

Opinnäytetyö (AMK)

Tieto- ja viestintäteknikka

2020

Jesse Sankala

MAINOSTEN ESTO- OHJELMISTO PI-HOLE

– Linux-käyttöjärjestelmille paikallisen verkon
kattava mainosten esto-ohjelma

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintäteknikka

2020 | 35 sivua

Jesse Sankala

MAINOSTEN ESTO-OHJELMISTO PI-HOLE

Työn tarkoituksena oli tutkia ja etsiä keinoja mainosten poistamiseen verkkoselailussa. Mainosten estäjiä on muutamia erilaisia, joita tässä työssä tarkastellaan.

Vaihtoehtoja mainosten estämiseksi ovat lisäosat verkkoselaimiin, ohjelmistot mobiililaitteisiin sekä mainosten esto-ohjelmisto Pi-Hole.

Pi-Hole on koko paikallisverkon kattava mainosten esto-ohjelmisto, joka asennetaan kerran ja toimii kaikilla verkkoon liitetyillä laitteilla. Ohjelmisto asennetaan Linux-pohjaiselle käyttöjärjestelmälle, joksi Pi-Holen ohjeissa suositellaan Raspbiania. Raspbiania käytetään yleensä Raspberry Pi, yhden piirilevyn tietokoneessa.

Mainosten esto-ohjelmisto Pi-Hole on hyvä ratkaisu, mikäli käyttää useaa laitetta samassa verkossa.

ASIASANAT:

Mainosten esto, Raspberry Pi, Linux, DNS

BACHELOR'S / MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2020 | 35 number of pages

Jesse Sankala

ADVERTISEMENT BLOCKING SOFTWARE PI-HOLE

The purpose of this work was to investigate and find ways to remove advertisements when browsing internet. There are a few different types of ad blockers, that will be considered in this work.

Options for blocking ads include add-ons for web browsers, software for mobile devices and Pi-Hole, ad-blocking software.

Pi-Hole is an ad-blocking software that covers the entire local network and is installed once and works on all devices connected to the network. The software is installed on Linux-based operating system, in which Pi-Hole documentation recommends Raspbian. Raspbian is commonly used on the Raspberry Pi, single-board computer.

Pi-Hole ad blocking software is a good solution if you use multiple devices on the same network.

KEYWORDS:

Ad blocker, Raspberry Pi, Linus, DNS

SISÄLTÖ

SANASTO	6
1 JOHDANTO	9
2 INTERNET	10
2.1 Historia	10
2.2 Nykypäivänä	11
2.2.1 Ominaisuudet	11
2.2.2 Käyttö	12
2.3 Vaarat	12
2.3.1 Haittaohjelmat	13
2.3.2 Seuranta	13
3 YKSITYISYYS	14
3.1 Riskit	14
3.2 Evästeet	15
3.3 Profilointi	16
3.4 Kohdennettua mainontaa	16
3.5 VPN, virtuaalinen erillisverkko	17
3.6 Tor verkkoselain	17
4 RASPBERRY PI	19
4.1 Käyttö	20
4.2 Etäkäyttö	21
5 PI-HOLE-OHJELMISTO	23
5.1 Vaatimukset	23
5.2 Asennus	23
5.3 Toiminnassa	24
5.3.1 Mainoksien esto	25
5.3.2 Seuranta ja muokkaus	26
5.3.3 YouTuben mainokset	28
5.4 Kaksoisoperaatio – VPN ja Pi-Hole	29
5.4.1 OpenVPN -ohjelmiston asennus	29
5.4.2 OpenVPN ja Pi-Holen yhdistäminen	29

5.5 Vaihtoehtoja	30
5.5.1 Ominaisuuksia	31
5.5.2 Mobiililaitteille	31
6 TULOKSET	32
LÄHTEET	33

SANASTO

ARPANET	Advanced Research Projects Agency Network Pakettikytkentäinen tietokoneverkko, josta kehittyi internet. (Wikipedia 2009)
CERN	Euroopan hiukkasfysiikan tutkimuskeskus. (Wikipedia 2012)
DARPA	Defense Advanced Research Projects Agency, organisaatio, joka tutkii ja kehittää sotilasvoimille teknologiaa. (Wikipedia 2010)
DHCP	Dynamic Host Configuration Protocol, jakaa IP-osoitteita verkkoon liittyville laitteille. (Wikipedia 2010)
DNS	Domain Name System, muuntaa verkko-osoitteet tietokoneille ymmärrettäviksi IP-osoitteiksi. (Wikipedia 2010)
Doksaus	Doxing, on internet-slangia ja tarkoittaa toisen ihmisen henkilötietojen etsimistä ja luvaton jakelemista julkisuuteen. (Wikipedia 2015)
FTP	File Transfer Protocol, tiedonsiirtomenetelmä kahden tietokoneen välille, toimii asiakas-palvelin -periaatteella. Asiakas ottaa yhteyden palvelimelle, joka tarjoaa palvelun. (Wikipedia 2013)
GPIO	General Purpose Input-Output, yleiskäyttöinen pinni. (Wikipedia 2016)
IP-osoite	Internet Protocol, tietokoneen "postiosoite". (Wikipedia 2013)
Milnet	Military Network, Sotilasvoimien kommunikaatioverkko. (Wikipedia 2001)

NRL	US Naval Research Laboratory, suorittaa perustutkimusta, soveltavaa tutkimusta, teknologista kehittämistä ja prototyyppien laatimista. (Wikipedia 2013)
NSFNET	National Science Foundation Network, tutki ja tuki suurta osaa nykyaikaisen internetin alkua. (Wikipedia 2013)
PoE	Power over Ethernet, tekniikka, jolla saadaan ethernet-lähiverkkoon liitetulle laitteelle käyttövirtaa saman kaapelin kautta. (Wikipedia 2010)
Regex	Regular expression, tietynlainen merkkijono, jolla voi tarkistaa tekstiä, jos esimerkiksi salasana on tarpeeksi isoja ja pieniä kirjaimia ja numeroita. (Wikipedia 2017)
SSH	Secure Shell, salattuun tietoliikenteeseen tarkoitettu protokolla. Yleisin SSH:n käyttötapa on ottaa etäyhteys protokollan ohjelmalla palvelimeen ja käyttää toista konetta konsolin kautta. (Wikipedia 2008)
TCP	Transmission Control Protocol, pitää huolen, että paketit saapuvat määränpään oikeassa järjestyksessä ja tarvittaessa hävinnyt paketti voidaan lähettää uudelleen. (Wikipedia 2011)
VNC	Virtual Network Computing, protokolla tietokoneen graafisen käyttöliittymän etäkäyttöön. (Wikipedia 2007)
VoIP	Voice-over-Internet Protocol, lähettää ääntä reaaliaikaisesti internetin tai IP:n välityksellä, puhe muutetaan digitaaliseksi ja siirretään paketteina verkon yli. (Wikipedia 2009)
VPN	Virtual Private Network, yhdistää yksityisen verkon salatun tunnelin kautta toiseen verkkoon julkisen verkon läpi, päätarkoituksena piilottaa tietokoneen sijainti. (Wikipedia 2012)

WWW

World Wide Web internetissä toimiva hypertekstijärjestelmä, jota luetaan selaimilla. Jotka hakevat verkkosivuksi kutsuttuja dokumentteja palvelimilta ja piirtää ne näytölle. (Wikipedia 2008)

1 JOHDANTO

Nykypäivänä jokaiselle ihmiselle internetin käyttö on päivittäistä toimintaa. Ihmiset etsivät internetistä tietoa päivittäiseen toimintaan. Internetistä voidaan etsiä tietoa ostettavista tai tilattavista tuotteista tai verrata tuotteiden hintoja kauppojen välillä. Internetistä löytyy myös tuoreimmat uutiset reaaliaikaisena. Moni lehti onkin vähentänyt paperilehtien painamista sen vuoksi, koska ihmiset löytävät tietoa paremmin ja nopeammin digilehdistä.

Verkkosivustot ja niiden päivittäminen ei ole kuitenkaan ilmaista. Tämän vuoksi verkkosivujen omistajat myyvät sivuilta tilaa mainostajille. Mainosten määrä on kasvanut niin suureksi, että se häiritsee lukijaa, joten mainokset halutaan pois verkkosivuilta.

Tämän opinnäytetyön tarkoituksena on tutkia ja etsiä keinoja mainosten poistamiseen verkkosivuilta. Verkkoselaimen lisäosilla mainoksia pystyy estämään, mutta se kohdistuu vain yhteen tiettyyn verkkoselaimeen ja poistaa ongelman vain yhdestä laitteesta. Tämän vuoksi opinnäytetyö kohdistuu erityisesti, mainosten esto-ohjelmistoon Pi-Hole, joka poistaa mainokset kaikista paikallisverkkoa käyttävistä laitteista verkkoselaimesta huolimatta.

Pi-Hole tehtiin alun perin Raspberry Pi -tietokoneelle, joka on pienikokoinen, vähävirtainen ja -tehoinen tietokone, johon yleensä asennetaan Raspbian-käyttöjärjestelmä. Pi-Hole on ilmainen ja koko verkon kattava mainoksien estäjä Linux-pohjaisella käyttöjärjestelmällä.

Pi-Hole toimii kaikissa laitteessa, jotka on kytketty samaan verkkoon, koska se on koko verkon DNS-palvelin. Mikäli verkkosivu hakee mainossivuja, Pi-Hole estää sen latauksen.

Päädyin tähän opinnäytetyöhön sen vuoksi, koska itseäni häiritsee useat mainokset selatessani verkkosivuja. Aloin tutkimaan aihetta, sen eri vaihtoehtoja ja päädyin hankkimaan itselleni mainosten esto-ohjelmisto Pi-Holen.

