

Nama : M. Andre Sofyan

NIM : 09011281520130

TUGAS JARINGAN KOMPUTER

Capturing data from www.detik.com

Hasil capture dengan menggunakan Wireshark

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet (No. 16264) is a TCP segment with the following details:

- Frame 16264: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
- Ethernet II, Src: 8c:e1:17:e3:83:04 (8c:e1:17:e3:83:04), Dst: Azurewav_48:4a:49 (28:c2:dd:48:4a:49)
- Internet Protocol Version 4, Src: 203.190.242.132, Dst: 192.168.1.8
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50283 (50283), Seq: 442, Ack: 398, Len: 0

The packet bytes are displayed in hexadecimal and ASCII:

```
0000 28 c2 dd 48 4a 49 8c e1 17 e3 83 04 08 00 45 00 (.HJI.. ..E.  
0010 00 28 0b 4f 40 00 fb 06 f4 8c cb be f2 84 c0 a8 -(00... ..  
0020 01 08 00 50 c4 6b cf 26 d4 f4 58 fc d9 a3 50 10 ...P.k.& .OX...P.  
0030 12 91 82 7d 00 00 ....)
```

Hasil capture dengan menggunakan command prompt

The screenshot shows a Windows command prompt window with the following output:

```
C:\WINDOWS\system32\cmd.exe  
C:\Users\Sofyan>netstat -a  
  
Active Connections  
  
Proto Local Address Foreign Address State  
TCP 0.0.0.0:135 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:445 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:2508 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:49664 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:49665 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:49666 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:49667 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:49668 DESKTOP-F9V4QNK:0 LISTENING  
TCP 0.0.0.0:49674 DESKTOP-F9V4QNK:0 LISTENING  
TCP 127.0.0.1:1001 DESKTOP-F9V4QNK:0 LISTENING  
TCP 127.0.0.1:6543 DESKTOP-F9V4QNK:0 LISTENING  
TCP 127.0.0.1:50013 DESKTOP-F9V4QNK:0 LISTENING  
TCP 127.0.0.1:50013 www:50043 ESTABLISHED  
TCP 127.0.0.1:50014 DESKTOP-F9V4QNK:0 LISTENING  
TCP 127.0.0.1:50043 www:50013 ESTABLISHED  
TCP 127.0.0.1:65000 DESKTOP-F9V4QNK:0 LISTENING  
TCP 192.168.1.8:139 DESKTOP-F9V4QNK:0 LISTENING  
TCP 192.168.1.8:50049 hk2sch130022129:https ESTABLISHED  
TCP 192.168.1.8:50080 sc-in-f188:https ESTABLISHED  
TCP 192.168.1.8:50130 sb-in-f100:http ESTABLISHED  
TCP 192.168.1.8:50164 103.49.221.211:http ESTABLISHED  
TCP 192.168.1.8:50165 103.49.221.172:https TIME_WAIT  
TCP 192.168.1.8:50169 172:https ESTABLISHED  
TCP 192.168.1.8:50178 sin10s01-in-f78:https TIME_WAIT  
TCP 192.168.1.8:50180 172:http ESTABLISHED  
TCP 192.168.1.8:50181 103.49.221.232:http ESTABLISHED  
TCP 192.168.1.8:50182 232:http ESTABLISHED
```

Tabel Source :

IP	INFO
192.168.1.8	50344 → 443 [RST, ACK] Seq=335 Ack=6207 Win=0 Len=0
192.168.1.8	[TCP Dup ACK 16202#1] 50345 → 443 [ACK] Seq=934 Ack=7712 Win=66560 Len=0 SLE=9110 SRE=9385
192.168.1.8	Client Hello
192.168.1.8	50343 → 443 [ACK] Seq=210 Ack=3490 Win=66048 Len=0
192.168.1.8	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request

Tabel Destination :

IP	INFO
203.190.242.122	[TCP segment of a reassembled PDU]
203.190.242.122	Application Data
203.190.242.223	[TCP segment of a reassembled PDU]
203.190.242.132	[TCP Keep-Alive ACK] 80 → 50283 [ACK] Seq=442 Ack=398 Win=4753 Len=0
203.190.242.223	50286 → 443 [ACK] Seq=3874 Ack=356863 Win=66560 Len=0

