

# **Avoimien tietolähteiden käyttö poliisitoiminnassa: Pikaopas poliisille yleisvalvonnan tekemiseen Facebookin avulla**

Janne Ruotsalainen & Jesse Raunama

11/2021

# TIIVISTELMÄ

**Tekijät:** Janne Ruotsalainen & Jesse Raunama

**Opinnäytetyön muoto:** Toiminnallinen

**Julkisuusaste:** Julkinen

**Ohjaaja:** Ossi Kaario & Joni Tonteri

**Tutkinto:** Poliisi (AMK)

---

Tämän toiminnallisen opinnäytetyön tarkoituksena on tuottaa poliisille pikaopas yleisvalvonnan tekemiseen Facebookin avulla, avoimia tietolähteitä käyttäen. Opinnäytetyö on tarkoitettu rikostorjunnassa työskenteleville poliiseille, mutta myös valvonta- ja hälytyssektorin toiminnan tueksi. Tavoitteena on helposti saatavilla oleva ja helposti ymmärrettävä opas poliisin henkilöstön käyttöön, josta selviää miten ja mitä harvemmin käytettyjä avoimia tietolähteitä pystyy käyttämään hyödyksi rikostorjunnassa. Kansalaiset käyvät verkossa paljon omaa keskustelua eri rikosten ympärillä, tietävät ennalta jonkin tapahtuman tai rikoksen tapahtuvan taikka omaavat sellaista tietoa, mihin poliisilla ei ole pääsyä joko heti tai koskaan, jos yleisvalvontaa ei ole.

Opinnäytetyössämme käymme läpi aiheemme valintaan liittyviä näkökulmia ja opinnäytetyön rajauksesta. Käymme läpi opinnäytteen tavoitteet sekä ajankohtaisuuden. Tämän jälkeen kerromme yleisimmistä sekä hieman harvinaisemmista verkossa olevista avoimista tietolähteistä. Käymme läpi yksinkertaisimmista keinoista selvittää pieniä asioita nopeasti miltäkin sivustolta. Viimeisinä asioina opinnäytetyössämme tarkastelemme koko opinnäytetyö prosessin, luotettavuuden ja tarpeen jatkotutkimuksille.

Opinnäytetyömme liitteenä on produkti, joka on pikaopas poliisille yleisvalvonnan tekemiseen Facebookin avulla. Oppaaseen on alkuun tiivistetty ohje, kuka ja miten saa tehdä poliisina yleisvalvontaa.

---

**Sivumäärä:** 29+4

**Tarkastuskuukausi ja vuosi:** 11/2021

**Avainsanat:** Avoimet tietolähteet, OSINT, Yleisvalvonta, Opas poliisille

# SISÄLLYS

1 JOHDANTO.....	1
1.1 Aiheen valinta.....	1
1.2 Toiminallinen opinnäytetyö.....	1
1.3 Opinnäytetyön rajaaminen.....	2
2 OPEN SOURCE INTELLIGENCE – AVOIMET TIETOLÄHTEET.....	3
3 YLEISVALVONTA.....	4
4 HAKUKONEET OSINT-TOIMINNASSA.....	5
4.1 Google (google.com).....	6
4.2 Bing (bing.com).....	7
4.3 Yandex (yandex.com).....	7
4.4 Tor-verkko (The Onion Router, torproject.org).....	8
4.4.1 Ahmia (ahmia.fi).....	9
4.4.2 Dark Search (sarsearch.io).....	9
5 SOSIAALINEN MEDIA.....	10
5.1 Facebook (facebook.com).....	11
5.2 Profiilin yksityiskohdat.....	11
5.3 Facebookin Base64 koodaus.....	12
5.4 Twitter (twitter.com).....	13
5.5 Instagram (intagram.com).....	15
5.6 LinkedIn (linkedin.com).....	16
5.7 Snapchat (snapchat.com).....	17
6 YHTEISÖT.....	18
6.1 Reddit (reddit.com).....	19
6.2 Tiktok (tiktok.com).....	20
6.3 Tinder (tinder.com).....	20
6.4 Discord (discord.com).....	22
7 PRODUKTIN KUVAUS.....	23
8 YHTEENVETO JA POHDINTA.....	23
8.1 Johtopäätökset ja kritiikki.....	23
8.2 Luotettavuuden arviointi.....	24
8.3 Eettisyyden arviointi.....	26
8.4 Jatkotutkimukset.....	27
LÄHTEET.....	29
Liite 1. PIKAOPAS POLIISILLE YLEISVALVONNAN TEKEMISEEN FACEBOOKIN AVULLA.....	30

# 1 JOHDANTO

## 1.1 Aiheen valinta

Opinnäytetyömme aiheen idea tuli meille työharjoittelun aikana rikostutkinnan osajaksolla. Rikostutkinnan aikana pohdimme sitä, miten jo olemassa olevaa tietoa voisi saada kaivettua verkosta esiin poliisille käyttökelpoiseksi dataksi, kohtuullisen helpolla vaivalla, jos olisi tarvittavat tiedot, taidot ja resurssit toimenpiteisiin. Meillä molemmilla on jo entuudestaan ollut kiinnostusta avoimien tietolähteiden käyttöön mm. Poliisiammattikorkeakoulusta yhden tehtävän osalta, jossa opiskelijoiden piti kerätä mahdollisimman paljon tietoa avoimia tietolähteitäkin hyödyntäen. Rikostorjunnan osajaksolla tämä mielenkiinto vain kasvoi kasvamistaan ja aloimmekin pohtia, miten ammattikorkeakoulu laajuisen opinnäytetyön voisi tehdä kyseisestä aiheesta.

Otimme selvää jo tehdyistä opinnäytetöistä aiheen ympäriltä ja selvittelyiden jälkeen päätimme, että teemme tutkimuksen siitä, miten avoimia tietolähteitä käytetään tällä hetkellä poliisin suorittaman esitutkinnan apuna. Huomasimme omien kokemuksiemme ja aikaisempien tutkimuksien pohjalta sen, että aihetta käsitellään poliisissa mielestämme liian vähän eikä aiheeseen ole tarvittavalla laajuudella koulutusta. Näin ollen suunnitelmamme opinnäytetyöstämme tarkentui poliisilaitoskohtaiseksi kartoittamiseksi avoimien tietolähteiden käytöstä esitutkinnassa ja lisätutkinnan tarpeen selvittämiseksi.

Suunnitelmat muuttuivat kesken opinnäytteen tekemisen, koska emme saaneet haastateltavia poliiseja, jotka käyttäisivät avoimia tietolähteitä apunaan rikostutkinnassa. Halusimme kuitenkin pitää aiheemme avoimien tietolähteiden käytössä poliisin näkökulmasta. Päätimme, että teemme toiminnallisen opinnäytetyön, jonka produktina olisi opas poliisille avoimien tietolähteiden käyttöön. Oppaasta on hyötyä etenkin poliiseille, jotka eivät sosiaalisen median maailmassa normaalisti ole. Oppaan avulla jokainen yksittäinen poliisi pystyy tekemään yksinkertaisia tiedusteluja avoimia tietolähteitä käyttäen.

## 1.2 Toiminnallinen opinnäytetyö

Opinnäytteemme tarkoituksena on, että poliisi osaisi hyödyntää jokapäiväisessä työssään tehokkaasti jo olemassa olevaa tietoa ja tietää, mistä ja miten sitä tietoa voi etsiä. Tämä ajatus mielessä pitäen, rakensimme opinnäytteemme teoriapohjan Suomessa suuressa käytössä olevien sosiaalisen medioiden pohjalta sekä huomioimme sen, miten yksittäinen poliisi pääsee pimeään verkkoon hakemaan tietoa taikka suorittamaan yleisvalvontaa.

Opinnäytetyömenetelmiä pohtiessamme tulimme siihen lopputulokseen, että mahdollisimman selkeä, yksinkertainen ja helposti ymmärrettävä tuotos toiminnallisen opinnäytetyön produktina olisi

kaikista toimivin ja käyttäjäystävällisin. Olisimme halunneet tehdä tutkimuksellisen opinnäytteen, mahdollisesti yhdistäen sen toiminnalliseen opinnäytteeseen, mutta puute avoimien tietolähteiden päivittäisessä poliisitoiminnassa käyttämisessä johti pelkkään toiminnalliseen opinnäytteeseen.

Kuten edellä mainitsimme, opinnäytetyön suunnitelmat muuttuivat kesken tutkimuksen, tutkimuksellisesta opinnäytetyöstä toiminnalliseen. Toiminnallisen opinnäytetyömme produkti tulee olemaan pikaopas poliisille yleisvalvonnan tekemiseen Facebookin avulla. Avoimien tietolähteiden käyttöä ei tunneta mielestämme tarpeeksi, eikä osata suorittaa tiedustelua avoimista tietolähteistä tarvittavalla laajuudella, joten opas yksinkertaisimpiin toimintoihin tulee tarpeeseen. Opas lisää poliiseille tietoisuutta valtavaan massaansa tietoa, joka on saatavilla avoimista tietolähteistä. Samalla opas myös mahdollisesti lisää kiinnostusta ja yksittäisen poliisin motivaatiota kyseistä asiaa kohtaan, jolloin myös oppiminen, käytännön tekeminen ja osaaminen karttuu tehokkaammin. Myös kynnys suorittaa edes pienimuotoista tiedustelua avoimista tietolähteistä pienentyy, kun tietää mitä ja miten voi asioita tehdä.

Toiminnallisessa opinnäytteessä, tunnetaan myös tutkimuksellisena kehittämistyönä, toteutetaan työelämää kehittävä prosessi, tuotos tai produkti. Produkti voi olla esimerkiksi opas, ohje tai vaikka suunnitelma jonkin tietyn projektin toteuttamisesta. Opinnäytteen lopullinen versio on kaksi osainen, raportti ja itse tuotos eli produkti. Toiminnallisen opinnäytetyön avulla tekijä osoittaa sen, että hän osaa soveltaa oppimaansa teorian tietoa käytäntöön. Vaikka toiminnallinen opinnäytetyö keskittyykin itse tekemiseen tai kehittämistoimintaan, on toiminnallisessakin opinnäytetyössä oltava kirjallinen raporttiosuus. Raporttiosuudessa osoitetaan tekijöiden perehtyneen tutkittavana olevaan aiheeseen ja raporttiosuudessa samalla rajataan tutkielman aihe sekä kirjallisessa muodossa raportoidaan itse produkti. (Haikansalo & Korander 2021, 2.)

### **1.3 Opinnäytetyön rajaaminen**

Avoimien tietolähteiden tiedustelusta eli OSINT-toiminnasta on tehty useampia opinnäytetöitä aikaisemminkin, joten tässä opinnäytteessä halusimmekin keskittyä sellaiseen näkökulmaan, jota ei ole vielä tutkittu. Aiheen rajaamisessa piti tehdä tiukka linja mitkä avoimet tietolähteet otamme tutkielmaan mukaan ja mistä näkökulmasta asiaa käsittelemme, koska avoimia tietolähteitä maailmassa on lukematon määrä. Avoimia tietolähteitä ei myöskään ole virallisesti määritelty vain yhdellä tavalla, vaan määrittelyjä voi olla useampia. Tässä opinnäytetyössä rajaamme avoimet tietolähteet täysin avoimiin, kaikille saatavilla oleviin lähteisiin, riippumatta siitä, tarvitseeko tiedon äärelle pääseminen rekisteröitymistä tai maksua. Keskitymme tässä opinnäytetyössä vain verkossa oleviin avoimiin tietolähteeseen siksi, koska nyky maailmassa suurin osa tiedosta on sähköisessä muodossa ja verkosta saatavilla. Avoimia tietolähteitä ovat myös mm. painetut lehdet ja televisio, mutta niitä emme käsittele tässä opinnäytetyössä.

Verkossa olevat avoimet tietolähteet rajaamme tähän tutkimukseen yleisimpiin ja tunnetuimpiin internetin ja Tor-verkon hakukoneisiin, sekä sosiaalisten medioiden ja yhteisöjen alustoihin. Sivutamme myös mobiiliapplikaatioita, joista on kehitetty nykyään myös www-verkkosivut.

Olemme ottaneet opinnäytetyöhön mukaan myös joillekin tuntemattomimpia alustoja ja palveluita mukaan siksi, koska niiden käyttäjäryhmät on rajautunut selkeästi taikka palvelut ovat kohtuullisen uusia ja niiden suosio on nousemassa kovaa vauhtia.

Oppaassa keskitymme maailman käytetyimpään sosiaaliseen mediaan, joka on myös suomessa käyttäjämäärältään suurin ja käyttäjiä on eri ikäryhmistä. Produktia avataan opinnäytteen raportissa enemmän myöhemmässä vaiheessa.

