

Sisekaitseakadeemia
Politsei- ja piirivalvekolledž

Martin-Erik Ilus

**DIGITAALSETE TÕENDITE VISUAALNE
ESITLEMINE SÜÜTEOMENETLUSES**

Lõputöö

Juhendaja:

Anna Illamaa, MA

Kaasjuhendaja:

Gea Ling

Tallinn 2023

SISEKAITSEAKADEEMIA LÕPUTÖÖ ANNOTATSIOON

Politsei- ja piirivalvekolledž	Juuni 2023
<p>Töö pealkiri eesti keeles: „Digitaalsete tõendite visuaalne esitlemine süüteomenetluses“</p> <p>Töö pealkiri võõrkeeles: „Visualization of Digital Evidence in Offence Proceedings“</p> <p><i>Lühikokkuvõte:</i> Lõputöös uuritakse digitaalsete tõendite visualiseerimist süüteomenetluses. Töö maht on 50 lehekülge ning lõputöö koostamisel on kasutatud 52 allikat.</p> <p>Lõputöö eesmärgiks on leida peamised kitsaskohad digitaalsete tõendite visuaalsel esitlemisel süüteomenetluses ning pakkuda nendele probleemidele lahendusi.</p> <p>Lõputöö uurimisprobleemiks on küsimus, kuidas parandada digitaalsete tõendite visuaalset esitlemist süüteomenetluses? Lõputöös kasutati andmekogumismetodina poolstruktureeritud intervjuud. Kokku intervjueeriti 13 inimest, viis prokurööri, neli kohtunikku ja neli Politsei- ja Piirivalveameti ametnikku.</p> <p>Lõputöö teoreetilises osas antakse ülevaade digikriminalistikast, digitaalse tõendi olemusest, infotehnoloogilistest vahenditest ja andmekandjatest, digitaalsete tõendite visuaalsest esitlemisest ja sellega seotud probleemidest.</p> <p>Lõputöö uurimuslikus osas tuuakse välja võimalikud lahendused digitaalsete tõendite visuaalse esitlemise parandamiseks süüteomenetluses. Näiteks, uuema ja parema tarkvara kasutusele võtmine ja koolituste läbiviimine digitaalsete tõendite visualiseerimise teemal. Lõputöös teeb autor järeldusi ning ettepanekuid, digitaalsete tõendite visuaalse esitlemise parandamiseks süüteomenetluses.</p>	
Lisad:	
Võtmesõnad: Digitaalsed tõendid, visualiseerimine	
Võõrkeelsed võtmesõnad: Digital evidence, visualization	
Säilitamise koht:	
<p>Töö autor: Martin-Erik Ilus</p> <p>Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalistest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud.</p> <p>Annan Sisekaitseakadeemiale tasuta loa (lihtlitsentsi) minu loodud teose reprodutseerimiseks säilitamise ja elektroonilise avaldamise eesmärgil, sealhulgas Sisekaitseakadeemia raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni. Annan loa teose üldsusele kättesaadavaks tegemiseks Sisekaitseakadeemia veebikeskkonna kaudu sealhulgas Sisekaitseakadeemia raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.</p> <p>Olen teadlik, et nimetatud õigused jäävad alles ka autorile. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.</p>	
Allkiri: /digitaalselt allkirjastatud/	Kommentaar
Vastab lõputöö nõuetele Juhendaja: Anna Illamaa	Allkiri: /digitaalselt allkirjastatud/
Vastab lõputöö nõuetele Kaasjuhendaja: Gea Ling	Allkiri: /digitaalselt allkirjastatud
Kaitsemisele lubatud	
Kolledži direktor / instituudi juhataja: Allkiri:	

SISUKORD

MÕISTETE JA LÜHENDITE SELGITUSED.....	4
SISSEJUHATUS.....	6
1. TEOREETILISED LÄHTEKOHAD.....	9
1.1 Digikriminalistika.....	9
1.2 Digitaalne tõend.....	10
1.3 Infotehnoloogilised vahendid ja andmekandjad.....	12
1.4 Digitaalsete tõendite visuaalne esitlemine.....	13
1.5 Digitaalsete tõendite visuaalse esitlemisega seotud probleemid.....	17
2. EMPIIRILINE OSA.....	19
2.1 Uuringu meetodika, protsess ja valim.....	19
2.2 Intervjuu tulemused.....	23
2.3 Järeldused ja ettepanekud.....	35
KOKKUVÕTE.....	40
SUMMARY.....	42
VIIDATUD ALLIKATE LOETELU.....	44
LISA 1. INTERVJUU KÜSIMUSED.....	50

MÕISTETE JA LÜHENDITE SELGITUSED

Bait – *byte* on mälumahu mõõtühik, mis vastab ühele märgile. (Vallaste, 2023);

Bitt – digitaalse informatsiooni väikseim ühik, mis võib omada ainult üht kahest võimalikust väärtusest (0 või 1). (Vallaste, 2023);

Digitaalne tõend - antud töö kontekstis peetakse digitaalseks tõendiks olulise väärtusega informatsiooni ja andmeid süüteomenetluse jaoks, mida talletatakse, saadakse või edastatakse elektroonilise seadmega;

Digikriminalist – antud töö kontekstis peetakse digikriminalistiks isikut, kes omab eriteadmisi IT ja digikriminalistika valdkonnas ja kelle põhiülesanded on elektrooniliste andmete töötlemine, analüüsimine ja dokumenteerimine süüteomenetluses;

KrMS - Kriminaalmenetluse seadustik;

Kroonikohus/ Magistraadikohus - kohtud Inglismaal ja Walesis, mis arutavad kõrgemaid esimese astme kriminaalasju (European e-Justice, 2016);

Logifail - arvuti tegevuse päevik, mida kasutatakse nii statistilistel eesmärkidel kui ka varundamise ja taaste jaoks (Vallaste, 2023);

Manussüsteem – *embedded system* on arvutisüsteemi muu süsteemi (auto, lennuki, digikaamera, mobiiltelefoni, maksekaardisüsteemi) lahutamatu funktsionaalne osa. Kogu tarkvara salvestatakse alatiseks püsimälule. (Vallaste, 2023);

Meta-andmed - andmete digitaalne kirjeldus, mis vastab täpselt defineeritud mallile või ka selliste kirjelduste kogumik (Vallaste, 2023);

MMS – *Multimedia Messaging Service* (multimeedium-sõnumiteenus). Täiustatud lühisõnumiteenus, mis võimaldab mobiiltelefonide vahel edastada graafikat, videoklippe ja helifaile. (Vallaste, 2023);

PPA – Politsei- ja Piirivalveamet;

SMS – *Short Message Service* (lühisõnumiteenus), mis kujutab endast kahepoolset lühikeste tekstisõnumite vahetamist mobiiltelefonide vahel. (Vallaste, 2023);

Traadita võrk – *wireless network* on võrk, milles edastatakse andmeid klientide ja serverite ning muude võrguseadmete vahel ilma, et kasutatakse füüsilist kaablit või juhet. (Vallaste, 2023);

Visuaalne esitlemine/ Visualiseerimine – antud töö kontekstis peetakse visualiseerimist ja visuaalset esitlemist meetodiks, millega on võimalik esitada erinevaid andmeid ja teavet.

SISSEJUHATUS

Tänapäeval, kus tehnoloogia ja digitaalne maailm areneb väga kiiresti, on digitaalsed tõendid saanud lahutamatuks osaks menetluspraktikast. Vähemalt 85% süüteo menetlustest on sellised, kus kasutatakse digitaalseid tõendeid (Euroopa Komisjon, 2019, p.1). Digitaalseteks tõenditeks loetakse mistahes digitaalses vormis esinevat teavet, mida on võimalik kasutada kohtus tõendamiseseme asjaolude selgitamisel. Digitaalse tõendi kõige lihtsamaks näiteks võib lugeda andmeid, mis on saadud digitaalsest seadmest, fotosid või kirjavahetust. Peale nende on olemas teist tüüpi andmeid, näiteks ajatemplid ja asukohad (nn meta-andmed), mida eriteadmistega ametnikud peavad tuvastama digitaalsete andmete vaatlemise käigus. Komplitseeritud digitaalsete tõendite mõistmiseks esitatakse neid eriteadmistega ametnike poolt visuaalselt, millega kaasnevad erinevad aktuaalsed probleemid, näiteks esitatavate andmete usaldusväärsus süüteo menetluses ning andmete mõistmise keerukus.

Eriteadmistega ametnikul tuleb leida selline digitaalsete tõendite esitlemise viis, et kõik menetluse osapooled mõistaksid neid üheselt. Kuna digitaalseid tõendeid on erinevaid, on keeruline leida visualiseerimise meetodit, mis selgitaks konkreetset tõendit kõige täpsemalt ja aitaks kaasa juhtumi lahendamisele.

Lõputöö teema **aktuaalsust** toetavad erinevad arengukavad, mis kinnitavad, et ka sisejulgeolekus liigutakse aina enam digitaliseerumise poole. Siseministeeriumi 2016 aasta aruandes „Siseturvalisuse arengukava 2015–2020“ on välja toodud, et 2015 aastaks valmisid Politsei- ja Piirivalveametil erinevad kavad, mis olid seotud küberkuritegude lahendamise tõhustamisega ja digitaalsete tõenditega, mille jaoks koostati ka vastav tegevusplaan (Siseministeerium, 2016, lk 8). Siseministeeriumi „Siseturvalisuse arengukava 2015-2020“ mainib, et üheks oodatavaks arengusuunaks on vajalike digitaalsete tõendite säilitamine ning küberkriminalistika võimekuse väljaarendamine (Siseministeerium, 2015, lk 86). Seda kõike toetab 01.04.2021 heaks kiidetud eelnõu, mille kohaselt muutus kriminaalmenetlus täielikult digitaalseks, andes sellega paindlikumad võimalused menetluse läbiviimiseks (Justiitsministeerium, 2021). Mainimata ei saa jätta ka valitsuse poolt heaks kiidetud eelnõud, mis näeb ette

ülemineku paberivabale menetlusele tsiviil- ja haldusajades (Justiitsministeerium, 2022).

Siseministeeriumi värskem „Siseturvalisuse arengukava 2020-2030“ sätestab, et nii digitaalsetes kui ka infoajastu keskkondades on vaja võtta kasutusele uudseid lähenemisi (Siseministeerium, 2021, lk 39). Meie menetlussüsteemi muudetakse aina digitaalsemaks, kuid sellest vähem tähtis ei saa olla digitaalsete tõendite mõistmine ja visuaalne esitlemine.

Lõputöö teema on **uudne**, sest digitaalne maailm on kiiresti arenev ja pidevas muutumises. Käesolev töö käsitleb digitaalsete tõendite visualiseerimisega seotud probleemi, mida süvitsi varem uuritud ei ole. Eelnevalt on seda teemat ligilähedaselt käsitlenud Palm (2013, lk 4-5), kelle töös on keskendutud ametnike võimekusele koguda digitaalseid tõendeid ning neid korrektselt talletada. Kaasa arvatud Luuk'i (2017, lk 7) magistritöö „Digitaalsete tõendite kasutamise erisused“, kus autor uuris digitaalseid tõendeid, nende erinevaid aspekte ning milline seos on digitaalsetel tõenditel kohtumenetlusega. Ülalpool mainitud tööd on käsitlenud digitaalsete tõendite kogumist, talletamist ja nende üleüldist olemust. Antud lõputöös keskendutakse digitaalsete tõendite mõistetavusele, mis looks olulist väärtust süüteomenetluse tõhusamaks toimimiseks.

Eelnevalt kirjutatu põhjal püstitatakse järgnev **uurimisprobleem**: Kuidas parandada digitaalsete tõendite visuaalset esitlemist süüteomenetluses? Uurimisprobleemi lahendamiseks püstitatakse järgnevad **uurimisküsimused**:

1. Kuidas toimub hetkel süüteomenetluses digitaalsete tõendite visualiseerimine?
2. Milliseid digitaalseid tõendeid visualiseeritakse Eestis kõige rohkem?
3. Millised on peamised probleemid digitaalsete tõendite visuaalsel esitlemisel?
4. Kuidas saaks parandada digitaalsete tõendite visualiseerimise protsessi?

Lõputöö **eesmärgiks** on leida peamised kitsaskohad digitaalsete tõendite visuaalsel esitlemisel süüteomenetluses ning pakkuda nendele probleemidele lahendusi.

Eesmärgi täitmiseks püstitatakse 3 **uurimisülesannet**:

1. Anda teoreetiliste allikate põhjal ülevaade digitaalsete tõendite visualiseerimisega seotud teemadest.
2. Analüüsida intervjueeritavate vastuseid ning arvamusi sellest, mida nähakse kitsaskohtadena digitaalsete tõendite visualiseerimisel süüteomenetluses.
3. Analüüsida intervjuusid ja teooriat ning esitada järeldused ja lahendused.

Lõputöö eesmärgi täitmiseks viiakse läbi kvalitatiivne empiiriline uuring. Hirsjärvi, et al. (2007, lk 155) on välja toonud, et inimest eelistatakse rohkem teadmiste kogumisel, kuna inimene on võimeline kohanema muutuvate olukordadega ning sellise uuringuga on uuritaval võimalik väljendada oma seisukohti ja arvamust. Ühtlasi võimaldab sellise uuringu läbiviimine kasutada induktiivset analüüsi, mis võimaldab teha järeldusi või luua uusi teooriaid. (2007, lk 155)

Valimiks on eesmärgipärane valim (Õunapuu, 2012). Intervjueeritavateks on valitud isikud, kes on kokku puutunud digitaalsete tõenditega ning nende visualiseerimisega. Isikuid valitakse kolmest ametkonnast, milleks on prokuratuur, kohus ja Politsei- ja Piirivalveamet (edaspidi PPA). Valimi suuruseks on 15 isikut. Andmete kogumise meetodina kasutatakse poolstruktureeritud intervjuud (Laherand, 2008, lk 181).

Lõputöö koosneb kahest peatükist. Esimeses peatükis antakse teoreetiline ülevaade digitaalsetest tõenditest ning nende visualiseerimisest. Teises peatükis tutvustatakse empiirilise osa metoodikat ja analüüsitakse läbiviidud intervjuusid ning tehakse lõputöö kohta järeldused.

