Roope Alakärppä

DIGITAALISEN TODISTUSAINEISTON TURVALLINEN HALTUUNOTTO

Opinnäytetyö

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus (ylempi AMK)

2023

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä	Roope Alakärppä
Työn nimi	Digitaalisen todistusaineiston turvallinen haltuunotto
Toimeksiantaja	Tulli
Vuosi	2023
Sivut	61 sivua, liitteitä 5 sivua
Työn ohjaaja	Marko Oras

TIIVISTELMÄ

Tietoteknisten laitteiden yleistynyt käyttö digitaalisessa yhteiskunnassa luo uusia mahdollisuuksia sekä rikollisille että rikostutkijoille. Tämä tutkimus käsittelee digitaalista todistusaineistoa sisältävien tietoteknisten laitteiden turvallista haltuunottoa rikostutkinnassa. Työn tutkimusongelmana oli, että toimeksiantajalla ei ollut henkilöstölle ohjeistusta digitaalisen todistusaineiston turvalliseen haltuunottoon. Työn tavoitteena oli tutkia, miten tietoteknisiin laitteisiin tallentunut digitaalinen todistusaineisto otetaan turvallisesti haltuun.

Työ tehtiin toimintatutkimuksena, joka on interventiotutkimuksen alamuoto. Laadulliselle tutkimukselle tyypillisen ongelman selvittämisen lisäksi työssä luotiin interventio, joka tähtää ongelman poistamiseen. Interventiona toimiva tuotos ohjaa toimeksiantajan henkilöstöä digitaalisen todistusaineiston turvalliseen haltuunottoon. Tutkimukseen valittu aineisto koostui pääosin tutkimusmenetelmänä käytetyn systemoidun kirjallisuuskatsauksen avulla hankitusta vertaisarvioidusta tutkimustiedosta. Aineiston analysointiin hyödynnettiin teemoittelua, jonka tarkoitus oli auttaa työn tulosten käsittelyssä.

Opinnäytetyön tuloksista nähdään, että haltuun otettavien tietoteknisten laitteiden vääränlainen käsittely aiheuttaa haasteita digitaalisen todistusaineiston saatavuuteen, eheyteen ja luottamuksellisuuteen. Haasteita voidaan lieventää oikeilla toimintatavoilla sekä tarkalla dokumentoinnilla. Tietoteknisten laitteiden toimintatapaa voidaan kuitenkin manipuloida anti-forensiikalla, jonka vuoksi tyhjentävää opasta niiden oikeaoppisesta käsittelystä oli hankala luoda.

Työssä tutkittiin digitaalisen forensiikan parhaita käytäntöjä ja saatiin onnistuneesti luotua vakioidut toimintaohjeet, jotka mahdollistavat digitaalisen todistusaineiston turvallisen haltuunoton. Tulosten perusteella digitaalisen todistusaineiston saatavuutta ja eheyttä voidaan parantaa pitämällä avoinna oleva laite käynnissä sekä eristämällä laite verkkoyhteyksistä. Luottamuksellisuutta lisää hallintaketju, johon on dokumentoitu kaikki laitteelle tehdyt toimenpiteet. Työn tulokset kehittävät toimeksiantajan henkilöstön osaamista ja mahdollistavat digitaalisen todistusaineiston paremman hyödyntämisen rikostutkinnassa.

Asiasanat: data, digitaalinen forensiikka, rikostutkinta, todistusaineisto

South-Eastern Finland University of Applied Sciences

Degree title	Master of Engineering
Author	Roope Alakärppä
Thesis title	Secure seizure of digital evidence
Commissioned by	Finnish Customs
Time	2023
Pages	61 pages, 5 pages of appendices
Supervisor	Marko Oras

ABSTRACT

The increased use of information technology devices in the digital society creates new opportunities for both criminals and criminal investigators. This study deals with the secure seizure of devices containing digital evidence in criminal investigations. The research problem was that the commissioner did not have instructions for the staff on the secure seizure of digital evidence. The objective of the study was to investigate how digital evidence stored on information technology devices is seized securely.

The study was conducted as an action research, which is a subform of an intervention study. In addition to qualitive research problem solving, the study created an intervention that aimed to eliminate the problem. The output acting as an intervention directs the commissioners' personnel in the secure seizure of digital evidence. The material selected for the study consisted mainly of peer-reviewed research studies obtained though systematic literature review, which was used as a research method. Thematic analysis was used to analyze the data in order to assist in processing the results of the study.

The results of the thesis show that the mishandling of seized information technology devices poses challenges to the confidentiality, integrity, and availability of digital evidence. These challenges can be mitigated by correct operating methods and accurate documentation. However, the operation of information technology devices can be manipulated with anti-forensics, making it difficult to create an exhaustive guide to their proper handling.

The thesis examined the best practices of digital forensics and successfully created standard operating procedures that enable the secure seizure of digital evidence. The results show that the availability and integrity of digital evidence can be improved by keeping the open device running and by isolating the device from network connections. Confidentiality is ensured by a chain of custody documenting all actions taken on the device. The results of the work develop the skills of the commissioners' personnel and enable better utilization of digital evidence in criminal investigations.

Keywords: criminal investigation, data, digital forensics, evidence

SISÄLLYS

LIITTEET

1 JOHDANTO

Digitaalisella todistusaineistolla viitataan tietoteknisten laitteiden sisältämään tietosisältöön, joka on digitaalisessa muodossa olevaa todisteaineistoa. Tietoteknisen tutkinnan eli digitaalisen forensiikan tarkoitus on todisteiden esille hakemista erityyppisistä tietoteknisistä laitteista, kuten tietokoneista ja mobiililaitteista. Digitaalinen todistusaineisto voi olla mitä tahansa laitteeseen tallentunutta dataa, ja digitaalisen forensiikan käyttö osana rikosten selvittämistä on rikoslajineutraalia. Digitaalisessa muodossa olevat todisteet voivat liittyä kyberrikosten lisäksi myös esimerkiksi talous- ja huumausainerikoksiin. (Sisäministeriö 2017, 44.)

Tietotekniikan kehittyminen ja lisääntynyt tietoverkkojen käyttö lisää entisestään digitaalisen forensiikan tarvetta rikosten tutkinnassa. Se onkin merkittävässä roolissa nykypäivän rikostutkinnassa, mutta tietoteknisten laitteiden vääränlainen käsittely voi pahimmassa tapauksessa jopa hävittää olemassa olevat todisteet. Digitaalisen todistusaineiston turvallinen haltuunotto on kriittinen vaihe todisteiden turvaamisessa ja niiden oikeuskelpoisuuden säilyttämisessä. Tässä tutkimuksessa on tarkoitus tutkia alan parhaita teknisiä käytäntöjä, joilla varmistetaan digitaalisen todistusaineiston luotettavuus ja eheys haltuunoton yhteydessä.

Tiedonhaun perusteella Suomessa ei ole tehty aiheesta vastaavia tutkimuksia, jotka olisivat vapaasti saatavilla. Juhana Riekkisen kirjoittama väitöskirja *Sähköiset todisteet rikosprosessissa* (2019) keskittyy digitaalisen todistusaineiston laillisuusnäkökulmaan. Kansainvälisesti aiheesta on tehty aiempaa tutkimusta, jota analysoidaan työn kirjallisuuskatsauksessa. Kaakkois-Suomen ammattikorkeakoulun (Xamk) kyberturvallisuuden koulutus haluaa erottautua muista Suomen kyberturvallisuuden koulutuksista sillä, että se käsittelee kyberturvallisuutta enemmän teknisestä näkökulmasta. Tämän perusteella on luontevaa, että työssä keskitytään enemmän tekniseen kuin hallinnolliseen näkökulmaan digitaalisen todistusaineiston haltuunottoprosessissa.

Digitaalisen todistusaineiston potentiaalinen hyöty rikosasioissa on saanut lainvalvontaorganisaatiot luomaan ohjeistuksia ja suosituksia parhaista käytännöistä, joilla varmistetaan sen oikeusvarma takavarikointi ja säilytys (Holt ym. 2020, 92). Tämän työn tavoitteena on antaa tutkittuun tietoon perustuva tietopohja digitaalisen todistusaineiston turvallisesta käsittelystä. Tutkimuksen lisäksi opinnäytteen liitteeksi laaditaan tuotos, joka toimii kirjallisena opastuksena sen työvaiheista toimeksiantajaorganisaation henkilöstölle. Työn tuloksia voi hyödyntää myös muut digitaalista forensiikkaa käyttävät organisaatiot. Oppaan laatiminen vaatii syvällistä tietoa aihealueesta, jota tullaan käsittelemään työn teoreettisessa viitekehyksessä ja tuloksissa. Toimeksiantajan rooli on suojella yhteiskuntaa osana Euroopan unionin tulliliittoa, joka antaa tutkimukselle laajemman yhteiskunnallisen merkityksen.

Opinnäytteen tekijä työskentelee toimeksiantajan organisaatiossa rikostutkijana digitaalisen todistusaineiston asiantuntijatehtävissä. Tutkimusaiheen valintaa tukee Tullin strategia 2020–2023, jonka yhtenä kärkiteemana on varmistaa henkilöstön osaaminen (Tulli 2022). Digitaalinen forensiikka on kyberturvallisuuden osa-alue ja tämä työ kuuluu kyberturvallisuuden alaan.

2 DIGITAALINEN FORENSIIKKA

Digitaalinen forensiikka on määritelty tieteellisesti johdettujen ja todistettujen menetelmien käytöksi todistusaineiston tunnistamiseksi, säilyttämiseksi, keräämiseksi ja esittämiseksi niin, että se voidaan ottaa käsiteltäväksi oikeudessa. Sen yleisiä työvaiheita ovat haltuunotto, jäljentäminen, tutkiminen, analysointi ja raportointi. Näiden vaiheiden käyttöä on suositellut muun muassa Yhdysvaltojen tekniikkaa ja standardeja kehittävä National Institute of Standards and Technology (NIST). Tämän määritelmän ja tunnistettujen työvaiheiden perusteella on vuosien varrella ehdotettu lukuisia digitaaliforensisia malleja ja toimintaohjeita, jotka sopivat erilaisiin tutkimusmenetelmiin sekä virastoissa vaihteleviin organisaatiopolitiikkoihin. (Ali ym. 2017, 10; Mothi ym. 2020, 1.)

Alan suurin ongelma on laitteiden ja ohjelmistojen jatkuva tekninen kehitys sekä moninaisuus, jotka vaikeuttavat viitekehysten ja standardointimallien luomista. Aihealueen haasteeksi on todettu myös tutkijoiden riittämätön koulutus, harjoit-

telu ja tieto laitteiden asianmukaisiin haltuunotto-, kuljetus- ja säilytysmenetelmiin. Tässä opinnäytteessä keskitytään digitaalisen forensiikan haltuunottovaiheeseen, jonka tarkoituksena on ottaa haltuun tietotekniset laitteet niiden tietosisältöä muuttamatta. (Ali ym. 2017, 9.)

Perinteisesti tietoteknisten laitteiden haltuunotto on ollut yksinkertaista, sillä laitteiden koko fyysinen muistialue on saatu jäljennettyä ja tutkittua. Tätä kautta on päästy käsiksi myös mahdollisesti poistettuihin tietoihin, joita järjestelmä ei ole vielä ylikirjoittanut uudella datalla. Tämä lähestymistapa oli aiemmin tehokas, kun tiedot olivat tallennettu selkokielisenä ja salaamattomina laitteiden muistiin. Nykyaikaiset laitevalmistajien käyttöönottamat suojamekanismit, kuten laitesalaus on muuttanut digitaalisen forensiikan haltuunottovaiheen merkitystä. Nykyään laitteen koko muistialueen jäljentäminen ei usein pysty tarjoamaan selkokielistä ihmiselle luettavaa dataa. (Fukami ym. 2021, 8.) Salaukset estävät datan lukemisen salausalgoritmilla, jos salausavain ei ole tiedossa (Shafiee Hasanabadi ym. 2020, 3). Siksi laitteen haltuunotto joko salaus purettuna tai salausavaimen hankkiminen on nykyään digitaalisen forensiikan yksi päätavoitteista (Fukami ym. 2021, 8).

2.1 Digitaalisen forensiikan kohteet

Digitaalisen forensiikan kohteena on tietoteknisille laitteille tallentunut digitaalinen tieto eli data, jota voidaan käyttää todisteena rikosasioissa. Digitaalinen todistusaineisto on terminä tarkoituksellisesti moniselitteinen, sillä sitä voidaan löytää kaikista laitteista, jotka ovat verkkoyhteydessä tai tallentavat tietoa sähköisesti. Digitaalisessa muodossa olevaa todistusaineistoa voi löytyä esimerkiksi tietokoneista, älypuhelimista, älykelloista, digitaalikameroista, älytelevisioista ja muista älylaitteista. (Holt ym. 2020, 93.) Mikä tahansa tieto, joka on tallennettu tai poimittu digitaalisesta mediasta, voi olla digitaalinen todiste (Lone & Naaz 2019, 45).

Tässä opinnäytteessä keskitytään kahden erityyppisen laitteen, mobiililaitteen ja tietokoneen, turvalliseen haltuunottoon. Mobiililaitteista puhuttaessa tarkoitetaan usein puhelimia, joita kuitenkin käytetään tällä hetkellä puheluiden lisäksi myös moneen muuhun. Mobiililaitteet ovat jatkuvasti verkkoyhteydessä ja niillä voidaan jakaa erilaista digitaalista sisältöä, kuten videoita ja dokumentteja. (Ali

ym. 2017, 2.) Siksi ne sisältävät usein rikostutkinnan kannalta merkityksellistä dataa, ja puhelimien tutkiminen on tullut lainvalvontaviranomaisille yhä kriittisemmäksi toiminnaksi. Puhelimien yleistyminen päivittäisen elämän tärkeiksi työkaluiksi on kuitenkin kasvattanut loppukäyttäjien huolta laitteiden turvallisuudesta ja yksityisyydestä. Käyttäjien yksityisyyden suojaamiseksi ja tietojen luottamuksellisuuden takaamiseksi, nykyaikaisissa mobiililaitteissa on tällä hetkellä oletuksena käytössä salaustekniikoita. Salausmenetelmiä käytetään usein kahdenlaisia. Toinen on koko levyn salaus (engl. Full Disk Encryption tai FDE) ja toinen tiedostopohjainen salaus (engl. File Based Encryption tai FBE). FDE on tekniikka, jossa koko käyttäjän dataosio salataan yhdellä salausavaimella, kun taas FBE salaa tiedot tiedostokohtaisesti eri avaimilla, jolloin tiedostot voidaan purkaa itsenäisesti. Nykyaikaisten mobiililaitteiden vahvat tietoturvaominaisuudet, kuten laitesalaus, luovat haasteita digitaalista forensiikkaa suorittaville tutkijoille. Tietojen saaminen laitteista on entistä vaikeampaa ja tekninen tutkinta keskittyykin enemmän turvaominaisuuksien ohittamiseen ja haavoittuvuuksien hyödyntämiseen, joiden avulla voidaan murtautua kohdelaitteisiin. (Fukami ym. 2021, 1–2.)

Perinteisesti dataa on käsitelty tietokoneilla ja se on edelleen tärkeä digitaalisen forensiikan kohde. Tietokoneelle tallentuneiden tiedostojen lisäksi niillä käytetään erilaisia järjestelmiä esimerkiksi yrityksen kirjanpitoon. Ne voivat toimia myös tiedostojenjako- tai verkkosivupalvelimina. Tietokoneiden haltuunotossa on samanlaisia haasteita kuin mobiililaitteissa. Näitä ovat muun muassa kiintolevyjen ja tiedostojen salaus sekä datan suuri määrä. Kasvava datan määrä ei näy pelkästään massamuistien tallennustilan kasvamisena, vaan myös laitteiden keskusmuistin kasvuna. Keskusmuistin rooli on kasvanut nykypäivän digitaaliforensisissa tutkimuksissa, koska se saattaa olla ainoa paikka, johon data on tallentunut selkokielisenä. Keskusmuistin analysoinnilla voidaan saada haltuun salausavain tai tietoa haittaohjelmasta, jolla voi olla merkityksellinen rooli tutkinnassa. (Schramp 2017, 44; Latzo ym. 2019, 56.)

2.2 Digitaaliset todisteet rikosprosessissa

Digitaalisen todistusaineiston haltuunottoa suoritetaan rikosten esitutkinnassa. Se on osa rikosprosessia, jossa viranomaiset keräävät rikoksiin ja rikosepäilyihin liittyviä tietoja. Rikosten esitutkinta toimitetaan esitutkintalain mukaisesti ja

tärkeimmät työkalut sen suorittamiseen on säädetty pakkokeinolaissa. Esitutkinta liittyy rikosprosessin alkuvaiheeseen, jossa hankitaan todistusaineistoa ja pyritään selvittämään rikosepäilyn tapahtumainkulkua. Esitutkinnassa hankittua todistusaineistoa voidaan hyödyntää rikosprosessin myöhemmissä vaiheissa, mikäli rikosasia etenee syyteharkintaan ja oikeudenkäyntiin. (Riekkinen 2019, 203–204.)

Suomessa ja Ahvenanmaalla esitutkintaviranomaisia ovat esitutkintalain 2. luvun 1 §:ssä määritetyt viranomaiset. Yleisenä esitutkintaviranomaisena toimii poliisi, jonka lisäksi erityisiä esitutkintaviranomaisia ovat rajavartio-, tulli-, ja sotilasviranomaiset siten, kuin niiden rikostorjuntaa koskevissa laissa on säädetty (Esitutkintalaki 22.7.2011/805, 2. luku 1. § mom. 2). Esitutkintaviranomaisten lisäksi myös muut viranomaiset hankkivat digitaalista todistusaineistoa. Rikostorjunnan sijaan sotilas- ja siviilitiedusteluviranomaiset keräävät esimerkiksi signaalitiedustelun avulla dataa tietoliikenneverkosta terrorismintorjuntaan ja varautumista sotilaallista uhkaa varten. (Riekkinen 2019, 204–205.)

2.2.1 Laite-etsintä

Pakkokeinolain 8. luvun 20 §:ssä määriteltyä laite-etsintää käytetään digitaalisen todistusaineiston löytämiseen ja jäljentämiseen tietoteknisistä laitteista. Käytön edellytyksenä on muun muassa, että rikosepäilystä säädetty ankarin rangaistus on vähintään kuusi kuukautta vankeutta, ja laitteesta voidaan olettaa löytyvän rikokseen liittyvää tietoa (Pakkokeinolaki 22.7.2011/806, 8. luku 21. §). Rikosepäilyjen rangaistusasteikko on nähtävillä rikoslaissa. Esimerkiksi perusmuotoisesta huumausainerikoksesta voidaan tuomita vankeutta enintään kahdeksi vuodeksi, joka mahdollistaa laite-etsinnän hyödyntämisen osana huumausainerikoksen selvitystä (Rikoslaki 30.5.2008/374, 50. luku 1. §).

Mikäli laite-etsinnän edellytykset täyttyvät, viranomainen voi ottaa tietoteknisen laitteen haltuun ja tutkia sen sisältämän tietosisällön. Joissain poikkeustapauksissa todistusaineisto voidaan asettaa hyödyntämiskieltoon, jolloin sitä ei voida hyödyntää esitutkinnassa. Oikeus voi asettaa todistusaineiston hyödyntämiskiellon esimerkiksi toimittajan lähdesuojan vuoksi, kuten korkeimman oikeuden ratkaisussa KKO:2019:112.

Haltuun otettu laite tulisi palauttaa jäljentämisen jälkeen ilman aiheetonta viivytystä. Mikäli jostain syystä laitetta ei voida muutaman päivän sisällä palauttaa takaisin, se voidaan takavarikoida. Pakkokeinolaki (7. luku 1. §) sanoo takavarikoinnin edellytyksistä seuraavasti: ”jos on syytä olettaa, että sitä voidaan käyttää todisteena rikosasiassa, se on rikoksella joltakulta viety, tai se tuomitaan menetetyksi” (Pakkokeinolaki 7. luku 1. §). Takavarikointi ei ole aina tarpeen, sillä laitteesta saatava todistusaineisto voidaan turvata jäljentämällä sen sisältö ja kohdistaa tutkinta laitteesta tehtyyn kopioon. (Riekkinen 2019, 235.)

Jossain tapauksissa viranomaisilla voi olla tarve jäljentää tietoja verkkopalveluista esimerkiksi jonkin tietyn käyttäjätilin osalta. Tällöin laite-etsintä voidaan toimittaa myös etäetsintänä, jolloin viranomaisella ei ole hallussaan itse tietosisällön sisältävää laitetta. Etäetsintää voidaan hyödyntää muun muassa pilvipalveluihin tallentuneiden tietojen jäljentämiseen, jolloin ei ole tarvetta ottaa haltuun tai takavarikoida itse pilvipalvelua tarjoavaa fyysistä palvelinta. (Riekkinen 2019, 235.)

2.2.2 Vapaa todistusteoria

Suomen todistuslainsäädännössä on omaksuttu niin sanottu vapaa todistusteoria, joka käsittää vapaan todistelun ja vapaan todistusharkinnan (Karppinen 2016, 47). Vapaan todistelun perusteet tulevat oikeudenkäymiskaaren 17. luvun 1 §:n 1. momentista. Sen mukaan ”asianosaisella on oikeus esittää haluamansa näyttö asian tutkivalle tuomioistuimelle ja antaa lausunto jokaisesta tuomioistuimessa esitetystä todisteesta, jollei laissa toisin säädetä” (Oikeudenkäymiskaari 12.6.2015/731, 17. luku 1. §). Sisällöltään todisteilla ei yleensä ole selkeitä rajoja, vaan se on viime kädessä prosessia johtavan tuomarin hallinnassa (Riekkinen 2019, 74). Tämän vuoksi todistusaineistona on mahdollista hyödyntää erilaisia digitaalisia todisteita laajasti, riippumatta siitä mistä ne ovat peräisin.

