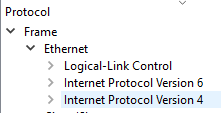
**LABO 9**

**IP-PAKKETTEN**

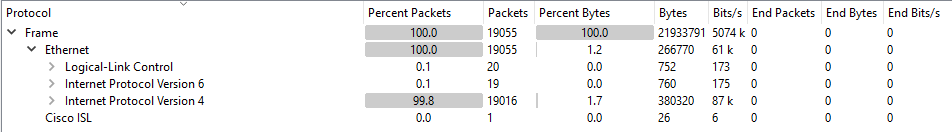
1. Download het bestand **Capture1.pcapng** (PCAPNG = Packet CAPture Next Generation) vanaf Leho (module Wireshark-files) en open dit bestand door erop te dubbelklikken.
2. Niet alle Ethernetpakketten in deze capture-file zijn IP-pakketten. Je kan dit snel zien door in het menu *Statistics* te klikken op *Protocol Hierarchy* en dan de rijen onder *Ethernet* dicht te klappen tot je onderstaande boomstructuur bekomt:



Hoeveel frames bevatten er bijgevolg geen IP-pakketten?

20

Plak hieronder een screenshot van het venster waarin je deze info gevonden hebt en markeer dit getal.



1. Sluit dit venster en keer terug naar je capture-file. Voer nu een filter in waarmee je de frames kunt weergeven die geen IP-pakketten bevatten.

!(eth.type == 0x0800) and !(eth.type==0x86dd)

Of

not ip and not ipv6

1. Welke filter moet je invoeren om na te gaan hoeveel IPv4-pakketten er afkomstig zijn van een device met IPv4-adres 31.13.92.14?

ip.src==31.13.92.14

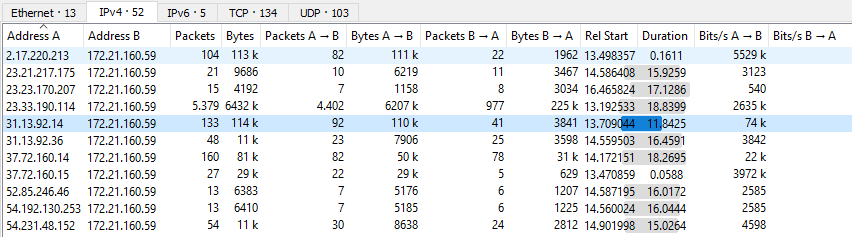
of

ip.src eq 31.13.92.14

Hoeveel zo’n pakketten zijn er dus?

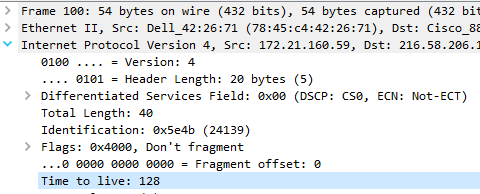
Antwoord = 92

Je kan dit getal ook terugvinden door statistische info over de capture-file op te vragen. Plak hieronder een screenshot van het venster waarin je deze info gevonden hebt en markeer dit getal.



1. Hoeveel routers kan pakket nr 100 nog passeren vooraleer het niet langer doorgestuurd zal worden?

Dat komt overeen met zijn TTL-waarde en deze is gelijk aan 128.



1. Welke IP-filter moet je invoeren om enkel de IP-pakketten te filteren die voor het TCP-protocol bestemd zijn?

ip.proto == 6

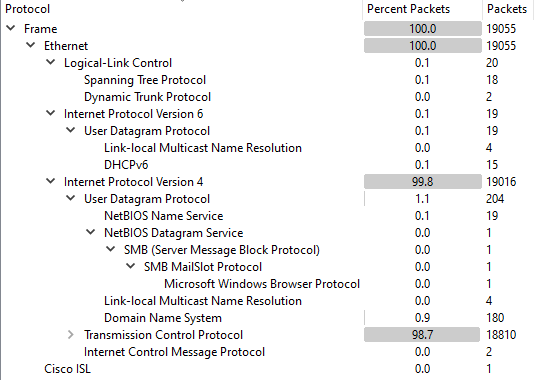
of eenvoudig:

tcp

Hoeveel zijn dat er dus?

18810

Je kan dit getal ook terugvinden via statistische info. Plak hieronder een screenshot van het venster waarin je dit gevonden hebt en markeer het gevraagde getal.



1. Filter de UDP-pakketten in de capturefile door gewoon *UDP* als filter in te voeren.

Bekijk de gefilterde pakketten om na te gaan welke waarde het protocol-veld van de IP-header van UDP-pakketten heeft en noteer die waarde hieronder.

17