Tor-selaimen käytön jättämät jäljet Windows 11 -laitteelle

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietojenkäsittelytiede
Joulukuu 2025
Hanna Kedonpää

TURUN YLIOPISTO
Tietotekniikan laitos

Hanna Kedonpää: Tor-selaimen käytön jättämät jäljet Windows 11 -laitteelle

TkK-tutkielma, 30 s.
Tietojenkäsittelytiede
Joulukuu 2025

Tor-selain on avoimen lähdekoodin selainohjelma, joka on erikoistunut peittämään käyttäjänsä toimia Internetissä. Kuitenkin myös Tor-selaimen käyttö jättää jälkiä sille päätelaitteelle, jolla sitä käytetään. Tässä tutkielmassa tarkastellaan, mitä jälkiä eli artefakteja selaimen käyttö jättää Windows 11 -laitteelle. Tutkittavia kohteita ovat laitteen rekisteri-, muisti- ja tallennustilan artefaktit.
Tutkielmassa tehdään kirjallisuuskatsaus tutkimuksista, joissa tarkastellaan Windows 11 -laitteelle jääviä Tor-selaimen artefakteja. Tuloksia täydennetään empiirisellä kokeella, jossa Tor-selainta käytetään virtuaalikoneella ja artefakteja etsitään kolmessa vaiheessa: selaimen ollessa käynnissä, selaimen sulkemisen jälkeen ja lopuksi selaimen poistamisen jälkeen. Tulokset osoittavat, että Tor-selaimen käytöstä jää jälkiä laitteen rekisteriin, muistiin ja tallennustilaan kaikissa kolmessa vaiheessa, vaikka jälkien määrä vähenee selaimen sulkemisen ja poistamisen jälkeen. Empiirisen kokeen tulokset osin vahvistavat ja osin haastavat aiempia tutkimustuloksia.
Kirjallisuuskatsauksen ja empiirisen kokeen tulosten perusteella suositellaan lisätutkimusta erityisesti sen selvittämiseksi, miten rekisterin, muistin ja tallennustilan eri analyysityökalut ja Tor-selaimen eri versiot vaikuttavat löydettävissä oleviin artefakteihin Windows 11 -laitteella. Valtaosa Tor-selaimen artefaktien tutkimuksesta keskittyy varhaisempiin Windows-versioihin, ja Windows 11 -versiota koskevien tutkimusten vähäinen määrä ja niiden osin erilaiset työkalut ja lähestymistavat rajoittavat tulosten vertailukelpoisuutta. Tutkielman tulokset kuitenkin täydentävät olemassa olevaa tutkimuskenttää ja luovat ajantasaisen kokonaiskuvan tässä vaiheessa vähän tutkitusta aiheesta.

Asiasanat: Tor-selain, digitaalinen forensiikka, muisti, rekisteri, tallennustila, tietoturva

Sisällys

1 Johdanto **1**

2 Tor-selain **5**

3 Windows-järjestelmän keskeiset forensiikka-alueet **8**

4 Tor-selaimen käytön jättämät artefaktit rekisteriin, muistiin ja tallennustilaan **12**

4.1 Pohdintaa 17

5 Tor-selaimen artefaktien empiirinen tarkastelu virtuaaliympäristössä **19**

5.1 Rekisteriartefaktit 21

5.2 Muistiartefaktit 22

5.3 Tallennustilan artefaktit 24

6 Lopuksi **29**

Lähdeluettelo **31**

1 Johdanto

Internet voidaan jakaa kolmeen osaan: pintaverkkoon (*World Wide Web*), syväverkkoon (*deep web*) ja pimeään verkkoon (*dark web*). Tavallisen Internetin selaajan käyttämä pintaverkko kattaa vain noin 4 % koko Internetin sisällöstä. Noin 90 % kuuluu syvään verkkoon, jonka sisältöjä tavalliset hakukoneet, kuten Google, eivät löydä. Jäljelle jäävä noin 6 % on pimeää verkkoa, jonka saavuttamiseen tarvitaan erikoistuneita selaimia, kuten Tor, I2P/ISP, Tails, Whonix tai Subgraph. Pimeän verkon kautta on mahdollista päästä käsiksi sellaisten sivustojen sisältöihin, joiden tarkan osoitteen tietää. Koska näiden sivustojen sisältö on salattua, ne yhdistetään usein rikolliseen toimintaan. [1]

Verkossa toimivat käyttäjät haluavat yhä useammin pysyä anonyymeinä esimerkiksi markkinapaikoilla, maksujärjestelmissä ja keskustelufoorumeilla. Tätä tarvetta varten on kehitetty anonymiteettiä suojelevia verkkoja, kuten avoimen lähdekoodin verkko Tor (*The Onion Routing*), joka suojaa käyttäjien henkilöllisyyttä ja verkkoyhteyttä salauksella. [1] Tor on anonymiteettiä suojelevista selaimista suosituin [2]. Tor-verkon kehittämisen päätarkoituksena oli mahdollistaa turvallinen viestintä julkisessa Internetissä yksityisyyden suojaamiseksi. Siitä tuli kuitenkin alusta myös laittomalle viestinnälle ja rikollisten suosima paikka ylläpitää kryptomarkkinoita, kuten Silk Road, Dream Market ja Dark Market. [3]

Useisiin selaimiin on lisätty yksityinen selaustila. Sen tavoitteena on, että selaimen käytöstä ei saa jäädä jälkiä, jotta voidaan estää paikallista tai verkon kautta

toimivaa hyökkääjää oppimasta käyttäjän selauskäyttäytymistä. Käyttäjän henkilöllisyyden täytyy myös pysyä piilossa sivustoilta, joilla hän vierailee. Kuitenkin muun muassa Chand ym. [4] ja Javed ym. [5] osoittavat, että myös anonymiteetistään tunnetun Tor-selaimen käytöstä voi jäädä päätelaitteelle jälkiä käyttäjän toiminnasta. Tämä heijastelee muun muassa Carveyn [6] esiin nostamaa, alun perin ranskalaisen kriminologi Edmond Locardin todistusperiaatetta, jonka mukaan jokainen kontakti jättää jäljen (*Every contact leaves a trace).*

Vaikka kaikki toiminnot Windows-järjestelmässä eivät jätä jälkiä helposti näkyvään paikkaan, hyödyllisiä tietoja on mahdollista löytää oikeita työkaluja käyttämällä ja tietämällä, mistä etsii. [6] Monissa tutkimuksissa onkin esitelty erilaisia menetelmiä arkaluonteisen tiedon keräämiseksi Windows-käyttöjärjestelmästä. Lopulta kyse ei ole vain teknisestä etsinnästä, vaan myös siitä, miten hajanaiset merkit laitteella muodostavat koherentin kertomuksen käyttäjän toiminnasta ja kuinka jälkiä tutkiva analyytikko kykenee yhdistämään sirpaleet kokonaisuudeksi, joka paljastaa enemmän kuin yksittäiset jäljet itsessään kertovat.

Jokaisen uuden Windows-version myötä käytettävissä näyttäisi olevan yhä enemmän jälkiä, joilla käyttäjän toimintaa laitteella voidaan jäljittää. Monet näistä jäljistä tallennetaan uusilla tavoilla ja eri paikkoihin: ei pelkästään rekisteriin, vaan koko tiedostojärjestelmään. [6] Voidaan päätellä, että uusien tallennustapojen ja jälkien lisääntyneen määrän ansiosta Windows 11 -laitteelle jääviä jälkiä on edelleen hyödyllistä tutkia. Lisäksi nopeasti kehittyvien tietotekniikan ja digitaalisen forensiikan alojen tutkijoiden on mukauduttava muutoksiin pysymällä ajan tasalla käyttöjärjestelmien kehityksestä ja työkaluista, mikä on Javedin ym. [5] mukaan ehdottoman tärkeää forensisten tutkimusten eheyden ja luotettavuuden takaamiseksi.

Tässä tutkielmassa tarkastellaan, mitä jälkiä Tor-selaimen käyttö voi jättää sille Windows 11 -laitteelle, jolla sitä käytetään. Tutkielmassa vastataan seuraavaan tutkimuskysymykseen:

TK1. Mitä jälkiä Tor-selaimen (versio 14.5.6) käytöstä jää Windows 11 -päätelaitteelle?

Tutkielma on rajattu vain Windows 11 -laitteelle jääviin jälkiin. Tor-selaimen jättämiä jälkiä tarkastellaan vain niissä tilanteissa, kun selain on asennettu suoraan laitteelle. Siten rajataan pois muun muassa Chandin ym. [4] esittelemä tilanne, jossa selainta käytetään siirrettävässä tilassa eli suoraan USB-tikulta.

Aineistoa haettiin Google Scholarilla, IEEE Xplorella, Science Directillä, Springer Linkillä ja UTU Volterilla, joiden kautta on löydettävissä runsaasti aineistoa tietoverkkojen turvallisuudesta ja digitaalisesta forensiikasta. Haut aloitettiin laajasti osumia antaneilla hakulauseilla, kuten "Tor browser forensics"ja "Windows forensics". Hakusanojen yhdistely AND- ja OR-sanoilla rajasivat löydettyä aineistoa tutkielman kannalta relevantimmaksi, etenkin, kun lopuksi hakusanojen joukkoon lisättiin "Windows 11", sillä siitä on Windowsin uusimpana versiona vähemmän tutkimusta kuin aiemmista versioista.

Hakutuloksia rajattiin suomeksi tai englanniksi kirjoitettuihin teoksiin, tieteellisiin artikkeleihin, väitöskirjoihin ja konferenssijulkaisuihin rajaten pois pro gradu -tutkielmat. Tutkielman kannalta keskeisimmät lähteet rajattiin vuosille 2021–2025, sillä viidessä vuodessa sekä Windowsiin että Tor-selaimeen on tullut useita päivityksiä. Lisäksi Windows 11 julkaistiin vuonna 2021. Muina lähteinä on käytetty myös vuotta 2021 vanhempia julkaisuja, joissa Tor-selaimen artefakteja tutkitaan aiemmissa Windows-versioissa. Erilaisilla hakulauseilla saatujen hakutulosten määrä on esitetty Taulukossa 1.1.

