

JURNAL MODUL 10

Kaenova Mahendra Auditama | 1301190324 | IF-43-02

Silakan browsing. Jangan lupa pencantuman sumber!

referensi: <https://gist.github.com/tuxfight3r/9ac030cb0d707bb446c7>

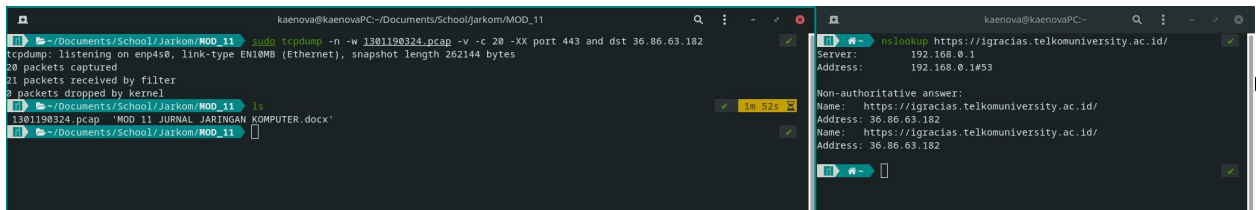
1. Syntax : tcpdump Jelaskan arti dari syntax setiap kategori dibawah ini!

- -n : tidak mengubah host address, port number, atau yang lainnya menjadi nama
- -c : menangkap paket dengan jumlah tertentu.
- -i : mendefinisikan suatu interface tertentu untuk menangkap paket tersebut.
- -v : memberikan informasi tambahan (verbose)
- -w : menuliskan paket-paket yang ditangkap kesuatu file tertentu
- -r : membaca file yang berisi paket-paket tertentu
- -X : menuliskan paket-paket tersebut dengan ASCII atau Hex
- -A : memprint semua paket dalam ASCII
- -s : membatasi panjang paket yang diterima

2. Lakukan capture packet (dalam 1 syntax) dengan syarat

- ip muncul dengan bentuk desimal (ex : 192.168.1.1) bukan dns (ex: igracias.com)
- Menyimpan hasil capture kedalam file bernama [nimkalian.pcap] (ex: 130317111.pcap)
- Memunculkan informasi flags,cksum,ack,win,option, dan length
- Limit jumlah paket = 20
- Menampilkan hexa dan ASCII
- ip tujuan merupakan ip igracias(cek terlebih dahulu menggunakan command nslookup)
- Port https(443)

Setelah itu lakukan akses ke halaman igracias. **Sertakan screenshot bahwa paket telah ter-capture.**

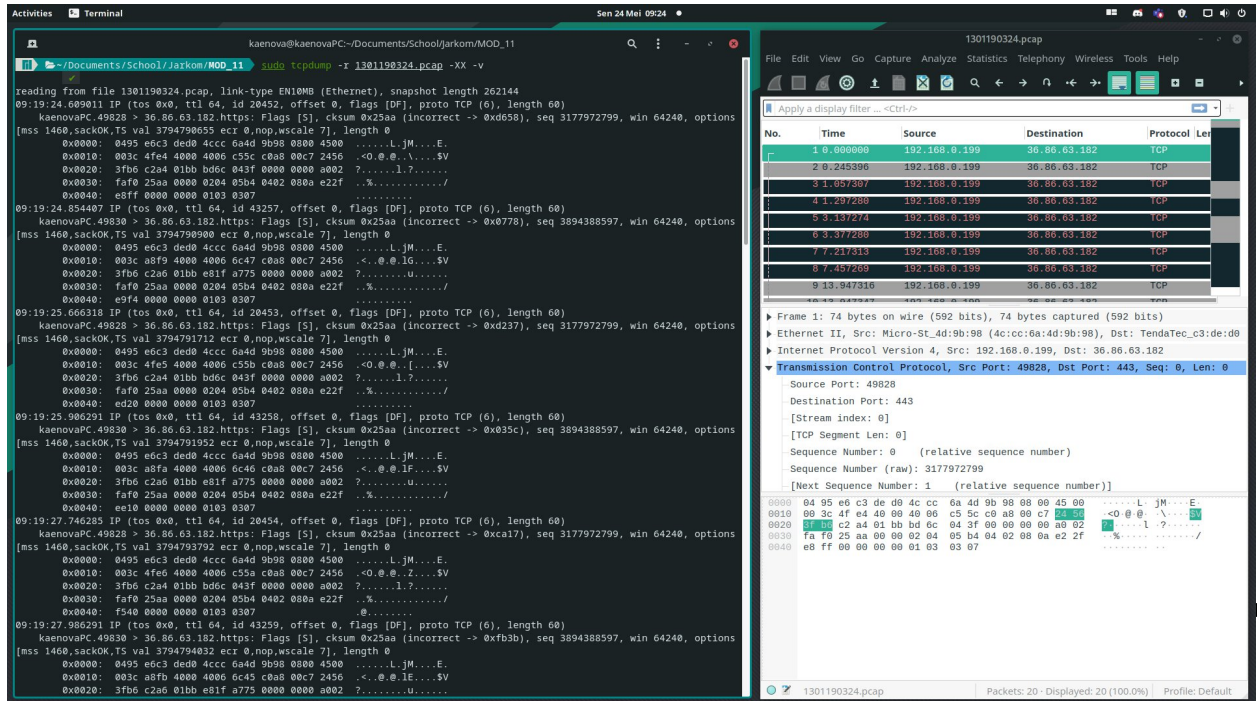


```
kaenova@kaenovaPC:~/Documents/School/Jarkom/MOD_11
$ sudo tcpdump -n -w 1301190324.pcap -v -c 20 -XX port 443 and dst 36.86.63.182
tcpdump: listening on enp4s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20 packets captured
21 packets received by filter
0 packets dropped by kernel
$ ls
1301190324.pcap  MOD_11 JURNAL JARINGAN KOMPUTER.docx
$
```

```
kaenova@kaenovaPC:~
$ nslookup https://igracias.telkomuniversity.ac.id/
Server: 192.168.0.1
Address: 192.168.0.1#53

Non-authoritative answer:
Name: https://igracias.telkomuniversity.ac.id/
Address: 36.86.63.182
Name: https://igracias.telkomuniversity.ac.id/
Address: 36.86.63.182
```

- Buka file [nimkalian.pcap] dengan syntax tcpdump di terminal. Jelaskan maksud dari bagian paket yang sudah tercapture. Dan menurut pendapat anda apa perbedaannya dengan capture packet dengan wireshark?