## **2 OPEN SOURCE INTELLIGENCE – AVOIMET TIETOLÄHTEET**

Avoimien tietolähteiden tiedustelu eli OSINT (Open Source Intelligence). OSINT-toiminnassa kerätään tietoa kaikista avoimista tietolähteistä, julkisista tai muutoin laillisin keinoin saatavilla olevista lähteistä. Avoimia tietolähteitä voi olla mm. painettu media, televisio, radio tai vaikkapa kartat. Verkossa oleva tieto on kuitenkin kaikkein keskeisintä, koska internetissä oleva tieto on kaikkien saatavilla, mistä päin maailmaa tahansa ja pääosin julkista tai muutoin laillisin keinoin saatavilla olevaa avointa tietoa (Nurmi 2017, 8–11).

Miten avoimet tietolähteet määritellään? On olemassa eri teorioita, miten avoimet tietolähteet luokitellaan. Jotkut sanovat, että vain ja ainoastaan ilmaiset kaikille avoimet lähteet ovat avoimia tietolähteitä. Toiset katsovat, että myös jonkinlaisen maksumuurin tai rekisteröinnin takana oleva tieto on avointa tietoa ja luokitellaan avoimeksi tiedoksi. Me tässä opinnäytetyössä katsomme, että avoimia tietolähteitä ovat kaikki ne, joihin jokaisella internetin käyttäjällä on pääsy, eikä sillä ole väliä onko tieto maksumuurin tai rekisteröinnin takana.

Internet voidaan jakaa tiedon pohjalta kolmeen eri osa-alueeseen tiedon saatavuuden ja sijainnin perusteella. Ensimmäinen osa on ns. näkyvä osa (Clear / Surface Web), jota suurin osa maailman ihmisistä käyttää päivittäin. Toinen osa johon internet ja siellä oleva tieto voidaan jakaa, on ns. syvä verkko (Deep Web) johon kuuluu esimerkiksi kaikki pankkipalvelut kirjautumisen takana eli verkkopankit sekä organisaatioiden tietokannat, joihin pääsee vain kyseisen organisaation älykortilla tai muulla vastaavalla tavalla kirjautumaan. Viimeinen, eli kolmas osa on ns. pimeäverkko (Darknet), johon kuuluu mm. tässäkin opinnäytetyössä käsiteltävä Tor-verkko. Lyhyesti sanottuna, pimeässä verkossa käyttäjä on anonyymi eikä palveluntarjoajaa, taikka sen käyttäjää pystytä jäljittämään tai se on ainakin erittäin hidasta, vaikeaa ja monimutkaista.

Internetin ja siellä olevan tiedon jakaminen kolmeen eri alueeseen, tiedon sijainnin ja saatavuuden perusteella on havainnollistettu kuvassa 1.



Kuva 1. Internet ja siellä oleva tieto voidaan jakaa kolmeen eri alueeseen, tiedon sijainnin ja saatavuuden perusteella. Lähde: Willner-Mäenpää 2018, 16.

Michael Bazzellin mukaan OSINT tarkoittaa kaikkea tietoa, mikä on löydetty avoimista tietolähteistä. Tämän jälkeen se on kerätty, hyödynnetty ja jaettu oikeaan aikaan, sopivalle kohderyhmälle vastaamaan tiettyä tiedustelun tarvetta. Poliisitoiminnallisesti avoimia tietolähteitä voidaan käyttää lukemattomiin eri tarkoituksiin, muutamana esimerkkinä kadonneiden etsintä ja vaativien tai pimeiden juttujen tutkiminen, joihin ei ole saatavilla tietoa mitään muuta kautta taikka ennalta estävästi havaita tapahtuma tai ilmiö, johon pystytään vaikuttamaan oikea aikaisesti oikeilla keinoilla. Kaikille avoimet tietolähteet pitävät sisällään lukemattoman määrän tietoa, joka on saatavilla internetistä oikeilla keinoilla. (Bazzell 2021, 5–6.)

### 3 YLEISVALVONTA

Poliisin suorittamasta yleisvalvonnasta ei ole erillistä lainsäädäntöä. Verkossa tapahtuvaan yleisvalvontaan on kuitenkin otettu kantaa nykyisen poliisilain esitöissä. Lain esitöiden mukaan, ei ole tarpeellista säätää erillistä toimivaltaa poliisille tähän tarkoitukseen, kun yleisvalvonta kohdistuu

verkkoympäristön avoimiin tietolähteisiin ja poliisi suorittaa tarkkailua passiivisesti eikä aktiivisesti. (HE 224/2010 vp, s. 34.)

Rikollisuus on siirtynyt entistä enemmän verkkoympäristöön vuosien saatossa ja tulee todennäköisesti lisääntymään entisestään. Tästä syystä myös poliisin pitää pystyä toimimaan entistä tehokkaammin verkkoympäristössä niin ennalta estävän poliisitoiminnan kuin rikosten paljastamiseen ja selvittämiseen liittyvissä tapauksissa. Verkossa on kansalaisilla suuri määrä tietoa ja aineistoa, mitä poliisilla ei ole käytössään ilman, että poliisi on itse verkkoympäristössä suorittamassa yleisvalvontaa. Poliisilla on erillinen kirje verkkoympäristössä tapahtuvaan yleisvalvontaan ja verkkoympäristössä toimimiseen. Verkkoympäristössä toimivalla poliisilla tuleekin olla selkeästi tiedossa, mitä hän saa tehdä, miten hän saa tehdä, milloin ja kenen määräyksestä. Kuka tahansa poliisi ei saa suorittaa verkkovalvontaa, vaan siihen on olemassa omat säädöksensä ja määräyksensä. Verkossa tapahtuva yleisvalvonta on helposti kallellaan poliisi- ja pakkokeinolaissa säädelyjen keinojen mm. tarkkailun ja suunnitelmallisen tarkkailun piiriin. Tästä syystä on ehdottoman tärkeää, että poliisina tietää milloin on oikeutettu tekemään yleisvalvontaa verkossa ja miten kyseistä toimenpidettä tehdään.

Yleissääntönä on, että verkossa suoritettavaa yleisvalvontaa tekevä poliisi on lukenut ”*poliisihallituksen kirje verkkoympäristössä tapahtuvaan tiedonhankintaan liittyen*” sekä, että salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu virkamies (STEKPOV) on tehnyt päätöksen kyseisen konstaapelin toimivan verkossa tapahtuvassa yleisvalvonnassa. Tämän jälkeen kyseinen päätöksessä mainittu konstaapeli on oikeutettu tekemään ns. ”valesähköpostin” ja ”valenimen” jolla hän voi toimia verkkoympäristössä paljastamatta itseään. Kaikki päällystöön kuuluvat virkamiehet eivät kuitenkaan ole STEKPOV henkilöitä, vaan heidän on nimenomaan pitänyt saada koulutus kyseiseen aihepiiriin ja heidät on pitänyt erikseen nimittää STEPKOV tehtäviin omien tehtäviensä ohella. (Poliisihallituksen kirje verkkoympäristössä tapahtuvaan tiedonhankintaan liittyen, POL-2017-11225)

## **4 HAKUKONEET OSINT-TOIMINNASSA**

Maailmassa on useita hakukoneita, joiden kautta useimmat avoimien lähteiden tiedustelua tekeville hakukoneiden käyttö on ensimmäinen tapa tehdä tiedustelua. Tässä käydään muutamaa hakukonetta läpi ja niiden yksinkertaisimpia ja tehokkaimpia hakukeinoja. Kaksi suurinta toimijaa hakukoneissa Yhdysvalloissa ovat Google ja Bing (Bazzell 2021, 181).

Yksinkertainenkin hakukonehaku henkilön, tai organisaation nimellä, tai Y-tunnuksella ohjaa tuloksiin sosiaalisen median palveluista ja yritystietopalveluista. Hakuja on suositeltavaa tehdä useilla



eri vaihtoehtoilla sisällyttäen eri nimet ja niiden kirjoitusmuodot. Yrityksillä myös kannattaa hakea myös aputoiminimiä. (Laurio 2020, 200.)

Hakukoneilla toimii useat samat tavat, riippumatta hakukoneesta. Kuitenkin on joitakin erityisyyksiä ja eroavaisuuksia, jotka tulisi tiedostaa hakukoneita käyttäessä.

#### **4.1 Google (google.com)**

Muutamalla yksinkertaisella säännöllä on mahdollista saada tarkempaa dataa hakukoneita käyttämällä. Hakukoneella hakemalla ei ole mahdollista rikkoa mitään. Hakemalla ja tarkennettua hakua käyttämällä hakukoneen ominaisuudet tulevat tutummaksi (Bazzell 2021, 181).

Lainausmerkkien käyttö Googlea käytettäessä on suotavaa. Asettamalla halutun nimen lainausmerkkien sisään, saadaan suuri ero informaation määrässä. Hakutulos Michael Bazzell antaa tulokseksi 147,00 sivua, jotka sisältävät sanat "Michael" ja "Bazzell". Näillä sivuilla ei ehdottomasti ole kyseiset sanat vierekkäin. Sana "Michael" voi olla jonkun toisen henkilön nimen vieressä ja sana "Bazzell" voi olla jonkun toisen henkilön nimen vieressä. Näin hakemalla voi saada epätarkkoja hakutuloksia. Ne voivat sisältää viittauksen henkilöön nimeltä "Michael Santo" tai "Barry Bazzell", mutta ei henkilöön "Michael Bazzell". Ei toivotun hakutuloksen välttämiseksi on suositeltua käyttää lainausmerkkejä kohdehaun nimen ympärillä. Hakutulos "Michael Bazzell" lainausmerkkejä käyttämällä tuo rajatumman hakutuloksen, 31,800 hakua. (Bazzell 2021, 181.)

Googlen kuvahaku ja käänteinen kuvahaku on erittäin hyvä toiminta, ja voikin auttaa tiedonhankinnassa paljonkin. Googlen kuvahaku hakee kuvia avainsanoilla, jotka ovat sijoitettuna kuvan tiedostoon. Tämä ei todellakaan ole aukoton haku ja yleensä antaakin täysin aiheeseen liittymättömiä hakutuloksia. Rajataksesi hakua sopimaan paremmin haluamaasi lopputulokseen, tulisi sinun käyttää lainausmerkkejä. Mitä enemmän käytät hakusanoja lainausmerkkien sisällä, sitä kohdennetummat tulokset ovat. Esimerkiksi hakiessasi henkilöä nimellä, tulisi kyseinen nimi olla lainausmerkkien sisällä, mutta myös muita hakusanoja, jotka liittyvät henkilöön. Mahdollisesti paikka, jossa kuva on otettu, ammatti, kotikaupunki, tekeminen, henkilökohtaiset kiinnostukset. Jos haluat edelleen tarkemman haun, Google työkalujen avulla pystyt rajaamaan hakutuloksia mm. tietyn kokosiin tai värisiin kuviin, tietyllä aikavälillä otettuihin kuviin tai vaikkapa kuvan tyyppiin. (Bazzell 2021, 194, 433–434.)

Googlen käänteinen kuvahaku on perinteistä kuvahakua paljon hyödyllisempi ja tehokkaampi keino löytää haluamansa. Googlen käänteistä kuvahakua tehdessä, haetaan tietyllä kuvalla samankaltaisia kuvia tai tarkalla kuvan linkillä haetaan samankaltaisia tai täysin samoja kuvia, eri sivustoilta. Pelkällä kuvalla tai linkillä haettaessa, hakutulokset voivat olla hyvinkin suuria. Mikäli lisää

esimerkiksi henkilön nimen hakukriteereihin, hakutulokset rajautuvat vain sopiviin kuvavaihtoehtoihin eri sivustoilta. (Bazzell 2021, 434.)

## **4.2 Bing (bing.com)**

Bing on Googlen jälkeen toinen maailman käytetyimmistä hakukoneista. Bing myös poissulkee yahoo.com hakukoneen siksi, että Yahoo alkoi vuonna 2009 käyttämään Bingin tarjoamia tuloksia. Bing hakukoneessa toimii pääsääntöisesti samat hakumekanismi, kuin Googlessa. Bingissä kuitenkin toi ensimmäisenä ajallisesti rajatun kuvavaihtoehdon maailmalle, joka toki on nykyään myös käytössä Googlessa. (Bazzell 2012, 193.)

Bingin yksi ominaisuus on linkkien hakutoiminto. Bing LinkFromDomain ominaisuudella, hakukoneella pystyt myös hakemaan tiettyjä linkkejä eri sivustoilta. Hakukone hakee kaikki sivustot, joissa linkki ilmenee, myös sellaiset, joissa linkit ovat kirjoitettu piiloon jonkin sivuston koodiin, eikä ole visuaalisesti havaittavissa pelkästään silmäilemällä sivustoa. Esimerkiksi hakemalla Bingissä "LinkFromDomain: intertechniques.com", kaikki yhteen kirjoitettuna lainausmerkkien sisälle, hakutulos näyttää kaikki sivustot, joissa on kyseinen linkki sijoitettu mihin tahansa sivustolle, koodaukset mukaan lukien. (Bazzell 2021, 194.)