Hakutuloksia rajattiin tarkastelemalla löydettyjä otsikoita ja abstrakteja. Erityisesti etsittiin lähteitä, joissa käsitellään Tor-selaimen jättämiä jälkiä laitteen rekisteriin, muistiin ja tallennustilaan. Lopulta muotoutui kolme keskeistä lähdettä, jotka ovat kaikki vuosilta 2023–2025 ja joissa tarkastellaan Tor-selaimen käytön jättämiä

Taulukko 1.1: Hakutulosten määrä eri hakulauseilla

	Google Scholar	IEEE Xplore	Science Direct	Springer Link	UTU Volter
"Tor browser"AND forensics AND Windows	592	2	27	20	5
"Tor browser"AND artefacts(/artifacts) AND Windows	328	2	21	14	5
"Tor browser"AND "Windows 11"	72	1	4	4	0

jälkiä Windows 11 -laitteelle.

Luku 2 esittelee Tor-selaimen ja siihen liittyvän Tor-verkon perusominaisuuksia ja käyttötarkoituksia. Luvussa 3 perehdytään Windowsin keskeisiin forensiikka-alueisiin: rekisteriin, muistiin ja tallennustilaan. Näistä kaikista voidaan voidaan löytää käyttäjän toiminnasta jääneitä artefakteja laitteella. Luku 4 esittelee, mitä Tor-selaimen käyttöön liittyviä artefakteja tutkimuskirjallisuudessa on löydetty Windows 11 -laitteilta. Luvussa 5 tuodaan esiin empiirisessä kokeessa löydetyt Tor-selaimen artefaktit ja verrataan tuloksia tutkimuskirjallisuudessa esitettyihin tuloksiin. Luku 6 tiivistää keskeiset tutkimustulokset sekä tutkimuskirjallisuudesta että tämän tutkielman empiirisestä kokeesta ja esittelee mahdollista jatkotutkimustarvetta.

2 Tor-selain

Tor-selain on ilmainen ja avoimen lähdekoodin selainohjelma, joka perustuu Firefox-selaimeen. Sen erikoisuus on niin sanottu sipulireititys (*onion routing*), jossa kaikki verkkoliikenne salataan useaan kertaan ja kuljetetaan useiden eri palvelimien kautta. Näitä palvelimia ylläpitävät vapaaehtoiset ympäri maailmaa. [7]

Tor-selain tukee erityisiä onion-verkkosivuja, joita ei löydy tavallisilla selaimilla. Tällaisten verkkosivustojen osoitteissa käytetään .onion-päätettä, eivätkä sivustot näy julkisissa verkkosivurekistereissä. [1], [8] Tor-verkko tarjoaa anonymiteettiä vaihtamalla IP-osoitetta Tor-solmujen kautta, mikä on merkittävin syy siihen, miksi pimeässä verkossa tapahtuvan toiminnan tutkiminen on vaikeaa [3]. Koska viestin alkuperää ei voida jäljittää IP-osoitteen vaihtelun vuoksi Tor-solmujen kautta, rikollisille tämä tarjoaa kätevän keinon toimia internetissä anonyymisti käyttäen näitä alustoja laittomiin tarkoituksiin [9]. Samaa asiaa painottaa myös Chertoff [8], joka nostaa esiin IP-osoitteen keskeisen roolin kyberrikosten tutkinnassa. Tor-verkon tarjoama suoja tekee pimeästä verkosta suuren haasteen viranomaisille.

The Tor Project Foundationin verkkosivujen [7] mukaan Tor-verkko tarjoaa yksityisyyttä ja nimettömyyttä verkossa käyttämällä useita eri tekniikoita:

1. Käyttäjä ei yhdistä suoraan haluamaansa verkkosivuun, vaan yhteys kulkee ensin Tor-verkon kautta. Tämä piilottaa käyttäjän suoran yhteyden kohteeseen.

2. Lopullinen kohdesivusto ei näe käyttäjän oikeaa IP-osoitetta. Se näkee vain

yhden Tor-verkon välityspalvelimen IP-osoitteen.

3. Yhteys kulkee kolmen Tor-välityspalvelimen kautta. Tätä kutsutaan Tor-piiriksi. Ensimmäinen palvelin eli sisääntulosolmu tietää käyttäjän IP-osoitteen, mutta ei hänen lopullista kohdesivustoaan. Toinen välityspalvelin eli keskisolmu näkee vain, että tietoa siirtyy palvelimelta toiselle. Kolmas välityspalvelin eli poistumissolmu tietää, mikä on kohdeosoite, mutta ei käyttäjän alkuperäistä IP-osoitetta. Näin mikään yksittäinen palvelin ei saa kokonaiskuvaa.

4. Käyttäjän liikenne salataan useaan kerrokseen: yksi kerros jokaiselle välityspalvelimelle. Jokainen palvelin poistaa vain oman kerroksensa salauksesta, mikä muistuttaa sipulin kuorimista kerros kerrallaan. Tästä tulee nimi sipulireititys.

5. Koska Tor on avoin ja ilmainen kaikille, siihen osallistuu paljon käyttäjiä ja palvelimia. Tämä tekee verkon laajamittaisesta tarkkailusta ja liikenteen seuraamisesta hyvin vaikeaa.

Hallitusten, Internet-palveluntarjoajien ja yritysten on mahdollista estää Tor-verkon käyttö sulkemalla pääsy verkon sisääntulo- ja poistumissolmuihin, koska Tor-välityssolmujen hakemisto on julkisesti saatavilla. Erityiset siltasolmut (*bridge node*) kuitenkin auttavat kiertämään nämä rajoitukset, sillä osa siltasolmuista on piilotettuja, minkä vuoksi niiden IP-osoitteita ei pystytä tunnistamaan ja estämään. Kun käyttäjä lähettää verkkoliikennettä siltasolmulle, se lähetetään eteenpäin käyttäjän valitsemalle sisääntulosolmulle. Viestintä jatkuu tämän jälkeen normaalisti, mutta piilotettu siltasolmu on yksi lisäsolmu liikenteen reitillä ja toimii välityspisteenä. [10] Siltasolmut ovat siten tärkeä osa Tor-verkon yksityisyyden takaavaa infrastruktuuria erityisesti paikoissa, joissa valvonta ja sensuuri ovat laajamittaisia. Tor-verkkoa hyödyntävätkin monet eri tahot: yksityisyyttään varjelevat kansalaiset,

tietonsa kilpailijoilta salaavat yritykset sekä viranomaiset, jotka tarvitsevat toiminnalleen näkymättömyyttä. Myös ihmisoikeuksien puolustajat ja journalistit käyttävät Tor-verkkoa viestintään, jonka täytyy pysyä salassa ja suojattuna. [11] Läheskään kaikki Tor-verkon käyttö ei siten liity rikolliseen toimintaan.

3 Windows-järjestelmän keskeiset forensiikka-alueet

Windowsin keskeiset forensiikka-alueet ovat rekisteri, muisti (RAM) ja tallennustila. Kaikista niistä voidaan saada toisiaan täydentäviä tietoja käyttäjän toimista päätelaitteella.

Rekisteri. Windowsin rekisteri on hierarkkinen tietokanta, johon tallennetaan tietoa järjestelmästä. Sieltä voi löytyä esimerkiksi käyttäjätilejä, salasanoja ja salausavaimia. Forensiikan näkökulmasta rekisteriin tallennettu tieto voi olla tärkeä todiste, koska lähes jokainen tietokoneella tehty toimenpide tallentuu sinne. [12]

Javedin ym. [5] mukaan rekisteriforensiikka on olennainen vaihe Tor-artefaktien jäljittämisessä usein senkin jälkeen, kun selain on jo poistettu laitteelta. Huomautusta tarkentavat Arshad ym. [13]. He toteavat, että kun Tor-selain asennetaan, se luo rekisteriin useita merkintöjä, jotka liittyvät selaimeen ja sen asennusprosessiin. Näiden rekisteriavainten arvot voivat muuttua sen mukaan, onko selain avattu vai suljettu. Tämä on hyödyllistä, kun halutaan selvittää, onko käyttäjä vain asentanut Torin vai onko hän myös käyttänyt sitä. Sen sijaan nämä rekisterimerkinnät eivät paljasta, mitä sivustoja on selattu. Lisäksi rekisterimerkinnöistä voidaan selvittää, mitä ohjelmia on äskettäin käytetty. Nämä rekisteriavaimet säilyvät järjestelmässä vielä senkin jälkeen, kun Tor-selain on poistettu, mikä tukee Javedin ym. [5] näkemystä siitä, että rekisterin tutkimisesta on käyttäjän toiminnan jäljittämisessä

paljon hyötyä myös Tor-selaimen poistamisen jälkeen.

Arshadin ym. [13] mukaan Windowsin rekisteri toimii ikään kuin käyttöjärjestelmän muistikirjana, johon tallentuu tietoa ohjelmien käytöstä, käyttäjistä ja ajankohdista. Forensiikan näkökulmasta rekisteristä voidaan löytää vihjeitä siitä, kuka käytti konetta, mitä ohjelmia tai toimintoja suoritettiin, milloin nämä tapahtumat sattuivat ja missä kohtaa järjestelmää ne tapahtuivat. Tämä tieto voi auttaa yhdistämään tietyt toimet tiettyyn käyttäjään.

