# **Øving til Lagmodell og Wireshark**

Hensikten med øvingen er å bli kjent med Lagmodellen (forenklet 5-lag OSI) ved å analysere pakkefangst med Wireshark (WS).

**0. Få en hensiktsmessig pakkefangst**

Pakkefangst med Wireshark viser at det går en overveldende mengde pakker med mange ulike protokoller over trådløsnettet på campus, og sikkert også på hjemmenettet. Vi skal avgrense denne første undersøkelsen til en usikret HTTP-webside.

a. Start fangst i Wireshark: Når du starter Wireshark vises mange nettverkskort på din pc. Dobbeltklikk på nettverkskortet hvor det er aktivitet, mest sannsynlig Wi-Fi kortet.

b. Gjør oppslag på *datakom.no* eller annen webside som bruker usikret HTTP (ikke kryptert overføring HTTPS)

c. Sett display-filter i Wireshark ved å skrive HTTP. Feltet skifter farge til grønt når det er skrevet et lovlig filter. Nå skal bare et fåtall pakker vises, og hvis det er slik kan du stoppe videre pakkefangst.

A screen shot of a computer

Description automatically generated

**1. Undersøk protokollene i pakkene**

Wireshark viser ett pakkehode per linje for den pakken man studerer. Detaljene i pakkehodet vises ved å åpne denne linjen (>).

Når man markerer en protokoll-linje (pakkehode) viser Wireshark hvor stort pakkehodet er. Verdien kan leses nederst til venstre «på bunnlinjen».

Fyll inn tabell

1. Hvilke protokoller brukes for HTTP-pakkene?
2. Hvor hører disse protokollene til i Forenklet 5-lags OSI-modell?
3. Hvor stort er pakkehodet for hver protokoll?

|  |  |  |  |
| --- | --- | --- | --- |
| **Lagets navn** | **Protokoll** | **Lag nummer i lagmodell** | **Størrelsen på pakke-header (ant. byte)** |
| Lenkelag | Ethernet | 4 | 14 |
| Nettverkslag | Internet Protocol - IP | 3 | 20 |
| Transportlag \*) | Transmission Control Protocol – TCP | 2 | 32 |
| Appl.lag \*\*) | Hypertext Transfer Protocol - HTTP | 1 | 409 |

\*) TCP-SYN pakken har noen «options» som gjør dette pakkehodet noe større. SYN-pakkene inneholder ikke meldingsdata, men brukes bare for å etablere forbindelse  
\*\*) HTTP-meldingens størrelse avhenger av hvilken pakke man ser på, ulike parameterlengder

**3. Hvordan vet mottaker hvilken protokoll (prosess) på laget over som er mottaker av nyttelasten i pakken?**

Når en pakke kommer til mottaker skjer det motsatte av innpakking, pakkehodene blir skrelt av og innholdet (nyttelasten) sendt opp til laget over. Det kan være mange aktuelle protokoller på laget over så derfor har avsender for enkelhets skyld lagt inn beskjed om hvilken protokoll som er mottaker. «Har lagt inn» betyr at det er et felt i pakkehodet hvor denne informasjonen ligger.

1. Hva heter dette protokollfeltet på de ulike lagene og hvilken verdi har det?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lag | Gjeldende  Protokoll | Datafelt navn | Datafelt Verdi | Mottaker  protokoll |
| Lenkelag |  |  |  |  |
| Nettverkslag |  |  |  |  |
| Transportlag |  |  |  |  |

\*) sender og mottaker bruker forskjellige Portnummer, webtjener lytter på port 80

**4. Hvilken protokoll bruker navnetjenesten DNS på transportlaget?**

DNS (applikasjonlaget) kan velge blant to typer tjenester på transportlaget, enten pålitelig overføring med TCP eller upålitelig (best effort) med UDP.

Start Wireshark og sett display-filter «DNS». Vent til det dukker opp noen DNS-pakker, f.eks etter bruk av Nettleseren på ny webside, eller ved å pinge en webside fra CMD.

1. Hvilken protokoll er det DNS her benytter på transportlaget?

**5. Adresser**

1. Hvilken konfigurering har egen PC?

Pakker går mellom likestilte lag som kan befinne seg på ulike maskiner. Man må kunne identifisere kilde/avsender og destinasjon/mottaker på de ulike lagene. Derfor inneholder pakkehodene slike adresser. Man finner setting for egen PC slik: *Windows: kjør Ledetekst (eller CMD)*

* *>ipconfig* som viser IP-info for nettverkslaget
* *>ipconfig /all* for mer detaljer, blant annet MAC-adresser

Fyll inn tabell med hvilke adresser er din egen PC konfigurert med

|  |  |
| --- | --- |
| **Adressefelt** | **Verdi** |
| MAC-adresse |  |
| IPv4 |  |
| Default gateway IPv4 |  |
| Nettmaske |  |

1. Hvilke mottakeradresser sender din PC til?

Wireshark viser mottakeradresser (dst) i pakkene som sendes. Bruk kommando *CMD*>*ping* på et par webadresse mens Wireshark fanger. Finn mottakeradresser (dst) i pakkene som sendes. Fyll inn tabell:

|  |  |  |
| --- | --- | --- |
| **Ping på webadresse** | **Dst MAC (lenkelaget)** | **Dst IPv4 eller IPv6** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Hvilken enhet er det som har MAC-adressen som pakken sendes til?

For å finne/verifisere svaret kan man undersøke ARP-tabell på egen PC. Denne tabellen viser en oversikt som knytter MAC-adresser til aktuelle IP-adresser. Her vil det vises en «kjent» IP-adresse for denne MAC-adressen. Slik søker man egen ARP-tabell: Cmd>arp -a

Og enheten som har MAC-adressen hvor pakkene sendes til er: