

# JARINGAN KOMPUTER

“Capturing Data”



Nama : Dyah Citra Soraya  
NIM : 09011281520107  
Dosen Pengampuh : Deris Stiawan, M.T., PHD

**JURUSAN SISTEM KOMPUTER**

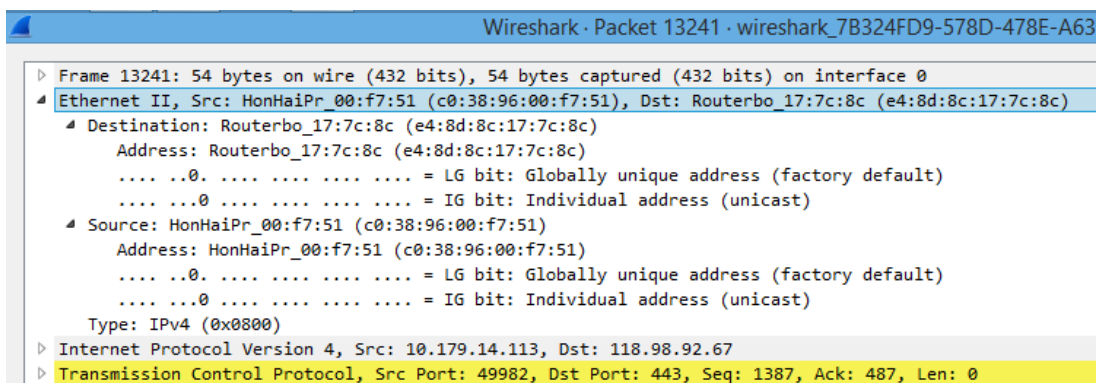
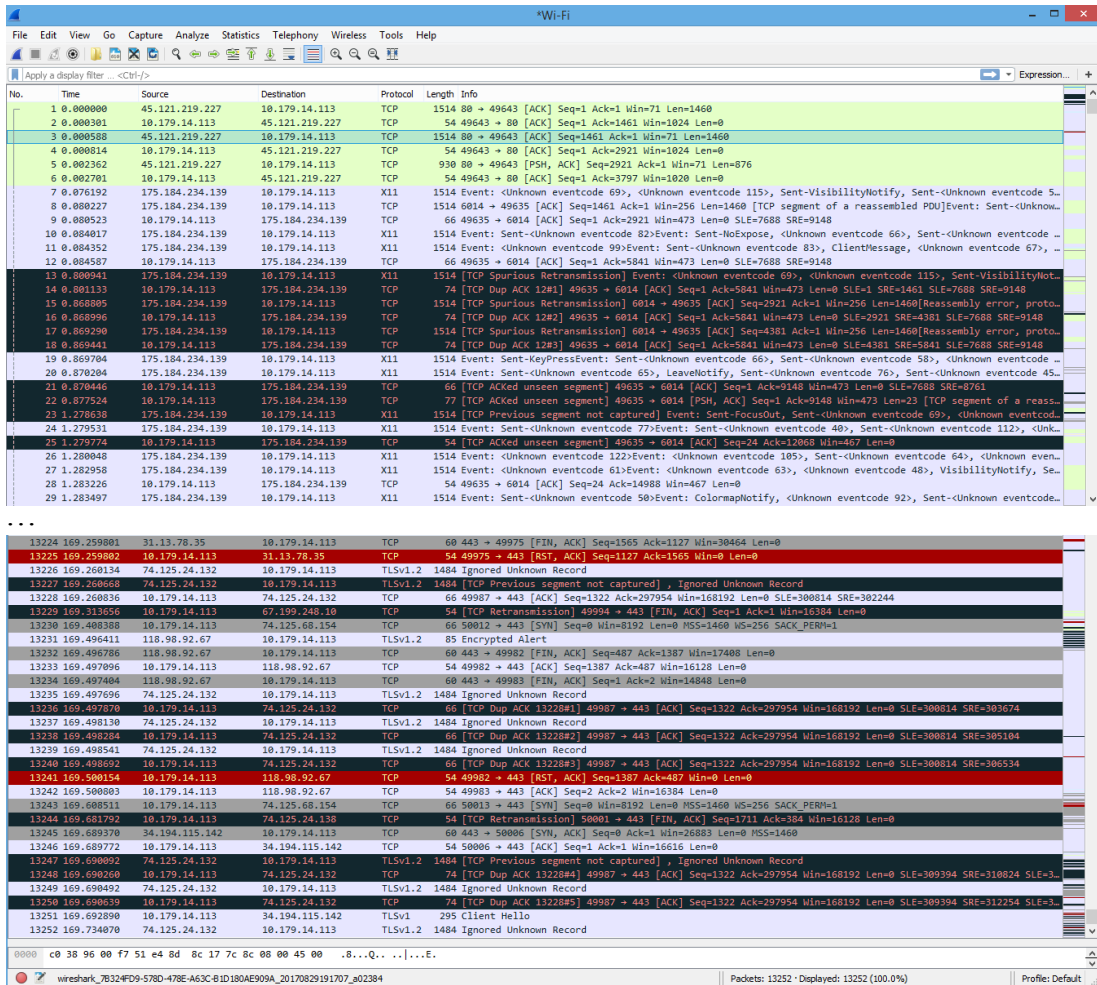
**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2017**