Bingin kuvahaku toiminto on vastaavanlainen kuin Googlessa. Bingissä on kuitenkin hyvänä erona se, että hakutuloksia voi rajata kuvan muodon mukaan sekä esimerkiksi valita rajausehdoista pelkästään "pää" tai "pää ja hartiat" kuvia. Bingin kuvahakutoiminto myös ehdottaa automaattisesti mitä rajauksia haussa voisi käyttää. Kun Bingissä avaa kuvahaussa tulleen kuvan auki, Bing ehdottaa heti perään uusia samojen kriteereiden täyttämiä kuvia sinulle. Tämä toiminto voi ohjata sinun tiedonhankintasi sellaisen tiedon äärelle, josta sinulla ei aikaisemmin ollut havaintoakaan. (Bazzell 2021, 194, 433–434.)

## **4.3 Yandex (yandex.com)**

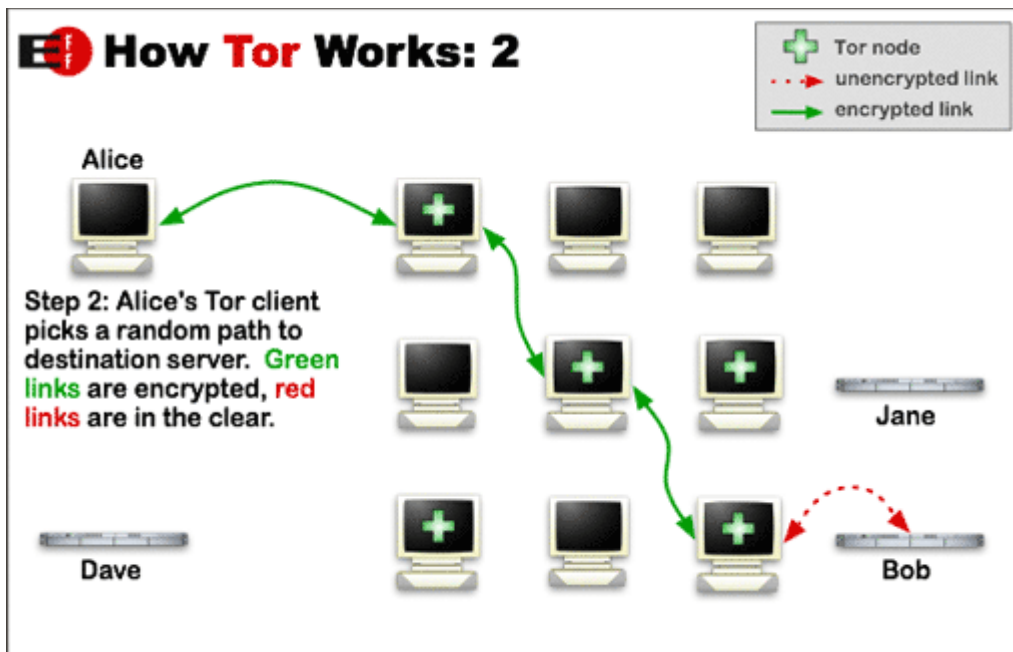
Yandex hakukoneen käyttö ei ole entuudestaan ollut kauhean tuttua ja suosittua, sen yksinkertaisuuden ja suppeiden hakutoimintojen takia. Nyt, viime vuosina Michael Bazzell on löytänyt Yandexistä hyödyllisiä toimintoja, mitä ei ole aikaisemmin tiennyt tai muutoinkaan muissa hakukoneissa ei ole mahdollista käyttää. Hakutulokset näillä toiminnoilla voi tuottaakin hakijalle paljon uutta tietoa, varsinkin heille, jotka suorittavat esimerkiksi henkilöille kattavia taustatutkimuksia (Bazzell 2021, 195).

Yandexissa on suurilta osin samat perustoiminnot kuin Googlessa ja Bingissä, mutta tulokset ovat suppeampia. Muutamat poikkeukset Yandexin hakukoneessa on verrattuna kahteen suurimpaan Googleen ja Bingiin. Yandexilla on erityispiirteensä puuttuvan sanan hakeminen. Yandex

hakukoneella voi hakea lauseesta puuttuvaa sanaa toiminnolla "Open Source \* Techniques". Tässä tapauksessa hakukone hakee lauseita, joissa on kyseiset edellä mainitut sanat, mutta tähti-merkin (\*) paikalla on mikä tahansa sana. Kyseisellä haulla löytyy lähteenä käytetty kirja, mutta myös paljon muita esimerkiksi "Open Source Resposive Techiniques" lauseita sisältäviä sivuja. Tällä tavalla voikin tehokkaasti hakea esimerkiksi henkilön nimeä, mitä itse ei tiedä. (Bazzell 2021, 196.)

Puuttuvan sanan lisäksi, Yandex hakukoneessa on mahdollista hakea lauseita tai vaikka nimiä, joissa on useampi sama sana. Toiminolla pystyy erottelemaan kirjoitustyylin, jotta hakutulokset sisältävät haetut sanat riippumatta siitä, onko ne kirjoitettu yhteen, väliviivalla tai miten tahansa. Toimintoa ei ole käytössä muissa hakukoneissa, joka on suuri etu Yandexille. Useamman saman sanan hakeminen nopeuttaa, helpottaa ja parhaassa tapauksessa tuo jopa uutta ja lisää tietoa hakijalle. Esimerkkinä henkilö, jonka nimessä on kaksi samaa sanaa "Carina Abad Abad". Käyttämällä pelkkiä lainausmerkkejä haussa, saa varmasti suuren osan hakutuloksista, mutta haku kuitenkin rajaa pois ne vaihtoehdot, joissa nimi on kirjoitettu eri tavalla. Esimerkiksi AbadAbad, Abad-Abad tai Abad,Abad. Useamman saman sanan haku toimii seuraavasti. Haetaan nimi ilman lainausmerkkejä, käyttämällä huutomerkkiä jokaisen sanan edessä: !Carina !Abad !Abad. Tällä tavalla hakutulokset pitävät sisällään esimerkiksi kaikki edellä mainitut kolme kirjoitustyyliä nimestä. (Bazzell 2021, 196.)

#### 4.4 Tor-verkko (The Onion Router, torproject.org)



Kuva 2. Havainnollistava kuva, miten Tor-verkko toimii salattuna. Lähde: Tor Project 2018

Kuvassa kaksi on havainnollistettu, miten Tor-verkon salaus toimii niin, ettei alkuperäinen sivuston käyttäjä ei paljastu. Kuvassa kaksi oleva Tor-verkon käyttäjä Alice, joka käyttää Tor-verkkoa omalla laitteellansa, yhdistää oman laitteensa toiseen satunnaisen Tor-verkkoa käyttävän käyttäjän laitteeseen. Tämä toistuu niin, että reitti kohdesivustolle kulkee yhteensä kolmen eri satunnaisen Tor-verkon käyttäjän laitteen välillä, joiden kaikkien välillä on salattu yhteys. Lopullinen kohdesivustolle muodostuva yhteys joko on tai ei ole salattu, riippuen kohdesivustosta. Kuitenkin alkuperäinen sivuston käyttäjä Alice on salassa edellä mainittujen toimenpiteiden vuoksi.

Tor (The Onion Router) eli Tor-verkko on suunniteltu täysin anonyymiin internetin käyttöön, jota on miltein mahdotonta jäljittää, vähintäänkin erittäin vaikeaa ja työlästä. Tor, nimensä mukaisesti (Onion) on rakennettu monesta kerroksesta, jotka muodostuvat kaikki yleisistä avoimista palvelimista, Tor-verkon käyttäjistä, jossa on yli 6 000 "kerrosta" salauksia. Tor-verkossa tästä syystä onkin monia laittomia sivustoja, joiden kautta myydään esimerkiksi huumeita ja aseita. Tor-verkossa olevat sivustot toimivat samalla periaatteella kuin verkon käyttö. Siitä syystä palvelimia on erittäin vaikea paikantaa ja yhdistää henkilöihin. (Bazzell 2021, 211.)

Tor-verkko on täysin laillista käyttää ja sen saa kuka tahansa ladattua omalle laitteelleen osoitteesta <https://www.torproject.org>. Kuten edellä mainittu, Tor-verkko muodostuu monesta eri käyttäjästä ja niistä syntyvistä kerroksista.

Vaikkakaan yksikään hakukone ei kata kaikkia hakutuloksia, ei normaalissa verkossa mutta ei myöskään Tor-verkossa. Tor-verkossa on siis useita Tor-hakukoneita normaalin verkon tavoin, jotka ovat varsin tehokkaita, seuraavaksi käymme läpi muutamia suosituimpia ja tehokkaimpia niistä.

#### **4.4.1 Ahmia (ahmia.fi)**

Ahmia.fi Tor-hakukone on Tor-verkossa olevista hakukoneista kaikista tehokkain. Kyseinen hakukone ei anna kaikkia hakutuloksia normaalin verkon kautta, joten sitä tulee käyttää Tor-selaimella, joka on ilmaiseksi ja laillisesti ladattavissa. Ahmia-hakukonetta suositellaankin jokaiseen Tor-selaimen ensimmäiseksi hakukoneeksi, josta lähteä etsimään tietoa. (Bazzell 2021, 211.)

#### **4.4.2 Dark Search (sarsearch.io)**

Dark Searchin hakukone on Ahmia.fi rinnalla erittäin hyvä. Dark Search täydentää Ahmia hakukonetta ja antaa kattavia tuloksia sellaisista hauista, joista ei Ahmia hakukoneesta saa montaa tulosta. Esimerkiksi "OSINT" haulilla Ahmia hakukone antoi viisi tulosta, kun taas Dark Search antaa

51 tulosta. Dark Search toimii hyvin myös Tor-verkossa haettaessa sähköpostiosoitteita. (Bazzell 2021, 211.)

## 5 SOSIAALINEN MEDIA



Datalähde: DNA, Digitaaliset elämäntavat, 2020, <https://www.stinfo.fi/data/attachments/00513/ceded4cb-ddeb-4441-9081-46990b8e41ac.pdf> (N=1036, 16-74-vuotiaat), käyttö vähintään viikoittain, SVT:n väestötiedot 2020 (stat.fi), kuva: Harto Pönkä, 12.4.2021.

Kuva 3. Suomessa viikkotasolla käytetyimmät sosiaaliset mediat ja niiden käyttäjämäärät. Lähde: Innwise, Sosiaalisen median käyttö Suomessa: somekatsaus 04/2021

Suomalaisten käytetyin yhteisöpalvelu vuonna 2020 oli Facebook, jota seurasi 58 prosenttia 16–89-vuotiaista. Toiseksi käytetyin oli WhatsApp, jota käytti 50 prosenttia 16–89-vuotiaista. Kolmanneksi käytetyin oli Instagram, jota käytti 39 prosenttia. Nuoret käyttivät WhatsAppia useammin kuin Facebookia, kuten myös Instagramia. Vanhemmissa ikäluokissa asianlaita oli päinvastainen. (Tilastokeskus, 2020, s. 2.)

## Liitetaulukko 25. Seuratut yhteisöpalvelut 2020, %-osuus väestöstä

	16-24v	25-34v	35-44v	45-54v	55-64v	65-74v	75-89v	Miehet	Naiset	Kaikki
Facebook	67	81	76	66	52	42	13	53	63	58
WhatsApp	78	72	58	56	44	27	6	46	53	50
Instagram	80	65	50	40	24	12	2	33	45	39
Snapchat	71	26	5	6	2	0	0	13	16	14
Twitter	27	20	18	14	10	4	1	16	11	13
LinkedIn	8	25	21	20	10	3	1	15	11	13
TikTok	34	9	3	2	1	0	0	5	8	6
Jodel	25	13	2	0	0	0	0	4	7	5
Suomi24	4	3	3	3	4	3	1	4	3	3
Joku muu	12	10	6	5	2	2	1	5	6	6

Taulukko 1. Suomalaisien seuraamat yhteisöpalvelut ikäryhmittäin vuonna 2020. Lähde: Tilastokeskus 2020.

### 5.1 Facebook (facebook.com)

Facebookiin kirjautumisen jälkeen etsi-valikko ilmestyy Facebook sivun yläreunaan. Kannattaa ajatella hakutulokset kahteen eri osaan. Avainsana haulla etsitään tiettyä geneeristä termiä, nimeä, lokaatiota, tai kokonaisuutta. Filtröity haku on tapa, millä voi rajata ei toivottuja hakutuloksia (Bazzell 2021, 220).

Kirjoittamalla henkilön oikean nimen hakukenttään johtaa tuloksiin, joista suurin osa ei liity etsittyyn henkilöön. Muista sosiaalisista medioista poiketen Facebookin käyttäjät yleensä käyttävät omaa nimeään luodessaan profiilia. Tämä profiili linkittyy usein työnantajaan, lukioon, yliopistoon, tai yleisiin mielenkiinnonaiheisiin. Facebookilla on miljardeja aktiivisia käyttäjiä, joten on todennäköistä, että hakutuloksiin ilmestyy useita käyttäjiä, joilla on sama nimi kuin henkilöllä, josta tehdään tiedustelua. (Bazzell 2021, 220.)