Vapaan todistusharkinnan periaatteella tarkoitetaan sitä, että erilaiset muotosäännöt eivät rajoita tuomarin harkintavaltaa, vaan hän päättää todisteiden näyttöarvosta ja riittävyydestä oman harkintansa perusteella. Oikeudenkäymiskaaren 17 luvun 1 §:n 2. momentin mukaan tuomioistuimen tulee ottaa huomioon asian käsittelyn aikana esiin tulleet todisteet ja muut seikat ennen kuin se

tekee päätöksen siitä, mitä asiassa on pidettävä totena. (Riekkinen 2019, 75.) Momentin toisen virkkeen mukaan ”tuomioistuimen on perusteellisesti ja tasapuolisesti arvioitava todisteiden ja muiden seikkojen näyttöarvo vapaalla todistusharkinnalla, jollei laissa toisin säädetä” (Oikeudenkäymiskaari 17. luku 1. §). Kiteytettynä vapaa todistusteoria antaa asianosaisille mahdollisuuden esittää vapaasti erilaisia todisteita ja tuomioistuimen harkita, minkä merkityksen se esiin tulleille seikoille antaa päätöksessään.

2.3 Alkuperäisyys ja eheys

Digitaalinen todistusaineisto eli data eroaa huomattavasti perinteisistä paperidokumenteista. Tietoteknisille laitteille tallennetut tiedot ovat alttiita muun muassa tahallisille tai tahattomille muutoksille sekä häviämiselle, tuhoutumiselle ja vioittumiselle, vaikka ne olisivat edelleen tekijänsä hallussa. Dataa voidaan myös siirtää, jakaa ja kopioida helposti, ja sen käytettävyyteen vaikuttaa muun muassa laitteiston ja ohjelmiston yhteensopivuus. Joskus myös tiedon tekijää, alkuperää ja hallintaketjua (engl. Chain-of-custody tai CoC) voi olla vaikeaa tai mahdotonta määrittää. Hallintaketju on määritelty prosessiksi, jota käytetään todisteiden kronologisen historian ylläpitämiseen ja dokumentointiin. Hallintaketju antaa mahdollisuuden dokumentoida ja raportoida kaiken mitä todisteille on tapahtunut hankkimishetkestä lopulta sen esittämiseen oikeudessa. Digitaalisen forensiikan tavoitteena on varmistaa, että löydetyt digitaaliset todisteet ovat oikeudessa hyväksyttäviä. (Bulbul ym. 2013, 254; Rogers 2015, 101.) Tämän vuoksi datalta vaaditaan hallintaketjun ylläpitämistä ja sitä on ylläpidettävä koko tutkintaprosessin ajan (Lone & Naaz 2019, 45). Vaikka tutkija luottaa tiedon alkuperäisyyteen ja ylläpitää katkeamatonta alkuperäketjua, datan haavoittuvuus ja herkästi särkyvä luonne vaatii silti sen erityisen huolellista käsittelyä. Lisäksi luotettavuus ja tarkkuus eivät ole enää suoraan yhteydessä alkuperäisyyteen, sillä ne voivat vaarantua joko yhdessä tai erikseen. (Rogers 2015, 102.)

Todisteiden eheyden säilyttäminen on ensiarvoisen tärkeää sekä fyysisissä että digitaalisissa todisteissa. Eheys käsitteenä tarkoittaa, että digitaalista tietoa ei tarkoituksellisesti tai vahingossa muuteta alkuperäisestä ilman asianmukaista lupaa. Digitaalisissa todisteissa tämä tarkoittaa, että tiedot pysyvät muuttumat-

tomina, kun niitä hankitaan, analysoidaan ja raportoidaan. Mikäli dataa jäsennellään tai muuten muokataan esimerkiksi raportointia varten, se tulisi aina suorittaa datasta tehtyyn kopioon. Alkuperäinen todistusaineisto tulisi aina säilyttää koskemattomana sen eheyden varmistamiseksi. (Meffert ym. 2016, 87, 89.)

Useimmat ymmärtävät intuitiivisesti alkuperäisyyden aitouden ominaisuutena, mutta harva pystyy tunnistamaan tarkalleen mitä sen varmistamiseen, arvioimiseen ja takaamiseen vaaditaan. Alkuperäisyyden on historiallisesti ymmärretty johtuvan asiakirjojen luomisolosuhteista ja säilytystavasta sekä -paikasta. Asiakirjan allekirjoitus sekä todistajien läsnäolo vahvistivat asiakirjan aitouden. Mikäli asiakirjan aitoutta epäiltiin, voitiin kuulustella allekirjoittajia ja todistajia sen alkuperäisyyden todentamiseksi. (Rogers 2015, 99.)

Alkuperäisyyden määritelmäksi on esitetty, että tieto on sitä mitä se väittää olevansa, sen on luonut tai lähettänyt henkilö, jonka väitetään luoneen tai lähettäneen sen, ja se on luotu tai lähetetty väitettynä aikana. Tieto on siis alkuperäistä, kun se vastaa sitä mitä sen väitetään olevan eikä sitä ole millään tavalla peukaloitu. Alkuperäiset tiedot ovat sellaisia, joiden aitous voidaan varmistaa, ja joiden eheys voidaan osoittaa katkeamattomalla hallintaketjulla. Tiedon alkuperäisyys ei kuitenkaan takaa sisällön luotettavuutta, sillä sisältö voi alun perinkin voinut olla epäluotettavaa. (Rogers 2015, 100–101.)

3 TUTKIMUSASETELMA

Ylemmän ammattikorkeakoulun opinnäyte on tieteellinen työ, jossa täytyy olla ongelma. Ilman ongelman määritystä on mahdotonta tehdä tutkimusta tieteellisenä. Tutkimustehtävän tarkka rajaaminen ja määrittely ovat tärkeitä, koska sen on tarkoitus ohjata koko tutkimusprosessia. (Kananen 2017b, 56.) Työn tutkimusongelmana oli, että Tullin valvontaosastolla ei ollut ohjeistusta digitaalisen todistusaineiston turvalliseen haltuunottoon. Aihealueen syvällisempi osaaminen on vain hiljaista tietoa heillä, jotka ovat erikseen saaneet siihen koulutuksen. Myös henkilöillä, jotka ovat saaneet siihen koulutuksen, ei ole yhtenäistä tapaa toimia eli menetelmiä, joilla varmistetaan haltuun otettavien tietoteknisten laitteiden turvallinen käsittely. Tilanteita, joissa tulee ottaa haltuun tietoteknisiä laitteita, voi tulla yllättäen sekä harvoin, jolloin saatu koulutus voi myös unohtua.

Tutkimusaiheet ovat melkein aina liian laajoja kokonaisuuksia, jotta niistä selviäisi loppuun asti saamalla aikaan opinnäytetyön. Erilaisten tietoteknisten laitteiden kirjo on suuri ja kasvaa jatkuvasti. Tässäkin työssä tietoteknisten laitteiden kirjo on liian laaja yksittäisen tutkielman aiheeksi, jonka vuoksi tutkimusaihetta tulee rajata. Rajaamisella tarkoitetaan sitä, mitä tekijöitä työssä otetaan huomioon ja mitä jätetään työn ulkopuolelle. Rajaaminen on tärkeää ilmiön ongelman hallinnassa ja itse tutkimuksen toteutumisen mahdollistamisessa. Se tapahtuu usein ongelman hahmottuessa ja tutkimuksen edetessä. (Kananen 2017b, 57–58.)

Tämän työn rajaus fokusoitui toimeksiantajalle merkityksellisimpiin digitaalista todistusaineistoa sisältäviin laitteisiin. Nämä ovat käytännössä yleisimpiä verkkoon kytkettyjä päätelaitteita ja niiden toimintaa ohjaavia käyttöjärjestelmiä sekä ohjelmistoja, jotka vaikuttavat digitaalisen forensiikan prosessiin. Työn ulkopuolelle jätettiin erilaiset esineiden internet -laitteet (engl. Internet of Things tai IoT). IoT-laitteisiin ei ole luotu standardeja turvalliseen käsittelyyn, sillä niistä kaivataan vielä lisätutkimusta (Markakis ym. 2020, 1199). Kotona ja yrityskäytössä olevien verkkolaitteiden forensiikkaa olisi ollut myös mielenkiintoista tutkia, mutta opinnäytteen kokonaisuuden hallittavuuden vuoksi se jätettiin työn ulkopuolelle.

3.1 Tutkimuskysymykset

Tutkimuksen taustalla oleva tutkimusongelma muutetaan tutkimuskysymyksiksi, jotka helpottavat itse tutkimusprosessia. Niiden tarkoitus on ohjata aineistonkeruuta ja tutkimusta. Yksittäinen tutkimuskysymys ei ole yleensä riittävä ja sitä täydennetään metakysymyksillä, jotka toimivat tutkimuksen apukysymyksinä. Näihin kysymyksiin saadut vastaukset ratkaisevat tutkimusongelman. Onnistuneilla tutkimuskysymyksillä saadaan myös hahmotettua opinnäytetyön runkoa. (Kananen 2017b, 60–61.)

Ensisijaisesti työssä pyrittiin vastaamaan siihen, *miten tietotekninen laite otetaan turvallisesti haltuun*. Tutkimuksen apukysymyksinä olivat *mitkä tekijät vaikuttavat prosessiin*, *miten katoava data saadaan taltioitua* sekä *millä keinoilla voidaan varmistaa digitaalisen todistusaineiston alkuperäisyys ja eheys*. Näihin

kysymyksiin vastaamalla voidaan tulosten pohjalta luoda työn tuotos, joka ratkaisee tutkimusongelman.

3.2 Tavoite

Työn tavoitteena oli tutkimusasetelmassa määritellyn ongelman poistaminen. Ongelman poistaminen vaati yhtenäisten menetelmien luomisen, joilla varmistetaan digitaalisen todistusaineiston turvallinen haltuunotto. Opinnäytetyön liitteeksi oli tarkoitus luoda oppaat tietoteknisten laitteiden turvalliseen haltuunottoon, jotka merkitään salatuiksi. Tarkoituksena oli tehdä kaksi eri versiota, jotka ovat tarkoitettu eri kohdehenkilöille. Toinen opas on suunnattu taktisille tutkijoille, joka kuvaa välttämättömät alkutoimet, joilla varmistetaan laitteiden turvallinen haltuunotto. Toinen opas on suunnattu tietoteknisille tutkijoille, joiden päätehtävä on turvata digitaalinen todistusaineisto. Sen sisältö on laajempi, joka sisältää myös katoavan datan taltiointia haltuun otettavista tietoteknisistä laitteista.

3.3 Metodologiset valinnat

Työn tutkimusongelmaan luotu ratkaisu vaati syvällistä ymmärrystä ilmiöstä, johon perehdyttiin analysoimalla aihealueen aiempia tutkimuksia. Tämän kaltaiseen tutkimukseen sopii käytettäväksi kvalitatiivinen eli laadullinen tutkimusote. Kvalitatiivinen tutkimus soveltuukin parhaiten käytettäväksi, kun ilmiöstä halutaan saada holistinen näkemys (Kananen 2017b, 33).

Tutkimuskysymykset ja tavoite määrittävät työssä käytettävät tutkimusmetodit. Työn tavoite pyrki ongelmanratkaisuun, joka voidaan saavuttaa vain teoilla. Tämän vuoksi pelkästään laadullisen tutkimuksen ilmiön kuvaus ei ole riittävä. Työn voidaan katsoa olevan interventionistinen, sillä siinä tehtiin laadulliselle tutkimukselle tyypillisen ongelman selvityksen lisäksi interventio. Interventio on keino, joka pyrkii muutokseen ja ongelman poistamiseen. Interventiotutkimus on yläkäsite muutokseen pyrkiville tutkimusmuodoille, joita ovat toimintatutkimus, kehittämistutkimus ja konstruktiivinen tutkimus. (Kananen 2017a, 10, 35.)

Syrjälän ym. (1994, 17) mukaan toimintatutkimus tarkoittaa muun muassa oman työn kehittämistä ja tutkimista käytännön työelämässä. Se on ammatilli-

sen kehittymisen ja oppimisen prosessi, johon liittyy työelämän käytännön ongelmien tunnistaminen ja niiden poistaminen. Kehittämistutkimuksen ja toimintatutkimuksen tavoitteena on luoda tuotos sillä erolla, että toimintatutkimuksen muutos kohdistuu usein ihmisten toimintaan (Kananen 2019, 84). Kuten nimestä voi päätellä, toimintatutkimuksen tarkoitus on viedä tutkimus mukaan toimintaan ja se antaa myös toimijan itse osallistua prosessiin. Toimintatutkimuksessa katsotaan yleisesti eduksi, että tutkijalla on jonkinlainen rajapinta aiheensa varsinaiseen ilmiöön. (Kananen 2014, 11, 16.)

Tämän tutkimuksen voidaan katsoa kuuluvan toimintatutkimukseen, jonka oleellisia elementtejä ovat tutkimus, toiminnan kehittäminen, yhteistoiminta ja tutkijan mukana oleminen (Coghlan & Brannick 2010, 4). Tietoa digitaalisen todistusaineiston haltuunotosta viranomaistoiminnassa voidaan saada haastattelujen, havaintojen ja aiempien tutkimusten kautta, mutta tietoa sen syvimmistä prosesseista voidaan saavuttaa ja kokea vain itse toiminnan kautta. Lisäksi laki viranomaisten toiminnan julkisuudesta saattaa hankaloittaa haastattelun saantia ja niiden sisältöä julkiseen opinnäytetyöhön. Suppealla haastattelulla saatava tieto ei ole riittävä, sillä prosessit sisältävät usein piilotietoa, jota ei voida nähdä ilman osallistumista prosessiin. (Kananen 2017a, 35.) Työn tuotoksen sisältö vaati myös yhteistyötä toimeksiantajaorganisaatiossa työskentelevien asiantuntijoiden kanssa. Organisaation asiantuntijoiden mukanaolo intervention kehittämisessä antaa sille luotettavuutta ja mahdollistaa paremmin sen, että sitä voidaan hyödyntää organisaatiossa.

3.4 Aiemmat tutkimukset

Aiheeseen liittyviä aiempia tutkimuksia kotimaisista opinnäytetöistä haettiin finna.fi-hakupalvelun kautta. Hakulausekkeena käytettiin Boolen operaattoria suomeksi ja englanniksi aineistoista ajalta 2012–2022. Suomenkielinen hakulauseke oli: **”elektroninen todistusaineisto” OR ”digitaalinen todistusaineisto” OR ”digitaalinen forensiikka”**. Englanninkielisenä hakulausekkeena käytettiin: **”electronic evidence” OR ”digital evidence” OR ”digital forensics”**. Näiden tuloksena löytyi yhteensä neljä tutkimusta, jotka olivat vähintään ylemmän korkeakoulutason opinnäytetöitä tai väitöskirjoja. Tätä tutkimusta vastaavaa työtä ei aineistosta löytynyt. Lähimpänä aihetta oli Juhana Riekkisen

väitöskirja *Sähköiset todisteet rikosprosessissa* (2019), jossa tutkittiin digitaalisen todistusaineiston todistusoikeutta rikosprosessissa.

Alustavaa tietoa ulkomailla tehdyistä aihealueen tutkimuksista haettiin Kaakkois-Suomen ammattikorkeakoulun kirjaston (Kaakkuri) ulkomaisten artikkelien haulla. Hakulauseke **"digital forensics" AND secure* AND seizure** tuotti yhteensä 85 tulosta. Kun tulokset rajattiin koskemaan vain vuosien 2012–2022 vertaisarvioituja tutkimuksia, joissa on kokoteksti saatavilla, saatiin hakutuloksia 48 kappaletta. Näistä mainittakoon esimerkiksi Halil Ibrahim Bulbulin ym. (2013) *Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM)*. Tutkimus perustuu kirjallisuuskatsaukseen, ja siinä on muodostettu menettelymalli digitaalisen todistusaineiston haltuunotosta rikospaikalla. Malli perustuu kirjallisuuskatsauksessa tunnistettuihin 25:en eri rikospaikan toimintaohjeeseen. Tämäntyyppisten tutkimusten voidaan katsoa olevan äärimmäisen hyödyllisiä tämän opinnäytteen tausta-aineistona.

3.5 Tutkimusmenetelmä

Kirjallisuuskatsauksen katsotaan olevan systemaattinen tutkimusmenetelmä, joka perustuu tieteelliseen ja prosessimaiseen toimintaan (Suhonen ym. 2016, 7). Se perehdyttää tutkijan aiheeseen ja antaa lisätietoa ilmiöstä sekä siitä aiemmin tehdyistä tutkimuksista. Kirjallisuuskatsauksen voidaan katsoa olevan metodi ja tutkimustekniikka, jonka avulla tutustutaan ilmiön aiempaan tutkimustietoon. Sen tarkoituksena on koota aiempien tutkimusten tuloksia, joiden pohjalta voidaan luoda uusia tutkimustuloksia. (Kananen 2019, 40.) Kirjallisuuskatsaus voidaan jakaa kolmeen erityyppiseen lähestymistapaan. Näistä yleisimmin käytetään kuvailevaa kirjallisuuskatsausta, jossa ei ole määritelty tarkasti tiukkoja sääntöjä. Muita lähestymistapoja ovat meta-analyysi sekä systemaattinen kirjallisuuskatsaus. Näissä tekniikoissa noudatetaan tarkemmin niille ominaisia kriteerejä ja niiden huolellinen käyttö lisää tutkimuksen luotettavuutta. (Salminen 2011, 6, 11.)

Systemaattinen kirjallisuuskatsaus on näyttöön perustuvaa, joka tarkoittaa tutkitun tiedon käyttämistä päätöksentekoon. Työn tuotoksessa on tarkoitus etsiä tuloksellisin ja tehokkain toimintatapa, jossa hyödynnetään näyttöön perustuvaa päätöksentekoa. Tämä kytkeytyy parhaista käytännöistä oppimisen (engl.

best practices) sekä benchmarking-malleihin, joissa etsitään paras toimintatapa tutkimuksen avulla. (Salminen 2011, 10.) Salakari (2020, 3, 13) on käyttänyt Turun ammattikorkeakoulun koulutusaineistossaan systemaattista ja systemoitua kirjallisuuskatsausta synonyymeinä, jossa hän esittää, että systemoituun katsaukseen tarvitaan useampi kuin yksi tekijä. Suhonen ym. (2016, 14) taas erottelee Turun yliopiston julkaisussa systemoidun katsauksen olevan systemaattisen katsauksen alatyyppi. Eroavaisuudeksi mainitaan, että systemoidun katsauksen tekee yleensä vain yksi tutkija, kun taas systemaattisessa katsauksessa on kaksi tai useampi tutkija sen eri vaiheissa. Systemoidun katsauksen aineiston arviointi, analyysi ja synteesi eivät myöskään ole niin kokonaisvaltaisia ja järjestelmällisiä kuin systemaattisessa katsauksessa. Suhosen ym. mukaan työn tutkimusmenetelmän voidaan siis katsoa olevan systemoitu kirjallisuuskatsaus, jossa on systemaattisen kirjallisuuskatsauksen piirteitä. (Suhonen ym. 2016, 14.) Valitun tutkimusmenetelmän tavoitteena oli antaa organisaatiolle viimeisimpään tutkimustietoon pohjautuvia parhaita käytäntöjä, joilla varmistetaan päätelaitteiden oikeaoppinen käsittely todisteiden turvaamiseksi.

3.5.1 Aineistonkeruumenetelmät

Työn laadullinen tutkimusote kytkeytyy vahvasti aineistonkeruumenetelmään. Aineisto voi perustua primääriaineistoon eli työtä varten tehtyyn aineistoon tai sekundääriseen aineistoon, kuten jo olemassa oleviin tutkimuksiin. Työn metodologisissa valinnoissa pohdittiin, että esimerkiksi haastattelulla saatava tieto olisi todennäköisesti liian suppeaa ja tarkoituksenmukaisempaa olisikin käyttää tutkittuun näyttöön perustuvaa aineistoa. Haastattelut ovat yleinen aineistonkeruutapa, mutta tässä työssä sekundääriaineiston voidaan katsoa olevan parempi keino tutkimusongelman ratkaisuun. Menetelmän valinnan tuleekin lähteä tutkimuksellisista perusteista, eikä siitä mikä olisi tutkijalle mieleisin. (Kananen 2019, 28–29.)

Kirjallisuuskatsauksen aineistonkeruu aloitetaan muotoilemalla hakusanat tutkimuskysymyksistä. Hakusanat ovat kriittisessä roolissa, sillä ne määräävät hakutulosten ja aineiston kattavuuden. Tulosten luotettavuuteen tulee myös kiinnittää huomiota ja tarkastella kriittisesti aiheesta tehtyä tutkimusta. Tutkija voi olla myös eri mieltä tutkimuksissa väitetyistä asioista. (Kananen 2019, 41.)

3.5.2 Aineiston analyysimenetelmät

Systemaattinen kirjallisuuskatsaus vaatii analyyttisen otteen, jotta se ei ole vain pelkkä katsaus tai kooste aihealueen kirjallisuudesta. Aineiston kriittinen tarkastelu tuo parhaimmillaan esiin aiempien tutkimusten aukkoja tai puutteita, joista voidaan löytää aiheita uusille tutkimuksille. Analyysimenetelmä on sidoksissa aineistonkeruumenetelmään, joka määrää lähestymistavan aineistossa käytettävään analyysimenetelmään. (Kananen 2019, 40, 55.)

Aineiston analyysiin on monia tapoja. Erityisesti laadullisen tutkimuksen analysointi koetaan usein vaikeaksi, sillä vaihtoehtoja on paljon eikä analyysiin ole tiukkoja sääntöjä. Analyysimenetelmät voidaan kuitenkin jakaa kahteen eri pääkategoriaan, jotka ovat selittämiseen ja ymmärtämiseen pyrkivät lähestymistavat. Ymmärtämiseen pyrkivässä käytetään usein laadullista analyysia ja selittämiseen pyrkivässä tavallisesti tilastollista analyysia. Analyysimenetelmän valinnan tulee tukea tutkimustehtävää ja valinta perustuu siihen, mikä tapa tuo parhaiten ongelmaan vastauksen. Laadullisen aineiston tyypillisimmät analyysimenetelmät ovat tyypittely, teemoittelu, sisällönerittely, keskusteluanalyysi sekä diskurssianalyysi. (Hirsjärvi ym. 2013, 224.)