Rekisteriin on tallennettu paljon tietoa, joka auttaa käyttöjärjestelmää ja ohjelmia toimimaan oikein, eli se kertoo, mitä niiden pitäisi tehdä, mihin tallentaa tietoja ja miten reagoida eri tilanteissa. Rekisterin avulla voidaan esimerkiksi määrätä, että tietokone tyhjentää muistin vara- eli sivutustiedoston sammutettaessa. Kun Windowsissa ajetaan sovellus, kuten Pasianssi, se käyttää ensimmäisellä käynnistyskerralla oletusasetuksia esimerkiksi korttien jakotavassa ja pisteytyksessä. Käyttäjä voi muuttaa näitä asetuksia haluamallaan tavalla, kuten säätää pelin ikkunan kokoa ja sijaintia. Kun sovellus suljetaan ja tietokone sammutetaan, tehdyt muutokset säilyvät. Tämä johtuu siitä, että asetukset tallennetaan Windowsin rekisteriin. Seuraavalla käyttökerralla sovellus lukee rekisteriin tallennetut asetukset ja avautuu käyttäjän aiemmin määrittelemässä muodossa. [6]

Carveyn [6] mukaan rekisterissä olevaan tietoon liittyy usein jokin aikaleima, minkä vuoksi rekisteriä voidaan pitää osittain lokitiedoston kaltaisena. Jokaisella rekisteriavaimella on niin sanottu LastWrite-aika, joka kertoo, milloin avainta on viimeksi muutettu. Tämä aika päivittyy aina, kun avain luodaan tai sen arvoja tai alihakemistoja lisätään, poistetaan tai muokataan. Näin rekisteri tallentaa tietoa myös tapahtumien ajankohdista, mikä tekee siitä hyödyllisen lähteen laitteen käyttäjän toiminnan jäljittämisessä. Carvey nostaa esiin Javedin ym. [5] ja Arshadin ym. [13] tapaan, että rekisteristä löytyvä tietomäärä laitteen käyttäjän toimista on usein suuri vielä senkin jälkeen, kun käyttäjä on yrittänyt peittää jälkensä niin

sanotuilla antiforensiikkatoimilla, sillä käyttäjät eivät aina ymmärrä, että heidän vuorovaikutuksensa käyttöjärjestelmän ja usein myös sovellusten kanssa tallentuu automaattisesti.

Windowsin rekisterissä tieto on järjestetty erityisiin osiin, joita kutsutaan avaimiksi (*keys*). Avaimet ovat kansioita ja alikansioita, jotka näkyvät rekisterieditorin vasemmassa osassa. Avaimissa on myös niiden oikeusteknisesti arvokas LastWrite-aikaleima. Oikeassa reunassa näkyvät arvot (*values*) ovat rakenteeltaan yksinkertaisempia ja sisältävät tietoa tietyssä muodossa, kuten yksittäisenä merkkijonona, useampana merkkijonona, binääritietona tai DWORD-arvona, joka on 32-bittinen binääriluku. [6]

Kun uusia Windows-versioita kehitetään, myös tiedon tallennuspaikat ja -muodot rekisterissä muuttuvat: joitain avaimia tai arvoja saatetaan lisätä, siirtää, muokata tai poistaa kokonaan [6]. Tämä puoltaa tarvetta tutkia uusimpien Windows-versioiden forensiikkaa, sillä rekisteri näyttäisi olevan merkittävä forensinen tietolähde.

Muisti. Järjestelmän muisti voi olla haihtuvaa tai ei-haihtuvaa. Haihtuva muisti tallentaa tietoja väliaikaisesti, kun taas ei-haihtuva muisti säilyttää tiedot järjestelmässä. [14] RAM eli satunnaispääsyinen muisti on haihtuvaa, eli se menetetään sammuttamisen yhteydessä. Haihtuvan muistin analyysin laatu riippuu suuresti siitä, kuinka laadukas muistikopio järjestelmästä on saatu. [15]

Muisti tallentaa prosessien sen hetkisen toiminnan, rekisterit, prosessien pinot, poistetut tiedostot ja salatut tiedot. Muistiforensiikassa analysoidaan fyysiseen muistiin tallennettua dataa, kun käyttöjärjestelmä on käynnissä. [14] Muistista voi löytää tietoja esimerkiksi avoinna olleista sovelluksista, käytetyistä tiedostoista ja muista selaimen käyttöön liittyvistä yksityiskohdista [4].

Niin kauan kun järjestelmä on käynnissä, sen RAM-muistiin jää jälkiä siellä tehdyistä toimista. Siten Tor-selaimen käytöstä jäävät artefaktit voidaan löytää ja

tutkia ottamalla muistivedos epäillyn koneesta. Analysoimalla muistivedosta siihen sopivalla työkalulla, kuten Bulk Extractorilla, voidaan saada selville esimerkiksi selatut URL-osoitteet, käytetyt sähköpostiosoitteet ja verkkosivustoille syötetyt henkilötiedot. [10] Myös Javed ym. [5] korostavat, että muistivedoksesta voidaan saada merkittäviä todisteita Tor-selaimen käytöstä, kuten vierailtuja verkkosivustojen osoitteita, HTTP-pyyntöihin liittyviä otsikkotietoja ja Tor-selaimen käynnistysohjelma.

Tallennustila. Tallennustila on yleisnimitys kaikelle tietokoneessa käytettävissä olevalle datan säilytystilalle. Siihen voivat kuulua muun muassa kiintolevyt, SSD-levyt ja USB-muistit.

Kumarin ym. [10] mukaan todisteita Tor-selaimen käytöstä voi olla vaikea saada sen jälkeen, kun selain on poistettu laitteelta. Tällöin tieto saadaan Prefetch-tiedostoista, jotka sijaitsevat Windows-koneessa hakemistossa C:\Windows\Prefetch. Niistä saadaan tietoa selaimen metadatasta, kuten selaimen luontiajasta ja viimeisimmästä käynnistysajasta, selaimen käynnistyskertojen määrästä, selaimen käynnistyshakemistosta ja tiedostonimestä. Javed ym. [5] lisäävät, että Prefetch-tiedostot tallentavat tietoja aiemmin avatuista sovelluksista, jotta ne käynnistyisivät myöhemmillä käynnistyskerroilla nopeammin.

Laitetta tutkittaessa voidaan havaita monenlaisia aikaleimoja. Windows jättää päätelaitteelle aikaleimoja, kun tiedosto tai kansio on luotu tai sen sijaintia muutettu (*File/Folder Created*), sitä on muokattu (*File/Folder Modified*) tai kun tiedostoa tai kansiota on viimeksi käsitelty tai siihen on viitattu jollain tavalla tiedostojärjestelmän kautta (*Last Accessed*). Tämä ei kuitenkaan edellytä, että tiedostoa tai kansiota välttämättä avattiin, vaan jopa viruksentorjuntaohjelman suorittama tarkastus voi muokata aikaleimaa. Tämän vuoksi Last Accessed -aikaleima ei ole välttämättä hyödyllinen forensiikan näkökulmasta. Entry Modified Time -aikaleima taas muuttuu, kun tiedoston metadata muuttuu, esimerkiksi koko tai sijainti levyllä. [16]

4 Tor-selaimen käytön jättämät artefaktit rekisteriin, muistiin ja tallennustilaan

Tässä luvussa tarkastellaan, millaisia artefakteja Tor-selaimen käytöstä on löydetty Windows 11 -laitteen rekisteristä, muistista ja tallennustilasta. Tor-selaimen forensiikkaa on tutkittu aiemmissa Windows-versioissa jo melko runsaasti, mutta Windows 11 -ympäristöön jääviä artefakteja tarkastellaan tutkimuksissa [4], [5] ja [10]. Tor-artefaktien keräämiseksi Windows 11 -ympäristössä on myös esitetty malli [17], mutta tutkimus ei erittele, miten selaimen eri tilat (auki, suljettu, poistettu) vaikuttavat artefaktien säilymiseen, ja tutkimus painottuu verkkoliikenteen analyysiin ja virtuaalisen tutkimusympäristön rakentamiseen.

Vaikka kaikki tarkastellut tutkimukset liittyvät Tor-selaimen forensiikkaan Windows 11-ympäristössä, niiden lähestymistavat ovat erilaiset. Chand ym. [4] tarkastelevat laitteen tallennustilaan ja muistiin jääviä artefakteja, kuten välimuistitiedostoja, evästeitä, selaushistoriaa ja paikallista tallennustilaa, ja pyrkivät muodostamaan aikajanan käyttäjän toimista selauksen aikana. Tutkimuksessa ei kerätty tietoja rekisteristä, ja tarkastelun kohteena oli muitakin selaimia kuin Tor. Javed ym. [5] tarkastelevat vain Tor-selainta ja sen rekisteriin, muistiin ja tallennustilaan tallentuneita artefakteja. Tutkimus painottaa erityisesti rekisteriartefakteja. Kumar ym.

[10] kuvaavat menetelmiä, joilla artefakteja voidaan palauttaa erityisesti muistista ja tallennustilasta ja hieman rekisteristäkin. Tutkimuksen perusteella saa yleiskuvan siitä, mitä artefakteja on mahdollista löytää erilaisilla menetelmillä, vaikka tutkimus ei pyrikään esittämään löydettyjä artefakteja yhtä tarkasti kuin tutkimuksissa [4] ja [5].

Eri tutkimuksissa löydetyt artefaktit esitetään ensin tutkimuskohtaisesti ja luvun lopussa koottuna taulukkoon, jossa ne on jaoteltu muisti-, rekisteri- ja tallennustila-artefakteihin. Ratkaisuun on päädytty siitä syystä, että Chand ym. [4] eivät jaottele löydettyjä artefakteja tämän kolmijaon mukaisesti vaan erilaisten selaustilanteiden mukaan.

Chand ym. [4] tarkastelevat laitteelle asennetun Tor-selaimen jättämiä jälkiä, kun selainta käytetään normaalitilassa (*normal mode*) ja yksityisessä tilassa (*private mode*) neljässä eri selaustilanteessa (esim. T1). Mahdollisia jääviä jälkiä olivat selaushistoria, kirjanmerkit, välimuisti, evästeet, kirjautumistiedot, sivukuvakkeet (pienet sivuston ikonit selaimen välilehdissä), esikatselukuvat (*thumbnails*), lataukset, hakusanat ja eniten vieraillut sivustot. Kaikissa tilanteissa alku on samanlainen: laite käynnistetään, virtuaalikone käynnistetään, selain avataan ja verkkoa selataan. Eri selaustilanteet etenivät tämän jälkeen seuraavasti:

T1: Selain suljetaan, virtuaalikone suljetaan.