# CAPTURING DATA

## A. Case Web Browsing (vemale.com) menggunakan aplikasi Wireshark.



Maka :

- IP Source : 10.179.14.113
- IP Destination : 118.98.92.67
- MAC Source : e4:8d:8c:17:7c:8c
- MAC Destination : c0:38:96:00:f7:51
- Waktu : ± 1 menit

B. Case Web Browsing (vemale.com) menggunakan CMD.

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Citra>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             Dyah:0                 LISTENING
TCP   0.0.0.0:445             Dyah:0                 LISTENING
TCP   0.0.0.0:2500            Dyah:0                 LISTENING
TCP   0.0.0.0:49152          Dyah:0                 LISTENING
TCP   0.0.0.0:49153          Dyah:0                 LISTENING
TCP   0.0.0.0:49154          Dyah:0                 LISTENING
TCP   0.0.0.0:49155          Dyah:0                 LISTENING
TCP   0.0.0.0:49156          Dyah:0                 LISTENING
TCP   0.0.0.0:49177          Dyah:0                 LISTENING
TCP   10.179.14.113:139      Dyah:0                 LISTENING
TCP   10.179.14.113:49299    192-154-102-2:2858     ESTABLISHED
TCP   10.179.14.113:49340    ee2-54-251-160-139:https CLOSE_WAIT
TCP   10.179.14.113:49429    ee2-34-206-244-230:https CLOSE_WAIT
TCP   10.179.14.113:49431    a23-0-186-234:http     CLOSE_WAIT
TCP   10.179.14.113:49635    139:6014               ESTABLISHED
TCP   10.179.14.113:49677    eag1e607:8000          CLOSE_WAIT
TCP   10.179.14.113:49679    eag1e607:444           ESTABLISHED
TCP   10.179.14.113:49805    hosted-by:9999         ESTABLISHED
TCP   10.179.14.113:49962    150:http               CLOSE_WAIT
TCP   10.179.14.113:50308    rajf3-1:https          TIME_WAIT
TCP   10.179.14.113:50314    iad30s10-in-f196:https TIME_WAIT
TCP   10.179.14.113:50318    rajf4-1:https          TIME_WAIT
TCP   10.179.14.113:50320    rajf4-1:https          TIME_WAIT
TCP   10.179.14.113:50323    e:https                TIME_WAIT
TCP   10.179.14.113:50325    srv081-165-240-87:https TIME_WAIT
TCP   10.179.14.113:50327    sin11s01-in-f226:https TIME_WAIT
TCP   10.179.14.113:50328    sin11s01-in-f226:https TIME_WAIT
TCP   10.179.14.113:50329    rajf4-1:https          TIME_WAIT
TCP   10.179.14.113:50335    e:https                TIME_WAIT
TCP   10.179.14.113:50342    srv139-11-213-95:https TIME_WAIT
TCP   10.179.14.113:50344    163-172-32-82:http    TIME_WAIT
TCP   10.179.14.113:50349    sa-in-f94:https        TIME_WAIT
TCP   10.179.14.113:50350    74.125.24.113:https    TIME_WAIT
TCP   10.179.14.113:50351    sa-in-f113:https       TIME_WAIT