Tutkimusta tukee parhaiten ymmärtämiseen pyrkivä laadullinen analyysi. Analyysimenetelmänä käytettiin teemoittelua, joka on laadullisen tutkimuksen analyysimenetelmä ja sisällönanalyysin muoto. Teemoittelussa aineistosta etsitään olennaisimmat teemat eli aiheet, jotka liittyvät tutkimusongelmaan. (Juhila 2021.) Teemoittelua käytetään usein teemahaastattelussa, mutta tässä työssä sen tavoitteena oli paikantaa tutkimusongelmaan liittyviä aihealueita, joista muodostettiin työn runkoa. Aineistosta johdettiin analyysin perusteella tulokset ja johtopäätökset, joiden perusteella muodostettiin työn tuotos.

4 TOTEUTUS

Työssä toteutettu systemoitu kirjallisuuskatsaus tehtiin tutkimuksellisena, joka pyrkii virheettömyyteen ja toistettavuuteen. Katsaus tehtiin yksin, jonka vuoksi sen luotettavuuden arviointiin kiinnitettiin erityistä huomiota tarkalla ja kattavalla dokumentaatiolla. Huolellisesti tehty kirjallisuuskatsaus on tärkeää työn onnistumisen kannalta, sillä huolimattomasti tehty katsaus tuottaa epäluotettavaa tietoa. (Pudas-Tähkä & Axelin 2007, 46.)

Kirjallisuuskatsaus tehdään hakemalla aineistoja tutkijoiden määrittelemillä hakusanoilla. Vain yhdellä hakusanalla hakeminen tuo usein liikaa sekä epäolennaisia hakutuloksia. Hakusanojen yhdistämisellä hakulausekkeiksi voidaan rajata ulos aiheeseen liittymättömiä tuloksia Boolen logiikalla. Hakusanojen yhdistäminen tapahtuu käyttämällä Boolen operaattoreita AND, OR ja NOT. AND- ja NOT-operaattori rajaa hakutuloksia, sillä AND tarkentaa hakua yhdistämällä hakusanoja ja NOT poissulkee hakutuloksista määritellyn hakusanan sisältävän artikkelin. Hakutulosten laajentaminen tapahtuu OR-operaattorilla, joka ottaa hakutuloksiin mukaan molemmat määritellyt hakusanat. Hakulausekkeissa voidaan myös yhdistää AND- ja OR-operaattoreita sulkeilla, sekä hakusanoja sitaateilla, jos hakusana on monisanainen. Sitaattien käyttöä kutsutaan fraasihauksi, jota käytetään, kun hakusana sisältää kaksi tai useampaa sanaa. (Xamk 2022a.)

4.1 Hakulausekkeet

Tutkimuskysymysten pohjalta suoritettiin testihakuja tietokantoihin, joiden tulosten avulla muodostettiin hakulausekkeita käyttämällä Boolen logiikkaa. Testihaussa perehdyttiin tietokantojen ominaisuuksiin ja hakulausekkeet muodostettiin niin, että ne toimivat sellaisenaan jokaisessa tutkimukseen valitussa tietokannassa. Testihaussa kävi ilmi, että digitaalisen forensiikan lisäksi tutkimuksia on tehty useista pienemmistä osa-alueista, jotka ovat keskittyneet vain tiettyihin laitteisiin. Näitä ovat muun muassa tietokone-, mobiili-, verkko- ja muistiforensiikka. Hakutulosten rajaaminen digitaaliseen forensiikkaan sekä näiden kaikkien osa-alueiden kattavuuden varmistamiseksi, hakulausekkeisiin lisättiin digitaalisen forensiikan sijaan vain sana forensiikka. Kaikki hakulausekkeet muodostettiin suomenkielisen tutkimuksen puutteen vuoksi vain englannin kielellä.

Digitaalisen todistusaineiston turvalliseen haltuunottoon liittyviä tutkimuksia haettiin sen suoralla käännöksellä. Hakulauseke ottaa huomioon sekä digitaalisen että elektronisen todistusaineiston, sillä molempia termejä esiintyy alan tutkimuksissa. Haltuunotto on lisäksi huomioitu kahdella eri kirjoitusasulla.

Hakulauseke 1: (digital OR electronic) AND evidence AND secure AND (seizing OR seizure) AND forensics.

Työn tutkimussuunnitelmassa tehdyn alustavan tiedonhaun ja perehtymisen perusteella oli jo tiedossa erilaisia tekijöitä, jotka vaikuttavat digitaalisen forensiikan prosessiin. Näitä ovat ainakin salaukset, anti-forensiset prosessit sekä verkkoyhteydet. Yhdistämällä hakulausekkeeseen tiedossa olevia tekijöitä, saadaan niistä haettua lisätietoa. Näiden avainsanojen sisältämistä artikkeleista on myös mahdollista löytää prosessiin vaikuttavia lisätekijöitä. **Hakulauseke 2: encryption AND anti-forensics AND network AND forensics.**

Katoavan datan taltiointi liittyy usein laitteiden keskusmuistissa olevaan tietosisältöön. Tekniikoita sen taltiointiin haettiin yhdistämällä kaksi eri termiä, jotka viittaavat katoavaan dataan tai muistiin.
Hakulauseke 3: ("volatile data" OR "volatile memory") AND forensics.

Digitaalisen todistusaineiston käsittely nojaa vahvasti tietoturvan perusperiaatteisiin, kuten luottamuksellisuuteen ja eheyteen. Näillä pyritään varmistamaan, että digitaalisessa muodossa oleva data on alkuperäistä, eikä sitä ole muokattu. Luotettavuutta todisteiden alkuperäisyyteen ja eheyteen tuo tarkasti dokumentoitu hallintaketju tai kirjausketju, jotka otettiin myös mukaan neljänteen hakulausekkeeseen.
Hakulauseke 4: (integrity OR authenticity) AND ("chain-of-custody" OR "audit trail") AND (digital OR electronic) AND evidence AND forensics.

4.2 Tietokannat

Hakulausekkeiden avulla aineistoa haettiin Kaakkois-Suomen ammattikorkeakoulu Xamkille hankituista e-aineistoista. Haku suoritettiin neljään eri ulkomaisten artikkelien tietokantaan, Academic Search Elite (EBSCO), Emerald Premier, Sage Premier sekä Science Direct. Tietokantojen valinta perustui siihen, että ne kaikki sisältävät tekniikan alaan liittyviä artikkeleita. Valitut tietokannat ja niiden sisältö on kuvattu taulukossa 1.

Taulukko 1. Käytetyt tietokannat ja niiden sisältö.

ID	Tietokanta	Sisältö
A	Academic Search Elite (EBSCO)	Eri alojen artikkeleita ml. tekniikka ja tiede.

B	Emerald Premier	Artikkeleita useilta eri aihealueilta, kuten tekniikasta.
C	Sage Premier	Monialainen tietokanta, joka sisältää tiede- ja teknologia-alan lehtiä ja artikkeleita.
D	Science Direct	Monialainen tietokanta e-lehdistä ja niiden artikkeleista ml. tekniikan aihealueelta.

Tietokannoille annettiin oma tunniste (ID), jota käytettiin hakutulosten raportoinnissa. Myös hakulausekkeille annettiin niiden määrittelyn yhteydessä numerotunniste (1–4), jonka tarkoitus oli yksinkertaistaa hakutulosten raportointia. Esimerkiksi tietokantaan C suoritettu hakulauseke 3 tarkoittaa, että Sage Premier -tietokannasta haettiin aineistoa hakulausekkeella: **("volatile data" OR "volatile memory") AND forensics**.

4.3 Sisäänotto- ja poissulkukriteerit

Kirjallisuuskatsaukselle laadittiin sisäänotto- ja poissulkukriteerit, joiden perusteella kerätty aineisto karsittiin ensin otsikkotasolla, sitten abstraktitasolla ja viimeiseksi koko tekstin perusteella (taulukko 2). Sisäänotto- ja poissulkukriteerien tulee olla tarkoituksenmukaisia, jotta niillä saatu tieto antaa vastaukset tutkimukselle määriteltyihin tutkimuskysymyksiin. Niiden tarkka ja täsmällinen kuvaus antaa myös tutkimukselle luotettavuutta ja ehkäisee systemaattisia virheitä. (Pudas-Tähkä & Axelin 2007, 48.)

Taulukko 2. Aineiston sisäänotto- ja poissulkukriteerit.

Sisäänottokriteerit	Poissulkukriteerit
Vertaisarvioitu tutkimusartikkeli	Ei vertaisarviointia eikä tutkimusartikkelin tuntomerkkejä
Julkaisuvuosi on 2012–2022 ja sisältö ajantasaista	Artikkeli on julkaistu ennen vuotta 2012 tai koskee vanhentunutta tekniikkaa
Julkaisukieli on suomi tai englanti	Julkaistu muulla kielellä kuin englanniksi tai suomeksi
Kokoteksti saatavilla	Julkaisua ei ole saatavilla kokonaisuudessaan
Artikkelin sisältö liittyy tutkimusongelmaan tai rajauksen mukaisiin päätelaitteisiin	Artikkelin sisältö ei liity tutkimusongelmaan tai keskittyy muihin, kuin tietokoneisiin ja mobiililaitteisiin
Hyväksytään eri metodein tehdyt tutkimukset	

Valituista tietokannoista Emerald Premier, Sage Premier ja Science Direct sisältävät vain vertaisarvioituja artikkeleita. Academic Search Elite mahdollistaa sen laittamisen hakukriteeriksi. Julkaisuvuosi sekä kokotekstin saatavuus voidaan lisäksi asettaa kaikissa tietokannoissa hakuehdoiksi. Artikkeleiden tutkimuskohde saadaan selville otsikon ja abstraktin perusteella, mutta artikkeleiden tutkimuksellisuutta voidaan arvioida vasta, kun ne on valittu tarkempaan sisällönanalyysiin. Kriteerien tarkoituksena oli saada aihealueesta luotettavaa ja viimeisintä tutkimustietoa, jonka avulla tutkimusongelma ratkaistaan.

4.4 Tutkimusten valinta ja laadunarviointi

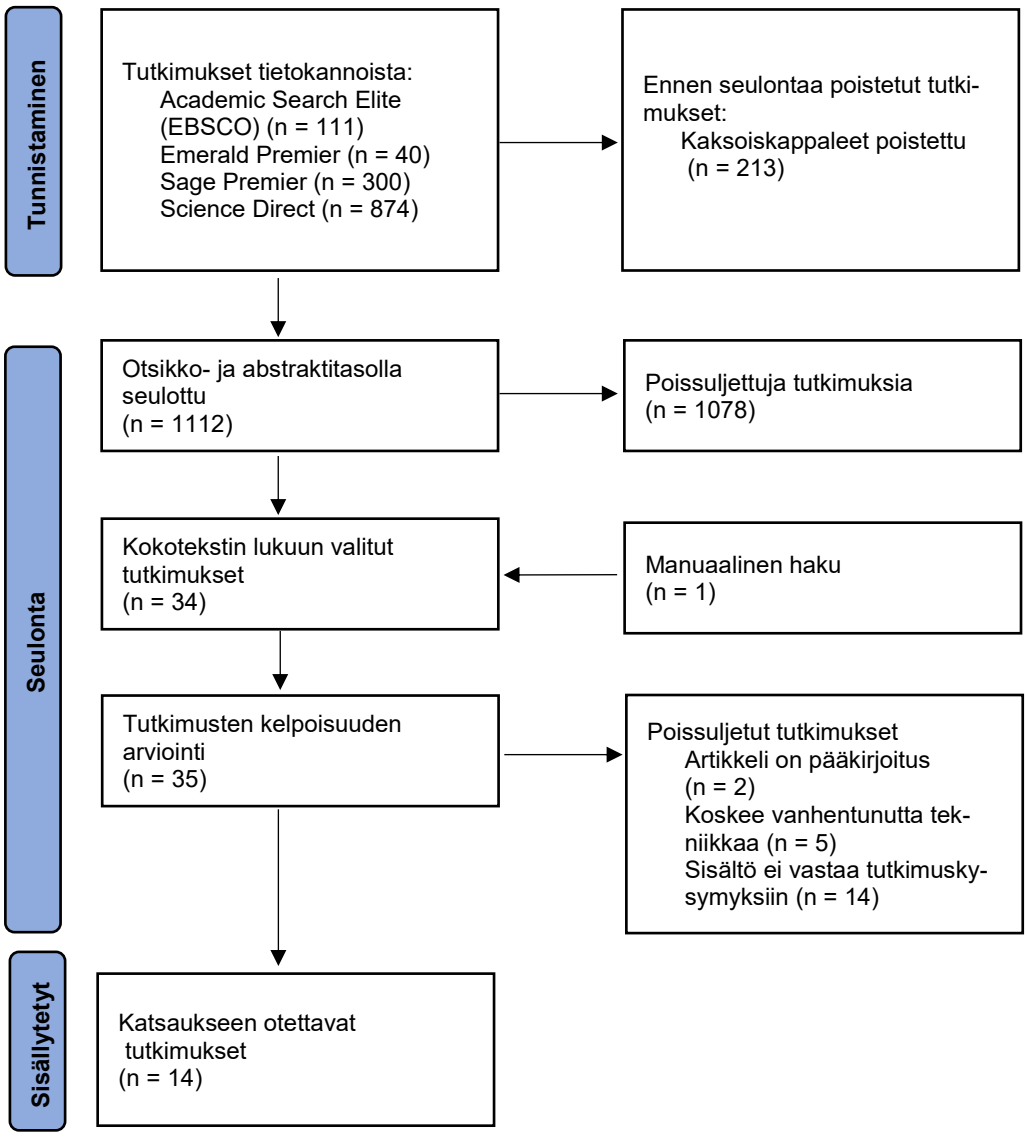
Valituilla hakulausekkeilla suoritettiin hakuja valittuihin tietokantoihin käyttämällä kirjallisuuskatsaukselle määriteltyjä sisäänotto- ja poissulkukriteerejä hakuehtoina. Haut tehtiin maaliskuussa 2022 ja hakutulosten viitteet tuotiin viitteidenhallintaohjelmaan käsiteltäväksi. Tietokantojen hakuehdoiksi valittiin hakusanojen haku koko teksteistä vuosilta 2012–2022. Hakutulokset rajattiin koskevan vain artikkeleita, joissa kokoteksti oli saatavilla. Hakutuloksia saatiin yhteensä 1325 kappaletta, ja ne ovat eroteltu lähteiden mukaan taulukossa 3. Tietokannoista selvästi suurin tietolähde oli Science Direct (D), jonka hakutulokset vastaavat noin kahta kolmasosaa tuloksista. Viitteidenhallintaohjelmalla poistettiin tutkimusten kaksoiskappaleet, joita oli yhteensä 213 kappaletta. Tämän jälkeen alkuperäisartikkelien lukumäärä oli 1112 kappaletta.

Taulukko 3. Tiedonhakutaulukko

Tietokanta	Hakulauseke	Tulokset
A	1	79
A	2	2
A	3	9
A	4	21
B	1	19
B	2	3
B	3	6
B	4	12
C	1	232
C	2	42
C	3	3
C	4	23
D	1	209
D	2	315

D	3	190
D	4	160

Mahdollisen tutkimusaineiston löytämisen jälkeen, tulee arvioida aineiston käyttökelpoisuutta. Aineistoa jätetään usein katsauksen ulkopuolelle sisäänotto- ja poissulkukriteerien mukaisesti, jotta vain oleellinen tieto päätyy mukaan tutkimukseen. Poissulku tapahtuu usein vaiheittain. (Flinkman & Salanterä 2007, 92.) Tässä työssä alkuperäisartikkeleita verrattiin sisäänotto- ja poissulkukriteereihin ensin otsikkotasolla, joista jatkotarkasteluun valittiin 81 tutkimusta. Abstraktien luvun jälkeen valittiin tietokannoista haettavaksi kokotekstin tarkasteluun yhteensä 34 artikkelia. Lisäksi kokotekstin lukuun valittiin artikkelien lähdeluetteloista yksi julkaisu. Tiedonhakuprosessi on esitetty flow-kaaviona kuvassa 1.



Kuva 1. Tiedonhaku mukaillen PRISMA 2020 flow-kaaviota (Page ym. 2021).

Taulukointi on yksi tapa tallentaa ja esittää tietoa. Kirjallisuuskatsauksen aineiston kerääminen taulukkomuotoon voi auttaa aineiston hallinnassa ja tarkastelussa. Sen lisääminen raporttiin antaa myös lukijalle nopean yleiskatsauksen systemoituun katsaukseen sisältyvien tutkimusten keskeisistä piirteistä. Taulukossa olisikin hyvä raportoida tekijöiden lisäksi myös tutkimusten keskeiset tiedot, kuten sen tarkoitus ja tulokset. (Flinkman & Salanterä 2007, 92.) Katsaukseen valitut tutkimukset ja niiden tarkoitus sekä keskeiset tulokset on esitelty liitteessä 1.

Katsaukseen sisällytettiin lopulta sisäänottokriteerien perusteella 14 tutkimusta. Suurin syy tutkimusten poissulkuun oli se, että tutkimuksen sisältö ei antanut vastausta tutkimuskysymyksiin. Tutkimuskysymykset oli suunnattu päätelaitteiden haltuunottoon ja moni tutkimuksista liittyi digitaalisen forensiikan analyysivaiheeseen, joka on haltuunotosta erillinen prosessi. Toiseksi suurin syy tutkimusten poissulkuun on teknologian nopea kehittyminen. Tutkimuksissa kävi ilmi, että ne olivat kohdistettu esimerkiksi vanhentuneisiin käyttöjärjestelmiin. Tällainen tutkimustieto ei ole ajankohtaista eikä sitä ollut mahdollista hyödyntää työn tuloksissa.

4.5 Aineiston analysointi

Tutkimukseen valittu aineisto koostui pääasiassa systemoidun kirjallisuuskatsauksen avulla hankitusta vertaisarvioidusta tutkimustiedosta. Lisäksi aineistoa täydennettiin manuaalisella haulla, jossa otettiin huomioon tutkimusartikkelien lähteet. Aineiston toisella lukukerralla ne teemoiteltiin eri luokkiin, joka on esitetty liitteessä 2. Teemoittelun tavoitteena oli jäsennellä tutkimuksia, jonka tarkoitus oli auttaa työn tulosten käsittelyssä. Taulukossa on eritelty systemoidun katsauksen tutkimukset sekä suora sitaatti tekstistä, jonka tarkoitus on avata teemoittelun lähtökohtia.

4.6 Yhteenveto tiedonhaun tuloksista

Kirjallisuuskatsauksen tavoitteena oli löytää sekundääriaineistosta tutkimuksia, jotka vastaavat mahdollisimman hyvin työn tutkimuskysymyksiin. Aineistoa haettiin laajasti eri hakulausekkeilla ja eri tietokannoista, joista käytiin läpi yli tuhat

hakutulosta. Lopuksi vain noin prosentin verran tutkimuksista otettiin mukaan katsaukseen, joka johtui tiukoista sisäänottokriteereistä. Ottaen huomioon tulosten suuren määrän, tämä oli kuitenkin jopa tavoiteltu tulos. Valitun tutkimusaineiston kokotekstien lukemisen perusteella niiden voitiin katsoa vastaavan hyvin työn tutkimusongelmaan.

Mikäli sisäänotto- ja poissulkukriteerit olisivat olleet sallivammat, olisi mukaan katsaukseen otettu myös muita julkaisuja, kuten virallistietoa ja standardeja. Virallistietoa ja standardeja oli usein käytetty valittujen tutkimusartikkelien taustatietona. Tämä ei kuitenkaan ollut nyt mahdollista, eikä olisi ollut hyvän tieteellisen käytännön mukaista muuttaa kriteereitä jälkikäteen. Näitä julkaisuja voidaan kuitenkin hyödyntää työn tulosten luotettavuuden tarkastelussa vertaamalla työn tuloksia muuhun luotettavaksi katsottuun tietoon. Toinen seikka, joka voi vaikuttaa tuloksiin on kielivalinta. Haetut tutkimukset olivat vain englanninkielisiä, joka saattoi rajoittaa hakutuloksia.

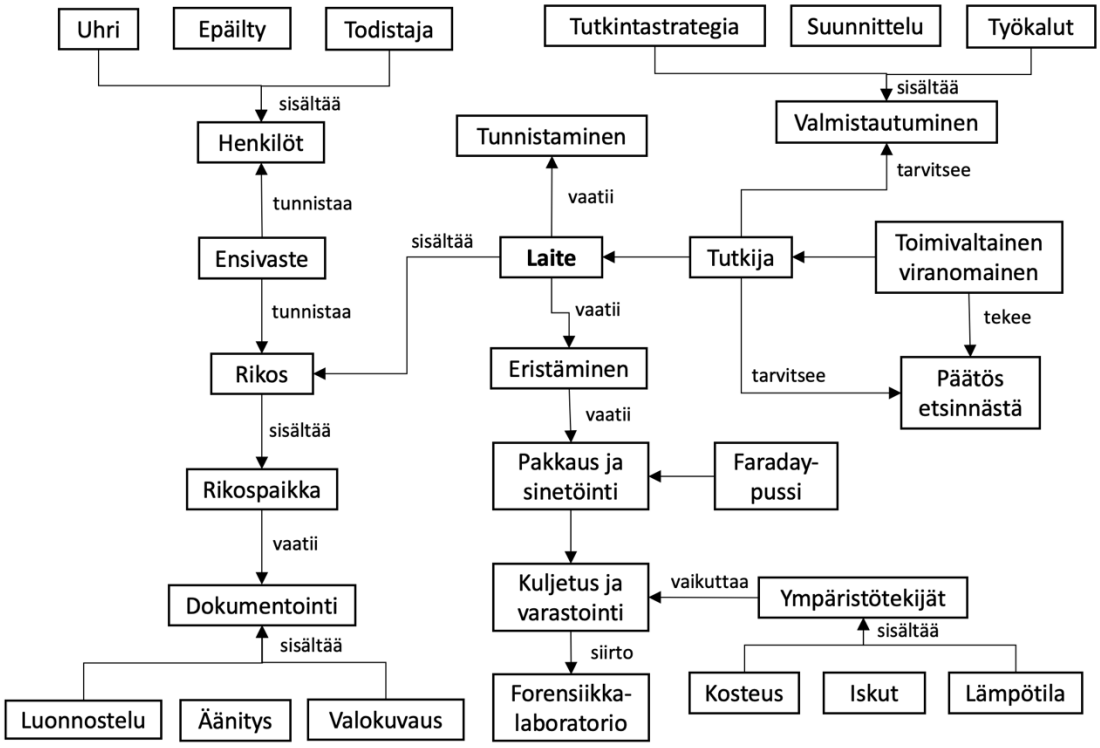
5 TUTKIMUSTULOKSET

Tutkimustulosten aineisto koostui 14:sta eri vertaisarvioidusta tutkimusartikkelista. Tutkimuksia oli tehty maailmanlaajuisesti eri maanosissa, kuten Aasiassa, Euroopassa, Lähi-Idässä ja Pohjois-Amerikassa. Parhaiten edustettuina olivat eurooppalaiset tutkimukset, joita oli puolet tutkimuksista. Metodeja oli käytetty laajasti ja eri tutkimusmenetelmiä olivat muun muassa kehittämistutkimus, kyselytutkimus ja kirjallisuuskatsaus. Aineiston analysoinnissa positiivinen huomio oli, kuinka eri tutkimusten tulokset tukivat toisiaan, joka osaltaan antaa niille luotettavuutta. Mittaustulosten toistettavuus eli reliaabelius on myös digitaalisen forensiikan tieteenlajin yksi perusta. Aineistolle tehdyn analyysin perusteella tutkimusten tuloksilla oli mahdollista saavuttaa opinnäytteelle asetetut tavoitteet.