2 INTERNET

Internetillä ei ole valvovaa organisaatiota, joten sen käyttäytyminen on erittäin arvaamatonta. Tämän vuoksi Internet on demokratiaa parhaimmillaan ja pahimmillaan. Internet määritellään maailmanlaajuiseksi verkkojen verkoksi eli tietoverkoksi, joka muodostuu pienemmistä toisiinsa kytketyistä verkoista. (Mediat, 2K 2002) (Peda.net 2010)

Internetin käyttöön kehitettiin protokollia, jotka ovat käytännössä keskustelun sääntöjä, miten viestejä käytetään ja mitä viestit sisältävät. TCP on tällainen sääntö, joka kehitettiin viestittämään laitteiden välillä. Se voi esimerkiksi pyytää verkkosivun palvelimelta. IP on toinen protokolla. Se kertoo tietokoneen osoitteen sitä tarvitsevalle palvelimelle, joka lähettää verkkosivun. Näitä protokollia ei kehitetty tietoturva- tai salausta mielessä, koska ne tehtiin alun perin vain luotettaville tahoille ja ei laajamittaiseen käyttöön. (Wikipedia 2005)

2.1 Historia

1960-luvulla Yhdysvaltojen puolustusvoimat aloittivat ARPANET-tutkimusprojektin, jonka tarkoituksena oli luoda ydiniskun kestävä tietoverkko. Rakennus aloitettiin 1960-luvun lopulla ja 1970-luvulla ARPANETiin kuului 23 tietokonetta. Olennaisessa roolissa oli kehittää datasiirron protokolla, TCP/IP. (Mediat, 2K 2002) (Peda.net 2010)

1983 ARPANET jaettiin kahteen osaan. Milnet verkkoa käytettiin sotilaalliseen toimintaan. ARPANETiä käyttivät tiedeyhteisöt, johon 1980-luvun lopussa yhdistettiin yliopistojen ja tutkimuslaitosten supertietokoneet mahdollistaen nopean tiedonhankinnan. Tästä syntyi nykyisen internetin runko NSFNET. (Mediat, 2K 2002) (Peda.net 2010)

Vuonna 1990 CERNissä julkaistiin WWW:n prototyyppi ja 1990-luku oli internetin nopean kasvun ja kehityksen aikaa, kun erilaiset tiedonvälitykseen liittyvät keksinnöt seurasivat toisiaan nopeassa tahdissa. Internetin läpimurto tapahtui 1994–95, kun internetin kaupallinen potentiaali houkutteli. Tällöin internetistä tuli hyvin nopeasti mainospaikka, täynnä mainosbannereita ja kotisivuja. (Mediat, 2K 2002)

2.2 Nykypäivänä

Nykyisin internetiä käytetään hyvin suuressa osassa tiedon välitykseen, yhteyden pitämiseen ja median suoratoistoon. Verkkosivut mahdollistavat asioiden julkistamisen potentiaalisesti suurelle yleisölle ilman suurta viivettä esimerkiksi uutissivustojen nopean päivityksen uusien uutisten ilmaantuessa. Suosituilla sivustoilla on myös mahdollista ostaa mainostilaa, jolla mainostaja saa näkyvyyttä ja sivuston pitäjä saa tukea sivuston ylläpitoon. (Wikipedia 2005)

2.2.1 Ominaisuudet

Sähköposti on tärkeä yhteydenpitopalvelu, jolla lähetetään viestejä yhden tai useamman henkilön välillä, mahdollistaen kuvien tai dokumenttien lähetyksen samalla. (Wikipedia 2005)

Internet puhelut ovat myös yleisiä käyttämällä VoIPia, (engl. Voice-over-Internet Protocol) joka on protokolla, jota kaikki internetin kautta menevät puhelut käyttävät. Idea alkoi 1990-luvulla, jolloin ajatuksena oli kehittää radiopuhelin tyylinen ohjelma. Nykyään VoIP ohjelmat ovat helppokäyttöisiä ja yhtä käteviä kuin puhelimet, toisena etuna on myös hinta, joka voi olla ilmainen tai maksaa vähemmän kuin normaalit puhelut, varsinkin pitkän matkan puhelut. Verkon laatu vaikuttaa myös puhelun laatuun mutta usein on parempi verrattuna normaaliin puheluun. Huonona puolena on hätänumeron puute ja luotettavuus. Ennalta täytyy sopia sama ohjelma, jolla soitella, mutta normaalissa puhelimestakin on numeron jako. (Wikipedia 2005)

Internetissä voi myös helposti jakaa tiedostoja esimerkiksi sähköpostin välityksellä tai verkkosivulla, jossa on käytössä FTP (engl. File Transfer Protocol), joka mahdollistaa verkkosivulla kävijän ladata tiedostoja. (Wikipedia 2005)

Suoratoisto on reaaliaikaista median lähetystä sen välittömään käyttöön. Monet radiot ja televisiot käyttävät internetiä median live-lähetykseen. Suosittuja suoratoistopalveluita ovat esimerkiksi Netflix, Yle areena, Spotify ja YouTube. (Wikipedia 2005)

2.2.2 Käyttö

Internet antaa joustavuutta työaikoihin ja työpaikkaan. Internetiin pääsee mistä vain ja usean laitteen kautta ja mahdollisesti langattomasti. Verkossa on myös verkkosivuja, jotka ovat tehty helpommaksi käyttää mobiililaitteilla. Internetissä on myös paljon virallista ja epävirallista opetuksellista materiaalia. (Wikipedia 2005)

Internet mahdollistaa tietokoneen ja tietojen käytön etänä. Etäkäytössä kannattaa käyttää turvaa eli todennusta, jolla täytyy kirjautua jonkinlaisilla tunnuksilla tai ohjelmalla, joka käyttää salausta. Etänä esimerkiksi kirjanpitäjä voi tarkastella dokumentteja kotoaan, joka voi olla eri maassa kuin työpaikka. (Wikipedia 2005)

Monet kuitenkin käyttävät internetiä katsoakseen uutisia ja säätä, suunnitellakseen ja varatakseen lomaa tai seurata henkilökohtaisia kiinnostuksen kohteita. Sosiaalisen verkostoitumisen verkkosivut, kuten Facebook tai Twitter, ovat tehneet uusia tapoja ihmisille pysyä yhteydessä. LinkedIn-sivun tapaiset sivut mahdollistavat ammatillisen yhteyden. (Wikipedia 2005)

Internetissä on myös pelejä, joita voi pelata muiden internetin käyttäjien kanssa. Pelejä on laidasta laitaan, kuten ammuskelupeleistä roolipeleihin ja uhkapeleihin. (Wikipedia 2005)

2.3 Vaarat

Yksityisille ja organisaatioille on riski kirjoittaessaan, varsinkin julkisille sivuille, sosiaalisessa mediassa asiointia tai kiistanalaista viestiä, joka saattaa johtaa suureen takaiskuun muilta internetin käyttäjiltä. Tällainen takaisku on usein vastaväittelyä tai julkista pilkkaa haukkumalla, vihapuheella tai jopa tappouhkauksilla. Verkossa ihmiset usein käyttäytyvät loukkaavammin kuin kasvotusten. (Wikipedia 2005)

Organisaatioille takaisku voi olla vahingoittavaa tuotemerkeille, varsinkin jos media julkaisee asiasta. Kuitenkin ihmiset, jotka ovat kyseisen organisaation puolella voi puolustaa tuotemerkkiä jopa nostaa sen mainetta muiden silmissä. (Wikipedia 2005)

Reddit kieltää henkilökohtaisen tiedon julkaisemista ”doksauksen” pelosta. Doksauksella tarkoitetaan toisen ihmisen henkilötietojen etsimistä ja luvattonta jakelemista

julkisuuteen. Säännöissä sanotaan, että jos julkaisussa on henkilötietoja, on ne sensuroitava. (Reddit 2005)

2.3.1 Haittaohjelmat

Internetissä on myös haitallisia ohjelmia, joihin sisältyy viruksia, matoja, ohjelmia palvelunestohyökkäyksiin, kiristysohjelmia ja vakoiluohjelmia. Nämä aktiviteetit nimitetään tietotekniikkarikollisuudeksi. Suurella kaavalla on myös spekuloitu mahdollisesta tietotekniikka-, tai verkkosodasta. (Wikipedia 2010)

2.3.2 Seuranta

Suurin osa tietokoneseurannasta on tietojen ja liikenteen seuranta. Esimerkiksi Yhdysvalloissa lainvalvojen on pystyttävä esteettömästi seuraamaan puheluita ja verkkoliikennettä. Tietokoneet viestittelevät toisilleen pilkkomalla viestin pieniksi palasiksi, joita kutsutaan paketeiksi. Paketit menevät tietokoneelta toiselle, kunnes ne pääsevät kohdekoneelle, jossa paketit kootaan takaisin viestiksi. On olemassa ohjelmia, jotka kaappaavat paketteja, kun ne menevät verkossa ja toisella ohjelmalla tarkastellaan sisältöä. Toisia ohjelmia käytetään liikenteen analysointiin, joka hakee tärkeää tai tietynlaista haluttua sisältöä. (Wikipedia 2005)

Jotkut maat estävät tietynlaista sisältöä internetissä, erityisesti poliittista tai uskonnollista sisältöä. Internetin tarjoajat estävät usein lainvalvojen määräämää sisältöä. (Wikipedia 2005)