Henkilön profiilia tarkastellessa oletusnäkyvä on "aikajana" välilehti. Tässä näkyvät käyttäjän perustiedot kuten, sukupuoli, asuinpaikka, perheenjäsenet, ystävät, siviilisääty, mielenkiinnonkohteet, koulutus ja työkokemus. Tällä sivulla on usein myös käyttäjän kuva ja uusimmat postaukset heidän sivullaan. Tätä dataa tutkimalla on mahdollista löytää lisäinformaatiota käyttäjästä, mutta tässä ei välttämättä ole kaikki saatavissa olevat tieto käyttäjästä. (Bazzell 2021, 221.)

### 5.2 Profiilin yksityiskohdat

Profiilia tutkimalla pystyy analysoimaan käyttäjän julkisesti avointa sisältöä. Facebook kerää ja tallentaa paljon ylimääräistä informaatiota jokaisen käyttäjän toiminnasta sen tietoverkossa. Joka

kerta, kun joku "tykkää" jostain tai on merkitty kuvaan Facebook tallentaa tuon tiedon. Yksityiskoh-  
tien löytäminen voi olla vaikeaa. (Bazzell 2021, 224.)

Päästäkseen käsiksi haluttuun tietoon täytyy selvittää profiilin käyttäjännumero. Tämä numero mah-  
dollistaa muuten piilotetun tiedon etsimisen Facebookista. Käyttäjän numeron saa selville katso-  
malla jokaisen käyttäjän lähdekoodista. Lähdekoodin näkyville saaminen eroaa hieman jokaisessa  
selaimessa. Firefoxissa ja Chromessa lähdekoodin saa näkyviin klikkaamalla hiiren oikealla näp-  
päimellä "näytä sivun lähdekoodi". Selaimessa etsi kohta "userID". Esimerkiksi Mark Zuckerbergin  
lähdekoodia tarkastelemalla löytyy "userID": "4"

On myös mahdollista etsiä käyttäjän käyttäjännumero internetistä löytyvillä hakukoneilla, kuten:

<https://fb-search.com/find-my-facebook-id>

<https://findidfb.com/>

<https://lookup-id.com/>

(Bazzell 2021, 224.)

### 5.3 Facebookin Base64 koodaus

Haettaessa käyttäjän julkaisemia kuvia täytyy käyttää kaavaa ja URL osoitetta:

<https://facebook.com/search/photos/?q=photos&epa=FILTERS&filters=>

Osoite muodostuu seuraavista osioista:

<a href="https://facebook.com/">https://facebook.com/</a>	The Facebookin internetdomain
search/	Ohjeistaa Facebookin suorittamaan haun
Photos/	Tarkentaa halutun informaation tyyppin
?q=photos	Hakee kaikki kuvat (on myös mahdollista hakea postauksia tai videoita)
&epa=FILTERS&filters=	Päättää URL:n tarvittavalla filterillä (Bazzell 2021, 225.)

Seuraavaksi tavoiteltu data täytyy muotoilla ja vaihtaa se Base64 koodaukseksi. Base64 koodaus  
on erittäin yleinen ja voidaan generoida millä browserilla tahansa. (Bazzell 2021, 225.)

```
{"rp_author": {"name": "author", "args": "4"}}
```

Kyseinen komento kertoo Facebookille, että etsitään tietoa tietyltä käyttäjäprofiililta (julkaisija) ja numero 4 on profiilin numero. Tämä komento täytyy purkaa Base64:ksi. Sen voi tehdä muun muassa osoitteessa: <https://codebeautify.org/base64-encode>. Data muutettuna Base64:ksi on:

*eyJycF9hdXRob3liOiJ7XCJuYX'11XCI6XCJhdXRob3JclixcimFyZ3Ncipcij Rcin0ifQ==*

Kaksi viimeistä “==” ovat vapaavalintaisia, eivät pakollisia. Kun syötetään saatu base64 URL osoitteen jatkoksi saadaan seuraava URL osoite:

<https://www.facebook.com/search/photos/?q=photos&epa=FILTERS&filters=eyJycF9hdXRob3liOiJ7XCJuYX'11XCI6XCJhdXRob3JclixcimFyZ3NcipcijRcin0ifQ>

Kyseisellä URL osoitteella on mahdollista nähdä Mark Zuckerbergin julkaisemat kuvat.

(Bazzell 2021, 225–227.)

Muita hyödyllisiä ja yleisimpiä URL tiedusteluja ovat

Posts by User/Year:	Julkaisut spesifiltä käyttäjältä kaikilta sivuilta (vuosiluvulla suodatettuna)
Photos by User/Year:	Kuvat spesifiltä käyttäjältä kaikilta sivuilta (vuosiluvulla suodatettuna)
Videos by User/Year:	Videot spesifiltä käyttäjältä kaikilta sivuilta (vuosiluvulla suodatettuna)
Posts by Location/Year:	Spesifistä sijainnista tehdyt julkaisut (vuosiluvulla suodatettuna)
Photos by Location/Year:	Spesifistä sijainnista julkaistut kuvat (vuosiluvulla suodatettuna)
Videos by Location/Year:	Spesifistä sijainnista julkaistut videot (vuosiluvulla suodatettuna)

(Bazzell 2021, 228.)

#### 5.4 Twitter (twitter.com)

Twitterin etusivulle tulee heti ensimmäisenä kirjautumisvaihtoehto ilman muita hakukenttiä. Sen takia, jos hakee tietoa Twitteristä ilman kirjautumista, pitää mennä suoraan osoitteeseen



twitter.com/explore. Näin saat itsellesi näkyviin perusmuotoisen hakukentän, joka ei eroa oikeastaan muista normaaleista hakukentistä millään tavalla. (Bazzell 2021, 241.)

Tarkennetun haun Twitterissä, ilman sisäänkirjautumista, saa osoitteella [twitter.com/search-advanced](https://twitter.com/search-advanced). Näin saat rajattua hakuasi esimerkiksi tiettyihin käyttäjiin, avainsanoihin, paikkoihin tai vaikkapa lausahduksiin. Tämän tarkennetun haun huono puoli on se, että se yleensä rajautuu vain tuoreimpiin "twiitteihin" eli noin seitsemästä kymmeneen päivään vanhoihin twiitteihin. Tämä haku on hyvä tapa hakea tuoretta tietoa, mutta jos tarvitsee päästä koluamaan Twitterin arkistojen helmiä, ilman sisään kirjautumista se ei onnistu. (Bazzell 2021, 241.)

Twitterin erona muihin sosiaalisiin medioihin on se, että ihmiset harvoin käyttävät Twitterin käyttäjänimenä omaa nimeään. Sen takia oman kohdehenkilön hakeminen ilman tiedossa olevaa käyttäjätunnusta voi olla haastavaa (Bazzell 2021, 241.) Ilman sisäänkirjautumista voi yrittää normaalin haun ([twitter.com/explore](https://twitter.com/explore)) tai tarkennetun haun ([twitter.com/search-advanced](https://twitter.com/search-advanced)) kautta. Kolmantena vaihtoehtona on mennä Twitter Directoryyn ([twitter.com/i/directory/profiles](https://twitter.com/i/directory/profiles)), jonka kautta voi aakkosjärjestyksessä hakea käyttäjätunnuksia (Bazzell 2021, 241). Ensimmäisenä kannattaa yrittää hakea kohdehenkilön muiden sosiaalisen medioiden käyttäjätunnuksia, jonka jälkeen lähteä etsimään vasta directoryn kautta (Bazzell 2021, 246).

Seuraavaksi käydään läpi, miten hakea twiittejä tietystä paikasta. Twitter mahdollistaa hakuja GPS-koordinaattien perusteella ja vielä enemmänkin. Oletetaan, että tiedät jonkin kyseisen paikan, josta hakea twiittejä. Selvität kyseisen paikan GPS-koordinaatit ja alueen säteeksi määrittelet yhden kilometrin. Kyseisellä haullla Twitter näyttää kaikki twiitit, jotka ovat julkaistu yhden kilometrin säteellä kyseisistä koordinaateista. Säteen mitan voi määrittää myös 5, 10 tai 25 kilometriä, jolloin haku on vielä tarkka. Muut kilometrimäärät antavat vääriä hakutuloksia (Bazzell 2021, 246).

Tarkennettuna hakuja voit lisäksi käyttää hakusanaa, esimerkiksi "fight", jolloin hakutuloksissa on mainittuna kyseinen sana. Jos käyttää hakusanaa, silloin ainut välilyönti osoitekenttään tulee "km" ja "fight" sanan väliin, muuten koko osoite kirjoitetaan yhteen. Kyseisen haun osoitekenttään muodostuisi siis seuraava osoite, kun haetaan koordinaateilla: 43.430242, 89.736459, kilometrin säteellä kyseisistä koordinaateista ja hakusanalla "fight":

[twitter.com/search?q=geocode:43.430242,-89.736459,1km "fight"](https://twitter.com/search?q=geocode:43.430242,-89.736459,1km%20fight) (Bazzell 2021, 246.)

Kun Twitterissä haluaa hakea tietyn käyttäjän lähettämiä tai saamia twiittejä, tarvitsee käyttää "from" "to" hakua. Esimerkiksi käyttäjältä SultryAsian käyttäjälle HydeNS533k. Haku kirjoitetaan Twitterin normaaliin hakukenttään seuraavasti: `from:sultryasian to:hydens533k`. Tätä hakua voi käyttää myös pelkästään joko "from" tai "to" hauilla, jolloin hakutulokset näyttävät joko vain kyseisen käyttäjän lähettämät twiitit tai kyseiselle käyttäjälle osoitetut twiitit. (Bazzell 2021, 245.)

Edellä mainittua hakua voi muokata niin, että saa aikavälin laitettua, jolloin twiitit on lähetetty. Esimerkiksi 1.1.2015 ja 5.1.2015 aikavälillä lähetetyt twiitit Humanhacker käyttäjältä menisi seuraavasti, "from:humanhacker since:2015.1.1 until:2015.1.5". Hakua voi myös rajata esimerkiksi hakusanoihin tietyllä aikavälillä, esimerkiksi "Bomb threat" since:2015.1.1 until:2015.5.1", jolloin hakutulokset olisivat kyseisenä aikavälillä twiitattuja, joissa on sanat "bomb threat". (Bazzell 2021, 247.)

Twitterissä toimii myös heittomerkeillä haku, eli pakolliset sanat, niin kuin edellisesti esimerkistä näimme. Twitterissä toimii myös OR hakutoiminto, jolla pystyy valitsemaan useita eri hakusanoja esimerkiksi selvittämään uhkailuja jotain henkilöä kohtaan. "Michael Parker" kill OR stab OR fight OR beat OR punch OR death OR die (Bazzell 2021, 246.) Kyseinen haku antaa Twitterissä hakutuloksiksi ne twiitit, joissa on mainittu henkilö Michael Parker sekä jokin edellä listatuista sanoista OR sanalla eriteltyinä. Kaikki edelliset hakutyylit voi yhdistää, jolloin hakutulokset tiivistyvät entisestään ja antavat mahdollisesti nopeammin tarkempia haluttuja tuloksia tai vaihtoehtoisesti rajaa joitain tuloksia pois, jotka voisivat olla hyödyllisiä tutkimukselle.

## 5.5 Instagram (intagram.com)

Viimeisten vuosien aikana Instagram on tiukentanut tietosuojansa, joka on johtanut siihen, että useat hyödylliset sivustot ja tavat OSINT:in kannalta eivät toimi nykyään. Siitä huolimatta Instagramistakin voi löytyä paljonkin hyödyllistä tietoa oikeilla tavoilla etsittäessä. Instagramin omat hakuvaihtoehdot ovat hyvinkin rajattuja, ja siksi Bazzell ei suosittele käyttämään Instagramin omaa hakukenttää. (Bazzell 2021, 271.)

Käyttämällä muita hakukoneita, kuten Google, saa huomattavasti enemmän hakutuloksia kohteelle. Googlea käyttäessä, pitää muistaa Googlen hakutavat. Pelkästään Instagramista haettavia tuloksia halutessaan, pitää Googlen haussa käyttää kyselyn alussa "site: instagram.com" kyselyä, rajatakseen hakutulokset vain Instagramin sivustolle. Tämän haun perään voikin sitten kirjoittaa joko lainausmerkkejä käyttäen tietyn sanan tai mitä tahansa muu onkaan tiedustelun kohteena, myös ilman lainausmerkkejä. (Bazzell 2021, 272.)

Voit hakea esimerkiksi tietylle käyttäjätunnukselle kohdistettuja julkaisua Googlestä rajaamalla haku seuraavanlaisesti:

Site: instagram.com " @hak5darren"

Näin saat hakutulokset, joissa on mainittu kyseinen profiili, joka voi olla viranomaistoiminnassa monessakin eri tapauksessa hyödyllistä.

