VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Nina Nurmela

VERKKOMAINONNAN KÄYTTÄJÄ-SEURANNALTA SUOJAUTUMINEN

Liiketalous
2016

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Nina Nurmela
Opinnäytetyön nimi	Verkkomainonnan käyttäjäseurannalta suojautuminen
Vuosi	2016
Kieli	suomi
Sivumäärä	57
Ohjaaja	Antti Mäkitalo

Opinnäytetyö tutkii, miten yksityisten kuluttajien toimia internetissä seurataan verkkomainostajien toimesta. Mainonnan päämääränä on tuottaa oikeaa tietoa, oikeille yleisöille ja oikeaan aikaan, ja internetin tekniikka on mahdollistanut tämän tavalla, johon perinteinen media ei kykene. Verkkomainonta pystyy kohdistamaan mainonnan yksittäisille käyttäjille reaaliaikaisesti selainkäytön ja internetsurffauksen perusteella. Käyttäjien kiinnostusten kohteiden tavoittelusta koituu myös yksityisyysongelmia, kun mainosyhtiöt sekä muut seuraajat saavat käyttöönsä yhä enemmän henkilökohtaisia tietoja käyttäjistä.

Työn teoreettisessa osuudessa selvitetään mainostajien motiivit käyttäjäseurantaan ja minkälaisia keinoja heillä on seurannan toteuttamiseen. Välineistä yleisimmässä käytössä ovat HTTP-evästeet. Käytännön osuudessa käydään yksityiskohtaisesti läpi konkreettisia keinoja, joilla käyttäjät voivat torjua seurantaevästeitä. Ilmaisia keinoja ovat käytettävän laitteen selaimen asetusten muokkaaminen sekä erilaisten selainlaajennusten asentaminen. Maksullisista keinoista käsitellään F-Secure-tietoturvayrityksen FreeDome-niminen VPN-toteutus. Jokaisesta työkalusta käydään läpi, miten ne vaikuttavat seurannan torjumiseen käytännössä internetiä selatessa.

Tutkimuksessa havaittiin käyttäjäseurannan tärkeys verkkomainostajille. Käyttäjien kiinnostusten kohteiden kartoittaminen helpottaa merkittävästi oikean kohdeyleisön löytämistä kullekin mainokselle, ja se parantaa markkinointi-investointien tuottoa. Seurantaevästeitä pystyy helposti torjumaan työssä esitellyillä keinoilla, mutta puutteita havaittiin sekä mainosyhtiöiden omassa palvelussa evästeiden kieltämiseksi että virallisissa rajoitustoimissa.

Avainsanat yksityisyys, seuranta, mainonta, evästeet

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Nina Nurmela
Title	Protection from Online Advertising User Tracking
Year	2016
Language	Finnish
Pages	57
Name of Supervisor	Antti Mäkitalo

The study researches how the internet behavior of individual consumers is tracked by online advertisers. The focus of marketing is to produce the right information to the right audiences at the right time, and internet technology has made this possible in ways traditional media cannot. Online advertising is capable of targeting advertisements to individual users in real time based on the user's browsing behavior. Gathering user interests also causes privacy issues when advertisers and other trackers can obtain increasingly much intimate information on users.

The theoretical part of the study explores advertisers' motives for user tracking and what means they have for conducting the said tracking. The most common tool is HTTP cookies. The practical section describes in detail the concrete methods users can utilize to block tracking cookies. Cost-free methods include modifying the browser settings of the device in use and installing various browser extensions. Paid methods are represented by a VPN implementation called FreeDome made by the information security company F-Secure.

The study revealed the importance of user tracking to internet advertisers. Mapping user interests significantly eases finding the right target audiences for each advertisement, and it improves the return on investment. Tracking cookies are easy to block with the tools explained in the study, but deficiencies were observed both in the advertising industry's own tracking cookie opt-out service and in the official cookie usage restriction policies.

Keywords Privacy, tracking, advertising, cookies

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

1 JOHDANTO

Yksityisyys internetissä on valtava aihe, joka tuli todenteolla esille vuonna 2013, kun Edward Snowden paljasti yhdysvaltalaisen National Security Agencyn maailmanlaajuisen tietoliikennevakoilun. Internetseurannasta hyötyvät niin valtiolliset kuin kaupalliset toimijat, ja internetin tekniikka mahdollistaa laajan ja organisoidun seurannan toteuttamisen. Kun seurannasta on niin ilmeistä hyötyä, käyttäjien oikeus yksityisyyteen uhkaa kärsiä siitä.

Verkkomainonta on alue, joka kannustaa yhä mittavampaan käyttäjäseurantaan. Mitä yksityiskohtaisemmin mainostavat tahot tietävät yksittäisten kuluttajien haluista ja kiinnostuksenkohteista, sitä todennäköisemmin mainokset osataan kohdentaa oikein. Tämän työn tavoitteena on vastata seuraaviin kysymyksiin:

1. Mitkä ovat mainostajien motiivit käyttäjien seurantaan?
2. Miten mainostajat seuraavat käyttäjiä ja profiloivat heitä?
3. Miten käyttäjä voi suojautua mainostajien seurannalta?

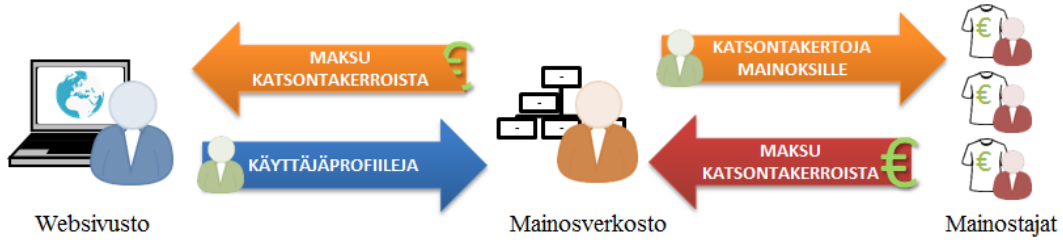
Työssä on tutkittu läheisesti HTTP-evästeiden suhdetta verkkomainonnan käyttäjäseurantaan. Tutkimusmateriaalina on käytetty aihepiirin kirjallisuutta ja tutkimuksia. Internet-teknologian nopean kehityksen takia lähdemateriaalina on pyritty käyttämään mahdollisimman uutta tietoa. Evästeiden toimintaa käytännössä on tutkittu Mozilla Firefox- ja Google Chrome -selaimilla niiden suurimman suosion vuoksi (W3Schools). Tietotekniikassa on monia englanninkielisiä vakiintuneita termejä ja ilmaisuja, joten Firefoxin esimerkit ovat suomenkielisiä ja Chromen englanninkielisiä, jotta molemmankieliset termit tulisivat tutuiksi.

2 MAINOSTAJIEN MOTIIVIT KÄYTTÄJÄSEURANTAAN

Kuehn kuvailee internetmainontaa kaksipuolisilla markkinoilla. Käyttäjät ja mainostajat tarvitsevat toisiaan muodostaakseen transaktioita, ja websivusto luo näille ryhmille yhteisen kohtaamisalustan (kuvio 1). Websivusto tarjoaa käyttäjille houkuttelevan, usein ilmaisen palvelun. Mainostajille sivusto tarjoaa potentiaalisten asiakkaiden huomiota mainoksille. Vastineeksi mainostilasta sivusto saa mainostajilta korvauksen, joka mahdollistaa palvelun ylläpitämisen. (Kuehn 2014.)

Kuvio 1. Internetmainonnan markkinakaava.

Mainokset voivat tulla sivustoille mainosverkoston kautta (kuvio 2). Tällöin mainosverkosto toimii välittäjänä sivustolle ja mainostajille. Mainosverkosto tarjoaa mainostajien tuotteille huomiota potentiaalisilta asiakkailta, ja mainostaja maksaa verkostolle tästä huomiosta. Verkosto maksaa osan tuotosta sivustolle, joka mainokset näyttää. Mitä paremmin verkosto pystyy näyttämään oikeat mainokset oikeille käyttäjille, sitä paremman tuoton se saa mainostajilta. Täten mainosverkostoille on hyödyllistä luoda mahdollisimman kattavia ja tarkkoja profiileja käyttäjistä. (Castelluccia & Narayanan 2012.)



Kuvio 2. Mainosverkoston rooli verkkomainonnassa.

Selainkäyttöön perustuva mainonta (online behavioral advertising, OBA) on käyttäjän aikaisemman selainkäytön hyväksikäyttämistä internetmainosten koh-

dentamisessa. Mikäli käyttäjä on esimerkiksi katsellut lomamatkoja, voi hän myöhemmin muilla sivustoilla nähdä mainoksia kyseisistä matkustuskohteista. (EDAA.)

Mainostajat ovat halukkaita maksamaan kohdennetusta mainostuksesta jopa kaksinkertaisen summan verrattuna vakiomainontaan (Kuehn 2014). Kohdennettu mainonta voi nostaa mainosinvestointien tuottavuutta 30–50 prosenttia. Internetissä on lähes rajattomasti mainostilaa, joten tietämällä, kuka käyttäjä on kiinnostunut mistäkin asiasta, riski väärin kohdennetusta mainonnasta pienenee. (Suich 2014.) Käyttäjien harrastukset ja intohimon kohteet ovat myös asioita, joihin käytettävissä oleva ylimääräinen raha investoidaan, joten mainostajat haluavat tietää mahdollisimman paljon yksittäisten kuluttajien haluista (Vaidhyanathan 2011, 112-113).

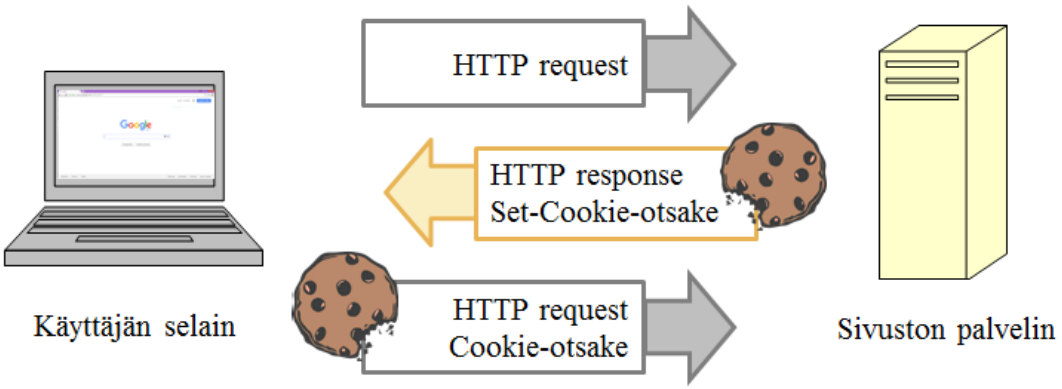
3 MAINONNAN SEURANTAKEINOT

Yleisin keino käyttäjäseurantaan ovat HTTP-evästeet (Tirtea, Castelluccia & Ikonomou 2011). Evästeistä on myös hienovaraisempi ja vaikeammin estettävissä oleva muoto, Adobe Flash –selainohjelman evästeet.

3.1 Evästeet

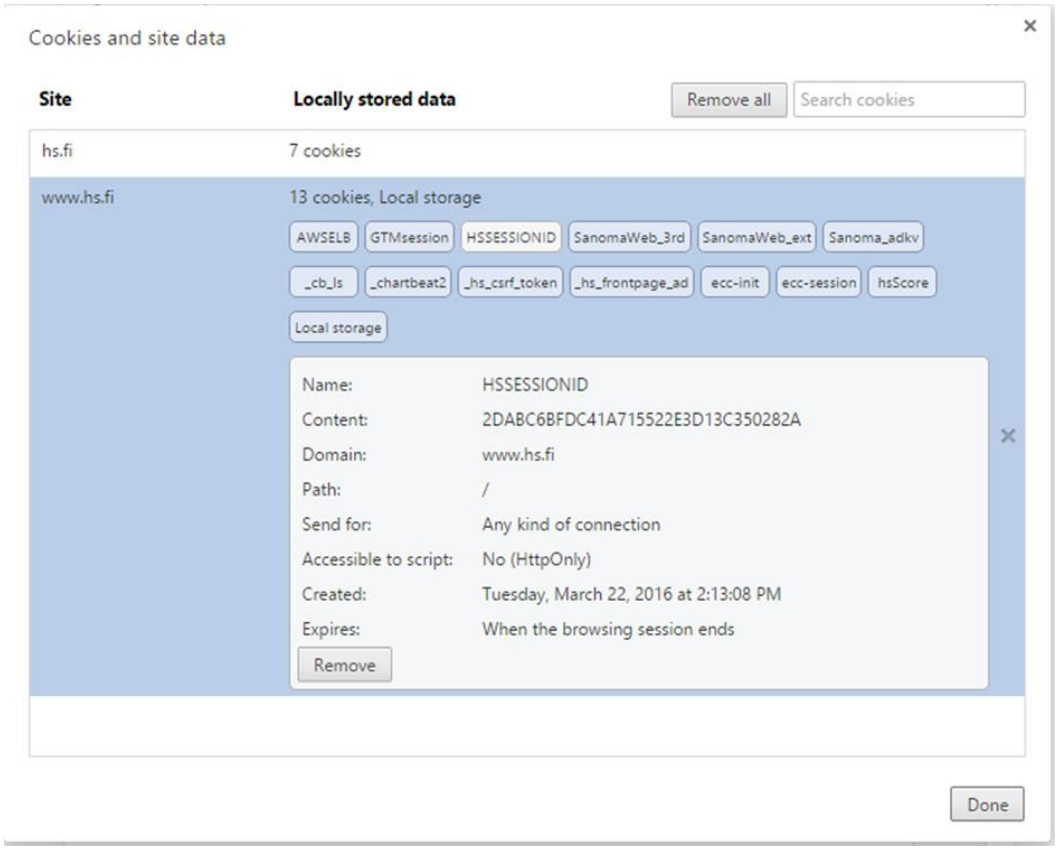
HTTP-protokolla, web-sivustojen liikenne, on tilaltaan *stateless*: se ei itsessään pysty muodostamaan yhteyttä kahden peräkkäisen sivuhaun välille. Käyttäjien tarpeet kuitenkin vaativat, että palvelin, jolla peräkkäiset sivuhaut tehdään, muistaa millä sivuilla sama käyttäjä on käynyt. Esimerkiksi verkkokauppa, pelkällä HTTP-liikenteellä, ei osaisi säilyttää asiakkaan ostoskorin sisältöä hänen selatessaan tuotesivustoja (Järvinen 2010, 165). Evästeet ovat tekniikka, jolla tämä yhteys, *state*, voidaan luoda. (Tirtea et al. 2011.)

Eväste (*cookie*) on HTTP-palvelimen käyttäjän selaimelle luoma tiedosto, jonka sisältämillä tiedoilla palvelin identifioi käyttäjän. Kun käyttäjä hakee www-sivun, selain lähettää yhteyspyynnön (*HTTP request*) sivuston palvelimelle, joka puolestaan lähettää vastauksen (*HTTP response*) mukana tekstinpätkiä, jotka toimivat evästeinä tämän palvelimen ja selaimen välillä. (Tirtea et al. 2011.) RFC6265-standardin (Barth 2011) mukaan palvelin lähettää evästeet Set-Cookie-nimisessä otsakkeessa, ja selain palauttaa ne Cookie-otsakkeessa, kun palvelimeen otetaan uudelleen yhteys (Kuvio 3).



Kuvio 3. HTTP-selainliikenne.

Evästeet voivat sisältää tietoja kuten istunnon id-tiedon, jolla palvelin tunnistaa jokaisen eri selaimen; kielipreferenssin; sivustokustomoinnit ja selainistunnon välimuistiin tallennetun datan. Yksi eväste voi sisältää tietoa 4,096 kilotavun verran. (Tirtea et al. 2011.) Palvelimet päättävät itse miten ja millaisia evästeitä ne asettavat, mutta evästeiden täytyy olla syntakseiltaan standardien mukaisia (Barth, 2011).



Kuvio 4. www.hs.fi –sivuston asettamia evästeitä Google Chrome –selaimessa.

Eväste muodostuu nimi=arvo-parista ja sen attribuuteista, eli ominaisuuksista. Seuraavassa taulukossa on esitelty kuvion 4 evästeen ”HSSESSIONID=2DABC6BFDC41A715522E3D13C350282A” attribuutit. RFC6265-standardin (Barth 2011) mukaiset attribuutit määrittelevät evästeen toimintaa.

Taulukko 1. Evästeen attribuutit.