3 YKSITYISYYS

Internetissä yksityisyydellä tarkoitetaan käyttäjän omien tietojen suojaamista ja tiedon keräystä eri paikoista. 1997 yksityisyys määriteltiin, että käyttäjän pitäisi pystyä määrittelemään itse millä ehdoilla yksityistä tietoa, jolla voisi tunnistaa henkilökohtaisesti käyttäjän, kerätään ja käytetään. Internetin suosion nousussa 1990-luvun lopulla selvisi, että internetin ja yhtiöiden täytyy seurata uusia sääntöjä suojellakseen käyttäjien yksityisyyttä. (Wikipedia 2011)

Täydellinen anonymisuus ei ole tarpeen jokaiselle käyttäjälle. Ei-henkilökohtaisesti tunnistettavaa tietoa, kuten IP-osoite annetaan verkkosivuille helppouden kannalta, ja se on vaikea pitää piilossa. Mikäli haluaa pitää tietoja yksityisenä, on oltava varovainen mitä katsoo internetissä ja mitä tietoja sinne täyttää. Kun ostetaan tuotteita, niitä seurataan ja sen seurauksena jotkut yritykset voivat lähettää roskapostia ja muita mainoksia samantyyppisistä tuotteista. (Wikipedia 2011)

Sosiaaliseen mediaan julkaiseminen voi olla haitallista tai vaarantaa haitallisille hyökkäyksille, koska tietyt asiat ovat pysyviä eikä niitä saa jälkikäteen poistettua. Esimerkiksi kommentit blogeissa, kuvissa ja verkkosivuilla, kuten Facebookissa tai Twitterissä. Kommentoinnin jälkeen joku voisi potentiaalisesti löytää ja lukea ne. Työnantajat voivat myös tutkia potentiaalisen työnhakijan verkkokäyttötymistä, mahdollisesti vaikuttaen työpaikan mahdollisuuteen. (Wikipedia 2011)

3.1 Riskit

Yrityksiä palkataan tutkimaan, mitä verkkosivuja ihmiset käyttävät, ja sitten esimerkiksi lähetetään mainoksia käyttäjän verkkoselaushistorian mukaan. (Wikipedia 2011)

Monet sosiaalisen median verkkosivut yrittävät suojata henkilökohtaista tietoa. Esimerkiksi Facebookissa yksityisyys asetukset ovat saatavilla, joista voi estää henkilöitä näkemästä profiilisivua, ja valita ketkä näkevät kuvia ja videoita. Samanlaisia asetuksia on myös Google Plus:ssa ja Twitterissä, joissa voi muokata asetuksia, kun on laittanut yksityistä tietoa sivuille. (Wikipedia 2011)

Lapset ja alaikäiset käyttävät usein internetiä mukaan lukien sosiaalista mediaa tavoin, joka voi vaarantaa yksityisyyttä. Nuoret eivät välttämättä tiedä, että kaikkea tietoa ja selaamista voidaan seurata. (Wikipedia 2011)

3.2 Evästeet

Evästeet (engl. cookies) ovat tietoja, jotka on tallennettu käyttäjän tietokoneelle ja auttavat automatisoimaan verkkosivuja ja -ominaisuuksia. Niitä voidaan myös käyttää tallentamaan erityistä historiaa, kuten Google Analyticsin käyttämiä kutsutaan seuranta evästeiksi (engl. tracking cookies). Aikaisemmin verkkosivut eivät ole varoittaneet evästeiden käytöstä, mutta seuranta evästeitä alettiin käyttämään pidemmän aikakaavan mukaan tallentamaan verkkohistoriaa. Evästeet ovat mainostajien päätapa löytää potentiaalisia asiakkaita, joten useat käyttäjät poistavat evästeet jopa kuukausittain. Tämän takia jotkut mainostajat ovat alkaneet käyttämään pysyviä evästeitä. (Wikipedia 2011)

Evästeillä on myös monia hyviä puolia, joita monet eivät välttämättä tiedä. Yksi näistä hyvistä puolista on se, että mikäli verkkosivu tarvitsee sisäänkirjautumisen, evästeet mahdollistavat sisäänkirjautumisen automaattisesti. Evästeet voivat myös seurata ja näyttää käyttäjälle sopivia verkkosivuja, jotka mahdollistavat ilmaiset verkkosivut. Monet verkkosivut ovat ilmaisia käyttää, mutta ne myyvät verkkosivuilla mainostilaa, jotka ovat personalisoituja käyttäjille. Tämän ominaisuuden jotkut näkevät myös negatiivisena puolena. Yksi yleisimmistä heikkouksista ovat käyttäjän tunnukset tallennettuna evästeissä, joita hakkerit hyväksikäyttävät. (Wikipedia 2011)

Evästeet ovat usein harmittomia, paitsi kolmannen osapuolen evästeet, joita vierailtu verkkosivu ei ole tehnyt, vaan joku muu mainoksia tekevä yritys. Nämä evästeet ovat vaarallisia, koska ne tallentavat samat tiedot kuin muutkin evästeet. Esimerkiksi selailutavat ja usein vierailut sivut menevät kolmannen osapuolen tietoon ja he voivat myydä tietoja eteenpäin. (Wikipedia 2011)

Evästeet yhdistetään yleensä ponnahdusikkunoihin, jotka ovat yleisiä, mutta harvoin personalisoituja. Ikkunat voivat olla ärsyttäviä, koska ikkunoita on usein vaikea sulkea piilotetun sulkunappulan takia. Pahimmassa tapauksessa ne voivat viedä muille sivuille. (Wikipedia 2011)

Evästeet nähdään yleensä haittana, koska niitä ei näy, kun käyttää verkkosivuja. Käyttäjää saattaa pelottaa idea, että joku seuraa millä verkkosivuilla vieraillee ja mitä niissä tekee. (Wikipedia 2011)

Evästeet voi myös poistaa käytöstä, jolloin voi laskea riskejä, mutta rajoittaa tai estää toimintoja verkkosivuilla. Kaikki suosituimmat verkkoselaimet sisältävät ominaisuuden poistaa evästeet käytöstä manuaalisesti. Jotkut selaimet, kuten Firefox tai Opera, sisältävät ominaisuuden, joka poistaa evästeet automaattisesti sulkiessa selaimen. (Wikipedia 2011)

3.3 Profilointi

Profilointi on toimintaa, joka kerää ja analysoi useaa toimintaa. Algoritmeilla tai muilla matemaattisilla tekniikoilla saadaan selville tietynlaisia tai samanlaisia käyttötapoja. Kun nämä yhdistetään ja käytetään yksilöimään yhtä tai useampaa henkilöä, kutsutaan profiileiksi. Profilointia ei käytetä vain henkilöryhmissä vaan käytetään usein myös henkilökohtaisesti kuten luottotietoihin, hintadiskriminointiin tai tietoturvaohjelmien identifiointiin. (Wikipedia 2009)

Jotkut keräävät ihmisten verkkoselausta ja potentiaalisesti voi yhdistää tiettyyn käyttäjään, sekä yhdistää henkilökohtaisesti kuka selaili, ja millä sivuilla. Yleensä tätä tietoa käytetään oikein, kuten "tyypillinen internetin käyttäjä" statistiikkaan, josta selviää, mitä keskiverto käyttäjä tekee verkkosivuilla, jota käytetään myynnin analysointiin. Tosin tämä tieto ei välttämättä aiheuta yksityisyyden rikkomista, alkuperäinen profilointi saattaa. (Wikipedia 2009)

Profilointi on ongelma yksityisyyden kanssa, kun tietoja aletaan yhdistämään ja saadaan selville henkilökohtaista tietoa. (Wikipedia 2009)

3.4 Kohdennettua mainontaa

Kohdennetulla mainonnalla tarkoitetaan mainoksia, jotka liittyvät käyttäjän kiinnostuksen kohteisiin. Esimerkiksi haetaan uutta pesukonetta ja sitten selailaan muita sivuja, jolloin muillakin sivuilla esiintyy mainoksia, joissa näkyy missä myydään pesukoneita. Näihin

käytetään evästeitä, joista näkyvät millä sivuilla on käyty. Ja profiloinnilla yhdistetään haut käyttäjiin. (GCFLearnfree 2016)

Esimerkiksi Facebook käyttää 98 erilaista tietoa mainosten tekoon käyttäjälle, joihin kuuluu paikkakunta, ikä, kieli, sukupuoli, koulutus. (Dewey 2016)

3.5 VPN, virtuaalinen erillisverkko

Yksi yleisimmistä ja helpommista keinoista anonyymisoida verkkokäyttöä on käyttää VPN:ää, (engl. Virtual Private Network) virtuaalinen erillisverkko. VPN tehdään tekemällä tietokoneen ja VPN:n tarjoajalle yksityinen yhteys yleensä käyttämällä salausta (engl. Encryption). Salaus on prosessi, jolla muutetaan viestin tietoja niin, että vain lähettäjä ja vastaanottaja osaa muuttaa viestin takaisin ja jos joku kolmas osapuoli saa viestin, se näyttää vain merkkisotkulta. (Wikipedia 2012)

VPN kehitettiin mahdollistamaan toimistojen ohjelmien ja resurssien käytön etänä, kotoa tai mistä tahansa. VPN:ää voi myös käyttää ohittamaan geo-estoa, sensurointia tai suojata henkilökohtaista identiteettiä ja pysyä anonyyminä internetissä. Geo-esto estää tiettyjä internet sisältöä näkymästä tietyissä maissa, kuten esimerkiksi Netflix sarjoja, jotka näkyvät vain Yhdysvalloissa. VPN:n avulla saadaan näyttämään sijainnin olevan esimerkiksi Yhdysvalloissa, vaikka siellä ei fyysisesti ollakaan. VPN luo salatun yhteyden, jonka julkinen internet yhteys on toisaalla, esimerkiksi Yhdysvalloissa. Useat sivustot estävät tunnetut VPN:n palvelimet. (Wikipedia 2012)

