     38.81.32.37:https      TIME_WAIT
  TCP    10.94.14.108:55489     96.45.49.139:http      TIME_WAIT
  TCP    10.94.14.108:55492     96.45.49.139:http      TIME_WAIT
  TCP    10.94.14.108:55493     *:http                 TIME_WAIT
  TCP    10.94.14.108:55510     58.26.1.123:http       TIME_WAIT
  TCP    10.94.14.108:55511     58.26.1.123:http       TIME_WAIT
  TCP    10.94.14.108:55512     38.81.32.37:https      TIME_WAIT
  TCP    10.94.14.108:55517     138.108.140.100:http   TIME_WAIT
  TCP    10.94.14.108:55518     138.108.140.100:http   TIME_WAIT
  TCP    10.94.14.108:55519     74.125.24.94:https     TIME_WAIT
  TCP    10.94.14.108:55520     74.125.24.132:https    TIME_WAIT
  TCP    10.94.14.108:55521     74.125.24.94:https     TIME_WAIT
  TCP    10.94.14.108:55522     74.125.24.147:https    TIME_WAIT
  TCP    10.94.14.108:55526     74.125.24.113:https    TIME_WAIT
  TCP    10.94.14.108:55527     74.125.24.102:https    TIME_WAIT
  TCP    10.94.14.108:55528     74.125.24.102:https    TIME_WAIT
  TCP    10.94.14.108:55529     74.125.24.102:https    TIME_WAIT
^C
C:\Users\10>
```