ATTRIBUUTTI	ARVO	SELITYS
Domain	www.hs.fi	Eväste lähetetään vain www.hs.fi -verkkotunnukselle (ei esim. www.tyopaikat.hs.fi -aliverkkotunnukselle. Kuvion 4 hs.fi-evästeet lähetetään myös www.tyopaikat.hs.fi -aliverkkotunnukselle).
Path	/	URL-osoite, jolle eväste lähetetään (Rantala 2005, 222). "/" lähettää evästeen kaikille URL-osoitteille www.hs.fi -verkkotunnuksen alla. Vertailuna: attribuutin arvo "/nyt" lähettäisi evästeen vain www.hs.fi/nyt -URL-osoitteeseen sekä sen aliosoitteisiin, esim. www.hs.fi/nyt/artikkeli1.html. Evästettä ei lähetettäisi, kun haetaan www.hs.fi- tai www.hs.fi/uutiset -sivu.
Send for	Any kind of connection	Määrittelee, lähetetäänkö eväste vain silloin, kun käytössä on "turvallinen" (*secure*) yhteys. Käyttäjän selain määrittelee itse, mikä on turvallinen yhteys. "Any kind of connection" -arvo lähettää evästeen kaikilla yhteysmuodoilla.
Accessible to script	No (HttpOnly)	Määrittelee, saako evästeen lähettää muille yhteysmuodoille kuin HTTP-liikenteelle. HttpOnly-arvo lähettää evästeen vain HTTP-liikenteelle.
Created	Tuesday, March 22, 2016 at 2:13:08 PM	Milloin eväste on tallennettu selaimelle.
Expires	When the browser session ends	Milloin eväste poistetaan automaattisesti. Kuvion 4 eväste poistuu, kun selainistunto suljetaan.

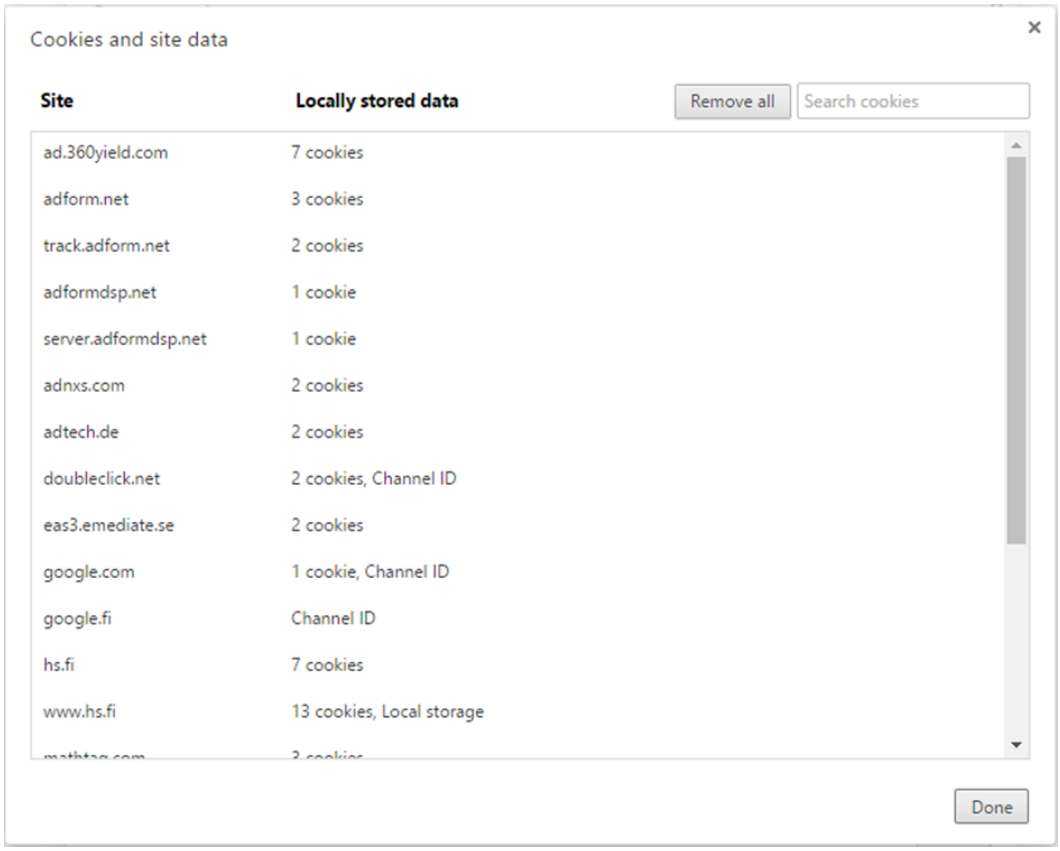
Kun www.hs.fi -palvelin lähettää käyttäjän selaimelle kuvion 4 mallisen evästeen, Set-Cookie-otsakkeen syntaksi on seuraavanlainen:

Set-Cookie: HSSESSIONID=2DABC6BFDC41A715522E3D13C350282A; Domain=www.hs.fi; Path=/; HttpOnly

3.1.1 Evästeiden käyttö mainonnassa

Evästeitä on sekä ensimmäisen että kolmannen osapuolen luomia. Ensimmäisen osapuolen evästeet ovat sen sivuston, jolla käyttäjä on vieraillut, itse tekemiä (kuviossa 5 hs.fi-sivuston evästeet). Kolmannen osapuolen evästeet ovat muun kuin itse pääasiallisen sivuston tekemiä evästeitä (kuvion 5 muut kuin hs.fi-sivuston evästeet), mutta jotka kuitenkin ladataan www-sivun mukana. (Tirtea et al. 2011.) Toinen osapuoli on käyttäjä ja hänen laitteensa (Castelluccia & Narayanan 2012).

Ensimmäisen osapuolen evästeet ovat usein tarpeellisia sivuston toiminnan varmistamiseksi. Kolmannen osapuolen evästeet tulevat sivuille muualta kuin itse sivuston palvelimelta, mutta ne sisällytetään selaimen HTTP-yhteyspyynnön vastaukseen samalla lailla kuten itse sivuston sisältö. Kolmannen osapuolen evästeet ovat usein mainosyhtiöiden tekemiä, mutta niitä voidaan käyttää myös sivuston käytön analysoimiseen ja muuhun kolmansien osapuolten tarjoamaan sisältöön. (Tirtea et al. 2011.)

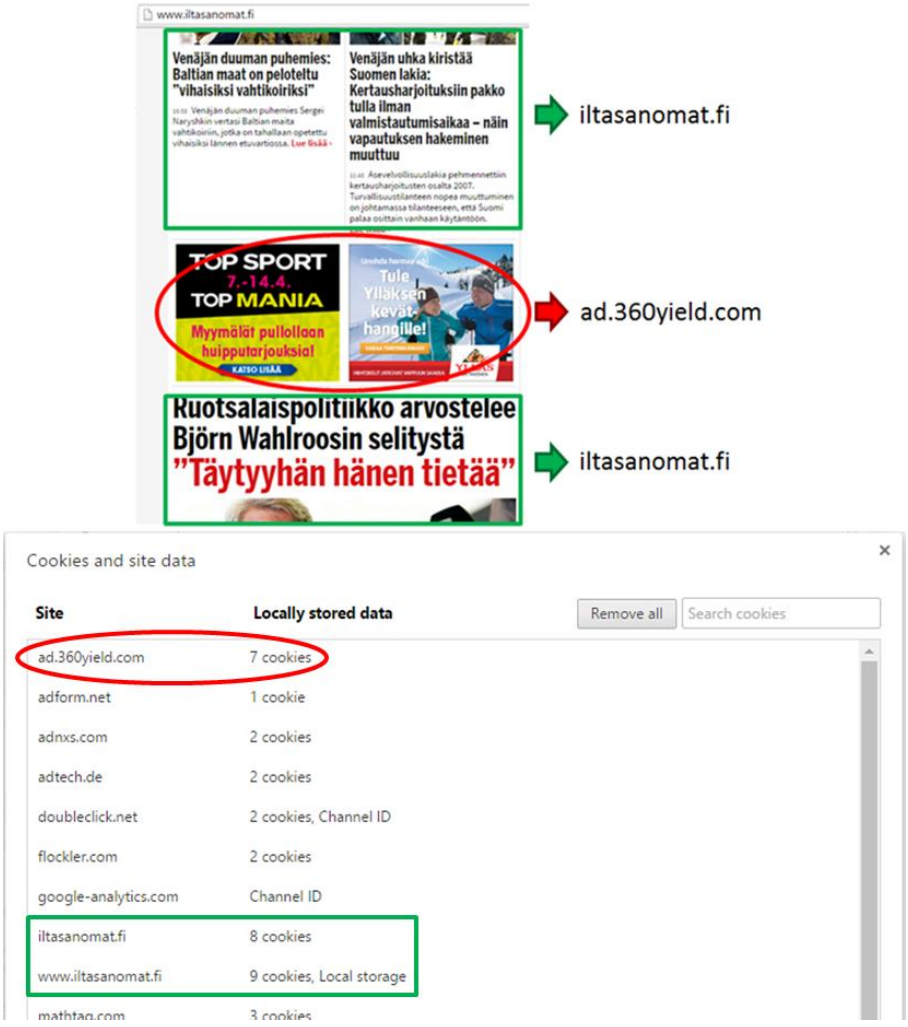


Kuvio 5. Ensimmäisen ja kolmannen osapuolen evästeitä Google Chrome -selaimessa.

Kuviossa 5 on vierailtu www.hs.fi –sivustolla. Hs.fi-evästeet tulevat hs.fi-sivuston palvelimelta, eli tässä tapauksessa palvelimelta, jonka sivuston käyttäjä on selaimen osoitepalkkiin kirjoittanut; kyseessä on ensimmäisen osapuolen palvelin. Doubleclick.net-evästeet taas tulevat doubleclick.net-palvelimelta, joka ei ole sivuston omistama, mutta jonka sisältöä sivusto silti lataa ja tarjoaa käyttäjälle. Tällainen palvelin on kolmannen osapuolen palvelin.

Sivustojen palvelujen tarjoamisen lisäksi evästeet ovat yksi pääkeinoista käyttäjien seurantaan. Selain lähettää evästeen takaisin vain sen luoneelle sivustolle: täten sivustot eivät näe toisten verkkotunnusten asettamia evästeitä, eikä evästeen luoja voi sitä kautta tietää, missä käyttäjä on surffannut. Yksittäinen kolmas osapuoli voi kuitenkin seurata käyttäjää niillä sivustoilla, jotka lataavat tältä osapuolelta sisältöä. (Tirtea et al. 2011.)

Kun käyttäjä vierailee sivustolla ja lataa mainoksen, mainoksen omistava palvelin lähettää selaimelle yhden tai useampia evästeitä. Esimerkkinä kuvio 6. Kuvakaappauksessa on vierailtu www.iltasanomat.fi-sivustolla. Vierailun aikana on ladattu ad.360yield.com-nimiseltä mainosyhtiöltä mainoksia. Ad.360yield.com voi selaimen HTTP request –yhteyspyynnön aikana tallentaa käyttäjälle evästeitä. Mikäli evästeissä on annettu yksilöivä id-tunnus, voi mainosyhtiö luoda käyttäjästä lokin ja lisätä siihen tietoa aina, kun käyttäjä vierailee sivulla, joka lataa mainosyhtiöltä sisältöä, ja täten luoda käyttäjän surffailutavoista profiilia (Roesner, Kohno & Wetherall 2012).

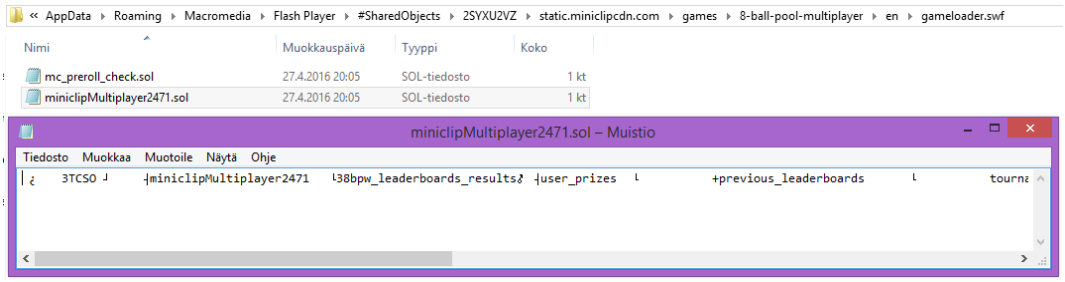


Kuvio 6. Ensimmäisen ja kolmannen osapuolen sisältö ja evästeet eriteltynä Google Chrome -selaimessa.

3.1.2 Flash-evästeet, Local Shared Object

Koska HTTP-evästeiden torjunta ja poistaminen on helppoa (kappale 4.1), käyttäjien tarkasta seurannasta riippuvaiset osapuolet tarvitsevat tehokkaampia keinoja tavoitteidensa saavuttamiseksi.

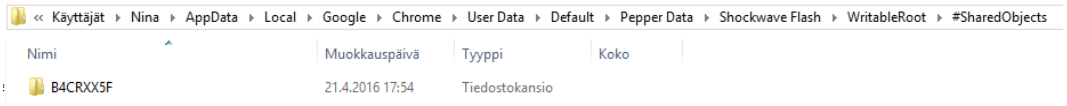
Local Shared Object, yleiseltä nimitykseltään ”Flash-evästeet”, ovat Adobe Flash -selainohjelman käyttämiä tiedostoja, jotka tallennetaan paikallisesti käyttäjän laitteelle HTTP-evästeiden tapaan (kuvio 7). Tiedostojen avulla Flash-ohjelma voi tallentaa sen käyttämän sisällön tilan, kuten Flash-pohjaisen videon äänenvoimakkuuden. (Soltani, Canty, Mayo, Thomas & Hoofnagle 2009; Ayenson, Wambach, Soltani, Good & Hoofnagle 2011.)



Kuvio 7. MiniclipMultiplayer2471.sol-niminen Flash-eväste www.miniclip.com-sivustolta saatuna.

Flash-evästeillä on monia ominaisuuksia, jotka voivat hyödyttää kolmannen osapuolen seurantatarkoituksia. Toisin kuin HTTP-evästeet, selain ei kontrolloi Flash-evästeitä: ne tallennetaan lisäosan omaan kansioon käyttäjän laitteella, kaikki laitteen selaimet voivat käyttää evästeitä vaikka ne olisivat toisen selaimen tallentamia, ja kun selaimesta poistetaan eväste-, välimuisti- ja selaustiedot, Flash-tiedot eivät poistu. (Soltani et al. 2009; Ayenson et al. 2011.)

Poikkeuksen Flash-evästeiden toimintaan tekee Google Chrome -selain, joka käsittelee Flash-lisäosaa integroidusti (kappale 4.2) (Siegler 2011). Chrome ei käytä globaaleja Flash-evästeitä, vaan se tallentaa evästeensä omaan kansioon (kuvio 8).



Kuvio 8. Google Chromen oma Flash-evästekansio.

Flashin globaaliuden lisäksi sen evästeet ovat mittavasti suurempia kuin HTTP-evästeet: 100 kilotavua verrattuna 4 kilotavuun. Flash-evästeillä ei ole myöskään automaattista poistopäivämäärää, vaan ne säilyvät, kunnes ne manuaalisesti poistetaan. (Soltani et al. 2009; Ayenson et al. 2011.)

Riskin käyttäjän yksityisyydelle muodostaa Flash-evästeiden mahdollisuuden käyttää niitä poistettujen HTTP-evästeiden uudelleenluonnissa. Mikäli sama sivusto luo sekä HTTP-evästeen että Flash-evästeen, ja käyttäjä poistaa HTTP-evästeet, voi Flash-eväste luoda uudelleen tämän HTTP-evästeen jos niillä on samat id-tiedot. (Soltani et al. 2009; Ayenson et al. 2011.)