VPN ei voi tehdä verkkokäytöstä täysin anonyymistä, mutta lisää turvaa, estämällä yksityisen tiedon antoa kuten sijainnin. VPN:n saa ostamalla yritysiltä, jotka erikoistuvat VPN-palvelujen myyntiin. VPN:n pystyy myös tekemään itse. (Wikipedia 2012)

3.6 Tor verkkoselain

Tor on ilmainen ohjelma, joka mahdollistaa anonyymin verkkoselailun ja kommunikoinnin verkossa. Nimi tulee ohjelman alkuperäisestä projekti nimestä "The Onion Router". Tor välittää verkkoliikenteen tuhansien välityspalvelimien kautta peittääkseen käyttäjän sijainnin ja käyttöä verkkoliikenteen seuraajilta tai palvelimen ylläpitäjältä. Tor suojaa siis

vain käyttäjän yksityisyyttä, mutta ei piilota, että verkkopalveluja käytetään käyttämällä Toria. Jotkut verkkosivut estävät tiettyjä toiminnallisuuksia, mikäli käyttää Toria. (Wikipedia 2007) (LEMMiNO 2016)

Tor toimii nimensä mukaisesti sipulireitityksen avulla, jossa viestintä salataan kerrostetusti, ja verkkoliikenne kulkee salatusti välityspalvelimien kautta. Välityspalvelimet purkavat salauksen kerroksen, josta selviää liikenteen seuraava IP-osoite, jonne paketti lähetetään, jossa taas puretaan seuraava kerros. Kunnes lopulta päästään halutulle verkkosivulle, joka näkee vain viimeisen välityspalvelimen tiedot mutta ei käyttäjän tietoja. (Wikipedia 2007)

NRL aloitti kehittämään sipulireititystä 1990-luvulla, ja DARPA jatkoi 1997. Tavoitteena oli kehittää kommunikaatioväline internetin välityksellä, jotta välissä oleva salakuuntelija ei voisi selvittää lähdettä tai määränpäättä. NRL kuitenkin huomasi ongelman, jos pelkästään Yhdysvaltojen organisaatiot käyttävät tätä uutta salausteknologiaa. Kun käyttäjät menevät verkkosivuille käyttämällä tätä salausteknologiaa, verkkosivun hallitsijat tunnistaisi sen ja täten tunnistaisi käyttäjän joksikin Yhdysvaltojen organisaatioksi. Jotta teknologia olisi todellisesti anonymi, se tarvitsisi olla kaikkien käytettävissä. Tämän takia se julkaistiin ilmaisena kaikille käytettäväksi. (Wikipedia 2007) (LEMMiNO 2016)

Torin käyttötarkoitus ei ole täysin ratkaista anonymisyys verkossa tai poistaa jälkiä, vaan vähentää jälkien johtamista käyttäjään. Tästä johtuen Toria saatetaan käyttää myös laittomuuksiin. Suurin osa käyttäjistä kuitenkin käyttää Toria vain parantaakseen yksityisyyttä verkossa. Normaalit verkkoselaimet ovat kuitenkin nopeampia selailussa kuin Tor, johtuen salauksesta. (Wikipedia 2007)

4 RASPBERRY PI

Raspberry Pi on pienikokoinen yhden piirilevyn tietokone. Raspberry Pi:stä on monta erilaista versiota, Model A ja Model B, joista molemmista numeroituja ja plus versioita, jotka ovat päivitettyjä ja uusilla ominaisuuksilla. On myös saatavilla vielä pienempiä kompakteja Pi Zero versioita, jotka myös kuluttavat vähemmän virtaa.

Raspberry Pi:n voi ostaa myös pakettina, jossa tulee mukana kotelo (Kuva 1). Kotelo suojaa pölyltä ja osumilta, jos se putoaa. Paketissa on myös muistikortti, jossa on Raspbian käyttöjärjestelmä valmiiksi asennettuna. Raspbian on linux pohjainen käyttöjärjestelmä, joka on optimoitu Raspberry Pi:lle.



Kuva 1. Raspberry Pi 3 kotelossa.

Raspberry Pi 3:ssa on virtaportti, johon sopii 5V MicroUSB virtalähde. Tukee myös virtaa Ethernet-portin kautta (POE, engl. Power-Over-Ethernet), ja virtaa GPIO-pinnien kautta. Siinä on myös Hdmi portti videolle, AUX portti äänelle, 4 USB porttia ja Ethernet portti (Kuva 2).

GPIO-pinnit (engl. General purpose input-output) on yleiseen ja kaikenlaiseen käyttöön tarkoitettu portti, jolle ei ole mitään ennalta määriteltyä käyttötarkoitusta ja on oletuksena pois käytöstä. GPIO:ta käytetään useaan tarkoitukseen ja rajoitteena on vain virta, ajoitukset ja ohjelmien kyky käyttää porttia järkevästi. Porttia käytetään yleensä

logiikkana ja se ei pysty antamaan suurempaa virtaa laitteille. Sitä voidaan kuitenkin käyttää releen kautta ohjaamaan suuren virran laitteita, kuten valoja, lämmittimiä tai moottoreita. Tai monitoroimaan tai ohjaamaan muita mikropiirejä. Sen saa myös lukemaan yksinkertaisempia sensoreita, kuten lämpömittareita tai kiihtyvyyssantureita. Rele on sähköllä toimiva kytkin.



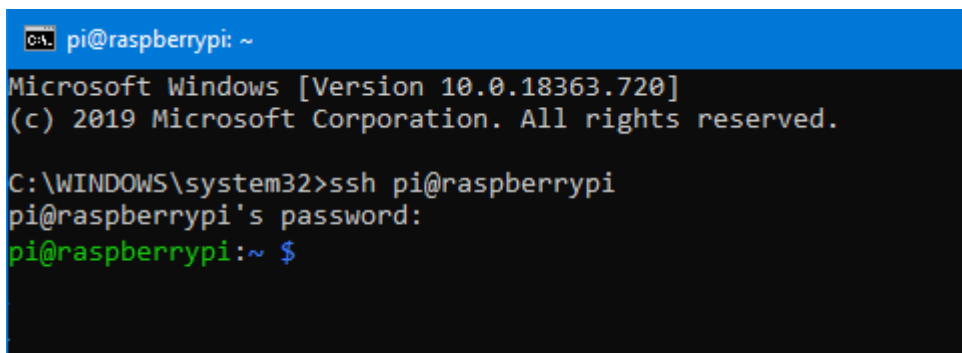
Kuva 2. Raspberry Pi 3 toiselta puolelta ja avattuna.

4.1 Käyttö

Käyttöjärjestelmä asennetaan muistikortille, joka on paketissa valmiina. Raspberry Pi:tä voi käyttää kuten muitakin tietokoneita liittämällä näytön HDMI-porttiin ja USB-portteihin näppäimistön ja hiiren. Kun ensiasetukset on laitettu, Raspbiania voi käyttää normaalina tietokoneena, selata verkkosivuja ja käyttää ohjelmia. Mukana tulee ilmaisia ohjelmia kuten esimerkiksi Chromium, Libreoffice ja muita ohjelmointiohjelmia. Raspberry Pi 3 tukee myös langatonta verkkoa, joten minimissään ei tarvitse kuin virtajohdon olla kiinni.

4.2 Etäkäyttö

Raspberry Pi:tä voi myös käyttää etänä eli käyttää muilta tietokoneilta tai laitteilta. Raspberry Pi:stä pitää ottaa käyttöön SSH- tai VNC Server -palvelintoiminnot. Windows 10:stä pitää ottaa SSH-lisäosa käyttöön, jolla voi komentokehotteen (engl. command line) kautta ottaa yhteyden Raspberry Pi:hin (Kuva 3). SSH on pelkästään tekstimuotoinen, jota voi käyttää komentojen syöttämiseen ja tietokoneen tilojen selvittämiseen. SSH:lla on myös helppo syöttää ja muokata asioita, kun ei tarvitse eri valikoissa selailia.

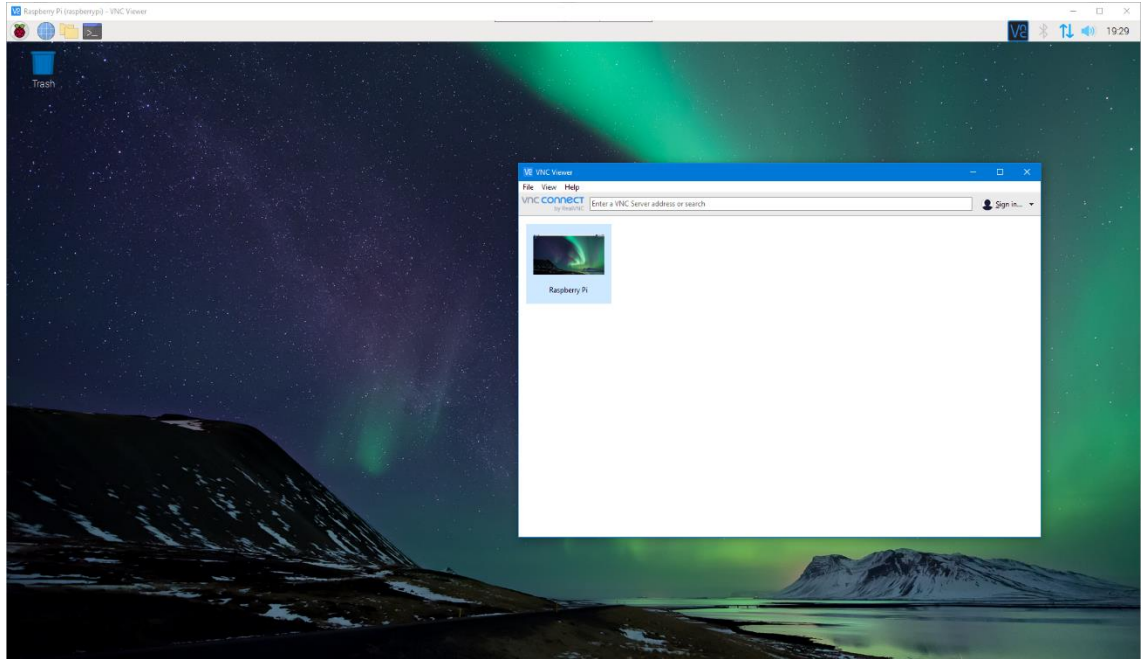
A screenshot of a Windows command prompt window. The title bar is blue and contains the text 'pi@raspberrypi: ~'. The main area is black with white text. It shows the Microsoft Windows version (10.0.18363.720) and copyright information (© 2019 Microsoft Corporation). The user has entered the command 'ssh pi@raspberrypi' and the prompt has changed to 'pi@raspberrypi:~ \$', indicating a successful connection to the Raspberry Pi.

```
pi@raspberrypi: ~
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ssh pi@raspberrypi
pi@raspberrypi's password:
pi@raspberrypi:~ $
```

Kuva 3 Komentokehote.