1. TEOREETILISED LÄHTEKOHAD

1.1 Digikriminalistika

Digikriminalistika on üks kohtuekspertiisi harudest, mis mängib ühiskonnas olulist rolli, tulenevalt erinevate digitaalsete seadmete levimusest (Harshita, Amarnath, 2021, p. 97). Vincze (2016, p. 184) toob välja, et digikriminalistikat saab defineerida kui teaduslikult tuletatud materjalide ja tõestatud meetodite kasutamist, digitaalsetest allikatest pärinevate digitaalsete tõendite säilitamiseks, kogumiseks, valideerimiseks, tuvastamiseks, analüüsimiseks, tõlgendamiseks, dokumenteerimiseks ja esitamiseks. Digikriminalistika eesmärk on süütegusid omavahel seostada või rekonstrueerida ja ennendada tegevusi, mis võiks menetlustoimingute läbiviimist häirida (Vincze, 2016, p. 184).

Süütegude toimepanemisel jääb maha erinevaid jälgi, nagu näiteks sõrmejäljed, DNA ja jalatsijäljed, mida kriminalistidel on võimalik uurida ja analüüsida. Sama kehtib ka mistahes digitaalse tegevuse puhul digitaalsetes seadmetes, mis jätavad endast maha digitaalseid jälgi digikriminalistidele uurimiseks. Iseäranis küberkuritegude puhul on digitaalsete tõendite hankimine eriti oluline ning peab olema tagatud nende korrektne käitlemine, et tõendid oleksid kohtus lubatavad (Harshita, Amarnath, 2021, p. 97).

Digikriminalistid kasutavad erinevaid tarkvarasid, seadmetel olevate andmete hõivamiseks. Näiteks *EnCase Forensic Imager tool*, mille abil saavad digikriminalistid hõivata andmeid väga paljudelt erinevatelt nutiseadmetelt nagu näiteks nutitelefonid või tahvelarvutid. Antud tarkvara annab kriminalistidele kõikide seadmel olevate andmete koopiafaili, tagades seadme rikkumatus. Saadud koopiafailidest on võimalik teha raportfail, mida saab edastada erinevatele menetlust juhtivatele osapooltele (Harshita, Amarnath, 2021, p. 99).

Digikriminalistid kasutavad ka tarkvara *Cellebrite*. Raportfailide lugemiseks mõeldud *Cellebrite Reader* pakub arenenud otsingumootorit, filtreid, ajatelge ja järjehoidjad, mis võimaldab andmeid põhjalikult analüüsida ja märkida nendest olulisemaid. Sõltuvalt sellest, mis teave on menetluse jaoks vajalik, saab vaatluse käigus valikuliselt

uurida seadmel olevaid andmeid ning need üheks aruandeks vormistada. Töötades raportfailiga, on võimalik edastada teavet ühe dokumendina, vähendades riski, et andmed võivad kaduda (Data Expert, 2023).

Digikriminalistika tarkvaradega on võimalik digitaalseid seadmeid, mis on lukus või ligipääsematud, muuta ligipääsetavaks, kasutada nn väljatõmbamise meetodit. Väljatõmbamise meetod tagab ka digitaalselt seadmelt kustutatud andmete taastamise ja hõivamise. Lisaks saab selle meetodiga eraldada andmeid e-mailidest, failidest, tekstifailidest, fotodest jne (Harshita, Amarnath, 2021, p. 98).

Kokkuvõtvalt saab öelda, et tänu digiseadmete arengule on hakanud olulist rolli mängima ka digikriminalistide töö. Olles üheks kohtuekspertiisi haruks, on digikriminalistidel kasutusel erinevad tarkvarad, millega saadakse menetluse jaoks vastuseid tõendamiseseme asjaoludele. Igale digitaalsele seadmele on olemas vastav tarkvara ning nendega on võimalik pääseda ligi nii lukustatud kui ka kustutatud andmetele. Kuna digitaalsed tõendid on muudetavad, siis on võimalik tervet protsessi teostada selliselt, et originaalandmed jäävad rikkumata ning neid on võimalik hiljem uuesti taasesitada. Samuti ei pruugi süütegu aset leida füüsilises maailmas, vaid digitaalses maailmas ning selle jaoks ongi vaja digikriminaliste, kes sealseid jälgi oskaksid leida ja esile tuua.

1.2 Digitaalne tõend

Mukasey, *et al.* (2012, p. ix) toovad välja, et digitaalsed tõendid on olulise väärtusega informatsioon ja andmed süüteomenetluse jaoks, mida talletatakse, saadakse või edastatakse elektroonilise seadmega. Samuti on Lewulis (2021, p. 2) kirjutanud, et digitaalsed tõendid sisaldavad mistahes tõendusväärtusega teavet, mis on talletatud või edastatud digitaalsete andmetena. See tähendab, et digitaalseid tõendeid võib leida e-maili kontodelt, sõnumivahetusest läbi teenusepakkuja, pankade rakendustest või meediaplattformidelt nagu „Facebook“ (Allen, *et.al.*, 2018, p. 22). Sarnaselt

sõrmejälgedele ja DNA-le on digitaalsed tõendid varjatud. Lisaks sellele on võimalik neid kiiresti muuta, kahjustada või hävitada (Mukasey, *et.al.*, 2012, p ix).

Baastasandil on digitaalsed andmed salvestatud andmekandjale väga väikeste üksuste jadana, mille väärtuseks on 0 või 1. Andmekandjal tähistavad 0 või 1 mikroskoopilist füüsilist seisundit, tavaliselt on selleks elektrilaengu tase. Iga üksik ühik on bitt ning kaheksast bitist koosnevaid rühmi nimetatakse baitideks. Iga bait tähistab kuueteistkümnend väärtust, mis omakorda tekitab rühma, mis suudab moodustada numbreid, tähti, sõnu ja kõiki muid arvutitesse ja nendega seotud seadmetesse salvestatud teabe ilminguid. Seega koosnevad kõik digitaalsed tõendid nullide ja ühtede jadadest, mida saab näha ja tõlgendada, ainult eritarkvaraga, mida oskavad tuvastada digikriminalistid (Vincze, 2016, p. 185).

Justiitsministeeriumi kriminaalmenetlusõiguse revisjoni tulemustest selgub, et kriminaalmenetluses digitaalsete tõendite kogumine on kasvujärgus, kuid pole spetsiifiliselt sätestatud selliste tõendite kogumise põhimõtteid. Sellest tulenevalt lähtutakse tavaliste tõendite uurimise ja kogumise regulatsioonidest (Justiitsministeerium, 2015, lk 9). Kriminaalmenetluse seadustiku (edaspidi KrMS) § 63 sätestab tõendite liigid. Tõendiks saab nimetada kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlust, ekspertiisiakti, eksperdi antud ütlust ekspertiisiakti selgitamisel, asitõendit, uurimistoimingut, kohtuistungit ja jälitustoimingu protokollit või videosalvestist, lisaks sellele ka muud dokumenti ning fotot, filmi või muud teabetalletust (Kriminaalmenetluse seadustik, 2012).

Digitaalsete tõendite usaldusväärsuse kohta on mitmeid arvamusi. Arvatakse, et digitaalse tõendi täpsus ja objektiivsus muudavad tõendi usaldusväärsemaks. Samas leitakse, et vähene võimekus kontrollida tõendi autentsust muudab selle nõrgemaks ja läbi selle vähem usaldusväärsemaks kui tavalise tõendi (Fredesvinda, 2007, p. 286).

Eestis ei ole digitaalne tõend eraldiseisva tõendi liigina õiguslikul tasandil defineeritud, kuid ta loetakse kaetuks KrMS § 63 sätestatuga, mis näitab, millises formaadis peab olema süüteos tuvastatud teave selleks, et seda saaks käsitleda tõendina. Oma olemuselt on digitaalne teave siiski 0-ide ja 1-tede jada, mis moodustab tervikuna erinevaid andmeid. Nende andmete fikseerimisel digikriminalisti poolt, käsitletakse neid kui

digitaalset tõendit. Digitaalsed tõendid on andmed, mis võivad tekkida meilivahetuse, helistamise või meediaplatvormi kasutamise käigus. Nende andmete väljatoomiseks kasutatakse erinevaid tarkvarasid, mis võimaldavad väga täpselt näidata andmete sisu ning vältida olukorda, kus küsimuse alla seatakse tõendi autentsus ja kontrollitavus.

1.3 Infotehnoloogilised vahendid ja andmekandjad

Oliver Olt, *et al.* (2013, lk 387) leiab, et tänapäeval kasutatakse aina rohkem igapäevases elus erinevaid infotehnoloogilisi vahendeid. Kuni 90ndate alguseni olid infotehnoloogilised vahendid vähe kasutusel tsiviilisikutel, selliseid vahendeid võis leida antud valdkonnale spetsialiseerunud või asjaarmastajate kodudest. Tänapäeval võib leida neid vahendeid peaaegu iga inimese taskust. Praegusel infoajastul võib suureks abiks olla ohvri või kurjategija valduses olnud infotehnoloogilisest vahendist, kust võib leida olulisi viiteid ja juhiseid süüteo tõendamiseks (Olt, *et al.*, 2013, lk 387).

Infotehnoloogiline vahend võib olla arvuti, mobiiltelefon, fotoaparaat, videokaamera, diktofon, MP3-pleier, GPS ehk positsioneerimisseade jms. Andmekandjad võivad olla kõvakettad, mälupulgad, mälukaardid, laserplaadid, magnetoptilised kettad ja varunduslindid. (Lanno, *et al.*, 2013, lk 387)

Arvutisüsteem infotehnoloogilise vahendina, võib koosneda andmekandjast, klaviatuurist ning monitorist. Arvutisüsteemid oma suureneva salvestusruumiga on olulised digitaalsete tõendite allikad. Arvutisüsteemis olevad andmed võivad sisaldada süüstavaid, mittesüüstavaid tõendeid ja nendega seotud omadusi, mis on uurimisel olulised: näiteks failide loomise aeg, nende tõenäoline looja, faili loomise asukoht (Casey, 2011, p. 7).

Ka asjade internet ja nutiseadmed võivad olla digitaalsete tõendite allikaks. Näiteks nutiseadmed edastavad sõnumeid ja e-kirju üle maailma. Olulist rolli võib mängida sõnumi saatja, saatmise aeg, sõnumi sisu. Nende kontrollimiseks võib osutada vajalikuks logifailide vahepealne kontrollimine serveritest ja ruuteritest, mis antud sõnumit käsitlesid. Mõned süsteemid saab konfigurereida selliselt, et need

jäädvustaksid seadmel kogu digitaalset tegevust. See võimaldab juurdepääsu kogu suhtlusele, sõnumitekstidele, telefonivestlustele ja manustele (Casey, 2011, p. 8).

Manussüsteemideks on navigatsioonisüsteemid, nutiseadmed, kiipkaardid ja teised süsteemid, mis on sünkroniseeritud arvutitega, milles võib olla digitaalseid tõendeid. Nutiseadmed võivad sisaldada suhtlusandmeid, fotosid ja videoid ning muid andmeid. Navigatsioonisüsteemide abil saab kindlaks teha sõiduki liikumisteedkonna ja tema asukoha. Paljude sõidukite andur- ja diagnostikamoodulid sisaldavad andmeid, mis võivad olla kasulikud liiklusõnnetuste põhjuste mõistmiseks. Andmed võivad kajastada sõiduki kiirust, piduri- või gaasipedaali asendit viimase viie sekundi jooksul enne kokkupõrget (Casey, 2011, p. 8).

Mõned kodumasinad võimaldavad ka kasutajatel neid programmeerida distantsilt läbi interneti. Kaasaegsetes mikrolaineahjudes võivad olla sisemised arvutid, millega on võimalik läbi interneti teavet alla laadida. Näiteks süütamise uurimisel võivad mikrolaineahjud sisaldada andmeid, mis võivad näidata, et tulekahju esile kutsumiseks oli mikrolaineahi programmeeritud konkreetsel ajal aktiveeruma (Casey, 2011, p. 8).

Tuginedes eelnevale võib öelda, et digitaalseid tõendeid on võimalik leida meie igapäevases elus kasutusel olevatest infotehnoloogilistest vahenditest või andmekandjatest. Enamike jaoks on digitaalsete tõendite talletajaks mobiiltelefon ja arvutis olev kõvaketas, kuid ei ole välistatud ka auto või mõni kodumasin. Nendest saadud digitaalsete tõendite põhjal, on võimalik määrata isiku läbitud teekond, ning kellega võidi vestelda selles ajavahemikus. Millele kõigele aitab kaasa ka pidev tehnoloogia areng, võimaldades meil talletada rohkem infot oma infotehnoloogilistele vahenditele ning läbi selle anda digikriminalistidele rohkem infot süütegude tõendamiseks.

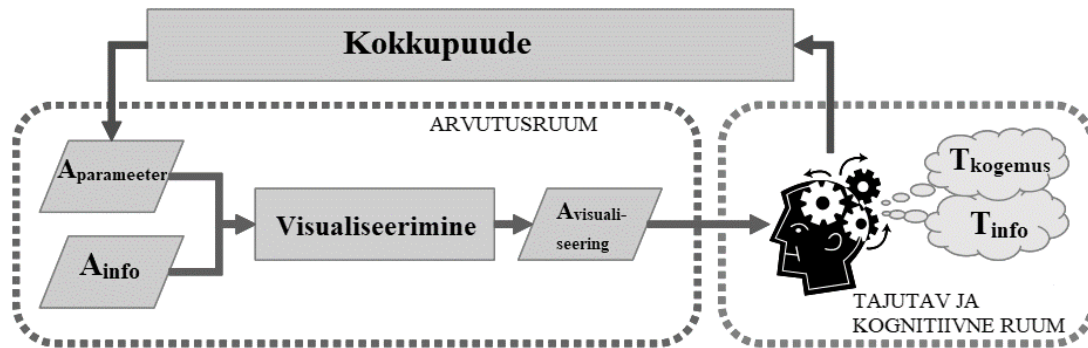
1.4 Digitaalsete tõendite visuaalne esitlemine

Kohtus hõlmab tõendite esitlemine endast ulatuslikke suulisi kirjeldusi ja uurimise käigus saadud tõendite visualiseerimist. Kogu protsess võib olla aeganõudev ja

töömahukas. Kohtusaalis kasutatavateks tõenditeks võivad olla sündmuskohaga seotud suulised ütlused, fotod või visandid sündmuskohast jne (Sheppard, *et.al.*, 2020, p.2). Digitaalseid tõendeid on hakatud rohkem kasutama, sest tarkvarad, digitaalne multimeedia sisu ja digiallkirjad on muutunud terve ühiskonna lahutamatuks osaks (Maurer, 2004, p. 933). Damian Schofield (2016, p. 3) märgib, et aina rohkem on hakatud kasutama visualiseeritud digitaalseid tõendeid suuliste kirjelduste asemel. See kõik on võimalik tänu meedia formaatides ja seadmetes toimunud arengule, mis võimaldavad kohtus tõendeid visualiseerida (Schofield, 2016, p. 3). Sarnaselt Damian Schofieldiga on Eneli Laurits (2016, p. 113) täheldanud suuremat digitaalsete tõendite kasutamist Eesti kriminaalmenetluses. Peale tema toob ka Radina Stoykova (2021, p. 1) välja, et näiteks Ühendkuningriikides on 90% kriminaalmenetlustes üheks osaks digitaalne element.