4 KEINOT SEURANNAN ESTÄMISEEN

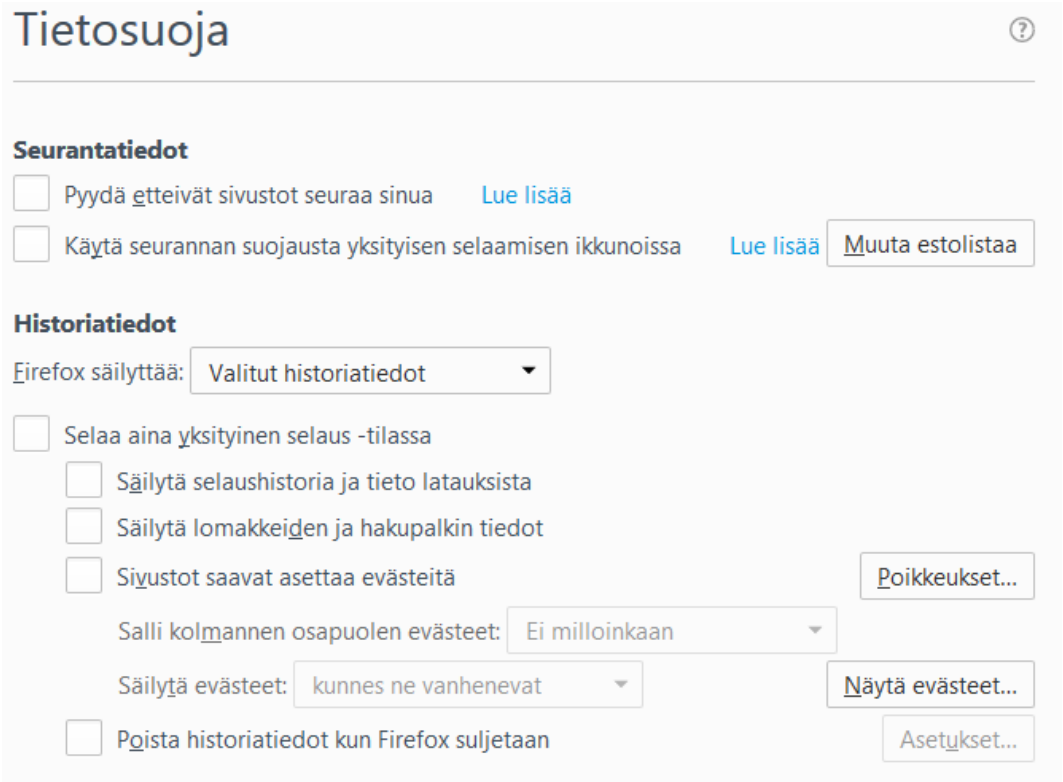
Mainostajien käyttäjäseurantaa voi estää käyttäjän toimesta muun muassa käytettävän selaimen asetuksilla, evästeiden hallinnalla, selainlaajennuksilla ja VPN-ohjelmilla.

4.1 Evästeiden torjuminen

HTTP-evästeitä voidaan torjua selainasetuksilla. Tässä kappaleessa on esitelty Mozilla Firefox- ja Google Chrome -selainten yksityisyysasetukset.

4.1.1 Selainasetukset; Mozilla Firefox

Kuviossa 9 on Firefox-selaimen yksityisyys- ja evästeasetukset. Taulukon 2 mukaiset asetukset vaikuttavat evästeiden säilyttämiseen selaimessa.



Kuvio 9. Mozilla Firefoxin yksityisyys- ja evästeasetukset.

Taulukko 2. Mozilla Firefoxin seurantatietoasetusten selitys.

ASETUS	SELITYS
Pyydä etteivät sivustot seuraa sinua	Selain lähettää HTTP-pyyntöjen aikana Do Not Track -nimisen otsakkeen (kappale 4.1.4).
Käytä seurannan suojausta yksityisen selaamisen ikkunoissa	Kun yksityinen selaus -tila on päällä (kappale 4.1.3), Firefox estää seurannan disconnect.me-palvelun tunnistamilta tahoilta (Mozilla).

Firefoxissa voi valita joko valmiiksi tehdyt historiatietoasetukset tai kustomoida omat asetukset ”Firefox säilyttää:” -pudotusvalikon kautta. Taulukossa 3 on selitetty pudotusvalikon asetukset.

Taulukko 3. Mozilla Firefoxin historiatietoasetusten selitys.

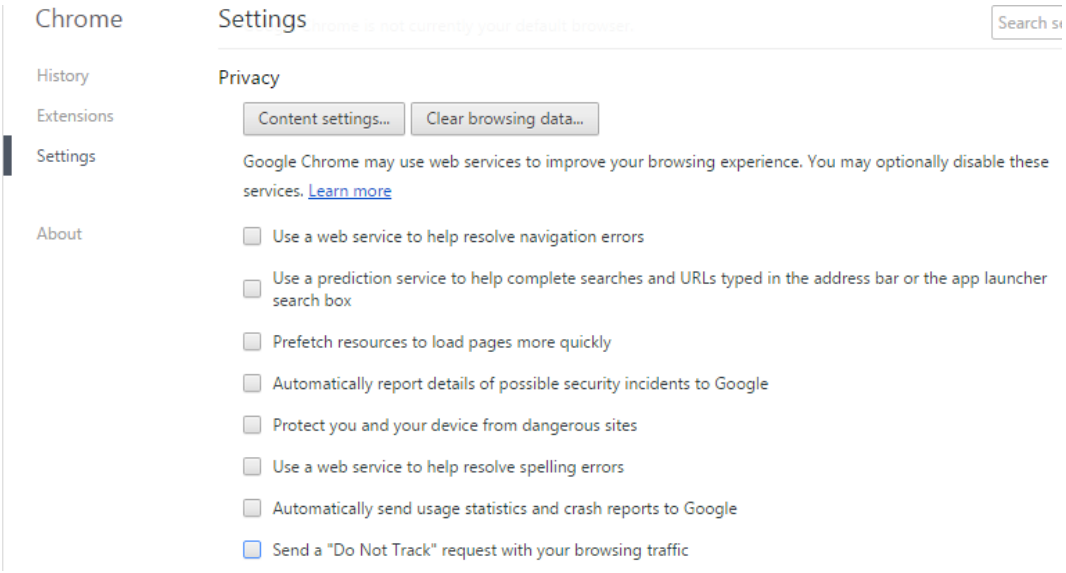
ASETUS	SELITYS
Täydelliset historiatiedot	Kaikki selaushistoria ja evästeet säilytetään viimeisiin päivämääriinsä asti, ellei käyttäjä manuaalisesti poista tietoja.
Ei mitään historiatietoja	Selaushistoriaa ei tallenneta. Evästeet poistetaan, kun kaikki selausikkunat suljetaan.
Valitut historiatiedot	Käyttäjä saa kustomoida historiatietoasetukset haluamikseen. Evästeiden kannalta merkittävä on ”Sivustot saavat asettaa evästeitä” -valinta.
Sivustot saavat asettaa evästeitä	Mikäli asetus ei ole valittuna, mitkään sivustot eivät saa asettaa evästeitä. Tämä voi estää kirjautumisen sivustoille, jotka käyttävät evästeitä istuntojen autentikointiin.
Salli kolmannen osapuolen evästeet	”Aina” antaa kaikkien kolmansien osapuolten asettaa selaimelle evästeitä. ”Vierailluilta sivustoilta” hyväksyy evästeet sivustoilta, joilla on aiemmin vierailtu. ”Ei milloinkaan” ei hyväksy kolmansien osapuolten evästeitä.

Säilytä evästeet:	”Kunnes ne vanhenevat” poistaa evästeet niihin merkityn päivämäärän mukaan. ”Kunnes Firefox suljetaan” poistaa evästeet kun selainistunto suljetaan.

”Poikkeukset”-painikkeella pääsee muokkaamaan, mitkä yksittäiset sivustot saavat tai eivät saa asettaa evästeitä. ”Näytä evästeet”-painikkeella voi tarkastella ja poistaa yksittäisiä evästeitä.

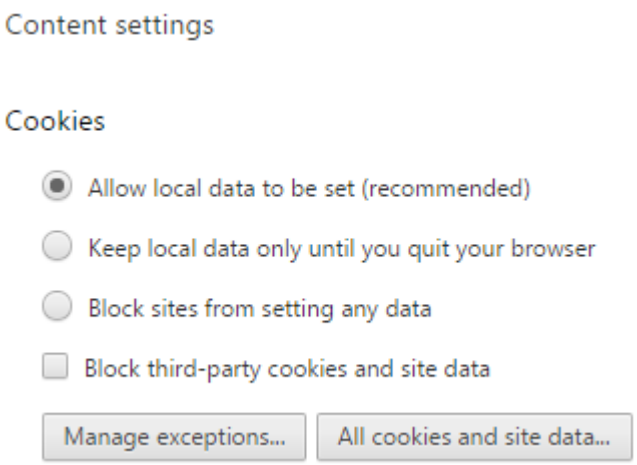
4.1.2 Selainasetukset; Google Chrome

Kuviossa 10 ovat Google Chrome -selaimen yksityisyysasetukset. ”Send a ”Do Not Track” request with your browsing traffic” -asetus lähettää samanlaisen seurannanestopyynnön kuin Firefoxissa.



Kuvio 10. Google Chromen yksityisyysasetukset.

”Content settings…” -nappulaa klikkaamalla pääsee Chromen evästeasetuksiin (kuvio 11).



Kuvio 11. Google Chromen evästeasetukset.

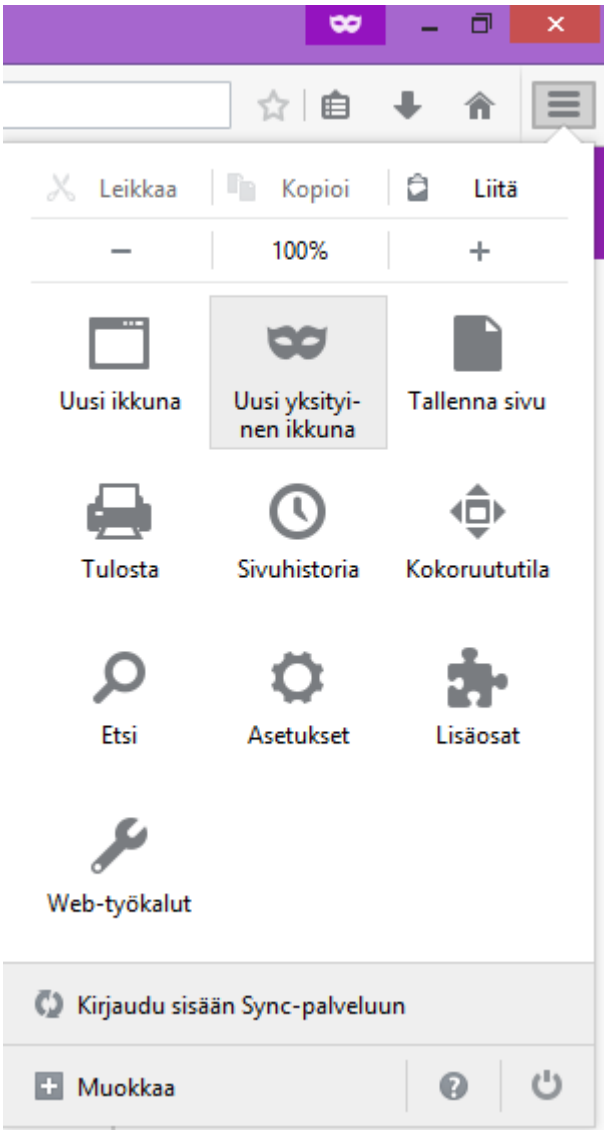
Taulukko 4. Google Chromen evästeasetusten selitys.

ASETUS	SELITYS
Allow local data to be set (recommended)	Sallii ensimmäisen ja kolmannen osapuolen datan tallentamisen.
Keep local data only until you quit your browser	Sallii datan tallentamisen, mutta tiedot poistetaan kun selain suljetaan.
Block sites from setting any data	Kaikki datan tallentaminen estetään, sekä kolmansilta että ensimmäiseltä osapuolelta.
Block third-party cookies and site data	Erillinen asetus, jolla voidaan määrittää saavatko kolmannet osapuolet tallentaa dataa.

4.1.3 Yksityinen selaus

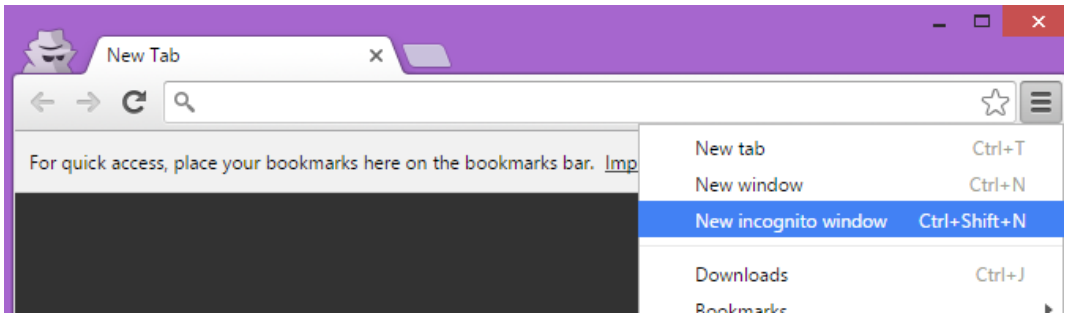
Selaimissa on erityinen “Yksityinen selaus”-tila, joka ei tallenna mitään tietoja, kuten evästeitä, selainistunnosta käyttäjän laitteelle. Mozilla Firefoxissa tila on nimeltään Yksityinen selaus, Google Chromessa Incognito.

Firefoxilla tila otetaan käyttöön painamalla oikean ylänurkan valikkopainiketta ja valitsemalla ”Uusi yksityinen ikkuna” (kuvio 12).



Kuvio 12. Mozilla Firefoxin Yksityinen selaus -tilan käyttöönotto.

Google Chromessa painetaan myös oikean ylänurkan valikkopainiketta ja valitaan ”New incognito window” (kuvio 13).



Kuvio 13. Google Chromen Incognito-tilan käyttöönotto.

4.1.4 Do Not Track

Do Not Track on yhdistelmä teknologiaa ja toimintalinjauksia. Do Not Track -otsake on teknisesti yksinkertainen ”DNT:1”-tieto, joka kertoo otsakkeen vastaanottajille, ettei käyttäjä halua toimiaan internetissä seurattavan. Poliittiset linjaukset määrittävät, miten vastaanottavat tahot reagoivat tietoon. (EFF a.)

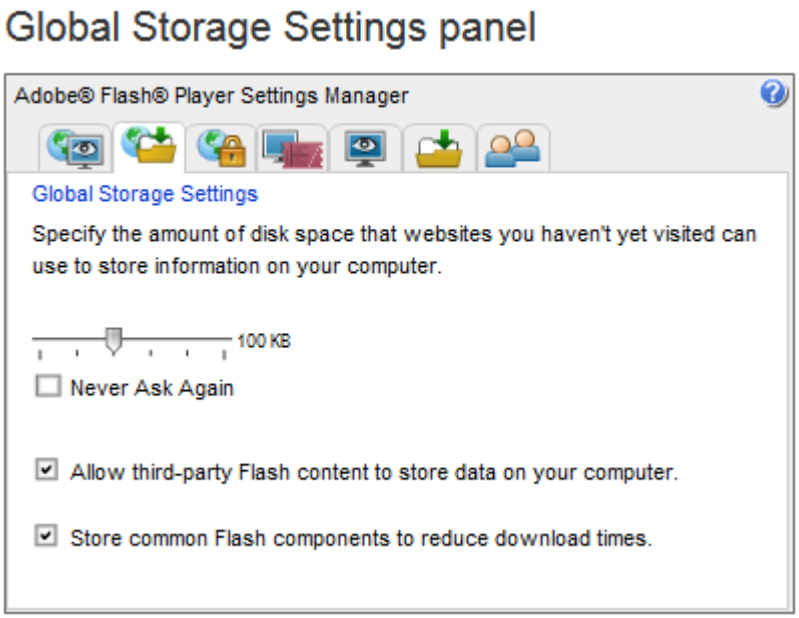
Selainten Do Not Track -asetuksen toimivuudesta ei kuitenkaan ole takeita, sillä otsakkeen pyynnön noudattaminen on palveluntarjoajille vapaaehtoista, ja sivustot saattavat silti tehdä seurantaa otsakkeesta huolimatta (Newman 2015). Ne jotka pyyntöä noudattavat, saattavat esimerkiksi lopettaa mainosten räätälöinnin käyttäjän selaustapojen mukaan (Singer 2013).

4.2 Flash-evästeiden hallinta

Flash-evästeitä voi hallita Adoben sivuilta löytyvän hallintapaneelin kautta osoitteessa

> https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html

Global Storage Settings -välilehdeltä löytyvät yleiset Flash-asetukset (kuvio 14). Asetuksilla voi määritellä globaalit asetukset Flash-sisällölle (talukko 5).