VNC-palvelimen avulla Raspberry Pi:tä voi käyttää ilman erillistä näppäimistöä, hiirtä ja näyttöä, suoraan toiselta tietokoneelta (Kuva 4 Kuva 4 VNC Client käytössä, joka on pienempi ikkuna. Isompi ikkuna on etäohjattu Raspberry Pi.). Käyttäjän tarvitsee ladata etäohjaavalle tietokoneelle VNC Client sovellus, jolloin se toimii samoin kuin Windowsin oma etäkäyttö, ja tukee useampia samanaikaisia käyttäjiä.



Kuva 4 VNC Client käytössä, joka on pienempi ikkuna. Isompi ikkuna on etäohjattu Raspberry Pi.

5 PI-HOLE-OHJELMISTO

Pi-Hole on koko paikallisen verkon kattava mainoksien estäjä, joka asennetaan kerran ja toimii kaikilla verkkoon liitettävillä laitteilla. Se asennetaan haluttuun tietokoneen Linux-pohjaiselle käyttöjärjestelmälle. Suosituksena on käyttää Raspbian-käyttöjärjestelmää. Pi-Hole toimii verkon DNS-palvelimena, ja tutkii verkon liikennettä ja estää DNS kyselyt valittuihin osoitteisiin. Sisältää paljon ominaisuuksia, joilla muokata toimintaa ja lisätä poikkeuksia.

Pi-Hole on hyvä valinta jos on laitteita, joille ei saa muunlaisia mainosten estäjiä. Mikäli on paljon laitteita, jokaiselle ei tarvitse erikseen asentaa mitään. Ei kuitenkaan toimi yhtä hyvin kuin esimerkiksi verkkoselaimelle saatavilla olevat lisäosat. Pi-Hole jättää verkkosivuille jotain mainoksen paikalle, kuten tyhjää tilaa.

Pi-Hole sopii hyvin asennettavaksi Raspberry Pi:lle vähäisen prosessointitehovaatimuksen takia. Pi-Holen sivuilta löytyy yksityiskohtaiset ohjeet asentamiselle ja yleiset käyttöohjeet.

5.1 Vaatimukset

Asennus tuetaan muutamalle Linux-pohjaiselle käyttöjärjestelmälle, kuten Raspbian, Ubuntu, Debian, Fedora tai CentOS. Ohjelma toimii parhaiten ja vähimmillä ongelmilla Raspbianilla. (Pi-Hole 2015)

Pi-Hole tarvitsee myös pysyvän IP-osoitteen, joka täytyy asettaa reitittimestä tai ennen asennusta käyttöjärjestelmästä. Tunnetaan myös DHCP-varauksena, reitittimissä. (Pi-Hole 2015)

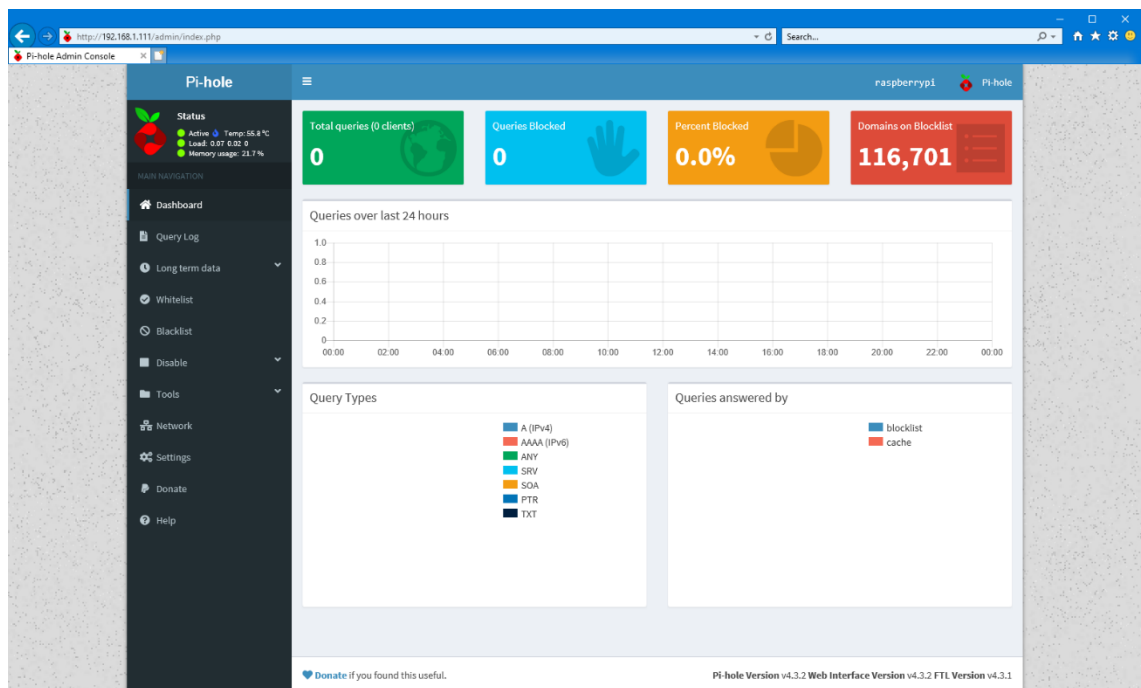
5.2 Asennus

Asennuksen voi tehdä helposti ja nopeasti yhdellä koodilla, joka lataa ja asentaa Pi-holen automaattisesti. Manuaalinen asennus on myös saatavilla, mikäli haluaa nähdä, mitä asennus tekee. (Pi-Hole 2015)

Reitittimestä pitää vaihtaa DNS palvelin Pi-Holen IP-osoitteeksi, jotta kaikki liikenne menee Pi-Holen kautta. Vaihtoehtoisesti voi myös vaihtaa DNS-palvelimen erikseen haluamista laitteista, mikäli se on mahdollista. (Pi-Hole 2015)

5.3 Toiminnassa

Kun asennus on suoritettu, ohjelma antaa salasanan, jolla voi kirjautua Pi-Holen verkkosivulle (Kuva 5). Verkkosivu löytyy Pi-Holen IP-osoitteesta, josta näkee tietoja eri hauista ja siellä voi muuttaa asetuksia. Tiedot voidaan myös piilottaa niin, ettei niitä näytetä tai kerätä ollenkaan.



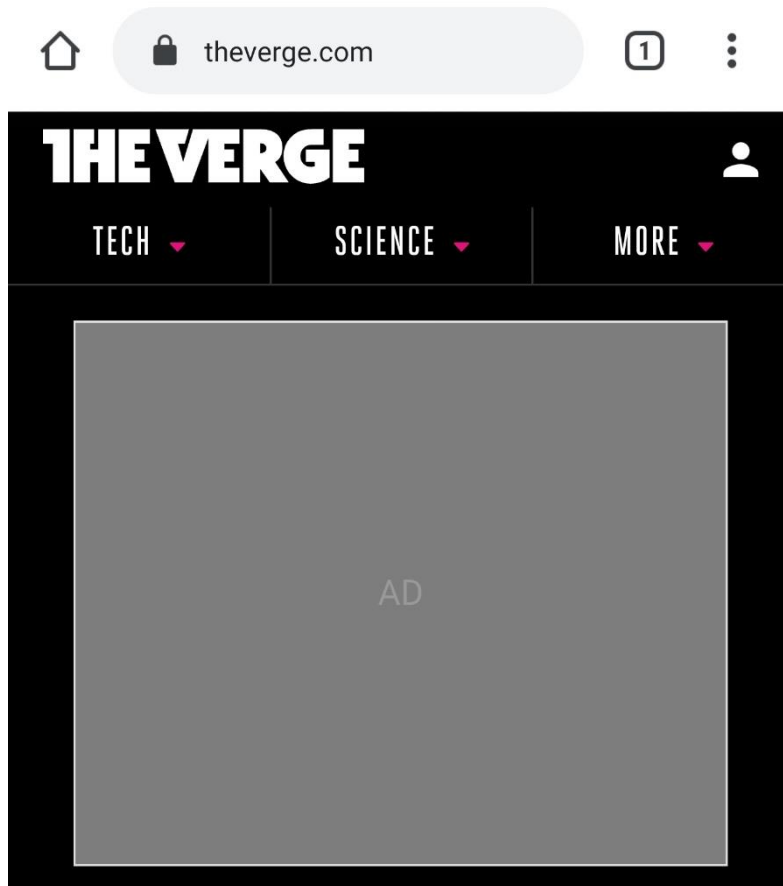
Kuva 5. Etusivu.