Tutkimustulosten tarkoituksena on vastata työlle asetettuihin tutkimuskysymyksiin. Tulokset on raportoitu työn tutkimuskysymysten ja aineiston teemoittelun mukaisesti omille alaotsikoille. On hyvä huomioida, että tuloksiin on kirjattu vain aineistosta nousseet asiat ilman opinnäytteen tekijän omia mielipiteitä. Tulokset ovat jaoteltu digitaalisen todistusaineiston turvalliseen haltuunottoon, prosessiin vaikuttaviin tekijöihin, katoavan datan taltiointiin sekä digitaalisen todistusaineiston alkuperäisyyden ja eheyden varmistamiseen.

5.1 Turvallinen haltuunotto

Tietoteknisen laitteen turvallinen haltuunotto rikospaikalla koostuu erilaisista vaiheista, kuten valmistelu, tapahtumapaikan turvaaminen ja kartoittaminen, todisteiden tunnistaminen, dokumentointi sekä taltiointi ja säilyttäminen (Mothi ym. 2020, 2). Lainvalvonnan sekä digitaaliforensisten yksiköiden on ylläpidettävä laadunvarmistusjärjestelmää, joka varmistaa todistusaineiston turvallisen käsittelyn ja luotettavuuden. Tämän järjestelmän ensimmäinen osa on vakioidut toimintaohjeet (engl. Standard Operating Procedures tai SOP) tai mallit, joissa on ohjeistettu prosessin vaatimat tehtävät. (Bulbul ym. 2013, 244.)



Kuva 2. Haltuunoton prosessikaavio mukaillen Ali ym. (2017, 20).

Ali ym. (2017) loivat tutkimuksessaan metamallinnuksen nykyaikaisten mobiililaitteiden haltuunottoprosessista (kuva 2). Tutkimusta varten kerättiin yhteensä 41 eri mobiiliforensiikan mallia ja viitekehystä. Se rakennettiin ensin 21 mallin pohjalta, jonka jälkeen se validoitiin kaksi kertaa käyttämällä kymmentä muuta mallia. Kehitetyn mallin tarkoituksena oli auttaa tunnistamaan mobiiliforensiikan yleisiä työvaiheita ja yksinkertaistaa digitaaliforensista prosessia. (Ali ym. 2017, 1, 12.)

Bulbulin ym. (2013) luoma rikospaikan digitaaliforensinen menettelymalli on sisällöltään hyvin samankaltainen. Sen pohjana on käytetty 25:tä eri yleistä digitaaliforensista mallia. Siinä otetaan huomioon kaikenlainen digitaalinen todistusaineisto eikä pelkästään mobiililaitteita. Bulbulin ym. mallissa otetaan huomioon samat työvaiheet, kuin Alin ym. (2017) mallissa rikospaikan turvaamisesta aina todisteiden kuljetukseen ja varastointiin. (Bulbul ym. 2013, 250–251.)

5.1.1 Turvaaminen

Haltuunotossa on huomioitava rikospaikan fyysisen turvallisuuden varmistaminen. Työturvallisuuden lisäksi tämän tarkoitus on suojella digitaalista todistusaineistoa. Kaikki henkilöt, jotka eivät ole mukana digitaalisen todistusaineiston haltuunottoprosessissa, tulisi poistaa tietoteknisten laitteiden ja digitaalisten todisteiden läheisyydestä. Digitaalisen todistusaineiston herkästi muuttuvan ja häviävän luonteen vuoksi on tärkeää varmistaa, ettei kukaan pääse käsiksi tietokoneisiin, mobiililaitteisiin tai muihin tietoteknisiin laitteisiin, jotta ne saadaan turvallisesti otettua haltuun. (Bulbul ym. 2013, 252.)

Myös paikalla olevien henkilöiden kuuleminen ja tietojen kerääminen tulisi suorittaa mahdollisimman aikaisessa vaiheessa todisteiden haltuunottoprosessia. Henkilöitä, joilla saattaa olla olennaisia tietoja tulee haastatella mielellään jo rikospaikalla. Tiedot voivat olla esimerkiksi käyttäjänimiä, salasanoja ja verkkotunnuksia. Saadut tiedot voivat myös auttaa tunnistamaan digitaalista todistusaineistoa sisältäviä laitteita. (Bulbul ym. 2013, 252.)

5.1.2 Tunnistaminen

Ensivasteena toimivien esitutkintaviranomaisten tulisi teoriassa osata tunnistaa ja ottaa haltuun kaikki digitaalinen todistusaineisto rikospaikalla. Holtin ym. (2020) tutkimuksen mukaan useimmat viranomaisorganisaatiot odottavat henkilöstön pystyvän tunnistamaan ja käsittelemään digitaalisia todisteita tehokkaasti. Osaavista henkilöistä on kuitenkin pulaa ja työ annetaan mieluummin tehtäväksi siihen erikoistuneelle henkilölle tai ryhmälle. Tämä ei kuitenkaan ole aina mahdollista varsinkaan pienemmillä osastoilla tai paikkakunnilla, jossa ei ole niin paljon resursseja kuin suurempien kaupunkien yksiköillä. (Holt ym. 2020, 99–100.) Tutkimuksessa tehty kysely osoitti kokemuksellisen oppimisen

ja henkilöstön koulutuksen tärkeyden. Nämä valmistelevat henkilöstöä digitaalisen todistusaineiston tunnistamiseen ja oikeaoppiseen käsittelyyn kentällä. Tutkimus huomauttaa, että kyselytutkimus perustui yhden osavaltion poliisivirastoon eikä ole siten täysin yleistettävissä. (Holt ym. 2020, 91.)

Yleisten ja tavanomaisten tietoteknisten laitteiden lisäksi tutkijan tulee ottaa huomioon myös mahdolliset vakoilulaitteet. Vakoilulaitteet ovat yleistyneet, sillä ne ovat halpoja ja helposti saatavilla Internetin kautta maista, joissa ei ole niitä koskevaa lainsäädäntöä. Ne voivat olla sisäänrakennettuina erilaisiin arkielämän tavaroihin, jonka vuoksi vakoilulaitteita saattaa olla hankala havaita. Näitä ovat esimerkiksi piilokamerat kynissä ja leluissa tai ääntä tallentava toimistotarvike. Bulbulin ym. (2013) tutkimuksen tekohetkellä vakoilulaitteiden tunnistamista ei ollut huomioituna missään alan kirjallisuudessa eikä standardeissa. Tähän sisältyy esimerkiksi ISO/IEC 27037:2012, jonka tarkoitus on ollut ohjata digitaalisen todistusaineiston tunnistamista ja käsittelyä. (Bulbul ym. 2013, 252.)

Tietoteknisiä laitteita ulkoisesti tarkastelemalla voi olla mahdotonta varmistaa sisältääkö laite relevanttia digitaalista todistusaineistoa. Tilanteissa, joissa kohdelaite ei ole lukittu tai tutkija voi hankkia laitteen lukituksen avaamiseen vaadittavat käyttäjän tunnistustiedot, on mahdollista selata laitteen sisältämää tietosisältöä. Laitteen lukituksen avaamiseen vaadittava käyttäjätunnistus voi olla esimerkiksi salasana, pääsykoodi, suojakuvio tai biometrinen tunnistaminen, kuten sormenjälki- tai kasvojentunnistus. Tietosisällön selaamiseen voidaan käyttää laitteen manuaalista tarkastamista (engl. device manual examination tai DME). Horsman (2022) esitteli tutkimuksessaan laitteen manuaalisen tarkastelumenetelmän, jossa laitteen käyttöliittymällä manuaalisesti etsitään, tunnistetaan ja kerätään dataa. Data voi olla laitteen tallennusalustalla tai muuten saatavilla laitteen kautta, kuten pilvipalvelussa. Sen käyttö tulisi olla osa jokaista digitaalisen forensiikan tutkimusta vähintään tulosten tarkastamiseksi. Joissain tapauksissa se voi olla myös ainoa keino jäljentää dataa, mikäli käytettävissä olevat digitaalisen forensiikan työkalut eivät muuten tue laitetta. (Fukami ym. 2021, 3; Horsman 2022, 2.)

5.1.3 Haltuunotto

Digitaalisen todistusaineiston haltuunotto on vaiheittainen prosessi, jota ohjaa siihen luotu toimintaohje. Menettelytapoja ohjaa erityisesti laitteen tila. Jos laite on käynnissä, noudatetaan erilaisia menettelytapoja, kuin laite olisi sammuneena. (Mothi ym. 2020, 4.) Erityisesti käynnissä olevan laitteen keskusmuistiin tallentuneet tiedot voivat kadota, ellei niitä jäljennetä ennen virran katkaisua (Bulbul ym. 2013, 253). Keskusmuistiin tallentuneen katoavan datan taltiointitekniikoita on kuvattu kappaleessa 5.3. Haltuunoton rinnalla kulkee kappaleessa 5.4.1 mainittu dokumentointiprosessi. Dokumentointia jatketaan koko tutkintaprosessin ajan ylläpitämällä hallintaketjua, jolla voidaan varmistaa haltuunotetun aineiston oikeuskelpoisuus (Lone & Naaz 2019, 45).

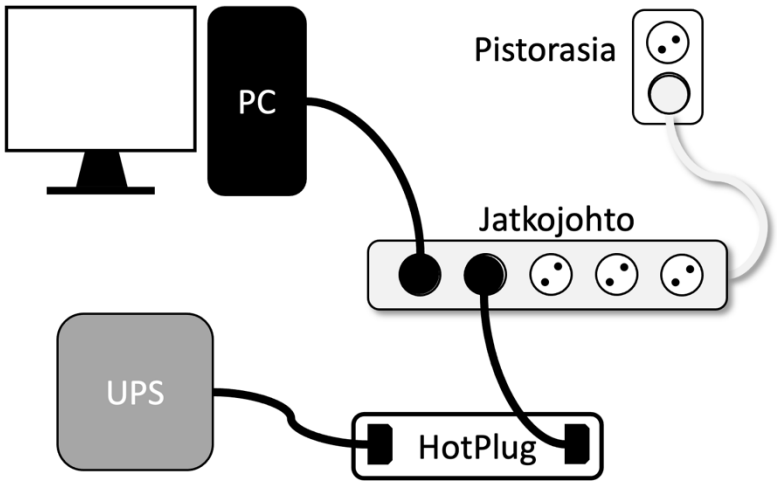
Lähtökohtaisesti digitaalisen todistusaineiston haltuunoton voi tehdä vain siihen erityisesti koulutettu asiantuntija, jotta voidaan taata, että toimenpiteet eivät heikennä todistusaineiston eheyttä (Bulbul ym. 2013, 245). Tämä ei kuitenkaan ole aina mahdollista varsinkaan pienemmissä virastoissa (Holt ym. 2020, 100). Tämän vuoksi haltuunotto voidaan yksinkertaistaa vain sellaisiksi välttämättömiksi toimiksi, jotka takaavat digitaalisen todistusaineiston eheyden. Laitteet tulee ottaa haltuun lähtökohtaisesti siinä tilassa, kun ne ovat. Mikäli laite on pois päältä eli sammuneena, sitä ei pidä käynnistää. Mikäli laite on päällä, se tulee pitää käynnissä ja varmistaa, että siihen ei tehdä muutoksia. Tämä tarkoittaa sitä, että mitään laitteen näppäimiä tai hiiren painikkeita ei klikata. Käynnissä olevaa laitetta ei tule myöskään siirtää, ennen kuin on varmistettu, että siirtämisen johdosta ei hävitetä digitaalista todistusaineistoa. (Bulbul ym. 2013, 250.)

5.1.4 Kuljetus ja varastointi

Tiedon säilyttäminen alkuperäisenä vaatii muutakin kuin turvallisen säilytyspaikan. Säilytys kattaa kaikki työkalut ja tekniikat sekä käytännöt ja menettelyt, joilla todistusaineistoa käsitellään, kuljetetaan ja varastoidaan. Näiden avulla pyritään varmistamaan, että materiaali pysyy luotettavana, saatavilla ja käyttökelpoisena ajan mittaan, myös teknologioiden muuttumisen jälkeen. Tiedon alkuperäisyys on kestävä huolenaihe digitaalisessa maailmassa, joka tulee ottaa huomioon myös laitteiden kuljetuksessa ja varastoinnissa. Alkuperäisyyden varmistaminen edellyttää myös yhteistyötä ryhmän eri henkilöiden välillä. (Rogers 2015, 98.)

Tietoteknisiin laitteisiin tallennetut digitaaliset todisteet ovat herkkiä muun muassa äärimmäisille lämpötiloille, kosteudelle, iskuille, magneettikentille sekä staattiselle sähkölle. Staattisella sähköllä tarkoitetaan sähkövarauksen kertymistä jonkin materiaalin tai esineen pinnalle. Sitä syntyy yleensä, kun materiaaleja vedetään erilleen tai hierotaan yhteen, jolloin syntyy sähkön epätasapainotila. Sähköstaattinen purkaus saattaa vaurioittaa tietoteknisiä laitteita ja niissä käytettäviä puolijohteita. Tämän vuoksi tutkijoiden tulisi välttää työkaluja sekä pakkausmateriaaleja, jotka voivat kerätä staattista sähköä, sillä ne voivat vahingoittaa tai tuhota todisteita. Nämä tulee kaikki ottaa huomioon, kun laitteita pakataan ja kuljetetaan forensiikkalaboratorioon. Jotkin laitteet vaativat lisäksi erityisiä pakkaus- ja kuljetustekniikoita, kuten erilaiset mobiililaitteet. Verkkoyhteydellä varustettuja mobiililaitteita tulisi estää vastaanottamasta ja lähettämästä tietoja, kun ne ovat tunnistettu ja kerätty todistusaineistoksi. Tutkijoilla tulisi olla signaaleilta suojaavia materiaaleja, kuten faraday-eristyspusseja tai alumiinifoliota mobiililaitteiden suojaamiseen varsinkin, jos laitetta ei ole saatu asetettua lentotilaan. Mobiililaitteiden kääriminen alumiinifolioon tai asettaminen faraday-pussiin estää niitä vastaanottamasta puheluja, viestejä tai dataa, joka voi muuttaa laitteen tietosisältöä. Sen tavoitteena on myös estää anti-forensisten tekniikoiden käyttäminen, joita on käyty läpi kappaleessa 5.2.1. (Bulbul ym. 2013, 252–254; Ali 2017, 21.)

Tietoteknisten laitteiden haltuunotto ja käynnissä pitäminen on yksinkertaista, jos laitteessa on virtalähteenä akku. Pöytätietokoneissa ei usein tällaista kuitenkaan ole, toisin kuin kannettavissa tietokoneissa ja mobiililaitteissa. Käynnissä olevan pöytätietokoneen siirtämiseen vaaditaan keskeytymätön virransyöttö, joka tehdään yleisesti UPS-laitteella. Termi UPS tulee englannin kielen sanoista uninterruptible power supply ja se toimii akun tavoin syöttäen virtaa siihen kytkettyyn laitteeseen. Schrampin (2017) tutkimuksessa esiteltiin Wiebetech HotPlug Field Kit -laite, joka alkaa syöttämään virtaa pöytäkoneeseen kytkettyyn jatkojohtoon, kun se irrotetaan pistorasiasta (kuva 3). (Schramp 2017, 46–47.)



Kuva 3. Virransyöttö HotPlug-laitteen kautta jatkojohtoon mukaillen Schramp (2017, 47).

Mobiililaitteen päällä pitäminen mahdollistaa muun muassa biometrisen tunnisteen käytön, jos kohdelaite on After First Unlock (AFU) -tilassa. AFU tarkoittaa, että kohdelaite on tilassa, jossa se on avattu esimerkiksi käyttäjän suojakoodilla vähintään kerran käynnistyksen jälkeen. Toinen käynnissä olevan mobiililaitteen mahdollinen tila on Before First Unlock (BFU), jossa laitetta ei ole käynnistyksen jälkeen avattu käyttäjän salausavaimella. BFU-tilassa biometrisen todentamisen käyttöönotto vaatii laitteen lukituksen avaamisen vähintään kerran. Lisäksi useimmissa biometristä todennusmenetelmää käyttävissä laitteissa on aikarajoitus. Tällöin laite vaatii salausavainta biometrisen todentamisen uudelleen käyttöönottoon, joka on esimerkiksi nykyaikaisissa iOS-laitteissa 48 tuntia. (Fukami ym. 2021, 4.)

5.2 Prosessiin vaikuttavat tekijät

Yksi digitaalisen forensiikan haasteista on anti-forensiikka, jollaiseksi luonnehditaan kaikki yritykset vaarantaa todisteiden saatavuus tai käyttökelpoisuus digitaaliforensisessa prosessissa. Sen avulla on mahdollista viivästyttää tai kokonaan estää tietoteknisen tutkinnan suorittaminen poistamalla tietoja tai estämällä työkalujen käyttö. (Stüttgen & Cohen 2013, 105.) Erilaiset anti-forensiset tekniikat voidaan jakaa tietojen piilottamiseen (muun muassa salaus ja steganografia), tietojen tuhoamiseen (levyn puhdistustyökalut, tiedostojen pyyhkiminen ja tuhoaminen) sekä hyökkäyksiin digitaalisen forensiikan työkaluja ja prosesseja vastaan (Meffert ym. 2016, 89). Digitaalisen forensiikan käytännöt muodostuvat erilaisista malleista ja vakioiduista toimintaohjeista, sillä ne ohjaavat

tutkijoita tarvittaviin toimenpiteisiin ja menettelyihin. Viimeisimmätkin mallit kuitenkin olettavat, että on turvallista siirtyä vaiheesta toiseen ottamatta huomioon anti-forensisia tekniikoita. Kirjallisuutta tarkasteltaessa on kuitenkin havaittu, että anti-forensiset prosessit voivat vaikuttaa digitaalisen forensiikan analyysivaiheen lisäksi myös niiden turvalliseen haltuunottoon. Jos anti-forensisia prosesseja ja tekniikoita ei oteta huomioon riskienhallinnassa, se voi vaarantaa sekä todisteiden että tutkinnan luotettavuuden. (Mothi ym. 2020, 1–4; Shafiee Hasanabadi ym. 2020, 1–2.)

5.2.1 Tietojen tuhoaminen ja piilottaminen

Suuri osa anti-forensisista prosesseista keskittyy digitaalisen todistusaineiston poistamiseen. Esimerkiksi nykyaikaisilla tietojen pyyhkimistekniikoilla voidaan poistaa todisteet turvallisesti ja estää datan mahdollinen palauttaminen digitaaliforensisissa tutkimuksissa. (Shafiee Hasanabadi ym. 2020, 3.) Mobiililaitteiden uudet turvamekanismit, joilla on mahdollista suojata tai tyhjentää esimerkiksi varastettu, kadonnut tai takavarikoitu älypuhelin, on hyvin tiedossa myös rikollisilla. Nämä turvaominaisuudet mahdollistavat laitteen tietosisällön tyhjentämisen etänä verkkoyhteyden avulla, jonka vuoksi onkin tärkeää eristää laite haltuunoton jälkeen täysin verkkoyhteyksistä. (Bulbul ym. 2013, 252.) Lukitun laitteen avaamisessa tulee huomioida, että laitteessa voi olla käytössä pakkotilanteisiin tarkoitettu vaihtoehtoinen salasana. Sen syöttäminen voi suorittaa joukon piilotettuja sääntöjä, kuten esimerkiksi tietojen pyyhkimisen, tai joidenkin toimintojen käytöstä poistamisen. Mikäli vaihtoehtoista salasanaa käytetään oikean salasanan sijasta, on suuri mahdollisuus, että laitteen tietoja ei voida enää palauttaa. (Fukami ym. 2021, 4.)

Datan piilottaminen voi onnistua myös käyttämällä steganografiatekniikkaa (Shafiee Hasanabadi ym. 2020, 3). Pääte- ja oheislaitteissa voi olla käytössä steganografiatekniikoita, kuten tiedostojärjestelmän piilottaminen tiedostojärjestelmään. Tämä voidaan luoda muun muassa TrueCrypt-salaustyökalulla. Mikäli tutkija saa haltuun salausavaimen ensimmäiseen salattuun tiedostojärjestelmään, mutta ei toiseen piilotettuun tiedostojärjestelmään, voi olla, että piilotettu tiedostojärjestelmä jää kokonaan huomioimatta. (Mothi ym. 2020, 3.) Datan piilottaminen voidaan tehdä myös käyttöjärjestelmän oletussovelluksilla. Yksi tapa on käyttää verkkoselainta yksityisessä selailutilassa. Se ei tallenna

selailutietoja, kuten sivuhistoriaa laitteen massamuistiin, vaan data on käytön jälkeen saatavissa vain laitteen keskusmuistista. (Shafiee Hasanabadi ym. 2020, 4.)

