

Oppgaver til leksjon 2

Alle deloppgavene må gjøres for å få godkjent denne oppgaven.

Mange deloppgaver kan løses med kommandoen *nslookup*, som er demonstrert i leksjonen. Noen oppgaver trenger flere ulike oppslag.

Hvis du har problemer med å bruke *nslookup* på egen maskin, går det an å fjerninnlogge på NTNU sin studentserver og kjøre *nslookup* der i stedet. Det gjøres slik:

1. Åpne et terminalvindu. Såvidt jeg vet heter det «Terminal» på mac. På windows, `cmd.exe`.
2. Bruk kommandoen *ssh* for å koble til NTNU sin maskin:

```
ssh brukernavn@login.stud.ntnu.no
```

Brukernavnet er det samme som du bruker i blackboard. Du blir spurt om passord, passordet er også det samme som du bruker i blackboard.

Maskinen har *nslookup* installert, og det virker akkurat som i leksjonen. (Hvis du får andre svar enn jeg fikk, er det fordi Internettet har endret seg i mellomtiden.)

Når du er ferdig med å bruke studentserveren, avslutter du med kommandoen *logout*.

1. Hva er ip-adressene på de datamaskinene som kjører webtjenester for `www.toyota.no`? Og hva heter maskinene som har disse adressene?
 Tips: *nslookup* kan finne ut begge deler. Slå opp navnet, og gjør deretter reversoppslag på ip-adressene du får.
2. Hva er sammenhengen mellom SMTP og MIME?
3. Hvem skjuler seg bak ip-adressen `129.242.126.10`?
4. Hva er tittelen på RFC 822 og når ble den skrevet?
5. Hvem er sponsor for toppnivådomenet «.museum»?
6. Finn IPv6-adressen til «ntnu.no»
7. Hva er ASCII forkortelse for? Hvilket ASCII-tegn er representert ved verdien 80 (desimalt)?
8. Hva oppnår vi med at et domenenavn kan ha flere IP-adresser knyttet til seg?
9. Hvilke maskiner håndterer epost for «bank.no»? Hvilke prioriteter og ip-adresser har de?
10. Kan det være noen vits i å ha mange domenenavn på én IP-adresse? Forklar.
11. Bruke wireshark

- Start opp pakkefangst med wireshark, som du installerte i forbindelse med forrige øving.
- Send en e-postmelding til deg selv, med det e-post-programmet du vanligvis bruker.
- Når du mottar denne eposten, åpner du den for å lese den på vanlig måte.
- Stopp pakkefangsten.

Undersøk pakkene du har fanget, og gjør rede for hva du finner. Sjekk om meldingsteksten og annen relevant informasjon kan leses i de fangede pakkene. Eller ser det ut som eposten er kryptert? Var det dns-trafikk i forbindelse med postformidlingen?

Tips: epost bruker protokoller som smtp, og pop/imap. Web-baserte løsninger bruker https eller eventuelt http.

12. Hvorfor bør vi kjøre *utgående* epost gjennom spamfilter? Vårt firma driver jo ikke med slikt?
13. Bruk verktøyet nslookup, slå opp spf-records. Finn ut hvilke maskiner (ip-adresser) som har lov til å sende epost for adressa.no (Adresseavisa i Trondheim). Pass på å slå opp alle direktiver av typen redirect, include og mx, så du ikke går glipp av noen.