Selleks, et mõista, kuidas visualiseerimine toimub, on Chen, *et al* (2009, p.3) välja töötanud visualiseerimise protsessi joonise (vt Joonis 1). Card, *et al* (1999, p.1) tõi välja, et andmete visualiseerimine on dünaamiliste, interaktiivsete ja odavate infotehnoloogiliste lahenduste ära kasutamine, et luua uusi arvutusruumi väliseid abivahendeid, millega tõsta meie kognitiivseid võimeid.

Joonise tegemisel lähtuti Card'i poolt öeldust. Joonisel on näha „Arvutusruumi“, kus toimub kogu digitaalse info analüüs ning „Tajutavat ja kognitiivset ruumi“, kus toimub inimese mõttetegevus. Välja on toodud, kuidas inimene puutub kokku erinevate parameetritega ($A_{\text{parameeter}}$), olgu selleks programmid või muud infotehnoloogilised lahendused, et analüüsida ja visualiseerida arvutusruumis olevat infot/andmeid (A_{info}). Visualiseerimise tulemusena tekib andmetele kehtestatud parameetrite järgi kokkuvõtlik teabetalletus ($A_{\text{visualiseering}}$). Antud teabetalletus kantakse üle „Tajutavasse ja kognitiivsesse ruumi“, kus toimub saadud info (T_{info}) analüüsimine ja mõtestamine, lähtudes isiku enda kogemustest (T_{kogemus}) ja teadmistest (Chen, *et.al.*, 2009, pp. 1-4).



Joonis 1. Tüüpiline visualiseerimise protsess

Eelpool nimetatud joonis on võetud aluseks *EPIC* analüüsimise mudeli loomisel. *EPIC* on akronüüm sõnadele *Explore*, *Investigate* ja *Correlate* ehk avasta, uuri ja loo seoseid. Antud mudelil on seitse eesmärki: digitaalse tõendi nähtavaks tegemine, digitaalse tõendi mahu vähendamine, pakkuda kõrgel tasemel ülevaateid digitaalsetest tõenditest, abistada tõendis oleva teabe kaardistamist, selgitada tõendi päritolu ja tähtsust, pakkuda tuge tõendusmaterjali väärtuse tuvastamiseks ja hõlbustada järelduste esitamist teistele menetlusosalistele/kohtule. Antud meetodi autorid viisid läbi uuringu 9 digikriminalisti seas. Uuringus võrreldi tekstipõhist uurimismeetodit, mida võimaldab *EnCase* ning lihtsamat uurimismeetodit, mis hõlmab endas esitlus- ja interaktsiooni tehnikaid, et teha kindlaks, kas protsessipõhine teabe visualiseerimine pakub eeliseid kasutajapõhisele visualiseerimisele. Tulemusena leiti, et *EPIC* meetodi lähenemisviis oli teistest parem, kuid tekstipõhine uurimismeetod oli osalejate jaoks kõige tuttavam, sest varasemalt on sellega tööalaselt kokku puutunud (Thinyane, *et.al.*, 2012, pp. 1-14).

Hales, *et al* (2017, p. 4) on märkinud, et üheks info visualiseerimise pioneeriks on Šotimaalt pärit insener William Playfair, kes kasutas oma teabe visualiseerimisel graafikuid, et lugeja oskaks saadud infot hinnata ja mõista. See siiski ei tähenda seda, et suulise selgitamise asemel piisaks ainult digitaalsetest tõenditest. Bob Manlowe, *et. al.* (2006, pp. 1-2) on välja toonud, et 72 tunni vältel edastatud suulisest infost võib meelde jääda 10% ning ainult visuaalide abil 20%, kuid kui lisada suulise esitluse juurde visuaalid, suudab inimene meelde jätta 65% kogu infost. Näiteks visualiseerimise olulisuse kohta saab tuua John Snow poolt tehtud diagrammi, kus oli

visualiseeritud Londonis olevat Soho linnakaarti ning märgitud selle peale kinnitatud koolerasse haigestunute juhtumid. Selline visualiseerimine võimaldas vaadata andmeid ja teavet teise nurga alt ning tänu sellele mõisteti, et need haigusjuhtumid leidsid aset veepumba läheduses. Visualiseerimise abiga mõisteti, et koolera on vee kaudu leviv haigus (Hales, *et.al.*, 2017, p. 4).

Siiski peab mõistma, et digitaalsete tõendite esitlemisel võib isegi väikseim muudatus mõjutada, kuidas edastatud infot hinnatakse ning lõplikku arvamuseni jõutakse (Rempel, 2019, p. 1289). Sellisel juhul tuleb digitaalseid tõendeid esitledes teha kindlaks muud aspektid, mis võivad mõjutada tõendi visualiseerimist. Kontrollitud peavad olema esitluspaigas olevad seadmed ning nende ühilduvus visualiseerimise tarkvaradega ja esitlemise võimekusega (Sheppard, *et.al.*, 2020, p. 2).

Viimase kahe aastakümne jooksul on masinaga loodud tõestused hakanud üle võtma inimeste funktsiooni ja tehissintellekti (inglise keeles *Artificial Intelligence*, (edaspidi: AI)) teemat on hakatud uurima ka digitaalse kohtumenetluse vaatest. Masinaga loodud digitaalsete tõendite seaduslikkuse kohta on aga märkimisväärselt vastunäidustusi ja skeptilisus selle valdkonna suhtes on suur. Solanke (2022, p. 1) uuris kohtute, juristide ja üldsuse väljendatud skeptitsismi taset AI-l põhinevate digitaalsete tõendite kogumiste tehnikate üle ja tema uuringu põhiline eesmärk oli anda juhiseid, kuidas parandada AI-põhise digitaalse kohtuekspertiisi tõlgendatavust. Kuna AI tugineb suuresti matemaatilistele, statistilistele ja arvutusteooriatele, siis ollakse skeptilised selles, kuidas AI teatud järeldusteni jõuab ja kui seletatavad ja arusaadavad need on. Autori enda isiklik arvamus oli, et vaidluseid tehisintellekti rakenduste üle tuleks leevendada. On arutletud selle üle, kas peaks kasutama juba loodud AI algoritme, looma uued või kasutama kahe algoritmi. Uuringust tuli välja, et olenemata, millist algoritmi kasutada, tuleb süsteemi usaldamiseks sinna lisada tõlgendavaid funktsioone, mille abil saaks ühtlustada ja ajakohastada valdkonnateadmisi. Tõlgendavad funktsioonid aitaksid vastata, miks selline otsus tehti ja see annaks probleemile või lahendusele uued mõõtmed. (Solanke, 2022, p. 1; 8)

Digitaalsete tõendite visualiseerimine on väga aeganõudev ja mahukas protsess, mille puhul ei piisa ainult digitaalse tõendi visualiseerimisest, vaid see nõuab enda kõrvale

ka suulise kirjeldamise osa. Digitaalse info edukaks visualiseerimiseks on võimalik kasutada diagramme kui ka erinevaid graafikuid, kuid vahel piisab videost või fotost. Olulist rolli digitaalsete tõendite visualiseerimisel võib mängida väikseimgi muudatus, sellepärast tuleb visuaalselt esitada teavet väga läbimõeldult. Vastasel juhul võib tekkida tõendi tõlgendamisel arusaamatusi. Vähendamaks olukorda, kus oluline teave kaotab oma väärtuse, on välja töötatud *EPIC* meetod, mis tugineb visualiseerimise üldistele printsiipidele. Tegemist on meetodiga, mida Eestis ei kasutata, kuid mida on võimalik lõimida meie hetkel kasutusel olevate meetoditega. Selle meetodi puhul otsustab digikriminalist, milline tõend on oluline. Nüüd on hakatud rääkima ka AI-st, mis võib kunagi mõjutada digitaalsete tõendite visualiseerimist. Kuna tegemist on uut tüüpi lähenemisega, siis on väga paljud inimesed siiski skeptilised selle võimekuses hindama erinevaid olukordasid. Küll aga pole välistatud, et AI-d hakatakse tulevikus kasutama ka Eesti riigiasutustes, et hõlbustada nii visualiseerimist kui ka kohtumenetlust.

1.5 Digitaalsete tõendite visuaalse esitlemisega seotud probleemid

Maailmas on saanud üldlevinuks isiklikud digitaalsed seadmed. Ühel inimesel võib enda kasutuses olla mitu erineva eesmärgiga digitaalset seadet (Hales, *et.al.*, 2017, p. 3). Casey (2010, p. 93) märkis, et tulenevalt suurest digitaalsest arengust on tekkinud ka palju „digitaalset tolmu“ ehk digitaalset andmeid on kogunenud ootamatutesse kohtadesse ja suurtes kogustes. Digikriminalistika jaoks on see oluline, sest see muudab digitaalsed seadmed põhjatuks infoallikaks. Küll aga on probleemiks, et tulenevalt andmete mahust, mis digitaalsetele seadmetele on talletatud, muutub ka nende analüüsimine aeganõudvamaks (Hales, *et al.*, 2017, p. 3).

Roussev, *et al.*, (2013, p. 158) tuvastasid, et aastatel 2003–2011 suurenes andmete maht, millega infotehnoloogia valdkonna kohtuekspert pidi tegelema, keskmiselt 6,65 korda, 84 GB-lt 559 GB-ni. Keerulisust lisab juurde see, et suured andmemahud saadakse enamasti binaarses vormingus ja erinevatest allikatest, mistõttu tuleb enne andmete analüüsi kasutada keerukaid andmete vähendamise tehnikaid (Lillis, *et.al.*,

2016, p. 10). 2015-ndal aastal ilmunud Iirimaa riikliku politsei aruandes on kirjutatud, et tulenevalt andmete mahukusest, võib kriminaalmenetluses oluliste digitaalsete tõendite uurimine kesta kuni 4 aastat. Taolistel juhtudel on kohtud viivituse tõttu pidanud mõned menetlused lõpetama (Garda Síochána Inspectorate, 2015, p. 205).

Sheppard, *et al.*, (2020, p. 8) toob oma uuringus välja, et kohtus olemasolevat tehnikat ja tarkvara ei suudeta kasutada otstarbepäraselt, sest puuduvad piisavad teadmised ja oskused, kuidas neid kasutada. Seda kinnitab ka Brian Leveson (2015, p. 17), kirjutades, et kõik isikud, kellel on regulaarne ligipääs kohtusaalis olevatele infotehnoloogilistele vahenditele, peaksid olema välja õpetatud ja teadlikud, kuidas neid kasutada. Sellest tulenevalt võivad menetlused jääda viibima, sest puudub esitlusvahendite ja tarkvarade kasutamise kompetents (Leveson, 2015, p. 17). Aastal 2014 lükati Inglismaal edasi 13 kohtuasja kroonikohtus ning 275 kohtuasja magistraadikohtus, sest tekkis probleeme tehnoloogia kasutamisega (Sheppard, *et al.*, 2020, p. 8). Peale puudulike teadmiste ja oskuste võib mõjutada tehnoloogia kasutamist selle hind. Mankeri (2015, p. 96) poolt läbi viidud uuringus toovad kohtunikud ja advokaadid välja, et peamiseks põhjuseks, miks kohtusaalis tehnoloogiat piiratud kasutatakse, tuleneb selle maksumusest.

Digitaalsete tõendite visualiseerimisega kaasnevad mitmed probleemid. Suurte andmemassiivide juurde on tekkinud ka „digitaalset tolmu“ ehk ebavajaliku infot, mis menetlusele kaasa ei aita. Digikriminalistide jaoks ongi väljakutseks saanud nende lõputute infoallikate analüüsimine ning olulise filtreerimine ebaolulisest, muutes digitaalsete tõendite leidmise aega nõudvaks protsessiks. Veel üheks problemaatiliseks osaks visualiseerimisel on vähesed teadmised ja oskused tehnikaga ümber käimiseks. Sellega kahjuks asi ei piirdu, vaid see hõlmab ka tarkvarasid, mis nõuavad vastavaid teadmisi, et säästa aega ja anda edasi vajalik info, mida digitaalse tõendiga üritatakse edastada. Paremad tarkvarad ja tehnika on aga kallid ja tänu rahaliste vahendite puudumisele ei saa paljud riigiasutused seda endale lubada.

2. EMPIIRILINE OSA

2.1 Uuringu meetodika, protsess ja valim

Töö raames viiakse läbi kvalitatiivne uuring, mille eesmärgiks on leida peamised kitsaskohad digitaalsete tõendite visuaalsel esitlemisel süüteomenetluses ning pakkuda nendele probleemidele lahendusi.

Kvalitatiivset uuringut võib defineerida kui uuringut, kus andmeid saadakse intervjuu, vaatluse ja sõnalise suhtlemise kaudu ning keskendutakse uuringus osalejate väljendatud tähendustele ja tõlgendustele (Laherand, 2008, lk 15). Teiste sõnadega on kvalitatiivne uuring suunatud inimeste kogemuste ja arusaamade mõistmisele (Laherand, 2008, lk 20). Inimliku kogemusena käsitletakse antud töös isikute tööalast kokkupuudet antud temaga ning sellest tekkinud arusaama probleemidest. Läbi kvalitatiivse uurimistöö on võimalik kasutada uurimise käigus saadud märkmeid, intervjuusid ning muid meetodeid, et tõlgendada saadud materjali praktiliselt ja teha antud teema nähtavaks teistele (Õunapuu, 2014, lk 53).

