OPINNÄYTETYÖ

MIIKA PAKANEN 2012

TIETOKONEEN ETÄHALLINTA YRITYS- JA KOTIKÄYTÖSSÄ

TIETOJENKÄSITTELYN KOULUTUSOHJELMA

ROVANIEMEN AMMATTIKORKEAKOULU

LUONNONTIETEIDEN ALA

Tietojenkäsittelyn Koulutusohjelma

Opinnäytetyö

TIETOKONEEN ETÄHALLINTA YRITYS- JA KOTIKÄYTÖSSÄ

Miika Pakanen

2012

Ohjaaja Martti Kemppainen

Hyväksytty _____2012_____

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

Luonnontieteiden ala
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön tiivistelmä

Tekijä	Miika Pakanen	Vuosi	2012
Työn nimi	Tietokoneen etähallinta yritys- ja kotikäytössä		
Sivu- ja liitemäärä	58 + 2		

Opinnäytetyössäni oli tarkoitus tutkia tietokoneen etähallinnan käyttöä koti- ja yritysympäristössä. Tavoitteenani oli kertoa mitä tietokoneen etähallinta on, selvittää millä eri tavoin sitä hyödynnetään yrityskäytössä sekä tutkia tietokoneen etähallintaa kotikäytössä.

Käyttämäni lähdeaineisto on suurimmaksi osaksi verkkoaineistoa, koska kirjallisuutta kyseisestä aiheesta on vaikea löytää.

Opinnäytetyö alkaa teoriaosuudella, jossa kerrotaan yleisesti tietokoneen etähallinnasta ja sen tietoturvasta. Teoriaosuuden tarkoituksena on selvittää lukijalle kuva siitä, mitä tietokoneen etähallinta on, mitä se vaatii ja mihin sitä käytetään sekä kertoa tietokoneen etähallinnan erilaisista tietoturvamenetelmistä. Teoriaosuuden jälkeen tulee yritysosuus, jossa tutkimuksen pääkohteena oli Lapin ammattiopiston Kairatien toimipiste. Kävin tutustumassa paikan päällä Kairatien toimipisteeseen ja sen eri etähallintamenetelmiin sekä haastattelemassa toimipisteen IT-tukihenkilöä. Lisäksi haastattelin kahden muun yrityksen IT-henkilöitä. Viimeisenä osuutena tutkin tietokoneen etähallintaa kotikäytön kannalta. Valitsin kaksi etähallintaohjelmaa, jotka soveltuvat kotikäyttöön, TeamViewer- ja NetOp Remote Control -ohjelman. Testasin ja tutkin näitä kahta ohjelmaa kahdella tietokoneella, jotka toimivat eri verkossa.

Opinnäytetyöprosessin lopputuloksena syntyi reilun 50 sivun mittainen raportti tietokoneen etähallinnasta. Raportti koostuu teorian avulla johdetusta tietokoneen etähallinnasta yritys- ja kotikäytössä.

Avainsanat: tietokoneen etähallinta, etätuki, etäyhteys, tietokoneen etähallinnan tietoturva

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

School of Business
And Administration
Business Information
Technology
Programme

Abstract of Thesis

Author Miika Pakanen Year 2012

Subject of thesis Remote control of the computer in a home environment and in a company environment.

Number of pages 58 + 2

The objective of this study was to examine the use of a remote control for a computer in a home environment and in a company environment. The purpose was to explain: what is the remote control of the computer, to clarify in how many different ways it is utilized in a business, and to study two remote control programs in a home use.

The data for this study is mostly sourced from the internet because it is difficult to find literature about the subject in question.

The thesis begins with the theoretical section in which it is generally explained about the remote control of the computer and about its information security. In the theoretical section the purpose is to clarify to the reader what the remote administration of the computer is, what it requires and where it is used and to describe the different information security methods of the remote administration of the computer.

The next section is methodological concerned with the company part in which the subject of the study was the Kairatie office of the Vocational College of Lapland. I became acquainted with the Kairatie office and its separate remote control method and I interviewed the IT-support person there. I also interviewed two other IT-support persons at two different companies. Finally, I studied the remote administration of the computer in home use. I chose two remote control programs which were suitable for home use. These programs were the TeamViewer and the NetOp RemoteControl. I examined these two programs with two computers which operated on a separate network.

The final result of the study process was to compile a fifty pages long report about computer's remote management. The report detailed a theory about the use of the remote control of the computer in a home environment and in a company environment.

Keywords: computer for remote control, remote management, remote assistance, remote access, computer for remote control security

SISÄLTÖ

KUVIOLUETTELO

1 JOHDANTO

Tietokoneiden etähallinta on yksi tärkeimpiä menetelmiä, mitä tarvitaan yritysten IT-lähituki ja ylläpitotehtävissä. Etähallintaohjelmat ovat nykyään kysyttyjä ja yleistyvät jatkuvasti, varsinkin yrityskäytössä. Tietokoneen etähallinta liitetään monesti pelkkään yritystoimintaan, mutta myös kotikäytössä sitä voidaan hyödyntää. Silti moni tavallinen kotikäyttäjä ei välttämättä ole koskaan edes kuullut niiden olemassaolosta. Tämän työni yksi tarkoitus onkin perehdyttää ihmisiä etähallintaan ja sen käyttöön.

Tutkin tässä työssäni etähallinnan käyttöä ja sen monipuolisuutta niin yrityskuin kotikäytössäkin. Tavoitteenani on selvittää, millä eri tavoin etähallintaa hyödynnetään yrityskäytössä sekä tutkia ja vertailla kahta etähallintaohjelmaa kotikäytön kannalta. Käyttämäni lähdeaineisto on suurimmaksi osaksi verkkoaineistoa, koska kirjallisuutta kyseisestä aiheesta on todella harvassa.

Jaoin tämän opinnäytetyön neljään osioon. Ensimmäisessä vaiheessa kerron etähallinnan teoriasta eli yleisesti siitä, mitä etähallinta on, mitä se vaatii ja mihin sitä käytetään. Etähallintaa käyttäessä on tärkeää muistaa myös tietokoneiden tietoturva, josta kerron toisessa osiossa. Kolmannessa vaiheessa tutkin etähallinnan käyttöä yrityksessä. Tutkimuksen kohteena on Rovaniemen ammattiopiston Kairatien toimipiste. Kyseisessä toimipisteessä on 550 tietokonetta joita hoitaa paikan päällä vain yksi IT-tukihenkilö (Sassi 2012). Näin etähallinnan osuus on merkittävä laitoksen IT-tuki toiminnassa. Kävin tutustumassa tämän laitoksen etähallintamenetelmiin ja haastattelemassa yksikön IT-tukihenkilöä. Lisäksi suoritin lyhyen sähköpostihaastattelun Lappset- ja LapIT-yrityksille koskien yrityksen tietietokoneiden etähallintaa.

Viimeiseksi tutkinnan kohteeksi valitsin etähallinnan kotikäytössä. Kotikäytössä etähallinta ei ole niin yleistä, mutta silti sitä pystytään hyödyntämään kotonakin monin eri tavoin. Valitsin kaksi etähallintaohjelmaa jotka soveltuvat kotikäyttöön, TeamViewer- ja NetOp Remote Control -ohjelman. Testasin ja tutkin näitä kahta etähallintaohjelmaa kahdella tietokoneella, jotka toimivat eri verkossa.

Opinnäytetyön aiheeksi valitsin tietokoneiden etähallinnan siksi, koska se on kiinnostanut minua suuresti aina. Yksi merkittävistä tekijöistä aiheen valin-

nassa oli myös se, että suoritin aiemmin työharjoitteluni Rovaniemen ammattiopiston Kairatien toimipisteessä. Sain tutustua harjoitteluni aikana tietokoneen etähallinnan toimintaan ja sen tuomiin moniin mahdollisuuksiin. Toimipisteen IT-tukihenkilö antoi mahdollisuuden toteuttaa yritysosuuteni heidän yksikössään, jonka myöhemmin toteutin tehdessään tätä opinnäytetyötä. Kotikäytössä TeamViewer-ohjelma on minulle jo entuudestaan pinnallisesti tuttu, joten se oli luonteva valinta toiseksi kotikäyttöohjelmaksi. NetOp-ohjelman valitsin puolestaan opettajan kehotuksesta.

2 TIETOKONEEN ETÄHALLINTA

2.1 Mitä on tietokoneen etähallinta?

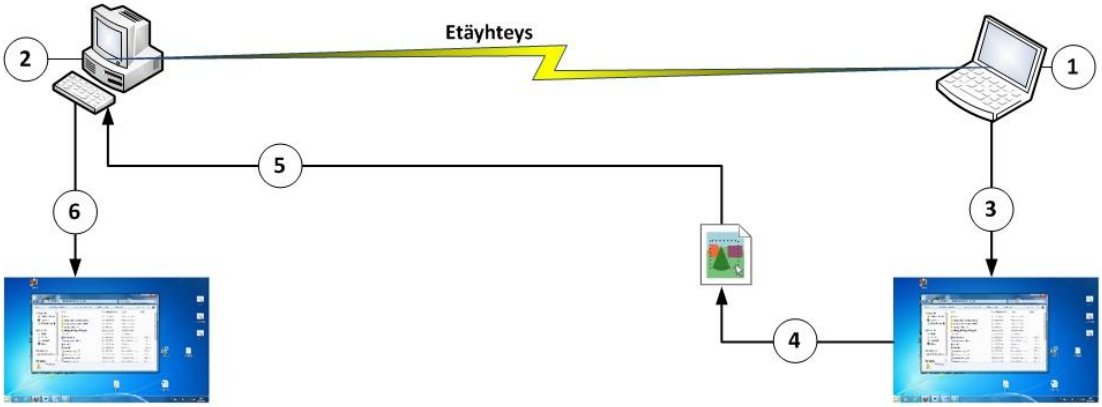
> ”Hankin eräille tutuille alkuvuodesta uuden tietokoneen, kun heidän vanhasta meni ilmeisesti emolevy. Heidän tietokoneen käyttötaitonsa rajoittuvat lähinnä selaimen ja tekstinkäsittelyohjelman käyttämiseen. Heitä on täytynyt neuvoa usein koneen käytössä ja tuli mieleeni jonkinlaisen etähallintaohjelman asentaminen. Välimatkaa on 20 kilometriä ja ei kannata lähteä paikan päälle parin minuutin hommaa varten. Siis, onko mitään sopivaa ohjelmaa tähän tarkoitukseen?” (Haveri 2011.)

Näin kysyy nimimerkki Mika Haveri Tietokonelehden keskustelupalstalla internetissä. Ja hän ei ole ainoa kyselijä, monet muutkin ihmiset ovat kiinnostuneita etähallinnasta. Silti on monia tavallisia kotikäyttäjiä, jotka eivät välttämättä ole koskaan edes kuullut niistä. Monille kotikäyttäjille sana etähallinta saattaa aiheuttaa jo käsitteenä epäilyttäviä mielikuvia ja muodostuu käsitys, että etähallinta on laitonta ja vaarallista. Mitään laitonta siinä ei kuitenkaan ole, kunhan käyttäjät muistavat tietosuojakäytännöt ja käyttävät sitä oikein.

Etähallinta tarkoittaa menettelyä, jossa yhdistetään kaksi eri tietokonetta niin, että yhdestä tietokoneesta voidaan tarkastella ja hallita myös toista tietokonetta, sen tiedostoja, toimintoja ja koko käyttöjärjestelmää. Yleensä on kaksi yleistä syytä mihin etähallintaa käytetään. Tietokone-avustajat voivat etähallinnan avulla käyttää ja hallita tietokonetta, ohjata ja opastaa käyttäjää, asentaa ja päivittää ohjelmia ja etsiä ratkaisuja ongelmiin. Nämä toimenpiteet ovat hyvin yleisiä yrityskäytössä. Etähallintaa voidaan käyttää myös tilanteessa, kun ihmiset ovat poissa kotoaan. Etähallinnan avulla he voivat etsiä tietoja, joita heillä on tallennettuna kotona tietokoneelle. (Lacoma 2012.)

Vaikka etähallinta kuulostaa monimutkaiselta, etäkäytön prosessi on silti hyvin yksinkertainen. Tämä prosessi on kuvattuna kuviossa 1. Etähallintaohjelmat määrittävät palvelimena toimivan tietokoneen (1), johon asiakastietokone (2) voi ottaa yhteyttä. Palvelinkone kaappaa näyttökuvan oman tietokoneensa ruudusta (3), pakkaa sen jollakin pakkausmenetelmällä joka voidaan helposti siirtää verkossa (4) ja lähettää tämän pakatun kuvan asiakaskoneelle (5). Asiakaskone purkaa sitten tämän pakatun kuvan takaisin luettavaan

muotoon ja palvelinkoneen näyttö näkyy asiakaskoneen etähallintaohjelmassa (6). Palvelinkone suorittaa tämän prosessin useita kertoja sekunnissa. Tuloksena on jatkuvasti päivitetty kuva, joka näyttää mitä toisessa tietokoneessa tapahtuu. Muut ominaisuudet antavat hiiren ja näppäimistön hallintaan. (Lacoma 2012.)



Kuvio 1. Etäkäytön prosessi.

Tämä nimimerkki Mika Haverin internet-palstalle kirjoittama teksti on aika hyvä esimerkki siitä, kuinka hyvin etähallintaa voidaan käyttää kotikäytössä. Sopivalla etähallintaohjelmalla voidaan antaa etätukea omalta tietokoneelta käsin, eikä tarvitse näin lähteä paikan päällä käymään.

Etähallintaan on olemassa useita erilaisia ohjelmia. Yleisesti etähallintaohjelmasta ladataan sovellus molempien käyttäjien tietokoneille. Ohjelmia on monentasoisia ja hintaisia, riippuen ohjelmiston laadusta. (Lacoma 2012.)

Etähallintaa voidaan käyttää myös selainpohjaisesti. Hallittava tietokone toimii www-palvelimena, johon voi muodostaa yhteyden miltä tahansa tietokoneelta tavallisella html-selaimella. Etähallinta onnistuu hitaallakin yhteydellä ja ilman erillisiä ohjelmia. Nämä versiot ovat todennäköisemmin vapaita sovelluksia, mutta myös todennäköisesti haavoittuvia ja alttiita viruksille. (Lacoma 2012.)

Nykyään yhä suurenemassa määrin voidaan käyttää etähallintaa myös matkapuhelimen ja tietokoneen välillä. Älypuhelimet ovat ominaisuuksiltaan samanlaisia kuin kannettavat tietokoneet. Keskitetyn etähallinnan avulla palveluntarjoaja tai asiakasorganisaation IT-tuki voi hallita työntekijöiden älypuhelimia ja PDA-laitteita keskitetysti, langattomasti ja ilman loppukäyttäjän osal-

listumista (Suomen mobiilitieto Oy 2012). Mobiililaitteelle asennettavan sovelluksen avulla taas voi ohjata etätietokoneita sekä siirtää tiedostoja etätietokoneen ja mobiililaitteen välillä (TeamViewer 2012a).

Etähallinnan perusperiaate on siis, että tietokoneella voidaan hallita toista tietokonetta ilman, että kenenkään tarvitsee itse olla fyysisesti paikalla sen toisen tietokoneen luona. Tämä säästää huomattavasti aikaa ja resursseja.

2.2 Muut käyttömahdollisuudet

Etäyhteydellä avulla voidaan tehdä myös paljon muutakin kuin pelkkää etähallintaa. Yksi merkittävimmistä etäyhteyksistä on VPN-yhteystekniikka (Virtual Private Network), joka muodostaa salatun yhteyden kahden tietokoneen tai lähiverkon välille. VPN-yhteyksiä käytetään yleisimmin yrityksissä, joilla on etätyöntekijöitä. Etätyöntekijät voivat ottaa yrityksen lähiverkkoon yhteyden kotoaan tai muualta yrityksen verkon ulkopuolelta VPN-yhteyttä käyttäen ja muodostavat näin "läpinäkyvän", salatun tunnelin etätyöntekijän ja yrityksen lähiverkon välille. Käytettäessä VPN-yhteyttä etätyöntekijälle näkyy yhdistämisen jälkeen koko yrityksen lähiverkko täysin samanlaisena, kuin se näkyisi, jos hän olisi kytkeytyneenä yrityksen lähiverkkoon paikan päällä. VPN-yhteyden avulla etätyöntekijän on mahdollista käyttää yrityksen lähiverkon julkisia hakemistoja ja palveluja omalta tietokoneelta käsin. (Afterdawn 2012.)

Jossakin tietyllä palvelimella voi olla ohjelmia, tekstejä, kuvia, tai muita tiedostoja, joita täytyy saada siirrettyä omalle tietokoneelle. Tai vaihtoehtoisesti täytyy omia tiedostoja saada siirrettyä palvelimelle. Tässä tapauksessa on kysymys yleensä siitä, että käyttäjä siirtää tekemänsä verkkosivut yrityksen palvelimelle. FTP (File Transfer Protocol) on yleisesti käytetty menetelmä tiedostojen siirtoon kahden tietokoneen välillä. FTP:tä käytetään yleisesti isompien tiedostojen välittämiseen verkon yli ja mm. verkkosivujen / kotisivujen hallinnointiin. FTP-palveluja voidaan käyttää aina niihin tarkoitetuilla FTP-ohjelmilla. Julkisia FTP-palveluja voidaan käyttää myös www-selaimilla. (Microsoft 2012d.)

Eräs mielenkiintoisimmista etäkäyttömenetelmistä on ns. etäaktivointi, joka mahdollistaa samassa lähiverkossa olevan tietokoneen käynnistämisen etäyhteyden kautta. Tämä tapahtuu niin, että kun käyttäjä lähettää sammuk-

sissa olevaan etätietokoneeseen erityisen Magic-tietopaketin, etätietokoneen verkkosovitin käynnistää tietokoneen. Tietokoneen verkkosovitin ”kuuntelee” koko ajan verkkoa, vaikka tietokoneen virta olisikin katkaistuna. Näin kun Magic-paketti saapuu, on verkkosovitin ”hereillä” ja pystyy käynnistämään tietokoneen. Tätä lähiverkkostandardia kutsutaan nimellä Wake On Lan (WOL). Wake On Lania käyttävät yleensä IT-tuki etäylläpitoa varten. Magic-paketin vastaanottavassa tietokoneessa on oltava Wake On Lania tukeva emolevy, verkkosovitin, sovittimen ohjain ja BIOS-järjestelmä. (Microsoft 2012e.)

2.3 Protokollat

Jotta etähallinta on mahdollista, tarvitsevat verkossa olevat eri valmistajien tekemät laitteet tiettyjä käyttäytymismalleja eli protokollia voidakseen kommunikoida keskenään. Etäyhteyksiin on olemassa useita kehitettyjä protokollia, joiden toiminta vaihtelee sen mukaan, mille käyttöjärjestelmälle kyseinen protokolla on kehitetty. Protokollat tarjoavat etähallintaohjelmille säännöt yhteyden muodostamiselle ja kommunikoinnille. Etähallintaan ei ole suunniteltu vakiintunutta protokollaa, vaan jokaiselle ohjelmalle on ohjelman valmistaja kehittänyt omanlaisen protokollan. Käytössä olevia yleisimpiä etäyhteysprotokollia ovat mm. vapaa VNC-protokolla (Virtual Network Computing) ja Windowsin RDP-protokolla (Remote Desktop Protocol). (The Free Directonary 2012.)

VNC on tietokoneen graafiseen etäkäyttöön tai pelkkään etäkatseluun tarkoitettu protokolla. VNC-protokolla on avoin ja alustariippumaton ja sitä tukevia palvelin- ja asiakasohjelmistoja löytyy kaikille yleisimmille käyttöjärjestelmille. Näin se tarjoaa asiakkaalle mahdollisuuden muodostaa yhteys palvelimeen mistä vain, paikasta riippumatta. VNC-protokolla ei myöskään vaadi suuria vaatimuksia asiakasohjelmalta eikä verkkoyhteydeltä. VNC-protokolla perustuu toiseen protokollaan, RFB-protokollaan (Remote Frame Buffer). Eri VNC-versiot ovat yhteensopivia toistensa kanssa, vaikka monissa versioissa on omia parannuksia. Tunnetuimpia versioita ovat RealVNC ja TightVNC. (Linux 2012.) Myös tämän työn kotikäyttö osiossa käytetty etähallintaohjelma TeamViewer perustuu VNC-protokollaan.

Microsoftin kehittämä RDP-protokolla on etäyhteyksien luomiseen Windows-käyttöjärjestelmissä tarkoitettu protokolla. Se perustuu ITU T.120 perheeseen. RDP on monikanavainen protokolla, joka pystyy tuottamaan virtuaalisia kanavia. Näiden virtuaalisten kanavien kautta voidaan kuljettaa laitteistojen käskyjä ja dataa, sekä mahdollistaa koodatut tiedot näppäimistöstä ja hiirestä. (Microsoft 2012a.)

Mainittujen protokollien lisäksi on myös muita vähän harvinaisempia protokollia. Esimerkiksi ARD-protokolla (Apple Remote Control) on vain MAC-käyttöjärjestelmille tarkoitettu protokolla. Se on Applen mukaan paras tapa hallita verkossa olevia MAC-laitteita (Apple 2012). X11-protokolla on taas Unix-käyttöjärjestelmille suunniteltu protokolla, joka mahdollistaa graafisen etäyhteyden sovelluksiin (Lineback 2012).

3 TIETOKONEEN ETÄHALLINNAN TIETOTURVA

3.1 Yleistä tietoturvasta

Etähallinnassa tietoturva-asiat on erityisesti otettava huomioon. Etähallinnan liikenne varsinkin kotikäytössä saattaa kulkea ulkoverkon eli internetin kautta, joten on tärkeää, ettei etähallittaviin tietokoneisiin pääse käsiksi ulkopuoliset tahot. On hyvä muistaa, että etähallinnan avulla voidaan tehdä lähes kaikki samat asiat kuin käytettäessä tietokonetta normaalisti itse paikan päällä.