T2: Selaushistoria poistetaan, selain suljetaan, virtuaalikone suljetaan.

T3: Selain suljetaan, muistivedos otetaan, virtuaalikone suljetaan.

T4: Selaushistoria poistetaan, selain suljetaan, muistivedos otetaan, virtuaalikone suljetaan.

Tutkimuksessa todettiin, että T1:ssä Tor-selaimen käytöstä jää jälkiä normaalitilassa kirjanmerkeistä, hakusanoista ja vierailluista sivuista ja yksityisessä tilassa vain hakusanoista. T2:ssa normaalitilassa jää kirjanmerkkejä, mutta yksityisessä tilassa ei mitään. T3:ssa normaalitilassa jää evästeitä, yksityisessä tilassa ei mitään. T4:ssä jää evästeitä ja hakusanoja sekä normaali- että yksityisessä tilassa.

Vaikka Chand, ym. [4] ovat luokitelleet löydettyjä artefakteja sen mukaan, mitä niistä löydettiin normaali- tai yksityisessä tilassa neljässä erilaisessa selaustilanteessa, tutkimusten vertailun kannalta kiinnostavinta on se, mitä artefakteja Tor-selaimen käytöstä on ylipäätään mahdollista löytää. Tämän vuoksi edempänä esiteltävässä Taulukossa 5.4 tutkimuksen [4] tuloksia on yksinkertaistettu jakamalla ne vain normaali- tai yksityisessä tilassa löydettyihin artefakteihin.

Chand ym. [4] eivät ole jaotelleet selaimen käytöstä jääviä jälkiä erikseen rekisterin, muistin ja tallennustilan löydöksiin. Tutkimuksessa kuitenkin mainitaan, että selaustilanteissa T1 ja T2 ei otettu muistivedosta, jolloin kyseisten selaustilanteiden artefaktit on löydetty tallennustilasta. Selaustilanteiden T3 ja T4 artefakteja taas tutkittiin muistivedoksista. Jotta eri tutkimusten löydösten vertailu olisi selkeää, Taulukossa 5.4 esitetään Chandin ym. [4] löytämät artefaktit jaoteltuna näihin osa-alueisiin.

Tutkimuksessa [5] otettiin muistivedos FTK Imagerilla Tor-selaimen ollessa auki, suljettu ja poistettu. Tulokset analysoitiin Tor-selaimen käyttöön liittyvien artefaktien tunnistamiseksi Bulk Extractorilla. Tutkimus osoitti, että muistivedosten analysointi eri vaiheissa (selain avoinna, suljettu ja poistettu) auttaa saavuttamaan yksityiskohtaisen kuvan Tor-selaimen käytöstä ja palauttamaan vieraillut onion-osoitteet, Tor.exe-tiedoston esiintymät ja Tor-selaimen käynnistyksen aikaleimat.

Rekisterianalyysissä löydettiin useita artefakteja. Ennen Tor-selaimen käynnistämistä rekisteristä oli löydettävissä merkinnät, jotka kertovat, että Tor-selain on

asennettu järjestelmään (*Tor Browser Installer*), asennusohjelman sijainnin järjestelmässä (*Location of Tor Installer*) ja sovelluksen nimen käyttöjärjestelmän näkökulmasta (*Name of Application*).

Selaimen käytön jälkeen rekisteristä löytyi seuraavia rekisteriavaimia:

Firefox-pohjaisen ohjelman suorittaminen. Tor-selain on Firefox-pohjainen, joten se voidaan tunnistaa firefox.exe-prosessiksi, vaikka kyseessä olisi Tor-selaimen käyttö.

Sovelluksen helppolukuinen nimi. Kun käyttäjä käynnistää ohjelman, sovelluksen helppolukuinen nimi (kuten "Tor Browser") tallentuu tähän rekisteriavaimeen.

Sovelluksen valmistajan nimi. Windowsin välimuistiin tallentuu ohjelman valmistajan nimi.

Firefoxin asennusohjelman sijainti. Tämä rekisterimerkintä kertoo, että Firefox-pohjainen ohjelma (Tor-selain) on asennettu ja asennusohjelma on suoritettu kyseisellä käyttäjätilillä.

Joitakin jälkiä Tor-selaimen käytöstä. Nämä tiedot kertovat, että ohjelma on käynnistetty Firefox-pohjaisella käynnistysohjelmalla kyseisessä käyttäjäprofiilissa.

Sovelluksen nimi käyttöjärjestelmän näkökulmasta, sen helppolukuinen nimi ja sovelluksen valmistajan nimi tallentuivat MuiCache-avaimen alle. Carveyn [6] mukaan MuiCache-avaimen alle syntyvät arvot ovat yleensä seurausta käyttäjän vuorovaikutuksesta käyttöliittymän kanssa: kun MuiCache-avaimessa näkyy suoritettavan tiedoston polku, se on merkki siitä, että kyseinen ohjelma on joskus avattu tai ajettu kyseisellä käyttäjätilillä. MuiCache-avain tarjoaa siten pysyvän tietolähteen niistä sovelluksista, joita käyttäjätilillä on suoritettu, vaikkakin ilman aikaleimaa. MuiCache-avain voi paljastaa erittäin hyödyllisiä vihjeitä käyttäjätilillä tapahtuneesta toiminnasta myös silloin, kun käytetty ohjelma on jo poistettu laitteelta.

Tallennustilan forensisessa tutkimuksessa yritettiin palauttaa kaikki Tor-selaimeen liittyvät jäljet sen jälkeen, kun selain oli poistettu järjestelmästä. Tiedostojen tor.exe ja firefox.exe sijainnit voitiin tunnistaa helposti. Tutkimuksessa todettiin myös, että Autopsy paljasti niiden olleen vähän aikaa sitten käytössä. Kaikki ladatut tiedostot löytyivät poistettujen tiedostojen kansiosta. Autopsyn avulla saatiin selville myös Torin asennusohjelman sijainti.

Tutkimuksessa havaittiin myös, että käyttöjärjestelmän Prefetch-tiedostoissa oli merkkejä Tor-selaimen käytöstä. Näistä tiedostoista saatiin siten lisätodisteita siitä, että Tor-selainta on käytetty, vaikka selain oli jo poistettu.

Kumar ym. [10] esittelevät käytännöllisen mallin, jolla Tor-selaimen käyttöön liittyviä artefakteja voidaan palauttaa. Tutkimuksessa mainitaan, että niitä voidaan löytää sekä muistista, tallennustilasta että rekisteristä.

Tutkimuksessa tutkittiin, mitä sähköpostin käyttöön liittyviä artefakteja laitteelle jää Tor-selaimen käytön yhteydessä. Artefakteja etsittiin seuraavissa vaiheissa:

1. Analyysi muistivedoksesta, kun selain on käynnissä.
2. Analyysi tallennustilasta, kun selain on käynnissä.
3. Analyysi muistivedoksesta, kun selain on suljettu.
4. Analyysi tallennustilasta, kun selain on suljettu.
5. Selvitetään, mitä artefakteja Torin käytöstä on edelleen mahdollista löytää, kun selain on poistettu.

Eniten artefakteja löytyi muistivedoksesta, joka otettiin käynnissä olevasta selaimesta. Suurin osa näistä tiedoista säilyi myös silloin, kun muistivedos otettiin vasta selaimen sulkemisen jälkeen. Kun muistivedos otettiin selaimen poistamisen jälkeen ja sitä tutkittiin Bulk Extractorilla, muistivedoksesta ei enää saatu tietoja selaimen käytöstä. Löydettyjen artefaktien laatua ei eksplisiittisesti mainita. Tutkimuksessa

kerrotaan kuitenkin, että muistivedosten analysoinnissa etsitään sähköpostipalvelujen domaineja, sähköpostiosoitteita ja käyttäjänimiä sekä viestien sisältöön viittaavia tietoja. Nämä tiedot tunnistetaan Bulk Extractorin tuottamista tulostetiedostoista, kuten domain.txt ja email.txt. Kaikkia näitä tietoja on siten mahdollista löytää muistivedoksesta riippuen siitä, missä vaiheessa selaustapahtumaa muistivedos on otettu ja mitä työkaluja käytetään.

Tutkimuksessa mainitaan, että mikäli muistivedoksesta ei löyty artefakteja, niitä voi kuitenkin löytyä Prefetch-tiedostoista. Kuten Luvussa 3 kerrotaan, Prefetch-tiedostoista saadaan tietoa selaimen luontiajasta ja viimeisimmästä käynnistysajasta, selaimen käynnistyskertojen määrästä, selaimen käynnistyshakemistosta ja tiedostonimestä. Näin ollen Tor-selaimen asentaminen ja käyttö jättävät pysyviä jälkiä tallennustilan Prefetch-tiedostoihin myös selaimen poistamisen jälkeen.

Tutkimus osoittaa myös, millä tavoin rekisteristä voidaan löytää tietoa Tor-selaimen käytöstä, vaikka muistivedoksesta ei enää löytyisi tietoja. Polku, josta TOR-selain käynnistyy, voidaan löytää laitteen rekisteristä kohdasta HKEY_USERS\<SID>\SOFTWARE\Mozilla\Firefox\Launcher. Sieltä Tor-selaimen viimeisin käynnistysaika voidaan saada selville tarkastelemalla State-tiedostoa siinä hakemistossa, josta Tor-selain käynnistettiin. State-tiedoston hakemisto sijaitsee Tor-selaimen kansiossa \Tor Browser\Browser\TorBrowser\Data\Tor. Näin ollen rekisterimerkinnät voivat paljastaa, että Tor on ollut asennettuna ja käytössä.

Vaikka Kumar ym. [10] eivät mainitse artefaktien tarkkaa määrää eikä muistivedoksista löytyneiden artefaktien tarkkaa laatuakaan, yleiskuva sen löydöksistä on samansuuntainen kuin muissa tutkimuksissa.