Instagramin pienet profiilikuvat ovat aina kooltaan 150x150 pikseliä. Lataamalla ne kuvat, saa vain todella paljon pakatut tiedostot eikä kuva suurene. (Bazzell 2021, 274.) On tapoja, joilla saa kuvan

suurennettua itse monen mutkan kautta, mutta sitä ei käydä tässä läpi, koska löytyy myös helpompia tapoja. Helpommat tavat saada pieni profiilikuva tunnistettavaksi kuvaksi, on käyttää valmiita sivustoja.

downloadgram.com

dinsta.com/ photos

instadp.org

gramsave.com

gramv10.com

instadownloader.co

instafollowers.co

instaoffline.net

Instagramissa kuka tahansa voi vaihtaa käyttäjänimensä, mutta profiilin sivun lähteessä säilyy aina sama käyttäjännumero. Käyttäjännumero on hyvä tarkastaa, jos kuvia on tarkoitus käyttää virallisesti. Samalla sivun lähteestä on nopea myös tarkastaa kuvan latausaika, sekunnin tarkkuudella. Käyttäjännumero löytyy sivun lähteestä "Owner :{" ja tämän sulun jälkeen oleva numerosarja on käyttäjän id-tunnus. Instagram ilmoittaa kylläkin kuvan latauspäivämäärän, mutta ei aikaa. Joten samalla sivun lähteestä kannattaa tarkistaa aika seuraavasti. "taken\_at\_timestamp" Tämä antaa sinulle uniikin numerosarjan, josta aikaa ei suoraan voi havaita. Siirtämällä kyseinen numerosarja sivustolle "epochconverter.com" saat näkyviin sekunnilleen kellonajan, kun kuva on ladattu palvelimelle. (Bazzell 2021, 275) Nämä tiedot eivät anna paljoa lisätietoa OSINT:in näkökulmasta, mutta viranomaistoiminnassa on erittäin tärkeää saada kerättyä mahdollisesti näyttöä ja käyttäjä ID-numerolla sekä tarkalla latauskellonajalla voi olla suuri merkitys. Tarkan kellonajan voi myös hakea kommentista. Kellonaika löytyy myös sivun lähteestä, hakemalla kyseinen kommentti ja sen perässä luettava teksti "created\_at: numerosarja". Kyseinen numerosarja siirretään taas edellä mainitulle sivustolle, ja näin saat sekunnin tarkkuudella kommentin päivämäärän ja kellonajan. (Bazzell 2021, 277.)

Kuten edellä jo mainittu, Instagramin omat hakuvaihtoehdot ovat hyvinkin suppeita ja vähäisiä. Instagramista haettaessa tietoa kannattaakin tukeutua muihin hakukoneisiin ja niiden erikoisuuksiin, kuten Googleen. Google Chromeen on myös saatavilla hyvä lisäohjelma, jolla pystyt lataamaan tiedostot ja kuvat pakattuna tiedostona itsellesi. Tiedosto on "Downloader for Instagram, ja se löytyy osoitteesta <https://chrome.google.com/webstore>. (Bazzell 2021, 282.)

## 5.6 LinkedIn (linkedin.com)

LinkedIn palvelussa on oman palvelimen takaa jo hyvät rajatut hakuvaihtoehdot. LinkedIn antaa käyttäjän rajata hakuaan seitsemällä eri rajauksella. *Henkilöt, julkaisut, yhtiöt, työt, koulut ja*

*tapahtumat*. LinkedIn keskittyy yritysmaailmaan ja verkostoitumiseen, sen takia palvelussa vallitsee yleisesti hyvin luottamuksellinen ja asiallinen yleishenki. Tämä johtaa siihen, että käyttäjät päivittävät profiiliaan useasti ajantasaiseksi, mahdollisine ajantasaisin yhteystietoineen ja kuvineen. Sivustolta löytää myös usein henkilön koko työ- ja opiskeluhistorian, pätevyyksineen. Tämän takia LinkedIn on erinomainen esimerkiksi henkilön taustatarkistuksia varten. (Bazzell 2021, 286–287.)

LinkedIn, niin kuin muutkin sosiaaliset mediat, näyttää suuren osan sisällöstään vain käyttäjilleen. LinkedIn on myös siitä erilainen, että pitää olla oikeat kontaktit, jotta pystyy nähdä joidenkin käyttäjien tietoja. Tämän pystyy kuitenkin kiertämään käyttämällä erillisiä hakukoneita, esimerkiksi Googlea. Jos tiedät kohdehenkilöstäsi joitain tietoja, voit käyttää taas Googlen rajattua hakua: "Site: LinkedIn.com" ja kirjoittaa perään minkä tiedon pohjalta lähdet etsimään lisää tietoa, esimerkiksi kohteen ammatti hänen työpaikallaan "Account Executive at Uber". Näin pystyt kiertämään osan estoista ja nähdä profiileista enemmän tietoa, kuin menemällä esimerkiksi suoraan Uberin virallisen sivuston kautta käyttäjän profiiliin. (Bazzell 2021, 289–292.)

## 5.7 Snapchat (snapchat.com)

Snapchat on pääsääntöisesti puhelimille kehitetty sovellus, jolla ei ole varsinaisia internet-sivustoja, joista hakea tietoa OSINT tarkoituksessa. Joitakin lisäyksiä on tullut vuosien saatossa, mutta nekin hyvin suppeita. Selaimella pystyy hakemaan esimerkiksi *avainsana haulla*, *Snapchat-tarinoita*, *käyttäjätunnuksia* ja *Snapchat karttaa*. (Bazzell 2021, 294.)

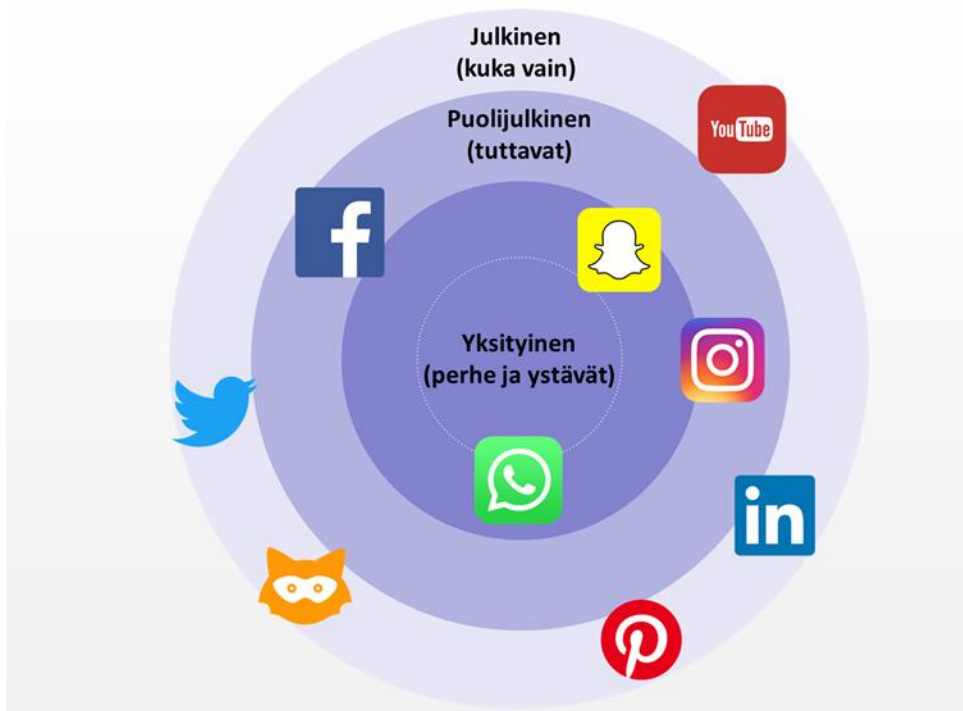
Avainsanahaulla (<https://story.snapchat.com/search?q=haettava> sana) haetaan tiettyä sanaa koko Snapchat palvelusta. Haku usein osoittautuu epäonnistuneeksi, mutta on kokeilemisen arvoinen, koska tulokset saattavat olla hyvinkin hyödyllisiä. Snapchat-tarinoita (<https://story.snapchat.com/s/haettavan> käyttäjän käyttäjätunnus) voi hakea, jolloin näkee tuoreimmat tarinat tietyltä käyttäjältä, jotka ovat asetettu julkisiksi. Käyttäjätunnushaulla (<https://www.snapchat.com/s/haettavan> käyttäjän käyttäjätunnus) voi hakea tietyn käyttäjän tunnusta, mutta tämä haku voi johtaa suoraan myös Snapchat-tarina hakuun. Snapchat-karttaa selailemalla ([map.snapchat.com](https://map.snapchat.com)), voi nähdä julkiset tarinat ja paikat mistä ne ovat julkaistu. Kartasta voi olla hyötyä, jos seuraa isoja tapahtumia tai kokoontumisia. (Bazzell 2021, 294.)

On olemassa myös sivustoja, jotka tarjoavat OSINT-toimintoja Snapchatissä. Sivustot katoavat yleensä nopeasti tai vaihtavat nimeä. Sivustot eivät myöskään tarjoa kaikkea dataa, vaan ovat kehitettyjä joitakin tiettyjä toimintoja varten. Hakemalla hakukoneilla "Snapchat search users" löytää parhaiten sen hetkiset aktiiviset sivustot, joista voi yrittää hakea tietoa. Snapchat on yleisesti ottaen hyvin yksityinen ja erittäin hankala lähde etsiä tietoa OSINT-menetelmillä. (Bazzell 2021, 295.)

## 6 YHTEISÖT

Seuraavaksi käsittelemme muutamia internetin sosiaalisia yhteisöjä. Miksi olemme jakaneet osiot kahteen eri lukuun, sosiaaliseen mediaan ja sosiaalisiin yhteisöihin vaikkakin kaikki ovat osiltaan sosiaalisia medioita. Syy tähän on se, että palvelut, jotka olemme laittaneet sosiaalisen median alle, on erittäin suuria ja niitä käyttää kaiken ikäiset ihmiset, kaikista taustoista tulevat, missä maassa tahansa, mihin tarkoitukseen tahansa. Sosiaaliset yhteisöt ovat enemmänkin palveluita, jotka ovat joko paljon pienempiä tai niiden käyttäjät ovat iältään rajattuja tai muutoin elämän tilanteeltaan rajattuja. Kokonaisuudessaan yhteisöt ovat jollain tapaa enemmän rajattuja johonkin tiettyyn kategoriaan tai kohdeyleisöön (Bazzell 2021, 305).

Alla olevassa havainnollistavassa kuvassa neljä, havainnollistetaan miten yhteisöt eroavat sosiaalisesta mediasta. Yhteisöt ovat lähinnä julkisia, eli kenelle vain avoimia. Sosiaalisen median alustat ovat joko puolijulkisia (käyttäjä itse valitsee sen, kenelle sisältö näkyy), julkisia, tai yksityisiä. Yksityisiin sosiaalisiin medioihin luokitellaan sellaiset alustat, joiden sisältä on tarkoitettu vain hyvin rajatulle yleisölle, esimerkiksi viestintä sovellus WhatsApp.



Somepalvelut on sijoitettu kuvaan niiden tyypillisen käyttötavan mukaan. Vrt. Dunbarin sosiaaliset piirit: 5, 15, 50, 150.  
Datan lähde: AudienceProject Insights 2020, App & Social media usage, suomalaiset vastaajat (n. 2000, 15-75-vuotiaat)

Kuva 4. Sosiaalisten medioiden alustojen luokittelu niiden tyypillisen julkisuustason mukaan.  
Lähde: Innowise. Sosiaalisen median käyttö Suomessa: somekatsaus 04/2021.

Esimerkiksi Tiktok on suuren suosion saanut nuorempien keskuudessa, mutta vanhemmat ihmiset eivät ole vielä kovinkaan suuri käyttäjäryhmä. Tiktok ei ole yllä olevassa havainnollistavassa

kuvassa, mutta Tiktok sijaitisi kuvassa julkisen ympyrän alueella. Tinder taas on karkeasti ajateltuna, pääsääntöisesti sinkkuja täynnä, joka luonnollisesti erottelee parisuhteessa olevat pois. Tinder sijaitisi yllä olevassa kuvassa puolijulkisen ja julkisen välimaastossa. Discordin ajatellaan olevan nykyään rikollisuuden, tarkemmin ottaen kyberrikollisten suosiossa, ja sijaitisi kuvassa puolijulkisen alueella.

## 6.1 Reddit (reddit.com)

Redditin hakukenttä on parantunut viime vuosien saatossa, ja nykyään se on kohtuullisen hyvä. Redditin ominaispiirteitä on se, että käyttäjät pystyvät poistamaan kommentteja, jotka ovat ristiriidassa oman alkuperäisen julkaisunsa kanssa. Onneksi Redditissä on mahdollista hakea myös niin kutsuttu arkisto esiin ja nähdä poistettu sisältö.

Redditistä poistettu sisältö voidaan nähdä sivun lähteessä esimerkiksi käyttäjän inteltechniques tuhat viimeisintä kommenttia, poistetut tai olemassa olevat:

*<https://api.pushshift.io/reddit/search/comment/?author=inteltechniques&sort=asc&size=1000>*.

Viimeisimpien kommenttien määrää voi itse muuttaa, vaihtamalla URL osoitteen perässä olevaa numeroa (1000) haluamakseen.

Muita poistettuja tietoja voi myös nähdä samaan tyyliin.

