# Case 1. Tietovuodon analysointi

# Johdanto

Tehtävässä analysoidaan erästä tapahtumaa käyttäen hyväksi tapahtuma-ajalta tehtyä verkkoliikenteen kaappausta. Analysointiin tarvitset Wireshark-ohjelman. Kaappaus on tiedostossa, jonka voi ladata tästä linkistä:

<https://www.dropbox.com/s/19wqzea2sro0o9h/CyberOps_case1.pcapng?dl=0>

<https://www.dropbox.com/s/19wqzea2sro0o9h/CyberOps_case1.pcapng?dl=0>

Tehtävään saa ohjausta tuntien yhteydessä (ja sitä mahdollisesti tehdään tunneilla).  Tehtävää saa toki tehdä itsenäisesti etu- tai jälkikäteen ja tehtävästä saa vaihtaa tietoja muiden opiskelijoiden kanssa mutta toivottavaa on, että toisille annettaisiin ennemmin selvittämiseen liittyviä vihjeitä kuin suoria ratkaisuja (älä pilaa toisilta onnistumisen mahdollisuutta)! Tehtävän voi myös tehdä pareissa (tai pienessä ryhmässä) mutta jokaisen tulee silti tehdä oma palautus.

Tehtävänannon lopussa on vinkkejä (jos niitä kaipaa) sekä palautusohje. Tehtävän voi ratkaista lukuisilla erilaisilla tavoilla ja vinkit ovat vain yksi keino.

# Tehtävä

Ratkaise seuraava skenaario analysoimalla annettua pcap-tiedostoa. Analyysin perusteella kirjoita lyhyt mutta tarkka kuvaus siitä, mitä skenaariossa on tapahtunut (maks. 2 sivua, pdf-muoto). Tue analyysiä ottamalla raporttiin mukaan täsmällisiä sopivia kaappauskuvia pakettianalysoinnista. Palauta raportti palautuskansioosi (ks. palautus) ja merkitse tehtävä suoritetuksi.

Analysointiin riittää Wireshark-ohjelma mutta muitakin työvälineitä saa halutessaan käyttää. Mikäli käytät muita ohjelmia, niin mainitse ne raportissa.

## Skenaario

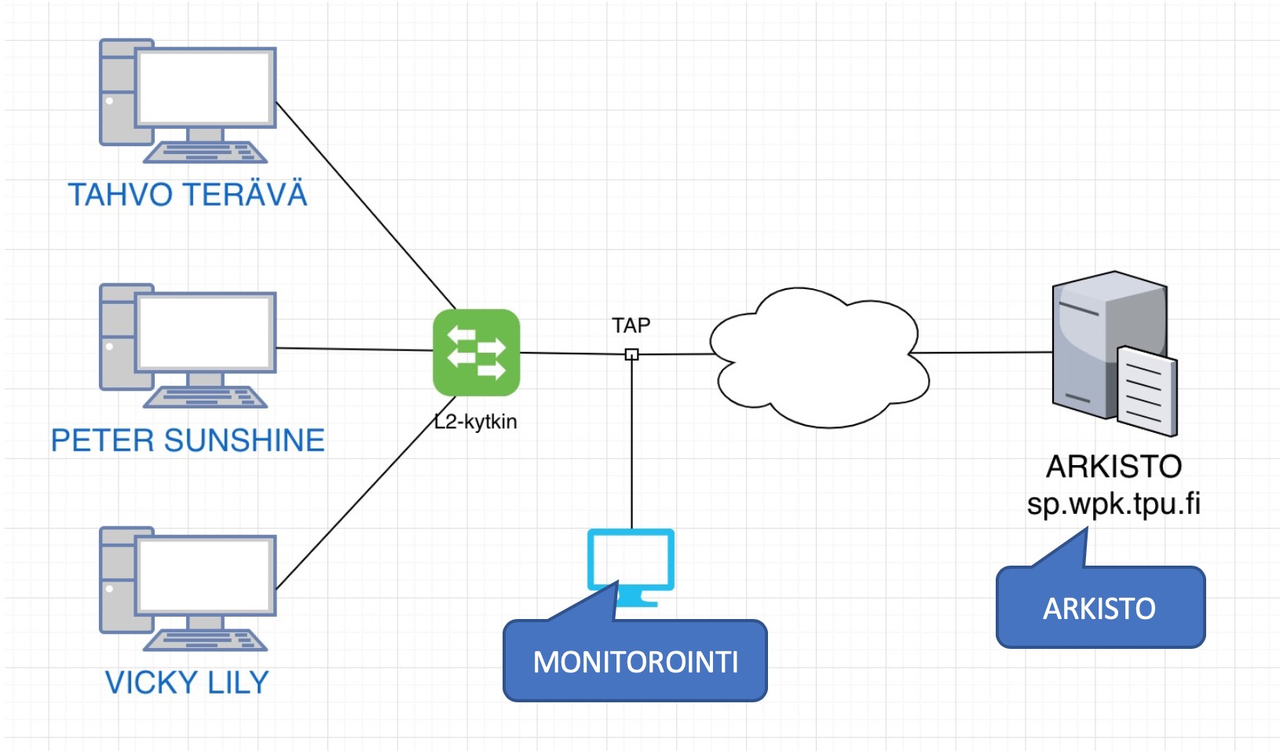
Eräs yhtiö on hävinnyt monta tarjouskilpailua ulkomaiselle kilpailijalleen. Yhden hävityn tarjouskilpailun jälkeen yrityksen edustajien tietoon saatettiin asioita, jotka saivat heidät epäilemään, että yrityksen luottamuksellista tietoa (tehtyjen tarjouksien yksityiskohtia) on vuotanut kilpailijalle.