Kuvitellaan tilanne, että jokin ulkopuolinen taho onnistuu luvattomasti saamaan itselleen tietokoneen hallinnan. Tämä tapahtuu usein tietoverkon välityksellä käyttäen hyväksi kyseessä olevasta tietokoneesta löytyneitä tietoturva-aukkoja, ohjelmistovirheitä tai puutteellisia turva-asetuksia. Tällöin tietokoneen kaapanneella ulkopuolisella taholla olisi täysi pääsy kaikkiin tietokoneella tallennettuihin tietoihin. Jos tietokoneen sisältämä tieto on tärkeää, voi menetys olla hyvinkin suuri. Tietokoneen kaapannut ulkopuolinen taho voi myös esimerkiksi esiintyä tietokoneen oikeana omistajana. Tietokoneen kaappauksen uhrin kannalta kyseessä on vakava tapahtuma, sillä hänen omien tietojensa ja materiaalinsa mielivaltaisen väärinkäytön lisäksi kaikki jäljet kaapatulla tietokoneella tehdyistä rikoksista osoittavat häneen. Tästä syystä on hyvin tärkeää, että etähallintaohjelman tietoturva on kunnossa. (Tietosuojavaltuutetun toimisto 2010.)

Verizon Business RISK Team totesi tuoreessa raportissaan, että kaikissa tutkituissa tunkeutumistapauksissa yli 40 prosentissa käytettiin etähallintaa ja etähallintaohjelmistoja hyödyksi. Kuitenkin tietokoneen etähallinnassa hyödyt ovat huomattavasti riskejä suurempia, kun vain muistaa keskittyä kunnolla tietoturvaan. (Tietotekniikan tuoteuutiset 2012.)

Tietokoneiden etähallinnassa tietoturva voidaan jakaa kahteen osioon, käyttäjän tunnistamiseen ja etäyhteyden suojaukseen.

3.2 Käyttäjän tunnistaminen

Käyttäjän tunnistaminen eli autentikointi on prosessi, jolla varmistutaan siitä, että käyttäjä on se, kuka hän väittää olevansa. Tunnistus voidaan suorittaa kysymällä käyttäjältä salasanaa, varmennuspolettia tai biometristä tunnistetta. (Huntington 2006.)

Yleisin tapa suorittaa käyttäjän tunnistus on salasanan kysely. Siinä käyttäjää pyydetään syöttämään oikea käyttäjätunnus ja salasana jotta tämä voisi kirjautua sisään. Salasanan kysely on kuitenkin kaikista epäturvallisin tunnistustapa, koska mahdollisuus salasanan murtamiseen on helppo. Niinpä salasanan pituus, salasanassa käytetyt merkit ja salasanan voimassaoloaika ovat erittäin tärkeitä kohtia salasanan muodostamisessa. Yleensä vain pelkkä salasanapohjainen tunnistaminen on vaarallinen, koska käyttäjien salasanat eivät ole aina tarpeeksi monimutkaisia. (Huntington 2006.)

Käyttäjä voidaan tunnistaa myös käyttäen tunnistukseen jotain mitä käyttäjällä on, esimerkiksi varmennuspolettia tai biometristä tunnistusta, jossa tunnistuksessa käyttäjältä otetaan esimerkiksi kuva sormenjäljestä. (Huntington 2006.)

Etähallintaohjelmistoissa käyttäjä tunnistetaan yleensä tietokoneen IP-osoitteen, tietokoneen nimen tai ohjelman itse luoman tietokoneen ID-numeron perusteella. Tämän lisäksi käyttäjä määrittelee salasanan itse tai ohjelma luo etähallintayhteyden ajaksi erillisen istuntosalasanan.

3.3 Etäyhteyden suojaus

Etäyhteyden suojaukseen on käytössä monia erilaisia salausmenetelmiä. Salausmenetelmien tarkoitus on varmistaa tietojen luottamuksellisuus, eheys ja kiistämättömyys. Salauksen tulisi aina olla sen verran vahva, että sen murtaminen kohtuullisessa ajassa ja kohtuullisin resurssein ei ole mahdollista. Aika ja resurssit riippuvat kussakin tapauksessa siitä, kuinka tärkeitä salattavat tiedot ovat. (Viestintävirasto 2009.) Tietokoneiden etähallinnassa salauksen tarkoitus on vähentää tai estää kokonaan tuntemattomia ulkopuolisia tahoja pääsemästä hyväksikäyttämään etäyhteyttä. Tunnetuimpia salausmenetelmiä ovat AES, DES, RSA, SSH ja SSL/TLS.

AES (Advanced Encryption Standard) ja DES (Data Encryption Standard) kuuluvat symmetrisiin salausalgoritmeihin. Symmetrisissä salausalgoritmeissa viestin lähettäjä ja vastaanottaja käyttävät sekä salaukseen että salauksen purkuun samaa salausavainta. Symmetristen salausmenetelmien huomattavin etu on salausmenetelmän nopeus. Ongelmana on avainten hallinta viestin lähettäjän ja vastaanottajan saman salausavaimen takia. AES-algoritmi

tukee salausavaimia joiden koot ovat 128, 192 ja 256 bittiä, toisin kuin DES, joka tarjoaa vain 56-bittisen avaimen. Bittien koot tarkoittavat, että esimerkiksi AES jakaa tiedot 128, 192 tai 256 bittisiin lohkoihin. DES algoritmeja ei voida enää nykyään pitää turvallisina kaikkiin käyttötarkoituksiin, koska DES-salaus on onnistuttu murtamaan eri menetelmillä. 256-bittinen AES-salaus on puolestaan tällä hetkellä vahvin käytettävissä oleva salausmenetelmä. AES onkin DES-algoritmin standardoitu seuraaja vuodesta 2002 lähtien. Muita yleisesti käytössä olevia symmetrisiä salausalgoritmeja ovat mm. IDEA (International Data Encryption Algorithm), Blowfish, RC5 ja CAST (Viestintävirasto 2007a).

RSA kuuluu puolestaan epäsymmetrisiin salausalgoritmeihin, joita kutsutaan myös julkisen avaimen algoritmeiksi. Näissä käytetään viestin salaamiseen ja salauksen purkuun eri avaimia, joista toinen on julkinen ja toinen yksityinen avain. Julkisella avaimella salattu viesti voidaan avata kyseisen avainparin yksityisellä avaimella ja päinvastoin. Salattaessa esimerkiksi sähköpostiviestiä, viesti salataan vastaanottajan julkisella avaimella ja vastaanottaja avaa viestin omalla yksityisellä avaimella. Näin kolmas osapuoli ei pysty purkamaan hänen julkisella avaimellaan salattua viestiä, koska vastaanottajan yksityinen avain on ainoastaan vastaanottajan hallussa. Epäsymmetrisen salauksen huomattavimpia etuja symmetrisiin salausalgoritmeihin verrattuna on avaintenhallinnan yksinkertaisuus. Heikkoutena on taas salauksen hitaus. Suosituin epäsymmetrinen salausalgoritmi on RSA, jonka vahvuus perustuu suurten lukujen tekijöiden jakamisen vaikeuteen. Epäsymmetrisiin salausalgoritmeihin kuuluvat myös Diffie-Hellman ja siitä kehitetty ElGamal. (Viestintävirasto 2007b.)

SSH ja SSL ovat salaavia tiedonsiirtoprotokollia. SSH-protokollaa (Secure SHell) käytetään erityisesti pääteyhteyksien salaamiseen, kun taas SSL-protokolla (Secure Socket Layer) on yleisesti käytössä www-palveluiden yhteydessä. (Viestintävirasto 2012.) SSH mahdollistaa turvallisen etäyhteyden verkon ylitse tietokoneesta toiseen. SSH-protokollaa voidaan käyttää erilaisiin käyttötarkoituksiin, kuten ottaa etäyhteys SSH-asiakasohjelmalla SSH-palvelimeen päästäkseen käyttämään toista tietokonetta tai perustaa VPN (RSA Laboratories 2012). SSH-protokollasta on versiot SSH1 ja SSH2. SSH1-version rakenteessa on merkittäviä puutteita, jotka tekevät siitä haa-

voittuvaisen, ja sitä on pidetty suojaustasoltaan heikkona. SSH2-versiossa nämä asiat on korjattu ja se on huomattava parannus aiempaan. Versiota SSH2 suositellaankin nykyään käytettäväksi. (Bitvise 2011.)

SSL-protokolla on yksi tavallisimpia tapoja suojata tietoliikennettä. Protokollan tehtävänä on luoda salattu kanava salaamattoman verkon, kuten internetin ylitse, jotta voidaan kommunikoida yksityisesti. SSL-protokollan on kehittänyt Netscape Communications Corporationin vuonna 1994. Netscape luovutti kehityksen IETF-standardointiorganisaatiolle (Internet Engineering Task Force), joka sitten kehitti SSL-protokollasta oman versionsa ja antoi sille nimeksi TLS (Transport Layer Security). TLS 1.0 on SSL 3.0:n seuraaja, jossa käytetään SSL-protokollaa pohjana. (Microsoft 2012b.)

3.4 Yksilönsuoja

Käytettäessä etähallintaa ei ole tavallisesti mahdollista valvoa tietokonetta huomaamatta, koska etäällä olevalle tietokoneen käyttäjälle on tietosuojasyistä ilmoitettava tietokoneeseen pääsystä (TeamViewer 2012c). Tietokoneen käyttäjä saattaa käsitellä työasemallaan luottamuksellisia tietoja, joten laitoksissa tai jossain muussa yrityksessä on hyvä ilmoittaa etähallintaohjelmien olemassaolosta. Työaseman käyttäjällä olisi hyvä olla asetus, jolla on mahdollisuus joko hyväksyä tai torjua etäistuntopyyntö ennen kuin etähallitsija saa tietokoneen hallintaan. Niin yritys- kuin kotikäytössäkin etähallitsijan on aina ennen etäistuntoa sovittava tai kysyttävä lupa etäällä olevalta käyttäjältä. Etäyhteyttä tulee näin käyttää vain ja ainoastaan ennalta sovittuihin tarkoituksiin.

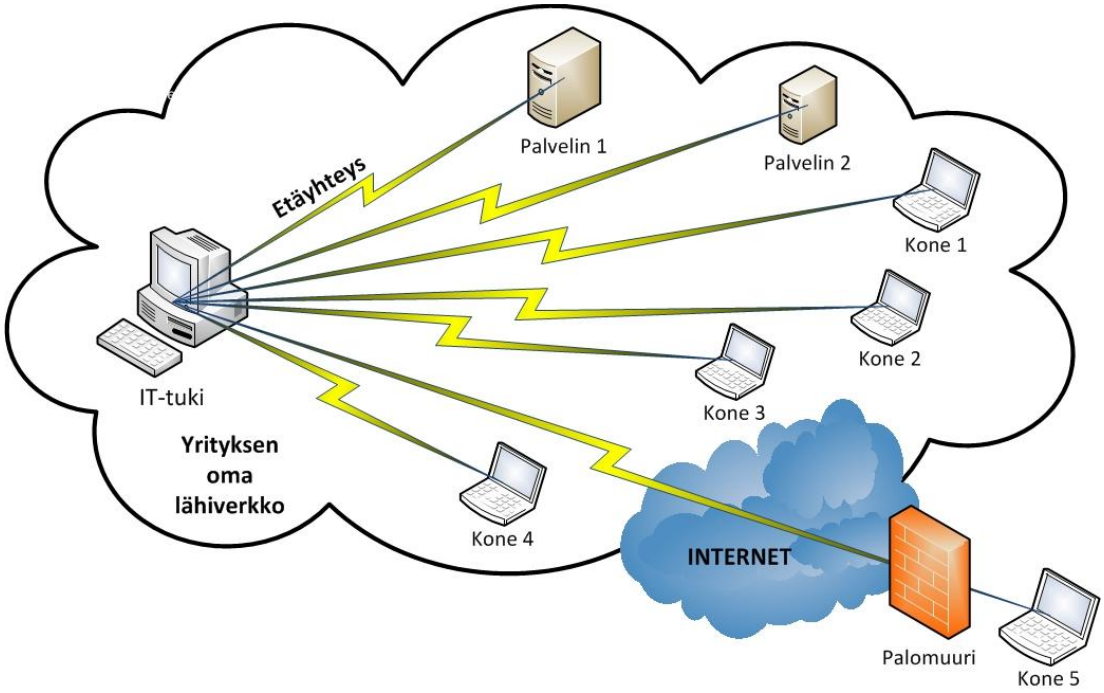
Jos käyttäjä ottaa tietokoneen luvattomasti hallintaan, on kysymys viestintäsalaisuuden loukkaamisesta, josta kerrotaan rikoslaissa, Suomen rikoslaki (9.6.2000/531) KPL 38:3: ”Joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.” (Finlex 2012)

4 TIETOKONEEN ETÄHALLINTA YRITYSKÄYTÖSSÄ

4.1 Yrityskäyttö

Etähallinta voidaan toteuttaa organisaatiossa tai laitoksessa monella eri tavalla. Ei voi sanoa, mikä olisi paras tapa muodostaa etäyhteys, koska organisaatiot poikkeavat toisistaan mm. käyttäjämääriltään, verkkotopologialtaan, etähallinnan tarpeiltaan tai maksuvalmiudeltaan. Suurelle organisaatiolle laadittu etähallintaympäristö voisi olla pienelle organisaatiolle ylimitoitettu, eli liian kallis ja monimutkainen suhteessa siitä saatavaan hyötyyn. Ei ole olemassa yhtä ja oikeaa tapaa etähallinnan toteutukseen. (Kuusisto 2011.)

Yleensä yritysympäristössä laitteet joiden välille halutaan muodostaa etäyhteys, ovat yrityksen omassa lähiverkossa. Tällöin yhteys voidaan muodostaa helposti, nopeasti ja turvallisesti eikä verkkoliikennettä tarvitse ohjata palomuurin läpi oman lähiverkon ulkopuolelle.



Kuvio 2. Tietokoneiden etähallinta yrityskäytössä.

Kuvio 2 on esimerkkinäkymä yrityksen etähallinnasta. Tästä nähdään, että IT-tuki voi hallinnoida kaikkia kuvassa näkyviä neljää eri konetta sekä kahta palvelinta yrityksen oman lähiverkon sisällä. Kun yhteys joudutaan muodostamaan lähiverkon ulkopuolelle koneeseen 5, täytyy muodostaa yhteys internetiin ja ohjata yhteys palomuurin läpi. Kaikki verkkoliikenne mikä tapahtuu

yrityksen oman lähiverkon puolella, on turvallisempaa kuin liikenne internetin yli (Kuusisto 2011).

Jotta etäyhteys voidaan muodostaa, on kaikissa verkon laitteissa oltava hallintaohjelmisto asennettuna oikein määritetyillä asetuksilla. Etäohjelmien lisäksi ylläpito tarvitsee jonkin tiedon kohdetietokoneesta mihin etäyhteys avataan, esimerkiksi tietokoneen nimi tai IP-osoite. Paras tilanne on silloin, kun yrityksen lähiverkon paikallisiin tietokoneisiin voidaan muodostaa etäyhteys välittömästi, mikäli vain laite ja käyttöjärjestelmä ovat käytettävissä. (Kuusisto 2011.) Yrityksissä ja suurissa laitoksissa onkin keskitetysti hallittuihin työasemiin asennettu etähallinnan mahdollistava ohjelmisto.

Yrityskäytössä etähallinnalla on pääasiassa kaksi käyttötarkoitusta. Sen avulla lähituki tai ns. helpdesk voivat nopeammin auttaa työaseman käyttäjää ongelmatilanteissa. Myös työasemien järjestelmien päivitys ja ylläpito onnistuu etähallinnan avulla kätevästi. Yhdellä ainoalla tietokoneella voidaan hoitaa laitoksessa, esimerkiksi koulussa, 200 muuta työasemaa etähallinnan avulla.

4.2 Tietokoneen etähallinta Kairatien ammattiopistolla

4.2.1 Kairatien ammattiopisto

Lapin ammattiopisto on Rovaniemen koulutuskuntayhtymän ammatillinen oppilaitos, joka järjestää ammatillista perus- ja aikuiskoulutusta kaikilla koulutusaloilla lukuun ottamatta liikunta-alaa ja matkailu-, ravitsemis- ja talousalaa (Lapin ammattiopisto 2011a). Toimipisteitä Lapin ammattiopistolla on yhteensä kahdeksan, joista kuusi sijaitsee Rovaniemellä ja yksi Sodankylässä sekä yksi Kittilässä. (Lapin ammattiopisto 2011b.)

Opiskelijoita Lapin ammattiopistossa opiskelee vuosittain n. 5000. Ammatillisessa peruskoulutuksessa heistä on n. 2450 ja ammatillisessa lisä- ja täydennyskoulutuksessa 2400. Henkilökuntaa lapin ammattiopistossa on noin 460, joista 350 on opettajia ja loput ovat tukipalvelu- ja hallintohenkilöstöä. (Lapin ammattiopisto 2011a.) Kairatien toimipisteessä näistä 5000 lapin ammattiopiston opiskelijasta opiskelee 900 ja henkilökuntaa on 65, joista IT-tukihenkilöitä on vain yksi (Sassi 2012). Kairatien toimipisteessä sijaitsee lii-

ketalouden, tietojenkäsittelyn, rakennusalan sekä ajoneuvo- ja ilmailutekniikan opetustilat (Lapin ammattiopisto 2011c).

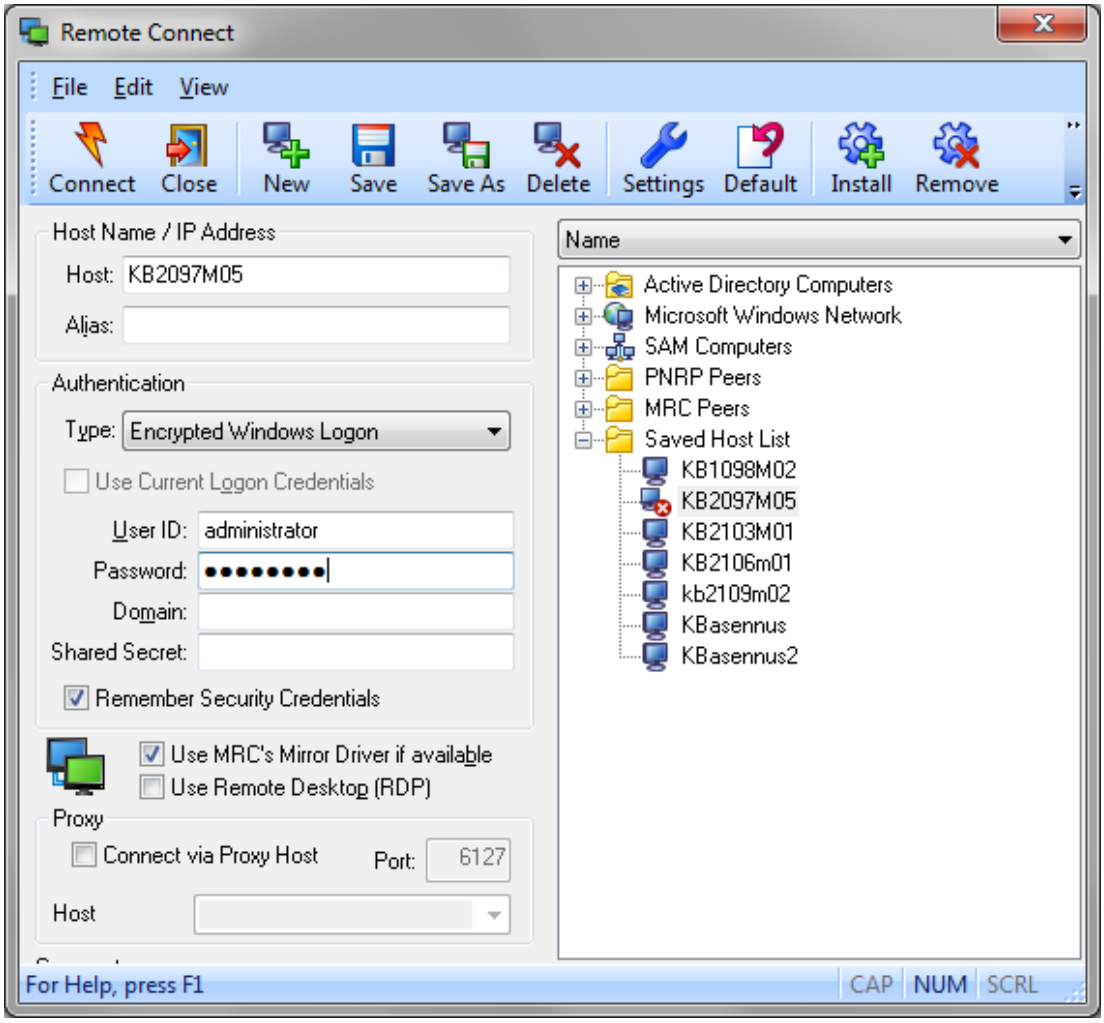
Opinnäytetyöni yritysosuuden pääkohteena on Lapin ammattiopiston Kairatien toimipiste, tekstissä myöhemmin mainittuna Kairatien ammattiopisto. Tarkoituksenani on kertoa miten Kairatien toimipiste käyttää etähallintaa, mitä eri etähallintaohjelmia siellä on käytössä ja mitä muita etähallintamenetelmiä siellä käytetään. Kairatien toimipisteessä on yhteensä 550 tietokonetta, joita hoitaa paikan päällä siis vain yksi IT-tukihenkilö. Tämän takia etähallinnan osuus on merkittävä laitoksen IT-tuki toiminnassa. Etähallinta auttaa ja nopeuttaa huomattavasti tietokoneiden ylläpitoa ja tukitoimintaa. (Sassi 2012.) Kävin tutustumassa tämän laitoksen etähallintamenetelmiin ja haastattelemassa yksikön IT-tukihenkilöä Olli Sassia.

4.2.2 DameWare NT Utilities

DameWare NT Utilities on monipuolinen Windowsin etähallintaan tarkoitettu ohjelmisto joka on käytössä Kairatien ammattiopistolla. DameWaressa on paljon ominaisuuksia ja sillä on mahdollisuus tehdä paljon muutakin kuin pelkkää etähallintaa. DameWare NT Utilities sisältää Mini Remote Control- ja Exporter -työkalut, joiden avulla ylläpitäjät voivat hallita mm. Active Directoryä, käyttäjäryhmiä, tulostimia, levyasemia, palveluita ja rekistereitä. (DameWare 2012a.) Kairatien Ammattiopistolla DameWaren ohjelmistoa käytetään pääasiassa etähallintaan, jolla työasemien ylläpidetään ja annetaan käyttäjille etätukea (Sassi 2012).

