Tietoliikenteen perusteet 2, syventäviä tehtäviä 3

Syventävät tehtävät 1 ja 2 sisältävät joitakin tämänkin kurssi kannalta tärkeitä harjoituksia, mutta niiden painotus on kuitenkin edeltävässä tietoliikenteen perusteet 1 –kurssissa.

Nämä tehtävät kohdistuvat nimenomaan tietoliikenteen perusteet 2 –kurssin sisältöön. Tehtävät 1 ja 2 osioon 2.4, tehtävä 3, 4 ja 5 osioon 2.3. Tehtävä 6 laajentaa tähän asti opittuja esittelemällä uuden ominaisuuden ja edellyttää tietojen yhdistelemistä osista 1 ja 2 sekä tietoliikenteen perusteet 1 –kurssista.

1) Sähköposteista
   a) Oletetaan, että Alice käyttää omalla laitteellaan (läppäri, kännykkä) toimivaa sähköpostiohjelmaa ja Helsingin yliopiston sähköpostipalvelua. Alice lähettää sähköpostin Bobille, joka käyttää Oulun yliopiston sähköpostipalvelua. Bobin sähköpostiohjelma hakee sähköpostin palvelimelta käyttäen IMAP-protokollaa. Selitä, miten sähköposti kulkee Alicen sähköpostiohjelmasta ensin Alicen palvelimelle ja sieltä edelleen Bobin palvelimelle. Mitä muita sovelluskerroksen protokollia mahdollisesti tarvitaan?
   b) Mitä tarkoittaa sähköpostitietojen kalastelu (phishing)? Mistä sen voi havaita? Miten siihen pitää reagoida? (Tausta-aineistona voisi toimia vaikkapa Kyberturvallisuuskeskuksen katsaus: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/katsaus-sahkopostitunnusten-kalastelusivustoihin)
   c) Tarkastele muutaman itsellesi saapuneen sähköpostiviestin täydellisiä otsakkeita. (Eri ohjelmissa nämä löytyvät eri tavoin – esim. view souce, full headers ja joistakin niitä voi olla lähes mahdotonta saada). Etsi otsakkeista rivit 'Received:'. Kuinka monta niitä tyypillisesti näissä viesteissä on? Käy läpi myös ainakin yhden viestin kaikki otsakerivit ja selvitä itsellesi mitä ne tarkoittavat.

2) SMTP
   a) HTTP protokolla on tilaton, koska palvelimen ei tarvitse tietää aiempaa viestihistoriaa, vaan se voi käsitellä jokaisen saapuvan pyynnön täysin itsenäisenä. Onko SMTP tilaton, kun asiakkaan ja palvelimen välillä kulkee useita viestejä? Miten tämä vaikuttaa ohjelman toteutukseen?
   b) SMTP protokollassa on viestit/komennot HELO ja MAIL FROM. Ovatko ne molemmat välttämättömiä? Miksi?
   c) Mitä eroa on SMTP protokollan MAIL FROM viestin/komennon ja sähköpostin FROM kentän välillä? Miksi ne molemmat tarvitaan?

3) Whois tietokanta
   a) Mikä on whois tietokanta? Millaista tietoa sieltä voi olettaa löytyvän?
   b) Selvitä Traficomin tietokannasta https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset/whois-palvelu-nayttaa-verkkotunnuksen-julkiset-tiedot Helsingin yliopiston autorisoitujen nimipalvelijoiden nimet ja IP-osoitteet. Mitä muuta tietoa sait?
   c) Miten edellisen kohdan tiedot eroavat fi-verkkotunnushaun (löydät sivulta https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset) antamista tiedoista?
   d) Selvitä Traficomin whois-palvelulla mit.edu:n tietoja. Miltä whois-palvelimelta tiedot tulivat?
   e) Mitä merkitystä whois tietokantojen tietojen julkisuudella on? Pitäisikö niiden olla julkisia vai salaisia?

