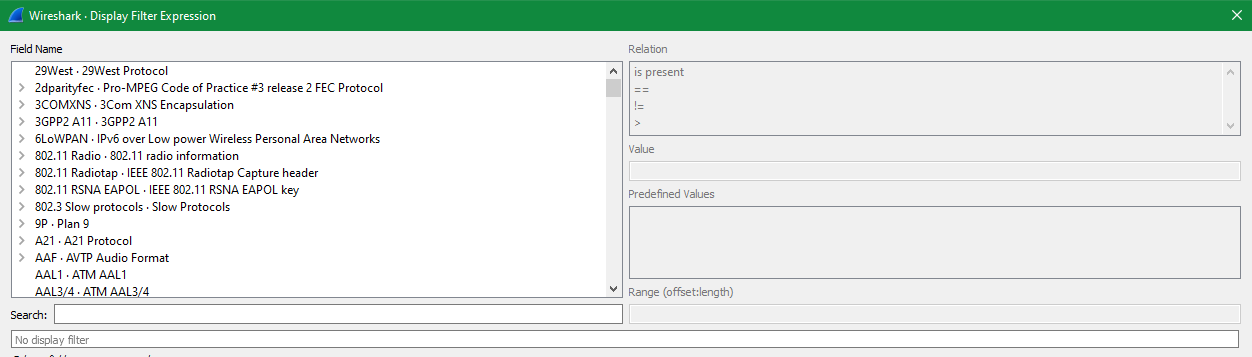
**­­­­­LABO 7**

**WIRESHARK FILTERING**

In dit labo leer je filters gebruiken in Wireshark.

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. Voer passende filters in om de volgende vragen te kunnen beantwoorden. **Vergeet ook niet om telkens de ingetikte filter onder de vraag te noteren.**

Tip 1: Je kan bij het opstellen gebruikmaken van de ingebouwde “Display Filter Expression” door rechts te klikken in het filtervakje en te kiezen voor “Display Filter Expression”.



Tip 2: Maak gebruik van de ingebouwde Wireshark manual pages (via Menu Help > Manual Pages > Wireshark Filter) voor bijkomende uitleg en voorbeelden van filters.

1. Hoeveel frames zijn er afkomstig van een device met MAC-adres 78:45:c4:42:26:71?

eth.src==78:45:c4:42:26:71

Antwoord = 3549

1. Hoeveel frames werden er uitgewisseld tussen de devices met MAC-adressen 78:45:c4:42:26:71 en 00:8e:73:88:a8:c8?

eth.addr==78:45:c4:42:26:71 and eth.addr == 00:8e:73:88:a8:c8

Antwoord = 19002

Tip: je kan dit antwoord controleren door statistische gegevens van de capture te bestuderen via het menu Statistics > Conversations.

1. Hoeveel broadcast frames werden er verstuurd?

eth.dst == ff:ff:ff:ff:ff:ff

alternatieve oplossing: eth.addr == ff:ff:ff:ff:ff:ff

Antwoord = 10

1. Wat is het pakketnummer van de laatste multicast frame waarin een IPv4-multicast-pakket voorkomt?

Tip: cfr PPT hoofdstuk 7 dia nr 9 voor de vorm van zo’n multicast-adres.

eth.dst[0:3]==01:00:5E

alternatieve oplossing: ip.addr >= 224.0.0.0

Antwoord = 13100

1. Hoeveel frames werden er vanaf een Cisco-device verstuurd?

Tip: maak gebruik van de OUI!

eth.src.oui\_resolved contains "Cisco"

Opmerking: om specifiek te zoeken op 00:8E:73 moet je deze omzetten naar een decimaal getal (36467) en volgende filter gebruiken: eth.src.oui == 36467 . Maar hiermee heb je nog niet alle Cisco frames. Immers, Cisco heeft meerdere OUI’s. In deze capture zitten er ook met OUI 94:d4:69 van Cisco.

Antwoord = 15487

1. Hoeveel IPv6-pakketten werden er verstuurd?

Tip: maak gebruik van het type-veld (cfr PPT hoofdstuk 7, dia nr 6 voor waarde van dit veld).

eth.type == 0x86dd

alternatieve oplossing: ip.version==6

alternatieve oplossing: ipv6

Antwoord = 19

Tip: ook dit antwoord kan je controleren door statistische gegeven van deze capture te bekijken!