4.1 Pohdintaa

Vaikka Chand ym. [4] eivät tutkineet rekisteriä, tutkimus osoitti, että jo tallennustilaan ja muistiin jäävät artefaktit voivat jo yksin paljastaa tärkeitä tietoja Torin

käytöstä. Javed ym. [5] taas laajentavat näkökulmaa rekisteriartefakteihin ja vahvistavat, että Torin käyttö jättää jälkiä myös rekisteriin järjestelmätason asetuksiin ja prosessitietoihin.

Kumar ym. [10] esittelevät käytännönläheisen mallin, jolla artefakteja voidaan palauttaa. Tutkimus ei kuitenkaan sisällä määrällisiä tuloksia, kuten "löydettiin 5 sähköpostiliitettä", vaan siinä mainitaan, oliko artefakteja ylipäätään löydettävissä tietyissä tilanteissa vai ei. Näin ollen tutkimus osoittaa muiden tutkimusten tavoin, että Tor-selaimen käyttö jättää jälkiä laitteelle ja että muistivedoksesta on mahdollista saada vielä useita tärkeitä tietoja selaimen sulkemisen jälkeenkin, mutta se ei pyri tekemään tarkkaa määrällistä analyysiä, jota voisi helposti vertailla muiden tutkimusten tuloksiin.

Siitä huolimatta, että olemassa oleva tutkimus Tor-selaimen forensiikasta painottuu varhaisempiin Windows-versioihin ja Tor-selaimen jättämiä artefakteja Windows 11 -ympäristössä on tutkittu vasta vähän, tässä tutkielmassa esitellyt tutkimukset tarjoavat merkittäviä ja toisiaan täydentäviä tietoja. Tutkimusten erilaiset painotukset muodostavat kokonaiskuvan siitä, millaisia jälkiä Tor-selaimen käyttö voi jättää järjestelmään, vaikkakin tutkimusten vähäisen määrän vuoksi vielä rajallisen. Jokainen tutkimus Tor-selaimen forensiikasta lisää ymmärrystä Torin toiminnasta uusimmassa käyttöjärjestelmässä ja tarjoaa arvokkaan lähtökohdan myöhemmille tutkimuksille, sillä kuten Carvey [6] on tuonut esiin, käyttöjärjestelmien jatkuva kehitys muuttaa olennaisesti sitä, miten ja mihin käyttäjän toiminnasta jääviä jälkiä tallentuu.

5 Tor-selaimen artefaktien empiirinen tarkastelu virtuaaliympäristössä

Tämän tutkielman empiirisen osuuden tarkoituksena on selvittää, mitä jälkiä Windows 11 -päätelaitteelle jää rekisteriin, muistiin ja tallennustilaan, kun sillä on selattu verkkoa, käytetty sähköpostia ja ladattu tiedostoja Tor-selaimella. Saatuja tuloksia verrataan tutkimuskirjallisuudessa esitettyihin tuloksiin. Tutkielmassa käytetyt työkalut (Taulukko 5.1) ovat olleet suosittuja selainartefaktien tutkimisessa ja hyvin käyttötarkoitukseensa sopiviksi todettuja, mikä puoltaa niiden valintaa myös tähän tutkielmaan.

Taulukko 5.1: Tutkielmassa käytetyt työkalut ja niiden käyttötarkoitukset

Työkalu	**Versio**	**Käyttötarkoitus**
Lenovo LOQ+ 15IRX10 i5-13HX/24 GB/1 TB (Windows 11 Home)	-	Fyysinen isäntäkone
VirtualBox (Windows 11 Home)	7.2.4 r170995	Virtuaalikone Tor-selaimen käyttämiseen
VirtualBox (Windows 11 Home)	7.2.4 r170995	Virtuaalinen forensiikkatyöasema
Tor-selain	14.5.6	Verkon selaaminen
Regshot	1.9.0	Rekisterimuutosten vertailu
FTK Imager	4.7.3.81	Muistin talteenotto
Bulk Extractor	2.1.0	Muistin analysointi
Autopsy	4.22.1	Tallennustilan analysointi
WinPrefetchView	1.37	Prefetch-tiedostojen analysointi

Regshot on ilmainen ja avoimen lähdekoodin työkalu, jolla laitteen rekisteristä voidaan ottaa tilannekuvia ja verrata niitä keskenään esimerkiksi järjestelmämuutosten tai uusien ohjelmien asennuksen jälkeen. Regshotia ovat hyödyntäneet muun muassa [13], [18], [19] ja [20].

FTK Imager on yhteensopiva Tor-selaimen kanssa. Sen avulla voidaan palauttaa selaushistoriaa, paikallisesti tallennettuja tietoja, verkkovälimuistia, evästeitä, väliaikaistiedostoja, metatietoja, lokitietoja, istuntotietoja ja kirjanmerkkejä. [4] FTK Imageria selainten forensiikan tutkimuksissa ovat käyttäneet muun muassa [21], [5], [18], [13], [20] ja [22]. FTK Imagerin keräämät muistitiedot analysoidaan Bulk Extractorin komentoriviversiolla. Bulk Extractor on ollut forensiikkatyökaluna käytössä esimerkiksi tutkimuksissa [18], [22] ja [20].

Autopsy on suosittu työkalu lokitiedostojen keräämiseen, selaimen välimuistin historian hakemiseen, poistettujen tiedostojen ja salasanojen palauttamiseen ja sähköpostien noutamiseen [4]. Tässä tutkielmassa sitä käytetään tallennustilan analyysissä. WinPrefetchView on Windows-apuohjelma, jolla täydennetään tallennustilan artefaktien tutkimusta analysoimalla Prefetch-tiedostoja.

Tutkielmassa noudatettiin Taulukossa 5.2 kuvattua menetelmää, joka on yhdistelmä tutkimusten [10] ja [5] lähestymistapoja.

Taulukko 5.2: Artefaktien kerääminen ja analysointi selaimen eri tiloissa

Selainta ei asennettu	Selain auki	Selain suljettu	Selain poistettu
Tilannekuva rekisteristä (Regshot)	Tilannekuva rekisteristä (Regshot)	Tilannekuva rekisteristä (Regshot)	Tilannekuva rekisteristä (Regshot)
	Analyysi muistivedoksesta (FTK Imager, Bulk Extractor)	Analyysi muistivedoksesta (FTK Imager, Bulk Extractor)	Analyysi muistivedoksesta (FTK Imager, Bulk Extractor)
	Analyysi tallennustilasta (Autopsy)	Analyysi tallennustilasta (Autopsy)	Analyysi tallennustilasta (Autopsy) Prefetch-tiedostojen tutkiminen (WinPrefetchView)

Virtuaalikoneessa Tor-selainta käytettiin seuraavalla tavalla:

1) Selain asennettiin.

2) Selain avattiin. Mentiin osoitteeseen www.google.com. Etsittiin Google-haulla hakusanoja *puppy* ja *birds*. Selattiin haulla löytyneitä kuvia ja avattiin haulla löytynyt Wikipedia-artikkeli Birds. Mentiin osoiterivin kautta osoitteisiin www.helsinki.fi ja www.harvard.com.

3) Kirjoitettiin DuckDuckGoGo-hakukoneeseen hakusana *horses* ja navigoitiin haulla löytyneeseen Wikipedia-artikkeliin Horse. Vierailtiin Facebookin onion-osoitteessa osoiterivin kautta. Kirjoitettiin osoiteriville *proton mail*, kirjauduttiin sähköpostiin suspicious_receiver5666@proton.me ja ladattiin sinne saapuneesta viestistä kuvatiedosto *kitten* ja PDF-tiedosto *Good day to you*, jonka sisältönä oli teksti *This is a happy message*. Vastaanotettiin ja avattiin sähköpostiviesti otsikolla *Are you hungry?*.

4) Suljettiin selain.

5) Poistettiin selain ja sen asennustiedosto, ladattu kuvatiedosto ja PDF-tiedosto. Tyhjennettiin roskakori.

5.1 Rekisteriartefaktit

Rekisteristä otettiin Regshot-työkalulla kolme tilannekuvaparia. Ensimmäinen kuvapari otettiin ennen Tor-selaimen asentamista ja selaimen käyttämisen jälkeen, kun selain oli edelleen auki. Toinen kuvapari otettiin selaimen ollessa edelleen auki ja sen sulkemisen jälkeen. Kolmannessa kuvaparissa vertailtiin tilanteita, joissa selain on suljettu ja poistettu. Kuvaparit kertovat, mitä arvoja rekisterissä poistettiin tai

muokattiin tai mitä sinne lisättiin kahden tilanteen välillä.

Ensimmäisessä tilannekuvaparissa (Taulukko 5.3) rekisteristä löydettiin samat rekisteriartefaktit kuin Javedin ym. tutkimuksessa [5]. Toisessa kuvaparissa rekisterissä oli edelleen kuusi firefox.exe-artefaktia, jotka kertoivat, että Tor-selaimen pääohjelma on ollut laitteella käynnissä.

Rekisteriartefakteja on edelleen havaittavissa kolmannessa kuvaparissa. Tor-selaimen käyttöön liittyviä avaimia on lisätty yksi ja arvoja kaksi. Muutokset ovat metatietoja selaimen käytöstä ja osoittavat, että se on ollut asennettuna laitteelle, vaikka tässä vaiheessa selain asennustiedostoineen on poistettu. Siten toistettiin Javedin ym. [5] tutkimustulos siitä, että joitakin rekisteriartefakteja säilyy senkin jälkeen, kun käyttäjä on poistanut selaimen ja sen asennustiedoston ja tyhjentänyt roskakorin.

