# **Bli kjent med Wireshark**

**Læringsmål**

*Kunnskap: Forstå hvordan lagmodellen gjenspeiles i hver enkelt pakke som vises i Wireshark.*

Det betyr å kunne identifisere pakkehoder for protokoller på hvert lag i lagmodellen og inspisere hva de inneholder.

*Ferdighet: Kunne bruke Wireshark.*

Det betyr å kunne velge nettverkskort, kunne sette fangst- og displayfiltre og lagre fangsten. Videre må man også kunne finne frem til datafelter i hvert enkelt pakkehode og se disse i sammenheng med samlet kommunikasjon.

**Generelle tips**

*Hvordan unngå å «drukne» i uønsket pakkefangst*

Det blir fort mange pakker og derfor vanskeligere å finne informasjonen man søker. Noen tips:

* Tren på å bruke fangst- og displayfilter slik at de viser «akkurat» det du er på jakt etter.
* Ha færrest mulig aktive program som kjører på PC. Kjør bare en nettleser med bare en fane, ikke samtidig med Facebook eller mail eller andre program som hele tiden søker etter oppdateringer.
* Gjør tiden mellom start og stopp av pakkefangsten kortest mulig.

*Fange pakker på trådløst nett som sendes fra andre maskiner*

Nettverkskortet kan fange opp alle radiosignaler, på ulike kanaler og med forskjellig SSID. Dette er allikevel «problematisk/du får det ikke til» på Windows, fordi det krever installasjon av egen programvare som «overstyrer» nettverkskortet. På MAC og Linux kan det gå. (Søk på nettet)

*Hva kan man finne ut dersom man klarer å fange andres pakker på trådløst nett?*

Svaret avhenger av krypteringsalgoritmen som brukes på det trådløse nettet.

* Ukryptert: Kan lese innholdet i alle pakker
* WEP: Felles passord som er lett å hacke. Kan da lese alle pakker
* WPA2 (typisk hjemmenett): Må kjenne passord for nettet (vanskelig å hacke). Men på eget hjemmenett kjenner man jo passordet...
* WPA2 Enterprise: Individuelle passord, alle pakker er kryptert, også broadcastpakker. Eduroam kjører WPA2 Enterprise (Med autentisering av brukere)

*Hvordan er min egen PC konfigurert?*

Det er essensielt å kunne finne konfigurering av egen PC. Hvilken IP-adresse har jeg, hvor finner jeg DNS og hva er IP-adressen til min ruter (default gateway)? Og hvilket IP-nett er jeg koplet til?

På Windows finner du dette i *CMD>ipconfig /all*. På MAC må man selv finne ut av bruken.

**Oppgaver**

|  |  |  |
| --- | --- | --- |
|  | **Oppgavetekst** | **Merknader** |
| 1 | Installere programmet | Lastes ned fra wireshark.org. |
| 2 | Velge nettverkskort å fange pakker på | Merk at programmet må kjøres som administrator, ellers dukker det ikke opp nettverkskort å fange på. Virtuelle nettverkskort, som f.eks. kan brukes til VPN, er det også mulig å ta pakkefangst på. |
| 3 | Teste ulike *displayfilter* | Merk at gyldige filter vises i grønt. Ugyldige filter, som *HTTPS,* vises i rosa. Stopp fangsten og test displayfilter  *Porter/protokoller: HTTP, DNS, tcp.port==80*  *IP-adresser: ip.addr == <verdi>*  *Kombinasjon: HTTP and ip.addr==<verdi>* |
| 4 | Vise detaljert pakkehodeinformasjon for hver protokoll i en pakke | Åpne/ekspander pakkehodet i «midtseksjonen» på Wireshark for henholdsvis lenkelag (Ethernet), nettlaget (IP), transportlaget (TCP eller UDP) eller applikasjonslag (f.eks HTTP). |
| 5 | Sette *fangstfilter* for å fange pakker etter bestemte kriterier | Start fangst på nytt og test  *tcp port 80*  *host <ip-adresse>* |
| 6 | Følg en TCP-strøm med kommando *Analyze* | Marker en tilfeldig HTTP-pakke, velg *Analyze/Follow/TCP stream* og studer resultatet |
| 7 | Undersøk hvilke endepunkter (adresser) som har vært involvert i kommunikasjonen - *Statistics* | Velg *Statistics/Endpoints* og studer hvilke MAC-, IP- og portadresser som er brukt i under fangsten. Kryss av og på for «Name resoltion». |
| 8 | Lagre pakkefangsten (etter filtrering med displayfilter) | Etter at man har gjort et passe utvalg kan akkurat disse pakkene lagres og analyseres senere. Bruk **Fil/Export specified packets** (Ikke bare «lagre som») |