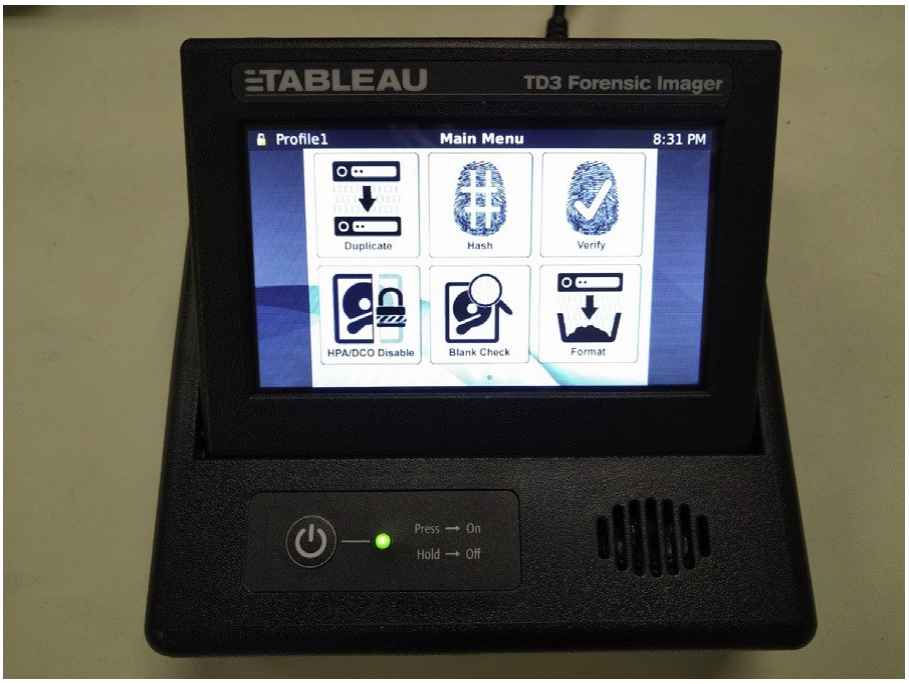
Nykyaikaiset laitteet varustetaan anti-brute-force-suojauksella, joka pyrkii estämään väsytyshyökkäyksen laitteen avaamiseksi. Brute-force eli väsytyshyökkäys voi kokeilla esimerkiksi jokaista mahdollista numeroyhdistelmää laitteen suojakoodin arvaamiseksi. Anti-brute-force-suojauksen avulla voidaan hidastaa toistuvien yritysten syöttämistä laitteelle aikarajoituksella tai tyhjentää laite kokonaan, kun laitteelle on syötetty väärä numeroyhdistelmä tarpeeksi monta kertaa. (Fukami ym. 2021, 4.) Anti-forensiikan ja laitteiden suojamekanismien vuoksi tutkijoiden onkin täytynyt alkaa kehittämään näiden vastaisia (anti-anti-forensiikka) menetelmiä, joilla voidaan kiertää ja puolustaa anti-forensisia tekniikoita vastaan (Shafiee Hasanabadi ym. 2020, 1).

5.2.2 Hyökkäykset työkaluja vastaan

Digitaalisten todisteiden eheyden varmistamiseksi käytetään erilaisia työkaluja, joihin voi helposti ajautua riippuvaiseksi. Työkaluriippuvuuden ongelmana on, että ne eivät ole täysin immuuneja hyökkäyksiä vastaan. Digitaalisen forensiikan tutkimuksissa käytettäviä työkaluja vastaan voidaan hyökätä erilaisilla anti-forensisilla tekniikoilla, jonka vuoksi työkalujen testaus on ensiarvoisen tärkeää. Yhdysvalloissa alan työkalujen testausta valvoo NIST, joka on perustanut tätä tarkoitusta varten Computer Forensic Tool Testing (CFTT) -ohjelman. CFTT arvioi digitaalisen forensiikan työkalujen luotettavuutta ja raportoi testituloksista verkkosivuillaan. (Mothi ym. 2020, 3–4.)

Kaksi merkittävää alalla käytössä olevaa työkalua ovat erilaiset ohjelmistoon sekä laitteistoon perustuvat kirjoitussuojat. Ohjelmistoon perustuva kirjoitussuoja estää käyttöjärjestelmää kirjoittamasta valittuun tallennusalustaan tai tiedostoon. Laitteistoon perustuva kirjoitussuoja on erillinen työkalu, joka kytketään fyysisesti kohdelaitteeseen (kuten kiintolevyyn) ja estää muutosten tekemisen todisteiden hankinnassa. Näistä laitteistoon perustuva kirjoitussuoja on yleisesti suositeltu vaihtoehto. (Meffert ym. 2016, 87–89.)

Yhdysvaltain kotimaan turvallisuusvirasto (engl. Department of Homeland Security tai DHS) on julkaissut raportin laajalti käytetystä ja laitteistoon perustuvasta Tableau TD3 -kirjoitussuojasta (kuva 4). DHS:n mukaan TD3:n avulla voitiin täysin jäljentää kohdelaitteen kaikki näkyvät ja piilotetut muistisektorit tarkasti. Tämä raportti ei kuitenkaan ottanut huomioon sitä, että TD3 on verkkolaite, jota vastaan voidaan hyökätä hyödyntämällä sen mahdollisia haavoittuvuuksia. Meffertin ym. (2016) tutkimuksessa laitetta vastaan hyökättiin ja tulokset osoittivat, että anti-forensiikalla voidaan vaarantaa sillä hankitun todistusaineiston eheys. Myös laitteen avulla hankitun todistusaineiston eheyden varmistamiseen käytettävä kryptografinen tiiviste (engl. hash) voitiin manipuloida niin, että tutkija ei huomaa todistusaineiston vaarantumista. Tutkimuksessa esiteltiin hyökkäyksen toimittaminen myös verkon kautta kyberhyökkäyksenä, sillä rikostekniset laboratoriot eivät usein ole täysin eristettyinä verkosta. Tämän vuoksi on äärimmäisen tärkeää ottaa digitaalisen forensiikan työkalujen tietoturvatestaus osaksi niiden testausprosessia. (Meffert ym. 2016, 90–95.)



Kuva 4. Muistin jäljentämiseen käytettävä Tableau TD3 -kirjoitussuoja (Meffert ym. 2016, 90).

Keskusmuistin analyysi on kasvattanut suosiota viime aikoina ja se on osoittautunut tehokkaaksi tekniikaksi muun muassa haittaohjelmien paljastamiseen vaarantuneissa tietojärjestelmissä. Kappaleessa 5.3 esitettyjen työkalujen käyttö aiheuttaa kuitenkin haasteita, sillä hankintatekniikat edellyttävät usein koodin suorittamista mahdollisesti vaarantuneessa järjestelmässä. Yksi esimerkki on rootkit-piilohaittaohjelmat, jotka pystyvät havaitsemaan digitaalisen

forensiikan työkaluja ja estämään niiden toiminnan. (Shafiee Hasanabadi ym. 2020, 4–5; Stüttgen & Cohen 2013, 105–106.) Strategisesti piilohaittaohjelman tehtävä on pysyä piilossa ja aiheuttaa mahdollisimman vähän havaittavia häiriöitä järjestelmän toimintaan. Tämän vuoksi sen havaitseminen on äärimmäisen hankalaa. Muistin taltiointiin käytettävät työkalut käyttävät usein dokumentoimattomia ohjelmointirajapintoja (engl. Application Programming Interface tai API), jonka anti-forensinen prosessi pystyy melko helposti erottamaan normaaleista järjestelmäprosesseista. Tämä antaa rootkitille mahdollisuuden suunnata anti-forensinen prosessi tiettyihin toimintoihin, jotka estävät työkalujen käytön vaikuttamatta järjestelmän normaaliin toimintaan. (Stüttgen & Cohen 2013, 108.)

Stüttgen & Cohen (2013) testasi tutkimuksessaan anti-forensisia tekniikoita kuutta eri ilmaista ja maksullista keskusmuistin taltiointiin käytettävää ohjelmaa vastaan. Tutkimuksen tuloksissa havaittiin, että jokainen työkalu oli haavoittuva anti-forensiikalle ja sen avulla voitiin estää täysin työkalujen käyttö. Ongelmat eivät olleet käyttöjärjestelmään sidonnaisia, vaan samat tulokset saatiin Windows, Linux ja macOS-käyttöjärjestelmillä. Näistä esimerkiksi macOS-käyttöjärjestelmän kerneliin syötetty kahden rivin koodi esti työkaluja hankkimasta tavuakaan keskusmuistia. (Stüttgen & Cohen 2013, 109–110.)

Stüttgen & Cohen (2013) loivat tutkimuksessaan heikkouksien havainnollistamisen lisäksi myös ratkaisun, joka sietää paremmin anti-forensiikkaa. Testissä kohdejärjestelmään oli otettu käyttöön erilaisia anti-forensisia tekniikoita. Yksi oli tarkoituksellisesti rikkinäinen KDBG (Kernel Debugging Data Block), jota yleisesti hyväksikäytetään keskusmuistin taltiointityökaluissa. Lisäksi käytössä oli artikkelin mukaan ainakin keskusmuistin käsittelyyn käytettävien MmMapMemoryDumpMdl() sekä MmGetPhysicalMemoryRanges() -ohjelmistorajapinnan hyökkäykset (engl. API hooking). Testityökalu luotiin avoimen lähdekoodin työkalusta Winpmem, ja muistin taltioinnissa hyödynnettiin kohdejärjestelmän laitteistoa kernelin API:n sijaan. Testityökalun hyödyntämä tekniikka oli helppo toteuttaa, ja sillä saatiin taltioitua onnistuneesti keskusmuisti kokonaisuudessaan vaarantuneesta järjestelmästä. Tekniikan havaittiin myös olevan riippumaton kohteen käyttöjärjestelmästä. Työkalua testattiin onnistuneesti avoimeen lähdekoodiin perustuvilla työkaluilla Winpmem (Windows), Linux pmem (Linux) sekä OSXPmem (macOS). (Stüttgen & Cohen 2013, 111–113.)

5.3 Katoavan datan taltiointi

Tietokoneen keskusmuisti saattaa usein sisältää merkityksellistä tietoa tutkinnalle ja sen rooli on kasvanut digitaalisen forensiikan tutkimuksissa. Keskusmuistiin tallentunutta selkokielistä dataa voidaan käyttää esimerkiksi kohdelaitteen salausavaimien hankkimiseen tai pelkästään RAM-muistissa toimivien haittaohjelmien analysointiin. Perinteisesti digitaalinen forensiikka on keskittynyt kiintolevyjen tutkintaan ja tietokoneiden haltuunotto tapahtui vetämällä virtajohto irti pistorasiasta. Tietokoneiden keskusmuistiin tallentunut data kuitenkin häviää nopeasti sen jälkeen, kun laitteesta katkaistaan virta. Tätä keinoa ei siksi voida enää käyttää ensisijaisena haltuunottokeinona, mikäli halutaan taltioida myös laitteiden katoavaa dataa niiden keskusmuistista. Nykyään on olemassa suuri määrä erilaisia tekniikoita ja työkaluja keskusmuistin taltiointiin, joilla kaikilla on omat etunsa ja haasteensa. (Schramp 2017, 44; Latzo ym. 2019, 56.)

Keskusmuistin taltiointiin käytettävien työkalujen tuloksia voidaan arvioida atomisuudella ja eheydellä. Taltioitu muisti on atominen, kun siinä ei ole merkkejä järjestelmän samanaikaisesta toiminnasta. Eheys taas viittaa hankintatavan tuhoavaan vaikutukseen, kuten muistin ylikirjoittamiseen ennen sen taltiointia. (Latzo ym. 2019, 56.)

Virtuaalikoneiden muistin tai nykytilan taltiointi on usein integroituna virtualisointiratkaisuihin, joka mahdollistaa niiden korkean atomisuuden ja eheyden. Päätelaitteissa sen sijaan taltiointiin käytettävän työkalun asennusaika vaikuttaa lopputuloksen eheyteen. Usein työkalut otetaan käyttöön vasta tapahtuman jälkeen. Tämä hieman muuttaa muistia ja heikentää eheyttä, kun työkalun ajuri asennetaan ja ladataan kohdelaitteelle. Yksi vaihtoehto päätelaitteiden atomiseen ja eheään keskusmuistin taltiointiin on hyödyntää käyttöjärjestelmään sisäänrakennettua lepotilaominaisuutta. Jos laite on asetettu lepotilaan, voidaan katoavan datan taltiointiin käyttää myös tiedostojärjestelmään tallentunutta lepotilatiedostoa. Käyttöjärjestelmä voi tallentaa keskusmuistin sisällön lepotilatiedostoon, jolloin se pysyy saatavilla myös virrankatkaisun jälkeen. Tämä vaatii sen, että lepotila on laitteella käytössä ja siihen tulee olla pääsy. Jos esimerkiksi laitteessa on salattu kiintolevy, johon ei ole salausavainta, ei lepotilatiedostoon

päästä käsiksi. Tämän vuoksi lepotilatiedostot ovat melko epäluotettava digitaaliforensinen hankintamenetelmä. (Latzo ym. 2019, 61–65.)

5.3.1 Kernel-tason työkalut

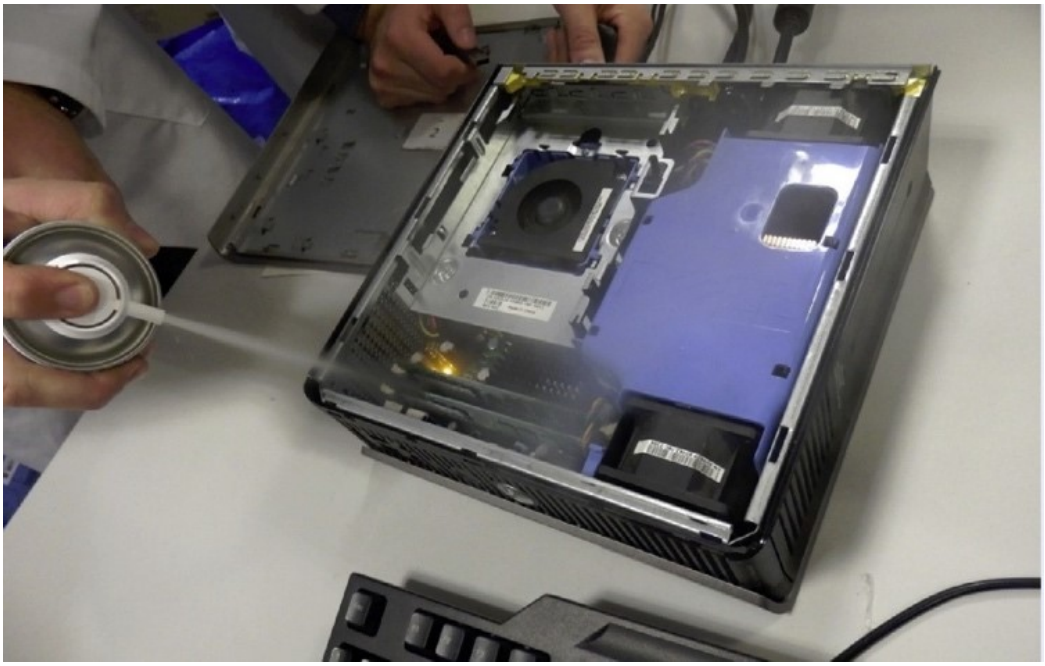
Erilaisia tekniikoita tai ohjelmia keskusmuistin taltiointiin ovat muun muassa käyttöjärjestelmän ytimeen eli kerneliin pohjautuvat ohjelmistot, kylmäkäynnistys (engl. cold boot), oikosiirto (engl. DMA tai direct memory access) sekä manuaalinen tallentaminen ja dokumentointi. Kernel vastaa keskusmuistin ylläpidosta, jonka vuoksi sitä käytetään laajasti muistin taltiointiin, ja suurin osa työkaluista on toteutettu kernelin ajureina. Keskusmuistin taltiointiin on useita ilmaisia ja maksullisia ohjelmia, kuten Pmem, LiME, FTK Imager, DumpIt sekä ProcDump. Näiden etuja ovat muun muassa niiden helppo ja nopea käyttöönotto, ja ne ovat mahdollista asentaa jälkikäteen. Työkalut ovat jaettu kernelkomponenttiin, joka mahdollistaa tarvittavat toiminnot muistin taltiointiin sekä käyttäjätilan komponenttiin, joka tarjoaa tutkijalle työkalun käyttöliittymän. (Latzo ym. 2019, 62–63.)

Kernel-tason työkalut suoritetaan aina kohdejärjestelmässä, joka aiheuttaa muutamia haasteita. Ensinnäkin atomisuus kärsii, sillä järjestelmää ei usein voida pysäyttää toimenpiteen ajaksi. Tämä johtaa todennäköisesti järjestelmän tilan muutoksiin muistin taltioinnin aikana. Toiseksi työkalun asennus muuttaa hieman järjestelmän ytimen muistia, joka heikentää eheyttä. (Latzo ym. 2019, 63.) On lisäksi mahdollista, että kohdelaitteessa on haittaohjelma, joka on onnistunut saamaan ydintason oikeudet. Haittaohjelman avulla voidaan kumota työkalun koko toiminta anti-forensisilla tekniikoilla. Tämä johtaa siihen, että ohjelmistoihin, jotka nojaavat kernelin objekteihin tai rakenteisiin ei voida enää täysin luottaa. (Latzo ym. 2019, 65.)

5.3.2 Kylmäkäynnistys

Kylmäkäynnistyksellä on mahdollista saada atominen kopio keskusmuistista, sillä se ei vaadi kohdejärjestelmän käynnissä pitämistä toimenpiteen aikana. Kylmäkäynnistystekniikka hyödyntää muistikampojen remanenssia datan taltiointiin. Kun muistikampoihin johdettava virta katkaistaan, niiden sisältö ei katoa välittömästi, vaan vähitellen. Tämän seurauksena niiden sisältämä tietosisältö pysyy saatavilla hetken aikaa virran katkaisun jälkeen, ja tätä aikaa voidaan

myös pidentää jäähdyttämällä muistikampoja (kuva 5). Yksinkertaisin tapa hyödyntää kylmäkäynnistystä on käynnistää kohdelaite uudelleen erillisellä ohjelmalla tai käyttöjärjestelmällä. Tämän tekniikan käytön voi estää, mikäli laitteen BIOS (Basic Input-Output System) -tietokoneohjelma tyhjentää keskusmuistin osana käynnistysprosessia. Laitteen suojausasetukset voivat olla myös määritelty estämään esimerkiksi USB-muistilta käynnistettävät käyttöjärjestelmät. (Schramp 2017, 48; Latzo ym. 2019, 68.)



Kuva 5. Kylmäsprayn käyttö pöytätietokoneen muistikampoihin. (Schramp 2017, 50).

Toinen tapa hyödyntää kylmäkäynnistystä on siirtää muistikammat fyysisesti toiseen samantyyppiseen tietokoneeseen tai RAM-levyasemaan, kuten Schrampin (2017) tutkimuksessa. Ennen siirtämistä muistikampoja tulee jäähdyttää esimerkiksi kylmäsprayn avulla, joka on tähän tarkoitukseen edullinen ja helposti saatava vaihtoehto. (Schramp 2017, 49.) Kylmäkäynnistystekniikan käyttö estää tehokkaasti järjestelmään mahdollisesti asennetut anti-forensiset prosessit, sillä siinä ei tarvitse hyödyntää kohdelaitteen käyttöjärjestelmää muistin taltiointiin (Latzo ym. 2019, 68).

5.3.3 Oikosiirto

Oikosiirtoon perustuvia ja tietokoneiden PCI-väylää hyödyntäviä DMA-hyökkäystyökaluja ovat muun muassa PCILeech sekä Inception. Näillä työkaluilla on lisäksi mahdollista ohittaa käyttöjärjestelmään kirjautuminen. DMA-työkalut

eivät usein vaadi toimimista kohdejärjestelmässä, sillä DMA-pyyntöjä voidaan lähettää ulkoisesta laitteesta. Perinteisiin kernel-tason työkaluihin verrattuna, oikosiirto ei häiritse prosessorin toimintaa, jonka vuoksi kohdelaitteeseen tehdään vähemmän muutoksia. Näiden etujen lisäksi oikosiirrossa on myös sen käyttöä rajoittavia tekijöitä. Oikosiirtoa ei voida käyttää, mikäli käytettävissä ei ole esimerkiksi työkalun vaatimaa FireWire- tai PCI Express-liitäntää. Nykyaikaiset laitteet myös suojaavat PCI-väylää DMA-hyökkäyksiltä. Hyökkäyksiä suojaa järjestelmän IOMMU (input-output memory management unit) -ominaisuus, jos se on käytössä ja oikein konfiguroitu. (Schramp 2017, 45; Latzo ym. 2019, 67–68.)

Laitteistopohjaista oikosiirtoa on pidetty ratkaisuna, joka sietää anti-forensisia prosesseja, kuten piilohaittaohjelmia. Erillisellä laitteella voidaan ohittaa laitteen prosessori ja päästä suoraan käsiksi muistiväylään sen taltiointia varten. Valitettavasti asia ei kuitenkaan näin ole, sillä oikosiirtoon voidaan vaikuttaa esimerkiksi manipuloimalla laitteen muistiohjaimen laitteistorekisteriä. Näin voidaan muuttaa DMA-hyökkäystyökalun näkymää saatavilla olevasta keskusmuistista, vaikka prosessorin näkymä pysyisi ennallaan ja laite toimisi normaalisti. (Stüttgen & Cohen 2013, 106.)