TCP   10.179.14.113:50352    ams16s21-in-f3:https   TIME_WAIT
TCP   10.179.14.113:50355    74.125.24.94:https     TIME_WAIT
^C
C:\Users\Citra>

```

- Source

IP	INFO
74.125.200.139	Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
10.179.14.113	Application Data
74.125.24.100	49666 → 443 [ACK] Seq=450 Ack=4198 Win=15104 Len=0
239.255.255.250	M-SEARCH * HTTP/1.1

- Destination

IP	INFO
74.125.200.139	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.179.14.6	Standard query 0x2f5b A isatap
10.179.14.113	POST /c.gif? HTTP/1.1 (application/json)
172.217.17.99	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

## C. Case Web Streaming (vidio.com) menggunakan aplikasi Wireshark.

The screenshot shows the Wireshark interface with a packet capture list. Packet 6 is highlighted in red, indicating a TCP RST. The packet details pane shows the RST flag set and the sequence number 62329.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.179.14.1	255.255.255.255	PMIPv6	154	32909 → 5678 Len=112
2	0.315554	23.0.177.143	10.179.14.113	TCP	60	443 → 62447 [ACK] Seq=1 Ack=1 Win=900 Len=0
3	0.315839	23.0.177.143	10.179.14.113	TLSv1.2	131	Application Data
4	0.316533	10.179.14.113	23.0.177.143	TLSv1.2	92	Application Data
5	0.318751	23.0.177.143	10.179.14.113	TLSv1.2	1510	Application Data
6	0.352657	10.179.14.113	10.179.18.1	TCP	54	62329 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.388490	10.179.14.113	23.0.177.143	TCP	54	62447 → 443 [ACK] Seq=405 Ack=1534 Win=64 Len=0
8	0.658694	23.0.177.143	10.179.14.113	TLSv1.2	131	[TCP Spurious Retransmission], Application Data
9	0.658788	10.179.14.113	23.0.177.143	TCP	66	[TCP Dup ACK 781] 62447 → 443 [ACK] Seq=405 Ack=1534 Win=64 Len=0 SLE=1 SRE=78
10	1.061221	23.0.177.143	10.179.14.113	TLSv1.2	1510	[TCP Spurious Retransmission], Application Data
11	1.061323	10.179.14.113	23.0.177.143	TCP	66	[TCP Dup ACK 782] 62447 → 443 [ACK] Seq=405 Ack=1534 Win=64 Len=0 SLE=78 SRE=1534
12	1.637564	HonHaiPr_a7:23:f2	Broadcast	ARP	42	Who has 10.179.14.28? Tell 10.179.14.78
13	2.707507	104.31.69.225	10.179.14.113	TCP	1514	80 → 62400 [ACK] Seq=1 Ack=1 Win=54 Len=1460 [TCP segment of a reassembled PDU]
14	2.707677	104.31.69.225	10.179.14.113	TCP	174	80 → 62400 [PSH, ACK] Seq=1461 Ack=1 Win=54 Len=120 [TCP segment of a reassembled PDU]
15	2.707764	10.179.14.113	104.31.69.225	TCP	54	62400 → 80 [ACK] Seq=1 Ack=1581 Win=64 Len=0
16	2.791208	104.31.69.225	10.179.14.113	TCP	1514	80 → 62400 [ACK] Seq=1581 Ack=1 Win=54 Len=1460 [TCP segment of a reassembled PDU]