5.2 Muistiartefaktit

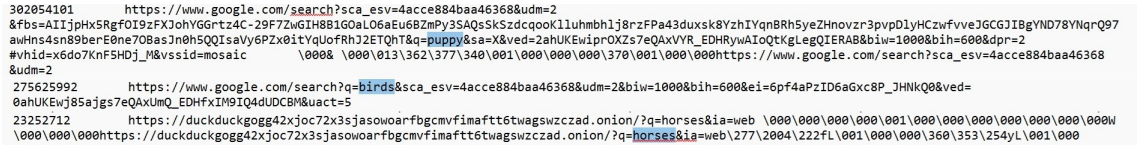
FTK Imagerilla otettiin kolme muistikuvaa: yksi selaimen käytön aikana, yksi sen sulkemisen jälkeen ja yksi sen poistamisen jälkeen. Tulokset analysoitiin Bulk Extractorilla, joka luo muistivedoksen sisällöstä helposti tarkasteltavia kansioita, kuten email.txt, json.txt ja url.txt.

Kun muistivedos otettiin selaimen ollessa auki, url.txt-tiedostosta oli helposti löydettävissä ne verkko-osoitteet, jotka kirjoitettiin suoraan osoiteriville (www.helsinki.fi, www.harvard.com, Facebookin onion-osoite) tai joihin päädyttiin Google-hakusanojen kautta esimerkiksi kuvahaussa navigoimalla (Four Paws, Wikipedia). Myös hakusanat *puppy*, *birds* (Google-haku) ja *horses* (DuckDuckGoGo-haku) löytyivät. Tiedostoista email.txt ja json.txt löytyi sähköpostiviestintään liittyviä tietoja, kuten viestin vastaanottajan ja lähettäjän sähköpostit, lähettäjän nimi, vastaanotetun viestin osittainen otsikko *"ou hungry?"*, maininnat vastaanotetusta kuvasta ja PDF-tiedostosta ja kuvan ja PDF-tiedoston nimet. Kuvat 5.1, 5.2 ja 5.3 esittävät kootusti muistivedoksen artefakteja selaimen ollessa auki.

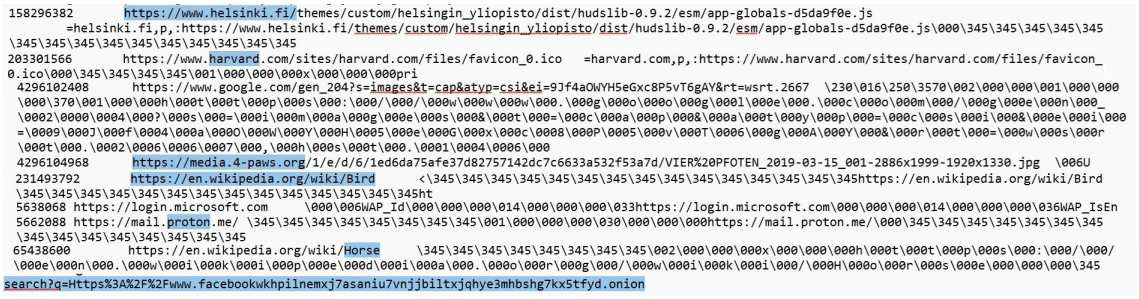
Taulukko 5.3: Rekisteriartefaktit selaimen ollessa käynnissä

Nro	Selitys	Sijainti rekisterissä
1	Tor-selaimen lataus	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1129379548-2865886240-4070013930\-1001\Device\HarddiskVolume3\Users\hanna\Downloads\tor-browser-windows-x86_64-portable-14.5.8.exe
2	Firefox.exe	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1129379548--2865886240-4070013930-1001\\Device\HarddiskVolume3\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe HKU\S-1-5-21-1129379548-2865886240-4070013930-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe
3	Sovelluksen helppo-lukuinen nimi	HKU\S-1-5-21-1129379548-2865886240-4070013930-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\hanna\Downloads\tor-browser-windows-x86_64 portable-14.5.8.exe.FriendlyAppName: "Tor Browser Portable Installer" HKU\S-1-5-21-1129379548-2865886240-4070013930-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe.FriendlyAppName: "Tor Browser"
4	Sovelluksen tekijätieto	HKU\S-1-5-21-1129379548-2865886240-4070013930-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe.ApplicationCompany: "Mozilla Corporation"
5	Tor-selaimen käynnis-tämiseen liittyviä tietoja	HKU\S-1-5-21-1129379548-2865886240-4070013930-1001\Software\Tor Project\Firefox\Launcher\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe|Image: 0x00000000 HKU\S-1-5-21-1129379548-2865886240-4070013930-1001\Software\Tor Project\Firefox\Launcher\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe|Launcher: 1B C3 31 F9 01 00 00 00 HKU\S-1-5-21-1129379548-2865886240-4070013933-1001\Software\Tor Project\Firefox\Launcher\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe|Browser: A7 32 36 F9 01 00 00 00 HKU\S-1-5-21-1129379548-2865886240-4070013933-1001\Software\Tor Project\Firefox\Launcher\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe|Telemetry: 0x00000000 HKU\S-1-5-21-1129379548-2865886240-4070013933-1001\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe|Progress: 0x00000001
6	Muita MuiCache-merkintöjä	HKU\S-1-5-21-1129379548-2865886240-4070013930-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\hanna\Downloads\tor-browser-windows-x86_64-portable-14.5.8.exe.FriendlyAppName: "Tor Browser Portable Installer" HKU\S-1-5-21-1129379548-2865886240-4070013930-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe.FriendlyAppName: "Tor Browser" HKU\S-1-5-21-1129379548-2865886240-4070013930-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\hanna\Desktop\Tor Browser\Browser\firefox.exe.ApplicationCompany: "Mozilla Corporation"

Selaimen sulkemisen jälkeen otetusta muistivedoksesta löytyivät edelleen käytetyt hakusanat, haetut osoitteet ja lähettäjän ja vastaanottajan sähköpostiosoitteet,



Kuva 5.1: Hakusanoja muistivedoksesta selaimen ollessa auki (kooste)

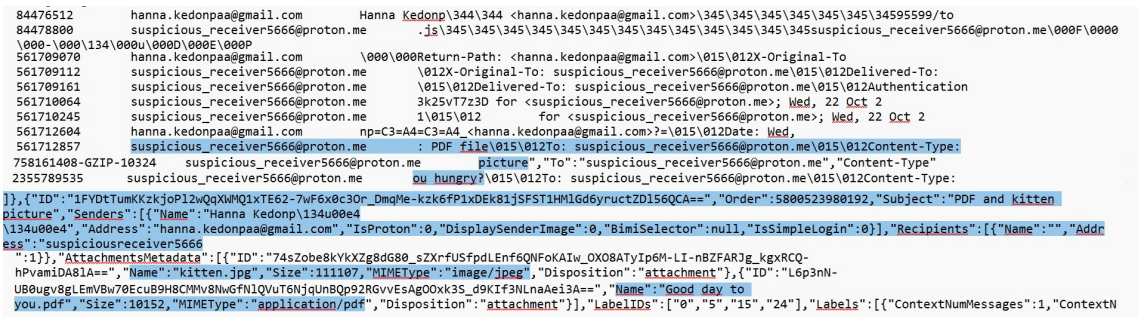


Kuva 5.2: Vierailtuja osoitteita muistivedoksesta selaimen ollessa auki (kooste)

mutta ei tietoja vastaanotetusta kuvasta, PDF-tiedostosta tai vastaanotetun viestin otsikosta. Selaimen poistamisen jälkeen artefaktit vähenivät hakusanoihin ja vierailtuihin sivustoihin.

5.3 Tallennustilan artefaktit

Tallennustilan artefakteja tutkittiin Autopsylla levykuvista, joissa selain oli ollut auki, suljettu ja poistettu. Lisäksi selaimen poistamisen jälkeen etsittiin selaimen



Kuva 5.3: Sähköpostiartefakteja muistivedoksesta selaimen ollessa auki (kooste)

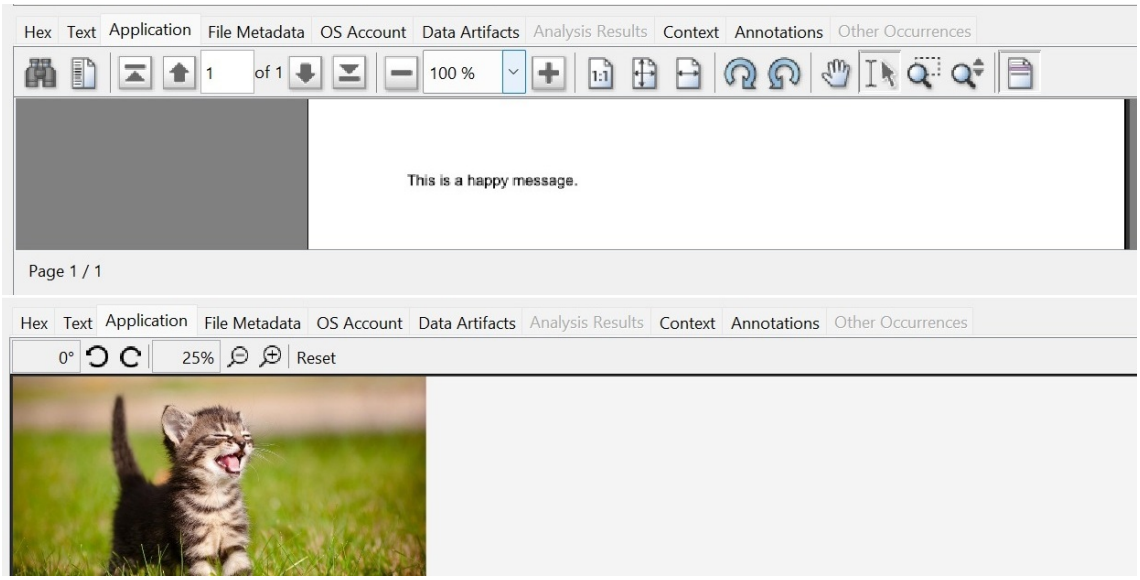
käyttöön liittyviä Prefetch-tiedostoja, jotka analysoitiin WinPrefetchViewillä. Tutkielmassa pyrittiin löytämään todisteita selaimen käytöstä, hakusanoja, ladattuja tiedostoja, vierailtuja osoitteita ja sähköpostitietoja. Koska tutkielmassa Windows on asennettu VirtualBox-ympäristöön, Javedin ym. [5] tapaan levykuva luotiin .img-raakamuodossa, joka on yhteensopiva Autopsyn kanssa. Analyysi toteutettiin Kumarin ym. [10] esittelemän mallin mukaisesti.