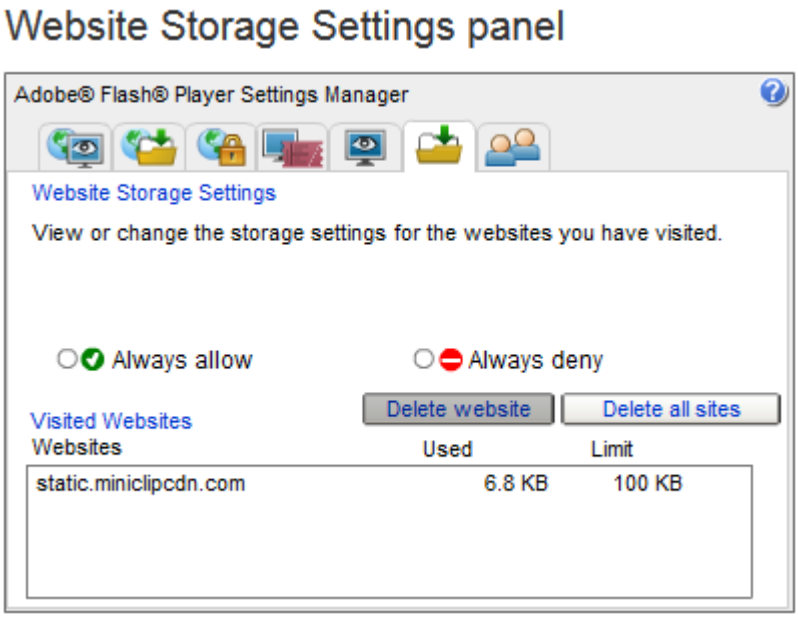


Kuvio 14. Adobe Flash Global Storage Settings -paneeli.

Taulukko 5. Adobe Flash Global Storage -asetusten selitys.

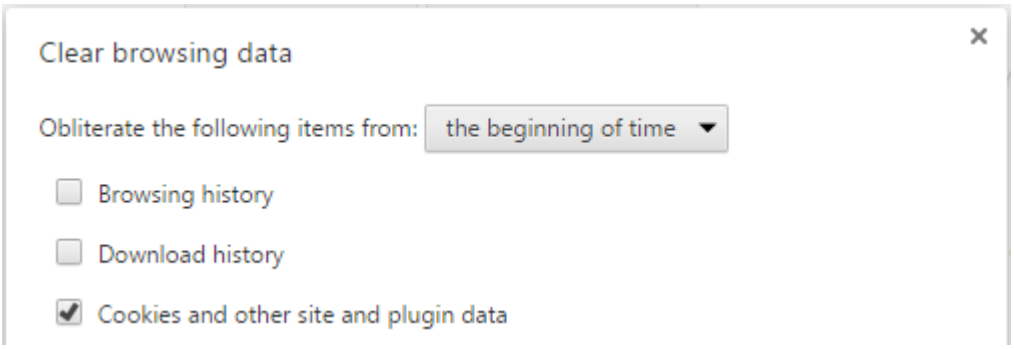
ASETUS	SELITYS
Tallennustilan laajuus -liukusäädin	Säätimellä määritellään, kuinka paljon sivustot voivat tallentaa data käyttäjän laitteelle. 100 kilotavua on oletuskoko. ”None”-asetuksella Flash-ohjelmat pyytävät lupaa lisädatan tallentamiseen. ”Unlimited” antaa ohjelmien tallentaa rajattomasti dataa.
Never Ask Again	Flash-ohjelmien ei anneta tallentaa dataa.
Allow third-party Flash content to store data on your computer.	Sallitaanko kolmansien osapuolien Flash-datan tallentaminen.
Store common Flash objects to reduce download times.	Tallennetaanko yleisesti käytetyt Flash-komponentit latausaikojen lyhentämiseksi.

Website Storage Settings -välilehdellä voi hallinnoida yksittäisten sivustojen Flash-evästeitä (kuvio 15). Asetuksilla voi valita, antaako valitun sivuston tallentaa dataa vai aina estää siltä datan tallentaminen. Sivustoja voi myös poistaa vierailtujen sivustojen listasta, joten seuraavan kerran, kun niiltä ladataan Flash-sisältöä, ne käyttävät globaaleja asetuksia.



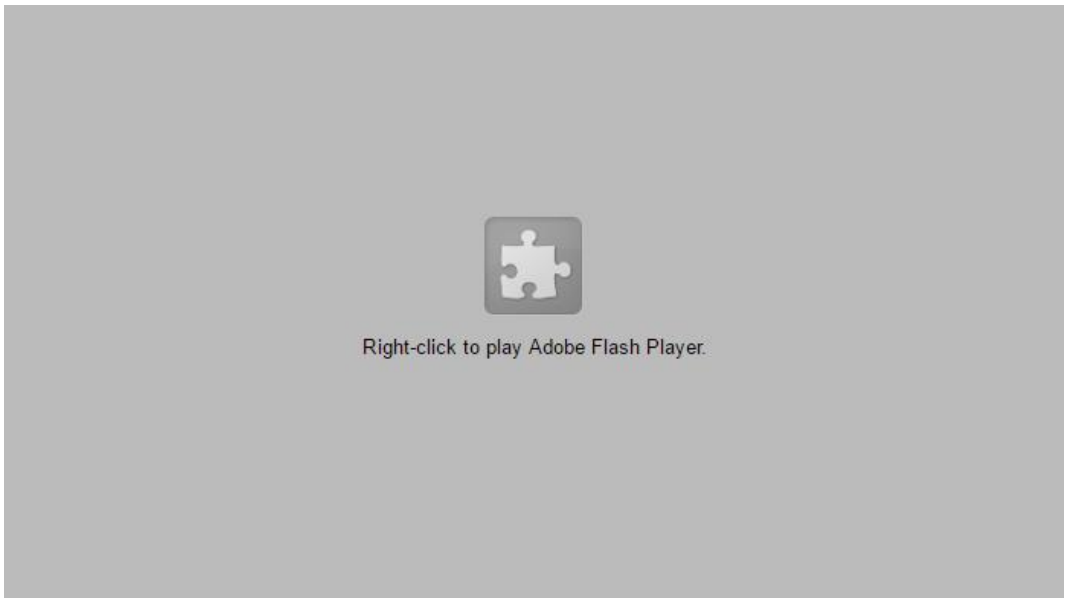
Kuvio 15. Adobe Flash Website Storage Settings -paneeli.

Google Chrome -selaimella Flash-evästeiden poisto on helppoa. Chrome käsittelee Flash-lisäosaa integroidusti, joten se tallentaa omat Flash-evästeensä omaan kansioonsa (kappale 3.1.2). Chromen Flash-evästeet poistetaan selaushistorian poistosta valitsemalla ”Cookies and other site and plugin data” (”Evästeet ja muut sivuston ja laajennuksien tiedot”) kuvion 16 mukaisesti.



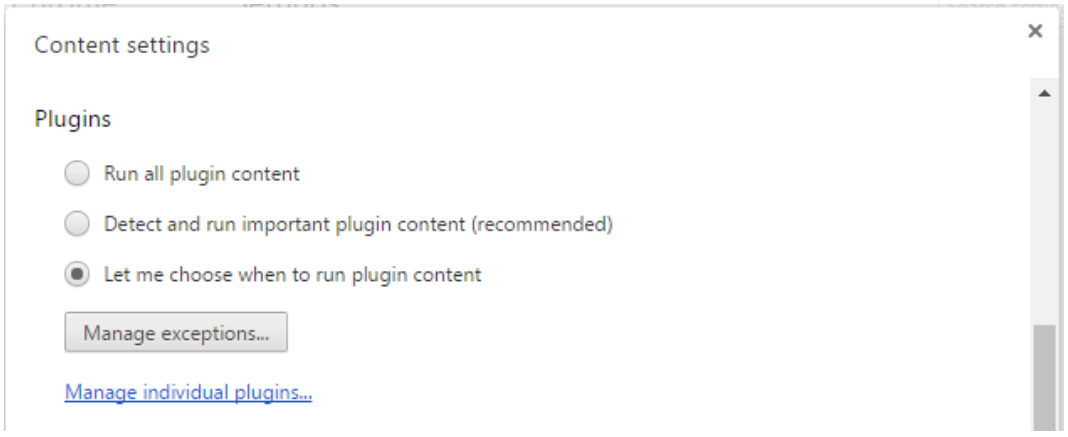
Kuvio 16. Google Chromen Flash-evästeiden poisto.

Käyttäjä voi hallita, mitä Flash-sisältöä ladataan myös asettamalla Flash-ohjelman ”click-to-play”-tilaan. Sen sijaan, että sivustot lataavat automaattisesti kaiken Flash-sisällön, käyttäjä valitsee itse mitä suoritetaan klikkaamalla sisällön paikkaa (kuvio 17). Flash-ohjelma on mahdollista myös ottaa kokonaan pois päältä.

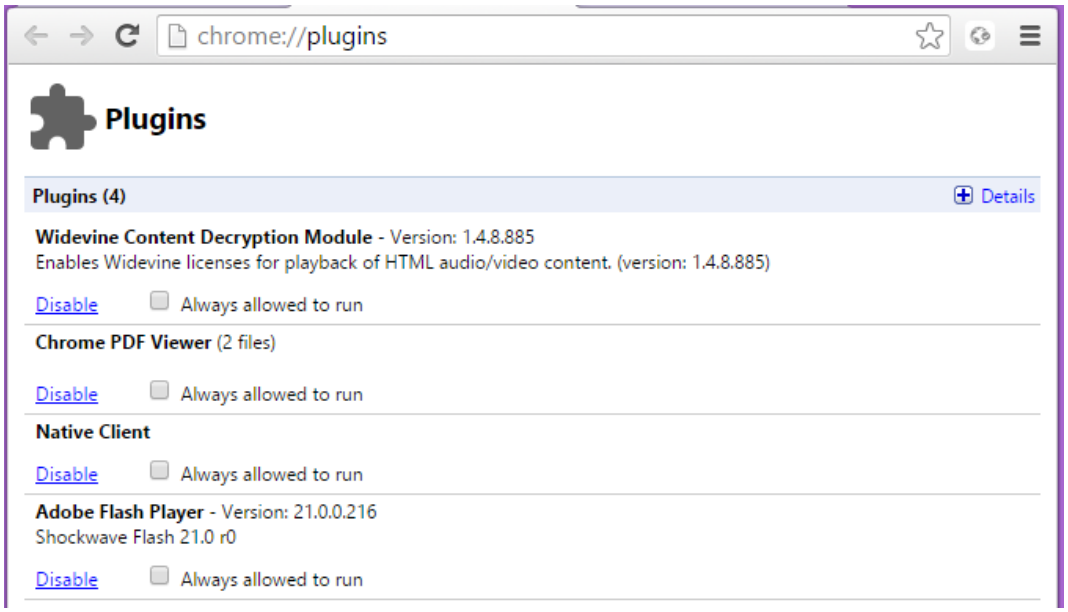


Kuvio 17. Google Chromessa Flash-sisällön korvaava click-to-play-paikka.

Google Chrome -selaimella click-to-play-tila otetaan käyttöön selaimen asetuksista kirjoittamalla osoitepalkkiin chrome://settings. Klikkaa ”Show advanced settings…” ja Privacy-kohdasta ”Content settings…”. Aukeavasta “Content settings” ikkunasta valitaan kohdasta Plugins “Let me choose when to run plugin content” (kuvio 18). Flashin poistamiseksi käytöstä valitaan “Manage individual plugins…” ja Adobe Flash Playerin kohdalla klikataan Disable (kuvio 19).

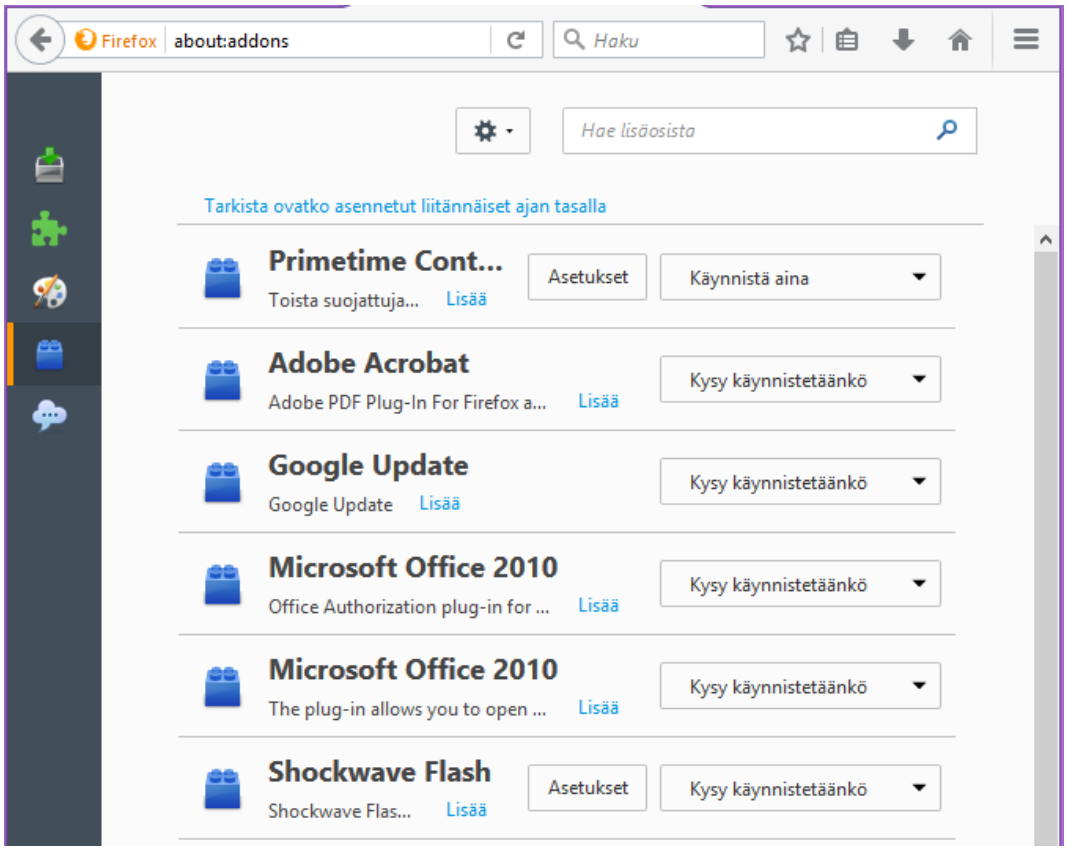


Kuvio 18. Google Chromen Content Settings -ikkuna.



Kuvio 19. Google Chromen yksittäisten laajennusten hallinta.

Mozilla Firefox -selaimella click-to-play-tila asetetaan Lisäosien hallinnasta kirjoittamalla osoitepalkkiin about:addons, ja valitsemalla Shockwave Flashin pudotusvalikosta ”Kysy käynnistetäänkö” (kuvio 20). Flashin estämiseksi valitaan ”Älä käynnistä koskaan”.



Kuvio 20. Mozilla Firefoxin lisäosien hallinta.

Mozilla Firefox -selaimelle on myös saatavilla lisäosa, joka poistaa Flash-evästeet automaattisesti, kun selainistunto suljetaan (kappale 4.4.3).

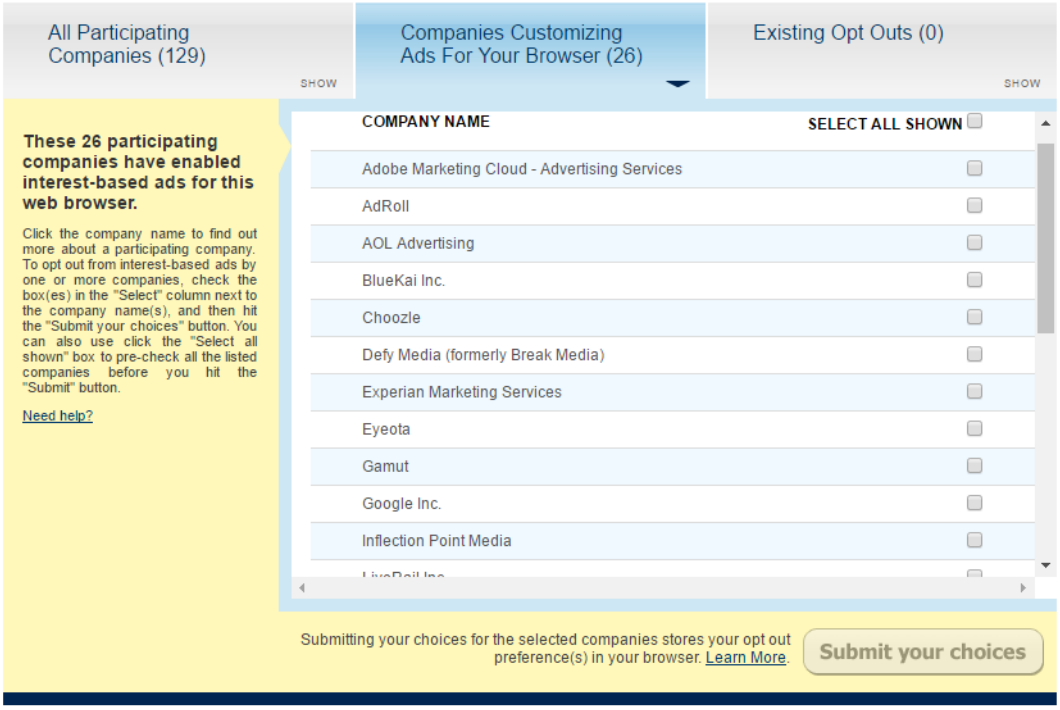
4.3 OBA Opt-Out

Kohdennetusta mainonnasta (kappale 2) on mahdollista kieltäytyä. Jotkin mainostajat tarjoavat erityisen OBA Opt-Out -mahdollisuuden, jolloin käyttäjä ei saa kohdennettua mainontaa tältä mainostajalta.