Blacklist-sivulta pystyy muokkaamaan estettyjä verkkosivuja, johon asennuksen aikana voi valita yleisimmät sivut. Mustalistalle ei lisätä esimerkiksi uutissivustoja, joilla on mainoksia, vaan uutissivut hakevat mainokset toisilta sivustoilta, jotka lisätään mustalistalle.

Network-sivulla on kaikki verkosta löytyvät laitteet. Laitteet näkyvät vihreänä, mikäli ne käyttävät Pi-Holea.

5.3.1 Mainoksien esto

Verkkosivuilla mainokset estetään, mutta useimmilla sivuilla silti näkyy mainoksille tehdyt välit (Kuva 6) tai "tiedostoa ei löytynyt"-kuva (Kuva 7) mainoksen tilalla.



Kuva 6. Mainoksen väli.



Kuva 7. Tiedostoa ei löytynyt.

Yksinkertaisesti Pi-Hole vain vertailee kaikkia osoitteita, joita laitteet pyytävät, kun käyttäjät lataavat verkkosivuja. Pi-Hole estää yhteyden, mikäli ne ovat mustalistalla.

5.3.2 Seuranta ja muokkaus

Verkkosivuja voi seurata kyselylista (Query log) sivulta (Kuva 8). Listalla näkyy laitteiden lataamat sivut, jos seuranta on käytössä. Sivut näkyvät vihreänä, jos se on päästetty läpi (forwarded) ja punaisena jos se on estetty (blocked). Kyselylista sivulta pystyy myös lisäämään tai poistamaan mainossivustoja nopeasti tarvittaessa, jolloin ne ilmestyvät Whitelist tai Blacklist sivuille.

Time	Action	Domain	IP	Status	Response	Action
2019-11-05 17:50:50	A	match.sharethrough.com	192.168.1.148	OK (forwarded)	CNAME (33.3ms)	Blacklist
2019-11-05 17:50:50	A	prebid-match.dotomi.com	192.168.1.148	OK (forwarded)	CNAME (144.4ms)	Blacklist
2019-11-05 17:50:50	A	ap.ljlt.com	192.168.1.148	Blocked (gravity)	- (0.2ms)	Whitelist
2019-11-05 17:50:49	A	secure.admxs.com	192.168.1.148	Blocked (gravity)	- (0.3ms)	Whitelist
2019-11-05 17:50:49	A	eu-u.openx.net	192.168.1.148	Blocked (gravity)	- (0.4ms)	Whitelist
2019-11-05 17:50:46	A	ice.360yield.com	192.168.1.148	OK (forwarded)	CNAME (55.7ms)	Blacklist
2019-11-05 17:50:46	A	guardian-d.openx.net	192.168.1.148	OK (forwarded)	IP (57.8ms)	Blacklist
2019-11-05 17:50:46	A	elb.the-ozone-project.com	192.168.1.148	OK (forwarded)	CNAME (31.5ms)	Blacklist
2019-11-05 17:50:46	A	hb-api.omnitags.com	192.168.1.148	OK (forwarded)	CNAME (32.7ms)	Blacklist
2019-11-05 17:50:46	A	ib.admxs.com	192.168.1.148	Blocked (gravity)	- (0.2ms)	Whitelist
2019-11-05 17:50:46	A	as-sec.casalemedia.com	192.168.1.148	Blocked (gravity)	- (0.3ms)	Whitelist
2019-11-05 17:50:46	A	hbopenbid.pubmatic.com	192.168.1.148	OK (forwarded)	CNAME (11.8ms)	Blacklist
2019-11-05 17:50:42	A	adservice.google.com	192.168.1.148	Blocked (gravity)	- (0.1ms)	Whitelist
2019-11-05 17:50:42	A	adservice.google.fi	192.168.1.148	OK (forwarded)	CNAME (21.5ms)	Blacklist
2019-11-05 17:50:42	A	googleads.g.doubleclick.net	192.168.1.148	Blocked (gravity)	- (0.2ms)	Whitelist
2019-11-05 17:50:42	A	www.googletagservices.com	192.168.1.148	Blocked (gravity)	- (0.3ms)	Whitelist
2019-11-05 17:50:42	A	clients1.google.com	192.168.1.148	OK (forwarded)	CNAME	Blacklist

Kuva 8. Kyselylista.

Suomalaiset mainossivut harvoin on estetty, joten suomalaiset mainokset pääsevät läpi. Silloin ne pitää itse lisätä mustalistalle (Kuva 9).

Pi-hole

Status: Active, Temp: 56.9°C, Load: 0.13 0.09 0.01, Memory usage: 22.6%

MAIN NAVIGATION: Dashboard, Query Log, Long term data, Whitelist, Blacklist, Disable, Tools, Network, Settings, Donate, Help

Blacklist

Add a domain (example.com or sub.example.com) [Add (exact)] [Add (wildcard)] [Add (regex)]

Exact blocking

adservice.google.fi [Remove]

Regex & Wildcard blocking

PI-hole Version v4.3.2 Web Interface Version v4.3.2 FTL Version v4.3.1

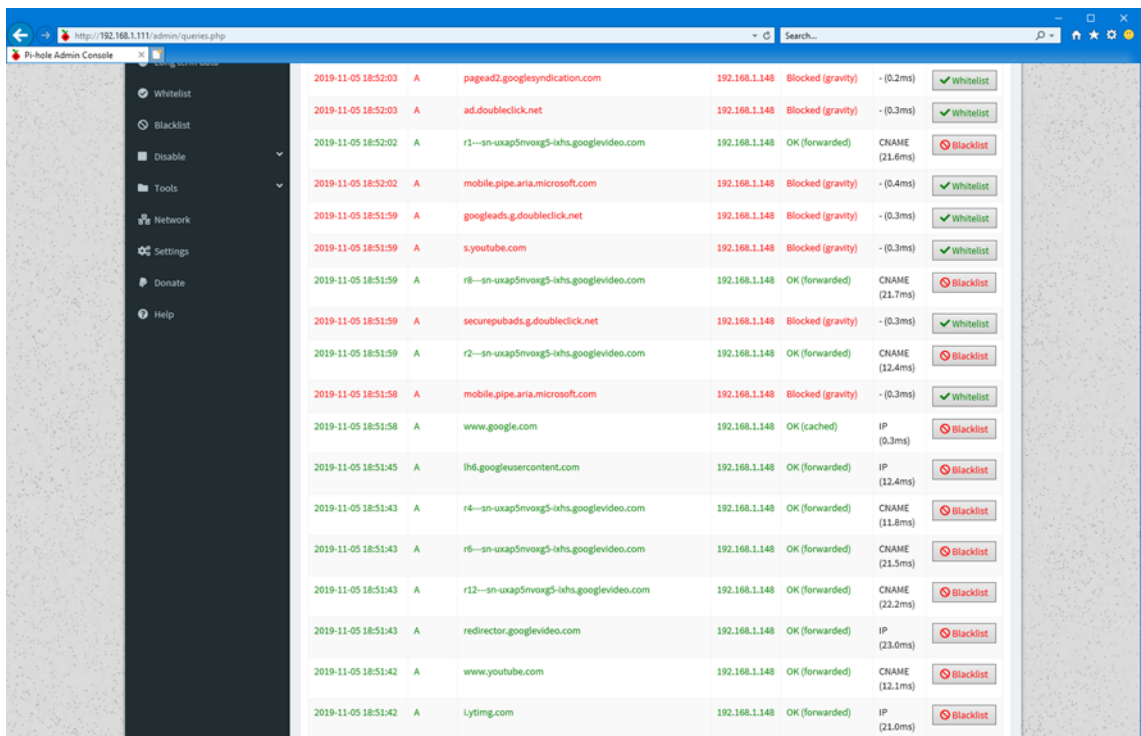
Kuva 9. Mustalista.

Pi-Hole tukee myös regexiä, jonka avulla voi estää sivuja, jotka ovat samannimisiä, mutta satunnaisilla kirjaimilla alussa. Regex (engl. Regular expression) on tietynlainen merkkijono, jolla voi tarkistaa tekstiä, jos esimerkiksi salasanassa on tarpeeksi isoja ja pieniä kirjaimia ja numeroita. Regexillä voi siis tehdä lauseen, jonka avulla voi estää kaikki sivut, jotka loppuvat tietynlaisesti.

Seurannan voi laittaa asetuksista pois päältä tai näyttää muutamalla eri tasolla anonyymisti eri tietoja.