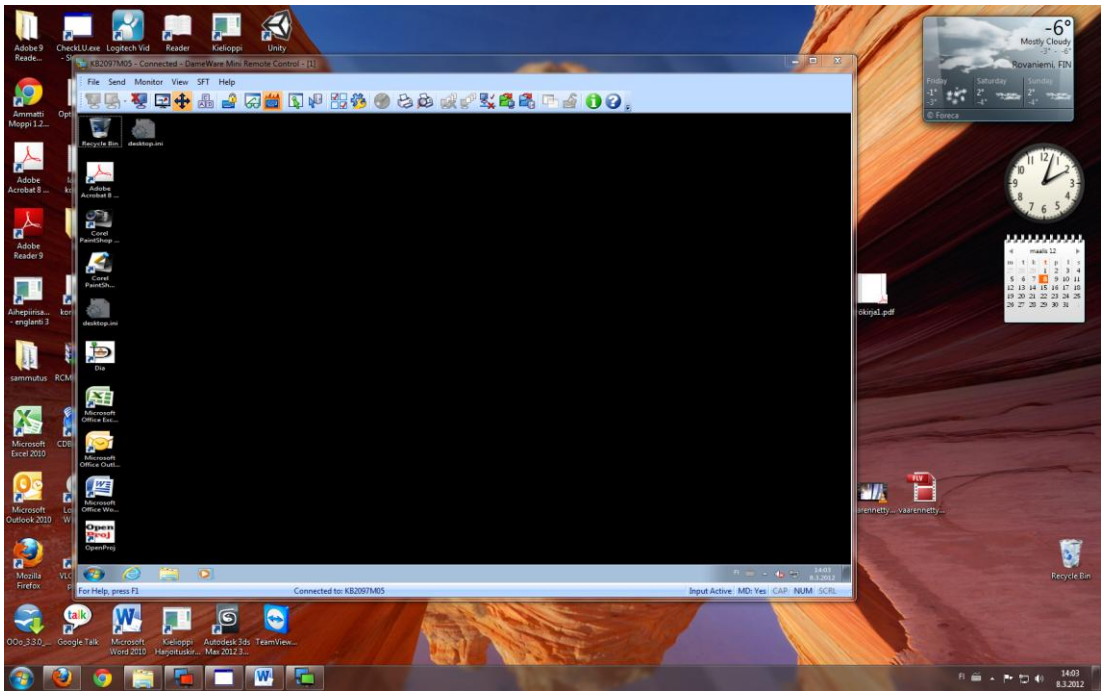
DameWaressa etäyhteys voidaan muodostaa Mini Remote- tai RDP -yhteyden avulla. Mini Remote Control on DameWare-ohjelman kevyt apuohjelma. Käytettäessä Mini Remote Controlia, ohjelmasta on asennettava etähallittavaan tietokoneeseen Client Agent -palvelu, joka avulla ylläpitäjät voivat muodostaa etäyhteyden tietokoneeseen. Jos kyseessä on uusi työasema, missä ei ole vielä Clien Agent -palvelua, voi palvelun asentaa etäältä, jolloin etäyhteysistunto alkaa välittömästä ilman että tietokoneen luona tarvitsee fyysisesti käydä. Tietokonetta ei tarvitse käynnistää myöskään uudelleen. Client Agent -palvelun ansiosta ylläpitäjät voivat hallita kaikkia tietokoneita, jotka ovat samassa verkossa. (DameWare 2012b.) Kairatien ammattiopistolla

Clien Agent -palvelu on asennettuna pääsääntöisesti kaikkiin tietokoneisiin (Sassi 2012).



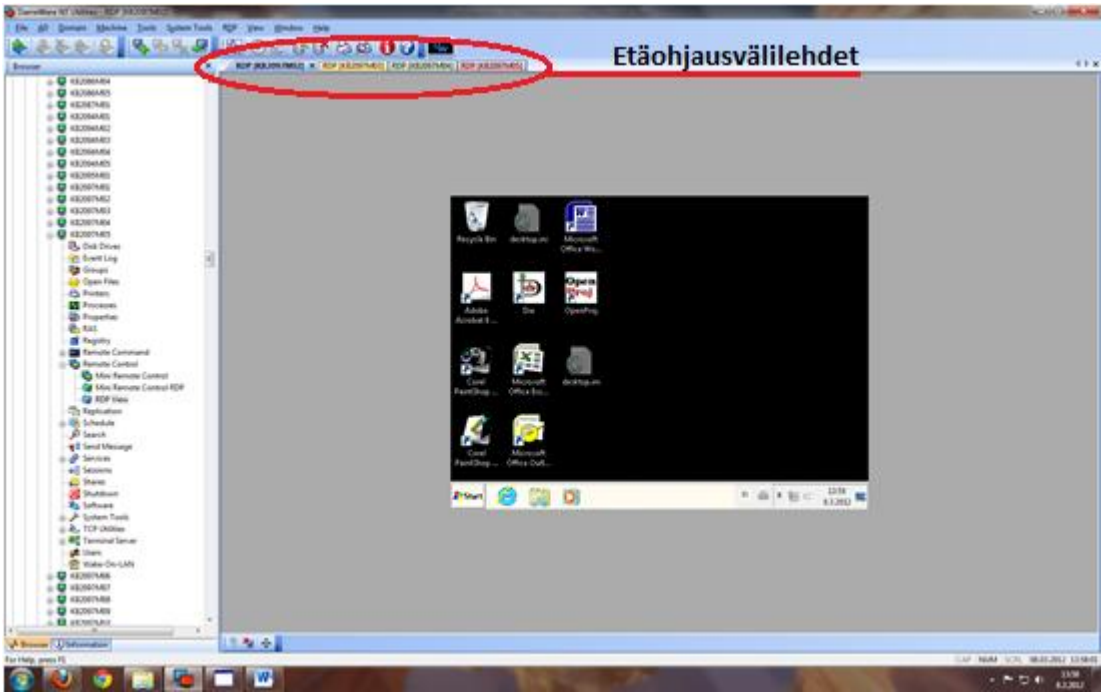
Kuvio 3. Yhteyden muodostaminen DameWare Mini Remote Control -ohjelmalla.

Kuvio 3 on näkymä Mini Remote Controlin yhdistämisvaiheesta. Yhdistäminen onnistuu, kun antaa etähallittavan tietokoneen nimen (Host), käyttäjätunnuksen (User ID) ja salasanan (Password). Tämän jälkeen aukeaa etäohjausikkuna, jossa näkyy etähallittavan tietokoneen työpöytä (Kuvio 4). Tämän etäohjausikkunan avulla henkilö voi antaa etähallittavalle henkilölle etätukea tai muuten hallinnoida hänen tietokonettaan.



Kuvio 4. DameWaren Mini Remote Control -ohjelmalla etäyhteys muodostettuna.

Toinen tapa jolla etäyhteys voidaan muodostaa, on RDP View. RDP-yhteys on huomattavasti kevyempi kuin Mini Remote. RDP View -yhteydellä onnistuu hyvin usean työaseman yhtäaikainen ylläpito, koska käytettäessä tätä yhteyttä etäohjausikkunat eivät aukea aina uuteen ikkunaan vaan ohjelman sisällä uuteen välilehteen, kuten kuviosta 5 voidaan nähdä.



Kuvio 5. DameWaren RDP View -ohjelmalla neljä etäyhteyttä muodostettuna.

Kuviossa 5 on avoinna neljä yhtäaikaista RDP View -yhteyttä eri työasemiin. Eri yhteydet näkyvät ohjelmassa omissa välilehdissään. Etätuki ei RDP View -yhteydellä ole mahdollista toisin kuin Mini Remotella, koska RDP View -yhteydessä etähallittava tietokone menee lukittuun tilaan etäyhteyden ajaksi.

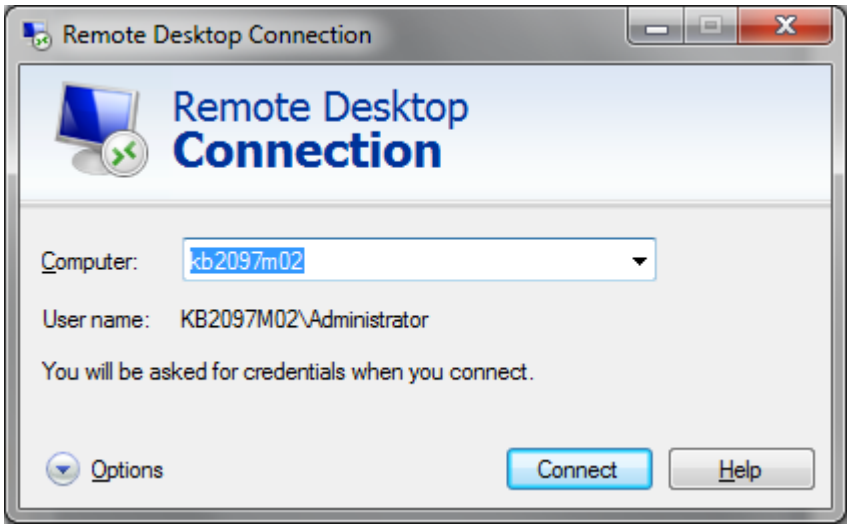
Itse etähallinnan lisäksi DameWarea käytetään Kairatien ammattiopistolla myös muutamien muiden toimintojen käyttöön. Yksi tärkeimmistä toiminnoista on tiedostojen jakaminen etätietokoneille. DameWarea käytetään myös kun halutaan katsoa etätietokoneen järjestelmä- tai ohjelmisto tietoja yksityiskohtaisesti. Tämä helpottaa IT-tukea tietokoneiden ylläpidossa. Myös etätietokoneiden sammuttamista, käyttäjän uloskirjaamista tai tietokoneiden uudelleenkäynnistämistä käytetään Kairatien ammattiopistolla DameWaren avulla. (Sassi 2012.)

4.2.3 Remote Desktop Connection

Remote Desktop Connection on Windowsin oma etähallintaohjelma, joka on sisällytetty Windowsin käyttöjärjestelmiin eikä sitä tarvitse erikseen asentaa. Tämä ominaisuus ei kuitenkaan toimi kaikissa Windowsin versioissa. Windows 7 -käyttöjärjestelmissä yhteys voidaan muodostaa vain Professional-, Ultimate- tai Enterprise -versioihin (Microsoft 2012c). Windows Vista -käyttöjärjestelmissä yhteyttä ei voi muodostaa Windows Vista Starter-, Windows Vista Home Basic-, Windows Vista Home Basic N- tai Windows Vista Home Premium -versioihin sekä Windows XP -käyttöjärjestelmissä Windows XP Home Edition -versioon (Microsoft 2012g).

Kairatien ammattiopistolla käytetään Remote Desktop Connection -ohjelmaa toisena varsinaisena etähallintaohjelmana DameWaren ohessa. Remote Desktop Connection on ainoastaan pelkkään etähallintaan tarkoitettu ohjelma ja se tukee vain yhden käyttäjän kirjautumista tietokoneelle kerrallaan. Kairatien Ammattiopistolla Remote Desktop Connection -ohjelmaa käytetään vain työasemien ylläpitoon. Etätuki ei ohjelmalla onnistu, koska etähallittava tietokone lukkiutuu aina etäyhteyden ajaksi.

Etäyhteyden muodostaminen onnistuu suhteellisen helposti. Yhteyttä muodostaessa avataan aluksi Remote Desktop Connection ohjelman yhdistämisikkuna, johon kirjoitetaan halutun tietokoneen nimi (Kuvio 6).



Kuvio 6. Yhteyden muodostaminen Remote Desktop Connection -ohjelmassa.

Kuviossa 6 aiotaan muodostaa etäyhteys kb2097m02-tietokoneeseen. Kun yhteyttä aletaan muodostaan, käyttäjältä kysytään vielä kyseisen tietokoneen tunnistetietoja, käyttäjätunnusta ja salasanaa. Jotta yhteys on mahdollista muodostaa, tietokoneiden on oltava samassa verkossa.

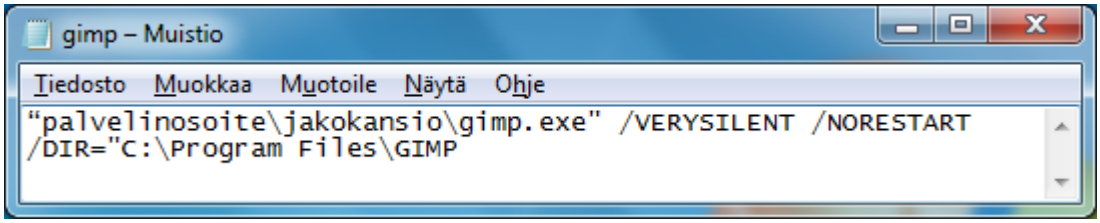
Jos kyseisessä etätietokoneessa ei ole mitään istuntoa käynnissä, käyttäjä pääsee käyttämään suoraan kohdetietokonetta. Mutta jos tietokoneessa on istunto käynnissä, käyttäjältä kysytään varmistusta yhteydenmuodostamisesta. Jos käyttäjä yhdistää tietokoneeseen käynnissä olevasta istunnosta huolimatta, istunnossa oleva henkilö kirjataan automaattisesti ulos tietokoneelta ja tietokone lukkiutuu. Tämän jälkeen etäkäyttäjä kirjautuu tietokoneessa olleen käyttäjän tilalle. Käyttäjällä täytyy olla järjestelmänvalvojan oikeudet päästäkseen ”kaappaamaan” tietokoneen. Etätietokoneen ruudun näkee vain hallitseva osapuoli.

4.2.4 PsExec

PsExec on kevyt apuohjelma, jonka avulla on mahdollisuus suorittaa eri prosesseja, esimerkiksi asentaa ohjelmia etäältä muihin tietokoneisiin ilman minkäänlaisia manuaalisia toimenpiteitä etätietokoneessa (Russinovich 2009). Etätietokoneen haltija ei huomaa prosessin edistymistä eikä hänelle tule asennukseen liittyviä ikkunoita. Tätä asennustapaa kutsutaan hiljaiseksi asennukseksi (Wikipedia 2012). Kairatien Ammattiopistolla käytetään hiljaisissa asennuksissa PsExec-sovellusta (Sassi 2012).

PsExec-sovellus ei vaadi minkäänlaista varsinaista asennusta. Ohjelman PsExec.exe-tiedosto täytyy vain olla samassa hakemistossa minne on määritelty komentotiedostot hiljaisia asennuksia varten (Sassi 2012).

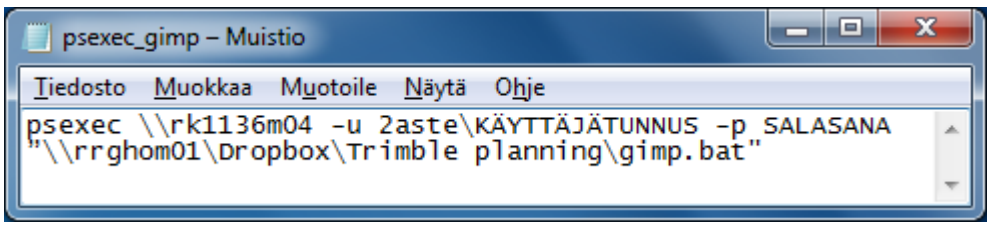
Jokaisella ohjelmalla joka halutaan asentaa hiljaisesti, on oltava oma hiljaisen asennuksen mahdollistava asennustiedosto, jossa määritellään hiljaisen asennuksen vaiheet. Tähän ei ole mitään yleistä mallia, mikä tekisi mistä tahansa ohjelmasta hiljaisen asennettavan, vaan jokaiseen ohjelmaan on erikseen tehtävä oma hiljainen asennustiedosto. Kuviossa 7 on esimerkki hiljaisesta asennustiedostosta Kairatien Ammattiopistolta. Tämä tiedosto on Gimp-ohjelmaan tehty hiljainen asennustiedosto *gimp.bat.* (Sassi 2012.)



Kuvio 7. Hiljainen asennustiedosto gimp.bat.

Tämä tiedosto käynnistää *gimp.exe*-sovelluksen *palvelinosoite\jakokansio*-osoitteesta. Komento */VERYSILENT* kehottaa asennusta olemaan hyvin hiljainen, jolloin asennuksen edistymistä ei näytetä lainkaan. Komento */NORESTART* ei automaattisesti käynnistä tietokonetta uudelleen asennuksen jälkeen, vaikka se olisi tarpeen. */DIR="C:\Program Files\GIMP*-komento ohittaa asennuksen oletushakemiston ja asentaa ohjelman määritettyyn hakemistoon, tässä tapauksessa C-asemalle, Program Files -kansiossa olevaan GIMP-kansioon. (Lawmay 2005.)

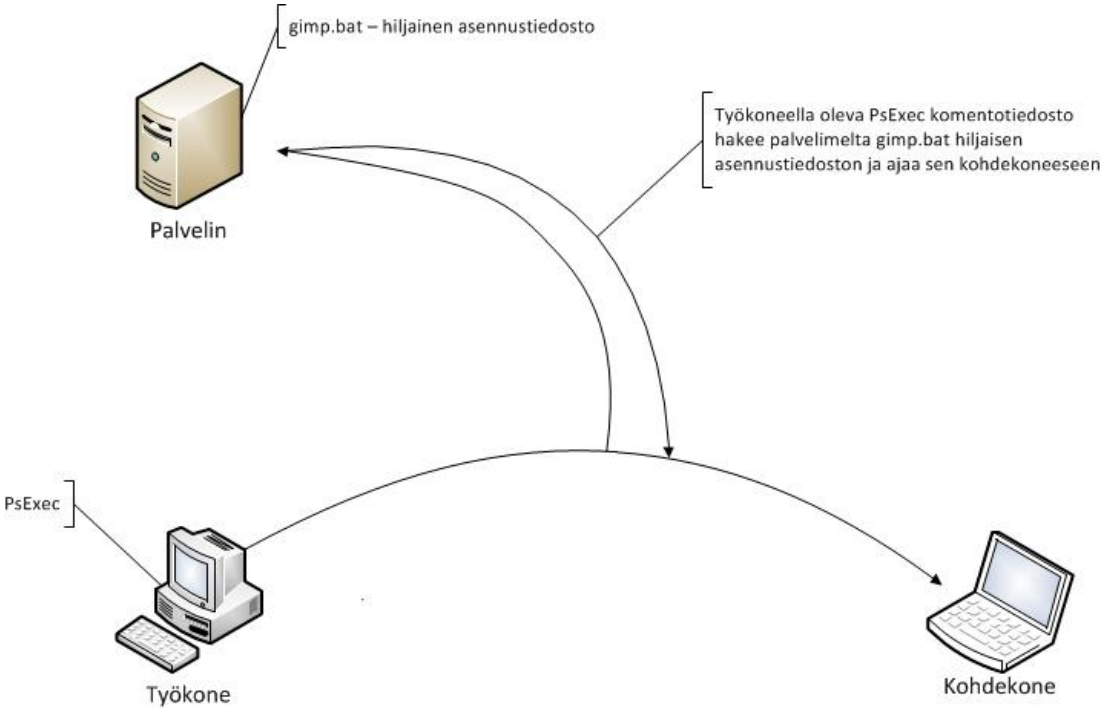
Tämän jälkeen, kun hiljainen asennustiedosto on määritelty, täytyy määritellä PsExec-komentotiedosto, jolla voidaan asentaa ohjelma etäisesti toisiin tietokoneisiin. Kuviossa 8 on esimerkki PsExec-komentotiedostosta.



Kuvio 8. PsExec-komentotiedosto.

Tässä tiedostossa komento *\\rk1136m04* ajaa kyseisen gimp.bat-sovelluksen rk1136m04-tietokoneeseen. Komento *-u 2aste\KÄYTTÄJÄTUNNUS -p SALASANA* märittää käyttäjän kirjautumisen (käyttäjätunnuksen ja salasanan) etätietokoneelle. *"\\rrghom01\Dropbox\Trimble planning\gimp.bat"*-komento kertoo polun, mistä ajettava sovellus, gimp.bat löytyy. (Russinovich 2009.) Eli tämä komentotiedosto siis käynnistää äsken määritellyn gimp.bat-tiedoston rk1136m04-tietokoneessa, joka sitten asentuu kyseiselle tietokoneelle täysin hiljaisesti aiemmin määritetyn hiljaisen asennustiedoston ansiosta. Jotta PsExec-komentotiedosto toimii, täytyy psexec.exe-tiedoston olla samassa kansiossa kun komentotiedosto suoritetaan.

Hiljaisen asennuksen prosessi on kokonaisuudessaan kuvattuna alla olevassa kuvassa (kuvio 9).



Kuvio 9. Hiljaisen asennuksen prosessi.

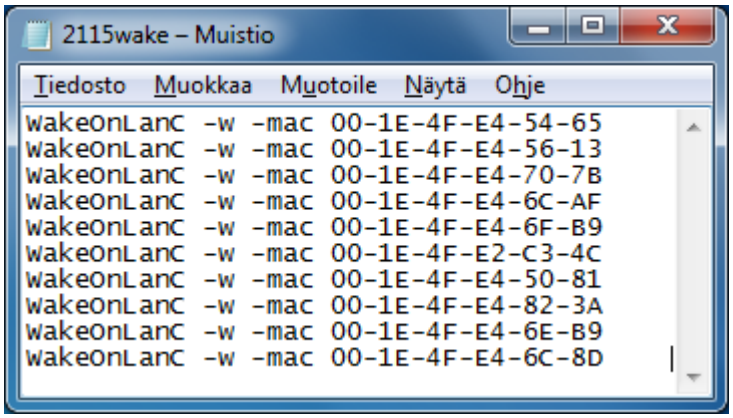
Kairatien ammattiopistolla hiljaisiin asennuksiin käytetään myös SMS-palvelinta. SMS-palvelin ei kuitenkaan ole vielä kovin suuressa käytössä.

4.2.5 Wake on Lan

Wake on Lan on toiminto, joka mahdollistaa samassa lähiverkossa olevan tietokoneen käynnistämisen etäyhteyden kautta. Wake on Lanin toimintaperiaatteesta kerrotaan luvussa 2.2 Muut käyttömahdollisuudet.

Kairatien ammattiopistolla käytetään Wake on Lania kevyen apuohjelman, WakeOnLanC:n avulla, joka toimii samalla periaatteella kuin aiemmassa luvussa ollut PsExec-sovellus. Niin kuin PsExec-sovellus, niin ei myöskään WakeOnLanC-sovellus vaadi asennusta, vaan ohjelman WakeOnLanC.exe-tiedosto täytyy olla samassa hakemistossa minne on määritelty komentotiedostot etätietokoneiden käynnistystä varten. (Sassi 2012.)