Digital Advertising Alliance, DAA, on suurten markkinointiyhtiöiden yhdistys, joka kehitti standardin Opt-Out-palvelua varten. Ohjelmaan liittyneet mainostajat näyttävät AdChoices-kuvakkeen mainoksen yhteydessä, jota klikkaamalla käyttäjä pääsee poistamaan mainostajan kohdennetun mainonnan käytöstä (kuvio 21). Opt-Out tapahtuu evästeillä, joissa on Opt-Out-tieto, ja jotka mainostaja tallentaa käyttäjän selaimelle. (Cranor 2012.)

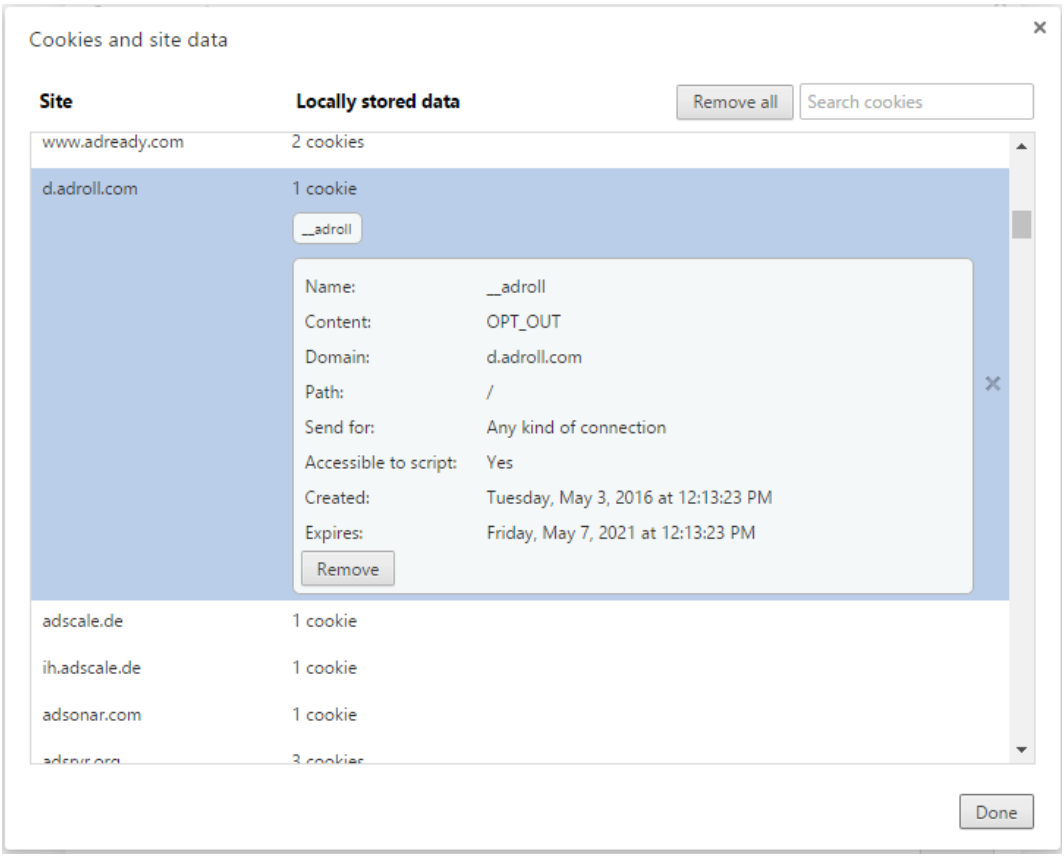
Kuvio 21. AdChoices-kuvake internetmainoksessa.

DAA:n sivuilta voi myös kerralla poistaa kohdennetun mainonnan käytöstä kaikilta liittyneiltä mainostajilta osoitteessa http://www.aboutads.info/choices. Sivun ohjelmalla voi nähdä, ketkä yhtiöt ovat mukana (All Participating Companies), keillä on tällä hetkellä kohdennettua mainontaa käytössä olevalle selaimelle (Companies Customizing Ads For Your Browser) ja keiden mainonnasta on kieltäydytty (Existing Opt Outs) (kuvio 22).



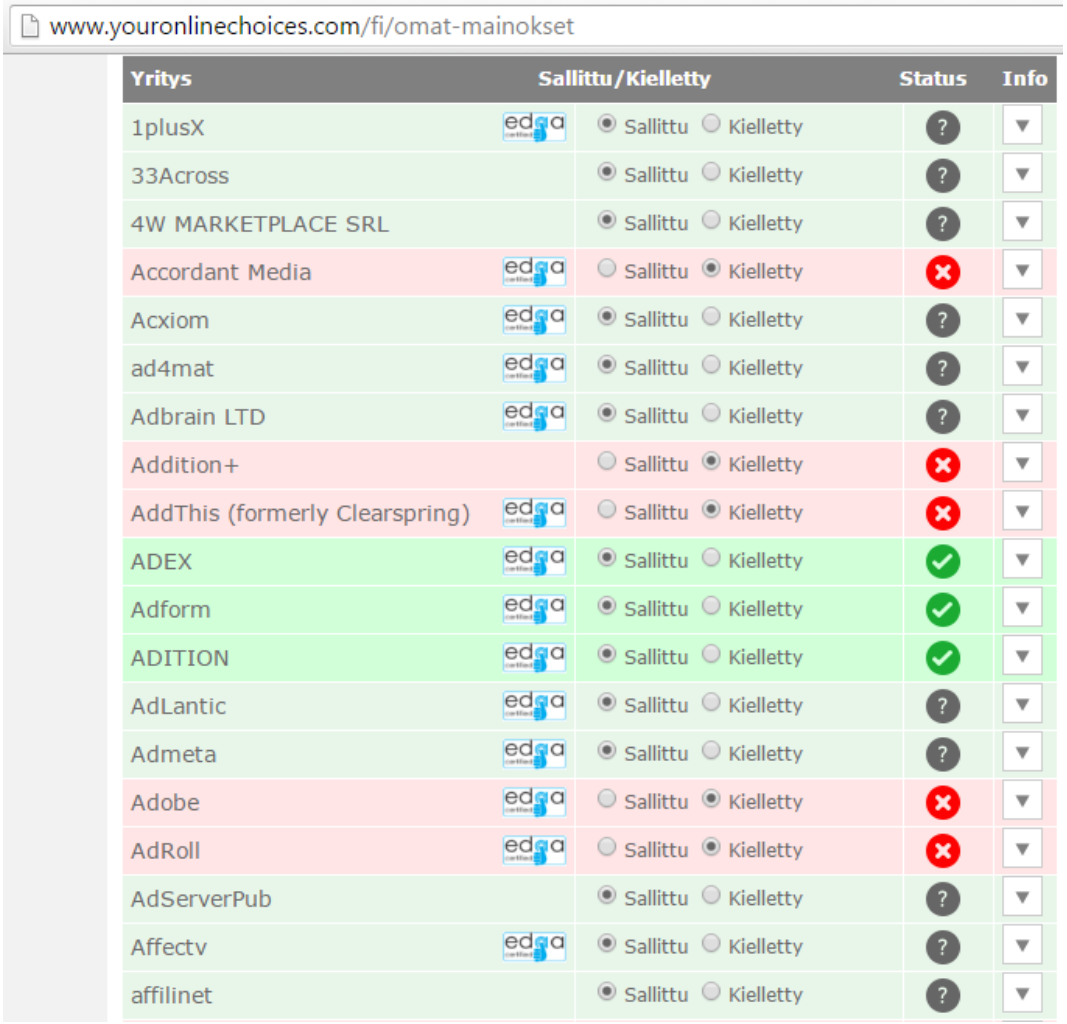
Kuvio 22. DAA:n OBA Opt-Out-paneeli.

Yhtiöiden nimiä klikkaamalla saa lisätietoa mainostajista. Kohdennetun mainonnan poistamiseksi klikataan valintaruutua nimen vieressä, tai ”SELECT ALL SHOWN” -valintaruutua, ja painamalla lopuksi ”Submit your choices”. Ohjelma tallentaa valittujen yhtiöiden Opt-Out-evästeet selaimelle (kuvio 23).



Kuvio 23. AdRoll-yhtiön Opt-Out-eväste Google Chomessa.

Opt-Out-palvelun ongelmana on sen hajanaisuus sekä pysymättömyys. Väyliä selainkäyttöön perustuvan mainonnan kieltämiseen on useita, eikä takeita ole, että kaikista löytyvät samat mainostajat. Esimerkiksi kun DAA:n palvelusta lataa palveluntarjoajien Opt-Out-evästeet, ja sen jälkeen vierailee eurooppalaisen EDAA:n palvelussa http://youronlinechoises.com, löytyy sieltä uusia mainostajia, joiden kohdennettua mainontaa ei ole kielletty (kuvion 24 sallitut mainostajat). Kohdennetun mainonnan käytöstä poistaminen edellyttää, että mainostaja on liittynyt Opt-Out-ohjelmaan, joten on mahdollista, että kaikki mainostajat eivät näissä ole mukana (Järvinen 2012, 194).



Kuvio 24. EDAA:n Opt-Out-paneeli.

Kohdennettu mainonta otetaan pois käytöstä lähettämällä käyttäjän selaimelle erityinen Opt-Out-HTTP-eväste. Mikäli käyttäjä säännöllisesti poistaa evästeet, poistuvat myös ladatut Opt-Out-evästeet, joten käyttäjän täytyy uudelleen hakea ne. (Tugend 2015.)

On myös mahdollista, että vaikka selain lähettää HTTP-pyynnön aikana mainostajalle takaisin Opt-Out-evästeen, mainostaja kerää edelleen käyttäjän selainkäyttötietoja, mutta ei näytä käyttäjälle kohdennettua mainontaa (Tugend 2015).

4.4 Selainlaajennukset

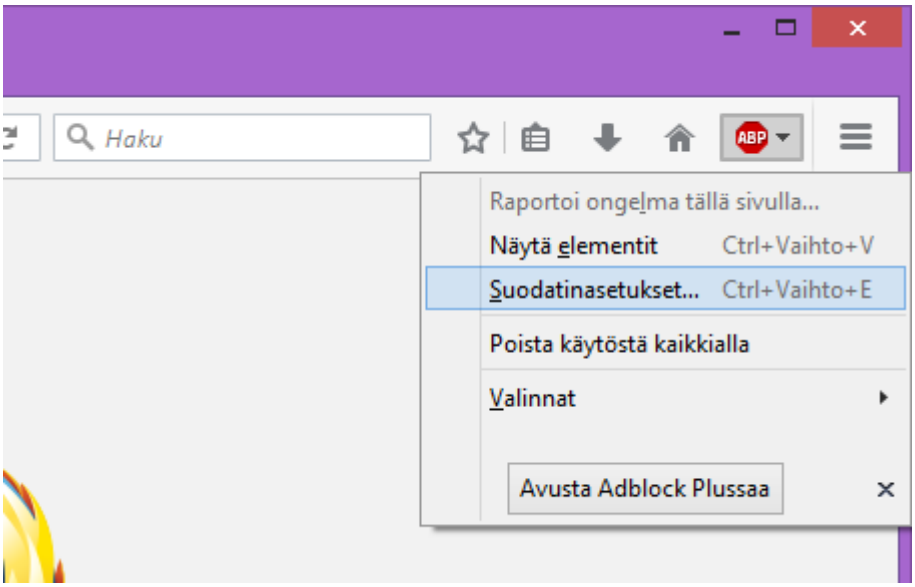
Selainlaajennukset antavat kustomoitavia vaihtoehtoja evästeiden hallintaan. Useimmat voi asettaa estämään joko kaiken niiden hallinnoiman sisällön, tai sallia vain käyttäjän haluaman sisällön.

4.4.1 Adblock Plus

Adblock Plus on yleisille alustoille saatavilla oleva lisäosa. Käyttämällä suodatuslistoja, se voi estää tiettyjen elementtien lataamisen internetsivustoilla. Suodatuslistoja on valmiiksi tehtyjä, ja käyttäjä voi myös itse määritellä mitä elementtejä estetään. Lisäosa ei siis itse estä sisältöä, vaan sille kerrotaan suodatusehtojen avulla, mitä estetään. (Adblock Plus.)

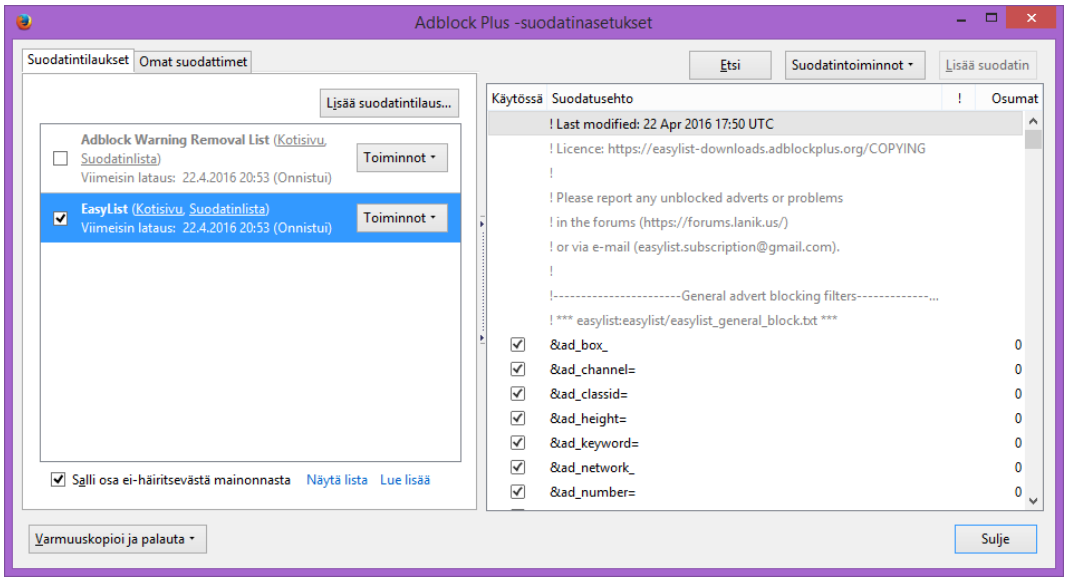
Adblock Plus -lisäosan voi ladata osoitteesta https://adblockplus.org/ ja painamalla Install for -painiketta sekä hyväksymällä asennuksen.

Lisäosan suodatinasetuksiin pääsee klikkaamalla ABP-ikonia selaimessa ja valitsemalla ”Suodatinasetukset…” (kuvio 25) tai painamalla näppäimiä Ctrl, vaihto ja E.



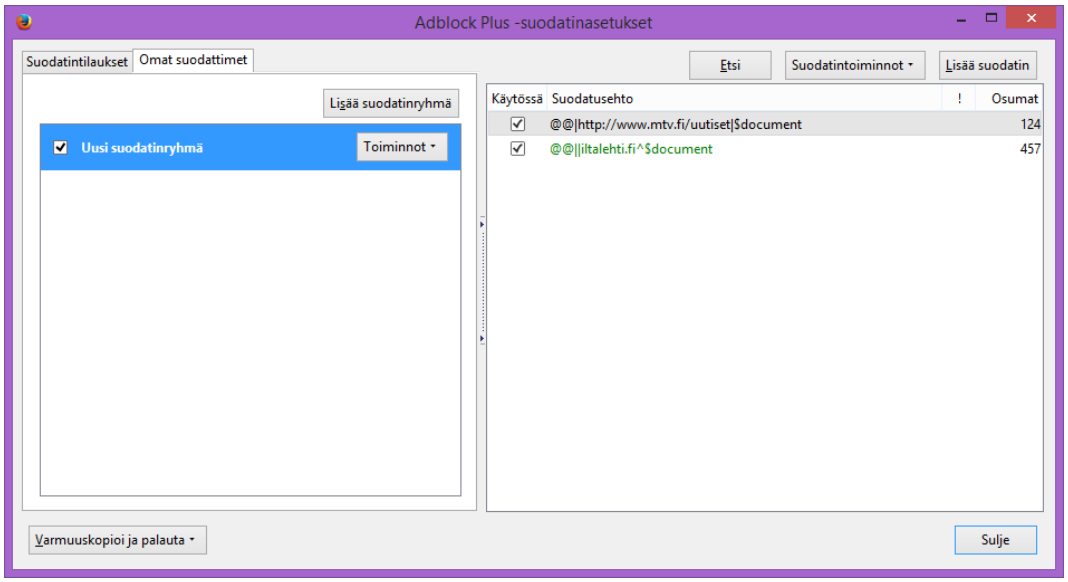
Kuvio 25. Reitti Adblock Plussan suodatinasetuksiin.