Andmete kogumise meetodina viiakse läbi poolstruktureeritud intervjuud prokuröride, kohtunike ja PPA ametnike seas, kes on oma ametist tulenevalt kokku puutunud digitaalsete tõenditega ja nende esitlemisega. Intervjuud valimiga kui andmete kogumise meetodit eelistatakse kirjalike testide ees seetõttu, et usaldatakse läbi vestluse ja vaatluse saadavat infot. Seda põhjendatakse inimese võimekusega kohaneda muutuvate olukordadega (Hirsjärvi, 2007, lk 155). Samuti on võimalik olla intervjuuga paindlik ja andmete kogumist vastavalt situatsioonile suunata ja reguleerida (Õunapuu, 2014, lk 177).

Intervjuu **valimiks** on ettekavatsetud valim. Uurimisobjektid on valitud kindla eesmärgi pärast, mitte juhusliku valimi järgi (Hirsjärvi, 2007, lk 155). Valimisse olid planeeritud 15 isikut ning valiku kriteeriumiteks olid teadmised digitaalsete tõendite ja visualiseerimise kohta. Valim koostati selliselt, et esindatud oleksid Eesti erinevate asutuste ametnikud ja saadud tulemused annaksid ülevaate digitaalsete tõenditega seotud probleemidest ja nende varieerumisest erinevate piirkondade lõikes. Valimi

moodustasid isikud, kes töötavad prokuratuuris, kohtus ja PPA-s. Antud töös on igale valimis osalenud ametnikule antud unikaalne kood ehk tunnus, mis tagab intervjuudes osalenud ametnike anonüümsuse.

Lõpliku valimi moodustavad 13 ametnikku, kelle unikaalne kood, esindatav üksus, tööstaaz ja intervjuu läbiviimise kuupäev on toodud tabelis 1 (Tabel 1). Lõplikku valimisse kuuluvad **5 prokuröri, 4 kohtunikku ja 4 PPA ametnikku**. Oma tööst tulenevalt puutuvad PPA ametnikud kokku digitaalsete tõenditega vahetult. Tehes koostööd prokuratuuriga, otsustatakse, millised tõendid on olulisemad ning need edastatakse prokurörile. Prokurör omakorda peab olema võimeline visualiseerima saadud tõendeid kohtunikele nõnda, et seda mõistaksid teised isikud, kes konkreetset süütegu vahetult ei kogenud ega sellega seotud uurimistoiminguid. Kõikide tõendite visualiseerimise edukuse otsustab lõpuks kohtunik, kellele neid tõendeid visualiseeritakse ning nende põhjal kas süüdi- või õigeksmõistev otsus langetatakse.

Valimisse kuuluvate isikute keskmine tööstaaz antud valdkonnas on 19 aastat. **Prokuröride puhul on esindatud** Põhja Ringkonnaprokuratuur, Viru Ringkonnaprokuratuur, Lõuna Ringkonnaprokuratuur, Lääne Ringkonnaprokuratuur ja Riigiprokuratuur. **Kohtunike puhul on esindatud** Harju Maakohus, Tartu Maakohus, Pärnu Maakohus ja Riigikohus. Intervjuude läbiviimiseks esitati taotlus Politsei- ja Piirivalveameti uurimistöde kooskõlastamise komisjonile, mis registreeriti dokumendihaldussüsteemi 02.03.2023 nr 1.1-14/42-2. **PPA ametnike puhul töötavad** kaks ametnikku Põhja Prefektuuris ja üks Keskkriminaalpolitsei majanduskuritegude büroo Lääne talituses. Neljas ametnik on Lõuna prefektuurist. Valimi moodustamisel võeti ühendust ka Viru Maakohtuga ja Ida prefektuuriga, kuid tulenevalt suurest töökoormusest ei olnud võimalik nimetatud asutustel antud töösse panustada.

Tabel 1. Intervjueeritavate unikaalsed tunnused, intervjueeritava esindatav üksus, intervjuu läbiviimise kuupäev ja tööstaaz (autori koostatud)

Intervjueeritava unikaalne kood	Intervjueeritava esindatav üksus	Tööstaaz	Intervjuu läbiviimise kuupäev	Töövaldkond
P1	Põhja Ringkonnaprokuratuur	16 aastat	02.03.2023	Küberkuriteod, inimkaubandus
P2	Viru Ringkonnaprokuratuur	15 aastat	13.02.2023	Narkokuriteod ja organiseeritud kuritegevus,
P3	Lõuna Ringkonnaprokuratuur	25 aastat	07.03.2023	Majandus-, maksu-, korrupsiooni-kuriteod
P4	Lääne Ringkonnaprokuratuur	25 aastat	15.02.2023	Majandus-kuriteod
RP1	Riigiprokuratuur	24 aastat	16.02.2023	Süüdistuse osakond
K1	Harju Maakohus	20 aastat	21.03.2023	Majandus ja maksu süüteod
K2	Tartu Maakohus	30 aastat	10.03.2023	Süüteoementlus, tsiviilõigusasjad ja eraõigusasjad
K3	Pärnu Maakohus	18 aastat	06.03.2023	Majandus-kuriteod
RK1	Riigikohus	26 aastat	07.03.2023	Kriminaalkolleegium ja Põhiseaduslikkuse järelevalve kolleegium
PP1	Põhja Prefektuur	6 aastat	08.03.2023	Kriminaalbüroo küber- ja majanduskuritegude talitus

Tabel 1 jätk. Intervjueeritavate unikaalsed tunnused, intervjueeritava esindatav üksus, intervjuu läbiviimise kuupäev ja tööstaaž (autori koostatud).

Intervjueeritava unikaalne kood	Intervjueeritava esindatav üksus	Tööstaaž	Intervjuu läbiviimise kuupäev	Töövaldkond
PP2	Põhja Prefektuur	9 aastat	22.03.2023	Seksuaalkuriteod ja lastekaitse grupp
PP3	Lõuna Prefektuur	13 aastat	23.03.2023	Küberkuriteod
PP4	Keskkriminaalpolitsei	24 aastat	20.03.2023	Majanduskuritegude büroo Lääne talitus

*P- Prokurör; RP - Riigiprokurör; K- Maakohtunik; RK- Riigikohtunik; PP- Politsei- ja Piirivalve ameti ametnik

Tulenevalt intervjueeritavate paiknemisest üle Eesti, valiti intervjuude läbiviimiseks *Microsoft Teams (for work)* rakendus, mille käigus salvestati videopilt koos heliga. Intervjuude keskmine kestus oli 43 minutit. Intervjuude sissejuhatuses räägiti lähemalt töö eesmärgist ja teema valikust. Lisaks räägiti läbi antud töö kontekstis digitaalse tõendi ja visualiseerimise tähendus. Intervjueeritavatelt küsiti küsimusi, mis hõlmasid nende igapäevast kokkupuudet antud valdkonnaga ning enda eriala spetsiifikast tulenevaid töökogemusi. Küsimused on toodud Lisas 1 (LISA 1).

Intervjuudega saadud andmed transkribeeriti ehk salvestatud intervjuud muudeti tekstidokumentideks (Laherand, 2008, lk 279). Transkribeerimiseks kasutati *Microsoft Word* tarkvara sees olevat lisa, mis on võimeline konverteerima mikrofoni kaudu kuuldavast vestlusest tekstidokumendiks. Peale konverteerimist loeti iga dokument läbi, kuulati salvestatud intervjuud ning vajadusel viidi sisse korrektuurid.

Andmeanalüüsi meetodina kasutati kvalitatiivset andmeanalüüsi, täpsemalt kvalitatiivse sisuanalüüsi alla kuuluvat koodipuu meetodit. Intervjueerimise käigus saadud andmed analüüsiti korduvalt läbi ning seejärel tõsteti esile olulisemad punktid, mille põhjal formuleeriti vastavad koodid. Iga kood paigutati kooditabelisse, sest läbi kooditabeli on võimalik kategoriseerida analüüsitud andmeid hõlpsamalt (Laherand, 2008, lk 291).

2.2 Intervjuu tulemused

Tulenevalt lõputöö uurimisküsimustest ja teoreetilistest lähtekohtadest moodustas autor vastuste leidmiseks 4 kategooriat, mis on toodud tabelis 2. Igale uurimisküsimusele vastab üks kategooria. (Tabel 2)

Tabel 2. Lõputöö uurimisküsimused ja neile vastavad kategooriad

Uurimisküsimused	Kategooriad
1. Kuidas toimub hetkel süüteo menetluses digitaalsete tõendite visualiseerimine?	<ul style="list-style-type: none">• Kokkupuude digitaalsete tõendite ja nende visualiseerimisega
2. Milliseid digitaalseid tõendeid visualiseeritakse Eestis kõige rohkem?	<ul style="list-style-type: none">• Enim kasutatavad digitaalsed tõendid Eesti praktikas
3. Millised on peamised probleemid digitaalsete tõendite visuaalsel esitlemisel?	<ul style="list-style-type: none">• Digitaalsete tõendite visuaalse esitlemisega seotud probleemid
4. Kuidas saaks parandada digitaalsete tõendite visualiseerimise protsessi?	<ul style="list-style-type: none">• Digitaalsete tõendite visuaalse esitlemise parendamine

Kõik moodustatud kategooriad jagunesid omakorda alakoodideks, mis on toodud tabelis 3. Tabelis 3 on toodud ka alakoodide esinemise sagedus intervjuudes ehk mitut intervjuueeritavat konkreetne kood puudutas ning kui tihedalt see esines. Kuna uurimisküsimused ja kategooriate alla kuuluvad alakoodid on omavahel tihedalt seotud, siis osad koodid täiendavad üksteist. (Tabel 3)

Tabel 3. Koodipuu - kategooriate alakoodid, nende esinemine ja esinemissagedus

Kategooria/Kood	Koodi esinemine intervjuudes	Koodi esinemissagedus kokku
KATEGOORIA 1 - KOKKUPUUDE DIGITAALSETE TÕENDITE JA NENDE VISUALISEERIMISEGA		
Kood 1 Tõendite esitamine digitaliseeritud kujul	13	32
Kood 2 Interaktiivsete dokumentide, protokollide tegemine	4	4
Kood 3 Kokkupuude on tihe	3	3
Kood 4 Digigrupiga koostöö	3	3
Kood 5 Tõendite ja dokumentide säilitamine digitaalselt	2	3
KATEGOORIA 2 - ENIM KASUTATAVAD DIGITAALSED TÕENDID EESTI PRAKTIKAS		
Kood 1 Videofailid	6	8
Kood 2 Fotod	4	4
Kood 3 Helisalvestised	4	4
Kood 4 Andmekandjate sisu	4	5
Kood 5 Jälgimisega seotud tõendid	4	5
Kood 6 Raportfailid	3	3
Kood 7 Suhtlusrakendustes toimuv vestlus	3	3
Kood 8 Pilvandmed	2	3
Kood 9 Krüptovaluuta	2	2
KATEGOORIA 3 - DIGITAALSETE TÕENDITE VISUAALSE ESITLEMISEGA SEOTUD PROBLEEMID		
Kood 1 Tarkvara probleemid	8	11
Kood 2 Töötajatega seonduvad probleemid	5	9
Kood 3 Digitaalsete tõenditega seonduvad probleemid	4	4
Kood 4 Pabertoimikud	3	4
Kood 5 Tehnika veab alt	3	5
Kood 6 Tõlkimise probleemid	3	3
Kood 7 Ollakse kinni vanades praktikates	3	3
Kood 8 Liiga mahukad digitaalsed tõendid	2	2
Kood 9 Seadusandlus	2	2

Tabel 3 jätk. Koodipuu - kategooriate alakoodid, nende esinemine ja esinemissagedus

Kategooria/Kood	Koodi esinemine intervjuudes	Koodi esinemissagedus kokku
KATEGOORIA 4 DIGITAALSETE TÕENDITE VISUAALSE ESITLEMISE PARENDAMINE		
Kood 1 Tehniliste seadmete abil	5	6
Kood 2 Eksperdi kutsumine	3	4
Kood 3 Tarkvarad	3	3
Kood 4 Koolitused	3	4
Kood 5 Ühtse praktika loomine	3	3
Kood 6 Digitaalselt ligipääsetav andmehoidla	2	3

Esimesele uurimisküsimusele vastuse leidmiseks loodi kategooria “ kokkupuude digitaalsete tõendite ja nende visualiseerimisega ”. Nimetatud kategooria jagunes omakorda viieks alakoodiks: tõendite esitamine digitaliseeritud kujul; interaktiivsete dokumentide, protokollide tegemine; kokkupuude on tihe; digigrupiga koostöö; tõendite ja dokumentide säilitamine digitaalselt.

Digitaliseeritud kujul tõendite esitamisega on kokku puutunud kõik valimisse kuuluvad isikud. Kolm vastanutest mainisid, et nad on oma karjääri jooksul puutunud kokku digitaalsete tõenditega ja nende visualiseerimisega tihedalt.

“...tegelikult olgem ausad, meie kuritegude puhul enamuse tõendiallikad on täna digitaalsed tõendid” (PP4, 2023).

Antud koodi alla on lisaks videofailide, pildifailide, helifailide ja pilveandmete esitamisele arvestatud ka digitahvlite kasutamine, tõendite kuvamine kohtusaali seinale, virtuaalne kohtumenetlus distantsilt, üldine esitlusvahenditega kokkupuude, kohtunikele tõendite esitlemine ja analoogteabe skaneerimine.

“...ma kuvan dokumentaalsed tõendid digitaliseeritult ekraani peal niiviisi, et kõik näevad. Ja see on väga mugav selles mõttes sa saad näidata seal kohe olulised kohad ekraanil ära” (P2, 2023).

Interaktiivsete protokollide ja dokumentide tegemisega kokkupuudet mainisid kolm prokurööri ja üks PPA ametnik. Prokurörid on antud koodi all kokku puutunud *sandbox*-i kasutamise, geograafiliste punktide visualiseerimisega ja videofailidest ajalisest järjestuses koondfailide tegemisega. PPA ametnik on antud koodi all kokku puutunud kompleksvaatlusega.