Kuviossa 10 on esimerkki WakeOnLanC-sovelluksen komentotiedostosta Kairatien ammattiopistolta.

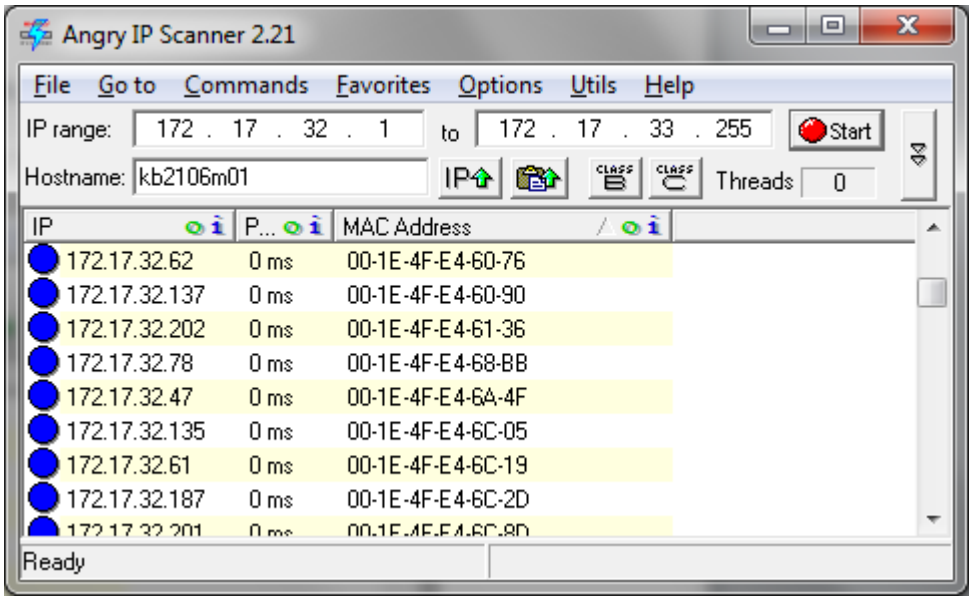


Kuvio 10. WakeOnLanC-komentotiedosto.

Tämä 2115wake.bat-komentotiedosto käy läpi luokan 2115 kymmenen tietokonetta MAC-osoitteiden perusteella, jotka on määritelty tiedostoon. Jos joku tietokoneista on sammuksissa, ohjelma herättää tietokoneen ja se käynnistyy.

Tietokoneiden MAC-osoitteiden lisääminen komentotiedostoon tapahtuu Angry IP Scanner -ohjelman avulla. Angry IP Scanner on kevyt ja yksinkertainen työkalu IP- ja MAC -osoitteiden skannaukseen. Sillä voidaan tarkistaa nopeasti, miten suuri joukko tietokoneita vastaa verkossa. Skannauksen voi kohdistaa yhteen osoitteeseen tai laajempaan osoitejoukkoon. (Pitkänen–Lehto 2010.)

Alla olevassa esimerkkikuvassa (kuvio 11) Angry IP Scannerilla on skannattu IP-osoitteet 172.17.32.1–172.17.33.255 (kuviossa on näkyvissä vain osa osoitteista), joista ohjelma on kerännyt myös tietokoneiden MAC-osoitteet.



Kuvio 11. Angry IP Scanner -ohjelmassa IP-osoitteita skannattuna.

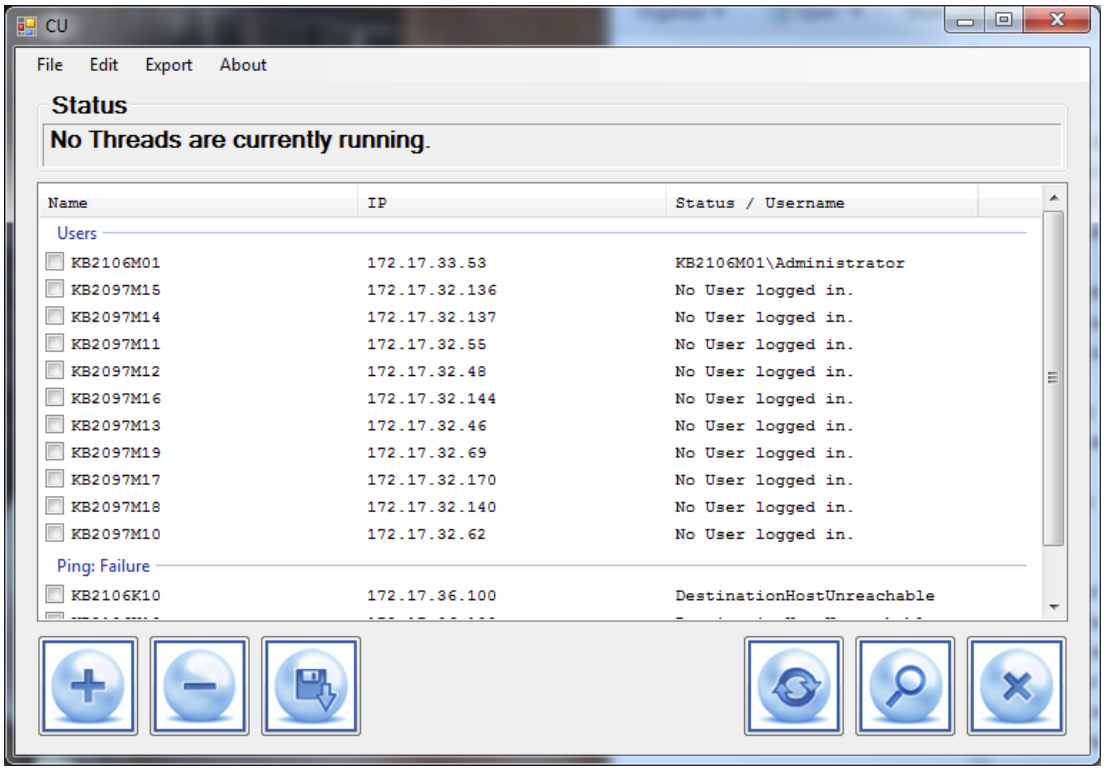
Skannauksen jälkeen valitaan halutut osoitteet ja siirretään ne Excel-taulukkolaskentaohjelmaa hyväksikäyttäen WakeOnLanC-komentotiedostoon.

4.2.6 CU

IT-tuelle yksi hyödyllisimmistä etäkäytön seurantasovelluksista on pieni ja kevyt sovellus nimeltään CU. CU on Rovaniemen koulutuskuntayhtymässä työharjoittelussa aikanaan olleen saksalaisen opiskelija Matthias Janssenin tekemä sovellus. Sovellus ei ole julkinen, vaan se on tehty ainoastaan Rovaniemen koulutuskuntayhtymän käyttöön. (Sassi 2012.)

CU-ohjelmalla on mahdollista seurata etäisesti samassa lähiverkossa olevien tietokoneiden tilaa, kuten ovatko tietokoneet päällä, sammuksissa tai kuka käyttäjä tietokoneelle on kirjautuneena.

Kuviossa 12 on kuva CU-ohjelmasta. Tässä kuvassa on CU-ohjelman avoin ikkuna, johon on skannattuna Kairatien ammattiopiston muutamia tietokoneita.



Kuvio 12. CU-ohjelmassa tietokoneita skannattuna.

Kuvasta voidaan todeta, että tietokoneeseen KB2106M01 (ensimmäinen rivi) on kirjautuneena Administrator-käyttäjä. Tietokoneet joihin ei ole kirjautuneena ketään, mutta ovat kuitenkin päällä, lukee ”No User logged in”. Tietokone KB2106K10 (viimeinen rivi) on kokonaan pois päältä tai tietokoneeseen ei jostain muusta syystä saada yhteyttä.

Ohjelmaan on mahdollisuus tallentaa tietokoneita ryhmiin esimerkiksi luokittain. Tämän avulla on mahdollisuus tarkistaa jonkun tietyn luokan tietokoneiden tilanne samalla kertaa. (Sassi 2012.)

4.2.7 Symantec Ghost

Symantec Ghost on tietokoneiden varmuuskopiointi ja käyttöönotto -ohjelmisto, jota käytetään Kairatien ammattiopistolla. Ghost-ohjelmalla voidaan esimerkiksi asentaa helposti ja nopeasti käyttöjärjestelmä tietokoneeseen. (Raitahila 2008.) Ghost-ohjelman käyttö ei ole varsinaista etähallintaa, mutta sillä on kuitenkin mahdollisuus asentaa tietokoneisiin käyttöjärjestelmiä etäisesti paikallisen verkon kautta.

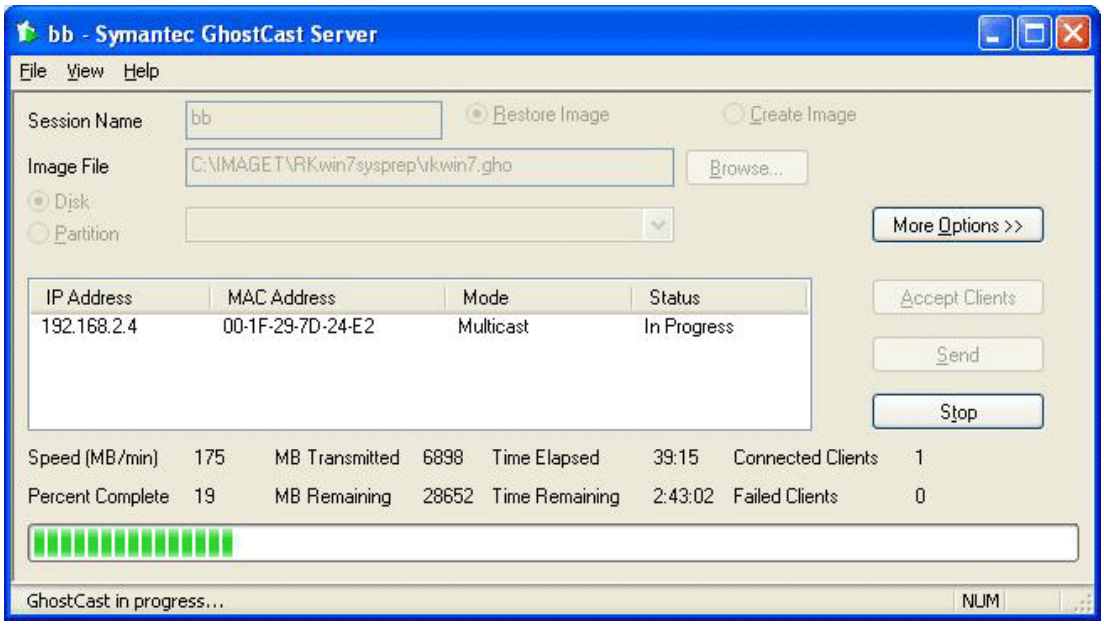
Ohjelman toiminta perustuu levykuvien (image) ottamiseen. Ghost-ohjelmalla voidaan luoda image jostain valmiista työaseman käyttöjärjestelmästä tai palauttaa luotu image johonkin toiseen työasemaan.

Ghost-ohjelma täytyy asentaa palvelinkoneelle, jonne luodut imaget tallennetaan ja josta voidaan jakaa luotuja imageja eteenpäin. Palvelinkoneen ja asiakaskoneen täytyy olla samassa verkossa, jotta imagen luominen tai palauttaminen onnistuu.

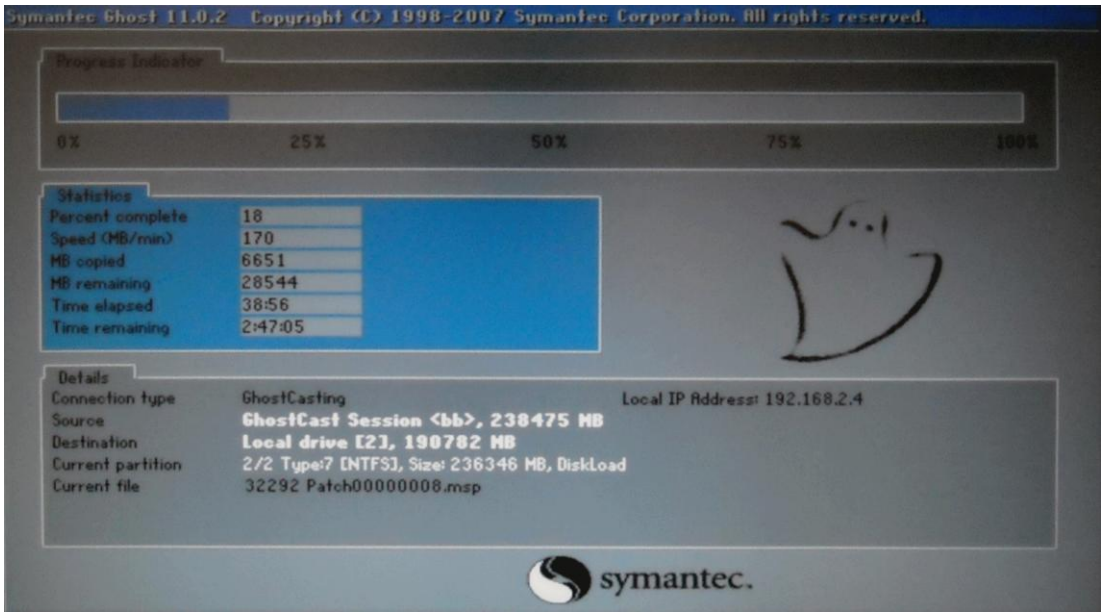
Jos halutaan tallentaa image jo valmiista ja toimivasta käyttöjärjestelmästä, pitää Ghost-ohjelma valmistella vastaanottamaan kiintolevyn tiedot asiakaskoneelta ja varastoimaan ne levynkuvaksi sekä asiakaskone valmistella lähettämään levynkuvaa (Raitahila 2008). Kun tarvittavat valmistelut on tehty, pitäisi asiakaskoneen löytää palvelinkone.

Jos taas halutaan lähettää valmis image johonkin työasemaan, täytyy palvelinkone valmistella lähettämään aikaisemmin luotu image asiakaskoneelle ja asiakaskone valmistella vastaanottamaan image palvelinkoneelta.

Alla olevat kuviot 13 ja 14 kuvaavat meneillä olevaa levynkuvan lähetystä. Kuvio 13 on palvelinkoneelta ja kuvio 14 asiakaskoneelta.



Kuvio 13. Symantec Ghost -ohjelman levynkuvan lähettäminen palvelinkoneelta.



Kuvio 14. Symantec Ghost -ohjelman levynkuvan vastaanottaminen asiakaskoneella.

Tätä ohjelmaa käytetään Kairatien ammattiopistolla esimerkiksi yhden luokan käyttöjärjestelmien tai ohjelmistojen uusimiseen. Symantec Ghost -ohjelman avulla luokan jokaiseen tietokoneeseen ei tarvitse erikseen asentaa käyttöjärjestelmää, vaan riittää kun valmistelee yhden tietokoneen ja luo siitä levykuvan. Tämän jälkeen lähettää tämän luodun levynkuvan luokan muihin tietokoneisiin. (Sassi 2012.)

4.2.8 Tietoturva

Kairatien ammattiopistolla käytetyt etähallintaohjelmat sisältävät omat suojausmenetelmät ja salausprotokollat.

DameWare-ohjelma sisältää monipuoliset tietoturva- ja salausominaisuudet, kuten useat autentikointimenetelmät jotka käyttävät päänsääntöisesti käyttöjärjestelmän sisäänrakennettuja turvallisuusmenetelmiä. DameWarella on myös mahdollista salata kaikki etätietokoneen ja paikallisen tietokoneen välinen viestintä käyttäen nykypäivän salaus-, hajautus- ja avaimenvaihtostandardeja. DameWare käyttää yhteyden salaukseen Microsoftin Cryptographic Service Providers -palveluita sekä käyttöjärjestelmän sisäistä CryptoAPI:a, jotka ovat FIPS-140-sertifioituja. Salaus on mahdollista pakottaa päälle kaikissa yhteyksissä. DameWarella on myös mahdollisuus rajoittaa pääsyä IP-osoitteiden, ryhmän jäsenyyden tai salasanan perusteella sekä vaatia käyttäjän lupa ennen etäkäyttöyhteyden muodostamista. DameWare Mini Remote

Control on ainoa tunnettu kolmannen osapuolen etähallintatyökalu, jossa on mahdollista käyttää Smart Card -kirjautumista tarvitsematta mitään Smart Card -väliohjelmistoa tai Smart Card -lukijaa asennettavaksi etätietokoneelle. (DameWare 2012b.) Kairatien ammattiopistolla ei kuitenkaan ole käytössä Smart Card -kirjautumisia.

Remote Desktop Connection käyttää yhteyden muodostamiseen Microsoftin RDP-protokollaa (katso luku 2.3 Protokollat). Microsoftin RPD-protokolla taas käyttää yhteyden salaamiseen RSA Securityn RC4 -salausta. RC4-salaus on suunniteltu tehokkaaseen salaamiseen pieniä määriä tietoja kerrallaan. Yhteyden salaamiseen käytetään 56- tai 128-bittistä avainta. (Microsoft 2012a.) Remote Desktop Connection -ohjelman palvelimen todennus -ominaisuus tarkistaa, että yhteys muodostetaan oikeaan etätietokoneeseen tai palvelimeen. Tämä suojaustoimenpide auttaa estämään yhteyden muodostumista väärään tietokoneeseen tai palvelimeen ja mahdollisesti paljastamasta luottamuksellisia tietoja. Vaaditun todennuksen vahvuus määräytyy ylläpitäjän määrittämän järjestelmän suojauskäytännön mukaan. (Microsoft 2012f.)

Lisää tietoturvaa laitoksen etähallintaan tuo Kairatien ammattiopistolla laitoksen lähiverkossa käytössä oleva VLAN (Virtual Local Area Network) (Sassi 2012). VLAN:n avulla lähiverkko on jaettu omiin loogisesti täysin erillisiin verkkoihin, ns. virtuaalisiin lähiverkkoihin. Verkko on fyysisesti yhtenäinen, mutta käyttäjät eivät voi liikennöidä kuin oman ryhmänsä jäsenten välillä. (Javvin Company 2012.)

Etähallinnan kannalta tämä tuo huomattavasti lisää tietoturvaa laitoksen etähallintaan, koska etähallinta ei onnistu kuin oman VLAN-ryhmän sisällä. Eri VLAN-verkkojen välillä liikenne kulkee palomuurin kautta. Kairatien ammattiopistolla lähiverkko on jaettu muutamaan omaan VLAN-ryhmään. Oppilaskäytössä on Oppilas-VLAN, henkilökunnalla Henkilökunta-VLAN sekä IT-tuella on oma Admin-VLAN. Admin-VLAN-verkosta on mahdollisuus hallinnoida kaikkia VLAN-verkkoja.

4.3 Tietokoneen etähallinta Lappset- ja LapIT -yrityksissä

Kairatien ammattiopiston etähallintamenetelmien tutustumisen lisäksi tein lyhyet sähköpostihaastattelut Lappset- ja LapIT -yrityksiin. Haastattelussa

kysyin, mitä etähallintaohjelmia kyseisessä yrityksessä on käytössä, käytössä olevien etähallintaohjelmien hyvät ja huonot puolet, miten yrityksessä on huolehdittu etähallintaohjelmien tietoturvasta sekä etähallintaohjelmien tulevaisuuden näkymät yrityksessä.

Lappset Group Oy on yksi maailman johtavista leikkipaikkavälinevalmistajista. Lappsetin tuotteita on jo yli 40 maassa. (Lappset 2012.) On siis selvää, että tällaisen yrityksen sisällä tietokoneiden etähallinta on tärkeä osa yrityksen IT-palveluja. Lappsetilta haastatteluun vastasi IT-henkilö Vesa Takala.

Lappsetilla on tällä hetkellä käytössä etähallintaohjelmana TeamViewer. Takalan mukaan TeamViewerin etuna on se, että ohjelma ei vaadi asennusta sekä se, että ohjelma toimii hankalienkin yhteyksien takaa. Aiemmin Lappsetilla on ollut käytössä DameWare ja pcAnywhere, mutta näistä on luovuttu TeamViewerin parempien ominaisuuksien takia. TeamViewerin heikkoutena Takala pitää sitä, että jos TeamVieweriä ei ole asennettu palveluksi, se ei toimi kun tietokoneesta kirjaudutaan ulos. TeamViewerin käytöstä ja ominaisuuksista kerrotaan tarkemmin luvussa 5.2. Etähallintaohjelmien tietoturvasta Lappsetilla on huolehdittu niin, että toistaiseksi TeamVieweria ei ole asennettu Windows palveluna, jolloin käyttäjän pitää laittaa yhteys itse päälle. Lisäksi tietokoneissa on virustorjunta- ja palomuuri -ohjelmistot. Tulevaisuudessa kaikilla Lappsetin käyttäjillä on mahdollisuus ottaa TeamViewer-ohjelmisto käyttöön, koska itsepalveluportaaliin on julkaistu TeamViewer-ohjelmisto, jonka käyttäjä voi halutessaan ”asentaa". (Takala 2012.)

LapIT Oy on voimakkaasti kasvanut kunta-alan IT-palveluja tarjoava yritys. LapIT:n palvelutuotanto toiminta jakautuu kolmeen osa-alueeseen toiminnoittain. Palvelupiste toimii rajapintana asiakkaan LapIT:n palvelutuotannon välillä. Yksikkö tuottaa neuvontapalveluita, (Palvelupiste/HelpDesk), sekä teknisiä tukipalveluita, joita käyttämällä asiakas saa parhaan mahdollisen hyödyn IT-ratkaisuistaan. Työasemapalvelut on yhdistynyt osaksi palvelukonseptia ja samalla palvelun sisältö ja rajanvedot ovat selkiytyneet. Sovellukset, palvelimet ja verkot tuottavat palveluita sekä suunnittelevat ja kehittävät palveluympäristöä LapIT:n asiakkaille. (LapIT 2012.) Haastattelin LapIT:ltä ICT-asiantuntijaa Risto Aaltosta.