EasyList-suodatinlista on Adblock Plussassa oletusarvoisesti päällä (kuvio 26). Se estää suuren osan internetmainonnasta, ja on käytössä myös monessa muussa mainonnanesto-ohjelmassa (EasyList).



Kuvio 26. Adblock Plus -lisäosan oletussuodatinasetukset sekä EasyList-suodatinlistan sisältöä.

Omat suodattimet -välilehdessä (kuvio 27) voi itse muokata, mitä web-sisältöä lisäosa estää tai sallii. Ohjeet omien suodattimien tekoon löytyy osoitteesta https://adblockplus.org/en/filters. Kuviossa 27 on käytetty esimerkkinä suodattimia iltalehti.fi- ja www.mtv.fi/uutiset -sivuille. Iltalehti.fi-suodattimessa on käytetty lisäosan valintaa ”Ei käytössä osoitteessa iltalehti.fi” ja mtv.fi/uutiset-suodattimessa valintaa ”Ei käytössä tällä sivulla”. Lisäosa näyttää mainokset kaikkialla iltalehti.fi-sivustolla, ja www.mtv.fi/uutiset-sivulla.



Kuvio 27. Adblock Plus -lisäosan omat suodattimet -välilehti.

Mainosten eston lisäksi Adblock Plussaan on saatavilla myös muun muassa seurannan- ja haittaohjelmanestolistoja osoitteessa https://adblockplus.org/en/features.

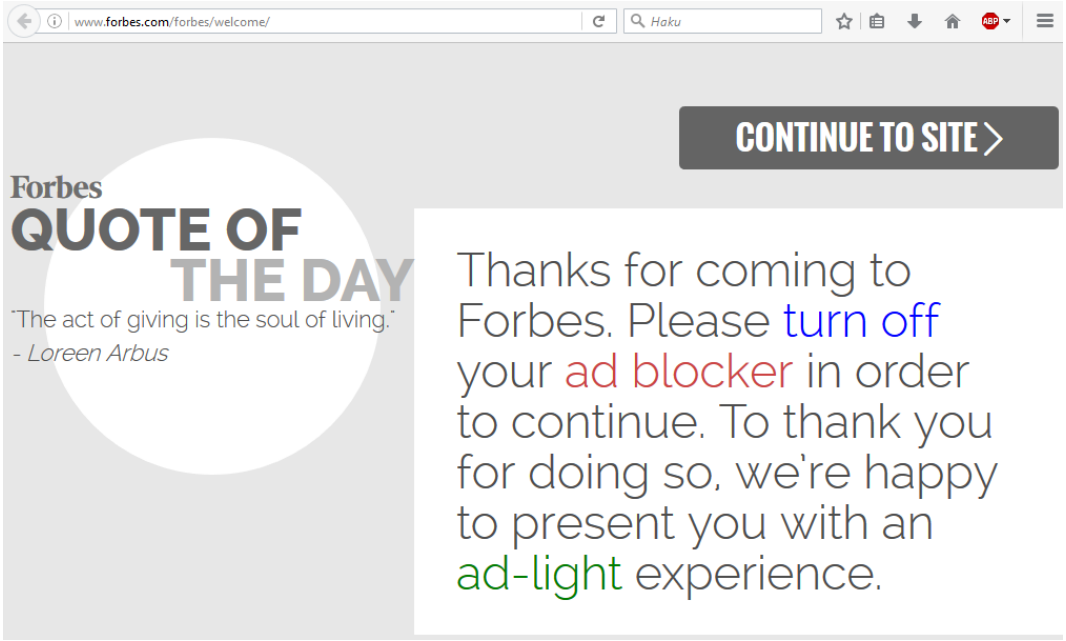
Adblock Plus oletusarvoisesti myös hyväksyy osan mainonnasta, joka on sen Acceptable Ads -ohjeiden mukaista ”ei-häiritsevää” mainontaa (Adblock Plus).

Kiistely mainoksenesto-ohjelmista

Mainoksenesto-ohjelmat ovat kiistanalaisia. Kriitikot arvostelevat ohjelmia siitä, kuinka ne ”varastavat” liiketuloja sivustojen ylläpitäjiltä ja edellyttävät ”suojelurahan” maksamista, jotta mainokset voi nähdä (Rothenberg 2016). Mainosten estäminen vähentää sivustojen mahdollisuuksia tarjota sisältöä, varsinkin mikäli mainostulot ovat sivuston ainoa keino ylläpitää toimintaa (Fisher 2010; Stiene 2015). Muun muassa www.forbes.com-sivusto vaatii käyttäjää ottamaan mainoksenesto-ohjelman pois käytöstä (kuvio 28).

Puolestapuhujat syyttävät mainosalaa itseään esto-ohjelmien suosiosta. Internetmainokset ovat ”päällekäyviä” ja yksityisyyden vastaisia (Kapko 2016). Mainosten infrastruktuurin (kappale 2) kautta voi myös tulla haittaohjelmia, kun pahantahtoiset mainostajat lisäävät mainoksensa mainosverkostoon (Karmina 2016).

Vuonna 2015 Google poisti 780 miljoonaa haitallista mainosta verkostoistaan (Ramaswamy 2016).



Kuvio 28. www.forbes.com-sivusto epää pääsyn käyttäjältä, jolla on Adblock Plus -lisäosa käytössä.

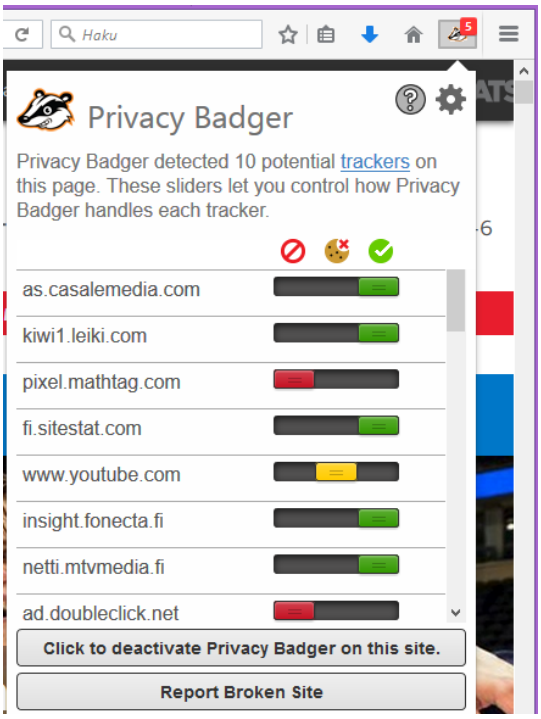
4.4.2 Privacy Badger

Privacy Badger on Electronic Frontier Foundationin, EFF, kehittämä selainlaajennus, joka on saatavilla Google Chromelle ja Mozilla Firefoxille. Se ei oletusarvoisesti estä mitään, mutta jos käyttäjän selatessa sivustoja se havaitsee kolmansia osapuolia, jotka yrittävät seurata käyttäjää eri sivustojen välillä käyttäjän Do Not Track -pyynnöstä huolimatta, se estää näitä osapuolia lataamasta sisältöä vastaisuudessa. (EFF b.)

Laajennuksen voi asentaa osoitteesta https://www.eff.org/privacybadger ja painamalla ”Install Privacy Badger” -painiketta sekä hyväksymällä asennuksen.

Privacy Badgerin estämät ja sallimat osapuolet kullakin sivustolla näkee painamalla laajennuksen kuvaketta selaimessa (kuvio 29). Vihreä liukusäätimen asetus on oletusasetus kaikille uusille laajennuksen havaitsemille osapuolille. Vihreä sal-

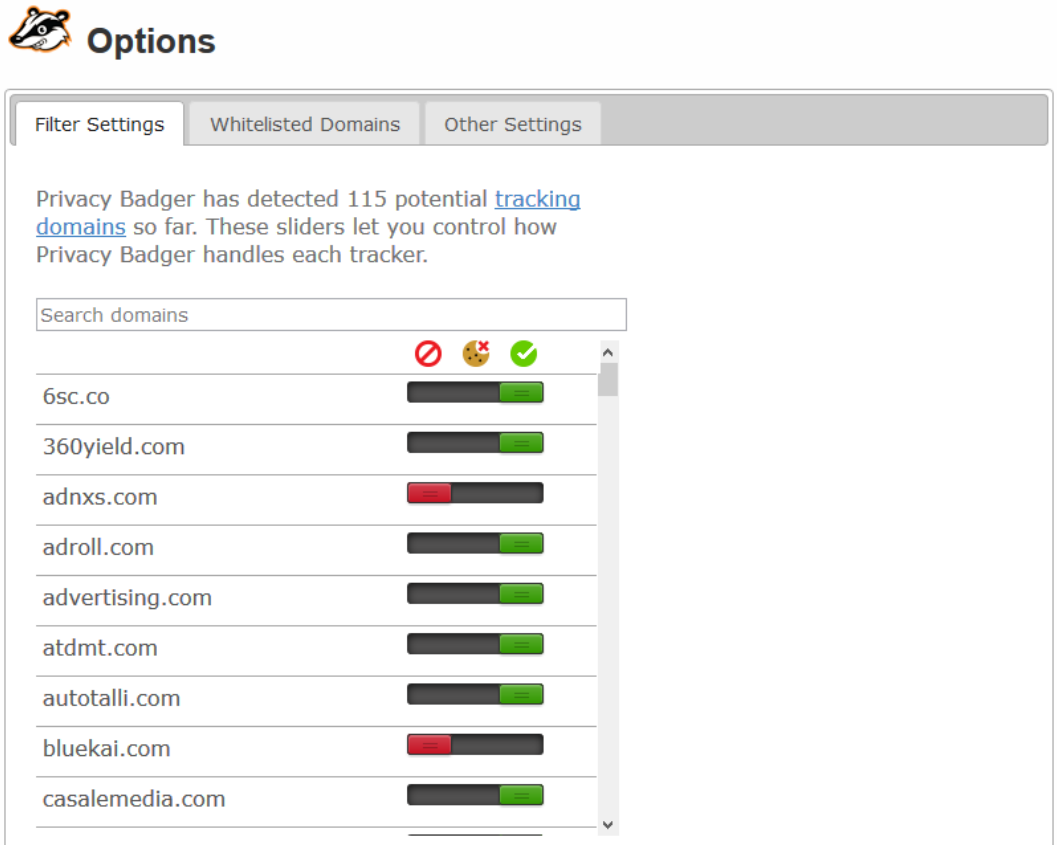
lii kyseessä olevan osapuolen sisällön lataamisen. Keltainen asetus tarkoittaa, että osapuolen sisältö ladataan, mutta sen evästeet estetään. Punainen estää osapuolen kokonaan. (EFF b.)



Kuvio 29. Privacy Badger -selainlaajennuksen havaitsemia potentiaalisia jäljittäjiä www.mtv.fi-sivustolla.

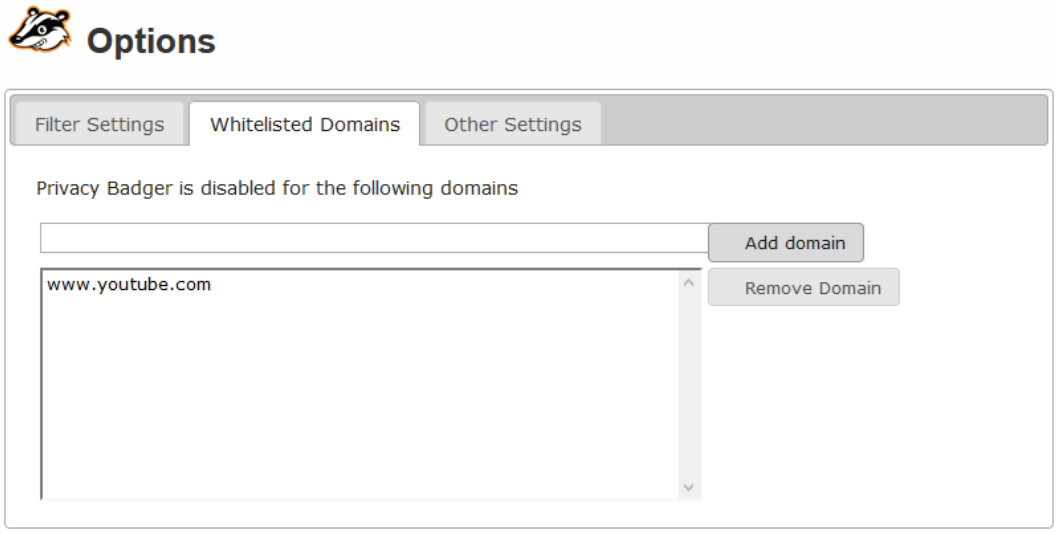
Privacy Badger hallinnoi asetuksia automaattisesti käyttäjän verkkoselailun perusteella, mutta käyttäjä voi myös itse muuttaa asetuksia liukusäätimillä.

Laajennuksen asetuksiin (kuvio 30) pääsee painamalla hammasrataksen kuvaketta.



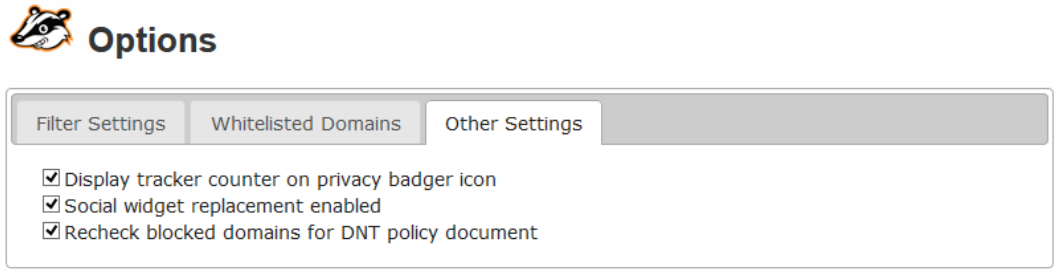
Kuvio 30. Privacy Badger -lisäosan kaikki tähän asti havaitsemat osapuolet ja niiden asetukset.

Whitelisted Domains -välilehti listaa sivustot, joilla käyttäjä on määritellyt Privacy Badgerin olevan pois päältä (kuvio 31). Sivustoja voi lisätä tai poistaa myös painamalla kyseisellä sivustolla ”Click to deactivate Privacy Badger on this site.” tai ”Click to activate Privacy Badger on this site.” (kuvio 29).



Kuvio 31. Privacy Badgerin sallimat sivustot.

Other Settings -sivustolla voi hallinnoida lisäosan muita asetuksia (kuvio 32). ”Display tracker counter on privacy badger icon” näyttää lisäosan ikonin ohessa, kuinka monta jäljittäjää sivustolla on löydetty. ”Social widget replacement enabled” korvaa sosiaalisen median painikkeet (kuvio 33). ”Recheck blocked domains for DNT policy document” tarkistaa, noudattavatko jo estetyt osapuolet käyttäjien Do Not Track -pyyntöä.



Kuvio 32. Privacy Badger -lisäosan muita asetuksia.

Kuvio 33. Privacy Badgerin korvaamia sosiaalisia painikkeita yle.fi-sivuston artikkelissa.