5.3.4 Manuaalinen taltiointi

Horsmanin (2022) tutkimuksessa esiteltyä laitteen manuaalista tarkastusmenettelyä voidaan hyödyntää katoavan datan taltiointiin kaikissa näytöllisissä päätelaitteissa. Nykyaikaisissa salausta hyödyntävissä mobiililaitteissa laite tulee olla avattuna tai tutkijalla tulee olla hallussaan käyttäjän todennustiedot eli suojakoodi, salasana tai biometriset tiedot, jotta laitetta voidaan tarkastella (Fukami ym. 2021, 3). Yksinkertaisuudessaan manuaalinen tarkastelu tarkoittaa itse kohdelaitteen käyttöä ja tiedon taltiointia siten, kun se esitetään laitteen näytöllä. Datan taltiointi tapahtuu usein valo- tai videokuvaamalla näyttöä erillisellä kameralla. Toinen tapa on käyttää laitteen ohjelmistoa ruutukaappausten tekemiseen, jonka jälkeen data siirretään tutkijalle joko verkkoyhteydellä tai suoraan ulkoiselle muistille. Laitteen manuaalisen tarkastusmenettelyn etuja ovat sen yksinkertaisuus sekä nopeus, kun taas suurimpana haasteena on eheyden säilyttäminen. Se ei korvaa perinteistä digitaalisen forensiikan analyy-

siä eikä sitä tule käyttää oikotienä datan nopeaan taltiointiin. Laitteen manuaalista läpikäyntiä tulisi käyttää vain silloin, kun se on tarkoituksenmukaista ja harkittua. (Horsman 2022, 2, 7.)

Kaikenlainen laitteiden käsittely altistaa digitaalisen todistusaineiston muutoksille, ja pahimmassa tapauksessa jopa poistaa laitteessa olevia tietoja. Tämän vuoksi ennen aloittamista onkin hyvä arvioida omia kykyjä suorittaa prosessi turvallisesti. Tutkijoiden olisi hyvä tutustua laitteeseen ennen manuaalisen tarkastelun suorittamista, jotta käsittelyvirheiden mahdollisuus pienenee. Tämä voidaan tehdä esimerkiksi tutustumalla laitteen käyttöohjeeseen. Manuaalisen tarkastusmenettelyn digitaalinen jalanjälki tulee myös huomioida ja dokumentoida prosessin aikana. Digitaalisia jälkiä voi tulla tarkoituksella tai vahingossa, kun ollaan vuorovaikutuksessa laitteen valikoiden ja tiedostojen kanssa. Tiedostojen avaaminen voi muuttaa esimerkiksi tiedostojen metatietoihin tallentuneita aika- ja päivämäärätietueita. Manuaalisella tarkastelulla voi olla vaikutusta laitteen tietojen eheyteen ja siinä tulee aina noudattaa erityistä varovaisuutta. (Horsman 2022, 5.)

5.4 Alkuperäisyyden ja eheyden varmistaminen

Tietoteknisten laitteiden hyödyntäminen on lisääntynyt nopeasti nykypäivän jatkuvasti kasvavassa digitaalisessa maailmassa. Digitaalisilla todisteilla on yhä enemmän merkitystä, sillä niitä käytetään tapahtumien todistamiseen ja henkilöiden tuomitsemiseen. Siksi on äärimmäisen tärkeää varmistaa digitaalisen todistusaineiston alkuperäisyys ja eheys sen koko elinkaaren ajan. Digitaalista todistusaineistoa on erittäin hankalaa käsitellä ja säilyttää fyysiseen todistusaineistoon verrattuna. Digitaalisen tiedon ominaisuuksia ovat muun muassa sen herkästi särkyvä ja helposti siirrettävä luonne, alttius manipulaatiolle ja poistamiselle sekä aikaherkkyys. Sen monimuotoinen ja epävakaa luonne aiheuttaa omanlaisia haasteita alkuperäisyyden ja eheyden varmistamiseksi. (Lone & Naaz 2019, 44.)

5.4.1 Dokumentointi

Todistusaineiston luotettavuutta voidaan parantaa tarkalla dokumentoinnilla. Se on jatkuvaa toimintaa, jota käytetään rikospaikan ja todisteiden dokumentoimiseen (Ali ym. 2017, 9). Dokumentointi sisältää muun muassa valokuvien, luonnosten ja videoiden ottamista rikospaikasta sekä fyysisistä todisteista. Dokumentoinnissa tulisi taltioida koko tila sekä todisteiden tarkka sijainti. Sen tavoitteena on kerätä mahdollisimman paljon tietoa, jotta rikospaikan pohjapiirros ja tärkeät yksityiskohdat säilyvät ja tallennetaan. Yleiskuvan taltioinnin lisäksi on tärkeää dokumentoida tarkasti haltuun otettavat laitteet. Dokumentoitavia asioita ovat muun muassa laitteen tila eli onko laite käynnissä tai sammuneena. Myös laitteen kunto tulisi tulla ilmi valokuvista, joista näkee, onko laite jollain tavalla vaurioitunut. Mikäli laitteeseen on kytketty oheislaitteita tai muita kaapeleita, ne tulee myös dokumentoida. Kun todisteita lopulta päätetään ottaa haltuun, ne tulisi merkitä yksilöllisesti ja kirjata hallintaketjuun. (Bulbul ym. 2013, 254.)

Fyysisten todisteiden lisäksi on tärkeää dokumentoida myös digitaaliset todisteet ja niille suoritetut toimenpiteet. Varsinkin digitaalisen todistusaineiston manuaalinen käsittely aiheuttaa usein muutoksia dataan. Aina kun ollaan vuorovaikutuksessa käynnissä olevan laitteen kanssa, on arvioitava ja hallittava riski alkuperäisen tiedon vaarantumiselle ja dokumentoida suoritetut toimenpiteet. Useimmissa tapauksissa tämä vaatii vähintään kameran, joka pystyy taltioimaan näytöllä näkyvän tiedon, mutta myös muita menetelmiä voi olla saatavilla. (Horsman 2022, 3, 6.) Käynnissä olevan laitteen näytöllä näkyvät ohjelmat ja prosessit tulisi dokumentoida valokuvaamalla. Jos haltuunoton aikana tapahtuu virheitä, niitä ei tule peitellä. Käsittelyn aikana tapahtuneet virheet voivat heikentää digitaalisia todisteita tai niiden saantia. Niin kauan kuin kaikki toimenpiteet on rehellisesti kirjattu ylös, niitä voidaan silti hyödyntää. (Bulbul ym. 2013, 254.)

5.4.2 Lohkoketju hallintaketjuna

Tietotekniikan kehitys viimeisen kahden vuosikymmenen aikana on tehnyt digitaalisten todisteiden keräämisestä, säilyttämisestä ja analysoinnista erittäin tärkeän työkalun rikosten esitutkinnassa ja niiden ratkaisemisessa. Digitaalisilla

todisteilla on tärkeä rooli varsinkin verkossa tapahtuviin rikoksiin, sillä sitä käytetään henkilöiden ja rikosten toisiinsa yhdistämiseen. Siksi on äärimmäisen tärkeää taata digitaalisen todistusaineiston alkuperäisyys, eheys ja tarkastettavuus, kun se liikkuu hallintaketjun eri hierarkiatasoissa tutkinnan aikana. (Lone & Naaz 2019, 44.)

Hallintaketju on prosessi, joka seuraa todisteiden liikkumista dokumentoimalla jokaisen todisteita käsitelleen henkilön sekä päivämäärän ja ajan, jolloin sitä on käsitelty (Ali ym. 2017, 9). Digitaaliforensista hallintaketjua voidaan kuvata prosessiksi, jolla dokumentoidaan ja ylläpidetään digitaalisen todisteen käsittelyn kronologista historiaa. Hallintaketjulla on tärkeä rooli missä tahansa tutkinnassa, koska se tallentaa yksityiskohtaisesti todistusaineiston koko elinkaaren. Erityistä varovaisuutta vaaditaan hallintaketjun suojaamiseksi luvattomalta muuttamiselta tai tuhoutumiselta. Hallintaketjun perimmäisenä tavoitteena on osoittaa, että väitetyt todisteet ovat sidoksissa epäiltyyn rikokseen, eivätkä ne ole totuudenvastaisesti hankittuja. Heikosti ylläpidetty hallintaketju voi johtaa jopa siihen, että digitaalinen todistusaineisto ei ole enää oikeuskelpoista. (Lone & Naaz 2019, 44–45.)

Lohkoketju on yksinkertaisuudessaan sarja yhdistettyjä tietorakenteita, joita kutsutaan lohkoiksi. Se seuraa kaikkea, mitä vertaisverkon hajautetussa järjestelmässä tapahtuu. Jokainen lohko on linkitetty edelliseen lohkoon osoittimella, jota kutsutaan tiivistemuotoiseksi osoittimeksi (engl. hash pointer). Tämä linkitys muodostaa lohkoista ketjun. Lohkoketjuun tallennetut tiedot ovat pysyviä ja peruuttamattomia. Jokainen osallistuja voi tarkistaa tietojen oikeellisuuden tarkastamalla ne kirjausketjusta itse. Lohkoketju on suunniteltu takaamaan tietojen läpinäkyvyys, alkuperäisyys, turvallisuus ja tarkastettavuus. Tämä tekee siitä mahdollisesti parhaan työkalun digitaaliforensisen hallintaketjun ylläpitoon ja jäljittämiseen. (Lone & Naaz 2019, 45.)

Lohkoketjua käytettiin ensin kryptovaluuttojen ydinteknologiana. Bitcoin on ensimmäinen ja tunnetuin hajautettu kryptografiaan perustuva virtuaalivaluutta eli kryptovaluutta. Lohkoketjuteknologian kehityksen myötä se on herättänyt eri aloilla huomattavaa kiinnostusta. Kryptovaluutan lisäksi tutkijat ovat alkaneet tutkia eri lähestymistapoja turvallisuusongelmien ratkaisemiseen lohkoketjun

avulla. Tähän mennessä sitä on käytetty laajasti eri aloilla, kuten lohkoketjupohjaiseen pilvipalveluun sekä IoT-laitteiden tietoturvaan. Digitaalisen forensiikan alalla lohkoketju on myös lupaava lähestymistapa todisteiden varmistamiseen ja hallintaan. (Tian ym. 2019, 152.)

Suojatun digitaalisen todistusaineiston hallintajärjestelmän tulisi varmistaa, että todisteita ei voida manipuloida eikä yksityisiä tietoja voida vuotaa. Lupaavan ratkaisun digitaalisen todistusaineiston hallintaan tuo hajautettu lohkoketju, joka on suunniteltu estämään tiedon manipulointi. Lohkoketjulla on kuitenkin haasteita suuren datamäärän ja yksityisyyden vuoksi. Näitä luovat digitaalisten todisteiden valtava määrä sekä todisteiden jäljitettävyyden ja yksityisyyden välinen ristiriita. Tähän ratkaisuksi Tian ym. (2019) ehdottivat Block-DEF viitekehystä, jossa digitaalisen todistusaineiston tiedot ja itse data säilytetään erikseen. Vain todisteiden tiedot tallennetaan lohkoketjuun ja data erilliselle luotettavalle alustalle. (Tian ym. 2019, 151.) Samankaltaiseen ratkaisuun päätyivät myös Lone & Naaz (2019), joiden lohkoketjuun perustuva ratkaisu Forensic-Chain on tarkoitettu digitaalisen forensiikan hallintaketjuksi. Se tuo mahdollisuuden säilyttää digitaalisen todistusaineiston sekä toimintamenettelyjen eheyden, läpinäkyvyyden, alkuperäisyyden, turvallisuuden ja tarkastettavuuden. Lohkoketjuun perustuva ratkaisu antaa mahdollisuuden käytettyjen menettelytapojen ja työkalujen tarkastamiseen, sekä minkä tahansa tapahtuman alkuperän jäljittämiseen. (Lone & Naaz 2019, 52.)

Tutkimuksissa molemmat sekä Forensic-Chain että Block-DEF -lohkoketjumallit todettiin hyödyllisiksi ja käyttökelpoisiksi. Niiden avulla voitiin varmistaa digitaalisen todistusaineiston alkuperäisyys, eheys, jäljitettävyys ja ylläpito hallintaketjussa. Ne pystyivät myös hyvin skaalautumaan ja varmistamaan lohkoketjuun tallennetun tiedon yksityisyyden. Lisäksi Forensic-Chainin tekijät pyrkivät myös kehittämään lohkoketjuun perustuvan lisäosan digitaaliforensisille työkaluille. Sen tarkoitus olisi automaattisesti tallentaa kaikki tutkijan todistusaineistolle tekemät toimet, jolla voidaan varmistaa työkalujen eheys ja johdonmukainen toiminta. (Lone & Naaz 2019, 54; Tian ym. 2019, 164.)

6 TULOSTEN VERTAILU

Työn tuloksissa oli kaksi erilaista digitaalisen forensiikan viitekehystä, jotka perustuivat kirjallisuuskatsaukseen. Viitekehykset oli validoitu vertaamalla työn tuloksia muihin forensiikkamalleihin. Samanlaista aineistotriangulaatiota hyödynnettiin vertaamalla tämän työn tuloksia alan muihin luotettaviksi katsottuihin viitekehyksiin. Vertailun tarkoituksena oli pyrkiä vahvistamaan tulosten oikeellisuus sekä nostaa esiin mahdollisia eroavaisuuksia tai tarkennuksia turvallisen haltuunoton prosessiin.

Vertailuaineisto koottiin alan virallistiedosta sekä manuaalisella haulla että asiantuntijayhteydenottojen perusteella. Virallistiedolla tarkoitetaan virallisten tahojen, kuten valtion laitosten tuottamaa tietoa (Xamk 2022b). Vertailuaineiston katsottiin olevan luotettavaa niiden julkaisijatahon perusteella ja niiden tuottamaa aineistoa hyödynnetään yleisesti alan tutkimustiedon lähteenä. Vertailuaineiston sisältö myös tuki tässä tutkimuksessa esiin tulleita tuloksia. Tutkimukseen valittu vertailuaineisto on esitetty taulukossa 6.

Taulukko 4. Vertailuaineisto.

Julkaisija	Vuosi	Otsikko
ENISA	2015	Electronic evidence – a basic guide for First Responders
Interpol	2021	Guidelines for digital forensic first responders
NIST	2014	Guidelines on Mobile Device Forensics
SWGDE	2020	SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling and Acquisition

Julkaisuista Euroopan unionin kyberturvallisuusvirasto ENISA muodosti yleistä yhteenvetoa toimista, jotka mahdollistavat erilaisen digitaalisen todistusaineiston haltuunoton. Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin (NIST) sekä digitaalisen todistusaineiston tieteellisen työryhmän (Scientific Working Group on Digital Evidence tai SWGDE) julkaisut keskittyivät mobiililaitteiden forensiikkaan. Kansainvälisen rikospoliisijärjestö (International Criminal Police Organization) Interpolin ohje sen sijaan käsitteli laajasti eri digitaalisen todistusaineiston tietolähteitä, kuten jopa esimerkiksi lentoalusten forensiikkaa.

Vertailuaineistoissa toistuvat samat perusperiaatteet digitaalisen todistusaineiston haltuunottoon. Käynnissä olevaa laitetta ei tule sammuttaa ja pois päältä

olevaa laitetta ei tule käynnistää (Interpol 2021, 17.) Vertailuaineisto ja tutkimustulokset eroavat toisistaan vain yksityiskohdissa, mutta eivät poissulkevasti. Vertailuosioon on nostettu aineistosta nousseet seikat, joita ei ollut huomioitu kirjallisuuskatsauksen tutkimuksissa.

6.1 Turvallinen haltuunotto

Digitaalisen todistusaineiston turvallinen haltuunotto alkaa tapahtumapaikan turvaamisella myös vertailuaineistossa. ENISA:n ja Interpolin julkaisuissa otetaan työturvallisuuden lisäksi huomioon myös se, että asiattomat henkilöt eivät saisi olla tekemisissä laitteiden tai virtalähteiden kanssa. Henkilöiden pääsy tapahtumapaikalle tulee kieltää ja asiattomat henkilöt poistaa tilasta. Lisäksi epäillyt eivät saa olla yhteydessä keneenkään, joka ei ole paikalla, jotta estetään tietojen etätuhoaminen. (ENISA 2015, 14; Interpol 2021, 15.)

6.1.1 Tunnistaminen

Laitteiden haltuunottoa ohjaa niiden oikeaoppinen tunnistaminen, joka saattaa määrätä millaisia tekniikoita haltuunottoon voidaan käyttää. Laitteen ulkokuoressa saattaa olla valmistajan merkki ja malli sekä muita tunnisteita, kuten sarjanumero. Puhelimissa on myös usein nähtävissä IMEI-koodi joko laitteen takakannessa, akun alla tai SIM-kelkassa. Jos laite on käynnissä, sen näytöllä näkyvät tiedot voivat myös auttaa sen tunnistamisessa. Näytöllä voi näkyä esimerkiksi valmistajan tai operaattorin nimi, tai näytön asettelusta voi käydä ilmi käytössä oleva käyttöjärjestelmä. (SWGDE 2020, 13–14.) Tunnistamisessa voidaan hyödyntää myös laitteen omistajaa kysymällä mikä laite on ja mitä tietoa se sisältää (NIST 2014, 24–25.)

6.1.2 Haltuunotto

Käynnissä ja lukitsemattomana oleva mobiililaite on otettava haltuun paikan päällä mahdollisimman pian. Mobiililaitteen näytön voi pitää käynnissä toistuvalla vuorovaikutuksella kosketusnäytön kanssa tai muuttaa automaattisen lukituksen asetuksia. Jos laitteen salasana saadaan talteen, sitä on testattava käyttämällä muita menetelmiä kuin puhelimen lukitsemista. Tiedossa oleva salasana, kuten pääsykoodi, voidaan myös ottaa pois käytöstä laitteen asetuk-

sista. (SWGDE 2020, 12; Interpol 2021, 26.) Aiemmin tutkijat eristivät mobiililaitteen verkkoyhteydet asettamalla sen lentotilaan. Mobiilikäyttöjärjestelmien uudempien versioiden lentotilaominaisuus ei kuitenkaan välttämättä poista Bluetoothia, Wifiä tai muita langattomia protokollia käytöstä, tai se saattaa katkaista niiden yhteyden vain tilapäisesti. Tutkijoiden tulisikin varmistaa manuaalisesti, että verkkoyhteydet ovat poistettu käytöstä. Tarvittaessa laite voidaan asettaa verkkoyhteydet eristävään faraday-pussiin. (SWGDE 2020, 13; Interpol 2021, 30.)

Käynnissä olevan tietokoneen näytön herättämisessä tulee välttää virtapainikkeen ja ”Enter”-näppäimen painamista, sillä ne voivat tahattomasti sammuttaa laitteen tai poistaa siinä olevia tietoja. Turvallisempia keinoja ovat muun muassa ”Shift”-näppäimen painaminen tai hiiren liikuttaminen. Kaikki tehdyt toimenpiteet tulee dokumentoida tarkasti ja tietokoneen kaikki aktiiviset prosessit tulee tarkistaa mahdollisten tietoja tuhoavien prosessien varalta. Jos havaitaan, että jokin tietoja tuhoava prosessi on käynnissä, kuten tiedostojen salaus tai poistaminen, on se keskeytettävä välittömästi. Tarvittaessa jopa sammuttamalla tietokone. Muita tarkistettavia asioita ovat muun muassa laitteen aika- ja päivämääräasetukset, verkkoyhteydet, pilvipalvelut sekä salatut levyosiot. Mikäli havaitaan avoinna olevia salattuja osioita, tulee arvioida niiden jäljentäminen paikan päällä ennen laitteen siirtämistä. Mikäli laite on tarkoitus siirtää käynnissä olevana, tulee virranhallinta-asetuksista tarkistaa, että tietokone ei siirry lepotilaan tai sammu kuljetukseen aikana. (Interpol 2021, 32.)

Sammuneena olevia mobiililaitteita tai tietokoneita ei tule käynnistää. Laitteesta tulee ainoastaan kerätä tunnistetiedot, kuten mallinumero, operaattori ja yksilölliset tunnistetiedot. (SWGDE 2020, 8.) Ei ole järkevää vaarantaa laitteesta mahdollisesti löytyvän digitaalisen todistusaineiston eheyttä käynnistämällä laitetta. Kiireellisissä tapauksissa joitain laitteita voidaan analysoida lukutilassa kirjoitussuojan kautta, jotta alkuperäinen data pysyy muuttumattomana. (Interpol 2021, 33.)

Laitteiden lisäksi kiinnostuksen kohteita ovat oheislaitteet, kaapelit, virtalähteet ja muut tarvikkeet. Joissain tapauksissa myös laitteiden pakkaukset, tuoteoppaat ja ohjelmistot voivat olla hyödyllisiä. (NIST 2014, 27, 29.) Erityisesti data-

ja virtakaapelit ovat tärkeitä ottaa haltuun yhdessä laitteen kanssa, sillä ne voivat olla laitemallille yksilöllisiä. Virta- tai datakaapelin puuttuminen voi mahdollisesti estää tai viivästyttää laitteen tutkimista. (Interpol 2021, 24, 34.)

6.1.3 Kuljetus ja varastointi

Mobiililaite voidaan ottaa haltuun lukitsemattomana, mutta joissain Android-laitemalleissa on käytettävissä kehittyneitä tietoturvaominaisuuksia laitteen lukituksen avaamiseen ja sulkemiseen. Näitä ovat muun muassa valmiiksi puhelimessa olevat älylukitusvaihtoehdot, kuten kehon tunnistus, luotetut paikat sekä luotetut laitteet. Kehon tunnistus pitää laitteen lukitsemattomana niin kauan kuin puhelin havaitsee, että se on edelleen omistajan hallussa. Jos puhelin havaitsee, että se on pois omistajan hallusta, kuten asetettuna pöydälle, puhelin voi lukkiutua. Luotetut paikat on suunniteltu avaamaan puhelin, kun se saapuu luotetuksi merkittyyn sijaintiin. Tämä määritetään yleisimmin paikannuspalvelun ja langattomien verkkojen avulla. Esimerkiksi omistajan koti voi olla merkitty luotetuksi paikaksi, jolloin se pysyy lukitsemattomana kodin läheisyydessä. Luotetut laitteet toimivat yleensä Bluetooth-yhteyden avulla. Käyttäjä voi esimerkiksi asettaa älykellon luotetuksi laitteeksi, jolloin puhelin ei vaadi pääsykoodia, kun älykello havaitaan laitteen läheisyydessä. Avoinna olevan mobiililaitteen älylukitusvaihtoehdot tulisikin siis tarkistaa ennen kuljetusta, jotta laite ei lukkiudu kuljetuksen yhteydessä. (SWGDE 2020, 11.)