Tietoturvasyistä en voi kuitenkaan tarkemmin kertoa, mitä etähallintaohjelmia LapIT käyttää tai on käyttänyt. Yleisesti voidaan kuitenkin todeta, että LapIT:llä on käytössä tällä hetkellä kaksi etähallintaohjelmaa ja aiemmin käytössä ei ole ollut muita. Tulevaisuudessa kuitenkin LapIT suunnittelee vaihtavansa etähallintaohjelmia, koska yrityksessä on välillä asiakkaita, jotka eivät ole yrityksen omassa verkossa ja heidän pitäisi kuitenkin saada näillekin tietokoneille yhteys. LapIT:llä etähallintaohjelmien tietoturvasta on huolehdittu niin, että työasemat on vakioitu tietoturvapolitiikan mukaisesti ja etähallintaohjelmissa määritellään henkilökohtaiset käyttäjätunnus ja salasana. Kyseiset tunnukset täytyy olla liitettynä tiettyyn ad-ryhmään, jolla on oikeus operoida työasemaa. (Aaltonen 2012.)

5 TIETOKONEEN ETÄHALLINTA KOTIKÄYTÖSSÄ

5.1 Kotikäyttö

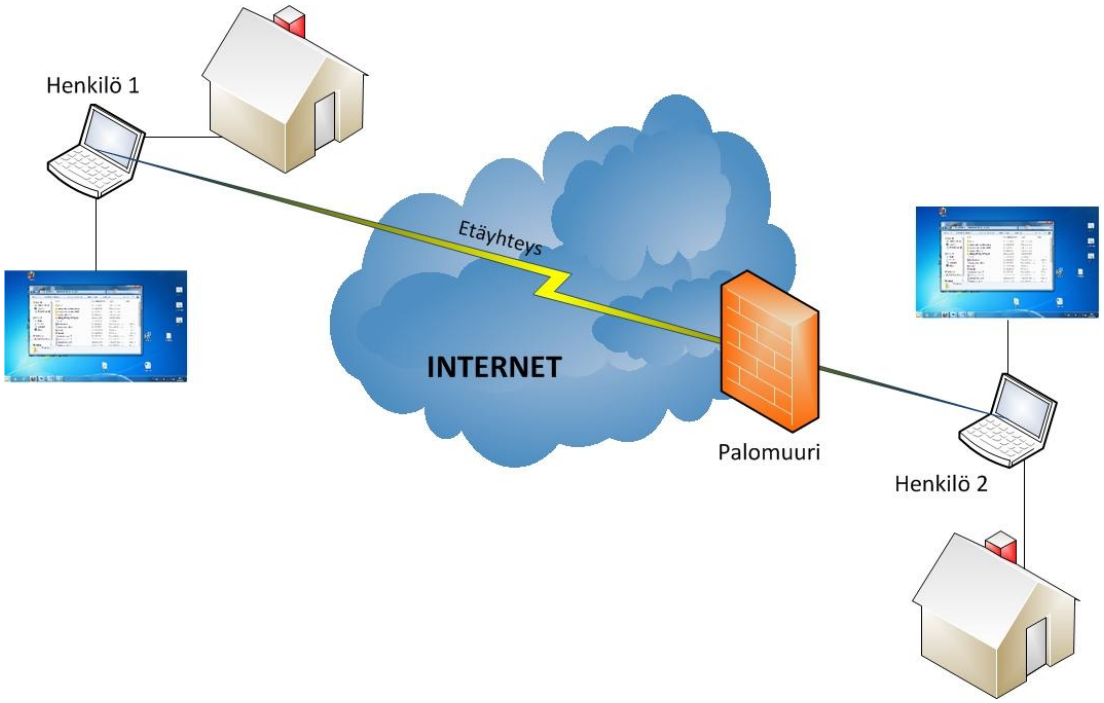
Vaikka etähallinnan käyttö onkin suositumpaa yrityksissä kuin kotikäytössä, niin myös kotikäytössä sitä voidaan hyvin hyödyntää. Otetaan kaksi esimerkkitapausta, missä kotikäyttötilanteissa etähallintaa voidaan hyödyntää:

Esimerkki 1: Henkilö X soittaa Helsingistä tietokoneista tietävälleen kaverilleen Rovaniemelle kysyäkseen tietokoneessa olevastaan ongelmasta. Kaveri ei osaa puhelimessa ratkaista tilannetta, joten hän ottaa etäyhteydellä kaverinsa tietokoneen hallintaansa. Tämän jälkeen Henkilö X pystyy näyttämään ongelman kaverilleen ja kaveri pystyy näyttämään ongelmaan ratkaisun. Vaikka välimatka on Helsingistä Rovaniemelle, ei se hidasta toimintaa millään tavalla. Kummassakin päässä täytyy vain olla internet yhteys käytössä.

Esimerkki 2: Henkilö X omistaa kaksi tietokonetta. Henkilö lähtee Suomesta ulkomaan matkalle ja ottaa toisen tietokoneensa mukaan, mutta toinen tietokone jää kotia. Matkalla hän huomaa, että kotia jääneeseen tietokoneeseen on jäänyt tärkeitä tiedostoja, joita hän tarvitsee. Hän ottaa mukana olevalla tietokoneellaan etäyhteyden kotona olevaansa tietokoneeseen ja ottaa sen etähallintaansa. Tämän jälkeen hän pystyy siirtämään kotona olevasta tietokoneesta tarvitsemansa tiedostot mukana olevaan tietokoneeseen. Vaikka välimatkassa olisi eroa tuhansia kilometrejä, ei se hidasta toimintaa. Kummassakin tietokoneessa täytyy olla internet yhteys käytössä, sekä kotia jääneessä tietokoneessa täytyy myös olla virta päälle kytkettynä.

Yritys ja kotikäytössä on se suuri ero, että kotikäytössä etähallintaa joudutaan käyttämään suurimmaksi osaksi internetin yli, kun taas yrityskäytössä etähallinta onnistuu monesti yrityksen oman lähiverkon kautta. Nimenomaan käytettäessä etähallintaa internetin kautta on kiinnitettävä suurta huomiota siihen, että tietosi eivät joudu vääriin käsiin. Turvallisuus ja tietosuoja ovat avainasemassa, kun kysymys on tällaisesta ohjelmasta.

Kuviossa 15 nähdään esimerkki etähallinnasta kotikäyttöympäristössä. Henkilö 1 on ottanut etäyhteyden henkilöön 2 internetin yli ja yhteys menee palomuurin läpi. Henkilö 1 tietokoneen näytössä näkyy sama kuva kuin mikä on henkilö 2 omassa tietokoneessa.



Kuvio 15. Tietokoneen etähallinta kotikäytössä.

Kuten yrityskäytössäkin, myös kotikäytössä molemmissa etäyhteyttä muodostamassa olevissa laitteissa on oltava etähallintaohjelmisto asennettuna oikeina määritetyillä asetuksilla. Palomuuriin on myös sallittava liikenne tälle etäyhteydelle.

Kotikäyttöön soveltuvia etähallintaohjelmia on monia, vaikka suurin osa etähallintaohjelmista onkin tehty yrityskäyttöön. Monia näistä ns. yritys-etähallintaohjelmista voidaan silti myös käyttää kotikäytössä. Tutkin tässä osiossa etähallinnan käyttöä nimenomaan kotikäytössä. Kotikäytön kannalta tärkeitä kriteereitä ohjelmaa valittaessa ovat ohjelman käyttöönotto, käytettävyys ja tietoturva sekä tiedonsiirto. Valitsin kaksi etähallintaohjelmistoa tutkinnan kohteeksi jossa tarkastelen näitä asioita. Ohjelmat ovat TeamViewer sekä NetOp Remote Control.

Suoritin tutkimukseni käyttäen kahta tietokonetta, pöytä- ja kannettavaa tietokonetta, jotka toimivat eri verkossa. Työn liitteenä on taulukko, jossa ovat molempien tietokoneiden järjestelmätiedot.

5.2 TeamViewer

5.2.1 Tietoa ohjelmasta

TeamViewer on TeamViewer GmbH kehittämä etäkäyttöohjelma, joka on perustettu Saksassa vuonna 2005. Yritys tekee päätoimisesti online-yhteistyöhön ja kommunikaatioon perustuvia sovelluksia. Yrityksen nopean alun ja suuren kasvun seurauksena ohjelma on asennettu yli 100 000 000 kertaa yli 200 maassa kaikkialla maailmassa. TeamViewer onkin yksi maailman johtavista etähallintaan erikoistuneista ohjelmista. Ohjelma on tällä hetkellä saatavana 30 eri kielellä. Yrityksen kehittämä perusteknologia pyörittää TeamViewerin maailmanlaajuisia serveriverkkoja, jotka puolestaan reitittävät yhteydet pohjautuen geolokalisaatioteknologiaan. (TeamViewer 2012e.)

TeamViewer on helppokäyttöinen ja yksityiskäyttöön täysin ilmainen ohjelma, joka on saatavilla myös suomen kielellä. Ohjelma toimii kolmella käyttöjärjestelmällä, Windowsilla, Linuxilla ja Macilla sekä myös iPhone, iPad ja Android järjestelmissä. TeamViewer toimii palomuurien ja NAT-reitittimien läpi eikä vaadi toimiakseen mitään ylimääräisiä asetuksia. TeamViewerillä on mahdollisuus ottaa yhteys autettavaan henkilöön myös www-selaimella, jolloin auttaja ei tarvitse mitään ylimääräistä ohjelmaa. (TeamViewer 2012a.) Testasin TeamVieweriä Windowsin käyttöjärjestelmien välillä sekä myös Windows- ja MAC- käyttöjärjestelmien välillä.

5.2.2 Ohjelman käyttöönotto

Ohjelman käyttämiseksi täytyy ensimmäiseksi ladata internetistä TeamViewer-ohjelma. TeamVieweristä on ladattavissa useita eri paketteja jotka on suunniteltu eri tarkoituksiin. Tietokoneen etähallitsija tarvitsee tietokoneelleen TeamViewer täysversio -paketin, joka on ns. All-In-One-paketti, jossa on kaikki ohjelman ominaisuudet. Tällä paketilla on mahdollista antaa sekä vastaanottaa etätukea. Myös etähallittava henkilö voi ladata tietokoneelleen täysversion, mutta käytännössä kuitenkin riittää, että etähallittavan tietokoneelle ladataan ohjelmasta kevyempi versio, TeamViewer QuickSupport -paketti, jonka asennus ja käyttö ovat helpompaa.

Ohjelman asennustiedostot voi ladata internetistä vapaasti ilman rekisteröitymisiä. Latasin ohjelmasta näiden kahden paketin uusimmat versiot niiden

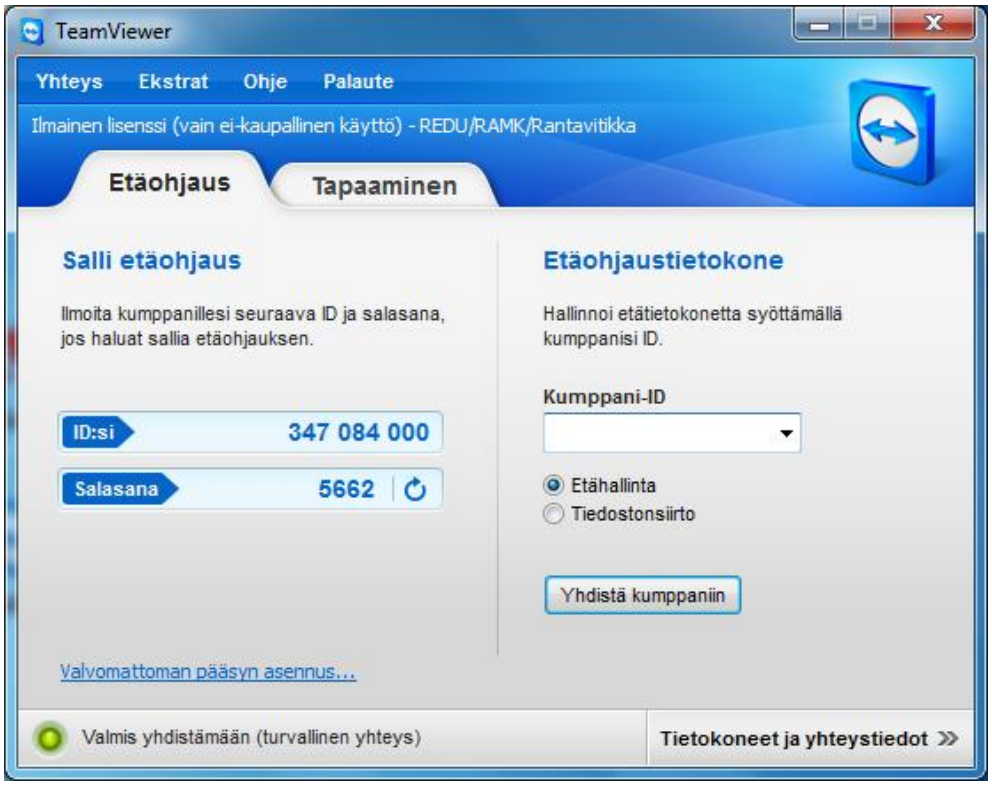
käyttämistä ja testaamista varten. Ohjelman uusin versio tässä testissä on v7.0.12541 ja täysversio-paketin koko on 3,9 MB sekä QuickSupport-paketti 3,3 MB (TeamViewer 2012b).

TeamVieweristä voi myös ostaa lisenssin, jolloin kaupallinen käyttökin on sallittua. Jos käyttäjä ei ole täysin tyytyväinen, tilauksen voi peruuttaa seitsemän päivän aikana ilman, että tarvitsee selittää sitä mitenkään. (TeamViewer 2012d.)

Kun tiedostot on ladattu tietokoneelle, voidaan aloittaa TeamViewer-ohjelman asennus. TeamViewer täysversio -pakettia ei välttämättä tarvitse edes asentaa jotta sitä pystytään käyttämään, mutta etähallitsijan kannattaa kuitenkin yleensä asentaa ohjelma. TeamViewer täysversio -asennuksen alussa ohjelma kysyykin, että asennetaanko ohjelma vai käynnistäänkö se ilman asennusta.

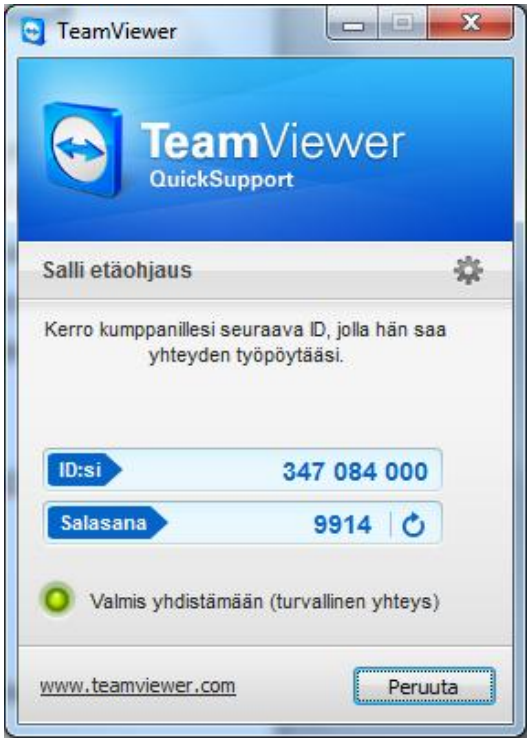
Asennuksen yhteydessä TeamViewer kysyy myös, että haluatko myöhemmin pääsyn tietokoneelle, jolle asennat TeamVieweriä tällä hetkellä. Tällä asetuksella voidaan asettaa TeamViewer-ohjelmaan kiinteä salasana, jonka avulla TeamVieweriä on mahdollista käyttää koska ja mistä tahansa käsin (tästä lisää luvussa 5.2.3). Kiinteää salasanaa ei voi asettaa, jos ohjelma käynnistetään ilman asennusta.

Tämän jälkeen ohjelma asentuu ja on käyttövalmis. Kun ohjelma käynnistetään, avautuu ohjelman aloitusikkuna (kuvio 16), johon ohjelma antaa tietokoneesi ID-numeron sekä kertakäyttöisen salasanan. Näiden tietojen avulla etähallitsijan on mahdollisuus ottaa tietokoneesi hallintaan. Jos taas halutaan itse ottaa toinen tietokone hallintaan, ikkunassa olevaan Kumppani-ID sarakkeeseen syötetään etähallittavan tietokoneen ID-numero.



Kuvio 16. TeamViewer täysversio -ohjelman aloitusikkuna.

Etähallittavalle henkilölle asennettava TeamViewer QuickSupport -paketti ei vaadi minkäänlaista varsinaista asennusta. Ladattu tiedosto täytyy vain aukaista, ja ohjelma on käyttövalmis. Käyttäjälle avautuu ikkuna, jossa ohjelma antaa tietokoneen ID-numeron sekä kertakäyttöisen salasanan (kuvio 17).



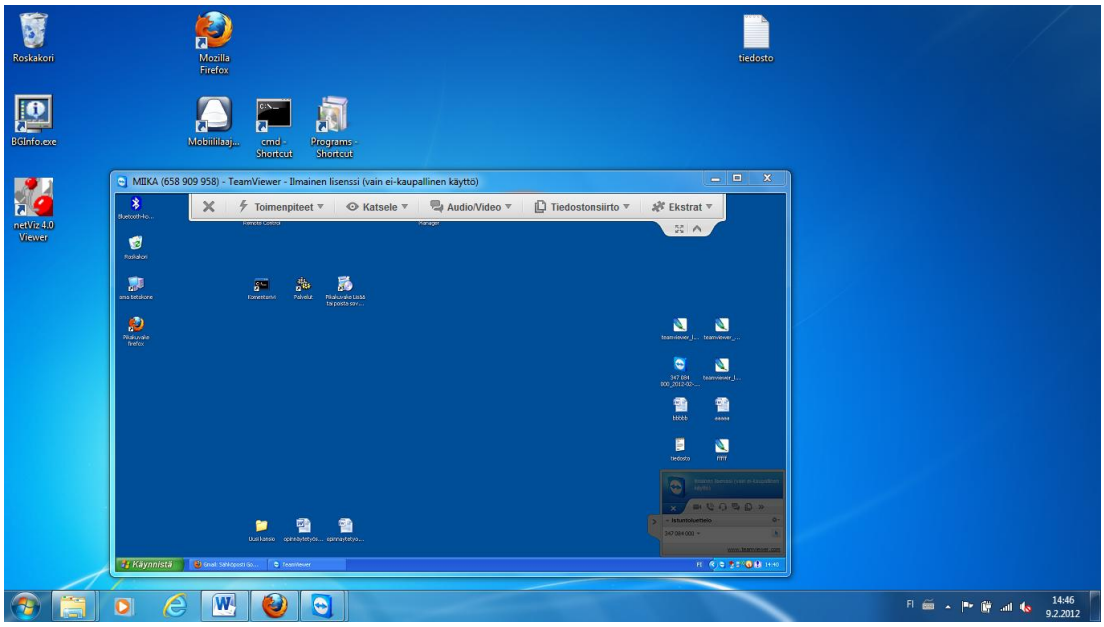
Kuvio 17. TeamViewer QuickSupport -ohjelman aloitusikkuna.

Niin kauan kuin tiedosto on avoinna, pääsy tietokoneelle on mahdollista samoilla tunnuksilla, mutta kun tiedosto on suljettu, ei tietokoneelle ole enää mahdollista päästä. QuickSupport-paketilla on mahdollisuus vain vastaanottaa etätukea.

5.2.3 Etähallinta

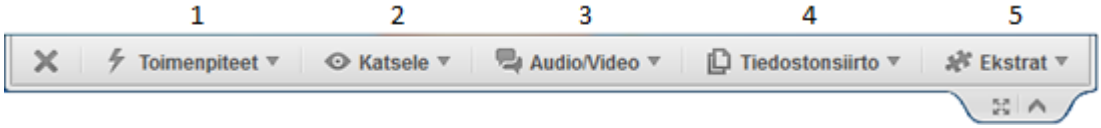
TeamViewer-ohjelman toiminta perustuu ID-numeroihin, jonka se luo jokaiselle käyttäjälle joka käynnistää ohjelman. ID-numero on yksilöllinen tunnus, josta käyttäjät voidaan tunnistaa. ID-numeron lisäksi jokaisella tietokoneella on oma salasana. Salasana on oletuksena kertaluontoinen, jonka ohjelma luo käyttäjälle aina uudelleen kun ohjelma avataan uudestaan.

Perusoletuksena on, että kun halutaan hallita toisen tietokonetta TeamViewerin etäohjauksen avulla, tulee kummassakin tietokoneessa olla käynnistettynä ohjelma. Etähallitsija kirjoittaa etähallittavan tietokoneen henkilöltään saamansa ID-numeron TeamViewer aloitusikkunassa olevaan sarakkeeseen (kuvio 16). Tämän jälkeen ohjelma kysyy vielä etähallittavan salasanaa. Salasanan kirjoittamisen jälkeen ohjelma yhdistyy etähallittavan henkilön tietokoneeseen ja etäohjausikkuna aukeaa, jossa on etähallittavan tietokoneen työpöytä (kuvio 18). Nyt etäohjaus on käytössä ja toisen tietokoneen hallinta onnistuu.



Kuvio 18. TeamViewer-ohjelmassa etäyhteys muodostettuna.

TeamViewer-ohjelmalla on mahdollisuus tehdä eri toimintoja etäyhteyden aikana ja näitä toimintoja voi säädellä etäohjausikkunan asetuspalkista (kuvio 19). Käyn asetuspalkin toiminnot läpi kuvion 19 numeroinnin mukaan.



Kuvio 19. TeamViewer-ohjelman etäohjausikkunan asetuspalkki.