4.4.3 BetterPrivacy

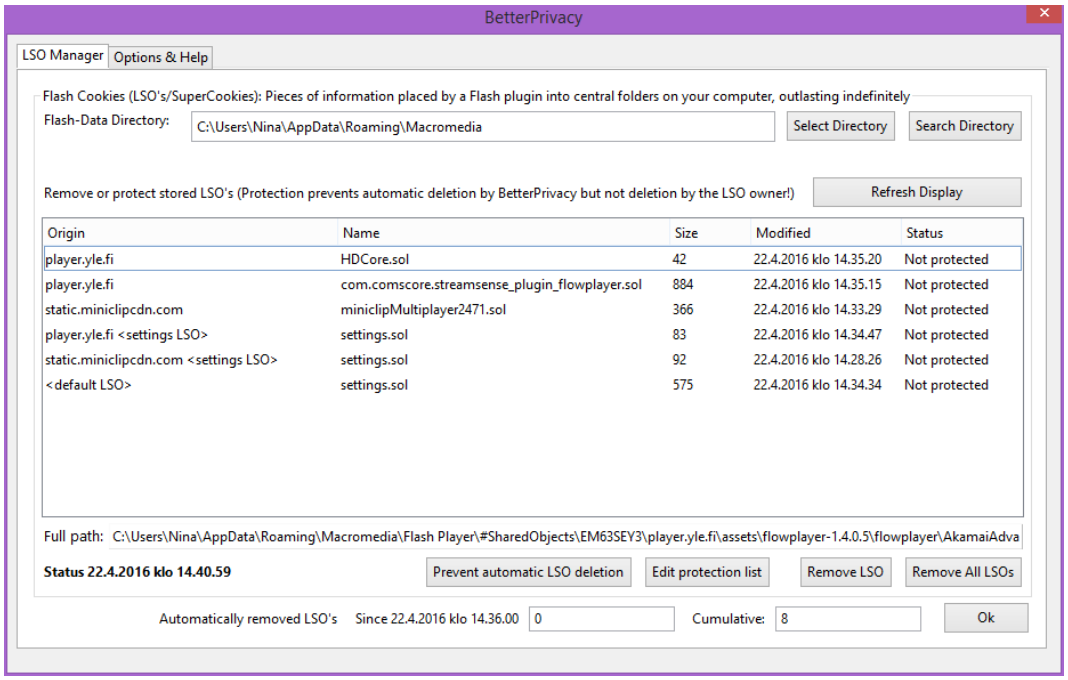
BetterPrivacy on Mozilla Firefox -selaimelle kehitetty lisäosa, joka poistaa Adobe Flash -selainohjelman tallentamat evästeet. Lisäosan voi asettaa poistamaan kaikki Flash-evästeet kun selainistunto suljetaan, tai sillä voi hallinnoida yksittäisiä evästeitä.

BetterPrivacy-lisäosan voi ladata osoitteesta https://addons.mozilla.org/fi/firefox/addon/betterprivacy/ ja painamalla ”+ Lisää Firefoxiin” -painiketta, hyväksymällä asennuksen ja käynnistämällä Firefoxin uudelleen.

BetterPrivacy hakee taustalla kansion, jonne Flash-evästeet on tallennettu. Oletusasetuksilla BetterPrivacy pyytää käyttäjän hyväksyntää poistaa löydetyt evästeet, kun selain suljetaan.

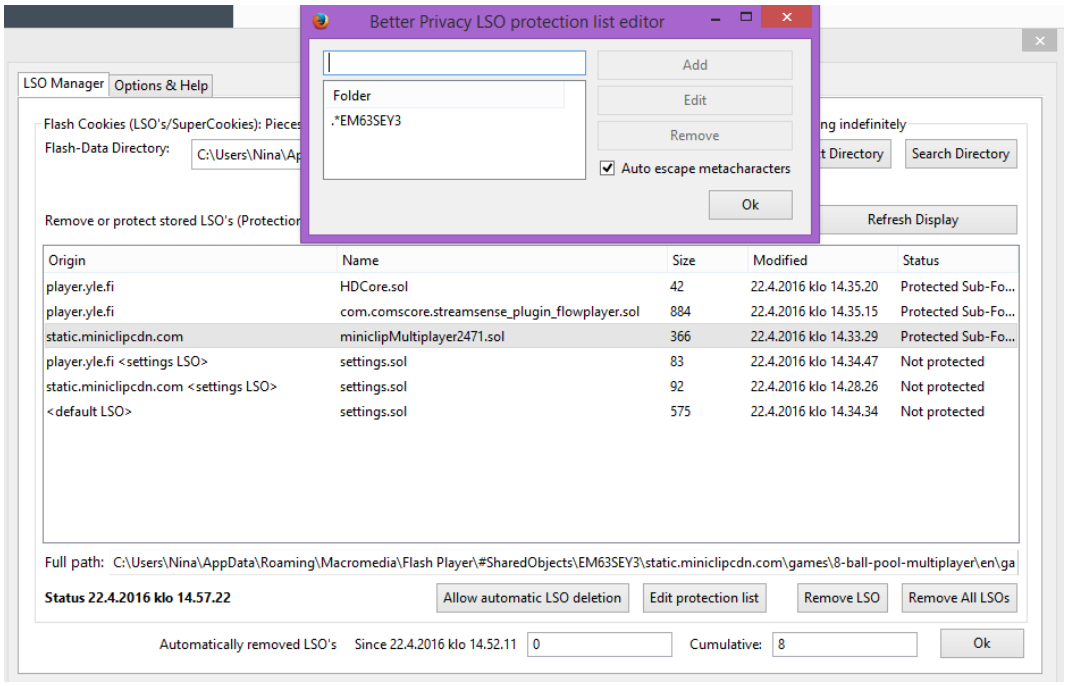
BetterPrivacyn asetuksia pääsee muokkaamaan selaimen lisäosien hallinnasta ja valitsemalla Asetukset, tai kirjoittamalla osoitepalkkiin ”about:addons”.

Asetusten ensimmäinen sivu, LSO Manager (kuvio 34), listaa Flash-evästeiden tallennuspaikan ja sen alikansioista löytyneet Flash-evästeet. Tallennuspaikan, josta BetterPrivacy etsii evästeitä, voi vaihtaa manuaalisesti Select Directory -valinnalla. Valitsemalla listasta evästeen ja painamalla ”Prevent automatic LSO deletion” voi halutut evästeet suojata, jolloin lisäosa ei poista niitä selainistunnon loputtua. ”Remove LSO”- ja ”Remove All LSOs” -painikkeilla voi poistaa valitun tai kaikki listan evästeet.



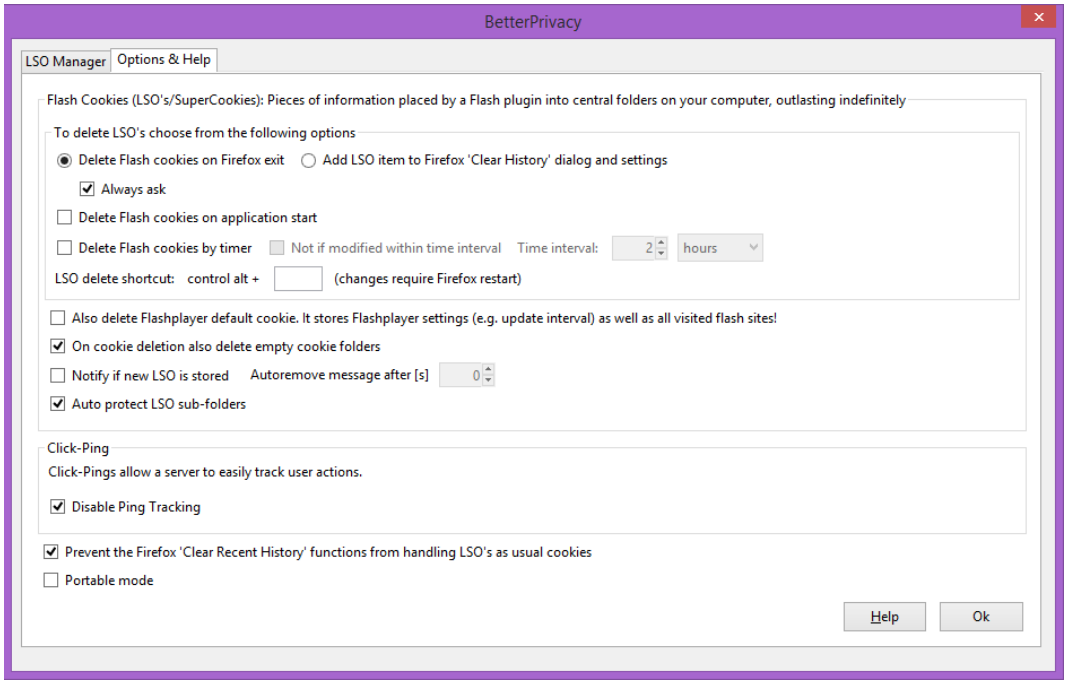
Kuvio 34. BetterPrivacy asetukset, sivu 1. Löydetyt evästeet ovat areena.yle.fi- ja miniclip.com-sivustojen tallentamia.

”Edit protection list” -painike avaa ikkunan, johon voi määritellä tietyt kansiot, joita lisäosa ei poista automaattisesti. Kuviossa 35 suojattuihin kansioihin on lisätty ”EM63SEY3”, jossa listan miniclipMultiplayer2471.sol -eväste sijaitsee (”Full Path” -tieto). BetterPrivacy on myös suojannut toisen sivuston asettamat evästeet evästeet HDCore.sol ja com.comscore.streamsense_plugin_flowplayer.sol, sillä ne sijaitsevat EM63SEY3-kansion alikansioissa (”Protected Sub-Folder”).



Kuvio 35. BetterPrivacyn suojatut kansiot -lista.

Asetusten toisella sivulla, Options & Help, voi muokata BetterPrivacyn asetuksia (kuvio 36). Taulukko 6 selittää tärkeimmät Flash-evästeiden poistoasetukset.



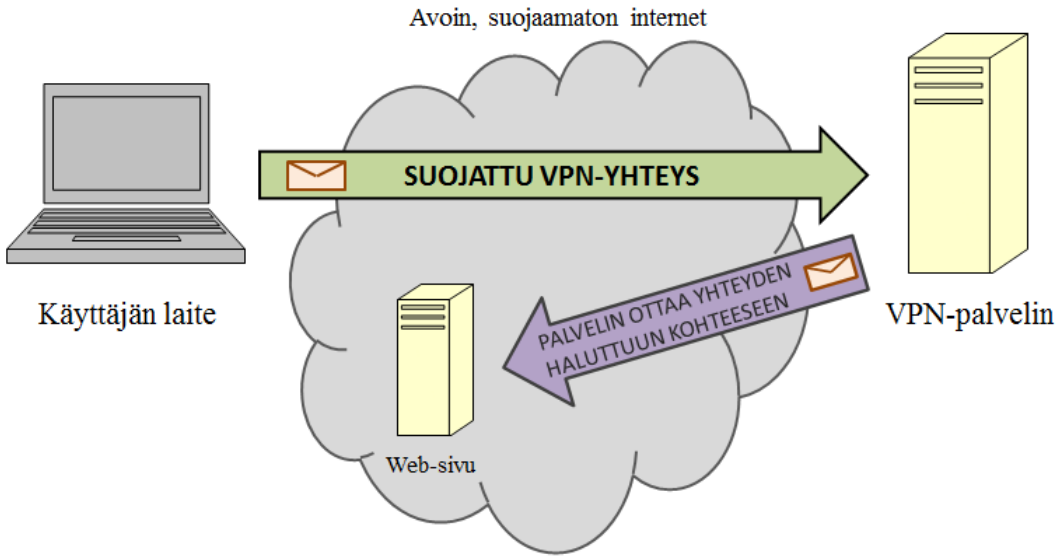
Kuvio 36. BetterPrivacy asetukset, sivu 2. Lisäosan oletusasetukset.

Taulukko 6. BetterPrivacyn Flash-evästeiden poistoasetukset.

ASETUS	SELITYS
Delete Flash cookies on Firefox exit / Add LSO item to Firefox ”Clear History” dialog and settings	Poistetaanko Flash-evästeet kun Firefox suljetaan, vai lisätäänkö Firefoxin sivuhistorian poisto -dialogiin valinta evästeiden poistamiselle.
Delete Flash cookies on application start	Evästeet poistetaan aina kun Firefox käynnistetään.
Delete Flash cookies by timer / Not if modified within time interval	“Time interval:” -valikolla muokataan evästeiden automaattinen poistoaika sekunneissa, minuuteissa, tunneissa tai päivissä. Jälkimmäinen valinta ei poista evästettä, mikäli sitä on muokattu poistoajan sisällä.
LSO delete shortcut	Määrittää näppäinyhdistelmän, jolla evästeet voi poistaa.

4.5 VPN

VPN, Virtual Private Network, salaa internetyhteyden luomalla salakirjoitetun tunnelin avoimen internetin sisälle käyttäjän laitteelta VPN-palvelimelle. Käyttäjän tietoliikenne kulkee ensin tunnelia pitkin VPN-palvelimelle ja sitten haluttuun kohteeseen (kuvio 37). Tunnelin sisällä liikkuva data on salattua, eivätkä ulkopuoliset pysty lukemaan sitä. VPN-yhteyksiä voidaan käyttää muun muassa etätyöntekijöiden yhdistämiseen yrityksen sisäverkon materiaaliin. (Bachrach & Rzeszut 2014)



Kuvio 37. VPN-yhteys.

Yritysten työntekijöiden tarpeiden lisäksi yksityisille käyttäjille VPN-yhteyksistä on hyötyä sijainnin piilottamisesta ja datavirran suojaamisesta. (Bachrach & Rzeszut 2014)

4.5.1 F-Secure FreeDome

FreeDome on tietoturvayritys F-Securen kaupallinen VPN-palvelu sekä tietokoneelle että mobiililaitteille. FreeDome estää käyttäjäseurannan, salakirjoittaa selainliikenteen ja piilottaa käyttäjän IP-osoitteen, tietokoneen yksilöivän numero-osoitteen, palveluntarjoajilta. Käyttäjä voi myös muuttaa virtuaalisen sijaintinsa

muuhun maahan. (F-Secure.) Tässä kappaleessa asennetaan FreeDomen 14 päivän kokeiluversio Windows 8.1-tietokoneelle ja esitellään sen toimintaa.

FreeDomen voi ladata osoitteesta www.f-secure.com/freedome ja lataamalla suoritettavan tiedoston. Tiedosto avaa asennusdialogin. Kun käyttöehdot on hyväksytty, FreeDome asentuu (kuvio 38).

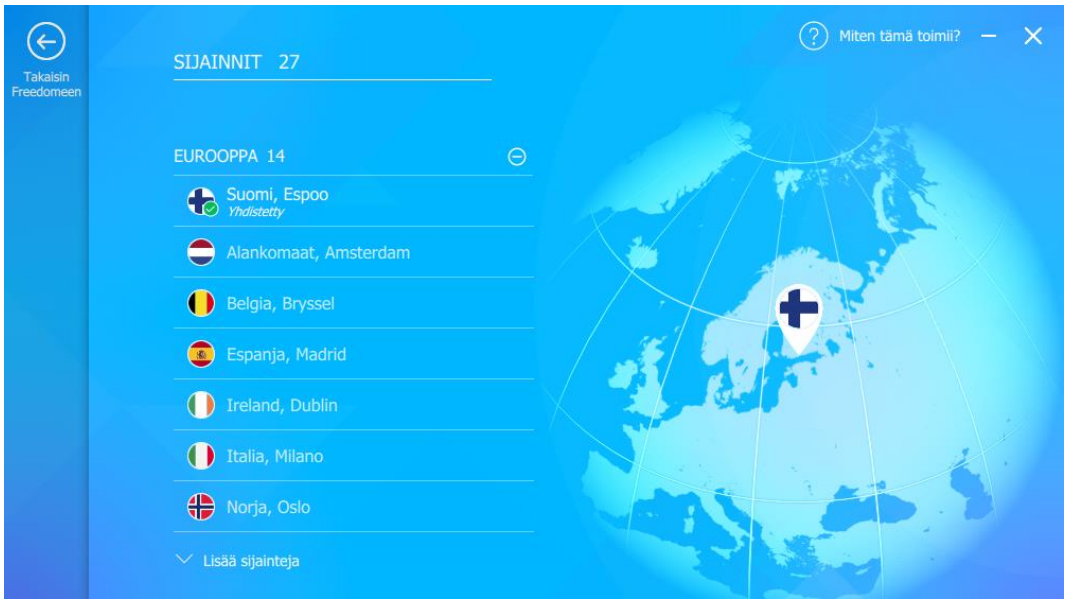
Kuvio 38. FreeDomen asennus Windowsille.

Oletusarvoisesti FreeDome ei ole päällä. Suojaus otetaan käyttöön painamalla POISSA-painiketta (kuvio 39). FreeDome ottaa yhteyden ikkunassa näkyvään sijaintiin, jonka kautta käyttäjän liikenne salataan (kuvio 40).

Kuvio 39. FreeDomen etusivu asennuksen jälkeen.

Kuvio 40. FreeDomen etusivu, kun suojaus on päällä.

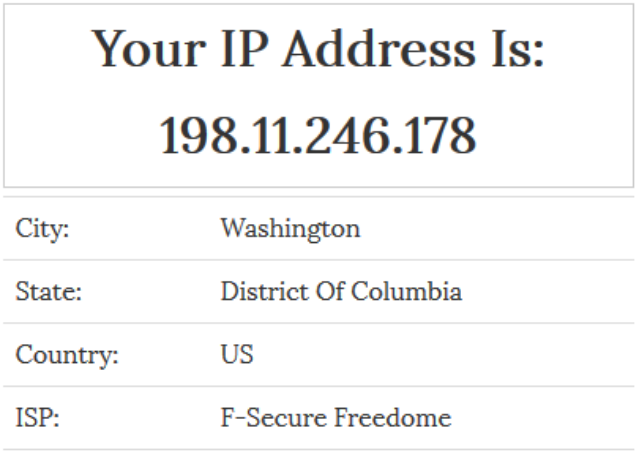
Käyttäjä voi vaihtaa virtuaalista sijaintiaan painamalla etusivun sijaintipainiketta. FreeDome avaa ikkunan, josta voi valita haluamansa sijainnin (kuvio 41). Laitteen sijainniksi vaihtuu tällöin valitun maan osoite.