Küll aga on tekkinud ka olukordi, kus liigne visualiseerimine on toonud rohkem kahju kui kasu. Riigikohtu kriminaalkolleegiumi kohtuotsus 1-18-437 kohaselt esitati kohtule isikute varalist seisundit kajastavate andmete vaatlusprotokoll. Tehtud vaatlusprotokoll ei vastanud vaatlusprotokolli olemuslikele nõuetele täitnud oma eesmärki. Protokollija oli kõrvutanud erinevaid tõendeid, teinud arvutusi, kokkuvõtteid ja järeldusi enda arusaamise järgi. Lisaks analüüsis protokolli koostaja ka tunnistaja kohtueelseid ütlusi ning vormistas oma hinnangu ja selleni jõudmise vaatlusprotokollina (R. L. kriminaalasi karistusseadustiku §256 lg 1 järgi, 2022). Protokolli koostaja oli suutnud üle visualiseerida digitaalseid tõendeid, luues sellega kohtule meelevaldselt, enda arusaama kohaselt ettekujutuse ning suunates neid kindla otsuse poole. Kohtu ülesanne on hinnata tõendeid kogumis ning nad peavad ise jõudma järeldusteni.

Seda kommenteeris ka intervjuu ajal kohtunik (K3): *“Kohtunik hindab ise tõendeid ja menetleja ei saa öelda, et see on see. Kohtunikul peab alati olema võimalus viimaseks sõnaks, et öelda, mida see tegelikult tähendab”* (K3, 2023).

Kolm vastanut, kes kõik olid PPA ametnikud, tõid välja, et nad on teinud koostööd digigrupiga. Seda seetõttu, et PPA ametnikud on esmased tõendite kogujad ning nemad konsulteerivad digigrupiga, milliseid infotehnoloogilisi vahendeid nendeni on vaja edastada, et teha järgmisi toiminguid. Prokurör ja kohtunik seda ei tee.

Lisaks mainiti ära ka tõendite ja dokumentide säilitamine digitaalselt ja nendega tutvumine toimikus. Teisisõnu, kõik digitaalsed tõendid jäetakse digitaalsele kujule ning nendega tutvumine on samuti infotehnoloogiliste vahendite abil tehtud kättesaadavaks.

Võttes kokku antud kategooria alla kuuluvad vastused ja kõikide intervjuueeritavate kogemused, saab digitaalsete tõendite visualiseerimise protsessi süüteomenetluses kirjeldada järgnevalt. Politseiametnikud teevad koostööd nii digikriminalistide kui ka prokuröridega. Politseiametnikud peavad oskama koguda erinevaid digitaalsete tõendeid. Kõik digitaalsed tõendid viiakse digikriminalistidele, kui nendes peaks leiduma tõendamiseseme asjaoludega seonduvaid andmeid. Politseiametnikud koostöös digikriminalistidega otsustavad, mis on antud andmetest võimalik välja selekteerida. Vaatluse tulemusena saadud andmed suunatakse prokuröridele. Salvestatakse digitaalne tõend CD peale ning vajadusel lisatakse ka programm, mis seda tõendit on võimeline esitlema. Kui kõik tõendid on kogutud, esitletakse neid kohtus. Fotosid on võimalik lisada välja printitud menetlustoimiku hulka, kuid saab ka koos videote ja helifailidega esitleda kohtusaalis olevatel ekraanidel. Kui tehniline võimekus lubab, on võimalus kasutada ka digitaalkaarti, samas selline võimekus mõndades kohtutes puudub. Alati ei pruugi selline digitaalsete tõendite esitlemine võimalik olla, sest kohus võib nõuda tõendeid pabertoimikus.

“Kriminaalmenetluse seadustik momendil sätestab, et meil on ikkagi pabertoimik ja see tähendab seda, et me pörkume kohtus igapäevaselt selle vastu, et kohus nõuab meilt tõendeid paberil “(P3, 2023).

Teisele uurimisküsimusele vastuse leidmiseks loodi kategooria “enim kasutatavad digitaalsed tõendid Eesti praktikas”. Nimetatud kategooria jagunes omakorda üheksaks alakoodiks: videofailid; fotod; helisalvestised; andmekandjate sisu; jälgimisega seotud tõendid; raportfailid; suhtlusrakendustes toimuv vestlus; pilveandmed ja krüptovaluuta.

Eesti praktikas puututakse digitaalsetest tõenditest kõige rohkem kokku videofailidega. Videofailidega kokkupuute töid välja kuus vastanut. Nende hulka kuulusid neli prokuröri ja kaks kohtunikku. Videofailide alla arvestati tänavakaamerate, turvakaamerate ja varjatud kaamerate salvestised ning ülekuulamiste salvestised.

Fotode, helisalvestiste, andmekandjate sisu ja jälgimisega seotud tõenditega kokkupuute mainisid neli vastanut. Andmekandjate sisu alla arvestati kõik vastused, kus mainiti mobiiltelefoni, arvutit, kõvakettaid, meilivahetusi. Jälgimisega seotud

tõendite alla koondati vastused, kus mainiti logifaile, IP aadresse ja geograafilisi tõendeid.

Lisaks olid intervjuueeritavad kokku puutunud ka telefonide raportfailidega, suhtlusrakendustes toimuvate vestlustega, pilveandmetega sh pangakonto andmetega ja krüptovaluutaga.

“...mõnes asjas on jällegi olulised just need häälsõnumid, mis on facebookis olnud või mingi sõnumi vahetuses, neid on palju” (K1, 2023).

“Kõige levinum on näiteks telefonide koopiatest tehtud vaatlusprotokollid” (RP1, 2023).

Intervjuu küsimusele “milliseid digitaalsete tõendeid on teie menetlustes kõige enam visualiseeritud?” ei nimetanud ükski PPA ametnik videofaile, fotosid ega helisalvestisi. Intervjuus osalenud PPA ametnikud on digitaalsetest tõenditest kokku puutunud andmekandjate sisu, jälgimisega seotud tõendite, pilveandmete ja krüptovaluutaga. Olgugi et PPA ametnikud ei toonud konkreetselt välja oma kokkupuudet videofailide, fotode ja helisalvestistega võib järeldada, et nad siiski puutuvad nendega kokku, sest andmekandjad on võimelised ka talletama foto-, video- ja helifaile. Järgnev tsitaat räägib andmekandja saatmisest PPA ametnike poolt digigrupile ning mida võib sealt leida: *“... jällegi oleneb, esiteks võib leiduda, ma ei tea 50 faili. Olgu need pildid või videod. Teiseks võib olla neid pool miljonit” (PP2, 2023).*

Prokuröride vastustest tulid välja kõik antud kategooriale vastavad koodid, v.a. krüptovaluuta. Kohtunikud ei nimetanud jälgimisega seotud tõendeid, pilveandmeid ja krüptovaluutat, kõiki teisi koode nimetati.

Kolmandale uurimisküsimusele vastuse leidmiseks loodi kategooria “digitaalsete tõendite visuaalse esitlemisega seotud probleemid”. Nimetatud kategooria jagunes omakorda üheksaks alakoodiks: tarkvara probleemid; töötajatega seonduvad probleemid; digitaalsete tõenditega seonduvad probleemid; pabertoimikud; tehnika veab alt; tõlkimise probleemid; ollakse kinni vanades praktikates; liiga mahukad digitaalsed tõendid; seadusandlus.

Suurimaks probleemiks digitaalsete tõendite visuaalsel esitlemisel peeti tarkvara probleeme. Tarkvaraga seotud probleeme mainis seitse intervjuueeritavat. Kõige rohkem erinevaid tarkvaraga seonduvaid probleeme tõi välja Lõuna Ringkonnaprokuratuuris töötav prokurör (P3). Tema tõi tarkvara probleemidena välja tarkvara ja litsentside puudumise, tarkvara puudumise kohtumajas ning olukorra, kus unustatakse vajalik tarkvara kaasa võtta. Tarkvara puudumist kohtumajas mainis ka Põhja Ringkonnaprokuratuuris töötav prokurör (P1). Viru Ringkonnaprokuratuuris töötav prokurör (P2) tõi välja selle, et infosüsteemid ei toeta mahukate andmekogude presenteerimist, talletamist ja nendega tutvumist. Ka Põhja ja Lõuna Prefektuuris töötavad PPA ametnikud (PP1, PP3, PP4) tõi välja tarkvara(de) puuduse üldiselt.

Põhja Prefektuuris töötav ametnik (PP1) tõi välja ka ebamugava olukorra, kus tarkvara haldajad tuleb Eestisse kutsuda. *“Programmi haldajad/esindajad peavad olema valmis tulema Eesti kohtusse tunnistusi andma, et kuidas see süsteem töötab, et see on probleem”*(PPI, 2023).

Samuti lisas ta, et häid tarkvarasid on väga raske soetada, sest pole raha nende ostmiseks: *“...kindlasti tarkvarad teeks oluliselt lihtsamaks seda, aga meil lihtsalt ei ole seda ressursi ja ma olen siin kaubelnud ja kaubelnud oma valdkonnas igasuguseid asju aga siitamaani me ei ole saanud”* (PPI, 2023)

Pärnu ja Harju Maakohtus töötavad kohtunikud (K1, K3) tõi ka välja üldised tarkvara probleemid ning Pärnu Maakohtu kohtunik mainis täpsemalt ära ka pilveteenuste puudumise.

“Meil ongi see probleem, et oleks vaja videot vaadata, kas ta peab ilmingimata CD plaadi peal olema. Meil võiks olla selline pilveteenus, kuhu saad sisse logida ja ta tuleb automaatselt kohtute infosüsteemi üle”(K3, 2023).

Teine suurem probleem, mis intervjuudest välja tuli on, töötajatega seonduvad probleemid. Antud probleemi mainisid ära viis intervjuueeritavat ja antud probleemid esinevad kõige enam just prokuröridel. Põhja Ringkonnaprokuratuuris töötav prokurör (P1) tõi välja, et enamasti on prokuröridel vähene arusaam ja teadmised, kuidas mõjuvat visualiseerimist luua ning vähe on ka fantaasiat, mis aitaks kaasa mõjuva

visualiseerimise loomisele. Ta tõi välja ka selle, et kohtueelses menetluses on rohkem vaja inimesi, kes oskavad digitaalset tõendit visualiseerida.

“Kohtueelse menetluse poole pealt selleks, et teha midagi, mida visualiseerida kohtus, selleks on mul vaja inimesi, kes seda oskavad teha. Me võime minna nii kaugemale ära, et meil ei ole lihtsalt niisugused inimesed tööl, kes aitaks mul mingit videoklippi või ägedat asja kokku kombineerida” (P1, 2023).

Lõuna Ringkonnaprokuratuuri prokurör (P3) mainis ära vähese väljaõppe ja selle, et spetsialiste ei jõuta välja koolitada. Viru Ringkonnaprokuratuuri prokurör (P2) nägi probleemina ka vähest teadlikkust visualiseerimise tarkvarade kasutamise kohta. Lõuna Prefektuuri ametnik (PP3) nägi samuti probleemi inimeste väheses väljaõppes. Ainult üks intervjuueeritav, Lõuna Ringkonnaprokuratuuri prokurör (P3), ütles otse, et tema ei ole oma töös otseselt digitaalsete tõendite visualiseerimise probleemidega kokku puutunud. Siiski oskas ta nimetada probleeme, mis suure tõenäosusega võivad tekkida ja need vastused on siiski antud kategooria all arvesse võetud.

Kolmas probleem, mida mainisid neli vastanut, koondub koodi alla “digitaalsete tõenditega seonduvad probleemid”. Tartu Maakohtu kohtunik (K2) tõi välja, et vahepeal võib probleemiks olla see, et keeruline on kindlaks teha digitaalse tõendi loomise kellaega või kuupäeva. Pärnu Maakohtu kohtunik (K3) tõi välja digitaalsete tõendite võimaliku halva kvaliteedi, mis raskendab tõendi sisu mõistmist. Lõuna Ringkonnaprokuratuuri prokurör (P3) rääkis võimalikust olukorrast, kus digitaalne tõend ei ole mingil põhjusel säilinud ja Lääne Ringkonnaprokuratuuri prokurör (P4) rääkis välistavate tõendite kasutamisest.

“Muidugi kõige keerulisem on esitleda sellist salvestist, mille peale ma tahan öelda, et sellel kellaajal see inimene seal ei olnud” (P4, 2023)

Kolm intervjuueeritavat tõi eraldiseisvate probleemidena välja ka pabertoimikud ja nende mahukuse, vana tehnika, tõlkimise probleemid ja vanades praktikates kinni olemise. Järgnev tsiteering räägib sellest, kui ühe pabertoimiku juurde kuulub mitu digitaalse tõendina talletatud e-kirjade vahetust ning pabertoimiku jaoks tähendaks see paberikulu: *“Ma eelnevalt kontrollin, et need on vajalikud asjad, need prinditakse*

välja, vaadatakse korra läbi, fikseeritakse ära, et tõepoolest nii on, ning siis nad võetakse arhiivi ruumi kokku. Ma ütlen, seal tekib nagu selline paberi kui ressursi kulutamine üle mõistlikkuse” (P4, 2023)

Samuti toob (K2) välja, et mitte ainult tehnika ei ole vana, vaid see isegi puudub.

“... minu meelest meie kohtunike laual olev arvutisüsteem on läinud halvemaks. Ma tean näiteks, et mitte kaua aega tagasi oli Tartu kohtumajas nii, et mingit statsionaarset arvutit seal ei olnud, käisid seal oma läpakaga” (K2, 2023).

Tõlkimise probleemide all toodi välja vastuolu, kus kohtupidamise keel on eesti keel, aga tarkvarad on inglisekeelsed.

“Probleem on täna jällegi see, et mida kaitsjad välja toovad ning mida siis prokurör ette näeb – tõlkimine. Isegi nii labased sõnad nagu „date“, „name“. See tundub mulle ebamõistlik. See on iga endast lugupidava menetleja, kaitsja või kohtuniku ajaraiskamine“ (P4, 2023).