1) Toimenpiteet
   - Vaihda puolia kumppanin kanssa. Vaihtaa niin, että etähallitsijasta tulee etähallittava ja etähallittavasta etähallitsija.
   - Ctrl+Alt+Del näppäinyhdistelmä etähallittavan tietokoneelle.
   - Lukitse, kirjaa ulos, uudelleenkäynnistä tai uudelleenkäynnistä vikasietotilassa etähallittava tietokone.
   - Näytä musta ruutu etähallittavan tietokoneen näytöllä. Tämän toiminnon ollessa päällä etähallittava ei näe mitä etäohjauksen aikana tapahtuu eikä pysty tekemään mitään.
2) Katsele
   - Etäohjausikkunan laadun ja resoluution asetukset.
   - Valitse yksi ikkuna/Valitse koko työpöytä. Valittaessa yksi ikkuna etäohjausikkunassa käsitellään vain valittua ikkunaa.
   - Poista taustakuva etähallittavasta tietokoneesta.
   - Näytä hiiren etäkursori etähallittavasta tietokoneesta.
3) Audio/Video
   - VoiP-puhelu. Siirtää mikrofoniäänet puolelta toiselle ja mahdollistaa näin puheyhteyden etähallinnan aikana.
   - Omat videot. Näyttää omaa webkamera kuvaa etähallittavalle tietokoneelle. Myös etähallittavan on mahdollista näyttää omaa webkamerakuvaa.
   - Chat -keskustelu etähallittavan kanssa.
   - Neuvottelupuhelu
4) Tiedostonsiirto
   - Tiedostonsiirto, aukaisee tiedonsiirtoikkunan.

- Tiedostolaatikko, aukaisee ns. jaettavan kansion, jonne on mahdollista laittaa tiedostoja jotka toinen osapuoli voi ladata sieltä omalle tietokoneelleen.

5) Ekstrat
   - Näyttökuva etähallittavan tietokoneen työpöydästä.
   - Mahdollisuus tallentaa etäohjaus.
   - VPN -yhteys.
   - Mahdollisuus päivittää etähallittavan TeamViewer-ohjelmistoversio.
   - Etätietokoneen järjestelmätiedot.
   - Lisäksi Ekstrat kohdan alapuolella olevasta  -merkistä on mahdollisuus laittaa etäohjausikkuna koko näytön kokoiseksi.

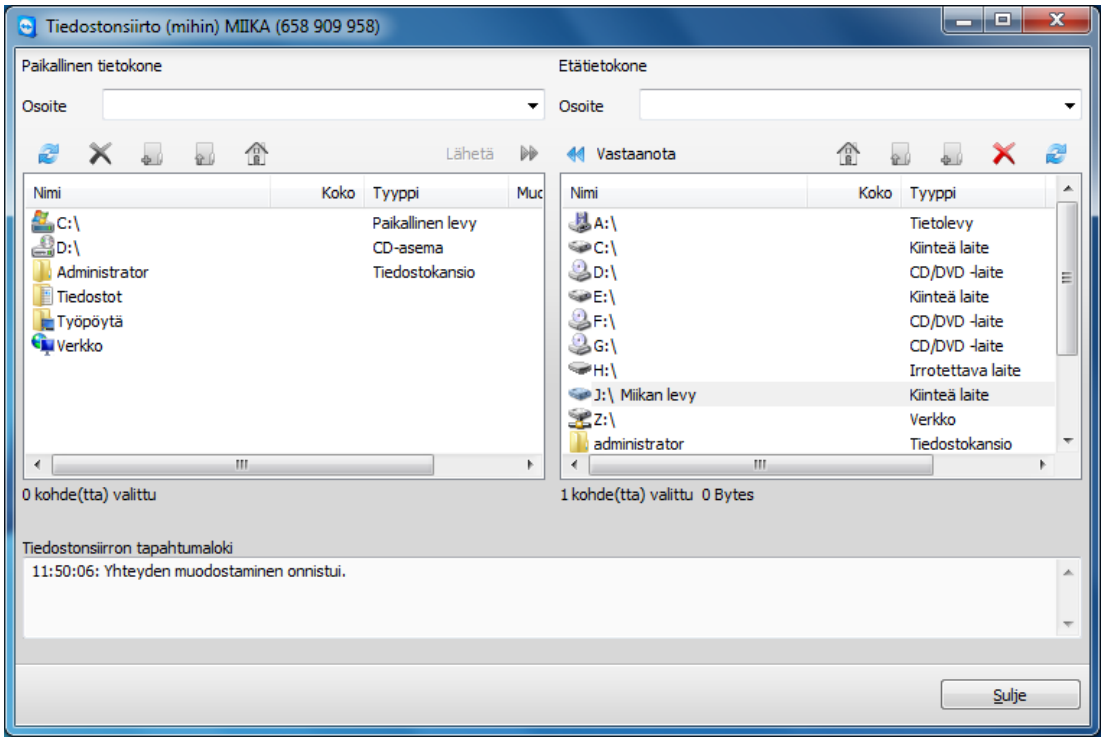
TeamViewer-ohjelmalla on mahdollisuus myös etähallita toista tietokonetta asentamatta mitään ohjelmaa sille tietokoneelle, jolla halutaan ottaa etäyhteys toiseen tietokoneeseen. Tämä etäyhteys tapahtuu internetselaimen kautta. Tätä toimintoa varten täytyy rekisteröityä TeamViewer-ohjelman internetsivuilla. Rekisteröityminen on ilmaista ja tunnukset ovat heti käytössä. Tämä mahdollistaa sen, että henkilö voi ottaa etäyhteyden toiseen tietokoneeseen mistä tietokoneelta vain, kunhan internetyhteys on käytössä. Etähallittaessa internetselaimen kautta edellä käydyt toiminnot ovat paljon suppeammat, eivätkä kaikki ominaisuudet ole käytettävissä.

Rekisteröitymisen jälkeen on mahdollista tallentaa tärkeimpien tietokoneiden ID-numerot ja salasanat (salasana vain, jos salasana on kiinteä) omalle yhteystietolistalleen, josta yhdistäminen onnistuu paljon vaivattomammin ja nopeammin.

Kiinteän salasanan asettaminen mahdollistaa sen, että etätietokoneelle on mahdollista päästä milloin vain, ns. 24/7, eikä kenenkään tarvitse päivystää toisessa päässä. Etätietokoneen täytyy vain olla käynnissä. Tämän toiminnon ollessa päällä TeamViewer-ohjelma käynnistyy aina itsestään tietokoneen käynnistyksen yhteydessä. (TeamViewer 2012a.)

5.2.4 Tiedonsiirto

Etähallinnan aikana on mahdollisuus avata tiedonsiirtoikkuna (kuvio 20), jonka avulla voi siirtää tiedostoja tietokoneelta toiselle.

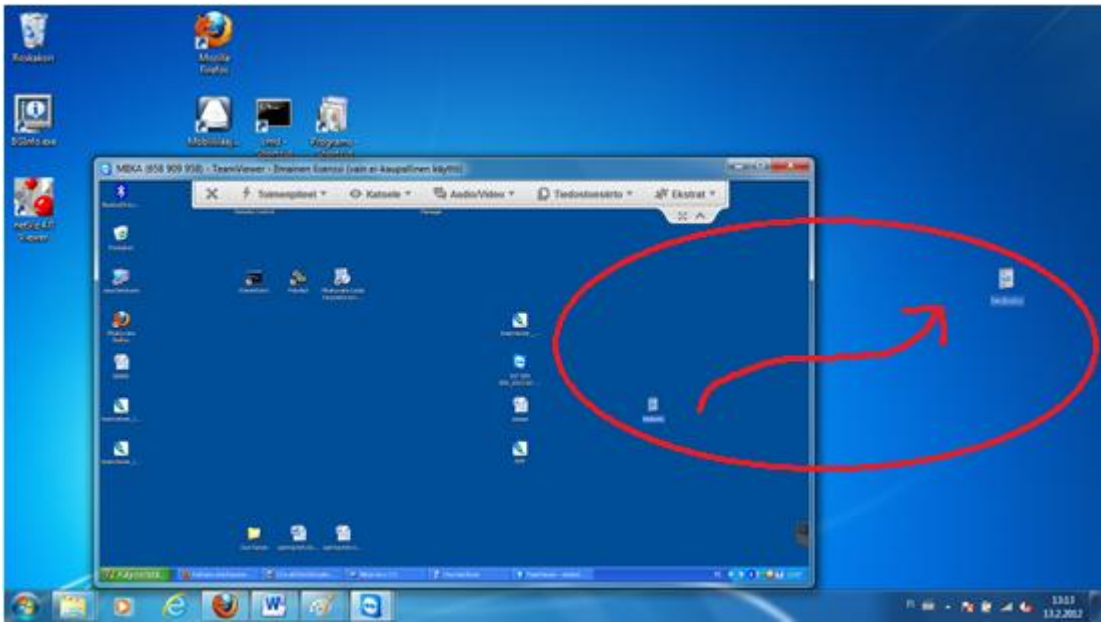


Kuvio 20. TeamViewer-ohjelman tiedonsiirtoikkuna.

Tiedonsiirtoikkunassa voi siirtää tiedostoja, jolloin tiedosto aina kopioituu toiselle tietokoneelle, poistaa tiedostoja ja luoda uusia kansioita.

TeamViewer-ohjelmalla on mahdollisuus yhdistää etätietokoneeseen vain myös pelkkää tiedonsiirtoa varten yhdistämättä ollenkaan etäohjausta. Tällöin aukeaa vain tiedonsiirtoikkuna, joka on samanlainen kuin etähallinnan aikana toteutetussa tiedonsiirrossa (kuvio 20).

TeamViewerissä on mahdollisuus siirtää tiedostoja ns. Vedä ja pudota -toiminnon avulla. Tämä toiminto nopeuttaa tiedostojen siirtoa ja mahdollistaa myös etäohjauksen samanaikaisesti. Tällä toiminnolla voi kopioida tiedostoja omalta tietokoneelta etätietokoneelle tai päinvastoin. Tässä etähallitsijan tarvitsee vetää haluamansa tiedosto joko etäohjausikkunasta omalle tietokoneelleen tai omalta tietokoneeltaan etäohjausikkunaan ja pudottaa se sitten haluamaasi kohtaan kuvion 21 kaltaisesti. Tällä toiminnon avulla voi helposti kopioida tiedostoja tai kokonaisia kansioita etätietokoneelle ja etätietokoneelta. (TeamViewer 2012a.)



Kuvio 21. TeamViewer-ohjelman tiedonsiirron Vedä ja pudota -toiminto.

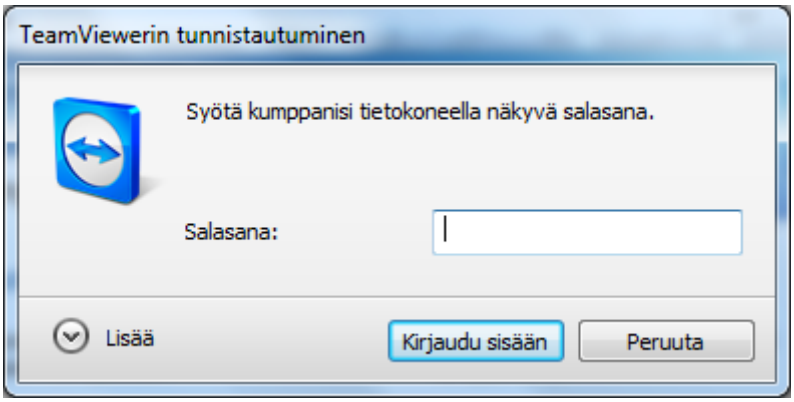
5.2.5 Tietoturva

”TeamViewer toimii täydellisellä salauksella RSA julkisen/yksityisen avainsalausprotokollan ja AES (256 bit) istuntosalauksen pohjalta. Tätä tekniikkaa käytetään myös https/SSL-suojauksessa, ja se on tämänhetkisen tekniikan tason mukaisesti täysin varma. Koska Private Key ei koskaan lähde asiakkaan tietokoneesta, tällä menetelmällä on varmistettu teknisesti, että internetissä väliin kytketyt tietokoneet eivät pysty purkamaan salausta, tämä koskee näin ollen myös TeamViewer-reititinpalvelinta.” (TeamViewer 2012c.)

TeamViewer-ohjelmassa on muutamia tietoturvan liittyviä menetelmiä, joita henkilön, jonka tietokonetta etähallitaan, on mahdollista tehdä tietoturvan edistämiseksi. Näitä toimintoja ovat:

1) ID-numero ja salasana

   Automaattisesti luodun Kumppani-ID:n lisäksi TeamViewer luo dynaamisen istuntosalasanan. TeamViewer kysyy etähallitsijalta salasanaa (kuvio 22) joka kerta, kun hän yrittää yhdistää etähallittavaan tietokoneeseen.



Kuvio 22. TeamViewer kysyy istuntosalasanaa.

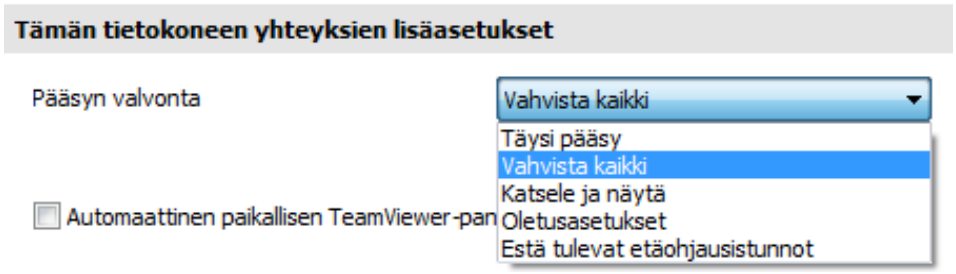
Istuntosalasana on oletuksena neljän merkin mittainen, mutta se kannattaa muuttaa pidemmäksi. Sen voi halutessaan muuttaa joko kuuden, kahdeksan tai 10 merkin mittaiseksi. Istuntosalasana muuttuu vakiosäädössä jokaisella käynnistyksellä. Salasanan voi kuitenkin asettaa muuttumaan vielä jopa joka yhteyden jälkeen. Tämä tarjoaa lisäturvallisuutta asiatonta järjestelmään pääsyä vastaan. (TeamViewer 2012a.)

2) Käyttäjän määrittely

Etähallittava henkilö voi tehdä ns. Black and Whitelist -luettelon, jolla hän voi halutessaan estää joitain tiettyjä käyttäjiä muodostamasta yhteyttä tietokoneeseensa tai sallia vain tiettyjen käyttäjien yhteydenmuodostuksen. Luetteloon kirjoitetaan halutun henkilön tietokoneen ID-tunnus.

3) Pääsyn Valvonta

TeamViewer-ohjelmassa on mahdollisuus muuttaa pääsyn valvonta asetuksia (kuvio 23). Näillä asetuksilla määritetään, minkälaiset oikeudet etähallitsijalle annetaan.



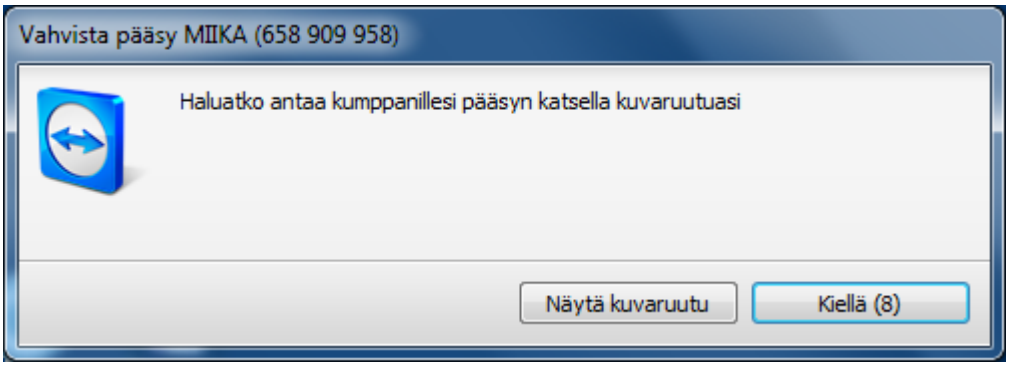
Kuvio 23. TeamViewer-ohjelman Pääsyn valvonta -asetukset.

Kuvion 23 mukaisista vaihtoehdoista Täysi pääsy antaa etähallitsijalle täydet oikeudet etähallittavaan tietokoneeseen. Vahvista kaikki toiminnol-

la taas etähallitsija joutuu kysymään lupaa kaikkiin toimintoihin. Tämä toiminto on turvallisin ja sitä kannattaa yleensä käyttää. Katsele ja näytä toiminnolla etähallitsija pystyy vain katselamaan etätietokoneen näyttöä ja osoittamaan kursorilla jotain tiettyä kohtaa, mutta ei voi itse valita eikä tehdä mitään muutoksia. Oletusasetuksilla on itse mahdollisuus muokata pääsyoikeuksia kutakin toimintoa varten.

4) Kulunvalvonta

Jos pääsyn asetuksista on niin määritelty, tärkeät toiminnot, kuten etähallinta ja tiedonsiirto, vaativat ylimääräisen, manuaalisen vahvistuksen käyttäjältä (kuvio 24).



Kuvio 24. TeamViewer kysyy pääsyn vahvistamista.

5.2.6 Muuta

TeamViewer-ohjelmalla voidaan luoda myös Tapaaminen monen henkilön kanssa. Tapaamisilla on mahdollisuus pitää koulutustilaisuuksia ja esittelyitä tai tehdä ryhmätöitä keskenään. Tämä toiminto on tarkoitettu enemmänkin yrityskäyttöön kuin kotikäyttöön. Tapaamiseen liittyminen perustuu samalla tavalla ID-numeroihin kuin etäohjauskin. Yksi henkilö luo tapaamisen, johon ohjelma luo oman yksilöllisen ID-tunnuksen. Henkilö voi lähettää tapaamisesta kutsun sähköpostilla muille osallistujille. Osallistujat voivat osallistua tapaamiseen napsauttamalla kutsusähköpostin linkkiä tai kirjautumalla suoraan internetselaimella tai TeamViewer-ohjelmalla. (TeamViewer 2012a.)

TeamVieweriä on mahdollisuus käyttää myös mobiililaitteissa. TeamViewer App -sovellus mahdollistaa etäpääsyn tietokoneelle iPhonella, iPod touchilla,

iPadilla ja Android -laitteilla. Tiedonsiirto ja kokouksiin osallistuminen on myös näillä mahdollista. (TeamViewer 2012a.)

Testasin myös etäohjausta ja tiedonsiirtoa Mac- ja Windows -käyttöjärjestelmien välillä. Yhteys onnistui, kun otti Windows-tietokoneelta yhteyden Mac-tietokoneeseen, mutta Mac-tietokoneelta ei saanut yhteyttä Windows-tietokoneeseen. Tämä johtui todennäköisesti siitä, että Mac-tietokoneelle ei ollut tarjolla yhtä uutta ohjelmistoversiota kuin Windows-tietokoneelle, joten jouduin käyttämään eri versioita. Windows-tietokoneelta onnistui hyvin etähallita Mac-tietokonetta, mutta tämä etäohjauksen aikainen ns. Vedä ja pudota -tiedonsiirto ei ollut mahdollista. Normaali tiedonsiirto onnistui, kun avasi yhteyden vain tiedonsiirtoa varten.

5.3 NetOp

5.3.1 Tietoa ohjelmasta

NetOp Solutions A/S on tanskalainen yhtiö, jonka pääkonttori sijaitsee Kööpenhaminassa. NetOp:n tytäryhtiöt Romaniassa tuottaa heidän ohjelmistojaan. NetOp:n myyntikonttoreita on Yhdysvalloissa, Britanniassa, Sveitsissä ja Kiinassa sekä he myyvät ohjelmistoja julkisille ja yksityisille asiakkaille 80 maassa. Yhtiö perustettiin vuonna 1981, mutta sen ensimmäinen etähallinta versio, NetOp Remote Control, perustettiin vuonna 1987. (NetOp 2009.)

NetOp Remote Control -ohjelmaa käytetään pääasiallisesti yrityksen tietoverkkojen etähallinnointiin, sovelluksien etäkäyttöön sekä muuten etätuen työkaluna (Nocom Software 2012). Valitsin tämän ohjelman kuitenkin tähän kotikäyttövertailuun, koska tällä ohjelmalla onnistuu sujuvasti myös yhdistäminen internetin yli, joka näin myös mahdollistaa kotikäytön.

NetOp Remote Control -ohjelman tärkeimpiä ominaisuuksia ovat kattava suojaus ja turvallisuusjärjestelmä. NetOp Remote Control on saatavilla usealle eri käyttöjärjestelmille: Windows, Linux, Mac, Solaris ja OS/2. NetOp:lla on saatavilla myös mobiililaitteille oma sovellus. NetOp on maksullinen ohjelma ja siihen on saatavilla suomenkielinen käyttötuki. (Nocom Software 2012.)

5.3.2 Ohjelman käyttöönotto

Jotta ohjelmaa voidaan alkaa käyttämään, täytyy ensimmäiseksi ladata internetistä NetOp-ohjelma. Ohjelma on maksullinen, mutta siitä on mahdollisuus ladata ilmaiseksi 30 päivän kokeiluversio. Sivuille täytyy ensin rekisteröityä ennen kuin pystyy lataamaan NetOp:n ohjelmistoja. Rekisteröityminen tapahtuu NetOp:n internet-sivuilla. Rekisteröitymisen jälkeen tunnukset ovat heti voimassa. NetOp lähettää myös latauslinkin rekisteröitymisen yhteydessä antamaasi sähköpostiin. Sähköpostiin tulee myös tiedot ohjelmiston vaatimista lisenssiavaimista.