5.3.3 YouTuben mainokset

YouTuben mainokset (Kuva 10) ovat hieman vaikeampia estää, koska Google käyttää satunnaisia sivuja, joilta lataa mainoksia. YouTube lataa kaikki videot googlevideo.com:sta, joten sitä ei voi estää. Muuten mikään video ei toimi. (faq-bot 2016)



Time	Action	Domain	IP	Status	Response Time	Action
2019-11-05 18:52:03	A	pagead2.googleadsyndication.com	192.168.1.148	Blocked (gravity)	~ (0.2ms)	Whitelist
2019-11-05 18:52:03	A	ad.doubleclick.net	192.168.1.148	Blocked (gravity)	~ (0.3ms)	Whitelist
2019-11-05 18:52:02	A	r1---sn-uxap5nvoxs5-ixhs.googlevideo.com	192.168.1.148	OK (forwarded)	CNAME (21.6ms)	Blacklist
2019-11-05 18:52:02	A	mobile.pipe.aria.microsoft.com	192.168.1.148	Blocked (gravity)	~ (0.4ms)	Whitelist
2019-11-05 18:51:59	A	googleads.g.doubleclick.net	192.168.1.148	Blocked (gravity)	~ (0.3ms)	Whitelist
2019-11-05 18:51:59	A	s.youtube.com	192.168.1.148	Blocked (gravity)	~ (0.3ms)	Whitelist
2019-11-05 18:51:59	A	r8---sn-uxap5nvoxs5-ixhs.googlevideo.com	192.168.1.148	OK (forwarded)	CNAME (21.7ms)	Blacklist
2019-11-05 18:51:59	A	securepubads.g.doubleclick.net	192.168.1.148	Blocked (gravity)	~ (0.3ms)	Whitelist
2019-11-05 18:51:59	A	r2---sn-uxap5nvoxs5-ixhs.googlevideo.com	192.168.1.148	OK (forwarded)	CNAME (12.4ms)	Blacklist
2019-11-05 18:51:58	A	mobile.pipe.aria.microsoft.com	192.168.1.148	Blocked (gravity)	~ (0.3ms)	Whitelist
2019-11-05 18:51:58	A	www.google.com	192.168.1.148	OK (cached)	IP (0.3ms)	Blacklist
2019-11-05 18:51:45	A	lh6.googleusercontent.com	192.168.1.148	OK (forwarded)	IP (12.4ms)	Blacklist
2019-11-05 18:51:43	A	r4---sn-uxap5nvoxs5-ixhs.googlevideo.com	192.168.1.148	OK (forwarded)	CNAME (11.8ms)	Blacklist
2019-11-05 18:51:43	A	r6---sn-uxap5nvoxs5-ixhs.googlevideo.com	192.168.1.148	OK (forwarded)	CNAME (21.5ms)	Blacklist
2019-11-05 18:51:43	A	r12---sn-uxap5nvoxs5-ixhs.googlevideo.com	192.168.1.148	OK (forwarded)	CNAME (22.2ms)	Blacklist
2019-11-05 18:51:43	A	redirector.googlevideo.com	192.168.1.148	OK (forwarded)	IP (23.0ms)	Blacklist
2019-11-05 18:51:42	A	www.youtube.com	192.168.1.148	OK (forwarded)	CNAME (12.1ms)	Blacklist
2019-11-05 18:51:42	A	lytimg.com	192.168.1.148	OK (forwarded)	IP (21.0ms)	Blacklist

Kuva 10. YouTuben mainokset.

Google vaihtaa tietyin väliajoin miltä sivuilta mainokset lähetetään, joten regexiä täytyy myös muokata. (faq-bot 2016)

5.4 Kaksoisoperaatio – VPN ja Pi-Hole

Raspberry Pille voi myös asentaa oman VPN palvelimen, jota kutsutaan OpenVPN -ohjelmaksi. Oma VPN mahdollistaa turvallisen tavan yhdistää omaan paikalliseen verkkoon ja käyttää omaa tietokonetta tai ohjelmia muualta maailmaa.

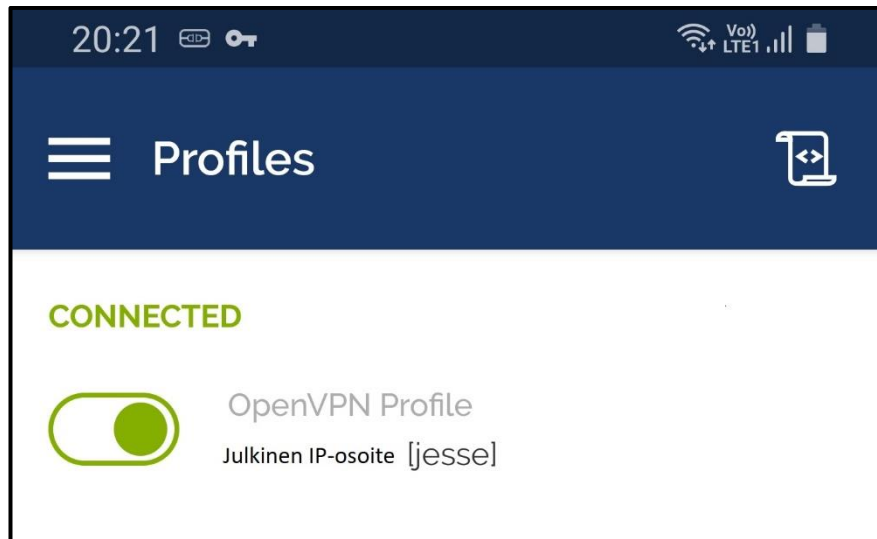
Pi-Holen verkkosivuilta löytyy ohjeet, joiden avulla saa VPN palvelimen ja Pi-Hole ohjelmiston toimimaan yhdessä, jolloin mainokset saa estettyä esimerkiksi puhelimesta, vaikka puhelin ei olisikaan omassa verkossa.

5.4.1 OpenVPN -ohjelmiston asennus

Ohjeiden mukaan VPN:n asennus onnistuu komentoilla, jotka laitetaan Raspberry Pi:in. Asennus myös luo käyttäjiä ja ovpn -tiedoston, joka annetaan käyttäjän laitteelle. VPN:ää voidaan käyttää vain sovelluksella, joka avaa yhteyden. Sovellus on saatavilla iOS, Android, Windows 10 ja Linux käyttöjärjestelmille. Kun käyttäjä avaa sovelluksen ja valitsee ovpn -tiedoston, voidaan VPN yhteys avata. Sen jälkeen tietokoneet näkevät, että VPN laite on paikallisessa verkossa, vaikka fyysisesti näin ei olekaan. (Pi-Hole 2015)

5.4.2 OpenVPN ja Pi-Holen yhdistäminen

Pi-Holen ja VPN toiminnan yhdistämiseen on myös helpot ohjeet, jotka vaativat muutaman lisäkomennon laittamista. Turvallisuuden lisäämiseksi Pi-Hole kannattaa olla palomuurin takana. Kun asetukset ovat oikein ja laitteet toiminnassa, mainokset estetään samoin VPN:n kautta kuin paikallisessa verkossa (Kuva 11). VPN lisää muutaman millisekunnin viivettä, mutta huonommalla yhteydellä viive voi olla pidempi. (Pi-Hole 2015)



Kuva 11. OpenVPN -ohjelmisto

5.5 Vaihtoehtoja

On useita tapoja estää mainoksia. Yksi suosituimmista on selaimeen asennettavat lisäosat. Niitäkin on monia ja toimivat hieman eri tavoin. Yleensä ne lukevat ja muokkaavat verkkosivujen koodia. Toiset paremmin ja nopeammin kuin toiset. Suosituimpia ovat Adblock, Adblock Plus ja uBlock Origin. Nimestä huolimatta Adblock ja Adblock Plus on eri yhtiöiden tekemät, ja koska ovat yhtiöiden omistuksessa, ne ovat ostettavissa. (Stampler 2013)

Ublock Origin on näistä suositeltavin avoimen koodin takia, jolloin kaikki näkevät koodin, jolla ohjelma on tehty. Sen estoasetuksia voi myös muuttaa kuten Pi-Holessa.

Kaikki kuitenkin vievät aikaa ja tietokoneelta resursseja, joten verkkosivujen lataus saattaa kestää muutaman sekunnin kauemmin kuin ilman estäjää. Mutta tässä ohjelmien erot huomaa. Testien mukaan uBlock Origin olisi muita tehokkaampi koska muilla kestää sivun lataus muutaman sekunnin kauemmin. Adblock Plussaa hidastaa myös ”hyväksytyt mainokset”-ominaisuus. (HAL9000 2017)

5.5.1 Ominaisuuksia

Adblock Plusassa on ominaisuus, joka estää vain häiritsevimmät mainokset, mutta näyttää jotain vähemmän häiritsevimpiä mainoksia. Tätä muun muassa Google on hyödyntänyt, ja kutsutaan hyväksyttäväksi mainoksiksi. Maksavat mainostajat saavat mainoksensa näkymään, vaikka käyttäjä on asentanut mainoksia estävän lisäosan. Käyttäjän täytyisi myös maksaa, ettei näe muita mainoksia kuin maksavien mainostajien. Adblock Plussan on myös huomattu olevan yhteydessä tuntemattomiin verkkosivuihin, jotka mahdollisesti tallentavat käyttäjien tietoja. (Statt 2015) (Andalur 2014)

Adblockilla on ominaisuus, jossa ilmestyy ponnahdusikkuna, joka pyytää lahjoituksia. Se saattaa olla huijausta, ja rahat menevät muuhun kuin ohjelman kehittämiseen. Adblock myös osti uBlockin, jonka jälkeen uBlock myös tuki hyväksyttäviä mainoksia, ja uBlockin tekijä teki uuden ohjelman nimeltä uBlock Origin. (Andalur 2014)

5.5.2 Mobiililaitteille

Mobiililaitteille mainoksien estäjät ovat hieman hankalampia. Muutamat vaativat roottamista, eli käyttöjärjestelmän uudelleenasetusta, joka mitätöi useimmissa tapauksissa takuun, tai monimutkaisia vaiheita. On myös erillisiä selaimia, jotka estävät mainoksia mutta sitten ei voi käyttää haluttua selainta, kuten Chrome tai Safari. Firefoxin mobiiliversioon on kuitenkin saatavilla lisäosia.

6 TULOKSET

Mainosten määrä verkkoselailussa on lisääntynyt huomattavasti. Työn tavoitteena oli löytää ratkaisu mainosten poistamiseen verkkoselaimista sekä kaikista internetiä käyttävistä laitteista.