17	2.791630	104.31.69.225	10.179.14.113	TCP	1514	80 → 62400 [ACK] Seq=3041 Ack=1 Win=54 Len=1460 [TCP segment of a reassembled PDU]
18	2.791736	10.179.14.113	104.31.69.225	TCP	54	62400 → 80 [ACK] Seq=1 Ack=4501 Win=64 Len=0
19	2.791983	104.31.69.225	10.179.14.113	TCP	1514	80 → 62400 [ACK] Seq=4501 Ack=1 Win=54 Len=1460 [TCP segment of a reassembled PDU]
20	2.792309	104.31.69.225	10.179.14.113	HTTP	350	HTTP/1.0 522 Unknown (text/html)
21	2.792414	10.179.14.113	104.31.69.225	TCP	54	62400 → 80 [ACK] Seq=1 Ack=6257 Win=64 Len=0
22	2.793465	10.179.14.113	104.31.69.225	TCP	54	62400 → 80 [ACK] Seq=1 Ack=6258 Win=64 Len=0
23	2.794584	10.179.14.113	104.31.69.225	TCP	54	62400 → 80 [RST, ACK] Seq=1 Ack=6258 Win=0 Len=0
24	3.695387	10.179.14.78	239.255.255.250	SSDP	415	NOTIFY * HTTP/1.1
25	3.798862	10.179.14.78	239.255.255.250	SSDP	431	NOTIFY * HTTP/1.1

... ..

2583	78.892201	52.76.1.73	10.179.14.113	TCP	60	443 → 62566 [FIN, ACK] Seq=5006 Ack=2191 Win=32000 Len=0
2584	79.006830	52.76.1.73	10.179.14.113	TCP	60	443 → 62567 [FIN, ACK] Seq=1 Ack=2 Win=27136 Len=0
2585	79.007077	58.26.1.122	10.179.14.113	TCP	60	443 → 62563 [FIN, ACK] Seq=1 Ack=2 Win=29216 Len=0
2586	79.007389	10.179.14.113	52.76.1.73	TCP	54	62567 → 443 [ACK] Seq=2 Ack=2 Win=16384 Len=0
2587	79.007474	10.179.14.113	58.26.1.122	TCP	54	62563 → 443 [ACK] Seq=2 Ack=2 Win=16384 Len=0
2588	79.007522	58.26.1.122	10.179.14.113	TLSv1.2	77	Encrypted Alert
2589	79.007998	10.179.14.113	58.26.1.122	TCP	54	62562 → 443 [RST, ACK] Seq=1010 Ack=954 Win=0 Len=0
2590	79.158575	58.26.1.122	10.179.14.113	TCP	60	443 → 62562 [FIN, ACK] Seq=954 Ack=1010 Win=31360 Len=0
2591	79.208429	58.26.1.122	10.179.14.113	TCP	60	[TCP Out-Of-Order] 443 → 62562 [FIN, ACK] Seq=954 Ack=1010 Win=31360 Len=0
2592	79.208546	58.26.1.122	10.179.14.113	TCP	60	[TCP Out-Of-Order] 443 → 62563 [FIN, ACK] Seq=1 Ack=2 Win=29216 Len=0
2593	79.208611	10.179.14.113	58.26.1.122	TCP	54	[TCP ZeroWindow] 62563 → 443 [ACK] Seq=2 Ack=2 Win=0 Len=0
2594	79.202209	58.26.1.122	10.179.14.113	TCP	60	[TCP Out-Of-Order] 443 → 62563 [FIN, ACK] Seq=1 Ack=2 Win=29216 Len=0
2595	79.202291	10.179.14.113	58.26.1.122	TCP	54	[TCP ZeroWindow] 62563 → 443 [ACK] Seq=2 Ack=2 Win=0 Len=0
2596	79.284744	58.26.1.122	10.179.14.113	TCP	77	[TCP Out-Of-Order] 443 → 62562 [FIN, PSH, ACK] Seq=931 Ack=1010 Win=31360 Len=23
2597	79.365980	10.179.14.78	239.255.255.250	SSDP	359	NOTIFY * HTTP/1.1
2598	79.369562	10.179.14.78	239.255.255.250	SSDP	350	NOTIFY * HTTP/1.1
2599	79.464884	10.179.14.78	239.255.255.250	SSDP	402	NOTIFY * HTTP/1.1
2600	79.567536	10.179.14.78	239.255.255.250	SSDP	416	NOTIFY * HTTP/1.1