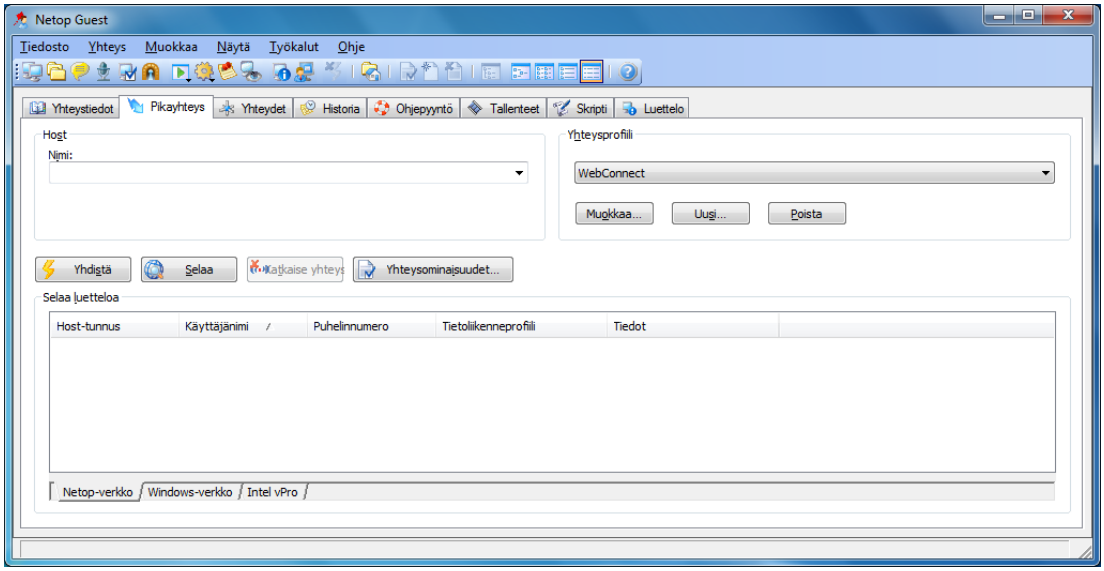
Ladattavissa ovat nyt kaikki NetOp Remote Control -moduulit, joita on yhteensä viisi kappaletta: Guest, Host, Gateway, Security Server ja Name Server. Guest-moduuli asennetaan tietokoneeseen, josta on tarkoitus etähallita toista tietokonetta. Etähallittavaan tietokoneeseen taas asennetaan erikseen asennettava Host-moduuli. Guest-moduuli mahdollistaa tietokoneen etähallitsemaan mitä tahansa toista tietokonetta, jossa on aktiivinen Host-moduuli. Gateway sovellus on Host-moduuli, jossa on reititintoimintoja NetOp-liikennettä varten, Security Server on Host-moduuli, joka keskittää tietoturvahallinnon ja lokimerkinnät ja Name Server on Host-moduuli, joka rekisteröi NetOp nimiä ja muuntaa niitä IP-osoitteiksi. (NetOp 2012.)

Ohjelman testausta ja käyttöä varten latasin ja asensin Guest ja Host -moduulit. Kun otetaan huomioon, että ohjelma tulee kotikäyttöön eikä käyttö ole näin kovin suurta, nämä kaksi moduulia riittävät. Guest-moduuli asennetaan etähallitsijan tietokoneelle, joka on ns. Guest-käyttäjä ja Host-moduuli etähallittavan tietokoneelle, joka on ns. Host-käyttäjä. Ohjelmasta on saatavilla useita kieliä. Asensin ohjelmasta suomenkielisen käyttöliittymän. Ohjelman uusin versio on versio 11 ja tiedostojen koot ovat: Guest 12.1 MB ja Host 10.4 MB.

Asennettaessa Guest-moduulia tulee asennuksessa huomioida muutamia tärkeitä kohtia, jotta etäyhteys on myöhemmin mahdollista. Ensiksikin, jotta ohjelma toimisi kunnolla, ohjelmalle täytyy antaa lupa vastaanottaa saapuvaa verkkoliikennettä Windowsin palomuurin kautta. Loppuvaiheessa asennusta tulee määrittää WebConnect-asetukset. Asetuksessa täytyy sallia, että NetOp-moduulilla on mahdollisuus muodostaa yhteys muihin NetOp-

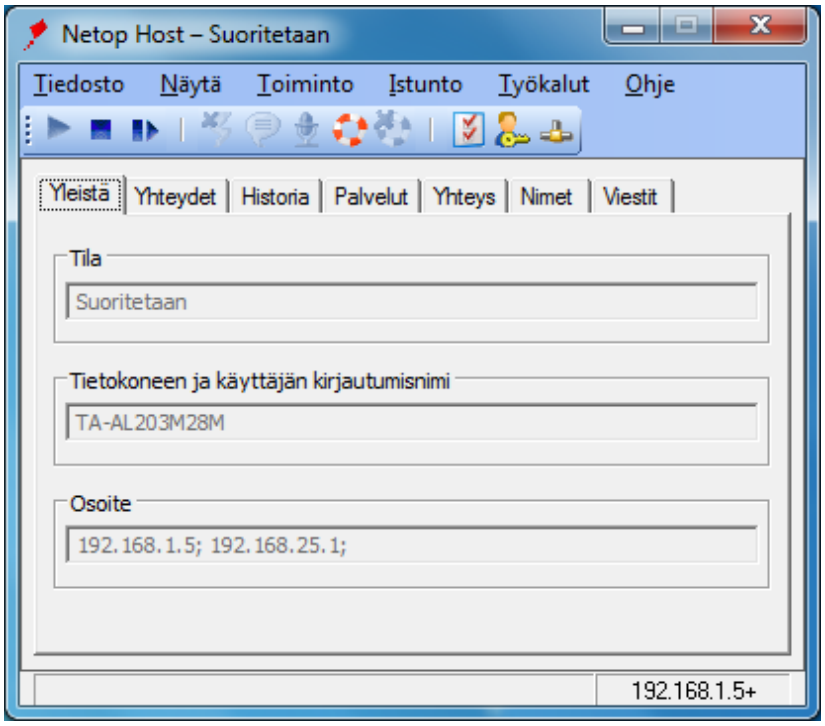
moduuleihin NetOp WebConnectin avulla. Näin yhdistäminen kumppaniin onnistuu internetin välityksellä.

Asennustoiminnon loputtua on ohjelma käyttövalmis. Kun ohjelma käynnistetään, avautuu ohjelman aloitusikkuna (kuvio 25), johon tulee antaa etähallittavan tietokoneen nimi ja valita yhteysprofiili.



Kuvio 25. NetOp Guest -ohjelman aloitusikkuna.

Asennettaessa Host-moduulia on tärkeää huomioida kohta, missä määritetään Guest-käytön oletussalasana. Vakiosäädöissä tätä salasanaa tarvitaan silloin, kun Guest-käyttäjä yhdistää Host-käyttäjään. Salasana on mahdollista vaihtaa myöhemmin. Host-moduulin asennuksessa tulee myös määrittää WebConnect-asetukset. Asennustoiminnon loputtua on ohjelma käyttövalmis. Kun ohjelma käynnistetään, avautuu ohjelman aloitusikkuna (kuvio 26), mistä näkee Host-moduulin tilan (onko Host käynnissä vai kiinni) ja oman tietokoneensa kirjautumisnimen.

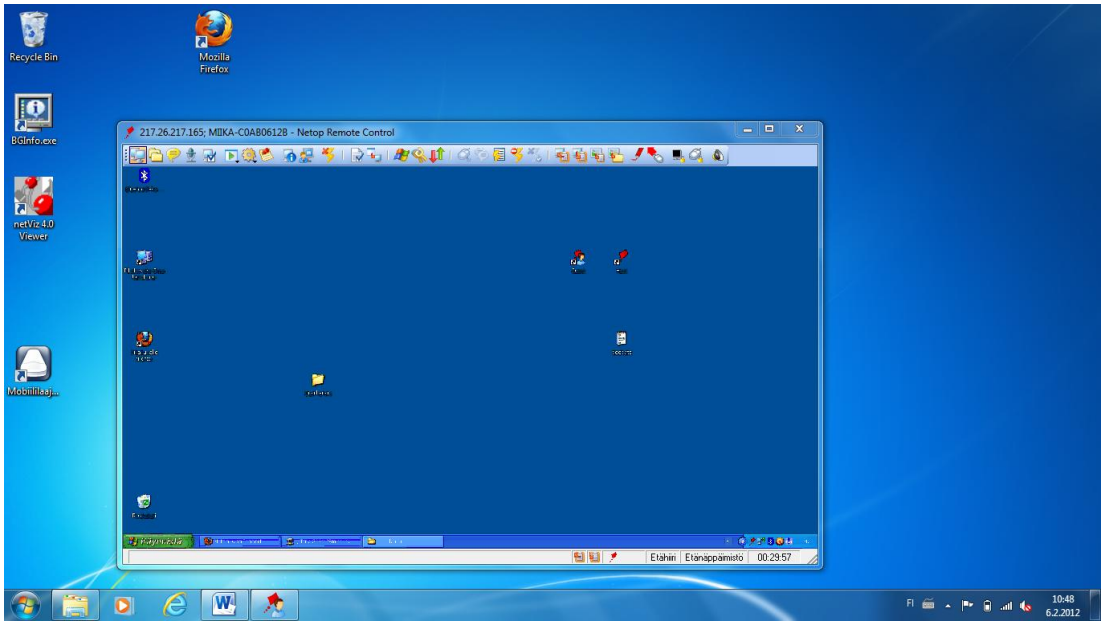


Kuvio 26. NetOp Host -ohjelman aloitusikkuna.

5.3.3 Etähallinta

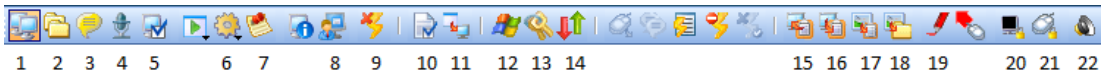
NetOp-ohjelman toiminta perustuu WebConnect-palveluun, jonka asetukset määriteltiin NetOp-moduulien asennusvaiheessa. WebConnect-palvelu tarjoaa Netop-moduuleille internet-yhteyden, jonka avulla ne voivat muodostaa yhteyden muihin NetOp-moduuleihin käyttämällä samaa palvelua.

Kun halutaan yhdistää tietokone toiseen tietokoneeseen NetOp Remote Control -ohjelman avulla, tulee etähallitsijan tietokoneessa olla päällä Guest-moduuli ja etähallittavalla Host-moduuli. Kun TeamViewer-ohjelma yhdistettiin ID-numeron ja salasanan avulla, NetOp yhdistetään tietokoneen nimen sekä salasanan perusteella. Tietokoneen nimen ja salasanan voi itse valita haluamansa mukaan. Host-käyttäjän täytyy ilmoittaa Guest-käyttäjälle nämä tiedot, jotta yhdistäminen onnistuu. Guest-käyttäjän yhteysprofiilin täytyy olla WebConnect, jotta käyttäjä onnistuu yhdistämisessä. Guest-käyttäjä kirjoittaa Host-käyttäjän tietokoneen nimen Guest-ohjelman aloitusikkunassa olevaan nimi sarakkeeseen (kuvio 25). Tämän jälkeen ohjelma kysyy vielä etähallittavan tietokoneen salasanaa. Salasanan kirjoittamisen jälkeen ohjelma yhdistyy etähallittavan henkilön tietokoneeseen ja etäohjausikkuna aukeaa, jossa on etähallittavan tietokoneen työpöytä (kuvio 27). Nyt etäohjaus on käytössä ja toisen tietokoneen hallinta onnistuu.



Kuvio 27. NetOp-ohjelmassa etäyhteys muodostettuna..

NetOp-ohjelmalla on mahdollisuus tehdä eri toimintoja etäyhteyden aikana samalla tavalla kuin TeamViewer-ohjelmallakin. Toiminnot ovat hyvin pitkälle samankaltaisia molemmissa ohjelmissa. Toimintoja voi säädellä NetOp-etäohjausikkunan asetuspalkista (kuvio 28). Käyn toiminnot läpi kuvion 28 numeroinnin mukaan.



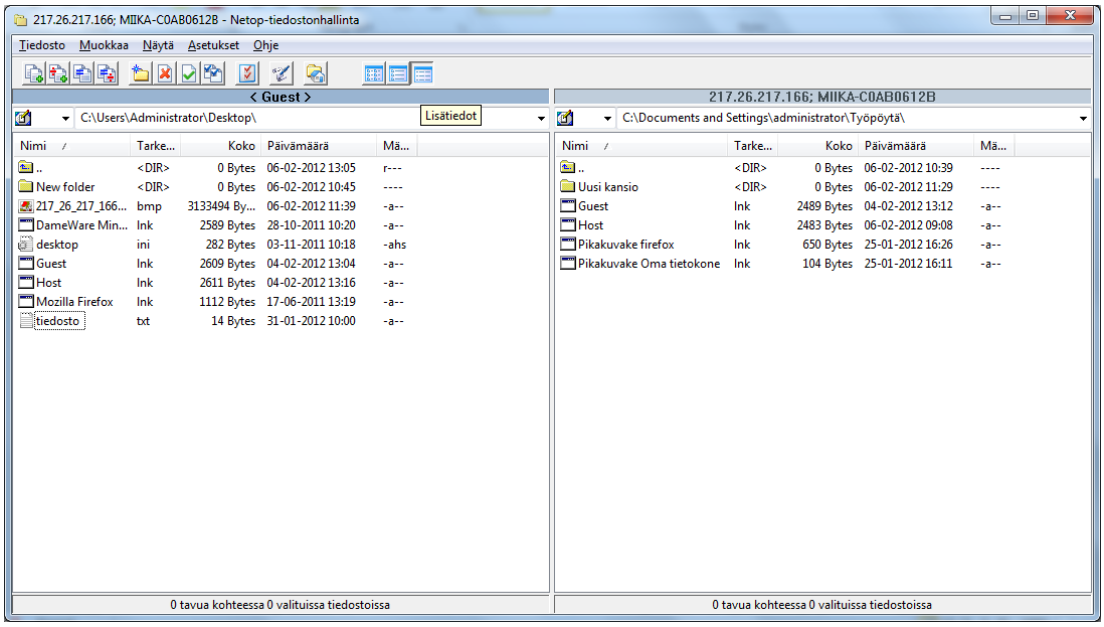
Kuvio 28. NetOp-ohjelman etäohjausikkunan asetuspalkki.

1) Yhdistää tai katkaisee etähallinta yhteyden.
2) Aukaisee tiedonsiirtoikkunan.
3) Aukaisee Chat-keskusteluikkunan.
4) Aukaisee puhe/video keskusteluyhteys-ikkunan.
5) Remote management, etähallittavan tietokoneen järjestelmäasetukset.
6) Kirjaudu ulos, käynnistä uudelleen, sammuta tai lukitse etähallittava tietokone.
7) Lähettää viestin omassa ikkunassaan etähallittavan tietokoneelle.
8) Näyttää näyttökuvaa etähallittavan tietokoneelle omasta tietokoneesta.
9) Lopeta etäyhteys.
10) Yhteysasetukset. Mm. näyttöön, työpöytään tai näppäimistöön/hiireen liittyviä asetuksia.
11) Aukaisee etäohjausikkunan koko ruudun kokoisena.

12) Aukaisee etähallittavan tietokoneen käynnistä valikon.
13) Tekee näppäinyhdistelmän Ctrl+Alt+Del etähallittavan tietokoneelle.
14) Käynnistää etähallittavan tietokoneen uudelleen.
15) Lähettää leikepöydän etähallittavan tietokoneeseen.
16) Ottaa leikepöydän etähallittavan tietokoneelta.
17) Tallentaa etähallittavan tietokoneen näytön leikepöydälle.
18) Tallentaa etähallittavan tietokoneen näytön valittuun tiedostoon.
19) Merkintätila. Tällä toiminnolla on mahdollista esimerkiksi piirtää tai korostaa jotain tiettyä kohtaa etähallittavan tietokoneen näytöllä. Merkinnät häviävät kun merkintätila otetaan pois käytöstä. Merkit eivät tallennu mihinkään.
20) Laittaa mustan ruudun etähallittavan tietokoneen näytölle. Tämän toiminnon ollessa päällä etähallittava ei näe mitä etäohjauksen aikana tapahtuu eikä pysty tekemään mitään.
21) Lukitsee etähallittavan tietokoneesta näppäimistön ja hiiren.
22) Siirtää mikrofoniäänet puolelta toiselle ja mahdollistaa näin puheyhteyden etähallinnan aikana.

5.3.4 Tiedonsiirto

Etähallinnan aikana on mahdollisuus avata tiedonsiirtoikkuna (kuvio 29), jonka avulla on mahdollisuus siirtää tiedostoja tietokoneelta toiselle.



Kuvio 29. NetOp-ohjelman tiedonsiirtoikkuna.

Tiedonsiirtoikkunassa tiedostoja voi siirtää tai kopioida tietokoneelta toiselle, synkronoida tai kloonata tiedostoja, poistaa tiedostoja sekä luoda uusia kansioita. Tiedonsiirto on mahdollista vaihtaa myös yhtä painiketta painamalla paikalliseksi, jolloin tiedostoja voi siirtää vain oman tietokoneen hakemistojen välillä.

NetOp-ohjelmassa on mahdollisuus yhdistää etätietokoneeseen myös vain pelkkää tiedonsiirtoa varten, samankaltaisesti kuin TeamViewer-ohjelmassakin. Tällöin aukeaa vain tiedonsiirtoikkuna, joka on samanlainen kuin etähallinnan aikana toteutetussa tiedonsiirrossa (kuvio 29).

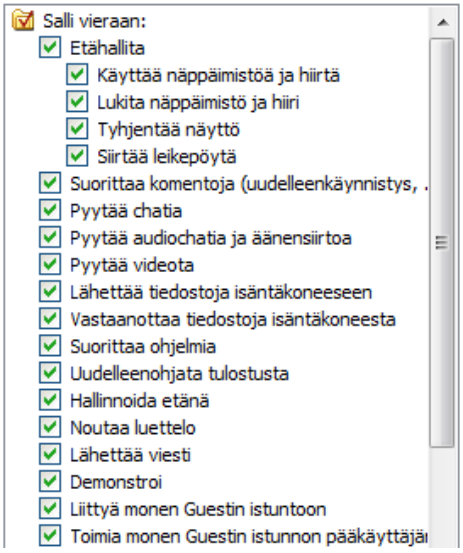
5.3.5 Tietoturva

NetOp Remote Control on suunniteltu niin, että kaikki henkilöt jotka koettavat luoda yhteyttä tietokoneeseesi ovat tunkeilijoita siihen asti, kunnes toisin todistetaan. Kun ohjelmalla yhdistetään toiseen käyttäjään, tulee yhteyspyyntöjen täyttää monia kriteereitä. Näihin kuuluvat käyttäjän tunnistus ja valtuuksien varmistaminen paikallisen tai keskitetyn järjestelmän avulla. Näitä järjestelmiä voivat olla esimerkiksi Windows Domain, Directory Service tai RSA SecurID server. Jokaiselle käyttäjälle sallitut roolit sanelevat, mitä toimintoja he voivat suorittaa etäkäyttöyhteyden kautta. NetOp Security Server -moduulilla on mahdollisuus kontrolloida kaikkia käyttäjiä käyttäjien tunnistus ja valtuuksien varmistamisen avulla. NetOp:n useiden palvelimien käytön ansiosta kuormantasaus ja vikasieto toimivat paremmin ja ylimääräinen aika jää olemattomaksi. NetOp Remote Control -ohjelman moduulienvälisen liikenteen suojauksessa käytetään 256 bittistä AES-salausta. NetOp:ssa on myös kattava tapahtumien kirjaus, jota voi käyttää apuna tunkeutujien hyökkäysten jäljittelemisessä. Tapahtumien kirjaus tallentaa tietoja paikallisesti ja keskitetysti. (Moonsoft 2008.)

En kuitenkaan tässä testissä käyttänyt ollenkaan Security Server -moduulia, koska kotikäytössä sen tarjoamia palveluita ei pysty täysin hyödyntämään johtuen siitä, että tietokoneet eivät toimi samassa lähiverkossa. NetOp-ohjelmassa on kuitenkin paljon tietoturvaan liittyviä asetuksia, joita henkilön, jonka tietokonetta etähallitaan, on mahdollista säädellä tietoturvan edistämiseksi ohjelman perusasetuksista. Näitä asetuksia ovat:

1) Etähallinnan toimintojen salliminen

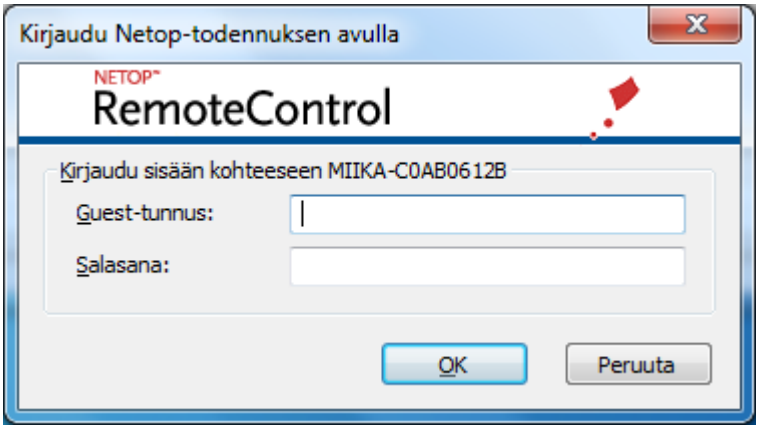
Host-käyttäjällä on mahdollisuus sallia tai estää, mitä kaikkea Guest-käyttäjä voi tietokoneella etähallinnan aikana tehdä (kuvio 30).



Kuvio 30. NetOp-ohjelman etähallinnan toimintojen sallinta-asetukset.

2) Käyttäjän määrittely

Host-käyttäjä voi lisätä Guest-käyttäjälle/käyttäjille omat tunnukset, jolloin tietokoneelle pääsevät vain nämä määritetyt käyttäjät. Jos Guest-käyttäjiä on monta, jokaiselle voidaan erikseen määritellä kohdassa 1) olevat asetukset. Guest-käyttäjälle määritellään nimi ja salasana, jotka hänen tulee tietää ottaessaan yhteyttä etähallittavan tietokoneeseen (kuvio 31).



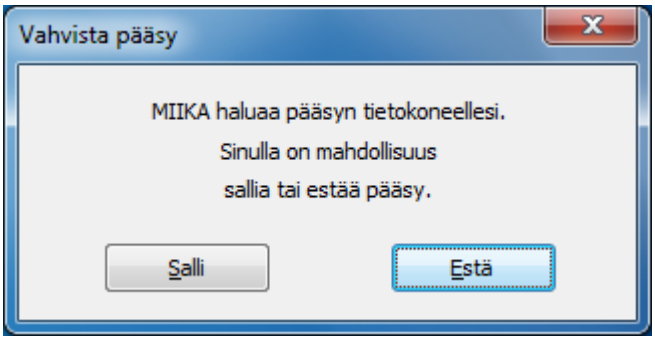
Kuvio 31. NetOp-ohjelma kysyy Guest-tunnuksia.

Jos käyttäjiä ei ole määritelty, ohjelma kysyy vain pelkkää salasanaa, joka luodaan jo ohjelman asennusvaiheessa.

3) Kulunvalvonta

Host-käyttäjä voi ottaa kulunvalvonta-asetuksen käyttöön, jolloin Guest-käyttäjä lähettää aina ensin pyynnön Host-käyttäjälle tietokoneelle pääsystä, ennen kuin tietokoneita voidaan yhdistää.