Tiettyä sanaa tai kommenttia, jolloin näkyy vain 25 viimeisintä: *<https://api.pushshift.io/reddit/search/comment/?=inteltechniques>*,

Kaventaakseen kyseisen haun tuloksia niin, että sama sana tai kommentti tulee esiin, mutta vain tietyn subredditin eli toisen käyttäjän toimesta:

*<https://api.pushshift.io/reddit/search/comment/?=inteltechniques&subreddit=privacy>*.

Jos haluaa rajata hakuaan tietylle käyttäjälle ja tietylle aikavälille, esimerkiksi 5–30 päivää ennen sinun suorittamaa hakua:

*<https://api.pushshift.io/reddit/search/comment/?author=inteltechniques&after=30d&before=Sd>*.

Kyseisillä linkeillä näkee siis vain kommentit. Jos haluaa nähdä muita kuin kommentteja, esimerkiksi viimeisimpiä tai poistettuja uusia lähetyksiä käyttäjältä inteltechniques, onnistuu se vaihtamalla URL osoitteesta sana "comment" sanaan "submission". (Bazzell 2021, 309.)

Internetissä on myös olemassa jo valmis toimiva Redditiin hakutyökalu (*redditsearch.io*), joka hakee vanhoja ja poistettua julkaisuja ja kommentteja. Haussa on omat kohtuullisen hyvinkin toimivat rajausmahdollisuudet. (Bazzell 2021, 305–310.)

Reddit on erittäin hyvä työkalu OSINT-toimintaan, juuri sen takia, että pystyy hakemaan vanhoja ja jo poistettuja julkaisuja sekä kommentteja. Sivun lähteestä myös näkee julkaisuajan, samalla tavalla kuin Instagramissa. Numerosarja syötetään edelleen samaiselle sivustolle, josta saat tarkan ajan sekunnilleen.

## 6.2 Tiktok (*tiktok.com*)

Tiktok on viimeisien vuosien saatossa tullut viraaliksi alustaksi, jossa voi jakaa erityyppisiä videoita. Tiktokissa ei ole laajaa hakukenttää suorittaa hakuja, mutta URL osoitteen kautta voi suorittaa yksinkertaisesti hakuja. Esimerkiksi tietyt käyttäjät ja tagit voi hakea Tiktokin oman haun kautta, tai suoraan URL osoitteeseen joko käyttäjätunnus ”<https://tiktok.com/@inteltechniques>” tai tagi ”<https://www.tiktok.com/tag/osint>” (Bazzell 2021, 314). Toisin sanoen ei siis suurta OSINT mahdollisuutta tätä kautta.

Google kuitenkin osoittaa hauissaan Tiktokin tulokset, joten Googlen käyttäminen on enemmän kuin suotavaa, jos lähdetään kohtuullisen tyhjältä pohjalta etsimään tietoa Tiktokista. Haku onnistuu perinteisellä tavalla:

”[site:tiktok.com osint](https://www.google.com/search?q=site:tiktok.com+osint)” tai suoraan URL osoitteistoon ”[google.com/search?q=site:tiktok.com+osint](https://www.google.com/search?q=site:tiktok.com+osint)”.

Kun kuitenkin löydät hakujesi jälkeen kohdehenkilösi tai henkilön, joka herättää mielenkiintoa, on hyvä avata sivun lähde. Sivun lähteestä löytää muutaman hyödyllisen tiedon, jotka kannattaa laittaa itselleen muistiin. Tiedoista löytää käyttäjän ID numeron (haulla: {”id”), joka on yksilöllinen ja aina sama. Sivulta löytää myös yksilöllisen nimen (haulla: *uniqueid*) sekä lempinimen (haulla: ”*nickname*”). Kaikkia näitä voi käyttää hyödyksi Google hauissa, joiden kautta voi löytyä julkaisuja, jotka ovat poistettuja tiktokista. Lempinimi on ainut, joka ei ole yksilöllinen ja on uudestaan käytettävissä, mutta id-numero ja yksilöllinen nimi on aina sama yhdellä käyttäjällä. (Bazzell 2021, 314.)

## 6.3 Tinder (*tinder.com*)

Jokaisella seuranhaku sivustolla on pääpiirteittäin samat asiat esillä. Yksi ominainen asia näiden sivustojen käyttäjille on myös se, että jos käyttäjä on yhdessä palvelussa, on hän myös todennäköisesti toisessakin seuranhakusivustolla (Bazzell 2021, 315).

Pääpiirteistä, piirteitä on kolme, jotka löytyvät jokaiselta sivustolta. Ensimmäinen piirre on jonkinlainen käyttäjänimi tai nimi. Käyttäjän nimi saattaa olla piilotettu muilta käyttäjiltä, mutta iso osa

näiden sivustojen käyttäjistä käyttää samaa käyttäjänimeä kuin jossain muussa palvelussa. Kannattaa siis etsiä käyttäjänimellä muista palveluista, niin voi löytää henkilön oikean nimen nopeastikin. Toisena piirteenä on tekstikenttä, johon voi kirjoittaa vapaan tekstin. Kyseinen teksti on usein kopioitu yhdeltä sivulta toiselle, joko kokonaan tai osittain. Tämän tekstin kopioimalla ja hakemalla kokonaan tai osittain, saattaa siis myös löytää henkilön oikeita profiileja tai profiileja muistakin palveluista kuin seuranhakupalveluista. Kolmantena yhtäläisyytenä on kuvat. Kuvat ovat myös yleensä myös useammassa palvelussa, kuin vain yhdellä seuranhakusivustolla. Tuntemattoman käyttäjän kuvia voi hakea käänteisellä kuvahaulla useasta eri hakukoneesta, joka usein myös johdattaa tämän kyseisen käyttäjän johonkin oikeaan sosiaalisen median profiiliin. (Bazzell 2021, 315–316.)

Tinder on tällä hetkellä suosituin seuranhakupalvelu. Tinder on pääsääntöisesti vain matkapuhelimilla käytettävissä, mutta viime vuosina on tullut mahdolliseksi kirjautua myös tietokoneella selaimen kautta palveluun. Palvelu on kuitenkin hyvin suojattu erilaisilta VPN palveluilta ym. Tämän takia suositellaan käyttämään matkapuhelinta, tarkemmin Androidin matkapuhelinta. iOSin käyttöjärjestelmissä on estoja GPS-paikannuksen muutoksille. (Bazzell 2021, 317.)

Tietokoneella kirjautuessa OSINT-tarkoituksessa Tinderiin, pitää kuitenkin noudattaa viiden askeleen reittiä ja olla kärsivällisyyttä onnistuakseen. Askeleet ovat:

1. Yhdistä tietokone avoimeen WIFI-verkkoon, ilman VPN palveluita käytössä, lähellä haluttua kohdetta.
2. Valitse kirjautumisvaihtoehdoista puhelinnumerolla.
3. Anna Google Voice puhelinnumero vahvistusta varten
4. Vahvista Google Voice puhelinnumeroon tullut tekstiviesti
5. Viimeistele kirjautumisesi kuvalla ja alias nimellä.

Tinderillä on hyvin tiukka kirjautumispolitiikka ja käyttäjiä estetään nopeasti, havaittuaan ne epäaidoiksi. Tämän takia on vaikeaa saada Tinder toimimaan halutulla tavalla tietokoneella. Puhelimella se toimii vain Android käyttöjärjestelmällä, lataamalla sovellus, joka näyttää väärän GPS-sijainnin Tinderille sekä vahvistettu käyttäjä Google Voice puhelinnumerolla. (Bazzell 2021, 316–318.)

Väärän profiilin tekeminen Tinderiin vaatii myös muuta. Et tietenkään voi käyttää mitä tahansa kuvia, sinulla pitää olla niihin oikeus. Yleiset kuvat verkosta tunnistetaan nopeasti vääräksi, joten sinun pitää saada jostain luvallisia kuvia käyttöösi, tarpeeksi monta. Esittely teksti pitää myös olla sopiva. Tyhjä on huono ja liika on liikaa. Juuri oikeanlaisia ja sinun toivomiasi kuvia saa pientä maksua vastaan osoitteesta *fiverr.com*. (Bazzell 2021, 318.)



## 6.4 Discord ([discord.com](https://discord.com))

Kuten aiemmin mainitsimme, Discord on nykyään tunnettu erityisesti kyberrikollisten käytössä olevana alustana. Discordissa käyttäjä voi luoda servereitä, joihin on määrittelemätön määrä pääsyjä. Pääsy serverille tapahtuu pyyntöjen kautta, suoraan URL-osoitteella. Kun käyttäjä pääsee jollekin Discordin serverille, on hänellä pääsy sen kyseisen serverin kaikkeen datahistoriaan. Discord luokitellaankin eräänlaiseksi ”pimeän verkon” lähteeksi, koska hakukoneet kuten Google ei tunnista Discordin servereitä. (Bazzell 2021, 319.)

Miten saada kutsu Discordin servereille? Kutsulinkkejä voi löytää muilta aiheeseen liittyviltä foorumeilta tai yksinkertaisesti kysymällä linkkiä johonkin serveriin. Sivustot, joista voi löytää jaettuja linkkejä on esimerkiksi *disboard.org*. Disboard on ilmainen sivusto, joka osoittaa avoimet kutsulinkit. Sivustolta voi hakea hakusanalla tiettyä aihepiiriä. Kutsulinkkejä voi jakaa kuka tahansa Discordin serverillä oleva käyttäjä. Jos Disboard sivuston kautta ei löydy aihepiirin linkkiä, voi kokeilla toista sivustoa, *discord.me*. (Bazzell 2021, 320.)

Discordin servereiltä pystyy tallentamaan kaiken tiedon omalle tietokoneelleen CSV tai HTML muodossa. Ensimmäiseksi pitää ladata Discord sovellus (<https://discord.com/download>), jonka jälkeen ladata sovelluksesta ”*DiscordChatExporter.zip*” tiedosto, joka sijaitsee osoitteessa ”<https://github.com/Tyrrrz/DiscordChatExporter/releases>”. Tämän jälkeen pitää molemmat ohjelmat avata ja kirjautua sisään Discord palveluun. Kirjautumisen jälkeen avata kohde serveri, jossa avata näppäinyhdistelmällä *Ctrl + Shift + I* ”*Discord developer options*”, josta edelleen avata ”*Applications*”. Tämän jälkeen valita ”*Local Storage*” kohdasta ”<https://discord.com>”. Valinnan jälkeen näppäinyhdistelmällä *Ctrl + R* avautuu ikkuna, jonka oikeassa laidassa on ”*Token*”, kopioida kyseinen avain ilman heittomerkkejä ja liittää se *DiscordChatExporter* ohjelmaan. Tämän jälkeen pitää valita haluttu serveri vasemmasta reunasta sekä haluttu kanava oikealta. Viimeisinä vaiheina pitää valita tallentamismuoto, esimerkiksi *CSV* tai *HTML* ja jättää päivämäärät tyhjäksi sekä valita tallentamispaikka ja tämän jälkeen ladata tiedot tietokoneelle. (Bazzell 2021, 320–321.)

Nyt olet ladannut koko serverin tiedot itsellesi, ja vaikka serveri todennäköisesti tämän jälkeen poistuu, niin olet saanut kaiken serverin historian tallennettua. Tämä pitää toistaa jokaiselle serverille, jonka tiedot haluat tallentaa itsellesi jatkotutkimuksia varten.

Samankaltaisia sivustoja kuin Discord löytyy, mutta Discord on kaikista suosituin sivusto. Varsinkin amatöörikyberrikollisten keskuudessa. Muut sivustot ovat *slack.com*, joka on suunnattu enemmän ammattilaisille. Muita sivustoja on *about.riot.im* ja *tox.chat*, jokaisella näillä sivustoilla on salattua viestintää ja parempaa yleistä turvallisuutta kuin Discordissa, mutta ovat myös vähemmän käytettyjä kuin Discord. (Bazzell 2021, 321.)

## 7 PRODUKTIN KUVAUS

Lähdimme suunnittelemaan opinnäytetyömme produktia siltä pohjalta, että saisimme tehtyä itse produktista mahdollisimman helposti luettavan ja ymmärrettävän. Halusimme oppaan pituudeksi maksimissaan viisi sivuisen, jotta opas näin ollen pysyy yksinkertaisena ja helposti lähestyttävänä. Oppaan suunnittelimme ja toteutimme Word-ohjelmalla. Oppaan alussa kerromme lyhyesti mitä oppaalla saavutetaan, ja mikä on sen tarkoitus sekä lyhyesti kertaamme poliisin verkossa suorittamaa yleisvalvontaa, jotta opasta voi myös käyttää irrallaan opinnäytetyön raporttiosuudesta. Oppaaseen loppujen lopuksi tuli kolme eri pääkohtaa. Ensimmäisenä kohtana on se, miten käyttäjän julkaisuja etsitään, jotka eivät välttämättä näy käyttäjän etusivulla. Toisena kohtana oppaassa on samalla periaatteella käyttäjän kuvien etsiminen ja kolmantena kohtana se, miten Facebookista voi hakea kuvassa näkyviä tekstejä.