Vaihtoehtoina löytyi verkkoselaimeen saatavat lisäosat, mobiililaitteille saatavat ohjelmistot sekä, mainosten esto-ohjelmisto Pi-Hole. Verkkoselaimeen saatavat lisäosat estävät mainokset vain käytettävissä olevan verkkoselaimen osalta ja mobiililaitteille saatavat ohjelmistot estävät mainokset vain kyseisen laitteen osalta, mutta Pi-Hole -ohjelmisto estää mainokset koko paikallisverkkoa käyttävissä laitteissa.

Tietokoneelle saatavat lisäosat saavat verkkosivut näyttämään paremmalta poistamalla mainoksen välin. Lisäosat ovat mainio valinta mainosten estossa, mikäli ne toimivat. Suurin osa lisäosista ovat ilmaisia.

Pi-Hole on koko paikallisverkon kattava mainosten estäjä, joka asennetaan kerran ja toimii kaikilla verkkoon liitettävillä laitteilla. Pi-Hole estää kaikki mainokset, jota laitteille tulisi, mutta mainokselle varattu tila jää näkyviin. Pi-Hole estää myös mobiilipeleissä näkyvät mainokset.

Raspberry Pi -tietokoneen etu onkin se, että se voi olla aina käynnissä ja poissa näkyvistä, pienen virrankulutuksen ja koon vuoksi. Pi-Hole itsessään on ilmainen mutta tarvitsee jonkinlaisen tietokoneen, jossa on Linux-pohjainen käyttöjärjestelmä. Pelkästään Raspberry Pi maksaa noin 35–60 € ja tuotepaketit, joissa on kotelo, johdot ja muistikortti mukana, maksavat noin 80–110 €, mallista ja ostopaikasta riippuen. Raspberry Pi:tä voi myös samanaikaisesti käyttää muuhunkin, paitsi verkkosivun ylläpitoon, koska se on jo Pi-Holen käytössä.

Pi-Holen voi yhdistää VPN:n ja Tor-selaimen kanssa, jotta saadaan todella hyvä turva kaikenlaiselta seurannalta.

Pi-Hole on mielestäni paras valinta, mikäli käyttää verkossa useaa laitetta. Kaikille laitteille ei siten tarvitse asentaa erikseen lisäosia. Kaikille laitteille ei edes voi asentaa lisäosia, kuten esimerkiksi älytelevisioihin.

Pi-Hole sopii sellaisille käyttäjille, jotka tietävät tai haluavat oppia Linux-käyttöjärjestelmästä.

LÄHTEET

- Andalur 2014. Security Stackexchange, Adblock Plus a security risk? Viitattu 29. huhtikuuta 2020 <https://security.stackexchange.com/questions/52361/is-adblock-plus-a-security-risk>.
- Dewey, C. 2016. The Washington Post, 98 personal data points that Facebook uses to target ads to you. Viitattu 28. huhtikuuta 2020 <https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/>.
- faq-bot 2016. Reddit, how do I block ads on YouTube. Viitattu 10. toukokuuta 2020 <https://discourse.pi-hole.net/t/how-do-i-block-ads-on-youtube/253>.
- GCFLearnfree 2016. What is targeted advertising? Viitattu 28. huhtikuuta 2020 <https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/>.
- HAL9000 2017. Raymond, 10 ad blocking extensions tested for best performance. Viitattu 2. toukokuuta 2020 <https://www.raymond.cc/blog/10-ad-blocking-extensions-tested-for-best-performance/view-all/>.
- LEMMiNO 2016. YouTube, The Dark Side of the Web. Viitattu 9. toukokuuta 2020 <https://www.youtube.com/watch?v=mUP0tx7lb2w>.
- Mediat, 2K 2002. Internetin historia. Viitattu 22. helmikuuta 2020 <https://www.2kmediat.com/tietoverkot/historiaa2.asp>.
- Peda.net 2010. Johdatus Cyberturvallisuuteen, Internetin lyhyt historia. Viitattu 22. helmikuuta 2020 <https://peda.net/jyu/it/do/kkv/2-internet/2ilh>.
- Peda.net 2010. Johdatus Cyberturvallisuuteen, Mikä on internet? Viitattu 22. helmikuuta 2020 <https://peda.net/jyu/it/do/kkv/2-internet/2moi>.
- Pi-Hole 2015. Pi-Hole, dokumentointi ja ohjeet. Viitattu 25. syyskuuta 2019 <https://docs.pi-hole.net/>.
- Pi-Hole 2015. Pi-Hole, Etusivu ja ohjelman lataus. Viitattu 25. syyskuuta 2019 <https://pi-hole.net/>.
- Pi-Hole 2015. Pi-Hole, OpenVPN asennus. Viitattu 5. kesäkuuta 2020 <https://docs.pi-hole.net/guides/vpn/setup-openvpn-server/>.
- Pi-Hole 2015. Pi-Hole, yhdessä LAN ja VPN. Viitattu 5. kesäkuuta 2020 <https://docs.pi-hole.net/guides/vpn/dual-operation/>.
- Reddit 2005. Redditin sisällön säännöt. Viitattu 5. kesäkuuta 2020 <https://www.redditinc.com/policies/content-policy>.
- Stampler, L. 2013. Business Insider, Google saved an estimated \$887 million by paying Adblock Plus to show its ads. Viitattu 29. huhtikuuta 2020 <https://www.businessinsider.com/google-saved-an-estimated-887-million-by-paying-adblock-plus-to-show-its-ads-2013-8?r=US&IR=T>.

Statt, N. 2015. The Verge, Unknown buyer scoops up popular Adblock extension. Viitattu 29. huhtikuuta 2020 <https://www.theverge.com/2015/10/2/9441319/adblock-acquisition-unknown-buyer>.

Wikipedia 2001. Wikipedia, Military Network (MILNET). Viitattu 7. kesäkuuta 2020 <https://en.wikipedia.org/wiki/MILNET>.

Wikipedia 2005. Wikipedia, Internet. Viitattu 23. helmikuuta 2020 <https://en.wikipedia.org/wiki/Internet>.

Wikipedia 2007. Wikipedia, Tor verkko. Viitattu 23. helmikuuta 2020 [https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network)).

Wikipedia 2007. Wikipedia, Virtual Network Computing (VNC). Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/VNC>.

Wikipedia 2008. Wikipedia, Secure Shell (SSH). Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/SSH>.

Wikipedia 2008. Wikipedia, World Wide Web (WWW). Viitattu 7. kesäkuuta 2020 https://fi.wikipedia.org/wiki/World_Wide_Web.

Wikipedia 2009. Wikipedia, ARPANET. Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/ARPANET>.

Wikipedia 2009. Wikipedia, Profilointi. Viitattu 23. helmikuuta 2020 [https://en.wikipedia.org/wiki/Profiling_\(information_science\)](https://en.wikipedia.org/wiki/Profiling_(information_science)).

Wikipedia 2009. Wikipedia, Voice over Internet Protocol (VoIP). Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/VoIP>.

Wikipedia 2010. Wikipedia, Defense Advanced Research Projects Agency (DARPA). Viitattu 7. kesäkuuta 2020 <https://en.wikipedia.org/wiki/DARPA>.

Wikipedia 2010. Wikipedia, Domain Name System (DNS). Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/DNS>.

Wikipedia 2010. Wikipedia, Dynamic Host Configuration Protocol (DHCP). Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/DHCP>.

Wikipedia 2010. Wikipedia, Power over Ethernet (PoE). Viitattu 7. kesäkuuta 2020 https://fi.wikipedia.org/wiki/Power_over_Ethernet.

Wikipedia 2010. Wikipedia, Turvallisuus internetissä. Viitattu 23. helmikuuta 2020 https://en.wikipedia.org/wiki/Internet_security.

Wikipedia 2011. Wikipedia, Transmission Control Protocol (TCP). Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/TCP>.

Wikipedia 2011. Wikipedia, Yksityisyys internetissä. Viitattu 23. helmikuuta 2020 https://en.wikipedia.org/wiki/Internet_privacy.

Wikipedia 2012. Wikipedia, CERN. Viitattu 7. kesäkuuta 2020 <https://fi.wikipedia.org/wiki/Cern>.

Wikipedia 2012. Wikipedia, virtuaalinen erillisverkko. Viitattu 23. helmikuuta 2020
https://en.wikipedia.org/wiki/Virtual_private_network.

Wikipedia 2012. Wikipedia, Virtual Private Network (VPN). Viitattu 7. kesäkuuta 2020
<https://fi.wikipedia.org/wiki/VPN>.

Wikipedia 2013. Wikipedia, File Transfer Protocol (FTP). Viitattu 7. kesäkuuta 2020
<https://fi.wikipedia.org/wiki/FTP>.

Wikipedia 2013. Wikipedia, IP-osoite. Viitattu 7. kesäkuuta 2020
<https://fi.wikipedia.org/wiki/IP-osoite>.

Wikipedia 2013. Wikipedia, National Science Foundation Network (NSFNET). Viitattu 7. kesäkuuta 2020
https://en.wikipedia.org/wiki/National_Science_Foundation_Network.

Wikipedia 2013. Wikipedia, United States Naval Research Laboratory (NRL). Viitattu 7. kesäkuuta 2020
https://en.wikipedia.org/wiki/United_States_Naval_Research_Laboratory.

Wikipedia 2015. Wikipedia, Doksaus. Viitattu 7. kesäkuuta 2020
<https://fi.wikipedia.org/wiki/Doksaus>.

Wikipedia 2016. Wikipedia, General Purpose I/O (GPIO). Viitattu 7. kesäkuuta 2020
<https://fi.wikipedia.org/wiki/GPIO>.

Wikipedia 2017. Wikipedia, Säännöllinen lauseke. Viitattu 7. kesäkuuta 2020
https://fi.wikipedia.org/wiki/S%C3%A4%C3%A4nn%C3%B6llinen_lauseke.