Capturing data from www.vidio.com

Hasil capturing menggunakan Wireshark

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet (No. 17415) is a TCP RST, ACK segment from 192.168.0.101 to 192.168.0.101. The details pane shows the following information:

- Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
- Ethernet II, Src: Azurewv_48:4a:49 (28:c2:dd:48:4a:49), Dst: 90:c7:d8:04:5c:68 (90:c7:d8:04:5c:68)
- Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
- User Datagram Protocol, Src Port: 64616 (64616), Dst Port: 53 (53)
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000  90 c7 d8 04 5c 68 28 c2 dd 48 4a 49 00 00 45 00  ....\h(. .HJ1..E.
0010  00 3d 01 b2 00 00 11 b7 47 c0 a8 00 65 c0 a8  ..,.....G...t...
0020  00 01 fc 68 00 35 00 29 5e 1b 82 4d 01 00 00 01  ...h.S.)^..M....
0030  00 00 00 00 00 00 04 61 70 69 73 06 67 6f 6f 67  .....a pis.goog
0040  6c 65 03 63 6f 6d 00 00 01 00 01                le.com. . . .
    
```

Hasil capture dengan menggunakan command prompt

```

C:\WINDOWS\system32\cmd.exe
C:\Users\Sofyan>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:445             DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:2508            DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:49664           DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:49665           DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:49666           DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:49667           DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:49668           DESKTOP-F9V4QNK:0     LISTENING
TCP   0.0.0.0:49674           DESKTOP-F9V4QNK:0     LISTENING
TCP   127.0.0.1:1001          DESKTOP-F9V4QNK:0     LISTENING
TCP   127.0.0.1:6543          DESKTOP-F9V4QNK:0     LISTENING
TCP   127.0.0.1:50013        DESKTOP-F9V4QNK:0     LISTENING
TCP   127.0.0.1:50013        www:62355              TIME_WAIT
TCP   127.0.0.1:50013        www:62364              ESTABLISHED
TCP   127.0.0.1:50014        DESKTOP-F9V4QNK:0     LISTENING
TCP   127.0.0.1:52001        DESKTOP-F9V4QNK:0     LISTENING
TCP   127.0.0.1:52001        www:62351              ESTABLISHED
TCP   127.0.0.1:52001        www:62352              ESTABLISHED
TCP   127.0.0.1:52001        www:62353              ESTABLISHED
TCP   127.0.0.1:52001        www:62354              ESTABLISHED
TCP   127.0.0.1:62351        www:52001              ESTABLISHED
TCP   127.0.0.1:62352        www:52001              ESTABLISHED
TCP   127.0.0.1:62353        www:52001              ESTABLISHED
TCP   127.0.0.1:62354        www:52001              ESTABLISHED
TCP   127.0.0.1:62634        www:50013              ESTABLISHED
  
```

Tabel Source :

IP	INFO
192.168.0.101	[TCP Previous segment not captured] Ignored Unknown Record
192.168.0.101	443 → 62693 [ACK] Seq=7693137 Ack=2776 Win=43136 Len=1394
192.168.0.101	443 → 62693 [ACK] Seq=7684773 Ack=2776 Win=43136 Len=1394
192.168.0.101	Previous segment not captured] Ignored Unknown Record
192.168.0.101	[TCP Fast Retransmission] Change Cipher Spec

Tabel Destination :

IP	INFO
23.60.152.79	62693 → 443 [ACK] Seq=2635 Ack=7386193 Win=568576 Len=0 SLE=7387587 SRE=7388981
23.60.152.79	62693 → 443 [ACK] Seq=2635 Ack=7388981 Win=568576 Len=0
23.60.152.79	62693 → 443 [ACK] Seq=2635 Ack=7444741 Win=568576 Len=0 SLE=7446135 SRE=7448923 SLE=7453105 SRE=7454499
23.60.152.79	Application Data
23.60.152.79	62693 → 443 [ACK] Seq=2494 Ack=7244016 Win=568576 Len=0

Perbedaan Capture Data menggunakan Wireshark dan Cmd;

dengan menggunakan Wireshark kita mendapatkan analisi data yang lebih lengkap dan terinci dibandingkan dengan menggunakan Cmd, selain itu juga Cmd hanya dapat membaca protocol TCP sedangkan pada Wireshark dapat membaca berbagai jenis protocol sehingga banyak data yang muncul, termasuk berbagai jenis data error yang terjadi saat pembacaan data.