Pikaoppaan tarkoituksena on auttaa poliiseja löytämään mahdollisimman hyvin tietoa avoimia tietolähteitä käyttäen. Valitsimme pikaoppaan alustaksi tarkoituksella Facebookin, koska se on eniten käytetty sosiaalisen median kanava Suomessa. Produktissa käydään vaihe vaiheelta ja kuvien avulla, miten saada tiedon hakemista kaiken mahdollisen hyödyn. Osa toiminnoista on itsestään selviä ja osa, taas suurimalle osalle käyttäjistä vähemmän tunnettuja. Facebookin käyttäjät voivat tehdä profiilistaan suljetun ja yksityisen, mutta iso osa Facebookin käyttäjistä eivät varmastikaan tiedä, mitä tietoja heistä löytyy. Pikaopas keskittyy käyttäjien julkaisuiden ja kuvien löytämiseen, mitkä eivät välttämättä näy kyseisen käyttäjäprofiilin etusivulla.

## 8 YHTEENVETO JA POHDINTA

### 8.1 Johtopäätökset ja kritiikki

Alkuperäisen suunnitelmamme mukaan, tutkielma oli tarkoitus tehdä avoimien tietolähteiden käytöstä poliisin suorittaman esitutkinnan aikana. Emme saaneet riittävästi haastatteluun tutkijoita, jotka käyttävät avoimia tietolähteitä työssään, päädyimme nykyiseen tutkimuslinjaan. Avoimet tietolähteet ja niiden tuoma suuri olemassa oleva tietomassa tuo niin rikollisille, kuin poliisillekin paljon uusia mahdollisuuksia ja täysin erilaisen toimintaympäristön. Perustuen tutkimuksen alkuperäisen suunnitelman epäonnistumiseen, avoimiin tietolähteisiin perustuvaa tiedustelua ja valvontaa tulisi poliisiorganisaatiossa kouluttaa enemmän jo poliisinperustutkinnon aikana sekä lisätä tietoisuutta varsinkin rikostorjunnassa työskentelevien keskuudessa.

Tietoverkkorikollisuus on ollut vuodesta toiseen kasvussa, mutta poliisin suorittama yleisvalvonta sekä avoimiin tietolähteisiin perustuva tiedustelu ja tiedon hakeminen ei tunnu olevan riittävällä tasolla. Osaltaan asiaan vaikuttaa mielestämme jo poliisin perustutkinnon aikana oleva vähäinen tieto ja koulutus aihepiirin ympärillä, osiltaan verkkoympäristön monimutkaisuus ja -muotoisuus sekä osiltaan lainsäädännön ja ohjeistuksen puutteellisuus yhdistettynä vähäisiin resursseihin ja juttupaineeseen rikostutkinnassa.

Suurin osa poliiseista tietää sosiaalisen median alustat sekä yleisimmät hakukoneet. Kysymys onkin siinä, että tietävätkö ja osaavatko, varsinkin rikostutkinnassa työskentelevät poliisit, käyttää hyödykseen palveluiden tarjoamia tarkennettuja hakuja, yhdistämällä hakutuloksia, hakemalla useasta eri lähteestä sekä hyödyntää keräämiään tietojaan rikostutkinnassa. Avoimet tietolähteet voivat olla varsinkin hyödyllisiä sellaisissa jutuissa, joissa ei lähtökohtaisesti ole mitään johtolankoja. Juttujen ei tarvitse olla suuria, mediaa kiinnostavia ja törkeitä rikoksia, mutta poliisi pystyisi avoimia tietolähteitä hyödyntäen mahdollisesti tarjoamaan yhdenvertaisempaa kohtelua koko Suomen kansalle, myös pienemmissä rikoksissa.

Kansalaiset käyvät verkossa paljon keskustelua lukemattomien eri aiheiden ympärillä, vuoden jokaisena päivänä. Verkko on jokaisen helposti anonyymisti kirjoitella ajatuksiaan, suunnitelmiaan ja tekojaan. Verkossa käydään myös paljon keskustelua isojen rikoskokonaisuuksien ympärillä, kansalaiset saattavat kirjoitella verkkoon sellaista tietoa, jota poliisilla ei ole eikä välttämättä muuta kautta pääsisi tiedon äärelle. Poliisin suorittamasta yleisvalvonnasta ja avoimiin tietolähteisiin perustuvasta tiedustelusta laajemmalla skaalalla olisi varmasti poliisille hyötyä rikosten selvittämisen taikka ennalta estämisen kannalta. Vaikka kansalaiset kirjoittavat yleiseen ns. perinteiseen verkkoon anonyymisti, kommentin kirjoittaja voi olla hyvinkin helposti paikannettavissa, myös täysin avoimin keinoin taikka tarpeen tullen poliisin toimivaltuuksilla. Kun kyse on Tor-verkosta, asia muuttuu, mutta asiaan perehtyneet asiantuntijat pääsisivät poliisissa, poliisin toimivaltuuksilla myös heidän jäljilleen tarvittaessa. Poliisi myös pystyy ennalta estämään tietoverkossa tapahtuvaa rikollisuutta sillä, että poliisi tiedottaa kansalaisia lyhyillä mutta ytimekkäillä tietopaketeilla, kunkin kansalaisen oman tietoverkkoturvallisuuden ja -käyttämisen huomioimalla.

## **8.2 Luotettavuuden arviointi**

Koko opinnäytetyöprosessi sujui yhteistyössä kohtuullisen jouhevasti, vaikkakin tutkimussuunnitelmamme vaihtui kesken tutkimuksen. Aloitimme opinnäytetyön varsinaisen tekemisen, tiedon keruun ja aikaisempien tutkimuksien lukemisen aihealueen ympäriltä työharjoittelujaksomme aikana, keväällä 2021. Valitsemamme aihe on ollut mielestämme kiinnostava jo ennen opinnäytteen tekemistä, mutta mielenkiintomme aiheeseen on kasvanut opinnäyteprosessin aikana. Tämän takia olemmekin kokeneet koko opinnäyteprosessin ja tutkimuksen tekemisen suurimmaksi osaksi

mielekkääksi. Sovimme heti prosessiin ryhdyttyämme selkeät aikataulutavoitteet, aina työn valmistumiseen asti. Prosessin aikana olemme molemmat oppineet paljon itse aihealueen ympäriltä, mutta myös tieteellisen tutkimuksen tekemisestä ja sen kirjoittamisesta. Saimme kerättyä työhön käytetyn aineiston kohtuullisen helposti ja nopeasti sekä aineiston keruussa karsimme paljon aiheita pois, samalla rajaamalla työtämme tarpeeksi tiiviiksi. Työmme edistyminen oli teoriapohjan jälkeen jonkin aikaa tauolla, koska yritimme löytää sopivia haastateltavia aiheeseen. Kun lopulta etsinnän lopputulos oli kiertänyt kehää henkilöltä toiselle, päätimme vaihtaa tutkimussuunnitelmaa toiminnalliseen opinnäytteeseen ja näin saimme opinnäytetyömme uudestaan käyntiin. Tämän jälkeen opinnäytetyö valmistuikin jouhevasti aina loppuun asti, suunnitellussa aikataulussa.

Kun vaihdoimme työmme toiminnalliseen opinnäytetyöhön, olimme yhtä mieltä siitä, että lopullisen produktin, eli oppaan, tulee olla mahdollisimman tiivis, helppo lukuinen ja käyttöinen sekä saatavuudeltaan helppo, mutta kuitenkin tarpeeksi kattava, että siitä olisi hyötyä sen lukijoille. Pidämmekin hyödyllisenä jo sitä, jos yksikin henkilö joka oppaan tai opinnäytetyön lukee, innostuu perehtymään asiaan enemmän ja mahdollisesti käyttää avoimia tietolähteitä hyödyksi omassa työssään. Näin tietoisuus avoimien tietolähteiden hyödyistä lähtee leviämään. Poliisilta toiselle, tutkijalta tutkijalle.

Päälähteenämme oli prosessin aikana Michael Bazzellin vuonna 2021 julkaisema teos Open Source Intelligence Techniques. Päätimme käyttää tätä teosta siksi, koska Bazzell on yksi maailman johtavista OSINT:in ammattilaisista ja kyseinen teos on ajantasainen tietoverkon alati muuttuvassa maailmassa. Tietoverkkoon liittyvät artikkelit, kirjallisuudet ja muut teokset vanhenevat nopeasti ja tieto ei ole enää paikkansapitävää, koska tekniikka kehittyy valtavaa vauhtia ja verkossa olevat palvelut muuttuvat välillä hyvinkin nopeasti. Hyödynsimme myös muita aikaisempia tutkimuksia aiheen ympäriltä sekä pyrimme käyttämään lähteitä vain sellaisia, joiden tieto ei ole ehtinyt vanhentua ja lähteestä saatua tietoa voi pitää luotettavana. Verkosta löytyy paljon artikkeleita aiheen ympäriltä, mutta tiedon luotettavuutta on hyvin vaikea arvioida, ellei tiedä varmaksi, kuka ja mistä kyseinen tieto on peräisin.

Yhteisöpalvelut eivät aina suhtaudu suotuisasti siihen, että niiden ohjelmistorajapintaa tai hakuominaisuuksia käytetään heidän mielestään sopimattomalla tavalla. Produktissamme toimivat neuvot toimivat opinnäytetyön julkaisun aikana, mutta opinnäytetyön kirjoitusprosessin aikana Facebookin omistama yritys vaihtoi nimensä Facebookista Metaksi. On siis hyvin todennäköistä, että produktimme neuvot, eivät toimi viiden vuoden päästä. Opinnäytetyön kirjoittamisen aikaan Facebook on käytetyin yhteisöpalvelu Suomessa, mutta se saattaa menettää asemansa suosituimpana yhteisöpalvelimenä.

### 8.3 Eettisyyden arviointi

Avoimien tietolähteiden käyttö viranomaistoiminnassa voi herättää ihmisissä paljonkin tunteita, kritiikkiä ja eriäviä mielipiteitä puolesta, sekä vastaan. Mielestämme avoimet tietolähteet ovat niimensä veroisesti avoimia tietolähteitä niin poliisille, muille viranomaisille kuin kenelle tahansa muul- lekin kansalaiselle. Jos tieto on avoimena ja laillisesti saatavilla verkosta, miksi se oli eettisesti väärin viranomaisen sitä tietoa hyödyntää. Toki, jos tieto on jonkinlaisen maksumuurin takana ja viranomainen joutuu maksamaan tietyn summan päästäkseen käsiksi tietoon, onko tiedon hankinta metodit olleet silloin eettisesti hyväksyttävää tai onko eettisesti oikein, jos viranomainen hyödyntää ostamalla jonkin palvelun kautta saatua tietoa? Näihin asioihin varmasti löytyy paljon hyviä puolesta ja vastaan argumentteja, mutta jos tieto on viranomaisen käsiin laillisesti päätynyt, ei siinä pitäisi olla eettisesti silloin mitään väärää myöskään hyödyntää viranomaistoiminnassa kyseistä tietoa. Tiedon luotettavuuden arviointi on asia erikseen. Viranomaisen pitää aina varmistaa tiedon luotettavuus, ennen kuin tietoa voidaan käyttää.

Poliisin verkossa suoritettavan yleisvalvonnan näkökulmasta mielestämme ei ole eettisesti mitään väärää, mutta jos poliisi on verkossa nimettömänä ns. ”valekäyttäjänimellä” eettisyyden arviointi muuttuu täysin. Onko eettisesti oikein, että kansalainen ei tiedä jonkin käyttäjän verkossa olevan poliisi suorittamassa virkatehtävää. Onko eettisesti oikein, että verkossa ei pysty tunnistamaan mahdollisesti kuka poliisi on käyttäjänimen takana eikä tätä pysty kansalainen itse yksilöimään? Poliisin verkossa suorittama yleisvalvonta on passiivista, onko se eettisesti oikein, että kansalainen ei välttämättä ymmärrä sitä, että poliisi valvoo myös verkossa tapahtuvaa keskustelua ja muuta liikennettä. Meidän näkemyksemme mukaan, se ei eettiseltä kannalta eroa siitä, että poliisi suorittaa liikennevalvontaa tunnuksittomalla virka-autolla mahdollisesti vielä ilman virkavaatetusta. Poliisilla ei ole velvollisuutta ilmoittaa jokaisesta suorittamastaan valvontatehtävästä, tapahtuu se verkossa tai liikenteessä. Poliisilla on kuitenkin velvollisuus toimia aina lain edellyttämällä tavalla sekä tietää, mihin ja minkälaisiin toimenpiteisiin on oikeutettu ja jopa velvoitettu virkansa puolesta aina erilaisissa toimintaympäristöissä.

Hallituksen esityksessä Eduskunnalle poliisilainsäädäntöä ja eräksi siihen liittyviksi laeiksi HE 224/2010 vp, on otettu kantaa siihen, miten poliisi voi toimia peitetehtävissä tietoverkkoympäristössä ja miten peitetehtävät kyseisessä ympäristössä suhteutetaan reaali maailman toimintaympäristöön ja siellä suoritettaviin peitetehtäviin. Hallituksen esityksessä on myös otettu kantaa perusteluineen siihen, millaisissa tilanteissa peitetoiminnan edellytykset tulisi saattaa tuomioistuimen ratkaistavaksi.