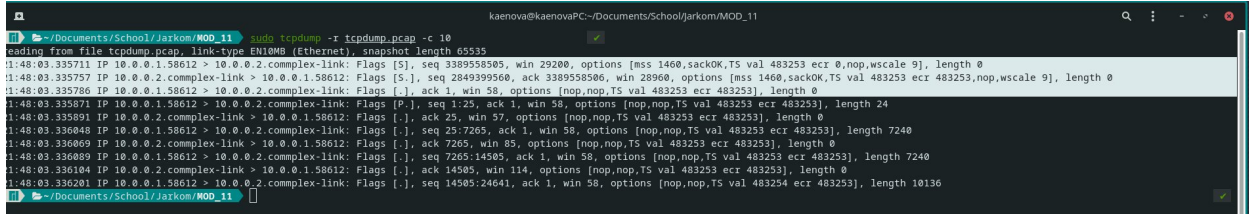


The screenshot displays two side-by-side windows. The left window is a terminal running the command `tcpdump -r 1301190324.pcap -XX -v`. It shows the raw packet data for an HTTP GET request to `https://36.86.63.182/` from source IP `192.168.0.199` to destination IP `36.86.63.182`. The packet is a TCP segment with sequence number 3177972799 and window size 64240. The payload is an HTTP GET request for `/` with a status of 200 OK.

The right window is Wireshark, showing the same packet capture. The packet list pane shows the selected packet (No. 1) with details expanded to show the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet details pane shows the raw packet data in hexadecimal and ASCII.

Terlihat perbedaannya bahwa sebenarnya informasi yang ditampilkan atau di dapatkan itu sama, hanya saja dalam wireshark terlihat dengan GUI sehingga lebih mudah dilihat, dan tcpdump hanya mengambil paket-paket yang ada pada jaringan tidak melakukan analisis

4. Buka file tcpdump.pcap melalui syntax tcpdump untuk melihat hasil capture paket. Cari threeway handshaking minimal 1 (lakukan filter dengan penampilan paket hanya 10 paket saja).



```

kaenova@kaenovaPC:~/Documents/School/Jarkom/MOD_11
~/Documents/School/Jarkom/MOD_11 $ sudo tcpdump -r tcpdump.pcap -c 10
reading from file tcpdump.pcap, link-type EN10MB (Ethernet), snapshot length 65535
11:48:03.335711 IP 10.0.0.1.58612 > 10.0.0.2.complex-link: Flags [S], seq 3389558505, win 29200, options [mss 1460,sackOK,TS val 483253 ecr 0,nop,wscale 9], length 0
11:48:03.335757 IP 10.0.0.2.complex-link > 10.0.0.1.58612: Flags [S.], seq 2849399560, ack 3389558506, win 28960, options [mss 1460,sackOK,TS val 483253 ecr 483253,nop,wscale 9], length 0
11:48:03.335786 IP 10.0.0.1.58612 > 10.0.0.2.complex-link: Flags [.] , ack 1, win 58, options [nop,nop,TS val 483253 ecr 483253], length 0
11:48:03.335871 IP 10.0.0.1.58612 > 10.0.0.2.complex-link: Flags [P.], seq 1:25, ack 1, win 58, options [nop,nop,TS val 483253 ecr 483253], length 24
11:48:03.335891 IP 10.0.0.2.complex-link > 10.0.0.1.58612: Flags [.] , ack 25, win 57, options [nop,nop,TS val 483253 ecr 483253], length 0
11:48:03.336048 IP 10.0.0.1.58612 > 10.0.0.2.complex-link: Flags [.] , seq 25:7265, ack 1, win 58, options [nop,nop,TS val 483253 ecr 483253], length 7240
11:48:03.336069 IP 10.0.0.2.complex-link > 10.0.0.1.58612: Flags [.] , ack 7265, win 85, options [nop,nop,TS val 483253 ecr 483253], length 0
11:48:03.336089 IP 10.0.0.1.58612 > 10.0.0.2.complex-link: Flags [.] , seq 7265:14505, ack 1, win 58, options [nop,nop,TS val 483253 ecr 483253], length 7240
11:48:03.336104 IP 10.0.0.2.complex-link > 10.0.0.1.58612: Flags [.] , ack 14505, win 114, options [nop,nop,TS val 483253 ecr 483253], length 0
11:48:03.336201 IP 10.0.0.1.58612 > 10.0.0.2.complex-link: Flags [.] , seq 14505:24641, ack 1, win 58, options [nop,nop,TS val 483254 ecr 483253], length 10136
~/Documents/School/Jarkom/MOD_11 $

```

5. Menurut pendapat anda, apa perbedaannya antara mencari threeway handshaking menggunakan wireshark dan tcpdump?

Syntax flag yang digunakan berbeda dengan wireshark. Pada tcpdump, flags 'S' diartikan dengan SYN, sementara flags '.' itu untuk ACK. Pada wireshark flags yang ditampilkan tersebut dituliskan SYN dan ACK