Mikäli laitetta ei ole saatu eristettyä verkkoyhteyksistä, se tulee kuljettaa ja varastoida faraday-pussin avulla. Mobiililaitteet, joiden yhteys verkkoon on estetty, lisäävät virrankulutusta yrittäessään saada yhteyttä tukiasemiin. Tämä kuluttaa laitteen akkua normaalia nopeammin. Laitteen käynnissä pitämiseksi se tulee liittää ulkoiseen virtalähteeseen, kuten kannettavaan virtapankkiin. Sekä mobiililaite että virtalähde tulee laittaa faraday-pussin sisälle. Jos virtalähdettä ei aseteta faraday-pussiin, virtalähteen kaapeli voi toimia antennina ja laite muodostaa yhteyden verkkoon. (NIST 2014, 29; SWGDE 2020, 8.) Laitteen sammuttaminen sen eristämiseksi verkosta aiheuttaa riskin, että autentikointimenetelmät kytkeytyvät päälle tai tehostetut suojausominaisuudet otetaan käyttöön, jolloin tietosisältöön ei mahdollisesti päästä käsiksi (SWGDE 2020, 13; Interpol 2021, 20).

6.2 Prosessiin vaikuttavat tekijät

On olemassa sekä etänä että paikallisesti suorittavia komentoja, jotka ovat suunniteltu tuhoamaan todistusaineistoa. Etänä suoritettavia komentoja vastaan voidaan suojautua ottamalla laite haltuun verkkoyhteydet suojaavaan faraday-pussiin. (Interpol 2021, 24.) Faraday-pussin käyttö on kuitenkin turhaa, mikäli laboratoriossa ei ole verkkoyhteyksiltä suojattuja säiliöitä tai työtiloja laitteiden käsittelyyn. Koko työalueen suojaaminen voi olla kallis, mutta tehokas tapa suorittaa jatkotoimenpiteet turvallisesti. Halvempi vaihtoehto on esimerkiksi faraday-teltta, jota voidaan tarvittaessa myös siirtää. Kaapeleiden syöttäminen telttaan on kuitenkin ongelmallista, sillä ilman asianmukaista eristystä ne voivat käyttäytyä antennina, mikä tekee teltan tarkoituksen merkityksettömäksi. Pienemmälle organisaatiolle tarkoituksenmukaisempi voi olla kannettava suojattu säiliö. Se mahdollistaa jatkotoimenpiteiden suorittamisen turvallisesti, kun laite on asetettu sen sisään. Säiliöissä on myös eristetyt kaapeliliitännät, jotka estävät verkkoyhteydet esimerkiksi datan siirtoa varten. Tämä menetelmä on yksi yleisimmin käytetyistä. (NIST 2014, 32.)

Kappaleessa 6.1.2 mainitut ”turvalliset näppäimet” on voitu määritellä laitteessa uudelleen, jotta ne eivät toimi oletusarvoisesti. Tietyn tai tiettyjen näppäinten painallusten yhdistelmä voi käynnistää haitallisen komennon, jonka tarkoituksena on estää digitaalisen todistusaineiston haltuunotto. Kappaleessa 6.1.3 mainitut älylukitusmekanismit voidaan määritellä myös automaattisesti pyyhkimään laitteen tiedot, kun laitteen paikannustiedot määrittävät laitteen saapuneen tai poistuneen tietystä sijainnista. Tämä menetelmä voi käyttää myös langattomien verkkojen tukiasemia sijainnin määrittämiseen. (NIST 2013, 30.)

Laitteet voivat sisältää myös prosessiin vaikuttavia viruksia tai muita haittaohjelmia. Haittaohjelmat pyrkivät usein levittäytymään muihin laitteisiin langallisten tai langattomien liitäntöjen kautta, joka voi saastuttaa myös tutkijan käyttämät työkalut. Laitteen oletusohjelmia on myös voitu korvata tarkoituksellisesti haitallisilla ohjelmilla, jotka ovat suunniteltu muuttamaan tai poistamaan laitteen tietoja. Tämän vuoksi on tärkeä pyrkiä välttämään käynnistämästä kohdelaitteen sovelluksia. (NIST 2014, 30).

6.3 Katoavan datan taltiointi

Käynnissä olevan laitteen live-analyysin tarkoituksena on saada mahdollisimman paljon tietoa laitteesta ennen sen sammuttamista. Menettelyn tarkoitus on muuttaa alkuperäistä dataa mahdollisimman vähän, mukaan lukien tutkinnan kannalta kiinnostavat haihtuvat tiedot kuten laitteen välimuisti. Se on tarpeen erityisesti laitteissa, joissa on käytössä salattuja levyosioita. Näitä ovat esimerkiksi BitLocker, FileVault, VeraCrypt, TrueCrypt tai BestCrypt ja vastaavat salausratkaisut. Live-analyysillä on mahdollista taltioida data salaamattomana ilman tiedossa olevaa salausavainta. (Interpol 2021, 32.)

Katoavan datan taltiointiin tulisi käyttää työkalua, jolla on mahdollisimman vähän vaikutusta kohdelaitteeseen. Esimerkiksi välimuistin taltiointiin on tietojen ylikirjoittamisen välttämiseksi parempi käyttää tekstipohjaista DumpIt-työkalua kuin graafisella käyttöliittymällä varustettua FTK Imageria. Työkaluilla tehtäviä jäljennöksiä ei tule koskaan tallentaa kohdelaitteelle tai epäillyn muihin medialaitteisiin, sillä se voi ylikirjoittaa tärkeää todistusaineistoa. (Interpol 2021, 19.)

Vapaasti saatavien työkalujen lisäksi on olemassa myös joitakin erityisesti lainvalvontaviranomaisia varten kehitettyjä työkaluja, jotka voivat auttaa live-analyysissä. Yksi niistä on FiRST, joka on Berliinin poliisin kehittämä FREETOOL-hankkeeseen kuuluva työkalu. FiRST:n tarkoitus on ilmoittaa tutkijalle voiko laitteen sammuttaa turvallisesti. Se tarkastaa merkkejä muun muassa salaus- ja levynpyyhintäohjelmistoista, pilvi- ja verkkotallennuspaikoista sekä virtualisoinnista. Jos työkalu havaitsee näitä merkkejä, se varoittaa tutkijaa ja kehottaa ottamaan yhteyttä asiantuntijaan ennen laitteen sammuttamista. (Interpol 2021, 19.)

Työkalujen lisäksi ENISA ja Interpol tuovat julkaisuissaan esiin komentoja, joita voidaan ajaa kohdelaitteen komentokehotteella. Komennoilla voidaan saada erilaisia tietoja kohdejärjestelmästä, kuten käynnissä olevat prosessit, aktiiviset verkkoyhteydet ja salatut levyosiot. Näiden käyttöä voidaan harkita, jos käytössä ei ole erityistä tietojen keräämiseen tarkoitettua työkalua. (ENISA 2015, 11–13; Interpol 2021, 18–19.)

6.4 Alkuperäisyyden ja eheyden varmistaminen

Digitaalisen todistusaineiston eheys on varmistettava haltuunoton kaikissa vaiheissa. Mikään toimenpide ei saisi muuttaa tietoja, joita voidaan myöhemmin käyttää todisteena. Todisteiden eheysvaatimus on tärkein tekijä päätettäessä, mitä toimenpiteitä haltuun otettaville laitteille tehdään. Päällä olevien laitteiden tiedot kuitenkin muuttuvat jatkuvasti niiden dynaamisen luonteen vuoksi. Kun todistusaineistoa ei voida kerätä muuttamatta sitä, keruuvaiheet on dokumentoitava niin tarkasti kuin mahdollista. (ENISA 2015, 6–7.)

6.4.1 Dokumentointi

Laitteista voidaan dokumentoida perustietojen lisäksi myös muita huomioita kuten, jos jokin laite on ollut esimerkiksi vain lasten käytössä (Interpol 2021, 16). Erityisen tärkeää on dokumentoida laitteisiin asetettu päivämäärä, kellonaika ja aikavyöhyke esimerkiksi ottamalla kuva käynnissä olevan laitteen näytöstä. Päivämäärä- ja aika-asetukset voivat tulla automaattisesti verkosta tai ne ovat voitu asettaa manuaalisesti. Tutkinnan kannalta on merkitystä, mikäli laitteen aika-asetukset on asetettu manuaalisesti eri aikaan, kuin mitä ne todellisuudessa ovat. Tämä voi aiheuttaa sen, että laitteelle tallentuneet aikaleimat ovat harhaanjohtavia. (NIST 2014, 41; Interpol 2021, 32.)

Dokumentoinnissa ei voida myöskään poissulkea perinteistä (ei sähköistä) todistusaineistoa. Rikospaikan dokumentoinnissa tulee ottaa huomioon esimerkiksi paperilapuille ja vihkoihin kirjoitetut käyttäjätunnukset ja salasanat. Ylös kirjatuilla salasanoilla tai palautuskoodeilla voi olla merkitystä tutkinnan kannalta, ja niillä voidaan saada pääsy laitteille tallennettuihin salattuihin tietoihin. (NIST 2014, 28; Interpol 2021, 10.)

ENISA korostaa julkaisussaan dokumentoinnin tärkeyttä. Kaikki todistusaineisto ja sen yksityiskohdat tulee kirjata hallintaketjuun, sillä ne voivat olla tutkinnan kannalta ratkaisevan tärkeitä. On parempi kirjata ylös liian monta yksityiskohtaa, kuin kirjata liian vähän yksityiskohtia toteutetuista toimista. On esimerkiksi suositeltavaa kirjata ylös mitä näppäimiä on painettu ja mitä hiirenliikkeitä on tehty, eikä vain kirjata yleisluonteisesti, että tiedostot ovat jäljennetty. (ENISA 2015, 7.)

7 INTERVENTIO

Tutkimustulosten perusteella tehty tuotos eli interventio on työn liitteenä julkisuuslain mukaisesti salattuna. Julkisuuslain mukaan Tullin taktisia ja teknisiä menetelmiä koskevia tietoja sisältävät asiakirjat ovat salassa pidettäviä, jos niiden tiedon antaminen vaarantaisi rikosten selvittämistä (Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621, 6. luku 24. § kohta 5). Vaikka oppaat ovat salattuina, ne perustuvat työn tutkimustuloksiin. Toimeksiantaja tai tekijä voi harkintansa mukaan myös jakaa niitä muille viranomaisille salassapitomääräykset huomioiden.

Interventioita tehtiin kaksi kappaletta eri kohderyhmille. Ensimmäinen opas toimii yleisluontoisena ohjeena Tullin valvontaosaston henkilöstölle, jotka kohtaavat työssään digitaalista todistusaineistoa. Opas sisältää yleisohjeet sekä mobiililaitteiden että tietokoneiden turvalliseen haltuunottoon. Toisessa oppaassa otettiin erityisesti huomioon, vaatiiko olosuhteet tietojen taltioinnin tekemistä paikan päällä. Opas on suunnattu tietoteknisille tutkijoille ja sisältää laajemman ohjeistuksen laitteiden oikeaoppiseen käsittelyyn, kernel-tason työkaluja sekä hyödyllisiä komentokehotteella suoritettavia komentoja.

Tuotoksen kehittäminen oli syklinen prosessi, jota kehitettiin toimeksiantajan arvioinnin perusteella. Toimeksiantajan organisaatiossa työskentelevien erityisasiantuntijoiden mukanaolo toi tuotokselle sen vaatimaa luotettavuutta, jotta sitä voidaan hyödyntää viranomaistoiminnassa. Ensimmäiset versiot tuotoksista luotiin toukokuussa ja toiset versiot marraskuussa 2022. Kolmannet ja viimeiset versiot luotiin maaliskuussa 2023 sähköiseen muotoon, joka mahdollistaa niiden helpon siirrettävyyden ja tulostamisen. Tuotokset jaettiin toimeksiantajalle tiedostomuodossa, joka sallii tarvittaessa niiden muokkaamisen ja päivittämisen. Tämä mahdollistaa tuotosten jatkokehittämisen, mikäli ohjeistus tulevaisuudessa ei ole enää ajankohtaista tietoteknisen kehityksen tai toimintatapojen muutoksen seurauksena.

8 JOHTOPÄÄTÖKSET

Digitaalisen todistusaineiston turvallinen haltuunotto perustuu tietoon siitä, miten erilaiset tietotekniset laitteet toimivat ja miten niitä on mahdollista käyttää. Laitteet käsittelevät niihin tallentunutta dataa eritavoin ja tätä tapaa on myös

mahdollista manipuloida. Tämän vuoksi on hankalaa luoda tyhjentävää opasta niiden oikeaoppisesta käsittelystä. On kuitenkin mahdollista luoda toimintaohje yleisistä periaatteista, jotka mahdollistavat digitaalisen todistusaineiston turvallisen haltuunoton.

Ensisijaisesti työssä pyrittiin vastaamaan siihen, *miten tietotekninen laite otetaan turvallisesti haltuun*. Tutkimuksen apukysymyksinä olivat *mitkä tekijät vaikuttavat prosessiin*, *miten katoava data saadaan taltioitua* sekä *millä keinoilla voidaan varmistaa digitaalisen todistusaineiston alkuperäisyys ja eheys*. Prosessiin vaikuttavia tekijöitä löydettiin tutkimuksessa useita, joista vakavimmat voivat täysin hävittää digitaalisen todistusaineiston. Näitä haitallisia prosesseja voidaan kuitenkin ehkäistä oikeilla toimintatavoilla. Laitteissa esiintyvää katoavaa dataa voidaan taltioida sekä manuaalisesti että automaattisesti eri työvälineillä. Vastuu sen taltioinnista voidaan siirtää eteenpäin, kun tutkija osaa ottaa haltuun ja kuljettaa laitteen turvallisesti asiantuntijalle. Digitaalisen todistusaineiston alkuperäisyyden ja eheyden varmistamisessa korostuu oikeiden toimintatapojen noudattaminen sekä niiden tarkka dokumentointi.

Työn tavoitteena oli ongelman selvityksen lisäksi myös luoda interventio, joka toimii oppaana tai toimintaohjeena digitaalisen todistusaineiston turvalliseen haltuunottoon. Työn tuloksia voidaan pitää onnistuneena, sillä niiden tulkinnalla oli mahdollista päästä tähän tavoitteeseen. Työn onnistumista tuki aineistonkeruun toteutus sekä sovelletun vertailuaineiston käyttäminen. Tekijän johtopäätös on, että tietoteknisen laitteen turvallinen haltuunotto voidaan kiteyttää yhteen lauseeseen, mikäli siinä ei ole tietoja tuhoavia prosesseja käynnissä. Pidä laite päällä ja eristettynä verkkoyhteyksistä.

9 POHDINTA

Ylemmän korkeakoulun opinnäytteen on tarkoitus osoittaa opiskelijan kykenevän itsenäiseen asiantuntijatyöskentelyyn ja tässä myös koen onnistuneeni. Suurin haaste työn viimeistelyn lisäksi oli tutkimussuunnitelma, joka vaati tutustumista tieteelliseen tutkimusprosessiin. Laadukkaasti tehty tutkimussuunnitelma kuitenkin tuki työn tavoitteisiin pääsyä. Varsinkin perustellut metodologiset valinnat ja oikeiden asioiden tutkiminen teki itse työn tekemisestä helppoa.

Alan tieteelliseen tutkimustietoon perehtyminen syvensi ammatillista osaamistani digitaalisesta forensiikasta, jonka lisäksi opin myös itse tekemään tutkimuksen tieteellisenä. Tämä on kehittänyt ammattitaitoani ja opinnäytetyön tekemisestä on varmasti apua myös työelämän kehittämisprojekteissa.

Vaikka opinnäytteen tarkoitus oli osoittaa itsenäistä asiantuntijatyöskentelyä, olisi sen tekemiseen voinut paremmin hyödyntää oppilaitoksen, toimeksiantajan tai muiden organisaatioiden asiantuntijoita. Työn tulosten kannalta tällä ei välttämättä olisi ollut suurta merkitystä, sillä se perustui sekundääriaineistoon. Tulosten raportointiin sen sijaan olisi voinut olla hyötyä olemalla aktiivisempi ja kysymällä neuvoa. Raportoinnin onnistuin kuitenkin mielestäni sekä ohjaajan palautteen perusteella pitämään selkokielisenä, jotta työn tulokset ovat lukijalle mahdollisimman helposti ymmärrettäviä.

9.1 Luotettavuustarkastelu

Tutkimuksen luotettavuustarkastelussa suuressa roolissa on työssä tehty systemoitu kirjallisuuskatsaus, jolla on suora vaikutus työn tulosten luotettavuuteen. Kirjallisuuskatsauksen tuloksena saadun tiedon luotettavuutta pyrittiin lisäämään tarkoilla sisäänottokriteereillä, joita oli muun muassa se, että aineistona käytettiin vertaisarvioitua tutkimustietoa. Systemoitu kirjallisuuskatsaus sekä muut tutkimuksessa tehdyt valinnat ja menetelmät perusteltiin ja dokumentoitiin tarkasti, joka mahdollistaa niiden luotettavuustarkastelun arvioinnin (Kananen 2017b, 178). Voidaankin sanoa, että systemoitua kirjallisuuskatsausta ja digitaalisen todistusaineiston turvallista haltuunottoa yhdistää tärkeys dokumentoida mieluummin liika tietoa kuin liian vähän.

Työn validiteettia eli oikeiden asioiden tutkimista voidaan pitää onnistuneena, sillä ne mahdollistivat tavoitteisiin pääsyn eli intervention luomisen ongelman ratkaisemiseksi. Saatujen tulosten luotettavuutta lisää aineistotriangulaationa tehty tulosten vertailu, joka ei tuonut ilmi ristiriitoja tulosten ja vertailuaineistona käytetyn virallistiedon välillä. Sen sijaan aineistovertailu tuotti osaltaan tarkempaa tietoa joistain toimenpiteistä digitaalisen todistusaineiston turvalliseen haltuunottoon, joka auttoi työn tavoitteisiin pääsyä.

Opinnäytetyö tehtiin tullirikosten selvittämisen tueksi, mutta saatuja tuloksia voidaan yleistää myös muuhun forensiseen tutkimukseen. Digitaalisen todistusaineiston turvallista haltuunottoa voidaan hyödyntää myös muussa viranomaistoiminnassa sekä onnettomuuden tai vikatilanteiden selvittämisessä. Toimintatutkimuksen ongelmanratkaisuun tähtäävää tuotosta voidaan arvioida vain tuloksen vertaamista tavoitteisiin ja arvioinnin suorittavat ne, jotka olivat prosessissa mukana (Kananen 2014, 137).

9.2 Jatkotutkimusaiheet

Digitaalisen todistusaineiston haltuunotto on ensimmäinen osa digitaalista forensiikkaa, johon sisältyy myös muita työvaiheita (kuva 6). Aihealueen laajentaminen antaa mahdollisuuden tehdä jatkotutkimusta näistä myöhemmistä vaiheista. Näin saataisiin Suomen viranomaisille selkeä ja tutkittuun tietoon perustuva viitekehys, joka ohjaa digitaalisen forensiikan prosessia haltuunotosta raportointiin.

Kuva 6. Digitaalisen forensiikan työvaiheet.

Hyökkäävästä kyberturvallisuudesta kiinnostuneelle sopiva jatkotutkimusaihe voisi olla jäljentäminen. Tietoteknisten laitteiden uudet jäljentämiskeinot vaativat yleensä uusien haavoittuvuuksien löytämistä ja hyödyntämistä niin, että päästään käsiksi laitteissa olevaan dataan salaamattomana. Puolustavasta kyberturvallisuudesta kiinnostuneelle sopiva aihealue voisi olla datan tutkiminen ja analysointi. Uusia tietoteknisiä laitteita tulee markkinoille jatkuvasti, ja välillä jopa uusia tiedostojärjestelmiä, jotka tallentavat dataa uudella tavalla. Niiden tutkiminen tuo alalle uutta tietoa ja auttaa forensista analyysiä tekeviä yksiköitä.

Digitaalisen forensiikan tuloksena muodostetaan yleensä tietotekninen raportti, jossa esitetään forensisen analyysin tulokset. Tällä hetkellä Suomen viranomaisilla ei ole yhtenäistä raportointitapaa tulosten esittämiseen, vaan niiden ulkoasu ja sisältö vaihtelee. Tutkimalla sekä luomalla yhtenäisen ja oikeuskelpoisen

raportointitavan voitaisiin kehittää tietoteknisen tutkinnan raportointia, tiedonhallintaa sekä tulosten ymmärrettävyyttä rikosprosessin myöhemmissä vaiheissa.

LÄHTEET

Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A. & Saeed, F. 2017. A metamodel for mobile forensics investigation domain. *PLoS ONE* 4, 1-32. PDF-dokumentti. Saatavissa: https://doi.org/10.1371/journal.pone.0176223 [viitattu 28.3.2022].

Bulbul, H.I., Güçlü Yavuzcan, H. & Ozel, M. 2013. Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). Forensic Science International 233 (2013), 244–256. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.forsciint.2013.09.007 [viitattu 22.2.2022].

Coghlan, D. & Brannick, T. 2010. Doing action research in your own organization. 3. painos. Lontoo: SAGE Publications.

ENISA. 2015. Electronic evidence – a basic guide for First Responders. PDF-dokumentti. Saatavissa: https://op.europa.eu/en/publication-detail/-/publication/12d3bbc9-c813-457e-b9a2-ec0de70f33d2 [viitatttu 9.11.2022].

Esitutkintalaki 22.7.2011/805.