Yrityksellä on arkistointijärjestelmä, jonne luottamukselliset dokumentit arkistoidaan kuvatiedostoina (.jpg). On herännyt epäily, että tietovuodot liittyvät arkistointijärjestelmään tallennettuihin dokumentteihin.

Yrityksen verkon liikennettä oli seurattu tekemällä osittaisia liikennekaapauksia (PCAP-tiedostoja). Yhdessä tiedostossa näkyy liikennettä, joka ajoittuu hetkeen, jolloin epäillään tietoja vuodetun.

Oheisesta kuvasta selviää verkon topologia, kyseisenä aikana konttorilla olleet työntekijät sekä muut tarpeelliset tiedot. Arkistointijärjestelmän toimialuenimi on sp.wpk.tpu.fi.

**Tehtävänä on saada selville, mitä on tapahtunut?**



**Haaste**: saatko selvitettyä, minkä nimisestä firmasta skenaariossa on kyse. Vinkki: tieto löytyy yrityksen tekemästä tarjouksesta.

## Vinkit etenemiselle

Tässä muutama vinkki siihen, kuinka pcap-tiedostoa voisi ryhtyä analysoimaan:

1. Yritä selvittää laitteiden IP-osoitteet. Aloita arkisto-palvelimesta. Se on ainoa laite, josta sinulla on jokin varma tieto jo olemassa. Hyödynnä tuota tietoa. Mikä on arkisto-palvelimen ip-osoite?
2. Selvitä käyttäjistä, kuka on käyttänyt mitäkin työasemaa (IP-osoite) ja mitä he ovat tehneet (noin suurin piirtein).
3. Selvitä, millaista liikennettä arkistopalvelimen ja käyttäjien työasemien välillä on ollut. Kuka on kirjautunut järjestelmään? Kuka on ladannut tiedostoja? Mitä tiedostoja?
4. Lopuksi huomioi vielä, että kaikki ei välttämättä ole niin miltä ensin näyttää… ;-)
5. Haaste-osuus: kaappauksesta pystyy erottamaan ladatun tiedoston ja tallentamaan sen erillisenä (huom. jpg-tiedostomuoto).

## Vinkkejä Wiresharkiin

Tässä muutamia vinkkejä kuinka analyysi voi alkaa tekemään Wiresharkilla:

1. Pyri suodattamaan kaappausta erilaisilla suodattimilla aina sopivasti
2. Hyvä alkukohta suodattimille on valikko Statistics:
   1. Statistics → Protocol Hierarchy
   2. Statistics → Conversations
   3. Statistics → Endpoints
3. Valitse noiden valikkojen kautta kiinnostava asia ja hiiren kakkospainikkeella aseta siihen liittyvä suodatin.
4. Suodata lisäksi ainakin IP-osoitteilla…

# Palautus

Palauta tekemäsi analyysi opintojakson palautuskansioon ja merkitse se suoritetuksi. Jokaisen tulee palauttaa oma selvitys vaikka tehtävän olisikin tehnyt yhteistyössä toisten kanssa. Selvityksessä on hyvä mainita kenen kanssa työ on tehty.

LOPPU