Host-käyttäjä voi joko sallia tai estää Guest-käyttäjän pääsyn (kuvio 32).



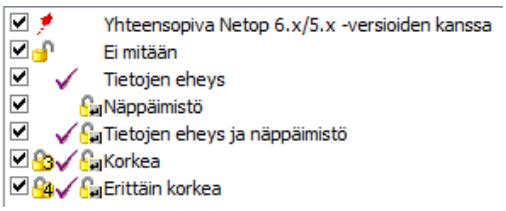
Kuvio 32. NetOp-ohjelman kysyy pääsyn vahvistamista.

4) MAC/IP-osoitteiden tarkastus

Tämä on yksi parhaista tavoista varmistua, että kyseessä on oikea Guest-käyttäjä. Host-käyttäjä voi lisätä Guest-käyttäjän/käyttäjien tietokoneiden MAC/IP-osoitteet omalle listalleen. Kun MAC/IP-osoitteiden tarkistus ominaisuus on käytössä, Host-käyttäjä voi rajoittaa yhteyksiä vain niille, joiden osoitteet hän on listalle lisännyt.

5) Salaus -asetus

Tällä osiolla Host-käyttäjä pystyy määrittelemään mitkä osa-alueet etäyhteydestä salataan etähallintayhteyden aikana (kuvio 33). Tietoturvan kannalta on suositeltavaa, että kaikki osa-alueet ovat aina sallittuina eli salattuina.



Kuvio 33. NetOp-ohjelman salauksen asetukset.

5.3.6 Muuta

NetOp-ohjelmaa on mahdollisuus käyttää myös mobiililaitteissa. Netop Mobile and Embedded -sovellus mahdollistaa etäpääsyn tietokoneelle älypuhelimilla, kämmentietokoneilla sekä muilla mobiililaitteilla ja sulatetuilla järjestelmillä. Myös tiedonsiirto sekä chat-keskustelu tietokoneen ja mobiililaitteen välillä on mahdollista. (NetOp 2010.)

En voinut testata NetOp-ohjelmaa Windows ja Mac -käyttöjärjestelmien välillä, koska asennettaessa ohjelmaa Mac-käyttöjärjestelmälle ohjelma kysyy sarjanumeroa. 30 päivän kokeiluversio ei sisällä ohjelmien sarjanumeroita, eikä asennusta voinut näin toteuttaa ilman sitä.

5.4 Ohjelmien vertailu

Ohjelmista löytyy monia eroja, vaikka ne ovatkin pääpiirteissään samankaltaisia. Suurimmat erot löytyvät kotikäyttäjän kannalta ohjelman käyttöönotossa. TeamViewer on huomattavasti yksinkertaisempi ja nopeampi ottaa käyttöön kuin NetOp Remote Control. NetOp Remote Control -ohjelman käyttöönottamiseksi täytyy ensin rekisteröityä NetOp:n sivuille, ladata ohjelmapaketit ja asentaa ohjelmat. TeamViewer-ohjelmastakin täytyy ohjelmapaketit ladata tietokoneelle, mutta mitään rekisteröitymistä se ei vaadi, eikä välttämättä ohjelman asennustakaan. Riittää, kun avaa lataamansa tiedoston. Lisäksi jos asentaa ohjelman, on TeamViewer-ohjelman asennus paljon selkeämpi ja nopeampi prosessi kun NetOp Remote Control -ohjelman.

Käytettävyydeltään ohjelmat ovat hyvinkin samankaltaisia ja samoja ominaisuuksia löytyy monia. TeamViewer-ohjelman tiedonsiirrossa on kuitenkin yksi merkittävä etu NetOp Remote Control-ohjelman tiedonsiirtoon verrattuna. Tämä on ns. Vedä ja pudota toiminto, missä TeamViewer-ohjelmalla on mahdollisuus siirtää tiedostoja suoraan etäohjausikkunasta omalle tietokoneelle ja päinvastoin. Tämä toiminto nopeuttaa etähallinnan aikana suoritettavaa tiedonsiirtoa huomattavasti.

Tietoturvan osalta kummatkin ohjelmat ovat kotikäyttäjän kannalta hyvinkin turvallisia ja suojauksista voi halutessaan huolehtia monella eri tavalla. NetOp Remote Control -ohjelmaan on kuitenkin mahdollisuus saada enemmän tietoturvaan liittyviä menetelmiä. NetOp Remote Control -ohjelmassa on la-

dattavissa SecurityServer Host -moduuli, joka huolehtii yksinomaan ohjelman tietoturvasta.

Suuri yksittäinen ero löytyy ohjelman hinnasta. TeamViewer kun on yksityiskäyttöön täysin ilmainen, kun taas NetOp Remote Control maksaa ja vaatii lisenssit.

Tein ohjelman eri ominaisuuksista taulukon josta näkee, sisältyykö mainittu ominaisuus kyseiseen ohjelmaan. Taulukko on nähtävänä tämän työn liitteenä (Liite 2).

6 POHDINTA

Opinnäytetyöni tarkoituksena oli tutkia tietokoneiden etähallintaa koti- ja yrityskäytössä. Tietokoneiden etähallinta yrityksissä on nykypäivänä yksi tärkeimpiä menetelmiä tietokoneiden ylläpidollisissa tehtävissä ja tukitoiminnassa. Sen sain huomata myös omakohtaisesti ollessani työharjoittelussa Kairatien ammattiopistolla kolme kuukautta vuoden 2011 alusta.

Oikeastaan opinnäytetyöprosessini lähti liikkeelle jo tästä työharjoittelustani. Siellä minua kiinnosti tietokoneiden etähallinta ja sen tuomat eri käyttömahdollisuudet, joten mietin jo silloin, että voisin valita opinnäytetyöni aiheeksi tietokoneiden etähallinnan. Kotikäytössäkin olin jo aikaisemmin käyttänyt etähallintaa auttaessani tuttujani tietokoneongelmissa.

Yksityiskäytössä etähallinnan käyttöönotto ei ole nykypäivänä enää kovinkaan vaikeaa. Lähes jokaiseen käyttöjärjestelmään on saatavana omat versiot etähallintaohjelmista, eivätkä monet etähallintaohjelmat edes vaadi palomuuriasetusten muokkaamista toimiakseen. On silti tärkeää muistaa tietoturva-asetukset käytettäessä etähallintaa.

Tulevaisuudessa etähallinta tulee varmasti kehittymään entisestään ja luodaan uusia sovelluksia ja erilaisia etähallintamenetelmiä. Uskoisin, että etähallinta mobiililaitteiden ja tietokoneiden välillä tulee varmasti yleistymään, vaikka jo nykyäänkin se on mahdollista. Tavalliselle kotikäyttäjälle saattaa olla tulevaisuudessa ihan arkipäivää se, että hallitsee kännykällään täysin myös omaa tietokonettaan.

Varsinaisen opinnäytetyöni tekemisen aloitin vuoden 2012 tammikuun loppupuolella. Mielenkiintoni opinnäytetyötä kohtaan ja halu saada työni valmiiksi saman kevään aikana vaikuttivat siihen, että sain opinnäytetyöni valmiiksi muutaman kuukauden uurastuksen jälkeen. Ensimmäisenä tein opinnäytetyössäni kotikäyttöosuuden ja viimeisenä yritysosuuden. Näiden välissä valmistin teoria- ja tietoturvaosuudet. Yritysosuuden tutkittavaksi yritykseksi oli luontevaa valita Kairatien ammattiopisto työharjoitteluni perusteella. Myöhemmin vielä laajensin yritysosuuttani haastattelemalla kahta muuta yritystä sähköpostitse, jotta yritysosuudesta tulisi vähän laajempi kuva. Kotikäyttöohjelmista TeamViewerin valitsin omavaltaisesti, koska se oli minulle jo entuu-

destaan jonkin verran tuttu. Opinnäytetyöni ohjaava opettaja ehdotti NetOp-ohjelmaa, joten valitsin sen toiseksi ohjelmaksi.

Vaikeinta opinnäytetyössäni oli sen aloittaminen ja alkuun pääseminen sekä aiheen lukkoon lyöminen. Sen jälkeen kun sain päätettyäni aiheen lopullisesti, suunniteltua opinnäytetyöni rakenteen ja pääsin työssäni alkuun, työni valmistui ikään kuin itsestään ja materiaalia kertyi aluksi liikaakin. Lopulta työstäni tuli reilun 50 sivun mittainen raportti, vaikka aluksi mielessäni oli että teen siitä vain noin 20–30 sivun mittaisen tiiviin paketin.

Opinnäytetyössäni tutkin paljon etähallintaohjelmien toimintaa. Samalla kun tutkin, kirjoitin tutkimuksistani raporttia, josta sitten lopulta valmistui tämä opinnäytetyöraporttini. Työtäni helpotti se, että aiheesta löytyi hyvin tietoa, vaikka kirjallisuutta kyseisestä aiheesta onkin todella vaikeaa löytää. Melkein kaikki lähteeni ovatkin internetistä. Vaikka lähteitä onkin paljon, nostaisin tärkeimmiksi lähteiksi etähallintaohjelmien käyttömanuaalit. Lisäksi työtäni auttoi se, että samantyyppisestä aiheesta oli tehty muutamia muita opinnäytetöitä, joita sitten käytin apuna suunnitellessani ja rakentaessani työtä.

Mielestäni opinnäytetyö prosessini sujui kokonaisuudessaan hyvinkin onnistuneesti ja se antoi hyvin kokemusta tulevalle IT-alalle.

LÄHTEET

Aaltonen, R. 2012. LapIT Oy:n ICT-asiantuntija. Sähköpostitiedonanto 20.4.2012.

Afterdawn Oy 2012. Ohjelmat. Verkko. VPN. Osoitteessa http://www.download.fi/verkko/vpn/. 24.2.2012.

Apple Inc 2012. Apple Remote Desktop 3. Osoitteessa http://www.apple.com/fi/remotedesktop/. 25.2.2012.

Bitvise limited 2011. About SSH. Osoitteessa http://www.bitvise.com/ssh2. 28.2.2012.

DameWare 2012a. DameWare NT Utilities: A Complete Remote Windows Admin Solution. Osoitteessa http://www.dameware.com/Products/Dameware-NT-Utilities/Product-Overview.aspx. 9.3.2012.

DameWare 2012b. DameWare Mini Remote Control – The Power Tool for Remote Management. Osoitteessa http://www.dameware.com/Products/Mini-Remote-Control/Product-Overview.aspx. 9.3.2012.

EMC Corporation 2012. RSA Laboratories. What is SSH? Osoitteessa http://www.rsa.com/rsalabs/node.asp?id=2296. 28.2.2012.

Finlex - Valtion säädöstietopankki 2012. Rikoslaki 19.12.1889/39. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001. 28.2.2012.

Haveri, M. 2011. Etähallintaohjelma. Osoitteessa http://www.tietokone.fi/keskustelu/ohjelmat/24073. 23.2.2012.

Huntington, G. 2006. What is authentication? Osoitteessa http://www.authenticationworld.com/. 28.2.2012.

Javvin Company 2012. ISL & DISL: Cisco Inter-Switch Link Protocol and Dynamic ISL Protocol. Osoitteessa http://www.javvin.com/protocolISL.html. 15.3.2012.

Kuusisto, J. 2011. Etähallintaohjelmiston hyödyntäminen satakunnan ammattikorkeakoulun liiketoiminta ja kulttuuri porin yksikössä. Opinnäytetyö. Satakunnan ammattikorkeakoulu. Osoitteessa https://publications.theseus.fi/bitstream/handle/10024/37545/juho_kuusisto.pdf?sequence=1. 10.3.2011.

Lacoma, T. 2012. How does a remote connection work? Osoitteessa http://www.ehow.com/how-does_6016489_remote-connection-work_.html. 22.2.2012.

Lapin ammattiopisto 2011a. Esittely. Lapin ammattiopisto lyhyesti. Osoitteessa http://www.lao.fi/Suomeksi/Esittely.iw3. 10.3.2012.

Lapin ammattiopisto 2011b. Esittely. Toimipisteet. Osoitteessa http://www.lao.fi/Suomeksi/Esittely/Toimipisteet.iw3. 10.3.2012.

Lapin ammattiopisto 2011c. Esittely. Toimipisteet. Rovaniemi, Kairatie 75. Osoitteessa http://www.lao.fi/Suomeksi/Esittely/Toimipisteet/Rovaniemi,_Kairatie_75.iw3. 10.3.2012.

LapIT Oy 2012. Strategiset liiketoiminta-alueemme (SBA). Osoitteessa http://www.lapit.fi/index9b91.html?deptid=10605. 23.4.2012.

Lappset Group Oy 2012. Osoitteessa http://www.lappset.fi. 23.4.2012.

Lawmay 2005. Inno Setup Command Line Switches and Exit Codes. Osoitteessa http://www.appdeploy.com/tips/detail.asp?id=113. 7.3.2012.

Lineback, N. 2012. X11 - X windowing system. Osoitteessa http://toastytech.com/guis/remotex11.html. 25.2.2012.

Linux.fi-wiki 2010. VNC. Osoitteessa http://linux.fi/wiki/VNC. 24.2.2012.

Microsoft 2012a. MSDN community. Remote Desktop Protocol. Osoitteessa http://msdn.microsoft.com/en-us/library/windows/desktop/aa383015%28v=vs.85%29.aspx. 24.2.2012.

Microsoft 2012b. MSDN community. TLS vs. SSL. Osoitteessa http://msdn.microsoft.com/en-us/library/aa380515%28v=VS.85%29.aspx. 28.2.2012.

Microsoft 2012c. Windows 7. Etätyöpöytäyhteys. Osoitteessa http://windows.microsoft.com/fi-FI/windows7/products/features/remote-desktop-connection. 8.3.2012.

Microsoft 2012d. Windows 7. FTP (File Transfer Protocol): usein kysytyt kysymykset. Osoitteessa http://windows.microsoft.com/fi-FI/windows7/File-Transfer-Protocol-FTP-frequently-asked-questions. 24.2.2012.

Microsoft 2012e. Windows 7. Mitä on aktivointi lähiverkon avulla? Osoitteessa http://windows.microsoft.com/fi-FI/windows7/What-are-Wake-on-LAN-capabilities. 24.2.2012.

Microsoft 2012f. Windows 7. Mitä ovat palvelimen todennusasetukset? Osoitteessa http://windows.microsoft.com/fi-FI/windows7/What-are-server-authentication-options. 14.3.2012.

Microsoft 2012g. Windows Vista. Yhteys toiseen tietokoneeseen Etätyöpöytäyhteyden avulla. Osoitteessa http://windows.microsoft.com/fi-FI/windows-vista/Connect-to-another-computer-using-Remote-Desktop-Connection. 8.3.2012.

Moonsoft 2008. NetOp Remote Control 8.0. Täydellinen, skaalautuva ja turvallinen etäkäyttöohjelma IT-ammattilaisille. Osoitteessa http://www.moonsoft.fi/materials/danware_netop_remote_control_8sf.pdf. 8.2.2012.

NetOp 2009. Company. Osoitteessa http://www.netop.com/company/about-netop.htm. 30.1.2012

NetOp 2010. NetOp Remote Control Mobile Embedded. Osoitteessa http://www.netop.com/fileadmin/netop/resources/products/administration/mobile/datasheets/Mobile-and-Embed_Datasheet_EN_A4_Web.pdf. 9.2.2012.

NetOp 2012. NetOp Remote Control Secure Remote Management and Support. Administrator's Guide. Version 11. Osoitteessa http://www.netop.com/fileadmin/netop/resources/products/administration/remote_control/manuals/NetopRemoteControlAdministratorsGuide_EN.pdf. 7.2.2012.

Nocom Software 2012. Tuotteet. NetOp Remote Control. Osoitteessa http://www.nocomsoftware.fi/website1/1.0.1.0/260/4/?item=prod_prod-s1/29. 27.1.2012.

Pitkänen, J. – Lehto, T. 2010. Yksinkertainen ja kevyt ip-skanneri. Osoitteessa http://www.tietokone.fi/softa/windows/angry_ip_scanner_2_21. 7.3.2012

Raitahila, I. 2008. Symantec Ghost käyttöopas. Osoitteessa http://raita.sytes.net/ghost/. 9.3.2012.

Russinovich M. 2009. PsExec v1.98. Osoitteessa http://technet.microsoft.com/fi-fi/sysinternals/bb897553. 7.3.2012.

Sassi, O. 2012. Lapin ammattiopiston, Kairatien toimipisteen ATK -tukihenkilön haastattelu. 6.3.2012 ja 8.3.2012.

Suomen Mobiilitieto Oy 2012. Mobiililaitteiden etähallinta Mobile Manager-palveluna. Osoitteessa http://kotisivukone.fi/files/mobiilitieto.palvelee.fi/tiedostot/mobile_manager_-esitys_012009_mobiilitieto_v1.pdf. 23.2.2012

Takala, V. 2012. Lappset Group Oy:n IT-henkilö. Sähköpostitiedonanto 19.4.2012.

TeamViewer 2012a. TeamViewer 7 manual Remote Control. Osoitteessa http://www.teamviewer.com/en/res/pdf/TeamViewer7_Manual_RemoteControl_EN.pdf. 27.1.2012.

TeamViewer 2012b. Lataa. Nykyinen versio. TeamViewer lataus. Osoitteessa http://www.teamviewer.com/fi/download/index.aspx. 31.1.2012.

TeamViewer 2012c. Miksi TeamViewer? Turvallisuus. Osoitteessa http://www.teamviewer.com/fi/products/security.aspx. 2.2.2012.

TeamViewer 2012d. Osta. Yleiskuva lisenssistä. Osoitteessa http://www.teamviewer.com/fi/licensing/index.aspx. 1.2.2012.

TeamViewer 2012e. Yhteydenotto. Yritys. TeamViewer - yritys. Osoitteessa http://www.teamviewer.com/fi/company/company.aspx. 26.1.2012.

The free dictionary 2012. Remote desktop software. Osoitteessa http://encyclopedia.thefreedictionary.com/Remote+desktop+software. 24.2.2012.

Tietosuojavaltuutetun toimisto 2010. Tietokoneen kaappaus, mikä se on? Osoitteessa http://www.tietosuoja.fi/uploads/1obsco_2.pdf. 27.2.2012.

Tietotekniikan tuoteuutiset 2012. Miksi IT-ammattilaiset ympäri maailmaa valitsevat etähallintaan Netopin? Ennennäkemätön tietoturva ja vakaus ovat muutamia syitä... Osoitteessa http://www.tuoteuutiset.fi/pdf/TIE309s30.pdf. 27.2.2012

Viestintävirasto 2007a. Tietoturva- ja suoja. Salausmenetelmät. Symmetrinen salaus. Osoitteessa http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/symmetrinensalaus.html. 27.2.2012.

Viestintävirasto 2007b. Tietoturva- ja suoja. Salausmenetelmät. Epäsymmetrinen salaus. Osoitteessa http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/epasymmetrinensalaus.html. 27.2.2012.

Viestintävirasto 2009. Tietoturva- ja suoja. Salausmenetelmät. Osoitteessa http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html. 27.2.2012

Viestintävirasto 2012. Tietoturva- ja suoja. Lyhenteet ja määritelmät. Osoitteessa http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/yhenteetjamaaritelmat.html. 28.2.2012.

Wikipedia 2011. Asennus (tietotekniikka). Osoitteessa http://fi.wikipedia.org/wiki/Asennus_%28tietotekniikka%29. 7.3.2012.

LIITTEET

KOTIKÄYTTÖTIETOTIETOKONEIDEN JÄRJESTELMÄTIEDOT Liite 1

	Pöytätietokone	Kannettava tietokone
Käyttöjärjestelmä	Microsoft Windows XP Home Edition	Microsoft Windows 7 Enterprise
Prosessori	AMD Athlon 64 Processor 3500+, ~2,2GHz	Intel Core i3-2310M CPU, ~2,1GHz
Fyysinen muisti	3072 Mt RAM	4096 Mt RAM
Kovalevy	298,1 Gt	232,6 Gt
Näytönohjain	NVIDIA GeForce 7300 GT	Intel HD Graphics Family
Valmistaja ja malli	NVIDIA AWRDACPI	Dell Inc. Latitude E6520
Verkko, mihin tietokone on kytketty	Laajakaista 24/1 M Sonera	Mobiililaajakaista Saunalahti

KOTIKÄYTTÖOHJELMIEN VERTAILU Liite 2

	Team-Viewer	NetOp
Käyttöönotto		
Ei vaadi rekisteröitymistä	x	
Ohjelmaa ei tarvitse välttämättä asentaa	x	
Suomen kielinen käyttöliittymä	x	x
Etähallinta		
Chat-keskustelu	x	x
Puhe/Video -yhteys	x	x
Etäkoneen järjestelmätiedot	x	x
Etäohjausikkuna koko ruudun kokoiseksi	x	x
Musta ruutu etäkoneelle	x	x
Etäkoneen uudelleenkäynnistys	x	x
Etäkoneen uudelleenkäynnistys vikasietotilassa	x	
Etäkoneen sammutus	x	x
Kirjaudu ulos etäkoneelta	x	x
Lukitse etäkone	x	x
Vaihda puolia etähallittavan kanssa	x	
Etäkoneen järjestelmäasetusten etähallinta		x
Näyttää näyttökuvaa omasta koneesta etäkoneelle		x
Merkintätila		x
Etäkoneen näppäimistön ja hiiren lukitseminen		x
Etähallinta Internet-selaimen kautta	x	
Kiinteä salasana	x	
Tiedonsiirto		
Etäyhteys pelkkään tiedonsiirtoon	x	x
Tiedonsiirto etähallinnan aikana	x	x
Tiedoston siirtäminen		x
Tiedoston kopioiminen	x	x
Tiedoston sykronoiminen/kloonaaminen		x
Vedä ja pudota toiminto	x	
Tietoturva		
256 bittinen AES-salaus	x	x
Yhteyssalasana kertakäyttöinen	x	
Black and Whitelist -luettelo	x	
MAC/IP -osoitteiden tarkistus		x
Etähallitsijan oikeuksien rajaaminen	x	x
Ylimääräisen vahvistuksen lähettäminen etähallittavalle koneelle	x	x
Käyttäjien lisääminen		x
Käyttöalustat		
Windows	x	x
Linux	x	x
MAC	x	x
Solaris		x
OS/2		x
Mobiili	x	x
Hinta		
Ilmainen yksityiskäytössä	x	