Ensin analysoitiin levykuva, joka oli otettu selaimen ollessa auki. Autopsy paljasti merkittäviä tietoja selaimen käytöstä, muun muassa osoiteriville kirjoitetut hakusanat ja verkosta ladattujen tiedostojen nimet, tyypit ja sisällöt. Lisäksi Autopsy näytti levylle tallennetut tiedostot ja asennetut ohjelmat.

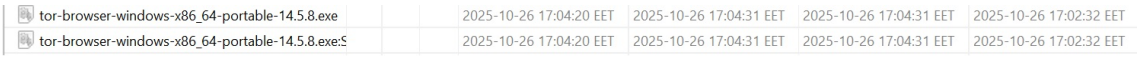
Sähköpostista ladatut tiedostot Good day to you.pdf ja kitten.jpg löytyivät kansiosta Web Downloads, mikä osoittaa, että ne on ladattu verkosta (Kuva 5.4). Tiedostot voi myös avata ja niiden sisältöä tarkastella.

On huomattava, että Tor-selaimen lataaminen ei näy kansiossa Installed Programs. Tämä johtuu siitä, että laitteellakaan se ei tallennu asennettujen ohjelmien listaan vaan itsenäiseksi kansiokseen. Sen sijaan tor.exe ja firefox.exe löytyvät Autopsyssa kansiosta File Types > Executable > .exe (Kuva 5.5). Levykuvassa niiden sijainnit ovat Users/käyttäjänimi/Desktop/Tor Browser/Browser/firefox.exe ja Users/käyttäjänimi/Desktop/Tor Browser/Browser/TorBrowser/tor.exe.

Seuraavaksi tarkasteltiin levykuvaa, joka otettiin selaimen ollessa suljettu. Selaimen sulkeminen ei näytä estävän sähköpostiartefaktien palauttamista. Samat verkon selaamistiedot ja tiedostot sisältöineen löytyivät samoista kansioista kuin ensimmäisessä levykuvassa. Samat tulokset saatiin levykuvasta, joka otettiin selaimen poistamisen jälkeen. Tor.exe ja firefox.exe löytyvät niin ikään edelleen samasta sijainnista levykuvassa kuin selaimen ollessa auki, mutta File Types > Executable > .exe -kansiossa ne on merkitty punaisella rastilla sen merkiksi, että tiedostot on levykuvaa otettaessa jo poistettu laitteelta.



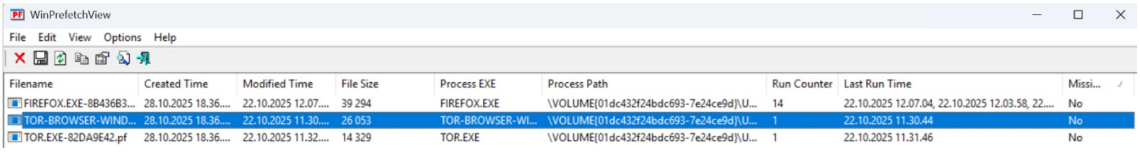
Kuva 5.4: Sähköpostista ladatut tiedostot Web Downloads -kansiossa



Kuva 5.5: Tor-selaimen asennustiedosto File Types > Executable > .exe -kansiossa

Sijainnista C:\Windows\Prefetch löytyi kolme selaimen käytöstä kertovaa artefaktia: *FIREFOX.EXE-8B436B3A.pf, TOR.EXE-82DA9E42.pf* ja *TOR-BROWSER-WINDOWS-X86_64-PO-C5A6D906.pf*. Kun Tor-selainohjelma on suoritettu, Windows on luonut siitä Prefetch-tiedostoja, jotka näyttäisivät säilyvän laitteella myös sen jälkeen, kun käyttäjä on pyrkinyt peittämään kaikki jäljet selaimen käytöstä. Tiedostot analysoitiin WinPrefetchView-ohjelmalla.

Kuvan 5.6 mukaisesti sarake Created Time näyttää ajan, jolloin tiedosto on kopioitu analysoitavaksi. Modified Time näyttää, milloin Prefetch-tiedoston sisältöä on viimeksi päivitetty, mikä tapahtuu aina, kun ohjelma suoritetaan. Process Path kertoo polun käynnistettyyn tiedostoon. Run Counter näyttää Tor-selaimen käynnistyskertojen määrän ja Last Run Time viimeisimmän käynnistyskerran. Artefakteista voidaan selvästi todeta, että laitteella on käytetty Tor-selainta. Nämä tiedot saadaan, vaikka käyttäjä olisi ehtinyt poistaa selaimen asennuksen.



Kuva 5.6: Prefetch-tiedostot WinPrefetchViewissä

Tarkasteltujen tutkimusten ja tämän tutkielman tulokset on esitetty Taulukossa 5.4. Löydetyt artefaktit on jaettu rekisteri-, muisti- ja tallennustilan artefakteihin. Selaimen tila (auki, suljettu tai poistettu) on mainittu, mikäli tieto on ollut saatavilla.

Taulukko 5.4: Tor-selaimen jättämät artefaktit eri tutkimuksissa

Tutkimus	**Rekisteriartefaktit**	**Muistiartefaktit**	**Tallennustilan artefaktit**
[4]	Ei tutkittu	Normaalitila: Kirjanmerkit Hakusanat Vieraillut sivustot Evästeet Yksityinen tila: Hakusanat Evästeet	Normaalitila: Kirjanmerkit Hakusanat Vieraillut sivustot Yksityinen tila: Hakusanat
[5]	Selain auki, suljettu ja poistettu: Jälki Tor-selaimen asennuksesta, asennusohjelman sijainti, sovelluksen nimi ja helppolukuinen nimi, firefox.exe, sovelluksen valmistajan nimi, Firefoxin asennusohjelman sijainti, jälkiä Tor-selaimen käytöstä	Selain auki, suljettu ja poistettu: Vieraillut sivustot Tor.exe Torin käynnistysohjelma Aikaleimat	Selain auki, suljettu ja poistettu: Firefox.exe ja tor.exe Torin asennustiedoston sijainti
[10]	Jälki Tor-selaimen asennuksesta, selaimen viimeisin käynnistysaika	Selain auki ja suljettu: Sähköpostipalveluiden domainit, sähköpostiosoitteet ja käyttäjänimet, tietoja kirjoitetuista ja avatuista viesteistä	Selain auki ja suljettu: Sähköpostista ladattujen tiedostojen nimet, tyypit ja sisällöt Selain poistettu: Prefetch-tiedostot (viimeisin käynnistysaika, käynnistyskertojen määrä, polku käynnistettyyn tiedostoon, tiedostonimi)
Tämä tutkielma	Selain auki: Jälki Tor-selaimen asennuksesta, asennusohjelman sijainti, sovelluksen nimi ja helppolukuinen nimi, firefox.exe, sovelluksen valmistajan nimi, Firefoxin asennusohjelman sijainti, jälkiä Tor-selaimen käytöstä Selain suljettu: firefox.exe Selain poistettu: Metatietoja selaimesta	Selain auki: Vieraillut sivustot, hakusanat, sähköpostipalveluiden domainit, sähköpostiosoitteet ja käyttäjänimet, tietoja kirjoitetuista ja avatuista viesteistä Selain suljettu: Vieraillut sivustot, hakusanat, sähköpostipalveluiden domainit, sähköpostiosoitteet Selain poistettu: Vieraillut sivustot, hakusanat	Selain auki, suljettu ja poistettu: Sähköpostista ladattujen tiedostojen nimet, tyypit ja sisällöt Firefox.exe ja tor.exe Vieraillut sivustot Selain poistettu: Prefetch-tiedostot (viimeisin käynnistysaika, käynnistyskertojen määrä, polku käynnistettyyn tiedostoon, tiedostonimi)

6 Lopuksi

Sekä aiempi tutkimus että tässä tutkielmassa löydetyt artefaktit osoittavat, että tietoa Tor-selaimen käytöstä laitteella saadaan sekä laitteen rekisteristä, muistista että tallennustilasta. Yksityiskohtaisinta tietoa saadaan silloin, jos laite voidaan tutkia, kun selain on vielä käynnissä. Selaimen sulkemisen ja poistamisen jälkeen artefaktien määrä vähenee, mutta oikeilla työkaluilla tutkittaessa niitä on mahdollista löytää missä tahansa vaiheessa.

Eri tutkimuksissa löydettiin osin erilaisia artefakteja, mihin on useita syitä. Tutkimustulosten erot löydetyissä artefakteissa voivat johtua muun muassa käytetyistä työkaluista, kuten myös Javed ym. [5] muistuttavat. Kumar ym. [10] taas nostavat esiin, että löydettyjen artefaktien määrä riippuu siitä, onko selain käynnissä, suljettu vai poistettu tarkasteluhetkellä. Tämän tutkielman tulokset myötäilevät molempien huomioita, sillä eri työkalut paljastivat erilaisia artefakteja ja artefaktien määrä riippui selaimen tilasta. Useita työkaluja ja selaimen mahdollisimman monia tiloja (asennettu, auki, suljettu, poistettu) yhdistämällä voidaan löytää enemmän artefakteja kuin rajatummalla menetelmällä.