Flinkman, M. & Salanterä, S. 2007. Integroitu katsaus - Eri metodeilla tehdyn tutkimuksen yhdistäminen katsauksessa. Teoksessa Johansson K., Axelin A., Stolt M. & Ääri R-L. (toim.) Systemaattinen kirjallisuuskatsaus ja sen tekeminen. Turku: Turun yliopisto, 84–100.

Fukami, A., Stoykova, R. & Geradts, Z. 2021. A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation* 38. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.fsidi.2021.301169 [viitattu 28.3.2022].

Hirsjärvi, S., Remes, P. & Sinivuori, E. 2013. Tutki ja kirjoita. 15.–17. painos. Porvoo: Bookwell Oy.

Holt, T. J., Clevenger, S. & Navarro, J. 2020. Exploring digital evidence recognition among officers and troopers in a sample of a state police force. *Policing: An International Journal* 1, 91–103. PDF-dokumentti. Saatavissa: https://doi.org/10.1108/PIJPSM-07-2019-0119 [viitattu 28.3.2022].

Horsman, G. 2022. Conducting a ‘manual examination’ of a device as part of a digital investigation. *Forensic Science International: Digital Investigation* 40. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.fsidi.2021.301331 [viitattu 28.3.2022].

Interpol. 2021. Guideline for digital forensics first responders. PDF-dokumentti. Saatavissa: https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf [Viitattu 9.11.2022].

Juhila, K. 2021. Teemoittelu. Teoksessa Vuori, J. (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-do-

kumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaope-tus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/teemoittelu [viitattu 17.2.2021.]

Kananen, J. 2014. Toimintatutkimus kehittämistutkimuksen muotona: Miten kirjoitan toimintatutkimuksen opinnäytetyönä? Jyväskylä: Jyväskylän ammatti-korkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 8.2.2022].

Kananen, J. 2017a. Kehittämistutkimus interventiotutkimuksen muotona: Opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylä: Jyväskylän ammattikor-keakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 8.2.2022].

Kananen, J. 2017b. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jy-väskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaak-kuri.finna.fi/ [viitattu 7.2.2022].

Kananen, J. 2019. Opinnäytetyön ja pro gradun pikaopas: Avain opinnäyte-työn ja pro gradun kirjoittamiseen. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 14.2.2022].

Karppinen, R. 2016. Todistamiskielloista. Teoksessa Lappalainen, J & Ojala, T (toim.) Kirjoituksia todistusoikeudesta. Helsinki: Hakapaino Oy, 47–62. PDF-dokumentti. Saatavissa: https://oikeus.fi/hovioikeudet/helsinginhovioikeus/ma-terial/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetut-julkaisut/kirjoituksiatodistusoikeudesta2006/JPfULfz9b/Kirjoituksia_todistusoi-keudesta_2006.pdf [viitattu 20.7.2022].

Korkein oikeus 20.12.2019 112.

Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621

Latzo, T., Palutke, R. & Freiling, F. 2019. A universal taxonomy and survey of forensic memory acquisition techniques. *Digital Investigation* 28, 56–69. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.diin.2019.01.001 [Viitattu 28.3.2022].

Lone, A. H. & Naaz, R. 2019. Forensic-chain: Blockchain based digital foren-sics chain of custody with PoC in Hyperledger Composer. *Digital Investigation* 28, 44–55. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.diin.2019.01.002 [viitattu 28.3.2022].

Markakis, E., Nikoloudakis, Y., Pallis, E., Panagiotakis, S. & Stoyanova, M. 2020. A Survey on the Internet of Things (IoT) Forensics: Challenges, Ap-proaches, and Open Issues. IEEE Communications Surveys & Tutorials 22, 1191–1221. PDF-dokumentti. Saatavissa: https://ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8950109 [viitattu 13.2.2022].

Meffert, C. S., Baggili, I. & Breitinger, F. 2016 Deleting collected digital evi-dence by exploiting a widely adopted hardware write blocker. *Digital Investiga-tion* 18, 87-96. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.diin.2016.04.004 [viitattu 28.32022].

Mothi, D., Janicke, H. & Wagner, I. 2020. A novel principle to validate digital forensic models. *Forensic Science International: Digital Investigation* 33. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.fsidi.2020.200904 [viitattu 28.3.2022].

NIST. 2014. Guidelines on Mobile Forensics. NIST Special Publication 800-101: 1. PDF-dokumentti. Saatavissa: https://nvlpubs.nist.gov/nistpubs/special-publications/nist.sp.800-101r1.pdf [Viitattu 9.11.2022].

Oikeudenkäymiskaari 12.6.2015/731.

Page, M., Mckenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., Mcdonald, S. & Moher, D. 2021. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Saatavissa: https://doi.org/10.1136/bmj.n71 [viitattu 22.3.2022].

Pakkokeinolaki 22.7.2011/806.

Pudas-Tähkä S-M. & Axelin A. 2007. Systemaattisen kirjallisuuskatsauksen aiheen rajaus, hakutermit ja abstraktien arviointi. Teoksessa Johansson K., Axelin A., Stolt M. & Ääri R-L. (toim.) Systemaattinen kirjallisuuskatsaus ja sen tekeminen. Turku: Turun yliopisto, 46–57.

Riekkinen, J. 2019. Sähköiset todisteet rikosprosessissa: Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen. Lapin yliopisto. Oikeustieteiden tiedekunta. Väitöskirja. Helsinki: Alma Talent.

Rikoslaki 30.5.2008/374.

Rogers, C. 2015. Authenticity of Digital Records: A Survey of Professional Practice. *L'authenticité des documents numériques: Un survol des pratiques professionnelles* 2, 97-113. PDF-dokumentti. Saatavissa: http://doi.org/10.1353/ils.2015.0015 [viitattu 28.3.2022].

Salakari, M. 2020. Systemoitu kirjallisuuskatsaus tiedon tuottamisen menetelmänä. PDF-dokumentti. Saatavissa: https://tohtori.turkuamk.fi/uploads/2020/04/92b18b03-kirjallisuuskatsaus_20.4.20.pdf [viitattu 19.3.2022].

Salminen A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa: Vaasan yliopisto. PDF-dokumentti. Saatavissa: https://urn.fi/URN:ISBN:978-952-476-349-3 [viitattu 15.2.2022].

Schramp, R. 2017. Live transportation and RAM acquisition proficiency test. *Digital Investigation* 20, 44–53. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.diin.2017.02.006 [28.3.2022].

Shafiee Hasanabadi, S., Habibi Lashkari, A. & Ghorbani, A. A. 2020. A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of forensic agents' behaviour. *Forensic Science International:*

Digital Investigation 35. PDF-dokumentti. Saatavissa: https://doi.org/10.1016/j.fsidi.2020.301024 [viitattu 28.3.2022].

Sisäministeriö. 2017. Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-324-136-7 [viitattu 2.2.2020].

Stüttgen, J. & Cohen, M. 2013. Anti-forensic resilient memory acquisition. *Digital Investigation* 10, 105–115. PDF-Dokumentti. Saatavissa: https://doi.org/10.1016/j.diin.2013.06.012 [viitattu 27.4.2022].

Suhonen, R., Axelin, A. & Stolt, M. 2016. Erilaiset kirjallisuuskatsaukset. Teoksessa Stolt, M., Axelin, A. & Suhonen, R. (toim.) Kirjallisuuskatsaus hoitotieteessä. 2. korjattu painos. Turku: Turun yliopisto, 7–22.

Syrjälä, L., Syrjäläinen, E., Ahonen, S. & Saari, S. 1994. Laadullisen tutkimuksen työtapoja. Helsinki: Kirjayhtymä.

SWGDE. 2020. SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition. PDF-dokumentti. Saatavissa: https://drive.google.com/file/d/1sVko_Uo7o6iootWwn9IoLJ3mrMVX-qTDg/view?usp=sharing [Viitattu 9.11.2022].

Tian, Z., Li, M., Qiu, M., Sun, Y. & Su, S. 2019. Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences* 491, 151-165. Saatavissa: https://doi.org/10.1016/j.ins.2019.04.011 [viitattu 28.3.2022].

Tulli. 2022. Tullin strategia. WWW-dokumentti. Saatavissa: https://tulli.fi/tietoa-tullista/tullin-toiminta/strategia [viitattu 3.2.2022].

Xamk. 2022a. Tiedonhankinta: 3. Miten yhdistää hakusanat. WWW-dokumentti. Päivitetty 16.3.2022. Saatavissa: https://libguides.xamk.fi/tiedonhankinta/porras3 [viitattu 18.3.2022].

Xamk. 2022b. Tiedonhankinta: 4. Tunnistatko tutkimustiedot ja erilaiset lähdeaineistot. Päivitetty 18.10.2022. Saatavissa: https://libguides.xamk.fi/tiedonhankinta/porras4 [viitattu 23.10.2022].

Liite 1/1

Systemoidun kirjallisuuskatsauksen aineisto

Tekijät	Otsikko	Tarkoitus	Tulokset
Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A. & Saeed, F. Malesia & Jemen: 2017.	A metamodel for mobile forensics investigation domain	Tutkia mobiiliforensiikan ongelmia ja haasteita.	Mobiiliforensiikan tiedonhallinnan puute aiheuttaa ongelmia varsinkin uusille forensiikkatutkijoille, joka johtuu käsitteiden ja termien epäselvyydestä, sekä hankaluudesta ymmärtää alan erilaisia prosesseja.
Bulbul, H.I., Güçlü Yavuzcan, H. & Ozel, M. Turkki: 2013.	Digital forensics – An Analytical Crime Scene Procedure Model (ACSPM)	Tutkia erilaisia malleja rikospaikan digitaalisten todisteiden hallintaan.	Rikospaikan digitaaliselle forensiikalle ei ole luotu menettelymallia todisteiden hallinnan laadun takaamiseksi. Tähän ehdotetaan analyyttistä menettelymallia.
Fukami, A., Stoykova, R. & Geradts, Z. Alankomaat & Norja: 2021.	A new model for forensic data extraction from encrypted mobile devices	Tutkia nykyaikaisia mobiiliforensiikan tekniikoita ja päivittää uusi toimintatapamalli mobiiliforensiikkaan.	Ehdotettiin uutta mallia mobiililaitteiden tutkintaan, joka ottaa huomioon nykyajan haasteet, kuten laitesalauksen.
Holt, T. J., Clevenger, S. & Navarro, J. Yhdysvallat: 2020.	Exploring digital evidence recognition among officers and troopers in a sample of a state police force	Tutkia kuinka hyvin poliisiviranomaiset tunnistavat digitaalisia todisteita rikospaikoilla.	Vastaajat, joilla oli viimeaikaisinta kokemusta ja koulutusta digitaalisista todisteista rikospaikoilla, havaitsivat todennäköisemmin laitteita, jotka voivat sisältää digitaalista todistusaineistoa.
Horsman, G. Yhdistynyt kuningaskunta: 2022.	Conducting a 'manual examination' of a device as part of a digital investigation	Tutkia laitteiden manuaalisen läpikäynnin etuja ja rajoituksia sekä luoda viitekehys manuaaliseen tarkasteluun.	Ehdotettiin uutta viitekehystä laitteiden manuaaliseen tarkastusmenettelyyn, joka ottaa huomioon sen tarpeellisuuden nykyajan laitteissa.
Latzo, T., Palutke, R. & Freiling, F. Saksa: 2019.	A universal taxonomy and survey of forensic memory acquisition techniques	Tutkia ja luoda yhteenvetoa eri tekniikoista keskusmuistin jäljentämiseen.	Tutkimus paljasti, että mitä alemmalta kerrokselta keskusmuisti saadaan jäljennettyä, sitä eheämpi se on alkuperäiseen verrattuna. Tutkimuksessa todetaan kuitenkin, että mitä korkeamman käyttöoikeuden muistin hankinta vaatii, sitä vaikeampaa se on.
Lone, A. H. & Naaz, R. Intia: 2019.	Forensic-chain-Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer	Tutkia ja kehittää lohkoketjutekniikan käyttöä digitaalisen todistusaineiston eheyden ja alkuperäisyyden varmistamiseksi.	Ehdotettiin Forensic-chain lohkoketjumallia, joka säilyttää digitaalisen todistusaineiston hallintaketjun koskemattomana.

Meffert, C. S., Baggili, I. & Breitinger, F. Yhdysvallat: 2016	Deleting collected digital evidence by exploiting a widely adopted hardware write blocker	Tutkia Tableau TD3 -laitteen luotettavuutta digitaalisen forensiikan tutkimuksissa.	Laitteen suojaus saatiin murrettua ja osoitettiin teoriassa ja käytännössä, miten sen luotettavuus voidaan vaarantaa kyberhyökkäyksellä.
Mothi, D., Janicke, H. & Wagner, I. Yhdistynyt kuningaskunta: 2020.	A novel principle to validate digital forensic models	Tutkia ja kehittää viitekehys digitaalisen todistusaineiston mallien validoimiseen, joka ottaa huomioon mahdolliset anti-forensiset prosessit.	Ehdotettiin matemaattiseen kaavaan perustuvaa ratkaisua olemassa olevien digitaalisen forensiikan mallien validoimiseksi.
Rogers, C. Kanada: 2015.	Authenticity of Digital Records- A Survey of Professional Practice	Tutkia tietoammattilaisten käytäntöjä digitaalisten tietueiden alkuperäisyyden arvioimiseksi ja suojaamiseksi.	Tutkimus osoitti, että tietoammattilaiset luottavat edelleen perinteisiin menetelmiin, vaikka he väittävät luottavansa enemmän teknisiin ratkaisuihin, jos aineiston alkuperäisyyden todistamista vaaditaan.
Schramp, R. Alankomaat: 2017.	Live transportation and RAM acquisition proficiency test	Verrata eri forensiikkalaboratorioiden menettelytapoja keskusmuistin jäljentämiseen.	Tutkimuksessa tehty testi ei ollut tarkoitus olla vaativa, mutta vain kolmasosa onnistui jäljentämään laitteen keskusmuistin. Tärkeimpänä ehdotuksena on hankkia vastaava testilaite ennen operaation suorittamista.
Shafiee Hasanabadi, S., Habibi Lashkari, A. & Ghorbani, A. A. Kanada: 2020.	A survey and research challenges of anti-forensics- Evaluation of game-theoretic models in simulation of forensic agents' behaviour	Kartoittaa aiempia tutkimuksia anti-forensiikasta ja muodostaa taksonomia sen vaikutuksista digitaalisen forensiikan prosessiin.	Ehdotettiin peliteoreettista lähestymistapaa, joka arvioi anti-forensiikan vaikutuksia osana digitaalisen forensiikan prosessia.
Stüttgen, J. & Cohen, M. Saksa & Sveitsi: 2013.	Anti-forensic resilient memory acquisition	Testata eri anti-forensisia tekniikoita ja niiden vaikutuksia muistin taltiointiin käytettäviä työkaluja vastaan.	Työkalujen käyttöä ja tuloksia voidaan manipuloida anti-forensiikalla. Avoimeen lähdekoodiin perustuvia työkaluja voidaan kuitenkin räätälöidä sellaisiksi, että anti-forensiset prosessit eivät pysty tunnistamaan niitä.
Tian, Z., Li, M., Qiu, M., Sun, Y. & Su, S. Kiina & Yhdysvallat: 2019.	Block-DEF- A secure digital evidence framework using blockchain	Tutkia ja kehittää lohkoketjutekniikan käyttöä digitaalisen todistusaineiston eheyden ja alkuperäisyyden varmistamiseksi	Ehdotettiin Block-DEF lohkoketjumallia, joka säilyttää digitaalisen todistusaineiston hallintaketjun koskemattomana.

Aineiston teemoittelu

Tekijät	Sitaatti	Selite	Teema
Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A. & Saeed, F. Malesia & Jemen: 2017.	”The common phases of mobile forensics include Preservation, Acquisition, Examination and Analysis and Reporting. National Insitute of Standards and Technology (NIST) also recommends these phases. Preservation is a process of securely maintaining custody of property without altering or changing the content of data that reside on devices and removable media.”	Mobiiliforensiikan haltuunottovaiheessa on tarkoitus suojata laitteiden tietosisältöä muutoksilta.	Haltuunotto
Bulbul, H.I., Güçlü Yavuzcan, H. & Ozel, M. Turkki: 2013.	”Digital evidence, stored on the computers and electronic devices, is fragile and sensitive to extreme temperatures, humidity, physical shock, static electricity, and magnetic fields. In order to avoid such disadvantages crime scene examiner should take precautions when documenting, photographing, packaging, transporting, and storing digital evidence to avoid altering, damaging, or destroying the data.”	Digitaalinen todistusaineisto on altis muutoksille, joka tulee ottaa huomioon sen käsittelyssä.	Haltuunotto, Prosessiin vaikuttavat tekijät
Fukami, A., Stoykova, R. & Geradts, Z. Alankomaat & Norja: 2021.	”As mobile devices become essential tools for daily life, security and privacy concerns grow, and modern smartphone vendors have implemented multiple types of security protection measures - such as encryption - to guard against unauthorized access to the data on their products.”	Lisääntynyt huolestuneisuus turvallisuudesta ja yksityisyydestä on saanut mobiilivalmistajat kehittämään laitteiden turvamekanismeja.	Prosessiin vaikuttavat tekijät
Holt, T. J., Clevenger, S. & Navarro, J. Yhdysvallat: 2020.	”Since line officers are the first responders at most crime scenes, they should theoretically be able to identify and secure all appropriate forms of digital and physical evidence while awaiting specialized investigators.”	Ensivasteena toimivan henkilöstön tulisi osata tunnistaa ja ottaa haltuun digitaalinen todistusaineisto.	Haltuunotto
Horsman, G. Yhdistynyt kuningaskunta: 2022.	”In addition to the traditional digital forensic examination workflow, in some cases first responders/investigators have the option to ’manually examine’ a device live, in order to quickly identify and evaluate any valuable content it may contain.”	Laitteiden manuaalisen tarkastelun hyödyntäminen osana digitaalisen todistusaineiston tunnistamista ja haltuunottoa.	Haltuunotto
Latzo, T., Palutke, R. & Freiling, F. Saksa: 2019.	"The increased use of encryption and remote storage techniques impedes the recovery of digital evidence. In such cases it is necessary to perform live memory acquisition and analysis in order to retrieve cryptographic keys or track the location of network storage areas”	Salausten ja ulkoisten tallennustilojen lisääntynyt käyttö lisää tarvetta jäljentää käynnissä olevan laitteen muisti.	Katoavan datan taltiointi

Lone, A. H. & Naaz, R. Intia: 2019.	”Digital evidence plays an important role in cybercrime investigation, as it is used to link individuals with criminal activities. Thus it is utmost importance to guarantee integrity, authenticity, and auditability of digital evidence as it moves along different levels of hierarchy in the chain of custody during cybercrime investigation.”	Digitaalisen todistusaineiston tärkeä rooli rikostutkinnassa kasvattaa tarvetta sen eheyden ja alkuperäisyyden varmistamisessa.	Alkuperäisyys ja eheys
Meffert, C. S., Baggili, I. & Breitinger, F. Yhdysvallat: 2016	”The issue with depending on tools is that while they are helpful in expediting the forensics process, they are not immune to attacks. One thing to consider is how tools commonly used in digital forensics may be exploited using anti-forensics, which is why tool testing is of paramount importance to the digital forensics community.”	Ala on hyvin työkaluriippuvainen ja niiden testaus on tärkeää, sillä työkaluja vastaan voidaan hyökätä anti-forensiikalla.	Prosessiin vaikuttavat tekijät
Mothi, D., Janicke, H. & Wagner, I. Yhdistynyt kuningaskunta: 2020.	”One of the challenges of digital forensics is anti-forensics. Anti-Forensics has the ability to delay the investigation or to prevent the investigation from taking place by deleting evidence. This poses a threat to the investigation process if proper measures are not taken.”	Digitaalisen forensiikan haasteena on anti-forensiikka, joka tulee ottaa huomioon prosessissa.	Prosessiin vaikuttavat tekijät
Rogers, C. Kanada: 2015.	”Authenticity of digital material is an enduring concern. However, while most people intuitively understand what authenticity is, few are able to identify exactly what is required to ensure, assess, and guarantee it.”	Digitaalisen materiaalin alkuperäisyys on pysyvä huolenaihe, sillä kaikki eivät tunnista mitä sen varmistamiseen vaaditaan.	Alkuperäisyys ja eheys
Schramp, R. Alankomaat: 2017.	”The content of Random Access Memory (RAM) of a computer contains forensically relevant information, most notably encryption keys. However, actually acquiring it can be challenging.”	Keskusmuisti sisältää oleellista tietoa, mutta sen taltiointi voi olla haastavaa.	Katoavan datan taltiointi
Shafiee Hasanabadi, S., Habibi Lashkari, A. & Ghorbani, A. A. Kanada: 2020.	Digital forensic investigators’ aim is identifying, collecting and presenting reliable, accurate, and admissible evidence in court. However, anti-forensics manipulate, obfuscate, hide, and remove the remaining piece of evidence in a compromised system.	Digitaalisen forensiikan tutkijan tarkoitus on tuoda esille luotettavaa todistusaineistoa, jota anti-forensiset prosessit pyrkivät vaarantamaan.	Prosessiin vaikuttavat tekijät
Stüttgen, J. & Cohen, M. Saksa & Sveitsi: 2013.	”The process of memory acquisition presents unique evidentiary challenges since many acquisition techniques require code to be run on a potential compromised system, presenting an avenue for anti-forensic subversion.”	Keskusmuistin taltiointi vaatii usein koodin ajamista kohdelaitteessa, joka altistaa sen anti-forensisille prosesseille.	Katoavan datan taltiointi, Prosessiin vaikuttavat tekijät

Tian, Z., Li, M., Qiu, M., Sun, Y. & Su, S. **Kiina & Yhdysvallat: 2019.**	"The analytical and experimental results show that Block-DEF is a scalable framework, it guarantees the integrity and validity of evidence, and balances privacy and traceability well.”	Lohkoketjuun perustuvalla viitekehyksellä on mahdollista varmistaa todistusaineiston oikeellisuus ja eheys.	Alkuperäisyys ja eheys