4) Nimipalvelukyselyjä – tee joukko nimipalvelukyselyjä ja selvitä seuraavia asioita
   a) nslookup – yksinkertainen työkalu (linux, windows)
      i) Tee nslookup kysely jokaisesta helsinki.fi alueen autoritäärisestä nimipalvelijasta ja kysy niihin liittyvien A, NS ja MX tietueiden sisältöjä. Huomaa, että kaikkia ei välttämättä ole.
      ii) Tee vastaavat kyselyt osoitteista mooc.fi ja yle.fi. Mitä yllättävää näissä on?
   b) dig – monipuolisempi ja tarkemmin hallittava työkalu (linux, ei windows)
      i) Selvitä itse vaiheittain dig komennolla www.helsinki.fi:n IP-osoite aloittaen jostain juurinimipalvelijasta [a-m].root-servers.net ja edeten vaiheittain vastaukseen asti. Kuinka monta kyselyä teit?
      ii) Selvitä vastaavasti www.bbc.co.uk nimeen liittyvä IP-osoite. Montako kyselyä nyt tarvitsit?

5) Internetin päätöksen teko. Internetiin liittyviä päätöksiä tehdään erilaisissa organisaatioissa. Alan ammattilaisen on hyvä tunnistaa nämä organisaatiot ja niiden tehtävät.
   a) Mistä asioista IANA (www.iana.org) huolehtii ja mitkä ovat sen tehtävät?
   b) Entä ICANN (etsi about ICANN sivulta www.icann.org)?
   c) Miten IETF (ietf.org) liittyy Internetin päätöksen tekoon? Mitä se tekee?

6) Videokuvan lähettäminen HTTP:llä on varsin tavallista. Yhä useammalla www-sivulla on videolinkkejä. Tähän on käytännössä kaksi kilpailevaa menetelmää MPEGin Dynamic Adaptive Streaming over http (DASH) ja Applen HTTP Live Streaming. Kummassakin on sama perusidea, johon tutustutaan tässä tehtävässä. Tavoitteena on siis tarjota videopalvelu, joka mukautuu käyttäjän kapasiteettiin. Tämä tehdään tyypillisesti niin, että palvelimella on N versiota videokuvasta (joilla on N erilaista kuvataajuutta ja laatua) ja M versiota äänestä (kaikki eri koodaustaajuuksia ja laatuja). Oletetaan nyt, että mediasoitin (media player) voi koska tahansa valinta minkä tahansa yhdistelmän näistä kuva- ja ääniversioista.
   a) Kuinka monta mediatiedostoa (kuva ja ääni yhdessä) palvelimelle täytyy tallettaa, jotta palvelin voi millä tahansa hetkellä lähettää yhdessä ja samassa suoratoistosignaalissa (streaming media) sekä kuvan että äänen? Kullakin mediatiedostolla on siis oma muista poikkeava URL.
   b) Entä jos palvelin lähettää kuva- ja äänisignaalin erikseen ja mediasoitin yhdistää nämä signaalit. Kuinka monta tiedostoa tässä tapauksessa palvelimelle pitää tallettaa?

☆ Ylimääräinen tehtävä: Jos sähköpostiprotokollan toiminta kiinnostaa tarkemmin, niin tutustu Wiresharkin avulla mallitiedostoon smtp.pcap (http://wiki.wireshark.org/SampleCaptures).
Se sisältää sähköpostin protokollan kaappauksen. Siirron aikana tapahtuu myös muutama verkkovirhe, joten kaappauksessa on myös uudelleenlähetyksiä. Tarkastele SMTP protokollan toimintaa. Montako ko. protokollan viestiä vastaanottava postikone lähettää? Mitä viestejä ne ovat? Mitkä viestit sisältävät lähetetyn sähköpostin varsinaisen sisällön? (TCP:n tavuvirran voi saada näkyville 'Follow TCP stream' valinnalla, tällöin ei enää näytetä verkkokerroksen pakettijakoa.)