Olulist rolli mängib ka oskus saadud andmeid visualiseerida, mitte olla vanas praktikas kinni, sest kui ei suudeta edasi anda olulist teavet siis võib see mõjutada/kahjustada tõendi väärtust.

“... me astume sammu edasi, et me oskame andmeid visualiseerida, väga hästi, aga samas kui me hakkame seda ebaefektiivselt tegema siis see on juba halb tulemus, mis on vaja kunagi uuesti korrigeerida” (PP4, 2023)

Viru Ringkonnaprokuratuuri prokurör (P2) ja Põhja Prefektuuri ametnik (PP1) töid välja ka digitaalsete tõendite mahu probleemi.

“Digitaalsete tõendite visualiseerimise esmaseks probleemiks on see, et nad on mahukad, ning nende avamine võtab kohtusaalis kindlasti kauem aega” (P2, 2023).

“Keerulisemaks teeb ka see, et need on väga mahukad tihti peale” (PP1, 2023).

Ringkonnaprokuratuuri prokurör (P3) ja Põhja Prefektuuri ametnik (PP4) töid välja seadusandluse probleemi. Näiteks saab tuua riigikohtu lahendi 1-20-1208, kus prokuratuur väitis, et KrMS §91¹ annab õiguse andmekandjatesse sisenemiseks,

eesmärgiga neid läbi otsida, juhul kui läbiotsimismääruses on luba antud. Kaitsjad sellega ei nõustunud, selgitades, et seadus sätestab vaid neli objekti, mille suhtes tohib antud paragrahvi rakendada. Nendeks on: hoone, ruum, sõiduk, piirdega ala, kuid mobiiltelefonid nende hulka ei kuulu. Sellega nõustus ka maakohus, et KrMS §91¹ ei anna alust andmekandjatesse siseneda ning läbiotsimiskohast arvuti, telefoni või mõne muu andmekandjate kopeerimiseks ja ära võtmiseks (R. L. kriminaalasi karistusseadustiku § 184 lg 2¹ järgi, 2022).

„Ei saa olla midagi nii abstraktset nagu digimaailm. Antud probleem on seadusandja poolt täiesti reguleerimata.“ (K3, 2023).

Empiiriline uuring kinnitas kõiki digitaalsete tõendite visuaalse esitamisega seotud probleeme, mis mainiti ära ka teoreetilises osas:

- Andmete suur maht,
- Keerulised andmete vähendamise tehnikad sh tarkvarad,
- Töötajatega seotud probleemid - tehnikat ja tarkvara ei osata kasutada otstarbepäraselt, puuduvad piisavad teadmised ja oskused,
- Tarkvara puudumine - kallis hind,

Lisaks teoreetilises osas kajastatud probleemidele tuli intervjuude käigus välja veel probleeme, mis antud teemaga seonduvad. Nendeks olid näiteks tõlkimise, pabertoimikute, seadusandluse ja tehnika probleemid.

Neljandale uurimisküsimusele vastuse leidmiseks loodi kategooria “digitaalsete tõendite visuaalse esitlemise parandamine”. Nimetatud kategooria jagunes omakorda kuueks alakoodiks: tehniliste seadmete abil; eksperdi kutsumine; tarkvarad; koolituste tegemine; ühtse praktika loomine; digitaalselt ligipääsetav andmehoidla.

Kui intervjueeritavatelt küsiti, millised oleksid nende ettepanekud digitaalsete tõendite visuaalse esitlemise parandamiseks, siis kõige rohkem nimetati, et kaasa võiksid aidata tehnilised seadmed ja lahendused. Selle koodi alla minevaid vastuseid nimetasid viis intervjueeritavat. Viru Ringkonnaprokuratuuris töötav prokurör (P2) ütles, et parandada tuleks digitaalsete tõendite visuaalset kvaliteeti, et fotod ja videod oleksid parema resolutsiooniga ning selgesti arusaadavad. Lõuna Ringkonnaprokuratuuris

töötav prokurör (P3) arvas, et digitahvlite kasutamine teeks visuaalse esitlemise protsessi lihtsamaks. P3 tõi oma intervjuus välja, et neil veel hetkel digitahvli kasutamise võimekust pole.

“Ma ise ei ole kasutanud digitahvlit, kuid seda kiidetakse. Ta on funktsionaalne, põhimõtteliselt sa võid näiteks kuvada sinna kuritöö sündmuskoha ja siis joonistada ise peale, näiteks, kus keegi asus, mida keegi tegi, tuginedes tõenditele” (P3, 2023).

Enamik prokuröre tõi lahendusena välja eksperdi, asjatundja või spetsiifiliste tehniliste teadmistega inimeste kutsumise ja kaasamise protsessi.

“... selles mõttes jube hea on digikriminaliste kohtus üle kuulata, et siis sa saadki sellise piisava teabe” (P2, 2023)

Kuigi digitaalsete tõendite visuaalse esitlemisega seotud suurimaks probleemiks peeti tarkvara probleeme, siis tarkvara, kui lahendust mainisid ainult 3 vastanutest.

“... ütleks see sama “Püüton”, “Pandas”, “Jupyter” me oleme samas ajastus, et kui me suudame selle asja praegusel ajal edukalt tööse võtta kasutusele, siis me tegelikult oleks natukene oma ajast ees. Kui see viibib veel 5-10 aastat siis me hakkame nägema igalpool, et erasektoris kasutatakse seda ja me oleme siis natuke ebaefektiivsena riigiasutusena sabas sörkinud” (PP3, 2023).

“Ma ütleks, et tahakski seda programmi poolt. Hakkaks mingisugused programmid tekkima või me kulutaksime natukene raha selle peale, et laseks kirjutada endale siis nii öelda vajalikke programme, mis oleksid ka seaduse poolt vastu võetud” (PP4, 2023).

Lahendusena pakkusid intervjuueeritavad välja ka koolituste läbiviimise ja kolleegide vahel teadmiste jagamise.

“... kuidas seda oskuslikult teha, on pigem kolleegide vahel kogemuste jagamine. Ja just nimelt selle tehnilise võimekuse endale selgeks tegemine” (P3, 2023).

Mitmetest intervjuudest oli aru saada, et digitaalsete tõendite valdkond ei ole kõige paremini reguleeritud ja on mitmeid vastuolulisi teemasid - seadusandlus, keele ja tõlkimisega seotud probleemid ja rakendatavad praktikad. Selle üldise olukorra

lahenduseks kerkis intervjuudest välja ka ühtse Parima praktika kontseptsiooni loomise vajadus, mida mainisid kolm Põhja Prefektuuris töötavat ametnikku (PP1, PP2, PP4). PP1 tõi lahendusena välja ka paremate juhendite loomise.

“... noh selles vallas kindlasti on vaja koolitusi. Kaasa aitaks ka parimate praktikate loomine. Võibolla mingid juhendid” (PP1, 2023).

Eraldi lahenduse ja koodina tuli välja ka digitaalse ligipääsetava andmehoidla või E-toimiku loomine. See lahendus vastab hästi pabertoimikute mahukuse probleemile.

“Mida ma tahan öelda, on see, et kõvaketastega nende andmete vedamine, see on suhteliselt ebanormaalne tegevus. Võibolla tuleb politseil tulevikus mõelda, kuidas teha need andmed, mis neil on hoiul andmehoidlas, kättesaadavaks menetlusosalistele digitaalselt” (P2, 2023).

“Video ja helisalvestiste puhul minu arust oleks mõistlik luua üks andmehoidla. Kui ma olen kogunud tõendid ja pannud andmehoidlasse siis sinna ta jääbki, ta ei liigu sealt kuhugi. Ainus, mis tuleb, on kasutajaliidesed” (K2, 2023).

Antud intervjuude käigus pakuti intervjuueeritavatele välja ka lahendus seletava sõnastiku kujul, mis sisaldaks eelkõige tehnilisi termineid ja oleks ajas muutuv ja uuendatav. Selle idee kiitsid heaks neli vastanut. Toodi välja, et taoline sõnastik oleks abiks just uutele alles alustavatele spetsialistidele või siis saaks seda kasutada toimiku lisana, et hiljem oleks kohtunikel lihtsam lahendit kirjutada, kuid jäädi ka seisukohale, et kui tekib küsimusi, kutsutakse kohtuistungile eriteadmistega isik, kes digitaalset valdkonda mõistab.

“See sõnastik ei aita meid selles mõttes, kui ta puudutab tõeliselt tehnilisi termineid” (P1, 2023).

... põhimõtteliselt mina olen mõlema käega poolt, et kui kunagi peaks mingi selline asi nagu tekkima, et kasvõi tõesti sõnastik või mingi käsiraamat, kuid selle tingimuseks peaks olema see, et see on kättesaadav nii PPA-le, prokuratuurile kui ka kohtule” (PP2, 2023).

“Kui on olemas väga keerulised kõrgetasemelised asjad, nt IT-teemad, siis ei ole sellest sõnastikust mingit kasu. Mis sa sellega teed? Aga muudel juhtudel, näiteks koolituse materjalina võib ikka abiks olla, alustavatele kohtunikele ja prokuröridele” (K2, 2023)

“... selline üldhariv sõnastik. Miks ka mitte. Aga see võiks olla siuke ajas muutuv ja vabatahtlik” (RP1, 2023).

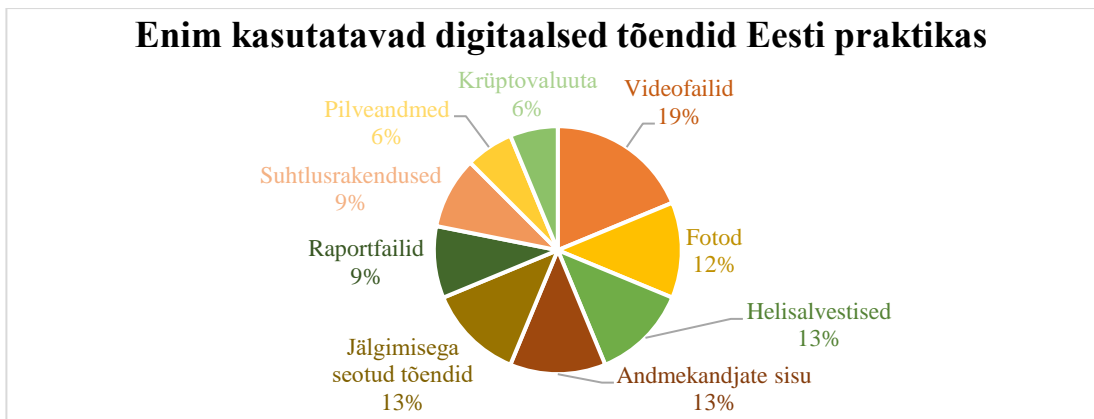
2.3 Järeldused ja ettepanekud

Lõputöö teoreetilises osas anti ülevaade digitaalsetest tõenditest, digikriminalistikast, infotehnoloogilistest vahenditest, digitaalsete tõendite visualiseerimisest ning visualiseerimisega kaasnevatest probleemidest. Empiirilises osas viidi läbi kvalitatiivne uuring, mille raames viidi läbi poolstruktureeritud intervjuud prokuröride, kohtunike ja Politsei-ja Piirivalveameti ametnikega üle Eesti. Töö empiirilises osas analüüsiti intervjuueeritavate ütlusi ja vaatepunkte digitaalsete tõendite visualiseerimise osas, lähtudes uurimisküsimustest ning kõrvutati seda teoreetilise osaga. Antud peatükis esitatakse lõputöö järeldused.

Esimene uurimisküsimus otsis vastust sellele, kuidas toimub hetkel süüteomenetluses digitaalsete tõendite visualiseerimine. Intervjuu tulemustega selgus, et kõik vastajad on puutunud kokku digitaalsete tõenditega. Lähtudes ametnike, kohtunike ja prokuröride vastustest, toimuvad hetkel digitaalsete tõendite visualiseerimine ja sellega seotud tegevused järgnevalt. Kuna Politsei- ja Piirivalve ametnikud on esmased reageerijad sündmuskohale, siis nemad teevad aktiivselt koostööd digigrupiga ehk digikriminalistidega ning läbi selle otsustavad, millistelt digitaalsetelt seadmetelt on vajadus tõendeid otsida ning millised kaasa võtta. Teoreetilises osas mainiti ka digikriminalistide töö olulisust, sest digitaalsete seadmete kasutamine jätab jälgi ning sõltuvalt süüteo liigist võib olla sellel suur kaal juhtumi lahendamiseks (käesolev töö lk 9). Tehes koostööd digigrupiga ning prokuratuuriga, vaadatakse digiseadmetest saadud tõendeid ning otsustatakse, millised tõendid esitatakse prokurörile, et menetlustoimik kokku panna. Üks PPA ametnik täheldas, et nüüdisajal toime pandud

kuriteod hõlmavad palju digitaalseid tõendeid. Seda arvamust toetab ka teoreetiline osa, kus Eneli Laurits toob välja digitaalsete tõendite suuremat kasutuselevõtmist Eestis (käesolev töö lk 14). Intervjuule vastanud prokuröridest kolm on läbi digigrupi ja PPA ametnike koostöö puutunud kokku ka interaktiivsete protokollidega, mida nad on pidanud esitama kohtule ja kaitsjale. Kohtunikud puutuvad kokku tõenditega läbi esitlemiste (käesolev töö lk 13-14). Prokurörid tulevad menetlustoimikutega kohtusse, projitseerivad seinale eeluurimise käigus kogutud tõendeid. Kohus vaatab tõendite omavahelised seosed üle ning läbi selle langetatakse otsus. Lõputöö autor jõudis **järeldusele**, et kõik riigiasutused puutuvad aktiivselt kokku digitaalsete tõenditega ning nende visualiseerimisega. Peamiselt puutuvad sellega kokku prokurörid, kes näevad, kuidas tõendid on kogutud ning lõpuks integreerivad need kohtule esitlemiseks menetlustoimikusse, et seda kohtule esitada. Hetkel kasutatakse digitaalsete tõendite visualiseerimiseks erinevaid tehnilisi seadmeid, mis võimaldavad tõendeid kuvada seinale või ekraanile. Seda toetab ka teoreetiline osa, kus on mainitud, et on hakatud kasutama rohkem digitaalseid tõendeid tänu meedia formaatides ja seadmetes toimunud arengule (käesolev töö lk 14).