Tässä tutkielmassa löydettiin selaimen ollessa auki samat rekisteriartefaktit kuin Javedin ym. [5] tutkimuksessa. Tunnistettujen rekisteriartefaktien määrä kuitenkin väheni selaimen sulkemisen ja poistamisen jälkeen, mikä poikkeaa mainitun tutkimuksen tuloksista. Yksi syy voi olla, että vertailun kohteena olevassa tutkimuksessa käytetään rekisteriartefaktien analyysissä Regshotin lisäksi Regeditiä, joka täy-

dentää rekisterianalyysiä ja mahdollistaa artefaktien yksityiskohtaisen tarkastelun. Regshot taas vertailee vain kahden rekisterikuvan muutoksia, jolloin tietyt artefaktit voivat jäädä huomaamatta, vaikka ne olisivat olemassa.

Myös muistivedoksista ja tallennustilasta löydettyjen artefaktien määrään ja laatuun vaikuttaa, missä vaiheessa selaustapahtumaa analysoitava data on on otettu ja mitä työkaluja sen analysointiin käytetään. Muistivedoksista selaimen ollessa käynnissä tai suljettuna löydettiin useita samanlaisia artefakteja kuin vertailun kohteena olevissa tutkimuksissa. Selaimen poistamisen jälkeen löydetyt artefaktit kuitenkin poikkeavat eri tutkimuksissa. Tässä tutkielmassa ja Javedin ym. [5] tutkimuksessa löydettiin joitakin muistiartefakteja vielä tässäkin vaiheessa, kun taas Kumar ym. [10] totevat, että selaimen poistaminen poisti myös muistiartefaktit. Tallennustilan artefaktien osalta tämän tutkimuksen tulokset ovat lähimpänä Kumarin ym. [10] tutkimustuloksia, joskaan heidän tutkimuksensa ei mainitse vierailtujen sivustojen osoitteita.

Tässä tutkielmassa luotiin kahdella toisiaan täydentävällä menetelmällä ajantasainen kuva Tor-selaimen jättämistä artefakteista Windows 11 -päätelaitteelle. Ensiksi tehty kirjallisuuskatsaus kokosi yhteen viime vuosien tutkimustulokset ja analysoi niiden keskeiset erot ja yhtäläisyydet. Tätä täydennettiin kokeellisella osuudella, jonka tuloksia verrattiin aiempiin tutkimustuloksiin. Tulokset sekä vahvistavat että haastavat aiempia tutkimustuloksia.

Jatkotutkimusta tarvitaan erityisesti sen selvittämiseksi, miten rekisterin, muistin ja tallennustilan eri analyysityökalut ja Tor-selaimen eri versiot vaikuttavat löydettävissä oleviin artefakteihin. Lisäksi olisi hyödyllistä tutkia systemaattisesti ja yhtenäisillä menetelmillä selaimen eri tilojen vaikutusta artefaktien säilymiseen ja selittää tutkimuksissa havaitut ristiriidat erityisesti muistivedosten artefakteissa. Tällainen laaja, vertaileva tutkimus auttaisi kehittämään luotettavia menetelmiä Tor-selaimen forensiikkaan.

Lähdeluettelo

[1] P. P. Sajan, C. Balanb, M. D. Priya ja A. Sreedeep, "Tor browser forensics", *Turkish Journal of Computer and Mathematics Education*, vol. 12, nro 11, s. 5599–5608, 2021. url: https://www.proquest.com/scholarly-journals/tor-browser-forensics/docview/2639736687/se-2.

[2] V. K. Vatsavayi ja K. S. Varma, "Retrieving TOR browser digital artifacts for forensic evidence", teoksessa *Machine Intelligence and Soft Computing*, D. Bhattacharyya ja N. Thirupathi Rao, toim., vol. 1280, Advances in Intelligent Systems and Computing, Singapore: Springer, 2021, s. 265–274, ISBN: 978-981-15-9515-8 978-981-15-9516-5. DOI: 10.1007/978-981-15-9516-5_23.

[3] A. Chetry ja U. Sharma, "Dark web activity on tor – investigation challenges and retrieval of memory artifacts", teoksessa *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 1*, sarja Advances in Intelligent Systems and Computing, vol. 1165, Singapore: Springer, s. 953–964, ISBN: 978-981-15-5112-3 978-981-15-5113-0.

[4] R. R. Chand, N. A. Sharma ja M. A. Kabir, "Advancing web browser forensics: Critical evaluation of emerging tools and techniques", *SN Computer Science*, vol. 6, nro 4, s. 355, 5. huhtikuuta 2025, ISSN: 2661-8907. DOI: 10.1007/s42979-025-03921-6.

[5] M. S. Javed, S. M. Sajjad, D. Mehmood, K. Mansoor, Z. Iqbal, M. Kazim ja Z. Muhammad, "Analyzing tor browser artifacts for enhanced web foren-

sics, anonymity, cybersecurity, and privacy in windows-based systems", *Information*, vol. 15, nro 8, s. 495, 19. elokuuta 2024, ISSN: 2078-2489. DOI: 10.3390/info15080495.

[6] H. Carvey, *Windows Registry Forensics. Advanced Digital Forensic Analysis of the Windows Registry*, 2. painos. Syngress, 2016, ISBN: 978-0-12-803291-6.

[7] "Tor Project | Anonymity Online". (n.d.), url: https://www.torproject.org/ (viitattu 26. 09. 2025).

[8] M. Chertoff, "A public policy perspective of the dark web", *Journal of Cyber Policy*, vol. 2, nro 1, s. 26–38, 2017. url: https://doi.org/10.1080/23738871.2017.1298643.

[9] D. Rathod, "Darknet forensics", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 6, nro 4, s. 77–79, heinäkuu 2017, ISSN: 2278-6856. url: https://www.researchgate.net/profile/Digvijaysinh-Rathod-2/publication/321698383_Darknet_Forensics/links/5a2b896ca6fdccfbbf8540a0/Darknet-Forensics.pdf.

[10] A. Kumar, K. Sondarva, B. N. Gohil, S. J. Patel, R. Shah, S. Rajvansh ja H. P. Sanghvi, "Forensics analysis of TOR browser", teoksessa *Information Security, Privacy and Digital Forensics*, S. J. Patel, N. K. Chaudhary, B. N. Gohil ja S. S. Iyengar, toim., Singapore: Springer, 2024, s. 331–341, ISBN: 978-981-99-5091-1. DOI: 10.1007/978-981-99-5091-1_24.

[11] J. Nurmi, "Understanding the Usage of Anonymous Onion Services. Empirical Experiments to Study Criminal Activities in the Tor Network", väitöskirja, Tampereen yliopisto, Tampere, 2019. url: http://urn.fi/URN:ISBN:978-952-03-1091-2.

[12] H. Carvey, "The windows registry as a forensic resource", *Digital Investigation*, vol. 2, nro 3, s. 201–205, syyskuu 2005, ISSN: 17422876. DOI: 10.1016/j.diin.2005.07.003.

[13] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. Ahmed Memon ja Y. Javed, "Forensic analysis of tor browser on windows 10 and android 10 operating systems", *IEEE Access*, vol. 9, s. 141 273–141 294, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3119724.

[14] M. Parekh ja S. Jani, "Memory forensic: Acquisition and analysis of memory and its tools comparison", *International Journal of Engineering Technologies and Management Research*, vol. 5, nro 2, s. 90–95, 27. huhtikuuta 2020, ISSN: 2454-1907. DOI: 10.29121/ijetmr.v5.i2.2018.618.

[15] H. Nyholm, K. Monteith, S. Lyles, M. Gallegos, M. DeSantis, J. Donaldson ja C. Taylor, "The evolution of volatile memory forensics", *Journal of Cybersecurity and Privacy*, vol. 2, nro 3, s. 556–572, syyskuu 2022, Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 2624-800X. DOI: 10.3390/jcp2030028.

[16] C. Easttom, J. Phelan, S. Steuber, V. I. Balkissoon, W. Butler, R. S. Bhagavatula, K. Rodriquez et al., *Windows Forensics: Understand Analysis Techniques for Your Windows*. Springer, 2024, ISBN: 979-8-8688-0193-8. DOI: https://doi.org/10.1007/978-8-8688-0193-8.

[17] M. Rawashdeh, Q. A. Al-Haija ja M. Qasaimeh, "Analysis of TOR artifacts and traffic in windows 11: A virtual lab approach and dataset creation", teoksessa *2023 14th International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan: IEEE, 21. marraskuuta 2023, s. 1–6, ISBN: 979-8-3503-0786-3. DOI: 10.1109/ICICS60529.2023.10330539.

[18] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal ja Y. A. Bangash, "Forensic analysis of tor browser: A case study for privacy and anonymity on the web", *Forensic Science International*, vol. 299, s. 59–73, kesäkuu 2019, ISSN: 03790738. DOI: 10.1016/j.forsciint.2019.03.030.

[19] A. Warren. "Tor browser artifacts in windows 10". (22. helmikuuta 2017), url: https://www.giac.org/paper/gcfa/10332/tor-browser-artifacts-windows-10/114292 (viitattu 05. 10. 2025).

[20] T. Leng ja A. Yu, "A Framework of Darknet Forensics", teoksessa *Proceedings of the 3rd International Conference on Advanced Information Science and System*, sarja AISS '21, New York, NY, USA: Association for Computing Machinery, 19. tammikuuta 2022, s. 1–6, ISBN: 978-1-4503-8586-2. DOI: 10.1145/3503047.3503082.

[21] G. B. Akintola, "Performance evaluation of four different forensic tools for web browser analysis", *International Journal of Scientific Research in Multidisciplinary Studies*, vol. 10, nro 10, s. 68–82, 31. lokakuuta 2024, ISSN: 24549312. url: https://www.isroset.org/pdf_paper_view.php?paper_id=3655&9-ISROSET-IJSRMS-10019.pdf.

[22] S. Kauser, T. Safdar Malik, M. Hilmi Hasan, E. Akashah P. Akhir ja S. Muhammad Husnain Kazmi, "Windows 10's browser forensic analysis for tracing p2p networks' anonymous attacks", *Computers, Materials & Continua*, vol. 72, nro 1, s. 1251–1273, 2022, ISSN: 1546-2226. DOI: 10.32604/cmc.2022.022475.