TCPDUMP

Sintassi: **tcpdump [opzioni] [espressioni]**

Le **opzioni** stabiliscono il modo di funzionamento del programma e il tipo di informazioni da visualizzare. Ad esempio:

```
tcpdump    # info essenziali di tutti i pacchetti dall'interfaccia principale

tcpdump -i  eth1       # utilizza una interfaccia diversa

tcpdump  -w file.pcap  # salva i pacchetti catturati nel file

tcpdump  -w file.pcap  -Z <user>  # crea file con uid <user>

tcpdump -r  file.pcap  # legge i pacchetti dal file anziche' dall'interfaccia

tcpdump -X             # contenuto dei primi 68 byte di ogni pacchetto

tcpdump -X -s 1500     # come sopra ma visualizza 1500 byte

tcpdump -n             # non risolve gli indirizzi IP

tcpdump -nn            # non risolve gli indirizzi IP e le porte

tcpdump -F filter.txt  # legge le espressioni da file

tcpdump -c 100         # cattura 100 frame , quindi termina
```

Se non viene impostato il numero di frame da catturare (opzione -c) il programma deve essere terminato premendo ctrl/C.

Le espressioni ci consentono di applicare un filtro sui pacchetti da catturare.

Nell'espressione possiamo combinare mediante operatori logici:

Tipo e direzione: host, net, port, src, dst,

Protocollo: ether, ip, ip6, arp, tcp, udp,

Alcuni esempi:

```
tcpdump    ether host 00:0c:29:df:d4:21

tcpdump -X ether dst  01:80:C2:00:00:00 -i eth0

tcpdump dst host 192.135.11.1 # filtra i pacchetti destinati  all'indirizzo IP

tcpdump  net 160.78.124.0/24  # Indirizzo appartenente alla rete indicata

tcpdump  host 172.28.34.100  and port 25 # Traffico SMTP dell'host

tcpdump "host  172.28.34.100  and (not src net 172.28.34.0/24 or not dst net
172.28.34.0/24)" Tutto il traffico tra la il sistema locale e l'esterno della
LAN.

tcpdump udp

tcpdump "ip[0] & 0x0f > 5"

tcpdump "(tcp[13] & 0x03 !=0 and not src and dst host localhost)"
```

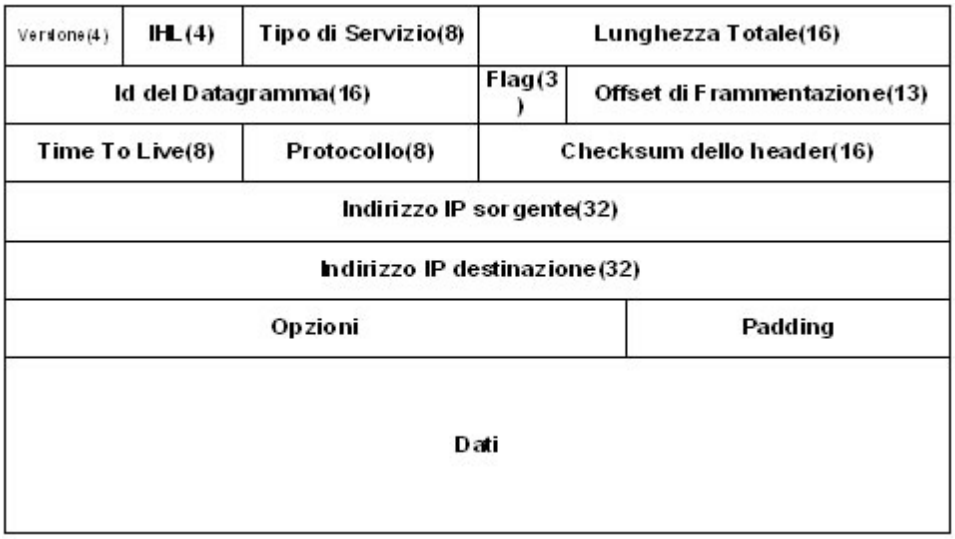
```
tcpdump -nn  "tcp[tcpflags] & (tcp-syn|tcp-fin) != 0"

tcpdump "tcp[tcpflags] & (tcp-syn|tcp-fin) != 0" # pacchetti con SYN o FIN attivi

tcpdump -nn  "tcp[12] >> 4 > 5”  #pacchetti tcp con opzioni nell'intestazione (HLEN > 5)
```

nota: tcp[13] è il 14mo byte dell'header TCP. Contiene i 6 bit di codice: URG,ACK,PSH,RST,SYN,FIN

Intestazione IP



Intestazione TCP