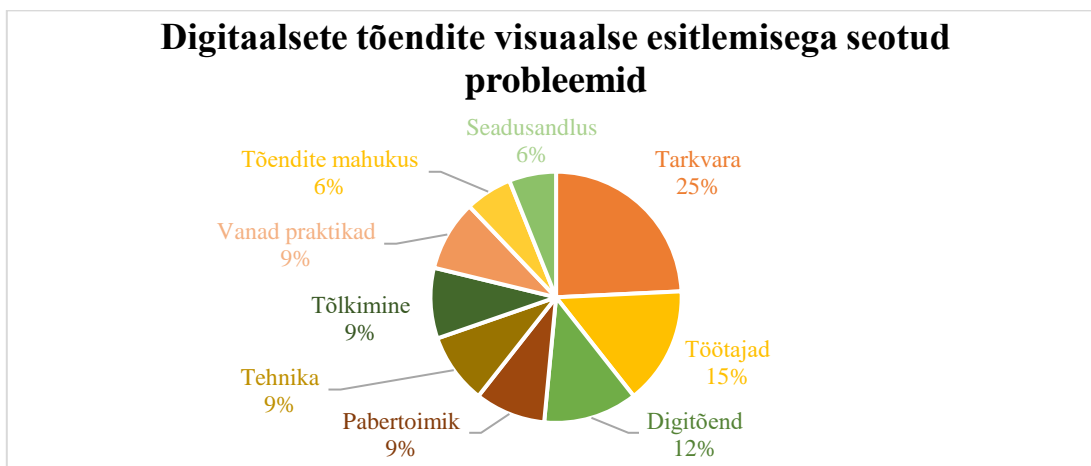
Teisele uurimisküsimusele, milliseid digitaalseid tõendeid visualiseeritakse Eestis kõige rohkem (vt Joonis 2), vastasid intervjueeritavad, et peamiselt puututakse kokku videofailidega, olgu nendeks jälitus-, turva-, tänavakaamera salvestised või menetluse jooksul tehtud ülekuulamise salvestised. Teisena toodi välja kokkupuude jälitustoimingutega saadud digitaalsete tõenditega. Kolmandaks on märgitud andmekandjate sisu. Andmekandjateks arvestati mobiiltelefonid, arvutid ja kõvakettad, mis on võimelised talletama digitaalseid tõendeid. Autor jõudis **järelduseni**, et kõige enam visualiseeritakse video-, heli- ja fotofaile. Olgugi et ükski PPA ametnik ei toonud intervjuu jooksul välja suurt kokkupuudet video-, heli- ja fotofailidega (käesolev töö lk 28), vaid andmekandjatega, mille eesmärgiks ongi talletada erinevat teavet, sealhulgas eelpool nimetatud tõendeid. Kui need juurde arvestada, oleksid eelpool mainitud tõendid enim visualiseeritud. Sama kehtib ka jälitusega saadud tõendite puhul.



Joonis 2. Enim kasutatavad digitaalsed tõendid Eesti praktikas (2023, autori koostatud)

Kolmanda uurimisküsimuse puhul, millised on peamised probleemid tõendite visuaalsel esitlemisel (vt Joonis 3), leidsid intervjuueeritavad, et peamiseks murekohaks digitaalsete tõendite visualiseerimisel on tarkvarade puudus ning nende rahaline maksumus. Probleemi on käsitletud ka teoreetilises osas (käesolev töö lk 18). Riigiasutustel pole piisavalt rahalisi vahendeid, et soetada paremaid tarkvarasid või rahastada vastava programmi välja töötamist (käesolev töö lk 29). Vastanutest puutusid probleemiga peamiselt kokku PPA ametnikud ja prokurörid. Samuti on murekohaks digitaalsete tõendite esitlemisega seotud oskused. Inimestel puudub teadlikkus kuidas efektiivselt kasutada erinevaid visualiseerimise tarkvarasid nõnda, et visualiseerimise tulem oleks õige ja objektiivne. Peamiselt tõid selle mure välja prokurörid, kuid seda esines ka teistes gruppides. Oldi arvamusel, et rohkem on vaja inimesi, kes suudaksid digitaalseid tõendeid visualiseerida oskuslikult, kasutades ära oma loovust ning visualiseerimise tarkvarasid. Peale eelpool nimetatud probleemide toodi välja ka teisi probleeme, mis võivad tekkida digitaalsete tõenditega. Kohtunikud tõid välja, et vahel esitletava digitaalse tõendi kvaliteet on halb. Samuti on probleemiks keerukus digitaalsete tõendite puhul kindlaks teha, millal see tõend oli tekkinud nii kuupäevaliselt kui ka kellaajaliselt. Ülejäänud probleemid olid seotud sellega, et Eestis on menetluses kasutusel pabertoimikud ning tehnika on vana või see täielikult puudub. Antud probleemid leidsid kajastamist ka teoreetilises osas (käesolev töö lk 17-18). Autor jõudis **järelduseni, et tarkvara probleemi näevad PPA ametnikud**, kuid nende jaoks on probleeme mitu: mahukad digitaalsed tõendid, vanades praktikates kinni olemine, tõlkimise probleemid. Prokuröride jaoks on suureks probleemiks töötajate

väljakoolitamine ning vähene teadmine kuidas digitaalseid tõendeid visualiseerida, sest tehnoloogia pideva arenemisega seotult ei jõuta spetsialiste välja koolitada ja neid vajalikul tasemel hoida. Kohtunike jaoks on samuti murekohaks vähene teadlikkus kindlatest tarkvaradest, samuti tunnetatakse vajadust pilveteenuse järele, mis võimaldaks digitaalse tõendiga tutvuda ilma CD-plaati kasutamata.



Joonis 3. Digitaalsete tõendite visuaalse esitlemisega seotud probleemid (2023, autori koostatud)

Neljanda uurimisküsimuse, kuidas saaks parandada digitaalsete tõendite visualiseerimise protsessi, intervjuu vastustes tekib vastuolu. Kui kõige enam mainitumaks probleemiks seoses digitaalsete tõendite visualiseerimisega olid tarkvara probleemid, siis kõige enam mainivad vastajad, et visualiseerimise protsessi parandamiseks aitaks kaasa hoopis paremate tehniliste seadmete kasutusele võtmine. Tehniliste seadmetena toodi välja nii digitahtlild kui ka seadmed, mis aitaks parandada digitaalsete tõendite kvaliteeti ning läbi selle muuta need arusaadavamaks. Viis vastanut leidsid, et tehnilised seadmed võivad tõsta digitaalsete tõendite kvaliteeti, muutes nad paremini esitletavaks. Laialdasem digitahtlilite kasutusele võtmine annaks igal pool võimaluse teha mugavamalt reaalses märkmeid, tuginedes menetlusetoomikus olevatele tõenditele. Siiski leiti, et kui tekib vajadus visualiseeritavat digitaalset tõendit paremini esitleda, kaasatakse sellesse protsessi oma valdkonda tundev digikriminalist või ekspert. Kuna digikriminalist on oma valdkonna spetsialist, oskab ta selgitada visualiseeritavat tõendit nõnda, et menetlusosalised seda

ühtselt mõistaksid. Teoreetilises osas käsitleti samuti sõnaliste selgituste olulisust digitaalsete tõendite esitlemisel, sest sõnalised selgitused aitavad paremini mõista esitletavat digitaalset tõendit ning meelde jätta esitletavat teavet (käesolev töö lk 15). Peale tehniliste seadmete mainisid kolm intervjuueeritavat, et tarkvarad aitaksid digitaalsete tõendite visualiseerimisele kaasa. Viimasena toodi välja koolituste läbiviimine, et inimesed suudaksid mõista digitaalse tõendi erinevaid nüansse ning kuidas oma soovitud tulemust paremini teistele esitleda. Autor jõudis **järeldusteni**, et paremate digitaalsete seadmete kasutusele võtmine võib muuta küll digitaalsete tõendeid kvaliteetsemaks ja usaldusväärsemaks, kuid peamised digitaalsed tõendid tekivad siiski elektrooniliste seadmete kaudu, millele riigiasutusel võib puududa ligipääs. Samuti kvaliteet ei pruugi olla piisavalt hea. Sellisteks seadmeteks võivad olla näiteks inimese enda mobiiltelefon või ööklubi turvakaamera. Kui võtta kasutusele asutusesiselt paremad tehnilised seadmed nagu näiteks digitaalsed arvutid, on võimalik tõendeid paremini esitleda, kuid nende kvaliteet ja usaldusväärsus sõltub tõendite allikast. Lisaks peavad nende kõikide välja toodud lahenduste taga tegutsema pädevad inimesed, kes omavad igakülgset digitaalsete tõendite ja visualiseerimisega seotud kompetentsi. Ülalpool mainitud kokkuvõtte põhjal esitab töö autor Politsei- ja Piirivalveametile, Justiitsministeeriumile ja Siseministeeriumile, kui vastavat valdkonda koordineerivatele asutustele **ettepanekud**:

- Parima praktika juhendi välja töötamine digitaalsete tõendite visualiseerimisel;
- Võtta Politsei- ja Piirivalveametis, prokuratuuris ja kohtutes kasutusele ühetaolised riist- ja tarkvaralised lahendused, et hõlbustada digitaalsete tõendite visualiseerimist;
- Viia läbi eraldi ametkonnasiseseid ja ühiseid ametkondade vahelisi koolitusi ja kohtumisi, et paremini mõista digitaalsete tõendite olemust ja nende visualiseerimist.

KOKKUVÕTE

Tänases ühiskonnas, kus tehnoloogia ja digitaalne maailm areneb väga kiiresti, on digitaalsed tõendid saanud oluliseks menetluspraktika osaks. Digitaalseteks tõenditeks loetakse mistahes digitaalses vormis esinevat teavet, mida on võimalik kasutada kohtus tõendamiseseme asjaolude selgitamisel. Digitaalseteks tõenditeks võivad olla digitaalsetest seadmetest pärit fotod, videod või kirjavahetused, aga ka keerulisemad metaandmed, mille mõistmiseks on vaja eriteadmistega ametnikke. Kuna süüteomenetluste käigus saadud digitaalsetest tõenditest kogutakse erineva teabega andmeid, on keeruline leida universaalset visualiseerimise meetodit, mis selgitaks konkreetset tõendit. Siseministeeriumi värskem „Siseturvalisuse arengukava 2020-2030“ näitab, et nii digitaalsetes, kui ka infoajastu keskkondades on vaja võtta kasutusele uudseid lähenemisi (Siseministeerium, 2021, lk 39). Meie menetlussüsteemi muudetakse aina enam digitaalsemaks, kuid sellest vähem tähtis ei saa olla digitaalsete tõendite mõistmine ja visuaalne esitlemine.

Antud lõputöö eesmärgiks oli leida peamised kitsaskohad digitaalsete tõendite visuaalsel esitlemisel süüteomenetluses ning pakkuda nendele probleemidele lahendusi. Töö teoreetilises osas anti ülevaade digikriminalistikast, digitaalse tõendi olemusest, infotehnoloogilistest vahenditest ja andmekandjatest, digitaalsete tõendite visuaalsest esitlemisest ja sellega seotud probleemidest. Töö empiirilises osas viidi läbi kvalitatiivne uuring, kus andmete kogumise meetodiks oli poolstruktureeritud intervjuu. Valimi moodustasid viis prokurööri, neli kohtunikku ja neli PPA ametnikku üle Eesti, kes kõik on oma ametist tulenevalt kokku puutunud digitaalsete tõenditega ja nende esitlemisega.

Kvalitatiivse uuringu käigus selgus, et kõik vastanud on oma töös kokku puutunud digitaalsete tõendite esitlemisega. Kõige tihedam kokkupuude digitaalsete tõenditega on prokuröridel, kes peavad jälgima, kuidas tõendid on kogutud ning lõpuks integreerivad need enda menetlustoimikusse, et seda kohtule esitada. Hetkel kasutatakse tõendite visualiseerimiseks erinevaid tehnilisi lahendusi, mis võimaldavad tõendeid kuvada seinale või ekraanile. Autor tuli järeldusele, et kõige enam

visualiseeritavaks digitaalseks tõendiks süüteomenetluse praktikas on video-, heli- ja fotofailid. Digitaalsete tõendite esitlemisega seotud probleem, mida kõige enam mainiti, oli tarkvarade puudus ning nende rahaline maksumus. Suurema probleemina nähti ka töötajate vähest teadlikkust ja oskust digitaalsete tõendite käsitlemisel. Kui kõige enam mainitumaks probleemiks seoses digitaalsete tõendite visualiseerimisega olid tarkvara probleemid, siis vastuoluliselt leidsid vastajad, et kõige enam aitaks visualiseerimise protsessi parandamiseks kaasa hoopis paremate tehniliste seadmete kasutusele võtmine. Tehniliste seadmetena toodi välja nii digitahvlid, kui ka seadmed, mis aitaks parandada digitaalsete tõendite esitlemise kvaliteeti ning läbi selle muuta need arusaadavamaks.

Uurimusest saadud vastuste põhjal esitati Politsei- ja Piirivalveametile, Justiitsministeeriumile ja Siseministeeriumile ettepanekud:

- Parima praktika juhendi välja töötamine digitaalsete tõendite visualiseerimisel;
- Võtta Politsei- ja Piirivalveametis, prokuratuuris ja kohtutes kasutusele ühetaolised riist- ja tarkvaralised lahendused, et hõlbustada digitaalsete tõendite visualiseerimist;
- Viia läbi eraldi ametkonnasiseseid ja ühiseid ametkondade vahelisi koolitusi ja kohtumisi, et paremini mõista digitaalsete tõendite olemust ja nende visualiseerimist.

Lõputöös leiti vastused kõigile esitatud uurimisküsimustele ning uurimisprobleemidele, täites sellega lõputöö eesmärgi, milleks oli leida peamised kitsaskohad digitaalsete tõendite visuaalsel esitlemisel süüteomenetluses ning pakkuda nendele probleemidele lahendusi. Töö autor leiab, et antud lõputöös uuringu tulemuste põhjal esitatud ettepanekud aitaksid parandada Politsei- ja Piirivalveameti, prokuratuuri ja kohtu tänast visualiseerimise taset ja võimekust. Lisaks leiab töö autor, et käesolevas lõputöös kajastatud probleemid vajaksid süviti käsitlemist eraldiseisva täiendava uurimistöö raames.