Kuvio 41. FreeDomen sijainninvaihto.

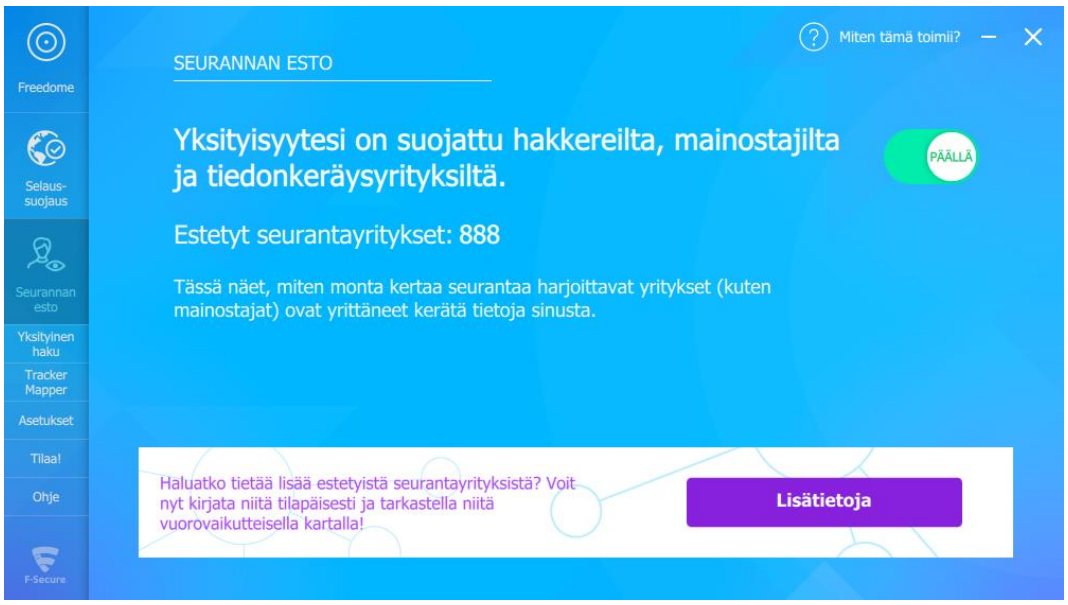
Valitaan esimerkkinä sijainniksi Yhdysvaltojen itärannikko. FreeDome ottaa yhteyden itärannikon palvelimeen (kuvio 42) ja vaihtaa sijainnin. Käyttäjän IP-osoite näyttää palveluntarjoajille tulevan Washingtonista (kuvio 43).

Kuvio 42. FreeDome vaihtaa käyttäjän virtuaalista sijaintia.



Kuvio 43. Käyttäjän IP-osoite FreeDomen virtuaalisella sijainnilla palvelussa www.whatismyip.com.

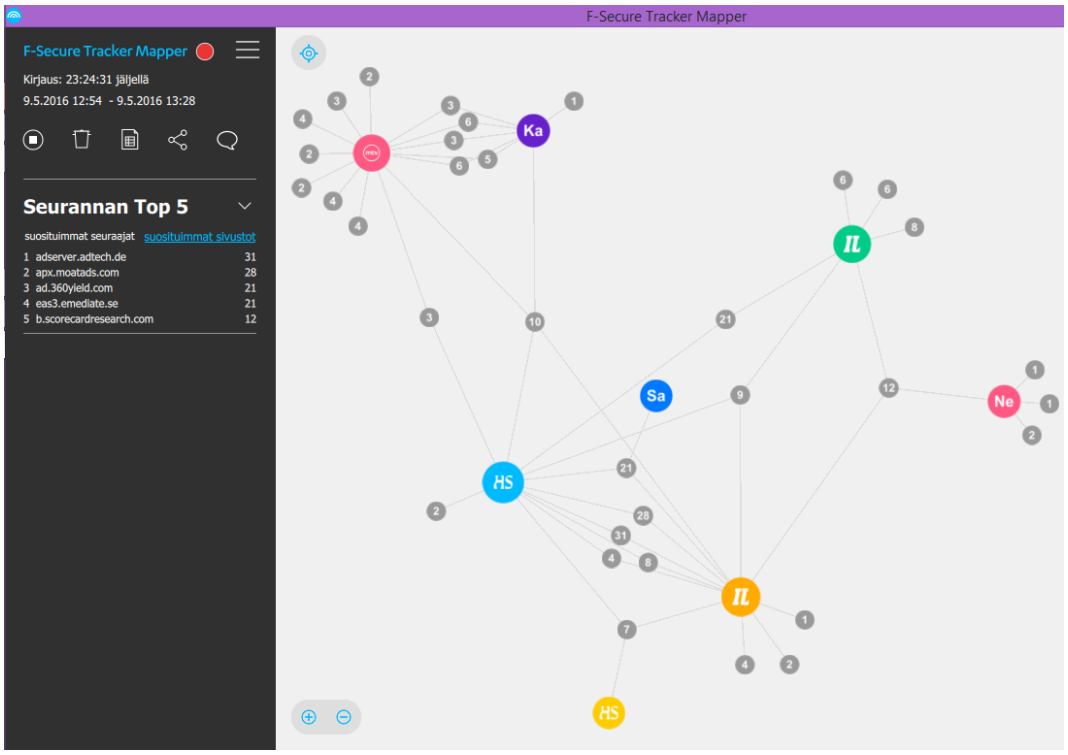
FreeDome suojaa käyttäjän nettiselaamisen seurannalta kaikissa selaimissa estämällä seurantaevästeet. FreeDome myös kertoo, kuinka monta seurantayritystä se on torjunut (kuvio 44).



Kuvio 44. FreeDomen seurannanesto.

Valitsemalla seurannan estosta ”Lisätietoja” tai vasemman laidan valikosta Tracker Mapper voi käyttäjä luoda 24 tunnin mittaisen reaaliaikaisen tilaston, johon merkitään Tracker Mapperin käynnissäoloajan aikana vieraillut sivustot sekä niihin liittyvien kolmansien osapuolien seurantayritykset (kuvio 45). Tracker Mapper linkittää yhteen seuraajat (kuvion 45 harmaat pallot) ja sivustot (värilliset

pallot). Jotkin seuraajat voivat liittyä enempään kuin yhteen sivustoon. Numerot kertovat, montako kertaa FreeDome on estänyt kyseisen seuraajan yrittämät käyttäjäseurannat.



Kuvio 45. FreeDome Tracker Mapper.

5 TULOKSET JA YHTEENVETO

Tämän opinnäytetyön tavoitteena oli vastata seuraaviin kysymyksiin:

1. mitkä ovat mainostajien motiivit käyttäjien seurantaan
2. miten mainostajat seuraavat käyttäjiä ja profiloivat heitä
3. miten käyttäjä voi suojautua mainostajien seurannalta.

Käyttäjäseurannan motivointiin löydettiin kannustimia mainosverkostoiden käytänteistä. Osuvampi mainosten kohdentaminen merkitsee todennäköisempää potentiaalisen asiakkaan tavoittamista. Mitä enemmän oikeita asiakkaita löydetään, sitä suuremmat kompensaatiot mainosverkosto saa mainostajilta, sillä mainostajat ovat halukkaita maksamaan kaksinkertaisia hintoja kohdennetusta mainonnasta vakiomainontaan verrattuna.

Yleisin mainostajien käyttämä väline käyttäjien seurantaan ovat HTTP-evästeet. Evästeet ovat tarpeellisia HTTP-tekniikassa, mutta ne myös mahdollistavat mainostajien käyttäjäseurannan: tallentamalla evästeisiin yksilöivän id-tunnuksen, voi mainostaja tunnistaa saman käyttäjän missä tahansa sivustolla, jolla vieraillessaan tämä käyttäjä lataa mainostajalta uudestaan sisältöä. Mainostaja voi täten seurata, mitä sivuja käyttäjä on katsellut ja päätellä siitä käyttäjän mahdolliset kiinnostustenkohteet. Evästeistä on myös hienovaraisempi versio, Adobe Flash -selainohjelman Flash-evästeet, joita sivustot voivat tallentaa käyttäjän laitteelle aina Flash-sisältöä ladattaessa.

Käyttäjällä on monenlaisia keinoja suojata internetsurffailunsa mainonnan seurannalta. Firefox- ja Chrome-selaimissa on molemmissa asetuksia, joilla evästeiden tallentamista ja poistoa voi hallita. Selaimissa voi myös tarkastella, mitä evästeitä on tallennettu ja poistaa yksittäisiä evästeitä. Flash-evästeiden hallinnoimiseksi täytyy vierailla Adoben sivulla, joka avaa Flash-evästehallintapaneelin. Flash-evästeet voi myös poistaa erillisellä selainlaajennuksella, jonka voi asettaa poistamaan evästeet automaattisesti. Selainlaajennuksia on HTTP-evästeidenkin estämiseen. Työssä läpikäydyn FreeDome VPN-toteutuksen avulla käyttäjä suoja-

taan seurantayrityksiltä, ja laitteen IP-osoitteen voi näyttää tulevan muualta maailmasta, jolloin mainostajien yksilöivää kohdentamista voi ”huijata”.

Kuluttaja- ja yksityisyysjärjestöt ovat kehittäneet ”Do Not Track” -käytäntöä, jolla käyttäjä voisi kertoa seurantaa yrittäville tahoille, ettei halua toimiaan internetissä seurattavan. Do Not Track -asetus on sekä Firefox- että Chrome-selaimissa, mutta sen noudattaminen on palveluntarjoajille vapaaehtoista. Asetuksen toimivuutta ei ole taattu. Puutteita löydettiin myös mainosyhtiöiden oman järjestön Digital Advertising Alliancen seurantaevästeiden esto-ohjelmasta. Esto toimii evästeiden avulla, ja mikäli käyttäjä poistaa selaimen evästeet, poistuvat myös seurannanestoevästeet. Tällä hetkellä kuluttajan paras suoja ovat hänen omat toimensa yksityisyytensä parantamiseksi.

Mainostajilla ja muilla seurantaa harjoittavilla tahoilla on muitakin keinoja käyttäjäseurannan toteuttamiseksi kuin HTTP-evästeet. Jatkotutkimuksen aiheena voisi olla näiden muiden seurantakeinojen kartoittaminen, jotta muodostuisi kokonaiskuva käyttäjäseurannan laajuudesta. Internetissä on myös muita seuraajia kuin mainostajat, ja heidän intressinsä voivat olla tutkimisen arvoisia. Opinnäytetyössä sivuttiin virallisia säädöksiä seurannan rajoittamiseksi sekä niiden tehottomuutta, joten aihetta olisi tutkimukseen yksityisyyslaeista ja -säädöksistä sekä niiden käytäntöönpanosta ja toimivuudesta.

LÄHTEET

Adblock Plus. About Adblock Plus. Viitattu 23.4.2016. https://adblockplus.org/en/about#acceptableads

Ayenson, M.D., Wambach, D.J., Soltani, A., Good, N. & Hoofnagle, C.J. 2011. Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning. Viitattu 2.5.2016. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390

Bachrach, D.G. & Rzeszut, E.J. 2014. 10 Don'ts on Your Digital Devices: The Non-Techies Survival Guide to Cyber Security and Privacy. Apress.

Barth, A. 2011. HTTP State Management. RFC6265. Viitattu 6.4.2016. https://www.rfc-editor.org/rfc/rfc6265.txt.

Castelluccia, C. & Narayanan, A. 2012. Privacy Considerations of Online Behavioural Tracking. European Network and Information Security Agency (ENISA). Viitattu 4.5.2016. https://www.enisa.europa.eu/publications /privacy-considerations-of-online-behavioural-tracking

Cranor, L.F. 2012. Can Users Control Online Behavioral Advertising Effectively? IEEE Security & Privacy. 10: 2. Viitattu 3.5.2016.

Electronic Frontier Foundation (EFF) a. Do Not Track. Viitattu 3.5.2016. https://www.eff.org/issues/do-not-track

Electronic Frontier Foundation (EFF) b. Privacy Badger. Viitattu 25.4.2016. https://www.eff.org/privacybadger

European Interactive Digital Advertising Alliance (EDAA). Tietoa selainkäyttöön perustuvasta mainonnasta. Viitattu 3.5.2016. http://www.youronlinechoices.com/fi /tietoa-selainkayttoon-perustuvasta-mainonnasta

F-Secure. F-Secure FreeDome VPN. Viitattu 10.5.2016. www.f-secure.com /freedome

Fisher, K. 2010. Why Ad Blocking Is Devastating to the Sites You Love. Ars Technica. Viitattu 23.4.2016. http://arstechnica.com/business/2010/03 /why-ad-blocking-is-devastating-to-the-sites-you-love/

Järvinen, P. 2010. Yksityisyys. 165; 194. Jyväskylä. Docendo.

Kapko, M. 2016. Why the Ad Industry Will Never Win the War on Ad Blockers. CIO Asia. Viitattu 23.4.2016. http://www.cio-asia.com/tech/industries /why-the-ad-industry-will-never-win-the-war-on-ad-blockers/?page=1%20

Karmina 2016. Malvertising Via Skype Delivers Angler. Viitattu 23.4.2016. https://labsblog.f-secure.com/2016/02/10/malvertising-via-skype-delivers-angler/

Kuehn, A. 2013. Cookies Versus Clams: Clashing Tracking Technologies and Online Privacy. Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media. 15: 6. Viitattu 15.5.2016.

Mozilla. Tracking Protection in Private Browsing. Viitattu 20.4.2016. https://support.mozilla.org/fi/kb /tracking-protection-pbm?as=u&utm_source=inproduct

Newman, J. 2015. EFF's New Do Not Track Standard Seeks to Stop Sneaky Data Collection. PCWorld. Viitattu 3.5.2016. http://www.pcworld.com/article/2956421/privacy /eff-s-new-do-not-track-standard-seeks-to-stop-sneaky-data-collection.html

Ramaswamy, S. 2016. How We Fought Bad Ads In 2015. Viitattu 23.4.2016. https://googleblog.blogspot.fi/2016/01/better-ads-report.html

Rantala, A. 2005. Web-ohjelmointi. 222. Porvoo. Docendo.

Roesner, F., Kohno, T. & Wetherall, D. 2012. Detecting And Defending Against Third-Party Tracking on the Web. USENIX. Viitattu 7.4.2016. https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner

Rothenberg, R. 2016. Avauspuhe. IAB Annual Leadership Meeting. Viitattu 23.4.2016. http://www.iab.com/news /rothenberg-says-ad-blocking-is-a-war-against-diversity-and-freedom-of-expression/

Siegler, MG. 2011. Google Chrome Can Now Clean Up Flash's Cookie Mess. TechCrunch. Viitattu 20.4.2016. http://techcrunch.com/2011/04/26/chrome-flash-cookies/

Singer, N. 2013. Wrangling Over 'Do Not Track'. The New York Times. Viitattu 3.5.2016. http://bits.blogs.nytimes.com/2013/07/15/wrangling-over-do-not-track/

Soltani, A., Canty, S., Mayo, Q., Thomas, L. & Hoofnagle, C.J. 2009. Flash Cookies and Privacy. Viitattu 2.5.2016. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862&rec=1&srcabs=1898390&alg=1&pos=1

Stiene, G. 2015. Is Ad Blocking Theft? VentureBeat. Viitattu 23.4.2016. http://venturebeat.com/2015/04/04/is-ad-blocking-theft/

Suich, A. 2014. Little Brother. The Economist. Viitattu 15.5.2016. http://www.economist.com/news/special-report/21615869-technology-radically-changing-advertising-business-profound-consequences

Tirtea, R., Castelluccia, C. & Ikonomou, D. 2011. Bittersweet Cookies. Some Security and Privacy Considerations. European Network and Information Security

Agency (ENISA). Viitattu 6.4.2016. https://www.enisa.europa.eu/activities /identity-and-trust/library/pp/cookies/

Tugend, A. 2015. Key to Opting Out of Personalized Ads, Hidden in Plain View. The New York Times. Viitattu 3.5.2016. http://www.nytimes.com/2015/12/21/business/media /key-to-opting-out-of-personalized-ads-hidden-in-plain-view.html?_r=0

Vaidhyanathan, S. 2011. The Googlization of Everything (And Why We Should Worry). 112-113. University of California Press.

W3Schools 2016. Browser Statistics. Viitattu 15.5.2016. http://www.w3schools.com/browsers/browsers_stats.asp