2601	79.571329	10.179.14.78	239.255.255.250	SSDP	359	NOTIFY * HTTP/1.1
2602	79.576494	10.179.14.78	239.255.255.250	SSDP	430	NOTIFY * HTTP/1.1
2603	79.576805	58.26.1.122	10.179.14.113	TCP	60	443 → 62563 [RST] Seq=2 Win=0 Len=0
2604	79.577067	58.26.1.122	10.179.14.113	TCP	60	443 → 62563 [RST] Seq=2 Win=0 Len=0
2605	79.770227	Routerbo_17:7c:8c	Broadcast	ARP	60	Who has 10.179.14.52? Tell 10.179.14.1
2606	80.471314	60.253.96.7	10.179.14.113	TCP	60	37059 → 62335 [PSH, ACK] Seq=307 Ack=61 Win=256 Len=4

Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 Ethernet II, Src: HonHaiPr\_00:f7:51 (c0:38:96:00:f7:51), Dst: Routerbo\_17:7c:8c (e4:8d:8c:17:7c:8c)  
 Internet Protocol Version 4, Src: 10.179.14.113, Dst: 10.179.18.1  
 Transmission Control Protocol, Src Port: 62329, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000 e4 8d 8c 17 7c 8c c0 38 96 00 f7 51 08 00 45 00 ...|.8...Q..E.

wireshark\_7b32fd9-578d-478e-a63c-01d180ae909a\_20170829205601\_01528 | Packets: 2606 · Displayed: 2606 (100.0%) | Profile: Default

The screenshot shows the details of Packet 6 in Wireshark. The Ethernet II section shows the source MAC address as c0:38:96:00:f7:51 and the destination MAC address as e4:8d:8c:17:7c:8c.

Wireshark · Packet 6 · wireshark\_7B324FD9-578D-478E-A63C-B1D

Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

- Interface id: 0 (Device\NPF\_{7B324FD9-578D-478E-A63C-B1D180AE909A})
- Encapsulation type: Ethernet (1)
- Arrival Time: Aug 29, 2017 20:56:01.539528000 SE Asia Standard Time [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1504014961.539528000 seconds [Time delta from previous captured frame: 0.033906000 seconds]
- Epoch Time: 1504014961.539528000 seconds [Time delta from previous displayed frame: 0.033906000 seconds]
- Time since reference or first frame: 0.352657000 seconds
- Frame Number: 6
- Frame Length: 54 bytes (432 bits)
- Capture Length: 54 bytes (432 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- Protocols in frame: eth:ethertype:ip:tcp
- Coloring Rule Name: TCP RST
- Coloring Rule String: tcp.flags.reset eq 1
- Ethernet II, Src: HonHaiPr\_00:f7:51 (c0:38:96:00:f7:51), Dst: Routerbo\_17:7c:8c (e4:8d:8c:17:7c:8c)
  - Destination: Routerbo\_17:7c:8c (e4:8d:8c:17:7c:8c)
  - Source: HonHaiPr\_00:f7:51 (c0:38:96:00:f7:51)
  - Type: IPv4 (0x0800)

Maka :

- IP Source : 10.179.14.113
- IP Destination : 10.179.18.1
- MAC Source : e4:8d:8c:17:7c:8c
- MAC Destination : c0:38:96:00:f7:51
- Waktu : ± 1 menit

#### D. Case Web Browsing (vemale.com) menggunakan CMD.