SUMMARY

In today's society, where technology and the digital world are developing very quickly, digital evidence has become an important part of procedural practice. Digital evidence is any information in digital form that can be used in court to explain the circumstances of the subject of evidence. Digital evidence can include photos, videos or correspondence from digital devices, as well as more complex metadata that requires officers with specialized knowledge to understand. Since digital evidence obtained during criminal proceedings collects data with different information, it is difficult to find a universal visualization method that explains a particular piece of evidence. The Ministry of the Interior's latest "Internal Security Development Plan 2020-2030" shows that it is necessary to introduce new approaches in both digital and information age environments (Ministry of the Interior, 2021, p. 39). Our procedural system is becoming more and more digital, but the understanding and visual presentation of digital evidence cannot be less important.

The aim of this thesis was to find the main bottlenecks in the visual presentation of digital evidence in criminal proceedings and to offer solutions to these problems. In the theoretical part of the work, an overview was given of digital forensics, the nature of digital evidence, information technology tools and data carriers, visual presentation of digital evidence and related problems. In the empirical part of the work, a qualitative study was conducted, where the data collection method was a semi-structured interview. The sample consisted of five prosecutors, four judges and four PBGB officials from all over Estonia, all of whom have come into contact with digital evidence and its presentation due to their profession.

During the qualitative research, it was revealed that all respondents have come across the presentation of digital evidence in their work. Prosecutors have the closest contact with digital evidence, who must monitor how the evidence is collected and ultimately integrate it into their case file for presentation in court. At the moment, various technical solutions are used to visualize the evidence, which allow the evidence to be displayed on a wall or screen. The author came to the conclusion that video, audio and photo files are the most visualized digital evidence in the practice of criminal

proceedings. The most cited problem with presenting digital evidence was the lack of software and its financial cost. The lack of awareness and skills of employees in handling digital evidence was also seen as a bigger problem. While software issues were the most cited problem with digital evidence visualization, paradoxically, respondents felt that the use of better technical equipment would help improve the visualization process the most. As technical devices, both digital boards and devices were brought out to help improve the quality of presenting digital evidence and thereby make it more understandable.

Based on the answers received from the research, proposals were submitted to the Police and Border Guard Board, the Ministry of Justice and the Ministry of the Interior:

- Developing a best practice guide for visualizing digital evidence;
- Adopt uniform hardware and software solutions in the Police and Border Guard Board, prosecutor's office and courts to facilitate the visualization of digital evidence;
- Conduct separate intra-agency and joint inter-agency trainings and meetings to better understand the nature of digital evidence and its visualization.

The thesis found answers to all research questions and research problems, thus fulfilling the purpose of the thesis, which was to find the main bottlenecks in the visual presentation of digital evidence in criminal proceedings and to offer solutions to these problems. The author of the work believes that the proposals presented in this thesis based on the results of the study would help to improve the current visualization level and capability of the Police and Border Guard Board, the prosecutor's office and the court. In addition, the author of the work believes that the problems reflected in this thesis need to be addressed in depth in the framework of a separate additional research work.

VIIDATUD ALLIKATE LOETELU

Allen, J. & Hallene, A., 2018. Digital Evidence. *American Journal of Family Law*, 32 (1), pp. 21-24.

Card, S. K., Mackinlay, J. D., Shneiderman, B., 1999. *Readings in Information Visualization: Using Vision To Think*. Burlington: Morgan Kaufmann.

Casey, E., 2010. Digital dust: Evidence in every nook and cranny. *Digital investigation*, 6(3-4), pp. 93-94.

Casey, E., 2011. *Digital Evidence and Computer Crime. Third Edition*. Waltham: Academic Press.

Chen, M., Ebert, D. S., Hagen, H., Laramee, R. S., Liere, R. V., Ma, K.-L. Ribarsky, W., Scheuermann, G. & Silver, D., 2009. Data, Information, and Knowledge in Visualization. *IEEE Computer Graphics and Applications*, 29(1), pp. 1-5.

Data Expert, 2023. *Cellebrite Reader*. [Võrgumaterjal] Leitav: <https://www.dataexpert.eu/products/mobile-forensics-cellebrite/cellebrite-reader/> [Kasutatud 28. 01. 2023].

European e-Justice., 2016. *Kohtukorraldus liikmesriikides Inglismaa ja Wales*. [Võrgumaterjal] Leitav: https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-ew-et.do?member=1%E2%80%9D [Kasutatud 28. 01. 2023].

Euroopa Komisjon, 2019. Recommendation for a council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters. [Võrgumaterjal] Leitav: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070> [Kasutatud 06.02.2023].

Fredesvinda, I., 2007. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study. *Journal of Digital Forensic Practice*, 1 , pp. 285-289.

Garda Síochána Inspectorate., 2015. *Changing Policing in Ireland*. [Võrgumaterjal] leitav: <https://www.gsinsp.ie/wp-content/uploads/2020/01/Changing-Policing-in-Ireland.pdf> [Kasutatud 22. 01. 2023]

Harshita, T., Amarnath, M., 2021. A Comparitve Study of Digital Forensic Tools for Data Extraction From Electronic Devices. *Journal of Punjab Academy of Forensic Medicine & Toxicology*, 21(1), pp. 97-104.

Hales, G., Ferguson, I. & Archibald, J., 2017. Insight: An Application of information Visualisation Techniques to Digital Forensics Investigations. *Intl. Journal on Cyber Situational Awareness*, 2 (1), pp. 1-18.

Hirsjärvi, S., Remes, P. & Sajavaara, P., 2007. *Uuri ja kirjuta*. Tallinn: Medicina.

Justiitsministeerium, 2015. *Kriminaalmenetlusõiguse revisjoni lähteülesanne*. [Võrgumaterjal] Leitav: https://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf [Kasutatud 05. 12. 2022].

Justiitsministeerium, 2021. *Kriminaalmenetlus muutub täielikult digitaalseks* [Võrgumaterjal] Leitav: <https://www.just.ee/uudised/kriminaalmenetlus-muutub-taielikult-digitaalseks-0> [Kasutatud 06.04.2023].

Justiitsministeerium, 2022. *Kohtumenetlus muutub paberivabaks* [Võrgumaterjal] Leitav: <https://www.just.ee/uudised/kohtumenetlus-muutub-paberivabaks> [Kasutatud 06.04.2023].

Kriminaalmenetluse seadustik (2003) RT I 2003, 27, 166.

Laurits, E ., 2016. Criminal procedure and digital evidence in Estonia. *Digital Evidence and Electronic Signature Law Review*, 13, p. 113-120.

Laherand, M.-L., 2008. *Kvalitatiivne uurimisviis*. trükk. Tallinn: OÜ Infotrükk

Lanno, Ü., Rump, M., Rodi, K., Riikoja, A., Mei, Erik., Sadam, M., Ivask, I., Kriiska-Maiväli, K., Rosin, G., Olt, O., Tõns, K., Rebane, H., Randmäe, H., Eskor, L., Kristjankroon, E., Laanet, S., Juhe, A., Rausberg, P., Toomet, M., Saarik, V., Rodes, L., Kaing, H. & Lindmäe, H., 2013. *Kriminalistikaekspertiisid*. Tallinn: Paar OÜ

Leveson, B., 2015. *Review of Efficiency in Criminal Proceedings*. [Võrgumaterjal]
Leitav: <https://www.judiciary.uk/wp-content/uploads/2015/01/review-of-efficiency-in-criminal-proceedings-20151.pdf> [Kasutatud 28. 01. 2022]

Lewulis, P., 2021. Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. *International Journal of Electronic Security and Digital Forensics*, 13(4), pp. 1-19.

Lillis, D., Becker, B, A., O'Sullivan, T. & Scanlon, M., 2016. Current Challenges and Future Research Areas for Digital Forensic Investigation. *Security and Law*, 6, pp. 9-20.

Luuk, M, 2017. *Digitaalsete tõendite kasutamise erisused*. Magistritöö. Tartu: Tartu Ülikool.

Maurer, U., 2004. New approaches to digital evidence. *Proceedings of the IEEE*, 92 (6), pp. 933-947.

Manker, C., 2015. Factors Contributing to Limited Use of Information Technology in State Courtrooms. *Walden Dissertations and Doctoral Studies*, 1, pp. 1-160.

Manlowe, B & Bloomer, A. D., 2006. *Trial Academy Use of Technology in the Courtroom*. Chicago: International Association of Defense counsel.

Mukasey, M.-B., Sedgwick, J.-L. & Hagy, D.-W., 2012. *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. Washington: National Institute of Justice.

Palm, K, 2013. *Digitaalsed tõendid ja nende talletamine Põhja prefektuuri näitel*. *Bakalaureusetöö*. Tallinn: Sisekaitseakadeemia.

- Ploom, T., Koolmeister, I., Kangur, A., Lind, S., Pajula, E. & Sirk, I., 2007. *Väärteomenetluse seadustik. Kommenteeritud väljaanne*. Tallinn: Juura.
- Rempel, E., Hamovitch, L., Zanella, L. & Burke, T.-M., 2019. The power of technology: Examining the effects of digital visual evidence on jurors' processing of trial information. *Applied Cognitive Psychology*, 33 (6), pp. 1288-1295.
- Roussev, V., Quates, C. & Martell, R., 2013. Real-time digital forensics and triage. *Digital Investigation*, 10(2), pp. 158-167.
- R. L. kriminaalasi karistusseadustiku järgi §256 lg 1 järgi (2022) 1-18-437.
- R. L. kriminaalasi karistusseadustiku järgi §184 lg 2¹ järgi (2022) 1-20-1208.
- Schofield, D., 2016. The use of computer generated imagery in legal proceedings. *Digital Evidence and Electronic Signature Law Review*, 13, pp. 1-25.
- Siseministeerium, 2016. *Aruanne „Siseturvalisuse arengukava 2015–2020“ täitmisest 2015. aastal.* [Võrgumaterjal] Leitav: <https://www.siseministeerium.ee/media/233/download> [Kasutatud 25. 10. 2022]
- Siseministeerium, 2015. *Siseturvalisuse arengukava 2015-2020.* [Võrgumaterjal] Leitav: <https://www.siseministeerium.ee/siseturvalisuse-arengukava-2015-2020> [Kasutatud 26. 10. 2022].
- Siseministeerium, 2021. *Siseturvalisuse arengukava 2020-2030.* [Võrgumaterjal] Leitav: <https://www.siseministeerium.ee/stak2030#arengukava-ja-selle-> [Kasutatud 26. 10. 2022].
- Sheppard, K., Fieldhouse, S. -J. & Casella, J. P., 2020. Experiences of evidence presentation in court: an insight into the practice of crime scene examiners in England, Wales and Australia. *Egyptian Journal of Forensic Sciences*, 10 (8), pp. 1-12.
- Solanke, A. A., 2022. Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Proceedings of the Twenty-Second Annual DFRWS USA*. 42, pp. 1-12.

Stoykova, R., 2021. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, pp. 1-20.

Thinnyane, H., Slay, J. & Osborn, G., 2012. Visualizing Information in Digital Forensics. *IFIP Advances in Information and Communication Technology*. 35(47) pp 1-14.

Vallaste, 2023. *Bitt*. [Võrgumaterjal] Leitav: <http://www.vallaste.ee/> [Kasutatud 21. 01. 23]

Vallaste, 2023. *Embedded system*. [Võrgumaterjal] Leitav: <http://www.vallaste.ee/> [Kasutatud 21. 01. 23]

Vallaste, 2023. *log (2)*. [Võrgumaterjal] Leitav : <http://www.vallaste.ee/> [Kasutatud 30.01.23]

Vallaste, 2023. *Metadata* [Võrgumaterjal] Leitav : <http://www.vallaste.ee/> [Kasutatud 30.01.23]

Vallaste, 2023. *MMS (Multimedia Messaging Service)*. [Võrgumaterjal] Leitav: <http://www.vallaste.ee/> [Kasutatud 21. 01. 23]

Vallaste, 2023. *SMS (Short Message Service)*. [Võrgumaterjal] Leitav: <http://vallaste.ee/> [Kasutatud 21. 01. 23]

Vallaste, 2023. *Wireless network*. [Võrgumaterjal] Leitav: <http://www.vallaste.ee/> [Kasutatud 21. 01. 23]

Vincze, E. A., 2016. Challenges in digital forensics. *Police Practice and Research*, 17 (2), pp. 183-194.

Õunapuu, L, 2012. *Valimid kvantitatiivsetes ja kvalitatiivsetes uurimustes*. Tartu Ülikool. [Võrgumaterjal] Leitav: https://dspace.ut.ee/bitstream/handle/10062/27764/ettekavatsetud_valim.html [Kasutatud 20. 01. 2023].

Õunapuu, L, 2014. *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes*. Tartu Ülikool. [Võrgumaterjal] Leitav:

http://dspace.ut.ee/bitstream/handle/10062/36419/ounapuu_kvalitatiivne.pdf
[Kasutatud 06. 01. 2023].

LISA 1. INTERVJUU KÜSIMUSED

(Enne intervjuud selgitatakse intervjuueeritavatele, mida mõeldakse digitaalsete tõendite all ja nende visualiseerimisel.)

1. Kuidas olete kokku puutunud digitaalsete tõenditega ja nende visualiseerimisega?
2. Milliseid digitaalseid tõendeid on teie menetlustes kõige enam visualiseeritud?
3. Milliseid visualiseerimisega seonduvaid probleeme on digitaalsete tõendite esitlemisel tekkinud?
4. Millised küsimused tekivad digitaalsete tõendite visualiseerimisel?
5. Kas eelnevalt välja toodud probleemide lahendamiseks piisaks seletavast sõnastikust, mis selgitaks digitaalsete tõendite olemust?
6. Kuidas hindate praegust digitaalsete tõendite visualiseerimise võimekust?
7. Kuidas näeb välja Teie arvates hea digitaalse tõendi visualiseerimine?
8. Kuidas lisab digitaalsete tõendite visualiseerimine lisaväärtust otsuste langetamisse?
9. Millised on Teie ettepanekud, et parandada digitaalsete tõendite visualiseerimist?