*”Tietoverkoissa tapahtuvalle ihmisten väliselle vuorovaikutukselle on luonteenomaista tietynlainen toimivien henkilöiden identiteettien epäselvyys. Tietoverkoissa käytetään esimerkiksi nimimerkkejä tai muita vastaavia henkilöiden yksilöintitapoja. Lisäksi tietoverkoissa tapahtuvan peitetoiminnan*

*dokumentointi on muuhun peitetoimintaan verrattuna helpompaa, joten peitetoiminnan toteuttamistapa on jälkikäteen tarkemmin selvitettävissä. Fyysiset työturvallisuusriskit puuttuvat tietoverkkoympäristöstä. Tämän vuoksi tietoverkoissa tapahtuvalle peitetoiminnalle ei tulisi asettaa yhtä tiukkoja edellytyksiä kuin reaali maailmassa toteutettavalle toiminnalle.” (HE 224/2010 vp, s. 46.)*

*”Momentissa säädettäisiin myös yksinomaan tietoverkossa tapahtuvaa peitetoimintaa koskevasta päätöksenteosta. Tällaisesta peitetoiminnasta päättäisi keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu virkamies.” (HE 224/2010 vp, s. 119.)*

*”...jos peitetoiminnalla saatua tietoa on tarkoitus käyttää oikeudenkäynnissä syyllisyyttä tukevana selvityksenä, peitetoiminnasta päättäneen poliisimiehen on saatettava tuomioistuimen ratkaistavaksi, olivatko 28 §:n 2 momentissa tarkoitettut peitetoiminnan edellytykset olemassa tai oliko kysymys peitetoiminnasta 3 §:ssä tarkoitetuissa tapauksissa... Yksinomaan tietoverkossa toteutettava peitetoiminta ei edellyttäisi tuomioistuimen ratkaisua.” (HE 224/2010 vp, s. 120.)*

#### **8.4 Jatkotutkimukset**

Opinnäytetyöprosessin aikana avoimien tietolähteiden käytöstä heräsi jatkotutkimus ajatuksia. Ideoita jatkotutkimuksille tuli henkilöiltä, joihin olimme prosessin aikana yhteydessä ja jotka ohjasivat ja auttoivat meitä prosessin aikana. Jatkotutkimuksista heräsi myös meille itse erilaisia ajatuksia, lähinnä siksi, että mielestämme aihetta tulisi tutkia mahdollisimman paljon, jotta siitä olisi konkreettisesti hyötyä poliisin toiminnalle.

Ensinäkin meidän mielestämme aihetta tulisi tutkia ja kartoittaa niin, että tiedetään minkälaisissa työtehtävissä poliisi käyttää avoimia tietolähteitä hyödyksi sekä se, että millaisella koulutuksella aiheeseen avoimia tietolähteitä käyttää hyödyksi. Toisena asiana meille itsellemme heräsi ajatus siitä, kuinka moni rikostutkija ymmärtää avoimien tietolähteiden potentiaalisen hyödyn tutkinnan apuvälineenä. Pitäisikö selvittää se, kuinka iso osa tutkijoista on tietoisia aiheesta, mutta eivät osaa hakea tietoa tehokkaasti taikka eivät tiedä mikä tieto on laillista hyödyntää viranomaistoiminnassa. Mielestämme aiheesta olisi hyvä tehdä myös jatkotutkimusta siitä näkökulmasta, onko poliisin perustutkintoa suorittavilla aiheesta tietoa, taitoa taikka onko heillä ylipäänsä kiinnostusta ja motivaatiota avoimien tietolähteiden hyödyntämiseen tiedonkeruussa viranomaistoiminnassa.

Opinnäytteen tekemisen aikana, muualta tulleita ajatuksia ja kiinnostavia näkökulmia mahdollisiin jatkotutkimuksiin tuli esimerkiksi siihen, että miten erilaisten sosiaalisten medioiden palveluiden käyttöehdot suhtautuvat viranomaisten harjoittamaan tiedonkeräämiseen, kun se tapahtuu avoimien tietolähteiden periaatteella? Mielestämme tulisi myös tehdä tutkimusta siitä, mitkä ovat ne rajavedot poliisin suorittamaan verkossa tapahtuvaan yleisvalvontaan aktiivisen ja passiivisen

toiminnan välillä, pitääkö poliisin virkatehtäviin verkossa käytettävän käyttäjätilin olla aina selvästi yksilöitäväksi tiettyyn poliisiin, riittääkö yleismalkaisesti selvästi erottuvaksi poliisin käyttäjätiliksi vai millä perusteilla poliisi voi suorittaa virkatehtäviään niin sanotusti ”valekäyttäjätilillä”, jota ei pysty yksilöidä poliisiksi. Lisäksi mielestämme tulisi tehdä tutkimusta siitä, miten sosiaalisten medioiden ohjelmointirajapintojen, valmiiden OSINT-työkalujen/ohjelmistojen hyödyntämistä viranomaistoiminnassa tiedonkeruun näkökulmasta arvioidaan lainsilmissä.

Yleisesti katsottuna, avoimien tietolähteiden tutkiminen viranomaistoiminnassa näkökulmasta riippumatta tulee olemaan hyödyllinen. Jokainen suoritettu tutkimus on pieni pala lisää kehittääkseen tietoverkkoympäristössä toimimista, erityisesti tutkimuksen tekijöille itselleen, mutta myös tulevaisuudessa heidän kollegoilleen, joiden kanssa he suorittavat yhteistyössä viranomaistoimintaa. Tietoverkkoympäristö poliisin toimintaympäristönä tulee vain tulevaisuudessa laajenemaan, yleistymään ja monimutkaistumaan, joten kansalaisten yhdenvertaisen kohtelun, oikeusturvan ja palvelun takaamiseksi poliisi ei saisi pudota tämän kehityksen kyydistä.

## LÄHTEET

Bazzell, Michael 2021: Open source intelligence techniques: Resources for searching and analyzing online information. Eight edition.

[www.facebook.com](http://www.facebook.com) Luettu 14.11.2021

Haikansalo, Anu & Korander, Timo 2021. Poliisi (AMK) -opinnäytetyön ohje. Tampere. Poliisiammattikorkeakoulu.

HE 224/2010. Hallituksen esitys Eduskunnalle poliisilaiksi ja eräiksi siihen liittyviksi laeiksi. Luettavissa: [https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he\\_224+2010.pdf](https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_224+2010.pdf) Luettu 18.10.2021

Innowise. Sosiaalisen median käyttö Suomessa: somekatsaus 04/2021. Luettavissa: <https://www.innowise.fi/fi/sosiaalisen-median-kaytto-suomessa-somekatsaus-04-2021/> Luettu 18.10.2021.

Laurio, Juha-Matti 2020: Talousrikosten tutkinta ja tutkintapyynnön laatiminen. Helsinki, Kauppa-kamari

Nurmi, Petri 2017: OSINT: avointen lähteiden Internet-tiedustelu. Helsinki. Aalto-yliopisto. Turvallisuusjohtamisen koulutusohjelma. Kehitysprojekti.

Poliisihallituksen kirje POL-2017-11225, 2017. Poliisihallituksen kirje verkkoympäristössä tapahtuvaan tiedonhankintaan liittyen.

Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö, kuva 4. 2020. Helsinki.

Tor-project 2019, Tor-verkon toimintaperiaate, kuva 2. Luettavissa: <https://2019.www.torproject.org/about/overview.html.en> Luettu: 18.10.2021.

Willner-Mäenpää, Daniela 2018: Tor-verkkoa hyödyntävä rikollisuus. Poliisiammattikorkeakoulu. mAMK-opinnäytetyö.



## **LIITE 1. PIKAOPAS POLIISILLE YLEISVALVONNAN TEKEMISEEN FACEBOOKIN AVULLA**

Janne Ruotsalainen & Jesse Raunama

## **LIITE 1: Pikaopas poliisille yleisvalvonnan tekemiseen Facebookin avulla.**

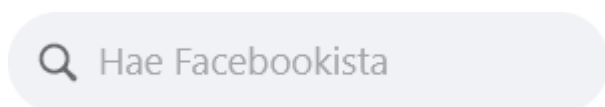
Tämän pikaoppaan tarkoituksena on auttaa poliisia suorittamaan yleisvalvontaa Facebookista. Facebook on edelleen Suomen käytetyin yhteisöpalvelu, ja ihmiset jakavat tiedostamattaan tietoa itsestään, vaikka he olisivat yrittäneet piilottaa tietoa suljetulla profiililla. Tämä pikaopas keskittyy julkaisuihin ja kuvien löytämiseen.

Poliisin suorittamasta yleisvalvonnasta ei ole erillistä lainsäädäntöä. Verkossa tapahtuvaan yleisvalvontaan on kuitenkin otettu kantaa nykyisen poliisilain esitöissä. Lain esitöiden mukaan, ei ole tarpeellista säätää erillistä toimivaltaa poliisille tähän tarkoitukseen, kun yleisvalvonta kohdistuu verkkoympäristön avoimiin tietolähteisiin ja poliisi suorittaa tarkkailua passiivisesti eikä aktiivisesti. (HE 224/2010 vp, s. 34.)

1. Kirjautu Facebookin osoitteessa [facebook.com](https://www.facebook.com)

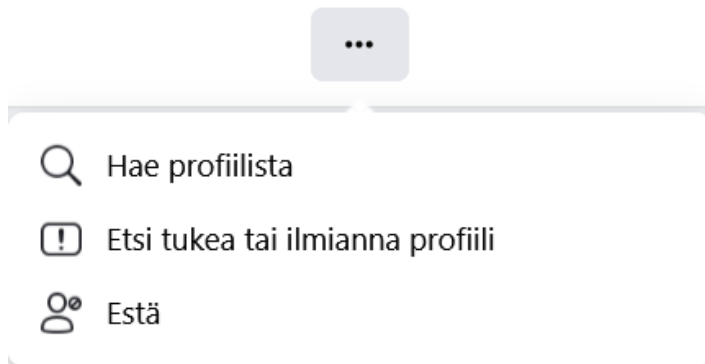
### **Julkaisuiden etsiminen**

2. Syötä henkilön nimi "Hae Facebookista" kohtaan.



Kuvakaappaus sivulta [facebook.com](https://www.facebook.com)

3. Tällöin oletuksena tulee näkyviin henkilön julkaisut ja perustiedot, joissa näkyy esimerkiksi:
  - Sukupuoli
  - Asuinpaikka
  - Perheenjäsenet, ystävät, siviilisääty
  - Koulutus ja työkokemus
  - Julkaisut
4. Jokaisesta Facebook käyttäjästä pystyy hakemaan tietoa klikkaamalla "..." kuvaketta. Tämän jälkeen valitse "Hae profiilista". Tällä tavalla pystyy hakemaan julkisia henkilöön päivityksiä, kuvia ja julkaisuja, jotka eivät välttämättä näy käyttäjän etusivulla.



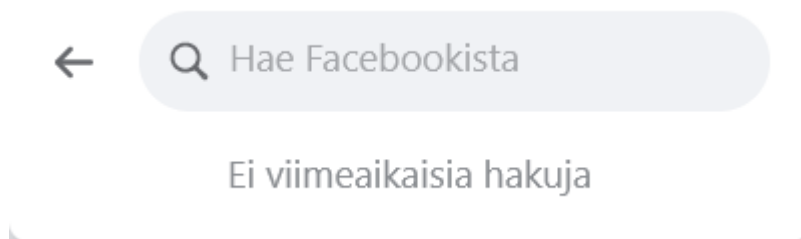
Kuvakaappaus sivulta facebook.com 14.11.2021

5. Kannattaa hakea henkilön etunimellä, sukunimellä ja näiden yhdistelmällä. Voi myös kokeilla hakea lempinimellä, nimimerkillä tai kiinnostuksen kohteilla.

### **Kuvien etsiminen**

On myös mahdollista löytää kuvia, jotka eivät näy henkilön profiilin etusivulla

1. Klikkaa Facebookin hakukenttää.



Kuvakaappaus sivulta facebook.com 14.11.2021

2. Kirjoita henkilön etu- ja sukunimi hakukenttään
3. Valitse vasemmasta reunasta "kuvat"



Kuvat

Julkaisija



Kuvan tyyppi



Merkitty sijainti



Julkaisupäivä



Kuvakaappaus sivulta facebook.com

4. Valitse "julkaisija" ja kirjoita henkilön etu- ja sukunimi kenttään. Tämän jälkeen ilmestyy muut mahdolliset julkiset kuvat.

#### Facebookin haku osaa myös hakea kuvassa näkyviä tekstejä.

1. Kirjoita hakukenttään haluttu teksti.



Hae Facebookista

Kuvakaappaus sivulta facebook.com

Valitse kuvat



Kuvat

Kuvakaappaus sivulta facebook.com

2. Valitsemalla sivun keskeltä kuvien alapuolelta "näytä kaikki" kuvaketta on mahdollista saada näkyviin lisää kuvia.

Näytä kaikki

Tämä toiminto erittäin kätevä varsinkin etsiessä avainsanalla.