```

Command Prompt
TCP 10.179.14.112:139 DESKTOP-7JBA6MF:0 LISTENING
TCP 10.179.14.112:48945 DESKTOP-7JBA6MF:0 LISTENING
TCP 10.179.14.112:58956 91.190.218.51:12350 CLOSE_WAIT
TCP 10.179.14.112:59037 111.221.77.142:40027 CLOSE_WAIT
TCP 10.179.14.112:59040 hk2sch130021738:https ESTABLISHED
TCP 10.179.14.112:59073 hk2sch130021218:https ESTABLISHED
TCP 10.179.14.112:59111 192.229.232.200:https CLOSE_WAIT
TCP 10.179.14.112:59378 185.189.92.234:https ESTABLISHED
TCP 10.179.14.112:59495 74.125.24.97:https TIME_WAIT
TCP 10.179.14.112:59497 sc-in-f102:https ESTABLISHED
TCP 10.179.14.112:59501 server-54-230-156-181:https TIME_WAIT
TCP 10.179.14.112:59502 server-54-230-156-181:https TIME_WAIT
TCP 10.179.14.112:59503 103.3.56.92:https ESTABLISHED
TCP 10.179.14.112:59511 21:https TIME_WAIT
TCP 10.179.14.112:59513 server-54-230-156-87:https CLOSE_WAIT
TCP 10.179.14.112:59514 server-54-230-156-87:https CLOSE_WAIT
TCP 10.179.14.112:59515 sa-in-f156:https ESTABLISHED
TCP 10.179.14.112:59516 sa-in-f156:https TIME_WAIT
TCP 10.179.14.112:59518 server-54-230-156-146:https CLOSE_WAIT
TCP 10.179.14.112:59521 ec2-52-74-120-185:https ESTABLISHED
TCP 10.179.14.112:59527 sa-in-f105:https ESTABLISHED
TCP 10.179.14.112:59530 sa-in-f94:https ESTABLISHED
TCP 10.179.14.112:59531 sa-in-f94:https ESTABLISHED
TCP 10.179.14.112:59540 ec2-52-74-205-135:https CLOSE_WAIT
TCP 10.179.14.112:59542 ec2-52-74-205-135:https CLOSE_WAIT
TCP 10.179.14.112:59543 a23-0-182-207:https ESTABLISHED
TCP 10.179.14.112:59544 server-54-230-159-100:https CLOSE_WAIT
TCP 10.179.14.112:59562 202.43.88.44:https ESTABLISHED
TCP 10.179.14.112:59570 sa-in-f156:https ESTABLISHED
TCP 10.179.14.112:59571 sa-in-f156:https ESTABLISHED
TCP 10.179.14.112:59572 sa-in-f154:https ESTABLISHED
TCP 10.179.14.112:59573 sa-in-f154:https ESTABLISHED
TCP 10.179.14.112:59574 sin11s01-in-f226:https ESTABLISHED
TCP 10.179.14.112:59575 sin11s01-in-f226:https ESTABLISHED
TCP 10.179.14.112:59578 sc-in-f95:https ESTABLISHED
TCP 10.179.14.112:59579 sc-in-f95:https ESTABLISHED
TCP 10.179.14.112:59585 sa-in-f148:https ESTABLISHED
TCP 10.179.14.112:59586 sa-in-f148:https ESTABLISHED
TCP 10.179.14.112:59587 sin11s01-in-f226:https ESTABLISHED
TCP 10.179.14.112:59588 sin11s01-in-f226:https ESTABLISHED
TCP 10.179.14.112:59589 sin11s01-in-f226:https ESTABLISHED
TCP 10.179.14.112:59590 sa-in-f154:https ESTABLISHED
TCP 10.179.14.112:59591 sa-in-f154:https ESTABLISHED
TCP 10.179.14.112:59597 111.221.29.254:https ESTABLISHED
^C

```

- Source

IP	INFO
10.179.14.113	Application Data
239.255.255.250	M-SEARCH * HTTP/1.1
45.121.219.227	Change Cipher Spec, Encrypted Handshake Message
224.0.0.251	Standard query 0x0000 PTR _233637DE._sub._googlecast._tcp.local, "QM" question

- Destination

IP	INFO
10.179.14.113	62329 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.179.14.113	443 → 62445 [FIN, ACK] Seq=24 Ack=2 Win=1013 Len=0
104.103.70.40	HTTP/1.0 200 OK (JPEG JFIF image)
10.179.14.113	Client Hello